Sécurité de la plateforme Xanadu

Dernière mise à jour: 17/12/2025

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La présente documentation a été traduite pour vous simplifier sa lecture, à l'aide d'un logiciel de traduction. Tous les efforts possibles ont été déployés pour fournir une traduction précise, toutefois, la traduction automatique ne peut en aucun cas remplacer les traducteurs humains. La traduction est fournie « en l'état ». Aucune garantie, quelle qu'elle soit, express ou implicite, n'est fournie concernant la précision, la fiabilité ou l'exactitude des traductions, quelle que soit la langue cible. En raison des limites inhérentes au logiciel de traduction, certaines traductions du contenu peuvent ne pas être exactes. La langue officielle de la présente documentation est l'anglais Toute déviation ou différence générée par la traduction ne peut en aucun cas être considérée comme juridiquement contraignante, et ne pourra avoir d'effet juridique sur la conformité ou l'application des dispositions de la documentation.

Certains des exemples et graphiques présentés ici sont fournis à des titres d'illustration uniquement.ªucune association ou connexion réelle à des produits ou services ServiceNow n'est voulue et ne devrait être inférée.

ServiceNow, le logo ServiceNow, Now et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays. Les autres sociétés et noms de produits peuvent être des marques commerciales des sociétés respectives avec lesquelles ils sont associés.

Veuillez lire les Conditions d'utilisation du site Web de ServiceNow à l'adresse www.servicenow.fr/terms-of-use.html

Traduction automatique

Siège social de la société
2225 Lawson Lane
Santa Clara, CA 95054
États-Unis
(408) 501-8550

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sommaire

Sécuriser votre instance **10**

ServiceNow Vault **12**

Sécurité de la plateforme **15**

Centre de sécurité 17

Vue d'ensemble 19

Sécurisation renforcée de la sécurité 20

Scanner de sécurité 26

Mesures de sécurité 32

Actions du client 39

Bonnes pratiques de sécurité 42

Apprentissage de la sécurité 47

Annonces de bannières de sécurité 48

Tableaux de bord sur la posture de sécurité 48

Notifications des événements de sécurité 51

Centre de sécurité de l'instance 56

Centre de sécurité de l’instance vers ServiceNow Centre de sécurité migration 66

Surveiller les événements de sécurité 68

Vérifier le score de conformité quotidien et configurer les paramètres de propriété de sécurité 74

Rechercher des définitions de sécurité incorrectes 84

Mesures d’instance de surveillance 85

Activer l’interface ISC Agent virtuel 98

Paramètres de la sécurisation pour la sécurité de l'instance 99

Paramètres de sécurisation renforcée 201

Base de référence des paramètres de sécurisation renforcée 202

Contrôle d'accès 225

API et service web 275

Architecture, conception et modélisation des menaces 290

Authentification 299

Logique métier 328

Communications 331

Configuration 336

Protection des données 347

Gestion et enregistrement des erreurs 351

Fichier et ressources 358

Code malveillant 366

Gestion des sessions 368

Cryptographie stockée 382

Validation, nettoyage et codage 383

Service d'exportation de journal (LES) 417

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Service d'exportation de journal rôles....419
Sources du journal....421
Créer une configuration de source de journal....421
Consommateur Kafka....423
Consommateur de MID Server....427
Rapport du journal d'examen....433
Journaux....435
Journaux système....436
Journalisation, audit et erreurs....451
Gestion des secrets....452
Exploration de la gestion des secrets....453
Configuration des secrets accessibles aux clients....458
Tableau de bord de gestion des secrets....476
Signature de code....487
Explorer la signature de code....491
Configuration de la signature de code....493
Utilisation de la signature de code....515
Référence de signature de code....530
Analyse anti-virus....536
Exploration de l'analyse antivirus....538
Configurer Analyse anti-virus....539
Examen des fichiers mis en quarantaine....540
Connaître les attributs de dictionnaire pour Analyse anti-virus....541
Assainisseur HTML....542
Exploration de l'assainisseur HTML....543
Configuration de l'assainisseur HTML....546
Activation de l'assainisseur HTML....547
Audit....548
Explorer l'audit....550
Configuration de l'audit pour une table....553
Affichage des tables Audit système et Changement de relation d'audit....555
Connaître les ensembles d'historique....556
Paramètres de sécurité élevée....568
Exploration des paramètres de sécurité élevée....569
Configuration de la propriété du bac à sable de script....581
Activation des paramètres de sécurité élevée....585
VPN (Virtual Private Network)....588
Explorer le réseau privé virtuel (VPN)....589
Activation d'un service VPN....592
Configuration d'une adresse pour la communication VPN....592
Autres paramètres et ressources de sécurité....592
[store-future: BEGIN review]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés des paramètres de sécurité....593
Guide de déploiement sécurisé du MID Server....599
Comportement réversible....604
Propriétés de sécurité déconseillées....604
Utilisation du contrôle d'accès au contenu JavaScript....605
Autres ressources de sécurisation renforcée....607
[End]
Confidentialité de la plateforme....608
Confidentialité des données....609
Exploration de la confidentialité des données....610
Séparation de domaine et confidentialité des données....611
Types de champs pris en charge pour l'anonymisation....612
Rôles Confidentialité des données....613
Confidentialité des données (classique)....614
Confidentialité des données....626
Détection de données....632
Explorer Détection de données....633
Activer Détection de données....635
Classer les données dans Détection de données la page Résultats....635
Détection de données Emplois....636
Détection de données rôles....644
Détection de données Résultats des tâches....646
Détection de données Types de données pris en charge....648
Numérisation avec configuration granulaire....649
Data Classification....651
Exploration de la classification des données....653
Installation des données de démonstration du module d'extension Data Classification....654
Création de classifications des données....656
Affectation de classifications de données à des entrées de dictionnaire....657
Analyser les classifications de données à l'aide du tableau de bord Vue d'ensemble....658
Séparation de domaine et Data Classification....660
Anonymisation des données....661
Créer des techniques d'anonymisation....661
Créer des politiques d'anonymisation....664
Créer une tâche d'anonymisation....668
Activer les tâches parallèles pour l'anonymisation des données....672
Chiffrement....673
Key Management Framework....674
Explorer le cadre de gestion des clés....675
[store-future: BEGIN review]
[End]
Offre groupée d'abonnements pour Encryption and Key Management....677

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comprendre le cadre de gestion des clés....678
Actions de gestion des clés....710
Importer une clé à partir d'un service Web....713
Intégrité de Key Management Framework....716
Préparer votre instance pour la dépréciation de GlideEncrypter....717
Déconseiller l'utilisation de 3DES par GlideEncrypter pour les champs password2....719
Échange de ressources du cadre de travail de gestion des clés....721
Sécurité de l'infrastructure....729
Chiffrement Password2 avec Key Management Framework (KMF)....731
Certificats....734
Exploration des certificats....735
Génération d'un certificat client LDAP....737
Chargement d'un certificat dans une instance....739
Chiffrement au niveau des colonnes....740
Explorer Chiffrement au niveau des colonnes....741
Configuration de Chiffrement au niveau des colonnes....744
Utilisation du chiffrement au niveau des colonnes....748
Chiffrement au niveau des colonnes – Entreprise....777
Chiffrement dans le cloud avec la gestion des clés....781
Opérations de gestion des clés....783
Politique de contrôle du quorum....791
Transactions de gestion des clés....796
Journalisation de Chiffrement dans le cloud....798
Détection de sabotage....800
Chiffrement intégral du disque....803
Chiffrement Edge....804
Explorer Chiffrement Edge....806
Planification pour Chiffrement Edge....818
Installation de Chiffrement Edge....827
Mise à niveau de Chiffrement Edge....878
Configuration de Chiffrement Edge....886
Chiffrement de la base de données....943
Exploration du chiffrement de base de données....945
Demande de rotation de clé de base de données....946
Chiffrement de la base de données avec commutateur contrôlé par le client....947
Gestion des accès....949
Accès zéro confiance....950
Exploration de l'accès zéro confiance....951
Activation de l'accès zéro confiance....953
Configuration du rôle d'accès à la session....954
Propriétés système d'accès Zero Trust....955
Tutoriel : Utiliser l'accès zéro confiance....958

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accès zéro confiance pour mobile 962
Domain Separation pour les fournisseurs de services 964
Explorer la séparation de domaine 966
Prise en charge par les applications pour Domain Separation 985
Pratiques recommandées de séparation de domaine pour les fournisseurs de services 994
Aide de Domain Separation 1036
Configuration et administration de Domain Separation 1038
Centre Séparation en domaines 1071
Authentification 1079
Authentification adaptative 1082
Authentification API 1141
Politique d'accès API 1153
Authentification basée sur certificat 1179
Association d'URL personnalisées à votre instance 1187
Sorties d'installation 1195
Authentification basée sur la plage IP 1197
Intégration LDAP 1200
Sessions simultanées limites 1267
Authentification locale 1271
Authentification multifacteur (MFA) 1298
Authentification unique (SSO) de plusieurs fournisseurs 1353
Authentification entrante et sortante OAuth 1444
S'inscrire automatiquement dans l'instance ServiceNow 1484
Authentification basée sur un jeton (connexions de l'utilisateur) 1495
Sécurité des services Web 1508
Règles de la liste de contrôle d'accès 1514
Exploration des listes de contrôle d'accès 1515
Configuration d'une règle ACL 1534
Gestionnaire de sécurité contextuelle 1539
Configuration ACL avancée 1544
Attributs de sécurité 1556
Notions fondamentales des attributs de sécurité 1557
Créer des attributs de sécurité 1557
Champ d'application de l'attribut de sécurité 1560
Rôles et restrictions de requête de champ 1561
Configurer un rôle de requête de champ 1561
Configurer les restrictions de requête de champ 1562
Filtration des données 1562
Exploration de la filtration des données 1563
Activation de la filtration des données 1566
Création de règles de filtrage des données 1566
Création de critères de sujet 1569

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Débogage de filtration de données....1573
Rôles de sécurité....1574
Explicit Roles....1575
Rôles à privilèges élevés....1583
Connexions et informations d'identification....1585
Explorer les informations d’identification, les connexions et les alias....1586
Mise en route des connexions....1602
Introduction aux informations d'identification....1613
Algorithmes d'authentification....1703
Contrôle d'accès ServiceNow®....1714
Explorer le ServiceNow® contrôle d’accès....1715
Activation du contrôle d’accès ServiceNow®....1718
Configuration ServiceNow® du contrôle d’accès....1720
Journalisation d’audit....1722
Identité....1723
Analyseur d'accès....1724
Exploration d’Access Analyzer....1725
Utilisation de l’analyseur d’accès....1726
Évaluation de l’autorisation....1747
Forum aux questions....1749
Simulateur d'accès....1755
Identité globale....1768
Exploration de l’ID fédéré....1770
Accéder aux critères d’ID fédéré....1771
Mise à jour des champs d’ID....1772
Identity Center....1773
Explorer Identity Center....1775
Activation d’Identity Center....1775
Identity Center pour les utilisateurs....1775
Mesures d’identité pour les administrateurs....1779
Système de gestion des identités entre domaines (SCIM)....1779
Fournisseur SCIM....1780
Client SCIM....1800
Audit d'identité et d'accès....1818
Exploration de l’audit d’identité et d’accès....1820
Résultats de l’audit d’identité....1821
Champs auditables de sécurité....1825
Champs pris en charge et non pris en charge pour l’accès à l’identité et l’audit....1829
Accéder à l’observateur....1831
[store-future: BEGIN review]
Configurer l’observation relative à l’accès....1831
Examiner les journaux de l’observateur d’accès....1832

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

[End]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécuriser votre instance

Sécurité de la plateforme fournit des options pour sécuriser l'instance.

ServiceNow Vault



Utilisez les outils de sécurité des données du produit

ServiceNow Coffre-fort

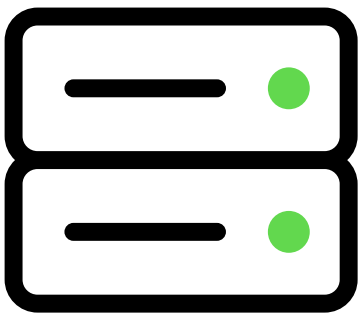
pour protéger les informations sensibles contre tout accès non autorisé, endommagement ou vol tout au long de leur cycle de vie.

Sécurité de la plateforme



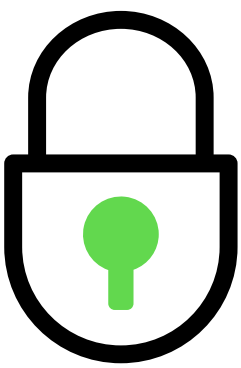
Sécurité de la plateforme fournit des options pour sécuriser l'instance.

Confidentialité de la plateforme



Confidentialité de la plateforme vous permet de masquer la date sensible sur l'instance.

Chiffrement



Protégez vos données sensibles et restez en conformité avec les exigences et les normes réglementaires.

Gestion des accès



Gestion d'accès vous permet d'accéder à l'instance

ServiceNow®

en toute sécurité.

Identité



En savoir plus sur les identités dans l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signature de code



La signature de code crée des signatures numériques pour les données qui sont vérifiées ultérieurement pour confirmer l’authenticité et l’intégrité des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Vault

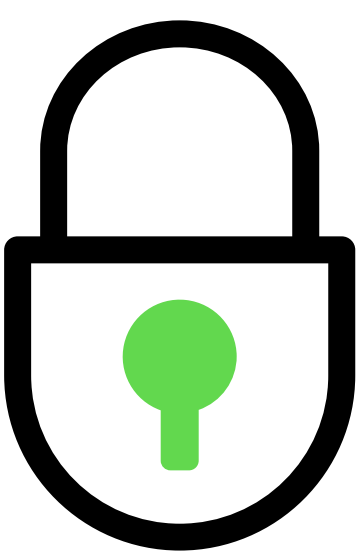
Utilisez les outils de sécurité des données du produit ServiceNow Coffre-fort pour protéger les informations sensibles contre tout accès non autorisé, endommagement ou vol tout au long de leur cycle de vie. Appliquez des protections telles que le chiffrement, la gestion des secrets et la confidentialité des données pour la rédaction et l'audit des informations sensibles. La page d'accueil de ServiceNow Coffre-fort constitue un emplacement unique pour rechercher des produits de sécurité des données ServiceNow Coffre-fort et y accéder.

ServiceNow Coffre-fort est un module d'extension payant que le personnel ServiceNow doit activer sur votre instance de production. ServiceNow Coffre-fort inclut les composants répertoriés ici.

Pour acheter un abonnement, contactez votre chargé de compte ServiceNow. Lorsque vous achetez un abonnement, certains modules d'extension sont activés automatiquement. Si après avoir acheté un module d'extension, celui-ci n'est pas automatiquement activé, vous pouvez l'activer manuellement via la liste **Toutes les applications** de votre instance.

Composants ServiceNow Coffre-fort

Chiffrement



Gestion des clés et chiffrement au niveau des colonnes est une suite de modules de chiffrement hautement configurables

Gestion des secrets



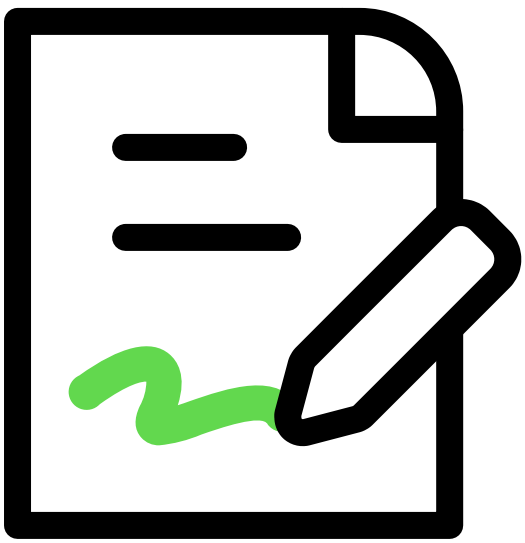
Solution pour remplacer tous les secrets codés en dur, tels que les mots de passe, les certificats et les clés API, sur la plateforme par la garde des secrets par le client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

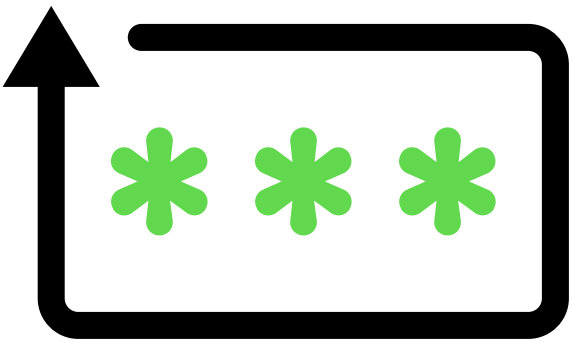
servicenow

Signature de code



Améliorez la sécurité en validant les scripts et les données de configuration d'application sensibles avant leur utilisation.

Confidentialité des données



Utilisez le module d’extension Confidentialité des données pour supprimer les informations personnellement identifiables (PII) des données utilisateur lors de la migration de ces données d’une instance de production vers une instance de non-production.

Détection de données



Journaux



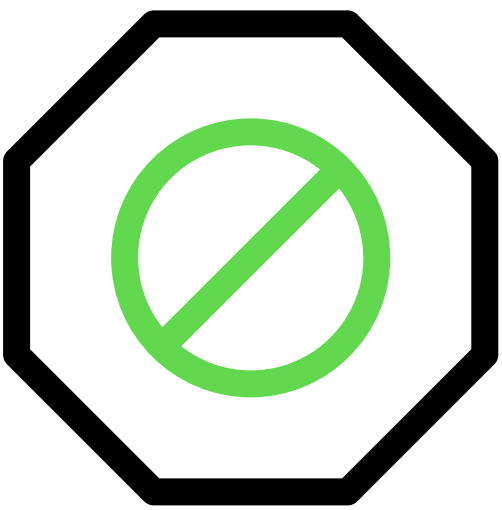
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le module d’extension Découverte de données vous permet de trouver des informations personnellement identifiables (PII) à partir des données utilisateur. Les données peuvent ensuite être classées pour d'autres mesures de sécurité.

Améliorez la sécurité, les performances et l’expérience utilisateur en important des données de journal ServiceNow dans l’analyse de [qa: BEGIN review][End]journaux d’entreprise à l’aide du service d’exportation de journaux.

Accès zéro confiance



[qa: BEGIN review][End]L’accès à la session ServiceNow permet aux organisations de réduire dynamiquement les privilèges des utilisateurs dans une session Web

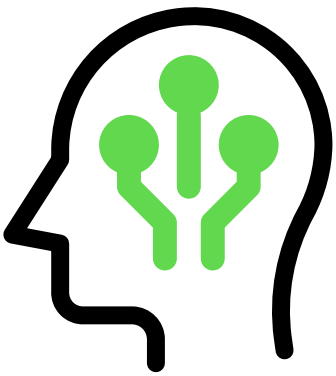
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécurité de la plateforme

Sécurité de la plateforme fournit des options pour sécuriser l'instance.

Centre de sécurité



Permettez aux administrateurs de maintenir en permanence le plus haut niveau de posture de sécurité et surveillez facilement les événements et comportements non sécurisés.

Paramètres de sécurisation renforcée



Le

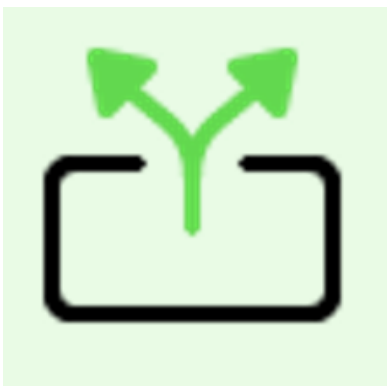
ServiceNow, Inc.

contenu des paramètres de sécurisation renforcée du Centre de sécurité contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans le

Now Platform

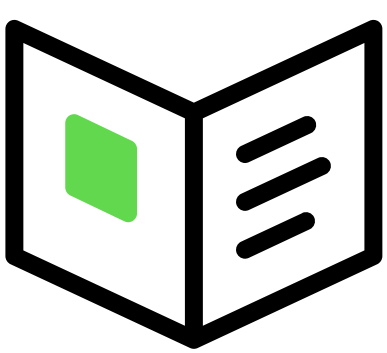
. Vous pouvez définir ces propriétés à l'aide de l'application Paramètres de sécurisation renforcée dans le Centre de sécurité.

Service d'exportation de journaux



Le service d'exportation de journaux (LES) vous permet d'exporter de manière transparente vos journaux d'instance, de système et d'application vers les outils d'analyse de sécurité de votre entreprise. Le service fournit une intégration hautement évolutive et presque en temps réel avec vos outils d'analyse, facile à configurer et à gérer.

Journaux



Gestion des secrets



Signature de code



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le module Journaux fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Utilisez ServiceNow Gestion des secrets pour une gestion granulaire de l'accès à vos mots de passe en fonction des besoins de votre entreprise.

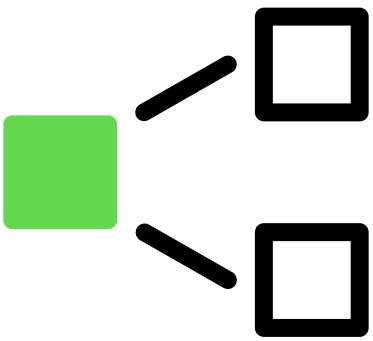
La signature de code crée des signatures numériques pour les données qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données.

Options d'analyse antivirus



Utilisez cette fonction Analyse anti-virus pour protéger votre instance contre les infections de virus qui peuvent être introduites par des pièces jointes dans vos enregistrements système, telles que les incidents, les problèmes et les stories.

Assainisseur HTML



Supprimez tout code indésirable et protégez-vous contre les problèmes de sécurité tels que les attaques de script site à site en assainissant le balisage HTML dans les champs HTML et les champs HTML traduits.

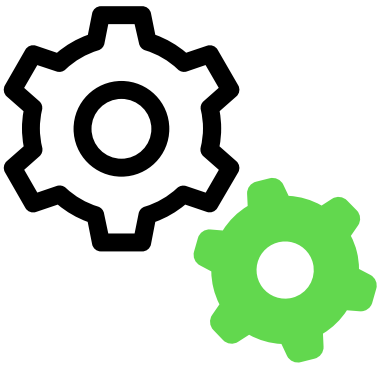
Audit



Suivez les modifications d'enregistrement sur les tables activées devant faire l'objet d'un audit. Par défaut, le système suit les modifications apportées aux tables d'incidents, de changements et de problèmes, entre autres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de sécurité élevée	VPN (Virtual Private Network)	Autres paramètres et ressources de sécurité
		
Les paramètres de sécurité élevée désignent plusieurs options de sécurité disponibles dans votre instance.	Utilisez un réseau VPN pour intégrer votre instance à des sources de données externes sur Internet.	Définissez des propriétés de sécurité en dehors d'Instance Security Center ainsi que d'autres ressources liées à la sécurité.

Centre de sécurité

ServiceNow Centre de sécurité est une application qui se compose d'un ensemble d'outils conçus pour aider votre organisation à maintenir la sécurité de vos déploiements ServiceNow. À l'aide du Centre de sécurité, vous pouvez améliorer la posture de sécurité et renforcer les niveaux de conformité avec une expérience utilisateur transparente.

Security Center est une application gratuite que les administrateurs système peuvent télécharger à partir du ServiceNow Store. Il est installé par défaut à partir de la version Vancouver. Il est également disponible dans le ServiceNow Store tous les trimestres, entre les versions de famille, pour faciliter l'adoption plus rapide de nouvelles fonctionnalités.

Important :
Centre de sécurité de l'instance (ISC) atteindra la fin des ventes d'ici septembre 2024. ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour en savoir plus, Centre de sécurité de l'instance vers ServiceNow Centre de sécurité migration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Page d'accueil



Affichez votre score de conformité à la sécurisation renforcée en pourcentage, analysez les principaux paramètres de sécurisation renforcée non conformes à corriger et affichez les résultats de vos analyses de sécurité.

Sécurisation renforcée de la sécurité



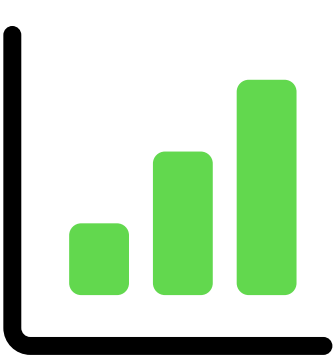
Découvrez comment les configurations de sécurisation renforcée sont conformes aux recommandations de sécurité de ServiceNow

Scanner de sécurité



Effectuer une analyse par rapport à un ensemble de contrôles de sécurité pour identifier les mauvaises configurations et les comportements non sécurisés

Mesures de sécurité



Surveillez plus de 50 mesures différentes qui aident à identifier les menaces de sécurité potentielles.

Antivirus



Affiche la tendance à laquelle les événements se produisent sur les fichiers potentiellement infectés.

Apprentissage de la sécurité



Un référentiel central de ressources de sécurité donnant accès aux documents de sécurité et de conformité ServiceNow.

Traduction automatique

Rôles d'utilisateur

Pour utiliser le Centre de sécurité, vous devez disposer de l'administrateur ou sn_vsc.security_center_viewer.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis	Utilisateur	Avantages
administrateur	Ce rôle accorde l'accès à l'ensemble des données, fonctions et fonctionnalités système, car les administrateurs ont la possibilité de remplacer les règles de liste de contrôle d'accès (ACL) et de contourner toutes les vérifications de rôles. Évitez d'affecter ce rôle à vos utilisateurs lorsque des rôles plus spécifiques sont disponibles.	Utilisez les outils du centre de sécurité pour améliorer la posture de sécurité de l'instance et surveiller les comportements liés à la sécurité.
sn_vsc.security_center_viewer	Ce rôle permet aux utilisateurs non-administrateurs d'accéder aux informations dans le centre de sécurité, mais il les empêche de modifier les outils du centre de sécurité ou d'apporter des changements à la configuration de l'instance. Par exemple, les propriétaires de plateformes, les analystes des opérations de sécurité ou les personnes concernées par la conformité peuvent avoir besoin d'accéder à certains indicateurs clés de performance (KPI) de sécurité, aux informations de sécurité et aux supports d'apprentissage de sécurité disponibles dans le centre de sécurité.	Gagnez en visibilité sur les outils du centre de sécurité pour surveiller la posture de sécurité de l'instance et surveiller les comportements de sécurité.

Traduction automatique

Premiers pas

- Centre de sécurité est inclus dans toutes les versions familiales à partir de Vancouver.
- Lisez la documentation du produit, en commençant par Vue d'ensemble.
- Terminez le cours de formation technique et de certification (TACO) pour Centre de sécurité.

Vue d'ensemble

Obtenez un résumé rapide de la posture de sécurité de votre instance sur la page de vue d'ensemble. Affichez votre score de conformité à la sécurisation renforcée en pourcentage,

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

découvrez les tendances graphiques de votre score de conformité, analysez les principaux paramètres de sécurisation renforcée non conformes à corriger et consultez les résultats de vos analyses de sécurité.

Le score de conformité à la sécurisation renforcée est un pourcentage qui indique dans quelle mesure vos paramètres de sécurité s'alignent sur les paramètres recommandés. Le récapitulatif du score de conformité à la sécurisation renforcée affiche ce pourcentage et les données associées aux changements récents du score. Utilisez le graphique de tendance du score de conformité à la sécurisation renforcée pour voir comment votre score de conformité a changé au fil du temps.

Améliorez votre score de conformité en utilisant les paramètres de sécurisation renforcée non conformes les plus fréquents. Cette liste affiche les 10 paramètres de sécurisation renforcée qui ont le plus d'impact négatif sur votre score de conformité à la sécurisation renforcée. Cette visibilité vous aide à classer par ordre de priorité les paramètres de sécurisation renforcée à corriger.

La section Résumé de l'analyse de sécurité affiche des graphiques à barres, qui reflètent le nombre de résultats au fil du temps pour chacune de vos analyses de sécurité.

1. Accédez au graphique de tendance du score de conformité à la sécurisation renforcée via la page de vue d'ensemble ou en naviguant vers **Sécurisation renforcée** > **Tendance des scores**.
2. Sélectionnez **Passer en revue la tendance du score** pour personnaliser la période et sélectionner des points sur la ligne de tendance à analyser.
3. Dans la section Synthèse de l'analyse de sécurité, sélectionnez une barre pour accéder à la page des résultats d'analyse de cette suite d'analyse.

Sécurisation renforcée de la sécurité

Utilisez l'outil de sécurisation renforcée du Centre de sécurité pour afficher votre score de conformité à la sécurisation renforcée, le comparer aux scores précédents et modifier les paramètres afin d'améliorer votre score de conformité et votre posture de sécurité.

Spécifiez les Paramètres de sécurisation renforcée valeurs recommandées pour les propriétés et modules d'extension liés à la sécurité dans la Now Platform. L'outil de sécurisation renforcée calcule le score de conformité du paramètre de sécurisation renforcée en pourcentage. Ce nombre indique le niveau de conformité de votre instance avec les paramètres de sécurisation renforcée du Centre de sécurité.

Formule de calcul du score de conformité à la sécurisation renforcée :

- Chaque paramètre de sécurisation renforcée a un score de risque compris entre 0 et 10.
- Le score est égal à la somme de tous les scores de risque de conformité divisée par la somme de tous les scores de risque.

Par exemple, si la somme de tous les scores de risque de conformité est de 25,4 et que le total de tous les scores de risque est de 34,9, le score de conformité sera (25,4/34,9) × 100, ce qui équivaut à 72,7. Cette décimale est arrondie au nombre entier le plus proche et sera donc égale à 73.

Ce calcul est effectué automatiquement le premier jour du mois, ou après une installation ou une réinstallation de ServiceNow Security Center.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison des scores de sécurisation renforcée

Gagnez en visibilité sur l'intégrité de vos paramètres de sécurisation renforcée et utilisez ces données pour améliorer la posture de sécurité de votre instance.

La page de comparaison des scores de sécurisation renforcée affiche tous les paramètres de sécurisation renforcée dont l'état de conformité a été modifié entre la première et la deuxième date, ainsi que leur impact sur le score de conformité à la sécurisation renforcée. Par exemple, si un paramètre est passé de conforme à non conforme, le score aura diminué.

Pour afficher les résultats de ces changements, entrez une date antérieure et une date récente dans le sélecteur de date en haut à droite de la page, puis sélectionnez Comparer. Vous trouverez ci-dessous une explication de chaque carte :

- Score de conformité à la sécurisation renforcée : affiche le score de conformité de votre instance sous forme de pourcentage pour les première et deuxième dates que vous avez sélectionnées.
- Impact du score des paramètres changés par priorité : affiche le nombre de paramètres de sécurisation renforcée dont l'état de conformité a changé entre les deux dates, organisé par valeur de priorité.
- Impact du score des paramètres changés par domaine de sécurité : affiche le nombre de paramètres de sécurisation renforcée qui ont changé l'état de conformité entre les deux dates, organisé par domaine de sécurité.
- Paramètres de sécurisation renforcée modifiés : affiche la liste des paramètres de sécurisation renforcée qui ont modifié les statuts de conformité entre les deux dates. Vous pouvez examiner les paramètres qui ne sont plus conformes et qui ont diminué votre score de comparaison de sécurisation renforcée pour voir s'il est possible de les rendre conformes afin d'augmenter votre score. Consultez Augmenter le score de conformité à la sécurisation renforcée.

Par exemple, dans la capture d'écran suivante, le score de conformité a augmenté, ce qui indique que la posture de sécurité s'est améliorée pendant cette durée.



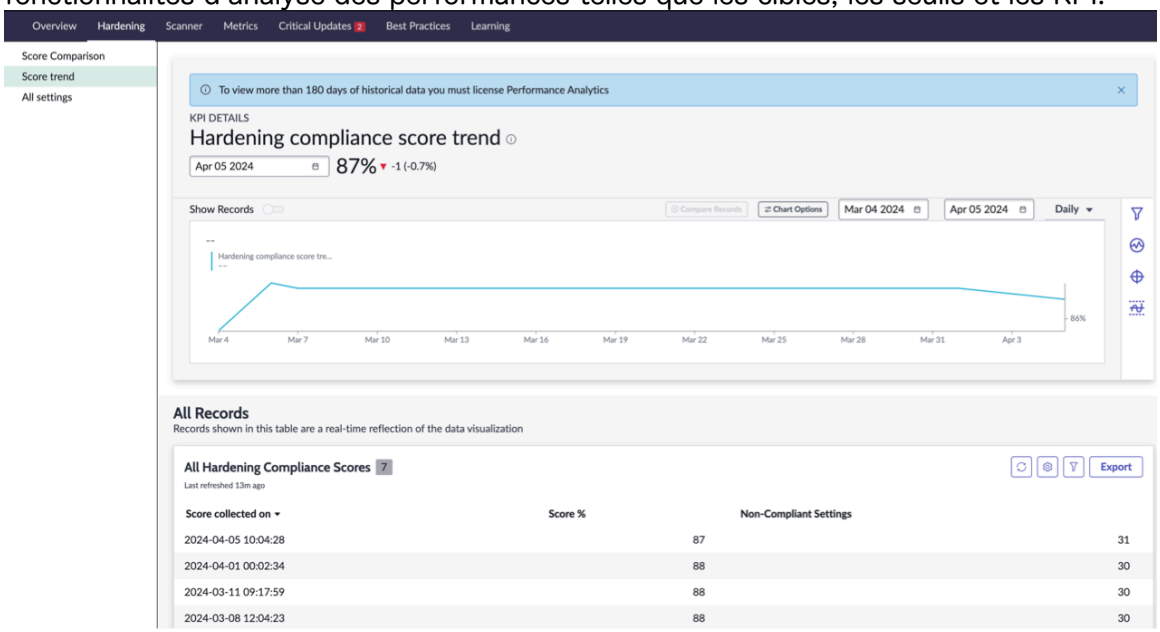
Tendance du score de conformité à la sécurisation renforcée

Affichez les tendances du score de conformité à la sécurisation renforcée sur une période donnée dans un graphique ou un tableau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Consultez les tendances de votre score de conformité sur une période donnée. Utilisez le sélecteur de date pour sélectionner une période à analyser, puis obtenez des informations plus approfondies sur les données en appliquant des fonctionnalités d'analyse des performances telles que les cibles, les seuils et les KPI.



Options de graphique : sélectionnez **Options de graphique** pour effectuer une analyse, afficher les séries chronologiques et afficher les données dans plusieurs types de graphiques.

Analyse

- Cible : les objectifs que votre organisation souhaite atteindre. Consultez Performance Analytics targets .
- Seuil : définit une plage normale de scores pour un indicateur et vous alerte lorsque certains événements se produisent. Consultez Performance Analytics thresholds .
- Prévision : décrit la capacité à prévoir les scores futurs en fonction du comportement passé. Consultez Performance Analytics scores forecasts .
- Tendance : montre comment la valeur d'un ou de plusieurs éléments change dans le temps.
- Commentaires : affiche des annotations sur des points de données individuels.
- Étiquettes : affiche les scores associés aux visualisations.
- Statistiques : affiche les statistiques relatives à votre score de conformité.

Séries chronologiques

- Score : score du KPI.
- Changement : changement de score pour cet indicateur.
- Pourcentage de changement : pourcentage de changement de scores.

Types de graphiques : reportez-vous à la section Time series visualization type use cases .

Table Tous les enregistrements

La table Tous les enregistrements affiche la date à laquelle les scores de conformité ont été collectés, les pourcentages de score et le nombre de paramètres non conformes. Vous

Traduction automatique

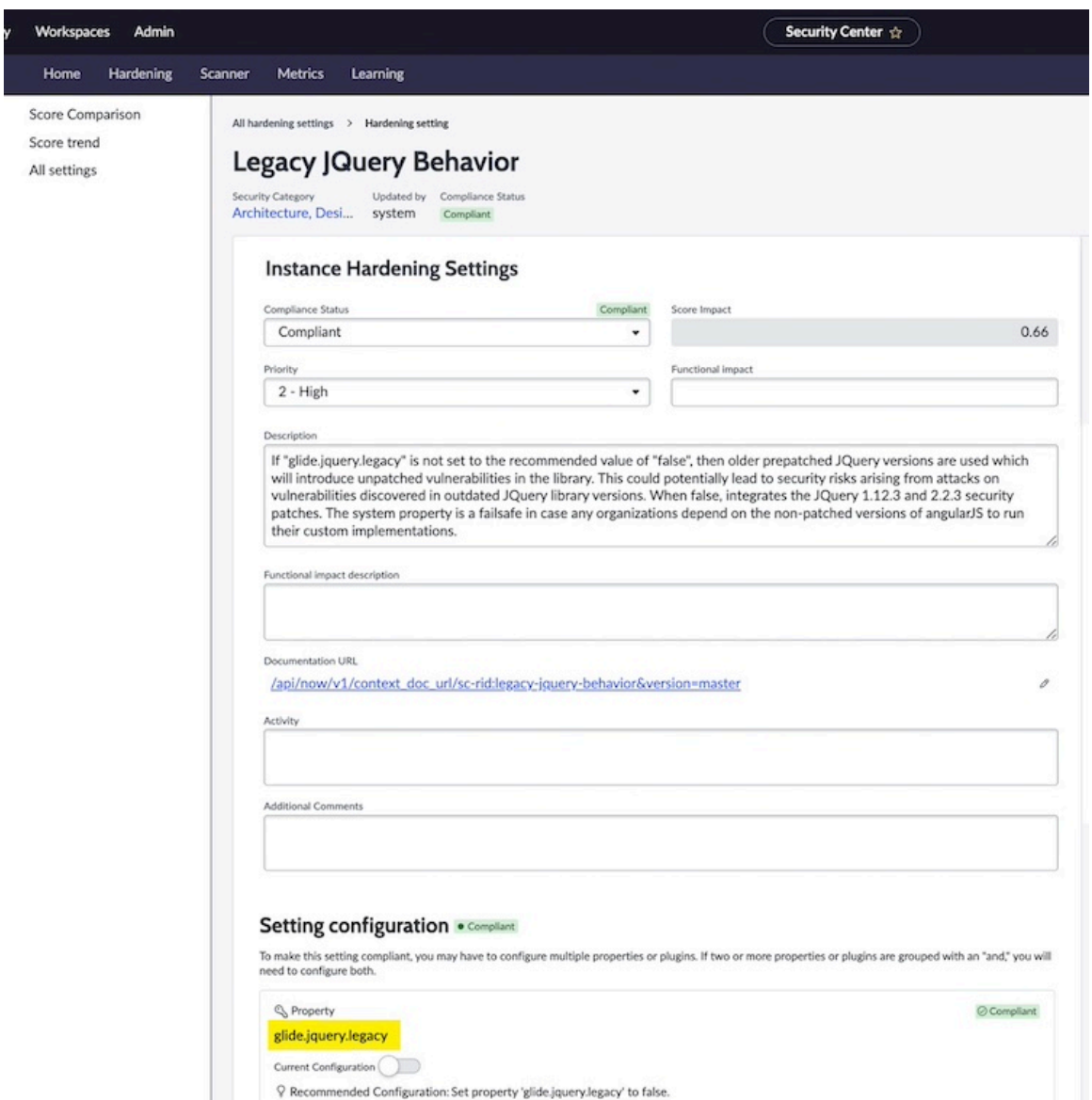
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pouvez utiliser cette table comme une autre option pour analyser la posture de sécurité de votre instance au fil du temps.

Détails des paramètres de sécurisation renforcée

Analysez les détails d'un paramètre de sécurisation renforcée en sélectionnant son lien dans l'application Centre de sécurité.

Accédez à la **Sécurisation renforcée** > **Tous les paramètres**, puis sélectionnez un paramètre de sécurisation renforcée pour être redirigé vers une page de l'outil de configuration renforcée qui affiche ses informations relatives à la sécurité.



Détails de configuration des paramètres de sécurisation renforcée

Attribut de configuration	Description
Statut de la conformité	Indique si le paramètre de sécurisation renforcée est conforme ou non.
Impact du score	Un pourcentage qui indique l'impact de ce paramètre de sécurisation renforcée sur votre posture de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de configuration des paramètres de sécurisation renforcée (suite)

Attribut de configuration	Description
Priorité	Un nombre compris entre 1 et 4, 1 ayant le poids le plus important qui indique la force de l'impact de ce paramètre de renforcement sur votre posture de sécurité.
Impact fonctionnel	L'impact de ce paramètre de sécurisation renforcée sur le fonctionnement de votre instance.
Description	Un aperçu général du paramètre de durcissement.
Documentation Url	Lien vers la documentation du paramètre de sécurisation renforcée.
Activité	Notifications de mises à jour liées au paramètre de sécurisation renforcée.
Configuration des paramètres	Détails relatifs à l'état de conformité de votre paramètre de sécurisation renforcée ainsi que des instructions sur la façon de les rendre conformes. **Remarque :** Certains paramètres de sécurisation renforcée peuvent vous obliger à configurer plusieurs propriétés et modules d'extension pour les rendre conformes.

Augmenter le score de conformité à la sécurisation renforcée

Augmentez votre score de conformité à la sécurisation renforcée en vous assurant que les paramètres de sécurisation renforcée sont conformes aux recommandations du système.

Avant de commencer

Rôle requis : administrateur

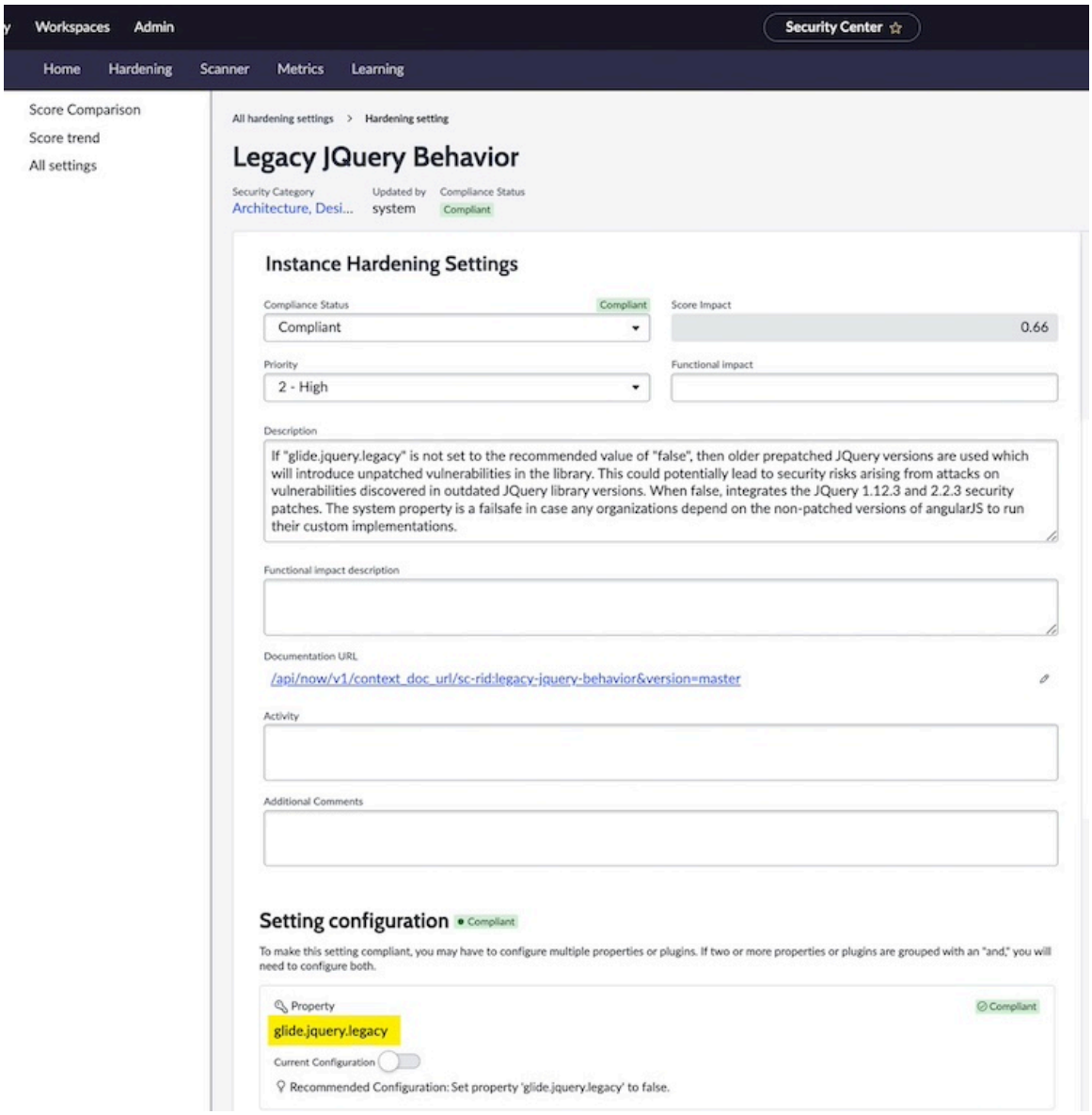
Identifiez les paramètres de sécurisation renforcée non conformes ayant l'impact le plus élevé sur votre instance. Examinez-les pour voir si vous pouvez vous conformer aux recommandations système afin d'augmenter votre score de conformité global.

Procédure

1. Accédez à la **Sécurisation renforcée** > **Tous les paramètres**.
2. Filtrez la colonne État de conformité pour afficher uniquement les paramètres de sécurisation renforcée non conformes.
3. Sélectionnez **Impact du score** pour trier du plus grand au plus petit.
4. Sélectionnez les paramètres et examinez les détails des paramètres pour décider si vous souhaitez vous conformer aux recommandations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Assurez-vous que le paramètre de durcissement est conforme.
6. Si vous mettez à jour un score de sécurisation renforcée non conforme pour le rendre conforme, accédez à la page d'accueil et sélectionnez **Mettre à jour le score** pour afficher le score le plus récent.
   Le score de sécurisation renforcée est arrondi à l'unité supérieure. Un score de 86,75 % sera arrondi à 87.

Tous les paramètres

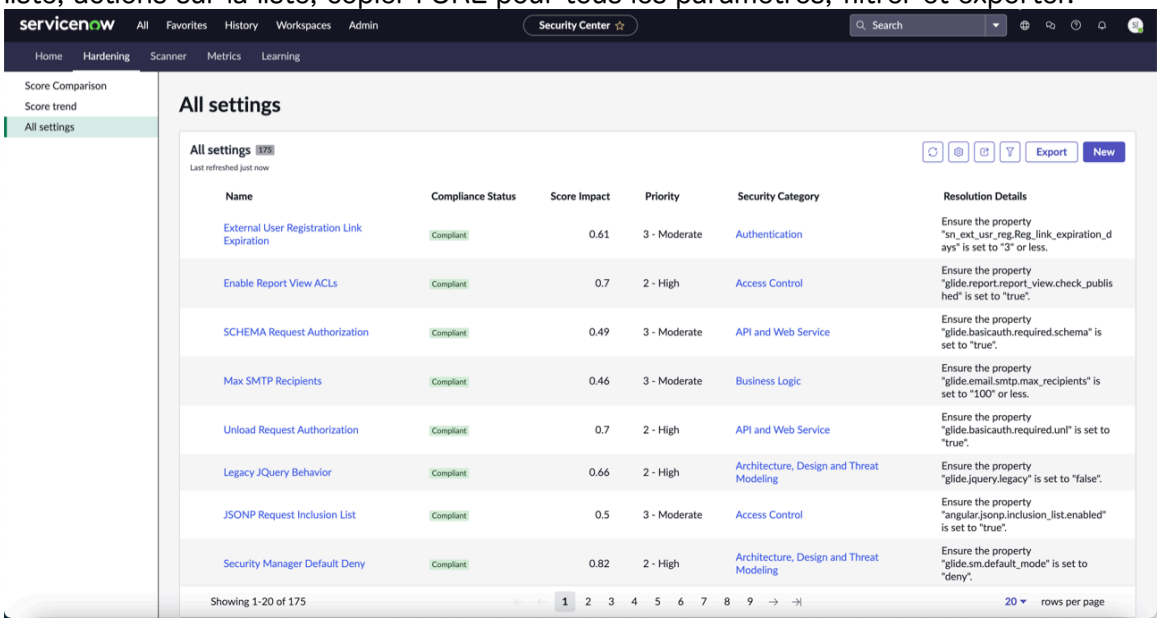
Affichez tous les paramètres de sécurisation renforcée disponibles dans votre instance à partir d'une seule page.

Table qui affiche tous les paramètres de sécurisation renforcée disponibles dans votre instance. Vous pouvez appliquer les opérations courantes pour une table en sélectionnant des icônes dans le coin supérieur droit de la table : actualiser la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

liste, actions sur la liste, copier l'URL pour tous les paramètres, filtrer et exporter.



- **Nom** : nom du paramètre de sécurisation renforcée de la propriété.
- **Statut de conformité** : **Conforme** indique que le paramètre de sécurisation renforcée est correctement configuré ; **Non conforme** indique que le paramètre de sécurisation renforcée de la propriété n'est pas configuré conformément à la recommandation du système.
- **Impact du score** : une valeur en pourcentage de l'impact de ce paramètre de sécurisation renforcée sur votre posture de sécurité. La somme de tous les impacts de score s'élève à 100 %.
- **Priorité** : valeur qui représente la criticité du paramètre : critique, élevée, modérée et faible. La relation entre l'impact du score et la priorité est qu'un impact de score plus élevé indique une criticité plus élevée.
- **Catégorie de sécurité** : catégorie de sécurité de la propriété.
- **Détails de la résolution** : Étapes à suivre pour corriger la vulnérabilité de sécurité du paramètre de sécurisation renforcée.

Pour en savoir plus sur la configuration d'un paramètre de sécurisation renforcée des propriétés, reportez-vous à la section Augmenter le score de conformité à la sécurisation renforcée.

Scanner de sécurité

Utilisez l'outil de scanner pour comparer votre instance à un ensemble de contrôles de sécurité afin d'identifier les erreurs de configuration. L'outil simplifie le processus de création de différentes suites de vérifications pour différents cas d'utilisation afin que vous puissiez analyser les résultats au fil du temps.

L'analyse de sécurité est une méthode qui permet d'examiner votre instance à la recherche de configurations qui indiquent des problèmes d'intégrité de sécurité. Cela vous permet d'identifier les opportunités d'implémentation des recommandations de sécurité pour votre organisation.

Lors de l'accès à l'outil de scanner, aucune comparaison n'est disponible tant que vous n'avez pas sélectionné la suite à comparer avec au moins deux résultats d'analyse de la suite. Vous pouvez utiliser la suite et les vérifications par défaut, ou vous pouvez créer vos propres vérifications et suites personnalisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison des scores de sécurisation renforcée

Gagnez en visibilité sur l'intégrité de vos paramètres de sécurisation renforcée et utilisez ces données pour corriger les menaces de sécurité afin d'améliorer la posture de sécurité de votre instance.

La page de comparaison des scores de sécurisation renforcée affiche les changements de sécurité dans vos paramètres de sécurisation renforcée entre la première et la deuxième date. Pour afficher des visualisations de ces changements, entrez une **date antérieure** et une **date récente** dans le sélecteur de date en haut à droite de la page, puis cliquez sur **Comparer**. Vous trouverez ci-dessous une explication de chaque carte :

- **Score de conformité à la sécurisation renforcée** : affiche le score de conformité de votre instance sous forme de pourcentage aux première et deuxième dates.
- **Impact du score des paramètres changés par priorité** : affiche le nombre de paramètres dont les priorités ont été modifiées.
- **Impact du score des paramètres modifiés par domaine de sécurité** : affiche le nombre de paramètres qui ont changé de catégories. Par exemple, passer du **contrôle d'accès** à la **protection des données**.
- **Paramètres de sécurisation renforcée modifiés** : affiche une vue consolidée des paramètres qui ont été modifiés ainsi que des données de sécurité associées dans la liste. En outre, il est possible d'appliquer des fonctionnalités courantes associées aux listes telles que l'actualisation, la liste des actions d'interface utilisateur, la copie d'URL, les filtres et l'exportation.

Par exemple, dans la capture d'écran suivante, le score de conformité est passé de 71 % à 73 %, ce qui indique que la posture de sécurité a été renforcée au cours de cette période.

Le nombre de paramètres dont la priorité a changé est de quatre au total : deux élevées et deux modérées. En outre, le nombre de paramètres qui ont changé la sécurité est de quatre au total : deux contrôles d'accès, un d'authentification et une logique métier. Les détails de sécurité de ces quatre paramètres sont également affichés dans la liste Paramètres de sécurisation renforcée modifiés. Vous pouvez afficher les paramètres non conformes et les corriger, ce qui recalculera le score de conformité à la sécurisation renforcée.

Vérifications du scanner de sécurité

Les vérifications sont des règles conçues pour détecter les anomalies au sein d'une instance, en s'exécutant sur des tables, des enregistrements ou des métadonnées.

Vous pouvez utiliser quatre types de vérifications avec l'outil de scanner pour identifier les problèmes et implémenter des recommandations de sécurité pour votre organisation : les vérifications de table, les vérifications de type colonne, les vérifications de script uniquement et les vérifications Linter.

Types de vérifications

Nom de vérification	Description
Vérifications de table	Utilisez cette option lorsque vous connaissez les tables et les vérifications spécifiques que vous souhaitez tester.
Vérifications de colonnes	Utilisez cette option pour implémenter la règle que vous avez créée afin d'itérer tous les enregistrements correspondant au type de champ de colonne cible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de vérifications (suite)

Nom de vérification	Description
Vérifications de scripts	Utilisez cette option pour vérifier les métadonnées, les configurations et exécuter des vérifications complexes en écrivant vos propres vérifications.
Vérifications Linter	Utilisez cette option pour identifier les problèmes dans un script. Lorsqu'une vérification linter est exécutée sur un enregistrement, une arborescence de syntaxe abstraite pour son code est générée et peut être utilisée pour analyser les problèmes liés au code.

Créer une suite

Créez et planifiez une suite personnalisée afin de pouvoir analyser la sécurité de votre instance pour votre organisation.

Avant de commencer

Rôle requis : admin ou sn_vsc.security_center_viewer.

Une suite est un ensemble de vérifications qui peut être utilisé pour une analyse. Affichez une liste des suites d'analyse disponibles dans votre instance, organisées dans une table en accédant à **Scanner** > **Suites**. Vous avez la possibilité de créer vos propres suites ou d'utiliser la suite par défaut, Auditor : il s'agit d'une suite prête à l'emploi par défaut qui contient des vérifications des bonnes pratiques de sécurité. Ces vérifications concernent les propriétés système, les modules d'extension et les tables qui peuvent affecter la posture de sécurité de votre instance. Les étapes suivantes montrent comment créer une suite ainsi que les différentes options disponibles pour les configurer.

Procédure

1. Accédez à la **Suites** > **Nouveau**.
2. Saisissez un **nom** et une **description** de suite, puis sélectionnez **Enregistrer**.
3. **Vérifications**
   C'est ici que vous ajoutez des vérifications à votre suite.
   a. Sélectionnez **Modifier**.
   b. Sélectionnez les vérifications que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour les placer dans votre suite.
   c. **Enregistrer**.
4. **Suites enfants**
   Il s'agit de l'endroit où vous ajoutez les suites enfants ou les suites placées sous les suites parentes.
   a. Sélectionnez **Modifier**.
   b. Sélectionnez les suites enfants que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour les placer dans votre suite enfant.
   c. **Enregistrer**.
5. **Suites parentes**
   C'est ici que vous ajoutez des suites parentes. Toutes les suites enfants sont exécutées lorsqu'une suite parente est utilisée dans une analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Sélectionnez **Modifier**.

b. Sélectionnez les suites enfants que vous souhaitez ajouter, puis sélectionnez Ajouter (**>**) pour les placer dans votre suite parente.

c. **Enregistrer**.

6. **Calendrier**
   Définissez une heure d'exécution de votre suite.

   a. Sélectionnez **Nouveau**.

   b. Entrez les détails de l'analyse planifiée.
   Les champs d'heure sont au format suivant : heure :minutes :secondes.

   c. **Enregistrer**.

Cloner la suite de l'auditeur des contrôles d'accès

Clonez et personnalisez la suite d'auditeurs des contrôles d'accès par défaut dans votre instance pour créer une suite adaptée aux pratiques de sécurité de votre organisation.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La suite d'auditeurs des contrôles d'accès par défaut fournie avec votre instance ne peut pas être modifiée. Toutefois, si vous souhaitez ajouter, supprimer ou modifier des vérifications pour les aligner sur les pratiques de sécurité de votre organisation, vous pouvez dupliquer les suites d'auditeurs des contrôles d'accès. La copie des suites d'audit des contrôles d'accès vous permet de les personnaliser et de créer une nouvelle suite basée sur celle par défaut. Les suites d'auditeurs des contrôles d'accès comprennent des vérifications liées aux bonnes pratiques de sécurité, couvrant les propriétés système, les modules d'extension et les tables qui ont un impact sur la posture de sécurité de l'instance. Les étapes suivantes montrent comment dupliquer les suites d'auditeurs des contrôles d'accès par défaut pour les adapter aux exigences de votre organisation.

Procédure

1. Accédez à la **Tout** > **Instance Scan** > **Suites**.
2. Sélectionnez **Nouveau** et saisissez un nom pour votre suite, ainsi qu'une description facultative.
3. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
4. Ajoutez les vérifications nécessaires pour votre analyse.

   a. Dans l'onglet **Vérifications** , sélectionnez **Modifier**.

   b. Ajoutez les conditions.
   Par exemple, pour ajouter des vérifications d'analyse, appliquez les champs, opérateurs, valeurs et conditions suivants :

   [Champ] [est] [Sécurité] ET [Application][est][Global]

   Par exemple, cela devrait ressembler à ce qui suit : La catégorie est Sécurité et l'application est Global.

5. Sélectionnez **Exécuter le filtre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez les vérifications d'analyse que vous souhaitez ajouter de la liste de collecte à la liste de vérification, puis sélectionnez le bouton Ajouter (>).
7. Sélectionnez **Enregistrer**.
   La suite à laquelle vos vérifications personnalisées ont été ajoutées a été créée.
8. Sélectionnez **Exécuter l'analyse de la suite**.

Afficher la suite de l'auditeur des contrôles d'accès

Affichez les vérifications disponibles dans les suites d'auditeurs des contrôles d'accès par défaut pour comprendre quelles vérifications sont exécutées lorsque cette suite s'exécute.

Pourquoi et quand exécuter cette tâche

Étapes que vous devez suivre pour accéder aux suites d'auditeurs des contrôles d'accès par défaut dans votre instance ServiceNow.

Procédure

1. Accédez à la suite de l'auditeur de contrôle d'accès en sélectionnant **Scanner** > **Suites** > **Auditeur de contrôles des accès** suite. Ensuite, pour examiner les vérifications de la suite, sélectionnez l'onglet **Vérifications** .
   Vous devriez voir la liste des 8 vérifications disponibles pour la suite.
2. Sélectionnez le nom d'un chèque que vous souhaitez analyser.
3. Analysez les champs associés à la vérification.

Nom	Description
Nom	Nom du chèque.
Application	Application à laquelle la vérification appartient (Centre de sécurité).
Catégorie	Catégorie associée au chèque.
Priorité	Le niveau d'urgence.
Version	Numéro de version du chèque.
Actif	État du chèque, par exemple, actif ou inactif.
Description brève	Un bref résumé de la vérification.
Description	Un résumé plus complet de la vérification.
Détails de la résolution	Incidents de sécurité potentiels atténués.
URL de documentation	Liens vers la documentation connexe dans la documentation produit ou les articles de la base de connaissances (KB).
Condition d'exécution	Conditions qui déclenchent le début des vérifications.
Table	Table à laquelle le chèque appartient.
Conditions	Logique conditionnelle appliquée aux vérifications.
Avancés	Options de configuration avancées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats de l'analyse

Affichez les données relatives à vos résultats d'analyse à partir d'une seule vue.

Un résultat d'analyse indique l'état et le type d'analyse. Vous pouvez également voir toutes les vérifications exécutées dans le cadre de l'analyse et toutes les autres informations liées à l'analyse, telles que les erreurs et les journaux d'analyse. Sélectionnez **Résultats** pour accéder au tableau de bord**des résultats de l'analyse** . Les résultats de l'analyse sont répertoriés dans la colonne **Résultats** . Cliquez sur un résultat pour l'explorer et afficher les détails :

- **Résultats de l'analyse** : affiche tous les résultats rencontrés lors de l'exécution des vérifications.
- **Suites** : affiche toutes les suites exécutées dans le cadre de l'analyse.
- **Vérifications** : affiche toutes les vérifications exécutées dans le cadre de l'analyse.
- **Échecs:** Affiche toutes les vérifications qui ont échoué lors de l'exécution de l'analyse. Il indique également la raison de son échec sous la forme d'un message d'erreur.
- **Journal d'analyse** : affiche les messages rencontrés pendant toute l'analyse.
- **Statistiques d'analyse** : affiche les statistiques relatives à l'analyse.
- **Cible** : affiche toutes les cibles par rapport auxquelles les vérifications ont été exécutées.

Résultats d'analyse

Un résultat est une référence à un enregistrement qui a enfreint une règle à partir d'une vérification de l'instance. Vous pouvez trouver l'enregistrement source et le nombre de fois où il a déclenché des règles d'une vérification donnée.

Accédez à **Résultats** pour afficher une liste des résultats de l'analyse sur votre instance. Sélectionnez un lien sous la colonne **Créé** pour explorer et afficher les détails granulaires d'un résultat :

- **Vérification** : liste des vérifications associées à l'analyse.
- **Catégorie** : catégorie de sécurité associée à l'analyse. Par exemple, un contrôle d'accès ou un code malveillant.
- **Nombre** : nombre de fois où l'enregistrement a enfreint les règles de vérification.
- **Priorité** : gravité du risque de sécurité : 1 est la priorité la plus élevée, tandis que 4 est la plus faible.
- **Résultat** : état et type de l'analyse.
- **Version de la vérification** : version modifiée de la vérification.
- **Table source** : l'enregistrement qui a enfreint une règle de la vérification.
- **Motif de désactivation** : le motif de désactivation du résultat.
- **Source** : date à laquelle le résultat a été créé.
- **Tâche** : permet de faciliter les affectations de tâches à partir de la recherche d'un enregistrement.
- **Domaine** : définit ce à quoi vous pouvez et ne pouvez pas accéder.
- **Brève description** : une brève explication de l'analyse.
- **Détails de la résolution** : instructions sur la façon de résoudre les problèmes d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures de sécurité

Utilisez l'outil Mesures pour surveiller plus de 50 mesures de sécurité différentes afin d'identifier les menaces de sécurité potentielles ou les comportements non sécurisés. Vous pouvez définir des seuils pour les notifications par e-mail, visualiser et analyser les données de plusieurs façons, exporter les données ou créer des tableaux de bord avec les mesures les plus importantes pour votre organisation.

Les mesures sont implémentées sous forme de visualisations du centre d'analyse qui activent un ensemble riche d'options, notamment l'envoi d'alertes par e-mail lorsque des seuils sont dépassés, la visualisation des cibles et l'affichage et le filtrage des événements sous-jacents.

Tableau de bord de mes mesures de sécurité

Affichez les mesures de sécurité dans votre instance à partir d'un seul tableau de bord.

Pour accéder à la page **Mesures, sélectionnez Mes mesures**. Cette page affiche le tableau de bord par défaut, mais vous pouvez également créer votre propre tableau de bord en sélectionnant **Modifier**.

Vous pouvez personnaliser votre propre tableau de bord en ajoutant des visualisations, des filtres, des en-têtes, des images, du texte enrichi et des listes. Pour en savoir plus sur les différentes façons de personnaliser votre tableau de bord, reportez-vous à la section Dashboards in Platform Analytics .

Configurer les mesures de sécurité pour envoyer des e-mails lorsque des seuils sont déclenchés

Découvrez comment configurer les mesures de sécurité afin que votre instance génère une notification par e-mail lorsqu'un seuil est déclenché.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Dans Centre de sécurité, accédez à **Mesures**.
2. Sélectionnez une mesure pour laquelle vous souhaitez définir un seuil dans votre organisation.

   Example

   Si vous souhaitez gérer les échecs de connexion, vous pouvez définir un seuil pour que les administrateurs ou les experts en sécurité de votre organisation soient informés lorsque les échecs de connexion atteignent un nombre spécifique. La mesure de sécurité appropriée à cibler dans ce cas est **utilisateurs** > **Échecs de connexion**.
3. Sélectionnez l'icône **Seuils** .
4. Sélectionnez l'icône **plus (+)** dans le panneau des seuils pour configurer le formulaire.
   Les options disponibles consistent à définir la visibilité, le type de seuil et la valeur de seuil.

   a. Pour la visibilité, sélectionnez **Pour tout le monde** si vous souhaitez que tout le monde reçoive la notification, ou **Pour moi** si vous souhaitez uniquement recevoir une notification.

   b. Dans Type de seuil, sélectionnez **Toujours le plus élevé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

C’est le champ qui déclenche la notification de seuil.

> **Remarque :**
> Une valeur de seuil ne doit être saisie que lorsque le **type de seuil** est défini sur **Inférieur** ou **Supérieur à**.

5. Sélectionnez **Enregistrer** pour créer le seuil.
   Ensuite, la notification doit être configurée.
6. Sélectionnez **Tout**, puis entrez **notification système**.
7. Accédez à la **E-mail** > **notifications**.
8. Dans la colonne **Nom** , saisissez `*pa thre`.
   Les notifications de seuil sont basées sur les événements et elles sont configurées dans la table Notification de seuils PA.
9. Sélectionner **une notification de seuils PA**.
   Il y a trois onglets dans les résultats :
   - Quand envoyer : spécifie ce qui doit se produire pour envoyer la notification par e-mail. Dans cet exemple, une fois le seuil précédemment défini atteint, l’e-mail est déclenché.
   - Qui recevra : spécifie les utilisateurs qui recevront la notification. Vous pouvez ajouter des utilisateurs et des groupes.
   - Ce qu’il contiendra : spécifie l’action des scripts qu’un utilisateur peut modifier pour personnaliser le message que les utilisateurs et le groupe recevront. Pour en savoir plus sur la création d’actions des scripts, reportez-vous à la section Script actions .

Personnaliser le tableau de bord des mesures de sécurité

Découvrez la flexibilité du tableau de bord des mesures de sécurité, qui peut être personnalisé avec des mesures provenant de diverses sources, telles que des graphiques et des tableaux. Adaptez le tableau de bord aux besoins spécifiques de votre organisation.

Avant de commencer

Pour personnaliser le tableau de bord des mesures de sécurité, assurez-vous de vous trouver dans le périmètre de l’application Centre de sécurité. Pour passer à ce périmètre, sélectionnez **Sélecteur d’application** > **Périmètre de l'application**et saisissez Centre de sécurité.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Implémentez et personnalisez les mesures de sécurité à l’aide du tableau de bord Centre de sécurité. Ajoutez des mesures et du contenu à votre tableau de bord à partir de différentes sources, telles que des graphiques et des diagrammes générés à partir d’un rapport. Découvrez les étapes requises pour ajouter un onglet à votre tableau de bord des mesures de sécurité afin de pouvoir le personnaliser pour répondre aux besoins de votre organisation.

Procédure

1. Dans l’application Seucirty Center, accédez au tableau de bord des mesures de sécurité en sélectionnant **des mesures**.
2. Passez en mode d’édition en sélectionnant **Modifier**.
3. Créez un onglet en sélectionnant **+Ajouter un onglet**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez également ajouter un nouvel onglet en sélectionnant l'icône **plus (+)** en regard d'un onglet existant.

4. Modifiez le titre de l'onglet que vous venez de créer en sélectionnant l'icône en forme de crayon et en saisissant un nom.
5. Ajoutez un élément à votre onglet en sélectionnant **Ajouter un nouvel élément**.
6. Sélectionnez **Enregistrer**.
7. **Facultatif :** Pour partager le tableau de bord avec les utilisateurs, les groupes et les rôles de votre organisation, sélectionnez **Menu Plus d'actions** > **Partager**.
   a. Saisissez le nom d'un utilisateur auquel vous souhaitez accorder l'accès.
   b. Sélectionnez **Confirmer**.

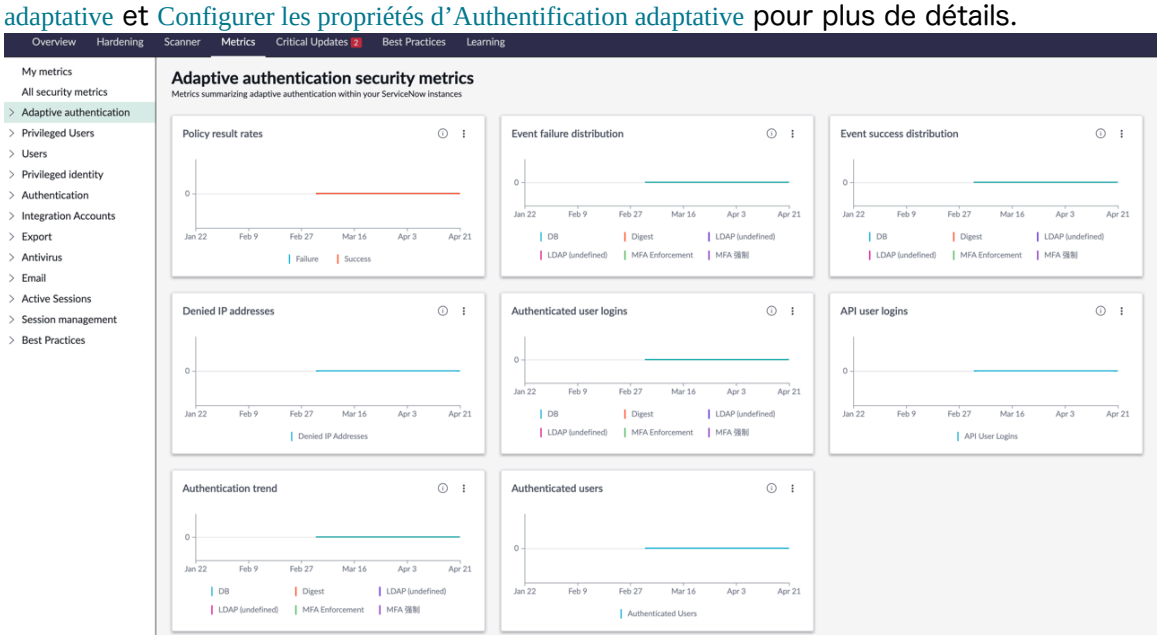
Toutes les mesures de sécurité

Accédez à **Toutes les mesures de sécurité** pour afficher une table contenant les données relatives aux mesures de sécurité de votre instance.

Mesures de sécurité pour l'authentification adaptative

Utilisez des politiques d'authentification pour évaluer les demandes d'authentification et pour refuser ou autoriser l'accès à votre instance en fonction des conditions de politique spécifiées.

Les mesures d'authentification adaptative vous permettent de surveiller la façon dont l'authentification adaptative est utilisée sur votre instance. Vous pouvez afficher un résumé de toutes vos mesures sur l'authentification adaptative, ou explorer et afficher des mesures individuelles telles que les taux de résultats des politiques ou les adresses IP refusées. Cette page nécessite que le module d'extension Authentification adaptative (`com.snc.adaptive_authentication`) pour l'authentification adaptative soit disponible dans votre instance. Vous devez également activer la politique d'authentification pour consulter les mesures. Voir Activer Authentification adaptative et Configurer les propriétés d'Authentification adaptative pour plus de détails.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Cette fonctionnalité a été publiée avec la version 1.2.

- Taux de résultats de la politique : tous les événements d'authentification adaptative ayant réussi ou échoué.
- Distribution d'échecs d'événements : tous les événements ayant échoué pour chaque type d'événement.
- Distribution de la réussite d'événement : événements réussis associés à chaque type d'événement.
- Adresses IP refusées : nombre d'adresses IP bloquées par l'instance, ainsi que leurs données associées.
- Connexions de l'utilisateur authentifiés : nombre d'événements comptés pour chaque type d'événement, à l'exclusion de l'événement de préconnexion.
- Connexions des utilisateurs de l'API : nombre d'événements associés aux politiques d'authentification API pour chaque type d'événement.
- Tendance en matière d'authentification : nombre total d'événements enregistrés.
- Utilisateurs authentifiés : nombre d'utilisateurs comptés pour chaque type d'événement, à l'exclusion de l'événement de préconnexion.

Utilisateurs privilégiés

Affichez la ligne de tendance des utilisateurs privilégiés (actifs et inactifs) et leur activité sur le Now Platform.

La section Vue d'ensemble des utilisateurs privilégiés affiche la ligne de tendance des utilisateurs privilégiés (actifs et inactifs) et leur activité sur le Now Platform. Les utilisateurs privilégiés sont des utilisateurs auxquels des rôles supplémentaires ont été affectés par des administrateurs pour accéder aux fonctionnalités telles que les paramètres de sécurité élevée, l'importation et les utilisateurs du portail.

Vous trouverez ci-dessous une explication des utilisateurs privilégiés :

- Nombre total d'utilisateurs : nombre total d'utilisateurs sur votre instance.
- Utilisateurs actifs : nombre total d'utilisateurs qui ont initié des sessions sur votre instance.
- Utilisateurs inactifs : utilisateurs qui ne se sont pas récemment connectés à votre instance.
- Utilisateurs inactifs qui ne sont pas bloqués : utilisateurs qui ne se sont pas connectés récemment, mais qui ont toujours accès à leur compte.
- Utilisateurs bloqués : utilisateurs qui ne sont pas autorisés à s'authentifier dans leur compte.
- Nouveaux utilisateurs : utilisateurs qui ont récemment été ajoutés à votre instance.
- Connexions réussies : utilisateurs qui se sont connectés avec succès.
- Échecs de connexion : échecs de tentatives de connexion.
- Connexions locales non protégées par MFA : utilisateurs qui se sont connectés sans MFA.
- Utilisateurs qui ne se sont jamais connectés : utilisateurs qui ne se sont jamais connectés à votre instance.
- Utilisateurs non connectés depuis le mois dernier : utilisateurs ne s'étant pas connectés au cours des 30 derniers jours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilisateurs non connectés depuis les 6 derniers mois : utilisateurs ne s'étant pas connectés au cours des 6 derniers mois.
- Utilisateurs non connectés depuis 1 an : utilisateurs qui ne se sont pas connectés au cours de l'année écoulée.
- Besoin de réinitialiser le mot de passe : utilisateurs qui doivent réinitialiser leur mot de passe.
- Échecs de réinitialisation de mot de passe pour les utilisateurs : nombre d'échecs de mot de passe par utilisateur.

Utilisateurs

Affichez la ligne de tendance du nombre total d'utilisateurs (actifs et inactifs) et de leur activité sur le Now Platform.

La section Vue d'ensemble des utilisateurs affiche la ligne de tendance du nombre total d'utilisateurs (actifs et inactifs) et leur activité sur le Now Platform.

Vous trouverez ci-dessous une explication du type d'utilisateurs :

- Nombre total d'utilisateurs : nombre total d'utilisateurs sur votre instance.
- Utilisateurs actifs : nombre total d'utilisateurs qui ont initié des sessions sur votre instance.
- Utilisateurs inactifs : utilisateurs qui ne se sont pas récemment connectés à votre instance.
- Utilisateurs inactifs qui ne sont pas bloqués : utilisateurs qui ne se sont pas connectés récemment, mais qui ont toujours accès à leur compte.
- Nouveaux utilisateurs : utilisateurs qui ont récemment été ajoutés à votre instance.
- Connexions réussies : utilisateurs qui se sont connectés avec succès.
- Échecs de connexion : échecs de tentatives de connexion.
- Connexions externes : authentifications qui utilisent un tiers.
- Connexions locales non protégées par MFA : connexions qui n'utilisent pas MFA.
- Utilisateurs non connectés depuis le mois dernier : utilisateurs ne s'étant pas connectés au cours des 30 derniers jours.
- Utilisateurs non connectés depuis les 6 derniers mois : utilisateurs ne s'étant pas connectés au cours des 6 derniers mois.
- Utilisateurs non connectés depuis 1 an : utilisateurs qui ne se sont pas connectés au cours de l'année écoulée.
- Besoin de réinitialiser le mot de passe : utilisateurs qui doivent réinitialiser leur mot de passe.
- Échecs de réinitialisation de mot de passe pour les utilisateurs : nombre d'échecs de mot de passe par utilisateur.

Identité privilégiée

Analysez les données relatives aux mesures pour les utilisateurs ayant une identité privilégiée.

Ce tableau de bord affiche les données relatives aux utilisateurs d'identité privilégiés et à leur activité sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Connexions d'administration : nombre total de connexions avec des utilisateurs disposant du rôle d'administrateur.
- Emprunt d'identité : nombre total d'emprunts d'identité effectués par les utilisateurs disposant du rôle emprunteur d'identité.
- Élévation : nombre total d'élévations de sécurité effectuées par les utilisateurs disposant du rôle security_admin.
- Connexions ServiceNow : nombre total de connexions par les employés de ServiceNow.
- Utilisateurs administrateurs ajoutés : nombre total d'utilisateurs ayant reçu le rôle administrateur.

Mesures d'authentification

Affichez les mesures liées à l'authentification sur votre instance à partir d'un tableau de bord.

Affiche les données pour les mesures liées aux schémas d'authentification telles que l'utilisation de la MFA, les comptes de services Web et l'utilisation des scanners biométriques.

- Utilisateurs inscrits pour MFA : nombre total d'utilisateurs inscrits pour utiliser MFA.
- Utilisateurs utilisant le contournement de la MFA : nombre total d'utilisateurs qui contournent l'authentification multifacteur.
- Utilisateur non MFA aux privilèges élevés : nombre total d'utilisateurs aux privilèges élevés qui n'utilisent pas la MFA.
- Utilisateurs de MFA actifs : nombre total d'utilisateurs de MFA actifs sur votre instance.
- Utilisateurs de MFA verrouillés : nombre total d'utilisateurs de MFA qui sont bloqués sur votre instance.
- Utilisateur du compte de service Web : nombre total d'utilisateurs avec un compte de service Web uniquement.
- Certificats X509 arrivant à expiration : nombre total de certificats X509 arrivant à expiration dans les 30 prochains jours.

Comptes d'intégration

Affichez les tendances des comptes d'intégration créés dans le Now Platform.

Le tableau de bord des comptes d'intégration affiche les tendances des comptes d'intégration créés dans le Now Platform.

Vous trouverez ci-dessous des explications sur les métriques des comptes d'intégration :

- Total des comptes d'intégration : tendances associées aux comptes d'intégration sur votre instance.
- Comptes d'intégration actifs : tendances associées aux comptes d'intégration actifs sur votre instance.
- Comptes d'intégration inactifs : tendances du nombre total de comptes d'intégration inactifs sur votre instance.

Exporter

Identifiez les données qui sont couramment exportées et identifiez les utilisateurs qui exportent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Total des exportations : nombre total d'enregistrements de table exportés par l'utilisateur.
- Exportations classées : nombre total d'enregistrements de table exportés, résumé par la classification de données qui leur est affectée.

Antivirus

Affiche la tendance à laquelle les événements se produisent sur les fichiers potentiellement infectés. Voyez quand ils sont détectés, placés en quarantaine, restaurés ou supprimés.

- Fichiers mis en quarantaine : nombre de fichiers potentiellement contenant des logiciels malveillants.
- Fichiers téléchargés : le nombre de fichiers téléchargés.
- Fichiers restaurés : nombre de fichiers qui ont été restaurés.
- Fichiers supprimés : le nombre de fichiers supprimés.

E-mail

Affiche les données relatives aux e-mails de courrier indésirable reçus en externe.

Les spams représentent le nombre de courriers indésirables reçus par jour.

Sessions actives

Affichez la ligne de tendance des utilisateurs actifs sur le Now Platform.

La ligne de tendance peut être visualisée pour les mesures suivantes :

- Sessions utilisateur : mesures liées aux sessions utilisateur actives sur votre instance.
- Sessions d'utilisateurs privilégiés : mesures relatives aux utilisateurs privilégiés ou à ceux auxquels des rôles supplémentaires ont été affectés.

Gestion des sessions

Affichez les mesures relatives aux sessions utilisateur et à la fréquence de verrouillage des sessions.

Classification des données

Accédez aux mesures de sécurité pour la classification des données sur votre instance ServiceNow.

La classification des données vous permet d'appliquer des étiquettes de classification des données aux entrées de dictionnaire existantes dans n'importe quelle table afin de fournir une visibilité sur les types de données hébergées dans vos instances, de vous conformer aux lois sur la confidentialité et de répondre aux exigences réglementaires du secteur.

Voir Classification des données pour plus d'informations.

- **Données classifiables** : Tables ou colonnes pouvant être classées.
- **Données classifiées** : entrées de dictionnaire, tables ou colonnes classifiées.

Les données sont affichées graphiquement dans un graphique personnalisable qui fournit une analyse détaillée telle que la définition d'objectifs, de seuils, de tendances, de statistiques ou de prévisions. Les données sont également organisées sous forme d'enregistrements dans une table. Consultez Analytics Hub pour plus d'informations.

Traduction automatique

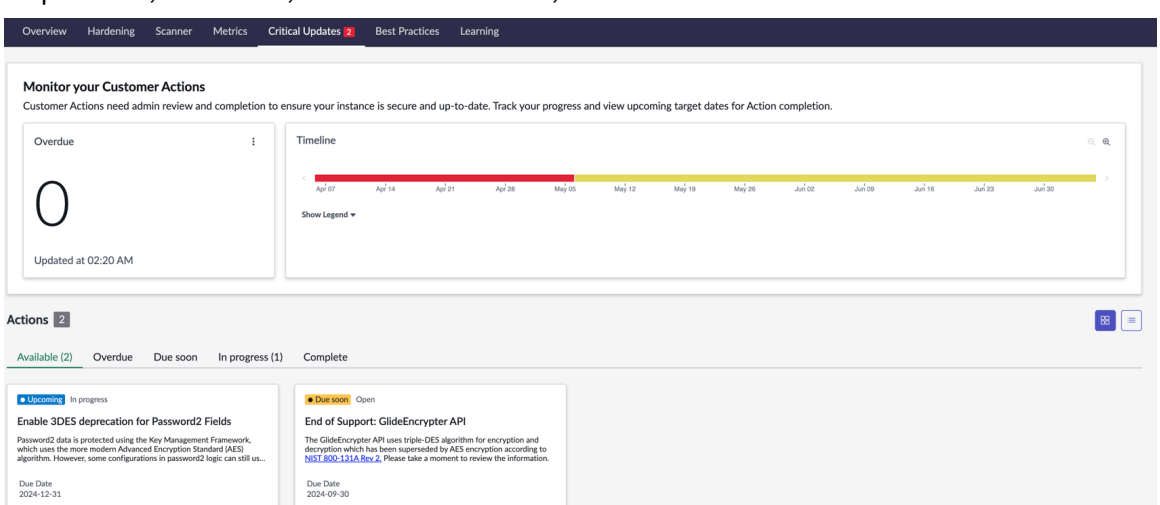
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Actions du client

Améliorez la posture de sécurité de votre instance en vous assurant que les actions client recommandées par le système sont implémentées à temps.

Actions client est un outil qui aide les administrateurs à implémenter des mises à jour de sécurité importantes en fonction de leur instance et de la configuration des modules d'extension. Une action du client est un changement recommandé sur une instance qui vise à vous aider à comprendre l'importance des changements liés à la sécurité. Customer Actions vous aide à implémenter les étapes pour analyser, mettre à jour et tester les mises à jour de sécurité sur votre instance. Implémentez une action du client pour éviter toute interférence avec la personnalisation de votre instance. Les actions client implémentées manuellement sont différentes des mises à jour automatiques rendues sur votre instance du code ou des fonctionnalités de ServiceNow avec des versions familiales ou des correctifs.

Sur la page d'accueil Actions client, vous pouvez voir la chronologie des actions client afin de pouvoir classer par ordre de priorité le moment de l'implémentation des étapes. La chronologie de la capture d'écran affiche les actions du client en retard et celles qui arrivent bientôt à échéance. En outre, vous pouvez suivre la progression de vos actions client sous le libellé Mises à jour. Sélectionnez les onglets afin de voir les actions du client disponibles, en retard, bientôt à échéance, en cours ou terminées.



Démarrer:

- Accéder à cet outil en accédant à **Actions du client** dans Centre de sécurité.
- Les actions du client sont incluses dans l'application Centre de sécurité à partir de Washington DC.

Implémenter des étapes pour les actions du client

Découvrez comment implémenter des actions client sur votre instance afin d'améliorer sa posture de sécurité.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

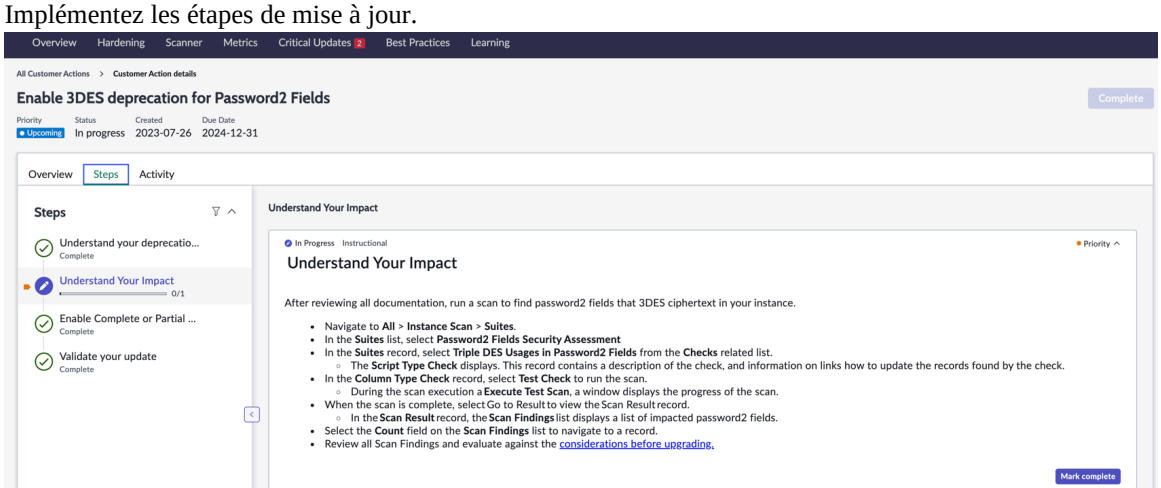
Customer Actions (CA) vous fournit des instructions étape par étape sur la façon d'implémenter les changements sur votre instance afin d'améliorer votre posture de sécurité. CA extrait le contenu pertinent de la documentation produit pour vous guider à chaque étape du processus de mise en œuvre. Suivez les étapes ci-dessous pour savoir comment implémenter une action du client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à l'application**Customer Actions**.
2. Cliquez sur une action du client à implémenter.
   Sous la section **Mises à jour** , l'onglet Disponible répertorie toutes les actions du client sur votre instance. Cliquez sur une action de client sous cet onglet pour afficher les instructions.
3. Lisez la vue d'ensemble pour savoir pourquoi l'action du client est nécessaire et pour vous préparer à l'implémentation des étapes.
   Cliquez sur **Passer à l'étape suivante** pour passer aux détails de l'implémentation.
4. Implémentez les étapes de mise à jour.



   a. Lisez chaque groupe d'instructions et implémentez-les dans votre instance.
   b. Cliquez sur **Marquer comme terminé** lorsque vous avez terminé avec un ensemble d'instructions.
   c. Répétez les étapes a à b jusqu'à ce que vous ayez terminé toutes les étapes de mise à jour.
   d. Cliquez sur **Terminer**.
   L'action du client ne doit plus être disponible dans la section Mises à jour de la page d'accueil Actions du client.

Afficher l'activité des actions du client

Affichez les détails de toutes les activités liées à vos actions client.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Les activités seront répertoriées de la plus récente à la plus ancienne afin que vous puissiez d'abord analyser l'activité la plus récente. Chaque mise à jour d'une activité est horodatée, et vous pouvez utiliser la recherche et le filtre pour interroger des informations spécifiques.

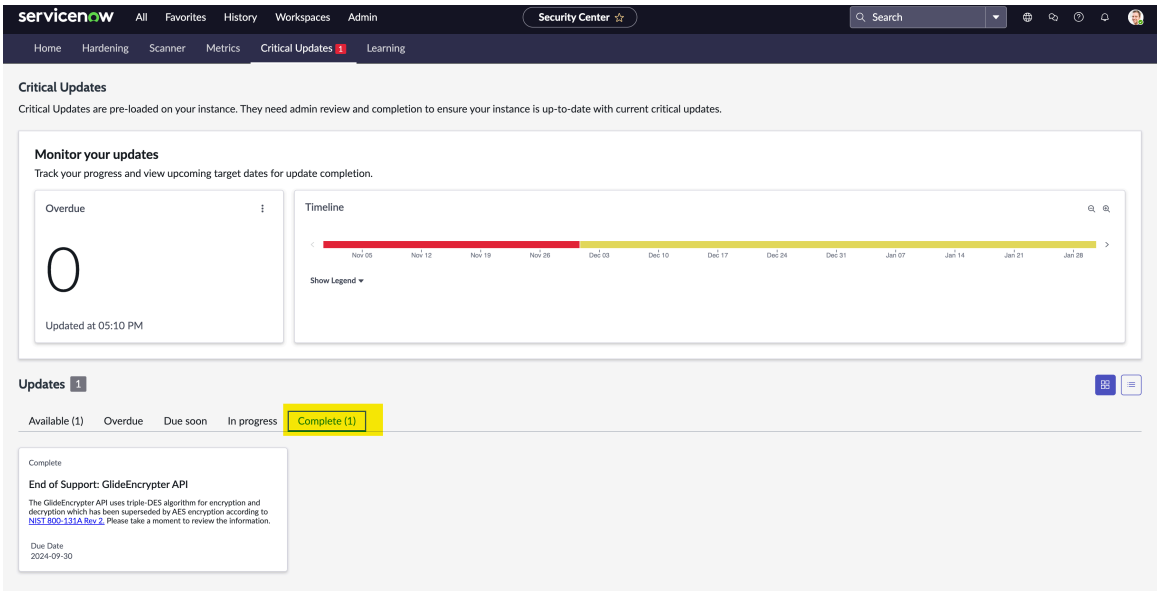
Procédure

1. Accédez à l'application **Actions du client** dans Centre de sécurité.
2. Accédez à l'étiquette**Mises à jour** des actions du client.
3. Cliquez sur un état, puis sélectionnez une action client à partir de cet état.

   Dans l'exemple ci-dessous, l'état **Terminé** est sélectionné, puis l'action du client pour **Fin de support : API GlideEncrypter** est sélectionnée.

Traduction automatique

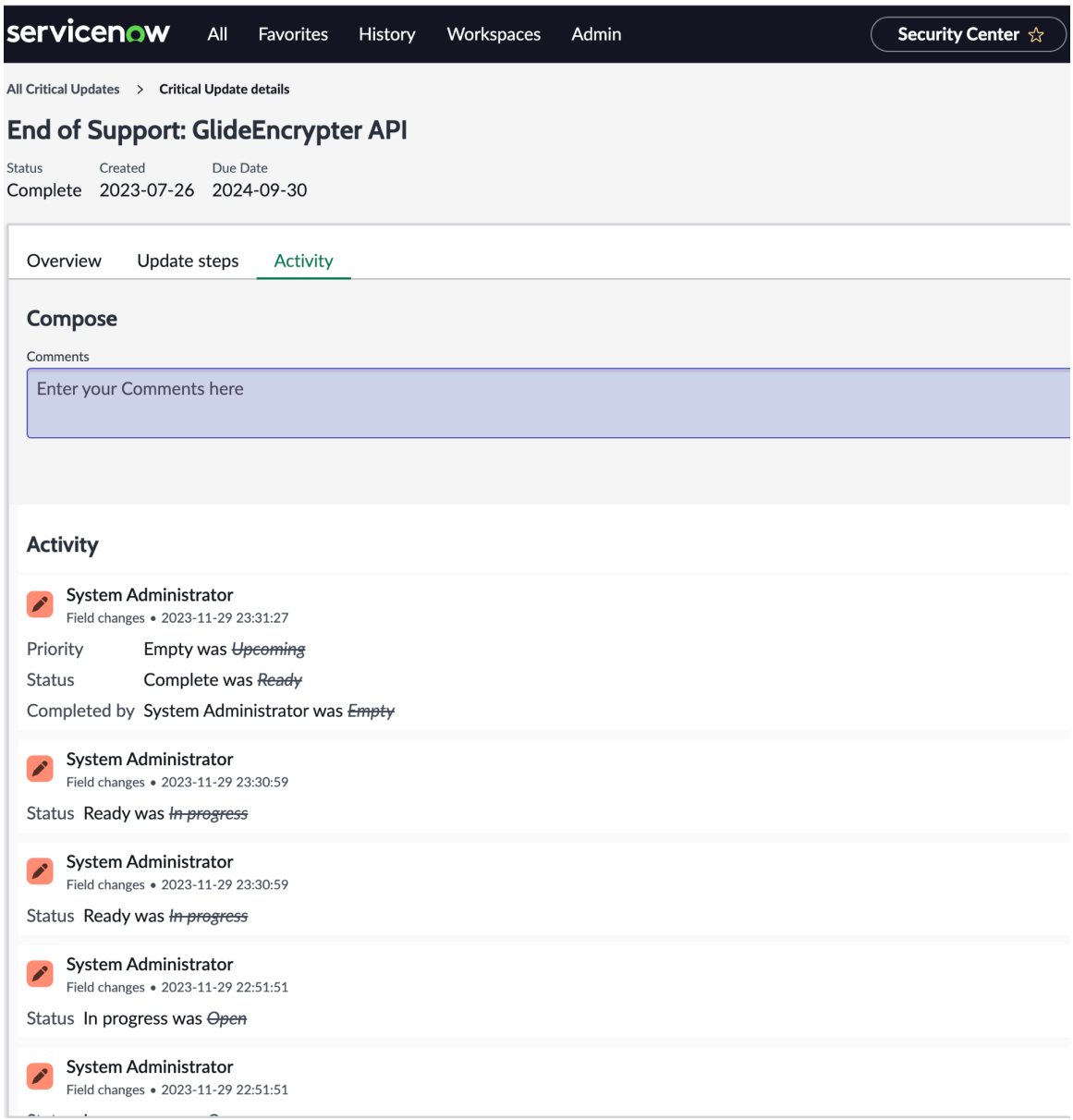
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Affichez l’activité de votre action client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Toute l'activité liée à une action du client est automatiquement enregistrée. De plus, vous avez la possibilité d'ajouter des commentaires supplémentaires aux activités.

Bonnes pratiques de sécurité

Utilisez les bonnes pratiques de sécurité pour implémenter des tâches de configuration de la confidentialité et de la sécurité sur votre instance ServiceNow.

Utilisez les bonnes pratiques de sécurité pour passer en revue les suggestions de sécurité de ServiceNow, identifier celles qui amélioreraient le plus votre posture de sécurité et suivre les instructions étape par étape sur la façon de les implémenter.

Les bonnes pratiques de sécurité fournissent les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La page d'accueil affiche une vue d'ensemble de votre progression dans la mise en œuvre des meilleures pratiques de sécurité. Vous pouvez également organiser et gérer des listes de bonnes pratiques de sécurité en fonction des objectifs de votre organisation.
- La page de vue d'ensemble fournit des détails sur chaque bonne pratique de sécurité, les étapes à suivre pour les implémenter, ainsi qu'un enregistrement de toutes les activités et commentaires.
- La page des étapes de la tâche vous fournit des instructions sur la façon d'implémenter les meilleures pratiques de sécurité.
- La page d'activité suit l'historique de l'utilisateur et les actions du système liées à vos bonnes pratiques de sécurité.

Page d'accueil des bonnes pratiques de sécurité

La page d'accueil comprend des graphiques qui représentent le nombre total de bonnes pratiques de sécurité terminées dans l'ensemble, le nombre de bonnes pratiques achevées par niveau de maturité et un tableau présentant toutes les bonnes pratiques de sécurité disponibles.

La table vous permet d'appliquer des filtres afin de trier et d'enregistrer des listes filtrées, que vous pouvez utiliser comme listes de travail pour différents cas d'utilisation ou rôles. Pour plus d'informations, reportez-vous à la rubrique Enregistrer une liste filtrée .

Vous trouverez ci-dessous des explications sur les champs associés au tableau des bonnes pratiques de sécurité.

Résumé des champs utilisés dans la table des bonnes pratiques de sécurité

Nom	Description
Nom	Mot utilisé pour identifier une bonne pratique de sécurité.
Niveau de maturité	Applications et fonctionnalités qui ont été classées par ordre d'impact pour vous fournir des résultats mesurables. Les valeurs des niveaux de maturité sont les suivantes : • Créer une base • Améliorer l'expérience • Optimiser la fonctionnalité • Ajouter des fonctionnalités avancées Ceux-ci peuvent également être considérés comme des phases ramper, marcher, courir et voler.
Statut	État actuel des bonnes pratiques de sécurité : • Ouvrir • En cours • Terminé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résumé des champs utilisés dans la table des bonnes pratiques de sécurité (suite)

Nom	Description
Priorité	Ordre d'importance pour la mise en œuvre d'une bonne pratique de sécurité dans votre organisation : • Immédiat • Plus tard • Non applicable
Objectifs	Catégorie de sécurité abordée par une bonne pratique de sécurité : • Résoudre les configurations de sécurité initiales • Sécuriser les e-mails • Journaux de surveillance • Gérer les contrôles d'accès • Protéger avec chiffrement • Maintenir les instances à jour
Date de première introduction	Version du centre de sécurité dans laquelle les bonnes pratiques de sécurité ont été introduites.
Modifié	Version du centre de sécurité dans laquelle les bonnes pratiques de sécurité ont été modifiées pour la dernière fois.
Supprimé	Version du centre de sécurité dans laquelle les bonnes pratiques de sécurité ont été supprimées.

Page de vue d'ensemble des bonnes pratiques de sécurité

Lorsque vous sélectionnez une bonne pratique de sécurité dans le tableau des bonnes pratiques de sécurité, vous accédez à une page avec les sous-onglets suivants : Vue d'ensemble, Étapes de la tâche et Activité.

En haut de la page de vue d'ensemble, vous pouvez afficher des informations générales sur les bonnes pratiques de sécurité, notamment la priorité, le niveau de maturité et l'état.

Le menu déroulant **Priorité** vous permet de spécifier les bonnes pratiques de sécurité qui sont importantes pour vous à ce moment-là et qui ne sont pas applicables.

La section des détails fournit du contenu sur les fonctionnalités associées aux bonnes pratiques de sécurité, et la section de documentation fournit un ou plusieurs liens où vous pouvez trouver des informations supplémentaires.

La carte **de progression** sur la droite indique le nombre d'étapes terminées par rapport au nombre total d'étapes incluses. Sélectionnez **Accéder à l'étape suivante** pour accéder à l'étape incomplète suivante.

La carte **d'historique de mise à jour** de bonne pratique fournit un instantané des informations de version pour la bonne pratique. Vous pouvez suivre la version de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Security Center dans laquelle la bonne pratique de sécurité a été publiée et les versions dans lesquelles elle a ensuite été mise à jour.

Page des étapes de la tâche Bonnes pratiques de sécurité

Lorsque vous sélectionnez les étapes de **tâche** du sous-onglet, vous êtes redirigé vers une page qui vous fournit des instructions étape par étape sur la façon d'implémenter les meilleures pratiques de sécurité. Pour plus d'informations, consultez Respecter une bonne pratique de sécurité .

Page d'activité Bonnes pratiques de sécurité

Les activités sont répertoriées de la plus récente à la plus ancienne afin que vous puissiez analyser d'abord l'activité la plus récente. Chaque mise à jour d'une activité est horodatée, et vous pouvez utiliser la recherche et le filtre pour interroger des informations. Pour plus d'informations, reportez-vous à la section Application de filtres au tableau des bonnes pratiques de sécurité .

Suivre une bonne pratique de sécurité

Découvrez comment appliquer une bonne pratique de sécurité sur votre instance ServiceNow.

Pourquoi et quand exécuter cette tâche

Pour implémenter les bonnes pratiques de sécurité sur votre instance ServiceNow, procédez comme suit.

Procédure

1. Accédez aux bonnes pratiques de sécurité en sélectionnant **Tout** sur votre instance ServiceNow, puis en saisissant **les bonnes pratiques**.
2. Appliquez un filtre pour afficher les bonnes pratiques de sécurité à implémenter.
   a. Accédez à la table **des bonnes pratiques** dans l'interface utilisateur.
   b. Sélectionnez le menu kebab ou l'élément avec trois points verticaux (⋮) dans la colonne **État** .
   c. Sélectionnez les options **Ouvrir** et **En cours** , puis sélectionnez **Appliquer**.
3. Sélectionnez le nom d'une bonne pratique de sécurité à implémenter.
4. Sélectionnez **Accéder à l'étape suivante**.
5. Sélectionnez une étape de tâche dans la liste **des étapes** de la tâche.
6. Sélectionnez l'icône du caret vers le bas (v) pour afficher les instructions d'implémentation de cette étape.
7. Lisez les instructions, puis implémentez-les sur votre instance ServiceNow.
8. Sélectionnez **Marquer l'étape comme terminée** lorsque vous avez terminé la tâche.

   Remarque :
   Vous pouvez ignorer la tâche si vous souhaitez y revenir plus tard ou si elle ne s'applique pas aux objectifs de votre organisation. En outre, vous pouvez rouvrir une étape de tâche terminée en sélectionnant l'étape de tâche, puis en sélectionnant **Redémarrer l'étape**.

9. Sélectionnez **Complete Best Practice (Terminer les bonnes pratiques**).

Vous pouvez suivre une bonne pratique de sécurité à tout moment. Vous n'êtes pas obligé de terminer toutes les étapes et ce n'est pas grave si vous les sautez. Toutefois,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

envisagez d'insérer un commentaire dans le sous-onglet Activité lors de l'exécution d'une bonne pratique de sécurité lorsque vous n'avez pas terminé toutes les étapes d'une référence d'audit.

Afficher l'activité d'une bonne pratique

Suivez l'historique chronologique et horodaté associé à une bonne pratique de sécurité que vous suivez sur votre instance ServiceNow, ainsi que l'utilisateur qui a initié l'activité.

Procédure

1. Accédez au Gestionnaire des bonnes pratiques de sécurité en sélectionnant **Tout** sur votre instance ServiceNow, puis entrez Bonne pratique.
2. Dans la table Bonnes pratiques, sélectionnez une bonne pratique de sécurité pour laquelle vous souhaitez afficher l'activité dans la colonne **Nom** .
3. Sélectionnez l'onglet **Activité** .

Parmi les exemples d'activités que vous pouvez afficher, citons les changements de champs, par exemple si l'état d'une bonne pratique de sécurité est passé d'Ouvert à Terminé, ou lorsqu'une étape de tâche est terminée ou ignorée. De plus, vous pouvez saisir des informations supplémentaires relatives à une activité en saisissant un commentaire dans la zone de texte.

Afficher les données des bonnes pratiques terminées

Consultez des représentations visuelles du nombre total de bonnes pratiques achevées ou segmentées par niveau de maturité.

Pourquoi et quand exécuter cette tâche

Effectuez les actions pour afficher des graphiques qui fournissent des tendances visuelles des bonnes pratiques de sécurité qui ont été effectuées globalement et par niveau de maturité.

Procédure

1. Accédez à l'application Centre de sécurité et accédez à l'onglet **Bonnes pratiques** .
2. Sous la carte **Gérer vos bonnes pratiques** , sélectionnez le graphique **global terminé** .
3. Consultez le graphique pour afficher les tendances concernant les configurations des bonnes pratiques de sécurité qui ont été effectuées.
4. Sélectionnez **Terminé par niveau de maturité** pour afficher un graphique qui affiche les tendances des meilleures pratiques achevées par niveau de maturité.

Appliquer des filtres à la table des bonnes pratiques de sécurité

Appliquez des filtres pour renvoyer des résultats plus pertinents pour vos bonnes pratiques de sécurité.

Procédure

1. Accédez au Gestionnaire des bonnes pratiques de sécurité en sélectionnant Tout sur votre instance ServiceNow et en saisissant **les** bonnes pratiques.
2. Accédez à la table **des bonnes pratiques** et sélectionnez un champ auquel vous souhaitez appliquer un filtre en sélectionnant son menu kebab ou celui avec trois points verticaux (⋮).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrer un filtre pour une utilisation ultérieure

Découvrez les étapes d'enregistrement des filtres dans vos bonnes pratiques de sécurité pour une réutilisation ultérieure.

Pourquoi et quand exécuter cette tâche

Après avoir créé des filtres dans la table des bonnes pratiques de sécurité, vous pouvez les enregistrer pour les utiliser lors de votre prochaine authentification dans votre instance. Si vous souhaitez plus de flexibilité sur le type de filtres que vous pouvez créer, vous pouvez appliquer un filtre avancé.

Procédure

1. Sélectionnez l'icône du panneau Afficher le filtre ( ).
2. Dans le panneau de la boîte de dialogue **Filtre** , faites défiler vers le bas et sélectionnez **Vue avancée**.
3. Créez un filtre en ajoutant des conditions qui contiennent un champ, un opérateur et des valeurs.
4. Sélectionnez **Enregistrer le filtre**
5. Entrez le nom du filtre.
6. Sélectionnez une autorisation.
7. Sélectionnez **Enregistrer**.
8. Sélectionnez **Mettre à jour** pour appliquer le filtre enregistré à la table des bonnes pratiques de sécurité.

Utiliser un filtre enregistré

Découvrez les étapes d'utilisation des filtres que vous avez enregistrés pour vos bonnes pratiques de sécurité.

Pourquoi et quand exécuter cette tâche

Une fois que vous vous êtes déconnecté de votre instance, vos filtres sont réinitialisés aux paramètres par défaut. Les étapes suivantes montrent comment récupérer un filtre enregistré afin de pouvoir l'appliquer à nouveau dans la table des bonnes pratiques de sécurité.

Procédure

1. Sélectionnez l'icône Afficher le panneau de filtre ( ).
2. Dans la boîte de dialogue Filtre, faites défiler vers le bas et sélectionnez **Vue avancée**.
3. Sélectionnez **Utiliser un filtre existant**, puis sélectionnez un filtre enregistré dans la liste déroulante.
4. Sélectionnez **Mettre à jour** pour appliquer le filtre enregistré.

Apprentissage de la sécurité

Accédez aux supports d'apprentissage sur la sécurité à partir d'une seule page.

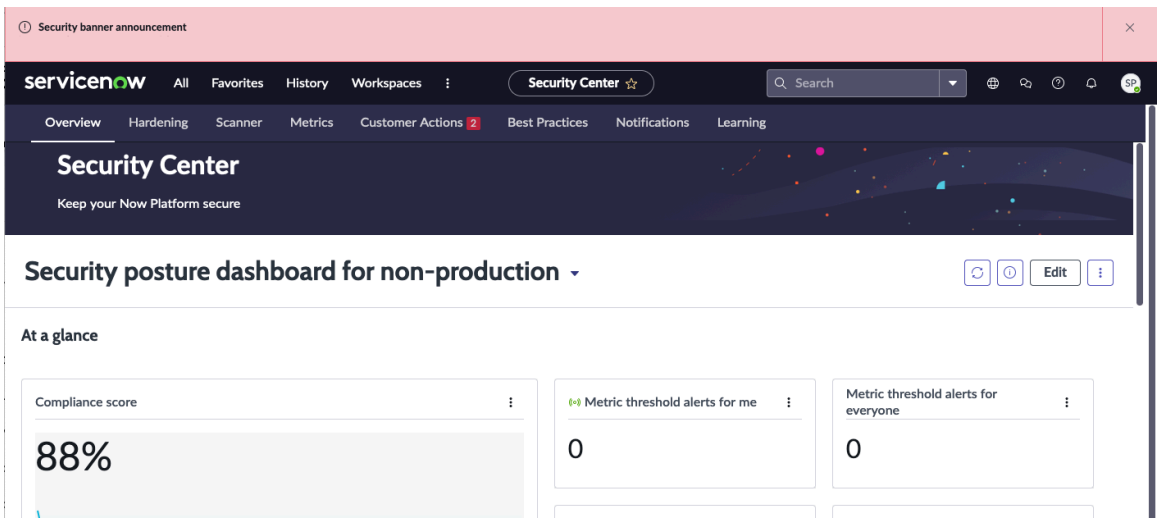
Lisez des livres blancs sur la sécurité, des ebooks, des articles de la base de connaissances, de la documentation produit et des discussions de la communauté à partir d'une vue consolidée en accédant à **Apprentissage**. Le contenu est organisé en en-têtes et en fiches d'interface utilisateur descriptives pour vous permettre d'identifier rapidement la ressource appropriée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Annonces de bannières de sécurité

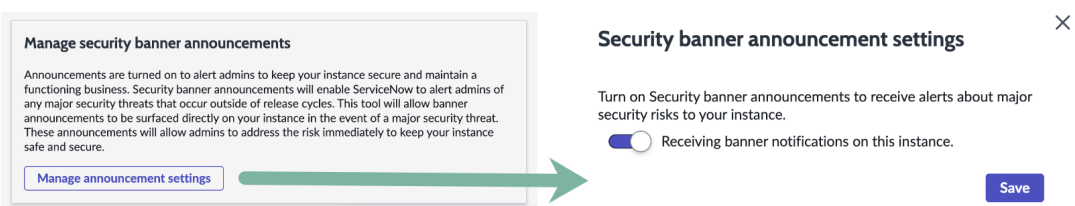
Activez les annonces de bannière de sécurité pour rester informé des alertes de sécurité urgentes et critiques à l'aide de bannières haute visibilité visibles par les administrateurs dans l'interface utilisateur de l'instance.



Les annonces de bannière de sécurité sont des annonces affichées aux administrateurs clients, envoyées par ServiceNow, pour vous tenir informé des correctifs de menaces de sécurité potentielles qui ont été découvertes récemment. Ces alertes contiennent un résumé du risque de sécurité et incluent un lien vers lequel vous pouvez en savoir plus et agir pour sécuriser votre instance.

Activer ou désactiver les annonces de bannières de sécurité

La fonctionnalité de bannière de sécurité est activée par défaut. Pour activer ou désactiver les annonces de bannière de sécurité, accédez à **Sécurité de système** > **Centre de sécurité** > **Notifications**. Sur cette page, sélectionnez le bouton **Gérer les paramètres de l'annonce** .



Tableaux de bord sur la posture de sécurité

Utilisez les tableaux de bord personnalisables sur la posture de sécurité à une ou plusieurs instances pour surveiller vos KPI de sécurité. Ces tableaux de bord regroupent les informations importantes concernant la sécurité de vos instances en un seul emplacement et incluent un certain nombre de widgets de tableau de bord du système de base.

Accès aux tableaux de bord sur la posture de sécurité

Accéder au tableau de bord Posture de sécurité en naviguant vers **Tout** > **Centre de sécurité**. Le contenu du tableau de bord Posture de sécurité se trouve dans l'onglet **Vue d'ensemble** .

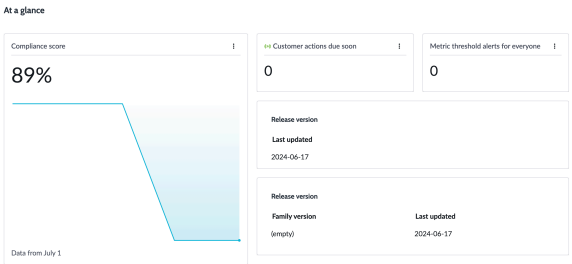
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

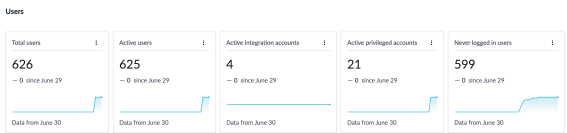
Composants de tableau de bord

Le tableau de bord est divisé en plusieurs sections contenant des widgets liés à un aspect de la sécurité de l'instance. Sélectionnez n'importe quel widget sur le tableau de bord pour afficher plus de détails sur cet aspect de la sécurité de votre instance.

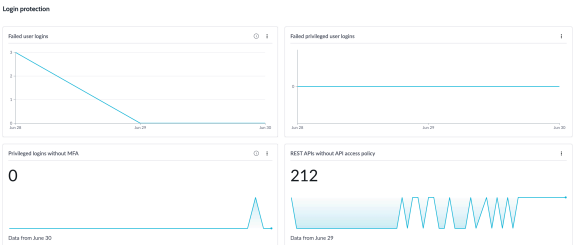
La section **En un coup d'œil** affiche une vue d'ensemble de la sécurité d'une instance, comme le score de conformité, les actions du client à échéance et les informations de mise à jour et de version de l'instance.



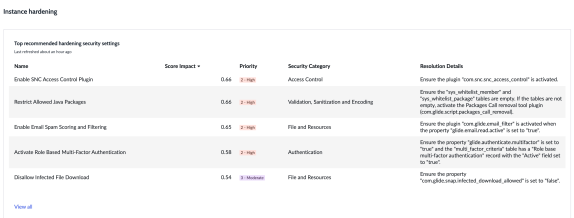
La section **Utilisateurs** fournit des informations sur les utilisateurs de votre instance. Les widgets de cette section affichent des informations utilisateur et un graphique linéaire montrant les changements apportés à ces informations au fil du temps. Sélectionner un widget pour afficher plus de détails



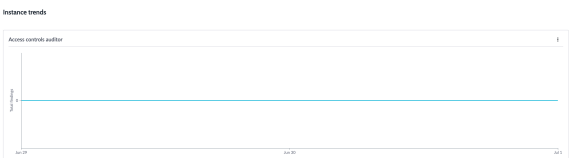
La section **Protection de connexion** comprend des informations sur les échecs de connexion, y compris les échecs de tentatives de connexion pour les utilisateurs privilégiés.



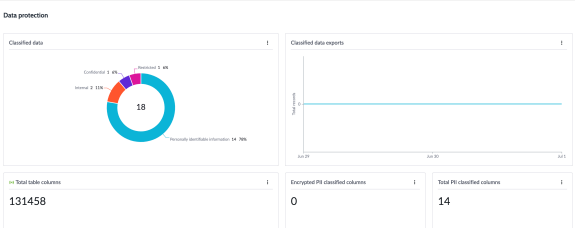
La section **Renforcement de l'instance** contient les paramètres de sécurité de renforcement recommandés que vous pouvez modifier pour améliorer la sécurité de l'instance. Utilisez cette section pour connaître la priorité et l'impact potentiel de ces changements.



Le tableau de bord **Tendances de l'instance** affiche les résultats de la suite d'analyse de l'auditeur des contrôles d'accès.



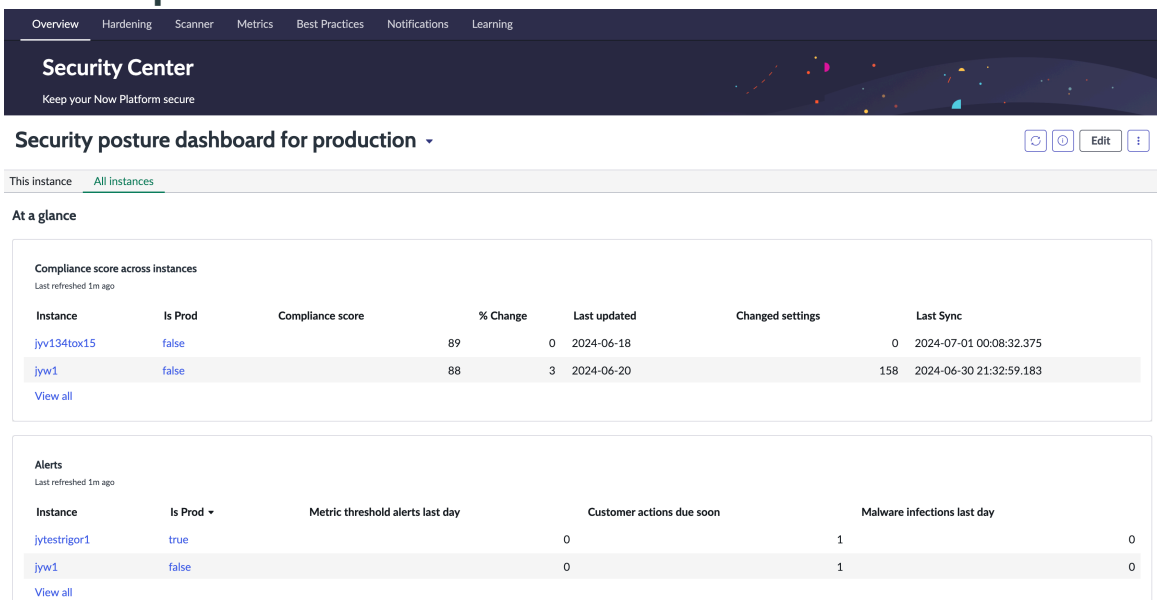
Utilisez la section **Protection des données** pour obtenir une vue d'ensemble des données classifiées, telles que les informations personnelles identifiables (PII). Le tableau de bord permet également de suivre les exportations de données classifiées,



Traduction automatique

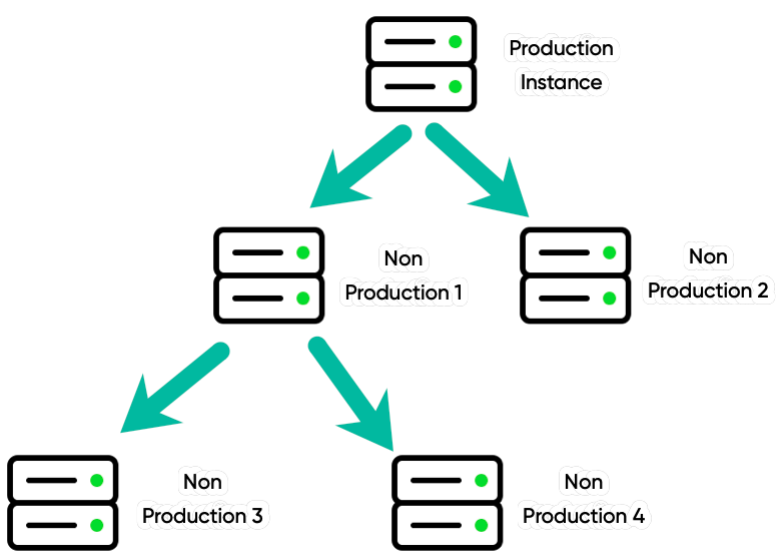
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Examiner plusieurs instances



Visualisez le niveau de sécurité de vos instances de non-production sans quitter votre instance de production à l'aide de l'onglet **Toutes les instances** en haut du tableau de bord. L'onglet **Toutes les instances** affiche une version condensée des mêmes informations que l'onglet **Cette instance** , mais inclut également les données de toutes vos instances de non-production.

Par défaut, l'onglet **Toutes les instances** affiche des informations sur l'instance de production, toutes les instances clonées à partir de la production et toutes les instances clonées à partir des instances clonées. Dans cet exemple, deux instances sont clonées à partir de la production et deux instances supplémentaires sont clonées à partir de l'un de ces clones. Les cinq instances s'affichent dans l'onglet **Toutes les instances** .



Personnalisation du tableau de bord

Le tableau de bord de la posture de sécurité de l'instance ne peut pas être personnalisé, mais vous pouvez dupliquer le tableau de bord en sélectionnant l'icône **Actions supplémentaires** (⋮) et en **sélectionnant Dupliquer**. Vous pouvez modifier le tableau de bord en double.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notifications des événements de sécurité

Affichez, gérez et analysez les politiques de notification d'événement de sécurité par défaut sur votre instance ServiceNow, et accédez à la fonctionnalité permettant de créer de nouvelles politiques personnalisées.

Personnalisez et créez facilement des politiques de notification qui déclenchent des notifications par e-mail lorsque les utilisateurs prennent des mesures dans la Now Platform qui peuvent ne pas être sécurisées ou qui nécessitent une surveillance de l'administrateur.

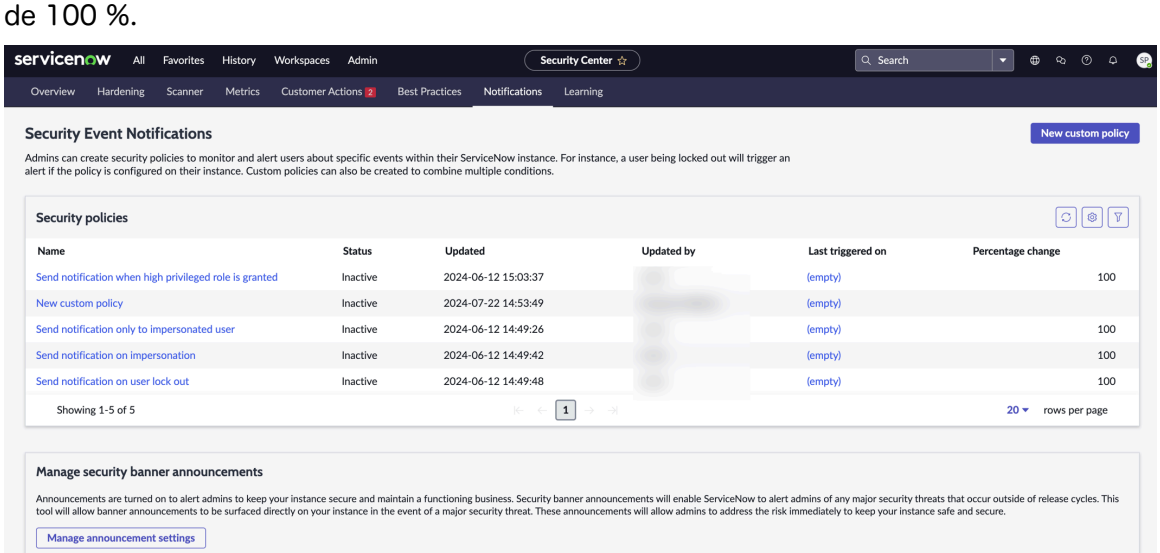
Les notifications d'événement de sécurité se composent de deux parties : la configuration de la politique de sécurité et la configuration des notifications. La configuration de la stratégie vous permet de spécifier la combinaison d'événements et d'actions qui déclenche des notifications. La configuration des notifications vous permet de spécifier les destinataires des e-mails et le format des e-mails.

Les administrateurs peuvent personnaliser les valeurs des politiques par défaut, cloner et modifier les politiques par défaut ou créer leurs propres politiques personnalisées.

Vue d'ensemble des notifications d'événements de sécurité

Dans la vue d'ensemble des notifications d'événements de sécurité, vous pouvez voir une table qui organise toutes les politiques de sécurité disponibles sur votre instance.

Ce tableau comprend des colonnes affichant le nom de la politique, son état (actif ou inactif), la date et l'heure de la dernière mise à jour, la mise à jour de l'utilisateur, la date et l'heure du dernier déclenchement, ainsi que le changement en pourcentage, ou le taux de changement pour les déclencheurs hebdomadaires, calculé en pourcentage. Par exemple, si cette politique déclenche en moyenne 5 notifications par semaine et qu'elle s'est déclenchée 10 fois la semaine dernière, cela représente une augmentation en pourcentage de 100 %.



En outre, vous pouvez sélectionner le bouton **Nouvelle politique personnalisée** pour créer une politique personnalisée adaptée aux cas d'utilisation de votre organisation.

Page de vue d'ensemble des notifications d'événements de sécurité

Accédez à la page d'accueil des notifications d'événement de sécurité, puis sélectionnez l'une des politiques que vous souhaitez examiner ou personnaliser. L'onglet Vue d'ensemble vous fournira un instantané rapide de la politique. Pour personnaliser la politique, sélectionnez l'onglet **Paramètres de politique** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour les stratégies par défaut, vous ne pouvez pas modifier le déclencheur ni la logique de condition. Si vous souhaitez apporter de tels changements, vous devez d'abord dupliquer la stratégie en sélectionnant le bouton Dupliquer en haut à droite de la page.

Remarque :
Pour afficher le bouton Dupliquer, vous devez sélectionner l'icône du menu kebab (menu à trois points) à droite du bouton Mettre à jour, en haut à droite.

N'oubliez pas de sélectionner le bouton Mettre à jour une fois que vous avez terminé les modifications. Et n'oubliez pas de désactiver la stratégie jusqu'à ce que vous soyez prêt à commencer à déclencher des notifications. Vous pouvez activer et désactiver la politique à l'aide du bouton en haut à droite, à côté du bouton Mettre à jour.

Accédez à un instantané des politiques de notification d'événement de sécurité sur votre instance, où les données sont organisées en cartes d'interface utilisateur. Analysez les détails et les sections d'activité, et utilisez la fonctionnalité permettant d'ajouter des informations supplémentaires aux politiques de sécurité, par exemple par le biais de commentaires.

Champs et fonctionnalités de la table de vue d'ensemble

Étiquette	Description
Nom	Nom de la politique de notification d'événement de sécurité.
Statut	L'état d'une politique peut être actif ou inactif.
Mis à jour	Date et heure de la dernière mise à jour de la politique.
Mis à jour par	Utilisateur qui a mis à jour une politique.
Dernier déclenchement le	Date et heure de dernière exécution de la politique.
Nombre de déclenchements la semaine dernière	Nombre de déclencheurs qu'une politique a générés au cours des 7 derniers jours.
Changement de pourcentage	Taux de changement des déclencheurs hebdomadaires, calculé en pourcentage.

Créer des politiques personnalisées de notification d'événement de sécurité

Découvrez comment créer des notifications d'événements de sécurité personnalisées et spécifiques aux besoins de votre organisation. Cela vous permet de surveiller les actions effectuées par les utilisateurs et les groupes sur votre instance et de générer des notifications pour les risques de sécurité potentiels.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à l'application Centre de sécurité et sélectionnez **Notifications**.
2. Sélectionnez **Nouvelle stratégie personnalisée**.
3. Sélectionnez l'un des trois types d'événements qui déclencheront le début de la politique, puis sélectionnez **Créer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Configurez la politique.
   Reportez-vous à la section Configurer les préférences pour les politiques de notification d'événement de sécurité pour savoir comment configurer votre nouvelle stratégie personnalisée de notification d'événement de sécurité.

Modifier les politiques de notification d'événement de sécurité

Découvrez comment modifier les paramètres de vos stratégies de notification d'événement de sécurité.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la page d'accueil des **notifications** d'événement de sécurité et sélectionnez l'une des politiques que vous souhaitez modifier.

   Remarque :
   Vous ne pouvez pas modifier le déclencheur ou la logique de condition des politiques par défaut. Pour modifier ces paramètres, vous devez d'abord dupliquer la stratégie, ce qui peut être fait en sélectionnant la flèche vers le bas en regard de **Mettre à jour**, puis en sélectionnant **Dupliquer**.

2. Sélectionnez **les paramètres de stratégie** pour modifier les paramètres.
3. Sélectionnez **Mettre à jour** pour enregistrer vos changements.
4. **Facultatif :** Sélectionnez **Désactiver** jusqu'à ce que vous soyez prêt à déclencher des notifications.
5. **Facultatif :** Commencez à déclencher des notifications en **sélectionnant Activer**.
   Reportez-vous à la section Configurer les préférences pour les politiques de notification d'événement de sécurité pour savoir comment configurer votre nouvelle stratégie personnalisée de notification d'événement de sécurité.

Configurer les préférences pour les politiques de notification d'événement de sécurité

Découvrez comment personnaliser les stratégies de notification d'événement de sécurité pour Centre de sécurité qu'elles soient en adéquation avec les besoins spécifiques de votre organisation.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
La page **Paramètres de stratégie** vous permet de personnaliser les paramètres d'une stratégie de notification d'événement de sécurité. Ici, vous pouvez ajuster les options liées au moment où la politique s'exécute, à la logique conditionnelle et aux notifications qui sont envoyées.

Procédure

1. Dans Security Center, sélectionnez **Notifications**.
2. Dans la table Politiques de sécurité, sélectionnez une politique de notification d'événement de sécurité que vous souhaitez configurer.
   Par exemple, **Envoyer une notification lorsqu'un rôle hautement privilégié est accordé**.
3. Sélectionnez **Paramètres de stratégie**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Configurez les paramètres de stratégie.

Options de configuration des paramètres de politique

Étiquette	Ce qu'il faut configurer
Quand exécuter	**Déclencheur** : événement qui démarre la police.
Conditions	Logique conditionnelle et conditions à appliquer à vos stratégies. ○ **Logique de condition** : deux options ▪ **Toutes les conditions doivent être remplies pour déclencher cette politique** : toutes les conditions doivent être valides pour que la politique envoie des notifications. ▪ **Toutes les conditions doivent être remplies pour déclencher cette politique** : des notifications seront envoyées si l'une d'entre elles est valide. ○ **Ajouter une condition** : sélectionnez Ajouter une condition et indiquez les valeurs appropriées pour celle-ci. Vous pouvez supprimer une condition en sélectionnant **Supprimer la condition**.
Notifications	Le corps de l'e-mail et les destinataires de l'e-mail : ○ **Notification** : sélectionnez l'un des modèles de notification prédéfinis. Consultez Créer un e-mail personnalisé pour les notifications d'événements de sécurité pour plus d'informations. ○ **Ajouter une notification** : sélectionnez Ajouter une notification. ○ **Groupes** : sélectionnez le groupe qui doit recevoir la notification. ○ **Utilisateurs** : sélectionnez les utilisateurs qui doivent recevoir la notification. Vous pouvez supprimer une notification en sélectionnant **Supprimer la notification**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous souhaitez rendre une politique inactive, sélectionnez **Désactiver**. Si vous souhaitez reproduire une stratégie, sélectionnez la flèche vers le bas en regard du bouton **Mettre à jour** (

).

5. Sélectionnez **Mettre à jour** pour enregistrer vos paramètres.

Créer un e-mail personnalisé pour les notifications d'événements de sécurité

Découvrez comment créer un e-mail personnalisé pour les notifications d'événements de sécurité en configurant de nouvelles notifications, en définissant des déclencheurs, en définissant des destinataires et en créant du contenu d'e-mail avec des champs d'événement dynamiques.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Sélectionner **Notifications système** > **Notification**.
2. Sélectionnez **nouveau**.
3. Saisissez un **nom** pour le champ de notification.
4. Sélectionnez le champ en regard de **la table** et saisissez la notification de politique de sécurité (*sn_vsc_security_policy*).
5. Configurez le nouvel enregistrement.
   L'enregistrement comporte trois onglets qui doivent être configurés : **Quand envoyer**, **Qui recevra** et **Ce qu'il contiendra**.

Onglet	Description
Quand envoyer	Sélectionnez le champ en regard de **l'étiquette Envoyer et** sélectionnez **Déclenché**.
Qui recevra	○ Sélectionnez l'icône locale en regard de **Utilisateurs/Groupes dans les champs**, puis sélectionnez à la fois **Utilisateurs** et **Groupes**. Sélectionnez l'icône **Ajouter un élément** (>) pour déplacer les champs dans le champ de texte **sélectionné** . ○ Cliquez avec le bouton droit sur la bannière de l'en-tête d'enregistrement et sélectionnez **Enregistrer**.)
Ce qu'il contiendra	Créez un modèle d'e-mail. Consultez Create an email template pour plus d'informations. Entrez les champs de l'événement dans le **message HTML.** Cela peut être fait en

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet	Description

	utilisant le ${event_id.FIELD_NAME}. Voici un exemple :
	`Role: ${event_id.role.URI_REF}`
	`Granted to: ${event_id.granted_to.URI_REF}`
	`Granted by: ${event_id.user.URI_REF}`
	`Logged at: ${event_id.sys_created_on}`
	`Security Center Notification: ${execution.policy.name}`

6. Sélectionnez **Soumettre**.
7. Ajoutez une notification personnalisée au modèle d'e-mail dans les notifications d'événements de sécurité.
   a. Dans Centre de sécurité, sélectionnez **Notifications** > **Paramètres de politiques**.
   b. Accédez à l'étiquette **Notifications** .
   c. Saisissez le nom de la notification personnalisée que vous avez créée dans le champ **Notification** .

Historique des notifications d'événements de sécurité

Explorez l'historique complet des notifications d'événements de sécurité sur votre instance.

La page **Notifications** fournit une vue d'ensemble de l'historique des notifications pour toutes les politiques de notification d'événements de sécurité sur votre instance. Vous pouvez afficher les données sous forme de graphiques, les présenter sous forme graphique et appliquer des fonctionnalités d'analyse des performances telles que les cibles, les seuils et les signaux KPI. Vous pouvez également afficher les données sous forme de tableau, ce qui vous permet d'utiliser des fonctionnalités standard telles que la recherche, le tri, le filtrage et l'interrogation.

Centre de sécurité de l'instance

Surveillez le niveau de conformité des contrôles de sécurité de l'instance, affichez les mesures de surveillance des événements de sécurité et configurez et gérez les paramètres de sécurité de l'instance à partir du Centre de sécurité de l'instance. Centre de sécurité de l'instance consolide plusieurs composants de sécurité clés dans une console de contrôle unique qui vous aide à détecter, protéger et répondre aux événements de sécurité basés sur l'instance.

Vue d'ensemble du Centre de sécurité de l'instance

Important :

Le Centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

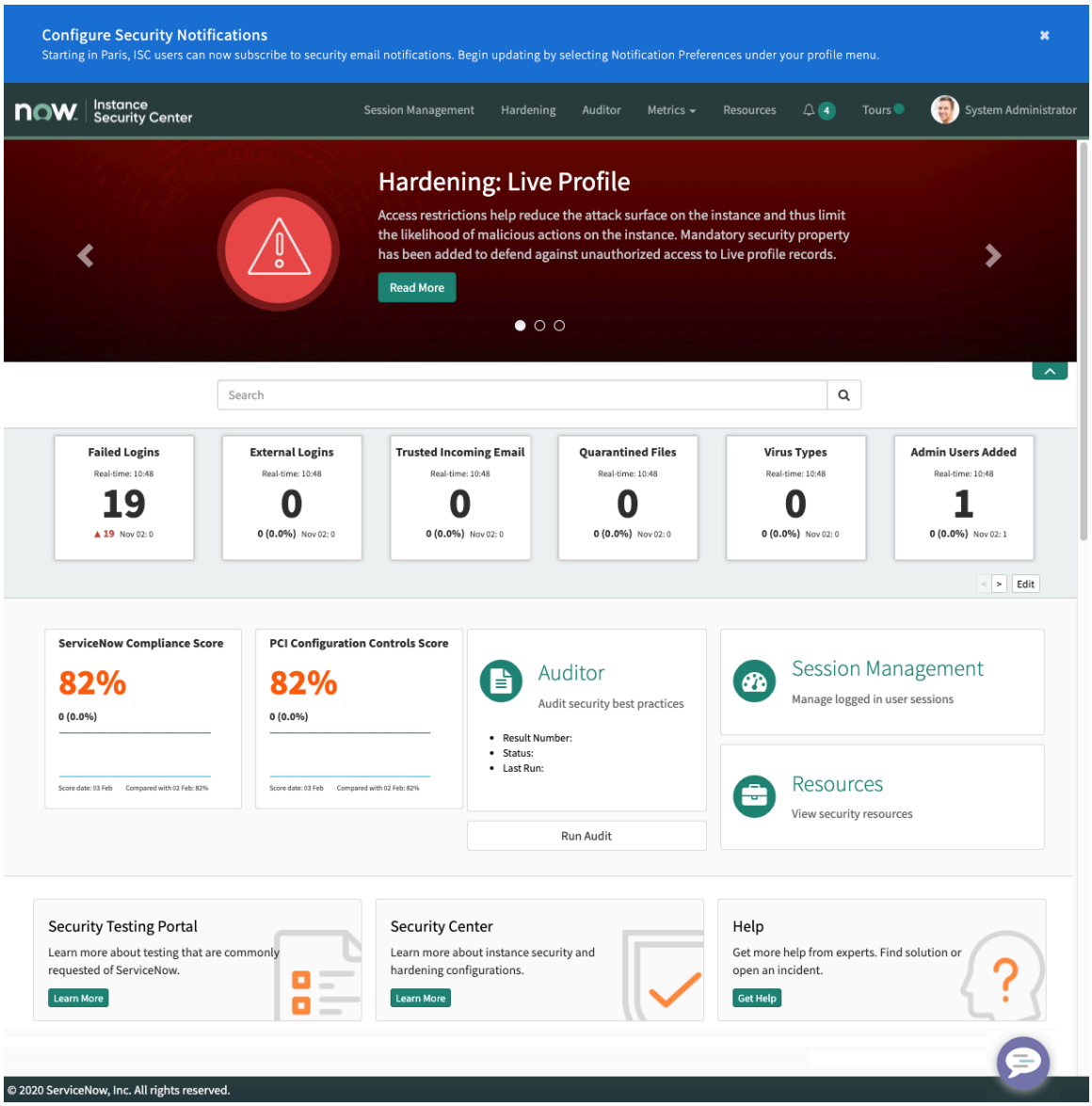
ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers ServiceNow Centre de sécurité migration.

Composants du Centre de sécurité de l'instance

Pour accéder au Centre de sécurité de l'instance, naviguez vers **Sécurité de système** > **Centre de sécurité de l'instance** ou sur la page d'accueil de l'administration système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La page d'accueil du centre de sécurité de l'instance contient les composants de sécurité suivants :

- Messages de l'administrateur
- Bannière de sécurité rotative
- Rechercher
- Ruban d'événement de sécurité
- Score de conformité quotidien
- Score des contrôles des configurations PCI
- Gestion des sessions
- Sécurisation renforcée
- Auditeur
- Mesures (utilisateur, e-mail et antivirus)
- Ressources
- Notifications de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Visites guidées
- Portail de test de la sécurité
- Centre de sécurité
- Aide
- Accès à l'Agent virtuel

À partir de la page d'accueil du Centre de sécurité de l'instance, vous pouvez afficher le score de conformité de sécurité de votre instance et surveiller son intégrité de sécurité globale. Vous pouvez ensuite configurer ou mettre à jour les propriétés système liées à la sécurité de votre instance afin qu'elles soient conformes aux exigences de sécurité.

Remarque :
Le Centre de sécurité de l'instance ne prend pas en charge Séparation de domaine.

Rôles d'utilisateur

Pour utiliser Centre de sécurité de l'instance, vous devez avoir le rôle administrateur ou security_dashboard_user.

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez Managing per-user subscriptions in Subscription Management et contactez votre représentant de compte.

roles

Rôle requis	Utilisateur	Avantages
administrateur	Ce rôle a accès à l'ensemble des fonctionnalités, fonctions et données système, car les administrateurs peuvent remplacer les règles de liste de contrôle d'accès (ACL) et subir avec succès toutes les vérifications de rôles. Évitez d'affecter ce rôle à vos utilisateurs lorsque des rôles plus ciblés sont disponibles.	Exploitez des Centre de sécurité outils pour améliorer la posture de sécurité de l'instance et surveiller les comportements liés à la sécurité.
sn_vsc.security_center_viewer	Ce rôle permet aux utilisateurs qui ne sont pas administrateurs de consulter les informations dans Centre de sécurité les Centre de sécurité outils, mais pas d'y apporter des modifications ou d'effectuer des changements de configuration d'instance en exploitant les Centre de sécurité outils. Par exemple, les propriétaires de plateformes, les analystes des opérations de sécurité ou les	Gagnez en visibilité sur Centre de sécurité les outils permettant de surveiller la posture de sécurité des instances et de surveiller les comportements de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

roles (suite)

Rôle requis	Utilisateur	Avantages
	personnes concernées par la conformité peuvent souhaiter ou avoir besoin de consulter certains des KPI de sécurité, des aperçus de sécurité et du matériel d'apprentissage de sécurité disponibles dans Centre de sécurité.	

Avertissement :
Pour vous assurer que Centre de sécurité de l'instance reçoit des informations de sécurité à jour à chaque mise à niveau, ne personnalisez pas ce module. Si vous modifiez des paramètres de sécurité sur votre instance, assurez-vous de les tester d'abord dans un environnement de non-production.

Messages de l'administrateur

Les messages et les rappels, destinés principalement aux administrateurs, s'affichent au-dessus de la bannière de sécurité rotative.

Par exemple, un message Configurer les notifications de sécurité s'affiche pour rappeler aux administrateurs de configurer les préférences pour les notifications de sécurité s'ils ne l'ont pas déjà fait. Il les oriente également vers la bonne page pour le faire.

Remarque :
La bannière de messages de l'administrateur ne s'affiche pas pour les utilisateurs non-administrateurs ou s'il n'y a pas d'élément actionnable pour les utilisateurs administrateurs.

Bannière de sécurité rotative

Pour vous aider à surveiller l'intégrité de sécurité de votre instance, des messages de sécurité d'instance critique apparaissent dans la bannière rotative.

- Deux à trois messages de sécurité tournent normalement à intervalles réguliers.
- Les points au bas de la bannière vous indiquent le nombre total de messages de sécurité actuels.
- Pour les parcourir, sélectionnez les points ou les flèches qui apparaissent de chaque côté des messages.

Les couleurs d'arrière-plan de la bannière indiquent la gravité relative des messages.

Couleur	Description
Rouge	Situation de sécurité critique nécessitant une réponse rapide, ou une recommandation sur la façon de protéger ou de répondre aux événements de sécurité critiques.
Gris foncé	Message d'avertissement non critique.
Bleu	Message d'informations générales.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour réduire ou réduire le contenu du texte de la bannière, sélectionnez  . Pour agrandir le contenu textuel, sélectionnez-le à nouveau.

- Lorsque vous utilisez à nouveau Centre de sécurité de l'instance, le contenu textuel apparaît réduit ou développé, selon la façon dont vous l'avez utilisé au cours de votre session précédente.
- Si le contenu du texte lui-même change, il apparaît comme agrandi pour tous les utilisateurs.

Rechercher

Utilisez la barre de recherche pour rechercher dans l'ensemble du Centre de sécurité de l'instance des ressources de sécurité qui vous aideront à comprendre et à résoudre les problèmes de sécurité. Vous pouvez rechercher les ressources liées à la sécurité suivantes :

- Now Support Base de connaissances Des articles
- Pages du Centre de sécurité de l'instance
- Liens externes Now Support
- Les widgets de sécurité PA, tels que le score de conformité quotidien et les e-mails entrants externes
- Contenu de la bannière

Ruban d'événement

Utilisez le ruban d'événement pour afficher les mesures clés de surveillance des événements de sécurité pour l'instance actuelle.

- Pour faire défiler manuellement les mesures, sélectionnez les flèches vers la droite ou vers la gauche.
- Pour configurer le ruban d'événement, sélectionnez **Modifier**.

Pour en savoir plus sur le ruban d'événement et sur sa configuration, consultez Surveiller les événements de sécurité et Configurer le ruban des événements de sécurité.

Score de conformité quotidien

La section Score de conformité quotidien contient les vignettes **Score de conformité quotidien**, **Gestion des sessions**, **Sécurisation renforcée**, **Auditeur** et **Ressources** .

Le score de conformité quotidien vous permet d'évaluer l'intégrité de votre instance du point de vue de la sécurité.

Le score de conformité quotidien est un score en pourcentage. Il est basé sur le degré de conformité des paramètres actuels des propriétés de sécurité de votre instance avec les valeurs de conformité publiées dans le Paramètres de la sécurisation pour la sécurité de l'instance.

- Pour en savoir plus sur les calculs quotidiens du score de conformité et sur l'impact de la sécurisation renforcée sur celui-ci, reportez-vous à la section Vérifier le score de conformité quotidien et configurer les paramètres de propriété de sécurité.
- Le bouton **Actualiser** permet à un administrateur de recalculer instantanément le score de conformité quotidien. Pour en savoir plus, consultez Comment les données de score, de tendance et de graphique de conformité quotidienne sont actualisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécurisation renforcée

Utilisez ce processus pour ajuster les propriétés spécifiques de configuration de sécurité qui affectent le score de conformité quotidien :

1. Pour accéder à la page Configurations de la conformité à la sécurisation renforcée et effectuer un renforcement de la sécurité de l'instance, sélectionnez la vignette **Score de conformité quotidien** ou le lien de **sécurisation renforcée** .
2. Indiquez si vous souhaitez afficher tous les contrôles de sécurité ou uniquement les contrôles de sécurité recommandés. Ensuite, sélectionnez la catégorie dans laquelle vous souhaitez travailler.
3. Définissez chaque propriété de configuration de sécurité dans la catégorie sélectionnée. Cliquez sur **Plus d'informations** pour afficher les informations détaillées d'une propriété.

Pour en savoir plus sur le renforcement et l'optimisation des propriétés de configuration de sécurité afin d'accroître davantage la conformité, reportez-vous à la section Ajuster les paramètres de sécurité de l'instance pour accroître la conformité.

Pour en savoir plus sur la façon dont les données de tendances et de graphiques sont actualisées, reportez-vous à la section Comment les données de score, de tendance et de graphique de conformité quotidienne sont actualisées.

Auditeur

Exécutez l'auditeur pour analyser votre instance et rechercher des définitions de sécurité incorrectes. Elle fournit des conclusions que vous pouvez corriger pour aider à améliorer la posture de sécurité de votre instance.

Pour accéder à la page Auditeur, sélectionnez la vignette **Auditeur** ou le lien **Auditeur** . Pour en savoir plus, consultez Rechercher des définitions de sécurité incorrectes.

Gestion des sessions

Utilisez Gestion des sessions pour :

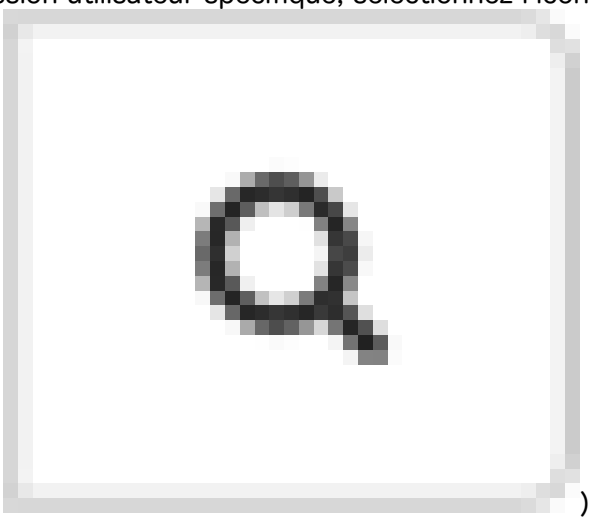
- Affichez et gérez les sessions de connexion de l'utilisateur.
- Affichez la session de connexion de l'utilisateur du nœud actuel auquel vous êtes connecté.
- Consultez les informations détaillées sur chaque session, telles que le nom d'utilisateur et l'adresse IP.
- Isolez et verrouillez les sessions utilisateur spécifiques qui présentent des risques de sécurité.

Pour accéder à la page Gestion des sessions, sélectionnez la vignette ou le lien **Gestion des sessions** .

Champ	Description
Utilisateur	Nom de l'utilisateur associé à cette session de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	• Pour localiser une session utilisateur spécifique, sélectionnez l'icône de recherche Spotlight () pour effectuer une recherche par utilisateur, par mot clé de l'agent utilisateur ou par adresse IP. Par exemple, si vous souhaitez trouver toutes les connexions actuelles à partir d'un type de navigateur spécifique, entrez le nom du navigateur comme mot-clé dans le champ **Agent d'utilisateur** . • Cliquez sur un nom d'utilisateur pour accéder à l'enregistrement du profil d'utilisateur. Vous pouvez modifier le profil d'utilisateur uniquement si un rôle administrateur vous est affecté. **Remarque :** Pour en savoir plus sur les profils d'utilisateur, consultez Créer un utilisateur .
MFA	Case à cocher indiquant si l'authentification multifacteur (MFA) est activée pour l'utilisateur connecté. Pour en savoir plus sur l'authentification multifacteur (MFA), consultez Authentification multifacteur (MFA).
Actifs	Case à cocher indiquant si l'utilisateur connecté est actif ou inactif.
Agent d'utilisateur	Type de navigateur et système d'exploitation de l'appareil pour la session de connexion de l'utilisateur.
Adresse IP	Adresse IP de l'utilisateur connecté.
Dernier accès	Date et heure du dernier accès de cette session utilisateur à l'instance. **Remarque :** Pour afficher des informations détaillées sur une session de connexion particulière, ou pour verrouiller la session elle-même, sélectionnez les champs **Agent utilisateur**, **Adresse IP** ou **Dernier accès** .

Mesures

Affichez les détails des types de mesures suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de mesure	Description
Utilisateur	Mesures de sécurité associées à l'activité de l'utilisateur dans l'instance. Pour accéder à la page Mesures utilisateur, sélectionnez le lien **Mesures** , puis **Mesures utilisateur**.
Exporter	Mesures de sécurité associées aux données exportées à partir de l'instance. Pour accéder à la page Exporter les mesures, sélectionnez le lien **Mesures** , puis sélectionnez **Exporter les mesures**.
Authentification	Mesures de sécurité associées à l'authentification, telles que les adresses IP peu utilisées, les échecs de connexion et les types de schémas d'authentification utilisés par vos utilisateurs. Pour accéder à la page Mesures d'exportation, sélectionnez le lien **Mesures** , puis **Mesures d'authentification**.
E-mail	Mesures de sécurité associées à des comportements anormaux liés aux e-mails entrants dans votre instance. Pour accéder à la page Mesures d'e-mail, sélectionnez le lien **Mesures** , puis **Mesures d'e-mail**.
Antivirus	Mesures de sécurité associées à l'activité de l'événement antivirus dans l'instance. Pour accéder à la page Mesures antivirus, sélectionnez la vignette **Antivirus** ou sélectionnez le lien **Mesures** , puis sélectionnez **Antivirus**.

Remarque :
Pour en savoir plus sur la surveillance de chaque type de mesure, reportez-vous Mesures d'instance de surveillanceà .

Ressources

Accédez aux Now Support Base de connaissances articles, ressources et blogs liés à la sécurité des instances. Ces ressources comprennent les paramètres de sécurité, le codage, la conformité, les correctifs et des rubriques connexes. Pour accéder à la page Ressources :

1. Cliquez sur la vignette ou le lien **Ressources** .
2. Dans la page Ressources, sélectionnez une catégorie :

Catégorie	Description
Directives recommandées	Accès aux directives de sécurité recommandées, y compris les articles du Paramètres de la sécurisation pour la sécurité de l'instanceGuide de codage sécurisé [KB0623354].
Ressources de sécurité	Accès à des ressources liées à la sécurité dans le Base de connaissances, notamment : ○ Test de sécurité de l'instance client ○ Articles de la base de connaissances du Centre de sécurité, de confiance et de conformité dans le cloud

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Notifications de sécurité

Une icône de notifications en forme de cloche () apparaît dans Centre de sécurité de l'instance, avec un décompte total de notifications de sécurité non lues. Les notifications sont conservées et incluses dans ce nombre jusqu'à ce que vous les marquiez comme lues.

1. Cliquez sur l'icône en forme de cloche pour afficher les cinq premières notifications de sécurité non lues.

   Une notification s'affiche lorsque **des événements Connexion administrateur**, **Déverrouillage administrateur**, **Échec de la connexion**, **Rôle de privilège élevé**, **Emprunt d'identité**, **Élévation de la sécurité** et **Synthèse hebdomadaire** ont lieu dans votre instance. Pour en savoir plus sur ces événements de sécurité, reportez-vous Surveiller les événements de sécuritéà .

2. Pour afficher les informations détaillées d'un événement de sécurité spécifique, sélectionnez la notification.

   Par exemple, si vous sélectionnez une notification de rôle de privilège élevé, vous pouvez afficher la table Rôles (sys_user_role). Utilisez cette table pour voir quels utilisateurs ont été affectés à des rôles privilégiés au cours d'une journée civile. Cet historique vous aide à déterminer si les rôles ont été correctement affectés.

3. S'il existe plus de cinq notifications non lues, sélectionnez **Afficher toutes les notifications** pour accéder à une page Toutes les notifications contenant une liste de toutes les notifications non lues.
   - Pour afficher les informations détaillées d'un événement de sécurité spécifique, sélectionnez la notification.
   - Pour marquer toutes les notifications répertoriées comme lues, sélectionnez **Marquer tout comme lu**.

Remarque :
En tant qu'administrateur, vous pouvez également configurer des préférences d'envoi de types spécifiques de notifications pour chaque type d'événement de sécurité. Pour en savoir plus, consultez Définir les préférences pour les notifications d'événements de sécurité.

Visites guidées

Cliquez sur le lien **Visites guidées** pour afficher une visite visuelle guidée du centre de sécurité de l'instance.

- La visite guidée comprend uniquement les fonctions de surveillance de sécurité répertoriées sur la page d'accueil.
- Il n'inclut pas les fonctions de sécurité auxquelles vous accédez lorsque vous sélectionnez les vignettes ou les liens sur la page d'accueil.

Portail de test de sécurité, centre de sécurité et aide

Il s'agit Now Support Portail de services d'une ressource centrale que vous utilisez pour gérer les instances, les tâches et les comptes. Vous pouvez également accéder à des ressources utiles que vous pouvez utiliser pour diagnostiquer et résoudre les problèmes techniques et de sécurité dans votre instance.

Pour accéder à ces ressources, sélectionnez **En savoir plus** ou **Obtenir de l'aide** dans les tuiles suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tuile	Description
Portail de test de la sécurité	Accès au tableau de bord de sécurité dans le portail de test de Now Support sécurité.
Centre de sécurité	Accès à la conformité de sécurité dans le Now Support portail de sécurité.
Aide	Accès aux ressources d'aide suivantes dans le Now Support portail de sécurité : • Demandez à un expert de trouver des réponses aux questions courantes. • Signalez un problème ou une panne à l'assistance technique globale en ServiceNow ouvrant un ticket. • Ressources d'assistance en libre-service, notamment : ◦ Vidéos ◦ Documentation ◦ ServiceNow Community ◦ Base de connaissances ◦ Portail d'erreurs connues ◦ Base de données RFX de sécurité • ServiceNow Community questions qui sont recommandées pour votre utilisation.

Accès à l'Agent virtuel

Il s'agit Agent virtuel d'une plate-forme permettant de fournir une assistance utilisateur par le biais de conversations au sein d'une interface de messagerie.

Une fois les modules d'extension associés installés, les Agent virtuel administrateurs peuvent accéder aux fonctions et Compréhension du langage naturel (NLU) en sélectionnant l'icône Agent virtuel :



Il vous permet d'effectuer les tâches suivantes :

- Posez des questions liées à la sécurité, puis obtenez des réponses récapitulatives rapides et des liens de référence pour en savoir plus.
- Obtenir des réponses liées aux processus tels que :
  - Centre de sécurité de l'instance
  - Sécurité de la plateforme
  - ServiceNow Politiques de sécurité
  - Confiance, gouvernance et risque
- Recherchez des ressources liées à la sécurité, telles que Base de connaissances des Now Support rubriques du portail de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour en savoir plus sur l'utilisation et l'activation de , Agent virtuelconsultez :

- Agent virtuel
- Activer l'interface ISC Agent virtuel

Centre de sécurité de l'instance vers ServiceNow Centre de sécurité migration

Découvrez les principales différences lors de la migration du Centre de sécurité de l'instance (ISC) vers ServiceNow Centre de sécurité (SSC).

Important :

Centre de sécurité de l'instance est un produit hérité dont la commercialisation prendra fin d'ici septembre 2024. Centre de sécurité ServiceNow est la solution que les clients doivent adopter à l'avenir. Pour en savoir plus, consultez l'article Processus de dépréciation (KB0867184) dans la base de connaissances Now Support.

ServiceNow Centre de sécurité (SSC) est une application de sécurité qui se compose d'un ensemble d'outils spécialement conçus pour aider les organisations à maintenir la sécurité de leurs ServiceNow déploiements. Grâce à SPC, les organisations peuvent améliorer leur posture de sécurité, renforcer leurs niveaux de conformité et le faire avec une expérience utilisateur transparente.

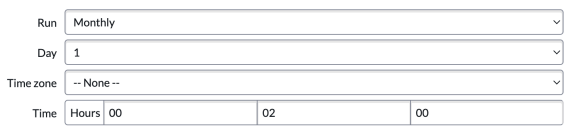
Utilisez ce document pour en savoir plus sur les améliorations apportées aux fonctionnalités de SPC et sur la façon d'exécuter des tâches dans SPC qui étaient auparavant effectuées dans ISC.

Sécurisation renforcée de la sécurité

Améliorations des fonctionnalités	ISC par rapport à SSC
Mises à jour de l'interaction de l'	• Passez en revue le tout dernier score en accédant à la vue d'ensemble ou à la page de comparaison de sécurisation renforcée. • Mettez à jour manuellement le tout dernier score en accédant à Vue d'ensemble et en sélectionnant Mettre à jour le score. • Modifiez la configuration des paramètres en sélectionnant un lien de nom de paramètre sur l'une de ces pages, puis apportez des modifications sur la page de **détails Paramètres** : ○ Vue d'ensemble ○ **Sécurisation renforcée** > **Tous les paramètres** ○ **Sécurisation renforcée** > **Comparaison**
Définir un calendrier pour recalculer votre score de conformité	À l'aide de SPC, vous pouvez définir le moment où le système déclenche une actualisation de votre score de conformité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Améliorations des fonctionnalités	ISC par rapport à SSC
	1. Accédez à la table Exécutions de script planifiées [sysauto_script]. 2. Recherchez et ouvrez l'enregistrement SC - Calculer la conformité mensuelle. 3. Utilisez les champs **Exécution**, **Jour**, **Fuseau horaire** et **Heure** pour définir votre calendrier préféré.  4. Sélectionnez **Mettre à jour** pour enregistrer vos changements.

Indicateurs KPI et mesures de sécurité

Améliorations des fonctionnalités	ISC par rapport à SSC
Améliorations apportées aux KPI	À l'aide de SCC, vous pouvez : • Affichez la tendance du score dans le temps. • Surveillez tous les KPI et mesures à l'aide de la même interface et des mêmes capacités d'analyse.
Améliorations apportées aux mesures	SCC inclut les améliorations suivantes en matière de mesures : • Plus de 65 mesures ont été ajoutées. • Surveillez et analysez les KPI et les mesures à partir d'une interface utilisateur unique. • Créez des cibles et des seuils pour les mesures.
Mises à jour de l'interaction de l'	Accédez aux mesures dans SPC en naviguant vers **Vue d'ensemble** > **Mesures**, puis en sélectionnant Mesure dans le menu de navigation. Vous pouvez également accéder à **Toutes les mesures**.

Scanner de sécurité

Améliorations des fonctionnalités	ISC par rapport à SSC
Nouvelle fonctionnalité	SCC comprend les fonctions suivantes : • Exécutez manuellement des analyses ou planifiez-les pour qu'elles s'exécutent à des heures précises. • Créez vos propres vérifications d'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Améliorations des fonctionnalités	ISC par rapport à SSC
	• Créez votre propre suite d'analyse. • Comparez les résultats de deux analyses.
Amélioration de la fonctionnalité d'e-mail	Configurez des notifications par e-mail pour rester informé des événements de sécurité sur votre instance.
Mises à jour de l'interaction de l'	• Pour exécuter l'analyse de l'auditeur, accédez à **Vue d'ensemble** > **Analyse** > **Suites** et en sélectionnant **Suite d'auditeurs** dans la liste. • Voir les résultats de l'analyse en accédant à **Vue d'ensemble** > **Analyse** > **Résultats**.

Fonctionnalités de sécurité supplémentaires

Améliorations des fonctionnalités	ISC par rapport à SSC
Fonctionnalité des sessions de surveillance	• Visualisez les activités de la session à l'aide de .Analytics Hub • Surveillez l'activité de la session en accédant à **Mesures** > **Sessions**.
Trouver des ressources	Accédez à toutes les ressources d'apprentissage sur une seule page à l'adresse **Vue d'ensemble** > **Apprentissage**.

Surveiller les événements de sécurité

Analysez les mesures d'événements dans votre instance afin d'identifier et de prévenir les événements de sécurité potentiels.

Important :

Le Centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers ServiceNow Centre de sécurité migration.

Dans le ruban de l'événement, qui se trouve sur la page d'accueil Sécurité de l'instance, vous pouvez analyser ces mesures et les détails qui les accompagnent pour identifier les événements de sécurité potentiels dans l'instance.

- Pour chaque mesure d'événement, un nombre de scores uniques en temps réel s'affiche, indiquant combien de fois l'événement s'est produit au cours de la journée dans cette instance. Ces rapports à score unique sont mis à jour automatiquement au fur et à mesure que les événements correspondants se produisent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Chaque mesure d'événement contient également des informations sur les tendances de conformité et les graphiques sur une plage de dates. Ces informations sont mises à jour quotidiennement lorsque vous exécutez la tâche d'analyse des performances. Pour en savoir plus, consultez la section **Analyse des détails de tendance d'événement** .

Types d'événements

Vous pouvez surveiller au moins six des types d'événements suivants. Pour plus de six événements, utilisez les flèches gauche ou droite sous le ruban d'événement pour les faire défiler. Pour en savoir plus sur la configuration du ruban d'événements, reportez-vous à la section Configurer le ruban des événements de sécurité.

Préférence de notification	Description
Connexions des administrateurs	Nombre de tentatives de connexion dans cette instance, au cours d'un jour calendaire, par des utilisateurs à qui un rôle administrateur est affecté.
Utilisateurs administrateurs ajoutés	Nombre d'utilisateurs ayant un rôle administrateur qui ont été ajoutés dans cette instance au cours de la journée civile. Par exemple, votre instance peut rencontrer un problème de sécurité si le nombre est de 10, mais que 4 utilisateurs sont connus pour avoir un rôle administrateur affecté.
E-mail entrant externe	Pour en savoir plus, consultez Mesures d'e-mail.
Connexions externes	Nombre d'utilisateurs avec un rôle de snc_external affecté qui se sont connectés à cette instance au cours de la journée civile. Ces connexions sont généralement utilisées à des fins de maintenance, d'assistance, de conseil ou d'audit. La surveillance de cette mesure vous permet de vérifier que les tentatives de connexion externe sont légitimes et qu'il ne s'agit pas de problèmes de sécurité potentiels. Pour en savoir plus sur l'affectation des rôles d'utilisateur externe, reportez-vous à la section Explicit Roles.
Échecs de connexion	Nombre de tentatives de connexion ayant échoué dans cette instance au cours de la journée civile. Cette mesure peut indiquer que des tentatives de connexion sont faites et compromettent la sécurité de votre instance.
Emprunts d'identité	Nombre de connexions d'emprunt d'identité dans cette instance au cours de la journée calendaire. Pour en savoir plus sur l'emprunt d'identité d'un utilisateur, consultez Emprunter l'identité d'un utilisateur .
Fichiers en quarantaine	Nombre de fichiers qui ont été mis en quarantaine lors de l'exécution Analyse anti-virus dans cette instance au cours d'un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préférence de notification	Description
	jour calendaire. Pour en savoir plus sur les fichiers mis en quarantaine et Analyse anti-virus, consultez et Mesures antivirusAnalyse anti-virus.
Élévations de la sécurité	Nombre de fois où un administrateur de sécurité a élevé la sécurité pour les utilisateurs standard en changeant leur rôle d'utilisateur affecté en un rôle de sécurité à privilège élevé au cours d'une journée civile. Ces rôles de sécurité à privilège élevé comprennent oauth_admin, administrateur, security_admin et emprunteur d'identité. • Cette mesure indique que quelqu'un a peut-être essayé d'augmenter la sécurité d'un utilisateur non autorisé. N'utilisez pas cette mesure seule pour détecter une compromission de sécurité spécifique. Au lieu de cela, traitez cette mesure comme une indication que vous devez vérifier une autre mesure pour voir si une compromission de sécurité s'est produite. • Pour en savoir plus sur l'amélioration de la sécurité des utilisateurs, consultez Élever à un rôle privilégié et Rôles à privilèges élevés.
Connexions SNC	Nombre de membres du personnel qui se sont connectés à cette instance à l'aide de Service et assistance client la technique de saut hi-hop au cours de la journée civile. Ces connexions sont généralement utilisées à des fins de maintenance, d'assistance, de conseil ou d'audit. Pour plus d'informations sur le contrôle ServiceNow de l'accès des employés de l'entreprise, consultez Contrôle d'accès ServiceNow.
Courrier indésirable	Pour en savoir plus, consultez Mesures d'e-mail.
E-mail entrant approuvé	Pour en savoir plus, consultez Mesures d'e-mail.
E-mail entrant non approuvé	Pour en savoir plus, consultez Mesures d'e-mail.
Types de virus	Nombre de types différents d'événements antivirus qui se sont produits dans cette instance au cours d'un jour calendaire. Pour en savoir plus sur les types d'événements antivirus, consultez Mesures antivirus.

Analyse des détails de tendance d'événement

Pour afficher les détails de la tendance d'une mesure d'événement, cliquez sur le nombre d'événements pour accéder à la page Centre d'analyse. Les détails qui s'affichent pour l'instance dépendent du type de mesure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, pour afficher la liste de chaque tentative échouée sur la page Journaux des événements du tableau de bord de sécurité :

- Sélectionnez la mesure **Échecs de connexion** .
- Dans la page, cliquez sur Afficher les Centre d'analyse**enregistrements**.
- Cliquez sur l'une des tentatives de connexion échouées.
- Le détail comprend le nom de l'utilisateur qui a tenté de se connecter, son adresse IP et le nom de la table à laquelle il a essayé d'accéder.

Vous pouvez configurer des déclencheurs de seuil d'événement dans le Centre d'analyse pour fournir des alertes lorsqu'un certain événement se produit dans une plage de scores pour un indicateur. Vous pouvez également définir des cibles qui vous permettent de visualiser la différence entre le score souhaité et le score réel d'un événement.

Par exemple, vous pouvez définir un seuil de 10 pour la mesure **Échecs de connexion** . Lorsque dix tentatives de connexion infructueuses ou plus se produisent au cours de la journée, une alerte est envoyée au personnel de sécurité spécifique. Vous pouvez également définir une cible similaire qui fournit un point culminant visuel lorsque 10 échecs de connexion se produisent au cours d'une Centre d'analyse journée.

Les données et les graphiques de tendance qui apparaissent dans la mosaïque du ruban d'événement et sont mis à jour après l'exécution de la tâche d'analyse Centre d'analyse des performances à 02h00 heure locale. Pour en savoir plus, consultez Comment les données de score, de tendance et de graphique de conformité quotidienne sont actualisées.

Information associée

Centre de sécurité de l'instance

Now Intelligence

Centre d'analyse

Cibles et seuils d'Analyse des performances

Configurer le ruban des événements de sécurité

Configurez le ruban des événements de sécurité sur la page d'accueil du centre de sécurité de l'instance pour inclure uniquement les événements pertinents pour le suivi de la sécurité de l'instance dans vos opérations. Vous pouvez également modifier l'ordre dans lequel les vignettes d'événement de sécurité s'affichent sur le ruban.

Avant de commencer

Rôle requis : security_dashboard_user ou admin

Pourquoi et quand exécuter cette tâche

Le ruban des événements de sécurité est initialement renseigné avec un ensemble complet d'événements de sécurité standard. Vous pouvez le personnaliser en supprimant les événements qui ne sont pas pertinents pour votre organisation.

- Par exemple, si vous soupçonnez que les problèmes de sécurité sont dus aux actions du personnel interne, incluez les indicateurs d'événements Connexions administrateur, Utilisateurs administrateurs ajoutés et Élévations de sécurité.
- Ces indicateurs surveillent le nombre de fois où des utilisateurs disposant de rôles d'administrateur ont tenté de se connecter et, si des utilisateurs administrateurs ont été ajoutés, les tentatives d'élévation des rôles de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour en savoir plus sur les types d'événements de sécurité qui apparaissent dans le ruban d'événements, reportez-vous à la section Surveiller les événements de sécurité.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Dans le ruban de l'événement, cliquez sur **Modifier** (< > Edit).
   Dans le formulaire Modifier les événements, la colonne **Sélectionné** contient les événements qui sont déjà répertoriés.
3. Pour ajouter des événements de sécurité au ruban d'événement, déplacez-les de la colonne **Disponible** vers la colonne **Sélectionné** .
   Pour modifier l'ordre dans lequel les événements s'affichent sur le ruban, sélectionnez-le, puis cliquez sur sa flèche vers le haut ou vers le bas pour le déplacer à sa position correcte.
   - Placez les événements dans le même ordre séquentiel qu'ils doivent apparaître sur le ruban d'événements du Centre de sécurité de l'instance.
   - Les événements que vous placez en haut de la colonne **Disponible** s'affichent de manière séquentielle, en commençant par le côté gauche du ruban d'événements Centre de sécurité de l'instance. Les événements placés vers le bas de la colonne s'affichent à droite sur le ruban d'événement.
4. Pour supprimer des événements de sécurité du ruban d'événements :
   - Dans la colonne **Sélectionné** , sélectionnez les événements de sécurité que vous souhaitez supprimer du ruban d'événements.
   - Déplacez-les de la colonne **Sélectionné** vers la colonne **Disponible** .
5. Cliquez sur **Enregistrer**.

Information associée

Centre de sécurité de l'instance

Définir les préférences pour les notifications d'événements de sécurité

Configurez les préférences relatives aux types de notifications que vous souhaitez recevoir pour les occurrences d'événements de sécurité spécifiques. Pour chaque type, vous indiquez si vous souhaitez recevoir des notifications par e-mail, par notification push dans Now Mobile, ou dans des applications de messagerie tierces telles que Slack ou Microsoft Teams.

Avant de commencer

Pour permettre aux applications de messagerie tierces d'envoyer des notifications d'événements de sécurité, vous devez activer le module d'extension Notification de messagerie (com.glide.notification.messaging). Chaque utilisateur doit configurer ses propres paramètres. Pour plus d'informations, consultez Notifications dans les applications de messagerie .

Rôle requis : admin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sur la page d'accueil d'Instance Security Center, cliquez sur le menu de profil, puis sur **Préférences de notification**.

Préférences de notification

Préférence de notification	Description
Connexion de l'administrateur	Envoyez le type de notification sélectionné chaque fois que d'autres utilisateurs avec des rôles d'administrateur affectés se connectent à cette instance à partir d'une adresse IP différente.
Déverrouillage par l'administrateur	Envoyer le type de notification sélectionné chaque fois qu'un compte pour un utilisateur à privilèges élevés a été déverrouillé.
Échec de la connexion	Envoyez le type de notification sélectionné chaque fois que d'autres utilisateurs ne parviennent pas à se connecter à cette instance en moins de tentatives que le nombre défini dans la `glide.user.max_unlock_attempts` propriété. Si vous ne configurez pas cette propriété, la valeur par défaut est 5. Pour en savoir plus sur cette propriété, reportez-vous à la section Spécifier le verrouillage pour les échecs de tentatives de connexion.
Rôle HP ajouté	Envoyez le type de notification sélectionné chaque fois qu'un rôle de sécurité à privilège élevé (y compris les rôles oauth_admin, administrateur, security_admin et emprunteur d'identité) est accordé à un autre utilisateur. Pour en savoir plus sur l'amélioration de la sécurité des utilisateurs, consultez Élever à un rôle privilégié et Rôles à privilèges élevés.
Emprunt d'identité	Envoyez le type de notification sélectionné chaque fois qu'un autre utilisateur emprunte votre identité. Pour en savoir plus sur l'emprunt d'identité d'utilisateurs, consultez Emprunter l'identité d'un utilisateur.
Élévation de la sécurité	Envoyez le type de notification sélectionné chaque fois que d'autres utilisateurs sont élevés au rôle d'administrateur de sécurité dans cette instance.
Résumé hebdomadaire	Envoyer une synthèse hebdomadaire sur le type de notification sélectionné. Il comprend :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préférence de notification	Description
	○ Récapitule toutes les activités de sécurité qui ont eu lieu dans cette instance tout au long de la semaine. ○ Le score de conformité quotidien actuel de l'instance.

2. Pour chaque type d'événement de sécurité, cochez les cases appropriées afin de désigner le type de notifications à vous envoyer.
   Vous pouvez sélectionner plusieurs méthodes de notification pour chacune.

3. Cliquez sur **Enregistrer**.

Vérifier le score de conformité quotidien et configurer les paramètres de propriété de sécurité

Passez en revue la mesure du score de conformité quotidien et les propriétés de configuration de sécurité pour voir si votre instance est conforme aux exigences de sécurité suggérées. Vous pouvez affecter le score de conformité quotidien en mettant à jour les propriétés de sécurité non conformes dans la page Configurations de la conformité à la sécurisation renforcée.

Important :

Le Centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers ServiceNow Centre de sécurité migration.

Le score de conformité quotidien est un score en pourcentage. Il est basé sur le degré de conformité des paramètres actuels des propriétés de sécurité de votre instance avec les valeurs de conformité publiées dans le Paramètres de la sécurisation pour la sécurité de l'instance.

Vérifiez régulièrement le score de conformité quotidien de votre instance. Suivez ces conseils lorsque vous évaluez votre score de conformité quotidien :

- Une valeur supérieure ou égale à 90 % indique que l'instance est conforme aux contrôles de sécurité critiques.
- Une valeur supérieure ou égale à 50 % et inférieure à 90 % indique un niveau modéré de conformité de la sécurité.
- Un niveau inférieur à 50 % indique un faible niveau de conformité en matière de sécurité.

Ajuster les paramètres de sécurité de l'instance pour accroître la conformité

À l'aide de la page Configuration de la conformité à la sécurisation renforcée, renforcez et optimisez les propriétés de sécurité non conformes qui affectent le score de conformité quotidien de votre instance. Son utilisation garantit que votre instance est conforme aux normes de sécurisation renforcée publiées, tout en répondant aux exigences de sécurité de votre entreprise.

Avant de commencer
Rôle requis : security_dashboard_user ou admin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

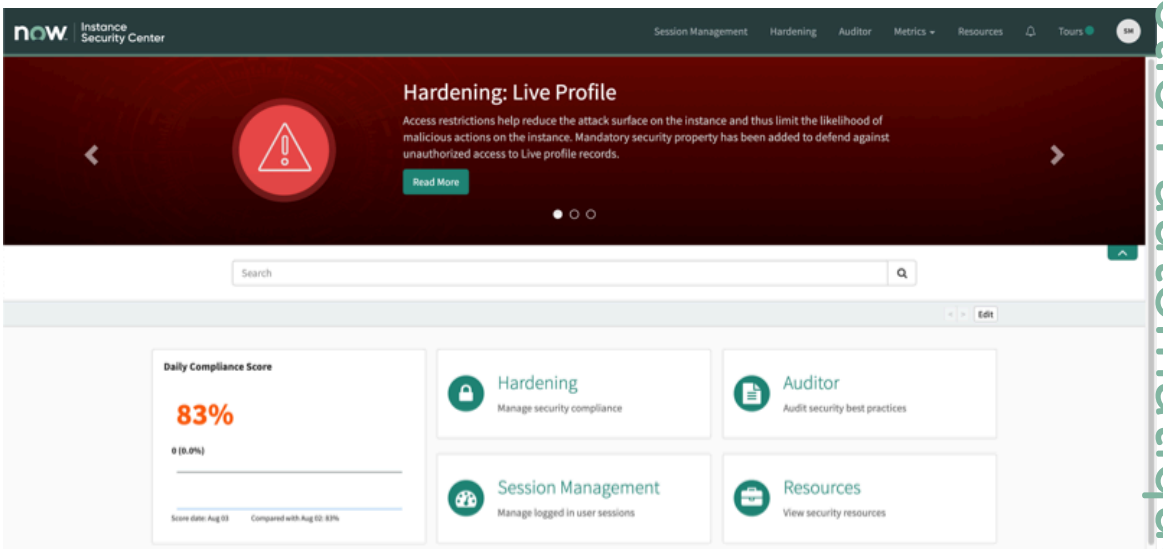
Consultez le contenu pour connaître les Paramètres de la sécurisation pour la sécurité de l'instance descriptions détaillées et les valeurs de conformité des modules d'extension et des propriétés système liés à la sécurité dans le Now Platform.

- Consultez les paramètres de renforcement de la sécurité de l'instance chaque fois que vous définissez ou mettez à jour des propriétés liées à la sécurité, même si certaines des valeurs de conformité peuvent ne pas convenir à votre instance.
- Lorsque vous mettez à jour ces propriétés, assurez-vous que l'instance continue de se comporter comme prévu. Consultez le personnel interne approprié qui possède l'expertise nécessaire pour déterminer les impacts sur la sécurité.

Remarque :
Si vous disposez d'un rôle administrateur, vous pouvez afficher et modifier les contrôles de sécurité. Si vous disposez d'un rôle security_dashboard_user, vous pouvez afficher les contrôles de sécurité, mais vous ne pouvez pas les modifier.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Cliquez sur la vignette **Score de conformité quotidien** ou sur le lien **de sécurisation renforcée** pour accéder à la page de configuration de la conformité à la sécurisation renforcée.



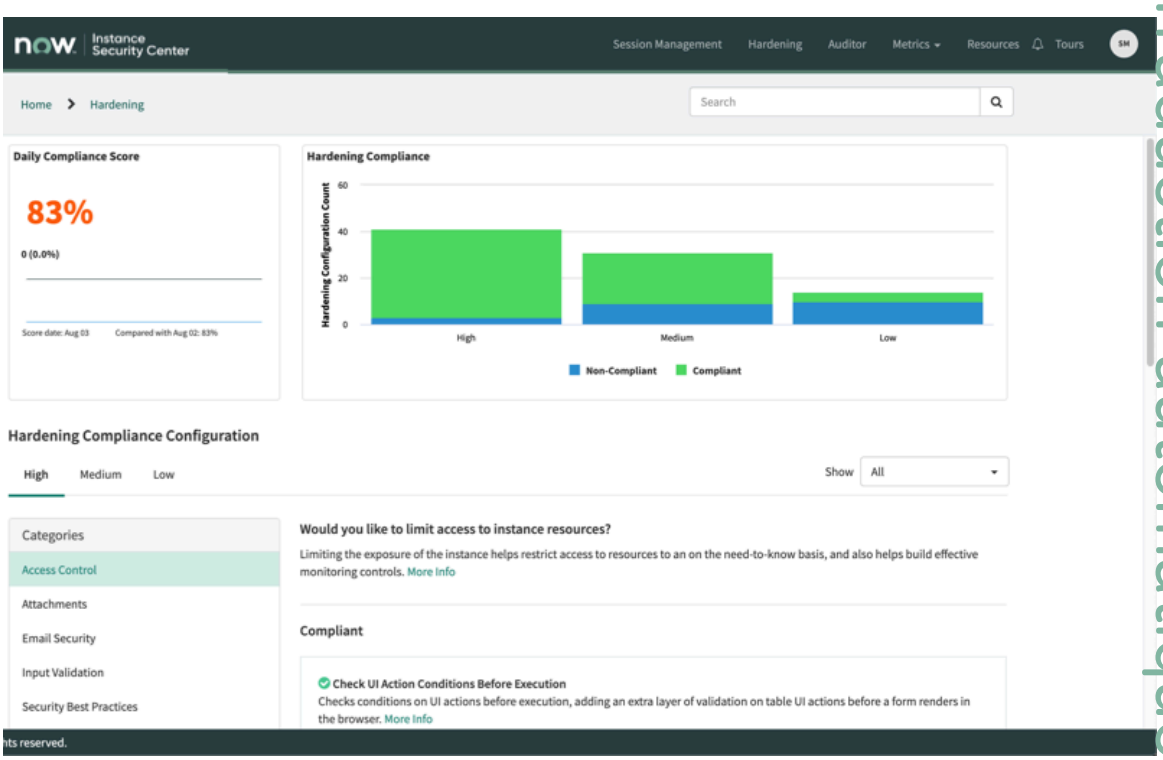
3. Dans le graphique de conformité à la sécurisation renforcée, affichez les statistiques pour les propriétés de configuration de sécurité conformes et non conformes.

Option	Description
Conforme	Nombre de propriétés de configuration de sécurité conformes aux valeurs de conformité des paramètres de sécurisation renforcée de la sécurité de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	Remarque : Vous ne pouvez pas modifier les paramètres des propriétés de sécurité conformes dans la configuration de la conformité à la sécurisation renforcée. Pour ce faire, vous devez les mettre à jour dans les propriétés système. Pour en savoir plus, reportez-vous à la section Ajouter une propriété système .
Non conforme	Nombre de propriétés de configuration de sécurité qui ne respectent pas les valeurs de conformité des paramètres de renforcement de la sécurité de l'instance. Vous pouvez mettre à jour les paramètres des propriétés non conformes.



Remarque :
Pour afficher le nombre de scores de sécurité conformes ou non conformes sur une plage de dates, déplacez le point bleu du curseur sous le score de conformité quotidien.

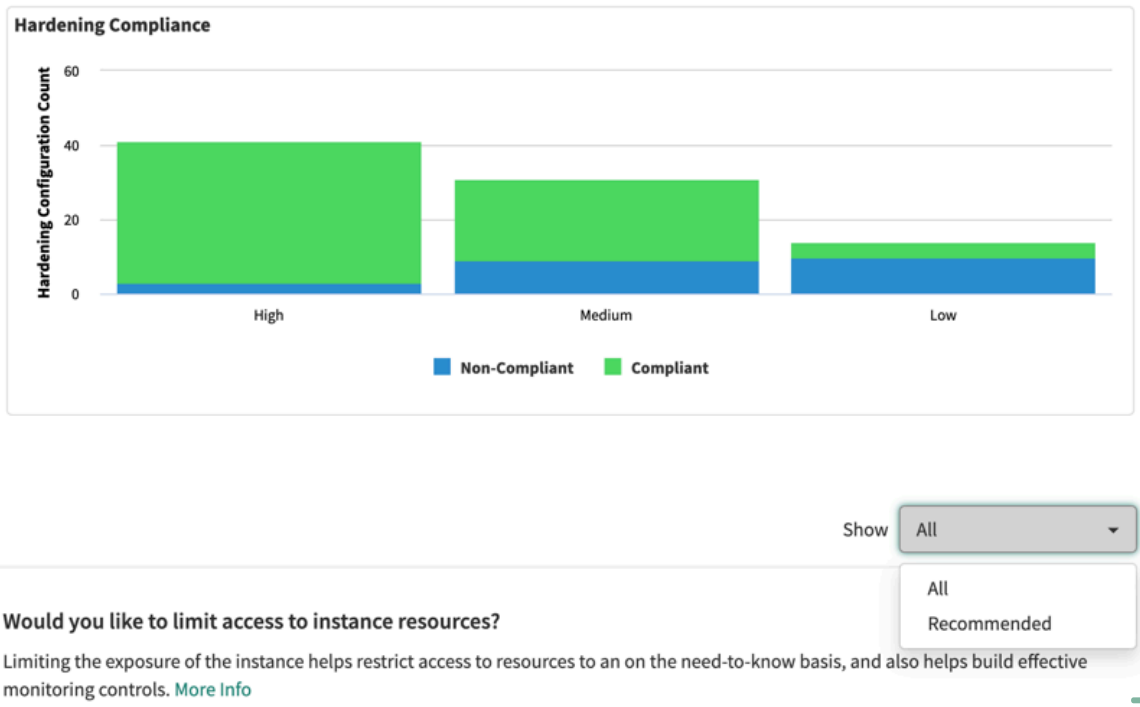
4. Dans la liste **Afficher** sous le graphique, spécifiez si vous souhaitez accéder à toutes les propriétés de configuration de sécurité ou uniquement à celles recommandées.

Option	Description
Tous	(Par défaut) Toutes les propriétés de configuration de sécurité conformes et non conformes dans chaque catégorie sélectionnée.
Recommandé	Seules les propriétés de configuration de sécurité recommandées s'affichent dans chaque catégorie sélectionnée. Ces propriétés de configuration de sécu-

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

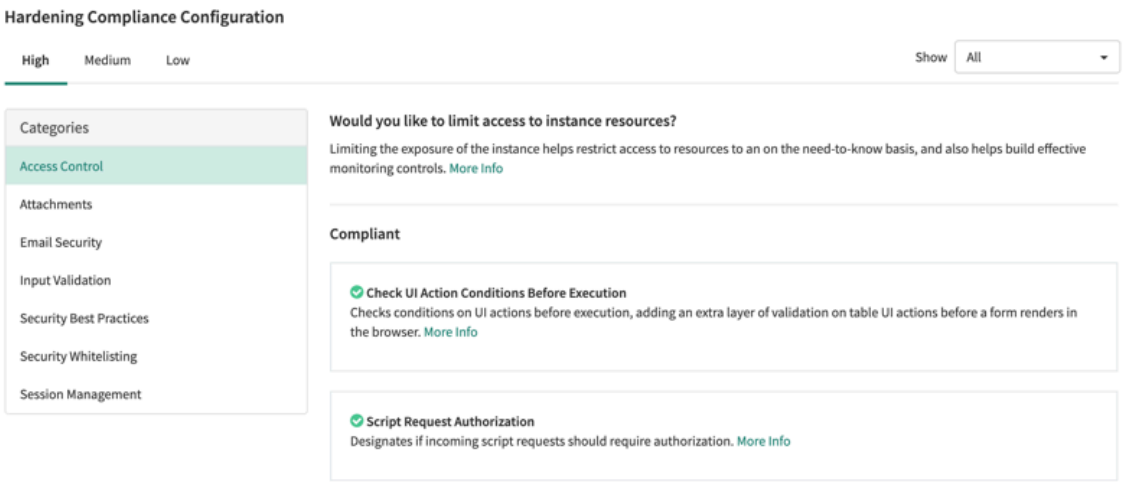
Option	Description
	rité sont un sous-ensemble sélectionné des propriétés les plus critiques utilisées pour sécuriser le Now Platformfichier . Considérez ces propriétés de configuration de sécurité comme le strict minimum de paramètres que vous devez définir pour sécuriser le Now Platformfichier . **Remarque :** Pour sécuriser entièrement votre instance, utilisez l'option **Tout** . Elle inclut également toutes les propriétés de configuration de sécurité recommandées.



5. Dans **Catégories**, sélectionnez la catégorie qui contient les propriétés de configuration de sécurité auxquelles vous souhaitez accéder :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Option	Description
Contrôle d'accès	Les contrôles d'accès déterminent s'il faut accorder ou refuser l'accès des utilisateurs à une ressource particulière en fonction des personnes autorisées à utiliser ces ressources. Pour en savoir plus, consultez Contrôle d'accès les paramètres de renforcement de la sécurité de l'instance.
Pièces jointes	Les contrôles de sécurité des pièces jointes permettent de valider les pièces jointes entrantes afin de protéger votre instance contre les fichiers malveillants envoyés par des attaquants. Pour en savoir plus, consultez Pièces jointes les paramètres de renforcement de la sécurité de l'instance.
Sécurité de la messagerie	La sécurité des e-mails englobe des propriétés de configuration de sécurité qu'un administrateur peut configurer pour s'assurer que des politiques de sécurité appropriées sont en place pour tous les e-mails entrants. Pour en savoir plus, consultez Sécurité des e-mails (renforcement de la sécurité de l'instance) les paramètres de renforcement de la sécurité de l'instance.
Validation de l'entrée	La validation des entrées inclut des propriétés liées à la sécurité qu'un administrateur peut configurer pour minimiser la saisie de données mal formées, quelle que soit leur source. Pour en savoir plus, consultez Validation de l'entrée les paramètres de renforcement de la sécurité de l'instance.
Communications sécurisées	Les propriétés de communications sécurisées sont celles qu'un administrateur peut configurer pour sécuriser le transport du trafic HTTP. Pour en savoir plus, consultez Communications sécurisées les paramètres de renforcement de la sécurité de l'instance.
Bonnes pratiques de sécurité	Les bonnes pratiques de sécurité englobent les tâches de sécurité qu'un administrateur doit effectuer périodiquement, dans un certain intervalle de temps, et incluent les propriétés de configuration associées. Pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	en savoir plus, consultez Bonnes pratiques de sécurité les paramètres de renforcement de la sécurité de l'instance.
Liste d'inclusion de sécurité	La liste d'inclusion de sécurité comprend des propriétés liées à la sécurité qu'un administrateur peut configurer pour restreindre le comportement aux listes d'inclusion connues. Pour en savoir plus, consultez Liste d'inclusion de sécurité les paramètres de sécurisation pour la sécurité de l'instance
Gestion des sessions	La gestion des sessions comprend des propriétés liées à la sécurité qu'un administrateur peut configurer pour garantir une gestion de session sécurisée dans le Now Platform. Pour en savoir plus, consultez Gestion des sessions les paramètres de sécurisation pour la sécurité de l'instance

6. Configurez les propriétés de sécurité non conformes dans la catégorie sélectionnée.
   - Sauf indication contraire, le fait de faire glisser l'interrupteur définit une propriété de sécurité sur le paramètre recommandé. Par exemple, vous définissez la plupart des contrôles sur vrai ou faux, mais certains nécessitent la saisie d'une ou de plusieurs valeurs, telles qu'une liste de valeurs séparées par des virgules.
   - Pour accéder à la rubrique Paramètres de la sécurisation renforcée de l'instance dédiée pour le contrôle de sécurité et en savoir plus, cliquez sur **Plus d'informations**.

Résultats

Le score de conformité quotidien augmente ou diminue en fonction des modifications que vous apportez aux paramètres de contrôle de sécurité non conformes.

Information associée

Centre de sécurité de l'instance

Comment les données de score, de tendance et de graphique de conformité quotidienne sont actualisées

Les données de graphique et de tendance dans Centre de sécurité de l'instance sont mises à jour après l'exécution de la tâche d'analyse des performances à 02h00 heure locale. Il apparaît dans la vignette Score de conformité quotidien, dans les tuiles du ruban Événement et dans les détails de la Centre d'analyse page lorsque vous cliquez sur l'une des tuiles de l'événement.

La tâche de gestion quotidienne des données [AppSec] est une tâche planifiée régulièrement qui s'exécute de nuit et effectue les tâches suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Vérifie si des utilisateurs valides ont été affectés aux tâches de gestion quotidienne des données [AppSec] et de collecte quotidienne de données [PA AppSec] lorsque vous les planifiez pour la première fois.
   - Si vous avez saisi un utilisateur valide dans le champ **Exécuter en tant que** , le traitement de la tâche se poursuit. Un utilisateur valide est un utilisateur qui n'est pas verrouillé hors de l'instance et auquel un rôle administrateur a été affecté.
   - Si vous avez entré un utilisateur non valide, un message d'erreur s'affiche au-dessus de la bannière de sécurité rotative dans Centre de sécurité de l'instance.

   Remarque :
   Pour en savoir plus sur la mise à jour de l'utilisateur affecté lors de l'exécution de travaux planifiés, consultez Créer ou planifier un travail de collecte de données .

2. Exécute la logique métier pour définir l'état de conformité des propriétés de sécurité que vous configurez dans la page Configuration de la conformité à la sécurisation renforcée. Pour en savoir plus, consultez Vérifier le score de conformité quotidien et configurer les paramètres de propriété de sécurité.
3. Exécute la tâche d'analyse des performances de collecte de données quotidiennes [PA AppSec] pour collecter des données de conformité et mettre à jour le score de conformité quotidien.

Actualisation manuelle du score de conformité quotidien

Si un rôle administrateur vous est affecté, vous pouvez également actualiser et recalculer le score de conformité quotidien à tout moment en cliquant sur **Actualiser**.

Remarque :
Le bouton **Actualiser** ne s'affiche pas pour les utilisateurs ayant un rôle security_dashboard_user affecté.

- La fonction d'actualisation effectue les mêmes tâches que la tâche d'analyse des performances Collecte de données quotidiennes, mais en temps réel et non par lots.
- Vous l'utilisez généralement lorsque vous souhaitez effectuer des mises à jour du score de conformité quotidien pour afficher immédiatement l'impact des activités de sécurité de l'instance.
- Il peut y avoir un léger délai avant que le score mis à jour n'apparaisse.

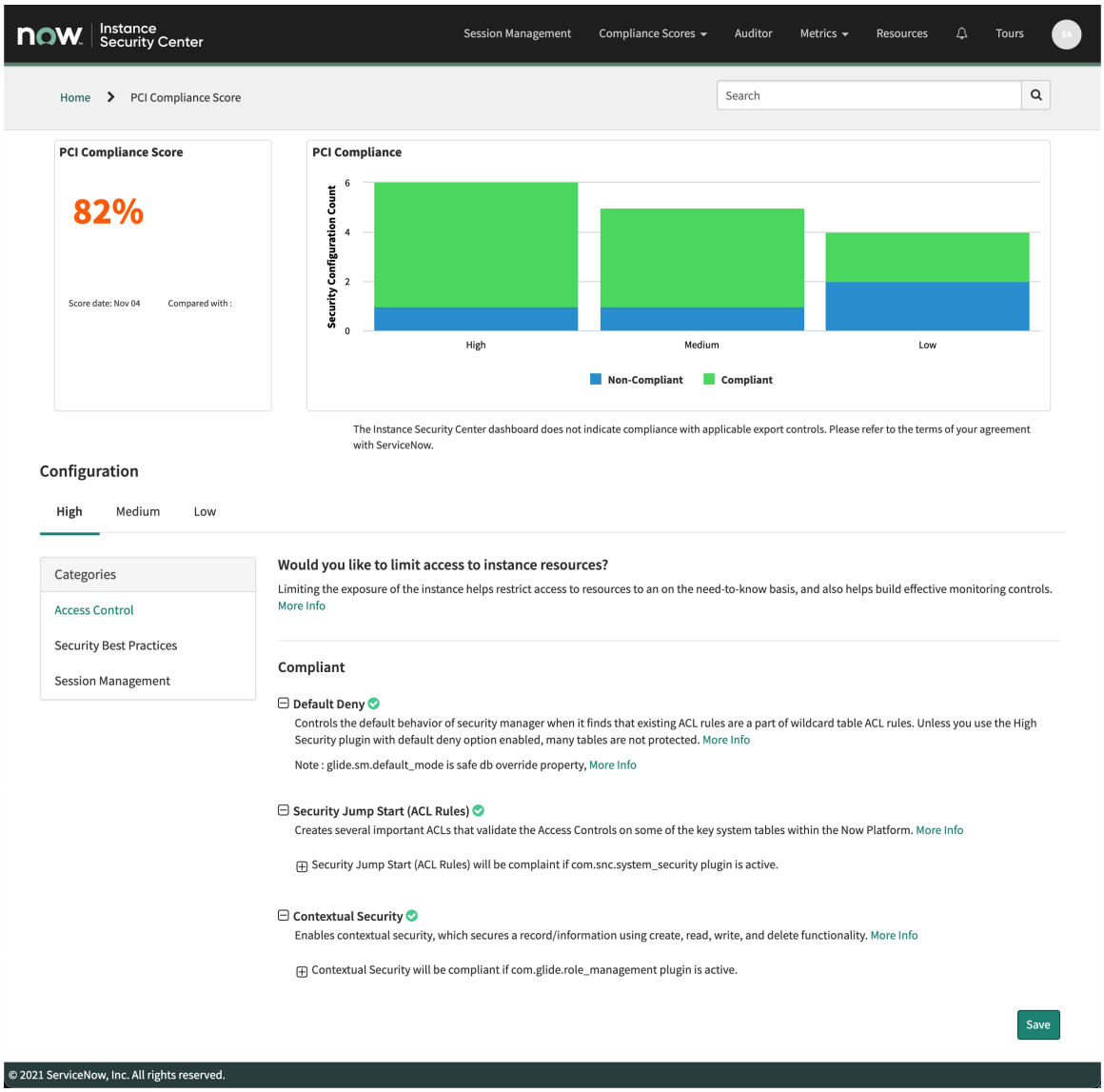
Remarque :
Lorsque vous effectuez une mise à niveau (par exemple, de vers Xanadu), le module d'extension Centre de London sécurité de l'instance (ISC) est automatiquement activé. Un script correctif fourni affecte automatiquement un utilisateur personnalisé sans rôles affectés.

Tableau de bord des scores de conformité PCI

Le tableau de bord des scores de conformité PCI indique dans quelle mesure votre instance est conforme aux normes de sécurité PCI (payment card industry). Utilisez le tableau de bord pour afficher votre score de conformité et modifier votre configuration afin d'améliorer la sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Rôles Now Platform requis

security_dashboard_user ou administrateur, nécessaire pour afficher le tableau de bord des scores de conformité PCI.

Accéder au tableau de bord des scores de conformité PCI

Pour ouvrir le tableau de bord, accédez à **Sécurité de système** > **Centre de sécurité de l'instance**. Dans le centre de sécurité de l'instance, cliquez sur **Scores de conformité** dans l'en-tête, puis sélectionnez **Score de conformité PCI**.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Utilisateur du tableau de bord de sécurité (security_dashboard_user)	Surveillez et gérez en permanence la conformité de la sécurité de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateur	Utilisation du tableau de bord
Administrateur (admin)	Surveillez en permanence la conformité de la sécurité de l'instance pour détecter les menaces de sécurité et y répondre.

Indicateurs

Indicateur	Description
Score de conformité PCI	Affiche le score de conformité de votre instance sous forme de pourcentage. Ce pourcentage représente le pourcentage de configurations de sécurité sur votre instance qui respectent les normes de conformité. L'indicateur affiche également la date à laquelle le score de conformité a été calculé, ainsi qu'une comparaison avec le score calculé précédemment.

Visualisation des données

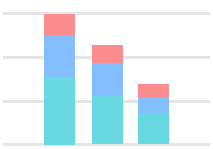
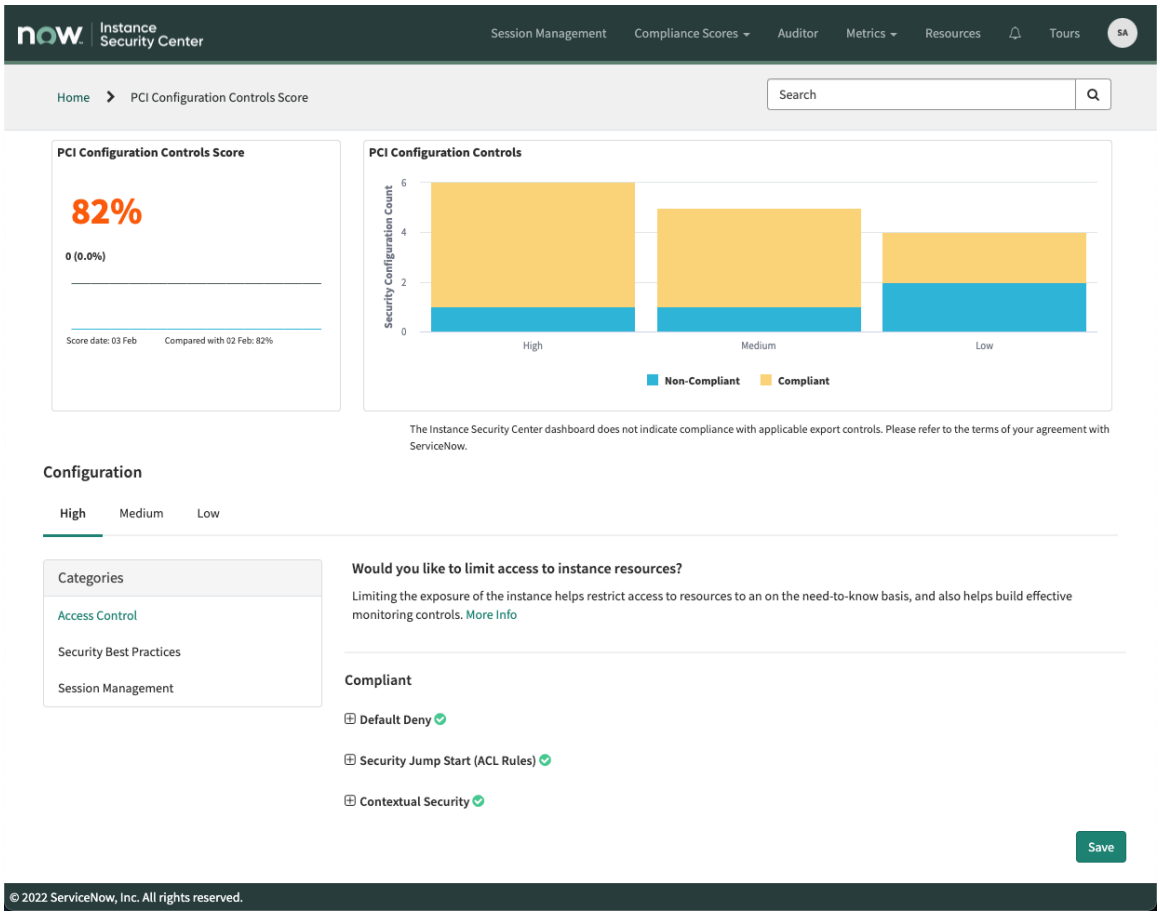
Titre	Type	Table source	Description
Conformité PCI	 Graphique à barres empilées	Configurations de sécurité [isc_security_configurations]	Affiche les configurations de sécurité conformes et non conformes dans les catégories haute, moyenne et faible. Cliquez sur une zone du rapport pour afficher les configurations de sécurité correspondantes.

Tableau de bord des scores des contrôles des configurations PCI

Utilisez le tableau de bord des scores des contrôles de configuration PCI pour examiner votre configuration PCI et déterminer quels contrôles de sécurité ne sont pas conformes. Vous pouvez changer la configuration des contrôles de sécurité non conformes à partir du centre de sécurité de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Rôles Now Platform requis

Le rôle security_dashboard_user ou administrateur est requis pour afficher le tableau de bord des scores de conformité PCI.

Accéder au tableau de bord des scores des contrôles des configurations PCI

Pour ouvrir le tableau de bord, accédez à **Sécurité de système** > **Centre de sécurité de l'instance**. Dans le centre de sécurité de l'instance, cliquez sur **Scores de conformité** dans l'en-tête, puis sélectionnez **Score des contrôles des configurations PCI**.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Utilisateur du tableau de bord de sécurité (security_dashboard_user)	Surveillez et gérez en permanence la conformité des contrôles de configuration PCI sur votre instance. Modifiez la configuration PCI pour assurer la conformité et améliorer la sécurité de l'instance.
Administrateur (admin)	Surveillez en permanence la conformité des contrôles de configuration PCI pour détecter les menaces de sécurité potentielles et y répondre.

Traduction automatique

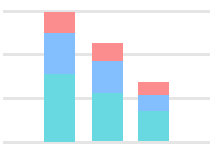
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Indicateurs

Score des contrôles des configurations PCI

Affiche le score des contrôles de configuration PCI de votre instance sous forme de pourcentage. Ce pourcentage représente le pourcentage de configurations de contrôle PCI de sécurité sur votre instance qui respectent les normes de conformité. L'indicateur affiche également la date à laquelle le score de conformité a été calculé, ainsi qu'une comparaison avec le score calculé précédemment.

Visualisation des données

Titre	Type	Table source	Description
Contrôles des configurations PCI	 Graphique à barres empilées	Configurations de sécurité [isc_security_configurations]	Affiche les configurations de contrôle PCI conformes et non conformes dans les catégories haute, moyenne et basse. Cliquez sur une zone du rapport pour afficher les configurations de sécurité correspondantes.

Rechercher des définitions de sécurité incorrectes

Exécutez l'auditeur pour analyser votre instance et rechercher des définitions de sécurité incorrectes. Elle fournit des conclusions que vous pouvez corriger pour aider à améliorer la posture de sécurité de votre instance.

Important :

Le Centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers ServiceNow Centre de sécurité migration.

L'auditeur effectue une évaluation « complète » de l'intégrité de votre instance qui analyse la configuration de votre système. Pour les analyses de sécurité, il compare votre configuration de sécurité actuelle aux définitions de bonnes pratiques et aux valeurs de conformité des propriétés de sécurité.

Du point de vue de la sécurité de l'instance, il fournit des informations et des recommandations sur ce que vous devez continuer à faire et sur ce que vous pouvez améliorer. Ces informations et recommandations vous aident à répondre aux questions suivantes :

- Les propriétés liées à la sécurité appropriées sont-elles définies ?
- Le module d'extension de haute sécurité est-il activé ?
- Existe-t-il des règles de contrôle d'accès adéquates ?

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exécuter l’auditeur et analyser les résultats de l’analyse

1. Pour exécuter l’auditeur, cliquez sur **Audit** sur la page d’accueil du Centre de sécurité de l’instance.
2. À l’issue de l’opération, ouvrez Résultats de l’analyse pour examiner et analyser les résultats de sécurité.
3. Pour examiner les détails d’un résultat d’analyse spécifique, double-cliquez sur le nombre de résultats. Ces informations comprennent son état, le type d’analyse, le temps d’exécution et les messages d’erreur.
4. Chacune des conclusions de l’auditeur contient des détails de résolution et une URL vers du contenu produit expliquant comment les traiter. Suivez les directives documentées pour résoudre les problèmes de chaque résultat.

Information associée

Paramètres de la sécurisation pour la sécurité de l'instance

Module d’extension de haute sécurité

Règles de la liste de contrôle d’accès

Mesures d’instance de surveillance

Surveillez les mesures d’utilisateur, d’exportation, d’authentification, de messagerie et antivirus de votre instance. Par exemple, vous pouvez surveiller la sécurité de vos e-mails en vérifiant les mesures de spam, d’e-mails externes et d’e-mails entrants provenant de domaines non approuvés ou approuvés pour votre instance. Analysez ces mesures pour rechercher des comportements de sécurité anormaux liés aux activités qui ont lieu dans votre instance.

Important :

Le Centre de sécurité de l’instance (ISC) a atteint la fin des ventes en septembre 2024 et n’est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l’avenir. Pour plus d'informations, consultez Centre de sécurité de l’instance vers ServiceNow Centre de sécurité migration.

Mesures des utilisateurs

Analysez les mesures utilisateur pour rechercher les comportements anormaux liés à des types spécifiques d’activité de l’utilisateur dans votre instance.

Non connecté Le mois dernier / Six derniers mois / L’année dernière

Indique le nombre d’utilisateurs qui ne se sont pas connectés à l’instance au cours du dernier mois, des six derniers mois et de la dernière année civile. Pour afficher les détails de l’utilisateur pour une mesure spécifique :

- Cliquez sur la mesure pour afficher la liste des utilisateurs qui ne se sont pas connectés à l’instance au cours de la période indiquée.
- Cliquez sur un nom d’utilisateur pour afficher plus de détails sur cet utilisateur.

Utilisateurs avec rôles de privilège élevé

Indique le nombre d’utilisateurs avec les types de rôles de privilège élevé suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle d'utilisateur	Description
administrateur	Rôle d'administrateur principal qui a accès à toutes les fonctionnalités, fonctions et données système, quelles que soient les contraintes de sécurité.
ais_high_security_admin	Rôle de privilège élevé qui permet à un utilisateur d'accéder aux paramètres de haute sécurité pour Recherche IA. Pour en savoir plus, reportez-vous à la rubrique Affecter des rôles à Recherche IA Administrateurs et utilisateurs .
password_reset_admin	Rôle d'administrateur qui permet à un utilisateur d'afficher l'état des activités de réinitialisation de mot de passe, d'identifier les menaces de sécurité potentielles et de surveiller la conformité aux politiques de sécurité des mots de passe. Pour en savoir plus, reportez-vous à la rubrique Réinitialisation du mot de passe et les rapports et journaux de changement de mot de passe .
script_include_admin	Rôle d'administrateur qui a également accès aux includes de script.
security_admin	Rôle de privilège élevé qui permet à un utilisateur de créer et de modifier les contrôles d'accès et les paramètres de sécurité élevée. Pour en savoir plus, reportez-vous à la rubrique Security_admin rôle.
user_admin	Rôle d'administrateur qui peut également gérer les utilisateurs, les rôles, les groupes d'utilisateurs, les rôles et les affectations de département.

Remarque :
Pour en savoir plus sur ces types de rôles administratifs, consultez Rôles administratifs spéciaux .

Pour afficher les détails d'utilisateur pour une mesure de rôle d'utilisateur spécifique :

- Cliquez sur la mesure de rôle Nombre d'utilisateurs pour afficher une liste des utilisateurs possédant ce type de rôle de privilège élevé.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet utilisateur. Vous pouvez ensuite déterminer si ces rôles critiques pour la sécurité sont affectés au personnel approprié.

Tendance des utilisateurs

Affiche des informations sur la tendance du nombre sur une période pour les types d'utilisateurs suivants :

Type de nombre	Description
Utilisateurs actifs	Nombre d'utilisateurs marqués comme actifs dans l'instance.
Utilisateurs inactifs	Nombre d'utilisateurs marqués comme inactifs dans l'instance.
Verrouillé	Nombre d'utilisateurs qui sont bloqués hors de l'instance.

Pour afficher les détails d'utilisateur pour un nombre d'utilisateurs spécifique (par exemple, Utilisateurs bloqués) :

- Cliquez sur la mesure **Utilisateurs bloqués** .
- Dans la page, cliquez sur Afficher les Centre d'analyse**enregistrements**.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet utilisateur. Vous pouvez alors déterminer s'il y a une raison pour laquelle cette personne est en lock-out et remédier à la situation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tendance des événements

Affiche des informations sur la tendance du nombre d'événements pour des types d'événements spécifiques, sur une période de temps :

Type d'événement	Description
Connexion de l'administrateur	Nombre d'utilisateurs disposant de rôles d'utilisateur administrateur aux privilèges élevés qui se sont connectés un jour spécifique.
Connexion externe	Nombre d'utilisateurs avec un rôle de snc_external affecté qui se sont connectés à cette instance au cours de la journée civile. Ces connexions sont généralement utilisées à des fins de maintenance, d'assistance, de conseil ou d'audit. La surveillance de cette mesure vous permet de vérifier que les tentatives de connexion externe sont légitimes et qu'il ne s'agit pas de problèmes de sécurité potentiels.
Échec de la connexion	Nombre d'échecs de tentatives de connexion sur un jour spécifique.
Emprunt d'identité	Nombre d'utilisateurs connectés un jour spécifique qui empruntent l'identité d'autres utilisateurs.
Élévation de la sécurité	Nombre de fois où un administrateur de sécurité a élevé la sécurité pour les utilisateurs standard en changeant leur rôle d'utilisateur affecté en un rôle de sécurité à privilège élevé au cours d'une journée civile. Ces rôles de sécurité à privilège élevé comprennent oauth_admin, administrateur, security_admin et emprunteur d'identité.
Connexion SNC	Nombre de Service et assistance client personnes qui se sont connectées à cette instance à l'aide de la technique hi-hopping au cours d'une journée spécifique.

Pour afficher les détails de l'utilisateur pour un nombre d'événements spécifique (par exemple, Emprunt d'identité) :

- Cliquez sur la mesure du nombre d'utilisateurs. La page Journaux des événements du tableau de bord de sécurité répertorie les journaux d'événements pour ce type d'événement.
- Cliquez sur un nom d'utilisateur pour afficher plus de détails sur cet événement.

Information associée

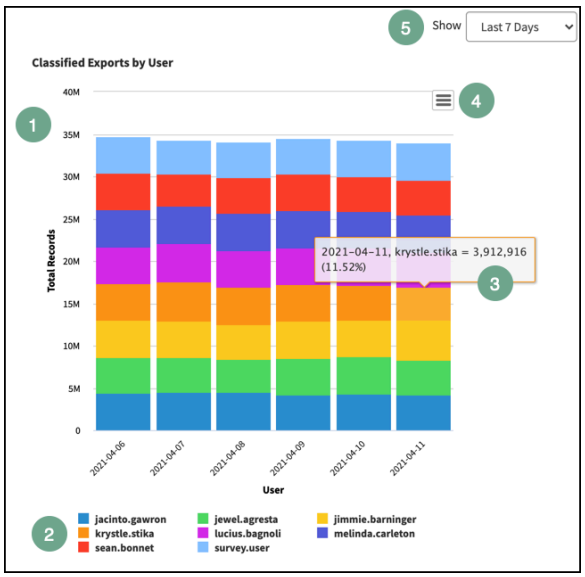
Centre d'analyse

Mesures d'exportation

Analysez les mesures d'exportation pour voir quelles données sont les plus couramment exportées et quels utilisateurs exportent le plus de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



1. Exporter le graphique

Chaque rapport affiche le nombre d'événements d'exportation par date, à l'aide d'une clé à code couleur pour indiquer quels utilisateurs ont effectué l'exportation. Cliquez sur une section colorée d'une colonne pour afficher la liste des enregistrements **d'événements d'exportation** [isc_export_event] correspondant à cette entrée.

2. Clé du rapport

La clé en bas du rapport indique quelles couleurs identifient quels utilisateurs ou tables.

3. Fenêtre contextuelle d'aperçu

Pointez sur une entrée du graphique pour afficher un aperçu contextuel. Cet aperçu affiche le nom de l'utilisateur ou de la table, ainsi qu'un nombre d'exportations et un pourcentage du total dans cette colonne.

4. Exportation d'images

Cliquez sur l'icône pour enregistrer le rapport en tant qu'image. Vous pouvez enregistrer le rapport au format PNG ou JPEG.

5. Plage de dates du rapport

Utilisez la liste **Afficher** pour afficher les exportations au cours des dernières 24 heures ou des 7 derniers jours.

Exporter les rapports de mesures

La page Mesures d'exportation affiche quatre rapports.

Exportations par utilisateur

Utilisez le rapport **Exportations par utilisateur** pour voir lequel de vos utilisateurs exporte le plus de données.

Exportations classées par utilisateur

Utilisez le rapport **Exportations classées par utilisateur** pour voir lequel de vos utilisateurs exporte le plus de données correspondant aux classifications telles que les informations confidentielles, restreintes ou personnelles. Les administrateurs peuvent définir les classifications utilisées par ce rapport dans l'onglet **Paramètres** .

Exportations par table

Utilisez le rapport **Exportations par table** pour voir à partir de quelles tables les exportations sont les plus fréquentes.

Exportations classées par table

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez le rapport **Exportations classées par table** pour voir à partir de quelles tables les exportations sont le plus fréquentes et correspondent à des classifications telles que les informations confidentielles, restreintes ou personnelles. Les administrateurs peuvent définir les classifications utilisées par ce rapport dans l'onglet **Paramètres** .

Remarque :
Les rapports de mesures d'exportation suivent uniquement les événements d'exportation. Les exportations à partir d'autres sources, telles que les API REST ou les workflows, ne sont pas suivies dans le cadre de cette fonctionnalité.

Exporter les paramètres des mesures

Utilisez les options de configuration de l'onglet Paramètres pour affiner les résultats de génération de rapports.

Accédez aux paramètres de vos mesures d'exportation en cliquant sur l'onglet **Paramètres** .

Champs de configuration des paramètres

Configurations des mesures d'exportation

Configuration	Description
Classifications des mesures	Ajoutez ou supprimez des classifications à ce champ pour déterminer quelles exportations sont incluses dans les rapports **Exportations classées par utilisateur** et **Exportations classées par table** . Ces rapports prennent en charge les classifications suivantes : • Informations personnellement identifiables • Confidentiel • Restreint • Interne • Public Pour plus de détails sur les classifications des données, consultez Classifications des données
Classifications des alertes	Ajoutez ou supprimez des classifications dans ce champ pour déterminer quelles exportations déclenchent des notifications de sécurité d'instance. Les classifications prises en charge dans le champ **Classifications pour les mesures** sont prises en charge ici. Pour plus de détails sur ces alertes, consultez la section Notifications de sécurité de la Centre de sécurité de l'instance page. Le champ **Seuil d'enregistrement** définit le nombre d'enregistrements exportés avant les déclenchements et les alertes de votre instance.
Seuil d'enregistrement	Nombre d'enregistrements qu'un utilisateur doit exporter pour déclencher une alerte. Pour déclencher une alerte, ces enregistrements doivent également correspondre aux classifications répertoriées dans le champ **Classifications des alertes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez le bouton **Enregistrer** (⌘ **+ s)** pour enregistrer vos paramètres.

Mesures d'authentification

Analysez les mesures d’authentification pour afficher les informations relatives à l’authentification, telles que les adresses IP peu utilisées, les échecs de connexion et les types de schémas d’authentification utilisés par vos utilisateurs.

Utilisez la page **Mesures d’authentification** pour afficher les rapports relatifs à votre configuration d’authentification. Les rapports suivants sont affichés dans cet onglet.

Remarque :
La page des mesures d’authentification nécessite le **module d’extension REST API Access Policy** (com.glide.rest.policy). Pour plus de détails sur cette fonctionnalité, consultez Politiques d’accès de l’API REST.

API sans politique d’authentification

Affiche un nombre en temps réel de toutes les API sans politique d’accès

Sécurisation renforcée : flux de récupération de compte

Sécurisation renforcée : paramètre lié à la fonctionnalité MFA basée sur les rôles

Comptes d’accès au service Web uniquement

Affiche le nombre d’enregistrements utilisateur dont l’option d’accès au service Web est activée dans `User` la table [sys_user].

Certificats X509 arrivant à expiration dans 30 jours

Affiche le nombre de tous les certificats X.509 de `X.509 Certificates` la table [sys_certificate] qui arrivent à expiration dans 30 jours.

Mesures d'authentification adaptative

Analysez les mesures d’authentification adaptative pour surveiller et ajouter des informations sur la façon dont l’authentification adaptative est utilisée sur votre instance.

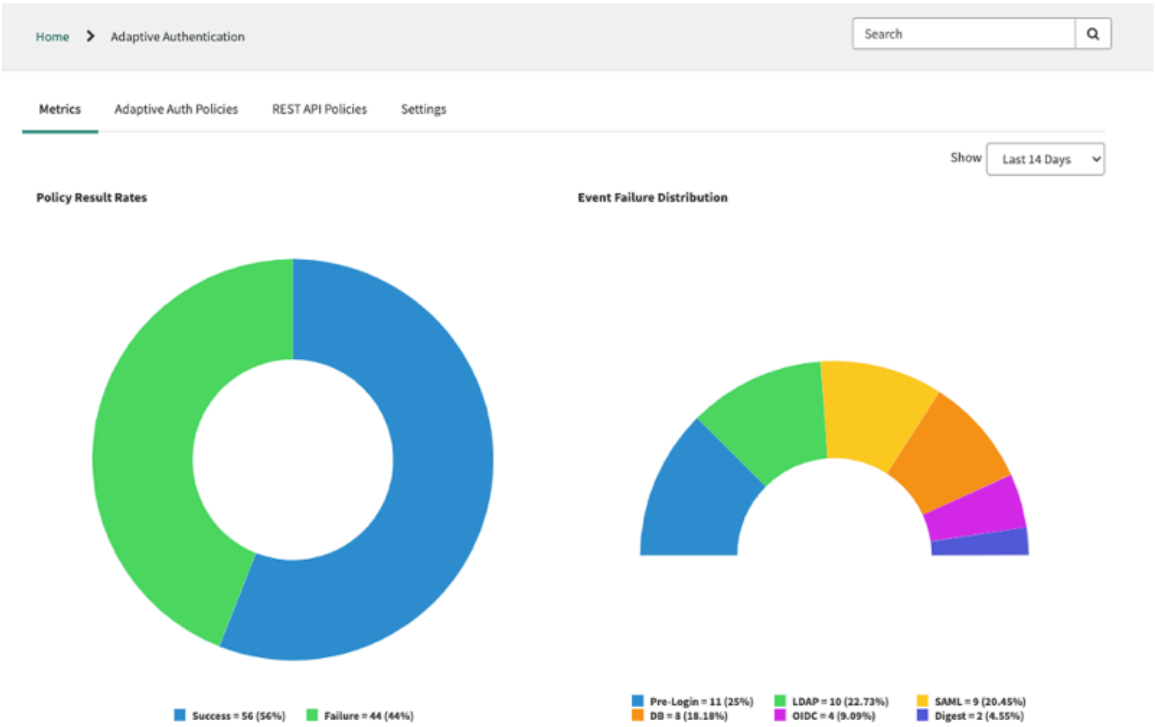
Affichez les rapports, les paramètres et les politiques associés à l’authentification adaptative sur place à l’aide de la page Mesures d’authentification adaptative. Les administrateurs de sécurité peuvent utiliser des rapports pour surveiller les résultats de leurs politiques d’authentification adaptative. Utilisez ces données pour obtenir des informations et adapter vos politiques afin d’améliorer leurs performances.

Remarque :
La page Mesures d’authentification adaptative nécessite le module d’extension **Authentification adaptative** (com.snc.adaptive_authentication). Pour plus d’informations sur cette fonctionnalité, reportez-vous à la section Authentification adaptative.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures



Utilisez l'onglet Mesures pour afficher **les** rapports relatifs à votre configuration d'authentification adaptative. Les rapports suivants sont affichés dans cet onglet.

- Taux des résultats de la politique
- Distribution d'échecs d'événements
- Distribution de la réussite d'événement
- Adresses IP refusées
- Connexions des utilisateurs d'authentification
- Connexions des utilisateurs de l'API
- Tendance en matière d'authentification

Utilisez la liste **Afficher** pour sélectionner une période pour les rapports affichés

Politiques d'authentification adaptative

Utilisez l'onglet **Politiques d'authentification adaptative** pour afficher les politiques d'authentification adaptative et les contextes de politique sur votre instance. Cliquez sur une entrée de ces listes pour afficher l'enregistrement associé. Pour plus de détails sur ces enregistrements, consultez Authentification adaptative

Paramètres

Utilisez l'onglet Paramètres pour afficher et configurer les propriétés système d'authentification adaptative. Pour plus d'informations sur ces propriétés, consultez Configurer les propriétés d'authentification adaptative

Mesures d'e-mail

Analysez les mesures de vos e-mails pour rechercher les comportements anormaux liés aux e-mails entrants dans votre instance. Par exemple, si les mesures indiquent un pic

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de spams provenant de domaines spécifiques, vous pouvez définir des actions entrantes empêchant leur remise à l'instance.

Pour chaque mesure d'e-mail, un nombre s'affiche pour chaque type d'e-mail remis ou envoyé à l'instance au cours d'un jour calendaire.

Préférence de notification	Description
E-mail entrant externe	Nombre d'e-mails entrants pour le jour du calendrier qui ont été remis à l'instance à partir de domaines d'e-mail externes. **Remarque :** Les domaines d'e-mail externes sont les domaines qui ne sont pas répertoriés dans la propriété système, car cette propriété suit uniquement vos domaines d'e-mail `security.list.internal.domains` internes. Pour en savoir plus sur cette propriété, reportez-vous à la section Propriétés système disponibles .
Courrier indésirable	Nombre d'e-mails entrants du jour civil qui ont été remis à l'instance et marqués comme courrier indésirable. Un nombre qui n'est pas conforme aux tendances historiques peut indiquer que des tentatives sont faites pour compromettre la sécurité de votre instance.
E-mail entrant approuvé	Nombre d'e-mails entrants envoyés à l'instance pour le jour calendaire à partir de domaines d'e-mail désignés comme approuvés.
E-mail entrant non approuvé	Nombre d'e-mails entrants vers l'instance pour le jour civil à partir de domaines d'e-mail désignés comme non approuvés. Vous pouvez désigner des domaines de messagerie non approuvés ou approuvés dans le formulaire Domaine non approuvé et approuvé afin de pouvoir suivre vos e-mails entrants qui sont envoyés par ces domaines. Pour savoir comment désigner des domaines de messagerie non approuvés ou approuvés, reportez-vous à la section Désigner des domaines d'e-mail comme non approuvés ou approuvés.

Après avoir cliqué sur une mesure d'e-mail, vous pouvez en apprendre davantage sur les problèmes de sécurité d'e-mail possibles dans votre instance en cliquant sur l'un des onglets suivants :

Commande	Description
Graphique	Nombre d'e-mails entrants et tendances dans le temps pour le type d'e-mail sélectionné (courrier indésirable, externe entrant, non approuvé ou approuvé).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commande	Description
Enregistrements	Enregistrements d’e-mail individuels qui compromettent le nombre quotidien pour le type d’e-mail sélectionné.
Plus d'informations	Informations supplémentaires pour le type d’e-mail sélectionné.

Remarque :
Les mesures d’e-mail s’appliquent uniquement aux e-mails entrants dans l’instance. Les mesures ne s’appliquent pas au trafic normal qui est traité via vos serveurs de messagerie à l’échelle de l’entreprise. Pour en savoir plus sur la définition des actions entrantes et leur impact sur le traitement de vos e-mails entrants, consultez Actions sur e-mail entrant .

Désigner des domaines d’e-mail comme non approuvés ou approuvés

Désignez des domaines d’e-mail spécifiques comme non approuvés ou approuvés afin de pouvoir surveiller les mesures des e-mails entrants provenant de ces sources dans votre instance.

Avant de commencer

Rôle requis : security_dashboard_user ou admin

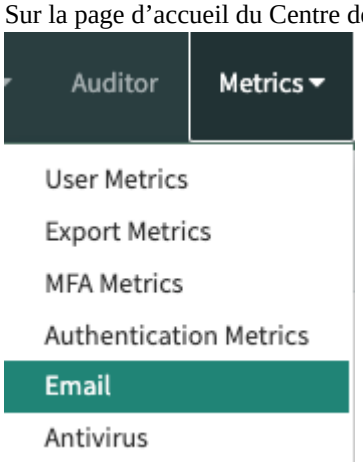
Pourquoi et quand exécuter cette tâche

Lorsque des domaines non approuvés ou approuvés envoient des e-mails à votre instance, leur nombre quotidien s’affiche dans les mesures **E-mail entrant non approuvé** ou **E-mail entrant approuvé** sur la page E-mail. Vous pouvez ensuite suivre l’activité des e-mails de ces domaines et utiliser les journaux d’e-mails pour afficher des e-mails entrants spécifiques. Vous pouvez également spécifier un utilisateur, généralement un gestionnaire ou un analyste de sécurité, à notifier chaque fois qu’une activité se produit à partir du domaine non approuvé ou approuvé.

Remarque :
La désignation d’un domaine d’e-mail comme n’étant pas approuvé ne sert qu’à des fins de suivi de la sécurité. Les administrateurs peuvent également configurer un filtre d’adresse système pour ignorer les e-mails provenant de domaines non approuvés. Pour en savoir plus sur le filtrage des e-mails afin de bloquer leur remise, voir Filtres d’adresse système .

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Centre de sécurité de l'instance**.
2. Sur la page d’accueil du Centre de sécurité de l’instance, sélectionnez **E-mail** dans le menu **Mesures** .



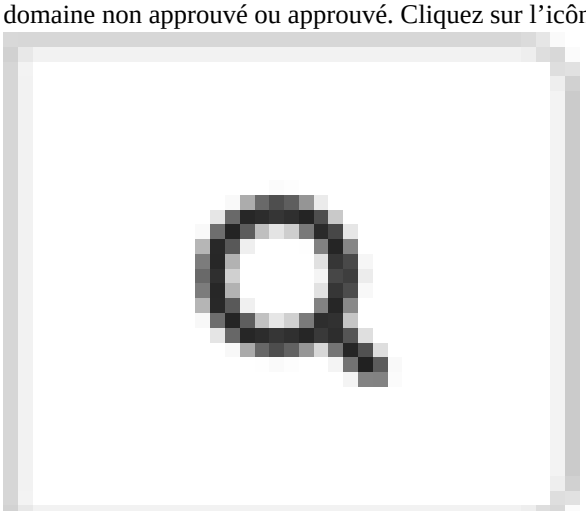
3. Sur la page E-mail, dans la section Domaines non approuvés et approuvés, cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Renseignez les champs du formulaire.

Formulaire Domaine non approuvé ou approuvé

Champ	Description
Domaine	Nom du domaine de messagerie que vous désignez comme non approuvé ou approuvé. Par exemple, saisissez servicenow.com pour désigner les ServiceNow employés qui peuvent envoyer des e-mails de confiance à l'instance.
Catégorie	Catégorie indiquant si le domaine d'e-mail n'est pas approuvé ou approuvé : **Non approuvé** Indique que le domaine d'e-mail n'est pas approuvé. Vous l'utilisez pour identifier les domaines qui envoient des e-mails suspects ou qui constituent une menace potentielle pour la sécurité de l'instance. **Approuvé** Indique que le domaine d'e-mail est de confiance. Vous l'utilisez pour identifier des domaines lorsque vos mesures indiquent que les e-mails entrants ne posent aucune menace pour la sécurité. Désigner le domaine comme approuvé vous permet de suivre son activité de messagerie entrante au fil du temps.
Actifs	Case à cocher permettant d'activer ou de désactiver l'état désigné comme non approuvé ou approuvé pour le domaine de messagerie spécifié.
Notify	Nom de l'utilisateur à notifier par e-mail lorsqu'une activité se produit dans le domaine non approuvé ou approuvé. Cliquez sur l'icône de recherche Spotlight () pour rechercher le nom de l'utilisateur. Ne renseignez pas le champ **Notification** si vous ne souhaitez pas que des notifications soient envoyées.

5. Sélectionnez **Enregistrer**.

Résultats

Les informations sur le domaine de messagerie non approuvé ou approuvé sont également ajoutées à la liste **Domaines non approuvés et approuvés** sur la page E-mail.

Information associée

Centre de sécurité de l'instance

Mesures d'e-mail

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mesures antivirus

Si le module d'extension est activé, il Analyse anti-virus s'exécute Analyse anti-virus dans votre instance pour la protéger contre les infections virales provenant des pièces jointes.

Les mesures suivantes s'affichent pour les 60 derniers jours d'activité et vous permettent d'évaluer l'efficacité des Analyse anti-virus fonctions.

Événements antivirus

Les événements antivirus indiquent le nombre d'événements antivirus dans votre instance, par date. Pour accéder aux événements antivirus, accédez à **Sécurité de système** > **Centre de sécurité de l'instance** et sélectionnez l'onglet Mesures. Les lignes de graphique à code couleur représentent les types d'événements antivirus suivants :

Couleur	Description
Bleu	Nombre de fichiers mis en quarantaine dans Analyse anti-virus cette instance pour la date indiquée.
Vert	Nombre de fichiers infectés téléchargés sur l'instance, puis mis en quarantaine jusqu'à la date indiquée. Ces fichiers sont principalement des pièces jointes d'e-mail qui contiennent un code virus ou rouge.
Jaune	Nombre de fichiers mis en quarantaine dans l'instance qui ont été supprimés pour la date indiquée.
Orange	Nombre de fichiers mis en quarantaine dans l'instance qui ont été restaurés pour la date indiquée. **Remarque :** Une fois Analyse anti-virus qu'il a été exécuté et qu'il a détecté des faux positifs, vous pouvez restaurer un fichier mis en quarantaine et le rendre accessible dans l'instance.

- Pour accéder à la Centre d'analyse page et afficher la carte de score détaillée et les informations d'analyse pour une date spécifique, cliquez sur une ligne colorée dans le graphique des événements antivirus. Par exemple, cliquez sur la ligne graphique bleue pour afficher les informations d'analyse des fichiers mis en quarantaine pour une date spécifique.
- Pour afficher les répartitions suivantes dans la page, cliquez sur l'icône Centre d'analyse , puis cliquez sur :

Répartition	Description
AppSec : source de l'événement antivirus	Source de l'événement antivirus. ○ **Lors du téléchargement :** S'est produit en raison du chargement d'un fichier infecté, généralement une pièce jointe. ○ **À partir de la quarantaine :** S'est produit en raison de la mise en quarantaine d'un fichier infecté, généralement une pièce jointe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Répartition	Description
	○ **En téléchargement :** S'est produit à la suite du téléchargement d'un fichier infecté, généralement une pièce jointe. ○ **À partir de l'enregistrement :** S'est produit en raison d'un enregistrement infecté dans une table.
AppSec : type d'événement antivirus	Type d'événement antivirus. ○ **Quarantaine:** S'est produit en raison de la mise en quarantaine d'un fichier, généralement une pièce jointe. ○ **Téléchargé:** S'est produit à la suite du téléchargement d'un fichier, généralement une pièce jointe. ○ **Restauré:** S'est produit en raison de la restauration d'un fichier mis en quarantaine. ○ **Supprimé:** S'est produit en raison de la suppression d'un fichier mis en quarantaine.
AppSec : outil de téléchargement d'antivirus	Nom de l'utilisateur connecté qui a téléchargé les fichiers à l'origine des infections virales détectées par l'application Analyse anti-virus .

Fichiers en quarantaine

Répertorie les fichiers infectés dans l'instance mise en quarantaine par Analyse anti-virus:

Champ	Description
Nom de fichier	Nom du fichier infecté.
Type de contenu	Type de contenu qui a été infecté dans le fichier. Par exemple, **application/x-dosexec** est un fichier exécutable d'application ou DOS infecté, tandis que **text/plain** est un fichier .txt infecté.
Table	Nom de la table qui contient le fichier infecté. Par exemple, **incident** apparaît pour un enregistrement de fichier d'incident.
Virus	Nom du fichier mis en quarantaine par Analyse anti-virus.
Détectée	Date et heure de détection du fichier infecté.
Créés par	Nom de l'utilisateur qui a mis en quarantaine le fichier infecté.
Créé	Date et heure de création de l'enregistrement du fichier de quarantaine.
ID système de table	Identificateur système de table affecté à l'enregistrement de fichier de quarantaine.

Remarque :
Vous pouvez également ajouter des **tuiles Fichiers en quarantaine** et **Types de virus** au ruban Événement. Pour en savoir plus, consultez Surveiller les événements de sécurité et Configurer le ruban des événements de sécurité.

Information associée

Analyse anti-virus

Configurer Analyse anti-virus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Examen des fichiers mis en quarantaine

Examen de l’activité antivirus

Centre d'analyse

Répartitions de Performance Analytics

Analytics, Intelligence and Reporting

Tableau de bord des mesures MFA

Le tableau de bord des mesures MFA affiche des informations sur la configuration de l’authentification multifacteur de vos instances. Utilisez le tableau de bord pour vous assurer que votre configuration MFA répond à vos normes de sécurité.

Rôles Now Platform requis

security_dashboard_user ou administrateur, nécessaire pour afficher le tableau de bord des scores de conformité PCI.

Accéder au tableau de bord des mesures MFA

Pour ouvrir le tableau de bord, accédez à **Sécurité de système** > **Centre de sécurité de l'instance**. Dans le centre de sécurité de l’instance, cliquez sur **Mesures** dans l’en-tête, puis sélectionnez **Mesures MFA**.

Cas d'utilisation

Pour obtenir des exemples sur la façon dont les différentes personnes de votre organisation utilisent ce tableau de bord, consultez ces cas d'utilisation.

Utilisateur	Utilisation du tableau de bord
Utilisateur du tableau de bord de sécurité (security_dashboard_user)	Surveillez et gérez en permanence la conformité de la sécurité de l’instance.
Administrateur (admin)	Surveillez en permanence la conformité de la sécurité de l’instance pour détecter les menaces de sécurité et y répondre.

Indicateurs

Utilisateurs inscrits pour MFA

Affiche le nombre total d’utilisateurs sur l’instance inscrits à la MFA . Cliquez pour ouvrir le centre d’analyse pour plus de détails.

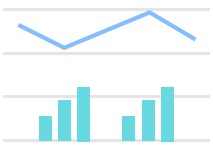
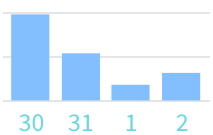
Utilisateurs utilisant le contournement de la MFA

Affiche le nombre total d’utilisateurs utilisant le contournement de la MFA. Cliquez pour ouvrir le centre d’analyse pour plus de détails.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisations des données

Titre	Type	Table source	Description
Utilisateurs MFA aux privilèges élevés			
Tendance des utilisateurs de MFA	 Graphique de tendance		

Activer l'interface ISC Agent virtuel

Si vous disposez du rôle administrateur, vous pouvez activer le module d'extension ISC Agent virtuel Conversations (com.glide.isc_virtualagent). L'activation de ce module d'extension installe les packs de Agent virtuel contenu et Compréhension du langage naturel (NLU), fournissant un accès à Agent virtuel partir du centre de sécurité de l'instance.

Avant de commencer

Important :

Le Centre de sécurité de l'instance (ISC) a atteint la fin des ventes en septembre 2024 et n'est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l'avenir. Pour plus d'informations, consultez Centre de sécurité de l'instance vers ServiceNow Centre de sécurité migration.

L'interface Agent virtuel dans Centre de sécurité de l'instance n'est disponible que pour les utilisateurs ayant des abonnements payants Agent virtuel et ayant activé le module d'extension Agent virtuel Glide (com.glide.cs.chatbot). Pour en savoir plus, consultez Activer l'Agent virtuel .

Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

L'interface ISC Agent virtuel vous permet d'effectuer les tâches suivantes :

- Posez des questions liées à la sécurité, puis obtenez des réponses récapitulatives rapides et des liens de référence pour en savoir plus.
- Obtenez des réponses relatives au centre de sécurité de l'instance, à la sécurité de la plateforme, aux politiques de sécurité ServiceNow, à la confiance, à la gouvernance, au risque et à d'autres processus.
- Recherchez des ressources liées à la sécurité, telles que les rubriques de la base de connaissances dans le portail de sécurité Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modules d’extension pour ISC Agent virtuel

Module d'extension	Description
ISC Agent virtuel Conversations [com.glide.isc_virtualagent]	Active le pack de contenu Conversations ISC Agent virtuel pour Centre de sécurité de l’instance.
Modèle ISC NLU pour Agent virtuel les conversations [com.glide.isc_nlu]	Active le pack de Compréhension du langage naturel contenu (NLU) pour Centre de sécurité de l’instance.

Remarque :
L’activation du module d’extension com.glide.isc_virtualagent active automatiquement com.glide.isc_nlu. Toutefois, si vous activez d’abord le module d’extension com.glide.isc_nlu, vous devez également l com.glide.isc_virtualagent activer manuellement.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Paramètres de la sécurisation pour la sécurité de l'instance

Les paramètres de renforcement de la sécurité de l'instance contiennent des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans la Now Platform. Vous pouvez définir la plupart de ces propriétés dans la page Configuration de la conformité à la sécurisation renforcée d'Instance Security Center.

Important :

Le Centre de sécurité de l’instance (ISC) a atteint la fin des ventes en septembre 2024 et n’est plus pris en charge ni disponible pour une nouvelle activation.

ServiceNow Le Centre de sécurité (SSC) est la solution recommandée pour l’avenir. Pour plus d'informations, consultez Centre de sécurité de l’instance vers ServiceNow Centre de sécurité migration.

Vue d'ensemble et objectif

Instance Security Center calcule un score de conformité quotidien, exprimé en pourcentage. Il est basé sur la conformité de vos paramètres de sécurité d'instance actuels avec les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

valeurs de conformité définies dans les paramètres de renforcement de la sécurité de l'instance.

Dans sa page Configuration de la conformité à la sécurisation renforcée, vous pouvez gérer les paramètres de configuration de sécurité spécifiques qui peuvent affecter le score de votre instance. Pour en savoir plus sur l'assurance que vos instances répondent aux exigences de sécurisation renforcée, consultez :

- Centre de sécurité de l'instance
- Ajuster les paramètres de sécurité de l’instance pour accroître la conformité

Consultez les paramètres de renforcement de la sécurité de l’instance chaque fois que vous définissez ou mettez à jour des propriétés liées à la sécurité, même si certaines des valeurs de conformité peuvent ne pas convenir à votre instance. Lorsque vous mettez à jour ces propriétés, assurez-vous que l’instance continue de se comporter comme prévu. Consultez le personnel interne approprié qui possède l’expertise nécessaire pour déterminer les impacts sur la sécurité.

Autres ressources

Pour la référence utilisateur, la Now Platform conserve des informations détaillées sur les options de configuration dans la documentation du produit. Les liens trouvés dans Sécuriser votre instance vous permettent d'accéder à la plupart du contenu de la sécurité. Consultez également les rubriques suivantes :

- Propriétés système disponibles
- Propriétés des paramètres de sécurité
- Paramètres de sécurité élevée

Tables de sécurisation renforcée de l'instance

Tables Configurations de Security

Les enregistrements de la table Configurations de Security [isc_security_configurations] contiennent les détails d'une configuration de sécurité. Dans un enregistrement, vous trouvez la description d'une configuration, son état de conformité et d'autres détails importants.

Utilisez l'enregistrement des configurations de sécurité pour afficher toutes les propriétés et dépendances que vous devez configurer pour rendre votre configuration conforme en un seul endroit.

Dans l'enregistrement des configurations de sécurité, vous pouvez voir les enregistrements de groupes de dépendance de sécurité et de dépendance associés à cette configuration.

Table Dépendances de Security

Les enregistrements de la table des dépendances de sécurité [isc_security_dependencies] définissent les critères entrants et sortants, ainsi qu'un type recommandé. Ce type définit le mode d'affichage de la dépendance dans Instance Security Center.

Table des groupes de dépendances

Utilisez les enregistrements de la table des groupes de dépendances [isc_dependency_groups] pour regrouper plusieurs dépendances. Toutes les dépendances d'un groupe doivent être conformes pour que le groupe soit considéré comme tel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contrôle d'accès (renforcement de la sécurité de l'instance)

Les contrôles d'accès déterminent si l'accès à une ressource particulière doit être accordé ou refusé. L'accès aux ressources n'est autorisé qu'aux utilisateurs autorisés à les utiliser.

L'autorisation n'est pas équivalente à l'authentification, car ces termes et leurs définitions sont souvent confondus.

- L'authentification consiste à fournir et à valider l'identité.
- L'autorisation inclut des règles d'exécution qui déterminent les fonctionnalités et les données auxquelles l'utilisateur (ou le mandant) peut accéder, garantissant ainsi la bonne allocation des droits d'accès une fois l'authentification réussie.

L'autorisation est un processus qui intervient après une authentification réussie. Vous pouvez configurer des propriétés de sécurité qui désignent si, après avoir déterminé qu'un utilisateur détient des informations d'identification valides associées à un ensemble bien défini de rôles et de privilèges, une autorisation de ressource se produit.

Voici quelques contrôles de sécurité qu'un administrateur peut configurer pour restreindre l'accès non autorisé aux entités sensibles dans le Now Platform.

- Règles de la liste de contrôle d'accès
- Configuration d'une règle ACL
- Contrôle d'accès ServiceNow

Accès à l'API de script GlideSystemUserSession

L'API scriptable GlideSystemUserSessionSandbox pouvant être appelée par le client expose les méthodes GlideSystemUserSession's addErrorMessageNoSanitization et addInfoMessageNoSanitization au bac à sable JavaScript. Cela permet à tous les utilisateurs d'appeler cette méthode via un script.

Lorsqu'elle est définie sur **vrai**, une session d'utilisateur en bac à sable (sandbox) est autorisée à appeler des informations ou des messages d'erreur sans nettoyage. Un avertissement est enregistré lorsque le message est appelé. Lorsque la valeur est définie sur **faux**, l'appel n'est pas autorisé.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sandbox.usersession.allow_unsanitized_messages`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurable dans le centre de sécurité de l'instance	Oui
Objectif	Cette propriété empêche l'appel de messages d'information ou d'erreur non nettoyés dans une session utilisateur bac à sable.
Type	vrai | faux booléen
Valeur recommandée	faux
Dépendances de Sécurité	La valeur de cette propriété est un remplacement sûr et ne peut pas être modifiée une fois modifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Élevé) Définir la propriété avec la valeur false n'entraînera aucune création ou journalisation de message si ces fonctions sont appelées.
Risque de sécurité	(Élevé) En l'absence d'assainissement approprié, il est possible d'accéder à des contenus potentiellement dangereux et le script dispose de la fonction d'erreur non désinfectée.
Références	Contrôle d'accès Remplacement sécurisé

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Autorisation pour l'exécution du script

Utilisez la `glide.script_processor.authorized_script_module_role` propriété pour limiter l'utilisation des scripts en cours `d'exécution à partir de sys_app_module` table au rôle défini au sein de la propriété.

Cette propriété empêchera tous les utilisateurs système d'exécuter un script à partir du sys_app_module sauf s'ils ont le rôle spécifié dans la propriété. Utilisez la propriété glide.script_processor.authorized_script_module_role pour spécifier le rôle qui peut exécuter des scripts.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.script_processor.authorized_script_module_role`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour exiger qu'un rôle désigné exécute un script à partir du `sys_app_module`.
Valeur recommandée	Zone de texte avec une liste de rôles séparés par des virgules.
Impact fonctionnel	(Moyen) Cette correction applique l'authentification sous la forme d'une autorisation par rôle défini. • Il effectue cette authentification lors du traitement des demandes de script sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes de script, les utilisateurs non autorisés peuvent accéder à du contenu/des données sensibles sur l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	Contrôle d’accès

Pour en savoir plus sur l’ajout ou la création d’une propriété système, reportez-vous à la section Add a system property .

Authentification de base : demandes JSONv2 (renforcement de la sécurité de l’instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.jsonv2` demandes JSONv2 entrantes doivent obtenir une autorisation de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.jsonv2
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l’instance	Oui
Objectif	Pour appliquer l’autorisation des demandes JSONv2.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette remédiation applique une combinaison de méthodes d’authentification, sous la forme d’une authentification de base et d’un contrôle d’accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données JSON sur l’instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui a besoin d’accéder à ce contenu, avec les autorisations de contrôle d’accès nécessaires. Pour plus d’informations, reportez-vous à la rubrique Service Web JSONv2 Service Web JSONv2 .
Risque de sécurité	(Élevé) Sans l’autorisation appropriée configurée sur les demandes JSON de source de données, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l’instance cible.
Références	Authentification Exiger une authentification de base pour les demandes JSONv2 entrantes

Pour en savoir plus sur l’ajout ou la création d’une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification de base : demandes SOAP (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.soap` demandes SOAP entrantes doivent obtenir une autorisation de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.soap
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour faire respecter l'autorisation des demandes SOAP.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données SOAP sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui a besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour plus d'informations, consultez Informations d'identification d'authentification de service Web SOAP et de Serveur MID et demandes SOAP.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur la source de données des demandes SOAP, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Accès en bloc pour le développeur délégué

Cette configuration affecte l'accès aux développeurs délégués qui mettent à jour les rôles d'utilisateur via le script. Lorsque la configuration est conforme, le développeur n'est pas en mesure de mettre à jour ou d'insérer des enregistrements dans la `table sys_user_has_role` sans également le rôle user_admin.

La valeur de cette propriété détermine si un développeur délégué est autorisé à accorder ou à recevoir un accès inattendu aux fonctionnalités de l'instance. Lorsque la propriété contient des rôles, seuls ces rôles peuvent exécuter des modules de script.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.sys.security.delegateddev.block_grant_roles`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	La valeur de cette propriété détermine si un développeur délégué est autorisé à accorder ou à recevoir un accès inattendu aux fonctionnalités de l'instance.
Type	interrupteur à bascule
Valeur recommandée	VRAI
Dépendances de Sécurité	aucun
Impact fonctionnel	(Élevé) Lorsqu'un utilisateur disposant du rôle delegated_developer tente de modifier un enregistrement dans sys_user_has_role, cette propriété active des contrôles de sécurité supplémentaires par rapport à l'opération. Les vérifications de sécurité supplémentaires valident que l'utilisateur a reçu le rôle user_admin s'il tente de créer ou de mettre à jour sys_user_has_role. S'il n'a pas le rôle user_admin , l'accès sera refusé. Lorsque la propriété a la valeur false, ces vérifications supplémentaires ne sont pas validées.
Risque de sécurité	(Élevé) Sans autorisation appropriée, des utilisateurs non autorisés peuvent accéder à du contenu/des données sensibles sur l'instance.
Références	Contrôle d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Vérifier les conditions de l'action de l'interface utilisateur avant son exécution (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la vérification des conditions des actions d'interface utilisateur dans les *glide.security.strict.actions* formulaires et les listes avant leur exécution. Lorsque vous définissez cette propriété sur **vrai**, elle ajoute une couche supplémentaire de validation sur la table des actions d'interface utilisateur avant qu'elles ne soient exécutées.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.strict.actions
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour garantir une validation supplémentaire sur la table, les actions d'interface utilisateur avant qu'elles ne soient exécutées.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction ajoute seulement une couche supplémentaire de validation pour vérifier les actions d'interface utilisateur sur la table/page cible sur l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait pas y avoir d'impact ici.
Risque de sécurité	(Moyen) La demande d'accès est toujours vérifiée lorsque des transactions ont lieu entre deux zones. Cette opération valide toutes les actions d'interface utilisateur avant que le formulaire ne s'affiche pour l'utilisateur final.
Références	Module d'extension de haute sécurité

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Module d'extension Sécurité contextuelle : gestion des rôles (renforcement de la sécurité de l'instance)

Activez le module d'extension Sécurité contextuelle : Gestion des`com.glide.role_management` rôles () pour activer la sécurité contextuelle, qui sécurise un enregistrement/des informations utilisant la création, la lecture, l'écriture et la suppression d'une fonctionnalité.

Une fois installé et activé, les rôles du dictionnaire (créés par Simple Security Manager) ne sont plus testés. Au lieu de cela, le Now Platform recherche des règles ACL sur les champs et les tables. Il sécurise les données à l'aide de règles ACL au lieu des règles de dictionnaire traditionnelles basées sur les rôles implémentées par un simple gestionnaire de sécurité. Même si vous configurez le formulaire de dictionnaire et ajoutez des rôles à une entrée de dictionnaire, aucun changement dans les droits ne se produit.

En savoir plus

Attribut	Description
ID de module d'extension	com.glide.role_management
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Contrairement au gestionnaire de sécurité simple, le gestionnaire de sécurité contextuelle connaît la hiérarchie de la table système. Vous pouvez potentiellement avoir des règles de sécurité différentes pour un champ en fonction de l'endroit où il apparaît dans la hiérarchie.
Valeur recommandée	Actif (module d'extension activé par défaut)
Impact fonctionnel	(Moyen) Ce rattrapage applique le niveau fonctionnel des contrôles d'accès, ce qui permettrait à l'application de déterminer les restrictions d'accès en se basant uniquement sur la table ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Élevé) Les contrôles d'accès au niveau fonctionnel doivent être appliqués du côté du serveur avant d'exécuter des opérations CRUD, afin de garantir le niveau d'accès approprié aux utilisateurs de l'instance.
Références	Gestionnaire de sécurité contextuelle

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à la section Activate a plugin .

Autorisation des demandes CSV (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.csv` demandes CSV (valeurs séparées par des virgules) entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.csv
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes CSV.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données CSV sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Récupération de données à partir d'un fichier au format CSV .
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes CSV entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Sécurité des services Web

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Refus par défaut (renforcement de la sécurité de l'instance)

Utilisez la *glide.sm.default_mode* propriété pour contrôler le comportement par défaut du gestionnaire de sécurité lorsqu'il détecte que des règles ACL font partie des règles ACL d'une table à caractère générique.

Lorsque le module d'extension Paramètres de sécurité élevée (*com.glide.high_security*) est activé lors de l'installation initiale de l'instance, il crée cette propriété et des règles ACL génériques voient le jour. Pour fournir un accès basé sur les rôles aux tables système, ces règles contrôlent un nombre important d'ACL et les opérations basées sur les enregistrements les plus courantes :

- Lecture
- Écriture
- Créer
- Supprimer

À moins que vous n'utilisiez le module d'extension de haute sécurité avec l'option de refus par défaut activée, de nombreuses tables ne sont pas protégées. Le Now Platform utilise un modèle de sécurité de refus par défaut qui empêche les utilisateurs non administrateurs d'accéder aux objets à moins qu'ils ne répondent à une règle ACL correspondante. À l'aide de ce modèle, il supprime de nombreux vecteurs d'attaque, tels que les scripts non sécurisés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.sm.default_mode
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	La meilleure pratique en matière de sécurité consiste à restreindre l'accès aux tables par un utilisateur non autorisé. • Si aucune règle ACL n'est en place pour les tables, cette propriété garantit qu'au moins les ACL génériques sont validées pour toute opération CRUD effectuée sur la table/le champ. • Ces règles restreignent les opérations de lecture, d'écriture, de création et de suppression sur toutes les tables, sauf si l'utilisateur a le rôle administrateur ou répond aux exigences d'une autre règle ACL de table.
Valeur recommandée	refuser
Impact fonctionnel	(Élevé) Si vous définissez cette propriété sur **Autoriser**, les règles ACL de table à caractère générique autorisent les opérations CRUD sur toutes les tables, sauf s'il existe des règles ACL de table spécifiques en place pour restreindre de telles opérations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Remarque : Ce module d'extension n'est pas conçu pour les instances existantes, car il peut modifier l'accès de sécurité aux tables déjà utilisées dans un environnement de production.
Risque de sécurité	(Élevé) Les utilisateurs non-administrateurs peuvent accéder aux objets qui correspondent aux règles ACL de la table de caractères génériques.
Références	Propriété de refus par défaut

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Double vérification des transactions entrantes (renforcement de la sécurité de l'instance)

La *glide.security.strict.updates* propriété permet une double vérification de la sécurité sur les transactions entrantes lors de la soumission d'un formulaire et ajoute une couche supplémentaire de validation de table avant qu'un formulaire ne s'affiche dans le navigateur. Cette propriété est définie sur **vrai** par défaut

En savoir plus

Remarque :
Cette propriété est définie sur **vrai** par défaut dans les versions ultérieures Vancouver et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client.

Attribut	Description
Nom de la propriété	glide.security.strict.updates
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour assurer une couche supplémentaire de vérification des autorisations utilisateur avant de présenter le formulaire dans le navigateur.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction ajoute une couche supplémentaire de validation pour vérifier les autorisations utilisateur sur la table/page cible sur l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait y avoir aucun impact.
Risque de sécurité	(Élevé) Vous devez toujours vérifier la demande d'accès lorsque des transactions ont lieu entre deux zones. Cette opération vérifie les autorisations lorsque le formulaire est demandé et avant que le rendu du formulaire ne se produise.
Références	Propriétés des paramètres de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer les ACL pour contrôler les détails du profil en direct (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si un utilisateur doit être en mesure d'afficher tous les champs de détail, tels que le nom de l'entreprise `glide.live_profile.details` et les numéros de téléphone, dans un profil actif.

Selon le paramètre de la `glide.live_profile.details` propriété, les événements suivants se produisent :

- Si la valeur est définie sur **Afficher**, l'accès aux informations de profil actif est accordé, quelles que soient les ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur **ACL**, l'accès aux informations de profil actif est restreint, conformément aux ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur **Masquer**, l'accès aux informations de profil actif est restreint, quelles que soient les ACL créées pour le profil d'utilisateur.

En savoir plus

Attribut	Description
Nom de la propriété	glide.live_profile.détails
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	L'objectif est de permettre uniquement aux utilisateurs autorisés d'accéder aux détails d'un profil actif (tels que le nom de la société, les numéros de téléphone)
Valeur recommandée	ACL
Impact fonctionnel	(Moyen) Si la propriété n'est pas activée, les utilisateurs non autorisés peuvent accéder aux détails du profil actif de tous les autres utilisateurs.
Risque de sécurité	(Moyen) Les demandes d'API doivent toujours respecter les ACL de table. Une restriction doit être appliquée pour empêcher les utilisateurs non autorisés d'accéder aux détails d'un profil actif.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activation de la vérification de l'ACL de AJAXGlideRecord (renforcement de la sécurité de l'instance)

Utilisez la propriété pour effectuer la validation de la règle de contrôle d'accès (ACL, Access Control Rule) lorsque l'accès `glide.script.secure.ajaxgliderecord` aux enregistrements côté serveur, tels que les tables, se fait grâce à des API GlideAjax à l'intérieur d'un script client.

À partir de scripts clients, il est possible d'interroger des données arbitraires sur le serveur à l'aide de l'attribut AJAXGlideRecord (GlideAjax -Client), en utilisant une syntaxe telle qu'un enregistrement Glide côté serveur. Il s'agit d'un outil puissant et utile dans de nombreux déploiements.

Si vous choisissez d'appliquer des listes de contrôle d'accès (ACL) aux appels de l'API GlideAjax, vous ne pouvez interroger que les données auxquelles l'utilisateur actuellement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

connecté a accès. Par exemple, si un utilisateur ESS qui n'a pas les droits de lecture de la table cmn_location est connecté, tout appel d'API GlideAjax à cette table échouera.

Si le est en cours d'exécution sans vérification d'appel Now Platform GlideAjax ACL, une API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder autrement.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.secure.ajaxgliderecord
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Assurez-vous que les ACL de sécurité sont vérifiées et validées même lorsque l'accès aux enregistrements s'effectue via des API côté client.
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cette remédiation applique la relation ACL avec les enregistrements côté serveur lorsque les demandes sont effectuées à l'aide des appels d'API AJAXGlideRecord. Si la configuration ACL n'est pas correctement configurée, il y a un impact potentiel. Pour plus de détails sur son impact et sur la façon de l'identifier, reportez-vous à l'article Audit et examen des transactions GlideRecord côté client (AJAXGlideRecord) [KB0550828] dans le HI Base de connaissances .
Risque de sécurité	(Élevé) Grâce aux scripts clients, il est possible d'interroger des données arbitraires du serveur via l'API GlideAjax. Impossible d'accéder aux ressources côté serveur sans autorisation appropriée, de sorte que l'utilisation de la validation ACL aide l'application à valider la demande en fonction de l'autorisation configurée.
Solution de contournement	Assurez-vous que les ACL appropriées sont créées pour les includes de script, les processeurs et les autres entités utilisées par une API GlideAjax (AJAXGlideRecord) afin qu'elle s'exécute sous l'autorisation appropriée. Implémentez des méthodes telles que `canRead ()`,`canWrite()`, `canCreate()` et `canDelete ()` pour effectuer l'autorisation utilisateur avant d'accéder aux enregistrements de table à l'aide de GlideRecord. Une autre méthode consiste à utiliser GlideRecordSecure. La classe est héritée du serveur GlideRecord qui effectue les mêmes fonctions que GlideRecord et applique également les ACL.
Références	Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Cette propriété appartient à la même famille de propriétés qui sécurisent et restreignent l'exécution de scripts provenant du client : • *glide.script.use.sandbox*: voir Bac à sable pour les scripts générés par le client. • *glide.script.allow.ajaxevaluate*: voir Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Autorisation des demandes Excel (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les *glide.basicauth.required.excel* demandes Excel entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.excel
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes Excel.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données Excel sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes Excel entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Module d'extension de rôle explicite (renforcement de la sécurité de l'instance)

Activez le module d'extension Explicit Role (*com.glide.explicit_roles*) pour fournir à l'instance les nouveaux rôles snc_internal et snc_external pour les applications B2B et B2C, empêchant ainsi les utilisateurs externes d'accéder aux données internes. Les utilisateurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de l'entreprise (employés) doivent avoir le rôle interne, tandis que les utilisateurs non professionnels (non-employés) doivent avoir le rôle externe.

Lorsque vous installez le module d'extension de rôle explicite :

- Elle affecte le nouveau rôle de snc_internal à tous les utilisateurs existants. Il affecte également toutes les tables sans aucun rôle avec le rôle snc_internal.
- Lorsque vous créez un utilisateur ou une table après avoir activé le module d'extension Explicit Role, l'utilisateur Now Platform ou la table est affecté au rôle snc_internal.
- La Now Platform empêche les utilisateurs ayant le rôle snc_external d'accéder à une table qui n'est pas explicitement affectée au rôle snc_external.
- Toutes les tables ayant le rôle public sont accessibles à la fois par les utilisateurs internes et externes.
- Certains widgets du portail de services nécessitent une connexion, mais pas de rôle d'utilisateur spécifique. Après l'installation du module d'extension de rôles explicites, ces portails deviennent inaccessibles aux utilisateurs externes.
  - Pour autoriser l'accès aux utilisateurs externes, modifiez votre widget pour modifier les rôles **requis de vide** à **snc_internal, snc_external**.
  - C'est le cas, par exemple, des clients qui utilisent l'application Case Management et qui ont besoin que des utilisateurs externes puissent joindre des fichiers à leurs enregistrements de ticket. La modification de la configuration du widget **encryption-context-picker** comme décrit permet aux utilisateurs externes de se joindre comme prévu.
  - Pour plus d'informations sur la configuration des widgets, consultez Configurer les options d'instance de widget

Remarque :
Ne déplacez pas les ensembles de mises à jour système entre les instances avec et sans le module d'extension Explicit Roles activé. Pour plus d'informations, consultez Ensembles de mises à jour système .

Résumé du rôle

snc_internal

Ce rôle est attribué à tous les utilisateurs internes (employés ou internes à une organisation). Tout nouvel utilisateur ajouté obtient également ce rôle lors de sa première connexion/emprunt d'identité, à condition que l'utilisateur ne dispose pas du rôle snc_external déjà affecté. Toutes les règles de contrôle d'accès (ACL) existantes sans rôle sont corrigées avec le rôle « snc_internal ». Pour les nouveaux ACL, le Now Platform ajoute automatiquement ce rôle si l'ACL est enregistrée sans rôle.

snc_external

Ce rôle indique que l'utilisateur est externe à votre organisation et qu'il ne doit pas avoir accès aux ressources, sauf si :

- Vous autorisez explicitement l'accès au rôle snc_external par le biais d'ACL, ou
- Vous leur accordez explicitement des rôles supplémentaires.

Par défaut, les utilisateurs ayant le rôle snc_external ne peuvent pas non plus accéder aux ressources autres que celles de type enregistrement, telles que les processeurs et les pages de l'interface utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

publique

Toutes les entités dotées d'un rôle public sont accessibles à la fois aux utilisateurs snc_internal et aux utilisateurs snc_external.

Lors de l'utilisation du module d'extension Explicit Role :

1. Vérifiez et validez qu'aucune table ayant le rôle public ne contient d'enregistrement sensible pour les utilisateurs externes, y compris les utilisateurs publics non authentifiés.
2. Si la table ayant le rôle public contient des données sensibles et que vous souhaitez restreindre les enregistrements sensibles aux utilisateurs externes, procédez comme suit :
   - Supprimer le rôle public de la table ou
   - Ajoutez des ACL scriptées supplémentaires à la table.
3. Vérifiez et validez que tous les points de terminaison, tels que les API REST scriptées, utilisent les rôles ou vérifient explicitement à l'aide de `GlideRecordSecure`canRead(),canWrite(), canUpdate() et canDelete().

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.explicit_roles
Type de configuration	Module d'extension > de définition du système
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Empêcher les utilisateurs externes d'accéder aux données internes.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Aucun impact significatif, car le module d'extension affecte automatiquement le rôle snc_internal à la table, de sorte que les utilisateurs internes existants disposent toujours de l'accès nécessaire.
Risque de sécurité	(Élevé) Les utilisateurs externes (non employés) peuvent accéder à de nombreuses tables sensibles dans le Now Platform qui n'ont aucun rôle affecté. Ils sont destinés à être accessibles uniquement aux utilisateurs internes (Employés).
Références	Explicit Roles

Étapes à configurer

Lors de la création d'une fonctionnalité ou d'une application avec les rôles explicites :

1. Créez un rôle qui hérite du rôle snc_external pour votre nouvelle fonctionnalité ou application.
2. Lors de la création d'un utilisateur externe, supprimez le rôle snc_internal et ajoutez le rôle nouvellement créé qui hérite du rôle snc_external.
3. Lors de l'ajout du nouveau rôle qui hérite du rôle snc_external à la table existante, vérifiez et validez que la table ne contient aucun enregistrement sensible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Lors de la création d'une table, vérifiez que la table n'est accessible que par les rôles d'utilisateur internes et externes autorisés.
5. Lors de la création de points de terminaison tels que l'API REST scriptée, utilisez GlideRecordSecure ou vérifiez explicitement les rôles à l'aide de `canRead()`,`canWrite()`, `canUpdate()` et `canDelete()`.

Lors de la création d'une table avec le rôle public, assurez-vous que la table ne contient aucun enregistrement sensible pour les utilisateurs externes, y compris les utilisateurs publics non authentifiés.

Autorisation des demandes d'importation (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les *`glide.basicauth.required.importprocessor`* demandes d'importation entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.importprocessor
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes d'importation.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification lors de l'importation de sources de données dans les tables/pages d'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Récupération de données à partir d'un fichier au format CSV .
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes d'importation de source de données, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Services web SOAP de sécurité Service web SOAP

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisation de demande de PDF (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.pdf` demandes PDF entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.pdf
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes PDF.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données PDF sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la rubrique Jeux d'importation de services Web .
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes PDF entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Surveillance des performances (ACL) (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour contrôler stats.do `glide.security.diag_txns_acl` , threads.do, thread_pool_stats et replication.do accès à partir d'une connexion non authentifiée.

Lorsque vous définissez cette propriété sur **vrai**, la `glide.security.diag_txns_acl` propriété autorise uniquement l'accès aux éléments suivants par le compte administrateur :

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sans activer ce paramètre, il est toujours possible d'accéder à ces ressources à partir d'une connexion non authentifiée.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.diag_txns_acl
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Restreindre l'accès aux pages de configuration au compte administrateur uniquement
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique uniquement le compte administrateur pour accéder aux données sensibles de l'application à des fins de journalisation et de dépannage.
Risque de sécurité	(Faible) Les données sensibles telles que les détails du serveur, les threads et les processus exécutés sur le serveur ne doivent jamais être visibles ou accessibles à l'utilisateur final sans privilèges appropriés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restriction IP de surveillance des performances (renforcement de la sécurité de l'instance)

Utilisez cette `glide.custom.ip.authenticate.allow` propriété pour permettre uniquement à une liste spécifiée séparée par des virgules ou à une plage d'adresses IP d'accéder aux pages stats.do, threads.do et replication.do. Si cette propriété n'est pas activée, il est possible d'accéder à ces types de pages à partir de n'importe quelle adresse IP.

Remarque :
Sur la base de certains changements récents, le contrôle d'accès à l'adresse IP doit être utilisé pour toutes les restrictions IP. Reportez-vous à la section Étapes de configuration dans Restreindre l'accès à des plages IP spécifiques.

En savoir plus

Attribut	Description
Nom de la propriété	glide.custom.ip.authenticate.allow
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Limitez l'accès uniquement aux pages de configuration aux adresses IP de la liste d'inclusion.
Valeur recommandée	Liste d'adresses IP séparées par des virgules.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Faible) Les pages d'informations sensibles sont accessibles même à partir d'une adresse IP non approuvée.
Risque de sécurité	(Faible) L'exposition inutile à l'instance cible sur Internet doit être limitée à l'aide de la fonctionnalité de contrôle d'accès IP.
Référence	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Protection de la vie privée sur les includes de script pouvant être appelés par le client (renforcement de la sécurité de l'instance)

Par défaut, les includes de script pouvant être appelés par le client qui ne définissent pas explicitement la visibilité sont publics. Si nécessaire, ajoutez la propriété pour activer le contrôle de la confidentialité sur tous les includes de script appelables par les clients accessibles via des `glide.script.ccsi.ispublic` pages publiques.

Lorsque vous ajoutez cette propriété, vous devez définir sa valeur sur **faux**, ce qui signifie que tous les includes de script pouvant être appelés par le client sont privés et modifie leur visibilité dans les pages publiques.

Remarque :
Vous ne pouvez pas ajouter la propriété avec une valeur **vrai** ou modifier sa valeur de **faux** à **vrai**. Si vous tentez de le faire, un message d'erreur s'affiche.

Si nécessaire, vous pouvez modifier le paramètre de confidentialité d'un include de script individuel pouvant être appelé par un client en ajoutant la fonction `isPublic()`.

- Le paramètre `isPublic()` a priorité sur la `glide.script.ccsi.ispublic` propriété.
- Par exemple, si vous définissez `isPublic()` sur **true** dans un script individuel, il devient public, ce qui remplace la propriété qui rend privés tous les autres includes de script pouvant être appelés par le `glide.script.ccsi.ispublic` client.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.ccsi.ispublic
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Rendre privé les includes de script pouvant être appelés par le client signifie que les invités qui accèdent aux pages publiques ne peuvent pas accéder à l'include de script pouvant être appelé par le client. Un utilisateur non connecté ne peut pas exécuter de script privé.
Valeur recommandée	faux
Impact fonctionnel	(Élevé) Si les includes de script pouvant être appelés par le client sont désignés comme publics (c'est-à-dire que cette propriété est manquante), les utilisateurs non authentifiés peuvent exécuter des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	scripts clients. Ajouter la propriété restreint l'exécution de scripts par un utilisateur non connecté.
Risque de sécurité	(Élevé) Si vous n'ajoutez pas cette propriété, les includes de script côté client contournent les ACL, ce qui peut entraîner des fonctionnalités publiques non prévues. Si le script client fournit des informations confidentielles, il peut présenter un risque potentiel négatif pour la sécurité.
Solution de contournement	Si vous définissez la propriété sur **faux,** tous les includes de script pouvant être appelés par le `glide.script.ccsi.ispublic` client sont privés. Vous pouvez modifier le paramètre de confidentialité d'un include de script individuel pouvant être appelé par un client en ajoutant la fonction isPublic(). La fonction isPublic a priorité sur la `glide.script.ccsi.ispublic` propriété. Ajoutez la syntaxe suivante à l'include de script : `isPublic :function(){return[vrai/faux] ;},`

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver l'accès public aux favoris

Utilisez le `glide.ui.magellan.favorites.allow_public` pour spécifier si les utilisateurs non authentifiés sont autorisés à voir **les favoris** dans le navigateur.

L'accès public aux favoris est conforme si `glide.ui.magellan.favorites.allow_public` la valeur est définie sur **faux**.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.magellan.favorites.allow_public`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Contrôlez si les utilisateurs non authentifiés sont autorisés à voir **les favoris** dans le navigateur.
Type	vrai/faux
Valeur recommandée	`false`
Dépendances de Sécurité	Définissez la valeur `glide.ui.magellan.favorites.allow_public`**sur faux**.
Impact fonctionnel	(Moyen) L'activation de cette propriété agit comme une couche de protection contre les utilisateurs non autorisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Moyen) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé aux données sensibles.
Références	Créer ou afficher des favoris

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès à des plages IP spécifiques (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour restreindre l'accès `com.snc.ipauthenticator` à des plages IP spécifiques. À moins que l'accès public ne soit destiné à l'instance, les administrateurs doivent limiter l'accès aux blocs réseau IP qui leur sont affectés.

Prérequis

Avant de définir cette propriété, vous devez activer le module d'extension Authentification `com.snc.ipauthenticator` basée sur la plage IP. Pour en savoir plus, consultez Authentification basée sur la plage IP et dans la section Étapes de configuration (ci-dessous).

En savoir plus

Attribut	Description
Nom du module d'extension	com.snc.ipauthenticator
Type de configuration	Sécurité de système > Contrôle d'accès à l'adresse IP
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour ajouter la plage d'adresses IP qui peut ou ne peut pas accéder à l'instance aux listes de domaines approuvés et non approuvés.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Des plages IP refusées par le client sont utilisées pour cet élément de rattrapage. Aucun impact, car le client définit la liste cible.
Risque de sécurité	(Faible) L'exposition inutile à l'instance cible sur Internet doit être limitée à l'aide de la fonctionnalité de contrôle d'accès IP.
Références	Authentification basée sur la plage IP

Étapes à configurer

1. Assurez-vous que le module d'extension com.snc.ipauthenticator est actif.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès à l'adresse IP**.
3. Cliquez sur **Nouveau** pour créer une liste d'exclusion (refus) ou une liste d'inclusion (autorisation) d'adresses IP.
4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisation de demande de RSS (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.rss` demandes RSS entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.rss
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes RSS.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification lors du traitement des demandes RSS sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Générateur de flux RSS .
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes RSS entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification de base RSS

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Navigateur Web SAML 2.0 Profil SSO (renforcement de la sécurité de l'instance)

Le `com.snc.integration.sso.saml20.update1` module d'extension garantit que le module d'extension SAML 2.0 Single Sign-On est actif.

Le langage de balisage d'assertion de sécurité (SAML) est une norme basée sur XML pour l'échange de données d'authentification et d'autorisation entre des domaines de sécurité. SAML échange des informations de sécurité entre un fournisseur d'identité (un producteur d'assertions) et un fournisseur de services (un consommateur d'assertions).

Il `com.snc.integration.sso.saml20.update1` s'agit d'un module d'extension requis, mais vous n'avez pas besoin de l'activer manuellement. Le `sso.multi.installer` installe tous les modules d'extension SAML requis et contient également des scripts d'implémentation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

saml2 qui fournissent des options pour la validation des réponses. Pour en savoir plus, reportez-vous aux rubriques de la section Références dans En savoir plus.

En savoir plus

Attribut	Description
Nom du module d'extension	com.snc.integration.sso.saml20.update1 (nouveau)
Type de configuration	Définition du système > Modules d’extension
Configurer dans le centre de sécurité de l’instance	Oui
Objectif	Pour se prémunir contre les attaques de script de site à site.
Valeur recommandée	Actif
Rôle requis	Votre administrateur ne peut pas activer le module d’extension. Demandez à la personne disposant de privilèges de sécurité élevés de l’activer sur l’instance.
Références	Authentification avec intégration SAML SAML Authentification Mettre à jour votre intégration SAML 2.0 existante

Pour en savoir plus sur l’activation d’un module d’extension, reportez-vous à la section Activate a plugin .

Autorisation de demande de script (renforcement de la sécurité de l’instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.scriptedprocessor` demandes de script entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.scriptedprocessor
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l’instance	Oui
Objectif	Pour appliquer l’authentification de base aux demandes de scripts.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Ce rattrapage applique l’authentification sous la forme d’une autorisation de base. • Il effectue cette authentification lors du traitement des demandes de script sur l’instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d’accéder à ce contenu, avec les autorisations de contrôle d’accès nécessaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes de script entrant, un utilisateur non autorisé accède au contenu/aux données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Démarrage rapide de la sécurité (règles ACL) (renforcement de la sécurité de l'instance)

Activez le module d'extension Security Quick Start (ACL Rules) (*com.snc.system_security*) pour créer plusieurs ACL importantes qui valident les contrôles d'accès sur certaines des tables clés du système.Now Platform

Ces règles permettent de démarrer rapidement la sécurisation de nombreuses tables système, simplifiant ainsi la mise en production d'une instance. Le module d'extension de démarrage rapide de la sécurité (règles ACL) est installé automatiquement sur toutes les nouvelles instances.

En savoir plus

Attribut	Description
ID de module d'extension	com.snc.system_security
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Activez le module d'extension de démarrage rapide de la sécurité (règles ACL) pour assurer une conformité de sécurité appropriée. Il fournit des ACL de base qui sécurisent les tables système en premier lieu au lieu de les créer manuellement pour chaque table système fournie avec la mise en service par défaut d'une instance. Ces ACL sont utiles lorsque l'instance nouvellement créée doit passer rapidement en production.
Valeur recommandée	Actif
Impact fonctionnel	(Moyen) Il y a un impact fonctionnel important si ce module d'extension est installé sans audit des ACL existantes sur l'instance. La sensibilisation et les définitions des clients sont nécessaires avant que la correction puisse avoir lieu.
Risque de sécurité	(Élevé) Le contrôle d'accès doit être appliqué pour verrouiller l'accès non souhaité à l'instance. Les règles de démarrage rapide ACL ont été créées pour fournir un point de départ pour sécuriser de nombreuses tables système afin de faciliter la mise en production rapide d'une entreprise.
Références	Démarrage rapide de la sécurité : règles ACL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étapes à configurer

Si ce module d'extension n'est pas activé sur votre instance, contactez ServiceNow le support. L'activation du module d'extension à ce stade peut modifier l'accès de sécurité aux tables déjà utilisées dans un environnement de production. Si un administrateur est intéressé par les nouvelles règles ACL fournies par le module d'extension, vous pouvez créer manuellement une ou plusieurs d'entre elles dans une instance existante si nécessaire. Cette liste d'ACL peut être utilisée à titre indicatif dans ce cas.

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à la section Activate a plugin .

Module d'extension de contrôle d'accès SNC (renforcement de la sécurité de l'instance)

Activez le module d'extension SNC Access Control (`com.snc.snc_access_control`) pour contrôler l'accès du personnel à vos instances Service et assistance client .

La configuration par défaut permet Now Platform au service clientèle et au support d'accéder aux instances via un processus interne qui crée des informations d'identification de support à court terme. Bien que tous les accès soient audités, certains clients préfèrent contrôler cet accès.

Ce module d'extension permet à l'administrateur client d'interdire Service et assistance client aux employés d'accéder à l'instance. Cette décision a un impact sur les SLA de support, car vous devez activer Now Platform l'accès avant que les activités de support puissent commencer. Pour en savoir plus, consultez Contrôle d'accès ServiceNow.

En savoir plus

Attribut	Description
Nom du module d'extension	com.snc.snc_access_control
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Interdit Service et assistance client aux employés d'accéder à l'instance
Valeur recommandée	Actif
Rôle requis	L'administrateur client ne peut pas activer ce module d'extension. Il doit être explicitement demandé, car l'activation du module d'extension nécessite des privilèges élevés.
Impact fonctionnel	(Faible) Si ce module d'extension est inactif, tous les Service et assistance client employés peuvent accéder à l'instance du client. L'activation du module d'extension permet au client de restreindre l'accès aux seuls employés autorisés Service et assistance client .
Risque de sécurité	(Faible) Exposition inutile de l'accès aux instances à un groupe plus large de personnes.
Références	Contrôle d'accès ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étapes à configurer

1. Pour demander le module d'extension, procédez comme suit dans Activation du contrôle d'accès ServiceNow. Les clients doivent demander le module d'extension SNC Access Control (com.snc.snc_access_control) auprès de HI.
2. Pour activer le contrôle d'accès SNC, procédez comme suit dans Configuration ServiceNow du contrôle d'accès. Configurez un enregistrement de contrôle d'accès pour spécifier un ou plusieurs Service et assistance client employés qui ont l'autorisation de se connecter à votre instance.

Vérification du type de contenu SOAP (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la `glide.soap.require_content_type_xml` validation d'un type de contenu comme texte/xml et protéger contre les demandes SOAP invalides.

- Lorsqu'elle est définie sur **vrai**, elle Now Platform valide le type de contenu comme text/xml et protège contre les demandes SOAP invalides.
- Si la valeur est définie sur **faux**, toutes les valeurs de type de contenu sont autorisées.

En savoir plus

Attribut	Description
Nom de la propriété	glide.soap.require_content_type_xml
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protection contre les demandes SOAP invalides
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation active la validation du type de contenu SOAP pour toutes les demandes SOAP entrantes. • Si vous utilisez un type de contenu autre que texte/xml pour les demandes entrantes, cela peut entraîner l'échec potentiel des transactions SOAP. • Si vous n'utilisez pas le type MIME correct, cela peut perturber les intégrations tierces.
Risque de sécurité	(Élevé) Lors de l'acceptation de demandes SOAP entrantes, la validation appropriée est effectuée pour s'assurer que le type de contenu pertinent est défini dans le cadre de la demande. Il limite les réponses SOAP non valides qui peuvent être considérées comme un risque pour la sécurité.
Référence	Types de contenu

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restriction IP stricte (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer un `glide.ip.authenticate.strict` ensemble strict d'adresses IP, comme DC et VPN de sécurité, pour accéder à cette instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ip.authenticate.strict
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Permet aux employés de ServiceNow d'accéder à l'instance uniquement par le biais d'un ensemble sécurisé de plages IP
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Si cette propriété n'est pas activée, les employés ServiceNow peuvent accéder à l'instance du client via toutes les plages IP. L'activation de la propriété restreint l'accès à un ensemble sécurisé de plages IP (VPN sécurisé, DC). **Remarque :** Si vous définissez cette propriété sur vrai, le Now Platform utilise une propriété plus restrictive `glide.ip.authenticate.allow.secured` au lieu de la restriction IP de surveillance des performances. Cette propriété ne peut pas être remplacée.)`glide.ip.authenticate.allow.secured` pour un ensemble de plages IP qui peuvent accéder à l'instance.
Risque de sécurité	(Faible) Exposition inutile de l'accès aux instances à un groupe plus large de personnes.
Référence	Authentification basée sur la plage IP

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Remarque :
Une règle de refus de tout doit être ajoutée au contrôle d'accès IP pour restreindre l'accès de toute adresse IP non ajoutée au contrôle d'accès IP. Toutes les adresses IP autorisées requises doivent ensuite être ajoutées au contrôle d'accès IP.

Autorisation de demande de déchargement (renforcement de la sécurité de l'instance)

Utilisez la propriété (useUnloadFormat) pour indiquer si les `glide.basicauth.required.unl` demandes de déchargement entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.unl
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes de déchargement.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données non téléchargées sur l'instance.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes de déchargement de source de données, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Autorisation de demande WSDL (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.wsdl` demandes WSDL (Web Services Description Language) entrantes doivent requérir une authentification de base.

Remarque :
Si vous choisissez de ne pas exiger l'authentification de base pour les demandes WSDL entrantes, vous devez modifier les règles de contrôle d'accès (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.wsdl
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes WSDL.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données WSDL sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les services Web WSDL, un utilisateur non autorisé peut accéder à du contenu/des données WSDL sensibles sur l'instance cible.
Références	Sécurité des services Web

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property.

Autorisation de demande XML (renforcement de la sécurité de l'instance)

Utilisez la propriété pour indiquer si les `glide.basicauth.required.xml` demandes XML entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.xml
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes XML.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données XML sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Étape de l'analyseur XML.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes XML entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autorisation de demande XSD (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.xsd` demandes XSD (XML Schema Definition) entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	glide.basicauth.required.xsd
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'authentification de base aux demandes XSD.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données XSD sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Sessions non interactives .
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les demandes XSD entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Pièces jointes (renforcement de la sécurité de l'instance)

De nombreux Now Platform processus métier permettent le téléchargement de données/informations. Il vérifie régulièrement la validité et la sécurité du texte, mais l'acceptation de ces fichiers peut introduire encore plus de risques.

Pour réduire le risque, vous devez valider les fichiers malveillants afin qu'ils Now Platform puissent se protéger correctement contre les attaquants qui envoient ces fichiers. Vous gérez ces fichiers en incluant une logique métier qui analyse les fichiers pendant le processus de chargement et rejette les fichiers perçus comme malveillants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Références internes

- Administration des pièces jointes
- Configurer les propriétés système des pièces jointes

Types MIME téléchargeables (renforcement de la sécurité de l'instance)

Utilisez la *glide.ui.attachment.download_mime_types* propriété pour spécifier une liste de types MIME séparés par des virgules qui doivent être téléchargés, mais qui ne doivent pas être affichés dans le navigateur.

Pour afficher une liste des types MIME existants, tapez /sys_attachment_icon_rule_list.do. Vous pouvez activer n'importe lequel de ces types MIME pour satisfaire aux exigences de conformité de sécurité dans le Now Platform.

Remarque :
Si vous définissez la propriété **Forcer le téléchargement des types MIME** sur **true**, elle remplace la propriété **Types MIME téléchargeables** , qui est une liste de types MIME téléchargeables séparés par des virgules. Pour en savoir plus, consultez Forcer le téléchargement des types MIME.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.attachment.download_mime_types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour empêcher l'affichage des types de fichiers dans le navigateur afin d'éviter toute exécution de script malveillante cachée.
Valeur recommandée	Certains types de fichiers définis, par exemple, text/html, text/csv.
Impact fonctionnel	(Faible) Ce rattrapage permet d'effectuer des contrôles de validation avant d'effectuer une action lorsque vous cliquez sur une pièce jointe dans une Now Platform application. Il n'y a pas d'impact potentiel, mais l'expérience utilisateur est altérée.
Risque de sécurité	(Moyen) Les vecteurs d'attaque de scripting côté client se déclinent en différentes saveurs et l'abus de pièce jointe de type MIME ne fait pas exception. Les attaquants peuvent abuser les types MIME et placer du contenu de script non souhaité dans la pièce jointe du côté de la victime pour capturer des informations sensibles. Dans le contexte actuel, renseignez la propriété avec une liste de types MIME de pièce jointe séparés par des virgules qui ne doivent pas être affichés en ligne dans le navigateur. Exemple : text/html

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la liste de refus pour les pièces jointes (renforcement de la sécurité de l'instance)

Utilisez la `glide.security.attachment_type.use_blacklist` propriété pour indiquer si le doit valider la pièce jointe par rapport à une liste d'exclusion Now Platform spécifiée.

Remarque :
Ne définissez pas la `glide.security.attachment_type.use_blacklist` propriété sur vrai tant que vous n'avez pas configuré les `glide.attachment.blacklisted.extensions` propriétés and `glide.attachment.blacklisted.types` . Pour en savoir plus, consultez Spécifier les extensions refusées et Spécifier les types de fichiers refusés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.attachment_type.use_blacklist
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Limitez l'opération de chargement (insertion/écriture/mise à jour) des pièces jointes dont l'extension et le type de fichier sont douteux, tels que exe, dll, jar, text/html.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Aucun impact sur la fonctionnalité, sauf en cas de tentative de chargement d'extensions ou de types de fichiers spécifiés dans les propriétés énumérées d'exclusion (`glide.attachment.blacklisted.extensions` et `glide.attachment.blacklisted.types`)
Risque de sécurité	(Moyen) Un utilisateur malveillant peut télécharger des pièces jointes infectées par un logiciel malveillant avec des extensions et/ou des types de fichiers exécutables courants.
Solution de contournement	Des propriétés sont disponibles dans le système de base qui résolvent le même problème avec des listes d'inclusion au lieu de listes d'exclusion. Pour en savoir plus, consultez : • Restreindre les extensions de fichiers • Restriction sur les types MIME de téléchargement

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer les restrictions de téléchargement de fichiers (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer les `glide.ui.strict_customer_uploaded_static_content` restrictions sur les types de fichiers qui peuvent être téléchargés lorsqu'ils ont été chargés à l'aide de la fonctionnalité Charger un fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous utilisez cette propriété avec la `glide.ui.strict_customer_uploaded_content_types` propriété, ce qui crée une liste de types de fichiers téléchargeables restreints délimités par des virgules. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.strict_customer_uploaded_static_content
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	S'assurer que les types de fichiers sécurisés sont autorisés à être téléchargés à partir de l'application.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction applique la restriction des téléchargements de fichiers en fonction des valeurs spécifiées dans la `glide.ui.strict_customer_uploaded_content_types` propriété. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.
Risque de sécurité	(Moyen) Les restrictions de téléchargement de fichiers doivent être appliquées à toutes les sources d'entrée d'utilisateur non approuvées.

Appliquer des règles strictes pour le téléchargement d'images par l'utilisateur (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer le `glide.security.strict.user_image_upload` contrôle d'accès pour le chargement/la mise à jour d'une photo de profil lorsqu'il est effectué sur un enregistrement utilisateur.

Ce paramètre ouvre la possibilité pour un utilisateur non autorisé de télécharger une image sur le profil d'un autre utilisateur.

- Lorsque vous définissez cette propriété sur **vrai**, les ACL de table sont appliquées lors du chargement de photos, et seuls les utilisateurs autorisés peuvent charger une image.
- Lorsque vous définissez ce paramètre sur **faux**, les ACL ne sont pas appliquées lors des chargements d'images dans le champ Photo.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.strict.user_image_upload
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour restreindre le téléchargement de l'image d'un utilisateur aux seuls utilisateurs autorisés.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Aucun impact sur la fonctionnalité car les utilisateurs autorisés peuvent toujours télécharger des images sur leur profil d'utilisateur.
Risque de sécurité	(Moyen) Lorsque vous définissez cette propriété sur **faux**, un utilisateur authentifié peut télécharger une image sur le compte d'un autre utilisateur sans autorisation.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Forcer le téléchargement Types MIME (renforcement de la sécurité de l'instance)

Utilisez la `glide.ui.attachment.force_download_all_mime_types` propriété pour forcer le téléchargement de toutes les pièces jointes de type MIME.

Remarque :
Si vous définissez la propriété **Forcer le téléchargement des types MIME** sur **true**, elle remplace la propriété **Types MIME téléchargeables** , qui est une liste de types MIME téléchargeables séparés par des virgules. Pour en savoir plus, consultez Types MIME téléchargeables.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.attachment.force_download_all_mime_types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour imposer le téléchargement de toutes les pièces jointes, au lieu de s'exécuter dans le navigateur.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction impose le téléchargement de toutes les pièces jointes. Aucun impact sur la fonctionnalité, mais il en résulte une altération de l'expérience utilisateur.
Risque de sécurité	(Élevé) Pour réduire les attaques de script côté client, les pièces jointes doivent être téléchargées de force plutôt que d'être rendues dans le contexte du navigateur.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les extensions de fichiers (renforcement de la sécurité de l'instance)

Définissez les types de fichiers qui peuvent être téléchargés sur votre instance à l'aide de la `glide.attachment.extensions` propriété système. Cette propriété utilise une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

liste de types d'extensions de fichier autorisés séparés par des virgules. Seuls les types d'extensions de fichier spécifiés peuvent être téléchargés en tant que pièces jointes.

Utilisez la *glide.attachment.extensions* propriété sur votre instance pour fournir les avantages suivants :

Amélioration de la sécurité

Utilisez cette propriété pour améliorer la sécurité en empêchant les utilisateurs de télécharger des fichiers nuisibles, tels que des virus, en tant que pièces jointes. Sécurisez votre instance en bloquant les types généralement utilisés par les programmes exécutables ou les scripts.

Évitez les types de fichiers incompatibles

Utilisez cette propriété pour empêcher les utilisateurs de charger des fichiers incompatibles. Par exemple, certains navigateurs ne prennent pas en charge les icônes au format PNG. En n'incluant pas l'extension de fichier `png` , vous pouvez empêcher les utilisateurs de télécharger des fichiers PNG.

Important :
Cette propriété ne restreint pas les fichiers en fonction du type de fichier réel (type MIME), mais uniquement en fonction de l'extension. Pour restreindre les chargements basés sur le type MIME, configurez la propriété une fois que vous avez terminé la *glide.security.file.mime_type.validation* configuration de la *glide.attachment.extensions* propriété. Pour plus d'informations sur la configuration *glide.security.file.mime_type.validation*, consultez Restriction de type MIME de téléchargement.

Étapes à configurer

1. Dans le navigateur de filtre de votre instance, saisissez `sys_properties.list`, puis appuyez sur Entrée.
2. Recherchez et ouvrez la *glide.attachment.extensions* propriété.
3. Dans le champ **Valeur** , saisissez les extensions de fichier que vous souhaitez autoriser pour le chargement en tant que pièces jointes. Séparez les multiples entrées dans le champ à l'aide de virgules. Voici un exemple de valeur pour plusieurs entrées *doc,docx,xls,xlxs,pdf,jpeg,jpg,png,ico*.

   Remarque :
   Si aucun type de fichier n'est spécifié dans le champ **Valeur** , n'importe quel type de fichier peut être chargé en tant que pièce jointe.

4. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

En savoir plus

Attribut	Description
Nom de la propriété	glide.attachment.extensions
Type de configuration	Propriété système (/sys_properties_list.do)
Configurable dans Centre de sécurité de l'instance	Non
Objectif	Pour permettre uniquement le téléchargement des extensions de fichier acceptables lors de la pièce jointe. Il bloque une tentative de téléchargement d'extensions potentiellement malveillantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	Certaines extensions de fichiers définies, telles que doc, docx, pdf, xls, xlsx
Impact fonctionnel	(Moyen) Cette correction restreint toutes les extensions de fichiers, à l'exception de celles qui figurent dans la liste d'inclusion. Aucun impact sur la fonctionnalité sauf en cas de tentative de chargement d'un fichier autre que les extensions acceptables par l'organisation.
Risque de sécurité	(Moyen) Comme la vérification du type MIME dépend de cette propriété, il est recommandé d'atténuer les vulnérabilités liées au chargement de fichiers malveillants.

Restreindre l'accès non authentifié aux pièces jointes (renforcement de la sécurité de l'instance)

Utilisez cette `glide.image_provider.security_enabled` propriété pour contrôler les paramètres de sécurité des images. Si la valeur est définie sur **vrai**, les images ne sont visibles que par les utilisateurs authentifiés et autorisés. Si elle est définie sur **faux**, les images sont visibles par toutes les personnes qui possèdent l'URL de la pièce jointe.

En savoir plus

Attribut	Description
Nom de la propriété	glide.image_provider.security_enabled
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Empêche tout accès non authentifié à la pièce jointe lorsqu'elle est rendue au format .iix.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Pas d'impact significatif sur la fonctionnalité. L'expérience utilisateur peut être un peu affectée, car l'utilisateur qui accédait directement au fichier .iix doit passer par l'authentification.
Risque de sécurité	(Élevé) Une restriction doit être appliquée pour les utilisateurs non authentifiés, car certaines pièces jointes peuvent contenir des informations sensibles.
Références	Administration des pièces jointes Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Spécifier les extensions de pièce jointe exclues (renforcement de la sécurité de l'instance)

Lorsque vous activez la validation de la liste d'exclusion dans le Now Platform, utilisez la propriété pour créer une liste délimitée par des `glide.attachment.blacklisted.extensions` virgules des types d'extensions de fichiers

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

téléchargeables restreints. Le chargement des types d'extensions de fichiers spécifiés est limité.

Prérequis

Définissez cette propriété avant de définir la `glide.security.attachment_type.use_blacklist` propriété sur vrai. Pour en savoir plus, consultez Activer la liste noire pour les pièces jointes.

En savoir plus

Attribut	Description
Nom de la propriété	glide.attachment.blacklisted.extensions
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Limitez l'opération de chargement (insertion/écriture/mise à jour) des pièces jointes dont l'extension de fichier est douteuse.
Type	Chaîne
Valeur recommandée	Extensions de fichiers spécifiées par l'utilisateur. Les exemples courants incluent ex, dll, xslx.
Impact fonctionnel	(Faible) Aucun impact sur la fonctionnalité sauf en cas de tentative de chargement d'une extension de fichier spécifiée sous cette propriété.
Risque de sécurité	(Moyen) Un utilisateur malveillant peut télécharger une pièce jointe infectée par un logiciel malveillant avec des extensions de fichiers exécutables courantes.
Solution de contournement	Les propriétés sont disponibles dans les fonctionnalités du système de base qui résolvent le même problème, avec une liste d'inclusion au lieu d'une liste d'exclusion. Pour en savoir plus, consultez : • Restreindre les extensions de fichiers • Restriction sur les types MIME de téléchargement

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Spécifier les types de fichiers de pièces jointes exclus (renforcement de la sécurité de l'instance)

Lorsque la validation de la liste d'exclusion est activée dans le Now Platform, utilisez la propriété pour créer une liste de types de fichiers téléchargeables restreints délimitée par des `glide.attachment.blacklisted.types` virgules. Le chargement des types de fichiers spécifiés est limité.

Prérequis

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définissez cette propriété avant de définir la `glide.security.attachment_type.use_blacklist` propriété sur vrai. Pour en savoir plus, consultez Activer la liste noire pour les pièces jointes.

En savoir plus

Attribut	Description
Nom de la propriété	glide.attachment.blacklisted.types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Limitez l'opération de chargement (insertion/écriture/mise à jour) des pièces jointes dont le type de fichier est douteux. Exemple : text/html.
Valeur recommandée	Certains types de fichiers définis (par exemple : text/html, text/csv).
Impact fonctionnel	(Faible) Aucun impact sur la fonctionnalité sauf en cas de tentative de chargement d'un type de fichier spécifié sous cette propriété.
Risque de sécurité	(Moyen) Un utilisateur malveillant peut télécharger une pièce jointe infectée par un programme malveillant avec des types de fichiers exécutables courants.
Solution de contournement	Les propriétés sont disponibles dans les fonctionnalités du système de base qui résolvent le même problème avec la liste d'inclusion plutôt qu'avec la liste d'exclusion. Pour en savoir plus, consultez : • Restreindre les extensions de fichiers • Restriction sur les types MIME de téléchargement

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Types de fichiers téléchargeables (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour créer une liste de types de fichiers téléchargeables restreints délimitée par des `glide.ui.strict_customer_uploaded_content_types` virgules. Les types de fichiers spécifiés sont les seuls qui peuvent être téléchargés en tant que contenu statique à partir d'une instance.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.strict_customer_uploaded_content_types
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour s'assurer que seuls les types de fichiers des listes d'inclusion sont autorisés à être téléchargés.
Valeur recommandée	Spécifié par l'utilisateur (commun : doc, docx, xls, xlsx, pdf, etc.)
Impact fonctionnel	(Moyen) Seuls les fichiers figurant sur des listes d'inclusion peuvent être téléchargés, ce qui peut affecter la politique de l'organisation. La liste d'inclusion séparée par des virgules doit être modifiée pour se conformer à la politique de l'organisation en matière de types de fichiers téléchargeables acceptables.
Risque de sécurité	(Faible) Les restrictions de téléchargement de fichiers doivent être appliquées à toutes les sources d'entrée d'utilisateur non approuvées.
Références	Propriétés des paramètres de sécurité Types de contenu

Étapes à configurer

1. Accédez à la **/sys_properties_list.do**.
2. Recherchez la propriété *glide.ui.strict_customer_uploaded_content_types*.
3. Spécifiez les types de fichiers téléchargeables acceptables dans une liste séparée par des virgules, comme indiqué, puis cliquez sur **Mettre à jour**. Voici un exemple de valeur correctement formatée pour la liste *ico,gif,png,jpg,jpeg,bmp,ogg,mp3,doc,docx,xls,pdf*.

Restriction de type MIME de téléchargement (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer la vérification du type MIME pour les *glide.security.file.mime_type.validation* chargements. Vous pouvez activer (propriété sur **true**) ou désactiver (définir la propriété sur **faux**) la validation de type MIME pour les pièces jointes de fichiers.

Prérequis

Avant de définir cette propriété, définissez-la *glide.attachment.extensions* . Le type MIME est vérifié pendant *glide.attachment.extensions* le chargement uniquement pour les extensions spécifiées dans Pour plus d'informations, reportez-vous à la section Restreindre les extensions de fichiers.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.file.mime_type.validation
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer la vérification du type MIME / des octets magiques pendant les téléchargements de fichiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette remédiation active la vérification de type MIME sur les pièces jointes à l'application. Aucun impact sur la fonctionnalité, sauf s'il y a une intention malveillante dans le chargement des fichiers, car cette validation vérifie simplement la mauvaise synchronisation entre le type MIME et les données.
Risque de sécurité	(Moyen) Pour réduire les vulnérabilités telles que l'inclusion de fichiers et les téléchargements de fichiers malveillants, la vérification du type MIME doit être activée.
Références	Administration des pièces jointes

Pour plus de détails sur la configuration des propriétés de sécurisation renforcée, reportez-vous Paramètres de la sécurisation pour la sécurité de l'instance à la section .

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Sécurité des e-mails (renforcement de la sécurité de l'instance)

Cette section contient des contrôles de sécurité qu'un administrateur peut configurer pour s'assurer que des politiques de sécurité appropriées sont en place pour tous les e-mails entrants.

Convertir les e-mails entrants en HTML (renforcement de la sécurité de l'instance)

Utilisez la propriété pour spécifier si le code HTML de l'e-mail `glide.email.inbound.convert_html_inline_attachment_references` entrant doit être converti afin que les images de l'e-mail apparaissent dans l'aperçu HTML du corps de l'e-mail.

Voici ce qui se produit lorsque la propriété système `glide.email.inbound.convert_html_inline_attachment_reference` est définie sur false :

- Dans le , les Now Platformliens cid rompus (ID de contenu) apparaissent à la place des images reçues. Le format dans lequel l'image de l'e-mail s'affiche dépend du paramètre de propriété lors de la réception de l'e-mail, et non du paramètre de propriété actuel.
- Le contenu « malveillant » reçu dans la pièce jointe n'est pas référencé dans le code HTML de l'e-mail. La pièce jointe elle-même est stockée dans la table sys_attachment.
- Le traitement des e-mails entrants ne met pas à jour les données HTML de l'e-mail pour refléter l'emplacement stocké de la pièce jointe dans la table sys_attachment. Il en résulte ce qui suit :
  - Les images en ligne n'apparaissent pas dans l'affichage de l'e-mail dans le formateur d'activité.

> **Remarque :**
> Pour résoudre ce problème avec le formateur d'activité, vérifiez d'abord s'il n'existe aucun problème de sécurité. Définissez ensuite la `glide.email.inbound.convert_html_inline_attachment_reference` propriété système sur**true** pour que les futurs e-mails reçus contiennent l'URL HTML nécessaire pour référencer l'image. La modification de la propriété ne met pas à jour les e-mails déjà reçus. La nouvelle valeur affecte uniquement les e-mails entrants reçus après la modification de la propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les images intégrées ne s'affichent pas lorsque l'e-mail est affiché dans l'aperçu HTML de l'e-mail.
- Lors de l'ajout de email.body_htm dans des actions entrantes entre les balises de code, les images sont manquantes.

Prérequis

Avant de définir cette propriété, définissez-la *glide.email.read.active* sur vrai. Pour plus d'informations, consultez Activer l'utilisation de votre propre serveur POP3 .

En savoir plus

Attribut	Description
Nom de la propriété	glide.email.inbound.convert_html_inline_attachment_references
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour restreindre le rendu de l'image dans l'aperçu du corps HTML.
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Une fois cette propriété configurée, l'utilisateur ne peut pas voir l'aperçu de l'image dans le corps de l'e-mail.
Risque de sécurité	(Moyen) Si la propriété n'est pas activée, un attaquant peut envoyer une image malveillante contenant un logiciel malveillant.
Références	Propriétés d'e-mail Configuration des messages entrants

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Notation et filtrage d'e-mails indésirables (renforcement de la sécurité de l'instance)

Installez le module d'extension Email Filter (*com.glide.email_filter*) pour installer le filtrage des e-mails dans l'instance. Ce filtrage identifie les en-têtes existants, ce qui vous permet de décider de l'action à exécuter avec l'e-mail en fonction de l'en-tête associé.

Chaque message envoyé par les Now Platform serveurs de messagerie est évalué pour déterminer s'il s'agit d'un spam.

Remarque :
Si une instance utilise un serveur de messagerie privé, cette rubrique ne s'applique pas. Pour plus d'informations, consultez la section Notation et filtrage d'e-mail indésirable.

Prérequis

Avant de définir cette propriété :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définissez la propriété *glide.email.read.active* sur true. Pour plus d'informations, consultez Activer l'utilisation de votre propre serveur POP3 .
- Ce filtre remplace la *glide.pop3.ignore_headers* propriété. Pour en savoir plus, reportez-vous à la section Propriétés système disponibles .

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.email_filter
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer un filtrage afin d'éviter le spamming des e-mails.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Les e-mails ne sont jamais filtrés, bloqués ou mis en quarantaine à partir de l'instance dans le cadre de la notation de spam. Elle est uniquement notée, puis envoyée à l'instance. Tout le filtrage est effectué dans l'instance avec le module d'extension Filtres d'e-mail.
Risque de sécurité	(Moyen) Les filtres d'e-mail permettent aux administrateurs d'utiliser un générateur de conditions ou un script conditionnel pour spécifier quand ignorer les e-mails entrants malveillants provenant d'un expéditeur connu/inconnu.
Références	Filtres d'e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à la section Activate a plugin .

Restreindre l'accès aux e-mails dont la table cible est vide (renforcement de la sécurité de l'instance)

Activez la propriété pour restreindre l'accès *glide.email.email_with_no_target_visible_to_all* de l'utilisateur aux e-mails, sauf s'il en est l'expéditeur ou qu'il possède le rôle administrateur.

Les utilisateurs non autorisés peuvent accéder aux e-mails de la table E-mails [sys_email] pour lesquels il manque un enregistrement cible. Au lieu d'appliquer des ACL aux entrées d'e-mail, cette propriété restreint l'accès uniquement à l'expéditeur de l'e-mail et aux utilisateurs disposant du rôle administrateur.

Remarque :
Les e-mails envoyés et reçus par l'instance apparaissent dans la table E-mails [sys_email]. Toutefois, seuls les e-mails reçus marqués avec un état Erreur et Ignoré doivent avoir une table cible vide.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.email.email_with_no_target_visible_to_all
Type de configuration	Propriétés système [sys_properties]
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour empêcher le client de messagerie d'afficher les e-mails lorsque l'utilisateur n'autorise pas l'accès.
Valeur recommandée	faux
Impact fonctionnel	(Faible) Les utilisateurs ne peuvent plus voir les e-mails dont la table cible est vide, sauf s'ils sont administrateurs ou expéditeur de l'e-mail.
Risque de sécurité	(Moyen) Si la propriété n'est pas activée, les utilisateurs non autorisés peuvent accéder à n'importe quel e-mail dont le champ target_table est vide.
Références	Propriétés avancées d'e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les e-mails par domaine pour la création d'utilisateurs (renforcement de la sécurité de l'instance)

Utilisez cette `glide.user.trusted_domain` propriété pour spécifier la liste délimitée par des virgules des domaines de confiance utilisés dans la création des utilisateurs à partir des e-mails entrants.

Par défaut, un astérisque (*) est utilisé pour approuver tous les domaines. Des domaines spécifiques doivent être fournis s'il n'est pas nécessaire d'autoriser les e-mails provenant de tous les domaines. L'instance ignore les e-mails provenant d'autres domaines, sauf s'ils proviennent de l'adresse d'un utilisateur existant. L'instance ne crée pas d'utilisateurs invités à partir d'un e-mail provenant de domaines non approuvés.

Prérequis

Avant de définir cette propriété :

- Définissez la propriété `glide.email.read.active` sur true. Pour plus d'informations, consultez Activer l'utilisation de votre propre serveur POP3 .
- Définissez la propriété `glide.pop3readerjob.create_caller` sur true. Pour en savoir plus, consultez Activer la création automatique d'utilisateurs .

> **Remarque :**
> Ignorez la `glide.user.default_password` propriété si elle `glide.pop3readerjob.create_caller` est définie sur **false**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.user.trusted_domain
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Valeur recommandée	Liste de domaines de confiance séparés par des virgules [par exemple, servicenow.com (un nom de domaine spécifique)].
Impact fonctionnel	(Moyen) Une fois cette propriété configurée, l'instance accepte uniquement les e-mails provenant de domaines de confiance. Si vous n'incluez pas le domaine dans la liste de confiance, les comptes sont créés automatiquement et cela a un impact sur les utilisateurs invités.
Risque de sécurité	(Moyen) Si la propriété n'est pas activée, un attaquant peut utiliser une campagne d'usurpation d'adresse e-mail/de spamming pour envoyer plusieurs e-mails, ce qui entraîne la création d'utilisateurs invités plus inutiles.
Références	Propriétés d'e-mail Configuration des messages entrants

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Validation de l'entrée (renforcement de la sécurité de l'instance)

Le Now Platform effectue la validation de l'entrée pour éviter les problèmes qui résultent de la saisie de données mal formées.

Cette section décrit les Now Platform contrôles de sécurité qu'un administrateur peut configurer pour minimiser la saisie de données mal formées, quelle que soit leur source. Ces sources incluent l'entrée manuelle de l'utilisateur, ou à partir d'une infrastructure, d'entités externes ou de systèmes de bases de données.

Autoriser le code HTML incorporé (renforcement de la sécurité de l'instance)

Utilisez la propriété pour désactiver la `glide.ui.security.allow_codetag` prise en charge de l'incorporation du code HTML créé à l'aide de la balise [code].

Il Now Platform atténue de nombreuses attaques par injection et intersites en mettant en œuvre des techniques d'échappement et d'encodage. Par conséquent, les utilisateurs ne peuvent pas écrire/soumettre d'entrées au format HTML pour les champs de journal. Toutefois, les champs de journal peuvent afficher du texte contenu dans des balises de code au format HTML.

- Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur `vrai`, les utilisateurs malveillants peuvent écrire du code JS HTML nuisible qui peut être exécuté sur un autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur `faux` afin que les administrateurs puissent empêcher les champs journaux de rendre le code HTML en désactivant la prise en charge de la balise `[code]`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.security.allow_codetag
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protégez-vous contre le script de site à site et l'exécution malveillante de scripts
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Cette correction applique le codage HTML sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur. Cette propriété est définie sur `vrai` par défaut. Dans cet état, votre instance affiche le rendu HTML dans les champs de journal et les formulaires. Si cette propriété est définie sur `faux`, le HTML n'est pas affiché correctement et les balises HTML peuvent apparaître dans les champs de journal des formulaires. Cela peut avoir un impact négatif sur les fonctionnalités et sur les interactions des utilisateurs avec les données qui en résultent.
Risque de sécurité	(Moyen) La validation des entrées doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur une session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Limiter la balise CODE dans les champs de journal Afficher les entrées de champ journal au format HTML Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Autoriser les balises JavaScript dans le HTML intégré (renforcement de la sécurité de l'instance)

La *`glide.ui.security.codetag.allow_script`* propriété désactive la prise en charge de l'incorporation du code JavaScript HTML créé à l'aide de la balise [code].

Remarque :
Cette propriété est définie sur **false** par défaut dans les versions ultérieures et ne Vancouver peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client.

Il Now Platform atténue de nombreuses attaques par injection et intersites en mettant en œuvre des techniques d'échappement et d'encodage. Par conséquent, les utilisateurs ne

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

peuvent pas écrire et soumettre des entrées au format HTML pour les champs de journal. Toutefois, les champs de journal peuvent afficher le texte contenu dans des balises de code au format HTML.

- Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur **vrai**, les utilisateurs malveillants peuvent écrire du code JavaScript HTML nuisible qui peut être exécuté sur un autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur **faux** afin que les administrateurs puissent empêcher les champs journaux de rendre le code JavaScript HTML en désactivant la prise en charge de la balise `[code]`.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.security.codetag.allow_script
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protège contre le script de site à site et l'exécution malveillante de scripts
Valeur recommandée	faux
Valeur par défaut	faux
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et restitue les résultats codés à l'utilisateur. Elle peut avoir un impact sur la fonctionnalité en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes.
Risque de sécurité	(Élevé) La validation des entrées doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Limiter la balise CODE dans les champs de journal Afficher les entrées de champ journal au format HTML Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Vérifier le HTML non désinfecté (renforcement de la sécurité de l'instance)

Utilisez la propriété pour appliquer le *`com.glide.security.check_unsanitized_html`* comportement de nettoyage de translated_html champs à un niveau global pour les affectations de champs.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet de mettre en forme

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le contenu à l'aide de balises HTML (par exemple, `<p>`, , `<font><a href><b><img>`,). Pour éviter toute activité malveillante, certaines balises HTML peuvent être interdites à l'aide d'une liste de blocage. Cette propriété empêche l'utilisation de balises non autorisées dans translated_html champs de votre instance.

- Définissez cette propriété sur **appliquer** pour appliquer le comportement de nettoyage de translated_html champs.
- Définissez la propriété sur **désactiver** pour désactiver l'assainissement HTML afin d'autoriser les balises HTML bloquées sur translated_html champs.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.security.check_unsanitized_html
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Empêche l'utilisation de balises HTML non sécurisées pour se protéger contre les attaques telles que le script de site à site.
Type	Chaîne
Valeur recommandée	*`appliquer`*
Impact fonctionnel	(Moyen) Ce rattrapage applique l'assainissement HTML sur l'interface utilisateur et restitue les champs HTML traduits à l'utilisateur. Cela peut avoir un impact sur la lisibilité et la mise en forme.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur les sessions utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Assainisseur HTML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Bac à sable pour les scripts générés par le client (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer le *`glide.script.use.sandbox`* sandboxing des scripts.

Il existe deux cas dans le Now Platform qui permettent au client d'envoyer des scripts au serveur pour évaluation :

Filtres ou requêtes

Il est légal d'envoyer un filtre au serveur tel que `assigned_to=JavaScript :getMyGroups()`.

API système

L'appel d'API permet au client d'exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Si vous activez le sandboxing de script, le script évalué à l'un de ces deux points d'entrée s'exécute dans un sandbox avec des droits réduits, avec les caractéristiques suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Seules les règles métier marquées client pouvant être appelé sont disponibles dans le bac à sable.
- Seules les inclusions de script marquées Client pouvant être appelé sont disponibles dans le bac à sable.
- Certains appels d'API (en grande partie, mais pas entièrement, limités à ceux traitant d'un accès direct à la base de données) ne sont pas autorisés.
- Vous ne pouvez pas insérer, mettre à jour ou supprimer des données depuis le bac à sable. Par exemple, tous les appels à `current.update()` sont ignorés. Si vous exécutez le sans activer le Now Platform sandboxing des scripts, aucune de ces restrictions ne s'applique.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.use.sandbox
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Applique la validation pour les requêtes JavaScript côté client qui sont lancées sur la plateforme
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cette correction applique la validation pour les requêtes JavaScript côté client lancées par rapport au Now Platformfichier . Il y a un impact potentiel si le client dispose de personnalisations qui incluent des requêtes JavaScript codées en dur pour effectuer des opérations CRUD.
Risque de sécurité	(Élevé) Le Now Platform fournit une grande variété de caractéristiques et de fonctionnalités via des requêtes JavaScript. Cependant, en l'absence d'autorisation et de validation appropriées, un attaquant peut effectuer des opérations non autorisées contre la plateforme.
Références	Configuration de la propriété du bac à sable de script *`glide.script.use.sandbox`* appartient à la même famille de propriétés qui sécurisent et limitent l'exécution des scripts provenant du client : • *`glide.script.allow.ajaxevaluate`*: voir Activer AJAXEvaluate. • *`glide.script.secure.ajaxgliderecord`*: Reportez-vous à la section Activation de la vérification de l'ACL de AJAXGlideRecord.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer AJAXEvaluate (renforcement de la sécurité de l'instance)

Utilisez la propriété pour restreindre l'exécution *`glide.script.allow.ajaxevaluate`* arbitraire du script client à l'aide de l'API système côté serveur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il existe deux cas dans le Now Platform qui permettent au client d'envoyer des scripts au serveur pour évaluation :

Filtres et/ou requêtes

Il est légal d'envoyer un filtre au serveur tel que : `assigned_to=javascript :getMyGroups()`

API système

L'appel d'API AJAXEvaluate permet au client d'exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Lorsque vous définissez cette propriété sur **false**, cela Now Platform n'active pas l'utilisation de l'appel d'API AJAXEvaluate à partir du script client.

En savoir plus

Attribut	Description
Nom de la propriété	glide.script.allow.ajaxevaluate
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Restreindre l'exécution arbitraire du script client à l'aide de l'API système côté serveur
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Cette correction force la désactivation du processeur AJAEvaluate. Cela peut avoir un impact sur la fonctionnalité si vous utilisez explicitement le processeur d'évaluation AJAX dans le cadre de scripts personnalisés. Pour plus d'informations, consultez GlideAjax .
Risque de sécurité	(Élevé) AJAXEvaluate peut autoriser l'exécution de code JavaScript arbitraire sur le navigateur client en appliquant les objets côté serveur.
Références	Configuration de la propriété du bac à sable de script GlideAjax *`glide.script.allow.ajaxevaluate`* appartient à la même famille de propriétés qui sécurisent et limitent l'exécution des scripts provenant du client : • *`glide.script.use.sandbox`*: voir Bac à sable pour les scripts générés par le client. • *`glide.script.secure.ajaxgliderecord`*: Reportez-vous à la section Activation de la vérification de l'ACL de AJAXGlideRecord.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Échapper à une formule Excel (renforcement de la sécurité de l'instance)

Utilisez la propriété pour empêcher l'injection Excel, également connue sous le *glide.export.escape_formulas* nom d'injection de formule.

L'injection Excel se produit lorsque des sites Web intègrent des entrées non fiables dans des fichiers Excel. Lorsque vous utilisez un tableur tel que Microsoft Excel ou LibreOffice Call pour ouvrir un fichier, toutes les cellules commençant par +, -, = ou @ sont interprétées comme une formule. Lorsque vous définissez la propriété sur **true**, les *glide.export.escape_formulas* valeurs de chaîne commençant par +, -, = ou @ sont précédées d'une seule apostrophe lorsque vous exportez vers des fichiers CSV, XLS ou XLSX.

En savoir plus

Attribut	Description
Nom de la propriété	glide.export.escape_formulas
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour empêcher l'application contre Excel ou l'injection de formule.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Des formules malveillantes peuvent être utilisées pour détourner l'ordinateur de l'utilisateur en exploitant les vulnérabilités du logiciel de tableur.
Risque de sécurité	(Moyen) Les formules malveillantes présentent un risque même lorsque la feuille de calcul d'intégration ne contient pas d'informations sensibles, car elles peuvent être utilisées pour compromettre l'ordinateur de l'utilisateur.
Solution de contournement	Comme alternative, envisagez de supprimer tous les espaces blancs de fin dans la mesure du possible et de limiter toutes les données fournies par le client à des caractères alphanumériques.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

HTML d'échappement (renforcement de la sécurité de l'instance)

Utilisez la propriété pour forcer les *glide.ui.escape_html_list_field* caractères d'échappement HTML pour les champs HTML d'une vue de liste.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet de mettre en forme le contenu à l'aide de codes HTML (par exemple, <p>, , <font><a href><b><img>,). Un utilisateur malveillant peut injecter du code HTML dans le champ de formulaire pour exécuter des scripts indésirables sur différentes sessions client/utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définissez cette propriété sur **vrai** pour effectuer une fuite HTML avant que les enregistrements/champs ne soient affichés dans le navigateur lorsque la table apparaît en tant que vue de liste.
- S'ils sont définis sur **faux** et que vous sélectionnez cette colonne dans une vue de liste lors de l'affichage d'une liste de tables ou d'enregistrements, ces champs au format HTML peuvent apparaître.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.escape_html_list_field
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour protéger les applications contre les attaques de script de site à site
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction applique le codage HTML sur l'interface utilisateur au niveau de l'analyseur HTML, ce qui renvoie les résultats codés à l'utilisateur. Elle peut avoir un impact sur la fonctionnalité en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur les sessions utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Échapper à JavaScript (renforcement de la sécurité de l'instance)

Utilisez la propriété pour forcer l'échappement des balises JavaScript (<script></script>) dans les *glide.html.escape_script* champs HTML au cours des vues de listes.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet à l'utilisateur de formater le contenu à l'aide de codes HTML (par exemple, <p>, , <font><a href> <b><img>,). Si vous définissez *glide.html.escape_script* la valeur **sur faux**, les balises (<script></script>) peuvent apparaître lorsque vous sélectionnez cette colonne dans une vue de liste tout en affichant une liste de tables ou d'enregistrements.

Un attaquant malveillant peut insérer du code JavaScript en l'intégrant dans les balises (<script></script>). L'attaquant peut en tirer parti en injectant un vecteur JS sophistiqué qui peut s'exécuter lorsqu'un utilisateur ouvre l'enregistrement de table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.html.escape_script
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour éviter les attaques de script de site à site contre une application.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur. Elle peut avoir un impact sur la fonctionnalité, en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes
Risque de sécurité	(Élevé) La validation des entrées doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Propriétés système disponibles Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Jelly d'échappement (renforcement de la sécurité de l'instance)

Utilisez la propriété pour forcer l'échappement *`glide.ui.escape_all_script`* de tous les scripts injectés dans Jelly.

Il échappe à toutes les chaînes JS et HTML incluses dans `<j :jelly> ... </j :jelly>` avant qu'ils ne soient écrits dans le flux de sortie, ce qui empêche ainsi l'apparition de plusieurs problèmes XSS.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.escape_all_script
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Si la propriété n'est pas définie sur **true**, les développeurs doivent effectuer plusieurs étapes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	sur chaque script Jelly personnalisé pour éviter les problèmes XSS. Ces étapes incluent la localisation des variables Jelly envoyées au flux de sortie pour s'afficher sur les pages Web et l'exécution de l'échappement sur chacune des balises suivantes : $â {JS :expression} $â {HTML :expression} OU $â {JS,HTML :expression}
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction applique l'échappement de Jelly au niveau de l'analyseur. Cela peut avoir un impact fonctionnel sur l'interaction de l'utilisateur avec les données résultantes.
Risque de sécurité	(Élevé) La validation des entrées doit avoir lieu sur toutes les entrées utilisateur saisies dans l'application. Ce faisant, les attaques par injection contre la plateforme peuvent être défendues et protégées.
Solution de contournement	L'interface utilisateur peut être affectée, car certains des scripts et balises HTML conçus pour le rendu d'une page Web peuvent sembler cassés. Cette correction envoie la page codée de sortie au navigateur pour rendu. Par exemple, au lieu de « ma chaîne ici », il peut afficher « <u>ma chaîne ici</u> », car la <u> balise a été correctement échappée. Dans ce cas, pour empêcher l'échappement, ajoutez le préfixe NOESC à l'expression Jelly pour empêcher l'échappement JS. Par exemple : • Avant : ($[jvar_context_menus]) ; • Après : ($[NOESC :jvar_context_menus]) ; • Avant : $[jvar_ui_policy_scripts] • Après : $[NOESC :jvar_ui_policy_scripts]
Références	Paramètres de sécurité élevée Balises Jelly

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

XML d'échappement (renforcement de la sécurité de l'instance)

La *glide.ui.escape_text* propriété force l'échappement des valeurs XML au niveau de l'analyseur avant de les transmettre au navigateur du client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Cette propriété est définie sur **vrai** par défaut dans les versions ultérieures Vancouver et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client.

Le script de site à site se produit lorsqu'un attaquant injecte du JavaScript malveillant dans un point d'entrée. La plateforme/l'application ne parvient pas à échapper au JavaScript malveillant avant de le transmettre au navigateur de la victime pour exécution. S'échapper dans ce contexte signifie ce qui suit :

- **&** --> &
- **<** --> <
- **>** --> >
- **"** --> "
- **'** --> '
- **/** --> /

Exemple : <![CDATA[<script>alert('XSS Attack') ;]] >

Échappement : <script>alert('Attaque XSS') ; </script>

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.escape_text
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	L'échappement XML permet d'éviter que les navigateurs n'analysent le code JavaScript malveillant intégré dans les données non approuvées et ne l'exécutent pas en tant que JavaScript. • Un utilisateur malveillant peut tenter une attaque XSS pour détourner la session d'autres utilisateurs ou rediriger l'utilisateur vers un site Web malveillant. • Le Now Platform contient du code pour sécuriser les cookies, mais pour l'échapper, cette propriété doit être définie sur **vrai**.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction applique le codage XML au niveau de l'analyseur XML sur l'interface utilisateur. Il restitue les résultats codés pour l'utilisateur, ce qui peut avoir un impact sur la fonctionnalité en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Solution de contournement	Une fois cette propriété définie sur **vrai**, le rendu s'arrête sur les balises HTML dans la description de l'élément de catalogue ou dans le texte d'aide de la variable d'élément de catalogue. Il est possible que vous ne puissiez pas utiliser le formatage HTML pour certains champs. Toutefois, si la *glide.ui.escape_text* propriété est désactivée, toutes les expressions JEXL seront précédées d'un encodeur de sortie : ${JS :expression} ${HTML :expression} ou ${JS,HTML :expression}
Références	Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Assainisseur HTML (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer l'include de script HTMLSanitizer, qui nettoie l'entrée *glide.html.sanitize_all_fields* HTML selon les attributs sur liste d'exclusion et d'inclusion configurés dans un script.

Les types de champs disponibles avec le dictionnaire/les champs incluent HTML et HTML traduit. Ces champs d'entrée HTML permettent aux utilisateurs d'écrire une entrée au format HTML, par exemple :

<h1>Test</h1>), en utilisant les balises HTML les plus basiques telles que <img>, <a href ⋯ >, et <iframe>.

Cela peut ouvrir la porte à un attaquant malveillant pour injecter un vecteur malveillant avec des balises HTML telles que :

[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href=" » onclick=alert(/xss/)].

En savoir plus

Attribut	Description
Nom de la propriété	glide.html.sanitize_all_fields
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Empêche les applications contre les attaques de script de site à site et d'injection HTML
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cette correction applique un mécanisme de codage de sortie HTML avant que les données utilisateur ne soient restituées à l'utilisateur. Si le client dispose d'une personnalisation qui implique le rendu de l'attribut HTML ou des données de contenu, il y a un impact sur la fonctionnalité.
Risque de sécurité	(Élevé) L'entrée de l'utilisateur doit être traitée en toute sécurité lorsque les données sont stockées et traitées sur l'application. Cela réduit les attaques de script de site à site côté client en encodant les données en sortie.
Solution de contournement	Cette propriété nettoie tous les champs HTML du système. Si vous devez activer l'assainissement HTML sur des champs individuels, voir Activer l'assainissement sur des champs individuels. Vous pouvez également configurer la liste d'inclusion ou la liste d'exclusion pour nettoyer les balises et les attributs HTML conformément à la politique de votre organisation.
Références	Activation de l'assainisseur HTML Assainisseur HTML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Interpolation Jelly/JS (renforcement de la sécurité de l'instance)

Utilisez la `glide.ui.jelly.js_interpolation.protect` propriété pour vous assurer que tout JavaScript sur le point d'être exécuté sur une page Jelly est protégé contre l'injection à l'aide de l'interpolation Jelly.

Lorsque vous définissez la propriété sur **true**, une application passe par une arborescence de scripts Jelly (imbriquée). Il enveloppe les expressions Jelly potentiellement dangereuses d'un filtre qui :

- Échappe à leurs résultats pour être en sécurité, ou
- Si leur sécurité ne peut pas être garantie, génère une SecurityException, car l'expression qui allait être évaluée représente un problème de sécurité possible.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.jelly.js_interpolation.protect

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour atténuer les attaques d'exécution de code malveillant qui peuvent se produire à l'aide de Jelly Injection.
Valeur recommandée	Vrai
Impact fonctionnel	(Élevé) Cette propriété fait une meilleure estimation de la mise entre guillemets d'une expression. Il peut citer à tort une expression légitime. Dans ce cas, il peut être nécessaire de marquer manuellement une expression comme sûre.
Risque de sécurité	(Moyen) L'injection JEXL est une forme d'injection d'entrée unique qui peut conduire à la fois à la falsification de requêtes intersites et à l'exécution Now Platform de code. La désactivation complète de la protection peut potentiellement ouvrir de nombreuses vulnérabilités de sécurité P1.
Solution de contournement	Pour marquer manuellement une expression comme sûre, ajoutez le préfixe SAFE à l'expression Jelly : `${SAFE :sysparm_input}` ; Ajouter aveuglément SAFE à chaque expression n'est pas la bonne façon d'aborder le problème, car cela peut ouvrir une faille de sécurité. • N'ajoutez SAFE à une expression que si vous pouvez garantir que l'expression ne contient pas d'entrée du client. • Si c'est le cas, il est possible qu'un client malveillant provoque l'évaluation du JavaScript privilégié.
Références	Balises Jelly Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Sécurité stricte des requêtes SOAP (renforcement de la sécurité de l'instance)

Utilisez la propriété pour appliquer la *`glide.soap.strict_security`* sécurité des services web.

Cette propriété utilise une combinaison de :

- Contestation/réponse d'authentification de base sur le protocole HTTP et
- Contrôles d'accès au niveau du système dans le module d'extension Sécurité contextuelle : Gestion des rôles.

Si vous définissez cette propriété sur **true**, elle effectue les actions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si l'utilisateur dispose du rôle approprié pour effectuer l'opération, il vérifie la demande SOAP entrante pour obtenir l'autorisation du rôle à valider. Il se produit lors des appels/demandes de service Web SOAP effectués sur Now Platform des tables lors de l'exécution des opérations CRÉER, LIRE, METTRE À JOUR ou SUPPRE.
- Vérifie les ACL au niveau du système tout en récupérant les données sous la forme de données SOAP sur la table.
- Vérifie les ACL au niveau du champ pour toute opération CRUD effectuée sur un champ de la table.

En savoir plus

Attribut	Description
Nom de la propriété	glide.soap.strict_security
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Assurez-vous que les ACL de sécurité sont vérifiées et validées même lorsque l'accès aux enregistrements se fait via des appels SOAP
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cette correction applique le contrôle d'accès au niveau du système tout en récupérant les données des tables/pages sous la forme de données SOAP sur l'instance. Si des utilisateurs accèdent actuellement à ces données, ils sont limités/autorisés à accéder aux données en fonction des règles ACL. Pour connaître les rôles par défaut ayant accès aux données SOAP, reportez-vous à la section Rôles SOAP .
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes SOAP entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Appliquer une sécurité stricte pour le SOAP entrant SOAP Web Service

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Communications sécurisées (renforcement de la sécurité de l'instance)

Les propriétés de communication sécurisées se rapportent à la sécurité du transport du trafic HTTP.

Certificat de confiance (renforcement de la sécurité de l'instance)

Par défaut, cette `com.glide.communications.trustmanager_trust_all` propriété est définie sur **false**. Le Now Platform seul fait confiance aux certificats qu'il peut vérifier par

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

rapport au magasin de certificats JVM. Les certificats autosignés ou signés par l'entreprise ne sont pas fiables.

Remarque :
Les valeurs de ces propriétés sont Remplacement sécurisé et ne peuvent pas être modifiées une fois modifiées (elles ne sont pas réversibles). Pour des raisons de sécurité, ne modifiez pas la valeur de cette propriété. Si vous avez d'autres questions, contactez Service et assistance client.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.communications.trustmanager_trust_all
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer la validation de certificat pour les demandes sortantes.
Valeur recommandée	faux
Impact fonctionnel	(Moyen) Cette remédiation applique une validation stricte sur le champ CA (autorité de certification) de certificat. Si une entité de confiance (CA) a émis le certificat, l'instance l'accepte pour une utilisation ultérieure.
Risque de sécurité	(Moyen) Pour des raisons de confidentialité et d'intégrité, l'application doit valider l'autorité de certification du certificat avant de l'utiliser pour toute opération transactionnelle.
Références	Certificats Vérification du nom d'hôte du client HTTP

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactivation de SSLv2/SSLv3 (renforcement de la sécurité de l'instance)

Utilisez la `glide.outbound.sslv3.disabled` propriété pour forcer le MID Server à utiliser TLS lors de connexions sortantes, telles que des demandes REST et SOAP. Normalement, les connexions sortantes d'une instance sont forcées d'utiliser TLS au lieu de SSL.

En savoir plus

Attribut	Description
Nom de la propriété	glide.outbound.sslv3.disabled
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer l'utilisation de TLS if lors de toutes les connexions sortantes de l'instance ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette remédiation impose l'utilisation de la version du protocole TLS lors de la communication sur HTTPS. Si des appareils utilisés par les clients/utilisateurs de l'instance ne prennent pas en charge la communication TLS, une panne potentielle peut se produire.
Risque de sécurité	(Moyen) Il a été prouvé que les versions héritées de SSL n'étaient pas sécurisées lorsqu'elles étaient utilisées pour l'implémentation de HTTP Secure Shell, en raison d'attaques côté client, notamment BEAST et SSL.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Vérification du nom d'hôte du client HTTP

Utilisez le pour vérifier le nom d'hôte et la `com.glide.communications.httpclient.verify_hostname` chaîne de certification présentés par les hôtes SSL distants.

Définissez `com.glide.communications.httpclient.verify_hostname`**l'option sur true** pour assurer la protection contre les attaques de l'homme du milieu (MITM) dans lesquelles les communications entre deux parties sont interceptées. La définition de cette propriété remplace la `com.glide.communications.trustmanager_trust_all` propriété.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.communications.httpclient.verify_hostname`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Désactivez le processus de vérification des certifications, qui évalue toutes les certifications de la chaîne de certification en vérifiant l'état de révocation.
Type	vrai | faux
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Permet à un certificat non validé de s'y connecter en tant qu'hôte non sécurisé.
Risque de sécurité	(Moyen) Permet ou empêche le client HTTP de se connecter à un nom d'hôte potentiellement dangereux sans exception.
Références	Certificats Certificat de confiance

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vérification du certificat révoqué

Utilisez cette propriété pour désactiver le processus de vérification des certifications qui évalue toutes les certifications de la chaîne de certification en vérifiant l'état de révocation.

Les appels d'API qui utilisent le module d'extension de haute sécurité peuvent vouloir configurer cette propriété. Si la chaîne de certification complète n'est pas définie dans le magasin de confiance d'instance ou si les certificats utilisés ne sont pas compatibles avec une vérification de révocation OCSP (Online Certificate Status Protocol), des erreurs peuvent être renvoyées aux appels d'API.

La vérification de la révocation du certificat peut être désactivée en définissant la propriété `com.glide.communications.httpclient.verify_revoked_certificate` sur **faux**.

Les erreurs associées à une incapacité à effectuer la vérification sont NPE, SSLPeerUnverifiedException, CertPathValidatorException. Ces erreurs peuvent être encapsulées dans une HttpException. Plusieurs facteurs peuvent influer sur la réussite d'un contrôle :

- L'URI doit être accessible à l'instance. Notez que l'implémentation OCSP d'origine peut ne pas avoir accès à une connexion proxy.
- Le service référent OCSP doit être en ligne au moment de la vérification.

Remarque :
Les valeurs de ces propriétés sont Remplacement sécurisé et ne peuvent pas être modifiées une fois modifiées (elles ne sont pas réversibles). Si vous avez d'autres questions, contactez Service et assistance client.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.communications.httpclient.verify_revoked_certif`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Désactivez le processus de vérification des certificats, qui évalue tous les certificats de la chaîne de certificats en vérifiant l'état de révocation. Seul un certificat de serveur auto-signé doit être chargé dans le magasin de confiance d'instance.
Type	vrai | faux
Valeur par défaut	VRAI
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen)
Risque de sécurité	(Moyen) Les appels d'API utilisant le module d'extension de haute sécurité ne seront pas vérifiés à l'aide d'une vérification de révocation OCSP dans le magasin de confiance d'instance.
Références	Certificats

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Bonnes pratiques de sécurité (renforcement de la sécurité de l'instance)

En plus des configurations de sécurité, un effort manuel supplémentaire est nécessaire pour sécuriser Now Platform davantage les applications au quotidien. Cette section contient les tâches de sécurité qu'un administrateur doit effectuer périodiquement, dans un certain intervalle de temps.

Options de définition automatique du type de contenu [supprimé dans Security Center 1.3.3]

L'en-tête HTTP de réponse X-Content-Type-Options est utilisé par le serveur pour indiquer que les types MIME (Multipurpose Internet Mail Extensions) annoncés dans les en-têtes Content-Type doivent être suivis.

La configuration de cet en-tête empêchera le navigateur d'interpréter les fichiers comme un autre élément déclaré par le type de contenu dans les en-têtes HTTP. Cet en-tête peut aider à atténuer les risques de confusion MIME.

Les options de définition automatique du type de contenu seront conformes si `glide.security.header.auto_set_x_content_type_options` elles sont définies sur **vrai**.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.header.auto_set_x_content_type_options`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Empêche le navigateur d'interpréter les fichiers comme autre chose que ce qui est déclaré par le type de contenu dans les en-têtes HTTP.
Type	booléen
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cet en-tête peut aider à atténuer les risques de confusion MIME.
Risque de sécurité	(Élevé) Si cette propriété n'est pas activée, le navigateur peut mal interpréter le type de contenu dans les en-têtes HTTP.
Références	Types MIME téléchargeables

Valeur de l'en-tête HTTP du contrôle de cache (renforcement de la sécurité de l'instance)

Utilisez la `glide.http.cache_control` propriété pour définir la valeur de contrôle du cache par défaut dans les en-têtes de réponse HTTP que le Now Platform envoie lors de la demande de données de contenu statique pour une page. Les images, CSS et JavaScript rendus de l'intérieur d'une page sont des exemples de contenu statique.

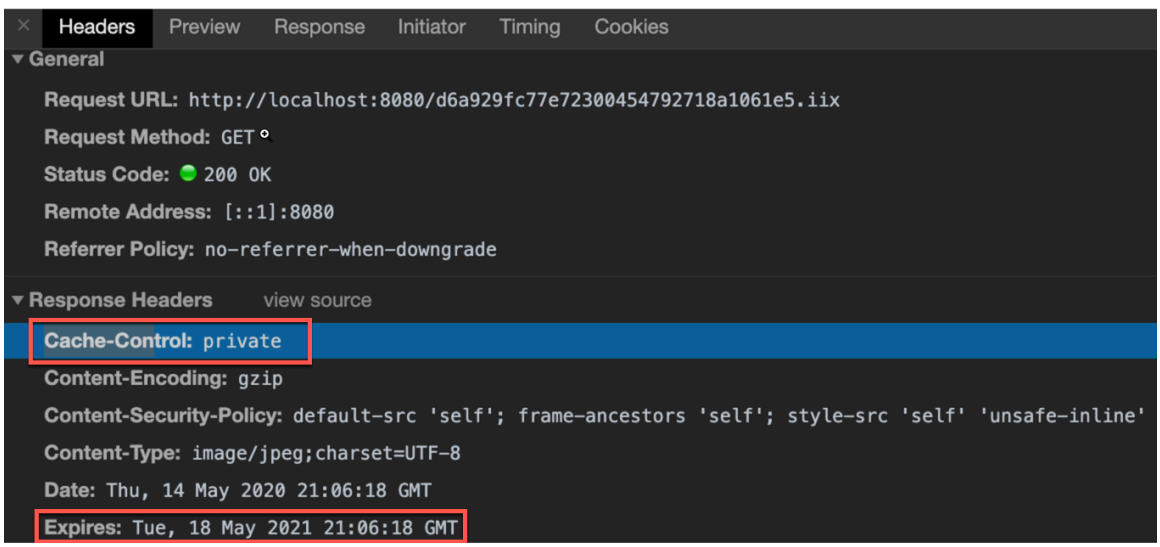
La `glide.http.cache_control` propriété définit la valeur de contrôle du cache par défaut dans les en-têtes de réponse HTTP sur **privé** ou **public**. La valeur par défaut est **public**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur	Description
privé	Le contenu statique peut être mis en cache au niveau du navigateur (client), mais pas au niveau du serveur proxy.
publique	Le contenu statique peut être mis en cache au niveau du navigateur (client), ainsi qu'au niveau du serveur proxy.

La valeur Expires (Expire) des en-têtes de réponse HTTP contrôle l'expiration du contenu statique et a une valeur par défaut de 369 jours. Pour remplacer manuellement la valeur par défaut, utilisez la `glide.http.expire.days` propriété.



Remarque :
Vous pouvez utiliser la `glide.http.cache` propriété désigner s'il faut activer ou désactiver la définition des valeurs Cache-Control et Expires dans les en-têtes de réponse HTTP. Sa valeur par défaut est **true**, ce qui vous permet de définir les éléments suivants :

- Valeur de contrôle de cache par défaut utilisant la `glide.http.cache_control` propriété.
- Expire la valeur par défaut à l'aide de la `glide.http.expire.days` propriété.

En savoir plus

Attribut	Description
Nom de la propriété	glide.http.cache_control
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour configurer la valeur de l'en-tête de réponse HTTP Cache-Control pour le contenu statique.
Valeur par défaut	publique
Valeur recommandée	privé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Moyen) Définit la valeur Cache-Control par défaut dans un en-tête de réponse HTTP.
Risque de sécurité	(Élevé) Si vous définissez cette propriété sur **public**, les instances avec CDN/proxys peuvent mettre en cache du contenu statique et s'afficher sans authentification. • **privé** est un paramètre plus approprié pour les instances avec la configuration CDN/proxy. • Si une instance n'a pas de configuration CDN/proxy, l'une ou l'autre valeur devrait convenir.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Appliquer la sécurité aux rapports

Désactivez cette propriété pour empêcher l'utilisateur de publier des rapports ou d'y accéder. Cette propriété désactive la fonctionnalité des rapports publiés dans la génération de rapports.

Activez la publication des rapports en définissant la `glide.report.published_reports.enabled`**sur vrai**.

Appliquer la sécurité aux rapports est conforme si `glide.report.published_reports.enabled` défini sur **faux**.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.report.published_reports.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Désactive la fonctionnalité des rapports publiés dans la génération de rapports.
Type	vrai | faux
Valeur recommandée	**false**
Impact fonctionnel	(Moyen) L'utilisateur ne peut pas publier de rapports.
Risque de sécurité	(Moyen) Si cette propriété n'est pas activée, les utilisateurs peuvent être en mesure d'accéder à des rapports exposant des données sensibles ou de les publier. La publication d'un rapport crée une URL que tout le monde, y compris les personnes qui ne sont pas des utilisateurs, peut utiliser pour accéder au rapport. Lorsque quelqu'un accède à l'URL, le rapport est généré avec les données actuelles de l'instance.
Références	Publier un rapport

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Module d'extension de haute sécurité (renforcement de la sécurité de l'instance)

Lorsque vous activez le module d'extension de haute sécurité, ce dernier crée ou met à jour des centaines de configurations différentes pour contrôler le niveau de sécurité de votre instance. Ces configurations atténuent la plupart des attaques OWASP les plus fréquentes en activant un contrôle d'accès strict, la validation d'entrée et l'encodage de sortie.

Ces configurations sont les suivantes :

- Contrôle d'accès
- Règles métier
- Propriétés système
- Action de politique d'interface utilisateur
- Actions des scripts
- Includes de script

Exemple

Reportez-vous aux exemples pour les propriétés suivantes :

Propriété	Rubrique
glide.ui.escape_all_script	Échapper à Jelly
glide.security.strict.actions	Vérifier l'action d'interface utilisateur avant son exécution
glide.security.csrf_previous.autoriser	Jeton anti-CSRF
glide.security.csrf.strict.validation.mode	Validation stricte du CSRF

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.high_security
Type de configuration	Définition du système > Modules d'extension : Développement
Objectif	L'activation de ce module d'extension est obligatoire. Il augmente le niveau de sécurité d'une instance, ce qui réduit la surface d'attaque en atténuant les 10 principales attaques OWASP, y compris CSRF, XSS, Sécurisation des cookies de session et les chargements de fichiers.
Valeur recommandée	Actif
Impact fonctionnel	(Élevé) Ce module d'extension active plusieurs configurations de sécurité système, qui peuvent également avoir un impact sur l'interface utilisateur et les fonctionnalités.
Risque de sécurité	(Élevé) De nombreuses configurations de sécurité sont involontairement laissées ouvertes, ce qui peut ouvrir la porte à certaines vulnérabilités critiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	Activation des paramètres de sécurité élevée Paramètres de sécurité élevée

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à la section Activate a plugin .

ID de connexion individuels (renforcement de la sécurité de l'instance)

Assurez-vous que tous les utilisateurs ont des ID d'utilisateur individuels, ce qui permet l'audit de toutes les activités utilisateur.

Remarque :
Les comptes d'utilisateurs locaux qui ne sont pas utilisés doivent avoir le marqueur **Actif** défini sur faux.

- Si vous définissez le marqueur **Actif** sur **faux** , le marqueur Verrouillé est automatiquement défini **survrai**. Si le marqueur **Verrouillé** est défini sur **vrai**, ce compte utilisateur ne peut pas s'authentifier auprès de l'instance.
- Définir le marqueur **Actif** sur **faux** ne supprime pas un utilisateur du Now Platform, mais supprime la visibilité des comptes non-administrateurs.
- Si **le marqueur Actif** est défini sur **faux** et **que le marqueur Verrouillé** est également défini sur **faux**, un utilisateur peut toujours se connecter à ce compte.

Pour en savoir plus sur les comptes d'utilisateurs, reportez-vous à la section Administration utilisateurs .

Brouillage de l'interface utilisateur mobile (renforcement de la sécurité de l'instance)

Utilisez cette `glide.ui.m.blur_ui_when_backgrounded` propriété pour griser tous les champs de l'instantané lors de l'enregistrement de l'image en processus de tâche d'arrière-plan. pour obscurcir.

Sur les appareils Android, le système d'exploitation Android prend une capture d'écran pour une utilisation dans le menu des tâches récentes lorsque l'application est envoyée en arrière-plan. Les utilisateurs peuvent également prendre des captures d'écran manuelles de l'application, qui sont stockées publiquement sur l'appareil.

Sur les appareils iOS, le système d'exploitation iOS permet également aux applications d'enregistrer un fichier image. Ce fichier représente le dernier écran vu par l'utilisateur lorsque l'application est envoyée en arrière-plan. Bien que l'objectif soit d'offrir une meilleure expérience utilisateur, cela crée également un risque de sécurité, car les images sont enregistrées sous forme de fichiers image PNG.

Remarque :
Cette configuration ou ce paramètre est basé sur l'instance. L'utilisateur doit donc se connecter à l'instance avec la propriété configurée.

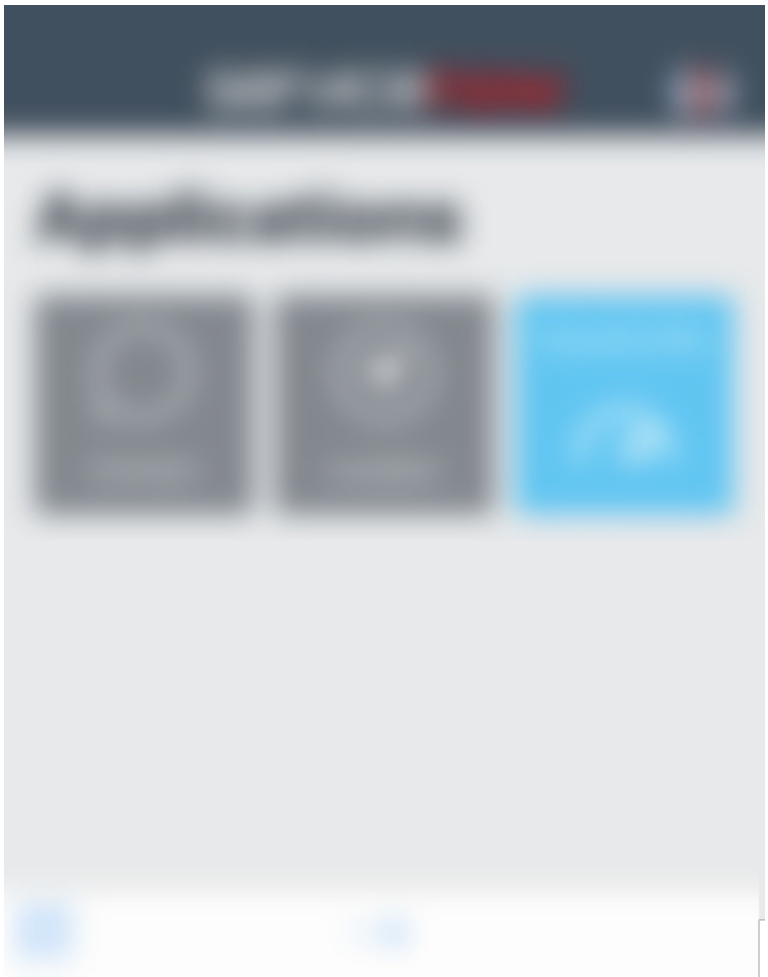
Pour masquer tous les champs de l'instantané dans l'application ServiceNow Classic, consultez Configurer l'option de floutage de l'application pour améliorer la sécurité .

Exemple

Lorsque vous définissez cette propriété sur **vrai**. L'application en arrière-plan est brouillée pour les appareils iOS et noircie pour les appareils iOS Android.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



En savoir plus

Attribut	Description
Nom de la propriété/du module d’extension	glide.ui.m.blur_ui_when_backgrounded
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurable dans le centre de sécurité de l’instance	Non
Objectif	Pour griser tous les champs de l’instantané lors de l’enregistrement de l’image pendant le processus de tâche d’arrière-plan.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Si la `glide.ui.m.blur_ui_when_backgrounded` propriété est définie sur **true**, les applications natives utilisent le paramètre défini sur le serveur pour flouter l’écran lorsque l’application entre en arrière-plan.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Il floute les captures d'écran prises par iOS et Android lorsque l'application entre en arrière-plan. • L'expérience utilisateur peut être affectée, car il ne peut pas voir le contenu lorsque l'application est envoyée en arrière-plan.
Risque de sécurité	(Moyen) Un appareil compromis (jailbreaké) permettrait à un attaquant d'avoir un accès complet au système de fichiers, avec un accès aux fichiers/instantanés contenant des informations sensibles.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Correctifs et mises à jour (renforcement de la sécurité de l'instance)

Assurez-vous que l'instance exécute le niveau de correctif le plus récent. Des correctifs de sécurité sont régulièrement publiés pour la Now Platform plupart des correctifs et correctifs d'urgence qui accompagnent les mises à jour des fonctionnalités du produit. La mise à niveau lorsque de nouveaux correctifs et correctifs d'urgence sont disponibles réduit le risque de vulnérabilités potentielles.

Il Now Platform subit en moyenne deux tests de pénétration par semaine.

- Bien que la plupart de ces tests n'aboutissent pas à des vulnérabilités significatives, des vulnérabilités sont détectées et corrigées régulièrement.
- Vous trouverez des informations sur Now Platform les versions, les correctifs et les correctifs d'urgence dans la section Notes de version de la documentation produit. Pour plus d'informations, consultez les notes de version des mises à niveau .

Supprimer les données de démonstration (renforcement de la sécurité de l'instance)

Les données de démonstration, en particulier les comptes de démonstration, sont généralement incluses lors de la création d'une instance. Si tel est le cas, toutes les données de démonstration doivent être supprimées avant d'utiliser l'instance en non-production ou en production.

Ouvrez une demande dans HI. Assurez-vous de créer un compte administratif avant de soumettre la demande.

Il est fortement recommandé que la suppression des données de démonstration en production soit vérifiée avec succès sur une instance de sous-production qui est un clone récent de l'instance de production.

Ressources internes

https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107

https://community.servicenow.com/community?id=community_blog&sys_id=786eaeaddbd0dbc01dcaf3231f961959

Suppression des données de démonstration à l'aide de Catalogue de services

Au lieu d'envoyer la demande comme un incident, certains utilisateurs peuvent demander la suppression des données de démonstration sur une instance à l'aide de Catalogue de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

services. Il s'agit notamment des utilisateurs internes et des utilisateurs disposant des rôles customer_admin ou partner_admin.

1. Accédez à https://support.servicenow.com/now .
2. Spécifiez l'instance à partir de laquelle supprimer les données de démonstration.

   Si vous rencontrez des difficultés pour trouver votre instance, faites précéder le nom de l'instance d'un * pour lancer une requête contained.
3. Cliquer sur **Libre-service** > **Supprimer les données de démonstration** > **.**
4. Spécifiez la date et l'heure de suppression des données de démonstration de l'instance sélectionnée.

   La date et l'heure doivent être postérieures d'au moins quatre heures à l'heure actuelle.
5. Cliquez sur **Envoyer**.

Une nouvelle demande de changement est créée et s'affiche automatiquement. La **date de fin prévue** est automatiquement calculée sur la base de la **date de début prévue** augmentée de cinq heures, ce qui correspond à la durée du processus. Dans la demande de changement. Utilisez la liste de surveillance pour ajouter tous les autres membres de votre équipe qui doivent être au courant de l'état de la demande de changement.

Liste d'inclusion de sécurité (renforcement de la sécurité de l'instance)

Un modèle de sécurité « positif » (également connu sous le nom de « liste d'inclusion ») est un modèle qui définit ce qui est autorisé et rejette tout le reste. Cette section contient des contrôles de sécurité qu'un administrateur peut configurer pour restreindre le comportement aux listes d'inclusion connues.

Remarque :
Les propriétés de la liste d'inclusion de sécurité doivent être configurées manuellement dans chaque instance, car les ensembles de mises à jour ne promouvront pas la configuration et renverront une erreur.

Vérifier les appels des membres de la liste d'autorisation (renforcement de la sécurité de l'instance)

Examinez et supprimez les entrées d'appel de membre de la liste d'inclusion au besoin de la table sys_whitelist_member.

Les entrées d'appel de membres ont accès aux ressources Java du côté serveur afin de réaliser des opérations basées sur les applications sans la validation appropriée. Étant donné que cela peut entraîner des divulgations ou des altérations non autorisées de données des clients, il s'agit d'un grave problème de sécurité.

En savoir plus

Attribut	Description
Nom de la table	sys_whitelist_member **Remarque :** Dans les versions récentes, seuls les employés ServiceNow peuvent accéder à cette table. Même les administrateurs ne sont pas en mesure de le faire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Table
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour examiner et supprimer des entrées de cette table.
Valeur recommandée	Aucun enregistrement ne doit exister dans la table (la liste doit être vide).
Impact fonctionnel	(Faible) Il ne devrait y avoir aucun impact tant que vous examinez et approuvez les résultats générés lors de l'exécution de l'outil de suppression des appels de packages. Pour garantir le bon fonctionnement de l'instance, testez les changements dans un environnement de non-production avant le déploiement dans l'environnement de production. Pour en savoir plus, reportez-vous à la section Outil de suppression des appels de packages.
Risque de sécurité	Les appels d'API côté client (élevés) qui entraînent la récupération de données ou l'accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Validez ces éléments pour l'autorisation et la restriction de l'accès aux objets sensibles.

Étapes à configurer

Remarque :
Les étapes suivantes sont similaires aux étapes décrites dans les sections Étapes de configuration de :

- Outil de suppression d'appel de packages
- Vérifier les appels de packages de la liste d'autorisation

Si vous les avez déjà effectuées, vous pouvez ignorer ces étapes.

1. Activez le module d'extension Packages Call Removal Tool. Pour en savoir plus, reportez-vous à la section Outil de suppression des appels de packages.
2. À l'aide du navigateur de filtre, accédez à **l'utilitaire de suppression des appels de packages**.
3. Cliquez sur chaque script en commençant par (1) à (4). Attendez la sortie, puis passez à la suivante.
4. Une fois que vous avez exécuté le script (4), une liste des champs affectés s'affiche sur la page Éléments d'appels de packages.
5. Résolvez tous les éléments des sections Proposé et Erreur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Cet outil peut signaler certains appels de package utilisés dans `sa_mapping_ext_commands` et `sa_custom_operation`. Ces appels de package appartiennent au Serveur MID. Comme il n'y a pas de classes, le code s'exécute dans Serveur MID. Si vous trouvez les appels de membres suivants dans la section Erreurs, marquez-les comme **rejetés** (ignorés). L'outil ne signale plus cet appel de membre.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content)` ;
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name)` ;
- `Packages.com.snc.sw.commands.HttpCallHandler` ;
- `Packages.com.snc.sw.dto.ProviderType.SSH`

6. Contactez ServiceNow le support pour un rattrapage supplémentaire.

Vérifier les appels de packages de liste d'autorisation (renforcement de la sécurité de l'instance)

Examinez et supprimez les entrées d'appel de package de liste d'inclusion au besoin de la table sys_whitelist_package.

Les entrées d'appel en paquet ont accès aux ressources Java du côté serveur afin de réaliser des opérations basées sur les applications sans la validation appropriée. Étant donné que cela peut entraîner des divulgations ou des altérations non autorisées de données des clients, il s'agit d'un grave problème de sécurité.

En savoir plus

Attribut	Description
Nom de la table	sys_whitelist_package **Remarque :** Dans les versions récentes, seul Service et assistance client l'accès à cette table est possible, même les administrateurs ne sont pas en mesure de le faire.
Type de configuration	Table
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour examiner et supprimer des entrées de cette table.
Valeur recommandée	Aucun enregistrement ne doit exister dans la table (la liste doit être vide).
Impact fonctionnel	(Faible) Il ne devrait pas y avoir d'impact tant que les résultats de l'exécution de l'outil de suppression des appels de packages sont examinés et approuvés. Pour garantir le bon fonctionnement de l'instance, testez les changements dans un environnement de non-production avant le déploiement dans l'environnement de production. Pour en savoir plus, consultez Outil de suppression d'appel de packages.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	Les appels d'API côté client (élevés) qui entraînent la récupération de données ou l'accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Validez ces éléments pour l'autorisation et la restriction de l'accès aux objets sensibles.
Solution de contournement	Contactez ServiceNow le support pour obtenir de l'aide.

Étapes à configurer

1. Activez le module d'extension Packages Call Removal Tool. Pour en savoir plus, reportez-vous à la section Outil de suppression des appels de packages.
2. À l'aide du navigateur de filtre, accédez à **l'utilitaire de suppression des appels de packages**.
3. Cliquez sur chaque script en commençant par (1) à (4). Attendez la sortie, puis passez à la suivante.
4. Une fois que vous avez exécuté le script (4), une liste des champs affectés s'affiche sur la page Éléments d'appels de packages.
5. Résolvez tous les éléments des sections Proposé et Erreur.

   Remarque :
   Cet outil peut signaler certains appels de package utilisés dans `sa_mapping_ext_commands` et `sa_custom_operation`. Ces appels de package appartiennent au Serveur MID. Comme il n'y a pas de classes, le code s'exécute dans Serveur MID. Si vous trouvez les appels de packages suivants dans la section Erreurs, marquez-les comme **Rejeté** (Ignoré). L'outil ne signale plus cet appel de package.

   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content)` ;
   - `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name)` ;
   - `Packages.com.snc.sw.commands.HttpCallHandler` ;
   - `Packages.com.snc.sw.dto.ProviderType.SSH`

6. Contactez ServiceNow le support pour un rattrapage supplémentaire.

Activer la liste d'autorisation d'URL pour la communication cross-origin entre iFrame (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer la *`glide.ui.concourse.onmessage_enforce_same_origin`* communication d'origine croisée entre les iframes.

OpenFrame ne peut traiter que les messages provenant de domaines de confiance spécifiés dans la *`glide.ui.concourse.onmessage_enforce_same_origin_whitelist`* propriété. Pour plus d'informations, consultez Spécifier la liste d'autorisation UTL pour la communication cross-origin entre iframes.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.concourse.onmessage_enforce_same_origin
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Activer l'inclusion de domaines de confiance, afin qu'ils puissent communiquer entre iframes pour openframe.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Si vous n'incluez pas les domaines prévus, la possibilité d'intégrer d'autres pages dans Now Platform les instances peut être limitée.
Risque de sécurité	(Élevé) Si une page Web contient des gestionnaires d'événements qui n'effectuent pas une validation d'origine appropriée, une page Web, ou un script de n'importe quelle origine, peut communiquer avec elle. Il peut également lancer n'importe quelle fonctionnalité exécutée par le gestionnaire d'événements.
Références	Vue d'ensemble d'OpenFrame

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Renforcer les liens relatifs (renforcement de la sécurité de l'instance)

Utilisez la propriété pour appliquer des *glide.cms.catalog_uri_relative* liens relatifs à partir du paramètre URI on /ess/catalog.do.

- Lorsque la valeur est définie sur **true**, seules les URL relatives sont autorisées via la page /ess/catalog.do à l'aide du *uri* paramètre.
- Lorsqu'elle est définie sur **faux**, toutes les URL sont autorisées, ce qui permet la liaison à un contenu externe non autorisé.

En savoir plus

Attribut	Description
Nom de la propriété	glide.cms.catalog_uri_relative
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour limiter les tentatives de lier un contenu externe non autorisé.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette correction applique la validation sur la page du catalogue de sorte que seules les URL relatives sont autorisées. Les liens existants vers des applications Web externes sont rompus.
Risque de sécurité	(Élevé) Les URL absolues peuvent présenter un risque de sécurité lorsqu'elles sont utilisées dans un paramètre ou une valeur de champ, redirigeant ainsi la page source vers un site Web contrôlé par un adversaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Outil de suppression d'appel de packages (renforcement de la sécurité de l'instance)

Activez et exécutez le module d'extension Packages Call Removal Tool (`com.glide.script.packages_call_removal`), puis décidez si chaque changement proposé doit être appliqué ou rejeté.

L'outil de suppression des appels de packages est un plugin qui :

- Analyse les scripts à la recherche d'appels de packages aux Now Platform classes Java.
- Propose des changements pour les remplacer par les noms GlideScriptable préférés.
- Facilite les changements de script.

Remarque :
S'il s'agit d'un enregistrement de système de base, l'utilisation de la recommandation de l'outil entraîne le marquage de l'élément comme customer_update. Il est possible que ce script ne prenne pas l'objet d'autres mises à jour à l'avenir. Dans les versions ultérieures, les tables sys_whtelist_xxx sont censées être vides. Cependant, il peut toujours être utile d'utiliser cet outil car il signale les appels Packages, xxx.

L'outil de suppression des appels de packages peut signaler certains appels de packages utilisés dans `sa_mapping_ext_commands` et `sa_custom_operation`. Ces appels de package appartiennent au Serveur MID. Comme il n'y a pas de classes, le code s'exécute dans Serveur MID. Si vous trouvez l'un des appels de package répertoriés suivants dans la section Erreurs, marquez-le comme Rejeté (ignoré). L'outil ne signale plus cet appel de package.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content)` ;
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name)` ;
- `Packages.com.snc.sw.commands.HttpCallHandler` ;
- `Packages.com.snc.sw.dto.ProviderType.SSH`

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.script.packages_call_removal
Type de configuration	Définition du système > Modules d'extension
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour supprimer/remplacer les appels de package/membre non autorisés par des noms Glide acceptables (GlideScriptable) qui n'autorisent qu'un accès autorisé aux données.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Cette remédiation remplacerait les appels de package par des API `GlideScriptable` et peut affecter les personnalisations qui incluent des appels de package. L'outil ne remplace pas automatiquement les appels de packages. Au lieu de cela, il fournit des suggestions qui sont stockées dans la table packages_call_item. Votre administrateur peut alors décider d'accepter ou de rejeter le changement proposé.

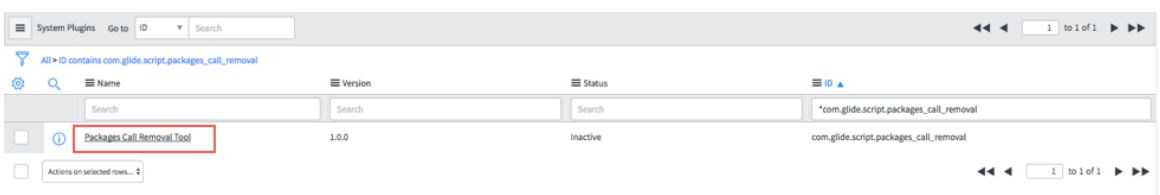
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

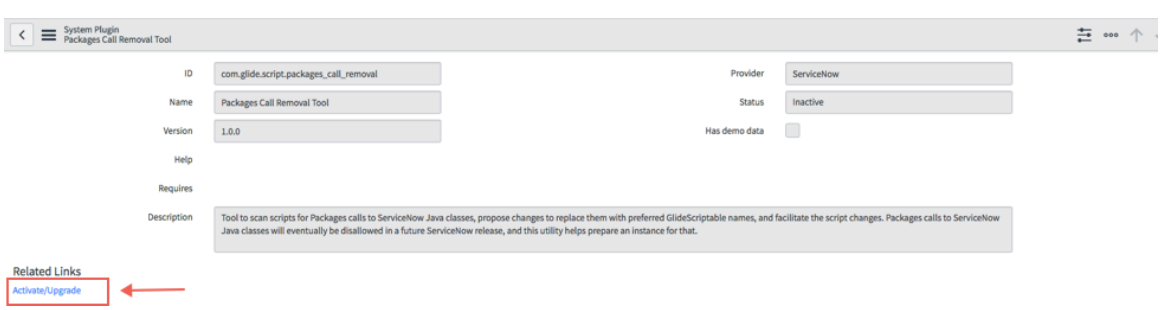
Attribut	Description
Risque de sécurité	(Moyen) Les appels d'API côté client qui entraînent la récupération de données ou l'accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Ils doivent être validés pour l'autorisation et la restriction de l'accès aux objets sensibles.

Étapes à configurer

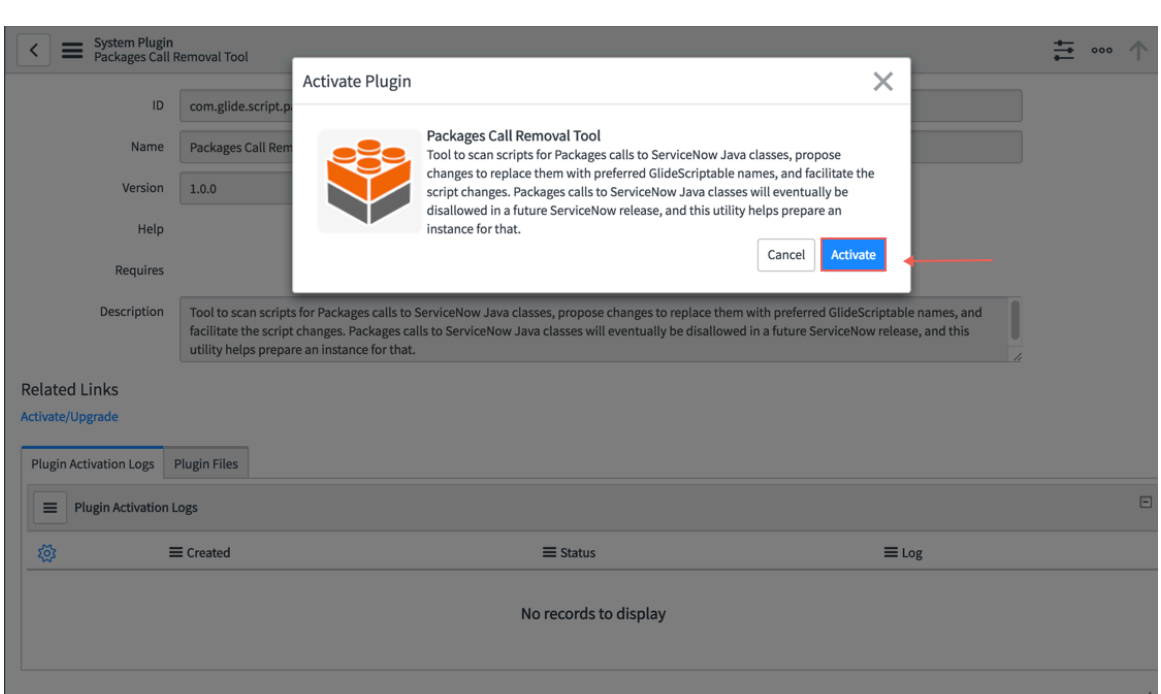
1. Accédez à la **Définition du système** > **Modules d'extension**



2. Recherchez l'ID du module d'extension = `com.glide.script.packages_call_removal`.



3. Cliquez sur **Activer/Mettre à niveau** pour activer le module d'extension.



4. Pour vérifier les appels de packages de liste d'inclusion et les appels de membres de listes d'inclusion, effectuez les actions décrites dans les sections Étapes de configuration des rubriques suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifier les appels des membres de la liste d'autorisation
- Vérifier les appels de packages de la liste d'autorisation

Spécifier la liste d'autorisation d'URL pour la communication cross-origin entre iFrame (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer la `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` communication d'origine croisée entre les iframes à partir de domaines de confiance que vous spécifiez dans une liste d'inclusion.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.concourse.onmessage_enforce_same_origin_whitelist
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Activer la liste d'inclusion des domaines de confiance, afin qu'ils puissent communiquer entre les iframes pour openframe.
Besoin	Obligatoire
Impact fonctionnel	(Moyen) Si vous ne mettez pas sur liste d'inclusion les domaines prévus, la possibilité d'intégrer d'autres pages dans les Now Platform instances peut être limitée.
Risque de sécurité	(Élevé) Si une page Web contient des gestionnaires d'événements qui n'effectuent pas une validation d'origine appropriée, une page Web, ou un script de n'importe quelle origine, peut communiquer avec elle. Il peut également lancer n'importe quelle fonctionnalité exécutée par le gestionnaire d'événements. La communication avec des iframes d'autres domaines constitue un risque pour la sécurité.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Liste d'autorisation d'URL pour les redirections de déconnexion (renforcement de la sécurité de l'instance)

Utilisez la `glide.security.url.whitelist` propriété pour ajouter une validation supplémentaire afin d'assurer que toute URL externe introduite doit faire partie des URL sur liste d'inclusion.

La redirection ouverte se produit lorsqu'une page Web vulnérable est redirigée vers une page malveillante et non approuvée qui peut compromettre l'utilisateur. Les attaques par redirection ouverte s'accompagnent d'une attaque de hameçonnage, car le lien vulnérable modifié est identique au site d'origine, ce qui augmente les chances de réussite de l'attaque de hameçonnage.

Cette propriété est applicable dans les cas suivants :

- /logout.do ?sysparm_goto_url={URL externe}
- /cms_login_redirect.do ?sysparm_goto_url={URL externe}

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après s'être déconnectés de l'instance, les utilisateurs sont dirigés vers un site de confiance externe :

- `/logout_redirect.do ?sysparm_url={URL externe}`
- `/saml_redirector.do ?sysparm_uri={URL externe}`

Lorsque SAML est activé, il invoque une URL de déconnexion du fournisseur d'identité (IdP).

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.url.whitelist
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour implémenter une redirection d'URL sécurisée lors de la connexion, de la déconnexion ou d'autres redirections. Cette propriété atténue l'une des 10 principales attaques de l'OWASP appelée Redirections et transferts invalidés.
Type	Chaîne séparée par des virgules et des espaces. Exemple : https://example.com, https://wiki.example.com.
Valeur	Les URL approuvées de votre organisation [certains FQDN (nom de domaine pleinement qualifié) définis, par exemple http://www.servicenow.com]
Impact fonctionnel	(Moyen) Cette correction applique la validation sur la page de déconnexion. Cela peut avoir un impact fonctionnel sur un utilisateur d'une instance avec une configuration SSO/SAML.
Risque de sécurité	(Élevé) La redirection ouverte côté client peut permettre à l'attaquant de rediriger les victimes/utilisateurs vers un site Web contrôlé par l'attaquant et est considérée comme un risque de sécurité.
Références	Erreurs et correctifs de l'authentification unique (SAML 2.0)

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Politique de sécurité du contenu du client intégré d'Agent virtuel (renforcement de la sécurité de l'instance)

Utilisez cette *`com.glide.cs.embed.csp_frame_ancestors`* propriété pour activer la configuration de la stratégie frame-ancestors uniquement pour la page `https://<votre-instance>.service-now.com/sn_va_web_client_app_embed.do` .

Le module d'extension Agent virtuel permet d'intégrer un client dans une page Web externe. Pour permettre l'intégration de la page client dans la page Web, la politique de sécurité du contenu doit autoriser la page externe en tant que cadre parent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Évitez d'utiliser uniquement « * » comme politique de sécurité du contenu, car cela activerait tous les domaines et rendrait l'application potentiellement vulnérable au détournement de clic.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.cs.embed.csp_frame_ancestors
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour activer la création d'une politique de sécurité du contenu personnalisée pour la page Agent virtuel intégrable.
Valeur recommandée	Définir sur les domaines approuvés
Impact fonctionnel	(Élevé) Le client incorporable d'Agent virtuel ne s'autorise pas à être incorporé dans des sites externes, sauf si la politique de sécurité du contenu est correctement configurée.
Risque de sécurité	(Moyen) Si elle n'est pas configurée correctement (en autorisant tous les cadres parents), elle peut éventuellement rendre la page client intégrable vulnérable au détournement de clic.
Références	Incorporer le client Web de l'Agent virtuel dans une page Web externe Pour en savoir plus sur la création d'une politique de sécurité du contenu frame-ancestors, cliquez ici.

Étapes à configurer

1. Accédez à la **/sys_properties_list.do**.
2. Recherchez la propriété *com.glide.cs.embed.csp_frame_ancestors*.
3. Attribuez une politique de sécurité de contenu acceptable (n'autorisez que l'entreprise ou d'autres domaines acceptés), puis cliquez sur **Mettre à jour**.

X-Frame-Options du client intégré Virtual Agent (renforcement de la sécurité de l'instance)

Utilisez cette *com.glide.cs.embed.xframe_options* propriété pour activer la configuration de l'en-tête X-Frame uniquement pour la page https://<votre-instance>.service-now.com/sn_va_web_client_app_embed.do .

Le module d'extension Agent virtuel permet d'intégrer un client dans une page Web externe. Pour permettre l'intégration de la page client dans la page Web, l'en-tête X-Frame-Options doit permettre d'inclure l'iframe dans le cadre parent.

Remarque :
Évitez d'utiliser allow-from* comme valeur d'en-tête X-Frame-Options, car cela activerait tous les domaines et rendrait l'application potentiellement vulnérable au détournement de clic.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	com.glide.cs.embed.xframe_options
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Pour activer la spécification de la directive pour l'en-tête X-Frame-Options pour la page Agent virtuel intégrable.
Valeur recommandée	SameOrigin
Impact fonctionnel	(Élevé) Le client incorporable d'Agent virtuel ne s'autorise pas à être incorporé dans des sites externes, sauf si l'en-tête X-Frame-Options est correctement configuré.
Risque de sécurité	(Moyen) Si elle n'est pas configurée correctement (en autorisant tous les cadres parents), elle peut éventuellement rendre la page client intégrable vulnérable au détournement de clic.
Références	Incorporer le client Web de l'Agent virtuel dans une page Web externe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

X-Frame-Options : SAMEORIGIN (renforcement de la sécurité de l'instance)

Utilisez la propriété pour définir l'en-tête de réponse X-Frame-Options sur SAMEORIGIN pour toutes les pages de l'interface `glide.set_x_frame_options` utilisateur.

Utilisez l'en-tête de réponse HTTP X-Frame-Options pour indiquer si le navigateur doit être autorisé à rendre une page dans un <frame> ou <iframe>. Les sites peuvent utiliser cette fonction pour éviter les attaques de détournement de clic en s'assurant que leur contenu n'est pas intégré dans d'autres sites. Un attaquant pourrait intégrer votre page dans sa propre page et faire en sorte que vos éléments de page fonctionnent de manière malveillante. L'utilisateur final peut penser que la page est légitime parce qu'elle ressemble à votre page. L'utilisateur final peut cliquer sur les éléments comme d'habitude uniquement pour exécuter des scripts ou des éléments malveillants.

En savoir plus

Attribut	Description
Nom de la propriété	glide.set_x_frame_options
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour atténuer les attaques de ClickJacking.
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Faible) Cette correction applique la restriction d'affichage d'une Now Platform application dans une application tierce sous la forme d'un iFrame. Si vous disposez d'une telle intégration, l'application ne s'affichera pas dans l'application tierce personnalisée.
Risque de sécurité	(Moyen) La stratégie Même origine vous permet d'empêcher un domaine de récupérer un script ou une ressource d'un autre domaine. Tous les navigateurs modernes prennent en charge cette fonctionnalité. La politique valide la connexion en fonction du protocole, du port et de l'hôte. CORS (Cross Origin Request) est une modification de la stratégie de même origine qui permet l'accès à des ressources/ scripts d'un autre domaine lorsqu'il est explicitement indiqué dans le cadre de la valeur de l'en-tête. • Dans ce cas, **l'en-tête X-Frame-Options** contrôle si l'application Now Platform peut être rendue sur le site Web tiers. • Cela réduit l'exposition sensible, car la valeur de la propriété, lorsqu'elle est définie sur **SAMEORIGIN** , ne permet pas au rendu de se produire.
Références	Propriétés système disponibles Configurer les iFrames

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Validation du traitement par une entité externe XML

Ces propriétés permettent l'expansion des entités et restreignent toute entité externe (par exemple, l'URL) lorsqu'elles sont incluses dans une référence XML DOCTYPE. DTD est essentiellement un schéma XML. Si vous recherchez une solution pour les déclarations d'entité qui pourraient avoir un potentiel pour XXE (entité externe), activez une défense sur liste d'inclusion contre XXE à l'aide des propriétés système.

Pour l'analyse XMLDocument et XMLUtil

Si vos personnalisations utilisent `XMLDocument` ou `XMLUtil`, définissez les propriétés système suivantes. Ils contrôlent l'expansion des entités et activent la validation des entités externes, ce qui permet de traiter uniquement celles figurant sur les listes d'inclusion.

Définition du seuil d'expansion de l'entité (renforcement de la sécurité de l'instance)

Utilisez la propriété pour réduire la limite maximale d'expansion de l'entité *`glide.xmlutil.max_entity_expansion`* .

Le Now Platform ne traite pas d'autres expansions d'entité supérieures à la limite autorisée spécifiée dans cette propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
3000 est le minimum par défaut imposé par le Now Platform, qui est considéré comme un seuil de sécurité. Par conséquent, la plateforme considère ce minimum par défaut si la valeur entière que vous saisissez est inférieure à 3000.

En savoir plus

Attribut	Description
Nom de la propriété	glide.xmlutil.max_entité_expansion
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques d'expansion d'entité XML/de milliards de rires.
Valeur recommandée	3000
Impact fonctionnel	(Faible) Si la personnalisation utilise une extension d'entités volumineuses, le peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Élevé) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Validation des entités XMLdoc/XMLUtil avec liste d'autorisation (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer la validation d'une entité externe et n'autorise `glide.xml.entity.whitelist.enabled` que le traitement de celles qui figurent sur liste d'inclusion.

- Si vous définissez cette propriété sur **vrai**, elle autorise uniquement le traitement des entités sur liste d'inclusion (paramètre recommandé).
- Si vous définissez cette propriété sur **faux**, elle autorise le traitement de toutes les entités externes.

Prérequis

Avant de définir cette propriété, définissez une liste de noms de domaine complets délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL atteignables à l'aide du processus XML Entity. propriété. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.xml.entity.whitelist.enabled`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques XXE.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Si la personnalisation utilise une entité externe, et non une inclusion répertoriée dans la `glide.xml.entity.whitelist` propriété, le Now Platform traitement ultérieur peut bloquer. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.
Risque de sécurité	(Élevé) Un attaquant peut utiliser la DTD pour inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela pourrait conduire à d'autres attaques en utilisant la relation de confiance du serveur avec d'autres entités.
Solution de contournement	Si vous n'utilisez pas l'expansion d'entité externe, désactivez-la. Pour en savoir plus, consultez Désactiver l'expansion des entités.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Pour les analyseurs XMLDocument2

Si vos personnalisations utilisent un analyseur XMLDocument2, utilisez les propriétés système suivantes pour activer la validation d'une entité externe.

Désactiver l'expansion des entités (renforcement de la sécurité de l'instance)

Si les personnalisations ne nécessitent pas d'expansion d'entité, utilisez la propriété pour désactiver complètement l'expansion d'entité `glide.stax.allow_entity_resolution` externe. Le XML termine l'analyse mais n'inclut aucune entité interne ou externe.

- Si vous définissez cette propriété sur **vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, sous réserve de la définition de la `glide.stax.whitelist_enabled` propriété.
- Si vous définissez cette propriété sur **false**, toute la résolution et l'expansion de l'entité sont bloquées. Pour en savoir plus, consultez Validation d'entité XMLdoc2 avec liste d'autorisation.

Prérequis

Avant de définir cette propriété :

- Définissez les `glide.xml.entity.whitelist.enabled` propriétés and `glide.stax.whitelist_enabled` sur true. Pour en savoir plus, consultez Validation des entités XMLdoc/XMLUtil avec liste d'autorisation et Validation d'entité XMLdoc2 avec liste d'autorisation.
- Définissez une liste de FQDN délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, car il s'agit des seules URL atteignables à l'aide du processus XML Entity. propriété. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	glide.stax.allow_entity_resolution
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre une attaque par expansion d'entité XML/Billion Laugh.
Valeur recommandée	faux
Impact fonctionnel	(Faible) Si la personnalisation utilise l'expansion des entités, le peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Élevé) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.
Solution de contournement	Si la personnalisation nécessite une expansion de l'entité, définissez cette propriété sur vrai et suivez les étapes documentées à la rubrique Validation d'entité XMLdoc2 avec liste d'autorisation.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Pour plus d'informations sur les ressources OWASp, consultez OWASp .

Validation d'entité XMLdoc2 avec liste d'autorisation (renforcement de la sécurité de l'instance)

Utilisez une propriété pour permettre le traitement, à l'aide de XMLDocument2, des entités externes apparaissant dans une liste d'inclusion.

Prérequis

Avant de définir cette propriété :

- Définissez la propriété `glide.xml.entity.whitelist.enabled` sur true. Pour en savoir plus, consultez Validation des entités XMLdoc/XMLUtil avec liste d'autorisation.
- Définissez une liste de noms de domaine complets délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, qui sont les seules URL atteignables à l'aide du processus XML Entity. propriété. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

En savoir plus

Attribut	Description
Nom de la propriété	glide.stax.whitelist_enabled
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques d'entités externes XML.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Si la personnalisation utilise une entité externe qui ne figure pas sur la liste d'inclusion, le peut bloquer la poursuite du Now Platform traitement. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.
Risque de sécurité	(Élevé) Un attaquant peut utiliser la DTD peut inclure des requêtes HTTP arbitraires que le serveur peut exécuter. En utilisant la relation de confiance du serveur avec d'autres entités, cela pourrait conduire à d'autres attaques.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traitement d'entité externe XML : liste d'autorisation (renforcement de la sécurité de l'instance)

Utilisez la `glide.xml.entity.whitelist` propriété pour permettre l'accès à une liste de FQDN délimités par des virgules, si nécessaire. Ces URL sont les seules qui peuvent être atteintes à l'aide du traitement d'entité XML.

Prérequis

Avant de définir cette propriété, définissez la `glide.xml.entity.whitelist.enabled` propriété, ce qui active la validation d'une entité externe et autorise uniquement le traitement de la liste d'inclusion que vous spécifiez dans la `glide.xml.entity.whitelist` propriété. Pour en savoir plus, consultez Validation des entités XMLdoc/XMLUtil avec liste d'autorisation.

En savoir plus

Attribut	Description
Nom de la propriété	glide.xml.entité.liste blanche
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour créer une liste d'inclusion des URL auxquelles le traitement d'entité XML peut accéder.
Valeur recommandée	Spécifié par l'utilisateur (par exemple, https://google.com)
Impact fonctionnel	(Faible) Le traitement d'entité externe peut être bloqué s'il n'est pas mentionné dans la liste d'inclusion. Lorsque la liste d'inclusion est activée, elle nécessite le formulaire PUBLIC d'une définition d'entité externe.
Risque de sécurité	(Élevé) Un attaquant peut utiliser la DTD peut inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	pourrait conduire à d'autres attaques utilisant la relation de confiance du serveur avec d'autres entités

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Gestion des sessions (renforcement de la sécurité de l'instance)

La gestion des sessions permet d'identifier correctement le trafic qui appartient à un utilisateur spécifique. Prenez des précautions pour vous assurer qu'il n'y a pas d'abus de la relation de confiance.

Les applications Web peuvent créer des sessions pour suivre les utilisateurs anonymes après la première demande de l'utilisateur. Par exemple, le maintien de la préférence de langue de l'utilisateur, en veillant à ce que :

- Identification de l'utilisateur sur toutes les demandes ultérieures.
- Application des contrôles d'accès de sécurité.
- Autorisation d'accès aux données privées de l'utilisateur.
- Augmentation de l'ergonomie de l'application.

Par conséquent, les applications Web actuelles peuvent fournir des options de session avant et après authentification.

Authentification et gestion des sessions

L'authentification est le processus qui consiste à vérifier qu'une personne, une entité ou un site Web est bien celui qu'il prétend être.

L'authentification tente de vérifier l'identité numérique de l'expéditeur d'une communication. Tester le schéma d'authentification signifie comprendre comment fonctionne le processus d'authentification et utiliser ces informations pour contourner le mécanisme d'authentification. Un exemple courant est le processus de connexion. L'authentification a lieu après la soumission d'un nom d'utilisateur, d'un ID d'utilisateur et d'un ou plusieurs éléments d'informations privées que seul l'utilisateur connaîtrait.

La gestion des sessions comprend des propriétés liées à la sécurité qu'un administrateur peut configurer pour assurer que des mécanismes de gestion de session sécurisée sont établis dans le Now Platformfichier .

Délai absolu de la session (renforcement de la sécurité de l'instance)

Utilisez la propriété pour définir une durée de vie maximale pour les `glide.ui.user_cookie.max_life_span_in_days` cookies utilisateur créés lorsque les utilisateurs se connectent avec la case **Se souvenir de moi** cochée. Lorsque le cookie expire, les utilisateurs qui ont coché la case **Se souvenir de moi** sont obligés de s'authentifier à nouveau dans l'instance.

Il permet au cookie utilisateur d'être valide pour la durée de jours spécifiés, à compter de sa première émission. La valeur par défaut est de 30 jours et la limite maximale est de 365 jours.

Remarque :
Pour appliquer une durée de session maximale pour toutes les sessions utilisateur actives, reportez-vous à la section Configure a maximum active time for user sessions .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.user_cookie.max_life_span_in_days`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour forcer les utilisateurs qui ont coché la case **Se souvenir de moi** à s'authentifier à nouveau après des jours spécifiques.
Impact fonctionnel	(Moyen) Cette propriété applique la reconnexion obligatoire en évitant toute sorte de rotation de cookie après une période donnée.
Risque de sécurité	(Moyen) Le fait que les cookies de l'utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer lors d'une configuration basée sur le temps.
Références	Propriétés système disponibles Mémoriser mon nom

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Jeton anti-CSRF (renforcement de la sécurité de l'instance)

Utilisez la propriété pour garantir l'utilisation `glide.security.use_csrf_token` d'un jeton de sécurité pour identifier et valide les demandes entrantes, qui sont ensuite utilisées pour prévenir ces attaques.

La falsification de requête inter-site (CSRF) est une attaque qui oblige un utilisateur final à exécuter des actions indésirables sur une application Web dans laquelle il est actuellement authentifié. Les attaques CSRF ciblent spécifiquement les demandes de changement d'état, et non le vol de données, car l'attaquant n'a aucun moyen de voir la réponse à la requête falsifiée.

Les propriétés suivantes peuvent être activées pour les contrôles supplémentaires sur le jeton CSRF :

- `glide.security.csrf_previous.time_limit`
- `glide.security.csrf_previous.allow`
- `glide.security.csrf.strict.validation.mode`

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.use_csrf_token
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour protéger l'application contre une éventuelle attaque CSRF.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. Chaque demande d'écriture contient un jeton CSRF (c'est-à-dire un ID de validation/CSRF lié à la session utilisateur). Lorsque la session utilisateur expire, le jeton de sécurité expire avec elle.
Risque de sécurité	(Élevé) La falsification des requêtes intersites constitue un risque de sécurité important qui porte atteinte à l'intégrité des données de l'instance. Un attaquant peut lancer l'attaque CSRF en abusant de la confiance d'un utilisateur d'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une requête mal formée au nom de l'attaquant de l'instance.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Changer les informations d'identification par défaut (renforcement de la sécurité de l'instance)

Utilisez la case à cocher **Mot de passe à réinitialiser** dans Utilisateurs et groupes pour vous assurer qu'un utilisateur illégitime ne peut pas tirer parti des données par défaut.

Ils Now Platform incluent des données par défaut lorsque l'instance est zbooted, ou lorsque vous mettez en service une nouvelle instance. Il peut contenir les comptes d'utilisateur de démonstration tels que l'administrateur par défaut, l'ITIL et l'employé. La définition de la propriété rend nécessaire la modification des informations d'identification par défaut de l'administrateur, de l'ITIL et de l'employé lors de la connexion à l'application.

Étapes à configurer

1. Connectez-vous avec le nom d'utilisateur **admin** et le mot de passe **admin**.
2. Accédez à la **Sécurité de système** > **Utilisateurs** > **Utilisateurs et groupes.**
3. Recherchez l'utilisateur sous ID d'utilisateur **admin** et Name **administrator**. Cliquez sur l'ID de l'utilisateur **administrateur** pour modifier les paramètres de l'utilisateur.
4. Modifiez le champ **E-mail** pour indiquer une adresse e-mail valide pour cet utilisateur.
5. Cochez la case **Réinitialisation du mot de passe requise** .
6. Cliquez sur **Mettre à jour**.
7. Déconnectez-vous.
8. Connectez-vous à nouveau pour être invité à définir un nouveau mot de passe.
9. Répétez les étapes 3 à 7 pour les comptes ITIL et d'employé.

Cookies HTTP uniquement (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer l'attribut HTTPOnly pour les `glide.cookies.http_only` cookies sensibles.

Utilisez l'attribut HTTPOnly pour empêcher les attaques, telles que le script de site à site, car il n'autorise pas l'accès au cookie à l'aide d'un script côté client, tel que

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

JavaScript. Il n'élimine pas les risques de cross-site scripting mais élimine certains vecteurs d'exploitation.

En savoir plus

Attribut	Description
Nom de la propriété	glide.cookies.http_only
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour atténuer le risque que le script côté client accède au cookie protégé.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation ajoute un marqueur HTTPOnly supplémentaire aux cookies de session, les protégeant ainsi contre le vol. • Si vous disposez d'une fonctionnalité personnalisée qui nécessite JavaScript pour accéder au cookie de l'utilisateur, cette fonctionnalité est interrompue. Cela ne devrait pas être le cas dans des circonstances normales. • Il Now Platform gère la gestion des sessions et il ne devrait pas y avoir de raison pour qu'un script personnalisé accède aux cookies de l'utilisateur.
Risque de sécurité	(Moyen) Les cookies de session de l'application authentifient un utilisateur final et fournissent des autorisations d'accès implicites à l'application. Cela signifie qu'il est nécessaire de les protéger contre le vol ou l'exportation. Les marqueurs HTTP Only protègent les cookies de session contre les injections JavaScript ou les vulnérabilités de script de site à site qui les volent.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Validation stricte CSRF (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer la `glide.security.csrf.strict.validation.mode` validation stricte du jeton CSRF. Si le jeton CSRF ne correspond pas, une nouvelle soumission de la demande est impossible.

En savoir plus

Attribut	Description
Nom de la propriété	glide.security.csrf.strict.validation.mode
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer une validation stricte du jeton CSRF et empêcher sa réutilisation.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette remédiation active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. Il vérifie si le jeton CSRF actuel a été utilisé précédemment. Si c'est le cas, cela empêche la soumission d'autres demandes d'écriture.
Risque de sécurité	(Moyen) La falsification des requêtes intersites constitue un risque de sécurité important qui porte atteinte à l'intégrité des données de l'instance. Un attaquant peut lancer l'attaque CSRF sur n'importe quel utilisateur d'instance en abusant de la confiance de l'utilisateur de l'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une requête mal formée à l'instance au nom de l'attaquant.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver l'authentification sans mot de passe (renforcement de la sécurité de l'instance)

Utilisez la propriété pour empêcher les *glide.login.no_blank_password* utilisateurs de se connecter Now Platform avec des mots de passe vierges ou en laissant le champ **Mot de passe** vide.

Même si l'administrateur attribue délibérément une valeur vide ou un mot de passe vide dans les enregistrements utilisateur, un utilisateur ne peut pas se connecter sans fournir une valeur dans le champ **Mot de passe** .

En savoir plus

Attribut	Description
Nom de la propriété	glide.login.no_blank_password
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Assurer une authentification forte car les noms d'utilisateur sont parfois faciles à deviner au sein d'une organisation.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Les opérations ne doivent pas utiliser de mots de passe vierges, car cela est considéré comme un risque de sécurité critique. Toutefois, s'il existe un cas valable pour une telle utilisation, il existe une possibilité de panne. Les utilisateurs avec des mots de passe vides ne peuvent pas se connecter à l'instance.
Risque de sécurité	(Élevé) Un attaquant est en mesure de se connecter à l'instance avec les noms d'utilisateur par défaut, ou par personne/groupe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	spécifique (généralement prénom.nom) sans mot de passe. Cela est considéré comme un risque de sécurité critique, car cela permettrait à un utilisateur public de violer la confidentialité et l'intégrité des données de l'instance.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer l'authentification multifacteur (MFA) (renforcement de la sécurité de l'instance)

Utilisez la propriété pour activer l'authentification `glide.authenticate.multifactor` à plusieurs facteurs (MFA) dans l'instance. La MFA est un besoin de sécurité qui demande à l'utilisateur de saisir plus d'un ensemble d'informations d'identification pour s'authentifier auprès d'une instance.

En savoir plus

Attribut	Description
Nom de la propriété	glide.authenticate.multifactor
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Renforcez la sécurité des instances en introduisant l'authentification multifacteur pour les connexions interactives des utilisateurs.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) L'activation de cette propriété améliore l'expérience de l'utilisateur. Il agit comme une couche supplémentaire de protection et de sécurité contre les informations d'identification compromises.
Risque de sécurité	(Moyen) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé aux données sensibles.
Références	Propriétés système d'authentification multifacteur

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Définir des critères d'authentification multifacteur basés sur les rôles

Utilisez la propriété pour appliquer l'authentification multifacteur (MFA) basée sur les `glide.authenticate.multifactor` rôles à tous les utilisateurs affectés à des rôles spécifiques.

Appliquer l'authentification multifacteur en fonction des rôles affectés à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » sont affectés à un utilisateur dans la liste des rôles multifacteur, MFA est appliquée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définissez cette propriété sur **vrai** pour appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
- Définissez cette propriété sur **faux** pour désactiver l'authentification multifacteur basée sur les rôles pour tous les utilisateurs affectés à des rôles spécifiques.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.authenticate.multifactor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
Type	vrai/faux
Valeur recommandée	`true`
Dépendances de Sécurité	**Activez l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Impact fonctionnel	(Moyen) L'activation de cette propriété améliore l'expérience de l'utilisateur. Il agit comme une couche supplémentaire de protection et de sécurité contre les informations d'identification compromises.
Risque de sécurité	(Moyen) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé aux données sensibles.
Références	Configurer les critères multifacteur basés sur les rôles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer les contrôles de la politique de Réinitialisation du mot de passe (renforcement de la sécurité de l'instance)

Utilisez la propriété **glide.enable.password_policy** pour activer les vérifications de la politique de mot de passe chaque fois qu'un utilisateur change son mot de passe à l'aide de l'interface utilisateur.

Pour définir la politique de mot de passe à utiliser une fois cette propriété activée, reportez-vous à la section Activer les politiques de mot de passe sur votre instance.

Remarque :
La **glide.enable.password_policy** ne s'applique pas lorsqu'un administrateur modifie un mot de passe ou ajoute un utilisateur via un script.

En savoir plus

Attribut	Description
Nom de la propriété	glide.enable.password_policy

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Configurer dans le centre de sécurité de l'instance	Oui
Type de configuration	Propriétés système (/sys_properties_list.do)
Objectif	Pour appliquer la politique de mot de passe au moment du changement de mot de passe.
Valeur recommandée	true (pour les mots de passe de complexité élevée)
Impact fonctionnel	(Moyen) Définir la propriété sur vrai active les vérifications de la politique de mot de passe lorsqu'un utilisateur réinitialise son mot de passe.
Risque de sécurité	(Moyen) Sans politique de mot de passe, un utilisateur peut créer un mot de passe faible, ce qui augmente la probabilité qu'un adversaire accède à l'instance.

Étapes à configurer

Si vous configurez ce paramètre dans la page Configuration de la conformité à la sécurisation renforcée dans Centre de sécurité de l'instance :

1. Sous **Moyen**, sélectionnez **Gestion des sessions**.
2. Dans le paramètre **Activer la vérification de la politique de réinitialisation du mot de passe** , sélectionnez **Moyen** pour les mots de passe de complexité moyenne ou **Fort** pour les mots de passe plus robustes et de complexité supérieure. La sélection de l'une de ces options définit la propriété **glide.enable.password_policy** sur true et démarre un workflow qui met automatiquement à jour votre politique de mot de passe.

En outre, vous pouvez définir la propriété système pour activer les *glide.apply.password_policy.on_login* vérifications de la politique de mot de passe au moment de la connexion.

Gestion des échecs de tentatives de connexion (renforcement de la sécurité de l'instance)

Deux actions des scripts sont disponibles afin qu'un administrateur de site puisse gérer le nombre de tentatives de mot de passe incorrect pour un utilisateur avant d'être bloqué par le Now Platform. Vous pouvez activer l'une ou l'autre de ces actions de script pour gérer les échecs de tentative de connexion.

En savoir plus

Attribut	Description
Nom de la propriété/du module d'extension	N/A
Type de configuration	Politique système > Actions des scripts
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer une politique stricte en cas d'échec de tentative de connexion afin d'éviter l'attaque par force brute des informations d'identification.
Valeur recommandée	Actif

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Faible) Cette remédiation permettrait à l'administrateur de l'instance de surveiller et de signaler tout accès utilisateur malveillant. Aucun impact sur la fonctionnalité, uniquement un changement de l'expérience utilisateur.
Risque de sécurité	(Moyen) Appliquez une stratégie de journalisation et d'audit définie afin de pouvoir identifier les activités suspectes et agir en temps opportun.
Références	

Étapes à configurer

1. Accédez à la **Politique système** > **Actions des scripts.**
2. Recherchez le nom *`*SNC User`*.
3. Pour activer la gestion des échecs de tentatives de connexion, changez l'état Actif des actions des *`SNC User Lockout Check with Auto Unlock`* scripts ou *`SNC User Lockout Check`* des scripts de **faux** à **vrai**.
4. Pour réinitialiser le compteur d'échecs de connexion après une connexion réussie, vous pouvez activer l'action des *`SNC User Clear`* scripts.

Saisie semi-automatique du champ de mot de passe (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour permettre aux navigateurs d'utiliser la saisie semi-automatique sur les champs de mot de passe dans les *`glide.login.autocomplete`* formulaires de connexion.

En savoir plus

Attribut	Description
Nom de la propriété	glide.login.autocomplete
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour désactiver le navigateur afin qu'il tente la saisie semi-automatique d'un champ de mot de passe.
Valeur recommandée	faux
Impact fonctionnel	(Faible) Cette correction entraîne la désactivation du marqueur de **saisie automatique du champ Mot de passe** afin que le cache de l'historique des mots de passe par le navigateur ne s'affiche pas dans le champ. Il ne devrait pas y avoir d'impact sur la fonctionnalité.
Risque de sécurité	(Faible) Les champs d'authentification utilisateur doivent être validés et ne doivent jamais laisser se produire la mise en cache côté client.
Références	https://support.servicenow.com/kb_view.do?sysparm_article=KB0563953

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Supprimer les informations d'identification de la page d'accueil (renforcement de la sécurité de l'instance)

Modifiez le contenu par défaut sur la page d'accueil pour supprimer les informations d'identification par défaut.

Remarque :
Deux enregistrements Comment se connecter font partie des données de démonstration du module d'extension CMS. Si vous n'installez pas les données de démonstration pour une instance, ces enregistrements n'existent pas. Dans ce cas, la configuration est considérée comme conforme à la sécurité conformément aux pratiques de sécurité recommandées. Pour en savoir plus, consultez Bonnes pratiques de sécurité.

Étapes à configurer

1. Accédez à la **Interface utilisateur du système** > **Contenu de page d'accueil** > **.**
2. Trouvez les deux sections avec une brève description de **Comment se connecter**.
3. Modifiez l'état Actif de chaque élément de **vrai** à **faux**.

Supprimer Se souvenir de moi (renforcement de la sécurité de l'instance)

Utilisez la propriété pour supprimer la case à cocher **« Se souvenir de moi »** de la page de connexion afin d'éviter que `glide.ui.forgetme` les informations de connexion ne soient mises en cache.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.forgetme
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour garantir qu'aucune information d'authentification n'est mise en cache.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation modifierait l'expérience utilisateur en le déconnectant automatiquement de l'instance à l'expiration de sa session. L'expiration de la session dépend uniquement de la valeur définie dans la propriété système, comme indiqué dans Gérer les sessions utilisateur .
Risque de sécurité	(Moyen) Lorsque vous cochez la case **Se souvenir de moi** lors de la connexion, un cookie supplémentaire est stocké sur l'ordinateur de l'utilisateur. • Son but est de rétablir automatiquement la session pour les visites ultérieures de l'utilisateur connecté. • Cela pose un risque de sécurité car il permet à la session de l'utilisateur d'être active jusqu'à ce qu'il se déconnecte délibérément. La probabilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	d'une attaque pour ce scénario augmente lorsque l'utilisateur final a laissé le navigateur sans surveillance ou s'il est compromis par une autre attaque.
Références	Supprimer la case à cocher Se souvenir de moi

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Rotation des identificateurs de session HTTP (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour activer la rotation des identificateurs de session HTTP afin de réduire les `glide.ui.rotate_sessions` failles de sécurité.

Si l'ID de session d'un utilisateur non authentifié ne change pas après l'authentification, une application Web est vulnérable à une attaque de fixation de session . Un utilisateur malveillant pourrait démarrer une session non authentifiée et donner l'ID de session associé à la victime. Une fois que la victime s'est authentifiée, l'utilisateur malveillant partage désormais cette session authentifiée.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.rotate_sessions
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette correction modifie l'ID de session lorsque l'utilisateur navigue d'une page non authentifiée vers des pages authentifiées. • Si vous utilisez un proxy ou codez en dur le SessionID lorsqu'un utilisateur se connecte pour la première fois, ou à toute autre fin, il peut y avoir un impact potentiel sur la fonctionnalité. • Si vous utilisez le module d'extension SAML 2.0 pour l'authentification Single Sign-on, il peut interférer avec le partage d'informations de session entre l'instance et le fournisseur d'identité. Dans ce cas, vous pouvez définir cette propriété sur false.
Risque de sécurité	(Tardif) SessionID permet de traiter et d'authentifier l'utilisateur de l'instance en conservant l'état de session sur le navigateur. Ainsi, SessionID est considéré comme une donnée sensible et doit être sécurisé par défaut. La rotation de session est un contrôle de sécurité qui applique la modification de sessionID

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	chaque fois que l'utilisateur navigue à partir de pages non authentifiées pour authentifier des pages.
Références	Authentification avec SAML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Cookies de session sécurisés (renforcement de la sécurité de l'instance)

Utilisez la *glide.ui.secure_cookies* propriété pour exiger des cookies correctement formatés

Lorsque vous définissez la propriété sur vrai, votre instance rejette une session si le format du cookie associé n'est pas attendu.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.secure_cookies
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Lorsque la propriété est définie sur vrai, les cookies mal formatés sont rejetés. Lorsqu'un tel cookie est rejeté, l'utilisateur doit se connecter à nouveau.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Politique de référence de la sécurité (renforcement de la sécurité de l'instance)

Utilisez cette propriété pour contrôler les données référentes qui doivent être envoyées dans les *com.glide.security.referrerpolicy* en-têtes de réponse HTTP lorsque Now Platform pages envoie des demandes de données. La valeur Referrer-Policy d'un en-tête HTTP contrôle quelles informations de référent doivent être incluses dans les demandes de données.

Valeurs de la politique de recommandation de sécurité

Définissez la *com.glide.security.referrerpolicy* propriété sur l'une des valeurs suivantes.

Valeur	Description
Par défaut	Now Platform L'instance gère le niveau d'informations envoyées dans les en-têtes de référent

Traduction automatique

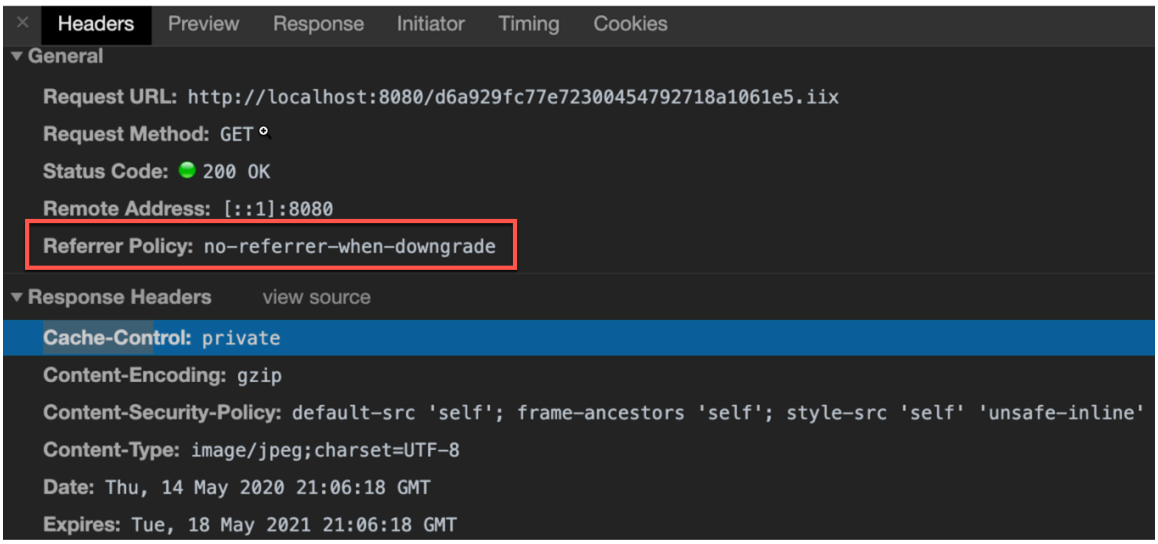
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur	Description
	qui est approprié pour la demande de page spécifique Now Platform .
d'origine identique	Now Platform Les pages envoient une URL référente complète au sein de l'instance et du même domaine, et aucun en-tête référent à l'origine extérieure. Ce paramètre garantit un bon niveau de sécurité de l'instance.
origine	Now Platform envoient l'URL de base dans l'en-tête référent au sein de l'instance et du même domaine, ainsi qu'en externe. Ce paramètre garantit un bon niveau de sécurité de l'instance.
origine-quand-origine croisée	Now Platform envoient l'URL entière dans l'en-tête référent au sein de l'instance et du même domaine, et envoient uniquement l'URL de base en externe. Ce paramètre garantit un bon niveau de sécurité de l'instance.
no-referrer-when-downgrade	Now Platform envoient l'origine, le chemin d'accès et la chaîne de requête dans l'URL, tant qu'il n'y a pas de rétrogradation dans un protocole de sécurité. **Remarque :** Ce paramètre ne garantit pas un bon niveau de sécurité d'instance dans le Now Platform et ne doit pas être utilisé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de politique de référence et résumé des valeurs



En savoir plus

Attribut	Description
Nom de la propriété	com.glide.security.referrerpolicy
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Contrôle la quantité de données entrantes envoyées via l'en-tête « référent » lorsqu'une Now Platform page envoie une demande de données.
Valeur recommandée	Par défaut
Impact fonctionnel	(Faible) Si la valeur est définie sur « Par défaut », l'instance Now Platform gère le niveau d'informations envoyées dans les en-têtes de référent.
Risque de sécurité	(Élevé) Définir cette valeur de propriété sur « no-referrer-when-downgrade » ne garantit pas un bon niveau de sécurité pour votre instance.
Référence	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy https://developer.mozilla.org/en-US/docs/Glossary/origin

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Délai d'activité de la session (renforcement de la sécurité de l'instance)

Utilisez la propriété pour désigner, en minutes, la valeur du délai d'expiration de l'activité `glide.ui.session_timeout` .

La définition de cette propriété a plusieurs impacts fonctionnels :

- Plus le délai d'expiration de session spécifié est long, plus la quantité de mémoire utilisée au cours d'une session de traitement est importante. Le système de base utilise une durée d'expiration du délai d'expiration Apache Tomcat par défaut de 30 minutes.
- L'utilisateur Now Platform se déconnecte toujours avec Se souvenir de moi. Après 30 minutes d'inactivité dans l'application, la plateforme déconnecte automatiquement l'utilisateur, sauf si la case à cocher **Se souvenir de moi** dans la page de connexion est cochée. Ce qui est différent, c'est qu'ils ne se reconnectent pas pour continuer.
- Si des jauges ou du contenu sur les pages d'accueil des utilisateurs s'actualisent automatiquement, ce délai peut ne jamais être atteint.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.session_timeout
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour appliquer le délai d'expiration de session.
Valeur recommandée	Délai spécifié par l'utilisateur en minutes. 30 minutes est la valeur recommandée, mais cette valeur peut varier en fonction de la fonctionnalité et des exigences de sécurité. Ne définissez pas cette valeur sur plus d'un jour.
Impact fonctionnel	(Moyen) Cette remédiation applique l'expiration en temps opportun du compte utilisateur. Aucun impact sur la fonctionnalité, mais l'expérience utilisateur est altérée.
Risque de sécurité	(Moyen) Le fait que les sessions utilisateur soient actives pour une durée indéterminée constitue un risque pour la sécurité et doit expirer sur une configuration basée sur le temps.
Références	Gérer les sessions utilisateur

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Délai d'expiration de la fenêtre de session (renforcement de la sécurité de l'instance)

Utilisez la `glide.ui.user_cookie.life_span_in_days` propriété pour définir le délai d'expiration du cookie Se souvenir de moi. La valeur par défaut est de 15 jours et le délai maximum est de 30 jours.

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.user_cookie.life_span_in_days

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Pour activer l'expiration par défaut du cookie « Se souvenir de moi ».
Valeur recommandée	Valeur entière définie par l'utilisateur (# de jours) [Exemple : 15]
Impact fonctionnel	(Moyen) Cette propriété est activée par l'utilisateur final lorsqu'il coche la case **Se souvenir de moi** sur la page de connexion et se connecte au Now Platform.
Risque de sécurité	(Moyen) Le fait que les cookies de l'utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer lors d'une configuration basée sur le temps.
Références	Propriétés système disponibles Mémoriser mon nom

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Configurer les mots de passe pour les comptes utilisateur créés automatiquement

Utilisez les propriétés système `glide.email.inbound.use_default_password` et `glide.user.default_password` pour définir comment créer des mots de passe pour les nouveaux utilisateurs créés à partir d'e-mails entrants.

Les propriétés système décrites dans ce document définissent la manière dont l'instance gère les mots de passe des comptes utilisateur générés à partir d'e-mails entrants. Votre instance doit être configurée avec la capacité de recevoir des e-mails et d'activer la création automatique d'utilisateurs. Consultez la section ci-dessous pour plus de détails sur ces configurations.

Une fois que votre instance est configurée pour créer automatiquement des comptes, vous pouvez utiliser les propriétés pour déterminer s'il faut utiliser un mot de passe par défaut et définir ce mot de passe, si nécessaire.

Prérequis

Pour utiliser ces propriétés, votre instance doit être configurée pour créer automatiquement de nouveaux comptes d'utilisateur.

- Vous devez configurer votre propre serveur POP3 afin qu'il stocke et reçoive des e-mails pour votre instance. Ensuite, vous devez définir la `glide.email.read.active` propriété système sur true. Pour en savoir plus sur la configuration d'un serveur POP3 sur votre instance, consultez Activer l'utilisation de votre propre serveur POP3 .
- Définissez la propriété `glide.pop3readerjob.create_caller` sur true. Avec ce changement de propriété, votre instance peut créer automatiquement des utilisateurs à partir d'un e-mail entrant. Pour en savoir plus, consultez Activer la création automatique d'utilisateurs .

> **Remarque :**
> Ignorez la `glide.user.default_password` propriété si elle `glide.pop3readerjob.create_caller` est définie sur **false**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment votre instance définit-elle les mots de passe ?

Dans Quebec et dans les versions antérieures de ServiceNow, votre instance crée de nouveaux comptes utilisateur à partir d'e-mails entrants à l'aide d'un mot de passe complexe défini dans la *glide.user.default_password* propriété système. Les utilisateurs utilisent ce mot de passe la première fois qu'ils se connectent, puis l'instance leur demande un nouveau mot de passe. Si vous avez mis à niveau votre instance vers une version ultérieure Rome ou ultérieure, ce processus reste inchangé. En tant qu'administrateur, vous pouvez mettre à jour votre instance pour utiliser la nouvelle méthode décrite ci-dessous.

Dans les nouveaux cas à partir de la version, les Rome comptes utilisateur créés à partir d'e-mails entrants n'ont pas de mot de passe. Lorsqu'un utilisateur accède pour la première fois à l'instance avec son nouveau compte, il doit saisir son nom d'utilisateur et cliquer sur le bouton **Mot de passe oublié ?** pour créer un mot de passe initial.

Dans Rome les versions ultérieures, vous pouvez choisir le processus que suit votre instance en définissant une valeur dans la *glide.email.inbound.use_default_password* propriété système. Pour modifier le comportement par défaut décrit ci-dessus, créez cette propriété système à l'aide des informations suivantes :

Champ de propriété système	Valeur
Nom	glide.email.inbound.use_default_password
Type	true|false
Valeur	Sélectionnez une valeur en fonction du comportement souhaité : **VRAI** Les nouveaux comptes utilisent un mot de passe par défaut défini dans la *glide.user.default_password* propriété système. **faux** Les nouveaux comptes n'ont pas de mot de passe par défaut. Les utilisateurs doivent définir un mot de passe, comme décrit précédemment dans cette section.

Pour plus d'informations sur la création de propriétés système, consultez Ajouter une propriété système .

Définir un mot de passe par défaut

Si votre instance est configurée pour utiliser un mot de passe par défaut, vous devez définir ce mot de passe à l'aide de la *glide.user.default_password* propriété système. Créez cette propriété à l'aide des informations suivantes :

Champ de propriété système	Valeur
Nom	glide.user.default_password
Type	mot_de_passe2
Valeur	Entrez un mot de passe unique à utiliser par défaut. Utilisez une complexité de mot de passe forte pour garantir la sécurité de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de sécurisation renforcée

Le ServiceNow, Inc. contenu des paramètres de sécurisation renforcée du Centre de sécurité contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans le Now Platform. Vous pouvez définir ces propriétés à l'aide de l'application Paramètres de sécurisation renforcée dans le Centre de sécurité.

Vue d'ensemble et objectif

Le centre de sécurité calcule un score de conformité quotidien, exprimé en pourcentage, basé sur la conformité des paramètres de sécurité de votre instance actuels avec les valeurs de conformité des paramètres de renforcement du centre de sécurité.

Vous pouvez gérer les paramètres de configuration de sécurité spécifiques qui peuvent affecter le score de votre instance directement à partir du Centre de sécurité.

Les configurations des paramètres de sécurisation renforcée sont expliquées à l'aide de plusieurs attributs décrits dans le tableau.

Détails de configuration des paramètres de sécurisation renforcée

Attribut de configuration	Description
Vue d'ensemble	Fournit une vue d'ensemble de haut niveau de la recommandation.
Nom de la configuration	Nom de la propriété ou du module d'extension.
Type de configuration	Décrit les endroits où la propriété peut être configurée en dehors du Centre de sécurité, comme dans les propriétés système (*`sys_properties_list.do`*).
Type de données	Décrit le type de valeur requis pour la configuration. Par exemple, le booléen vrai/faux, l'installation, le module d'extension, la chaîne, etc.
Valeur recommandée	Valeur recommandée par le centre de sécurité pour améliorer la conformité de la sécurité dans votre instance.
Valeur par défaut	La valeur sur laquelle la configuration est définie dans le système de base.
Catégorie	Nom et lien vers la catégorie du paramètre de sécurisation renforcée.
Risque de sécurité	**Score de gravité** : le score indique le risque de sécurité potentiel pour votre instance en fonction de la probabilité d'exploitation de la vulnérabilité. La vulnérabilité de sécurité est prise en compte et notée individuellement à l'aide du score CVSS (Common Vulnerability Scoring System) sur une échelle allant de **0,0** à **10,0**. Consultez https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator pour plus d'informations. **Évaluation de la gravité par score CVSS** : • Critique : 9,0-10,0 • Haute : 7.0-8.9 • Moyenne : 4,0 à 6,9 • Faible : .01-3.9 • Aucun : 0,0

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de configuration des paramètres de sécurisation renforcée (suite)

Attribut de configuration	Description
	Détails du risque de sécurité : décrit l'importance de la configuration des paramètres et le risque de ne pas utiliser la configuration recommandée.
Dépendances et prérequis	Paramètres ou configurations connexes requis avant ou en conjonction avec la configuration de sécurisation renforcée.
Impact fonctionnel	L'impact de ce paramètre de sécurisation renforcée sur le fonctionnement de votre instance.
Références	Liens vers la documentation de configuration ou d'autres informations utiles.

Remarque :
Certaines configurations ne peuvent être complétées que par Service et assistance client et seront indiquées comme telles.

Pour en savoir plus sur la façon de s'assurer que vos instances répondent aux exigences de sécurisation renforcée, reportez-vous à la section Sécurisation renforcée de la sécurité.

Autres ressources

Pour la référence utilisateur, la Now Platform conserve des informations détaillées sur les options de configuration dans la documentation du produit. Les liens trouvés dans Sécuriser votre instance vous permettent d'accéder à la plupart du contenu de la sécurité. Consultez également les rubriques suivantes :

- Propriétés système disponibles
- Propriétés des paramètres de sécurité généraux
- Paramètres de sécurité élevée

Base de référence des paramètres de sécurisation renforcée

Découvrez comment des versions de base distinctes pour les paramètres de sécurisation renforcée s'alignent sur les différentes versions de la famille et du magasin.

Centre de sécurité Le fonctionnement consiste à ingérer un sous-ensemble de propriétés système à partir d'une instance et à afficher les détails de sa configuration, ainsi que l'impact sur la sécurité de la non-conformité au sein de l'application. La base de référence sert de point de référence pour les propriétés système qui sont ingérées avec chaque version de l'application Centre de sécurité.

Vue d'ensemble de la base de référence des paramètres de sécurisation renforcée

Version du centre de sécurité	Version de base des paramètres de sécurisation renforcée	Familles soutenues	Date de mise en production de la boutique	Installé par défaut avec
SSC v1.1	Base de référence v1.0	Utah, Vancouver	mai 2023	Famille de Vancouver

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble de la base de référence des paramètres de sécurisation renforcée (suite)

Version du centre de sécurité	Version de base des paramètres de sécurisation renforcée	Familles soutenues	Date de mise en production de la boutique	Installé par défaut avec
SSC v1.2	Base de référence v1.0	Utah, Vancouver	août 2023	Stocker uniquement
SSC v1.3	Base de référence v2.0	Vancouver, Washington	nov. 2023	Famille Washington
SSC v1.5	Base de référence v4.0	Washington, Xanadu	mai 2024	Xanadu
SSC v1.6	Base de référence v4.0	Washington DC, Xanadu	Août 2024	

Nouveaux paramètres de sécurisation renforcée pour la version de base de référence 4.0

Voici une liste de tous les nouveaux paramètres de sécurisation renforcée publiés avec la base de référence de la version 4.0 du Centre de sécurité.

- Examiner les conditions de contrôle d'accès aux rôles explicites superflus [supprimé dans Security Center 1.5]
- Activer les règles de requête de gestion des commandes de travaux pour les organisations de services [Nouveau dans Security Center 1.5]
- Désactiver la racine de confiance ServiceNow
- Restreindre l'accès en lecture au contexte de flux [Nouveau dans Security Center 1.5]
- Limiter l'intervalle de jeton d'actualisation mobile d'accès à la session basée sur des politiques [Nouveau dans Security Center 1.5]
- Activer l'accès à la session basé sur des politiques pour mobile [Nouveau dans Security Center 1.5]
- Empêcher les utilisateurs inactifs de se connecter [Nouveau dans Security Center 1.5]
- Configurer les rôles administrateur du groupe d'affectation de gestion des événements [Nouveau dans Security Center 1.5]
- Appliquer le champ d'application de sécurité pour l'Espace de travail d'agent pour la gestion des tickets RH [Nouveau dans Security Center 1.5]
- Appliquer le Playbook pour les licences et les autorisations dans le champ d'application de sécurité [Nouveau dans Security Center 1.5]

Nouveaux paramètres de sécurisation renforcée pour la version de base de référence 2.0

Voici une liste de tous les nouveaux paramètres de sécurisation renforcée publiés avec la base de référence de la Centre de sécurité version 2.0.

- Appliquer l'utilisation d'alias d'informations d'identification [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Appliquer la vérification OCSP en cas d'erreur réseau [Nouveau dans Security Center 1.3]
- Vérifier la chaîne et le nom d'hôte des certificats [Nouveau dans Security Center 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifier la révocation du certificat [Nouveau dans Security Center 1.3]
- Définir une politique de sécurité de contenu sûre pour les fichiers SVG [Nouveau dans Security Center 1.3]
- Utilisation de l'opération multiple d'insertion sécurisée dans l'API de jeu d'importation [Nouveau dans Security Center 1.3]
- Activer le module d'extension Tables protégées [Nouveau dans Security Center 1.3]
- Appliquer la politique de référent sécurisé [Nouveau dans Security Center 1.3]
- Définir les rôles d'exception de délai d'expiration de session active [Nouveau dans Security Center 1.3]
- Invalider de manière proactive les sessions inactives [Nouveau dans Security Center 1.3]
- Valider le type MIME de fichier dans le service web soap AttachmentCreator [Nouveau dans Security Center 1.3]
- Authentification basée sur certificat non mise en application [Nouveau dans Security Center 1.3]
- Consigner les événements d'audit de session [Nouveau dans Security Center 1.3]
- Exiger l'authentification sur le processeur HTTP Gestion des événements [Nouveau dans Centre de sécurité 1.3]
- Appliquer des règles de sécurité au partage de tableaux de bord [Nouveau dans Security Center 1.3]
- Interdire le clonage cible [Nouveau dans Security Center 1.3]
- Appliquer la sécurité du champ d'application pour les services numériques du secteur public [Nouveau dans Security Center 1.3]
- Appliquer l'accès ACL inclus dans le champ d'application pour les informations request playbook [Nouveau dans Security Center 1.3]
- Limiter la durée de vie de la session active de l'invité [Nouveau dans Security Center 1.3]
- Limiter la durée de vie de la session active des intégrations [Nouveau dans Security Center 1.3]
- Restreindre l'accès aux bases de connaissances [Nouveau dans Security Center 1.3]
- Masquer les commentaires des utilisateurs sur les articles [Nouveau dans Security Center 1.3]
- Restreindre les paramètres OAuth au corps de publication [Nouveau dans Security Center 1.3]
- Limiter la taille des pièces jointes dans les flux de formation et de prédiction [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- S'assurer que la création/la suppression des tableaux de bord nécessite une vérification d'accès [Nouveau dans Security Center 1.3]
- Désactiver le comportement hérité de clôture du champ d'application GlideRecord [Nouveau dans Security Center 1.3]
- Appliquer les restrictions de périmètre de l'application [Nouveau dans Security Center 1.3]
- Exiger un accès en écriture pour accéder à la page Ajouter un élément du catalogue de services [Nouveau dans Security Center 1.3]
- Temps de validation du jeton anti-CSRF [Nouveau dans Security Center 1.3]
- S'assurer que les ACL des tables d'archivage sont vérifiées [Nouveau dans Security Center 1.3]
- Activer le gestionnaire de sécurité Java renforcé [Nouveau dans Security Center 1.3]
- Appliquer le privilège d'élévation stricte [Nouveau dans Security Center 1.3]
- Exiger l'effacement du presse-papiers lors de l'affichage l'application mobile en arrière-plan [Nouveau dans Security Center 1.3]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Appliquer les exigences en matière de chiffrement des appareils et de code d'accès [Nouveau dans Security Center 1.3]
- Limiter la durée de vie de session active de l'interface utilisateur [Nouveau dans Security Center 1.3]
- Activer le journal d'audit MID [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Instanciateurs de connexions jms requis [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Exiger un captcha pour l'expérience de visite d'un invité dans l'application Customer Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Vérifier l'emprunt d'identité dans l'évaluation ACL dans l'application RH [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]
- Restreindre les mises à jour des tickets RH à partir d'e-mails personnels [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Paramètres de sécurisation renforcée mis à jour pour la version de base de référence 4.0

Liste des paramètres de sécurisation renforcée qui ont été mis à jour dans la Centre de sécurité version de référence 4.0.

La version 4.0 de la base de référence inclut plusieurs mises à jour des brèves descriptions pour des raisons de style et de cohérence entre les enregistrements. En outre, de nombreux scripts associés à la propriété ont également été mis à jour pour améliorer la précision de la valeur par défaut pour les tickets où la propriété a été supprimée de la table sys_property.

Documentation	Mises à jour
Exiger une autorisation pour les demandes SOAP [mis à jour dans Security Center 1.3 et 1.5]	• Nouveau nom de la configuration technique : *glide.basicauth.required.soap, glide.soap.require_ws_security* • Ancien nom de la configuration technique : *glide.basicauth.required.soap*
Activer l'assainisseur HTML dans Agent virtuel [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer l'assainisseur HTML dans Agent virtuel • Ancienne description brève : Activer l'assainisseur HTML
Refuser l'accès interne aux rôles externes explicites [Mise à jour dans Security Center 1.5]	• Nouveau nom de la configuration technique : *glide.security.explicit_roles.enable_internal_us* • Ancien nom de la configuration technique : *glide.security.explicit_roles.enable_internal_us*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Définir les types MIME téléchargeables restreints [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Définir les types MIME téléchargeables restreints • Ancienne description brève : Restreindre les types MIME téléchargeables
Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes [Mise à jour dans Security Center 1.5]	• Nouvelle description brève : Définir les types MIME téléchargeables restreints • Ancienne description brève : Restreindre les types MIME téléchargeables
Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe [Mise à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe • Ancienne description brève : Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe (Applicabilité du module d'extension : inscription de l'utilisateur externe)
Désactiver le téléchargement des fichiers infectés	• Nouvelle description brève : Désactiver le téléchargement des fichiers infectés • Ancienne description courte : Désactiver le téléchargement des fichiers infectés
Désactiver le débogage MultiSSO	• Nouvelle description brève : Désactiver le débogage MultiSSO • Ancienne description brève : Désactiver le débogage MultiSSO (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)
Définir les adresses IP internes autorisées ServiceNow [mis à jour dans Security Center 1.3 et 1.5]	• Nouveau nom de la configuration technique : `glide.ip.authenticate.strict` • Ancien nom de la configuration technique : `glide.ip.authenticate.strict,glide.ip.authentica`
Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » [Mise à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » • Ancienne description courte : Appliquer Séparation de domaine sur les champs de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
	type « remontée pas à pas » (Applicabilité du module d'extension : Domain Separation)
Activer la récupération de compte [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Activer la récupération de compte • Ancienne description brève : Activer la récupération de compte (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)
Minimiser le seuil d'expansion des entités [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser le seuil d'expansion des entités pour GlideXMLUtil pouvant contenir des scripts • Ancienne description courte : Minimiser le seuil d'expansion des entités
Activer la version mise à jour du module d'extension MultiSSO [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Activer la version actualisée du module d'extension Multi SSO • Ancienne description courte : Activer la version actualisée du module d'extension Multi SSO (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)
Ne pas utiliser de certificats de démonstration pour les configurations SAML actives [Mise à jour dans Security Center 1.5]	• Nouvelle description brève : Ne pas utiliser de certificats de démonstration pour les configurations SAML actives • Ancienne description brève : Ne pas utiliser de certificats de démonstration pour les configurations SAML actives (Applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)
Minimiser la durée de contrainte SAML notBefore ou notOnOrAfter [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter » • Ancienne description brève : Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter » (applicabilité du module d'extension : authentification unique de plusieurs fournisseurs)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Bloquer les jetons anti-CSRF expirés [mis à jour dans Security Center 1.5]	• Nouvelle description brève : bloquer les jetons anti-CSRF expirés • Ancienne description brève : bloquer les jetons CSRF expirés
Exiger un captcha pour l'expérience de visite d'un invité dans l'application Customer Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Exiger un Captcha pour l'expérience de visite d'un invité dans l'application Service clientèle • Ancienne description brève : Exiger un Captcha pour l'expérience de visite d'un invité dans l'application Service clientèle (Applicabilité du module d'extension : expérience de visite d'un invité pour le service clientèle)
Vérifier l'emprunt d'identité dans l'évaluation ACL dans l'application RH [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH • Ancienne description brève : Vérifier l'emprunt d'identité dans l'évaluation ACL de l'application RH (applicabilité du module d'extension : application incluse dans le périmètre de ressources humaines)
Restreindre les mises à jour des tickets RH à partir d'e-mails personnels [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Restreindre les mises à jour des tickets RH à partir d'e-mails personnels • Ancienne description brève : Restreindre les mises à jour des tickets RH à partir d'e-mails personnels (Applicabilité du module d'extension : application incluse dans le périmètre de ressources humaines)
Activer le journal d'audit MID [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Activer le journal d'audit MID • Ancienne description courte : Activer le journal d'audit MID (Applicabilité du module d'extension : Serveur MID)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Appliquer l'utilisation d'alias d'informations d'identification [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Appliquer l'utilisation d'alias d'informations d'identification • Ancienne description courte : Appliquer l'utilisation d'alias d'informations d'identification (Applicabilité du module d'extension : Serveur MID)
Appliquer la validation stricte du jeton CSRF	• Nouvelle description brève : Appliquer la validation stricte du jeton CSRF • Ancienne description brève : Validation stricte du CSRF
Instanciateurs de connexions jms requis [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Instanciateurs de connexions JMS requis • Ancienne description brève : Instanciateurs de connexions JMS requis (Applicabilité du module d'extension : MID Server)
Limiter la taille des pièces jointes dans les flux de formation et de prédiction [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Limiter la taille des pièces jointes dans les flux de formation et de prédiction • Ancienne description brève : Limiter la taille des pièces jointes dans les flux de formation et de prédiction (Applicabilité du module d'extension : Intelligence documentaire de plateforme)
Limiter la taille du corps de réponse HTTP [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]	• Nouvelle description brève : Limiter la taille du corps de la réponse HTTP • Ancienne description courte : Assurez-vous que les réponses HTTP ne déclenchent pas d'exception de mémoire insuffisante en raison de la taille du corps de la réponse

Paramètres de sécurisation renforcée mis à jour pour la version de référence 2.0

Cette liste contient les paramètres de sécurisation renforcée qui ont été mis à jour dans Centre de sécurité la version de référence 2.0.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Restreindre les demandes JSONP aux URL approuvées [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Restreindre les demandes JSONP aux URL approuvées • Ancienne description brève : Liste d'inclusion des demandes JSONP
Minimiser la taille autorisée des pièces jointes [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la taille autorisée des pièces jointes • Ancienne description brève : Taille maximale autorisée des pièces jointes
Appliquer le certificat de confiance [mis à jour dans Security Center 1.3 et supprimé dans la version 1.5]	• Nouvelle description brève : Appliquer le certificat de confiance • Ancienne description brève : Certificat de confiance
Définir des options XFrame pour empêcher l'intégration de sites Web tiers [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Définir des options XFrame pour empêcher l'intégration de sites Web tiers • Ancienne description brève : Options XFrame
Activer l'assainisseur HTML dans Agent virtuel [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer l'assainisseur HTML dans Agent virtuel • Ancienne description brève : Activer l'assainisseur HTML
Restreindre l'accès en lecture des développeurs délégués [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Restreindre l'accès en lecture des développeurs délégués • Ancienne description brève : Liste d'autorisation d'accès en lecture des développeurs délégués
Activer le filtrage et la notation des e-mails indésirables [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer le filtrage et la notation des e-mails indésirables • Ancienne description brève : Filtrage et notation d'e-mails indésirables

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Module d’extension de haute sécurité [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Activer le module d’extension de haute sécurité • Ancienne description brève : Module d’extension de haute sécurité
Activer le module d’extension de sécurité contextuelle [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer le module d’extension de sécurité contextuelle • Ancienne description courte : Module d’extension de sécurité contextuelle
Appliquer l’assainissement HTML [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Appliquer l’assainissement HTML • Ancienne description brève : Vérifier le HTML non désinfecté
Définir l’utilisateur invité pour les demandes SOAP [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Définir l’utilisateur invité pour les demandes SOAP • Ancienne description brève : Utilisateur invité pour les demandes SOAP
Activer le module d’extension de contrôle d’accès SNC [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Activer le module d’extension du contrôle d’accès SNC • Ancienne description courte : Module d’extension du contrôle d’accès SNC
Activer le module d’extension de démarrage rapide de la sécurité (règles ACL) [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer le module d’extension de démarrage rapide de la sécurité • Ancienne description brève : Module d’extension de démarrage rapide de la sécurité (règles ACL)
Désactiver le comportement AngularJS hérité [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Désactiver le comportement AngularJS hérité • Ancienne description brève : Comportement AngularJS hérité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Limiter les sessions interactives simultanées [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Limiter les sessions interactives simultanées • Ancienne description courte : Sessions interactives simultanées : Limite d'authentification Glide
Limiter les sessions simultanées dans tous les nœuds [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Limiter les sessions simultanées dans tous les nœuds • Ancienne description courte : Limite de sessions simultanées dans tous les nœuds : limite d'authentification Glide
Minimiser le nombre de sessions interactives simultanées [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser le nombre de sessions interactives simultanées • Ancienne description brève : Sessions interactives simultanées : Glide : authentifier max.
Activer l'authentification multifacteur basée sur les rôles [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer l'authentification multifacteur basée sur les rôles • Ancienne description brève : Authentification multifacteur basée sur les rôles
Activer la version mise à jour du module d'extension MultiSSO [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Activer la version actualisée du module d'extension Multi SSO • Ancienne description courte : La version actualisée du module d'extension Multi SSO est activée
Minimiser la durée de contrainte SAML notBefore ou notOnOrAfter [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée de contrainte SAML « notBefore » ou « notOnOrAfter » • Ancienne description courte : contrainte SAML « notBefore » ou « notOnOrAfter »
Exiger une autorisation pour les demandes d'API [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes API • Ancienne description brève : Autorisation de demande d'API

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Exiger une autorisation pour les demandes CSV [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : exiger une autorisation pour les demandes CSV • Ancienne description brève : Autorisation des demandes de CSV
Exiger une autorisation pour l'API REST du courtier en données [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour l'API REST du courtier en données • Ancienne description brève : Autorisation de l'API REST du courtier en données
Exiger une autorisation pour les demandes Excel [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes Excel • Ancienne description brève : Autorisation des demandes d'Excel
Exiger une autorisation pour les demandes d'importation [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes d'importation • Ancienne description brève : Autorisation des demandes d'importation
Exiger une autorisation pour la demande JSONv2 [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour la demande JSONv2 • Ancienne description brève : Autorisation des demandes de JSONv2
Exiger une autorisation pour les demandes PDF [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes PDF • Ancienne description brève : Autorisation de demande de PDF
Exiger une autorisation pour les demandes RSS [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes RSS • Ancienne description brève : Autorisation de demande de RSS
Exiger une autorisation pour les demandes SCHEMA [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes SCHEMA • Ancienne description brève : Autorisation de demande de SCHEMA

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Exiger une autorisation pour les demandes SOAP [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Exiger une autorisation pour les demandes SOAP • Ancienne description brève : Autorisation de demande SOAP
Autorisation de la demande de déchargement	• Nouvelle description brève : Exiger une autorisation pour les demandes de déchargement • Ancienne description brève : Autorisation de la demande de déchargement
Exiger une autorisation pour la demande WSDL [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour la demande WSDL • Ancienne description brève : Autorisation de demande de WSDL
Exiger une autorisation pour les demandes XML [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger une autorisation pour les demandes XML • Ancienne description brève : Autorisation de demande XML
Exiger une autorisation pour les demandes de sortie XML	• Nouvelle description brève : Exiger une autorisation pour les demandes de sortie XML • Ancienne description brève : Autorisation de sortie XML
Activer le marqueur de cookie HTTP uniquement [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Activer le marqueur de cookie HTTP uniquement • Ancienne description brève : Marqueur de cookie HTTP uniquement
Désactiver l'exécution des requêtes de base de données brutes [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Désactiver l'exécution de la requête de base de données brute • Ancienne description brève : Exigences en matière de contrôle d'accès au niveau opérationnel

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Désactiver les messages d'erreur SQL [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Désactiver les messages d'erreur SQL • Ancienne description brève : Désactivation des messages d'erreur SQL
Convertir les images des e-mails entrants en pièces jointes [mis à jour dans Security Center 1.3 et supprimé dans la version 1.5]	• Nouvelle description brève : Convertir les images des e-mails entrants en pièces jointes • Ancienne description brève : Convertir les e-mails entrants en HTML
Minimiser la quantité de destinataires SMTP [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la quantité de destinataires SMTP • Ancienne description brève : Nombre maximal de destinataires SMTP
Formules Excel d'échappement [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Formules Excel d'échappement • Ancienne description brève : Échapper à une formule Excel
Activer l'assainisseur HTML [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Activer l'assainisseur HTML • Ancienne description courte : Assainisseur HTML
Valeur de l'en-tête HTTP du contrôle de cache [mise à jour dans Security Center 1.3]	• Nouvelle description brève : Valeur de l'en-tête HTTP du contrôle de cache • Ancienne description brève : Valeur de l'en-tête HTTP du contrôle de cache
Appliquer le comportement de l'instance de production [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Appliquer le comportement de l'instance de production • Ancienne description brève : Comportement de l'instance de production

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Définir les adresses IP internes autorisées ServiceNow [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Définir les adresses IP internes ServiceNow autorisées • Ancienne description courte : Liste d'autorisation d'accès pour les adresses IP
Désactiver le comportement JQuery hérité [Mise à jour dans Securty Center 1.3]	• Nouvelle description brève : Désactiver le comportement JQuery hérité • Ancienne description brève : Comportement JQuery hérité
Annuler le nom distinctif initial LDAP [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Annuler le nom distinctif initial LDAP • Ancienne description brève : Nom distinctif initial LDAP
Restreindre l'accès aux écritures de journal personnalisées [Mise à jour dans Securty Center 1.3]	• Nouvelle description brève : Restreindre l'accès aux écritures de journal personnalisées • Ancienne description brève : Sécurisation des écritures de journal personnalisées
Minimiser la durée de vie unique du vérificateur hors bande [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la durée de vie unique du vérificateur hors bande • Ancienne description brève : Durée de vie courte et unique du vérificateur hors bande
Désactiver les connexions SSLv2/SSLv3 sortantes [Mise à jour dans Securty Center 1.3]	• Nouvelle description brève : Désactiver les connexions SSLv2/SSLv3 sortantes • Ancienne description courte : Désactivation de SSLv2/SSLv3
Désactiver la création d'utilisateurs à partir d'e-mails entrants [Mise à jour dans Securty Center 1.3]	• Nouvelle description brève : Désactiver la création d'utilisateurs à partir d'e-mails entrants • Ancienne description courte : Restreindre les e-mails par domaine

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Restreindre l'accès à l'API de script GlideSystemUserSession [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client • Ancienne description brève : Protection de la vie privée sur les includes de script pouvant être appelés par le client
Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client • Ancienne description brève : Protection de la vie privée sur les includes de script pouvant être appelés par le client
Exiger la vérification de l'ACL AJAXGlideRecord [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger la vérification de l'ACL AJAXGlideRecord • Ancienne description courte : Activation de la vérification de l'ACL de AJAXGlideRecord
Appliquer le bac à sable pour les scripts générés par le client [Mise à jour dans Securty Center 1.3]	• Nouvelle description brève : Appliquer le bac à sable pour les scripts générés par le client • Ancienne description brève : Bac à sable pour les scripts générés par le client
Restreindre les types MIME chargés [Mise à jour dans Securty Center 1.3]	• Nouvelle description brève : Restreindre les types MIME chargés* Description brève • Ancienne description brève : Restriction de type MIME de téléchargement, LA VALEUR PAR DÉFAUT EST PASSÉE DE VRAI À FAUX.
Activer les ACL d'application administrateur incluses dans le champ d'application [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer les ACL d'application administrateur incluses dans le champ d'application • Ancienne description brève : Administrer les ACL d'application d'administration incluses dans le champ d'application

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Activer le jeton anti-CSRF [nouveau dans Security Center 1.3 et supprimé dans la version 1.5]	• Nouvelle description brève : Activer le jeton anti-CSRF • Ancienne description brève : Jeton anti-CSRF
Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Implémenter X-Frame-Options : en-tête de sécurité SAMEORIGIN • Ancienne description brève : X-Frame-Options : SAMEORIGIN
Exiger le brouillage de l'interface utilisateur de l'application mobile [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger le brouillage de l'interface utilisateur de l'application mobile • Ancienne description courte : brouillage de l'interface utilisateur d'une application mobile
Refuser par défaut en cas d'ACL vides [mis à jour dans Securty Center 1.3]	• Nouvelle description brève : Refuser par défaut en cas d'ACL vides • Ancienne description brève : Refus par défaut du Gestionnaire de sécurité
Valider le type de contenu SOAP [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Valider le type de contenu SOAP • Ancienne description brève : vérification du type de contenu SOAP
Appliquer la sécurité stricte des requêtes SOAP [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Appliquer la sécurité stricte des requêtes SOAP • Ancienne description brève : Sécurité stricte des requêtes SOAP
Activer la récupération de compte [mis à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Activer la récupération de compte • Ancienne description brève : Récupération de compte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable • Ancienne description courte : Validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable
Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » [Mise à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » • Ancienne description brève : Appliquer Séparation de domaine
Définir les types MIME téléchargeables restreints [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Restreindre les types MIME téléchargeables • Ancienne description courte : Liste de refus des types de Mime téléchargeables
Types MIME téléchargeables	• Nouvelle description brève : Définir les types MIME téléchargeables restreints • Ancienne description brève : Types de MIME téléchargeables
Script Jelly d'échappement [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Script Jelly d'échappement • Ancienne description courte : Escape Jelly
HTML d'échappement dans les vues de listes [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : HTML d'échappement dans les vues de listes • Ancienne description brève : HTML d'échappement
Scripts d'échappement dans le bloc-notes [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Scripts d'échappement dans le bloc-notes • Ancienne description courte : Échapper au bloc-notes
Balisage XML d'échappement [mis à jour dans Security Center 1.3]	• Nouvelle description brève : Balisage XML d'échappement • Ancienne description brève : XML d'échappement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Exiger le brouillage de l'interface utilisateur de l'application mobile classique [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : exiger le brouillage de l'interface utilisateur de l'application mobile classique • Ancienne description courte : Obfuscation classique de l'interface utilisateur d'une application mobile
Désactiver l'accès public aux favoris	• Nouvelle description brève : Désactiver l'accès public aux favoris • Ancienne description brève : Accès public aux favoris
Appliquer la sécurité stricte des cookies de session [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Appliquer la sécurité stricte des cookies de session • Ancienne description brève : Cookies de session sécurisés
Désactiver le code HTML intégré [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Désactiver le code HTML intégré • Ancienne description courte : Code HTML intégré
Désactiver les balises JavaScript dans le HTML intégré [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Désactiver les balises JavaScript dans le HTML intégré • Ancienne description brève : Autoriser les balises Javascript dans le HTML intégré
Minimiser la durée du délai d'expiration d'activité de la session [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la durée du délai d'expiration d'activité de la session • Ancienne description brève : Délai d'activité de la session
Restreindre les types de fichiers téléchargeables dans le contenu statique [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Restreindre les types de fichiers téléchargeables dans le contenu statique • Ancienne description brève : Restrictions de téléchargement des types de fichiers provenant d'un contenu statique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Minimiser la durée du délai d’expiration de la fenêtre de session [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la durée du délai d’expiration de la fenêtre de la session • Ancienne description brève : Délai d’expiration de la fenêtre de session
Minimiser la durée du délai absolu d’expiration de la session [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la durée du délai absolu d’expiration de la session • Ancienne description brève : Délai absolu de la session
Maximiser la durée du délai d’expiration de déverrouillage en cas d’échec de la connexion [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Maximiser la durée du délai d’expiration de déverrouillage en cas d’échec de la connexion • Ancienne description brève : Gestion du délai de déverrouillage en cas d’échec de la connexion
Restreindre les entités externes XML [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Restreindre les entités externes XML • Ancienne description brève : Liste d’autorisations d’URL pour validation d’entités XML
Minimiser le seuil d’expansion des entités [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser le seuil d’expansion des entités • Ancienne description brève : Définition du seuil d’expansion des entités
Minimiser la durée d’expiration de la demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la durée d’expiration de la demande de réinitialisation du mot de passe • Ancienne description brève : Expiration de la demande de réinitialisation du mot de passe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Minimiser le nombre maximal autorisé de tentatives de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser le nombre maximal autorisé de tentatives de demande de réinitialisation du mot de passe • Ancienne description courte : Tentatives maximales de demande de réinitialisation du mot de passe
Minimiser la durée de la fenêtre de tentatives maximales de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la durée de la fenêtre de tentatives maximales de demande de réinitialisation du mot de passe • Ancienne description courte : Fenêtre des tentatives maximales de demande de réinitialisation du mot de passe
Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe • Ancienne description brève : Fenêtre de nouvelle demande de demande de réinitialisation du mot de passe
Minimiser la durée de la fenêtre de succès de demande de réinitialisation du mot de passe [mis à jour dans Securty Center 1.3]	• Nouvelle description brève : Minimiser la durée de la fenêtre de succès de demande de réinitialisation du mot de passe • Ancienne description courte : Fenêtre de réussite de la demande de réinitialisation du mot de passe
Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe • Ancienne description courte : Fenêtre de déverrouillage de la demande de réinitialisation du mot de passe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Maximiser la complexité du SMS de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Maximiser la complexité du SMS de réinitialisation du mot de passe • Ancienne description brève : Complexité du SMS de réinitialisation du mot de passe
Minimiser la durée d'expiration du SMS de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser la durée d'expiration de SMS de réinitialisation du mot de passe • Ancienne description brève : Expiration du SMS de réinitialisation du mot de passe
Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour • Ancienne description brève : Réinitialisation du mot de passe Nombre maximal de SMS par jour
Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe • Ancienne description courte : Fenêtre de pause du SMS de réinitialisation du mot de passe
Activer la notification de code SMS pour l'inscription et la vérification [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Activer la notification du code SMS pour l'inscription et la vérification • Ancienne description brève : Notification du code SMS pour l'inscription et la vérification
Maximiser la durée du délai de vérification de la réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Maximiser la durée du délai de vérification de la réinitialisation du mot de passe • Ancienne description brève : Délai de vérification de la réinitialisation du mot de passe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Documentation	Mises à jour
Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe	• Nouvelle description brève : Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe • Ancienne description brève : Processus de réinitialisation du mot de passe/ notification de changement
Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes [Mise à jour dans Security Center 1.5]	• Nouvelle description brève : Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes • Ancienne description courte : Liste d'autorisation de domaines d'e-mails d'enregistrement d'utilisateurs externes
Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe [Mise à jour dans Security Center 1.3 et 1.5]	• Nouvelle description brève : Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe • Ancienne description brève : Expiration du lien d'Inscription de l'utilisateur externe
Restreindre les packages Java autorisés [Mise à jour dans Security Center 1.3]	• Nouvelle description brève : Restreindre les packages Java autorisés • Ancienne description brève : Liste d'autorisation de paquets Java

Paramètres de sécurisation renforcée supprimés pour la version de base de référence 4.0

Cette liste contient les paramètres de sécurisation renforcée qui ont été supprimés dans la Centre de sécurité version de base de référence 4.0.

- Appliquer les restrictions de périmètre de l'application
- Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe
- Valeur de l'en-tête HTTP du contrôle de cache
- Convertir les images des e-mails entrants en pièces jointes
- Activer le jeton anti-CSRF
- Appliquer le certificat de confiance
- Options de définition automatique du type de contenu

Paramètres de sécurisation renforcée supprimés pour la version de base de référence 2.0

Cette liste contient les paramètres de sécurisation renforcée qui ont été supprimés dans la Centre de sécurité version de base de référence 2.0.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activer la signature de code pour les données de configuration de l'application et les scripts
- Activer l'encrypteur Glide KMF
- Désactiver l'utilisation du chiffrement au niveau de l'instance
- Enregistrer tous les champs des requêtes HTTP sortantes

Contrôle d'accès

La catégorie de contrôle d'accès audite le processus de protection des ressources contre tout accès non autorisé en accordant et en refusant des demandes basées sur un modèle d'autorisation. Il s'agit notamment de s'assurer qu'une entité accédant à une ressource détient des informations d'identification valides pour ce faire, de créer et de protéger un ensemble bien défini de rôles ou d'autorisations et de s'assurer que les contrôles des rôles ou des autorisations sont protégés contre la relecture et l'altération.

Les contrôles d'accès déterminent si l'accès à une ressource particulière doit être accordé ou refusé. L'accès aux ressources n'est autorisé qu'aux utilisateurs autorisés à les utiliser.

Temps de validation du jeton anti-CSRF [Nouveau dans Security Center 1.3]

La `glide.security.csrf_previous.time_limit` propriété spécifie le délai en secondes avant l'expiration d'un jeton de sécurité.

Lorsqu'une session utilisateur expire, le jeton de sécurité expire avec elle, sauf si la propriété **Autoriser la réutilisation des jetons expirés est autorisée** est activée et qu'elle se trouve dans la période décrite dans cette propriété. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête intersite.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.csrf_previous.time_limit`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	86400 secondes ou 1 jour
Valeur par défaut	86400 secondes ou 1 jour
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée, la validation du jeton utilisée pour éviter les attaques de contrefaçon de requête intersite est désactivée.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété détermine la durée en secondes pendant laquelle un jeton de sécurité reste valide. Le jeton de sécurité expire à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	l'expiration de la session utilisateur, sauf si **l'option Autoriser la réutilisation de la propriété des jetons expirés** est activée et si le jeton se trouve dans la période spécifiée dans cette propriété. Ce jeton empêche les attaques de contrefaçon de requête de site à site. Elle a une valeur par défaut de 86 400 secondes ou 1 jour.

Appliquer Séparation de domaine sur les champs de type « remontée pas à pas » [Mise à jour dans Security Center 1.3 et 1.5]

La `glide.sys.domain.include_domain_condition_on_join` propriété contrôle si des conditions distinctes par domaine sont attribuées ou non à des requêtes de jointure afin de s'assurer qu'elles appliquent la fonctionnalité de séparation de domaine pour les champs de remontée pas à pas.

Cette `glide.sys.domain.include_domain_condition_on_join` propriété contrôle si des conditions distinctes par domaine sont attribuées ou non à des requêtes de jointure afin de s'assurer qu'elles appliquent la fonctionnalité de Séparation de domaine pour les champs de remontée pas à pas. Si `glide.sys.domain.include_domain_condition_on_join` elle n'est pas définie sur la valeur recommandée vrai sur une instance utilisant la séparation de domaine, des informations sensibles qui ne doivent pas être partagées avec un domaine spécifique peuvent alors être divulguées.

Remarque :
Lorsque le module d'extension Séparation de domaine est installé, un enregistrement sys_properties de cette propriété est installé avec sa valeur définie sur **vrai**, qui est sa valeur autre que la valeur par défaut. Dans le cas contraire, dans le système de base sans séparation de domaine installée, l'enregistrement de propriété n'existera pas et sa valeur autre que celle par défaut sera conservée.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sys.domain.include_domain_condition_on_join`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	Vrai, lorsque Séparation de domaine est installée, sinon la propriété n'existera pas.
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Objectif	Contrôle si des conditions distinctes par domaine sont attribuées ou non à des requêtes de jointure afin de s'assurer qu'elles appliquent la fonctionnalité de Séparation de domaine pour les champs de remontée pas à pas.
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails **du risque** de sécurité : si *glide.sys.domain.include_domain_condition_on_join* elle n'est pas définie sur la valeur recommandée vrai, des informations sensibles qui ne doivent pas être partagées avec un domaine spécifique peuvent être divulguées.
Références	Domain Separation pour les fournisseurs de services

Activer les ACL d'application administrateur incluses dans le champ d'application [Mise à jour dans Security Center 1.3]

Le *glide.security.scoped_administration.honor_global_acl* détermine si une application d'administration d'application peut hériter des règles de liste de contrôle d'accès global (ACL).

Cette propriété est particulièrement utile lorsqu'aucune ACL d'application d'administration incluse dans le périmètre n'est définie pour le périmètre de l'enregistrement.

Définissez la valeur *glide.security.scoped_administration.honor_global_acl* sur vrai pour empêcher un utilisateur ayant peu de privilèges et ayant des autorisations dans l'application d'accéder potentiellement à des enregistrements sensibles.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.security.scoped_administration.honor_global_acl*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Contrôle la règle d'accès ACL dans l'application d'administration incluse dans le périmètre.
Valeur recommandée	Vrai
Valeur par défaut	Vrai
Type de configuration	Booléen
Risque de sécurité	(Faible) Lorsque la valeur de la propriété est définie sur vrai et qu'aucune ACL d'application d'administration incluse dans le périmètre n'est définie pour le périmètre de l'enregistrement, les ACL globales sont honorées. Si la valeur est définie sur faux, alors qu'aucune ACL d'application administrateur incluse dans le périmètre n'est définie pour le champ d'application de l'enregistrement, les vérifications ACL sont ignorées.
Cote de risque de sécurité	3.8
Références	Access control rules in application administration apps

Pour en savoir plus sur l'activation d'un module d'extension, consultez Activate a plugin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer les règles de requête de gestion des commandes de travaux pour les organisations de services [Nouveau dans Security Center 1.5]

Utilisez la *sn_fsm.use_query_rules* propriété pour appliquer des règles et des filtres aux tables Gestion des services sur site.

Lorsque la *sn_fsm.use_query_rules* propriété est définie sur vrai, les règles et filtres de la table sn_query_rule sont utilisés pour déterminer l'accès en lecture des utilisateurs authentifiés aux tables Gestion des services sur site. Pour ce faire, il utilise des règles métier de requête et des ACL en lecture. Lorsque cette propriété est définie sur faux, les enregistrements ne sont pas filtrés en fonction des règles de requête. Les règles métier des requêtes ajoutent des validations de sécurité supplémentaires lorsqu'elles sont activées sur cette propriété, et elles filtrent les enregistrements des agents, des qualificateurs et des répartiteurs en fonction de leur territoire affecté ou de leur appartenance au territoire. Cela met en œuvre le principe du moindre privilège lors de la lecture des documents.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_fsm.use_query_rules*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : lorsque cette propriété est définie sur vrai, les règles et les filtres de sn_query_rule seront utilisés pour déterminer l'accès en lecture aux tables Gestion des services sur site en implémentant le principe du moindre privilège. Lorsqu'ils sont définis sur faux, les enregistrements ne sont pas filtrés en fonction des règles métier de requête et peuvent présenter un risque accru d'exposition des données des tables Gestion des services sur site.
Dépendances et prérequis	Aucun
Impact fonctionnel	Quand la valeur est définie sur vrai, les règles/filtres de sn_query_rule table seront utilisés pour déterminer l'accès en lecture aux tables liées à la gestion des services sur site. Par exemple, Commande de travaux (WO) et Table de commande de travaux (WOT) à l'utilisateur connecté via les règles métier des requêtes et les ACL en lecture. Si la valeur est définie sur false, les enregistrements ne sont pas filtrés en fonction des règles de requête.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	L'activation de cette propriété sécurise les données, et toutes les données (wm_task et wm_order) ne seront pas visibles par leurs utilisateurs.
Références	Field Service Management reference

Accès en bloc pour les développeurs délégués

Cette configuration affecte l'accès aux développeurs délégués qui mettent à jour les rôles d'utilisateur via le script. Lorsque la configuration est conforme, le développeur n'est pas en mesure de mettre à jour ou d'insérer des enregistrements dans la table de sys_user_has_role sans disposer également du rôle user_admin.

La valeur de cette propriété détermine si un développeur délégué est autorisé à accorder ou à recevoir un accès inattendu aux fonctionnalités de l'instance. Lorsque la propriété contient des rôles, seuls ces rôles peuvent exécuter des modules de script.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.sys.security.delegateddev.block_grant_roles`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	La valeur de cette propriété détermine si un développeur délégué est autorisé à accorder ou à recevoir un accès inattendu aux fonctionnalités de l'instance.
Type	interrupteur à bascule
Valeur par défaut	VRAI
Valeur recommandée	VRAI
Dépendances de Sécurité	aucun
Cote de risque de sécurité	6.7
Impact fonctionnel	(Élevé) Lorsqu'un utilisateur disposant du rôle delegated_developer tente de modifier un enregistrement dans la table sys_user_has_role, cette propriété active des contrôles de sécurité supplémentaires par rapport à l'opération. Les vérifications de sécurité supplémentaires valident que l'utilisateur a reçu le rôle user_admin s'il tente de créer ou de mettre à jour la table sys_user_has_role. S'ils n'ont pas le rôle user_admin, l'accès leur sera refusé. Lorsque la propriété a la valeur false, ces vérifications supplémentaires ne sont pas validées.
Risque de sécurité	(Modéré) Sans autorisation appropriée, des utilisateurs non autorisés peuvent accéder à du contenu/des données sensibles sur l'instance.
Références	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Bloquer les jetons anti-CSRF expirés [mis à jour dans Security Center 1.5]

Bloquez les jetons CSRF expirés pour éviter les attaques de contrefaçon de requête de site à site.

Vue d'ensemble

Les falsifications de requêtes intersites sont un type d'exploitation malveillante par lequel des commandes non autorisées sont exécutées pour le compte d'un utilisateur authentifié.

Détails de la configuration

Attribut	Description
Vue d'ensemble	Contrôle l'utilisation d'un jeton de sécurité expiré pour identifier et valider les demandes entrantes. Définissez la valeur **sur faux** pour empêcher un jeton précédemment expiré de valider une demande entrante.
Nom de la configuration	`glide.security.csrf_previous.allow`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	**false**
Valeur par défaut	**true**
Catégorie	Contrôle d'accès
Risque de sécurité	**Score de gravité** : 6,5
	Évaluation de gravité par score CVSS : moyenne
	Détails du risque de sécurité : applique un mécanisme anti-CSRF fort pour protéger les fonctionnalités authentifiées, et un mécanisme anti-automatisation ou anti-CSRF efficace protège les fonctionnalités non authentifiées.
Dépendances et prérequis	Aucun
Références	Activer le jeton anti-CSRF [nouveau dans Security Center 1.3 et supprimé dans la version 1.5], falsification de requête intersite .

Vérifier les conditions de l'action de l'interface utilisateur avant son exécution

Utilisez cette propriété pour activer la vérification des conditions des actions d'interface utilisateur dans les `glide.security.strict.actions` formulaires et les listes avant leur exécution. Lorsque vous définissez cette propriété sur vrai, elle ajoute une couche supplémentaire de validation sur la table des actions d'interface utilisateur avant qu'elles ne soient exécutées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.strict.actions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour garantir une validation supplémentaire sur la table, les actions d'interface utilisateur avant qu'elles ne soient exécutées.
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	3.3
Impact fonctionnel	(Faible) Cette correction ajoute seulement une couche supplémentaire de validation pour vérifier les actions d'interface utilisateur sur la table/page cible sur l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait pas y avoir d'impact ici.
Risque de sécurité	(Faible) La demande d'accès est toujours vérifiée lorsque des transactions ont lieu entre deux zones. Cette opération valide toutes les actions d'interface utilisateur avant que le formulaire ne s'affiche pour l'utilisateur final.
Références	Module d'extension de haute sécurité

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Configurer les rôles administrateur du groupe d'affectation de gestion des événements [Nouveau dans Security Center 1.5]

Utilisez la propriété pour définir les rôles autorisés à accéder administrateur au champ Groupe d'affectation dans les `evt_mgmt.connector_assignment_group_admin_roles` instances de connecteur.

La `evt_mgmt.connector_assignment_group_admin_roles` propriété contient une chaîne séparée par des virgules qui indique les noms de rôle qui ont un accès administrateur sur le champ Groupe d'affectation dans les instances de connecteur. La modification des rôles par défaut dans cette liste peut permettre à des utilisateurs non autorisés de modifier les intégrations d'événements sur l'instance. Pour empêcher tout accès non autorisé aux rôles, définissez `evt_mgmt.connector_assignment_group_admin_roles` la valeur admin,evt_mgmt_admin,sn_sow_srm.srm_admin. Examinez tous les rôles supplémentaires dans la chaîne de valeurs recommandées pour vous assurer que le rôle doit être inclus.

En savoir plus

Attribut	Description
Nom de la configuration	`evt_mgmt.connector_assignment_group_admin_roles`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	administrateur,evt_mgmt_admin,sn_sow_srm.srm_admin
Valeur par défaut	administrateur,evt_mgmt_admin,sn_sow_srm.srm_admin
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails du risque de sécurité : la modification des rôles par défaut peut permettre à des utilisateurs non autorisés de modifier les intégrations d'événements sur l'instance.
Dépendances et prérequis	Aucun
Références	Creating groups

Refuser l'accès interne aux rôles externes explicites [Mise à jour dans Security Center 1.5]

Plusieurs propriétés constituent ensemble la configuration du paramètre de sécurisation renforcée **de la liste de refus interne Activer les rôles explicites** . La `glide.security.explicit_roles.enable_internal_user_blacklist` propriété empêche d'affecter le rôle snc_internal à des utilisateurs externes et permet à la propriété d'affecter `glide.security.explicit_roles.internal_user_blacklist` le rôle snc_external.

Glide.security.explicit_roles.enable_internal_user_blacklist

Vous pouvez donner l'accès à votre instance à la fois aux utilisateurs internes et aux utilisateurs externes. Pour fournir une sécurité accrue, chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse faire la distinction entre les utilisateurs internes et externes.

Définissez la `glide.security.explicit_roles.enable_internal_user_blacklist` propriété sur la valeur recommandée, **vrai** , pour permettre d'affecter le rôle snc_external.

Définissez la valeur sur **faux** pour désactiver la possibilité d'affecter le rôle snc_external. Le rôle snc_internal par défaut sera attribué à tous les utilisateurs

Remarque :
Les instances sans rôles explicites installés ne sont pas affectées. À partir de la version Paris, les nouvelles installations de rôles explicites obtiennent la propriété avec la valeur par défaut true.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.explicit_roles.enable_internal_user_blackl`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Contrôle d'accès
Objectif	Permet l'affectation de classes d'utilisateurs spécifiées au rôle snc_external au lieu du rôle snc_internal.
Valeur recommandée	Vrai
Valeur par défaut	Vrai
Type de configuration	Booléen
Risque de sécurité	(Modéré) La désactivation de la propriété peut entraîner une affectation de rôle par défaut inappropriée.
Cote de risque de sécurité	5.4
Références	Rôles explicites dans CSM ,

Glide.security.explicit_roles.internal_user_blacklist

La `glide.security.explicit_roles.internal_user_blacklist` valeur détermine quelles classes d'utilisateurs (tables qui étendent sys_user) doivent être affectées au rôle snc_external au lieu du rôle snc_internal. La valeur par défaut csm_consumer_user customer_contact est définie pour s'aligner sur les cas d'utilisation dans les modules d'extension Customer Service Management.

La valeur de la propriété ne doit être modifiée que s'il existe des classes d'utilisateurs supplémentaires ou différentes auxquelles le rôle snc_external par défaut, au lieu du rôle snc_internal doit être affecté. Contactez l'assistance pour modifier ces valeurs.

Attribut	Description
Nom de la propriété	`glide.security.explicit_roles.internal_user_blacklist`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Permet l'affectation du rôle snc_external affecté par défaut, au lieu du rôle snc_internal.
Valeur recommandée	`csm_consumer_user`, `customer_contact`
Type de configuration	Chaîne
Risque de sécurité	(Modéré) La désactivation de la propriété peut entraîner une affectation de rôle par défaut inappropriée.
Cote de risque de sécurité	5.4
Références	Explicit Roles, corriger les affectations de rôles d'utilisateur externe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Refuser l'accès non autorisé aux éléments demandés

La `glide.sc.req_for.roles.default` propriété définit un comportement par défaut pour l'API `retrieveAddress` .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette propriété n'est fonctionnelle que lorsqu'elle `glide.sc.req_for.roles` n'a pas de valeurs. Si `glide.sc.req_for.roles` a des valeurs, alors cette propriété n'a aucune signification et les utilisateurs ayant uniquement des rôles définis ont accès à l'API.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sc.req_for.roles.default`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Lorsqu'aucun rôle n'est indiqué dans la propriété, le script include Client pouvant être appelé `ScriptServiceCatalogGetLocation` peut être appelé par n'importe quel utilisateur connecté sans privilèges et peut récupérer l'adresse de tous les autres utilisateurs du système. Cette propriété protège cette API afin qu'elle puisse être exposée aux utilisateurs non privilégiés.
Valeur recommandée	refuser
Valeur par défaut	refuser
Type de configuration	Liste de choix (autoriser | refuser)
Risque de sécurité	(Modéré) Si `glide.sc.req_for.roles.default` elle n'est pas définie sur la valeur recommandée de **refus** (autoriser) et que la valeur est `glide.sc.req_for.roles` vide, tout utilisateur peut demander des éléments pour d'autres utilisateurs, ce qui autorise un accès non autorisé aux ressources.
Références	Includes de script pouvant être appelés par le client

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le jeton anti-CSRF [nouveau dans Security Center 1.3 et supprimé dans la version 1.5]

Utilisez la propriété pour garantir l'utilisation `glide.security.use_csrf_token` d'un jeton de sécurité pour identifier et valide les demandes entrantes, qui sont ensuite utilisées pour prévenir ces attaques.

La falsification de requête inter-site (CSRF) est une attaque qui oblige un utilisateur final à exécuter des actions indésirables sur une application Web dans laquelle il est actuellement authentifié. Les attaques CSRF ciblent spécifiquement les demandes de changement d'état, et non le vol de données, car l'attaquant n'a aucun moyen de voir la réponse à la requête falsifiée.

Les propriétés suivantes peuvent être activées pour les contrôles supplémentaires sur le jeton CSRF :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *glide.security.csrf_previous.time_limit*
- *glide.security.csrf_previous.allow*
- *glide.security.csrf.strict.validation.mode*

En savoir plus

Attribut	Description
Nom de la propriété	*glide.security.use_csrf_token*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour protéger l'application contre une éventuelle attaque CSRF.
Cote de risque de sécurité	8.1
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Impact fonctionnel	(Faible) Cette remédiation active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. Chaque demande d'écriture contient un jeton CSRF (c'est-à-dire un ID de validation/CSRF lié à la session utilisateur). Lorsque la session utilisateur expire, le jeton de sécurité expire avec elle.
Risque de sécurité	(Élevé) La falsification des requêtes intersites constitue un risque de sécurité important qui porte atteinte à l'intégrité des données de l'instance. Un attaquant peut lancer l'attaque CSRF en abusant de la confiance d'un utilisateur d'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une requête mal formée au nom de l'attaquant de l'instance.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

S'assurer que les ACL des tables d'archivage sont vérifiées [Nouveau dans Security Center 1.3]

La *glide.security.enable_archive_table_acls* propriété contrôle si les listes de contrôle d'accès (ACL) de la table d'origine, la table à partir de laquelle la table d'archivage a été créée, sont évaluées comme fausses.

La *glide.security.enable_archive_table_acls* propriété ne doit pas être définie sur false car les ACL de la table d'origine seront évaluées quelle que soit sa valeur. Vous pouvez éviter d'ajouter des ACL supplémentaires pour une table d'archivage en ne les ajoutant pas.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.security.enable_archive_table_acls*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3 • Score CVSS : faible • Détails du risque de sécurité : si la propriété est définie sur faux, les ACL ajoutées aux tables archivées sont ignorées, ce qui est contre-intuitif et peut donc conduire à un contournement d'autorisation.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est définie sur true, toutes les ACL de lecture actives sur les tables d'archivage sont honorées. Si aucune ACL de lecture active n'existe ou si la propriété est définie sur faux, la table d'origine (table à partir de laquelle les données sont archivées) s'appliquera à la table d'archivage. **Remarque :** Seuls les ACL de lecture sont pris en charge sur les tables d'archivage. D'autres opérations sur les tables d'archivage sont pilotées en interne par un gestionnaire d'accès.

Activer le module d'extension de sécurité contextuelle [Mise à jour dans Security Center 1.3]

Activez le module d'extension Contextual Security (*com.glide.role_management*) pour activer la sécurité contextuelle, qui sécurise un enregistrement/des informations utilisant la création, la lecture, l'écriture et la suppression d'une fonctionnalité.

Une fois installé et activé, les rôles du dictionnaire (créés par Simple Security Manager) ne sont plus testés. Au lieu de cela, le Now Platform recherche des règles ACL sur les champs et les tables. Il sécurise les données à l'aide de règles ACL au lieu des règles de dictionnaire traditionnelles basées sur les rôles implémentées par un simple gestionnaire de sécurité. Même si vous configurez le formulaire de dictionnaire et ajoutez des rôles à une entrée de dictionnaire, aucun changement dans les droits ne se produit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
ID de module d'extension	`com.glide.role_management`
Type de configuration	Définition du système > Modules d'extension
Catégorie	Contrôle d'accès
Objectif	Contrairement au gestionnaire de sécurité simple, le gestionnaire de sécurité contextuelle connaît la hiérarchie de la table système. Vous pouvez potentiellement avoir des règles de sécurité différentes pour un champ en fonction de l'endroit où il apparaît dans la hiérarchie.
Valeur recommandée	Actif
Valeur par défaut	Il n'y a pas de valeur par défaut, car il s'agit d'un module d'extension et non d'une propriété Glide.
Cote de risque de sécurité	8.1
Impact fonctionnel	(Moyen) Ce rattrapage applique le niveau fonctionnel des contrôles d'accès, ce qui permettrait à l'application de déterminer les restrictions d'accès en se basant uniquement sur la table ACL.
Risque de sécurité	(Élevé) Les contrôles d'accès au niveau fonctionnel doivent être appliqués du côté du serveur avant d'exécuter des opérations CRUD, afin de garantir le niveau d'accès approprié aux utilisateurs de l'instance.
Références	Gestionnaire de sécurité contextuelle

Appliquer le Playbook pour les licences et les autorisations dans le champ d'application de sécurité [Nouveau dans Security Center 1.5]

Utilisez cette propriété pour déterminer si seules les listes de contrôle d'accès (ACL) du module d'extension Licence et autorisation seront utilisées pour déterminer l'accès au champ d'application ou si les ACL de tous les périmètres seront prises en compte.

Lorsque la `glide.enforce_security_scope.sn_gsm_lic_prmt` propriété est définie sur la valeur recommandée vrai, seules les ACL du module d'extension Licence et autorisation sont utilisées pour déterminer l'accès au champ d'application. Lorsque ce paramètre est configuré sur faux, les données de playbooks de licence et d'autorisation dans les tables principales du périmètre sont exposées, car les ACL de tous les périmètres ont l'accès. Pour réduire l'exposition des données, définissez sur `glide.enforce_security_scope.sn_gsm_lic_prmt` la valeur recommandée vrai.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_gsm_lic_prmt`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : la configuration de ce paramètre sur la valeur recommandée vrai sécurise les données de Licence et autorisation dans les tables principales du périmètre en prenant en compte uniquement les ACL à partir du *sn_gsm_lic_prmt* périmètre pour accorder l'accès. Si vous définissez ceci sur faux, les données de Playbooks de licence et d'autorisation sont exposées dans les tables principales du périmètre en tenant compte des ACL de tous les périmètres pour accorder l'accès. Par exemple, l'administrateur informatique peut accéder aux données de Licence et autorisation lorsque ce paramètre est défini sur faux.
Dépendances et prérequis	Aucun
Références	• Using License and Permit Playbook • Application scope

Appliquer le champ d'application de sécurité pour l'Espace de travail d'agent pour la gestion des tickets RH [Nouveau dans Security Center 1.5]

Configurez le module d'extension Espace de travail d'agent pour la gestion des tickets RH de sorte que les données des tables principales du périmètre ne soient accessibles qu'aux utilisateurs disposant des autorisations appropriées, en appliquant le principe du moindre privilège.

Lorsque le *glide.enforce_security_scope.sn_hr_agent_ws* module d'extension est configuré sur la valeur recommandée vrai, seules les listes de contrôle d'accès (ACL) du module d'extension Espace de travail d'agent pour la gestion des tickets RH sont utilisées pour déterminer l'accès à une ressource. Lorsque ce paramètre est défini sur faux, les données d'Espace de travail d'agent pour la gestion des tickets RH dans les tables principales du périmètre sont exposées, car l'accès est accordé aux ACL de tous les périmètres.Par exemple, un administrateur informatique peut accéder aux données d'Espace de travail d'agent pour la gestion des tickets RH lorsque ce paramètre est défini sur faux. Pour éviter que cela ne se produise, définissez *glide.enforce_security_scope.sn_hr_agent_ws* sur la valeur recommandée vrai qui garantit que le principe de moindre privilège existe, car les utilisateurs ne peuvent accéder qu'aux ressources pour lesquelles ils ont une autorisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_hr_agent_ws`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : Si vous configurez ce paramètre sur faux, les données d'Agent Workspace for HR Case Management dans les tables principales du périmètre sont exposées, car l'accès est accordé aux ACL de tous les périmètres.
Dépendances et prérequis	Agent Workspace for HR Case Management
Impact fonctionnel	La configuration de ce paramètre sur vrai applique l'exécution des ACL globales pour une table, si les ACL incluses dans le champ d'application n'existent pas pour celle-ci.
Références	• https://owasp.org/www-project-proactive-controls/#div-numbering • Add a component to Agent Workspace

Appliquer la validation stricte du jeton CSRF

Utilisez la propriété pour activer la `glide.security.csrf.strict.validation.mode` validation stricte du jeton CSRF. Si le jeton CSRF ne correspond pas, une nouvelle soumission de la demande est impossible.

La `glide.security.csrf.strict.validation.mode` propriété active la validation stricte du jeton CSRF qui empêche la réutilisation des jetons CSRF. Si cette propriété n'est pas définie sur la valeur recommandée, vrai, les jetons CSRF peuvent être réutilisés, ce qui ouvre la porte à des attaques CSRF.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.csrf.strict.validation.mode`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour appliquer une validation stricte du jeton CSRF et empêcher sa réutilisation.
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	(Moyen) La falsification des requêtes intersites constitue un risque de sécurité important qui porte atteinte à l'intégrité des données de l'instance. Un attaquant peut lancer l'attaque CSRF sur n'importe quel utilisateur d'instance en abusant de la confiance de l'utilisateur de l'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une requête mal formée à l'instance au nom de l'attaquant.
Impact fonctionnel	(Moyen) Cette remédiation active une étape de validation supplémentaire avant que l'utilisateur d'instance n'envoie une demande d'écriture à l'instance. Il vérifie si le jeton CSRF actuel a été utilisé précédemment. Si c'est le cas, cela empêche la soumission d'autres demandes d'écriture.
Risque de sécurité	(Moyen) La falsification des requêtes intersites constitue un risque de sécurité important qui porte atteinte à l'intégrité des données de l'instance. Un attaquant peut lancer l'attaque CSRF sur n'importe quel utilisateur d'instance en abusant de la confiance de l'utilisateur de l'instance. À l'aide d'attaques d'ingénierie sociale, un utilisateur peut soumettre une requête mal formée à l'instance au nom de l'attaquant.

Retournez à Configurer et charger votre clé fournie par le client pour charger votre clé enveloppée.

Restreindre l'accès en lecture des développeurs délégués [Mise à jour dans Security Center 1.3]

Si `com.glide.dd_allow_global_access_tables` elle ne contient pas la valeur recommandée de wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget et sp_page, ces tables peuvent être lues par un développeur délégué. Cela pourrait permettre au développeur délégué d'accéder en lecture à des informations sensibles.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.dd_allow_global_access_tables`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget sp_page

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur par défaut	wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget sp_page
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails des risques de sécurité : assurez-vous que *com.glide.dd_allow_global_access_tables* les options sont définies sur wf_activity, wf_activity_definition, wf_workflow, wf_workflow_version, sp_portal, sp_widget sp_page.

Désactiver les e-mails entrants pour les utilisateurs bloqués

Utilisez la propriété pour contrôler Inbound *glide.pop3.process_locked_out* Email Actions pour les utilisateurs actifs verrouillés.

Définissez cette propriété sur **faux** pour désactiver les e-mails entrants pour les utilisateurs bloqués.

Remarque :
Réfléchissez aux implications en matière de sécurité de l'autorisation des utilisateurs de domaines non approuvés, et aux raisons pour lesquelles ils ont été bloqués, avant d'autoriser les e-mails de ces domaines à déclencher des actions sur e-mail entrant.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.pop3.process_locked_out*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Cette propriété contrôle Inbound Email Actions pour les utilisateurs bloqués.
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Risque de sécurité	(Élevé) Lorsque vous définissez cette propriété sur **vrai**, il peut y avoir une divulgation d'informations car les e-mails entrants seraient reçus par des utilisateurs ayant des comptes bloqués.
Cote de risque de sécurité	7.5

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Double vérification des transactions entrantes

Utilisez la propriété pour activer la double vérification de la sécurité sur les transactions entrantes lors de la *glide.security.strict.updates* soumission du formulaire. Lorsque

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vous définissez cette propriété sur **true**, elle ajoute une couche supplémentaire de validation de table avant qu'un formulaire ne s'affiche dans le navigateur.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.security.strict.updates`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour assurer une couche supplémentaire de vérification des autorisations utilisateur avant de présenter le formulaire dans le navigateur.
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	(Faible) Cette correction ajoute une couche supplémentaire de validation pour vérifier les autorisations utilisateur sur la table/page cible sur l'instance. Tant que les contrôles d'accès sont définis de manière appropriée sur l'instance client, il ne devrait y avoir aucun impact.
Risque de sécurité	(Élevé) Vous devez toujours vérifier la demande d'accès lorsque des transactions ont lieu entre deux zones. Cette opération vérifie les autorisations lorsque le formulaire est demandé et avant que le rendu du formulaire ne se produise.
Références	Propriétés des paramètres de sécurité

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer les ACL pour contrôler les détails du profil en direct

Utilisez la propriété pour indiquer si un utilisateur doit être en mesure d'afficher tous les champs de détail, tels que le nom de l'entreprise `glide.live_profile.details` et les numéros de téléphone, dans un profil actif.

Selon le paramètre de la `glide.live_profile.details` propriété, les événements suivants se produisent :

- Si la valeur est définie sur Afficher, l'accès aux informations de profil actif est accordé, quelles que soient les ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur ACL, l'accès aux informations de profil actif est restreint, conformément aux ACL créées pour le profil d'utilisateur.
- Si la valeur est définie sur Masquer, l'accès aux informations de profil actif est restreint, quelles que soient les ACL créées pour le profil d'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.live_profile.details`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	L'objectif est de permettre uniquement aux utilisateurs autorisés d'accéder aux détails d'un profil actif (tels que le nom de la société, les numéros de téléphone)
Type de données	liste de choix
Valeur recommandée	ACL
Valeur par défaut	ACL
Cote de risque de sécurité	4.3
Impact fonctionnel	(Moyen) Si la propriété n'est pas activée, les utilisateurs non autorisés peuvent accéder aux détails du profil actif de tous les autres utilisateurs.
Risque de sécurité	(Modéré) Les demandes d'API doivent toujours respecter les ACL de table. Une restriction doit être appliquée pour empêcher les utilisateurs non autorisés d'accéder aux détails d'un profil actif.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer les ACL de l'affichage du rapport

Gérez une vérification de report_view ACL des rapports publiés.

Utilisez cette`glide.report.report_view.check_published` propriété pour gérer une vérification de report_view ACL pour les rapports publiés. Si la propriété n'est pas définie sur la valeur recommandée **vrai**, la vérification des ACL report_view pour les rapports publiés est désactivée.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.report.report_view.check_published`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : élevé • Score CVSS : 7,5 • Détails des risques de sécurité : si la propriété est définie sur **true**, la vérification des ACL report_view pour les rapports publiés est désactivée.
Dépendances et prérequis	Aucun

Activer la liste des URL autorisées pour la communication cross-origin entre iFrame

Utilisez la propriété pour activer la `glide.ui.concourse.onmessage_enforce_same_origin` communication d'origine croisée entre les iframes.

OpenFrame ne peut traiter que les messages provenant de domaines de confiance spécifiés dans la `glide.ui.concourse.onmessage_enforce_same_origin_whitelist` propriété. Pour plus d'informations, consultez Spécifier la liste d'autorisation UTL pour la communication cross-origin entre iframes.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.concourse.onmessage_enforce_same_origin`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Catégorie	Contrôle d'accès
Objectif	Activer la liste d'inclusion des domaines de confiance, afin qu'ils puissent communiquer entre les iframes pour openframe.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	4.2
Impact fonctionnel	(Moyen) Si vous n'incluez pas les domaines prévus, la possibilité d'intégrer d'autres pages dans Now Platform les instances peut être limitée.
Risque de sécurité	(Élevé) Si une page Web contient des gestionnaires d'événements qui n'effectuent pas une validation d'origine appropriée, une page Web, ou un script de n'importe quelle origine, peut communiquer avec elle. Il peut également lancer n'importe quelle fonctionnalité exécutée par le gestionnaire d'événements.
Références	Vue d'ensemble d'OpenFrame

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer les restrictions de périmètre de l'application [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour contrôler les autorisations des applications incluses dans le `glide.record.legacy_cross_scope_access_policy_in_script` périmètre.

Si la propriété est définie sur vrai, les applications incluses dans le `glide.record.legacy_cross_scope_access_policy_in_script` périmètre peuvent appeler des API qui ne doivent être disponibles que pour les applications globales. Cette propriété contourne les contrôles d'accès prévus pour la création et la mise à jour des développeurs pour ces applications incluses dans le périmètre.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.record.legacy_cross_scope_access_policy_in_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	vrai (lorsque la propriété n'existe pas dans la table sys_properties.)
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : si cette propriété n'est pas définie sur la valeur recommandée, les applications incluses dans le périmètre et les développeurs délégués pour ces applications peuvent créer et mettre à jour des enregistrements dans des tables globales telles que Incident.
Dépendances et prérequis	Aucun

Appliquer des règles de sécurité au partage de tableaux de bord [Nouveau dans Security Center 1.3]

Utilisez la `glide.cms.dashboards.sharing_with_secure_search` propriété pour contrôler si les utilisateurs peuvent partager des tableaux de bord.

Lorsque la propriété n'est pas définie sur **vrai**, les `glide.cms.dashboards.sharing_with_secure_search` utilisateurs peuvent partager des groupes et des rôles de tableau de bord auxquels ils n'ont pas accès. L'activation de cette propriété applique des listes de contrôle d'accès (ACL) lors de la recherche des tables sys_user, sys_user_role et sys_user_group pendant le processus de partage du tableau de bord. Le partage excessif d'un tableau de bord peut amener des utilisateurs, des groupes ou des rôles à accéder à des données qu'ils ne devraient pas avoir l'autorisation de consulter, ce qui peut compromettre les informations sensibles. Par conséquent, il est recommandé de le définir `glide.cms.dashboards.sharing_with_secure_search` sur vrai afin que les tableaux de bord ne soient partagés qu'avec les personnes disposant des autorisations appropriées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.cms.dashboards.sharing_with_secure_search`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée vrai, les listes de contrôle d'accès ne sont pas appliquées lors de la recherche dans les tables sys_user, sys_user_role et sys_user_group. Cela pourrait conduire à ce que les tableaux de bord soient partagés avec des utilisateurs non autorisés, exposant ainsi des informations sensibles.
Dépendances et prérequis	Aucun
Références	Access control
Impact fonctionnel	Cette propriété applique des règles de sécurité à la liste d'utilisateurs, de groupes d'utilisateurs et de rôles qui sont visibles lors du partage de tableaux de bord.

Appliquer la sécurité du champ d'application pour les services numériques du secteur public [Nouveau dans Security Center 1.3]

Utilisez la propriété pour contrôler la `glide.enforce_security_scope.sn_gsm` façon dont les données d'application de l'application Public Sector Digital Services sont accessibles.

L'application ServiceNow Services digitaux pour le secteur public vous permet de développer des applications pour le secteur public qui fournissent des services numériques aux citoyens, aux entreprises et aux agences.

Lorsqu'elle `glide.enforce_security_scope.sn_gsm` est définie sur faux, l'accès aux données de l'application dans les tables globales de l'application Public Sector Digital Services peut être accessible en fonction des listes de contrôle d'accès (ACL) de ces tables globales. Lorsque cette propriété est définie sur vrai, l'accès aux données résidant dans les tables globales est uniquement évalué en fonction des ACL expédiées directement dans l'application Public Sector Digital Services. Définir cette propriété sur faux peut entraîner la divulgation d'informations en raison d'ACL trop permissives.

Pour remédier à ce risque de sécurité, définissez sur `glide.enforce_security_scope.sn_gsm` vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_gsm`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : ne pas définir cette propriété sur la valeur recommandée peut entraîner la divulgation d'informations en raison d'ACL trop permissives.
Dépendances et prérequis	Aucun
Références	Configuring Public Sector Digital Services

Appliquer l'accès ACL inclus dans le champ d'application pour les informations request playbook [Nouveau dans Security Center 1.3]

Utilisez la propriété pour contrôler l'accès `glide.enforce_security_scope.sn_gsm_info_req` aux données du playbook pour la fonctionnalité Information Request Playbook.

L'application Information Request Playbook permet aux utilisateurs finaux du secteur public de soumettre et de suivre les demandes d'archives publiques et fournit aux agents gouvernementaux un processus prédéfini pour le traitement et la résolution de ces demandes. Si `glide.enforce_security_scope.sn_gsm_info_req` elle n'est pas définie sur vrai, un accès inattendu peut être accordé aux données du playbook pour l'application Information Request Playbooks. Définissez cette propriété sur vrai pour ne prendre en compte que les ACL du périmètre sn_gsm_info_req lors de l'octroi de l'accès.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enforce_security_scope.sn_gsm_info_req`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails des risques de sécurité : Si cette propriété est définie sur faux, les ACL de tous les périmètres sont prises en compte lors de l'octroi de l'accès aux données du playbook dans la table maître du périmètre. Cela exposerait les données du playbook de demande d'informations.
Dépendances et prérequis	Aucun
Références	• Using Information Request Playbook • Configure Information Requests service channel

Appliquer le privilège d'élévation stricte [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour contrôler si les `glide.security.strict_elevate_privilege` rôles marqués comme privilégiés doivent être élevés manuellement pour que les options du rôle soient attribuées à l'utilisateur.

Définissez cette propriété sur vrai pour ajouter une couche supplémentaire de validation de sécurité lorsqu'un utilisateur privilégié élève son rôle.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.strict_elevate_privilege`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,7 • Score CVSS : moyen • Détails du risque de sécurité : lorsque `glide.security.strict_elevate_privilege` cette option est définie sur faux, les rôles marqués comme privilégiés sont automatiquement élevés lors de la nouvelle session d'un utilisateur administrateur et n'ont pas besoin d'être élevés manuellement (à l'exception de security_admin).
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	Cette propriété exige strictement que les utilisateurs ayant le rôle administrateur élèvent les privilèges en cas de besoin.

Exiger la vérification de l'ACL AJAXGlideRecord [mis à jour dans Security Center 1.3]

Utilisez la propriété pour effectuer la validation de la règle de contrôle d'accès (ACL, Access Control Rule) lorsque l'accès `glide.script.secure.ajaxgliderecord` aux enregistrements côté serveur, tels que les tables, se fait grâce à des API GlideAjax à l'intérieur d'un script client.

À partir de scripts clients, il est possible d'interroger des données arbitraires sur le serveur à l'aide de l'attribut AJAXGlideRecord (GlideAjax -Client), en utilisant une syntaxe telle qu'un enregistrement Glide côté serveur. Il s'agit d'un outil puissant et utile dans de nombreux déploiements.

Si vous choisissez d'appliquer des listes de contrôle d'accès (ACL) aux appels d'API GlideAjax, vous ne pouvez interroger que les données auxquelles l'utilisateur actuellement connecté a accès. Par exemple, si un utilisateur ESS qui n'a pas les droits de lecture de la table cmn_location est connecté, tout appel d'API GlideAjax à cette table échouera.

Si le est en cours d'exécution sans vérification d'appel Now Platform GlideAjax ACL, une API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder autrement.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.script.secure.ajaxgliderecord`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Assurez-vous que les ACL de sécurité sont vérifiées et validées même lorsque l'accès aux enregistrements s'effectue via des API côté client.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	(Élevé) Cette remédiation applique la relation ACL avec les enregistrements côté serveur lorsque les demandes sont effectuées à l'aide des appels d'API AJAXGlideRecord. Si la configuration ACL n'est pas correctement configurée, il y a un impact potentiel. Pour plus de détails sur son impact et sur la façon de l'identifier, reportez-vous à l'article Audit et examen des transactions GlideRecord côté client (AJAXGlideRecord) [KB0550828] dans le HI Base de connaissances .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Élevé) Grâce aux scripts clients, il est possible d'interroger des données arbitraires du serveur via l'API GlideAjax. Impossible d'accéder aux ressources côté serveur sans autorisation appropriée, de sorte que l'utilisation de la validation ACL aide l'application à valider la demande en fonction de l'autorisation configurée.
Solution de contournement	Assurez-vous que les ACL appropriées sont créées pour les includes de script, les processeurs et les autres entités utilisées par une API GlideAjax (AJAXGlideRecord) afin qu'elle s'exécute sous l'autorisation appropriée. Implémentez des méthodes telles que `canRead ()`,`canWrite()`, `canCreate()` et `canDelete ()` pour effectuer l'autorisation utilisateur avant d'accéder aux enregistrements de table à l'aide de GlideRecord. Une autre méthode consiste à utiliser GlideRecordSecure. La classe est héritée du serveur GlideRecord qui effectue les mêmes fonctions que GlideRecord et applique également les ACL.
Références	Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client) Cette propriété appartient à la même famille de propriétés qui sécurisent et restreignent l'exécution de scripts provenant du client : • *`glide.script.use.sandbox`*: voir Bac à sable pour les scripts générés par le client. • *`glide.script.allow.ajaxevaluate`*: voir Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Appliquer les ACL au niveau des champs dans GlideRecordSandbox

Gérez les ACL au niveau des champs dans GlideRecordSandbox sur votre instance.

Utilisez lapropriété pour *`glide.sandbox.fields.check_acl`* appliquer des ACL au niveau des champs dans GlideRecordSandbox. Par exemple, cette propriété est appliquée lorsqu'un utilisateur peut fournir un script, comme dans *`sysparm_query`*. Si cette propriété n'est pas définie sur la valeur conseillée, **vrai**, les restrictions ACL peuvent être contournées, ce qui permet de compromettre les données sensibles, par exemple celles *`sys_user.user_password`* provenant d'un utilisateur non autorisé.

Avertissement :
La valeur de cette propriété est un aucun remplacement de base de données. Il ne peut pas être modifié ou remplacé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sandbox.fields.check_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur **faux** permet de contourner les restrictions ACL, ce qui pourrait exposer des données sensibles.
Dépendances et prérequis	Aucun

Appliquer l'utilisation d'alias d'informations d'identification [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Découvrez comment sécuriser vos informations d'identification contre toute utilisation non autorisée en configurant la propriété Serveur MID.

Le serveur MID (Management, Instrumentation, and Discovery) est une application Java qui s'exécute en tant que service Windows ou démon UNIX sur votre réseau local. Les propriétés du serveur MID sont répertoriées dans la table [ecc_agent_property]. Vous pouvez y accéder dans votre instance en accédant à **Serveur MID** > **Propriétés**. Les alias d'informations d'identification permettent à un administrateur d'utiliser des informations d'identification spécifiques sur les calendriers Discovery. Les alias d'informations d'identification fournissent un contrôle plus granulaire sur les informations d'identification qu'une table de découverte est autorisée à utiliser. Pour remédier à cette faille de sécurité, définissez la valeur `alias_filtering_behavior` sur strict pour empêcher l'exposition inutile des informations d'identification avec des privilèges élevés. Reportez-vous à la rubrique MID Server properties pour en savoir plus.

En savoir plus

Attribut	Description
Nom de la configuration	`alias_filtering_behavior`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	strict
Valeur par défaut	lâche
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 2 • Score CVSS : faible • Détails du risque de sécurité : lorsque ce paramètre de sécurisation renforcée n'est pas défini sur strict, toutes les informations d'identification sont utilisées, quels que soient leurs alias, pour les tables Découverte, ce qui augmente le risque d'accès non autorisé.
Dépendances et prérequis	Aucun
Références	• MID Server • Alias d'informations d'identification pour Détection

Appliquer les ACL de type GroupBy

Configurez votre instance pour effectuer des vérifications d'ACL sur les colonnes groupées.

Utilisez cette propriété pour configurer votre instance afin d'effectuer des vérifications d'ACL sur les colonnes groupées. Si cette propriété est définie sur la valeur recommandée **vrai**, l'attribut d'une *groupby_acl_check* table est alors défini pour honorer les ACL groupby. Si la propriété est définie sur **false**, il n'y a alors aucune vérification d'ACL sur les colonnes groupby d'une table susceptible d'entraîner une fuite d'informations.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.security.groupby_acl_check*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails des risques de sécurité : définir cette propriété sur **faux** désactivera la vérification des ACL sur les colonnes groupées, ce qui pourrait entraîner une fuite d'informations.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

S’assurer que la création/la suppression des tableaux de bord nécessite une vérification d’accès [Nouveau dans Security Center 1.3]

La `glide.processors.check_access_before_process` propriété active l’application de la liste de contrôle d’accès (ACL) pour la création ou la suppression de tableaux de bord lorsqu’un utilisateur est connecté. Cette propriété doit toujours être définie sur true.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.processors.check_access_before_process`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails du risque de sécurité : la désactivation de cette propriété en la définissant sur faux permet un contournement de l’ACL sur les tableaux de bord. Cela permet à tous les utilisateurs authentifiés avec des privilèges faibles de supprimer et d’ajouter des tableaux de bord.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété contrôle la possibilité de créer de nouveaux sys_dashboards et de supprimer des tableaux de bord existants lorsqu’un utilisateur ne dispose pas des droits d’accès nécessaires. Lorsque la valeur est définie sur faux, les utilisateurs ayant des rôles inappropriés peuvent ajouter et supprimer des entrées sys_dashboard (bien que la couche GlideRecord doive revérifier les ACL existantes). La valeur true limite les opérations d’ajout et de suppression pour les utilisateurs ne disposant pas des droits d’accès requis.

Renforcer la validation des paramètres de l’état OAuth

Configurez cette `glide.oauth.state.parameter.required`propriété pour empêcher votre instance contre les attaques de contrefaçon de requête de site à site (CSRF).

La `glide.oauth.state.parameter.required` propriété permet d’exiger le paramètre État dans une demande OAuth pour le flux du code d’autorisation. Le paramètre État est une valeur de chaîne qui ne doit pas contenir de caractères spéciaux ni être vide. Définir cette propriété sur **vrai** garantit qu’un attaquant ne peut pas effectuer d’attaques de contrefaçon de requête intersite (CSRF) pendant l’authentification, ce qui protège votre instance contre les attaques d’un utilisateur dont l’identité est empruntée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.oauth.state.parameter.required`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails des risques de sécurité : définissez cette propriété sur **vrai** pour vous assurer que les attaques CSRF sont empêchées.
Dépendances et prérequis	Aucun

Appliquer des règles strictes pour le téléchargement d'images par l'utilisateur

Utilisez la propriété pour activer le `glide.security.strict.user_image_upload` contrôle d'accès pour le chargement/la mise à jour d'une photo de profil lorsqu'il est effectué sur un enregistrement utilisateur.

Ce paramètre ouvre la possibilité pour un utilisateur non autorisé de télécharger une image sur le profil d'un autre utilisateur.

- Lorsque vous définissez cette propriété sur **vrai**, les ACL de table sont appliquées lors du chargement de photos, et seuls les utilisateurs autorisés peuvent charger une image.
- Lorsque vous définissez ce paramètre sur **faux**, les ACL ne sont pas appliquées lors des chargements d'images dans le champ Photo.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.strict.user_image_upload`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Pour restreindre le téléchargement de l'image d'un utilisateur aux seuls utilisateurs autorisés.
Valeur recommandée	VRAI
Cote de risque de sécurité	3.7
Impact fonctionnel	(Faible) Aucun impact sur la fonctionnalité car les utilisateurs autorisés peuvent toujours télécharger des images sur leur profil d'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Faible) Lorsque vous définissez cette propriété sur **faux**, un utilisateur authentifié peut télécharger une image sur le compte d'un autre utilisateur sans autorisation.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les domaines d'e-mail pour l'inscription des utilisateurs externes [Mise à jour dans Security Center 1.5]

Utilisez la propriété pour répertorier les `sn_ext_usr_reg.allowed_email_domains` domaines d'e-mail externes acceptables.

En savoir plus

Attribut	Description
Nom de la propriété	`sn_ext_usr_reg.allowed_email_domains`
Type de configuration	Propriétés système (/sys_properties_list.do), Propriétés des communautés
Catégorie	Contrôle d'accès
Objectif	Répertoriez les domaines d'e-mail pour autoriser l'e-mail de l'utilisateur pour l'inscription.
Valeur recommandée	Définir comme une valeur non vide
Type de configuration	Chaîne
Risque de sécurité	(Élevé) Les acteurs malveillants pourraient effectuer l'enregistrement à l'aide d'adresses e-mail provenant de domaines indésirables. Assurez-vous que `sn_ext_usr_reg.allowed_email_domains` cette valeur n'est pas définie.
Cote de risque de sécurité	7.5
Références	Communities

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Module d'extension de haute sécurité [mis à jour dans Security Center 1.3]

Lorsque vous activez le module d'extension de haute sécurité, ce dernier crée ou met à jour des centaines de configurations différentes pour contrôler le niveau de sécurité de votre instance. Ces configurations atténuent la plupart des attaques OWASP les plus fréquentes en activant un contrôle d'accès strict, la validation d'entrée et l'encodage de sortie.

Ces configurations sont les suivantes :

- Contrôle d'accès
- Règles métier
- Propriétés système
- Action de politique d'interface utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Actions des scripts
- Includes de script

Exemple

Reportez-vous aux exemples pour les propriétés suivantes :

Propriété	Rubrique
glide.ui.escape_all_script	Échapper à Jelly
glide.security.strict.actions	Vérifier l'action d'interface utilisateur avant son exécution
glide.security.csrf_previous.autoriser	Jeton anti-CSRF
glide.security.csrf.strict.validation.mode	Validation stricte du CSRF

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.high_security
Type de configuration	Définition du système > Modules d'extension : Développement
Catégorie	Contrôle d'accès
Objectif	L'activation de ce module d'extension est obligatoire. Il augmente le niveau de sécurité d'une instance, ce qui réduit la surface d'attaque en atténuant les 10 principales attaques OWASP, y compris CSRF, XSS, Sécurisation des cookies de session et les chargements de fichiers.
Valeur recommandée	Actif
Cote de risque de sécurité	9.8
Impact fonctionnel	(Élevé) Ce module d'extension active plusieurs configurations de sécurité système, qui peuvent également avoir un impact sur l'interface utilisateur et les fonctionnalités.
Risque de sécurité	(Élevé) De nombreuses configurations de sécurité sont involontairement laissées ouvertes, ce qui peut ouvrir la porte à certaines vulnérabilités critiques.
Références	Activation des paramètres de sécurité élevée Paramètres de sécurité élevée

Pour en savoir plus sur l'activation d'un module d'extension, consultez Activate a plugin

Respecter les ACL de remplacement de l'administrateur

La `glide.security.admin.override.accessterm` propriété contrôle les administrateurs afin qu'ils ne puissent pas remplacer l'évaluation de l'ACL, même lorsque le remplacement doit être en vigueur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.admin.override.accessterm`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Contrôle les administrateurs pour qu'ils ne puissent pas remplacer l'évaluation de l'ACL.
Type de données	Booléen
Valeur recommandée	Vrai
Valeur par défaut	Vrai
Risque de sécurité	(Faible) Les ACL sont évaluées de façon cumulative. S'il existe un certain nombre d'ACL sur un champ donné et que l'option Remplacements administrateur est définie sur faux (non sélectionnée) sur l'un d'eux, les remplacements administrateur effectifs pour toutes les ACL sont considérés comme faux.
Cote de risque de sécurité	3.8
Références	Règles de la liste de contrôle d'accès

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Empêcher les utilisateurs inactifs de se connecter [Nouveau dans Security Center 1.5]

Configurez cette propriété pour contrôler si des utilisateurs inactifs peuvent s'authentifier sur votre instance.

Définissez la valeur de la `glide.authenticate.only.allow.active.user.login` propriété sur vrai (recommandé), ce qui garantit que les utilisateurs de la table sys_user marquée comme inactives ne peuvent pas se connecter à l'instance et sont bloqués.

Si le paramètre est configuré sur faux, les utilisateurs peuvent toujours accéder à l'instance et aux données auxquelles ils avaient accès précédemment.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.only.allow.active.user.login`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée, vrai, les utilisateurs inactifs, comme un employé licencié, peuvent continuer à accéder à l'instance et à toutes les données.
Dépendances et prérequis	Aucun

Restreindre les demandes JSONP aux URL approuvées [Mise à jour dans Security Center 1.3]

Spécifiez des URL approuvées pour le service $http AngularJS afin d'autoriser ou de rejeter les demandes JSONP.

La *`angular.jsonp.inclusion_list.enabled`* propriété indique des URL fiables pour le service de $http angularJS afin d'autoriser et/ou de rejeter les demandes JSONP. Cette propriété est nécessaire, car il s'agit d'un changement qui peut avoir des conséquences importantes pour les clients, ils ont donc besoin d'une solution pour ajouter leurs URL fiables. Si cette propriété n'est pas définie sur la valeur recommandée, vrai, les demandes JSONP sont alors autorisées pour n'importe quelle URL

En savoir plus

Attribut	Description
Nom de la configuration	*`angular.jsonp.inclusion_list.enabled`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : moyen • Score CVSS : 5,4 • Détails du risque de sécurité : définir cette propriété sur **faux** active les requêtes JSONP vers n'importe quelle URL.
Dépendances et prérequis	Aucun

Désactiver l'exécution des requêtes de base de données brutes [Mise à jour dans Security Center 1.3]

Contrôlez si un utilisateur peut effectuer des requêtes SQL brutes sur la base de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La`glide.db.allow_unsafe_dbi_execute_sql` propriété permet aux utilisateurs d'effectuer des requêtes SQL brutes sur la base de données, ce qui peut donner accès à des tables et à des données hors des restrictions GlideRecord. Si cette propriété n'est pas définie sur la valeur recommandée , cela permet l'appel de à partir d'un `false`scriptable Glide, ce qui peut entraîner l'exécution d'instructions `dbi.executeStatement()` SQL malveillantes.

⚠ Avertissement :
Cette propriété est à la fois sécurisée et aucun remplacement de base de données.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.db.allow_unsafe_dbi_execute_sql`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 7,2 • Score CVSS : élevé • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur **faux,** l'appel de à partir d'un `dbi.executeStatement()` scriptable Glide peut être appelé.
Dépendances et prérequis	Aucun
Références	Règles de la liste de contrôle d'accès

Masquer les commentaires des utilisateurs sur les articles [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour contrôler si les `glide.knowman.show_user_feedback` commentaires sont visibles.

Lorsque `glide.knowman.show_user_feedback` cette option n'est pas définie sur jamais, les commentaires des utilisateurs ayant des rôles définis dans la propriété `glide.knowman.show_user_feedback.roles`Glide sont visibles sur les articles de la base de connaissances (KB). Étant donné que les commentaires peuvent contenir des informations sensibles, vous ne souhaitez peut-être pas qu'ils soient visibles. Si cette propriété n'est pas définie sur jamais, il pourrait y avoir des impacts sur la confidentialité si des informations sensibles sont divulguées dans les commentaires.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.knowman.show_user_feedback`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	liste de choix
Valeur recommandée	jamais
Valeur par défaut	Chargement en cours
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails des risques de sécurité : si vous ne définissez pas cette propriété sur « jamais », des informations sensibles peuvent être divulguées dans les commentaires de commentaires.
Dépendances et prérequis	Aucun
Impact fonctionnel	Affiche les commentaires des utilisateurs sur les articles de la base de connaissances en fonction des choix mentionnés dans la configuration.

Exiger l'authentification par défaut pour les includes de script pouvant être appelés par le client [Mise à jour dans Security Center 1.3]

Par défaut, les includes de script pouvant être appelés par le client qui ne définissent pas explicitement la visibilité sont publics. Si nécessaire, ajoutez la propriété pour activer le contrôle de la confidentialité sur tous les includes de script appelables par les clients accessibles via des `glide.script.ccsi.ispublic` pages publiques.

Lorsque vous ajoutez cette propriété, vous devez définir sa valeur sur **faux**, ce qui signifie que tous les includes de script pouvant être appelés par le client sont privés et modifie leur visibilité dans les pages publiques.

Remarque :
Vous ne pouvez pas ajouter la propriété avec une valeur **vrai** ou modifier sa valeur de **faux** à **vrai**. Si vous tentez de le faire, un message d'erreur s'affiche.

Si nécessaire, vous pouvez modifier le paramètre de confidentialité d'un include de script individuel pouvant être appelé par un client en ajoutant la fonction `isPublic()`.

- Le paramètre `isPublic()` a priorité sur la `glide.script.ccsi.ispublic` propriété.
- Par exemple, si vous définissez `isPublic()` sur **true** dans un script individuel, il devient public, ce qui remplace la propriété qui rend privés tous les autres includes de script pouvant être appelés par le `glide.script.ccsi.ispublic` client.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.script.ccsi.ispublic*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Rendre privé les includes de script pouvant être appelés par le client signifie que les invités qui accèdent aux pages publiques ne peuvent pas accéder à l'include de script pouvant être appelé par le client. Un utilisateur non connecté ne peut pas exécuter de script privé.
Valeur recommandée	faux
Valeur par défaut	faux
Cote de risque de sécurité	7.5
Impact fonctionnel	(Élevé) Si les includes de script pouvant être appelés par le client sont désignés comme publics (c'est-à-dire que cette propriété est manquante), les utilisateurs non authentifiés peuvent exécuter des scripts clients. Ajouter la propriété restreint l'exécution de scripts par un utilisateur non connecté.
Risque de sécurité	(Élevé) Si vous n'ajoutez pas cette propriété, les includes de script côté client contournent les ACL, ce qui peut entraîner des fonctionnalités publiques non prévues. Si le script client fournit des informations confidentielles, il peut présenter un risque potentiel négatif pour la sécurité.
Solution de contournement	Si vous définissez la propriété sur **faux,** tous les includes de script pouvant être appelés par le *glide.script.ccsi.ispublic* client sont privés. Vous pouvez modifier le paramètre de confidentialité d'un include de script individuel pouvant être appelé par un client en ajoutant la fonction isPublic(). La fonction isPublic a priorité sur la *glide.script.ccsi.ispublic* propriété. Ajoutez la syntaxe suivante à l'include de script : isPublic :function(){return[vrai/faux] ;},

Appliquer le comportement de l'instance de production [mis à jour dans Security Center 1.3 et 1.5]

Configurez si votre instance doit être gérée comme une instance de production ou de non-production.

Si la *glide.installation.production* propriété n'est pas définie sur la valeur recommandée **vrai**, l'instance n'est pas traitée comme une instance de production, ce qui permet l'exécution de zboot et d'autres scripts potentiellement dangereux. L'évaluation d'une instance de production en tant qu'instance de non-production peut entraîner des fuites d'informations ou des attaques par déni de service (DoS).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.installation.production`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails des risques de sécurité : la définition de cette valeur de propriété sur **faux** entraîne le traitement de l'instance comme une instance de non-production, ce qui permet l'exécution de zboot et d'autres scripts potentiellement dangereux.
Dépendances et prérequis	Aucun

Restreindre l'accès au script d'arrière-plan

Configurez lapropriété pour `glide.script_processor.admin` définir le rôle requis pour accéder au module Arrière-plan de script.

La `glide.script_processor.admin` propriété contient le rôle requis pour accéder au module Arrière-plan de script. Si cette propriété n'est pas définie sur la valeur recommandée **d'administrateur**, tout utilisateur, quel que soit son rôle, peut exécuter des scripts en arrière-plan sur l'instance. Cela permet aux acteurs malveillants de contourner le système d'ACL, en leur accordant un accès complet aux tables.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.script_processor.admin`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	administrateur
Valeur par défaut	administrateur
Catégorie	Contrôle d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 8,8 • Score CVSS : élevé • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée **d'administrateur** , n'importe quel utilisateur peut exécuter des scripts en arrière-plan sur l'instance.
Dépendances et prérequis	Aucun

Restreindre l'accès aux e-mails dont la table cible est vide

Activez la propriété pour restreindre l'accès `glide.email.email_with_no_target_visible_to_all` de l'utilisateur aux e-mails, sauf s'il en est l'expéditeur ou qu'il possède le rôle administrateur.

Les utilisateurs non autorisés peuvent accéder aux e-mails de la table sys_email_list qui n'ont pas d'enregistrement cible. Au lieu d'appliquer des ACL aux entrées d'e-mail, cette propriété restreint l'accès uniquement à l'expéditeur de l'e-mail et aux utilisateurs disposant du rôle administrateur.

Remarque :
Les e-mails envoyés et reçus par l'instance apparaissent dans la table sys_email_list. Toutefois, seuls les e-mails reçus marqués avec un état Erreur et Ignoré doivent avoir une table cible vide.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.email.email_with_no_target_visible_to_all`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer	Contrôle d'accès
Objectif	Pour empêcher le client de messagerie d'afficher les e-mails lorsque l'utilisateur n'autorise pas l'accès.
Valeur recommandée	faux
Valeur par défaut	VRAI
Cote de risque de sécurité	5.4
Impact fonctionnel	(Faible) Les utilisateurs ne peuvent plus voir les e-mails dont la table cible est vide, sauf s'ils sont administrateurs ou expéditeur de l'e-mail.
Risque de sécurité	(Modéré) Si la propriété n'est pas activée, les utilisateurs non autorisés peuvent accéder à n'importe quel e-mail dont le champ target_table est vide.
Références	Propriétés avancées d'e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0690043

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès aux module d'extension des plages d'adresses IP spécifiques

Utilisez le module d'extension pour restreindre l'accès *com.snc.ipauthenticator* à des plages IP spécifiques. À moins que l'accès public ne soit destiné à l'instance, les administrateurs doivent limiter l'accès aux blocs réseau IP qui leur sont affectés.

Prérequis

Avant de définir cette propriété, vous devez activer le module d'extension Authentification basée sur la plage IP (com.snc.ipauthenticator).*com.snc.ipauthenticator* Pour en savoir plus, consultez Authentification basée sur la plage IP et dans la section Étapes de configuration (ci-dessous).

En savoir plus

Attribut	Description
Nom du module d'extension	*com.snc.ipauthenticator*
Type de configuration	Sécurité de système > Contrôle d'accès à l'adresse IP
Catégorie	Contrôle d'accès
Objectif	Pour ajouter la plage d'adresses IP qui peut ou ne peut pas accéder à l'instance aux listes de domaines approuvés et non approuvés.
Valeur recommandée	Actif
Valeur par défaut	Aucun. Il s'agit d'un plugin, pas d'une propriété Glide ; Il n'y a donc pas de valeur par défaut.
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) Des plages IP refusées par le client sont utilisées pour cet élément de rattrapage. Aucun impact, car le client définit la liste cible.
Risque de sécurité	(Faible) L'exposition inutile à l'instance cible sur Internet doit être limitée à l'aide de la fonctionnalité de contrôle d'accès IP.
Références	Authentification basée sur la plage IP

Étapes à configurer

1. Assurez-vous que le module d'extension com.snc.ipauthenticator est actif.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès à l'adresse IP**.
3. Cliquez sur **Nouveau** pour créer une liste d'exclusion (refus) ou une liste d'inclusion (autorisation) d'adresses IP.
4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restreindre l'accès aux bases de connaissances [Nouveau dans Security Center 1.3]

La *glide.knowman.block_access_with_no_user_criteria* propriété est utilisée pour contrôler l'accès en lecture/écriture des utilisateurs sur les articles basés sur la base de connaissances.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.knowman.block_access_with_no_user_criteria*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 9,1 • Score CVSS : critique • Détails des risques de sécurité : Si cette propriété n'est pas définie sur la valeur conseillée, vrai, tout utilisateur peut lire et contribuer à une base de connaissances.
Dépendances et prérequis	Aucun
Impact fonctionnel	Refuse l'accès à une base de connaissances lorsque l'option Peut lire ou Peut contribuer n'est pas spécifiée.

Restreindre les autorisations pour le modèle CMDB

Utilisez la propriété système pour limiter l'accès *csm_cmdb_model.customer_visible_flag* des clients aux données de la table Modèles de produits en tant que contrôle d'accès supplémentaire au modèle CMDB.

Définissez la *csm_cmdb_model.customer_visible_flag* propriété sur **vrai** pour activer le champ Visible par le client pour les tables répertoriées ci-dessous :

- Table Modèles de produits [cmdb_model]
- Table Modèles logiciels [cmdb_software_product_model]
- Table Modèles d'application [cmdb_application_product_model]
- Table Modèles de consommables [cmdb_consumable_product_model]
- Table Modèles d'installation [cmdb_facility_product_model]
- Table Modèles matériels [cmdb_hardware_product_model]

Si vous définissez cette propriété sur **vrai,** toutes les valeurs cmdb_model sont masquées par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définissez la propriété sur **faux** pour ne pas prendre en compte la colonne/l'élément customer_visible sur la table cmdb_model et pour vous appuyer sur les bases cmdb_model ACL qui sn_esm_user sont accessibles.

En savoir plus

Attribut	Description
Nom de la propriété	`csm_cmdb_model.customer_visible_flag`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Lorsqu'elle est définie sur**tue true**, le système utilise le paramètre du champ Visible par le client pour déterminer l'accès aux données de modèle de produit sur le Customer Service Portal.
Valeur recommandée	VRAI
Valeur par défaut	faux
Type de données	Booléen
Risque de sécurité	(Modéré) Tout utilisateur disposant du rôle sn_esm_user et des ACL prêtes à l'emploi peut disposer d'autorisations pour le modèle CMDB. **Remarque :** Ce rôle a tendance à être accordé aux utilisateurs externes. Des utilisateurs externes pourraient sans le vouloir recevoir des autorisations pour le modèle CMDB.
Références	Limiter l'accès aux données des modèles de produits sur le Customer Service Portal

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès non authentifié aux pièces jointes

Utilisez cette `glide.image_provider.security_enabled` propriété pour contrôler les paramètres de sécurité des images. Si la valeur est définie sur **vrai**, les images ne sont visibles que par les utilisateurs authentifiés et autorisés. Si elle est définie sur **faux**, les images sont visibles par toutes les personnes qui possèdent l'URL de la pièce jointe.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.image_provider.security_enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Empêche tout accès non authentifié à la pièce jointe lorsqu'elle est rendue au format `.iix` .
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	VRAI
Impact fonctionnel	(Faible) Pas d'impact significatif sur la fonctionnalité. L'expérience utilisateur peut être un peu affectée, car l'utilisateur qui accédait directement au fichier .iix doit passer par l'authentification.
Risque de sécurité	(Élevé) Une restriction doit être appliquée pour les utilisateurs non authentifiés, car certaines pièces jointes peuvent contenir des informations sensibles.
Références	Administration des pièces jointes Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre l'accès aux écritures de journal personnalisées [Mise à jour dans Securty Center 1.3]

Utilisez cette `glide.live_feed.custom_journal.acl_check_enabled` propriété pour respecter les ACL sur les champs de journal personnalisés.

Si `glide.live_feed.custom_journal.acl_check_enabled` la valeur n'est pas définie sur la valeur recommandée, vrai, tous les utilisateurs ont alors accès à toutes les entrées de journal de la fonctionnalité de flux en direct. Définir la propriété sur vrai respecte les ACL sur les champs de journal personnalisé, ce qui est une bonne fonctionnalité.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.live_feed.custom_journal.acl_check_enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	À contrôler quels utilisateurs voient quelles écritures de journal en fonction des ACL.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Type de configuration	Booléen.
Risque de sécurité	(Modéré) Lorsque la valeur est définie sur vrai, seules les entrées de journal personnalisées qui passent l'ACL sont affichées dans Flux en direct, sinon tous les utilisateurs peuvent voir toutes les entrées de journal.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Restreindre l’accès en lecture au contexte de flux [Nouveau dans Security Center 1.5]

Utilisez la *com.snc.process_flow.reporting.require_flow_access* propriété pour appliquer si une vérification d’accès supplémentaire est requise pour qu’un utilisateur lise une vérification de flux.

Lorsque la *com.snc.process_flow.reporting.require_flow_access* propriété est définie sur la valeur recommandée vrai, une vérification d’accès supplémentaire est effectuée pour un utilisateur qui tente de lire un contexte de flux. Il peut y avoir une divulgation mineure d’informations si cette propriété est définie sur faux.

En savoir plus

Attribut	Description
Nom de la configuration	*com.snc.process_flow.reporting.require_flow_access*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails des risques de sécurité : définir cette propriété sur faux conserve son comportement existant. Définir cette propriété sur vrai applique la couche de sécurité ajoutée de l’accès en lecture.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est activée, la sécurité de lecture des enregistrements de contexte de flux est augmentée. L’instance impose qu’un utilisateur qui tente de lire le contexte de flux ait également un accès en lecture au flux parent.

Traduction automatique

Activer le module d’extension de démarrage rapide de la sécurité (règles ACL) [Mise à jour dans Security Center 1.3]

Activez le module d’extension Security Quick Start (ACL Rules) (com.snc.system_security*com.snc.system_security*) pour créer plusieurs ACL importantes qui valident les contrôles d’accès sur certaines des tables Now Platformclés du système.

Ces règles permettent de démarrer rapidement la sécurisation de nombreuses tables système, simplifiant ainsi la mise en production d’une instance. Le module d’extension de démarrage rapide de la sécurité (règles ACL) est installé automatiquement sur toutes les nouvelles instances.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
ID de module d'extension	`com.snc.system_security`
Type de configuration	Définition du système > Modules d'extension
Catégorie	Contrôle d'accès
Objectif	Activez le module d'extension de démarrage rapide de la sécurité (règles ACL) pour assurer une conformité de sécurité appropriée. Il fournit des ACL de base qui sécurisent les tables système en premier lieu au lieu de les créer manuellement pour chaque table système fournie avec la mise en service par défaut d'une instance. Ces ACL sont utiles lorsque l'instance nouvellement créée doit passer rapidement en production.
Valeur recommandée	Actif
Valeur par défaut	Aucun. Il s'agit d'un module d'extension et non d'une propriété Glide, il n'y a donc pas de valeur par défaut. Le plugin est installé par défaut sur zBoot (réinitialisation).
Cote de risque de sécurité	8.1
Impact fonctionnel	(Moyen) Il y a un impact fonctionnel important si ce module d'extension est installé sans audit des ACL existantes sur l'instance. La sensibilisation et les définitions des clients sont nécessaires avant que la correction puisse avoir lieu.
Risque de sécurité	(Élevé) Le contrôle d'accès doit être appliqué pour verrouiller l'accès non souhaité à l'instance. Les règles de démarrage rapide ACL ont été créées pour fournir un point de départ pour sécuriser de nombreuses tables système afin de faciliter la mise en production rapide d'une entreprise.
Références	Démarrage rapide de la sécurité : règles ACL

Étapes à configurer

Si ce module d'extension n'est pas activé sur votre instance, contactez ServiceNow le support. L'activation du module d'extension à ce stade peut modifier l'accès de sécurité aux tables déjà utilisées dans un environnement de production. Si un administrateur est intéressé par les nouvelles règles ACL fournies par le module d'extension, vous pouvez créer manuellement une ou plusieurs d'entre elles dans une instance existante si nécessaire. Cette liste d'ACL peut être utilisée à titre indicatif dans ce cas.

Utilisation de l'opération multiple d'insertion sécurisée dans l'API de jeu d'importation [Nouveau dans Security Center 1.3]

Utilisez la `com.glide.import_set_api.insert_multiple_optimize` propriété pour contrôler si `GlideRecordSecure` ou `GlideRecord` est utilisé pour l'opération Insertion multiple dans l'API de jeu d'importation.

Si `com.glide.import_set_api.insert_multiple_optimize` la valeur est définie sur la valeur recommandée faux, `GlideRecordSecure` est utilisé pour insérer les enregistrements et les listes de contrôle d'accès (ACL) au niveau de la table sont évaluées. Si cette propriété est définie sur vrai, `GlideRecord` sera utilisé pour insérer des enregistrements et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

les ACL au niveau de la table ne seront pas évaluées ; En outre, vous devez vous assurer que l'ACL du point de terminaison REST multiple d'insertion de l'API de jeu d'importation (sys_id : 3101b770ff2211105cf343d0653bf182) est active et que les utilisateurs disposent du rôle, import_transformer.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.import_set_api.insert_multiple_optimize`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails du risque de sécurité : Si cette propriété n'est pas définie sur faux, un utilisateur ayant peu de privilèges peut insérer des données dans des tables en dehors du cadre de ses rôles privilégiés.
Comportement réversible	Remplacement sécurisé et aucun remplacement de base de données.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété optimise les performances de l'API de jeu d'importation en utilisant GlideRecord pour enregistrer les données. Lorsque le paramètre est défini, un utilisateur d'intégration doit disposer du rôle import_transformer pour accéder à l'API.
Références	https://developer.servicenow.com/blog.do?p=/post/gliderecord-vs-gliderecordsecure

Appliquer la sécurité stricte des requêtes SOAP [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour appliquer la `glide.soap.strict_security` sécurité des services web.

Cette propriété utilise une combinaison de :

- Contestation/réponse d'authentification de base sur le protocole HTTP et
- Contrôles d'accès au niveau du système dans le Module d'extension Sécurité contextuelle : Gestion des rôles.

Si vous définissez cette propriété sur **true**, elle effectue les actions suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si l'utilisateur dispose du rôle approprié pour effectuer l'opération, il vérifie la demande SOAP entrante pour obtenir l'autorisation du rôle à valider. Il se produit lors des appels/demandes de service Web SOAP effectués sur Now Platform des tables lors de l'exécution des opérations CRÉER, LIRE, METTRE À JOUR ou SUPPRE.
- Vérifie les ACL au niveau du système tout en récupérant les données sous la forme de données SOAP sur la table.
- Vérifie les ACL au niveau du champ pour toute opération CRUD effectuée sur un champ de la table.

Les vérifications d'ACL ne sont effectuées que pour les appels d'API de table standard et non pour les services Web.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.soap.strict_security*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Valeur par défaut	VRAI
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cette correction applique le contrôle d'accès au niveau du système tout en récupérant les données des tables/pages sous la forme de données SOAP sur l'instance. Si des utilisateurs accèdent actuellement à ces données, ils sont limités/autorisés à accéder aux données en fonction des règles ACL. Pour connaître les rôles par défaut ayant accès aux données SOAP, reportez-vous à la section SOAP web service .
Risque de sécurité	(Modéré) Sans autorisation appropriée configurée sur les demandes SOAP entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Enforce strict security for inbound SOAP SOAP web service

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Instanciateurs de connexions jms requis [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

La *mid.property.jms.command.allowed_factory_names* propriété contrôle les instanciateurs de connexions de Service de messagerie Java (JMS) que le serveur MID peut utiliser.

Il est destiné à quelques usines sélectionnées nécessaires par les plugins pour l'activité ou l'action JMS. L'inclusion d'instanciateurs supplémentaires pourrait être une étape dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une chaîne d'attaque pour des vulnérabilités telles que l'insertion JDNI qui reposent sur les capacités qu'un attaquant peut exploiter dans les instanciateurs autorisés. Pour éviter toute possibilité d'exploitation de vulnérabilité, n'incluez pas les usines au-delà des valeurs par défaut nécessaires.

Pour remédier à ce risque de sécurité, passez en revue la liste des noms fournie à la propriété mid, *`mid.property.jms.command.allowed_factory_names`*. Assurez-vous que tous les noms d'instanciateurs Java supplémentaires au-delà de la valeur par défaut de connectionFactory, queueConnectionFactory et topicConnectionFactory sont nécessaires.

En savoir plus

Attribut	Description
Nom de la configuration	*`mid.property.jms.command.allowed_factory_names`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur par défaut	*`connectionFactory`*, *`queueConnectionFactory`*, *`topicConnectionFactory`*
Valeur recommandée	*`connectionFactory`*, *`queueConnectionFactory`*, *`topicConnectionFactory`*
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,1 • Score CVSS : moyen • Détails des risques de sécurité : Si le module d'extension Serveur MID (*`com.glideapp.agent`*) est actif, passez en revue la liste des noms fournie à la propriété *`mid.property.jms.command.allowed_factory_names`*MID. Assurez-vous que tous les noms d'instanciateurs supplémentaires au-delà de la valeur par défaut de connectionFactory, queueConnectionFactory et topicConnectionFactory sont nécessaires.
Dépendances et prérequis	Aucun

Traduction automatique

Examiner les conditions de contrôle d'accès aux rôles explicites superflus [supprimé dans Security Center 1.5]

Il est recommandé d'utiliser le module d'extension Explicit Roles pour exiger que tous les utilisateurs aient le rôle snc_internal pour accéder aux ressources internes, ou le rôle snc_external pour accéder aux ressources externes.

Après l'installation de ce module d'extension, le rôle snc_internal est affecté à tous les utilisateurs existants et les listes de contrôle d'accès (ACL) existantes sont renseignées avec les conditions de rôle. En raison d'une logique d'automatisation ou de l'intervention d'un administrateur d'instance, les rôles snc_internal ou snc_external peuvent être ajoutés de manière incorrecte à une ACL qui contient déjà une exigence de rôle plus stricte. Étant donné que l'évaluation du rôle ACL sera réussie pour tout utilisateur contenant un rôle mappé à une ACL, l'ajout de snc_internal ou de snc_external peut être trop large pour

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'objectif prévu d'une ACL. Cela peut entraîner une fuite de données si un utilisateur ayant peu de privilèges se voit accorder l'accès via l'ACL.

Par exemple, il ne serait pas nécessaire que les rôles snc_internal et administrateur soient mappés à la même ACL au sein d'une table. L'ACL est destinée à accorder l'accès aux administrateurs, auquel cas le rôle snc_internal est une erreur. Ou bien, l'ACL est destinée à accorder l'accès à tous les utilisateurs snc_internal, ce qui rend le rôle administrateur inutile. Lorsque le module d'extension Explicit Roles est installé, examinez les ACL qui contiennent une condition de rôle pour snc_internal ou snc_external tout en contenant une condition pour un autre rôle. Si les rôles sont en mesure de fonctionner pour un cas d'utilisation spécifique, le résultat doit être révisé périodiquement.

Important :
Dans la prochaine des lignes de base de référence de sécurisation renforcée d'ISM (version 1.6), cette vérification sera remplacée par une vérification appelée « Suite de vérifications de configuration ACL de rôles explicites ». À l'heure actuelle, la vérification peut entraîner trop de résultats pour être examinée.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.explicit_roles*, *sys_security_acl* et *sys_security_acl_role*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Aucun type de données
Valeur recommandée	Aucune valeur recommandée
Valeur par défaut	Aucune valeur par défaut
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : en raison de l'automatisation ou de l'intervention d'un administrateur d'instance, les rôles snc_internal ou snc_external peuvent être ajoutés à une ACL qui contient déjà une exigence de rôle plus stricte. Étant donné que l'évaluation du rôle ACL passera pour tout utilisateur contenant un rôle mappé à une ACL, l'ajout de l'un ou l'autre rôle sera trop large pour les besoins d'une ACL et pourrait entraîner une fuite de données si un utilisateur ayant peu de privilèges se voit accorder l'accès via l'ACL.
Références	Explicit Roles

Définir l'utilisateur invité pour les demandes SOAP [Mise à jour dans Security Center 1.3]

Configurez cette propriété pour contrôler le niveau d'accès des demandes SOAP non authentifiées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette propriété contrôle le niveau d'accès des demandes SOAP non authentifiées. Si la propriété n'est pas définie sur la valeur conseillée, ou *soap.guest*si elle est définie sur un utilisateur avec des privilèges limités, les demandes SOAP s'exécutent alors pour le compte de l'utilisateur. Si cette propriété est vide, elle permet un accès non authentifié aux opérations de niveau administrateur ou maintenance, ce qui annule tous les contrôles de sécurité au sein de l'instance.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.soap.guest_user*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	savon.invité
Valeur par défaut	savon.invité
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : définir cette propriété sur vide permet un accès non authentifié aux opérations de niveau administrateur ou de maintenance.
Dépendances et prérequis	Aucun

Activer le module d'extension de contrôle d'accès SNC [mis à jour dans Security Center 1.3]

Activez le module d'extension SNC Access Control (com.snc.snc_access_control*com.snc.snc_access_control*) pour contrôler l'accès du personnel à vos instances Service et assistance client .

La configuration par défaut de permet d'accéder aux instances via un processus interne qui crée des informations d'identification Now PlatformService et assistance client de support à court terme. Bien que tous les accès soient audités, certains clients préfèrent contrôler cet accès.

Ce module d'extension permet au service clientèle et au support d'empêcher Service et assistance client les employés d'accéder à l'instance. Cette décision a un impact sur les SLA de support, car vous devez activer Now Platform l'accès avant que les activités de support puissent commencer. Pour en savoir plus, consultez Contrôle d'accès ServiceNow.

En savoir plus

Attribut	Description
Nom du module d'extension	*com.snc.snc_access_control*
Type de configuration	Définition du système > Modules d'extension

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Contrôle d'accès
Objectif	Interdit Service et assistance client aux employés d'accéder à l'instance
Valeur recommandée	Actif
Valeur par défaut	Aucun. Il s'agit d'un module d'extension et non d'une propriété Glide, il n'y a donc pas de valeur par défaut. Le module d'extension n'est pas installé par défaut.
Rôle requis	L'administrateur client ne peut pas activer ce module d'extension. Il doit être explicitement demandé, car l'activation du module d'extension nécessite des privilèges élevés.
Cote de risque de sécurité	8.2
Impact fonctionnel	(Faible) Si ce module d'extension est inactif, tous les Service et assistance client employés peuvent accéder à l'instance du client. L'activation du module d'extension permet au client de restreindre l'accès aux seuls employés autorisés Service et assistance client .
Risque de sécurité	(Élevé) Exposition inutile de l'accès aux instances à un groupe plus large de personnes.
Références	Contrôle d'accès ServiceNow

Étapes à configurer

1. Pour demander le module d'extension, procédez comme suit dans Activation du contrôle d'accès ServiceNow. Les clients doivent demander le module d'extension SNC Access Control (com.snc.snc_access_control) auprès de HI.
2. Pour activer le contrôle d'accès SNC, procédez comme suit dans Configuration ServiceNow du contrôle d'accès. Configurez un enregistrement de contrôle d'accès pour spécifier un ou plusieurs Service et assistance client employés qui ont l'autorisation de se connecter à votre instance.

API et service web

La catégorie API et service Web garantit que les applications disposent d'une authentification, d'une autorisation et d'une gestion des sessions appropriées, qu'elles valident toutes les entrées qui traversent une limite de confiance et incluent des contrôles de sécurité pour tous les types d'API.

Des contrôles spécifiques dans cette catégorie traitent la validation de l'entrée par type de service, tels que la validation de schéma XDS pour les services Web SOAP ou la protection contre le déni de service pour les API GraphQL.

Valider le type de contenu SOAP [mis à jour dans Security Center 1.3]

Utilisez cette propriété pour activer la `glide.soap.require_content_type_xml` validation d'un type de contenu comme texte/xml et protéger contre les demandes SOAP invalides.

- Lorsqu'elle est définie sur **vrai**, elle Now Platform valide le type de contenu comme text/xml et protège contre les demandes SOAP invalides.
- Si la valeur est définie sur **faux**, toutes les valeurs de type de contenu sont autorisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.soap.require_content_type_xml`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Protection contre les demandes SOAP invalides
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Faible) Cette remédiation active la validation du type de contenu SOAP pour toutes les demandes SOAP entrantes. • Si vous utilisez un type de contenu autre que texte/xml pour les demandes entrantes, cela peut entraîner l'échec potentiel des transactions SOAP. • Si vous n'utilisez pas le type MIME correct, cela peut perturber les intégrations tierces.
Risque de sécurité	(Modéré) Lors de l'acceptation de demandes SOAP entrantes, la validation appropriée est effectuée pour s'assurer que le type de contenu pertinent est défini dans le cadre de la demande. Il limite les réponses SOAP non valides qui peuvent être considérées comme un risque pour la sécurité.
Référence	Types de contenu

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger une autorisation pour les demandes PDF [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.pdf` demandes PDF entrantes doivent requérir une authentification de base.

En savoir plus

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.pdf`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes PDF.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données PDF sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la rubrique Jeux d'importation de services Web .
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes PDF entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger l'authentification sur le processeur HTTP Gestion des événements [Nouveau dans Centre de sécurité 1.3]

Découvrez comment établir une authentification de base sécurisée pour les demandes Amazon Simple Notification Service (SNS) entrantes lorsque le module d'extension Gestion des événements (`com.glideapp.itom.snac`) est activé.

Si la `glide.basicauth.required.evtmgmthttpprocessor` propriété n'est pas définie sur la valeur recommandée, **vrai**, et que le module d'extension Gestion des événements (`com.glideapp.itom.snac`) est actif, l'authentification de base n'est pas requise pour toutes les demandes Amazon Simple Notification Service (SNS) entrantes. Cela peut entraîner un accès non authentifié aux données d'instance.

Pour corriger ce risque de sécurité, assurez-vous que `glide.basicauth.required.evtmgmthttpprocessor` cette option est définie sur**vrai** et qu'elle `com.glideapp.itom.snac` est active.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.basicauth.required.evtmgmthttpprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	API et service web
Risque de sécurité	• Score de gravité : 7 • Score CVSS : élevé • Détails du risque de sécurité : La non-définition`glide.basicauth.required.evtmgmthttpprocessor` de la valeur recommandée, vrai, et la non-activation du module d'extension entraînent la non-activation de l'authentification `com.glideapp.itom.snac` de base pour les demandes SNS entrantes. Cela peut entraîner un accès non authentifié aux données d'instance.
Dépendances et prérequis	Aucun
Références	• https://docs.aws.amazon.com/sns/latest/dg/welcome.html • Access control
Impact fonctionnel	Si `glide.basicauth.required.evtmgmthttpprocessor` elle n'est pas définie sur la valeur conseillée, Vrai, et si le module d'extension Gestion des événements (com.glideapp.itom.snac) est actif, l'authentification de base n'est pas requise pour toutes les demandes SNS entrantes des services web Amazon. Cela peut entraîner un accès non authentifié aux données d'instance.

Exiger une autorisation pour les demandes SOAP [mis à jour dans Security Center 1.3 et 1.5]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.soap` demandes SOAP entrantes doivent obtenir une autorisation de base.

En savoir plus

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.soapglide.soap.require_ws_securi`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour faire respecter l'autorisation des demandes SOAP.
Valeur recommandée	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	(Moyen) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données SOAP sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui a besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour plus d'informations, consultez Informations d'identification d'authentification de service Web SOAP et de Serveur MID et demandes SOAP.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur la source de données des demandes SOAP, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger une autorisation pour les demandes de déchargement [Mise à jour dans Security Center 1.3]

Utilisez la propriété (useUnloadFormat) pour indiquer si les `glide.basicauth.required.unl` demandes de déchargement entrantes doivent requérir une authentification de base.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.basicauth.required.unl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes de déchargement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Moyen) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données non téléchargées sur l'instance.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes de déchargement de source de données, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible. Assurez-vous que cela existe dans la sys_properties_table et qu'il `glide.basicauth.required.unl` est défini sur vrai.
Références	Authentification

Exiger une autorisation pour les demandes CSV [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.csv` demandes CSV (valeurs séparées par des virgules) entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.csv`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes CSV.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données CSV sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Pour en savoir plus, reportez-vous à la section Récupération de données à partir d'un fichier au format CSV.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes CSV entrantes, un utilisateur non autorisé peut accéder à du contenu et à des données sensibles sur l'instance cible. Assurez-vous que cela existe dans la table sys_properties et qu'il `glide.basicauth.required.csv` est défini sur vrai.
Références	Sécurité des services Web

Exiger une autorisation pour les demandes Excel [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.excel` demandes Excel entrantes doivent requérir une authentification de base.

En savoir plus

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.excel`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes Excel.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données Excel sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes Excel entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exiger une autorisation pour les demandes d'importation [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.importprocessor` demandes d'importation entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.importprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes d'importation.
Valeur recommandée	VRAI
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification lors de l'importation de sources de données dans les tables/pages d'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Récupération de données à partir d'un fichier au format CSV .
Risque de sécurité	(Modéré) Sans autorisation appropriée configurée sur les demandes d'importation de source de données, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Services web SOAP de sécurité Service web SOAP

Exiger une autorisation pour la demande JSONv2 [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.jsonv2` demandes JSONv2 entrantes doivent obtenir une autorisation de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.jsonv2`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'autorisation des demandes JSONv2.
Cote de risque de sécurité	7.5
Valeur recommandée	VRAI
Impact fonctionnel	(Moyen) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données JSON sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. • Créez un compte pour un utilisateur qui a besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour plus d'informations, reportez-vous à la rubrique Service Web JSONv2 Service Web JSONv2 .
Risque de sécurité	(Élevé) Sans l'autorisation appropriée configurée sur les demandes JSON de source de données, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification Exiger une authentification de base pour les demandes JSONv2 entrantes

Exiger une autorisation pour la demande WSDL [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.wsdl` demandes WSDL (Web Services Description Language) entrantes doivent requérir une authentification de base.

ℹ Remarque :
Si vous choisissez de ne pas exiger l'authentification de base pour les demandes WSDL entrantes, vous devez modifier les règles de contrôle d'accès (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.wsdl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes WSDL.
Valeur recommandée	VRAI
Cote de risque de sécurité	4.3
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données WSDL sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Moyen) Sans autorisation appropriée configurée sur les services Web WSDL, un utilisateur non autorisé peut accéder à du contenu/des données WSDL sensibles sur l'instance cible.
Références	Sécurité des services Web

Exiger une autorisation pour les demandes XML [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.xml` demandes XML entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.xml`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour appliquer l'authentification de base aux demandes XML.
Cote de risque de sécurité	7.5
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous forme de données XML sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Étape de l'analyseur XML .
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes XML entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification

Exiger une autorisation pour les demandes de sortie XML

Configurez cette propriété de sorte qu'une autorisation de base soit requise pour toutes les demandes XMLOutputProcessor entrantes.

Si la `glide.basicauth.required.xmloutputprocessor` propriété n'est pas définie sur la valeur recommandée, **vrai**, l'autorisation de base n'est alors pas requise pour les demandes XMLOutputProcessor entrantes, qui peuvent entraîner une divulgation d'informations non authentifiées de l'instance.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.basicauth.required.xmloutputprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	API et service web

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails **du risque** de sécurité : ne pas définir la propriété sur la valeur recommandée vrai peut entraîner une fuite d'informations sensibles de l'instance.
Dépendances et prérequis	Aucun

Exiger une autorisation pour les demandes XSD

Utilisez cette propriété pour indiquer si les `glide.basicauth.required.xsd` demandes XSD (XML Schema Definition) entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	glide.basicauth.required.xsd`glide.basicauth.required.xsd`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes XSD.
Valeur recommandée	VRAI
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système. • Il effectue cette authentification tout en récupérant les données des tables/pages sous la forme de données XSD sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Sessions non interactives .
Risque de sécurité	(Modéré) Sans autorisation appropriée configurée sur les demandes XSD entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	Authentification

Exiger une autorisation pour les demandes de script

Utilisez la propriété pour indiquer si les `glide.basicauth.required.scriptedprocessor` demandes de script entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.scriptedprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes de scripts.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.2
Impact fonctionnel	(Moyen) Ce rattrapage applique l'authentification sous la forme d'une autorisation de base. • Il effectue cette authentification lors du traitement des demandes de script sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires.
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes de script entrant, un utilisateur non autorisé accède au contenu/aux données sensibles sur l'instance cible.
Références	Authentification

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger une autorisation pour les demandes SCHEMA [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour exiger l'autorisation `glide.basicauth.required.schema` de base pour toutes les demandes du processeur de schéma de table entrante.

Le processeur Schebma de la table entrante gère les demandes de schéma entrantes pour la plateforme.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définissez `glide.basicauth.required.schema` sur la valeur **recommandée vrai pour** exiger l'autorisation de base pour toutes les demandes du processeur de schéma de table entrante. Définissez la valeur sur **faux** pour ne pas exiger l'autorisation de base pour toutes les demandes du processeur de schéma de table entrante.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.basicauth.required.schema`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour exiger l'autorisation de base pour toutes les demandes du processeur de schéma de table entrante.
Valeur recommandée	Vrai (valeur par défaut).
Type de configuration	Booléen
Risque de sécurité	(Modéré) Omettre l'authentification à partir de ce processeur entraîne un accès non authentifié aux données d'instance.

Exiger une autorisation pour les demandes RSS [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour indiquer si les `glide.basicauth.required.rss` demandes RSS entrantes doivent requérir une authentification de base.

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	`glide.basicauth.required.rss`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Pour appliquer l'authentification de base aux demandes RSS.
Valeur recommandée	VRAI
Cote de risque de sécurité	7.5
Impact fonctionnel	(Faible) Cette remédiation applique une combinaison de méthodes d'authentification, sous la forme d'une authentification de base et d'un contrôle d'accès au niveau du système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Il effectue cette authentification lors du traitement des demandes RSS sur l'instance. • Il restreint tous les utilisateurs invités qui accèdent actuellement à ces données. Le cas échéant, vous devrez peut-être créer un nouveau compte pour les utilisateurs qui ont besoin d'accéder à ce contenu, avec les autorisations de contrôle d'accès nécessaires. Pour en savoir plus, reportez-vous à la section Générateur de flux RSS .
Risque de sécurité	(Élevé) Sans autorisation appropriée configurée sur les demandes RSS entrantes, un utilisateur non autorisé peut accéder à du contenu/des données sensibles sur l'instance cible.
Références	Authentification de base RSS

Exiger une autorisation pour les demandes d'API [Mise à jour dans Security Center 1.3]

Utilisez cette propriété pour améliorer la sécurité de l'autorisation de base pour les `glide.basicauth.required.api` demandes REST entrantes.

Définissez la `glide.basicauth.required.api` propriété sur **vrai** pour exiger une autorisation pour toutes les demandes REST. Définissez la propriété sur **faux** pour contourner l'autorisation pour toutes les demandes REST.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.basicauth.required.api`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	API et service web
Objectif	Autorisation de base pour les demandes REST entrantes.
Valeur recommandée	Vrai (par défaut)
Type de configuration	Chaîne
Risque de sécurité	(Élevé) Si « glide.basicauth.required.api » n'est pas défini sur la valeur recommandée « vrai », cela désactive l'authentification de base sur la demande d'API et entraîne un accès non authentifié aux données d'instance.
Cote de risque de sécurité	8.6

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture, conception et modélisation des menaces

Ce contrôle étendu traite des considérations de conception de haut niveau et des éléments clés pour implémenter une application sécurisée. Cela couvre les locataires de la disponibilité, de l'intégrité du traitement de la confidentialité, de la non-répudiation et de la vie privée. De plus, des éléments d'un cycle de vie de développement logiciel sécurisé sont inclus.

Authentification basée sur certificat non mise en application [Nouveau dans Security Center 1.3]

La *glide.authenticate.mutual.enabled* propriété active l'authentification basée sur certificat, un type d'authentification réciproque pour les connexions REST entrantes aux API REST et SOAP dans le Now Platform.

L'authentification réciproque établit la confiance entre le serveur et le client en échangeant des certificats SSL (Secure Socket Layer) pour valider le certificat auprès d'une autorité de certification approuvée. Cela permet de vérifier qu'une source fiable se connecte au Now Platformfichier . Si cette instance n'est pas définie sur la valeur recommandée vrai, elle peut être vulnérable aux attaques de l'homme du milieu (MitM).

Pour remédier à cette menace de sécurité, activez l'authentification réciproque pour les services Web entrants. Si c'est la première fois que vous installez le module d'extension d'authentification basée sur certificat (*com.glide.auth.mutual)* pour le Now Platform, suivez les Configurer l'authentification basée sur certificat instructions. En outre, assurez-vous que la *glide.authenticate.mutual.enabled* propriété est définie sur vrai pour activer le module d'extension.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.authenticate.mutual.enabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Détails des risques de sécurité : Si cette propriété n'est pas définie sur la valeur conseillée, vrai, l'authentification basée sur certificat ne valide pas les certificats auprès d'une autorité de certification approuvée. Cela augmente les chances qu'un acteur malveillant attaque une instance à l'aide d'attaques MitM.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	• https://csrc.nist.gov/glossary/term/man_in_the_middle_attack • Authentification basée sur certificat • Configuration de l'authentification réciproque

Vérifier l'emprunt d'identité dans l'évaluation ACL dans l'application RH [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Utilisez la propriété pour empêcher un *sn_hr_core.impersonateCheck* utilisateur d'emprunter l'identité d'un autre utilisateur et d'accéder à ses informations RH.

Un paramètre sécurisé empêche un administrateur de voir les informations RH d'un autre utilisateur lorsqu'il utilise l'emprunt d'identité. Un paramètre non sécurisé pour cette propriété permet à un administrateur d'emprunter l'identité d'un utilisateur et d'accéder à des données RH telles que les résultats d'enquêtes ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été empruntée. En raison de la nature de ce type de données, telles que des informations qui ne devraient être disponibles que pour l'utilisateur lui-même, comme l'e-mail, cela n'est pas recommandé. Définir sur *sn_hr_core.impersonateCheck* vrai autorise uniquement l'accès aux informations RH lorsque l'utilisateur n'emprunte l'identité d'aucune autre personne.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_hr_core.impersonateCheck*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible • Détails du risque de sécurité : un paramètre non sécurisé pour cette propriété permet à un administrateur d'emprunter l'identité d'un utilisateur et d'accéder à des données RH telles que les résultats d'enquêtes ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été empruntée.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est définie sur vrai, elle empêche un administrateur de voir les informations RH d'un autre utilisateur lorsqu'il utilise l'emprunt d'identité. Lorsqu'elle est définie

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	sur faux, elle permet à un administrateur d'emprunter l'identité d'un utilisateur et d'accéder aux données RH telles que les résultats d'enquête ou les enregistrements d'audit avec l'accès de l'utilisateur dont l'identité a été empruntée. En raison de la nature de ce type de données, telles que des informations qui ne devraient être disponibles que pour l'utilisateur lui-même, comme un e-mail, cela n'est pas recommandé. Définir sn_hr_core.impersonateCheck sur vrai autorise uniquement l'accès aux informations RH si l'utilisateur n'emprunte l'identité d'aucune autre personne.

Désactiver les rapports publiés non authentifiés

Désactivez cette propriété pour empêcher l'utilisateur de publier des rapports ou d'y accéder. Cette propriété désactive la fonctionnalité des rapports publiés dans la génération de rapports.

Activez la publication des rapports en définissant la *glide.report.published_reports.enabled***sur vrai**.

Appliquer la sécurité aux rapports est conforme si *glide.report.published_reports.enabled* défini sur **faux**.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.report.published_reports.enabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	Désactive la fonctionnalité des rapports publiés dans la génération de rapports.
Type	vrai | faux
Valeur recommandée	**false**
Cote de risque de sécurité	6.5
Impact fonctionnel	(Moyen) L'utilisateur ne peut pas publier de rapports.
Risque de sécurité	(Modéré) Si cette propriété n'est pas activée, les utilisateurs peuvent être en mesure d'accéder à des rapports exposant des données sensibles ou de les publier. La publication d'un rapport crée une URL que tout le monde, y compris les personnes qui ne sont pas des utilisateurs, peut utiliser pour accéder au rapport. Lorsque quelqu'un accède à l'URL, le rapport est généré avec les données actuelles de l'instance.
Références	Publier un rapport

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renforcer les ACL de champs pour les demandes entrantes

Gérez le mode de validation des requêtes entrantes sur votre instance.

Utilisez la propriété pour vérifier comment les `glide.report.report_view.check_published` requêtes entrantes sont validées sur votre instance. Si la propriété est définie sur la valeur recommandée **vrai**, les ACL de champ sont vérifiées par rapport aux requêtes entrantes et rejetées si l'utilisateur n'est pas autorisé. Si la propriété est définie sur **faux**, les ACL ne sont pas vérifiées par rapport aux requêtes entrantes et continuent de s'exécuter, ce qui peut entraîner la divulgation d'informations à des parties non autorisées.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.export.query.enforce_field_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 4,4 • Score CVSS : moyen • Détails du risque de sécurité : si cette propriété est définie sur **faux**, les ACL ne sont pas vérifiées par rapport aux requêtes entrantes, ce qui peut entraîner la divulgation d'informations.
Dépendances et prérequis	Aucun

Appliquer les ACL en lecture sur les vues de rapport

Gérez la façon dont les ACL en lecture sont appliquées sur votre instance.

Utilisez la `glide.report.report_view.read_acl` propriété pour appliquer l'ACL de lecture (niveau de table) aux fonctions de génération de rapports lorsqu'il n'y a pas d'ACL de vue de rapport dans la table ou le champ. Si cette propriété n'est pas définie sur **appliquer**, les ACL peuvent être contournées, ce qui entraîne une fuite d'informations sensibles.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.report.report_view.read_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	appliquer
Valeur par défaut	appliquer
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur **Appliquer,** les ACL peuvent être contournées.
Dépendances et prérequis	Aucun

Définir les adresses IP internes autorisées ServiceNow [mis à jour dans Security Center 1.3 et 1.5]

Utilisez la `glide.ip.authenticate.strict` propriété pour spécifier les plages IP qui peuvent établir des connexions entrantes sur une instance.

Si `glide.ip.authenticate.strict` la valeur est définie sur vrai, seules les plages IP spécifiées dans `glide.ip.authenticate.allow.secured` peuvent établir des connexions entrantes sur une instance. Cette propriété contient une liste des plages IP internes ServiceNow essentielles uniquement (VPN sécurisé, DC).

Si `glide.ip.authenticate.allow.secured` elle n'est pas définie sur la valeur recommandée « 10.0.0.0/8, 37.98.232.0/21, 103.23.64.0/22, 149.96.0.0/17, 149.96.0.0/16, 199.91.136.0/21, 148.139.0.0/16, 127.0.0.1, 0:0:0:0:0:0:0:1 », elle peut autoriser des sources non approuvées en dehors du DataCenter ServiceNow et du VPN sécurisé à accéder aux points de terminaison de surveillance sensibles sur les instances.

⚠ Avertissement :
La valeur de cette propriété est un aucun remplacement de base de données. Il ne peut pas être modifié ou remplacé.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ip.authenticate.strict`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	Permet aux employés de ServiceNow d'accéder à l'instance uniquement par le biais d'un ensemble sécurisé de plages IP
Valeur recommandée	VRAI
Cote de risque de sécurité	4.3
Impact fonctionnel	(Faible) Si cette propriété n'est pas activée, les employés ServiceNow peuvent accéder à l'instance du client via toutes les plages IP. L'activation de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	propriété restreint l'accès à un ensemble sécurisé de plages IP (VPN sécurisé, DC). **Remarque :** Si vous définissez cette propriété sur `vrai`, le Now Platform utilise une propriété plus restrictive `glide.ip.authenticate.allow.secured` au lieu de la propriété de restriction IP de surveillance des performances (`glide.ip.authenticate.allow.secured`) pour un ensemble de plages IP pouvant accéder à l'instance.
Risque de sécurité	(Faible) Exposition inutile de l'accès aux instances à un groupe plus large de personnes.
Référence	Authentification basée sur la plage IP

Remarque :
Une règle de refus de tout doit être ajoutée au contrôle d'accès IP pour restreindre l'accès de toute adresse IP non ajoutée au contrôle d'accès IP. Toutes les adresses IP autorisées requises doivent ensuite être ajoutées au contrôle d'accès IP.

Désactiver le comportement JQuery hérité [Mise à jour dans Securty Center 1.3]

Le permet d'empêcher l'utilisation `glide.jquery.legacy` d'anciennes versions jQuery prédéfinies, ce qui introduirait des vulnérabilités non corrigées dans la bibliothèque.

Définissez `glide.jquery.legacy` sur la valeur **recommandée faux pour** empêcher l'utilisation d'anciennes versions jQuery prédéfinies qui introduisent des vulnérabilités non corrigées dans la bibliothèque. Définissez la valeur sur **vrai** pour autoriser les versions JQuery prédéfinies.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.jquery.legacy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	Prévenir les risques de sécurité potentiels découlant des attaques sur les vulnérabilités détectées dans les versions de bibliothèque jQuery obsolètes.
Valeur recommandée	Faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) Empêchez l'utilisation d'anciennes versions jQuery prédéfinies qui introduisent des vulnérabilités non corrigées dans la bibliothèque. La propriété système est une sécurité au cas où des organisations dépendent des versions non corrigées d'AngularJS pour exécuter leurs implémentations personnalisées.
Cote de risque de sécurité	7.1

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver le comportement hérité de clôture du champ d'application GlideRecord [Nouveau dans Security Center 1.3]

La `glide.record.legacy_cross_scope_access_policy_in_script` propriété désactive la clôture du champ d'application, ce qui permet aux applications du champ d'application d'accéder aux interfaces de script globales. Il a été créé en tant que correctif pour l'accès entre champs d'application de GlideRecord.

GlideRecord fournit un accès de création et de mise à jour entre champs d'application aux tables qui n'ont pas été configurées avec ce niveau d'accès. Afin d'éviter que les clients ne voient leurs applications interrompues lorsque ce comportement d'accès inclus dans le périmètre a été corrigé, la `glide.record.legacy_cross_scope_access_policy_in_script` propriété a été créée. Lorsque cette propriété est définie sur vrai, l'accès entre périmètres revient au comportement hérité, qui n'est pas sécurisé.

Cette propriété désactive la clôture du champ d'application, ce qui permet aux applications du champ d'application d'accéder aux interfaces de script globales. L'application de la clôture du champ d'application garantit que les applications ne peuvent accéder qu'aux ressources explicitement accordées ou dans le cadre de leur champ d'application désigné, appliquant ainsi le principe du moindre privilège.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.record.legacy_cross_scope_access_policy_in_script`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	vrai (lorsque la propriété n'existe pas dans la table sys_properties.)
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 5 • Score CVSS : moyen • Détails des risques de sécurité : la définition du champ d'application garantit que les applications ne peuvent accéder qu'aux ressources avec un accès explicite ou dans leur champ d'application, conformément au principe des privilèges minimum. La désactivation de cette fonctionnalité peut avoir des répercussions sur la confidentialité, la disponibilité et l'intégrité.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver le comportement AngularJS hérité [mis à jour dans Security Center 1.3]

Utilisez la propriété pour vous protéger contre les `glide.angular.legacy` risques de sécurité potentiels découlant des attaques sur les vulnérabilités détectées dans les versions de bibliothèque AngularJS obsolètes.

Définissez `glide.angular.legacy` sur la valeur **recommandée faux pour** empêcher l'utilisation des anciennes versions AngularJS prédéfinies. Définissez la propriété sur **true** pour utiliser les anciennes versions AngularJS prédéfinies.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.angular.legacy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Architecture, conception et modélisation des menaces
Objectif	La propriété système est une sécurité au cas où des organisations dépendent des versions non corrigées d'AngularJS pour exécuter leurs implémentations personnalisées.
Valeur recommandée	Faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) L'utilisation d'anciennes versions d'AngularJS peut entraîner des risques de sécurité découlant des attaques sur les vulnérabilités détectées dans les versions de bibliothèque AngularJS obsolètes.
Cote de risque de sécurité	7.1

Exiger une autorisation pour l'API REST du courtier en données [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour exiger l'autorisation `glide.basicauth.required.databrokerrestapiprocessor` de base pour toutes les demandes API REST du courtier en données entrantes.

Si cette propriété est définie sur **true**, alors l'autorisation est appliquée. S'il est défini sur **faux**, aucune autorisation n'est utilisée, ce qui peut entraîner une fuite d'informations sensibles de votre instance.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.basicauth.required.databrokerrestapiprocessor`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Architecture, conception et modélisation des menaces
Risque de sécurité	• Score de gravité : 8,6 • Score CVSS : élevé • Détails du risque de sécurité : Si la propriété est définie sur **faux**, l'authentification API n'est pas appliquée, ce qui permet à un acteur malveillant d'accéder à des données sensibles.
Dépendances et prérequis	Aucun

Refuser par défaut en cas d'ACL vides [mis à jour dans Securty Center 1.3]

Utilisez la `glide.sm.default_mode` propriété pour contrôler le comportement par défaut du gestionnaire de sécurité lorsqu'il détecte que des règles ACL font partie des règles ACL d'une table à caractère générique.

Lorsque le module d'extension Paramètres de sécurité élevée (com.glide.high_security) est activé lors de l'installation initiale de l'instance, il crée cette propriété et des règles ACL génériques voient le jour. Pour fournir un accès basé sur les rôles aux tables système, ces règles contrôlent un nombre important d'ACL et les opérations basées sur les enregistrements les plus courantes :

- Lecture
- Écriture
- Créer
- Supprimer

À moins que vous n'utilisiez le module d'extension de haute sécurité avec l'option de refus par défaut activée, de nombreuses tables ne sont pas protégées. Le Now Platform utilise un modèle de sécurité de refus par défaut qui empêche les utilisateurs non administrateurs d'accéder aux objets à moins qu'ils ne répondent à une règle ACL correspondante. À l'aide de ce modèle, il supprime de nombreux vecteurs d'attaque, tels que les scripts non sécurisés.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sm.default_mode`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Architecture, conception et modélisation des menaces
Objectif	La meilleure pratique en matière de sécurité consiste à restreindre l'accès aux tables par un utilisateur non autorisé. • Si aucune règle ACL n'est en place pour les tables, cette propriété garantit qu'au moins les ACL génériques sont validées pour toute opération CRUD effectuée sur la table/le champ. • Ces règles restreignent les opérations de lecture, d'écriture, de création et de suppression sur toutes les tables, sauf si l'utilisateur a le rôle administrateur ou répond aux exigences d'une autre règle ACL de table.
Valeur recommandée	refuser
Impact fonctionnel	(Élevé) Si vous définissez cette propriété sur **Autoriser**, les règles ACL de table à caractère générique autorisent les opérations CRUD sur toutes les tables, sauf s'il existe des règles ACL de table spécifiques en place pour restreindre de telles opérations. **Remarque :** Ce module d'extension n'est pas conçu pour les instances existantes, car il peut modifier l'accès de sécurité aux tables déjà utilisées dans un environnement de production.
Risque de sécurité	8.8
Références	Propriété de refus par défaut

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Authentification

La catégorie d'authentification couvre les principaux éléments de l'authentification moderne pour confirmer qu'une entité et ses revendications sont authentiques et correctes, résistent à l'usurpation d'identité et empêchent l'interception des mots de passe.

La norme ASVS s'appuie sur la spécification NIST 800-63b (https://pages.nist.gov/800-63-3/sp800-63b.html) pour cette section.

L'authentification comprend la politique de mot de passe, les contrôles et le stockage, l'implémentation appropriée des authentificateurs et l'implémentation appropriée des vérificateurs hors bande ou à usage unique.

Activer l'authentification multifacteur basée sur les rôles [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour appliquer l'authentification multifacteur (MFA) basée sur les `glide.authenticate.multifactor` rôles à tous les utilisateurs affectés à des rôles spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer l'authentification multifacteur en fonction des rôles affectés à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » sont affectés à un utilisateur dans la liste des rôles multifacteur, MFA est appliquée.

- Définissez cette propriété sur **vrai** pour appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
- Définissez cette propriété sur **faux** pour désactiver l'authentification multifacteur basée sur les rôles pour tous les utilisateurs affectés à des rôles spécifiques.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.authenticate.multifactor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
Type	vrai/faux
Valeur recommandée	`true`
Dépendances de Sécurité	**Activez l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Cote de risque de sécurité	7.2
Impact fonctionnel	(Moyen) L'activation de cette propriété améliore l'expérience de l'utilisateur. Il agit comme une couche supplémentaire de protection et de sécurité contre les informations d'identification compromises.
Risque de sécurité	(Modéré) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé aux données sensibles.
Références	Configurer les critères multifacteur basés sur les rôles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la récupération de compte [mis à jour dans Security Center 1.3 et 1.5]

La `glide.sso.acr.enabled` propriété contrôle la fonctionnalité de récupération de compte.

Défini sur `glide.sso.acr.enabled` la valeur **recommandée vrai pour** permettre la récupération du compte par ID d'utilisateur possible. Définissez la valeur sur **faux** pour interdire la récupération de compte par ID d'utilisateur.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sso.acr.enabled`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Contrôle la fonctionnalité de récupération de compte par ID d'utilisateur.
Valeur recommandée	Vrai (par défaut)
Type de configuration	Booléen
Risque de sécurité	Critique (si cette propriété n'est pas activée, les utilisateurs ne seront pas autorisés à récupérer leur compte par ID d'utilisateur.
Cote de risque de sécurité	9.1
Références	Pour plus d'informations, consultez Récupération de compte (ACR).

Exiger le brouillage de l'interface utilisateur de l'application mobile classique [Mise à jour dans Security Center 1.3]

Utilisez cette `glide.ui.m.blur_ui_when_backgrounded` propriété pour griser tous les champs de l'instantané lors de l'enregistrement de l'image en processus de tâche d'arrière-plan.

Sur les appareils Android, le système d'exploitation Android prend une capture d'écran pour une utilisation dans le menu des tâches récentes lorsque l'application est envoyée en arrière-plan. Les utilisateurs peuvent également prendre des captures d'écran manuelles de l'application, qui sont stockées publiquement sur l'appareil.

Sur les appareils iOS, le système d'exploitation iOS permet également aux applications d'enregistrer un fichier image. Ce fichier représente le dernier écran vu par l'utilisateur lorsque l'application est envoyée en arrière-plan. Bien que l'objectif soit d'offrir une meilleure expérience utilisateur, cela crée également un risque de sécurité, car les images sont enregistrées sous forme de fichiers image PNG.

Remarque :
Cette configuration ou ce paramètre est basé sur l'instance. L'utilisateur doit donc se connecter à l'instance avec la propriété configurée.

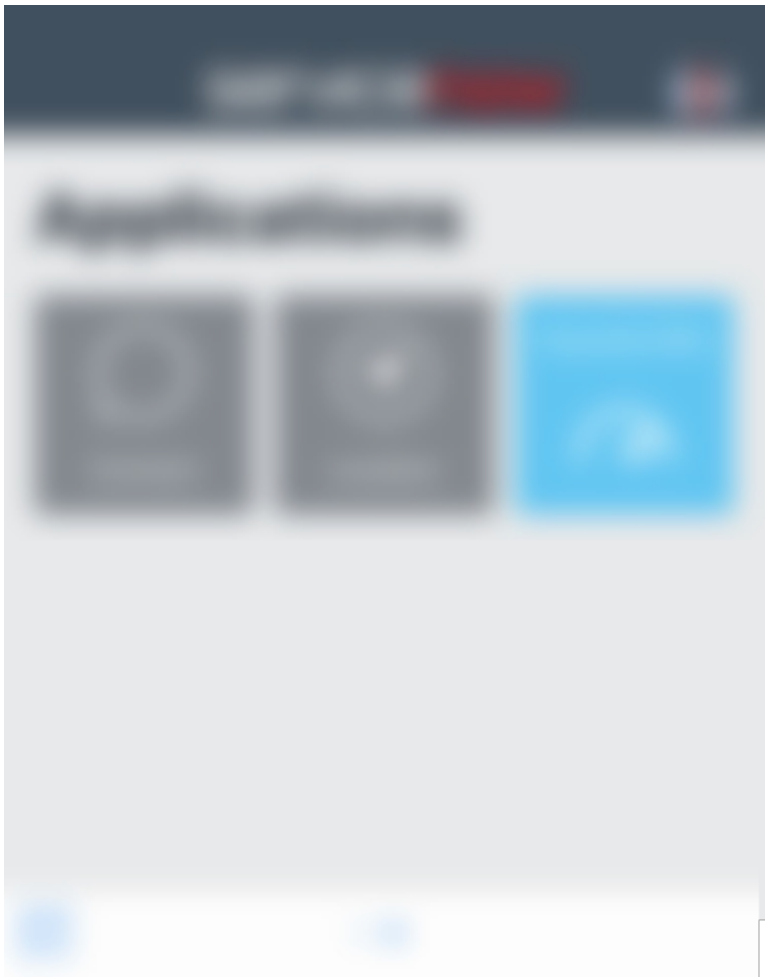
Pour masquer tous les champs de l'instantané dans l'application ServiceNow Classic, consultez Configurer l'option de floutage de l'application pour améliorer la sécurité .

Exemple

Lorsque vous définissez cette propriété sur vrai, l'application background est brouillée pour les appareils iOS et noircie pour les appareils iOS Android.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



En savoir plus

Attribut	Description
Nom de la propriété/du module d'extension	*glide.ui.m.blur_ui_when_backgrounded*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Pour griser tous les champs de l'instantané lors de l'enregistrement de l'image pendant le processus de tâche d'arrière-plan.
Valeur recommandée	VRAI
Cote de risque de sécurité	2.4
Impact fonctionnel	(Faible) Si la *glide.ui.m.blur_ui_when_backgrounded* propriété est définie sur true, les applications natives utilisent le paramètre défini sur le serveur pour flouter l'écran lorsque l'application entre en arrière-plan.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Il floute les captures d'écran prises par iOS et Android lorsque l'application entre en arrière-plan. • L'expérience utilisateur peut être affectée, car il ne peut pas voir le contenu lorsque l'application est envoyée en arrière-plan.
Risque de sécurité	(Moyen) Un appareil compromis (jailbreaké) permettrait à un attaquant d'avoir un accès complet au système de fichiers, avec un accès aux fichiers/instantanés contenant des informations sensibles.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver l'authentification sans mot de passe

Utilisez cette propriété pour empêcher les `glide.login.no_blank_password` utilisateurs de se connecter à la Now Platform avec des mots de passe vierges ou en laissant le champ **Mot de passe** vide.

Même si l'administrateur attribue délibérément une valeur vide ou un mot de passe vide dans les enregistrements utilisateur, un utilisateur ne peut pas se connecter sans fournir une valeur dans le champ **Mot de passe** .

En savoir plus

Attribut	Description
Nom de la propriété	`glide.login.no_blank_password`
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Assurer une authentification forte car les noms d'utilisateur sont parfois faciles à deviner au sein d'une organisation.
Valeur recommandée	VRAI
Impact fonctionnel	(Faible) Les opérations ne doivent pas utiliser de mots de passe vierges, car cela est considéré comme un risque de sécurité critique. Toutefois, s'il existe un cas valable pour une telle utilisation, il existe une possibilité de panne. Les utilisateurs avec des mots de passe vides ne peuvent pas se connecter à l'instance.
Risque de sécurité	(Élevé) Un attaquant est en mesure de se connecter à l'instance avec les noms d'utilisateur par défaut, ou par personne/groupe spécifique (généralement prénom.nom) sans mot de passe. Cela est considéré comme un risque de sécurité critique, car cela permettrait à un utilisateur public de violer la confidentialité et l'intégrité des données de l'instance.

Ne pas appliquer la politique de mot de passe lors de la connexion

Gérez la façon dont la complexité des mots de passe est gérée dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez cette`glide.apply.password_policy.on_login` propriété pour gérer la complexité des mots de passe. Si cette propriété est définie sur **faux**, il n'y a pas d'application de complexité de mot de passe pendant la connexion. Si elle est définie sur **vrai**, elle applique la complexité du mot de passe, ce qui peut entraîner des problèmes de conformité à la politique de l'organisation. Au lieu d'appliquer la complexité du mot de passe, la norme de vérification de la sécurité des applications (ASVS) suggère d'appliquer une longueur minimale de 12 caractères pour la longueur du mot de passe.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.apply.password_policy.on_login`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 4,4 • Score CVSS : moyen • Détails des risques de sécurité : définir cette propriété sur **vrai** pourrait entraîner une complexité de mot de passe et entraîner des problèmes de conformité de l'organisation.
Dépendances et prérequis	Aucun

Activer un contrôle de validation de mot de passe de liste de refus

Gérer les mots de passe de la liste de refus dans la table Mot de passe exclu.

Utilisez cette propriété pour surveiller les `glide.enable.blacklist_password` mots de passe de la liste de refus. Lorsque la propriété est définie sur **Vrai**, le mot de passe de l'utilisateur est vérifié par rapport à une liste de mots de passe de la liste de refus pour les empêcher d'utiliser un mot de passe provenant d'un ensemble de mots de passe violés. L'administrateur peut gérer la liste en insérant des mots de passe dans la table Mot de passe exclu.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.enable.blacklist_password`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Authentification
Dépendances et prérequis	Aucun
Références	Exclure les mots de passe via des politiques de mot de passe sur votre instance

Activer le captcha pour l'inscription des utilisateurs externes [Mise à jour dans Security Center 1.5]

Contrôle *sn_ext_usr_reg.captchaEnabled* si CAPTCHA est validé pour l'inscription de l'utilisateur externe.

Définissez *sn_ext_usr_reg.captchaEnabled* sur la valeur **recommandée vrai pour** éviter les attaques de création automatique de compte nécessitant un CAPTCHA pour l'enregistrement des utilisateurs externes. Définissez la valeur sur **faux** pour ne pas nécessiter de CAPTCHA pour l'inscription de l'utilisateur externe.

En savoir plus

Attribut	Description
Nom de la propriété	*sn_ext_usr_reg.captchaEnabled*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Cette propriété permet d'activer ou de désactiver la validation CAPTCHA lors de l'inscription d'utilisateurs externes sur des portails tels que CSP, Communauté. Cela est également utilisé dans les applications de magasin comme VAM et CSM Guest Walkup pour activer/désactiver le captcha.
Valeur recommandée	Vrai
Type de configuration	Booléen
Risque de sécurité	(Faible) La propriété contrôle l'activation de CAPTCHA lors de l'inscription de l'utilisateur externe. Une valeur unitaire peut entraîner une faille de sécurité.
Cote de risque de sécurité	3.7

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer CAPTCHA dans la réinitialisation du mot de passe

Utilisez la propriété pour activer ou désactiver l'exigence *password_reset.captcha.ignore* d'un défi CAPTCHA lorsqu'un utilisateur réinitialise son mot de passe.

Définissez *password_reset.captcha.ignore* sur la valeur **recommandée faux pour** exiger un défi CAPTCHA pour qu'un utilisateur réinitialise son mot de passe. Définissez la valeur sur **vrai** pour ignorer l'option CAPTCHA pour une réinitialisation du mot de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les CAPTCHA aident à prévenir les attaques d'automatisation en invitant l'utilisateur à un défi-réponse auquel les systèmes automatisés ne répondent pas facilement. Si CAPTCHA est désactivé, une personne malveillante peut avoir plus de succès lors d'attaques automatisées contre la fonctionnalité de réinitialisation du mot de passe.

Remarque :
Cette propriété est utilisée uniquement pour l'automatisation de la réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.captcha.ignore`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Cette propriété est utilisée pour activer ou désactiver la validation CAPTCHA pendant la réinitialisation du mot de passe.
Valeur recommandée	faux
Type de configuration	Booléen
Risque de sécurité	(Modéré) Une valeur unitaire peut entraîner une faille de sécurité.
Cote de risque de sécurité	5.5

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer l'OTP d'e-mail pour l'authentification multifacteur

Gérez la façon dont l'authentification à deux facteurs est appliquée sur votre instance.

Utilisez cette`glide.authenticate.multifactor.email.otp.enabled` propriété pour contrôler si un jeton pour l'authentification à deux facteurs est envoyé par e-mail. L'e-mail est considéré comme un facteur MFA faible auquel un attaquant est plus susceptible d'accéder pour contourner le MFA. En définissant cette propriété sur **faux**, le risque qu'un attaquant contourne l'authentification multifacteur lorsqu'il a compromis le mot de passe d'un utilisateur est réduit.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.multifactor.email.otp.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	VRAI
Catégorie	Authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails des risques de sécurité : définir cette propriété sur **faux** réduit le risque qu'un acteur malveillant contourne l'authentification à deux facteurs.
Dépendances et prérequis	Aucun
Références	Authentification multifacteur par e-mail

Activer les contrôles de la politique de réinitialisation du mot de passe

Utilisez la propriété **glide.enable.password_policy** pour activer les vérifications de la politique de mot de passe chaque fois qu'un utilisateur change son mot de passe à l'aide de l'interface utilisateur.

Pour définir la politique de mot de passe à utiliser une fois cette propriété activée, reportez-vous à la section Activer les politiques de mot de passe sur votre instance.

Remarque :
La **glide.enable.password_policy** ne s'applique pas lorsqu'un administrateur modifie un mot de passe ou ajoute un utilisateur via un script.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.enable.password_policy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Pour appliquer la politique de mot de passe au moment du changement de mot de passe.
Valeur recommandée	true (pour les mots de passe de complexité élevée)
Cote de risque de sécurité	7.4
Impact fonctionnel	(Moyen) Définir la propriété sur vrai active les vérifications de la politique de mot de passe lorsqu'un utilisateur réinitialise son mot de passe.
Risque de sécurité	(Modéré) Sans politique de mot de passe, un utilisateur peut créer un mot de passe faible, ce qui augmente la probabilité qu'un adversaire accède à l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étapes à configurer

Si vous configurez ce paramètre dans la page Configuration de la conformité à la sécurisation renforcée dans Centre de sécurité de l'instance :

1. Sous **Moyen**, sélectionnez **Gestion des sessions**.
2. Dans le paramètre **Activer la vérification de la politique de réinitialisation du mot de passe** , sélectionnez **Moyen** pour les mots de passe de complexité moyenne ou **Fort** pour les mots de passe plus robustes et de complexité supérieure. La sélection de l'une de ces options définit la propriété **glide.enable.password_policy** sur true et démarre un workflow qui met automatiquement à jour votre politique de mot de passe.

En outre, vous pouvez définir la propriété système pour activer les `glide.apply.password_policy.on_login` vérifications de la politique de mot de passe au moment de la connexion.

Activer l'accès à la session basé sur des politiques pour mobile [Nouveau dans Security Center 1.5]

Utilisez le module d'extension Zero Trust - Policy Based Session Access pour contrôler si les utilisateurs s'authentifiant via une application mobile verront leurs rôles réduits.

Le module d'extension Zero Trust - Policy Based Session Access permet aux administrateurs de sécurité de réduire l'accès des utilisateurs à une session en fonction de paramètres tels que l'adresse IP, l'emplacement, l'identification des attributs de fournisseur et les attributs de l'utilisateur avec des politiques d'authentification adaptative. Lorsque ce module d'extension est activé ou défini sur vrai, les rôles des utilisateurs s'authentifiant via un équipement mobile sont restreints en fonction des politiques du module d'extension. Les administrateurs d'instance peuvent souhaiter restreindre l'accès aux privilèges élevés lorsque les utilisateurs s'authentifient via un équipement mobile, car cela pourrait indiquer un environnement non sécurisé pour les opérations sensibles.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.session_access.mobile.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Contrôle d'accès
Risque de sécurité	• Score de gravité : 4,7 • Score CVSS : moyen • Détails du risque de sécurité : si ce paramètre de sécurisation renforcée est défini sur vrai, l'accès à la session basé sur des politiques est appliqué sur l'instance pour les connexions mobiles, et les utilisateurs qui ne proviennent pas d'un environnement approuvé ou qui n'utilisent pas d'appareils de confiance voient leur rôle avec des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	privilèges réduits. Vrai est le paramètre sécurisé. Si ce paramètre est configuré sur faux, l'accès à la session basé sur des politiques est désactivé et les utilisateurs continuent d'avoir des rôles complets, y compris les rôles à privilèges élevés comme administrateur, à tout moment.
Dépendances et prérequis	Aucun
Impact fonctionnel	Si l'administrateur a configuré la politique d'accès à la session sur l'instance, les rôles des utilisateurs seront réduits après la connexion mobile s'ils ne proviennent pas d'un environnement approuvé ou s'ils n'utilisent pas d'appareil de confiance.
Références	Authentification adaptative

Activer SSL dans LDAP Authentication

Gérez le chiffrement des demandes d'authentification LDAP sur votre instance.

Utilisez la`glide.ldap.use.ssl` propriété pour activer ou désactiver le chiffrement TLS pour les demandes d'authentification LDAP envoyées sur le réseau. Si cette propriété n'est pas définie sur la valeur conseillée, **vrai**, LDAP Authentication est susceptible de subir une attaque de l'homme du milieu.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ldap.use.ssl`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails des risques de sécurité : définir cette propriété sur **faux** rend LDAP Authentication vulnérable à une attaque de l'homme du milieu.
Dépendances et prérequis	Aucun
Références	Intégration LDAP

Minimiser la durée d'expiration du lien d'Inscription de l'utilisateur externe [Mise à jour dans Security Center 1.3 et 1.5]

Gérez le nombre de jours pendant lesquels un lien d'inscription est accessible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez la *sn_ext_usr_reg.Reg_link_expiration_days* propriété pour gérer qui peut accéder à un lien d'inscription. Si le lien est défini sur la valeur conseillée de **3**, un lien d'inscription peut être utilisé par une autre personne que l'utilisateur prévu si le lien est détecté à une date ultérieure.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_ext_usr_reg.Reg_link_expiration_days*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Entier
Valeur recommandée	3
Valeur par défaut	3
Catégorie	Authentification
Risque de sécurité	• Score de gravité : moyen • Score CVSS : 6,6 • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur l'entier 3, un utilisateur non intentionnel peut utiliser le lien d'inscription.
Dépendances et prérequis	Aucun

Gestion des échecs de tentatives de connexion

Deux actions des scripts sont disponibles afin qu'un administrateur de site puisse gérer le nombre de tentatives de mot de passe incorrect pour un utilisateur avant d'être bloqué par le Now Platform. Vous pouvez activer l'une ou l'autre de ces actions de script pour gérer les échecs de tentative de connexion.

En savoir plus

Attribut	Description
Nom de la propriété/du module d'extension	N/A
Type de configuration	Politique système > Actions des scripts
Catégorie	Authentification
Objectif	Pour appliquer une politique stricte en cas d'échec de tentative de connexion afin d'éviter l'attaque par force brute des informations d'identification.
Valeur recommandée	Actif
Cote de risque de sécurité	7.3
Impact fonctionnel	(Faible) Cette remédiation permettrait à l'administrateur de l'instance de surveiller et de signaler tout accès utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	malveillant. Aucun impact sur la fonctionnalité, uniquement un changement de l'expérience utilisateur.
Risque de sécurité	(Modéré) Appliquez une stratégie de journalisation et d'audit définie afin de pouvoir identifier les activités suspectes et agir en temps opportun.

Étapes à configurer

1. Accédez à la **Politique système** > **Actions des scripts.**
2. Recherchez le nom `*SNC User`.
3. Pour activer la gestion des échecs de tentatives de connexion, changez l'état Actif des actions des `SNC User Lockout Check with Auto Unlock` scripts ou `SNC User Lockout Check` des scripts de **faux** à **vrai**.
4. Pour réinitialiser le compteur d'échecs de connexion après une connexion réussie, vous pouvez activer l'action des `SNC User Clear` scripts.

Maximiser la durée du délai d'expiration de déverrouillage en cas d'échec de la connexion [Mise à jour dans Security Center 1.3]

Deux actions des scripts sont disponibles afin qu'un administrateur de site puisse gérer le nombre de tentatives de mot de passe incorrect pour un utilisateur avant d'être bloqué par le Now Platform. Vous pouvez activer l'une ou l'autre de ces actions de script pour gérer les échecs de tentative de connexion.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.user.unlock_timeout_in_mins`
Type de configuration	Politique système > Actions des scripts
Catégorie	Authentification
Objectif	Pour appliquer une politique stricte en cas d'échec de tentative de connexion afin d'éviter l'attaque par force brute des informations d'identification.
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Cette remédiation permettrait à l'administrateur de l'instance de surveiller et de signaler tout accès utilisateur malveillant. Aucun impact sur la fonctionnalité, uniquement un changement de l'expérience utilisateur.
Risque de sécurité	(Modéré) Appliquez une stratégie de journalisation et d'audit définie afin de pouvoir identifier les activités suspectes et agir en temps opportun.

Étapes à configurer

1. Accédez à la **Politique système** > **Actions des scripts.**
2. Recherchez le nom `*SNC User`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Pour activer la gestion des échecs de tentatives de connexion, changez l'état Actif des actions des *SNC User Lockout Check with Auto Unlock* scripts ou *SNC User Lockout Check* des scripts de **faux** à **vrai**.
4. Pour réinitialiser le compteur d'échecs de connexion après une connexion réussie, vous pouvez activer l'action des *SNC User Clear* scripts.

Exiger le brouillage de l'interface utilisateur de l'application mobile [Mise à jour dans Security Center 1.3]

Configurez la *glide.sg.blur_ui_when_backgrounded*propriété de sorte que l'interface utilisateur de l'application soit floue lorsque l'application est en cours d'exécution en arrière-plan.

Si cette propriété n'est pas définie sur la valeur conseillée, **vrai**, l'interface utilisateur de l'application mobile est visible lorsqu'elle est affichée à partir du commutateur d'application. L'interface utilisateur est toujours visible même lorsque l'application est en cours d'exécution en arrière-plan, ce qui offre un niveau de sécurité et de confidentialité inférieur aux utilisateurs finaux.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.sg.blur_ui_when_backgrounded*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 2,4 • Score CVSS : faible • Détails des risques de sécurité : définir la valeur sur **vrai** accroit le niveau de confidentialité sur l'appareil local en floutant l'interface utilisateur lorsque l'application est en cours d'exécution en arrière-plan.
Dépendances et prérequis	Aucun
Références	Brouillage de l'interface utilisateur mobile

Notifier les utilisateurs pendant le processus de réinitialisation/changement de mot de passe

Utilisez cettepropriété pour permettre aux utilisateurs finaux de réinitialiser ou de changer les mots de passe à l'aide d'un processus en libre-service.

Cette propriété permet à un utilisateur final de réinitialiser ou de modifier un mot de passe à l'aide d'un processus en libre-service. Votre organisation peut également implémenter un processus qui nécessite qu'un agent du Centre de services réinitialise les mots de passe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pour les utilisateurs finaux. Si un processus de modification et/ou de réinitialisation du mot de passe n'informe pas les utilisateurs lors de la mise à jour du mot de passe, un acteur malveillant peut être en mesure de bloquer l'accès de cet utilisateur à son compte à son insu. Cela donnerait à l'acteur malveillant plus de temps pour effectuer des activités malveillantes. Assurez-vous que le processus de réinitialisation du mot de passe informe les utilisateurs en cas de changement ou réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la configuration	*pwd_process.change, pwd_process.reset*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails du risque de sécurité : un acteur malveillant peut être en mesure de bloquer l'accès d'un utilisateur à son compte à son insu si aucune notification ne lui est envoyée lors de la réinitialisation d'un changement de mot de passe.
Dépendances et prérequis	Aucun

Supprimer les informations d'identification de la page d'accueil

Modifiez le contenu par défaut sur la page d'accueil pour supprimer les informations d'identification par défaut.

Deux enregistrements **de connexion** sont installés dans le cadre des données de démonstration du module d'extension CMS.

Remarque :
Si vous n'installez pas les données de démonstration pour une instance, ces enregistrements n'existent pas. Dans ce cas, la configuration est considérée comme conforme à la sécurité conformément aux pratiques de sécurité recommandées.

En savoir plus

Attribut	Description
Nom	*How to login*
Type de configuration	Table : sys_home
Catégorie	Authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour supprimer les informations d'identification par défaut de la page d'accueil qui ont été ajoutées avec des données de démonstration.
Valeur recommandée	Faux ou nul si aucune donnée de démonstration n'a été utilisée.
Valeur par défaut	Aucun. Il s'agit d'une configuration de table, pas d'une propriété Glide. Par conséquent, il n'y a pas de valeur pour la valeur par défaut.
Type de configuration	Booléen
Risque de sécurité	(Modéré) Des données de démonstration sont fournies pour le module d'extension CMS, qui comprend deux mots de passe par défaut inclus sur la page d'accueil. Si cette option n'est pas supprimée, un personne malveillante non autorisée peut accéder à l'instance.
Références	https://support.servicenow.com/kb_view.do?sysparm_article=KB0550107 Welcome pages

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser le nombre maximal de SMS de réinitialisation du mot de passe par jour [Mise à jour dans Security Center 1.3]

Gérez le nombre maximal de codes SMS envoyés pour vérification par jour par l'utilisateur.

La`password_reset.sms.max_per_day` propriété représente le nombre maximal de codes SMS qui peuvent être envoyés quotidiennement pour vérification par un utilisateur.

En savoir plus

Attribut	Description
Nom de la configuration	`password_reset.sms.max_per_day`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	10
Valeur par défaut	10
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails des risques de sécurité : Si cette propriété n'est pas définie sur la valeur recommandée de **10** ou moins, il est plus facile d'effectuer une attaque par force brute du code SMS.
Dépendances et prérequis	Aucun

Minimiser la durée d'expiration de la demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

Il `password_reset.request.expiry` désigne la période en minutes pendant laquelle un utilisateur doit effectuer le processus de réinitialisation du mot de passe.

Remarque :
Le paramètre de la propriété est prioritaire sur le `password_reset.request.expiry` paramètre de `glide.pwd_reset.onetime.token.validity`la propriété dont la valeur par défaut est de 12 heures.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.expiry`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Désigne la période en minutes pendant laquelle un utilisateur doit effectuer le processus de réinitialisation du mot de passe.
Valeur recommandée	Définir sur un nombre entier de **10** ou moins. La valeur par défaut est de 10.
Type de configuration	Valeurs entières
Risque de sécurité	(Modéré) Si la propriété n'est pas définie sur la valeur recommandée de 10 ou moins, cela augmente la possibilité pour quelqu'un d'autre de deviner et d'utiliser la demande et de tenter de réinitialiser le mot de passe.
Cote de risque de sécurité	4.2
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser le nombre maximal autorisé de tentatives de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

Le `password_reset.request.max_attempt` permet de contrôler le nombre maximal de tentatives infructueuses pour qu'un utilisateur puisse réinitialiser ou changer son mot de passe avant d'être verrouillé pour une période donnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.max_attempt`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Désigne le nombre maximal de tentatives infructueuses de réinitialisation du mot de passe qui peuvent avoir lieu avant que l'utilisateur ne soit exclu du processus de réinitialisation du mot de passe. La période de verrouillage est déterminée par la valeur de `password_reset.request.max_attempt_window`.
Valeur recommandée	Défini sur une valeur entière positive inférieure à trois. La valeur par défaut est de **3**. Lorsque vous déterminez la limite de la plage supérieure de la propriété, tenez compte de la tâche que l'utilisateur est en train d'effectuer.
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de **« 3** » ou sur une autre valeur faible raisonnable, une attaque par force brute contre le processus de réinitialisation du mot de passe peut se produire.
Cote de risque de sécurité	7.5
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée de la fenêtre de tentatives maximales de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

La `password_reset.request.max_attempt_window` propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit attendre pour réinitialiser ou changer son mot de passe après avoir dépassé le nombre maximal de tentatives infructueuses défini avec la `password_reset.request.max_attempt` propriété.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.max_attempt_window`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Désigne la période de verrouillage, en minutes, après que le nombre maximal de tentatives infructueuses de réinitialisation du mot de passe a été atteint.
Valeur recommandée	1440
Valeur par défaut	1440

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou moins, une attaque par force brute du compte peut se produire puisque le compte n'est pas verrouillé après un nombre maximum de tentatives d'authentification incorrectes.
Cote de risque de sécurité	7.5
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Maximiser la durée de la fenêtre de nouvelle tentative de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

La `password_reset.request.retry_window` propriété contrôle le nombre de minutes avant l'actualisation du nombre de tentatives de réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.retry_window`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Indique le délai en minutes avant que le nombre de tentatives de saisie de mot de passe ne s'actualise à partir de la dernière demande avant que le nombre de nouvelles tentatives ne soit remis à zéro.
Valeur recommandée	Défini sur une valeur entière positive de **1 440** ou plus. La valeur par défaut est **de 1 440** minutes.
Type de configuration	Valeurs entières positives.
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou plus, un processus de réinitialisation du mot de passe par force brute du compte peut se produire.
Cote de risque de sécurité	7.5
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée de la fenêtre de succès de demande de réinitialisation du mot de passe [mis à jour dans Securty Center 1.3]

La `password_reset.request.success_window` propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit attendre pour réinitialiser ou changer à nouveau son mot de passe après une réinitialisation réussie du mot de passe. L'utilisateur ne peut pas réinitialiser le mot de passe pour la durée spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.success_window`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Il désigne la période en minutes pendant laquelle un utilisateur doit attendre après avoir réinitialisé le mot de passe pour réinitialiser à nouveau le mot de passe.
Valeur recommandée	1440
Valeur par défaut	1440
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou moins, il est alors plus probable qu'une autre personne abuse de la fonctionnalité de réinitialisation de mot de passe pour obtenir un accès non autorisé à un compte utilisateur.
Cote de risque de sécurité	4.9
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Maximiser la durée de la fenêtre de déverrouillage de demande de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

La `password_reset.request.unlock_window` propriété contrôle le nombre de minutes pendant lesquelles un utilisateur doit attendre pour lancer une demande de réinitialisation après la dernière action de déverrouillage de compte réussie.

En savoir plus

Attribut	Description
Nom de la propriété	`password_reset.request.unlock_window`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Il désigne la période en minutes pendant laquelle un utilisateur doit attendre après avoir réinitialisé le mot de passe pour réinitialiser à nouveau le mot de passe.
Valeur recommandée	1440
Valeur par défaut	1440
Type de configuration	Valeurs entières positives
Risque de sécurité	(Élevé) Si la propriété n'est pas définie sur la valeur recommandée de 1 440 ou supérieure, elle augmente la possibilité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	pour un acteur malveillant d'obtenir un accès par mot de passe par force brute à l'aide d'outils automatiques.
Cote de risque de sécurité	5.9
Références	Configurer les propriétés de réinitialisation du mot de passe

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Maximiser la complexité du SMS de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

La *password_reset.sms.default_complexity* propriété contrôle la taille minimale requise pour la vérification du code SMS pendant la réinitialisation du mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	*password_reset.sms.default_complexity*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Indique la taille de vérification du code SMS requise pendant la réinitialisation du mot de passe.
Valeur recommandée	6
Valeur par défaut	4
Type de configuration	Valeur entière supérieure à zéro
Risque de sécurité	(Faible) Si la propriété n'est pas définie sur la valeur recommandée, un jeton de validation SMS faible est utilisé. Cela augmente la possibilité de deviner des jetons, ce qui pourrait conduire à la prise de contrôle du compte.
Cote de risque de sécurité	3.8

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée d'expiration du SMS de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

Contrôlez le nombre de minutes restantes avant l'expiration du code SMS.

La*password_reset.sms.expiry* propriété représente le nombre de minutes restantes avant l'expiration du code SMS.

En savoir plus

Attribut	Description
Nom de la configuration	*password_reset.sms.expiry*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	5
Valeur par défaut	5
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,6 • Score CVSS : moyen • Détails des risques de sécurité : Si cette propriété n'est pas définie sur la valeur recommandée de **5** ou moins, les chances qu'un acteur malveillant devine et utilise le code SMS pour réinitialiser le mot de passe augmentent.
Dépendances et prérequis	Aucun

Maximiser la durée de la fenêtre de pause du SMS de réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

Gérez la durée, en minutes, pendant laquelle un utilisateur doit attendre avant de pouvoir demander un nouveau code de réinitialisation du mot de passe.

Si cette propriété n'est pas définie sur la valeur recommandée de **2** minutes ou plus, un utilisateur malveillant peut alors lancer de nombreux codes de réinitialisation de mots de passe dans une brève période de temps. Cela augmente les chances qu'un acteur malveillant prédise le code de réinitialisation du SMS.

En savoir plus

Attribut	Description
Nom de la configuration	`password_reset.sms.pause_window`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	2
Valeur par défaut	2
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 4,8 • Score CVSS : moyen • Détails du risque de sécurité : assurez-vous que `password_reset.sms.pause_window` cette valeur est supérieure ou égale à 2.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Maximiser la durée du délai de vérification de la réinitialisation du mot de passe [Mise à jour dans Security Center 1.3]

Configurez le délai, en millisecondes, qu'un utilisateur doit attendre avant de soumettre une nouvelle demande de réinitialisation du mot de passe.

Un acteur malveillant pourrait tenter d'effectuer une attaque par force brute des identifiants de connexion à l'aide d'outils d'automatisation tels que des bots, contre lesquels la propriété de **délai de vérification du mot de passe de réinitialisation** permet de se défendre. La valeur de la propriété représente le délai, en millisecondes, qu'un utilisateur doit attendre avant de pouvoir effectuer une demande de réinitialisation du mot de passe. Si cette propriété n'est pas définie sur la valeur conseillée de **1 000** ou plus, la connexion est plus vulnérable aux attaques par force brute.

En savoir plus

Attribut	Description
Nom de la configuration	`password_reset.verification.delay`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	1 000
Valeur par défaut	1 000
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails des risques de sécurité : définir la valeur de la propriété sur moins de 1 000 rend votre connexion plus vulnérable aux attaques par force brute.
Dépendances et prérequis	Aucun
Références	Configurer le mot de passe pour un utilisateur

Minimiser la durée de contrainte SAML notBefore ou notOnOrAfter [mis à jour dans Security Center 1.3 et 1.5]

Configurez cette propriété pour ajouter une période de grâce au cours de laquelle les demandes et les réponses SAML sont considérées comme valides.

Cette propriété ajoute une période de grâce au cours de laquelle les demandes et les réponses SAML sont considérées comme valides. La valeur de la propriété représente le nombre de secondes à ajouter aux `NotBefore` contraintes et `NotOnOrAfter` pour tenir compte des différences de temps entre l'horloge du fournisseur d'identité (IdP) et celle du fournisseur de service (SP). Ces contraintes protègent contre les attaques par rejeu en refusant les demandes qui ne sont pas effectuées dans le délai spécifié. Si les horloges IdP et SP sont significativement différentes, la latence du réseau peut entraîner le refus de l'autorisation de la demande SAML.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.sso.saml2.clockskew`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	Moins de 60
Valeur par défaut	180
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : définir la valeur de la propriété sur 60 ou plus peut empêcher les contraintes de se défendre contre les attaques par relecture.
Dépendances et prérequis	Aucun

Désactiver la création d'utilisateurs à partir d'e-mails entrants [Mise à jour dans Securty Center 1.3]

Utilisez cette `glide.user.trusted_domain` propriété pour spécifier la liste délimitée par des virgules des domaines de confiance utilisés dans la création des utilisateurs à partir des e-mails entrants.

Un administrateur peut définir une propriété d'e-mail pour créer automatiquement des utilisateurs à partir d'e-mails entrants. Si cette propriété est définie sur la valeur non sécurisée, l'instance crée automatiquement des utilisateurs à partir de l'e-mail entrant. Chaque utilisateur créé aura le même mot de passe codé en dur par défaut, ce qui facilite le contournement de l'authentification par force brute.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.pop3readerjob.create_caller`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Valeur recommandée	faux
Valeur par défaut	faux
Cote de risque de sécurité	5.4
Impact fonctionnel	(Moyen) Une fois cette propriété configurée, l'instance accepte uniquement les e-mails provenant de domaines de confiance. Si vous n'incluez pas le domaine dans la liste de confiance, les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	comptes sont créés automatiquement et cela a un impact sur les utilisateurs invités.
Risque de sécurité	(Modéré) Si la propriété n'est pas activée, un attaquant peut utiliser une campagne d'usurpation d'adresse e-mail/de spamming pour envoyer plusieurs e-mails, ce qui entraîne la création d'utilisateurs invités plus inutiles.
Références	Configuration des messages entrants

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer l'authentification multifacteur basée sur les rôles [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour appliquer l'authentification multifacteur (MFA) basée sur les `glide.authenticate.multifactor` rôles à tous les utilisateurs affectés à des rôles spécifiques.

Appliquer l'authentification multifacteur en fonction des rôles affectés à l'utilisateur. Si les rôles « administrateur », « security_admin » ou « user_admin » sont affectés à un utilisateur dans la liste des rôles multifacteur, MFA est appliquée.

- Définissez cette propriété sur **vrai** pour appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
- Définissez cette propriété sur **faux** pour désactiver l'authentification multifacteur basée sur les rôles pour tous les utilisateurs affectés à des rôles spécifiques.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.authenticate.multifactor`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification
Objectif	Appliquer l'authentification multifacteur basée sur les rôles à tous les utilisateurs affectés à des rôles spécifiques.
Type	booléen
Valeur recommandée	`true`
Valeur par défaut	faux
Dépendances de Sécurité	**Activez l'authentification multifacteur basée sur les rôles** dans la **table Critères multifacteur**.
Cote de risque de sécurité	7.2
Impact fonctionnel	(Moyen) L'activation de cette propriété améliore l'expérience de l'utilisateur. Il agit comme une couche supplémentaire de protection et de sécurité contre les informations d'identification compromises.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Modéré) Si cette propriété n'est pas activée, il existe un risque d'accès non autorisé aux données sensibles.
Références	Configurer les critères multifacteur basés sur les rôles

Définir la longueur minimale du mot de passe

Définissez la longueur minimale d'un mot de passe utilisateur sur votre instance.

La`set.password.length` propriété définit la longueur minimale requise pour un mot de passe et est utilisée pour évaluer la conformité par rapport à la politique actuelle en matière de mots de passe. La valeur de la propriété est un nombre entier avec une valeur conseillée minimale de **12**. L'utilisation d'une longueur plus courte peut entraîner un échec de la conformité aux réglementations recommandées.

En savoir plus

Attribut	Description
Nom de la configuration	`set.password.length`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	12
Valeur par défaut	12
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails des risques de sécurité : définir la propriété sur une valeur inférieure à 12 peut entraîner des problèmes de conformité et augmenter le risque qu'une personne malveillante réussisse à forcer des mots de passe par force brute.
Dépendances et prérequis	Aucun

Définir la durée de vie de l'OTP pour la réinitialisation du mot de passe à 12 heures ou moins

Contrôlez la durée du lien dans l'e-mail de réinitialisation du mot de passe.

Cette propriété fait expirer le lien contenu dans l'e-mail de réinitialisation du mot de passe une fois le nombre d'heures indiqué dans la propriété passé. La durée de validité d'un jeton de réinitialisation du mot de passe doit être aussi courte que possible sans perturber l'expérience utilisateur normale.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.pwd_reset.onetime.token.validity`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	12
Valeur par défaut	12
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 5,6 • Score CVSS : moyen • Détails du risque de sécurité : le fait d'avoir une longue durée de validité pour le jeton de réinitialisation du mot de passe augmente le risque qu'un acteur malveillant prenne le contrôle du compte.
Dépendances et prérequis	Aucun

Minimiser la durée de vie unique du vérificateur hors bande [Mise à jour dans Security Center 1.3]

Gérez la durée des vérificateurs hors bande.

Un vérificateur hors bande est une méthode de livraison alternative pour les situations de code à usage unique. Par exemple, la réinitialisation d'un jeton multifacteur. Si cette méthode est activée par les administrateurs dans le module d'extension Authentification multifacteur (MFA) , un code à usage unique est fourni par e-mail. Définissez les vérificateurs hors bande à usage unique qui expirent au bout de 10 minutes afin de limiter la fenêtre de validité. Une fenêtre de temps plus longue laisse plus de temps pour que le code soit compromis par des moyens illicites tels que le phishing, l'ingénierie sociale ou les attaques par « shoulder surfing ».

En savoir plus

Attribut	Description
Nom de la configuration	`glide.multifactor.onetime.code.validity`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	10
Valeur par défaut	10
Catégorie	Authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,9 • Score CVSS : faible • Détails des risques de sécurité : définissez des vérificateurs hors bande à usage unique qui expirent au bout de 10 minutes. Tout ce qui est plus long augmente le risque que le code soit compromis par un mauvais acteur.
Dépendances et prérequis	Authentification multifacteur (MFA)
Références	

Appliquer les exigences en matière de chiffrement des appareils et de code d'accès [Nouveau dans Security Center 1.3]

La `glide.sg.device_encryption_enabled` propriété applique le chiffrement FIPS 140-2 (Federal Information Processing Standard). Le chiffrement et le code d'accès des appareils mobiles garantissent qu'un utilisateur non autorisé ne peut pas accéder au contenu d'un appareil, même si l'appareil est physiquement en sa possession.

Lorsqu'elle est définie sur `glide.sg.device_encryption_enabled` vrai, l'application mobile ServiceNow vérifie que le chiffrement de l'appareil et le code d'accès de l'appareil sont activés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sg.device_encryption_enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : Si le chiffrement ou le code d'accès n'est pas activé, l'utilisateur ne sera pas autorisé à se connecter à l'instance sur mobile
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque cette propriété est définie sur vrai, l'application mobile vérifie si le chiffrement de l'appareil est activé. Si le chiffrement n'est pas activé, les utilisateurs ne seront pas autorisés à se connecter à l'instance actuelle sur mobile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exiger un captcha pour l'expérience de visite d'un invité dans l'application Customer Service [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Le captcha pour l'expérience de visite des invités empêche les utilisateurs invités non authentifiés de créer des réservations en exigeant qu'ils effectuent une vérification captcha.

En savoir plus

Attribut	Description
Nom de la configuration	`sn_guest_walkup_cs.captcha.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails des risques de sécurité : si le captcha n'est pas activé, cela peut entraîner la création automatisée de rendez-vous indésirables pour submerger le système ou remplir toutes les places de réservation disponibles, créant ainsi une attaque par déni de service (DoS).
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété active ou désactive le captcha sur les widgets d'enregistrement de visite d'invité CSM. Par défaut, elle est définie sur vrai.

Activer la notification de code SMS pour l'inscription et la vérification [Mise à jour dans Security Center 1.3]

Cette`password_reset.sms.use_notify` propriété contrôle l'utilisation des notifications de code SMS pour la réinitialisation du mot de passe.

Si la `password_reset.sms.use_notify` propriété est définie sur la valeur conseillée, **vrai**, l'utilisateur est invité à effectuer une réinitialisation du mot de passe à l'aide de la vérification par SMS et de l'inscription de nouvel appareil, qui est plus sécurisée qu'un e-mail.

En savoir plus

Attribut	Description
Nom de la configuration	`password_reset.sms.use_notify`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Authentification
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : la définition de cette propriété sur**faux** fait de l'e-mail la méthode par défaut de récupération de mot de passe, qui est moins sécurisée que les SMS.
Dépendances et prérequis	Aucun

Logique métier

Cette catégorie examine la logique et le flux propres à chaque application selon les principes généraux de sécurité. Assurez-vous spécifiquement que la séquence prévue de flux de logique métier ne peut pas être contournée, que des limites existent pour détecter et empêcher les attaques automatisées, et que des protections contre les attaques d'usurpation, d'altération, de divulgation d'informations et d'élévation de privilège existent.

Voici quelques contrôles de sécurité qu'un administrateur peut configurer pour restreindre l'accès non autorisé aux entités sensibles dans Now Platform.

Limiter le nombre maximum de commentaires par utilisateur et par jour

Configurez la propriété pour limiter le `sn_kb_social_qa.max_comments_per_user_daily` nombre de commentaires QA par jour.

Si cette propriété n'est pas définie sur la valeur recommandée de **500** ou moins, il n'y a aucune restriction sur le nombre de commentaires QA par jour, ce qui pourrait entraîner un épuisement des ressources.

En savoir plus

Attribut	Description
Nom de la configuration	`sn_kb_social_qa.max_comments_per_user_daily`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	500
Valeur par défaut	500
Catégorie	Logique métier
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails du risque de sécurité : si vous ne définissez pas la valeur recommandée de cette propriété sur 500 ou moins, vous n'imposez aucune limite de commentaires QA par jour, ce qui pourrait entraîner l'épuisement des ressources.
Dépendances et prérequis	Aucun

Limiter le nombre maximum d'abonnements par utilisateur et par jour

Configurez la *sn_kb_social_qa.max_subscriptions_per_user_daily*propriété pour limiter le nombre maximal d'abonnements auxquels un utilisateur peut s'abonner par jour.

Si cette propriété n'est pas définie sur la valeur conseillée de **500** ou moins, il n'y a aucune restriction sur le nombre maximal de questions et réponses auxquelles un utilisateur peut s'abonner par jour. Cette absence de limitation peut entraîner un épuisement des ressources et avoir un impact sur la disponibilité de votre instance.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_kb_social_qa.max_subscriptions_per_user_daily*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	500
Valeur par défaut	500
Catégorie	Logique métier
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : définissez la valeur de la propriété sur 500 ou moins pour éviter l'épuisement des ressources.
Dépendances et prérequis	Aucun

Minimiser la quantité de destinataires SMTP [mis à jour dans Security Center 1.3]

Le *glide.email.smtp.max_recipients* spécifie le nombre maximal de destinataires que l'instance peut répertorier dans la ligne **À :** pour une notification par e-mail unique.

Définir sur *glide.email.smtp.max_recipients* la valeur conseillée de **100 ou moins**. Les notifications qui dépassent cette limite créent plutôt des notifications par e-mail en double adressées à un sous-ensemble de la liste des destinataires. Chaque notification par e-mail a le même nombre maximal de destinataires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.email.smtp.max_recipients`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Logique métier
Objectif	Si cette propriété est définie sur une valeur non sécurisée supérieure à la valeur par défaut de 100, un refus de service peut se produire sur l'instance.
Valeur recommandée	100
Valeur par défaut	100
Type de configuration	Entier
Risque de sécurité	(Modéré) Les notifications qui dépassent cette limite créent plutôt des notifications par e-mail en double adressées à un sous-ensemble de la liste des destinataires.
Cote de risque de sécurité	4.9

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Valider l'hôte distant

Définissez la propriété sur vrai pour empêcher les personnes malveillantes d'utiliser l'analyse des ports internes sur votre réseau.

Si la `glide.update_set.remote.check_host` propriété n'est pas définie sur la valeur **recommandée vrai,** la fonctionnalité de test de l'instance distante autorise l'analyse Team Development des ports internes, une méthode que les acteurs malveillants peuvent utiliser pour détecter les vulnérabilités d'un réseau. Il est alors possible d'énumérer tous les ports ouverts sur un hôte donné et, dans certains cas, d'extraire les données de réponse, ce qui pourrait entraîner une fuite d'informations ou un accès non autorisé aux données.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.update_set.remote.check_host`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Logique métier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails des risques de sécurité : Si vous ne définissez pas la propriété sur la valeur recommandée, **vrai** , des personnes malveillantes peuvent utiliser l'analyse des ports internes pour accéder à des données non autorisées.
Dépendances et prérequis	Aucun
Références	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0755132 Define a remote instance

Communications

Ce contrôle garantit un cryptage approprié à l'aide d'algorithmes et de chiffrements forts. Il s'agit notamment de s'assurer que la version recommandée de TLS est utilisée pour la connectivité client, d'utiliser des suites de chiffrement fortes, d'utiliser des certificats fiables et signés, de s'assurer que les connexions sont cryptées entre les composants et de consigner les échecs de connexion.

Appliquer le certificat de confiance [mis à jour dans Security Center 1.3 et supprimé dans la version 1.5]

Par défaut, cette `com.glide.communications.trustmanager_trust_all` propriété est définie sur **false**. Le Now Platform seul fait confiance aux certificats qu'il peut vérifier par rapport au magasin de certificats JVM. Les certificats autosignés ou signés par l'entreprise ne sont pas fiables.

Remarque :
Les valeurs de ces propriétés sont Remplacement sécurisé et ne peuvent pas être modifiées une fois modifiées (elles ne sont pas réversibles). Pour des raisons de sécurité, ne modifiez pas la valeur de cette propriété. Si vous avez d'autres questions, contactez Service et assistance client.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.communications.trustmanager_trust_all`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Communications
Objectif	Pour appliquer la validation de certificat pour les demandes sortantes.
Valeur recommandée	faux
Cote de risque de sécurité	6.6

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Moyen) Cette remédiation applique une validation stricte sur le champ CA (autorité de certification) de certificat. Si une entité de confiance (CA) a émis le certificat, l'instance l'accepte pour une utilisation ultérieure.
Risque de sécurité	(Moyen) Pour des raisons de confidentialité et d'intégrité, l'application doit valider l'autorité de certification du certificat avant de l'utiliser pour toute opération transactionnelle.
Références	Certificats Vérification du nom d'hôte du client HTTP

Désactiver les connexions SSLv2/SSLv3 sortantes [Mise à jour dans Securty Center 1.3]

Utilisez la `glide.outbound.sslv3.disabled` propriété pour forcer le MID Server à utiliser TLS lors de connexions sortantes, telles que des demandes REST et SOAP. Normalement, les connexions sortantes d'une instance sont forcées d'utiliser TLS au lieu de SSL.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.outbound.sslv3.disabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Communications
Objectif	Pour appliquer l'utilisation de TLS if lors de toutes les connexions sortantes de l'instance ServiceNow.
Valeur recommandée	VRAI
Valeur par défaut	fase
Cote de risque de sécurité	6.5
Impact fonctionnel	(Moyen) Cette remédiation impose l'utilisation de la version du protocole TLS lors de la communication sur HTTPS. Si des appareils utilisés par les clients/utilisateurs de l'instance ne prennent pas en charge la communication TLS, une panne potentielle peut se produire.
Risque de sécurité	(Modéré) Il a été prouvé que les versions héritées de SSL n'étaient pas sécurisées lorsqu'elles étaient utilisées pour l'implémentation de HTTP Secure Shell, en raison d'attaques côté client, notamment BEAST et SSL.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ne pas utiliser de certificats de démonstration pour les configurations SAML actives [Mise à jour dans Security Center 1.5]

Contrôlez si les certificats de démonstration sont utilisés dans les configurations SAML de production.

Les certificats de démonstration fournis par ServiceNow ne doivent pas être utilisés dans les configurations SAML de production, car ils sont communs à toutes les instances avec une phrase de sécurité connue. Si l'une des propriétés SAML utilisant un magasin de clés de certificat est active (*require_signed_authnrequest*, *require_signed_logoutrequest*ou *encrypt_assertion*), les données de démonstration ne doivent pas être utilisées. Étant donné que les données de démonstration sont partagées entre toutes les instances, il n'y a aucune garantie d'intégrité des demandes signées avec des certificats partagés. Par conséquent, tout message chiffré par l'IDP pourrait être déchiffré par un acteur malveillant s'il était intercepté.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.authenticate.sso.saml2.keystore*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	sys_id d'un magasin de clés personnalisé
Valeur par défaut	chaîne vide
Catégorie	Communications
Risque de sécurité	• Score de gravité : 3,9 • Score CVSS : faible
Dépendances et prérequis	Aucun

Appliquer la vérification OCSP en cas d'erreur réseau [Nouveau dans Security Center 1.3]

Découvrez comment configurer la propriété pour empêcher les *com.glide.communications.httpclient.ocsp_allow_network_error* acteurs malveillants de contourner les vérifications du protocole OCSP (Online Certificate Status Protocol).

Si *com.glide.communications.httpclient.ocsp_allow_network_error* elle n'est pas définie sur la valeur conseillée, faux, et que la vérification du protocole OCSP (Online Certificate Status Protocol) rencontre une erreur réseau (par exemple, un délai d'expiration ou un problème lors de l'extraction des informations de révocation), elle contourne la vérification de sécurité OCSP et la considère comme réussie. Cela pourrait permettre à un attaquant disposant d'un certificat révoqué de briser l'infrastructure à clé publique (PKI) et la confiance du certificat numérique qui est fondamentale pour le Web. L'utilisation de certificats révoqués est souvent un indicateur d'activité malveillante, à moins que les serveurs ne soient désynchronisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.communications.httpclient.ocsp_allow_network_er`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	VRAI
Catégorie	Communications
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails des risques de sécurité : Si vous ne définissez pas cette propriété sur faux, un acteur malveillant peut contourner le contrôle de sécurité OCSP.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété détermine si une demande contre l'URI OCSP (Online Certificate Status Protocol) de l'accès aux informations de l'autorité (AIA) entraîne une réussite ou un échec en cas d'erreur de connexion ou de délai d'expiration. Lorsqu'il est défini sur faux, l'état de révocation du certificat de serveur présenté ne peut pas être validé et entraîne une défaillance de communication avec ce point de terminaison. Si une erreur de réseau se produit lorsque la propriété est définie sur sa valeur par défaut true, le certificat est traité comme valide du point de vue de la révocation.

Vérifier la chaîne et le nom d'hôte des certificats [Nouveau dans Security Center 1.3]

Configurez la propriété pour éviter les `com.glide.communications.httpclient.verify_hostname` attaques de l'homme du milieu en vous assurant que le processus de vérification de certification est exécuté.

S'il `com.glide.communications.httpclient.verify_hostname` n'est pas défini sur **vrai**, cela pourrait permettre des attaques de l'homme du milieu, dans lesquelles les communications entre deux parties sont interceptées. Définir cette propriété sur faux désactive le processus de vérification du certificat. Pour remédier à cette menace de sécurité, définissez `com.glide.communications.httpclient.verify_hostname` sur **vrai** pour empêcher le client HTTP de se connecter à un nom d'hôte potentiellement dangereux.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.communications.httpclient.verify_hostname`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Communications
Risque de sécurité	• Score de gravité : élevé • Score CVSS : 7,4 • Détails du risque de sécurité : ne pas définir *com.glide.communications.httpclient.verify_hostname* sur la valeur recommandée vrai peut rendre votre instance vulnérable aux attaques de l'homme du milieu.
Dépendances et prérequis	Aucun
Impact fonctionnel	Vérifie le nom d'hôte et la chaîne de certification présentés par les hôtes SSL (Secure Socket Layer) distants. Définissez cette propriété sur vrai pour assurer la sécurité contre les attaques de l'homme du milieu (MITM). **Remarque :** Cette propriété remplace la *com.glide.communications.trustmanager_trust_all* propriété

Vérifier la révocation du certificat [Nouveau dans Security Center 1.3]

La *com.glide.communications.httpclient.verify_revoked_certificate* propriété vérifie la révocation du certificat pendant l'établissement de liaison TLS (Transport Layer Security) pour s'assurer que les contrôles de sécurité ne sont pas contournés.

Si *com.glide.communications.httpclient.verify_revoked_certificate* elle n'est pas définie sur la valeur recommandée, **vrai**, la révocation du certificat n'est pas vérifiée pendant l'établissement de liaison TLS. TLS crypte les données envoyées sur Internet pour s'assurer que les acteurs malveillants ne peuvent pas voir les informations sensibles telles que les mots de passe ou les numéros de carte de crédit. Le contournement de l'établissement de liaison TLS constitue un risque pour la sécurité, car un attaquant avec un certificat révoqué peut négliger de fournir un certificat valide et rompre l'infrastructure à clé publique (PKI) et la confiance du certificat numérique.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.communications.httpclient.verify_revoked_certif*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	VRAI
Catégorie	Communications
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails des risques de sécurité : la non-définition `com.glide.communications.httpclient.verify_revoked_cert` de la valeur recommandée vrai entraîne la non-vérification de la révocation du certificat pendant l'établissement de liaison TLS.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété doit être définie sur vrai pour s'assurer qu'une session TLS (Transport Layer Security) est démarrée avec un point de terminaison authentique. Si cette propriété est définie sur faux, le certificat n'est pas vérifié, ce qui pourrait compromettre la sécurité de l'instance.

Configuration

La catégorie Configuration garantit que les applications disposent d'un environnement de version sécurisé et de composants de bibliothèque tiers renforcés. Plus précisément, il s'agit de s'assurer qu'un pipeline de version et de déploiement est répétable et inclut des tests automatisés, et empêche le déploiement des problèmes de sécurité connus. Il s'agit notamment de maintenir les dépendances à jour et de les exempter de vulnérabilités connues.

Options de définition automatique du type de contenu [supprimé dans Security Center 1.3.3]

Configurez la propriété Options de définition automatique du type de contenu sur votre instance pour éviter les attaques par confusion MIME.

Utilisez cette propriété pour contrôler l'en-tête HTTP de réponse X-Content-Type-Options. L'en-tête HTTP de réponse X-Content-Type-Options est utilisé par le serveur pour indiquer que les types MIME publiés dans les en-têtes Content-Type doivent être suivis. Si cette propriété est définie sur false, il est possible pour un attaquant d'effectuer des attaques par confusion MIME ; Sila valeur est définie sur true , cet en-tête empêchera le navigateur d'interpréter les fichiers comme autre chose que le type de contenu dans les en-têtes HTTP.

⚠ Avertissement :
La valeur de cette propriété est un aucun remplacement de base de données. Il ne peut pas être modifié ou remplacé.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.header.auto_set_x_content_type_options`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 7,3 • Score CVSS : élevé • Détails des risques de sécurité : définir cette propriété sur **faux** peut permettre à une personne malveillante de mener des attaques par confusion MIME.
Dépendances et prérequis	Aucun
Références	Add a system property

Valeur de l'en-tête HTTP du contrôle de cache [mise à jour dans Security Center 1.3]

Utilisez la `glide.http.cache_control` propriété pour définir la valeur de contrôle du cache par défaut dans les en-têtes de réponse HTTP que le Now Platform envoie lors de la demande de données de contenu statique pour une page. Les images, CSS et JavaScript rendus de l'intérieur d'une page sont des exemples de contenu statique.

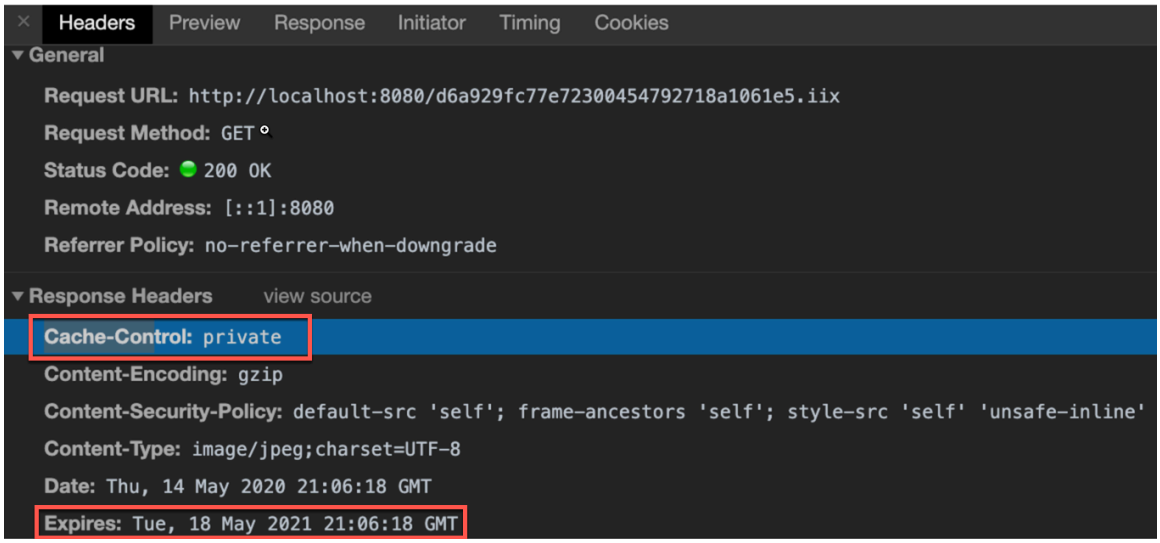
La `glide.http.cache_control` propriété définit la valeur de contrôle du cache par défaut dans les en-têtes de réponse HTTP sur **privé** ou **public**. La valeur par défaut est **private**.

Valeur	Description
privé	Le contenu statique peut être mis en cache au niveau du navigateur (client), mais pas au niveau du serveur proxy.
publique	Le contenu statique peut être mis en cache au niveau du navigateur (client), ainsi qu'au niveau du serveur proxy.

La valeur Expires (Expire) des en-têtes de réponse HTTP contrôle l'expiration du contenu statique et a une valeur par défaut de 369 jours. Pour remplacer manuellement la valeur par défaut, utilisez la `glide.http.expire.days` propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Vous pouvez utiliser la *glide.http.cache* propriété désigner s'il faut activer ou désactiver la définition des valeurs Cache-Control et Expires dans les en-têtes de réponse HTTP. Sa valeur par défaut est **true**, ce qui vous permet de définir les éléments suivants :

- Valeur de contrôle de cache par défaut utilisant la *glide.http.cache_control* propriété.
- Expire la valeur par défaut à l'aide de la *glide.http.expire.days* propriété.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.http.cache_control*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Pour configurer la valeur de l'en-tête de réponse HTTP Cache-Control pour le contenu statique.
Valeur recommandée	privé
Valeur par défaut	privé
Cote de risque de sécurité	4.3
Impact fonctionnel	(Moyen) Définit la valeur Cache-Control par défaut dans un en-tête de réponse HTTP.
Risque de sécurité	(Élevé) Si vous définissez cette propriété sur **public**, les instances avec CDN/proxys peuvent mettre en cache du contenu statique et s'afficher sans authentification. • **privé** est un paramètre plus approprié pour les instances avec la configuration CDN/proxy. • Si une instance n'a pas de configuration CDN/proxy, l'une ou l'autre valeur devrait convenir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver le débogage du serveur de messagerie instantanée

Activez ou désactivez les journaux système de votre instance en configurant cette propriété.

Utilisez cette propriété pour gérer la`glide.cs.debug`façon dont votre instance gère les journaux système. Si la propriété est définie sur la valeur **recommandée faux,** les journaux système ne sont pas activés. Si cette valeur est définie sur **true**, les journaux système sont activés. Définissez la propriété sur **vrai** uniquement lorsque vous souhaitez résoudre les problèmes, puis désactivez-la lorsque vous avez terminé. L'activation des journaux système peut entraîner la génération de nombreux messages, ce qui peut surcharger les journaux système. Les messages du journal peuvent exposer par inadvertance des informations sensibles.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.cs.debug`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 2,3 • Score CVSS : faible • Détails des risques de sécurité : l'activation des journaux système peut entraîner la génération de nombreux messages susceptibles de surcharger le système avec des messages de journal qui exposent par inadvertance des informations sensibles.
Dépendances et prérequis	Aucun

Désactiver le débogage des éléments de formulaire verrouillés

Voici la description de `glide.security.explain.write.locks`.

Définissez `glide.security.explain.write.locks` sur la valeur **recommandée faux pour** empêcher l'affichage d'explication des éléments de formulaire verrouillés. Définissez la valeur sur **vrai** pour afficher l'explication des éléments de formulaire verrouillés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.explain.write.locks`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Limite le comportement d'affichage de SecurityDebugger sans dépendre d'autres propriétés.
Valeur recommandée	faux
Valeur par défaut	faux
Type de configuration	Booléen
Risque de sécurité	(Faible) Empêchera l'affichage de l'explication sur les éléments de formulaire verrouillés. Cela rend l'application légèrement plus sécurisée, car moins d'informations sont fournies par le débogueur de sécurité.
Cote de risque de sécurité	3,5

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver le débogage MultiSSO

La `glide.authenticate.multisso.debug` propriété contrôle la journalisation du débogage pour l'authentification unique (SSO) multiple.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.authenticate.multisso.debug`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Désactive le débogage de l'authentification unique (SSO) à fournisseurs multiples.
Valeur recommandée	faux
Valeur par défaut	faux
Type de configuration	Booléen
Risque de sécurité	(Élevé) Définissez la propriété sur la valeur recommandée « Faux », sinon, le débogage MultiSSO est activé, ce qui peut entraîner une fuite d'informations sensibles involontaire.
Cote de risque de sécurité	4
Références	Propriétés, tables et scripts SSO de plusieurs fournisseurs

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Interdire le clonage cible [Nouveau dans Security Center 1.3]

Configurez la `glide.db.clone.allow_clone_target` propriété pour empêcher votre instance d'être utilisée comme cible de clone.

Si `glide.db.clone.allow_clone_target` elle n'est pas définie sur la valeur recommandée faux, l'instance peut être utilisée comme cible de clone ou comme enregistrement spécifiant l'URL d'instance et les informations d'identification utilisées pour le clonage. On parle de clone système lorsque tout ce qui se trouve dans une base de données est copié d'une instance à une autre. Il s'agit d'un risque de sécurité, car la base de données d'instance peut être écrasée lors du processus de clonage, ce qui entraîne une perte de données et un manque d'intégrité des données. En guise de rattrapage, assurez-vous que `glide.db.clone.allow_clone_target` cette option est définie sur faux.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.db.clone.allow_clone_target`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	VRAI
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 5,9 • Score CVSS : moyen • Détails des risques de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée faux, l'instance peut être utilisée comme cible de clone. Il s'agit d'un risque de sécurité, car la base de données d'instance peut être écrasée lors du processus de clonage.
Dépendances et prérequis	Aucun
Références	• System clone • Clone Target Registration and Authentication
Impact fonctionnel	Cette propriété fournit une sauvegarde supplémentaire qui empêche la clonage d'une instance de production. La valeur par défaut est false pour les instances de production et true pour les instances de sous-production telles que dev ou qa. Pour permettre à une instance d'être utilisée comme cible de clone, définissez cette propriété sur vrai.

Désactiver l'affichage de la trace de la pile d'erreurs SOAP

Gérez l'affichage des traces de la pile dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez la propriété pour gérer les `glide.soapfault.display_stack_trace`traces de la pile dans votre instance. Si cette propriété est configurée sur **faux**, des informations sensibles peuvent être divulguées. Si cette valeur est définie sur **true**, aucune trace de pile ne s'affiche.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.soapfault.display_stack_trace`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails des risques de sécurité : si vous réglez cette propriété sur **faux,** des informations sensibles peuvent être exposées à partir de la trace de la pile.
Dépendances et prérequis	Aucun

Restreindre l'accès à la surveillance des performances

Utilisez cette propriété pour contrôler stats.do `glide.security.diag_txns_acl` , threads.do, thread_pool_stats et replication.do accès à partir d'une connexion non authentifiée.

Lorsque vous définissez cette propriété sur **vrai**, la `glide.security.diag_txns_acl` propriété autorise uniquement l'accès aux éléments suivants par le compte administrateur :

- https://<instancename>.servicenow.com/stats.do
- https://<instancename>.servicenow.com/threads.do
- https://<instancename>.servicenow.com/replication.do
- https://<instancename>.servicenow.com/thread_pool_stats.do

Sans activer ce paramètre, il est toujours possible d'accéder à ces ressources à partir d'une connexion non authentifiée.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.diag_txns_acl`
Type de configuration	Propriétés système (/sys_properties_list.do)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Catégorie	Configuration
Objectif	Restreindre l'accès aux pages de configuration au compte administrateur uniquement
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) Cette remédiation applique uniquement le compte administrateur pour accéder aux données sensibles de l'application à des fins de journalisation et de dépannage.
Risque de sécurité	(Modéré) Les données sensibles telles que les détails du serveur, les threads et les processus exécutés sur le serveur ne doivent jamais être visibles ou accessibles à l'utilisateur final sans privilèges appropriés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la version mise à jour du module d'extension MultiSSO [mis à jour dans Security Center 1.3 et 1.5]

Vérifiez que vous utilisez la version 2 du module d'extension MultiSSO et qu'il est défini sur true pour réduire les vulnérabilités de sécurité.

Si le module d'extension SSO à fournisseurs multiples est activé sur votre instance, la version doit être v2 et la valeur doit être définie sur **vrai**. Les versions antérieures à MultiSSOv2, y compris SAML 1.1 et SAML 2.0, ne respectent pas les normes de sécurité, car elles utilisent des versions de bibliothèque OpenSAML avec des vulnérabilités et des expositions courantes connues (CVE). Si les CVE connus constituaient des menaces pour la sécurité dans des bibliothèques OpenSAML obsolètes, cela pourrait permettre à un acteur malveillant de falsifier des messages et de contourner l'authentification par le biais d'attaques par encapsulation de signature XML, en empruntant l'identité d'entités ou en permettant à des attaquants de l'homme du milieu d'obtenir un accès non autorisé à une instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.multissov2_feature.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 5 • Score CVSS : moyen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails des risques de sécurité : définir la valeur de la propriété sur **faux** signifie que vous utilisez des versions précédentes de MultiSSOv2 qui utilise des bibliothèques OpenSAML avec des failles de sécurité. Cela pourrait permettre à des acteurs malveillants de falsifier des messages.
Dépendances et prérequis	Aucun
Références	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0756504

Appliquer la politique de référent sécurisé [Nouveau dans Security Center 1.3]

Utilisez cette `com.glide.security.referrerpolicy` propriété pour vous assurer que l'en-tête HTTP Referrer-Policy envoie le niveau de données approprié à chaque ServiceNow® page afin d'éviter les fuites de données.

Lorsque la `com.glide.security.referrerpolicy` propriété est définie sur la valeur par défaut, elle s'assure que l'en-tête HTTP Referrer-Policy est géré avec le niveau approprié d'informations envoyées, spécifiquement adapté à la Now Platform® page de demande. Cela empêche les fuites de données non autorisées qui pourraient être accessibles à partir d'autres parties de l'URL complète, telles que le chemin d'accès et la chaîne de requête.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.security.referrerpolicy`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	Par défaut
Valeur par défaut	Par défaut
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails des risques de sécurité : assurez-vous que la `com.glide.security.referrerpolicy` propriété est définie sur défaut pour éviter les fuites de données non autorisées.
Dépendances et prérequis	Aucun
Références	Politique de référence
Impact fonctionnel	Cette propriété contrôle la quantité d'informations envoyées via l'en-tête de référent lorsqu'une requête est envoyée à partir d'une page :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• par défaut : l'instance s'occupera des en-têtes référents • same-origin : envoyer l'URL référente complète au sein de l'instance/du même domaine et aucun référent vers l'origine extérieure • origin : Envoyer uniquement l'origine en tant que référent à l'intérieur et à l'extérieur de l'origine • origin-when-cross-origin : envoyer l'URL référente complète au sein de l'instance/du même domaine et uniquement l'origine en dehors de l'origine

Implémenter x-frame-options : en-tête de sécurité SAMEORIGIN [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour définir l'en-tête de réponse X-Frame-Options sur SAMEORIGIN pour toutes les pages de l'interface `glide.set_x_frame_options` utilisateur.

Utilisez l'en-tête de réponse HTTP X-Frame-Options pour indiquer si le navigateur doit être autorisé à rendre une page dans un <frame> ou <iframe>. Les sites peuvent utiliser cette fonction pour éviter les attaques de détournement de clic en s'assurant que leur contenu n'est pas intégré dans d'autres sites. Un attaquant pourrait intégrer votre page dans sa propre page et faire en sorte que vos éléments de page fonctionnent de manière malveillante. L'utilisateur final peut penser que la page est légitime parce qu'elle ressemble à votre page. L'utilisateur final peut cliquer sur les éléments comme d'habitude uniquement pour exécuter des scripts ou des éléments malveillants.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.set_x_frame_options`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Configuration
Objectif	Pour atténuer les attaques de ClickJacking.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	7.1
Impact fonctionnel	(Faible) Cette correction applique la restriction d'affichage d'une Now Platform application dans une application tierce sous la forme d'un iFrame. Si vous disposez d'une telle intégration, l'application ne s'affichera pas dans l'application tierce personnalisée.
Risque de sécurité	(Moyen) La stratégie Même origine vous permet d'empêcher un domaine de récupérer un script ou une ressource d'un autre domaine. Tous les navigateurs modernes prennent en charge cette fonctionnalité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	La politique valide la connexion en fonction du protocole, du port et de l'hôte. CORS (Cross Origin Request) est une modification de la stratégie de même origine qui permet l'accès à des ressources/ scripts d'un autre domaine lorsqu'il est explicitement indiqué dans le cadre de la valeur de l'en-tête. • Dans ce cas, l'en-tête X-Frame-Options contrôle si l'application Now Platform peut être rendue sur le site Web tiers. • Cela réduit l'exposition sensible, car la valeur de la propriété, lorsqu'elle est définie sur **SAMEORIGIN** , ne permet pas au rendu de se produire.
Références	Propriétés système disponibles Configurer les iFrames

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Exiger un accès en écriture pour accéder à la page Ajouter un élément du catalogue de services [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour empêcher l'exécution d'opérations non autorisées sur les `glide.sc.request.add_item_write_access` éléments de catalogue.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sc.request.add_item_write_access`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails des risques de sécurité : Lorsque la propriété est définie sur faux, tout `glide.sc.request.add_item_write_access` utilisateur connecté peut accéder à la page de l'interface utilisateur Ajouter un élément de catalogue. Cela pourrait entraîner la réalisation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	d'opérations non autorisées sur les éléments de catalogue. Pour corriger ce risque de sécurité, définissez cette propriété sur vrai.
Dépendances et prérequis	Aucun
Impact fonctionnel	Lorsque la propriété est définie sur true, l'utilisateur doit avoir un accès en écriture à l'enregistrement dans le contexte de la page d'interface utilisateur.

Définir des options XFrame pour empêcher l'intégration de sites Web tiers [Mise à jour dans Security Center 1.3]

Configurez cette propriété pour empêcher le contenu d'une application Web d'être incorporé dans un site tiers.

Si cette propriété n'est pas définie sur la valeur recommandée **DENY** ou **SAMEORIGIN,** le contenu d'une application Web peut alors être incorporé dans un site tiers à l'aide d'un **ALLOW-FROM** URI ; Permettre à des sites tiers non approuvés d'activer des attaques telles que le détournement de clic.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.cs.embed.xframe_options`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	SameOrigin
Valeur par défaut	SameOrigin
Catégorie	Configuration
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée, le contenu d'une application Web peut être incorporé dans un site tiers, ce qui permet des attaques telles que le détournement de clic.
Dépendances et prérequis	Aucun

Protection des données

La catégorie de protection des données aborde les éléments de confidentialité, d'intégrité et de disponibilité (CIA) des données.

Les composantes de l'ICA sont les suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Confidentialité : Les données sont protégées contre tout accès non autorisé en transit et au repos.
- Intégrité : Les données sont protégées contre la création, la suppression ou la modification non autorisée.
- Disponibilité : Les données sont accessibles en cas de besoin.

Supprimer Se souvenir de moi

Utilisez la propriété pour supprimer la case à cocher **« Se souvenir de moi »** de la page de connexion afin d'éviter que `glide.ui.forgetme` les informations de connexion ne soient mises en cache.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.forgetme`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Protection des données
Objectif	Pour garantir qu'aucune information d'authentification n'est mise en cache.
Cote de risque de sécurité	3,5
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Impact fonctionnel	(Faible) Cette remédiation modifierait l'expérience utilisateur en le déconnectant automatiquement de l'instance à l'expiration de sa session. L'expiration de la session dépend uniquement de la valeur définie dans la propriété système, comme indiqué dans Managing user sessions .
Risque de sécurité	(Faible) Lorsque vous cochez la case **Se souvenir de moi** lors de la connexion, un cookie supplémentaire est stocké sur l'ordinateur de l'utilisateur. • Son but est de rétablir automatiquement la session pour les visites ultérieures de l'utilisateur connecté. • Cela pose un risque de sécurité car il permet à la session de l'utilisateur d'être active jusqu'à ce qu'il se déconnecte délibérément. La probabilité d'une attaque pour ce scénario augmente lorsque l'utilisateur final a laissé le navigateur sans surveillance ou s'il est compromis par une autre attaque.
Références	Supprimer la case à cocher Se souvenir de moi

Pour en savoir plus sur l'ajout ou la création d'une propriété système, consultez Add a system property

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exiger l'effacement du presse-papiers lors de l'affichage l'application mobile en arrière-plan [Nouveau dans Security Center 1.3]

La *glide.sg.clear_pasteboard_when_backgrounded* propriété contrôle si le texte copié à partir de l'application mobile ServiceNow est conservé dans le presse-papiers une fois que l'application est en mode arrière-plan.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.sg.clear_pasteboard_when_backgrounded*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Protection des données
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails du risque de sécurité : Si cette propriété n'est pas définie sur la valeur recommandée vrai, les informations sensibles peuvent être divulguées au presse-papiers Android ou iOS, où elles peuvent être exposées aux autres applications de l'appareil.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété efface le copier/coller du presse-papiers lorsque l'application ServiceNow passe en arrière-plan.

Restreindre les mises à jour des tickets RH à partir d'e-mails personnels [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Utilisez la*sn_hr_core.restrict_guest_email* propriété pour contrôler si un utilisateur peut répondre à un ticket RH avec son adresse e-mail personnelle.

Lorsque la propriété n'est *sn_hr_core.restrict_guest_email* pas définie sur vrai, un utilisateur peut envoyer un e-mail à partir d'un compte personnel en référence au ticket RH à inclure dans les notes de travail. Cela peut entraîner des problèmes mineurs de confidentialité ou d'intégrité si l'e-mail personnel est compromis ou si la communication n'est pas sécurisée. Un administrateur peut vouloir restreindre la capacité des utilisateurs à répondre aux tickets RH à partir de leur e-mail personnel, car il ne peut pas être sûr de l'identité de l'utilisateur qui accède au compte de messagerie personnel.

En savoir plus

Attribut	Description
Nom de la configuration	*sn_hr_core.restrict_guest_email*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Protection des données
Risque de sécurité	• Score de gravité : 3,5 • Score CVSS : faible • Détails des risques de sécurité : si cette propriété n'est pas définie sur vrai, cela peut entraîner des problèmes mineurs de confidentialité ou d'intégrité si l'e-mail personnel est compromis ou si la communication n'est pas sécurisée.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété contrôle si une réponse provenant d'une adresse e-mail personnelle met à jour ou non un ticket RH. Définir sur vrai, toute réponse provenant d'un e-mail personnel sera ajoutée aux notes de ticket. Si faux, le ticket et les notes ne seront pas mis à jour.

Restreindre les paramètres OAuth au corps de publication [Nouveau dans Security Center 1.3]

La `glide.oauth.allow.parameters.in.post.body.only` propriété contrôle l'acceptation des jetons d'accès par l'authentification OAuth entrante. Les jetons d'accès sont sensibles et ne doivent être acceptés que lorsqu'ils se trouvent dans le corps d'une demande POST.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.oauth.allow.parameters.in.post.body.only`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Protection des données
Risque de sécurité	• Score de gravité : 7,4 • Score CVSS : élevé • Détails du risque de sécurité : si `glide.oauth.allow.parameters.in.post.body.only` ce paramètre n'est pas défini sur la valeur recommandée, vrai, les jetons d'accès peuvent se trouver dans le paramètre de demande GET,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	ce qui pourrait persister dans les journaux de l'infrastructure du client et entraîner la prise de contrôle du compte en cas de fuite de ces journaux.
Dépendances et prérequis	Aucun
Références	• OAuth 2.0 • Gérer les jetons OAuth
Impact fonctionnel	Garantit que le processeur oauth_token.do accepte uniquement les paramètres de corps POST comme entrée pour tous les types d'accord pris en charge.

Gestion et enregistrement des erreurs

La catégorie Gestion et journalisation des erreurs traite de la qualité et de la verbosité des informations journalisées exposées aux personnes concernées.

Il s'agit notamment de s'assurer que les journaux et les messages d'erreur ne collectent pas d'informations sensibles, qu'ils protègent correctement les données conformément à la classification et qu'ils ont une durée de vie appropriée. En outre, cette catégorie concerne la gestion appropriée des erreurs et le fait de ne pas révéler les erreurs sensibles aux utilisateurs finaux, telles que les traces de pile verbeuses pour les exceptions non gérées ayant des implications en matière de sécurité.

Désactiver l'enregistreur pour les utilisateurs avec faibles privilèges dans le bac à sable de script

Gérez la capacité du système Glide à consigner les scripts en cours d'exécution dans l'environnement sandbox.

Utilisez cette propriété pour contrôler la `glide.security.sandbox_no_logging` capacité du système Glide à consigner les scripts en cours d'exécution dans l'environnement sandbox. Si `glide.security.sandbox_no_logging` la valeur est définie sur **faux**, la connexion est disponible pour les utilisateurs ayant des privilèges faibles via des scripts bac à sable. Il s'agit d'une faille de sécurité potentielle, car les utilisateurs ayant peu de privilèges peuvent injecter des journaux, ce qui permet à un acteur malveillant d'obfusquer une attaque. Configurez la propriété sur **vrai** pour empêcher les utilisateurs ayant des privilèges inférieurs qui utilisent un script bac à sable d'avoir une fonctionnalité de journalisation.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.sandbox_no_logging`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	VRAI
Catégorie	Gestion et enregistrement des erreurs
Risque de sécurité	• Score de gravité : 2,2 • Score CVSS : faible • Détails du risque de sécurité : définir cette propriété sur **faux** permet la journalisation des utilisateurs ayant des privilèges inférieurs, ce qui pourrait permettre à un acteur malveillant d'obscurcir une attaque.
Dépendances et prérequis	Aucun

Désactiver le débogage des cookies sécurisés

Gérez les messages du journal liés aux cookies dans votre instance.

Utilisez cette`glide.secure_cookie.debug` propriété pour gérer les messages de votre journal liés aux cookies. Si cette propriété est définie sur **faux**, aucun message de journal n'est affiché. Si elle est définie sur **true**, les messages des classes `SecureUserCookie` et `Cookie` sont consignés. Cela pourrait entraîner l'exposition d'informations sensibles dans votre instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.secure_cookie.debug`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Gestion et enregistrement des erreurs
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails du risque de sécurité : configurer cette propriété sur **vrai** peut entraîner l'exposition d'informations sensibles.
Dépendances et prérequis	Aucun

Désactiver les messages d'erreur SQL [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour désactiver le `glide.db.loguser` rendu des messages d'erreur SQL dans un navigateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.db.loguser`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion et enregistrement des erreurs
Objectif	Pour désactiver l'affichage des messages d'erreur SQL dans le navigateur.
Type	booléen
Valeur recommandée	faux
Valeur par défaut	VRAI
Cote de risque de sécurité	3.1
Impact fonctionnel	(Faible) Cette correction désactive l'affichage des messages d'erreur SQL. Il n'y a aucun impact sur les fonctionnalités.
Risque de sécurité	(Moyen) Aucune information SQL sensible pouvant aider un attaquant ne doit apparaître dans un message d'erreur sur une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le journal d'audit MID [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Le journal d'audit de la commande Serveur MID enregistre des détails tels que le nom de la commande, le hachage de la commande, le nom des informations d'identification utilisées et l'état d'exécution.

Une fois activés, les journaux d'audit peuvent être consultés par les utilisateurs ayant le rôle agent_security_admin dans la table ecc_agent_command_audit_log ou en naviguant vers **MID Server** > **Journaux d'audit de commande**.

Définissez `mid.log.command_audit.enable` sur vrai dans la table ecc_agent_property pour activer l'audit des commandes exécutées par le MID Server.

En savoir plus

Attribut	Description
Nom de la configuration	`mid.log.command_audit.enable`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Gestion et enregistrement des erreurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 2,2 • Score CVSS : faible • Détails des risques de sécurité : en cas d'enquête de sécurité, cette table peut être utilisée par les équipes de réponse aux incidents pour auditer les commandes exécutées sur le MID Server. Sans ce journal, il se peut qu'il n'y ait pas suffisamment de détails pour répondre à des situations telles que l'utilisation non autorisée du compte.
Dépendances et prérequis	Aucun

Activer le module d'extension Tables protégées [Nouveau dans Security Center 1.3]

Utilisez cette propriété pour empêcher les utilisateurs avec des privilèges plus élevés d'altérer les `com.glide.security.protected_table.enabled` tables de journal.

Lorsque la `com.glide.security.protected_table.enabled` propriété est définie sur **vrai**, le module d'extension Tables protégées est utilisé pour empêcher les utilisateurs avec des privilèges plus élevés sur une instance d'altérer les tables de journal. Les tables de journal suivantes disposent de protections spéciales lorsque cette propriété est définie sur **vrai** :

- syslog (aucun remplacement de base de données)
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- protected_table_configuration (aucun remplacement de base de données)

L'intégrité des journaux est importante pour déterminer l'activité malveillante sur une instance par un administrateur client.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.security.protected_table.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Gestion et enregistrement des erreurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 4,5 • Score CVSS : moyen • Détails du risque de sécurité : Le fait de ne pas définir *com.glide.security.protected_table.enabled* sur la valeur recommandée vrai permet aux utilisateurs avec des privilèges plus élevés sur une instance d'altérer les tables de journal.
Dépendances et prérequis	Aucun
Références	Journaux système

Enregistrer tous les champs de requête HTTP sortants [supprimé dans Security Center v1.3.2]

Configurez la propriété sur faux pour empêcher les*glide.outbound_http.security.log.allow.all.fields* champs HTTP sortants sensibles d'être consignés en texte brut.

Si cette propriété n'est pas définie sur la valeur recommandée faux, **les** champs HTTP sortants sensibles peuvent être consignés en texte brut. Cela peut réduire la posture de sécurité de votre réseau d'entreprise, car les demandes sortantes avec des données et des informations d'identification sensibles peuvent être consignées en texte brut qui n'est pas chiffré et peuvent être consultées par des utilisateurs ayant des privilèges inférieurs.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.outbound_http.security.log.allow.all.fields*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	30
Valeur par défaut	30
Catégorie	Gestion et enregistrement des erreurs
Risque de sécurité	• Score de gravité : 6,8 • Score CVSS : moyen • Détails des risques de sécurité : si vous ne définissez pas cette propriété sur **faux,** il est plus probable que des champs sortants sensibles soient consignés en texte brut, ce qui constitue un risque pour la sécurité.
Dépendances et prérequis	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Assainissement des journaux HTML

Configurez `glide.html_sanitize.discarded_log.enable` la propriété pour déterminer si les événements d'assainissement HTML seront journalisés dans votre instance.

Si cette propriété n'est pas définie sur la valeur recommandée **vrai**, les événements d'assainissement HTML ne sont pas consignés dans la `sys_log` table. Le manque de journalisation peut avoir un impact négatif sur les options automatisées de détection et d'enquête de sécurité de votre instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.html_sanitize.discarded_log.enable`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Gestion et enregistrement des erreurs
Risque de sécurité	• Score de gravité : 2,4 • Score CVSS : faible • Détails du risque de sécurité : Si cette propriété n'est pas définie sur la valeur recommandée **vrai**, les événements d'assainissement HTML ne sont pas consignés dans la table, ce qui peut avoir un impact sur les options automatisées de détection et d'enquête `sys_log` de sécurité.
Dépendances et prérequis	Aucun
Références	Activation de l'assainisseur HTML

Consigner les événements d'audit de session [Nouveau dans Security Center 1.3]

Définissez la `glide.authenticate.session_access.log_audit_event` propriété sur **vrai** afin que les événements d'audit de session soient créés dans la `sys_session_access_audit` table.

La connexion d'informations sur l'accès à la session vous aidera à analyser les attaques de cybersécurité. Les informations consignées comprennent l'utilisateur, l'ID de session (non sensible), l'adresse IP, les rôles et les politiques.

Remarque :
La `glide.authenticate.session_access.log_audit_event` propriété système est spécifique à l'accès zéro confiance. Pour plus d'informations, consultez Accès zéro confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.session_access.log_audit_event`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Gestion et enregistrement des erreurs
Risque de sécurité	• Score de gravité : 6,3 • Score CVSS : moyen • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur conseillée, vrai, les événements sont consignés. Cela pourrait vous empêcher de trouver des acteurs malveillants en cas de cyberattaque.
Dépendances et prérequis	Aucun

Enregistrer l'usurpation d'identité d'un utilisateur

Configurez `glide.sys.log_impersonation` pour contrôler si les événements d'emprunt d'identité de l'utilisateur sont journalisés dans votre instance.

Si cette propriété n'est pas définie sur la valeur conseillée, **vrai**, les événements d'emprunt d'identité de l'utilisateur ne sont plus consignés. L'absence de journalisation peut avoir un impact sur les fonctionnalités automatisées de détection et d'enquête de sécurité de votre instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sys.log_impersonation`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Gestion et enregistrement des erreurs
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen • Détails des risques de sécurité : si cette propriété n'est pas définie sur **vrai**, les événements d'emprunt d'identité de l'utilisateur ne sont plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	consignés, ce qui peut avoir un impact sur les options de détection et d'enquête de sécurité de votre instance.
Dépendances et prérequis	Aucun
Références	Impersonating users

Désactiver les messages d'erreur SQL détaillés pour le processeur d'importation

Configurez cette propriété pour contrôler si les messages d'erreur SQL détaillés sont affichés.

Si la propriété est définie sur **false**, un message d'erreur SQL détaillé s'affiche, ce qui peut entraîner la fuite d'informations sensibles. Pour éviter cela, définissez la propriété sur **vrai** pour afficher un message générique.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.import.error_message.generic`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Gestion et enregistrement des erreurs
Risque de sécurité	• Score de gravité : 3,1 • Score CVSS : faible • Détails des risques de sécurité : définir la propriété sur **faux** active les messages SQL détaillés, ce qui peut entraîner une fuite d'informations.
Dépendances et prérequis	Aucun

Fichier et ressources

La catégorie Fichier et ressources garantit que les applications traitent les données de fichier non approuvées en toute sécurité et stockent les données non approuvées provenant de sources non approuvées avec des autorisations limitées dans un emplacement approprié.

Cela inclut des contrôles tels que la prévention du déni de service par le biais de types de fichiers volumineux ou inattendus, la validation du type de fichier et la prévention de la traversée du chemin d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désactiver le téléchargement des fichiers infectés

Gérez cette propriété pour contrôler si les traces de la pile sont affichées dans votre instance.

Lorsque la propriété est définie sur true, les *com.glide.snap.infected_download_allowed* utilisateurs peuvent toujours télécharger des pièces jointes non analysées dans le cas où le service antivirus est en panne ou inaccessible. Cette situation expose potentiellement les utilisateurs au risque de télécharger un fichier malveillant, risquant ainsi d'infecter leur bureau, surtout si aucune autre protection de point de terminaison n'est installée sur l'appareil.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.snap.infected_download_allowed*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 6,7 • Score CVSS : moyen • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur conseillée, faux, vous risquez d'exposer votre instance au téléchargement de fichiers malveillants.
Dépendances et prérequis	Aucun

Activer le filtrage et la notation des e-mails indésirables [Mise à jour dans Security Center 1.3]

Installez le module d'extension Email Filter (*com.glide.email_filter*) pour installer le filtrage des e-mails dans l'instance. Ce filtrage identifie les en-têtes existants, ce qui vous permet de décider de l'action à exécuter avec l'e-mail en fonction de l'en-tête associé.

Chaque message envoyé par les Now Platform serveurs de messagerie est évalué pour déterminer s'il s'agit d'un spam.

Remarque :
Si une instance utilise un serveur de messagerie privé, cette rubrique ne s'applique pas. Pour plus d'informations, consultez la section Notation et filtrage d'e-mail indésirable.

Prérequis

Avant de définir cette propriété :

Définissez la propriété *glide.email.read.active* sur true. Pour plus d'informations, consultez Activer l'utilisation de votre propre serveur POP3 .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom du module d'extension	`com.glide.email_filter`
Type de configuration	Définition du système > Modules d'extension
Catégorie	Fichier et ressources
Objectif	Pour appliquer un filtrage afin d'éviter le spamming des e-mails.
Valeur recommandée	Actif
Valeur par défaut	Aucun. Il s'agit d'un module d'extension et non d'une propriété Glide, il n'y a donc pas de valeur par défaut.
Cote de risque de sécurité	8.1
Impact fonctionnel	(Faible) Les e-mails ne sont jamais filtrés, bloqués ou mis en quarantaine à partir de l'instance dans le cadre de la notation de spam. Elle est uniquement notée, puis envoyée à l'instance. Tout le filtrage est effectué dans l'instance avec le module d'extension Filtres d'e-mail.
Risque de sécurité	(Modéré) Les filtres d'e-mail permettent aux administrateurs d'utiliser un générateur de conditions ou un script conditionnel pour spécifier quand ignorer les e-mails entrants malveillants provenant d'un expéditeur connu/inconnu.
Références	Filtres d'e-mail https://support.servicenow.com/kb_view.do?sysparm_article=KB0549426

Pour en savoir plus sur l'activation d'un module d'extension, reportez-vous à la section Activate a plugin .

Activer l'analyse antivirus

La `com.glide.snap.enable_scan` propriété active la fonctionnalité d'analyse antivirus.

Définissez `com.glide.snap.enable_scan` sur la valeur **recommandée vrai pour** activer l'analyse antivirus.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.snap.enable_scan`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Fichier et ressources

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Pour activer ou désactiver l'analyse antivirus sur l'instance spécifique.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Type de données	booléen
Risque de sécurité	(Élevé) L'analyse antivirus permet de protéger votre instance contre les infections de virus qui peuvent être introduites par des fichiers joints dans vos enregistrements système, telles que les incidents, les problèmes et les stories.
Cote de risque de sécurité	7.7

Restreindre les types de fichiers téléchargeables dans le contenu statique [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour activer les `glide.ui.strict_customer_uploaded_static_content` restrictions sur les types de fichiers qui peuvent être téléchargés lorsqu'ils ont été chargés à l'aide de la fonctionnalité Charger un fichier.

Vous utilisez cette propriété avec la `glide.ui.strict_customer_uploaded_content_types` propriété, ce qui crée une liste de types de fichiers téléchargeables restreints délimités par des virgules. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.

⚠ Avertissement :
La valeur de cette propriété est un aucun remplacement de base de données. Il ne peut pas être modifié ou remplacé.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.strict_customer_uploaded_static_content`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Fichier et ressources
Objectif	S'assurer que les types de fichiers sécurisés sont autorisés à être téléchargés à partir de l'application.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	3.1
Impact fonctionnel	(Faible) Cette correction applique la restriction des téléchargements de fichiers en fonction des valeurs spécifiées dans la `glide.ui.strict_customer_uploaded_content_types` propriété. Pour en savoir plus, reportez-vous à la section Types de fichiers téléchargeables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Faible) Les restrictions de téléchargement de fichiers doivent être appliquées à toutes les sources d'entrée d'utilisateur non approuvées.

Limiter la taille des pièces jointes dans les flux de formation et de prédiction pour les points de terminaison GraphQL [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

La `glide.platform_ml_di.max_attachment_size_graphql` propriété contrôle la limite de taille maximale autorisée pour le renvoi de pièces jointes dans les points de terminaison GraphQL des flux de formation ou de prédiction.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.platform_ml_di.max_attachment_size_graphql`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	5,242,880
Valeur par défaut	5,242,880
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails des risques de sécurité : si cette propriété n'est pas définie sur la valeur recommandée de 5 242 880 ou moins, le renvoi de fichiers volumineux peut entraîner un déni de service (DoS).
Dépendances et prérequis	Aucun

Limiter la taille des pièces jointes dans les flux de formation et de prédiction [Nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

La `glide.platform_ml_di.max_attachment_size` propriété contrôle la limite de taille maximale autorisée pour le renvoi de pièces jointes dans les flux de formation et de prédiction.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.platform_ml_di.max_attachment_size`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	4,000,000

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	4,000,000
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails des risques de sécurité : s'il *glide.platform_ml_di.max_attachment_size* n'est pas défini sur la valeur recommandée de 4 000 000 ou moins, le renvoi de fichiers volumineux peut provoquer une attaque par déni de service (DoS).
Dépendances et prérequis	Aucun

Limiter la taille du corps de réponse HTTP [nouveau dans Security Center 1.3 et mis à jour dans la version 1.5]

Configurez les *glide.http.response.get_body.limit.enabled* propriétés et *glide.http.response.get_body.limit* pour protéger votre instance contre *les exceptions OutOfMemoryExceptions*.

Les *glide.http.response.get_body.limit.enabled* propriétés and *glide.http.response.get_body.limit* ont été introduites pour permettre une nouvelle fonctionnalité qui empêche *les exceptions OutOfMemoryExceptions* d'être levées lorsqu'une réponse à une requête est trop volumineuse. *OutOfMemoryExceptions* peut entraîner des attaques par déni de service (DoS) ainsi que d'autres problèmes susceptibles d'aider les pirates à compromettre une instance.

Pour protéger votre instance contre ces failles de sécurité, assurez-vous que *glide.http.response.get_body.limit.enabled* cette valeur est définie sur true, et qu'elle *glide.http.response.get_body.limit* ne dépasse pas 524 288 000 mégaoctets (500 Mo).

En savoir plus

Attribut	Description
Nom de la configuration	*glide.http.response.get_body.limit.enabled* et *glide.http.response.get_body.limit*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails du risque de sécurité : si vous ne définissez pas ces propriétés sur les valeurs recommandées, vous risquez de rendre votre instance vulnérable aux `attaques par déni de service`.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété réduit les risques d'une `exception OutOfMemoryException` due au chargement accidentel par un client d'un fichier volumineux en mémoire.

Limiter le nombre maximum de pièces jointes dans un e-mail

Configurez le nombre de pièces jointes d'e-mail entrant sur votre instance.

Cette`glide.email.inbound.max_attachment_count` propriété contrôle le nombre maximal de pièces jointes d'e-mail entrant sur votre instance. Si cette propriété n'est pas définie sur la valeur recommandée de **30** ou moins, les e-mails entrants peuvent alors entraîner une dégradation des performances de l'instance.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.email.inbound.max_attachment_count`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	30
Valeur par défaut	30
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 5,3 • Score CVSS : moyen • Détails des risques de sécurité : la définition de la valeur de la propriété sur une valeur supérieure à 30 peut entraîner des problèmes de dégradation.
Dépendances et prérequis	Aucun
Références	Email properties

Minimiser la taille autorisée des pièces jointes [Mise à jour dans Security Center 1.3]

Configurez la `com.glide.attachment.max_size` propriété pour contrôler la taille maximale autorisée pour une pièce jointe chargée.

Cette propriété contrôle la taille maximale d'une pièce jointe chargée. Si cette propriété n'est pas définie sur la valeur recommandée de **1 024** ou moins, la plateforme peut accepter

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

des fichiers volumineux susceptibles de remplir l'espace de stockage et d'entraîner une attaque par déni de service (DoS).

Remarque :
La taille réelle d'une pièce jointe est calculée en multipliant 1024 x 1024 par la valeur de la propriété. Si la valeur de la propriété est **1 024**, la taille maximale autorisée pour une pièce jointe est de 1 Go.

En savoir plus

Attribut	Description
Nom de la configuration	*com.glide.attachment.max_size*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1 024
Valeur par défaut	4096
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails des risques de sécurité : Si cette propriété n'est pas définie sur **1 024** ou moins, la plateforme peut accepter des fichiers volumineux susceptibles d'entraîner une attaque par déni de service.
Dépendances et prérequis	Aucun
Références	Attachment limit properties

Valider le type MIME de fichier dans le service web soap AttachmentCreator [Nouveau dans Security Center 1.3]

La *glide.attachment.enforce_security_validation* propriété détermine si les fichiers MIME (Multipurpose Internet Mail Extensions) subissent une validation.

S'il n'est pas défini sur la valeur recommandée vrai, il n'y a aucune validation pour les fichiers MIME, ce qui entraîne le chargement de fichiers malveillants avec des extensions de fichier incorrectes.*glide.attachment.enforce_security_validation* Lorsque cette propriété est définie sur **vrai**, les fichiers sont téléchargés avec l'extension de type de fichier correcte.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.attachment.enforce_security_validation*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	Booléen
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	VRAI
Catégorie	Fichier et ressources
Risque de sécurité	• Score de gravité : 7,5 • Score CVSS : élevé • Détails du risque de sécurité : Si la propriété est définie sur faux, il n'y a aucune validation pour les fichiers MIME pendant les chargements. Cela pourrait permettre de déguiser des fichiers malveillants en modifiant leur extension de fichier.
Dépendances et prérequis	Aucun
Références	https://developer.mozilla.org/en-US/docs/Web/HTTP/Basics_of_HTTP/MIME_types/Common_types
Impact fonctionnel	Définissez ce paramètre de sécurisation renforcée sur vrai pour exécuter des validations de type MIME et d'extension de fichier sur les pièces jointes chargées. Aucune validation n'est exécutée si cette propriété est définie sur faux. Cette propriété est définie sur vrai par défaut.

Code malveillant

La catégorie Code malveillant garantit que tous les efforts sont déployés pour confirmer que votre code est exempt de vulnérabilités et de fonctionnalités indésirables.

Il s'agit notamment de garantir une gestion sécurisée et appropriée des activités malveillantes, aucune attaque basée sur le temps, aucune communication sortante vers des destinations non approuvées et qu'aucun code non autorisé ou contrôlé par des pirates n'est inclus. Cette catégorie inclut les bibliothèques d'audit ou tierces provenant de la base de code de l'application.

Bloquer les appareils mobiles racines ou jailbreakés

Sécurisez votre instance en empêchant l'accès non autorisé des appareils jailbreakés.

Utilisez cette propriété pour sécuriser votre instance contre tout `glide.sg.allow_rooted_jailbroken_device` accès non autorisé par des appareils jailbreakés. Si un utilisateur tente de s'authentifier dans une instance à l'aide d'une application mobile alors que cette propriété est définie sur **false**, il reçoit l'alerte suivante : Ce périphérique paraît débridé et ne peut pas être utilisé pour accéder à cette instance. Veuillez contacter votre administrateur ServiceNow. L'application est gelée lorsque le message d'alerte est affiché, et la seule façon de masquer ce message est de sélectionner **Se déconnecter**. Si cette propriété est définie sur **vrai** , les utilisateurs s'authentifient dans une instance à l'aide d'un appareil jailbreaké.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.sg.allow_rooted_jailbroken_device`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Code malveillant
Risque de sécurité	• Score de gravité : 4,5 • Score CVSS : moyen • Détails des risques de sécurité : le manque de sécurité des appareils jailbreakés en fait une cible de choix pour les acteurs malveillants. Le fait que des entités non autorisées accèdent aux données de l'entreprise peut affaiblir la posture de sécurité d'un réseau d'entreprise.
Dépendances et prérequis	Aucun
Références	Contrôle d'accès

Activer la signature de code pour les données et les scripts de configuration de l'application [supprimé dans Security Center 1.3]

Gérez la signature de code pour les données de configuration de l'application et les scripts sur votre instance.

La signature de code peut contribuer à améliorer la sécurité en validant les données et les scripts de configuration d'application sensibles avant leur utilisation. La signature de code crée des signatures numériques pour les données qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données. Cette vérification empêche l'utilisation de données ou de scripts malveillants sur l'instance, qui pourrait entraîner une compromission complète de l'instance.

Utilisez cette propriété pour gérer la signature de code pour les données de configuration de l'application`com.snc.kmf.signature.validation.flag` et les scripts. Lorsque cette propriété est définie sur **vrai**, la signature de code est activée pour les données de configuration de l'application et les scripts.

> ⚠ **Avertissement :**
> Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`com.snc.kmf.signature.validation.flag`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	faux
Catégorie	Code malveillant
Risque de sécurité	• Score de gravité : 6 • Score CVSS : moyen • Détails du risque de sécurité : définir cette propriété sur **vrai** active la signature de code, ce qui contribue à améliorer la sécurité en validant les données et les scripts de configuration d'application sensibles.
Dépendances et prérequis	Aucun

Gestion des sessions

Cette catégorie examine la sécurité de l'état de l'application pour un utilisateur. Les sessions doivent être uniques à chaque individu, impossibles à deviner ou partager, et invalidées après des périodes d'inactivité ou lorsqu'elles ne sont pas requises. Cela inclut des facteurs tels que les attributs de cookie pour les sessions basées sur les cookies, la génération et le stockage de jetons de session, ainsi que les exigences en matière de réauthentification fédérée.

Minimiser la durée du délai absolu d'expiration de la session [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour définir une durée de vie maximale pour les `glide.ui.user_cookie.max_life_span_in_days` cookies utilisateur créés lorsque les utilisateurs se connectent avec la case **Se souvenir de moi** cochée. Lorsque le cookie expire, les utilisateurs qui ont coché la case **Se souvenir de moi** sont obligés de s'authentifier à nouveau dans l'instance.

Il permet au cookie utilisateur d'être valide pour la durée de jours spécifiés, à compter de sa première émission. La valeur par défaut est de 30 jours et la limite maximale est de 365 jours.

Remarque :
Pour appliquer une durée de session maximale pour toutes les sessions utilisateur actives, reportez-vous à la section Managing user sessions .

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.user_cookie.max_life_span_in_days`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour forcer les utilisateurs qui ont coché la case **Se souvenir de moi** à s'authentifier à nouveau après des jours spécifiques.
Valeur recommandée	Inférieur ou égal à 30

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	30 jours
Impact fonctionnel	(Moyen) Cette propriété applique la reconnexion obligatoire en évitant toute sorte de rotation de cookie après une période donnée.
Cote de risque de sécurité	4.2
Risque de sécurité	(Moyen) Le fait que les cookies de l'utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer lors d'une configuration basée sur le temps.
Références	Propriétés système disponibles Mémoriser mon nom

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Définir les rôles d'exception de délai d'expiration de session active [Nouveau dans Security Center 1.3]

La `glide.active.session.timeout.exception.roles` propriété contrôle les rôles qui sont exemptés d'une limite de délai d'expiration de session active.

Le délai d'expiration de session actif garantit qu'une session détournée ne peut pas être utilisée indéfiniment sans fournir à nouveau des informations d'authentification. Pour remédier à ce risque de sécurité, assurez-vous que la `glide.active.session.timeout.exception.roles` propriété est définie sur **edge_encryption, mid_server**.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.active.session.timeout.exception.roles`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	edge_encryption, mid_server
Valeur par défaut	edge_encryption, mid_server
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : Ne considérez une exception de limite de délai d'expiration de session active que pour les rôles de compte d'intégration interne. Si une exception est accordée à un rôle au délai d'expiration de session et que ce rôle est attribué à un utilisateur victime d'une attaque de détournement de session, un attaquant peut continuer à s'authentifier indéfiniment sur cette

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	session. Cela peut augmenter l'impact d'un incident de sécurité en donnant à un attaquant plus de temps pour utiliser un compte piraté.
Dépendances et prérequis	Aucun

Activer UserCookie version 3.1

Gérez la version de UserCookie activée sur votre instance pour sécuriser le stockage de la clé secrète dans le code source.

UserCookie v3 est généré uniquement lorsque la `glide.ui.secure.cookies.use_kmf` propriété est désactivée. UserCookie v3 n'est pas sécurisé en raison du stockage de la clé secrète pour les codes d'authentification de message basés sur le hachage (HMAC) dans le code source qui est identique pour tous les clients. Un acteur malveillant peut utiliser une clé secrète pour tenter de détourner des sessions utilisateurs. Pour remédier à cette menace de sécurité, assurez-vous que la `glide.ui.secure.cookies.use_kmf` propriété qui utilise UserCookie v3.1 est définie sur **vrai** . La clé secrète est stockée dans un stockage sécurisé tel que KMF.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.secure.cookies.use_kmf`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails du risque de sécurité : définir ce paramètre sur **faux** est une faille de sécurité car la clé secrète des codes d'authentification de message basés sur le hachage (HMAC) est stockée dans le code source.
Dépendances et prérequis	Aucun

Appliquer la réinitialisation du mot de passe aux demandes d'API

Gérez le fonctionnement de la fonctionnalité de réinitialisation du mot de passe sur votre instance.

Lorsqu'un utilisateur est marqué comme **Mot de passe doit être réinitialisé**, il doit fournir un nouveau mot de passe lors de la prochaine tentative d'authentification. Cette propriété contrôle si la réinitialisation du mot de passe est obligatoire avant d'effectuer des appels d'API. Si cette propriété n'est pas définie sur la valeur conseillée, **vrai**, les comptes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

utilisateur marqués comme **Mot de passe doit être réinitialisé** peuvent toujours effectuer des opérations en interrogeant l'API de table via l'authentification de base. Cette faille de sécurité peut entraîner des fuites d'informations si un compte inactif est compromis.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.api.user.reset_password.mandatory`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé • Détails des risques de sécurité : définir cette propriété sur **faux** peut entraîner une fuite d'informations si un compte inactif est compromis.
Dépendances et prérequis	Aucun

Activer le marqueur de cookie HTTP uniquement [mis à jour dans Security Center 1.3]

Utilisez la propriété pour activer l'attribut HTTPOnly pour les `glide.cookies.http_only` cookies sensibles.

Utilisez l'attribut HTTPOnly pour empêcher les attaques, telles que le script de site à site, car il n'autorise pas l'accès au cookie à l'aide d'un script côté client, tel que JavaScript. Il n'élimine pas les risques de cross-site scripting mais élimine certains vecteurs d'exploitation.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.cookies.http_only`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour atténuer le risque que le script côté client accède au cookie protégé.
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	VRAI
Cote de risque de sécurité	8
Impact fonctionnel	(Faible) Cette remédiation ajoute un marqueur HTTPOnly supplémentaire aux cookies de session, les protégeant ainsi contre le vol. • Si vous disposez d'une fonctionnalité personnalisée qui nécessite JavaScript pour accéder au cookie de l'utilisateur, cette fonctionnalité est interrompue. Cela ne devrait pas être le cas dans des circonstances normales. • Il Now Platform gère la gestion des sessions et il ne devrait pas y avoir de raison pour qu'un script personnalisé accède aux cookies de l'utilisateur.
Risque de sécurité	(Modéré) Les cookies de session de l'application authentifient un utilisateur final et fournissent des autorisations d'accès implicites à l'application. Cela signifie qu'il est nécessaire de les protéger contre le vol ou l'exportation. Les marqueurs HTTP Only protègent les cookies de session contre les injections JavaScript ou les vulnérabilités de script de site à site qui les volent.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser le nombre de sessions interactives simultanées [mis à jour dans Security Center 1.3]

Utilisez cette propriété avec le module d'extension Limite de sessions simultanées pour contrôler le nombre de sessions actives qui peuvent être ouvertes par un utilisateur.

Utilisez la propriété **Glide Authentifier le nombre maximal de sessions interactives simultanées** avec le module d'extension **Limite de session simultanée** (`com.glide.limit.concurrent.sessions`) pour contrôler le nombre de sessions actives ouvertes pour un utilisateur. La valeur recommandée est **1**, ce qui réduit le nombre de sessions ouvertes (un nombre plus élevé augmente la probabilité qu'une session puisse être détournée).

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.max.concurrent.interactive.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1
Valeur par défaut	1
Catégorie	Gestion des sessions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails des risques de sécurité : définir une valeur par défaut de la propriété supérieure à 1 augmente les risques de détournement de session.
Dépendances et prérequis	Le module d'extension **Sessions interactives simultanées** (`com.glide.limit.concurrent.sessions`) doit être actif.
Références	Sessions simultanées limites

Limiter les sessions simultanées dans tous les nœuds [Mise à jour dans Security Center 1.3]

Utilisez la `glide.authenticate.limit.concurrent.sessions.across.all.nodes` propriété avec le module d'extension Limite de sessions simultanées pour gérer le nombre de sessions suivies sur tous les nœuds.

Lorsque le module d'extension Sessions simultanées limites est actif, le nombre de sessions ouvertes peut être limité par utilisateur. Assurez-vous que, lorsque ce module d'extension est actif, la propriété (**Glide authentifier les sessions simultanées sur tous les nœuds**) est définie sur **vrai** afin que le nombre de sessions ouvertes soit suivi sur tous les nœuds au lieu d'un seul nœud d'application. Si cette propriété est définie sur **false**, plusieurs sessions peuvent être ouvertes sur plusieurs nœuds, ce qui augmente les risques de détournement de session.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.limit.concurrent.sessions.across.all.n`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails des risques de sécurité : lors de l'utilisation du module d'extension **Limite de sessions simultanées** , la définition de cette propriété sur **faux** permet l'ouverture de plusieurs sessions sur plusieurs nœuds, ce qui augmente le risque d'une vulnérabilité de sécurité telle qu'un détournement de session.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Dépendances et prérequis	Aucun
Références	Sessions simultanées limites

Module d'extension Limite de sessions simultanées

Configurez le module d'extension com.glide.limit.concurrent.sessions pour réduire les risques de détournement de session sur votre instance.

Ce module d'extension permet à un administrateur de limiter le nombre de sessions actives par utilisateur et/ou par rôle. Il est recommandé que ce module d'extension soit activé et configuré pour réduire la possibilité de détournement de session. Si ce module d'extension est activé et configuré, le nombre de sessions ouvertes pouvant être détournées est limité.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.limit.concurrent.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	module d'extension
Valeur recommandée	com.glide.limit.concurrent.sessions activé et configuré
Valeur par défaut	com.glide.limit.concurrent.sessions activé et configuré
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails des risques de sécurité : Si ce module d'extension n'est pas actif, les risques de détournement de session sont accrus.
Dépendances et prérequis	Aucun

Limiter la durée de vie de la session active de l'invité [Nouveau dans Security Center 1.3]

Utilisez cette `glide.guest.active.session.life_span` propriété pour contrôler la durée des sessions HTTP d'un invité actif.

La `glide.guest.active.session.life_span` propriété applique une durée de vie maximale sur les sessions HTTP d'invités actives, indépendamment de leur session inactive ou de la durée d'inactivité d'un utilisateur avant l'expiration et la fermeture de leur session. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives. Une valeur plus élevée pourrait permettre à un attaquant de rester plus longtemps dans une session volée, ce qui augmenterait la possibilité d'un incident de sécurité. Cette propriété est limitée aux utilisateurs invités qui disposent d'un accès avec peu de privilèges à une instance.

Pour corriger cette faille de sécurité, définissez `glide.guest.active.session.life_span` sur une valeur supérieure à 0 et inférieure ou égale à 720.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.guest.active.session.life_span`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1-720 (minutes)
Valeur par défaut	0
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails des risques de sécurité : la définition de la durée de vie maximale sur une valeur élevée permet à un acteur malveillant de disposer de plus de temps au sein d'une instance en cas de vol d'une session.
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette configuration applique la durée de vie maximale sur les sessions HTTP d'invités actives, quel que soit le délai d'expiration inactif. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives. La durée de vie maximale doit être supérieure au délai d'inactivité `glide.guest.session_timeout` (30 minutes par défaut).

Limiter les sessions interactives simultanées [Mise à jour dans Security Center 1.3]

Gérez le nombre de sessions interactives sur votre instance.

Utilisez cette `glide.authenticate.limit.concurrent.interactive.sessions` propriété pour gérer le nombre de sessions interactives sur une instance. Cette propriété est destinée à être utilisée avec le module d'extension Sessions simultanées limites(com.glide.limit.concurrent.sessions). Lorsque le module d'extension est actif et que la propriété est définie sur **false**, un utilisateur peut avoir n'importe quel nombre de sessions interactives simultanées sur une instance. Un plus grand nombre de sessions ouvertes signifie une plus grande possibilité de détournement de session.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.limit.concurrent.interactive.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur par défaut	faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails du risque de sécurité : lorsque le module d'extension est actif et que la propriété est définie sur **false**, un utilisateur peut avoir n'importe quel nombre de sessions interactives simultanées, ce qui augmente la possibilité d'un détournement de session.
Dépendances et prérequis	Aucun
Références	Limiter les sessions interactives simultanées [Mise à jour dans Security Center 1.3]

Limiter la durée de vie de la session active des intégrations [Nouveau dans Security Center 1.3]

La `glide.integrations.active.session.life_span` propriété applique la durée de vie maximale sur les sessions HTTP d'invités actives, quel que soit le délai d'expiration inactif. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.integrations.active.session.life_span`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	0 à 720
Valeur par défaut	0
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails des risques de sécurité : une durée de vie maximale plus longue pourrait permettre à un attaquant de persister plus longtemps dans une session volée, augmentant ainsi la portée d'un incident de sécurité. Cette propriété est limitée aux intégrations qui disposent d'un accès avec peu de privilèges à une instance. Définissez la propriété

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	`glide.integrations.active.session.life_span` Glide sur une valeur de 0 et inférieure ou égale à 720.
Dépendances et prérequis	Aucun

Limiter l'intervalle de jeton d'actualisation mobile d'accès à la session basée sur des politiques [Nouveau dans Security Center 1.5]

Utilisez la `glide.authenticate.session_access.mobile.refresh_token_interval` propriété pour régir le temps qui doit s'écouler avant qu'un utilisateur d'appareil mobile soit obligé de s'authentifier à nouveau.

L'utilisateur est invité à s'authentifier à nouveau uniquement si l'administrateur a configuré les attributs du fournisseur d'identité dans la stratégie de session (les attributs peuvent varier d'une connexion à l'autre) et que l'utilisateur s'authentifie à l'aide de l'authentification unique (SSO). La valeur par défaut représente le temps en secondes dont dispose un utilisateur avant d'être authentifié à nouveau. Une valeur par défaut plus élevée donne à un acteur malveillant plus de temps pour accéder à la session en cas de détournement de session.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.session_access.mobile.refresh_token_in`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1800 (secondes)
Valeur par défaut	1800 (secondes)
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,3 • Score CVSS : moyen • Détails du risque de sécurité : si la politique ZTA est activée sur l'instance, les utilisateurs qui utilisent SSO pendant la connexion mobile seront forcés de se déconnecter et de se reconnecter une fois que la valeur par défaut de 1 800 secondes (30 minutes) aura été supprimée. Si une valeur plus élevée est utilisée, les utilisateurs sont contraints d'attendre ce temps écoulé.
Dépendances et prérequis	Zéro confiance : accès à la session basé sur des politiques
Impact fonctionnel	Ce paramètre régit le délai, en secondes après la connexion, pendant lequel les utilisateurs seront forcés de se déconnecter des appareils mobiles s'ils utilisent l'authentification unique pour s'authentifier et si l'administrateur a configuré les attributs Identifier le fournisseur dans la politique d'accès à la session.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Limiter la durée de vie de session active de l'interface utilisateur [Nouveau dans Security Center 1.3]

La `glide.ui.active.session.life_span` propriété applique la durée de vie maximale sur les sessions HTTP authentifiées actives, quel que soit le délai d'expiration inactif.

La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.active.session.life_span`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1-720
Valeur par défaut	0
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,2 • Score CVSS : moyen • Détails des risques de sécurité : une durée de vie maximale plus longue pourrait permettre à un attaquant de rester plus longtemps dans une session volée, ce qui augmenterait la possibilité d'un incident de sécurité.
Dépendances et prérequis	Aucun
Impact fonctionnel	Applique la durée de vie maximale sur les sessions HTTP authentifiées actives, quel que soit le délai d'expiration inactif. La valeur configurée est en minutes. Une valeur de zéro désactive l'expiration des sessions actives. La durée de vie maximale doit être supérieure au délai d'expiration inactif glide.ui.session_timeout (30 minutes par défaut).

Invalider de manière proactive les sessions inactives [Nouveau dans Security Center 1.3]

La `glide.active.session.timeout.invalidate.session` propriété contrôle si une session de délai d'expiration est invalidée de manière proactive avant le serveur Tomcat.

Lorsqu'elle `glide.active.session.timeout.invalidate.session` n'est pas définie sur **vrai**, il peut y avoir un petit intervalle de temps pendant lequel une session expirée n'est pas invalidée (60 secondes ou plus selon la taille de la file d'attente). Si une session est piratée, un attaquant peut être en mesure d'utiliser une session pendant cette courte période de temps. Pour remédier à ce risque de sécurité, définissez sur `glide.active.session.timeout.invalidate.session`**vrai**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.active.session.timeout.invalidate.session`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Gestion des sessions
Risque de sécurité	• Score de gravité : 4,6 • Score CVSS : moyen • Détails du risque de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée vrai, une session expirée peut ne pas être validée. Cela augmente les chances qu'un mauvais acteur détourne une session.
Dépendances et prérequis	Aucun

Rotation des identifiants de session HTTP

Utilisez cette propriété pour activer la rotation des identificateurs de session HTTP afin de réduire les `glide.ui.rotate_sessions` failles de sécurité.

Si l'ID de session d'un utilisateur non authentifié ne change pas après l'authentification, une application Web est vulnérable à une attaque de fixation de session. Un utilisateur malveillant pourrait démarrer une session non authentifiée et donner l'ID de session associé à la victime. Une fois que la victime s'est authentifiée, l'utilisateur malveillant partage désormais cette session authentifiée.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.rotate_sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction modifie l'ID de session lorsque l'utilisateur navigue d'une page non authentifiée vers des pages authentifiées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Si vous utilisez un proxy ou codez en dur le SessionID lorsqu'un utilisateur se connecte pour la première fois, ou à toute autre fin, il peut y avoir un impact potentiel sur la fonctionnalité. • Si vous utilisez le module d'extension SAML 2.0 pour l'authentification Single Sign-on, il peut interférer avec le partage d'informations de session entre l'instance et le fournisseur d'identité. Dans ce cas, vous pouvez définir cette propriété sur false.
Risque de sécurité	(Modéré) SessionID permet de traiter et d'authentifier l'utilisateur de l'instance en conservant l'état de session sur le navigateur. Ainsi, SessionID est considéré comme une donnée sensible et doit être sécurisé par défaut. La rotation de session est un contrôle de sécurité qui applique la modification de sessionID chaque fois que l'utilisateur navigue à partir de pages non authentifiées pour authentifier des pages.
Références	Authentification avec SAML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser le nombre de sessions interactives simultanées [mis à jour dans Security Center 1.3]

Utilisez cette propriété avec le module d'extension Limite de sessions simultanées pour contrôler le nombre de sessions actives qui peuvent être ouvertes par un utilisateur.

Utilisez la propriété **Glide Authentifier le nombre maximal de sessions interactives simultanées** avec le module d'extension **Limite de session simultanée** (`com.glide.limit.concurrent.sessions`) pour contrôler le nombre de sessions actives ouvertes pour un utilisateur. La valeur recommandée est **1**, ce qui réduit le nombre de sessions ouvertes (un nombre plus élevé augmente la probabilité qu'une session puisse être détournée).

En savoir plus

Attribut	Description
Nom de la configuration	`glide.authenticate.max.concurrent.interactive.sessions`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	entier
Valeur recommandée	1
Valeur par défaut	1
Catégorie	Gestion des sessions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 3,7 • Score CVSS : faible • Détails des risques de sécurité : définir une valeur par défaut de la propriété supérieure à 1 augmente les risques de détournement de session.
Dépendances et prérequis	Le module d'extension **Sessions interactives simultanées** (`com.glide.limit.concurrent.sessions`) doit être actif.
Références	Sessions simultanées limites

Minimiser la durée du délai d'expiration d'activité de la session [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour désigner, en minutes, la valeur du délai d'expiration de l'activité `glide.ui.session_timeout` .

La définition de cette propriété a plusieurs impacts fonctionnels :

- Plus le délai d'expiration de session spécifié est long, plus la quantité de mémoire utilisée au cours d'une session de traitement est importante. Le système de base utilise une durée d'expiration du délai d'expiration Apache Tomcat par défaut de 30 minutes.
- L'utilisateur Now Platform se déconnecte toujours avec Se souvenir de moi. Après 30 minutes d'inactivité dans l'application, la plateforme déconnecte automatiquement l'utilisateur, sauf si la case à cocher **Se souvenir de moi** dans la page de connexion est cochée. Ce qui est différent, c'est qu'ils ne se reconnectent pas pour continuer.
- Si des jauges ou du contenu sur les pages d'accueil des utilisateurs s'actualisent automatiquement, ce délai peut ne jamais être atteint.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.session_timeout`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour appliquer le délai d'expiration de session.
Valeur recommandée	Délai spécifié par l'utilisateur en minutes. 60 minutes est la valeur recommandée, mais cette valeur peut varier en fonction de la fonctionnalité et des exigences de sécurité. Ne définissez pas cette valeur sur plus d'un jour.
Cote de risque de sécurité	7.5
Impact fonctionnel	(Moyen) Cette remédiation applique l'expiration en temps opportun du compte utilisateur. Aucun impact sur la fonctionnalité, mais l'expérience utilisateur est altérée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Élevé) Le fait que les sessions utilisateur soient actives pour une durée indéterminée constitue un risque pour la sécurité et doit expirer sur une configuration basée sur le temps.
Références	Gérer les sessions utilisateur

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser la durée du délai d'expiration de la fenêtre de session [Mise à jour dans Security Center 1.3]

Utilisez la `glide.ui.user_cookie.life_span_in_days` propriété pour définir le délai d'expiration du cookie Se souvenir de moi. La valeur par défaut est de 15 jours et le délai maximum est de 30 jours.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.user_cookie.life_span_in_days`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Gestion des sessions
Objectif	Pour activer l'expiration par défaut du cookie **Se souvenir de moi** .
Type de données	Entier
Valeur recommandée	15
Valeur par défaut	15
Cote de risque de sécurité	4.9
Impact fonctionnel	(Moyen) Cette propriété est activée par l'utilisateur final lorsqu'il coche la case **Se souvenir de moi** sur la page de connexion et se connecte au Now Platform.
Risque de sécurité	(Modéré) Le fait que les cookies de l'utilisateur soient actifs pour une durée indéterminée constitue un risque pour la sécurité et doit expirer lors d'une configuration basée sur le temps.
Références	Propriétés système disponibles Mémoriser mon nom

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Cryptographie stockée

Cette catégorie se concentre sur le cryptage des données stockées. Il englobe plusieurs aspects clés, tels que l'utilisation d'algorithmes et de modules cryptographiques établis, la garantie de la génération correcte de valeurs pseudo-aléatoires, la mise en œuvre d'un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cryptage basé sur la classification des données et le stockage et l'isolement sécurisés du matériel clé.

Activer l'encrypteur Glide KMF [supprimé dans Security Center 1.3.2]

Gérez les chiffreurs utilisés pour les champs Password2 sur votre instance.

Utilisez cette`glide.kmf.encrypter.enabled` propriété pour définir l'encrypteur KMF comme chiffreur par défaut pour les champs Password2. Cette propriété garantit l'utilisation de normes de chiffrement solides et conformes au lieu d'un chiffreur hérité. Pour vous assurer que l'encrypteur KMF est utilisé à la place de l'encrypteur hérité, définissez cette propriété sur **vrai**.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.kmf.encrypter.enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Cryptographie stockée
Risque de sécurité	• Score de gravité : 4,9 • Score CVSS : moyen • Détails des risques de sécurité : la définition de cette propriété sur **vrai** garantit l'utilisation de l'encrypteur KMF au lieu de l'encrypteur hérité.
Dépendances et prérequis	Aucun
Références	Chiffrement Password2 avec Key Management Framework (KMF)

Validation, nettoyage et codage

La validation, l'assainissement et l'encodage traitent la validation des entrées pour prévenir les vulnérabilités telles que le script de site à site (XSS), l'injection SQL et d'autres attaques.

Ce contrôle garantit que la validation d'entrée et le codage de sortie sont en place et correctement configurés, par exemple, le codage ou l'échappement des données de sortie. Cette catégorie comprend également des vérifications d'éléments tels que la désérialisation des objets, le sandboxing, le cas échéant, et la validation positive via des listes d'autorisation.

Restreindre l'accès à l'API de script GlideSystemUserSession [mis à jour dans Security Center 1.3]

L'API scriptable GlideSystemUserSessionSandbox pouvant être appelée par le client expose les méthodes GlideSystemUserSession's addErrorMessageNoSanitization

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

et addInfoMessageNoSanitization au bac à sable JavaScript. Cela permet à tous les utilisateurs d'appeler cette méthode via un script.

Lorsqu'elle est définie sur **vrai**, une session d'utilisateur en bac à sable (sandbox) est autorisée à appeler des informations ou des messages d'erreur sans nettoyage. Un avertissement est enregistré lorsque le message est appelé. Lorsque la valeur est définie sur **faux**, l'appel n'est pas autorisé.

> ⚠ **Avertissement :**
> Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.sandbox.usersession.allow_unsanitized_messages`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Contrôle d'accès
Objectif	Cette propriété empêche l'appel de messages d'information ou d'erreur non nettoyés dans une session utilisateur bac à sable.
Type	booléen
Valeur recommandée	faux
Valeur par défaut	VRAI
Cote de risque de sécurité	8.1
Impact fonctionnel	(Élevé) Définir la propriété avec la valeur false n'entraînera aucune création ou journalisation de message si ces fonctions sont appelées.
Risque de sécurité	(Élevé) En l'absence d'assainissement approprié, il est possible d'accéder à des contenus potentiellement dangereux et le script dispose de la fonction d'erreur non désinfectée.
Références	Contrôle d'accès

Désactiver les balises JavaScript dans le HTML intégré [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour désactiver la `glide.ui.security.codetag.allow_script` prise en charge de l'incorporation du code JavaScript HTML créé à l'aide de la balise [code].

Il Now Platform atténue de nombreuses attaques par injection et intersites en mettant en œuvre des techniques d'échappement et d'encodage. Par conséquent, les utilisateurs ne peuvent pas écrire et soumettre des entrées au format HTML pour les champs de journal. Toutefois, les champs de journal peuvent afficher le texte contenu dans des balises de code au format HTML. Assurez-vous que la `glide.ui.security.codetag.allow_script` propriété existe dans la table sys_properties et qu'elle est définie sur faux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur **vrai**, les utilisateurs malveillants peuvent écrire du code JavaScript HTML nuisible qui peut être exécuté sur un autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur **faux** afin que les administrateurs puissent empêcher les champs journaux de rendre le code JavaScript HTML en désactivant la prise en charge de la balise [code].

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.security.codetag.allow_script*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Protège contre le script de site à site et l'exécution malveillante de scripts
Valeur recommandée	faux
Valeur par défaut	faux
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et restitue les résultats codés à l'utilisateur. Elle peut avoir un impact sur la fonctionnalité en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes.
Risque de sécurité	(Élevé) La validation des entrées doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Limiter la balise CODE dans les champs de journal Afficher les entrées de champ journal au format HTML Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer le gestionnaire de sécurité Java renforcé [Nouveau dans Security Center 1.3]

La *glide.security.manager* propriété contient le nom de classe Java du gestionnaire de sécurité Java actuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.security.manager`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	`com.glide.sys.security.ContextualSecurityManager`
Valeur par défaut	`com.glide.sys.security.ContextualSecurityManager`
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 7,2 • Score CVSS : élevé • Détails du risque de sécurité : si `glide.security.manager` elle n'est pas définie sur la valeur recommandée , l'instance utilise peut-être un gestionnaire de sécurité Java obsolète pour lequel les politiques de `com.glide.sys.security.ContextualSecurityManager` sécurisat renforcée attendues sont manquantes. Sans ce durcissement, un acteur malveillant disposant d'un accès à l'exécution de script pourrait obtenir l'exécution de code à distance sur l'instance.
Dépendances et prérequis	Aucun

Appliquer l'assainissement HTML [mis à jour dans Security Center 1.3]

Utilisez la propriété pour appliquer le `com.glide.security.check_unsanitized_html` comportement de nettoyage de translated_html champs à un niveau global pour les affectations de champs.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet de mettre en forme le contenu à l'aide de balises HTML (par exemple, `<p>`, , `<font><a href><b><img>`,). Pour éviter toute activité malveillante, certaines balises HTML peuvent être interdites à l'aide d'une liste de blocage. Cette propriété empêche l'utilisation de balises non autorisées dans translated_html champs de votre instance.

- Définissez cette propriété sur **appliquer** pour appliquer le comportement de nettoyage de translated_html champs.
- Définissez la propriété sur **désactiver** pour désactiver l'assainissement HTML afin d'autoriser les balises HTML bloquées sur translated_html champs.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`com.glide.security.check_unsanitized_html`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Empêche l'utilisation de balises HTML non sécurisées pour se protéger contre les attaques telles que le script de site à site.
Type	Chaîne
Valeur recommandée	appliquer
Valeur par défaut	appliquer
Cote de risque de sécurité	7.3
Impact fonctionnel	(Moyen) Ce rattrapage applique l'assainissement HTML sur l'interface utilisateur et restitue les champs HTML traduits à l'utilisateur. Cela peut avoir un impact sur la lisibilité et la mise en forme.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur les sessions utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Assainisseur HTML

Appliquer le bac à sable pour les scripts générés par le client [Mise à jour dans Securty Center 1.3]

Utilisez la propriété pour activer le `glide.script.use.sandbox` sandboxing des scripts.

Il existe deux cas dans le Now Platform qui permettent au client d'envoyer des scripts au serveur pour évaluation :

Filtres ou requêtes

Il est légal d'envoyer un filtre au serveur tel que `assigned_to=JavaScript :getMyGroups()`.

API système

L'appel d'API permet au client d'exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Si vous activez le sandboxing de script, le script évalué à l'un de ces deux points d'entrée s'exécute dans un sandbox avec des droits réduits, avec les caractéristiques suivantes :

- Seules les règles métier marquées client pouvant être appelé sont disponibles dans le bac à sable.
- Seules les inclusions de script marquées Client pouvant être appelé sont disponibles dans le bac à sable.
- Certains appels d'API (en grande partie, mais pas entièrement, limités à ceux traitant d'un accès direct à la base de données) ne sont pas autorisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous ne pouvez pas insérer, mettre à jour ou supprimer des données depuis le bac à sable. Par exemple, tous les appels à current.update() sont ignorés. Si vous exécutez le sans activer le Now Platform sandboxing des scripts, aucune de ces restrictions ne s'applique.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.script.use.sandbox*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Applique la validation pour les requêtes JavaScript côté client qui sont lancées sur la plateforme
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	9.8
Impact fonctionnel	(Critique) Cette correction applique la validation pour les requêtes JavaScript côté client lancées par rapport au Now Platformfichier . Il y a un impact potentiel si le client dispose de personnalisations qui incluent des requêtes JavaScript codées en dur pour effectuer des opérations CRUD.
Risque de sécurité	(Critique) Le Now Platform fournit une grande variété de caractéristiques et de fonctionnalités via des requêtes JavaScript. Cependant, en l'absence d'autorisation et de validation appropriées, un attaquant peut effectuer des opérations non autorisées contre la plateforme.
Références	Configuration de la propriété du bac à sable de script *glide.script.use.sandbox* appartient à la même famille de propriétés qui sécurisent et limitent l'exécution des scripts provenant du client : • *glide.script.allow.ajaxevaluate*: voir Activer AJAXEvaluate. • *glide.script.secure.ajaxgliderecord*: Reportez-vous à la section Activation de la vérification de l'ACL de AJAXGlideRecord.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Convertir les images des e-mails entrants en pièces jointes [mis à jour dans Security Center 1.3 et supprimé dans la version 1.5]

Utilisez la propriété pour spécifier si le code HTML de l'e-mail `glide.email.inbound.convert_html_inline_attachment_references` entrant doit être converti afin que les images de l'e-mail apparaissent dans l'aperçu HTML du corps de l'e-mail.

Voici ce qui se produit lorsque la propriété système `glide.email.inbound.convert_html_inline_attachment_reference` est définie sur false :

- Dans le , les Now Platformliens cid rompus (ID de contenu) apparaissent à la place des images reçues. Le format dans lequel l'image de l'e-mail s'affiche dépend du paramètre de propriété lors de la réception de l'e-mail, et non du paramètre de propriété actuel.
- Le contenu « malveillant » reçu dans la pièce jointe n'est pas référencé dans le code HTML de l'e-mail. La pièce jointe elle-même est stockée dans la table sys_attachment.
- Le traitement des e-mails entrants ne met pas à jour les données HTML de l'e-mail pour refléter l'emplacement stocké de la pièce jointe dans la table sys_attachment. Il en résulte ce qui suit :
  - Les images en ligne n'apparaissent pas dans l'affichage de l'e-mail dans le formateur d'activité.

    Remarque :
    Pour résoudre ce problème avec le formateur d'activité, vérifiez d'abord s'il n'existe aucun problème de sécurité. Définissez ensuite la `glide.email.inbound.convert_html_inline_attachment_reference` propriété système sur **true** pour que les futurs e-mails reçus contiennent l'URL HTML nécessaire pour référencer l'image. La modification de la propriété ne met pas à jour les e-mails déjà reçus. La nouvelle valeur affecte uniquement les e-mails entrants reçus après la modification de la propriété.

  - Les images intégrées ne s'affichent pas lorsque l'e-mail est affiché dans l'aperçu HTML de l'e-mail.
  - Lors de l'ajout de email.body_htm dans des actions entrantes entre les balises de code, les images sont manquantes.

Prérequis

Avant de définir cette propriété, définissez-la `glide.email.read.active` sur vrai. Pour en savoir plus, consultez Enable using your own POP3 server .

En savoir plus

Attribut	Description
Nom de la propriété	`glide.email.inbound.convert_html_inline_attachment_refere`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour restreindre le rendu de l'image dans l'aperçu du corps HTML.
Valeur recommandée	faux
Cote de risque de sécurité	5.4

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Moyen) Une fois cette propriété configurée, l'utilisateur ne peut pas voir l'aperçu de l'image dans le corps de l'e-mail.
Risque de sécurité	(Moyen) Si la propriété n'est pas activée, un attaquant peut envoyer une image malveillante contenant un logiciel malveillant.
Références	Email properties Inbound mail configuration

Pour en savoir plus sur l'ajout ou la création d'une propriété système, consultez Add a system property

Désactiver AJAXEvaluate

Utilisez pour `glide.script.allow.ajaxevaluate` protéger l'API système des vulnérabilités de l'exécution du script client via les appels AJAX.

Une élévation au rôle security_admin est requise pour modifier la propriété.

Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.script.allow.ajaxevaluate`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Empêcher un utilisateur d'exécuter des scripts avec un privilège d'administrateur.
Valeur recommandée	faux
Valeur par défaut	faux
Type de configuration	Booléen
Impact fonctionnel	(Moyen) Cette correction force la désactivation du processeur AJAXEvaluate. Cela peut avoir un impact sur la fonctionnalité si vous utilisez explicitement le processeur d'évaluation AJAX dans le cadre de scripts personnalisés.
Risque de sécurité	(Élevé) Le processeur AjaxEvaluator exécute des scripts clients dans le bac à sable, mais il existe plusieurs propriétés supplémentaires qui peuvent permettre de développer ou de désactiver entièrement le champ d'application des activités dans le bac à sable.
Cote de risque de sécurité	7.3

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Références	Cette propriété appartient à la même famille de propriétés qui sécurisent et restreignent l'exécution de scripts provenant du client : • `glide.script.use.sandbox`: voir Bac à sable pour les scripts générés par le client. • `glide.script.allow.ajaxevaluate`: voir Activer AJAXEvaluate.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Désactiver l'expansion des entités dans l'analyseur de diffusion en continu XMLDocument2 [mis à jour dans Security Center 1.5]

Si les personnalisations ne nécessitent pas d'expansion d'entité, utilisez la propriété pour désactiver complètement l'expansion d'entité `glide.stax.allow_entity_resolution` externe. Le XML termine l'analyse mais n'inclut aucune entité interne ou externe.

- Si vous définissez cette propriété sur **vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, sous réserve de la définition de la `glide.stax.whitelist_enabled` propriété.
- Si vous définissez cette propriété sur **false**, toute la résolution et l'expansion de l'entité sont bloquées. Pour plus d'informations, consultez Validation d'entité XMLdoc2 avec liste blanche.

Prérequis

Avant de définir cette propriété :

- Définissez les `glide.xml.entity.whitelist.enabled` propriétés and `glide.stax.whitelist_enabled` sur true. Pour plus d'informations, consultez Validation d'entité XMLdoc/XMLUtil avec liste d'inclusion et Validation d'entité XMLdoc2 avec liste d'inclusion.
- Définissez une liste de FQDN délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, car il s'agit des seules URL atteignables à l'aide du processus XML Entity. propriété. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

> ⚠ **Avertissement :**
> Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.stax.allow_entity_resolution`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre une attaque par expansion d'entité XML/Billion Laugh.
Valeur recommandée	faux
Valeur par défaut	VRAI
Impact fonctionnel	(Faible) Si la personnalisation utilise l'expansion des entités, le peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Critique) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.
Solution de contournement	Si la personnalisation nécessite une expansion de l'entité, définissez cette propriété sur vrai et suivez les étapes documentées dans Validation de l'entité XMLdoc2 avec liste d'inclusion.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, consultez Add a system property

Pour plus d'informations sur les ressources OWASp, consultez OWASp .

Désactiver l'URL du contenu externe

Gérez la façon dont les métadonnées de liens externes sont utilisées dans votre instance avec la Messagerie instantanée de Connexion.

Utilisez la propriété pour gérer les `glide.ui.url.external.content` métadonnées des liens externes dans votre instance. Si la propriété est définie sur la valeur recommandée **faux**, aucune métadonnée de lien externe n'est rendue. Si la valeur **est définie sur vrai** , Connect Chat elle récupère les métadonnées de liens externes à partir de sources telles que YouTube ou les articles d'actualités pour afficher des messages plus riches. Cela peut entraîner des attaques de falsification de requête côté serveur (SSRF).

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ui.url.external.content`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	VRAI
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 8,1 • Score CVSS : élevé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails des risques de sécurité : définir cette propriété sur **vrai** peut exposer votre instance à des attaques de falsification de requête côté serveur (SSRF).
Dépendances et prérequis	Aucun
Références	Connect Chat

Définir les types MIME téléchargeables restreints [Mise à jour dans Security Center 1.3]

La *glide.ui.attachment.download_mime_types* propriété forcera le téléchargement de la liste spécifiée de types de fichiers dangereux sur le client et ne sera pas affichée dans le navigateur.

Si le type MIME d'un fichier est présent dans le, un *glide.ui.attachment.download_mime_types* téléchargement est forcé. Par exemple, le téléchargement de texte/html force un fichier HTML à être téléchargé sur le client en tant que fichier plutôt que d'être affiché en ligne dans le navigateur, empêchant ainsi une attaque XSS.

Pour afficher une liste des types MIME existants, tapez `/sys_attachment_icon_rule_list.do`. Vous pouvez activer n'importe lequel de ces types MIME pour satisfaire aux exigences de conformité de sécurité dans le Now Platform.

Remarque :
Le rôle security_admin est requis pour modifier la propriété.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.attachment.download_mime_types*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	En maintenant correctement la liste des types de fichiers dangereux qui ne peuvent pas être affichés dans le navigateur, vous éviterez les attaques de script de site à site (XSS).
Valeur recommandée	Liste des types MIME applicables ou de la valeur recommandée : `text/html,image/svg,image/svg+xml,application/xml`
Valeur par défaut	Liste des types MIME applicables pour la valeur par défaut : `text/html,image/svg,image/svg+xml,application/xml`
Type de configuration	Chaîne : toutes les valeurs séparées par des virgules des types MIME d'application.
Impact fonctionnel	(Faible) Ce rattrapage permet d'effectuer des contrôles de validation avant d'effectuer une action lorsque vous cliquez sur une pièce jointe dans une Now Platform application. Il n'y a pas d'impact potentiel, mais l'expérience utilisateur est altérée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Modéré) Les attaquants peuvent abuser les types MIME et placer du contenu de script non souhaité dans la pièce jointe du côté de la victime pour capturer des informations sensibles. La possibilité d'avoir des XSS peut conduire à une escalade de privilège facilement atteinte vers des rôles plus élevés, tels que l'administrateur, où un mouvement plus latéral peut être effectué. Dans le contexte actuel, renseignez la propriété avec une liste de types MIME de pièces jointes séparés par des virgules qui ne doivent pas être affichés en ligne dans le navigateur.
Cote de risque de sécurité	6.3
Propriétés associées	• `glide.ui.attachment.force_download_all_mime_types` • `glide.ui.attachment.tables_ignore_force_download`
Références	Forcer le téléchargement des types MIME.

Désactiver le code HTML intégré [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour désactiver la `glide.ui.security.allow_codetag` prise en charge de l'incorporation du code HTML créé à l'aide de la balise [code].

Il Now Platform atténue de nombreuses attaques par injection et intersites en mettant en œuvre des techniques d'échappement et d'encodage. Par conséquent, les utilisateurs ne peuvent pas écrire/soumettre d'entrées au format HTML pour les champs de journal. Toutefois, les champs de journal peuvent afficher du texte contenu dans des balises de code au format HTML.

- Cependant, il existe un risque de sécurité associé. Si la valeur est définie sur `vrai`, les utilisateurs malveillants peuvent écrire du code JS HTML nuisible qui peut être exécuté sur un autre navigateur client après le rendu des champs de journal.
- Définissez cette propriété sur `faux` afin que les administrateurs puissent empêcher les champs journaux de rendre le code HTML en désactivant la prise en charge de la balise [code].

En savoir plus

Attribut	Description
Nom de la propriété	glide.ui.security.allow_codetag
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Configurer dans le centre de sécurité de l'instance	Oui
Objectif	Protégez-vous contre le script de site à site et l'exécution malveillante de scripts
Valeur recommandée	faux
Valeur par défaut	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Cote de risque de sécurité	4.2
Impact fonctionnel	(Moyen) Cette correction applique le codage HTML sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur. Cette propriété est définie sur `vrai` par défaut. Dans cet état, votre instance affiche le rendu HTML dans les champs de journal et les formulaires. Si cette propriété est définie sur `faux`, le HTML n'est pas affiché correctement et les balises HTML peuvent apparaître dans les champs de journal des formulaires. Cela peut avoir un impact négatif sur les fonctionnalités et sur les interactions des utilisateurs avec les données qui en résultent.
Risque de sécurité	(Moyen) La validation des entrées doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur une session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.

Activer l'assainisseur HTML dans Agent virtuel [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour activer HTMLSanitizerService *`com.glide.cs.html.sanitizer.enabled`* .

En savoir plus

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

Attribut	Description
Nom de la propriété	*`com.glide.cs.html.sanitizer.enabled`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Empêche les applications contre les attaques de script de site à site et d'injection HTML.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8
Impact fonctionnel	(Élevé) Cette correction applique un mécanisme de codage de sortie HTML avant que les données utilisateur ne soient restituées à l'utilisateur. Si le client dispose d'une personnalisation qui implique le rendu de l'attribut HTML ou des données de contenu, il y a un impact sur la fonctionnalité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	(Élevé) L'entrée de l'utilisateur doit être traitée en toute sécurité lorsque les données sont stockées et traitées sur l'application. Cela réduit les attaques de script de site à site côté client en encodant les données en sortie.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la protection contre l'interpolation de Jelly JS

Utilisez la `glide.ui.jelly.js_interpolation.protect` propriété pour vous assurer que tout JavaScript sur le point d'être exécuté sur une page Jelly est protégé contre l'injection à l'aide de l'interpolation Jelly.

Lorsque vous définissez la propriété sur **true**, une application passe par une arborescence de scripts Jelly (imbriquée). Il enveloppe les expressions Jelly potentiellement dangereuses d'un filtre qui :

- Échappe à leurs résultats pour être en sécurité, ou
- Si leur sécurité ne peut pas être garantie, génère une SecurityException, car l'expression qui allait être évaluée représente un problème de sécurité possible.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.ui.jelly.js_interpolation.protect`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour atténuer les attaques d'exécution de code malveillant qui peuvent se produire à l'aide de Jelly Injection.
Valeur recommandée	VRAI
Valeur par défaut	faux
Cote de risque de sécurité	9
Impact fonctionnel	(Élevé) Cette propriété fait une meilleure estimation de la mise entre guillemets d'une expression. Il peut citer à tort une expression légitime. Dans ce cas, il peut être nécessaire de marquer manuellement une expression comme sûre.
Risque de sécurité	(Modéré) L'injection JEXL est une forme d'injection d'entrée unique qui peut conduire à la fois à la falsification de requêtes intersites et à l'exécution Now Platform de code. La désactivation complète de la protection peut potentiellement ouvrir de nombreuses vulnérabilités de sécurité P1.
Solution de contournement	Pour marquer manuellement une expression comme sûre, ajoutez le préfixe SAFE à l'expression Jelly :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	${SAFE :sysparm_input} ; Ajouter aveuglément SAFE à chaque expression n'est pas la bonne façon d'aborder le problème, car cela peut ouvrir une faille de sécurité. • N'ajoutez SAFE à une expression que si vous pouvez garantir que l'expression ne contient pas d'entrée du client. • Si c'est le cas, il est possible qu'un client malveillant provoque l'évaluation du JavaScript privilégié.
Références	Balises Jelly Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Activer la protection de l'interpolation Jelly JS pour les expressions imbriquées

Gérez la protection contre l'interpolation sur votre instance.

Utilisez la propriété pour gérer la protection contre l'interpolation*glide.ui.jelly.js_interpolation.protect_nested_expressions*. La protection contre l'interpolation garantit que lorsque des expressions Jelly sont utilisées en JavaScript, elles doivent être considérées comme sûres en relevant de certaines catégories ou en étant marquées comme SAFE dans l'expression elle-même. Si cette atténuation n'est pas activée, un acteur malveillant peut envoyer un paramètre GET à une page Jelly et entraîner l'évaluation du contenu de ce paramètre en tant que JavaScript côté serveur avec des privilèges d'administrateur. Si cette propriété n'est pas définie sur la valeur **recommandée vrai,** les expressions Jelly malveillantes interpolées en JavaScript sont autorisées et un utilisateur peut exécuter du code à l'aide d'un modèle Jelly.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.ui.jelly.js_interpolation.protect_nested_expressions*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	faux
Catégorie	Validation, nettoyage et codage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 9 • Score CVSS : critique • Détails des risques de sécurité : Si la propriété est définie sur **false**, les expressions Jelly malveillantes sont autorisées.
Dépendances et prérequis	Aucun

Renforcer les liens relatifs

Utilisez la propriété pour appliquer des *glide.cms.catalog_uri_relative* liens relatifs à partir du paramètre URI on /ess/catalog.do.

- Lorsque la valeur est définie sur **true**, seules les URL relatives sont autorisées via la page /ess/catalog.do à l'aide du *uri* paramètre.
- Lorsqu'elle est définie sur **faux**, toutes les URL sont autorisées, ce qui permet la liaison à un contenu externe non autorisé.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.cms.catalog_uri_relative*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour limiter les tentatives de lier un contenu externe non autorisé.
Valeur recommandée	VRAI
Valeur par défaut	faux
Cote de risque de sécurité	2.6
Impact fonctionnel	(Faible) Cette correction applique la validation sur la page du catalogue de sorte que seules les URL relatives sont autorisées. Les liens existants vers des applications Web externes sont rompus.
Risque de sécurité	(Élevé) Les URL absolues peuvent présenter un risque de sécurité lorsqu'elles sont utilisées dans un paramètre ou une valeur de champ, redirigeant ainsi la page source vers un site Web contrôlé par un adversaire.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Appliquer la vérification de la liste d'autorisations d'URL

Utilisez la *glide.security.url.whitelist* propriété pour ajouter une validation supplémentaire afin d'assurer que toute URL externe introduite doit faire partie des URL sur liste d'inclusion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La redirection ouverte se produit lorsqu'une page Web vulnérable est redirigée vers une page malveillante et non approuvée qui peut compromettre l'utilisateur. Les attaques par redirection ouverte s'accompagnent d'une attaque de hameçonnage, car le lien vulnérable modifié est identique au site d'origine, ce qui augmente les chances de réussite de l'attaque de hameçonnage.

Cette propriété est applicable dans les cas suivants :

- `/logout.do ?sysparm_goto_url={URL externe}`
- `/cms_login_redirect.do ?sysparm_goto_url={URL externe}`

Après s'être déconnectés de l'instance, les utilisateurs sont dirigés vers un site de confiance externe :

- `/logout_redirect.do ?sysparm_url={URL externe}`
- `/saml_redirector.do ?sysparm_uri={URL externe}`

Lorsque SAML est activé, il invoque une URL de déconnexion du fournisseur d'identité (IdP).

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.url.whitelist`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour implémenter une redirection d'URL sécurisée lors de la connexion, de la déconnexion ou d'autres redirections. Cette propriété atténue l'une des 10 principales attaques de l'OWASP appelée Redirections et transferts invalidés.
Type	Chaîne
Valeur par défaut	VRAI
Valeur recommandée	VRAI
Valeur	Les URL approuvées de votre organisation [certains FQDN (nom de domaine pleinement qualifié) définis, par exemple http://www.servicenow.com]
Cote de risque de sécurité	8.3
Impact fonctionnel	(Moyen) Cette correction applique la validation sur la page de déconnexion. Cela peut avoir un impact fonctionnel sur un utilisateur d'une instance avec une configuration SSO/SAML.
Risque de sécurité	(Élevé) La redirection ouverte côté client peut permettre à l'attaquant de rediriger les victimes/utilisateurs vers un site Web contrôlé par l'attaquant et est considérée comme un risque de sécurité.
Références	Erreurs et correctifs de l'authentification unique (SAML 2.0)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Formules Excel d'échappement [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour empêcher l'injection Excel, également connue sous le `glide.export.escape_formulas` nom d'injection de formule.

L'injection Excel se produit lorsque des sites Web intègrent des entrées non fiables dans des fichiers Excel. Lorsque vous utilisez un tableur tel que Microsoft Excel ou LibreOffice Call pour ouvrir un fichier, toutes les cellules commençant par +, -, = ou @ sont interprétées comme une formule. Lorsque vous définissez la propriété sur **true**, les `glide.export.escape_formulas` valeurs de chaîne commençant par +, -, = ou @ sont précédées d'une seule apostrophe lorsque vous exportez vers des fichiers CSV, XLS ou XLSX.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.export.escape_formulas`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour empêcher l'application contre Excel ou l'injection de formule.
Valeur recommandée	VRAI
Valeur par défaut	faux
Cote de risque de sécurité	6.5
Impact fonctionnel	(Faible) Des formules malveillantes peuvent être utilisées pour détourner l'ordinateur de l'utilisateur en exploitant les vulnérabilités du logiciel de tableur.
Risque de sécurité	(Modéré) Les formules malveillantes présentent un risque même lorsque la feuille de calcul d'intégration ne contient pas d'informations sensibles, car elles peuvent être utilisées pour compromettre l'ordinateur de l'utilisateur.
Solution de contournement	Comme alternative, envisagez de supprimer tous les espaces blancs de fin dans la mesure du possible et de limiter toutes les données fournies par le client à des caractères alphanumériques.
Références	Propriétés système disponibles

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

HTML d'échappement dans les vues de listes [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour forcer les `glide.ui.escape_html_list_field` caractères d'échappement HTML pour les champs HTML d'une vue de liste.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet de mettre en

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

forme le contenu à l'aide de codes HTML (par exemple, `<p>`, , `<font><a href><b><img>`,). Un utilisateur malveillant peut injecter du code HTML dans le champ de formulaire pour exécuter des scripts indésirables sur différentes sessions client/utilisateur.

- Définissez cette propriété sur **faux** pour effectuer une fuite HTML avant que les enregistrements/champs ne soient affichés dans le navigateur lorsque la table apparaît en tant que vue de liste.
- Si la valeur est définie sur **vrai** et que vous sélectionnez cette colonne dans une vue de liste lors de l'affichage d'une liste de tables ou d'enregistrements, ces champs au format HTML peuvent apparaître.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.escape_html_list_field*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour protéger les applications contre les attaques de script de site à site
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction applique le codage HTML sur l'interface utilisateur au niveau de l'analyseur HTML, ce qui renvoie les résultats codés à l'utilisateur. Elle peut avoir un impact sur la fonctionnalité en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur les sessions utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Échapper à JavaScript

Utilisez la propriété pour forcer l'échappement des balises JavaScript (`<script></script>`) dans les *glide.html.escape_script* champs HTML au cours des vues de listes.

HTML est l'un des types qui peuvent être affectés aux champs du dictionnaire. L'affectation de champs HTML à n'importe quel type de champ permet à l'utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

de formater le contenu à l'aide de codes HTML (par exemple, <p>, , <font><a href> <b><img>,). Si vous définissez *glide.html.escape_script* la valeur **sur faux**, les balises (<script></script>) peuvent apparaître lorsque vous sélectionnez cette colonne dans une vue de liste tout en affichant une liste de tables ou d'enregistrements.

Un attaquant malveillant peut insérer du code JavaScript en l'intégrant dans les balises (<script></script>). L'attaquant peut en tirer parti en injectant un vecteur JS sophistiqué qui peut s'exécuter lorsqu'un utilisateur ouvre l'enregistrement de table.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.html.escape_script*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour éviter les attaques de script de site à site contre une application.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Moyen) Cette correction applique l'échappement JavaScript sur l'interface utilisateur et renvoie les résultats codés à l'utilisateur. Elle peut avoir un impact sur la fonctionnalité, en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes
Risque de sécurité	(Élevé) La validation des entrées doit avoir lieu dans l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Références	Propriétés système disponibles Paramètres de sécurité élevée

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Script Jelly d'échappement [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour forcer l'échappement *glide.ui.escape_all_script* de tous les scripts injectés dans Jelly.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il échappe à toutes les chaînes JS et HTML incluses dans <j :jelly> ... </j :jelly> avant qu'ils ne soient écrits dans le flux de sortie, ce qui empêche ainsi l'apparition de plusieurs problèmes XSS.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.escape_all_script*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Catégorie	Validation, nettoyage et codage
Objectif	Si la propriété n'est pas définie sur **true**, les développeurs doivent effectuer plusieurs étapes sur chaque script Jelly personnalisé pour éviter les problèmes XSS. Ces étapes incluent la localisation des variables Jelly envoyées au flux de sortie pour s'afficher sur les pages Web et l'exécution de l'échappement sur chacune des balises suivantes : $â {JS :expression} $â {HTML :expression} OU $â {JS,HTML :expression}
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	7.3
Impact fonctionnel	(Moyen) Cette correction applique l'échappement de Jelly au niveau de l'analyseur. Cela peut avoir un impact fonctionnel sur l'interaction de l'utilisateur avec les données résultantes.
Risque de sécurité	(Élevé) La validation des entrées doit avoir lieu sur toutes les entrées utilisateur saisies dans l'application. Ce faisant, les attaques par injection contre la plateforme peuvent être défendues et protégées.
Solution de contournement	L'interface utilisateur peut être affectée, car certains des scripts et balises HTML conçus pour le rendu d'une page Web peuvent sembler cassés. Cette correction envoie la page codée de sortie au navigateur pour rendu. Par exemple, au lieu de « ma chaîne ici », il peut afficher « <u>ma chaîne ici</u> », car la <u> balise a été correctement échappée. Dans ce cas, pour empêcher l'échappement, ajoutez le préfixe NOESC à l'expression Jelly pour empêcher l'échappement JS. Par exemple :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Avant : ($[jvar_context_menus]) ; • Après : ($[NOESC :jvar_context_menus]) ; • Avant : $[jvar_ui_policy_scripts] • Après : $[NOESC :jvar_ui_policy_scripts]
Références	Paramètres de sécurité élevée Balises Jelly

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Scripts d'échappement dans le bloc-notes [Mise à jour dans Security Center 1.3]

Découvrez comment le bloc-notes est pris en compte dans la posture de sécurité de votre instance et comment le gérer afin que des scripts malveillants ne puissent pas être exécutés dessus.

Le bloc-notes est un moyen facile de définir des informations sur le serveur auxquelles vous pouvez accéder dans le navigateur. Un administrateur peut y faire figurer n'importe quoi, y compris des enregistrements arbitraires. Si cette propriété n'est pas définie sur la valeur **recommandée vrai,** il est possible d'exécuter des scripts malveillants tels qu'une vulnérabilité de script de site à site.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.ui.escape_scratchpad*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 6,5 • Score CVSS : moyen • Détails **du risque** de sécurité : si la propriété n'est pas définie sur la valeur recommandée vrai, il est possible d'exécuter des scripts malveillants comme une vulnérabilité de script de site à site.
Dépendances et prérequis	Aucun
Références	Workflow administration

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Balisage XML d'échappement [mis à jour dans Security Center 1.3]

Utilisez la propriété pour forcer l'échappement *glide.ui.escape_text* des valeurs XML au niveau de l'analyseur avant de les transmettre au navigateur du client.

Le script de site à site se produit lorsqu'un attaquant injecte du JavaScript malveillant dans un point d'entrée. La plateforme/l'application ne parvient pas à échapper au JavaScript malveillant avant de le transmettre au navigateur de la victime pour exécution. S'échapper dans ce contexte signifie ce qui suit :

- **&** --> `&`
- **<** --> `<`
- **>** --> `>`
- **"** --> `"`
- **'** --> `'`
- **/** --> `/`

Exemple : `<![CDATA[<script>alert('XSS Attack') ;]] >`

Échappement : `<script>alert('Attaque XSS') ; </script>`

Assurez-vous que la *glide.ui.escape_text* propriété existe dans la table sys_properties et qu'elle est définie sur vrai.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.escape_text*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	L'échappement XML permet d'éviter que les navigateurs n'analysent le code JavaScript malveillant intégré dans les données non approuvées et ne l'exécutent pas en tant que JavaScript. • Un utilisateur malveillant peut tenter une attaque XSS pour détourner la session d'autres utilisateurs ou rediriger l'utilisateur vers un site Web malveillant. • La Now Platform contient du code pour sécuriser les cookies, mais pour l'échapper, cette propriété doit être définie sur **vrai**.
Valeur recommandée	VRAI
Cote de risque de sécurité	8.8

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Impact fonctionnel	(Moyen) Cette correction applique le codage XML au niveau de l'analyseur XML sur l'interface utilisateur. Il restitue les résultats codés pour l'utilisateur, ce qui peut avoir un impact sur la fonctionnalité en fonction de l'interaction de l'utilisateur de l'instance avec les données résultantes.
Risque de sécurité	(Élevé) La validation de l'entrée doit avoir lieu sur l'application pour se défendre contre les attaques de script de site à site. Ces attaques permettent à des scripts étrangers de s'exécuter sur la session utilisateur dans le contexte du navigateur connecté. Les attaquants peuvent l'utiliser pour voler des informations de session et des données sensibles.
Solution de contournement	Une fois cette propriété définie sur **vrai**, le rendu s'arrête sur les balises HTML dans la description de l'élément de catalogue ou dans le texte d'aide de la variable d'élément de catalogue. Il est possible que vous ne puissiez pas utiliser le formatage HTML pour certains champs. Toutefois, si la *glide.ui.escape_text* propriété est désactivée, toutes les expressions JEXL seront précédées d'un encodeur de sortie : ${JS :expression} ${HTML :expression} ou ${JS,HTML :expression}

Échapper à la réponse XML

Gérez la façon dont les échappements XML sont gérés sur votre instance.

Utilisez cette propriété pour gérer si les réponses XML sont échappées. Si la propriété est définie sur la valeur recommandée faux, **les** réponses XML ne sont pas échappées, ce qui peut entraîner une attaque par injection XML. L'injection de contenu XML non intentionnel dans un message XML peut modifier la logique prévue d'une application.

En savoir plus

Attribut	Description
Nom de la configuration	*glide.soaprequest.unescape_xml_response*
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	faux
Valeur par défaut	faux
Catégorie	Validation, nettoyage et codage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Risque de sécurité	• Score de gravité : 6,4 • Score CVSS : moyen • Détails du risque de sécurité : définir cette propriété sur **faux** désactive l'échappement XML, ce qui peut entraîner une attaque par injection XML.
Dépendances et prérequis	Aucun

Activer l'assainisseur HTML [mis à jour dans Security Center 1.3]

Utilisez la propriété pour activer l'include de script HTMLSanitizer, qui nettoie l'entrée *`glide.html.sanitize_all_fields`* HTML selon les attributs sur liste d'exclusion et d'inclusion configurés dans un script.

Les types de champs disponibles avec le dictionnaire/les champs incluent HTML et HTML traduit. Ces champs d'entrée HTML permettent aux utilisateurs d'écrire une entrée au format HTML, par exemple :

`<h1>Test</h1>`), en utilisant les balises HTML les plus basiques telles que `<img>`, `<a href ⋯ >`, et `<iframe>`.

Cela peut ouvrir la porte à un attaquant malveillant pour injecter un vecteur malveillant avec des balises HTML telles que :

`[<IMG SRC=" &#14; JavaScript:alert('XSS');">][<IMG onmouseover="alert('xss')">],[a href=" » onclick=alert(/xss/)]`.

En savoir plus

Attribut	Description
Nom de la propriété	*`glide.html.sanitize_all_fields`*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Empêche les applications contre les attaques de script de site à site et d'injection HTML
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Élevé) Cette correction applique un mécanisme de codage de sortie HTML avant que les données utilisateur ne soient restituées à l'utilisateur. Si le client dispose d'une personnalisation qui implique le rendu de l'attribut HTML ou des données de contenu, il y a un impact sur la fonctionnalité.
Risque de sécurité	(Élevé) L'entrée de l'utilisateur doit être traitée en toute sécurité lorsque les données sont stockées et traitées sur l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	Cela réduit les attaques de script de site à site côté client en encodant les données en sortie.
Solution de contournement	Cette propriété nettoie tous les champs HTML du système. Si vous devez activer l'assainissement HTML sur des champs individuels, voir Activer l'assainissement sur des champs individuels. Vous pouvez également configurer la liste d'inclusion ou la liste d'exclusion pour nettoyer les balises et les attributs HTML conformément à la politique de votre organisation.
Références	Activation de l'assainisseur HTML Assainisseur HTML

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les packages Java autorisés [Mise à jour dans Security Center 1.3]

La configuration de ces propriétés protège contre l'exposition des API dangereuses au moteur de scripting.

Configurez les tables système et installez le module d'extension recommandé en conséquence.

Si la table et *sys_whitelist_package* ne *sys_whitelist_member* sont pas des valeurs vides, les API dangereuses peuvent être exposées au moteur de scripting. Les entrées correspondent à l'espace de noms Java qui n'a pas été approuvé par ServiceNow les équipes de sécurité.

Installez l'outil de suppression des appels de packages. Consultez Outil de suppression d'appel de packages pour en savoir plus.

Contact Service et assistance client pour modifier ces tables.

En savoir plus

Attribut	Description
Table, nom du module d'extension	Tables: • *sys_whitelist_member* • *sys_whitelist_package* Module d'extension : com.glide.script.packages_call_removal
Type de configuration	Configuration tabulaire, modules d'extension
Catégorie	Validation, nettoyage et codage
Objectif	Protégez-vous contre l'exposition des API dangereuses au moteur de scripting.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Valeur recommandée	Vide
Valeur par défaut	Aucun. Il s'agit d'une configuration de table et non d'une propriété Glide, il n'y a donc pas de valeur par défaut.
Type de configuration	liste de tables, module d'extension
Risque de sécurité	(Élevé) Les API dangereuses peuvent être exposées au moteur de scripting. Ces API prises en charge risquent de rendre l'instance instable et non sécurisée.
Cote de risque de sécurité	8.2

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Outil de suppression d'appel de packages

Activez et exécutez le module d'extension Packages Call Removal Tool (*com.glide.script.packages_call_removal*), puis décidez si chaque changement proposé doit être appliqué ou rejeté.

L'outil de suppression des appels de packages est un plugin qui :

- Analyse les scripts à la recherche d'appels de packages aux Now Platform classes Java.
- Propose des changements pour les remplacer par les noms GlideScriptable préférés.
- Facilite les changements de script.

Remarque :
S'il s'agit d'un enregistrement de système de base, l'utilisation de la recommandation de l'outil entraîne le marquage de l'élément comme customer_update. Cependant, il peut toujours être utile d'utiliser cet outil car il signale les appels Packages, xxx.

L'outil de suppression des appels de packages peut signaler certains appels de packages utilisés dans `sa_mapping_ext_commands` et `sa_custom_operation`. Ces appels de package appartiennent au Serveur MID. Comme il n'y a pas de classes, le code s'exécute dans Serveur MID. Si vous trouvez l'un des appels de package répertoriés suivants dans la section Erreurs, marquez-le comme Rejeté (ignoré). L'outil ne signale plus cet appel de package.

- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_content)` ;
- `Packages.com.snc.sw.util.JSONUtil.toJSONPlain(file_name)` ;
- `Packages.com.snc.sw.commands.HttpCallHandler` ;
- `Packages.com.snc.sw.dto.ProviderType.SSH`

En savoir plus

Attribut	Description
Nom du module d'extension	com.glide.script.packages_call_removal
Type de configuration	Définition du système > Modules d'extension
Objectif	Pour supprimer/remplacer les appels de package/membre non autorisés par des noms Glide acceptables (GlideScriptable) qui n'autorisent qu'un accès autorisé aux données.

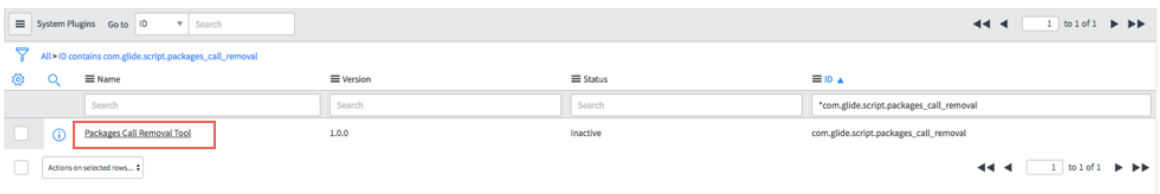
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

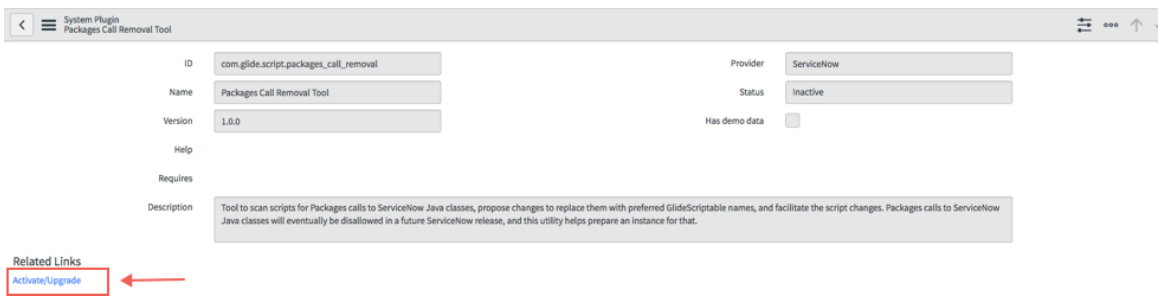
Attribut	Description
Valeur recommandée	Actif
Impact fonctionnel	(Faible) Cette remédiation remplacerait les appels de package par des API `GlideScriptable` et peut affecter les personnalisations qui incluent des appels de package. L'outil ne remplace pas automatiquement les appels de packages. Au lieu de cela, il fournit des suggestions qui sont stockées dans la table packages_call_item. Votre administrateur peut alors décider d'accepter ou de rejeter le changement proposé.
Risque de sécurité	(Moyen) Les appels d'API côté client qui entraînent la récupération de données ou l'accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Ils doivent être validés pour l'autorisation et la restriction de l'accès aux objets sensibles.

Étapes à configurer

1. Accédez à la **Définition du système** > **Modules d'extension**



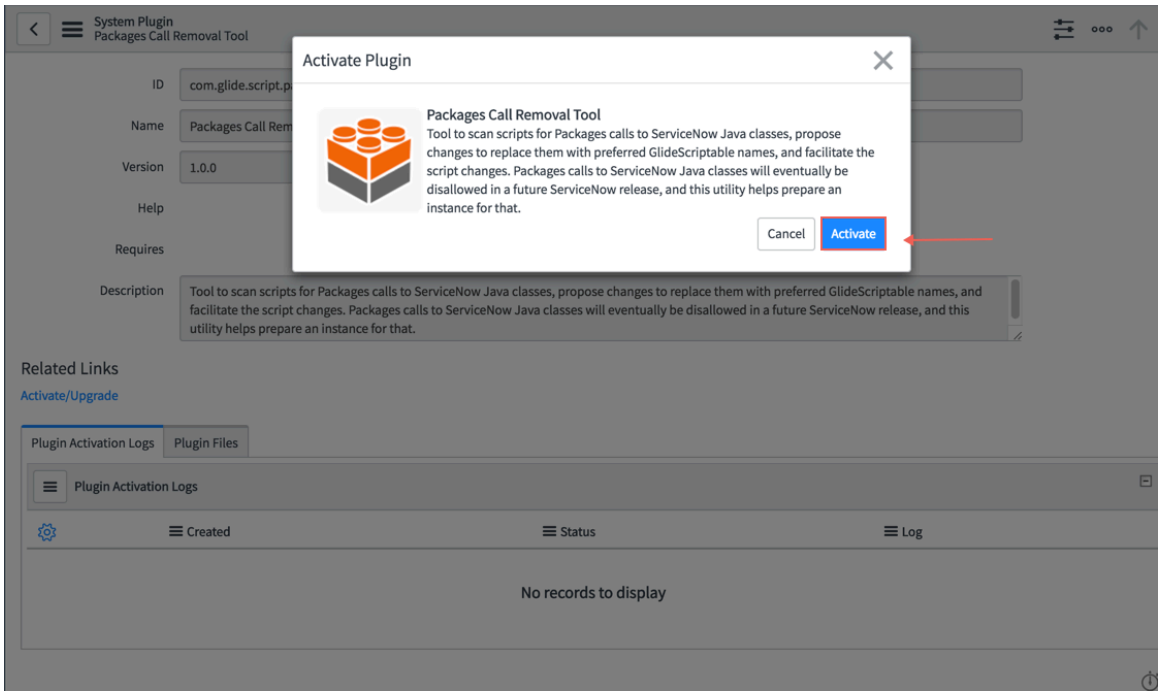
2. Recherchez l'ID du module d'extension = `com.glide.script.packages_call_removal`.



3. Cliquez sur **Activer/Mettre à niveau** pour activer le module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Pour vérifier les appels de packages de liste d'inclusion et les appels de membres de listes d'inclusion, effectuez les actions décrites dans les sections Étapes de configuration des rubriques suivantes :
   - Vérifier les appels des membres de la liste d'autorisation
   - Vérifier les appels de packages de la liste d'autorisation

Annuler le nom distinctif initial LDAP [mis à jour dans Security Center 1.3]

Utilisez cette propriété pour gérer le nom unique d'un enregistrement de serveur LDAP.

Cette propriété contrôle le nom unique d'un enregistrement de serveur LDAP qui est inséré lors de l'exécution d'un script correctif prêt à l'emploi (OOB). Si elle est définie sur la valeur recommandée « » ou vide, les données du serveur LDAP peuvent être énumérées par un utilisateur ayant des privilèges inférieurs.

En savoir plus

Attribut	Description
Nom de la configuration	`glide.ldap.initial.dn`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	chaîne
Valeur recommandée	vide
Valeur par défaut	vide
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 2,7 • Score CVSS : faible

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	• Détails des risques de sécurité : si vous définissez la valeur de la propriété sur « » ou sur vide, les données du serveur LDAP peuvent être accessibles à un utilisateur ayant des privilèges inférieurs.
Dépendances et prérequis	Aucun

Appliquer la sécurité stricte des cookies de session [Mise à jour dans Security Center 1.3]

Utilisez la *glide.ui.secure_cookies* propriété pour exiger des cookies correctement formatés

Lorsque vous définissez la propriété sur vrai, votre instance rejette une session si le format du cookie associé n'est pas attendu.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.ui.secure_cookies*
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour obtenir une authentification de session plus sécurisée.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	8.8
Impact fonctionnel	(Faible) Lorsque la propriété est définie sur vrai, les cookies mal formatés sont rejetés. Lorsqu'un tel cookie est rejeté, l'utilisateur doit se connecter à nouveau.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Minimiser le seuil d'expansion des entités [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour réduire la limite maximale d'expansion de l'entité *glide.xmlutil.max_entity_expansion* .

Le Now Platform ne traite pas d'autres expansions d'entité supérieures à la limite autorisée spécifiée dans cette propriété.

ⓘ Remarque :
500 est le minimum par défaut imposé par le Now Platform, qui est considéré comme un seuil de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.xmlutil.max_entity_expansion`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques d'expansion d'entité XML/de milliards de rires.
Valeur recommandée	3000
Valeur par défaut	100000
Cote de risque de sécurité	5.3
Impact fonctionnel	(Faible) Si la personnalisation utilise une extension d'entités volumineuses, le peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Modéré) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les types MIME chargés [Mise à jour dans Securty Center 1.3]

Utilisez la propriété pour activer la vérification du type MIME pour les `glide.security.file.mime_type.validation` chargements. Vous pouvez activer (propriété sur **true**) ou désactiver (définir la propriété sur **faux**) la validation de type MIME pour les pièces jointes de fichiers.

Prérequis

Avant de définir cette propriété, définissez-la `glide.attachment.extensions` . Le type MIME est vérifié pendant `glide.attachment.extensions` le chargement uniquement pour les extensions spécifiées dans Pour en savoir plus, consultez Restrict file extensions .

En savoir plus

Attribut	Description
Nom de la propriété	`glide.security.file.mime_type.validation`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Pour appliquer la vérification du type MIME / des octets magiques pendant les téléchargements de fichiers.
Valeur recommandée	VRAI
Valeur par défaut	VRAI

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Cote de risque de sécurité	5.4
Impact fonctionnel	(Moyen) Cette remédiation active la vérification de type MIME sur les pièces jointes à l'application. Aucun impact sur la fonctionnalité, sauf s'il y a une intention malveillante dans le chargement des fichiers, car cette validation vérifie simplement la mauvaise synchronisation entre le type MIME et les données.
Risque de sécurité	(Moyen) Pour réduire les vulnérabilités telles que l'inclusion de fichiers et les téléchargements de fichiers malveillants, la vérification du type MIME doit être activée.
Références	Administering attachments

Pour plus de détails sur la configuration des propriétés de sécurisation renforcée, reportez-vous Paramètres de la sécurisation pour la sécurité de l'instance à la section .

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Restreindre les entités externes XML [Mise à jour dans Security Center 1.3]

Utilisez la propriété pour activer la vérification du type MIME pour les `glide.security.file.mime_type.validation` chargements. Vous pouvez activer (propriété sur **true**) ou désactiver (définir la propriété sur **faux**) la validation de type MIME pour les pièces jointes de fichiers.

Prérequis

Avant de définir cette propriété, définissez-la `glide.attachment.extensions` . Le type MIME est vérifié pendant `glide.attachment.extensions` le chargement uniquement pour les extensions spécifiées dans

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.xml.entity.whitelist`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre les attaques XXE.
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Cote de risque de sécurité	5.4
Impact fonctionnel	(Faible) Si la personnalisation utilise une entité externe, et non une inclusion répertoriée dans la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
	`glide.xml.entity.whitelist` propriété, la Now Platform peut bloquer le traitement ultérieur.
Risque de sécurité	(Critique) Un attaquant peut utiliser la DTD pour inclure des requêtes HTTP arbitraires que le serveur peut exécuter. Cela pourrait conduire à d'autres attaques en utilisant la relation de confiance du serveur avec d'autres entités.

Exiger la validation des entités XMLdoc2 avec l'expansion des entités allowlistDisable [Mise à jour dans Security Center 1.3]

Si les personnalisations ne nécessitent pas d'expansion d'entité, utilisez la propriété pour désactiver complètement l'expansion d'entité `glide.xmlutil.max_entity_expansion` externe. Le XML termine l'analyse mais n'inclut aucune entité interne ou externe.

- Si vous définissez cette propriété sur **vrai**, toutes les entités externes tentent de résoudre ou de développer les entités sujets, sous réserve de la définition de la `glide.stax.whitelist_enabled` propriété.
- Si vous définissez cette propriété sur **false**, toute la résolution et l'expansion de l'entité sont bloquées. Pour en savoir plus, consultez Validation d'entité XMLdoc2 avec liste d'autorisation.

Prérequis

Avant de définir cette propriété :

- Définissez les `glide.xml.entity.whitelist.enabled` propriétés and `glide.stax.whitelist_enabled` sur true. Pour en savoir plus, consultez Validation des entités XMLdoc/XMLUtil avec liste d'autorisation et Validation d'entité XMLdoc2 avec liste d'autorisation.
- Définissez une liste de FQDN délimités par des virgules dans la `glide.xml.entity.whitelist` propriété, car il s'agit des seules URL atteignables à l'aide de la propriété de traitement d'entité XML. Pour en savoir plus, consultez Traitement d'entité externe XML : liste d'autorisation.

⚠ Avertissement :
Il s'agit d'une propriété de sphère de sécurité, ce qui signifie que la valeur ne peut pas être modifiée une fois qu'elle a été modifiée. Il n'est pas réversible.

En savoir plus

Attribut	Description
Nom de la propriété	`glide.stax.whitelist_enabled`
Type de configuration	Propriétés système (/sys_properties_list.do)
Catégorie	Validation, nettoyage et codage
Objectif	Ce contrôle de rattrapage doit être activé pour assurer la défense contre une attaque par expansion d'entité XML/Billion Laugh.
Valeur recommandée	VRAI
Valeur par défaut	faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Cote de risque de sécurité	9.8
Impact fonctionnel	(Faible) Si la personnalisation utilise l'expansion des entités, le peut bloquer le Now Platform traitement ultérieur.
Risque de sécurité	(Critique) Un attaquant peut utiliser cette vulnérabilité pour étendre les données de manière exponentielle, consommant rapidement toutes les ressources du système.
Solution de contournement	Si la personnalisation nécessite une expansion de l'entité, définissez cette propriété sur vrai et suivez les étapes documentées à la rubrique Validation d'entité XMLdoc2 avec liste d'autorisation.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Pour plus d'informations sur les ressources OWASp, consultez OWASp .

Définir une politique de sécurité de contenu sûre pour les fichiers SVG [Nouveau dans Security Center 1.3]

La `com.glide.csp.self_script_src_svg` propriété ajoute la directive **script-src none** à l'en-tête HTTP Content-Security-Policy lorsque des SVG (Scalable Vector Graphics) sont accessibles via l'extension de fichier IIX (Translation Memory Index).

La propriété empêche les `com.glide.csp.self_script_src_svg` pièces jointes malveillantes qui stockent des attaques de script de site à site (XSS) de s'exécuter dans une instance. Sans cette politique, un acteur malveillant pourrait amener un utilisateur à exécuter du code JavaScript arbitraire dans son navigateur Web, ce qui pourrait entraîner des failles de sécurité telles que l'exfiltration de données et la prise de contrôle de session.

En savoir plus

Attribut	Description
Nom de la configuration	`com.glide.csp.self_script_src_svg`
Type de configuration	Propriétés système (/sys_properties_list.do)
Type de données	booléen
Valeur recommandée	VRAI
Valeur par défaut	VRAI
Catégorie	Validation, nettoyage et codage
Risque de sécurité	• Score de gravité : 7,1 • Score CVSS : élevé • Détails des risques de sécurité : Si vous ne définissez pas cette propriété sur la valeur recommandée, vrai, un utilisateur peut exécuter du code JavaScript arbitraire provenant d'un acteur malveillant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Dépendances et prérequis	Aucun
Impact fonctionnel	Cette propriété empêche les fichiers SVG (Scalable Vector Graphics) d'accéder à des scripts externes.

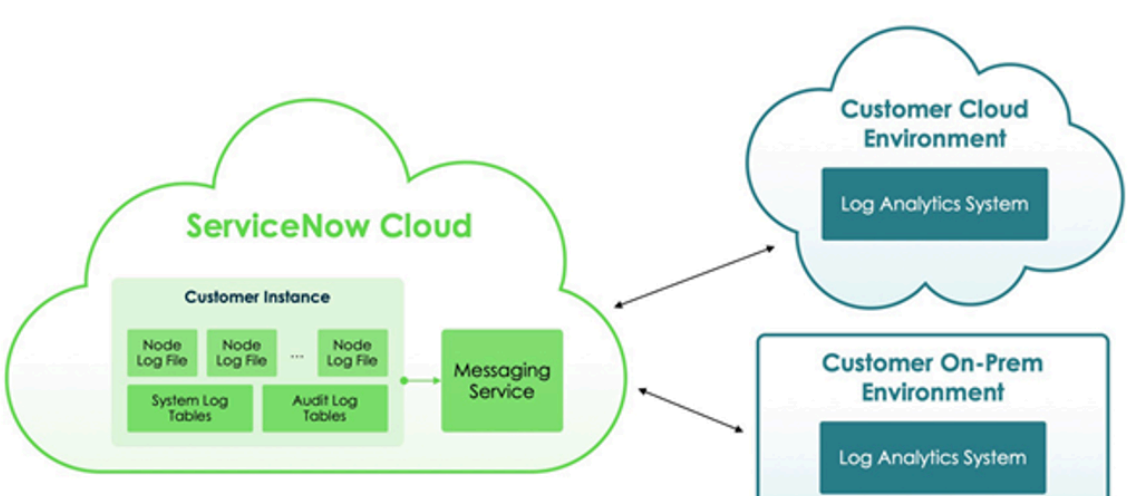
Service d'exportation de journal (LES)

Service d'exportation de journal (LES) vous permet d'exporter de manière transparente vos journaux d'instance, de système et d'application vers vos outils d'analyse de sécurité d'entreprise. Le service fournit une intégration hautement évolutive et presque en temps réel avec vos outils d'analyse, facile à configurer et à gérer.

L'outil d'intégration vous permet d'exploiter vos solutions analytiques pour effectuer les opérations suivantes :

- Détecter les ServiceNow menaces de sécurité et analyser les incidents de sécurité
- Dépanner et optimiser les ServiceNow performances de l'application
- Surveillez et optimisez l'expérience ServiceNow utilisateur

LES tire parti d'une Now PlatformService de messagerie Hermes fonctionnalité appelée , qui est un service de transport de données et de mise en file d'attente multilocataire et multi-clusters qui Apache Kafka permet à votre instance de produire et d'utiliser de gros volumes d'événements Kafka. Apache Kafka est une plateforme de streaming de données open source qui fournit un point d'intégration unique pour l'échange de données entre les systèmes business de votre organisation.



LES transmet une copie des événements de journal au fur et à mesure qu'ils sont générés vers le Service de messagerie Hermes .

Il Service de messagerie Hermes s'agit d'un service de transport de données et de mise en file d'attente Apache Kafka multilocataire et multi-clusters qui permet à votre instance de produire et de consommer de gros volumes d'événements Kafka. Il Service de messagerie Hermes s'agit d'une aptitude Now Platform disponible dans le cadre de Connexion au flux, Service d'exportation de journal (LES) et Réplication de données d'instance (Analyse de l'intégrité des journaux).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

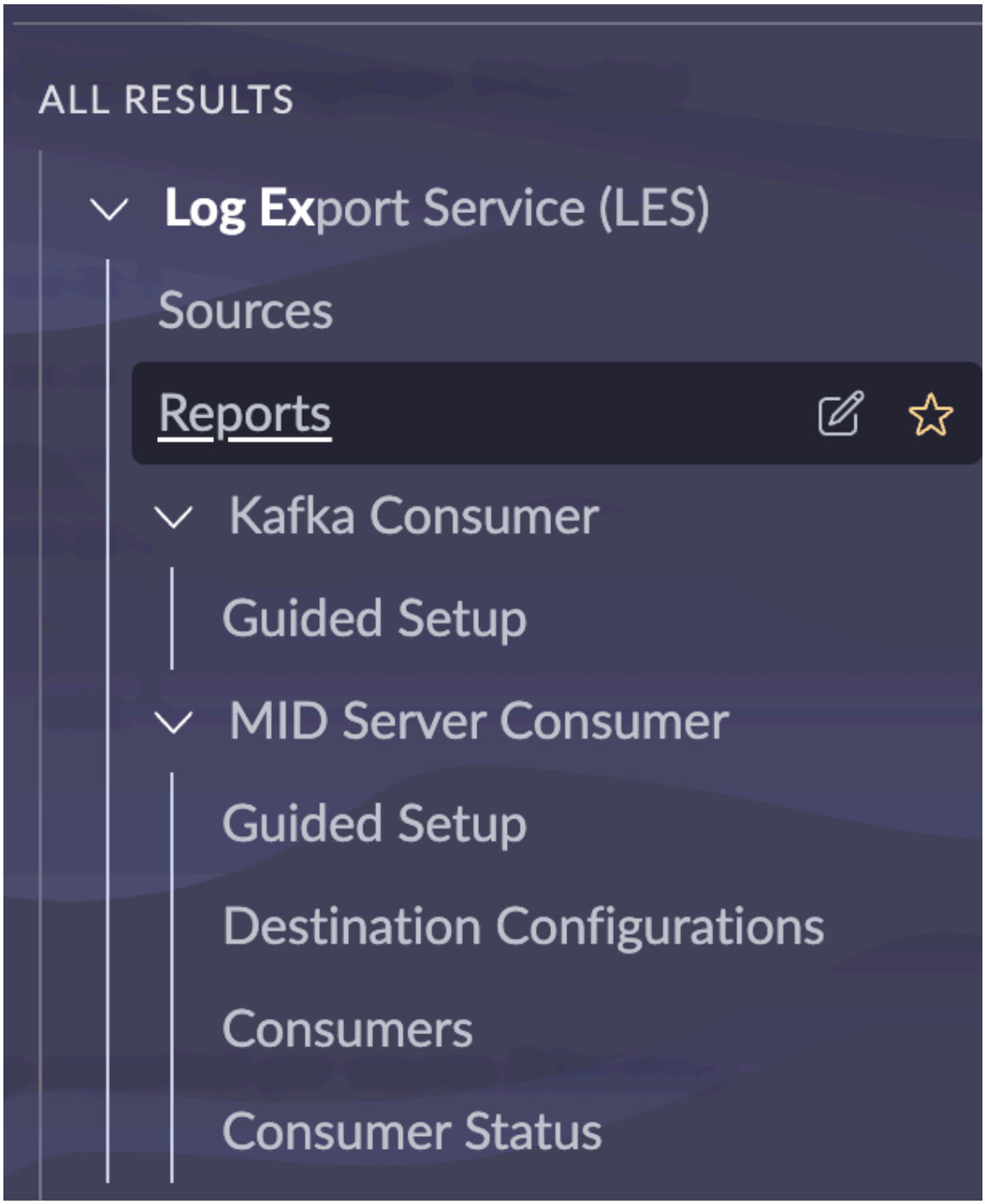
Les systèmes d'analyse de journaux externes, dans le cloud ou sur site, peuvent utiliser et utiliser les événements de journal provenant du Service de messagerie Hermes . LES fournit trois options de connectivité pour utiliser les journaux :

- Dédié Serveur MID: Un dédié Serveur MID est installé sur site ou dans le cloud qui s'y Service de messagerie Hermes connecte automatiquement, en extrait les événements de journal en continu puis les pousse vers les outils d'analyse de journaux via une connexion REST.
- Exploitez le connecteur Kafka de votre solution d'analyse de journaux (par exemple, Splunk) : un connecteur Kafka du produit d'analyse de journaux de votre choix est installé sur site ou dans le cloud et se connecte Service de messagerie Hermes automatiquement, extrait les événements de journal en continu, puis les transmet aux outils d'analyse de journaux.
- Directement à partir de votre système Kafka : votre système Kafka se connecte directement à et Service de messagerie Hermes utilise ses commandes et sa connectivité de protocole Kafka natives pour en extraire des événements de journaux.

Pour configurer et gérer le LES, vous devez l'installer à partir de ServiceNow Store. L'application LES fournit des configurations guidées pour vous aider à installer le service, des pages pour configurer le service (sources de journal, consommateurs et destinations) et des rapports pour comprendre la création et la consommation de journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Remarque :
vous pouvez également créer une nouvelle configuration source. Consultez Créer une configuration de source de journal pour plus d'informations.

Service d'exportation de journal rôles

Service d'exportation de journal est installé avec ces rôles.

Administration d'application [sn_logstoanalytics.admin]

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez Managing per-user subscriptions in Subscription Management et contactez votre représentant de compte.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce rôle est installé avec l'application LES et permet à un non-administrateur d'utiliser l'application.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Élevé

Indique s'il s'agit d'un rôle élevé. Les rôles élevés ne sont pas affectés à des utilisateurs ou à des groupes, et doivent être utilisés par élévation. Pour plus de détails, consultezÉlever à un rôle privilégié.

N°

Considérations particulières

Aucun.

Administrateur système [administrateur]

Pour en savoir plus sur la gestion des abonnements par utilisateur, consultez Managing per-user subscriptions in Subscription Management et contactez votre représentant de compte.

Le rôle administrateur est requis pour la configuration de l'application du magasin ERP.

Contient des rôles

Liste des rôles contenus dans le rôle.

- sn_templated_snip.template_snippet_admin
- [sn_employee.admin]
- taxonomy_admin
- sn_ace.ace_user
- [sn_hr_sp.esc_admin]

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Élevé

Indique s'il s'agit d'un rôle élevé. Les rôles élevés ne sont pas affectés à des utilisateurs ou à des groupes, et doivent être utilisés par élévation. Pour plus de détails, voir Élever à un rôle privilégié.

N°

Considérations particulières

Aucun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sources du journal

Service d'exportation de journal (LES) peut exporter des sources de journal à partir de certaines tables de journal système, de la table d'audit et des fichiers journaux de nœud d'application.

Voici les sources de journal qui peuvent être exportées par les LES.

- Tables de journaux système
  - Table syslog : affichez les avertissements et les erreurs pour les processus d'instance, les enregistrements et les événements non critiques, tels que l'utilisation de la mémoire sur le serveur
  - syslog_transaction table : afficher toute l'activité du navigateur pour une instance
  - sys_outbound_http_log table : affichez toutes les demandes et réponses concernant les services Web sortants tels que REST et SOAP
- Table d'audit : utilisez la vue de la table sys_audit enregistrer les modifications apportées aux tables choisies pour l'audit
- Fichiers journaux des nœuds d'application : utilisez les fichiers journaux localhost pour afficher les erreurs des nœuds d'applications. Votre instance dispose de plusieurs nœuds, et chaque nœud possède plusieurs fichiers journaux.

Reportez-vous à la rubrique Journaux système pour en savoir plus sur le schéma et l'objectif des sources de journal ci-dessus.

Créer une configuration de source de journal

Régulez et définissez des filtres sur les journaux à transmettre en créant une configuration de source de journal.

Avant de commencer

Rôle requis : admin ou sn_logstoanalytics.admin

Procédure

1. Accédez à la **Tout** > **Service d'exportation de journaux**.
   Une liste des configurations sources s'affiche.
2. **Sélectionnez Nouveau** si vous souhaitez créer une configuration source.
   Vous pouvez également sélectionner une configuration source existante si vous souhaitez la modifier.
   Le formulaire Source s'affiche.
3. Renseignez les champs du formulaire.

Formulaire source

Champs	Description
Type de source	Types de sources de journaux ○ Journal de nœud ○ Table Consultez Sources du journal pour plus d'informations.
Niveau de journal	Un ensemble de niveaux de journalisation standard qui peuvent être utilisés pour contrôler la sortie

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
	de journalisation. Conformément à la convention, chaque niveau transmettra des journaux de gravité égale ou supérieure. **Remarque :** Ce champ n'est visible que lorsque l'une des conditions suivantes est remplie. ○ Lorsque vous sélectionnez Journal de nœud comme type de source ○ Lorsque vous sélectionnez Table comme type de source et que la table est syslog
Accepte	Spécifie le format dans lequel les journaux sont transmis à Hermès. Ils peuvent être envoyés au format JSON ou en texte brut.
Table	Sélection de table pour les journaux de type table. **Remarque :** Ce champ n'est visible que lorsque vous sélectionnez Table comme type de source.
Type de filtre	Conditions pour transmettre les journaux de manière sélective. **Remarque :** Ce champ n'est visible que si vous sélectionnez syslog ou sys_audit comme table.

4. Sélectionnez **Soumettre** pour créer une nouvelle configuration source.

Créer plusieurs rubriques dans la table source LES

Utilisez les messages pour chaque type de source indépendamment en créant une rubrique unique par type de source.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Ajoutez la propriété système sn_logstoanalytics.kafka.multi_topics et définissez-la sur Vrai.
   Elle est définie sur faux par défaut.
2. Créez un enregistrement source.

   Remarque :
   Lorsque vous créez un nouveau type de source, une rubrique unique est créée pour celui-ci.

   Les noms des rubriques ont le suffixe comme type de source. Par exemple, sn_logstoanalytics.node_log a le node_log comme type de source.
3. **Facultatif :** Créez une autre rubrique pour une source différente comme dans les étapes précédentes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si sn_logstoanalytics.kafka.multi_topics est défini sur faux, la possibilité de créer plusieurs rubriques dans la table source est désactivée.

Remarque :
Cette fonctionnalité n'est pas compatible avec le consommateur du serveur MID (LES v2). Vous devez utiliser votre propre consommateur (ERP v1).

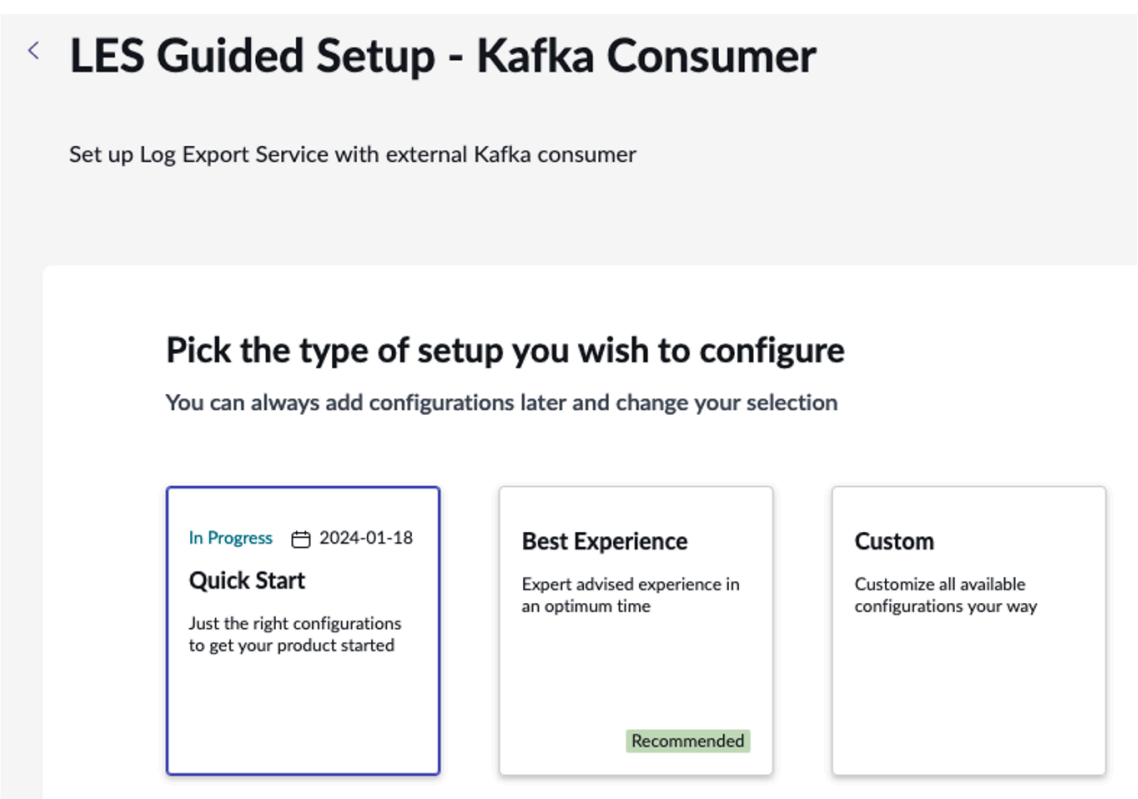
Consommateur Kafka

Utilisez la configuration guidée pour passer par la configuration initiale du LES. La configuration guidée vous assiste dans la planification du déploiement du produit et dans l'exécution de la configuration de base pour la mise en service.

La configuration guidée organise les activités de configuration en catégories. Chaque catégorie fournit des informations, telles que des conseils de planification, des étapes de pré-configuration et des liens d'accès à des contenus d'aide utiles. Les catégories fournissent également un ensemble de liens vers les pages de votre instance où vous effectuez la configuration. Le processus de configuration guidée conserve la trace de ce que vous avez terminé, de sorte que vous pouvez arrêter et reprendre là où vous vous étiez arrêté.

Page d'accueil de la configuration guidée

La page d'accueil de Guided Setup contient une vue d'ensemble des types de configuration pour votre configuration guidée. Vous pouvez sélectionner votre type de configuration guidée et sélectionner **Continuer** pour ouvrir les étapes de configuration guidée et commencer la configuration.



Les trois configurations de cette page (Démarrage rapide/Meilleure expérience/ Personnalisé) fournissent les mêmes tâches et fonctionnalités. Cela est nécessaire pour

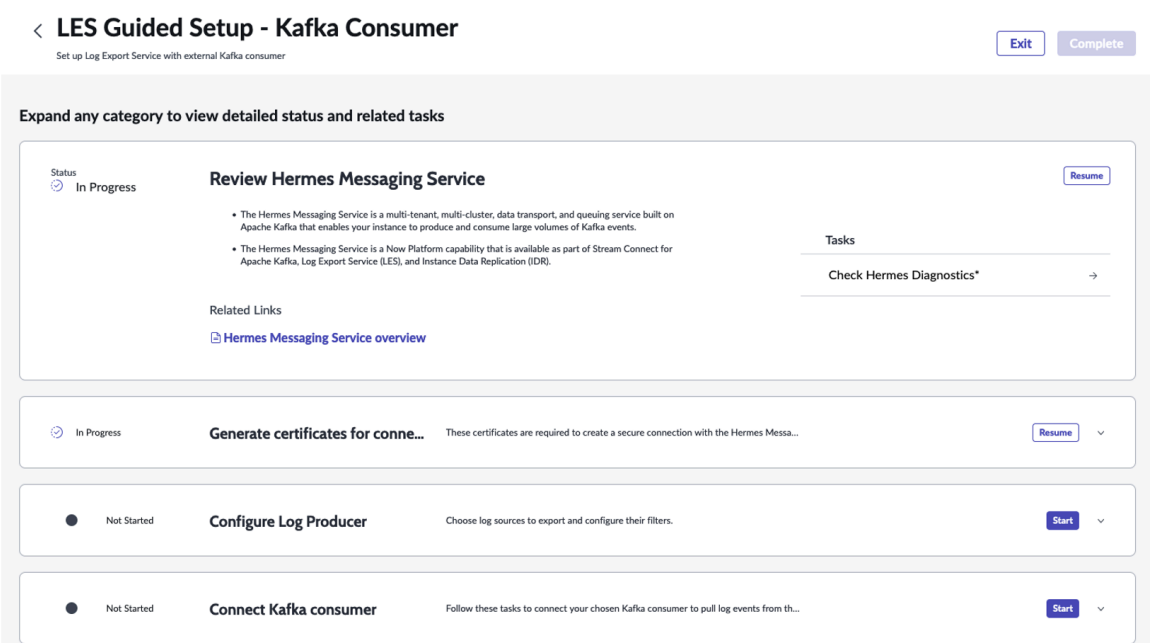
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

coordonner l'intégration entre l'instance ServiceNow et l'outil d'analyse de journal de destination avec l'administrateur respectif. L'administrateur d'analyse de journaux doit configurer son outil pour se connecter à l'instance ServiceNow en toute sécurité. Il est recommandé de partager le document avec l'administrateur Set up a secure connection to the Hermes Messaging Service d'analyse de journaux à l'avance. Même si vous avez marqué une tâche comme terminée, vous pouvez revenir en arrière et décocher son retour à l'état En cours. Pour ce faire, cliquez d'abord sur la zone **Modifier** dans le coin supérieur droit de la catégorie. Cliquez ensuite sur la zone **Modifier** de la tâche que vous souhaitez décocher. La case **Marquer comme terminé** ne sera plus marquée.

Page des catégories de configuration guidée

La page des catégories contient une vue d'ensemble et une description des catégories et des tâches associées. Vous pouvez cliquer sur la flèche de la liste déroulante pour afficher les informations sur la catégorie ou sur le bouton Démarrer pour ouvrir les étapes de configuration guidée et commencer la configuration.



Effectuez les tâches de chaque catégorie en suivant les instructions de configuration.

Configuration guidée pour les consommateurs Kafka

Implémentez les étapes suivantes pour obtenir une configuration guidée complète pour les consommateurs Kafka.

Avant de commencer

Accédez à la **Service d'exportation de journaux (LES)** > **Consommateur Kafka** > **Configuration guidée**. Sélectionnez le type de configuration que vous souhaitez configurer, puis cliquez sur **Continuer**.

Remarque :
Pendant l'installation de l'application Service d'exportation de journal , ServiceNow l'infrastructure sous-jacente sera mise en Service de messagerie Hermes service. Sachez que ce processus peut prendre jusqu'à deux heures à partir du moment où vous demandez l'installation de l'application Service d'exportation de journal .

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Examinez Service de messagerie Hermes les diagnostics.

   Il est recommandé de vérifier que le Service de messagerie Hermes est opérationnel à l'aide de l'outil de diagnostic, qui s'affiche Hermes à l'écran pendant cette étape. Si vous voyez une erreur « Page introuvable » sur cette page, n'est Hermes pas installé et vous devez contacter votre administrateur système.

   - Informations de configuration : les informations d'amorce suivantes permettent de se connecter au Service de messagerie Hermes fichier . Le « Producer Bootstrap » est la connexion utilisée pour envoyer des messages dans Hermes et le « Consumer Bootstrap 1 & 2 » est utilisé pour récupérer des messages dans Hermes.
     - Amorce du créateur
     - Amorce de consommateur 1
     - Amorce de consommateur 2
   - PKI d'instance : le composant d'infrastructure de clé publique d'instance (PKI) permet à une instance ServiceNow d'agir en tant qu'émetteur dans une hiérarchie de confiance X.509.
   - Connectivité d'amorce : cliquez sur **Exécuter le test** pour confirmer que le client externe est en mesure de se connecter aux ports d'instance définis (producteur et consommateur).
   - Connectivité de l'instance : cliquez sur **Exécuter le test** pour confirmer que l'instance est en mesure d'envoyer et de recevoir des messages.
   - Afficher les rubriques : cliquez sur la rubrique répertoriée pour récupérer l'horodatage du dernier message connu.

   Remarque :
   Vous pourrez accéder Hermes aux diagnostics à l'avenir pour résoudre d'éventuels problèmes de connectivité en revenant à cette étape de la configuration guidée ou en naviguant vers **Tout** > *Service de messagerie Hermes* > **Diagnostics**.

2. Générez des certificats pour une connexion Service de messagerie Hermes sécurisée et extrayez des événements de journal à partir de celle-ci.

   Vous allez utiliser ces certificats lors de la connexion de votre système externe.

   Configurez une connexion sécurisée à Service de messagerie Hermes . Consultez Set up a secure connection to the Hermes Messaging Service pour plus d'informations. Vous aurez besoin de ces certificats pour l'authentification et l'autorisation dans le client qui extraira les journaux d'Hermes.

   Remarque :
   Les rôles administrateur ou Hermes_admin sont requis pour cette étape.

3. Configurer le producteur de journaux : choisissez des sources de journal à exporter et configurez leurs filtres. Effectuez les tâches suivantes pour configurer le créateur de journaux.

   - Configurer les sources de journal à exporter : créez un enregistrement source pour chacune des sources de journal que vous souhaitez exporter.

     Remarque :
     Les rôles administrateur ou sn_logstoanalytics.admin sont requis pour terminer cette étape

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Cliquez sur **Nouveau** dans le coin supérieur droit

b. Sélectionner un type de source

c. Sélectionnez les filtres appropriés pour le type de source sélectionné

> **Remarque :**
> Les filtres sont différents selon le type de source sélectionné

d. Cliquez sur Mettre à jour.
Une fois créée, elle affiche le nom de la rubrique Hermes vers laquelle cette source de journal sera exportée. Notez le nom de la rubrique, vous en aurez besoin ultérieurement lors de la configuration de votre système de consommateur de journaux. Le champ Actif contrôle si cette source de journal va être exportée ou non. Si vous constatez des erreurs, revenez à la tâche « Vérifier les diagnostics Hermes » et vérifiez l'état Hermes.

- Valider le producteur de journaux : une fois que vous avez créé une source à partir de laquelle produire des journaux, vous pouvez afficher les enregistrements de journaux en direct dans la rubrique à l'aide de **Service de messagerie Hermes** > **Inspecteur de rubrique Hermes**.

  a. Sélectionner des rubriques externes

  b. Cliquer sur Répertorier les rubriques

  c. Sélectionnez la ligne correspondant à votre rubrique de l'étape précédente (répertoriée dans Sources)

  d. Ajuster la date de début du message si nécessaire

  e. Cliquez sur **Afficher** pour afficher un message du journal qui a été exporté vers la rubrique

4. Connecter le consommateur Kafka : suivez ces tâches pour connecter le consommateur Kafka de votre choix afin d'extraire les événements de journal d'Hermes.

- Identifier le consommateur Kafka : deux options s'offrent à vous en fonction de votre architecture d'analyse de journaux.
  - Si vous disposez de votre propre système Kafka et que vous le choisissez pour l'agrégation de journaux, vous pouvez vous connecter directement au service de messagerie Hermes via le protocole natif Kafka.
  - Si vous choisissez de connecter votre outil d'analyse de journaux directement à Service de messagerie Hermes, vous devez déployer un connecteur Kafka pris en charge par votre système d'analyse de journaux (c'est-à-dire Splunk Connect pour Kafka).

> **Remarque :**
> Dans les deux cas, vous devrez travailler avec l'administrateur de ces systèmes afin de coordonner la connexion avec le service de messagerie Hermes.

- Importer des certificats Hermes dans le système consommateur Kafka : connectez-vous à votre système client Kafka et assurez-vous que vous disposez des autorisations d'administrateur appropriées pour le configurer et le connecter à un système externe. Importez les certificats générés dans la tâche « Configurer une connexion sécurisée à Service de messagerie Hermes » dans votre connecteur Kafka ou votre serveur Kafka. Suivez les instructions de la documentation pour le consommateur Kafka que vous avez choisi.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurer les processus Kafka : le service de messagerie Hermes est conçu pour une haute disponibilité. Deux processus sont requis pour utiliser les messages d'Hermès. Deux processus sont requis, car Hermes utilise une paire de clusters Kafka à des fins de basculement. Si un cluster tombe en panne, les données sont produites pour l'autre cluster Hermes Kafka.

  Dans votre système client Kafka, vous devrez créer deux processus consommateurs distincts pour vous connecter aux deux clusters Hermes Kafka. Pour les deux processus, vous spécifierez la même rubrique Hermes Kafka, mais vous devrez configurer deux adresses d'amorce distinctes :

  - <instance_name>.service-now.com:4100,<instance_name>.service-now.com:4101,<instance_name>.service-now.com:4102,<instance_name>.service-now.com:4103
  - <instance_name>.service-now.com:4200,<instance_name>.service-now.com:4201,<instance_name>.service-now.com:4202,<instance_name>.service-now.com:4203

  Remarques importantes :

  - Lorsque vous accédez à la rubrique Kafka à partir de systèmes externes, vous devez ajouter « snc.<nom d'instance> » à la rubrique vers laquelle les journaux sont transférés.
  - Configurez chaque consommateur avec le même ID de groupe de consommateurs Kafka.
  - Installez vos fichiers keystore et truststore dans un emplacement auquel vos consommateurs peuvent accéder.
  - Si vos consommateurs en ont besoin, spécifiez les propriétés des convertisseurs JSON Kafka pour désactiver les schémas : « key.converter.schemas.enable=false », « value.converter.schemas.enable=false »
- Vérifier que le consommateur Kafka extrait les journaux d'Hermes : vérifiez dans le consommateur Kakfa que vous avez choisi que vous pouvez extraire les événements de journal du service de messagerie Hermes.

Consommateur de MID Server

Utilisez la configuration guidée pour passer par la configuration initiale du LES. La configuration guidée vous assiste dans la planification du déploiement du produit et dans l'exécution de la configuration de base pour la mise en service.

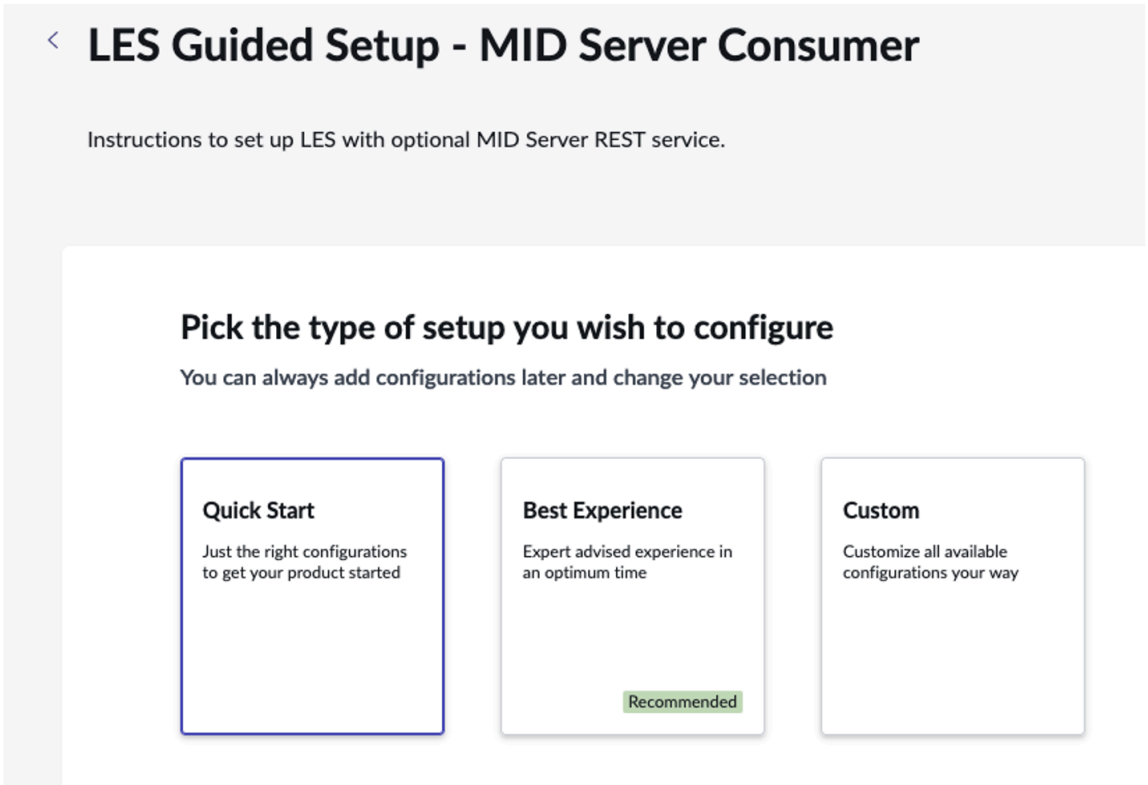
La configuration guidée organise les activités de configuration en catégories. Chaque catégorie fournit des informations, telles que des conseils de planification, des étapes de pré-configuration et des liens d'accès à des contenus d'aide utiles. Les catégories fournissent également un ensemble de liens vers les pages de votre instance où vous effectuez la configuration. Le processus de configuration guidée conserve la trace de ce que vous avez terminé, de sorte que vous pouvez arrêter et reprendre là où vous vous étiez arrêté.

Page d'accueil de la configuration guidée

La page d'accueil de Guided Setup contient une vue d'ensemble des types de configuration pour votre configuration guidée. Vous pouvez sélectionner votre type de configuration guidée et sélectionner **Continuer** pour ouvrir les étapes de configuration guidée et commencer la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



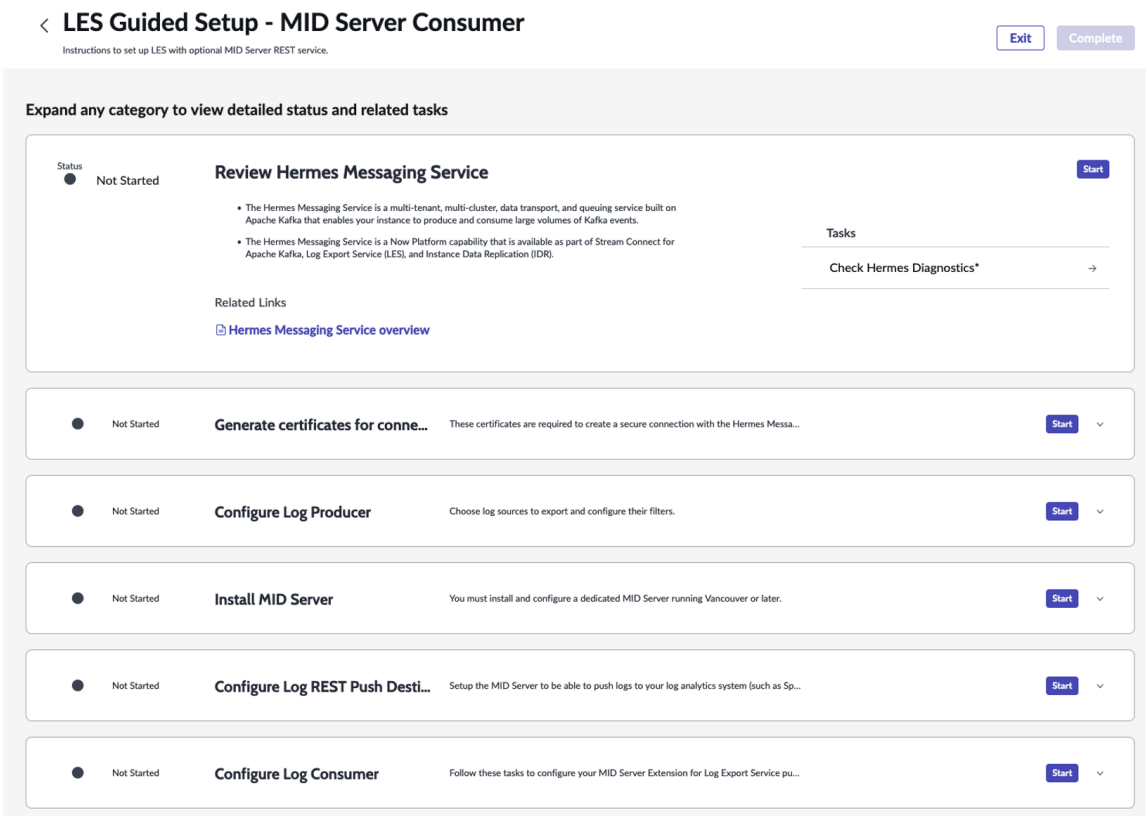
Les trois configurations de cette page (Démarrage rapide/Meilleure expérience/Personnalisé) fournissent les mêmes tâches et fonctionnalités. Un MID Server dédié est nécessaire pour diffuser en continu les journaux de votre instance vers votre système d'analyse de journaux. Le serveur MID a besoin d'une configuration unique pour établir une connexion sécurisée au service de messagerie Hermes. Même si vous avez marqué une tâche comme terminée, vous pouvez revenir en arrière et la décocher pour la ramener à l'état en cours. Pour ce faire, cliquez d'abord sur la zone **Modifier** dans le coin supérieur droit de la catégorie. Cliquez ensuite sur la zone **Modifier** de la tâche que vous souhaitez décocher. La case **Marquer comme terminé** ne sera plus marquée.

Page des catégories de configuration guidée

La page des catégories contient une vue d'ensemble et une description des catégories et des tâches associées. Vous pouvez cliquer sur la flèche de la liste déroulante pour afficher les informations sur la catégorie ou cliquer sur **Démarrer** pour ouvrir les étapes de configuration guidée et commencer la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Effectuez les tâches de chaque catégorie en suivant les instructions de configuration.

Configuration guidée pour les consommateurs de Serveur MID

Implémentez les étapes suivantes pour une configuration guidée complète pour les consommateurs de Serveur MID.

Avant de commencer

Accédez à la **Service d'exportation de journaux (LES)** > **Consommateur de Serveur MID** > **Configuration guidée**. Sélectionnez le type de configuration que vous souhaitez configurer, puis cliquez sur **Continuer**.

Remarque :
Pendant l'installation de l'application Service d'exportation de journal , ServiceNow l'infrastructure sous-jacente sera mise en Service de messagerie Hermes service. Sachez que ce processus peut prendre jusqu'à deux heures à partir du moment où vous demandez l'installation de l'application Service d'exportation de journal .

Rôle requis : administrateur

Procédure

1. Examinez Service de messagerie Hermes les diagnostics.

   Il est recommandé de vérifier que le Service de messagerie Hermes est opérationnel à l'aide de l'outil de diagnostic, qui s'affiche Hermes à l'écran pendant cette étape. Si vous voyez une erreur « Page introuvable » sur cette page, n'est Hermes pas installé et vous devez contacter votre administrateur système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Informations de configuration : les informations d'amorce suivantes permettent de se connecter à Service de messagerie Hermes. Le « Producer Bootstrap » est la connexion utilisée pour envoyer des messages dans Hermes et le « Consumer Bootstrap 1 & 2 » est utilisé pour récupérer des messages dans Hermes.
  - Amorce du créateur
  - Amorce de consommateur 1
  - Amorce de consommateur 2
- PKI d'instance : le composant d'infrastructure de clé publique d'instance (PKI) permet à une instance ServiceNow d'agir en tant qu'émetteur dans une hiérarchie de confiance X.509.
- Connectivité d'amorce : cliquez sur **Exécuter le test** pour confirmer que le client externe est en mesure de se connecter aux ports d'instance définis (producteur et consommateur).
- Connectivité de l'instance : cliquez sur **Exécuter le test** pour confirmer que l'instance est en mesure d'envoyer et de recevoir des messages.
- Afficher les rubriques : cliquez sur la rubrique répertoriée pour récupérer l'horodatage du dernier message connu.

Remarque :
Vous pourrez accéder Hermes aux diagnostics à l'avenir pour résoudre d'éventuels problèmes de connectivité en revenant à cette étape de la configuration guidée ou en naviguant vers **Tout** > *`Service de messagerie Hermes`* > **Diagnostics**.

2. Générez des certificats pour une connexion sécurisée à Hermes Messaging Service et extrayez les événements de journal à partir de celui-ci.

   Configurez une connexion sécurisée au service de messagerie Hermes. Consultez Set up a secure connection to the Hermes Messaging Service pour plus d'informations. Vous aurez besoin de ces certificats pour l'authentification et l'autorisation dans le client qui extraira les journaux d'Hermes.

   Remarque :
   Les rôles administrateur ou Hermes_admin sont requis pour cette étape.

3. Configurer le producteur de journaux : choisissez des sources de journal à exporter et configurez leurs filtres. Effectuez les tâches suivantes pour configurer le créateur de journaux.
   - Configurer les sources de journal à exporter : créez un enregistrement source pour chacune des sources de journal que vous souhaitez exporter.

     Remarque :
     Les rôles administrateur ou sn_logstoanalytics.admin sont requis pour terminer cette étape

     a. Cliquez sur **Nouveau** dans le coin supérieur droit

     b. Sélectionner un type de source

     c. Sélectionnez les filtres appropriés pour le type de source sélectionné

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les filtres sont différents selon le type de source sélectionné

d. Cliquez sur Mettre à jour
Une fois créée, elle affiche le nom de la rubrique Hermes vers laquelle cette source de journal sera exportée. Notez le nom de la rubrique, vous en aurez besoin ultérieurement lors de la configuration de votre système de consommateur de journaux. Le champ Actif contrôle si cette source de journal va être exportée ou non. Si des erreurs s'affichent, revenez à la tâche Vérifier les diagnostics Hermes et vérifiez l'état Hermes.

- Valider le producteur de journaux : une fois que vous avez créé une source à partir de laquelle produire des journaux, vous pouvez afficher les enregistrements de journaux en direct dans la rubrique à l'aide de **Service de messagerie Hermes** > **Inspecteur de rubrique Hermes**.

  a. Sélectionner des rubriques externes

  b. Cliquer sur Répertorier les rubriques

  c. Sélectionnez la ligne correspondant à votre rubrique de l'étape précédente (répertoriée dans Sources)

  d. Ajuster la date de début du message si nécessaire

  e. Cliquez sur **Afficher** pour afficher un message du journal qui a été exporté vers la rubrique

4. Installer le serveur MID : vous devez installer et configurer un serveur MID dédié exécutant Vancouver ou une version ultérieure.
   Effectuez les tâches suivantes pour installer le serveur MID.

   - Installer un serveur MID dédié : le serveur MID utilisé par le service d'exportation de journaux doit être dédié uniquement à cette fin et n'est pas censé exécuter d'autres processus. Ceci est important pour garantir la remise en temps opportun des messages de journal exportés à votre point de terminaison REST. Vous pouvez installer le nouveau serveur MID à l'aide de la Use MID Server guided setup commande ou en l'installant manuellement. Pour l'installation manuelle, suivez d'abord la Configure MID Server network connectivity documentation, puis la Installing the MID Server documentation ensuite.
   - Valider le serveur MID : vous devez valider manuellement le serveur MID après son installation pour lui permettre d'exécuter des tâches d'automatisation. Pour valider le Serveur MID que vous dédiez au LES, consultez Validate the MID Server

5. Configurer la destination push REST des journaux : configurez le serveur MID pour qu'il puisse transmettre les journaux par push à votre système d'analyse de journaux (tel que Splunk).
   Effectuez les tâches suivantes pour configurer la destination push REST du journal.

   - Ajouter des propriétés MID : vous devez ajouter des propriétés au serveur MID afin qu'il puisse se connecter à Hermès. Accédez aux **> propriétésde Serveur MID** et définissez les valeurs appropriées pour chacune des propriétés énumérées ci-dessous.

Nom	Valeur
mid.les.kafka.ssl.truststore.password	<mot de passe>
mid.les.kafka.ssl.keystore.password	<mot de passe>
mid.les.kafka.ssl.key.mot de passe	<mot de passe>
mid.les.kafka.ssl.truststore.location	<your_path>/<truststore>.p12

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Valeur
mid.les.kafka.ssl.keystore.location	<your_path>/<magasin de clés>.p12
mid.les.kafka.ssl.truststore.type	PKCS12
mid.les.kafka.ssl.keystore.type	PKCS12
mid.les.kafka.client.id	<instance_name>
mid.les.kafka.group.id	snc.<instance_name>.group1
mid.les.kafka.bootstrap.servers	<instance_name>.servicenow.com:4100,<instance_name>.servicenow.
mid.les.kafka.set2.bootstrap.servers	<instance_name>.servicenow.com:4200,<instance_name>.servicenow.

Suivez ces notes pour obtenir certaines des valeurs ci-dessus

- <mot de passe> est le mot de passe que vous définissez pour le magasin de clés et le magasin de clés de confiance.
- <your_path> s'agit du chemin d'accès au répertoire dans lequel vous conservez le keystore et les fichiers du truststore que vous avez téléchargés. Les certificats doivent se trouver sur le serveur sur lequel vous exécutez le MID
- <instance_name> s'agit du nom de votre instance ServiceNow. Si vous n'êtes pas sûr, vous pouvez le trouver dans le tableau sys_properties
- Vous pouvez obtenir les valeurs pour mid.les.kafka.bootstrap.servers et mid.les.kafka.set2.bootstrap.servers à partir de la page Diagnostics Hermes. Accédez à la **Service de messagerie Hermes** > **Diagnostics** et copiez les chaînes sous Consumer Bootstrap 1 et Consumer Bootstrap 2 respectivement.

◦ Configurer la destination : créez un nouvel enregistrement de configuration de destination, qui définit le point de terminaison REST vers lequel cette extension transfère les journaux.

Remarque :
les rôles administrateur ou sn_logstoanalytics.admin sont requis pour terminer cette étape.

a. Accédez à la **Service d'exportation de journaux (LES)** > **Destination Configurations**

b. Créer un enregistrement de configuration

c. Spécifier l'URL du point de terminaison souhaité pour les sources de journaux exportées

d. Recherchez ou créez des informations d'identification pour vous connecter à votre point de terminaison. Lors de la création d'informations d'identification pour votre point de terminaison, notez que seuls les types d'informations d'identification suivants sont valides avec LES : auth. de base, OAuth, clé API

e. Recherchez ou créez un script de transformation. Nous sommes livrés avec le script pré-écrit, **SplunkTransform** pour Splunk

6. Configurer le consommateur LOG : suivez ces étapes pour configurer votre extension de serveur MID pour le service d'exportation de journaux.

◦ Configurer le contexte de consommateur LES : Au cours de cette étape, vous allez mettre à jour l'enregistrement de consommateur LES pour qu'il s'exécute sur le MID Server dédié que vous venez d'installer pour le service d'exportation de journaux. Accédez à la **Serveur MID** > **Extensions** > **Contexte de consommateur LES** et mettez à jour l'enregistrement de consommateur LES en définissant les champs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur « Consommateur LES » pour ouvrir l'enregistrement de contexte du Serveur MID
- Sélectionner un Serveur MID spécifique pour le champ « Exécuter sur »
- Saisissez le nom du MID que vous avez validé à l'étape précédente pour le champ « Serveur MID »

Cliquez sur **Mettre à jour** pour enregistrer.

Remarque :
Nous livrons avec un contexte préconstruit. N'en créez pas un deuxième. Cela peut avoir des conséquences inattendues.

- Configurer le consommateur : créez un nouvel enregistrement de consommateur, qui représente le processus faisant partie de l'extension Serveur MID du service d'exportation de journaux. Accédez à la **Service d'exportation de journaux (LES)** > **Consommateurs** et créez un nouvel enregistrement de configuration en spécifiant la rubrique Hermes à partir de laquelle récupérer les messages du journal et la destination vers laquelle les relayer. Lorsque vous sélectionnez le module **Consommateurs** , il affiche des informations sur le nom du consommateur et la configuration de destination.

  a. Créer un enregistrement de consommateur

  b. Choisir une rubrique source dans la liste déroulante

  c. Choisir une configuration de destination

  d. Démarrer le consommateur

- Vérifier l'intégration du serveur MID : accédez à **Service d'exportation de journaux (LES)** > **État du consommateur** et affichez les champs État et Détails de l'état de l'enregistrement défini. Les informations contenues dans ces champs signalent l'état actuel du processus en cours d'exécution sur le MID Server, y compris les erreurs qui ont pu se produire lors du relais de messages au point de terminaison REST. Il s'agit uniquement d'une page d'affichage d'état. Accédez à la **Service d'exportation de journaux (LES)** > **Consommateurs** si vous souhaitez créer un enregistrement de consommateur. #Si l'état du consommateur indique que le processus a démarré, vous devez être en mesure d'inspecter votre point de terminaison pour afficher les journaux qui lui ont été relayés. En outre, vous pouvez consulter les journaux sur le serveur MID pour voir s'il existe des détails supplémentaires sur les erreurs qui peuvent être rencontrées. Vous pouvez également activer la journalisation de débogage sur le serveur MID pour obtenir des informations supplémentaires si nécessaire.

Remarque :
Si vous apportez une modification à l'un des enregistrements de consommateur, elle s'affiche sur la page d'affichage de l'état du consommateur. Si vous sélectionnez un nom d'enregistrement de consommateur sur la liste État du consommateur, le formulaire Consommateur de l'enregistrement sélectionné s'ouvre. Vous pouvez ensuite mettre à jour le nom et la configuration de destination de l'enregistrement sélectionné.

Rapport du journal d'examen

Analysez la taille de chaque journal de données en examinant le tableau de bord du rapport de journal.

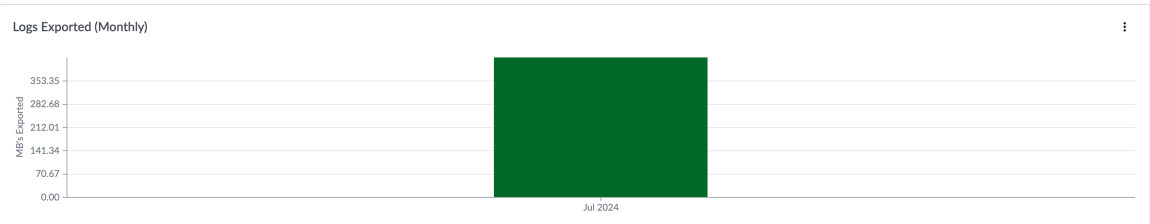
Avant de commencer
Rôle requis : admin ou sn_logstoanalytics.admin

Traduction automatique

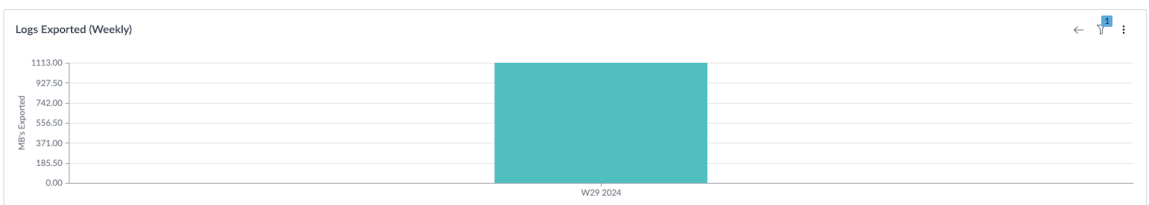
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

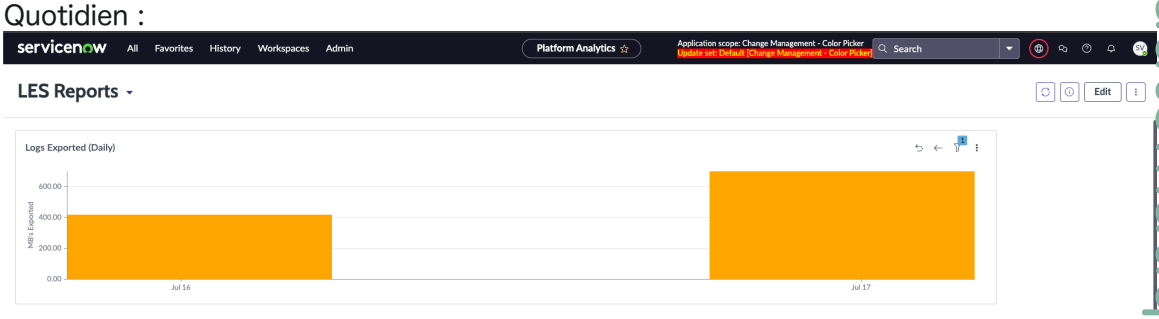
1. Accédez à la **Tout** > **Service d'exportation de journaux** > **Rapports**.
2. Examinez les données du journal dans les widgets suivants.
   - Journaux exportés (mensuels) : affiche les mégaoctets exportés par mois dans la vue initiale. Vous pouvez explorer le graphique pour afficher les données de chaque semaine ou de chaque jour. Vous pouvez afficher les données des 395 derniers jours.



Remarque :
Cliquez sur les flèches dans le coin supérieur droit du widget pour analyser les données. Vous pouvez également remonter jusqu'aux données parentes.

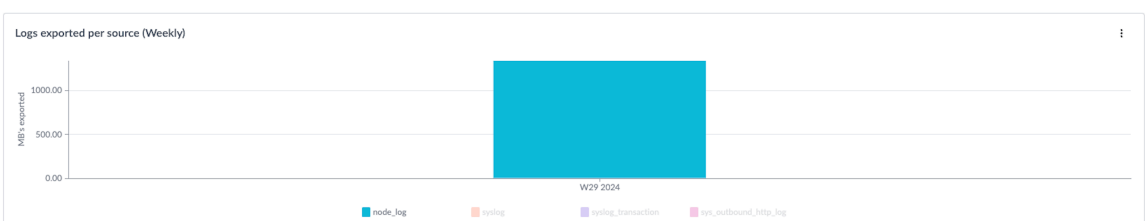


Quotidien :



Les données de ce rapport reflètent la collecte effectuée 4 heures auparavant.

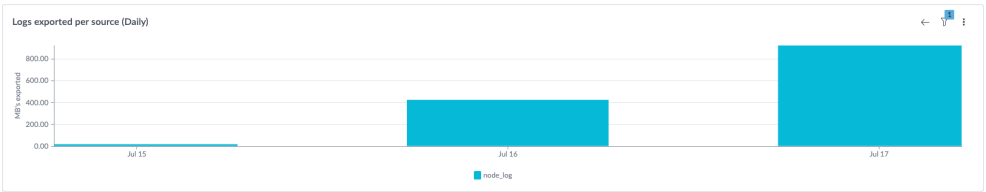
   - Journaux exportés par source (hebdomadaire) : ce widget indique le type de journaux exportés sur une base hebdomadaire. Vous pouvez également descendre dans la hiérarchie pour voir les données du journal quotidien. Vous pouvez afficher les données des 32 derniers jours.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez sélectionner ou désélectionner la source à partir de laquelle vous souhaitez afficher les données. Les sources à partir desquelles vous pouvez afficher les journaux sont : node_log, syslog, syslog_transaction et sys_outbound_http_log.

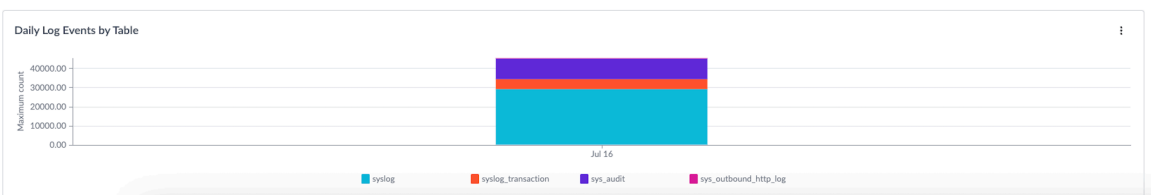


- Journal exporté par source (dernières 24 heures) : affiche les données des dernières 24 heures. Le graphique progresse chronologiquement de gauche à droite sur une échelle de 24 heures, les données les plus anciennes (24e heure) étant positionnées à droite et les données les plus récentes à gauche du rapport. Vous pouvez sélectionner ou désélectionner la source à partir de laquelle vous souhaitez afficher les données. Les sources à partir desquelles vous pouvez afficher les journaux sont : node_log, syslog, syslog_transaction et sys_outbound_http_log.



Remarque :
Selon l'heure de la journée à laquelle vous vérifiez ces données, le widget se met à jour dynamiquement pour refléter exactement les dernières 24 heures.

- Événements de journal quotidien par table : affiche les événements de journal générés par chaque table de journal par jour. Vous pouvez sélectionner ou désélectionner les tables dont vous souhaitez afficher les données.



Remarque :
Les tables à partir desquelles vous pouvez afficher les événements de journal sont : syslog, syslog_transaction, sys_audit et sys_outbound_http_log.

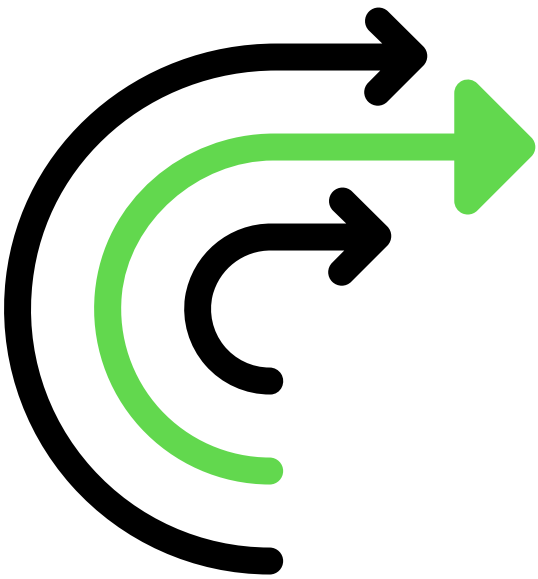
Journaux

Le module Journaux fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Traduction automatique

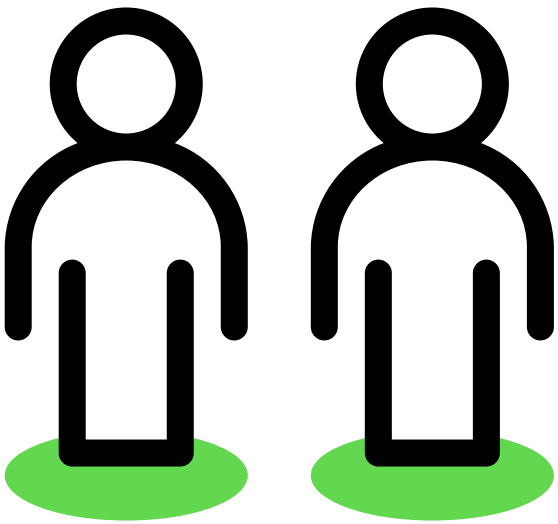
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journaux Système



Le module Journaux système fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Journalisation, audit et erreurs



Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et y réagir en temps opportun.

Traduction automatique

Journaux système

Le module Journaux système fournit une variété de journaux que vous pouvez utiliser pour résoudre et déboguer les transactions et les événements qui se produisent au sein de l'instance.

Accédez aux journaux suivants à partir du module Journaux système :

Journal	Description
Transactions	Toute l'activité de l'application pour une instance.
E-mail et push	Toutes les notifications par e-mail et tous les messages push envoyées à partir de toutes les instances du système.
Journaux des événements	Tous les événements système qui se produisent dans le système.
Importer	Activité d'importation de données au sein de la plateforme.
Changements de tables	Changements apportés à toutes les tables du système.
Connexion aux services Web sortants	Toutes les demandes de services Web sortantes, telles que les demandes REST et SOAP.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journal	Description
Images de signatures	Signatures électroniques pour le pavé de signature RH.
Système	Avertissements et erreurs pour les processus d'instance, les enregistrements et les événements non critiques, tels que l'utilisation de la mémoire sur le serveur.

Utilisez l'Explorateur de fichiers journaux pour rechercher et télécharger des journaux. Vous pouvez également rechercher des journaux archivés dans l'historique des journaux.

Autres journaux

Votre instance propose d'autres journaux en plus de ceux du module Journaux système. Par exemple, le Module de diagnostic du système fournit un historique des mises à niveau et des journaux de requêtes lentes, que vous pouvez utiliser pour mieux comprendre comment les requêtes affectent les performances de la plateforme. Enregistre Table Mises à jour du client chaque modification apportée au système.

Journal système

Affichez les avertissements et les erreurs pour les processus d'instance, les enregistrements et les événements non critiques, tels que l'utilisation de la mémoire sur le serveur.

Les informations suivantes sont suivies dans le journal système :

- Workflows
- Configuration
- Sessions de messageries instantanées
- Transactions pour chaque affichage de chaque page du système, y compris les temps de chargement pour le réseau, le serveur et le navigateur
- E-mail entrant et sortant
- Événements déclenchés dans le système
- Importations et intégrations
- Avertissements système, erreurs et journaux de script
- Informations sur la mise à niveau pour les activations de modules d'extension, les ensembles de mises à jour ou les mises à niveau système

Les entrées de journal s'affichent uniquement pour le jour en cours. Pour afficher d'autres fichiers journaux, utilisez l'explorateur de fichiers journaux. Ce journal fournit les informations suivantes pour toutes les occurrences :

Journal système

Champ	Description
Créé	Date et heure de l'activité de journalisation pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Niveau	Type de message. Les niveaux sont les suivants : Débogage, Erreur, Avertissement et Information.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journal système (suite)

Champ	Description
	• Un avertissement correspond à une erreur qui a été traitée et récupérée. • Une erreur est quelque chose qui doit être corrigé.
Message	Message généré par le système concernant la nature de l'événement.
Source	Nom du processus ou de la zone touchée par l'événement. Par exemple, la source de l'occurrence peut être EMAIL ou Memory.
Source Package	Nom du package d'application associé à l'occurrence. Cliquez sur le nom pour afficher l'enregistrement de l'application de stockage [sys_store_app] pour ce package.

Journalisation du workflow

- Chaque activité exécutée, y compris :
  - Date et heure de début
  - Date et heure de fin
  - État, par exemple, Terminé, Annulé, Expiré ou Erreur
  - Résultat
  - Description du panne, en cas d'erreur
- Historique de transition, y compris :
  - Heure de transition
  - Activité transférée de
  - Activité passée à
  - Transition qui a été déclenchée
- Journal de workflow, y compris toutes les instructions de journal ajoutées au workflow

Informations de configuration

- Action effectuée, y compris l'insertion, la mise à jour et la suppression
- Catégorie de changement
- Commentaires enregistrés avec le changement
- Nom du changement
- Différence XML du changement
- Ensemble de mises à jour auquel le changement est associé
- Date et heure du changement
- Utilisateur qui a effectué le changement
- Table dans laquelle le changement a été effectué
- Nom de l'objet en cours de modification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Type d'objet en cours de modification
- Vue dans laquelle le changement a été apporté, pour les changements apportés aux formulaires ou aux listes

Journaux de transactions

Le journal des transactions enregistre toute l'activité du navigateur pour une instance. Pour faciliter le débogage des problèmes système, vous pouvez filtrer les journaux de transactions par périmètre de l'application, en limitant les transactions qui s'affichent aux seules transactions provenant de périmètres spécifiques.

Le journal des transactions fournit les renseignements suivants pour toutes les activités.

Champ	Description
Créé	Date et heure de l'action de l'application pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Type	Type de transaction enregistrée.
Créé par	Utilisateur qui a créé cette activité.
Application d'origine	Périmètre de l'application à partir duquel la transaction est créée. Global s'affiche si la transaction provient du périmètre global.
Délai de réponse	Délai de réponse aller-retour pour la demande d'application, en millisecondes.
Délai réseau	Temps de latence de la réponse réseau après l'envoi de la demande d'application, en millisecondes.
Longueur de sortie	Taille de la chaîne de sortie envoyée par l'instance à l'application, en octets.
Compte SQL	Nombre de commandes SQL Server exécutées pour cette activité.
Nombre de règles métier	Nombre de règles métier exécutées pour cette activité.
Heure de règle métier	Temps écoulé pour l'exécution des règles métier de cette activité.
URL	Application ou module connecté par l'application cliente.
ID système	Identificateur généré par le système de l'instance client effectuant la demande. Cet ID est utilisé pour les environnements de cluster dans lesquels plusieurs instances (nœuds) communiquent avec la base de données.
Adresse IP	Adresse IP du client effectuant la demande.
Compressé avec GZIP	Indique si une page Web compressée a été demandée par l'application.
Protocole	Protocole HTTP utilisé par l'application pour cette instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Minutages des transactions clientes

Le module d'extension Client Transaction Timings améliore les journaux système en fournissant des informations supplémentaires sur la durée des transactions ayant lieu entre le client et le serveur.

Vous pouvez remonter jusqu'à la source des problèmes de performances en visualisant où le temps est consommé et comment le temps a été dépensé au cours d'une transaction.

Ce module d'extension nécessite l'activation de l'indicateur de temps de réponse et collecte des informations à partir des navigateurs suivants :

- Firefox
- Internet Explorer
- Chrome

Informations sur les transactions clientes

L'installation du module d'extension ajoute le module *Client Transactions* à l'application *Journaux système* . Il fournit une liste de toutes les transactions enregistrées entre le client et le serveur au cours du dernier jour :

Informations sur les transactions clientes

Champ	Description
Créé	Moment où la transaction a été enregistrée.
Temps de réponse	Nombre de ms dépensés par le serveur pour exécuter la transaction.
Temps de règle métier	Nombre de ms passés par les règles métier déclenchées par la transaction.
Temps SQL	Nombre de ms passés par la base de données SQL.
Temps de réponse client	(Load_completion_time) - (start_time). Il inclut le temps du serveur.
Délai réseau du client	Nombre de ms passées par le réseau par lequel le client se connecte.
Temps navigateur	Nombre de ms passés par le navigateur au cours de la transaction.
Heure du script client	Nombre de ms passés à exécuter des scripts clients.
Heure de politique d'interface utilisateur	Nombre de ms passés à exécuter la politique d'interface utilisateur.
Type	Type de transaction : • Formulaire • Liste • Autre
Table	Nom de la table apparue. Par exemple, incident, change_request.
Vue	Vue de ce formulaire/liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations détaillées sur le client

Une répartition plus détaillée des durées client pour tout le rendu de formulaire (mais pas le rendu de liste) est également suivie. Pour en afficher les détails, explorez un enregistrement de transaction client particulier et observez la liste connexe en bas de l'écran.

Informations détaillées sur le client

Champ	Description
Ordre	Ordre pendant la charge dans laquelle cette opération s'est produite.
Type	Type d'opération.
Nom	Nom descriptif de cette opération particulière
Durée	Nombre de ms nécessaires à cette opération.

Journaux push

Consultez le journal push pour suivre l'état des notifications push qui sont mises en file d'attente pour être envoyées à partir de votre système.

Pour afficher le journal push, accédez à **Journaux Système** > **Notifications push**. Les utilisateurs doivent avoir le rôle push_admin ou administrateur pour afficher le journal push.

Champs du journal push

Champ	Description
Réclamation	Numéro d'identification généré par la tâche planifiée qui envoie la notification push. Ce numéro est appliqué au champ **Réclamation** pour assurer la cohérence entre plusieurs travaux planifiés push.
Charge utile	Contenu de la notification push.
Nombre de files d'attente	Nombre de fois où le système a essayé d'envoyer la notification push. L'état de la notification push dépend de son nombre de files d'attente. • Si le nombre de files d'attente est de 0 pendant plus longtemps que prévu, aucune tâche planifiée n'essaie d'envoyer la notification push. • Si le nombre de files d'attente est supérieur à 0 et que le **type** est **réussi**, vous pouvez en déduire qu'il s'agit du nombre de fois où le système a essayé d'envoyer la notification push avant l'envoi final. • Si le nombre de files d'attente atteint 10, le système arrête d'essayer d'envoyer la notification push. Le **type** bascule sur **échec**.
ID de demande	Numéro d'identification unique de la notification push. À l'instar de l'ID de message d'un e-mail, l'ID de demande est utilisé comme jeton de corrélation pour la notification push.
Type	État indiquant si la notification push a été envoyée. La colonne Type peut comporter les valeurs suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs du journal push (suite)

Champ	Description
	• **échec** : le message n'a pas pu être envoyé. • **en attente** : le message est mis en file d'attente pour traitement. • **réussite** : le message a été envoyé avec succès, bien qu'il ne soit pas nécessairement reçu par l'appareil mobile.

Information associée

Travaux planifiés

Journal d'e-mails système et boîtes aux lettres

Le journal d'e-mail système enregistre tous les e-mails que l'instance crée ou reçoit. Les boîtes aux lettres système sont des vues filtrées de ce journal.

Chaque e-mail de notification que l'instance crée ou reçoit est enregistré dans un enregistrement d'e-mail [sys_email]. Vous pouvez accéder à un journal de ces enregistrements à l'adresse **Journaux Système** > **E-mails**.

Les boîtes aux lettres système sont des vues filtrées de la table E-mails [sys_email]. L'instance affecte un enregistrement d'e-mail à une boîte aux lettres système en fonction des valeurs des champs **Type** et **État** . Pour plus d'informations, consultez Boîtes aux lettres système .

Les champs suivants peuvent être inclus dans la mise en page du journal système et de n'importe quelle boîte aux lettres système :

Journal d'e-mail

Champ	Description
Boîte de réception	La boîte de réception système qui répertorie cet enregistrement d'e-mail. L'instance définit la valeur de ce champ en fonction des valeurs des champs **Type** et **État** .
État	L'état actuel de l'e-mail (Erreur, Ignoré, Traité ou Prêt).
Type reçu	Type d'e-mail entrant (Aucun, Transfert, Nouveau ou Réponse).
Type	L'état de l'e-mail. Les choix possibles sont les suivants : • reçu : le serveur a reçu cet e-mail. • reçu : ignoré : le serveur a reçu cet e-mail, mais il a été ignoré par l'instance à des fins d'action sur e-mail entrant. En règle générale, ces e-mails sont soit des spams, soit des réponses automatiques. Voir le champ Chaîne d'erreur pour plus de détails. • envoyer - échec : le serveur a tenté d'envoyer l'e-mail et a échoué. Voir le champ Chaîne d'erreur pour plus de détails. • envoyer - ignoré : le serveur a ignoré l'envoi de cet e-mail. En règle générale, il s'agit d'un e-mail qui a été généré mais qui n'avait pas d'adresse e-mail de destinataire ou qui est un e-mail en double. Voir le champ Chaîne d'erreur pour plus de détails.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journal d'e-mail (suite)

Champ	Description
	• send - ready : l'e-mail est prêt à être envoyé, mais n'a pas été envoyé par le serveur de messagerie. En règle générale, un e-mail ne reste dans cet état que pendant une courte période. • send - translation - ready : l'e-mail est généré lors de la traduction de l'e-mail et envoyé. En règle générale, un e-mail ne reste dans cet état que pendant une courte période. • sent : l'e-mail a été envoyé par l'instance sans erreur ni problème.
Cible	ID de document Référence à l'enregistrement si l'e-mail est généré par une insertion, une mise à jour ou la suppression d'un enregistrement particulier.
Utilisateur	Nom de l'utilisateur, issu de l'enregistrement utilisateur, de l'instance à partir de laquelle la notification par e-mail a été envoyée. **Remarque :** Il s'agit d'un champ de chaîne.
Type de notification	Type de notification. Les choix possibles sont les suivants : • Aucun • SMS • SMTP
UID	ID unique de l'e-mail stocké sur le serveur.
Créé	Date et heure de l'activité d'e-mail pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Supprimé	Pour les e-mails entrants, indique si l'e-mail a été supprimé du serveur de messagerie.
Poids	Le poids de l'e-mail, qui détermine la priorité d'envoi par rapport à d'autres notifications de la même table.
Importance	Indique que l'e-mail a été envoyé avec un niveau d'importance modifié, tel que Urgent.
Événement et notification d'origine	Pour les e-mails générés par les notifications, liste incorporée qui stocke l'événement et la notification qui a créé l'e-mail.
Objet	L'objet de l'e-mail. Pour les notifications, vous créez le texte de l'objet dans **Notification système** > **E-mail** > **Notifications**.
Message d'erreur	Chaîne d'erreur capturée à partir du serveur de messagerie pour déterminer pourquoi l'e-mail n'a pas été envoyé. Cette opération n'est consignée que si l'envoi de l'e-mail a échoué.
Destinataires	Adresses e-mail des destinataires.
Corps	Le corps de l'e-mail, affiché dans le balisage HTML brut. Utilisez le lien connexe Afficher l'aperçu du corps HTML pour afficher le corps du texte tel que rendu HTML.
Type de contenu	Le type de contenu de l'e-mail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journal d'e-mail (suite)

Champ	Description
En-têtes	Tous les en-têtes incorporés dans l'e-mail.

Journaux des événements

Le journal des événements enregistre tous les événements système qui se produisent dans le Now Platformfichier .

Ce journal fournit les informations suivantes pour tous les événements qui se produisent :

Journal des événements

Champ	Description
Créé	Date et heure de l'événement pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Nom	Nom de l'événement tel que répertorié dans le registre des événements.
URI	Requête HTTP qui a généré l'événement.
Param1	Valeur spécifique à l'événement qui dépend de l'événement et du destinataire.
Parm2	Valeur spécifique à l'événement qui dépend de l'événement et du destinataire.
Table	Table de base de données sur laquelle vous avez agi pour cet événement.
Traité	Date et heure auxquelles le traitement de l'événement a commencé. Cette heure reflète les paramètres régionaux de l'ordinateur exécutant l'instance.
Délai de traitement	Temps nécessaire pour traiter cet événement, en millisecondes.
File d'attente	Nom de la file d'attente du processeur.

Journaux d'importation

Le journal d'importation affiche des informations au format détaillé sur toute activité d'importation de données au sein de la plateforme.

Pour une vue plus détaillée des jeux d'importation qui ont produit un journal particulier, consultez **Ensembles d'importations** > **Historique de transformation**.

Ce journal fournit les informations suivantes pour toutes les importations :

Journal d'importation

Champ	Description
Créé	Date et heure de l'importation pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Niveau	Type de message affiché. Pour les fichiers d'importation, le niveau est Information.
Message	Message généré par le système concernant l'état de l'importation.
Source	Nom de la source externe de l'importation, telle qu'une intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Module de diagnostic du système

L'application System Diagnostics fournit des journaux relatifs à la plateforme.

Ces journaux sont disponibles :

Historique des mises à niveau

Suit chaque mise à niveau vers une instance.

Requêtes lentes

Fournit un aperçu de la façon dont les requêtes affectent les performances de la plateforme. Reportez-vous à la section Utiliser un journal de requêtes lent .

Table Mises à jour du client

Les modifications apportées dans le système sont enregistrées dans la table Mises à jour du client [sys_update_xml] par ordre chronologique. Il y a quelques exceptions, comme indiqué ci-dessous.

Pour accéder à cette table, saisissez `sys_update_xml.list` dans le filtre de navigation. Pour plus d'informations sur les ensembles de mises à jour, consultez Jeux de mises à jour système .

Les informations suivantes sont stockées à propos de chaque mise à jour :

Table Mises à jour du client

Champ	Description
Nom	Nom qui identifie l'enregistrement mis à jour.
Créé	Date et heure de création de l'enregistrement de mise à jour du client.
Créés par	L'utilisateur qui a effectué le changement.
Type	Type de la mise à jour.
Mis à jour	Date et heure de mise à jour de l'enregistrement de mise à jour du client.
Mis à jour par	L'utilisateur qui a effectué la mise à jour.
Mises à jour	Nombre de mises à jour de l'enregistrement.
Nom cible	Nom de l'élément qui a été modifié.
Vue	La vue du formulaire qui a été modifiée s'il s'agissait d'un changement de mise en page du formulaire.
Charge utile	Le contenu XML de l'enregistrement après le changement.
Ensemble de mises à jour distant	Référence à cet ensemble de mises à jour si le changement a été effectué par un ensemble de mises à jour distant.
Ensemble de mises à jour local	L'ensemble de mises à jour auquel le changement est associé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Certains changements d'application ne sont pas représentés par les enregistrements de mise à jour du client (sys_update_xml) Exemples :

- Types de métadonnées où updateSynch = false
- Changements en cascade aux tables et aux champs, tels que les changements de nom d'affichage
- Références de métadonnées non résolues provenant d'autres applications (ce qui entraîne l'absence de « valeur d'affichage » sur l'élément)
- sys_id changements pour les fichiers de fusion
- Changements apportés au flux/aux actions de flux susceptibles de générer des sys_documentation
- ua_table_license_config enregistrements générés lors de la création de la table
- Tâches exécutées en arrière-plan, telles que le traitement du langage naturel
- Tickets où sys_update_xml est modifié ou supprimé manuellement

Pour en savoir plus, reportez-vous à la section Valider les changements .

Historique du journal

Le système utilise la rotation de table et l'extension de table pour archiver les journaux plus anciens.

Par défaut, le système utilise le calendrier suivant pour archiver les journaux communs :

Calendrier d'archivage des journaux commun

Table	Archiver le calendrier	Rotations	Type
Événement [ecc_event]	Tous les jours	7	Rotation
File d'attente [ecc_queue]	Tous les jours	7	Rotation
Événement [sysevent]	Tous les jours	7	Rotation
Journal [syslog]	Toutes les semaines	8	Rotation
Journal des transactions [syslog_transaction]	Toutes les semaines	8	Rotation
Courriel [sys_email]	Tous les 30 jours	8	Extension

Utiliser le navigateur de fichier journal

L'instance fournit le navigateur de fichiers journaux des utilitaires et le téléchargement des fichiers journaux.

Utiliser **Journaux Système** > **Utilités** > **Navigateur de fichier journal de nœud** pour afficher une entrée du journal système. Vous pouvez rechercher des fichiers journaux à l'aide des filtres suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Navigateur de fichier journal

Champ	Description
Heure de début	Date et heure de début de la plage que vous souhaitez rechercher, pour les paramètres régionaux de l'ordinateur exécutant l'instance.
ID de session	Chaîne hexadécimale générée par le système qui identifie la session qui a généré l'entrée de journal.
Heure de fin	Date et heure de fin de la plage que vous souhaitez rechercher, pour les paramètres régionaux de l'ordinateur exécutant l'instance.
Message	Description de l'occurrence générée par le système.
Niveau	Type de message affiché. Les niveaux sont les suivants : Débogage, Erreur, Avertissement et Information. Un avertissement correspond à une erreur qui a été traitée et récupérée. Une erreur est quelque chose qui doit être corrigé.
Nom de thread	Identificateur généré par le système du thread qui a créé le fichier journal.
Lignes max.	Nombre maximal d'enregistrements renvoyés pour un filtre particulier.

L'instance crée des archives compressées de journaux système tous les 2 jours et purge les archives de journaux tous les 21 jours.

Important :
Lorsqu'un nœud est mis hors service, les fichiers journaux du nœud sont immédiatement purgés, ce qui signifie qu'ils ne sont pas archivés avant 21 jours supplémentaires.

Vous pouvez télécharger des archives de fichiers journaux et les afficher avec **Journaux Système** > **Utilités** > **Téléchargement du fichier journal de nœud**. Sélectionnez une archive de journaux dans la liste, puis cliquez sur **Télécharger le journal** sous *Liens connexes* pour ouvrir ou enregistrer l'archive.

Remarque :
Les fichiers journaux ne sont disponibles que pour le nœud auquel vous êtes actuellement connecté. Pour afficher le nœud actuellement connecté, accédez à **Diagnostics du système** > **Statistiques**.

Utilisez le nouveau bouton **Afficher les enregistrements Syslog** sur les formulaires Transaction et Transaction active pour afficher toutes les entrées de journal système qui ont été générées lors de l'exécution de la transaction. Une transaction peut comporter n'importe quel nombre d'entrées syslog. Les multiples entrées syslog pour toutes les transactions rendent difficile la co-relation d'une transaction avec leurs entrées syslog respectives. L'action d'interface utilisateur **Afficher les enregistrements Syslog** permet de co-relier les transactions actives et terminées à leurs entrées syslog respectives en créant une URL pour interroger la table syslog. L'identification des entrées syslog correctes pour une transaction particulière permet de déboguer et de résoudre les problèmes de sécurité.

Sécurité de journalisation améliorée

Explorez le champ **Attribution** dans les lignes du journal du nœud pour identifier le script ou le composant qui a généré le message du journal. Les lignes de début de transaction incluent le nouveau champ permettant d'identifier le type de demande effectuée.

Réalisez ce qui suit à l'aide des nouvelles améliorations :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Retracer l'origine source de chacune des lignes du journal
- Si les informations sur l'auteur ne sont pas disponibles, affichez le nom de classe Java et une attribution.
- Au début de chaque ligne de transaction, il contient l'ID et le type de transaction

Utilisez l'ID de transaction de chaque ligne de journal pour comprendre les informations données à chaque ligne de journal. Une fois que vous avez identifié le type de transaction, vous obtenez les informations d'origine de chaque ligne de journal. Le type de transaction et les informations d'origine de chaque ligne de journal vous donnent les informations de source requises de chaque ligne de journal de nœud.

Remarque :
SYS_UI_MACRO et SERVICE_PORTAL_WIDGET types de script dans l'attribution ne sont pas signalés.

Types de transaction

Voici la liste des types de transaction :

- Liste
- Formulaire
- XMLHttp
- Rapport
- SOAP
- Exporter
- Planificateur
- Recherche de texte
- Autre
- REST
- JSON
- AMB
- Archive
- Lot REST
- Instance Scan

Propriétés système

Les propriétés système requises pour cette fonctionnalité sont les suivantes :

- Glide.log.append.attribution : cette propriété est activée par défaut. Cela active/désactive les informations d'attribution de chaque ligne de nœud
- Glide.db.log.append.classname.attribution : cette propriété est activée par défaut. Active / désactive la journalisation de l'attribution du nom de classe Java

Éviter la falsification des journaux

Configurez les règles de protection des tables de journal système pour limiter le champ de modification et de suppression des enregistrements de journal d'application. Les règles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

vous permettent de déterminer la journalisation des changements ou des tentatives de changements dans ces tables.

Si vous êtes un security_admin, activez le module d'extension Tables protégées (com.glide.protected_tables) qui permet à la plateforme de restreindre les opérations de mise à jour, d'insertion et de suppression sur les tables de journaux système suivantes :

- syslog
- syslog_transaction
- sys_outbound_http_log
- sysevent
- sys_audit
- sys_push_notification
- syslog_app_scope
- protected_table_configuration (configuration non modifiable)

Remarque :
Le module d'extension com.glide.protected_tables protège uniquement les tables du journal système mentionnées ci-dessus. Toute tentative de mise à jour, d'insertion ou de suppression d'un enregistrement enregistre un message dans la table protected_table_log.

Pour plus d'informations, reportez-vous à la section Installation et configuration du module d'extension de protection des journaux .

Vous pouvez spécifier l'un des niveaux de protection de journal suivants pour chacune des tables de journaux système.

- Bloquer et enregistrer la tentative : bloque toute modification et journalise la tentative
- Bloquer uniquement la tentative : bloque toute modification et n'enregistre pas la tentative
- Uniquement enregistrer la tentative : ne bloque pas la modification, mais journalise la tentative
- Ne pas bloquer ni enregistrer la tentative : ne bloque pas la modification et n'enregistre pas la tentative

La plateforme utilise les niveaux de protection des journaux spécifiés pour chacune des tables de journaux système pour bloquer et/ou journaliser toute tentative de modification d'un enregistrement après sa création initiale.

Remarque :
Si vous êtes un security_admin, vous avez la possibilité de remplacer les niveaux de protection du journal par défaut dans chacune des tables du journal système pour l'adapter aux personnalisations de votre instance.

En cas de tentatives de modification des tables de journal système, elles sont consignées dans la table protected_table_log.

Remarque :
Si le niveau de protection n'est pas spécifié pour une table, toute tentative de modification n'est pas consignée dans la table protected_table_log.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour désactiver les opérations du module d'extension sur les tables du panneau d'administration, définissez la propriété com.glide.security.protected_table.enabled sur false. Pour plus d'informations, consultez Créer une propriété de protection de journal .

Configuration du module d'extension de protection des journaux

Configurez les règles de protection pour chaque table et opération pour terminer la configuration du module d'extension de protection des journaux.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tout** > **Tables protégées** > **Protection de journal**.
   La page Panneau d'administration s'affiche.

   Remarque :
   À partir de la version Utah , le module d'extension Tables protégées est installé par défaut, mais désactivé.

2. Élevez votre rôle à security_admin afin de continuer à configurer le module d'extension.

   a. Sélectionnez **Administrateur système**.

   b. Sélectionnez **Élever le rôle**.
   Le modal Élever le rôle s'affiche.

   c. Sélectionnez l'option security_admin pour élever votre rôle, puis sélectionnez **Mettre à jour**.

3. Configurez les règles de protection pour chaque table et opération. Les règles de protection s'appliquent à la mise à jour, à l'insertion et à la suppression. Les niveaux de protection ne peuvent pas être changés pour certaines tables. Les tables syslog et syslog_app_scope ont des valeurs fixes pour les protections de mise à jour et de suppression. La table protected_table_configuration a des valeurs de protection fixes pour les trois opérations.

   Remarque :
   Pour la table sysevent, les protections d'insertion ne peuvent pas être définies pour bloquer.

   Si **l'option Appliquer aux tables enfants** était activée pour syslog dans la version précédente, les tables enfants sont ajoutées à la protection des journaux avec les mêmes règles de protection que syslog lors de la mise à niveau vers la version Utah . Cela ne se produit que pour syslog, pas pour d'autres tables.

4. Activez la fonctionnalité en sélectionnant le bouton à bascule **Activer la protection des journaux** .

   Remarque :
   Vous pouvez désactiver ce module d'extension uniquement en modifiant la propriété com.glide.security.protected_table.enabled dans la table sys_properties.

Créer une propriété de protection de journal

Créez une propriété de protection des journaux pour éviter le risque d'altération des journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Si la `com.glide.security.protected_table.enabled` propriété n'existe pas dans la liste Propriétés système, sélectionnez **Nouveau**.
   Le nouveau formulaire de propriétés système s'affiche.
2. Renseignez les champs du formulaire

Champs	Description
Nom	Nom de la propriété en tant que com.glide.security.protected_table.enabled
Application	Application qui possède la propriété.
Description	Description de la propriété
Choix	
Type	Type de valeur : vrai ou faux
Valeur	Valeur réelle de la propriété
Ignorer le cache	Option permettant d'ignorer le contenu du cache
Privé	Possibilité de privatiser la propriété ○ Rôles de lecture ○ Rôles d'écriture

3. Sélectionnez **Soumettre** pour créer la propriété.

Journalisation, audit et erreurs (renforcement de la sécurité de l'instance)

Appliquez une stratégie de journalisation et d'audit afin de pouvoir identifier les activités suspectes et y réagir en temps opportun.

Pour en savoir plus sur les éléments qui peuvent être consignés dans l'instance, reportez-vous à la section Journaux système. Assurez-vous qu'il existe un calendrier pour surveiller les événements système tels que les connexions et les échecs de connexion à l'aide de **Journaux Système** > **Événements**.

Désactivation des messages d'erreur SQL (renforcement de la sécurité de l'instance)

Utilisez la propriété pour désactiver le `glide.db.loguser` rendu des messages d'erreur SQL dans un navigateur.

En savoir plus

Attribut	Description
Nom de la propriété	glide.db.loguser

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurable dans le centre de sécurité de l'instance	Non
Objectif	Pour désactiver l'affichage des messages d'erreur SQL dans le navigateur.
Type	true|false
Valeur recommandée	faux
Impact fonctionnel	(Faible) Cette correction désactive l'affichage des messages d'erreur SQL. Il n'y a aucun impact sur les fonctionnalités.
Risque de sécurité	(Moyen) Aucune information SQL sensible pouvant aider un attaquant ne doit apparaître dans un message d'erreur sur une page Web.

Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

Gestion des secrets

Utilisez ServiceNow Gestion des secrets pour une gestion granulaire de l'accès à vos mots de passe en fonction des besoins de votre entreprise.

Explorer



Découvrez les principales fonctionnalités et la valeur commerciale de Gestion des secrets.

Analyser



En savoir plus sur le tableau de bord Gestion des secrets.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer



Planifiez vos configurations de base.

Traduction automatique

Exploration de la gestion des secrets

Utilisez ServiceNow Gestion des secrets pour une gestion granulaire de l'accès à vos mots de passe en fonction des besoins de votre entreprise.

Important :
Les administrateurs doivent avoir le rôle de voir les modules et enregistrements associés à la gestion des secrets. Pour en savoir plus sur le rôle de gestion des secrets, reportez-vous Rôles de gestion des secretsà .

Sélectionnez parmi les versions Core et Enterprise de Gestion des secrets

Choisissez entre Gestion des secrets Core et Gestion des secrets d'entreprise en fonction des besoins de votre entreprise.

Gestion des secrets Core	Gestion des secrets d'entreprise
Vous pouvez activer Secrets Management Core sur votre instance sans frais supplémentaires. Le module d'extension offre la possibilité d'utiliser des groupes secrets avec des critères dans des tables non personnalisées fournies dans la plateforme qui ont été créées par ServiceNow les ServiceNow équipes d'ingénierie d'application.	Gestion des secrets Enterprise inclut des fonctions supplémentaires pour aider les administrateurs à créer et à gérer des groupes de secrets. Enterprise fournit les fonctionnalités suivantes en plus de celles répertoriées dans Core. • Utilisez des contrôles d'accès granulaires pour créer des groupes secrets en fonction de l'un de ces critères. ○ Périmètre ○ Table

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des secrets Core	Gestion des secrets d'entreprise
	◦ Colonne ◦ Enregistrement • Créez des secrets accessibles aux clients qui sont chiffrés à l'aide de votre propre clé qui ServiceNow ne peut pas accéder. • Utilisez le tableau de bord de gestion des secrets pour examiner les groupes de secrets configurés sur votre instance et en savoir plus sur les problèmes de sécurité potentiels. **Remarque :** Secrets Management Enterprise est un module d'extension payant que ServiceNow le personnel doit activer sur votre instance de production.

Utiliser des groupes secrets pour organiser vos secrets

Utilisez Gestion des secrets pour organiser vos secrets en groupes, puis appliquez des politiques d'accès à ces secrets au niveau du groupe.

Groupe secret de base

Ces groupes s'appliquent à tous les secrets d'un périmètre. Ces secrets sont déchiffrés par un module cryptographique commun et des politiques d'accès au module.

Groupe secret avec critères

Les groupes secrets avec critères fonctionnent de la même manière qu'un groupe secret de base, mais affinent davantage ce qui est inclus à l'aide de critères. Ces critères sont les suivants :

- Périmètre de l'application
- Package
- Table
- Colonne secrète
- Filtrer l'enregistrement

Les groupes secrets de l'un ou l'autre type peuvent être rendus accessibles à l'instance ou au client.

Groupes secrets côté instance

Les groupes secrets côté instance contiennent des secrets qui peuvent être déchiffrés par votre instance.

Groupes secrets côté client

Les groupes de secrets côté client utilisent une paire de clés publiques et privées pour garantir que les secrets ne peuvent être déchiffrés que par le client. Lorsque vous créez un groupe de secrets accessibles au client, vous chargez la clé publique dans l'instance et conservez la clé privée sur votre serveur MID. L'instance utilise la clé publique pour chiffrer vos secrets, mais ils ne peuvent être déchiffrés qu'à l'aide de la clé privée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour en savoir plus sur ces types de groupes, reportez-vous à Comprendre le côté client Gestion des secrets.

Utiliser des groupes secrets pour un contrôle plus granulaire

Bien que password2 soit disponible sur la ServiceNow plate-forme, Secrets Management fournit ces fonctionnalités supplémentaires.

Contrôles d'accès granulaires	**Password2** Avec password2, les administrateurs peuvent contrôler l'accès à un périmètre d'application, mais ne peuvent pas restreindre l'accès aux éléments du périmètre. **Gestion des secrets** Avec Gestion des secrets, les administrateurs peuvent restreindre l'accès en fonction des critères qu'ils définissent. Les types de critères peuvent être basés sur des critères tels que le package, la table ou la colonne.
Stockage sécurisé	Pour les groupes secrets côté client, la gestion des secrets utilise un nouveau schéma de chiffrement. Dans ce schéma de chiffrement, ServiceNow n'enregistre pas la clé de chiffrement. Pour cette raison, la sécurité de vos données ne dépend pas de ServiceNow la sécurité.

Appliquer des politiques d'accès au module à vos groupes

Une fois que vous avez regroupé vos secrets dans un groupe secret, vous pouvez appliquer des politiques qui déterminent comment vous pouvez accéder à ces secrets au niveau d'un groupe. Les politiques d'accès aux modules sont les mécanismes de contrôle d'accès que vous appliquez aux modules cryptographiques pour définir des contrôles au niveau de l'instance, tels qu'un délai de validité pour la clé cryptographique. Pour plus d'informations sur les politiques d'accès au module, consultez Vue d'ensemble de la politique d'accès au module.

Tables installées avec Gestion des secrets

Gestion des secrets ajoute ou modifie ces tables.

Nouvelles tables	
[sn_sm_secret_group]	Stocke des groupes secrets
[sn_sm_secret_group_criteria]	Stocke des groupes secrets de critères
[sn_sm_secret]	Stocke les secrets enveloppés
[sn_sm_identity_group]	Définit le groupe d'identités pour le mappage d'un groupe d'identités à la clé publique
[sys_kmf_wrapped_module_key]	Stocke les clés cryptographiques symétriques encapsulées
Tables modifiées	
[sys_kmf_crypto_module]	Ajout d'un type de module cryptographique. (Module cryptographique d'identité ou module cryptographique de groupe secret)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

[sys_kmf_module_key]	• Stocke la clé de chiffrement secrète conceptuelle (sans matériel de clé) • Stocke la clé publique d'identité
[sys_kmf_crypto_caller_policy]	Nouveau type de politique d'accès au module ajouté

Exemples de cas d'utilisation de la gestion des secrets

Garantissez la sécurité de la détection ITOM

Cette infographie présente une architecture de référence simplifiée sur la façon dont ServiceNow IT Operations Management (ITOM) Discovery peut être déployé par votre organisation. Comme le montre l'infographie, plusieurs serveurs Windows et Linux se connectent au MID Server et plusieurs agents MID Server activent le processus de détection pour mettre à jour la CMDB. Chaque transaction MID Server nécessite une authentification sécurisée, la gestion des informations d'identification d'authentification est donc essentielle du point de vue de la sécurité.

Accélérer la connectivité des workflows avec Integration Hub en toute sécurité

Utilisez ServiceNowle concentrateur d'intégration de pour vous connecter à différents systèmes à l'aide d'une interface de programmation d'application (API) automatisée. Chaque fois qu'Integration Hub se connecte à un système à l'aide d'une API, des informations d'identification d'authentification sont requises pour établir la connectivité. La gestion d'une multitude d'applications et d'API pour la connectivité nécessite une solution de gestion des secrets.

La gestion des secrets est un élément clé pour assurer la cybersécurité de votre organisation. Il couvre tous les processus et outils liés à la création, au stockage, à la transmission et à la gestion des informations d'identification numériques telles que les clés de chiffrement, les jetons API et les mots de passe. Pour gérer les secrets de manière sûre et efficace, vous pouvez élaborer une politique de gestion des secrets de base qui établit des règles et des procédures standard pour toutes les phases du cycle de vie d'un secret.

Comprendre le côté client Gestion des secrets

Découvrez comment gérer l'accès Gestion des secrets aux secrets et aux groupes.

Terminologie

La gestion des secrets côté client est conçue pour fournir une méthode de gestion des secrets sans l'utilisation de proxys et sans donner ServiceNow accès à vos données déchiffrées. Pour comprendre ce processus, commencez par utiliser les termes de chiffrement suivants.

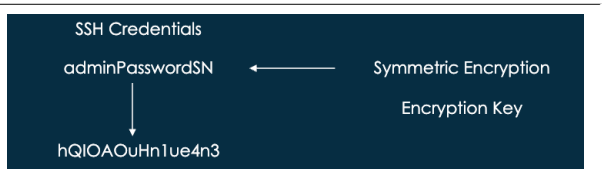
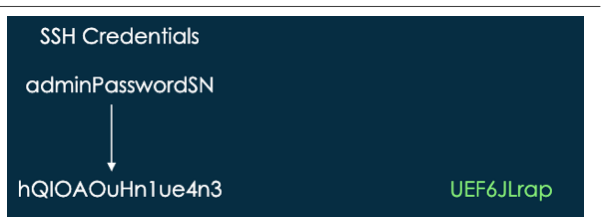
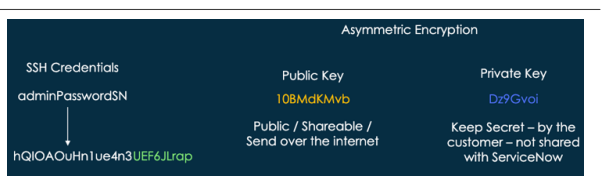
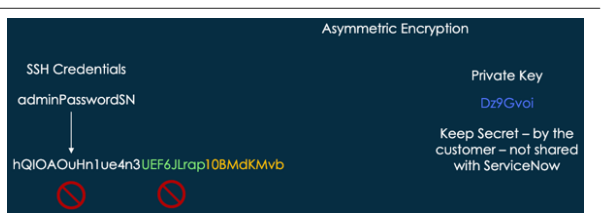
Terme	Description
Chiffrement symétrique	Le chiffrement symétrique utilise une seule clé identique pour chiffrer et déchiffrer les données. Si les données sont chiffrées avec une clé symétrique, cette clé est tout ce qui est nécessaire pour les déchiffrer.
Clé symétrique	La clé symétrique chiffre un secret, transformant votre mot de passe en texte clair en texte chiffré illisible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Terme	Description
Chiffrement asymétrique	Le chiffrement asymétrique utilise deux clés, l'une pour chiffrer et l'autre pour déchiffrer.
Clé publique	La clé publique est la moitié de la paire de clés asymétriques. Cette clé est stockée sur votre instance, qui utilise la clé pour chiffrer une clé symétrique. Cette clé symétrique chiffrée ne peut être déchiffrée que lorsqu'elle est associée à la clé privée.
Clé privée	La clé privée est la moitié de la paire de clés asymétrique. Cette clé est stockée dans un magasin de clés sur votre MID Server. ServiceNow n'a pas accès à cette clé. Associée à la clé publique, la paire de clés asymétrique permet de déchiffrer vos secrets.

Processus de chiffrement côté client

Une clé symétrique chiffre des informations d'identification (dans ce cas, un mot de passe administrateur), en les faisant passer d'un texte clair lisible à un texte chiffré chiffré.	
La clé symétrique (représentée en vert) peut être appliquée aux informations d'identification pour les chiffrer ou les déchiffrer.	
À ce stade, le chiffrement asymétrique commence à utiliser des clés publiques (jaunes) et privées (bleues).	
La clé publique chiffre les informations d'identification ainsi que la clé symétrique. La clé symétrique est maintenant protégée, elle ne peut donc pas être utilisée pour déchiffrer les informations d'identification. Bien que la clé publique puisse effectuer ce chiffrement, elle ne peut pas être utilisée seule pour le déchiffrer.	
Après avoir été chiffrée avec la clé publique, la clé privée est nécessaire pour déchiffrer les informations d'identification. Étant donné que seul le client possède cette clé, il est le seul à pouvoir accéder aux informations d'identification chiffrées.	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration des secrets accessibles aux clients

Découvrez comment configurer votre instance pour utiliser les secrets accessibles aux clients.

Utilisez cet exemple d'implémentation pour configurer Gestion des secrets sans utiliser de proxys ni donner ServiceNow accès à vos données déchiffrées.

Pour plus de détails sur l'utilisation côté Gestion des secrets client pour gérer l'accès aux mots de passe et aux groupes, reportez-vous à la section Comprendre le côté client Gestion des secrets.

Ces instructions supposent qu'un MID Server est configuré sur votre réseau local. Pour plus d'informations sur ce processus, reportez-vous à la section MID Server .

Vue d'ensemble du processus

1. **Créer des clés de chiffrement et un certificat**

   Créez des clés de chiffrement et un certificat à l'aide des commandes de terminal de votre environnement local.

2. **Ajouter votre certificat au magasin de clés de confiance ServiceNow**

   Chargez votre clé et votre certificat dans le magasin de ServiceNow clés approuvées.

3. **Créer un groupe secret avec des critères**

   Créez un groupe pour vos secrets. Groupes secrets pour organiser vos secrets en groupes. À l'aide de ces groupes, vous pouvez appliquer des politiques d'accès à ces secrets au niveau du groupe. Ensuite, associez votre groupe de secrets à un groupe d'identités, puis ajoutez votre MID Server à ce groupe d'identités.

4. **Charger la paire de clés publique/privée sur le serveur MID**

   Chargez votre paire de clés publique/privée sur votre MID Server. Cette paire de clés permet au MID Server de gérer les demandes d'authentification provenant de votre instance.

5. **Créer des informations d'identification et tester le chiffrement des informations d'identification**

   Créez des informations d'identification à authentifier dans un système tiers et testez qui ServiceNow ne peut pas accéder aux informations d'identification.

6. **Configurer Concepteur de flux pour gérer l'intégration**

   Sur votre instance, utilisez cette fonction Studio de workflow pour gérer une intégration entre votre réseau local et votre instance.

7. **Tester l'intégration des secrets chiffrés côté client de bout en bout**

   Testez votre intégration et examinez les détails de l'exécution pour confirmer que votre configuration fonctionne.

Créer des clés de chiffrement et un certificat

Créez des clés de chiffrement et un certificat à l'aide des commandes de terminal de votre environnement local.

Avant de commencer

Rôle requis : aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans votre environnement local, ouvrez Terminal (sous Mac ou Linux) ou Ligne de commande (sous Windows).
2. À l'aide du terminal, utilisez `cd` pour vous déplacer dans le dossier où vous souhaitez stocker vos clés de chiffrement.
3. À l'aide du terminal, saisissez les éléments suivants :

```
openssl req -newkey rsa:4096 -nodes -keyout sm_private_key.pem -x509 -days 365 -out
 sm_public_cert.pem
```

Remarque :
Cet exemple utilise OpenSSL pour générer des clés et des certificats. Vous pouvez remplacer d'autres outils comparables en fonction de vos besoins.

La commande génère une clé privée et un certificat public (avec la clé publique correspondante). Une série d'invites pour les informations requises suit, en commençant par « Nom du pays ».

4. Remplissez les invites avec les informations demandées.
Les invites suivantes s'affichent.
   - Nom du pays
   - Nom de l'état de la province
   - Nom de la localité (p. ex., ville)
   - Nom de l'organisation (p. ex., société)
   - Nom de l'unité organisationnelle (p. ex., section)
   - Nom commun (p. ex., nom d'hôte complet)
   - Adresse e-mail

Collaborez avec votre équipe de sécurité pour vous assurer que vous saisissez les informations de certificat correctes.

```
Country Name (2 letter code) []:US
State or Province Name (full name) []:CO
Locality Name (eg, city) []:Boulder
Organization Name (eg, company) []:ServiceNow
Organizational Unit Name (eg, section) []:Product Management
Common Name (eg, fully qualified host name) []:fake@servicenow.com
Email Address []:fake@servicenow.com
```

5. Vérifiez le dossier que vous avez choisi à l'étape 2 pour vérifier que la clé privée et le certificat public ont été créés.
Si vous avez utilisé les mêmes noms de fichiers que dans l'exemple de l'étape 3, vous devriez voir les fichiers suivants :
   - sm_private_key.pem
   - sm_public_cert.pem
6. Dans le même dossier, utilisez la commande suivante :

Important :
La commande spécifique à utiliser dépend de votre système d'exploitation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour Linux :	`cat sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`
Pour Windows :	`sm_private_key.pem sm_public_cert.pem > sm_keypair_bundle.pem`

Cette commande regroupe la clé privée et le certificat public dans un seul fichier à charger ultérieurement dans votre serveur MID.

7. Vérifiez à nouveau le dossier pour vérifier que le nouveau fichier contenant votre clé privée (sm_keypair_bundle.pem) et votre certificat public a été créé.

Ajouter votre certificat au magasin de clés de confiance ServiceNow

Chargez votre clé et votre certificat dans le magasin de ServiceNow clés approuvées.

Avant de commencer

Rôle requis : aucun

Le certificat public que vous avez créé dans cet exemple est considéré comme un certificat « autosigné » (ce qui signifie qu'il ne provient pas d'une autorité racine de confiance). Vous devez ajouter le certificat au magasin de ServiceNow clés de confiance pour pouvoir l'utiliser. Lorsque vous utilisez un certificat provenant d'une autorité de certification, vous n'avez pas besoin d'effectuer cette étape.

Procédure

1. Dans votre environnement local, ouvrez Terminal (sous Mac ou Linux) ou Ligne de commande (sous Windows).
2. À l'aide du terminal, utilisez `cd` pour accéder au dossier dans lequel vous avez créé vos clés de chiffrement.
3. Dans le terminal, entrez la commande suivante :

   ```
   cat sm_public_cert.pem
   ```

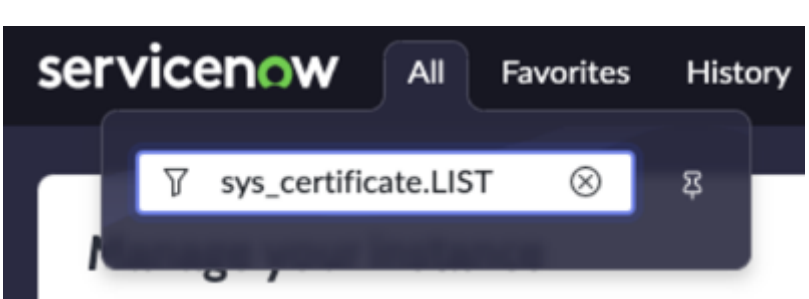
   Vous devez afficher le contenu de votre certificat public pour le copier dans le magasin de clés approuvé. Cette commande `cat` affiche le certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Copiez les informations du certificat dans votre presse-papiers.
   Commencez par et incluez la ligne `-----BEGIN CERTIFICATE -----` et terminez par et incluez la ligne `----- END CERTIFICATE -----`.
5. Sur votre ServiceNow instance, accédez à la liste des **certificats X.509** en saisissant `sys_certificate.LIST` dans le filtre de navigation.



6. Sélectionnez **Nouveau** pour créer un enregistrement **de certificat X.509** .
7. Renseignez les champs suivants du formulaire.

Champs du certificat X.509

Champ	Valeur
Nom	Nom du certificat. Ce nom peut être n'importe quel nom que vous choisissez.
Format	Sélectionner **PEM**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
	Remarque : Les fichiers PEM (Privacy Enhanced Mail) sont un type de fichier PKI (Public Key Infrastructure) utilisé pour les clés et les certificats. Les enregistrements que vous avez créés au cours des étapes précédentes sont de ce type de fichier.
Type	**Sélectionner le certificat du magasin de confiance**
Description brève	Description du certificat. Entrez une valeur qui vous permet de savoir à quoi sert ce certificat.
Certificat PEM	Collez les informations de certificat que vous avez copiées à l'étape 4.

8. Sélectionnez **Soumettre** pour enregistrer l'enregistrement.

Créer un groupe secret avec des critères

Créez un groupe pour vos secrets. Groupes secrets pour organiser vos secrets en groupes et vous permettre d'appliquer des politiques d'accès à ces secrets au niveau du groupe. Ensuite, associez votre groupe de secrets à un groupe d'identités, puis ajoutez votre serveur MID à ce groupe d'identités.

Avant de commencer

Rôle requis : admin, KMF_admin, sn_secrets.secret_manager et sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tout** > **Gestion des secrets** > **Groupes secrets avec critères**.
2. Sélectionnez **Nouveau** pour créer un **groupe secret avec enregistrement de critères** .
3. Renseignez les champs suivants du formulaire.

Groupe secret avec champs de critères

Champ	Valeur
Nom de groupe	Nom du groupe secret. Ce nom peut être n'importe quel nom que vous choisissez.
Type de secret	Sélectionnez **Client accessible**
Module de génération automatique	Cocher la case
Description brève	Description du groupe secret. Entrez une valeur qui indique l'utilisation de ce groupe.
Type de critère	**Sélectionner une table cible**
Table cible	**Sélectionner les informations d'identification SSH [ssh_credentials]**

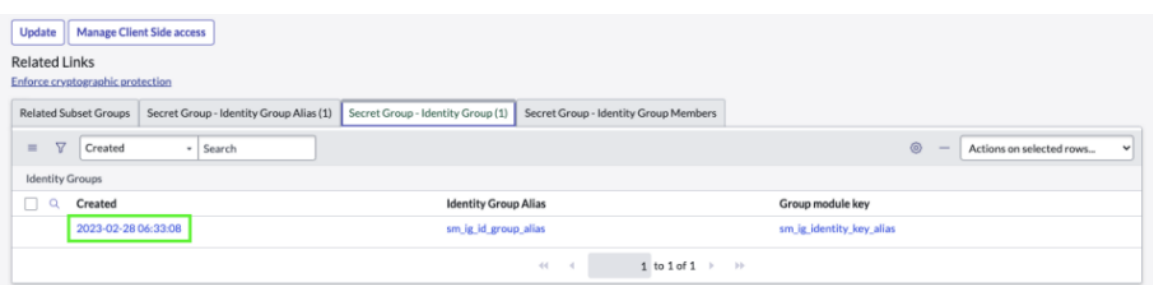
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) l'en-tête du formulaire et sélectionnez **Enregistrer** dans le menu contextuel pour enregistrer l'enregistrement.
5. Assurez-vous que la case **Actif** n'est pas cochée.
6. Sélectionnez le bouton **Gérer l'accès côté client** pour créer un groupe d'identités.
   Une fenêtre **d'alias de groupe d'identités** s'affiche.
7. Sélectionnez le bouton **Nouveau** .
8. Sélectionnez l'icône de référence ( ) en regard du champ **Alias du groupe d'identités** .
9. Dans le champ **Nom de l'alias du groupe** , saisissez une valeur.
   Ce nom peut être n'importe quelle valeur que vous voulez.
10. Si vous avez choisi un nom unique à l'étape 9, sélectionnez **Soumettre**.
11. Sélectionnez le bouton **Télécharger la clé d'identité** .
    La fenêtre **Importer le certificat de clé publique d'identité** s'affiche.
12. Dans le champ **Alias de clé d'identité** , saisissez une valeur.

> **Important :**
> Cette valeur peut être n'importe quelle valeur que vous voulez, mais elle doit correspondre exactement à ce que vous insérez dans le serveur MID dans les étapes ultérieures.

13. **Sélectionner Importer**
    La fenêtre **Pièce jointe** s'affiche.
14. Sélectionnez **Choisir un fichier**.
15. Sélectionnez le certificat public que vous avez créé lors des étapes précédentes.
    Ce certificat doit être le fichier `sm_public_cert.pem` .
16. Sélectionnez l'icône X pour fermer la fenêtre.
17. Sélectionnez **OK** pour fermer la fenêtre **Importer le certificat de clé publique d'identité** .
    Une bannière bleue **Les clés et les certificats sont importés avec succès dans la bannière de l'instance** , ce qui confirme la réussite de l'importation.
18. Sélectionnez **Soumettre**.
    La liste **Identity groups (Groupes d'identité**) s'affiche.
19. Cochez la case située à gauche de votre enregistrement de groupe d'identités dans la liste.
20. Sélectionnez le bouton **Associer un groupe secret** .
    Vous êtes renvoyé à votre **enregistrement Groupe secret avec critères** . Les listes **connexes « Groupe secret – Groupe d'identités – Grouped'identités » et « Groupe secret – Groupe d'identités »** sont visibles. Ces listes connexes affichent les enregistrements que vous avez créés lors des étapes précédentes.
21. Dans la liste connexe **Groupe secret – Groupe d'identités** , sélectionnez le champ **Créé** pour l'enregistrement de cette liste.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un enregistrement **de groupe d'identités** s'affiche.

22. Dans la liste connexe **Membres du groupe d'identités** , sélectionnez le bouton **Nouveau** .
Un enregistrement de **membre du groupe d'identités** s'affiche.
23. Dans le champ **Table Membre**, sélectionnez **Serveur MID [ecc_agent].**
24. Sélectionnez l'icône de référence ( ) en regard du champ d'enregistrement du **membre du groupe d'identités** , puis sélectionnez votre serveur MID.

> **Remarque :**
> Si vous cochez **la case Inclure tous les enregistrements** , tous les MID Server connectés à votre instance sont ajoutés au groupe d'identités.

25. Sélectionnez **OK** pour fermer la fenêtre **Sélectionner le document** .
26. Sélectionnez **Soumettre**.
27. Revenir à **Tout** > **Gestion des secrets** > **Groupes secrets avec critères**et ouvrez l'enregistrement que vous avez créé à l'étape 2.
28. Activez le champ **Actif** .
29. Sélectionnez **Mettre à jour** pour enregistrer l'enregistrement.

Charger la paire de clés publique/privée sur le serveur MID

Chargez votre paire de clés publique/privée sur votre serveur MID. Cette paire de clés permet au MID Server de gérer les demandes d'authentification provenant de votre instance.

Avant de commencer

Rôle requis : aucun

Étant donné qu'il ServiceNow n'a pas accès à la clé privée, il ne peut pas l'associer à la clé publique pour déchiffrer la clé symétrique, puis déchiffrer les informations d'identification. Si le serveur MID tente d'utiliser ces informations d'identification chiffrées, il ne peut pas déchiffrer les informations d'identification pour authentification sans accès à la clé privée.

Au cours de ces étapes, vous chargez la clé privée sur le serveur MID pour compléter le trousseau de clé publique/privée. Ce chargement accorde l'accès au serveur MID sans donner ServiceNow d'accès.

Pour accorder au serveur MID l'accès à la clé privée, vous devez créer une commande à exécuter en tant qu'administrateur dans Powershell. Dans cet exemple, la commande est destinée à l'ordinateur virtuel Windows Azure.

> **Important :**
> Assurez-vous que le système sur lequel vous effectuez ces étapes a accès à la fois au serveur MID et au fichier de paire de clés.

Procédure

1. Dans votre environnement local, localisez le dossier dans lequel vous avez créé votre paire de clés dans les Créer des clés de chiffrement et un certificat étapes.
2. Recherchez et copiez le chemin d'accès complet au fichier `manage-certificates.bat` .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Ce fichier se trouve dans votre dossier de Serveur MID. Selon l'endroit où vous avez stocké votre dossier de Serveur MID, votre chemin d'accès peut ressembler à cet exemple :

```
C:
\Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__
patch4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manag
e-certificates.bat
```

3. Créez un fichier texte et collez le chemin d'accès dans le fichier.
4. Dans le fichier texte, ajoutez ce qui suit après le chemin d'accès :
   `-un your_identity_key_alias`

   Remplacez `your_identity_key_alias` par le nom de l'alias de clé d'identité que vous avez créé lors du chargement de votre certificat public.
5. Recherchez et copiez le chemin d'accès complet à votre fichier de paire de clés.

Remarque :
Si vous avez utilisé les noms dans ces étapes, ce fichier est nommé `sm_keypair_bundle.pem`.

6. Dans votre fichier texte, ajoutez ce chemin à la fin de la ligne, en ajoutant un espace entre ce chemin et les informations précédentes.
   Le texte dans votre fichier texte doit ressembler à cet exemple :

```
C:
\Users\<your_user_account>\Documents\SM_Implementation\mid.utah-07-08-2022__patch
4b01-31-2023_02-07-2023_1702.windows.x86-64\sm_ig_MIDS\bin\scripts\manage-certificat
es.bat -a your_identity_key_alias
 C:\Users\<your_user_account>\Desktop\sm_keypair_bundle.pem
```

Remarque :
Dans cet exemple, le fichier `sm_keypair_bundle.pem` se trouve sur le bureau pour raccourcir le chemin d'accès.

7. Copiez l'intégralité du texte de votre fichier texte dans le presse-papiers.
8. Recherchez Powershell sur votre système et choisissez l'option **Exécuter en tant qu'administrateur** .
9. Collez le texte de votre fichier texte dans PowerShell, puis appuyez sur Entrée.
   En cas de réussite, le message suivant s'affiche :

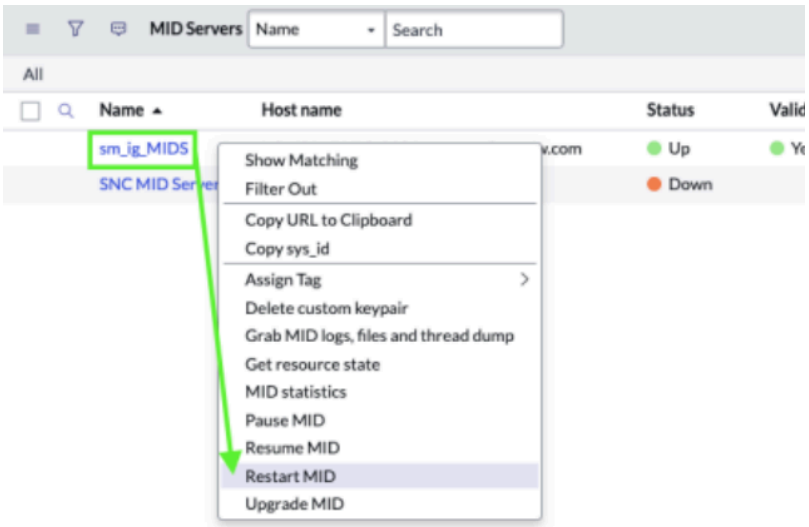
```
Installed certificate with alias: <your_identity_key_alias> into the MID keystore.
```

Conseil :
Si vous ne voyez pas ce message, assurez-vous que votre commande ne comporte pas d'erreurs, d'espaces ou de guillemets inutiles. Assurez-vous que le chemin d'accès complet est saisi correctement.

10. Redémarrez votre serveur MID en accédant à votre enregistrement de serveur MID, en cliquant avec le bouton droit de la souris sur l'enregistrement et en sélectionnant **Redémarrer MID.**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le redémarrage du serveur MID synchronise la paire de clés chargée dans le magasin de clés MID en vue de son utilisation avec les opérations. Attendez que le serveur MID redémarre avec l'état **Actif** et la valeur validée **Oui avant** de continuer.

Créer des informations d'identification et tester le chiffrement des informations d'identification

Créez des informations d'identification pour vous authentifier dans un système tiers.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la liste **des informations d'identification SSH** en saisissant `ssh_credentials.list` dans le filtre de navigation.
2. Sélectionnez **Nouveau** pour créer un enregistrement **d'informations d'identification SSH** .
3. Renseignez les champs suivants du formulaire.

Formulaire d'informations d'identification SSH

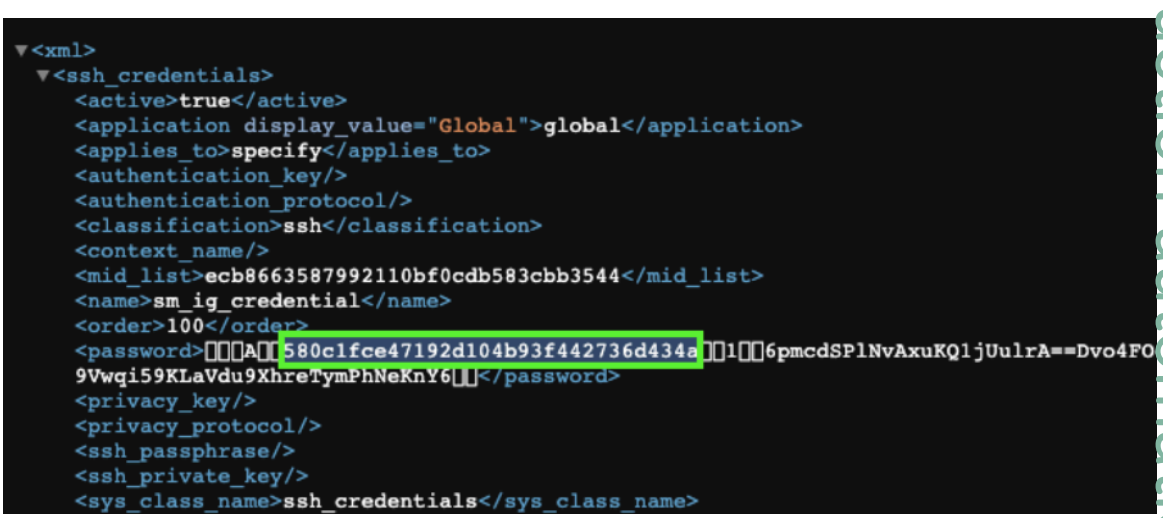
Champ	Valeur
Nom	Entrez un nom pour votre enregistrement d'informations d'identification. Ce nom peut être n'importe quelle valeur que vous voulez.
Concerne	**Sélectionner des serveurs MID spécifiques**
Serveurs MID	Sélectionnez votre Serveur MID.
Nom d'utilisateur	Entrez le nom d'utilisateur.
Mot de passe	Saisissez le mot de passe associé à l'utilisateur dans le champ **Nom d'utilisateur** .

4. Sélectionnez l'icône de verrouillage ( ) en regard du champ **Alias d'informations d'identification** .

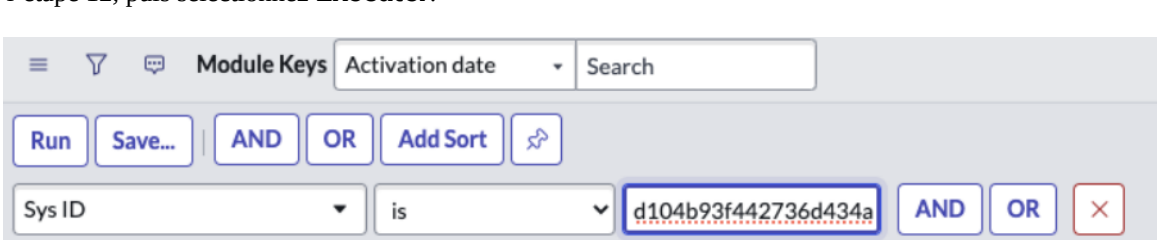
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez l'icône de référence ( ) pour ouvrir la liste **des alias de connexion et d'informations d'identification** .
6. Sélectionnez **Nouveau** pour créer un enregistrement **d'alias de connexion et d'informations d'identification** .
7. Entrez un nom dans le champ **Nom** .
8. Sélectionnez **Informations d'identification** dans le champ **Type** .
9. Sélectionnez **Soumettre**.
   Vous êtes renvoyé à l'enregistrement **des informations d'identification SSH** . Dans les étapes suivantes, vous testez que les informations d'identification sont chiffrées.
10. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) l'en-tête du formulaire et sélectionnez **Afficher le code XML**.
11. Recherchez la balise XML `<password>` dans le code XML.
12. Copiez le sys_id de cette balise `<mot de passe>` dans votre presse-papiers.
    Le sys_id est un code de 32 caractères représentant la clé symétrique utilisée pour chiffrer ces informations d'identification. Le mot de passe chiffré que vous avez saisi dans la table Informations d'identification SSH se trouve à droite des deux ensembles de cases sur cette même ligne.



13. Accédez à la liste **Clés du module** en saisissant `sys_kmf_module_key.list` dans le filtre de navigation.
14. Filtrez la liste des enregistrements dans lesquels le champ **ID** système correspond au sys_id que vous avez copié à l'étape 12, puis sélectionnez **Exécuter**.



   Votre recherche doit renvoyer un seul enregistrement **de clé de module** . Cet enregistrement vous indique que vous avez créé une clé symétrique et que vous l'utilisez.
15. Accédez à la liste des **clés de module encapsulées** en saisissant `sys_kmf_wrapped_module_key.list` dans le filtre de navigation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

16. Filtrez la liste des enregistrements dans lesquels le champ **Module de chiffrement** correspond au module de chiffrement que vous avez créé lors des étapes précédentes, puis sélectionnez **Exécuter**.
Votre recherche doit renvoyer un seul enregistrement **de clé de module encapsulé** . À partir de cette liste, vous pouvez vérifier les éléments suivants :
    - La colonne **Matériel de clé encapsulée** indique que la clé symétrique dans le module de chiffrement (qui est utilisée pour chiffrer les informations d'identification SSH) est chiffrée par la clé publique que vous avez chargée dans le groupe d'identités.
    - Le champ **ID système de clé encapsulée** indique que c'est la clé (la clé symétrique du module de chiffrement) qui est chiffrée par **l'ID système de la clé d'encapsulation** (la clé publique chargée dans le groupe d'identité).

    Si les champs précédents ne figurent pas dans votre liste par défaut, vous pouvez les ajouter à la liste en sélectionnant l'icône **Personnaliser la liste** ( ).

Remarque :
Votre instance exécute une tâche de nettoyage toutes les 10 minutes, ce qui supprime les clés orphelines et aide à empêcher la prolifération des clés non associées après la mise à jour de vos informations d'identification.

Configurer Concepteur de flux pour gérer l'intégration

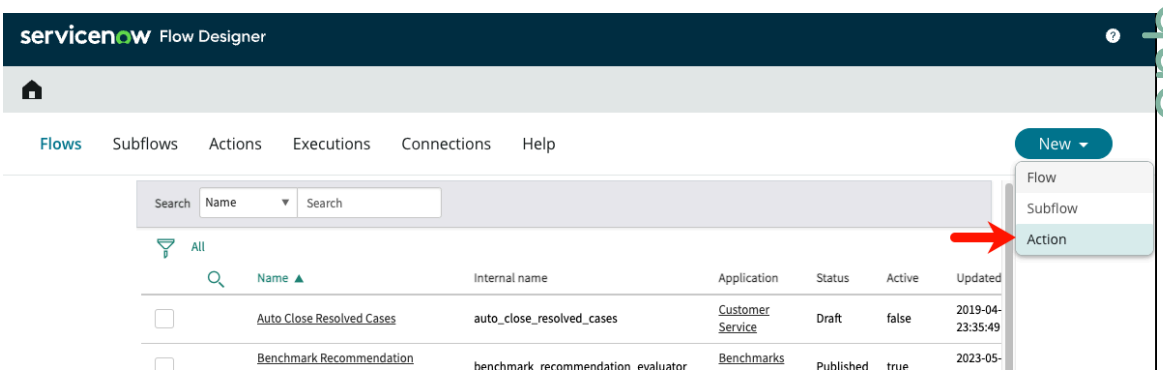
Sur votre instance, utilisez cette fonction Studio de workflow pour gérer une intégration entre votre réseau local et votre instance.

Avant de commencer
Rôle requis : administrateur

Au cours de ces étapes, vous allez créer un Studio de workflow flux de travail pour créer un fichier texte sur votre système local.

Procédure

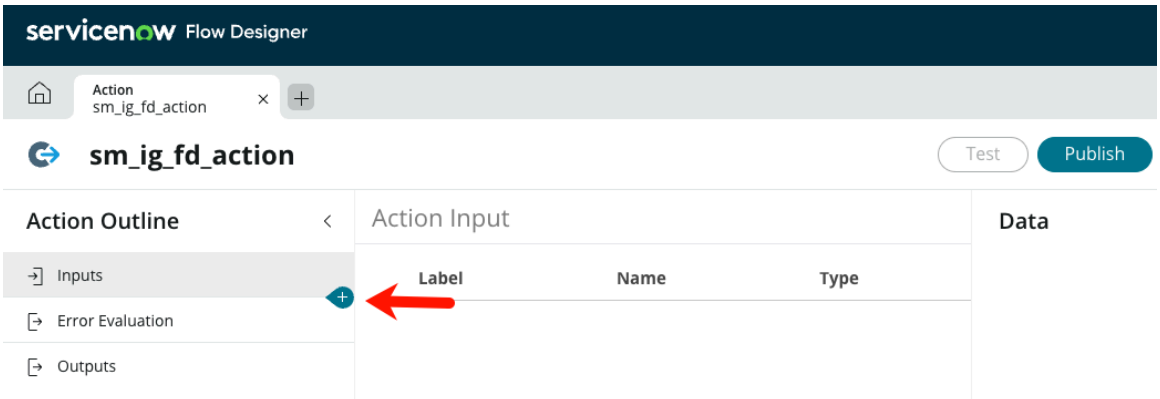
1. Sur votre instance, accédez à **Tout** > **Automatisation des processus** > **Concepteur de flux**.
2. Créez une action en ServiceNow sélectionnant **Nouveau** , puis **Action**.



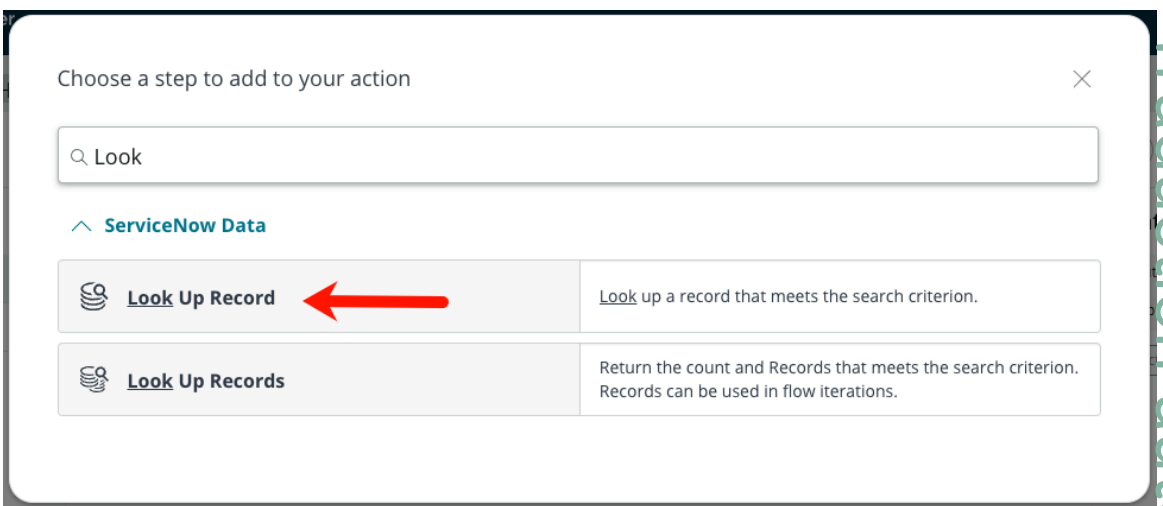
3. Entrez un nom dans le champ **Nom de l'action** , puis sélectionnez **Soumettre**.
4. Créez une étape en sélectionnant le signe plus entre **Entrées** et **Évaluation de l'erreur** dans le **plan d'action**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Dans la fenêtre **Choisir une étape à ajouter à votre action** , sélectionnez **Rechercher un enregistrement**.



6. Dans la section **Étape Rechercher un enregistrement** , sélectionnez **Serveur MID [ecc_agent]** dans le champ **Table** .
7. Créez une autre étape en sélectionnant le signe plus sous votre **étape Rechercher un enregistrement**.
8. Dans la fenêtre **Choisir une étape à ajouter à votre action** , sélectionnez **SSH**.

> **Remarque :**
> Si l'option **SSH** ne s'affiche pas, vous devez activer le module d'extension requis.

9. Dans la section **Étape SSH** , saisissez les informations suivantes :

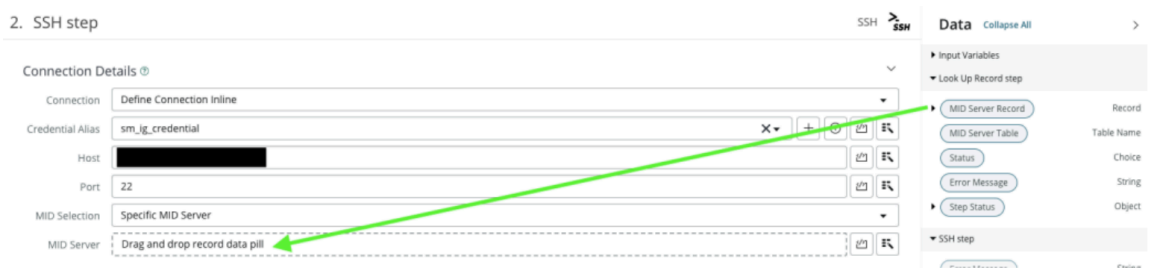
Champ	Valeur
Connexion	**Sélectionner Définir l'inline de la connexion**
Alias d'informations d'identification	Sélectionnez l'alias d'informations d'identification pour les informations d'identification SSH créées lors des étapes précédentes.
Hôte	Saisissez l'adresse IP de l'hôte auquel vous vous connectez via SSH.
Port	Entrez 22.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Sélection de MID	**Sélectionnez un Serveur MID spécifique**.

10. Pour remplir le champ de **Serveur MID** , faites glisser la pilule **d'enregistrement de Serveur MID** de la section **Données** vers le champ.



Avertissement :
Lorsque vous faites glisser la pilule dans le champ, sélectionnez la pilule et non la flèche noire à côté de la pastille.

11. Dans la section **Configuration SSH** , entrez la valeur suivante dans le champ **Commande** .

```
/bin/date > sm_ig_text_file.txt
```

Cette commande crée un fichier texte dans votre système local à l'aide des secrets déchiffrés du serveur MID. Le Serveur MID accorde l'accès à l'instance ServiceNow (via Studio de workflow) sans jamais donner à l'instance ServiceNow l'accès au secret déchiffré.

Conseil :
La commande `/bin/date` insère la date/heure actuelle dans le fichier texte créé. Cette commande démontre que l'intégration se produit en temps réel en fonction de la date/heure actuelle par rapport à la création du fichier texte.

12. Sélectionnez le bouton **Enregistrer** pour enregistrer le workflow.

Tester l'intégration des secrets chiffrés côté client de bout en bout

Testez votre intégration et examinez les détails de l'exécution pour confirmer que votre configuration fonctionne.

Avant de commencer

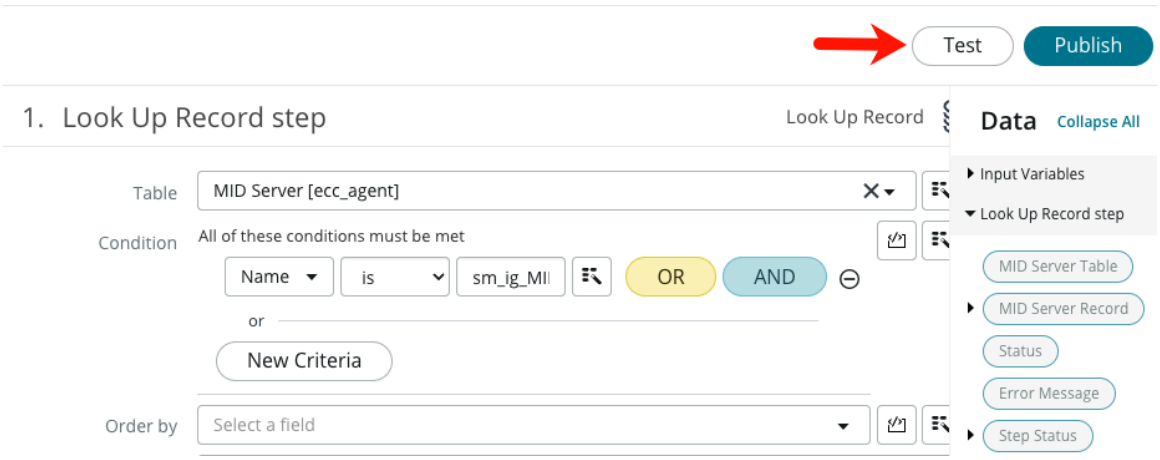
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans Studio de workflow Sélectionnez le bouton **Test** dans le coin supérieur droit de l'écran.



2. Dans la fenêtre **Action du test** , sélectionnez **Exécuter le test**.
3. Sélectionnez **L'exécution de votre test terminée. Affichez les détails d'exécution de l'action.**
4. Actualisez votre écran jusqu'à ce que vous **voyiez Exécution du test - Terminé** dans le coin supérieur droit de l'écran.
5. Sélectionnez la flèche **Étapes** en bas à gauche de l'écran.
6. Faites défiler vers le bas jusqu'à ce que vous voyiez un en-tête **Données de sortie d'étape** avec le message de réussite suivant :

```
{"Step Status";{"code";0,"message";"Success"}}
```

7. Après avoir vu ce message dans Studio de workflow, vérifiez que votre fichier texte a été créé dans votre système local.

Tester des informations d'identification Windows Management Instrumentation chiffrées avec Gestion des secrets

Vérifiez que vos informations d'identification WMI (Windows Management Instrumentation) sont chiffrées avec Gestion des secrets et utilisez un workflow IntegrationHub pour effectuer les tests de bout en bout.

Avant de commencer

Rôle requis : administrateur

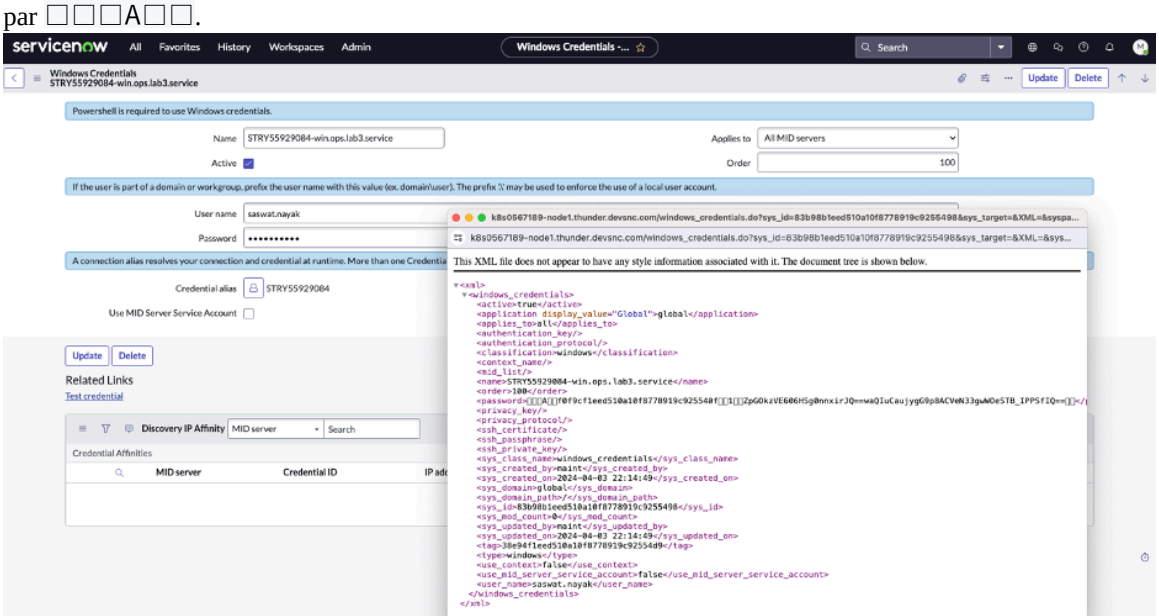
- IntegrationHub Enterprise doit être actif sur votre instance. Pour plus de détails, voir Request an Integration Hub plugin .
- Vous devez disposer d'un groupe de secrets configuré sur votre instance. Reportez-vous aux étapes 1 à 3 indiquées dans la section Configuration des secrets accessibles aux clients.
- Vous devez avoir des informations d'identification configurées chiffrées avec Gestion des secrets. Reportez-vous aux étapes 1 à 9 indiquées dans la section Créer des informations d'identification et tester le chiffrement des informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Confirmez que le Serveur MID souhaité est associé au groupe secret.
   Ouvrez l'enregistrement Groupe secret avec critères [sn_sm_criteria_secret_group] et recherchez votre serveur MID dans la liste **Groupe secret – Membres du groupe d'identités** . Si votre serveur MID n'est associé à aucun groupe, reportez-vous Créer un groupe secret avec des critèresà .
2. Confirmez que les informations d'identification sont chiffrées avec Gestion des secrets.
   a. Accédez à la **Tout** > **Centre d'intégration** > **Connexions et informations d'identification** > **Informations d'identification**.
   b. Ouvrez votre enregistrement d'informations d'identification.
   Vérifiez qu'un alias d'informations d'identification est répertorié dans le champ **Alias d'informations d'identification** . Si vous n'en avez pas encore créé un, reportez-vous à la section Créer un alias de connexion et d'informations d'identification.
   c. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) l'en-tête de votre enregistrement d'informations d'identification, puis sélectionnez **Afficher** XML dans la liste.
   d. Dans la vue XML de l'enregistrement, recherchez le mot de passe et confirmez que la valeur commence par □□□A□□.



3. Créez un workflow de test dans Studio de workflow.
   a. Accédez à la **Tout** > **Automatisation des processus** > **Studio de workflow**.
   b. Sélectionnez **Nouveau**, **puis Action dans** la liste.
   c. Saisissez un nom dans le champ **Nom de l'action** .
   Laissez le champ **Application** défini sur Global.
   d. Sélectionnez le bouton **d'action Générer** .
4. Configurez une étape de recherche d'enregistrement dans Studio de workflow.

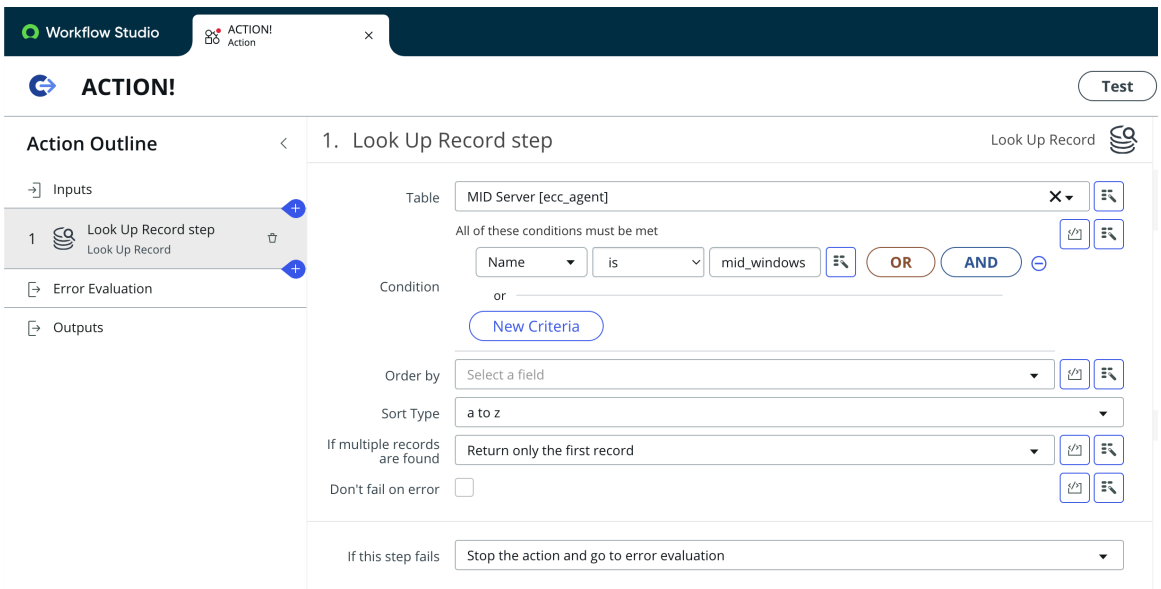
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans Plan **d'action**, sélectionnez le bouton Plus pour ajouter une nouvelle étape.
Recherchez et sélectionnez le type **d'étape Rechercher un enregistrement** .

b. Dans le champ **Table**, sélectionnez **Serveur MID [ecc_agent].**

c. Pour la condition, sélectionnez **Nom est**, suivi du nom de votre serveur MID.



Important :
Assurez-vous que le serveur MID sélectionné est le même que celui associé au groupe secret.

5. Configurez une étape de recherche d'enregistrement dans Studio de workflow.

a. Dans Plan **d'action**, sélectionnez le bouton Plus pour ajouter une nouvelle étape sous votre étape Rechercher un enregistrement.
Recherchez et sélectionnez le type d'étape **PowerShell** .

b. Dans le formulaire **Étape PowerShell** , renseignez les champs selon vos besoins.

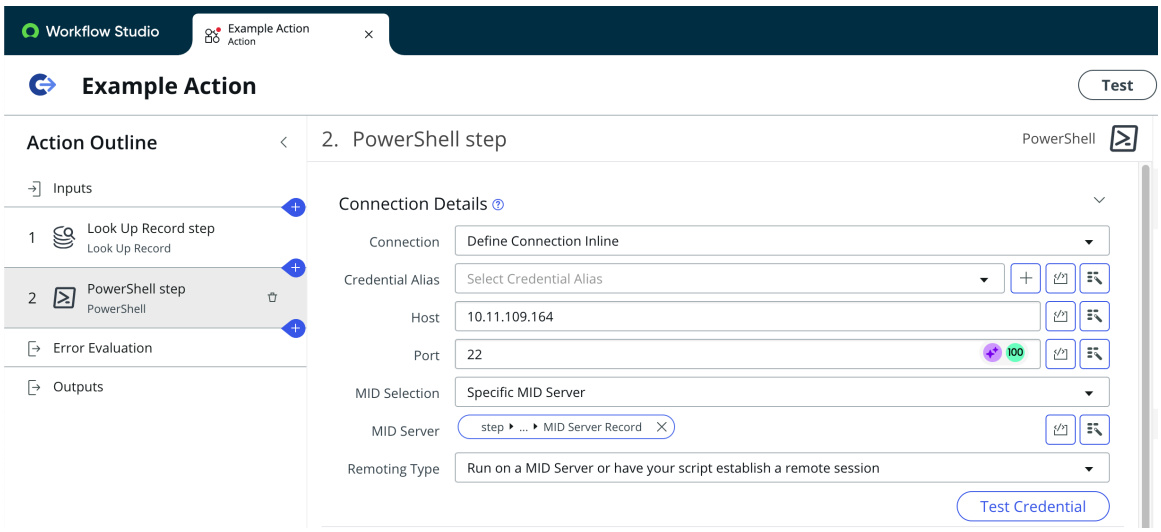
Champs d'étapes PowerShell

Champ	Valeur
Connexion	**Sélectionner Définir l'inline de la connexion**
Alias d'informations d'identification	Sélectionner votre alias d'informations d'identification
Hôte	Entrez l'adresse IP du serveur Windows cible
Port	Saisissez 22 si ce n'est pas déjà le cas par défaut.
Sélection de MID	Sélectionnez **MID Server spécifique**
Serveur MID	Faites glisser le curseur dans la pilule **d'enregistrement de Serveur MID** à partir du panneau **de données**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
	Cette pastille de données est visible dans le panneau **Données** sur le bord droit de l'écran, sous **l'étape Rechercher un enregistrement**.
Type d'accès à distance	Sélectionnez **Exécuter sur un serveur MID ou demandez à votre script d'établir une session à distance**



6. Créez un script pour votre action de test.

a. Dans le champ **Type de script** , sélectionnez **Script aligné**.

b. Utilisez le script suivant, en remplaçant l'exemple de chemin d'accès par le chemin d'accès de votre hôte de test.

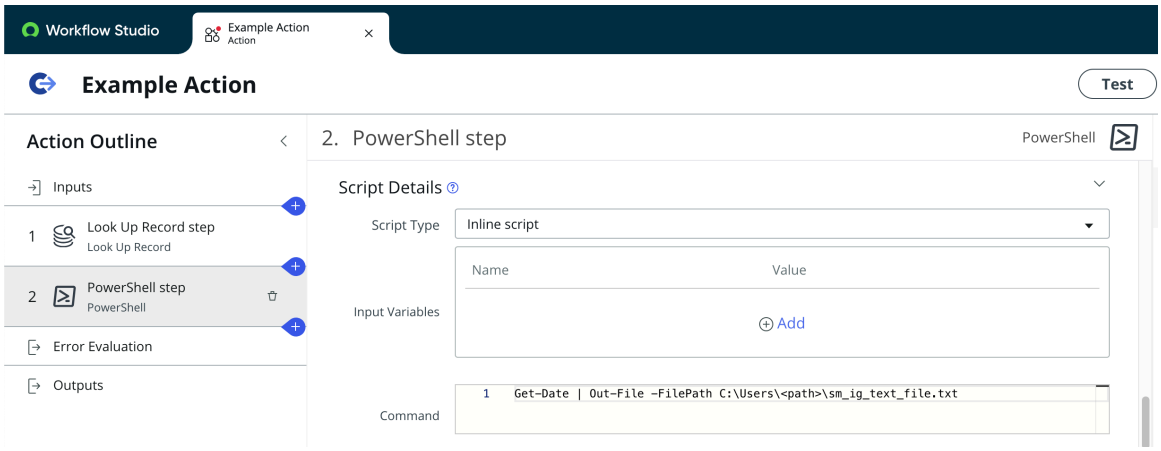
```
Get-Date | Out-File -FilePath C:\Users\<path>\sm_ig_text_file.txt
```

Remarque :
Vous pouvez également exécuter votre propre script adapté à la configuration de votre hôte distant. Il est important de confirmer qu'une connexion a été établie à l'aide de la valeur chiffrée SM.

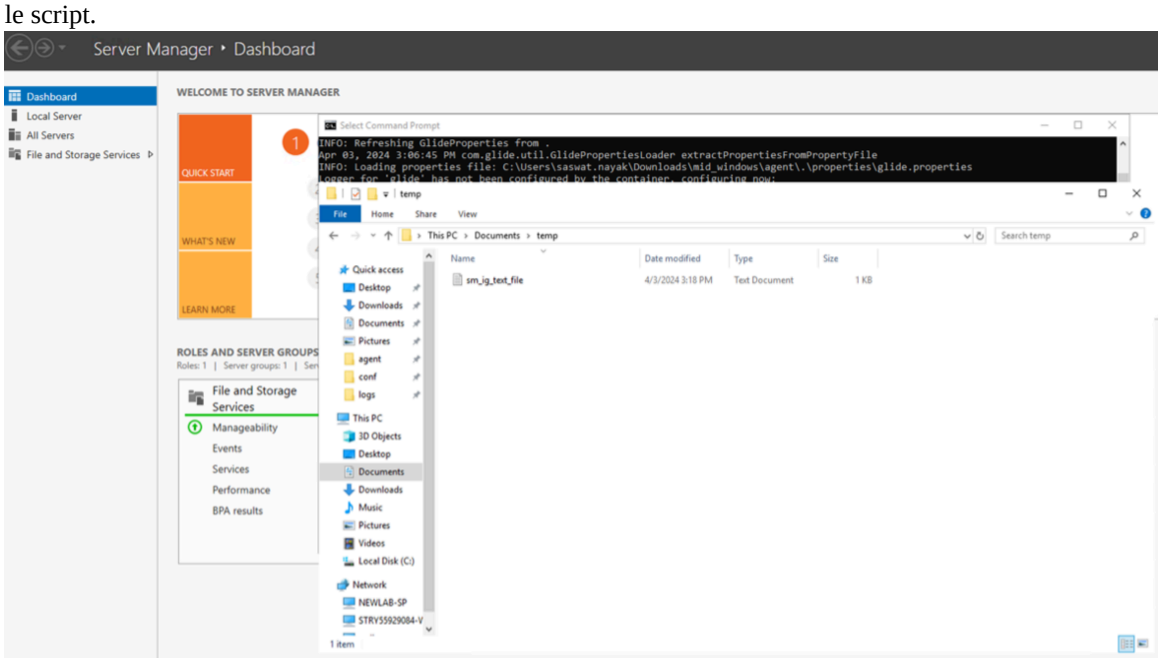
c. Sélectionnez le bouton **Enregistrer** pour enregistrer votre action.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Sélectionnez le bouton **Test** pour tester votre action.
8. Examinez les journaux de sortie pour voir s'il y a des messages d'erreur.
9. Vérifiez qu'un fichier de test a été créé sur le serveur hôte dans le chemin d'accès que vous avez fourni dans le script.



Clonage et gestion des secrets

Découvrez comment reconfigurer les groupes de secrets et les groupes de secrets clients après un clone.

Une fois que vous avez cloné une instance, il est possible que vous deviez reconfigurer vos groupes secrets et groupes de secrets clients pour qu'ils fonctionnent comme prévu.

Origine du groupe de secrets	Comportement après un clone
Groupes de secrets de l'instance d'origine de l'instance cible	Fonctionne comme prévu après l'importation manuelle du module de chiffrement manquant. Consultez Exporting and importing data via XML .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Origine du groupe de secrets	Comportement après un clone
Groupes de secrets clients d'origine de l'instance cible	Fonctionne comme prévu après l'importation manuelle du module de chiffrement manquant. Consultez Exporting and importing data via XML .
Groupes de secrets d'instance clonés à partir de l'instance source	Ne fonctionne pas à moins d'être configuré manuellement
Groupes de secrets clients clonés à partir de l'instance source	Travailler si configurer manuellement sg/identity group/alias/mid

Tableau de bord de gestion des secrets

Utilisez le tableau de bord de gestion des secrets pour examiner les groupes secrets configurés sur votre instance et en savoir plus sur les problèmes de sécurité.

Vue d'ensemble du groupe secret



L'onglet **Vue d'ensemble des groupes secrets** affiche des informations sur vos groupes secrets configurés. Utilisez cet onglet pour afficher des informations sur les groupes de secrets configurés sur votre instance.

Groupe secret par type

Affiche un graphique en secteurs montrant les groupes secrets installés sur votre instance, regroupés par type de secret (côté instance du côté client).

Groupe secret par type de critère

Affiche un graphique à secteurs montrant les groupes secrets avec des critères configurés sur votre instance selon le type de critères utilisés.

Nombre de groupes de secrets inactifs

Affiche le nombre de groupes secrets inactifs configurés sur votre instance.

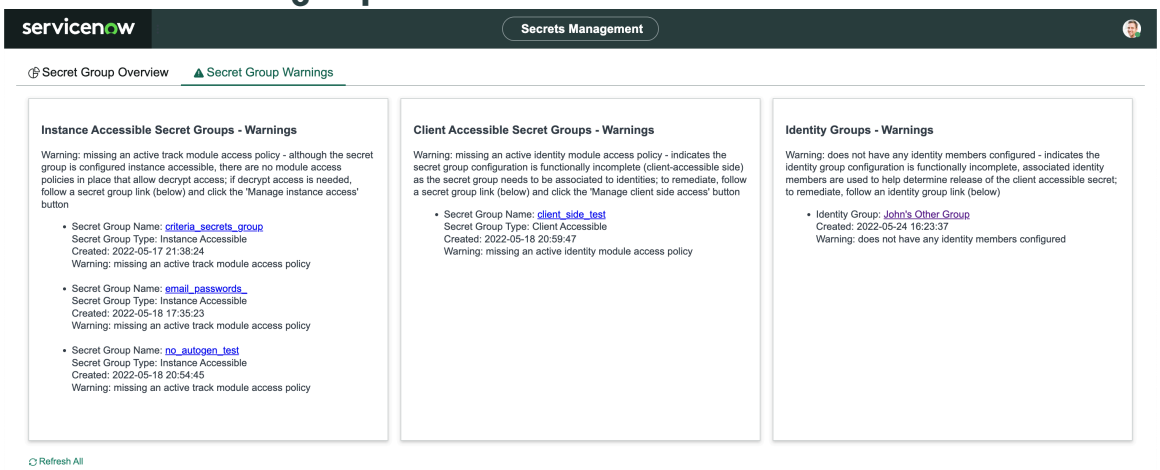
Nombre de secrets dédiés

Affiche un nombre de secrets dans des groupes secrets de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissements de groupes secrets



L'onglet **Avertissements des groupes secrets** affiche les avertissements relatifs à vos groupes secrets et groupes d'identité.

Groupes secrets accessibles aux clients - Avertissements

Cette carte affiche des avertissements s'il existe des groupes secrets pour lesquels aucune politique d'accès active n'est en place. Sélectionnez un nom de groupe secret pour afficher cet enregistrement.

Groupes secrets accessibles aux clients - Avertissements

Cette carte affiche des avertissements s'il existe des groupes secrets accessibles aux clients qui n'ont pas de politique d'accès au module d'identité (MAP) active. Sélectionnez un nom de groupe secret pour afficher cet enregistrement.

Groupes d'identité - Avertissements

Cette carte affiche des avertissements s'il existe des groupes d'identité dont aucun membre n'est configuré. Sélectionnez le nom du groupe d'identité pour afficher l'enregistrement.

Remarque :
Le tableau de bord de gestion des secrets fait partie de Secrets Management Enterprise. Secrets Management Enterprise est un module d'extension payant que ServiceNow le personnel doit activer sur votre instance de production.

Rôles de gestion des secrets

La gestion des secrets ajoute ces rôles.

Administrateur des secrets [sn_secrets.admin]

Affectez des rôles de secrets non-administrateur à d'autres utilisateurs. Les administrateurs de secrets ont les mêmes privilèges que le gestionnaire et le visionneur de secrets.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aucun.

Considérations particulières

Important :
Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

- Un utilisateur doit avoir à la fois les rôles administrateur et security_admin pour se voir attribuer le rôle sn_secret.admin.
- Évitez d'accorder un rôle administrateur lorsque des rôles plus ciblés sont disponibles.

Gestionnaire de secrets [sn_secrets.manager]

Accordez ce rôle aux utilisateurs qui doivent être en mesure d'exécuter l'une des fonctions suivantes.

- Afficher les enregistrements de groupes secrets et secrets
- Afficher l'historique d'accès et d'autres informations sur l'activité d'utilisation
- Créer des groupes et des filtres secrets
- Créer des fournisseurs de secrets
- Déplacer les secrets entre les groupes secrets
- Modifier les paramètres du groupe secret et du fournisseur secret

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Important :
Les gestionnaires de secrets ne peuvent pas voir les secrets en texte brut.

Visionneuse de secrets [sn_secrets.viewer]

Accordez ce rôle aux utilisateurs qui doivent être en mesure d'afficher les enregistrements de groupes secrets et secrets.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Aucun.

Considérations particulières

Aucun.

Créer un module de chiffrement de groupe secret

Créez un module de chiffrement de groupe secret pour effectuer le chiffrement et le déchiffrement.

Avant de commencer

Rôle requis :

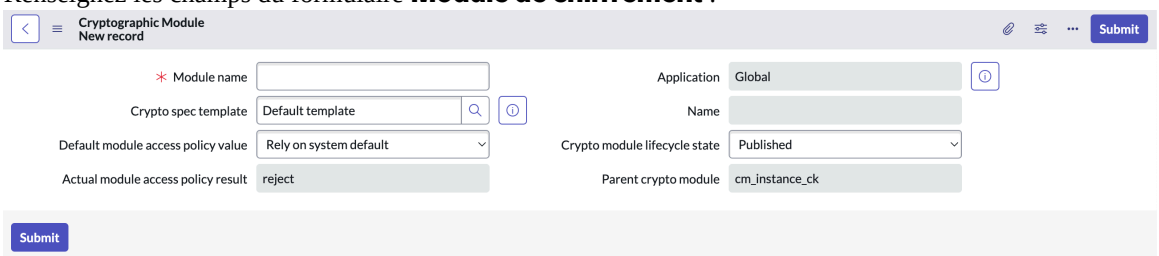
- administrateur
- sn_secrets.admin
- sn_secrets.secret_manager
- sn_kmf.cryptographic_manager
- sn_kmf.admin

Procédure

1. Accédez à la **Tout** > **Gestion des secrets** > **Créer un module de chiffrement de groupe secret**.
2. Sélectionnez le type de module de chiffrement de groupe que vous souhaitez créer.

Type de module de chiffrement	Description
Créer un module de chiffrement secret accessible à l'instance	Créez des secrets accessibles à l'instance qui peuvent être déchiffrés par votre instance.
Créer un module de chiffrement secret accessible aux clients	Créez des secrets accessibles aux clients qui sont chiffrés à l'aide de votre propre clé, à laquelle ServiceNow vous ne pouvez pas accéder.

3. Renseignez les champs du formulaire **Module de chiffrement** .



Champ	Description
Nom du module	Nom descriptif pour votre module
Application	Le périmètre de l'application qui contient votre module. Ce champ est automatiquement renseigné avec le module actuel.
Modèle de spécification de chiffrement	**Le modèle par défaut** est sélectionné par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom du module. Ce nom est généré automatiquement en fonction du nom de l'application et du module.
Valeur de la politique d'accès au module par défaut	○ S'appuyer sur le système par défaut ○ Refuser ○ Trace
État du cycle de vie du module de chiffrement	Indique si le module se trouve à l'état **Brouillon** ou **Publié** .
Résultat réel de la politique d'accès au module	Ce champ est fourni à titre d'information et est en lecture seule.
Module de chiffrement parent	Le module de chiffrement parent, qui est déterminé par le type de module de chiffrement que vous avez sélectionné à l'étape précédente. Ce champ est en lecture seule.

4. Sélectionnez **Soumettre**.

Créer un groupe secret de base

Créez un groupe secret de base pour regrouper tous les secrets, quels que soient leurs critères.

Avant de commencer

Rôle requis : administrateur

Les groupes secrets de base peuvent contenir n'importe quel secret que vous leur ajoutez, quels que soient leur table, leur champ d'application ou leur application. Après l'avoir créé, vous ajoutez manuellement des secrets au groupe. Pour créer un groupe spécifique pour tous les secrets qui partagent un attribut commun tels que ceux-ci, créez un groupe secret avec des critères à l'aide des instructions de la section Créer un groupe secret avec des critères.

Procédure

1. Accédez à la **Tout** > **Gestion des secrets** > **Groupes secrets**.
2. Sélectionnez **Nouveau**.
3. À **la section Quel type de groupe secret voulez-vous créer ?** sélectionnez **Groupe secret de base**.
4. Renseignez les champs du formulaire **Groupe secret** .

Champs de groupes secrets

Champ	Description
Nom de groupe	Nom du groupe **Remarque :** Les noms de groupes secrets ne peuvent contenir que des minuscules, des chiffres et des traits de soulignement (_)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type de secret	Indique si le groupe est **accessible à l'instance** ou **au client**.
Module de génération automatique	Génère un nouveau module de chiffrement pour ce groupe secret. Ce module crypte et décrypte vos données. Ce champ est activé par défaut.
Application	L'application incluse dans le périmètre pour cet enregistrement. Ce champ en lecture seule est automatiquement renseigné avec le champ d'application actuel.
Description brève	Description du groupe
Module de chiffrement	Sélectionnez le module de chiffrement à utiliser avec ce groupe. Ce module crypte et décrypte vos données. Ce champ n'est visible que lorsque **Module de génération automatique** n'est pas sélectionné. Pour plus d'informations sur les politiques d'accès au module, consultez Vue d'ensemble de la politique d'accès au module **Remarque :** Vous pouvez examiner les politiques d'accès au module associées à votre groupe secret à l'aide du bouton **Gérer l'accès à l'instance** .

5. Cliquez sur **Envoyer**.

Remarque : Lorsqu'il est créé, un groupe secret est désactivé par défaut. Revenez à l'enregistrement du groupe et sélectionnez **Actif** pour activer le groupe.

Créer un groupe secret avec des critères

Créez un groupe secret avec des critères pour organiser automatiquement les secrets saisis dans les champs Password2 lorsqu'ils partagent un critère commun, tel qu'une table, un périmètre ou une application.

Avant de commencer

Rôle requis : administrateur

Les secrets de ce type de groupe secret doivent tous partager des critères communs. Pour les groupes qui ne disposent pas de cette restriction, envisagez de créer un groupe secret de base. Familiarisez-vous avec la création d'un groupe secret de base dans Créer un groupe secret de base.

Procédure

1. Accédez à la **Tout** > **Gestion des secrets** > **Groupes secrets**.
2. Sélectionnez **Nouveau**.
3. Dans le **menu Quel type de groupe secret voulez-vous créer ?** prompr, sélectionnez **Groupe secret avec critères**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Renseignez les champs du formulaire **Groupe secret** .

Champs de groupes secrets

Champ	Description
Nom de groupe	Nom du groupe **Remarque :** Les noms de groupes secrets ne peuvent contenir que des minuscules, des chiffres et des traits de soulignement (_)
Type de secret	Indique si le groupe est **accessible à l'instance** ou **au client.**
Module de génération automatique	Génère un nouveau module de chiffrement pour ce groupe secret. Ce module crypte et décrypte vos données. Ce champ est activé par défaut.
Application	L'application incluse dans le périmètre pour cet enregistrement. Ce champ en lecture seule est automatiquement renseigné avec le champ d'application actuel.
Description brève	Description du groupe
Type de critère	Les critères que partagent les secrets de ce groupe. ○ Périmètre ○ Package ○ Table cible ○ Colonne secrète ○ Filtrer l'enregistrement
Module de chiffrement	Sélectionnez le module de chiffrement à utiliser avec ce groupe. Ce module crypte et décrypte vos données. Ce champ n'est visible que lorsque **Module de génération automatique** n'est pas sélectionné. Pour plus d'informations sur les politiques d'accès au module, consultez Vue d'ensemble de la politique d'accès au module **Remarque :** Vous pouvez examiner les politiques d'accès au module associées à votre groupe secret à l'aide du bouton **Gérer l'accès à l'instance** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
En fonction de votre configuration, le **module de chiffrement** peut utiliser une valeur sélectionnée automatiquement.

Lorsque le champ **Type de critère** est défini sur Package et que le champ **Module de génération automatique** est sélectionné :	Le champ **Module de chiffrement** est vide et en lecture seule. Un sous-module Password2 existant est utilisé. Si aucun sous-module Password2 n'est trouvé, le module Glide Encrypter au niveau de l'instance est utilisé.
Lorsque le champ **Type de critère** est défini sur Package et que le champ Module de **génération automatique** est désélectionné : (Le champ **Module de génération automatique** ne peut être désélectionné que par les utilisateurs d'entreprise)	Le champ **Module de chiffrement** est modifiable et les administrateurs peuvent sélectionner un module de chiffrement à utiliser.

5. Sélectionnez et maintenez enfoncé (ou cliquez avec le bouton droit de la souris) l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

Remarque :
Lorsqu'il est créé, un groupe secret est désactivé par défaut.

6. Une fois l'enregistrement enregistré, des champs supplémentaires peuvent apparaître en fonction de la façon dont vous avez configuré votre groupe.

Champs de groupe secret supplémentaires

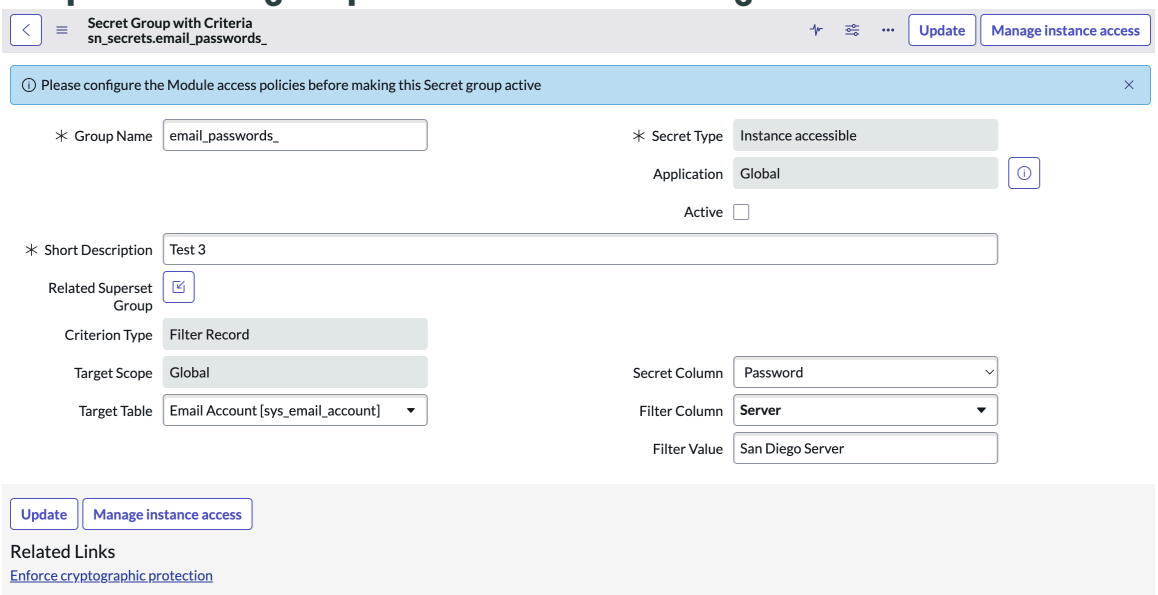
Champ	Description
Périmètre cible	Champ d'application partagé par les secrets à affecter à ce groupe. Ce champ n'est disponible que lorsque vous sélectionnez Périmètre dans le champ **Type de critère** .
Package cible	Package partagé par les secrets à affecter à ce groupe. Ce champ n'est disponible que lorsque vous sélectionnez Package dans le champ **Type de critère**.
Table cible	Table partagée par les secrets à affecter à ce groupe. Ce champ n'est disponible que lorsque vous sélectionnez Table ou Colonne secrète dans le champ **Type de critère** .
Périmètre cible	Périmètre d'application de la table sélectionnée dans le champ **Table cible** . Ce champ n'est visible que lorsque vous sélectionnez Table, Colonne de filtre ou Colonne secrète dans le champ Type de **critère** .
Colonne secrète	Colonne de table qui contient les secrets pasword2 que vous incluez dans ce groupe. Les champs disponibles dans cette liste sont déterminés par la table sélectionnée dans le champ **Table cible** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si aucune colonne de la table de sélection ne contient de secrets, ce champ s'affiche uniquement sous forme de sélection.
Colonne de filtre	Colonne de la table sélectionnée dans la **table cible** que vous souhaitez utiliser comme filtre. Ce champ ne peut pas être un champ Password2.
Valeur de filtre	La valeur que vous souhaitez utiliser comme filtre. Ce filtre s'applique au champ sélectionné dans le champ **Colonne de filtre** .

Example: Groupe accessible à l'instance contenant tous les mots de passe d'un compte de messagerie pour un serveur de messagerie



Que faire ensuite

Après la création de votre groupe, tous les nouveaux enregistrements correspondant aux critères seront chiffrés. Pour chiffrer des enregistrements existants à l'aide du module de chiffrement de ce groupe, vous devez exécuter une tâche de sécurité. Pour plus de détails, voir Exécuter des tâches de sécurité de gestion des secrets.

Les groupes accessibles aux clients ont besoin d'une clé publique fournie par le client pour chiffrer vos secrets. Pour connaître la procédure de chargement de cette clé, reportez-vous à la section Charger une clé publique pour la gestion des secrets.

Charger une clé publique pour la gestion des secrets

Téléchargez une clé publique pour chiffrer vos secrets.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Gestion des secrets** > **Groupes secrets**et ouvrez l'enregistrement du groupe secret.
2. Dans l'enregistrement, sélectionnez le bouton **Gérer l'accès côté client** .
   Un nouvel enregistrement de groupe d'identité s'ouvre.
3. Sélectionnez le bouton **Télécharger la clé d'identité** .
   Une fenêtre **Importer un certificat de clé publique d'identité** s'affiche.
4. Saisissez un alias pour votre clé dans le champ **Alias de clé d'identité** .
5. Sélectionnez le bouton **Importer** pour charger la clé à partir de votre environnement local.
6. Sélectionnez le bouton **OK** .
   Le champ **Clé du module Groupe** utilise le nom de l'alias de la clé d'identité.
7. Sélectionnez **Soumettre** pour enregistrer l'enregistrement du groupe d'identité.

Exécuter des tâches de sécurité de gestion des secrets

Planifiez une tâche de gestion des secrets pour effectuer des tâches de chiffrement sur les champs secrets de votre instance.

Avant de commencer

Rôle requis : sn_kmf.admin, security_admin et sn_secrets.admin

Pour effectuer ces étapes, vous devez vous élever au rôle security_admin. Pour plus d'informations sur ce processus, reportez-vous à la section Élever à un rôle privilégié

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Tâches de Sécurité** > **Créer**.
2. À **l'invite Quel type de tâche de sécurité voulez-vous créer ?** , sélectionnez **Tâche de gestion des secrets**.
3. Renseignez les champs du formulaire.

Formulaire Tâche de gestion des secrets

Champ	Description
Nom	Nom de la tâche de sécurité
État	L'état initial de la tâche est Nouveau. Une fois que la tâche a été exécutée comme prévu, l'état est mis à jour en conséquence
Début de la fenêtre de temps	Heure de début de la tâche au format 24 heures. La tâche commence à s'exécuter à l'heure choisie.
Fin de la fenêtre de temps	Heure de fin de la tâche au format 24 heures. Si la tâche n'est pas terminée à ce moment-là, elle se poursuit pendant la fenêtre de traitement spécifiée suivante jusqu'à ce que la tâche soit terminée.
Niveau de mise en application	Si la tâche affecte toutes les tables, ou une sélection de tables ou de champs spécifiques. Sélectionnez parmi

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Toutes les tables ○ Tables spécifiques ○ Champs spécifiques ○ Packages spécifiques **⚠ Avertissement :** La sélection de l'option **Toutes les tables** peut affecter les performances de l'instance. Envisagez de planifier en dehors des heures de pointe.
Packages	Packages à inclure dans cette tâche. Le chiffrement est appliqué aux packages sélectionnés. Cette option s'affiche uniquement lorsque le champ **Niveau d'application** est défini sur **Packages spécifiques**
Tables	Tables à inclure dans cette tâche. Le chiffrement est appliqué à tous les champs applicables dans les tables sélectionnées. Cette option s'affiche uniquement lorsque **le niveau d'application** est défini sur **Tables spécifiques**
Champs	Tables à inclure dans cette tâche. Le chiffrement est appliqué à tous les champs sélectionnés. Cette option s'affiche uniquement lorsque **le niveau d'application** est défini sur **Champs spécifiques**
Mode de tâche	Sélectionnez parmi **Password2 vers Gestion des secrets** Chiffrez tous les champs password2 au sein de vos groupes de secrets à l'aide des modules de chiffrement définis dans la politique d'accès au module de chaque groupe. **Gestion des secrets vers Password2** Chiffrez à nouveau les données dans vos groupes secrets à l'aide du chiffrement password2. Pour plus d'informations sur ce type de chiffrement, consultez Chiffrement Password2 avec KMF. **Mise en application d'un groupe secret** Interroge toutes les données qui doivent correspondre au groupe sélectionné dans le champ **Groupe secret** . Si toutes les données trouvées par la requête se trouvent déjà dans le groupe, la tâche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	n'apporte aucun changement. Si la requête trouve des données qui ne se trouvent pas encore dans le groupe, la tâche chiffre à nouveau ces données au sein du groupe secret. **Remarque :** Si les données trouvées dans cette requête sont déjà chiffrées et que vos instances ne peuvent pas déchiffrer ces données, elles ne sont pas chiffrées et ajoutées au groupe de secrets.
Groupe secret	Groupe secret contenant les secrets à chiffrer. Ce champ n'est disponible que lorsque **l'option Groupe secret** est sélectionnée dans le champ **Mode de tâche** .
Forcer la nouvelle saisie des données	
Résumé	Affiche des informations sur la progression de la tâche. Le résumé affiche également les enregistrements qui n'ont pas pu être chiffrés par la tâche.

4. Sélectionnez **Soumettre**.

Que faire ensuite

La tâche interroge toutes les données qui doivent correspondre au groupe secret sélectionné. Si toutes les données trouvées par la requête se trouvent déjà dans le groupe, la tâche n'apporte aucun changement. Si la requête trouve des données qui ne se trouvent pas encore dans le groupe, la tâche chiffre à nouveau ces données au sein du groupe secret. (Si l'instance peut le déchiffrer, ce qui n'est peut-être pas le cas pour les secrets chiffrés côté client).

Signature de code

La signature de code crée des signatures numériques pour les données qui sont vérifiées ultérieurement pour confirmer l'authenticité et l'intégrité des données. La signature de code est un module sous licence de ServiceNow Coffre-fort.

Signature de code et cercle de confiance

Le Circle of Trust (COT) est un prérequis pour la signature de code qui crée une communication sécurisée entre vos instances de confiance et de production afin de garantir que seuls les utilisateurs autorisés peuvent accéder à la fonctionnalité de signature de code.

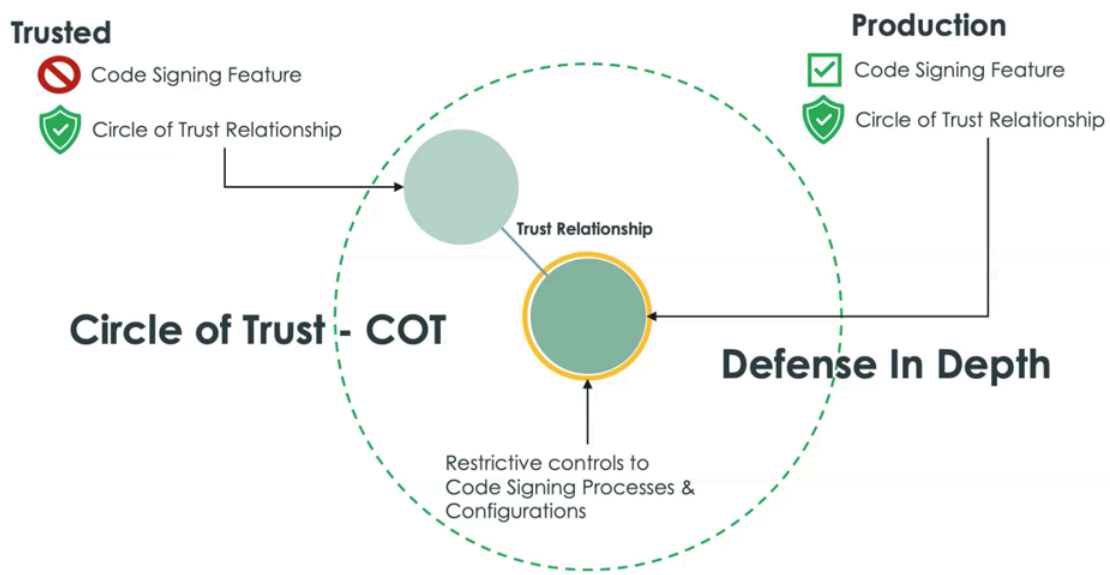
Plusieurs mesures de sécurité permettent d'empêcher les acteurs malveillants de désactiver ou d'utiliser à mauvais escient la signature de code en cas de compromission d'une instance de production. Dans le cadre de la stratégie de défense en profondeur, le COT utilise les composants suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Des contrôles qui restreignent même les comptes administrateur les plus puissants sont établis dans l'instance de production pour protéger les processus et la configuration de signature de code.
- Les instances de confiance sont tenues de collaborer avec les instances de production pour établir la Circle of Trust relation. Au moins une instance de confiance est requise, mais plusieurs instances de confiance peuvent être configurées pour collaborer avec l'instance de production.

Vue d'ensemble du cercle de confiance

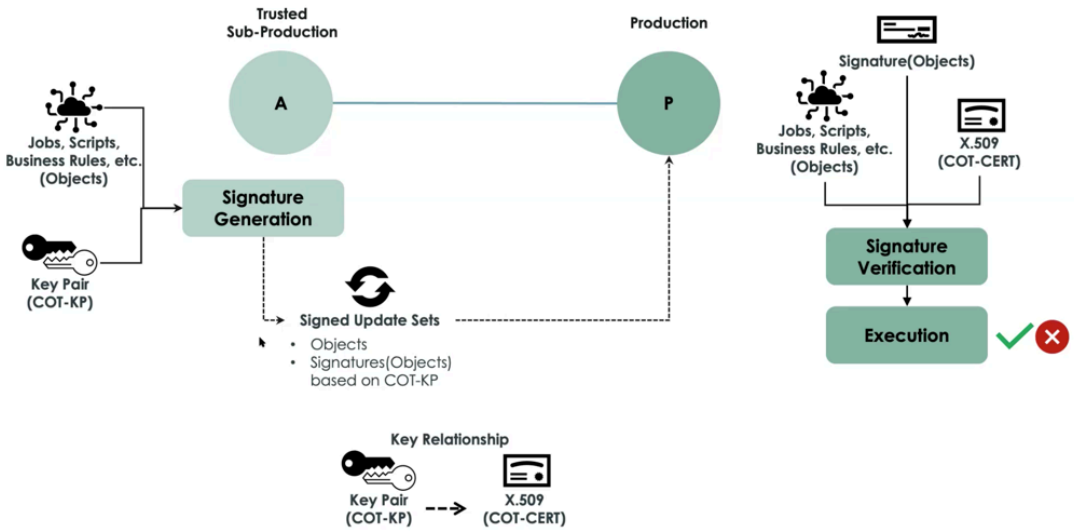


Le utilise Circle of Trust des tâches, des scripts et des règles métier ainsi qu'une paire de clés pour générer des signatures pour signer les ensembles de mises à jour vers l'instance de production. Lorsque la tâche est appelée, la signature est vérifiée ainsi que le certificat approuvé pour exécuter les mises à jour de l'instance de production.

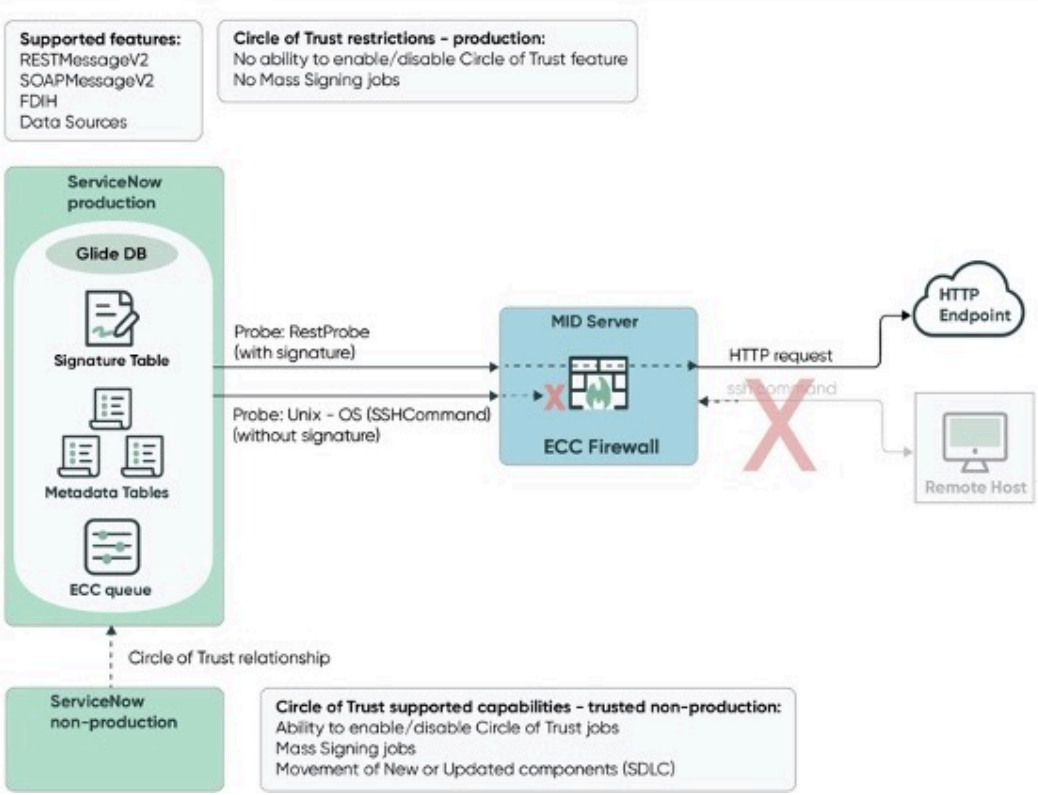
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Processus d'ensembles de mises à jour approuvés



Flux de signature de code



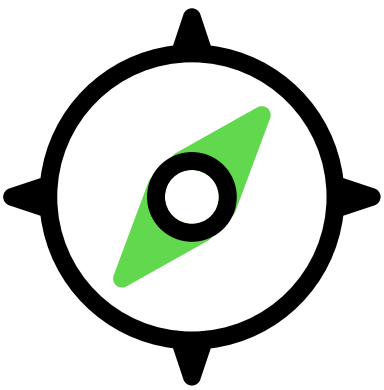
Le Circle of Trust nécessite une relation de confiance initiale entre les instances de confiance et de production qui empêche tout utilisateur non autorisé, quel que soit le niveau d'autorisation, d'accéder à des activités non approuvées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

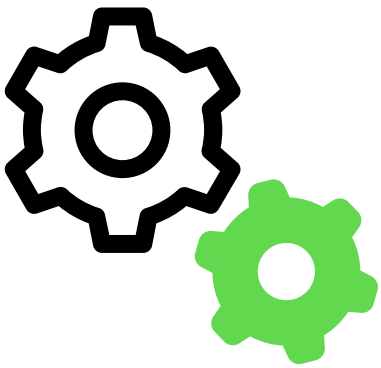
Premiers pas

Explorer



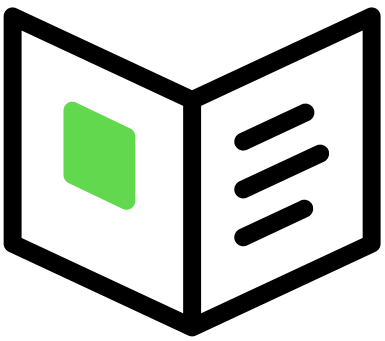
Découvrez les principales fonctionnalités et la valeur commerciale de la signature de code.

Configurer



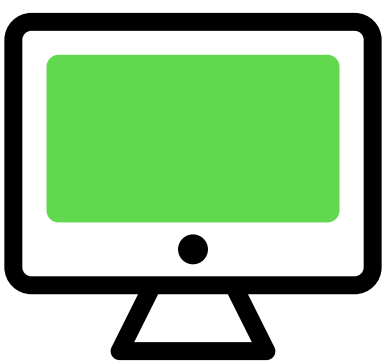
Activez et configurez la signature de code.

Référence



Obtenir des détails sur les propriétés et le dépannage

Utiliser



Découvrez comment utiliser la signature de code pour vérifier l'authenticité et l'intégrité de vos données.

Dépannage et demande d'aide

- https://www.servicenow.com/community/secops/ct-p/security-operations
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer la signature de code

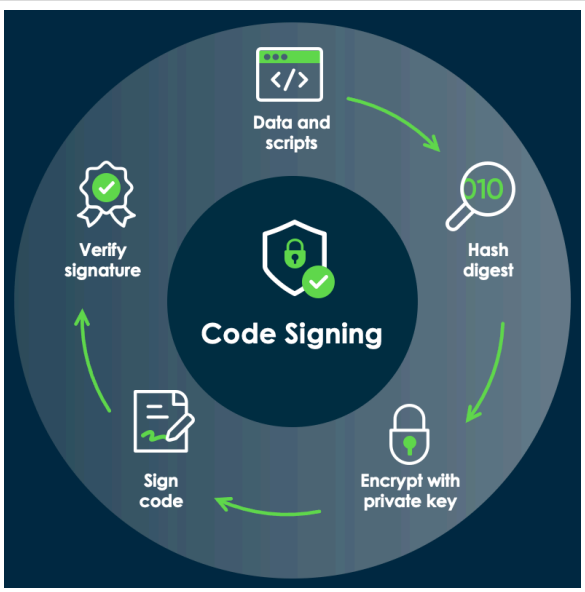
La signature de code peut contribuer à améliorer la sécurité en validant les données et les scripts de configuration d'application sensibles avant leur utilisation.

La signature de code crée des signatures numériques pour les données, qui sont ensuite vérifiées pour confirmer l'authenticité et l'intégrité des données. La signature de code est un module sous licence de ServiceNow Coffre-fort.

Remarque :
L'équipe Service et assistance client doit accorder l'accès à la signature de code.

La signature de code déclare l'intention derrière l'opération en cours d'exécution et valide si la ressource ou l'enregistrement peut être utilisé aux fins prévues. Pour faciliter la signature de code, le Key Management Framework (KMF) utilise des certificats numériques et le chiffrement asymétrique standard de l'industrie pour les signatures numériques.

Utilisez la signature de code en interne côté plateforme et infrastructure. La signature de code permet de signer le contenu de tables spécifiques ou d'un sous-ensemble d'enregistrements dans une table de métadonnées donnée.



La signature de code utilise un (COT) sécurisé Circle of Trust entre vos instances de confiance et de production pour garantir que seules les instances autorisées et sécurisées peuvent accéder à la fonctionnalité de signature de code.

Cas d'utilisation

La signature de code peut être utilisée pour les opérations avec les et Hub d'intégration.Serveur MID La notarisation est l'utilisation de la signature de code pour créer des signatures numériques pour les enregistrements de file d'attente ECC utilisés dans les opérations de serveur MID et les opérations du concentrateur d'intégration.

Par exemple, un script include écrit par ServiceNow pour créer des enregistrements de file d'attente ECC lors de l'exécution est signé comme « contenu du système de base ». Il est signé comme « correctement émis par l'instance ServiceNow », par opposition à une insertion dans la file d'attente ECC à partir d'un script en arrière-plan ou d'une autre origine qui n'est pas validée et signée.

Hub d'intégration peut utiliser la signature de code pour signer le contenu dynamique généré sur la plateforme et valider les parties critiques des données d'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil :

Les horodatages garantissent que les enregistrements signés n'expirent pas à l'expiration du certificat, à condition que l'enregistrement ait été signé avant l'expiration du certificat. Une période de grâce de 4 heures autour de la fenêtre de validité du certificat existe pour garantir que les différences de temps entre les serveurs n'invalident pas intentionnellement les certificats.

Validation et tâches de signature de code

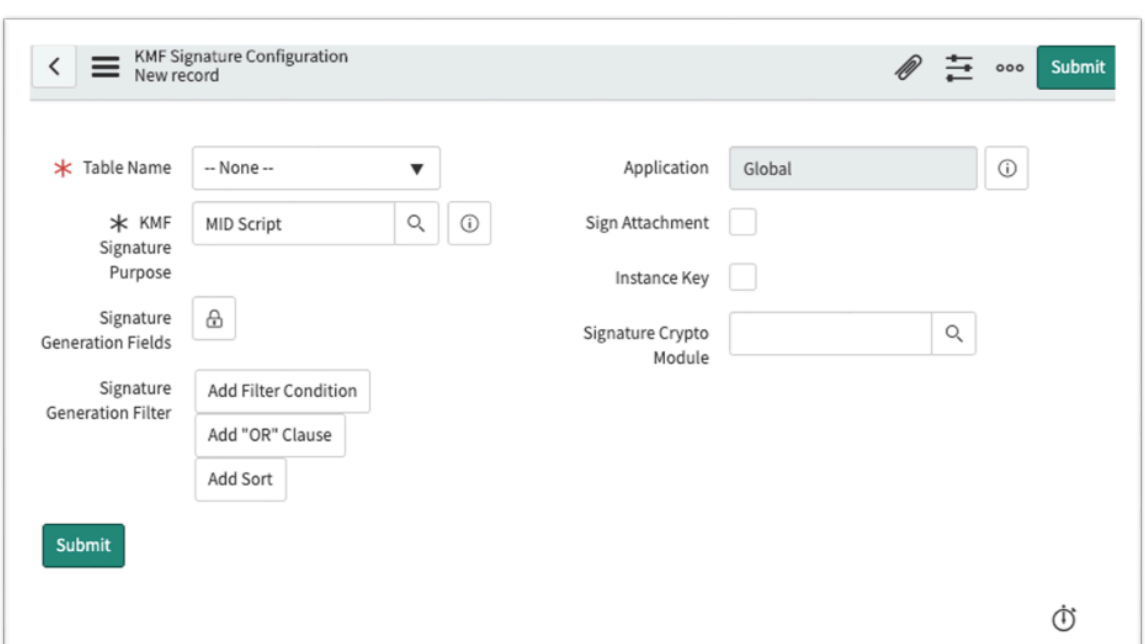
Toutes les tables de métadonnées avec des configurations valides sont signées au moment de la création à l'aide du module d'extension de métadonnées de signature de code (`com.glide.code_signing`). Si vous choisissez de signer les tables, les utilisateurs administrateurs ayant le rôle d'administrateur de sécurité ont accès aux tâches de chiffrement de signature de code :

- Signez les ensembles de mises à jour.
- Enregistrements de signatures en masse.
- Pièces jointes de signature en masse.

Signer l'ensemble de mises à jour

Cette tâche signe les enregistrements qui correspondent à une configuration de signature dans l'ensemble de mises à jour. La tâche ajoute également tous les nouveaux enregistrements de signature et les certificats de vérification à l'ensemble de mises à jour.

Enregistrement de signature KMF pour l'ensemble de mises à jour



Enregistrements de signatures en masse

Cette tâche signe tous les enregistrements qui correspondent à la configuration de signature appliquée sur une table de métadonnées spécifique.

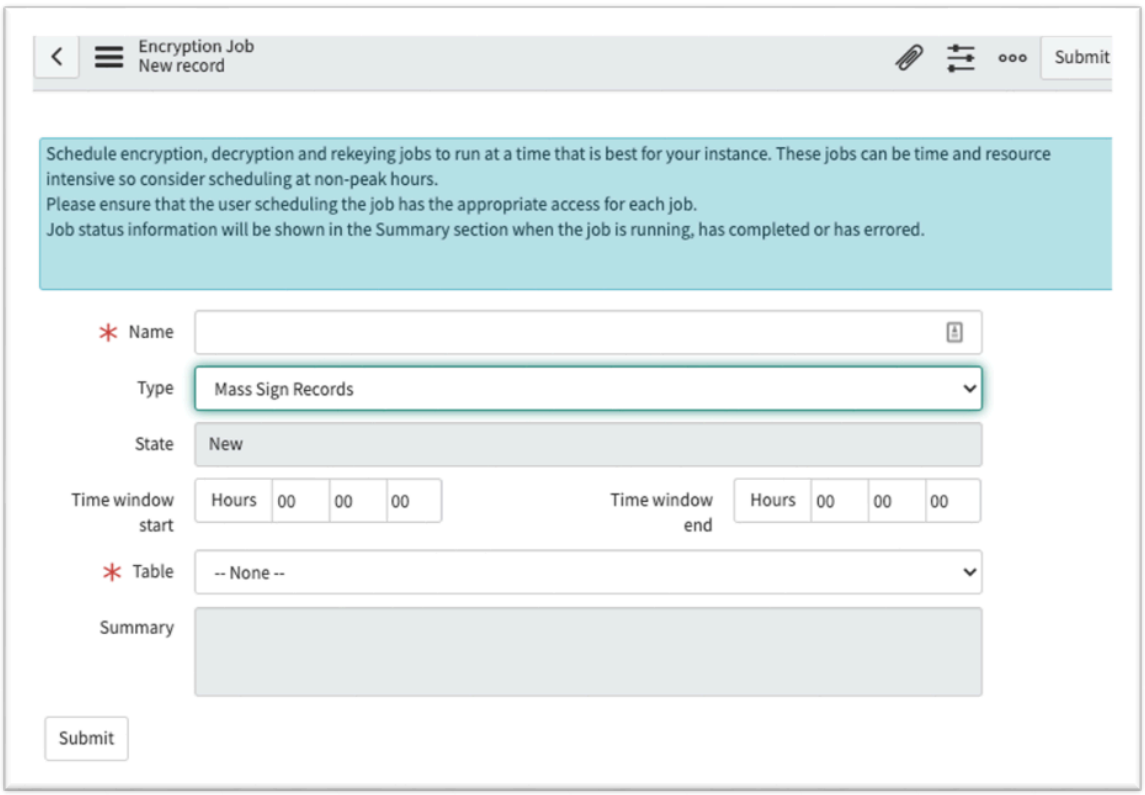
Pièces jointes de signature en masse

Cette tâche signe tous les enregistrements de pièces jointes qui sont joints à une table qui correspond à une configuration de signature spécifiée.

Traduction automatique

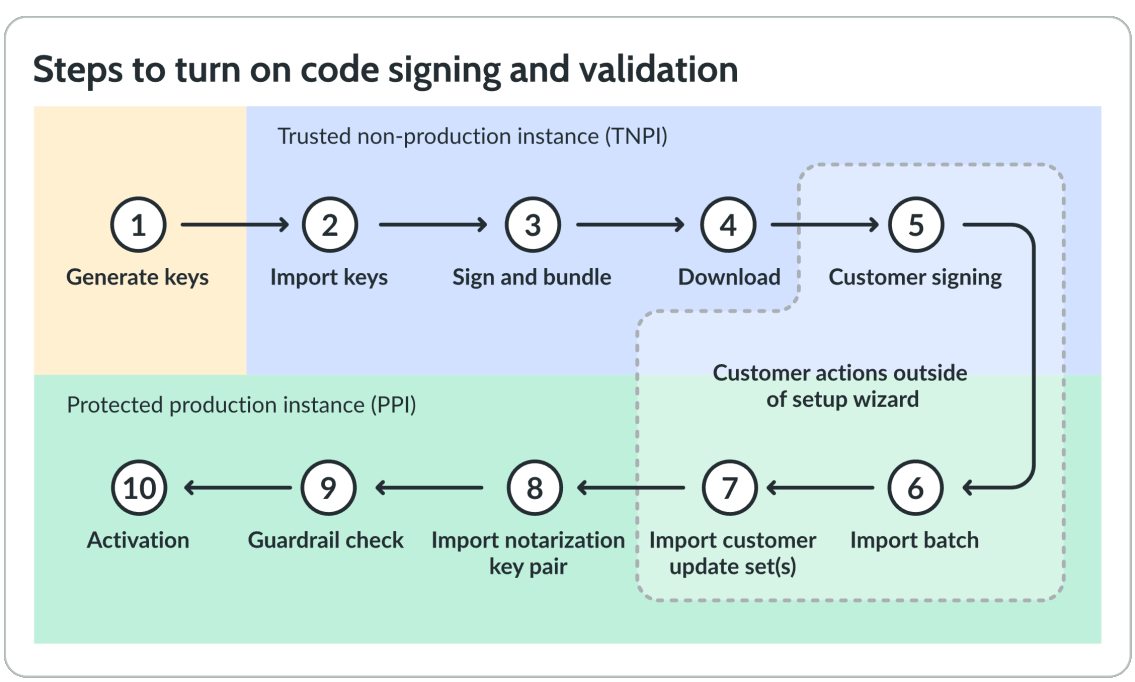
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche de chiffrement pour signer en masse les enregistrements



Configuration de la signature de code

Activez et configurez la signature de code pour vérifier l'authenticité et l'intégrité de vos données.



La fonctionnalité Signature de code exige une relation de confiance initiale entre les instances de confiance et les instances de production afin d'empêcher tout utilisateur non autorisé, quel que soit le niveau d'autorisation, d'accéder à des activités non approuvées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Reportez-vous à chaque rubrique pour effectuer les étapes de configuration afin d'établir l'option Circle of Trust avec Code Signing Enterprise :

Affecter le rôle d'administrateur de signature de code

Affectez le rôle d'administrateur de signature de code à un utilisateur pour accéder à l'expérience de configuration de signature de code.

Configurer Code Signing Enterprise sur votre instance de non-production de confiance

Activez la signature de code sur votre instance de non-production de confiance (TNPI).

Chargez votre fichier de configuration de signature de code sur votre instance de production protégée

Chargez le fichier de configuration généré sur votre instance de non-production de confiance.

Configurer la signature de code d'entreprise sur votre instance de production protégée

Activez et configurez la signature de code sur votre instance de production protégée (PPI).

Activer la validation de certificat

Activez la validation de certificat sur votre instance.

Désactiver la signature de code

Désactivez la signature de code sur votre instance de production protégée (PPI).

Remarque :
Cette étape facultative ne fait pas partie de la configuration initiale de la signature de code

Affecter le rôle d'administrateur de signature de code

Affectez le rôle d'administrateur de signature de code à un utilisateur pour accéder à l'expérience de configuration de signature de code.

Avant de commencer

Rôles requis :

- administrateur
- security_admin

Important :
L'utilisateur auquel le rôle d'administrateur de signature de code est affecté doit se trouver dans le champ d'application global.

Procédure

1. Sélectionnez une instance de non-production à utiliser comme instance de non-production de confiance (TNPI).
   La TNPI permet de créer des tâches, de signer des enregistrements et d'effectuer d'autres tâches nécessaires avant d'activer la validation de signature sur votre instance de production protégée (PPI).
2. Accédez à la **Tout** > **Signature de code** > **Administration du rôle de signature de code**.
3. Accordez à un utilisateur le rôle d'administrateur de signature de code en déplaçant un utilisateur de la liste **Utilisateurs disponibles** vers la liste **Utilisateur(s) sélectionné(s).**
4. Sélectionnez **Enregistrer**.

Important :
L'utilisateur affecté au rôle doit se déconnecter et se connecter à nouveau pour effectuer des tâches de signature de code.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
L'utilisateur sélectionné a le rôle d'administrateur de signature de code. Un utilisateur disposant de ce rôle peut accéder à l'expérience de configuration de signature de code et affecter d'autres rôles de signature de code aux utilisateurs.

Pour en savoir plus sur les rôles de signature de code, reportez-vous à la section Rôles installés avec Signature de code.

Configurer Code Signing Enterprise sur votre instance de non-production de confiance

Activez et configurez la signature de code sur votre instance de non-production de confiance (TNPI).

Avant de commencer
Rôles requis :

- administrateur
- security_admin
- codesigning_admin

> **Remarque :**
> Le rôle codesigning_admin peut être affecté à l'aide du processus décrit à la section Affecter le rôle d'administrateur de signature de code.

- sn_kmf.cryptographic_manager

Vous devez disposer d'au moins une paire de clés cryptographiques et d'un certificat (extension de fichier p12) pour la signature client et l'administration du cercle de confiance (COT). Pour améliorer la sécurité, envisagez d'utiliser des paires de clés cryptographiques distinctes pour la signature client et l'administration COT.

> **Avertissement :**
> Une fois ce processus terminé, vous aurez téléchargé un fichier de configuration qui doit être installé sur votre PPI dans l'heure qui suit. Vérifiez que vous disposez de suffisamment de temps après ce processus pour charger le fichier de configuration dans votre instance de production. Pour obtenir plus de détails sur ce processus, voir Chargez votre fichier de configuration de signature de code sur votre instance de production protégée.

Procédure

1. Sur votre TNPI, accédez à **Tout** > **Signature de code** > **Configuration de la signature de code** pour ouvrir la page de configuration de la signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **Instance de non-production de confiance**.
3. Cliquez sur le bouton **Suivant** .
4. Dans le champ **Action, sous Sélectionner l'action que vous souhaitez accomplir**, sélectionnez **Activer la signature de code**.
5. À côté **de Pièces jointes** , dans la section **Paire de clés de signature du client et certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.

> **Conseil :**
> Si l'option **+Ajouter un fichier** n'est pas disponible, vérifiez que vous êtes dans le périmètre Global et que vous disposez du rôle sn_kmf.cryptographic_manager.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
7. Sélectionnez **Importer**.
8. Sélectionnez **Continuer** pour passer à la section suivante.
9. À côté **de Pièces jointes** , dans la **section Paire de clés d'administration COT et certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.
10. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
11. Sélectionnez **Importer**.
12. Sélectionnez **Continuer** pour passer à la section suivante.
13. Dans la section **Effectuer des tâches de non-production de confiance** , attendez que toutes les tâches soient terminées.

    Votre instance génère et exécute automatiquement ces tâches. Si vous avez utilisé la signature de code avant la Vancouver publication, des tâches sont créées et exécutées pour mettre à jour vos signatures.

    Dans certains cas, aucune tâche n'est nécessaire. **Aucune tâche nécessaire s'affiche** sur cette page.
14. Sélectionnez **Continuer** pour passer à la section suivante.
15. Sur la page **Exporter le fichier de configuration** , sélectionnez **Exporter** pour créer et télécharger un fichier de configuration utilisé pour activer la signature de code sur votre instance de production protégée. Le processus d'exportation télécharge un fichier XML sur votre ordinateur local pour l'utiliser dans les étapes détaillées de la section Configurer la signature de code d'entreprise sur votre instance de production protégée.

Chargez votre fichier de configuration de signature de code sur votre instance de production protégée

Chargez le fichier de configuration généré sur votre instance de non-production de confiance.

Avant de commencer

Rôles requis :

- administrateur
- security_admin
- codesigning_admin

> **Remarque :**
> Le rôle codesigning_admin peut être affecté à l'aide du processus décrit à la section Affecter le rôle d'administrateur de signature de code.

- sn_kmf.cryptographic_manager

Vous avez également besoin du fichier de configuration généré au cours des étapes détaillées dans la section Configurer Code Signing Enterprise sur votre instance de non-production de confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
2. Sélectionnez **Importer un ensemble de mises à jour à partir d'un fichier XML** en bas de la liste **Ensembles de mises à jour récupérés** .
3. Sélectionnez **Choisir un fichier**, puis sélectionnez votre fichier de configuration (extension de fichier xml).
4. Sélectionnez **Charger**.
   Vous devez voir l'ensemble de mises à jour de **configuration de signature de codes** dans la liste **Ensembles de mises à jour récupérés** .
5. Sélectionnez et ouvrez l'ensemble de mises à jour **de configuration de Codesign** .
6. Sélectionnez **Prévisualiser le lot d'ensembles de mises à jour**.
   Si des conflits se produisent pendant l'aperçu, résolvez-les en sélectionnant **Accepter la mise à jour distante** ou **Résoudre les conflits CS connus**.
7. Après avoir résolu tous les conflits, sélectionnez **Valider le lot d'ensembles de mises à jour**.

Configurer la signature de code d'entreprise sur votre instance de production protégée

Activez et configurez la signature de code sur votre instance de production protégée (PPI).

Avant de commencer

Rôles requis :

- administrateur
- security_admin
- codesigning_admin

Remarque :
Le rôle codesigning_admin peut être affecté à l'aide du processus décrit à la section Affecter le rôle d'administrateur de signature de code.

- sn_kmf.cryptographic_manager

Procédure

1. Sur votre PPI, accédez à **Tout** > **Signature de code** > **Configuration de la signature de code** pour ouvrir la page de configuration de la signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **Instance de production protégée**.
3. Cliquez sur le bouton **Suivant** .
4. Cochez la case **Veuillez confirmer que l'ensemble de mises à jour de configuration de signature de code a été importé et validé** .
5. Cliquez sur le bouton **Suivant** .
6. Attendez la fin de l'installation du certificat.
   Un message d'alerte bleu s'affiche indiquant que des éléments du fichier de configuration sont en cours d'installation. L'alerte disparaît en quelques secondes à la fin de l'installation.
7. À côté **de Pièces jointes** , dans la **section Paire de clés d'exécution/de notarisation et de certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser à des fins d'exécution/de notarisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez réutiliser une paire de clés de l'instance de non-production approuvée (TNPI) ou en charger une nouvelle spécialement pour cette utilisation.

Conseil :
Si l'option **+Ajouter un fichier** n'est pas disponible, vérifiez que vous êtes dans le périmètre Global et que vous disposez du rôle sn_kmf.cryptographic_manager.

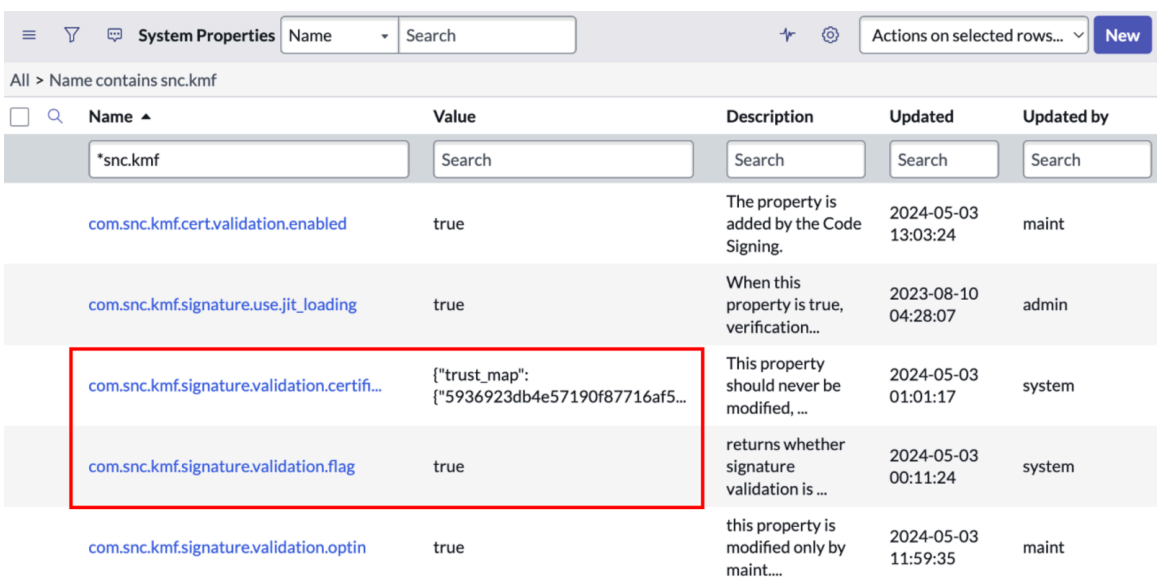
8. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
9. Sélectionnez **Importer**.
10. Sélectionnez **Continuer** pour passer à la section suivante.
11. Patientez pendant que votre instance effectue une vérification de garde-fou.
    Cette vérification analyse votre instance à la recherche de signatures non valides et peut prendre un certain temps. Ne quittez pas ou n'actualisez pas la page tant que l'analyse n'est pas terminée.
12. Si l'analyse trouve des signatures non valides, sélectionnez **Télécharger le rapport**.

    La sélection de **Télécharger le rapport** télécharge un rapport (scan_report.txt) que vous pouvez utiliser pour examiner et corriger les signatures non valides.

    Après avoir résolu les erreurs, actualisez la page pour réexécuter la vérification.
13. S'il n'y a pas d'erreur, sélectionnez **Terminer la configuration**.
14. Attendez que les tâches de configuration soient terminées.
    Votre instance exécute une ou plusieurs tâches pour terminer le processus de configuration. Ne quittez pas ou n'actualisez pas la page tant que les tâches ne sont pas terminées. Lorsque vous avez terminé, vous devriez voir un message **Configuration de signature de code terminée avec succès** .

Résultats

La validation de signature est maintenant appliquée sur votre instance de production. Vous pouvez vérifier que vous avez terminé correctement en examinant vos propriétés système. Recherchez la propriété **com.snc.kmf.signature.validation.flag** dans la table Propriétés système [sys_property] et vérifiez qu'elle a la valeur **true**. Vérifiez que la propriété **com.snc.kmf.signature.validation.certificate_trust** n'a pas de valeur vide.



Activer la validation de certificat

Protégez votre instance avec une validation basée sur des certificats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis :

- codesigning_admin
- security_admin
- sn_kmf.cryptographic_manager

Procédure

1. Sur votre instance de non-production de confiance (TNPI), accédez à **Tout** > **Signature de code** > **Configuration de la signature de code** pour ouvrir la page de configuration de la signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **Instance de non-production de confiance**.
3. Cliquez sur le bouton **Suivant** .
4. Dans le champ **Action, sous Sélectionner l'action que vous souhaitez accomplir**, sélectionnez **Activer la validation de certificat**.
5. Cliquez sur le bouton **Suivant** .
6. À côté **de Pièces jointes** , dans la section **Paire de clés de signature du client et certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.

   Conseil :
   Si l'option **+Ajouter un fichier** n'est pas disponible, vérifiez que vous êtes dans le périmètre Global et que vous disposez du rôle sn_kmf.cryptographic_manager.

7. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
8. Sélectionnez **Importer**.
9. Sélectionnez **Continuer** pour passer à la section suivante.
10. À côté **de Pièces jointes** , dans la **section Paire de clés d'administration COT et certificat** , sélectionnez **+Ajouter un fichier** pour charger une paire de clés cryptographiques (extension de fichier p12) à utiliser pour la signature du client.
11. Dans le champ **Mot de passe** , saisissez le mot de passe de la paire de clés chargée.
12. Sélectionnez **Importer**.
13. Sélectionnez **Continuer** pour passer à la section suivante.
14. Dans la section **Effectuer des tâches de non-production de confiance** , attendez que toutes les tâches soient terminées.

    Votre instance génère et exécute automatiquement ces tâches. Si vous avez utilisé la signature de code avant la Vancouver publication, des tâches sont créées et exécutées pour mettre à jour vos signatures.

    Dans certains cas, aucune tâche n'est nécessaire. **Aucune tâche nécessaire s'affiche** sur cette page.

15. Sélectionnez **Continuer** pour passer à la section suivante.
16. Sur la page **Exporter le fichier de configuration** , sélectionnez **Exporter** pour créer et télécharger un fichier de configuration utilisé pour activer la signature de code sur votre instance de production protégée. Le processus d'exportation télécharge un fichier XML sur votre ordinateur local pour l'utiliser dans les étapes détaillées à la section Configurer la signature de code d'entreprise sur votre instance de production protégée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

17. Sur votre instance de production protégée (PPI), accédez à **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
18. Sélectionnez **Importer un ensemble de mises à jour à partir d'un fichier XML** en bas de la liste **Ensembles de mises à jour récupérés** .
19. Sélectionnez **Choisir un fichier**, puis sélectionnez votre fichier de configuration (extension de fichier xml).
20. Sélectionnez **Charger**.
21. Revenez à la page de configuration de la signature de code à l'adresse **Tout** > **Signature de code** > **Configuration de la signature de code**.
22. Utilisez l'assistant pour terminer votre configuration, en sélectionnant les options pour terminer l'activation de la validation du certificat.

Désactiver la signature de code

Désactivez la signature de code sur votre instance de production protégée (PPI).

Avant de commencer

Rôle requis : admin, codesigning_admin

Procédure

1. Sur votre instance de non-production de confiance (TNPI), accédez à **Tout** > **Signature de code** > **Configuration de la signature de code** pour ouvrir la page de configuration de la signature de code.
2. Dans le champ **Type d'instance** , sélectionnez **Instance de non-production de confiance**.
3. Cliquez sur le bouton **Suivant** .
4. Dans le champ **Action** , sous **Sélectionner l'action que vous souhaitez accomplir**, sélectionnez **Désactiver la signature de code**.
5. Dans le panneau **Exporter le fichier de configuration** , sélectionnez **Exporter** pour télécharger l'ensemble de mises à jour.
   Le processus d'exportation télécharge un fichier XML sur votre ordinateur local pour l'utiliser lors des étapes suivantes.
6. Sélectionnez **Terminé**.
7. Connectez-vous à votre instance de production protégée (PPI).
8. Chargez vos fichiers de configuration en suivant les étapes de la section Chargez votre fichier de configuration de signature de code sur votre instance de production protégée.
9. Accédez à la **Tout** > **Signature de code** > **Configuration de la signature de code** pour ouvrir la page de configuration de la signature de code.
10. Dans le champ **Type d'instance** , sélectionnez **Instance de production protégée**.
11. Cliquez sur le bouton **Suivant** .
12. Cochez la case **Veuillez confirmer que l'ensemble de mises à jour de configuration de signature de code a été importé et validé** .
13. Cliquez sur le bouton **Suivant** .
14. Attendez la fin de l'installation du certificat.
    Une fois l'opération terminée, un message **Configuration de signature de code terminée avec succès** s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats

Vous pouvez vérifier que vous avez terminé correctement en examinant vos propriétés système. Recherchez la propriété **com.snc.kmf.signature.validation.flag** dans la table Propriétés système [sys_property] et vérifiez qu'elle a la valeur **faux**.

Charger les paires de clés et les certificats requis pour la signature de code

Établissez la relation dans une instance de non-production désignée à l'aide de la signature de code. Cette première étape charge deux clés cryptographiques dans l'environnement de non-production afin d'établir une source fiable pour les mises à jour de l'instance de production.

Avant de commencer

Rôles requis : security_admin et sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

La première étape de l'établissement de la relation consiste à établir la fondation de la fiducie dans une instance de non-production désignée à l'aide de la signature de code. Pour effectuer cette tâche, vous avez besoin des éléments suivants.

- Vous devez disposer de deux paires de clés publiques/privées RSA 4 096 bits à charger dans les modules de chiffrement de signature de code :
  - Une paire pour le module cryptographique cm_code_signing
  - Une paire pour le module cryptographique cm_code_attest

  Pour en savoir plus sur ces touches, reportez-vous à la section Créer des paires de clés et des certificats de signature de code.

  Important :
  Ces paires de clés doivent être signées par une autorité de certification publique ou par l'autorité de certification interne de votre organisation. Le certificat ne peut pas être autosigné.

- Un fichier Public Key Cryptography Standard #12 (.p12) contenant vos certificats feuille et intermédiaire.

Procédure

1. Importez vos clés à partir du magasin de clés.
   a. Accédez à la **Tout** > **Gestion des clés** > **Modules de chiffrement** > **Tout**.
   b. Recherchez et ouvrez le module de chiffrement nommé `cm_code_signing`.
   c. Dans la liste **Spécifications de chiffrement** , sélectionnez le nom de la spécification de chiffrement pour l'ouvrir.
   d. Dans l'écran **Importer la clé depuis le magasin de clés** , sélectionnez **Importer la clé**.
2. Répétez la première étape pour importer le module cryptographique nommé `cm_code_attest`.
3. Dans le champ **Saisir le mot de passe du magasin de clé** , saisissez le mot de passe de défi que vous avez créé lors de la génération de votre certificat RSA.

   Remarque :
   Le mot de passe de défi que vous avez créé est appelé ici **mot de passe de magasin de clé**. Dans d'autres parties du processus, il peut s'agir d'un **mot de passe d'importation** ou **d'exportation**. Dans tous les cas, ce mot de passe est le même que celui que vous avez créé dans les étapes précédentes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez le bouton **Parcourir** en regard de **Importer un magasin de clé/certificat**.
5. Sélectionnez un fichier Public Key Cryptography Standard #12 (.p12) contenant votre certificat de distribution (mentionné dans la section Avant de commencer en haut de ce document).
6. Sélectionnez **OK**.

> **Important :**
> Si vous utilisez votre propre autorité de certification interne, vous devez charger les certificats intermédiaires de l'autorité de certification interne en suivant le processus des étapes 5 et 6.

Une fois l'importation de votre clé et de votre ou vos certificats réussis, un message de confirmation s'affiche.

Vous pouvez valider que la clé et les certificats sont présents sur votre instance dans la table Certificats X.509 [sys_certificate]. Ces enregistrements ont un type de **certificat de magasin de confiance**.

Vous pouvez valider votre clé dans la table Modules de chiffrement [sys_kmf_crypto_module].

Que faire ensuite

Exportez le certificat en production. Consultez Préparer les certificats du cercle de confiance pour en savoir plus.

Préparer les certificats du cercle de confiance

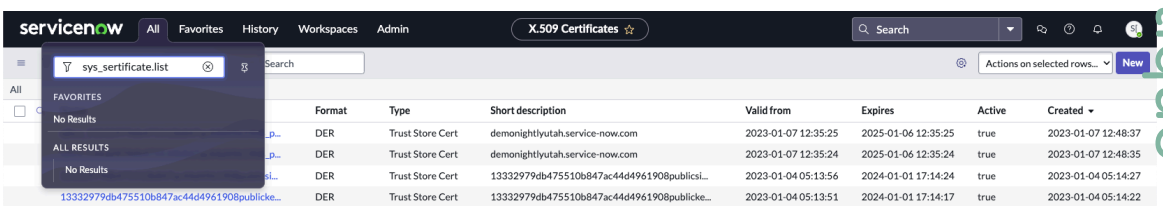
Créez un ensemble de mises à jour dans l'environnement approuvé pour exporter le certificat approuvé vers l'environnement de production.

Avant de commencer

Rôles requis : admin, security_admin

Procédure

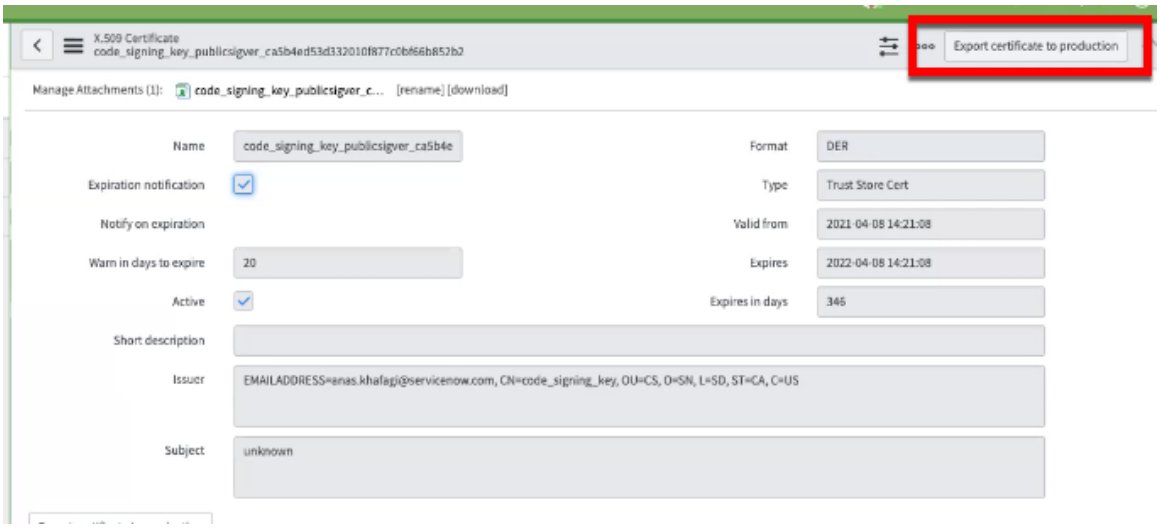
1. Dans l'environnement approuvé, accédez à **sys_certificate.liste**.



2. Ouvrez le certificat X.509 le plus récemment créé et généré avec le type **Certificat de magasin de confiance**.
   Vous devrez peut-être ajouter le champ **Créé** à la liste pour trouver l'enregistrement le plus récent. Voir Listes personnelles .
3. Sélectionnez **Exporter le certificat en production**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une signature est créée avec le certificat.

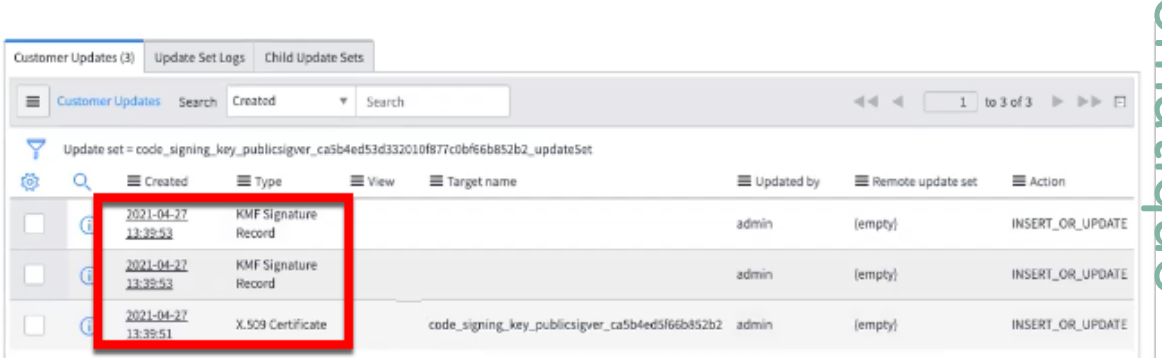
4. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
5. Recherchez et ouvrez la mise à jour de signature de code.

   Cette mise à jour commence par le texte code_signing_key_publicsigver.

   Un nouvel enregistrement d'ensemble de mises à jour de signature de code a été créé par les étapes précédentes. Pour trouver cet enregistrement, triez la liste à l'aide du champ **Créé par** et recherchez les enregistrements dans le champ **Nom** .

6. Affichez les enregistrements de signature pertinents et le certificat X.509.

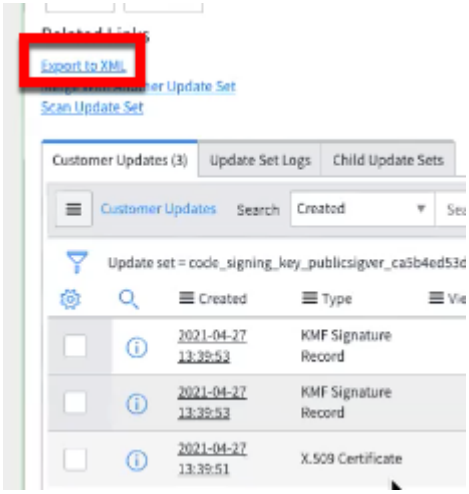
   L'ensemble de mises à jour comprend la pièce jointe pour l'enregistrement de signature, ainsi que l'entrée de la signature dans la table et le certificat.



7. Sélectionnez le lien connexe **Exporter vers XML** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Récupérez l'ensemble de mises à jour en production.
   Consultez Retrieve an update set pour en savoir plus.

> **Important :**
> Répétez ces étapes pour votre deuxième paire de clés. N'oubliez pas qu'il existe une clé pour les modules de chiffrement cm_code_attest et cm_code_signing.

Importer et installer des certificats pour le cercle de confiance

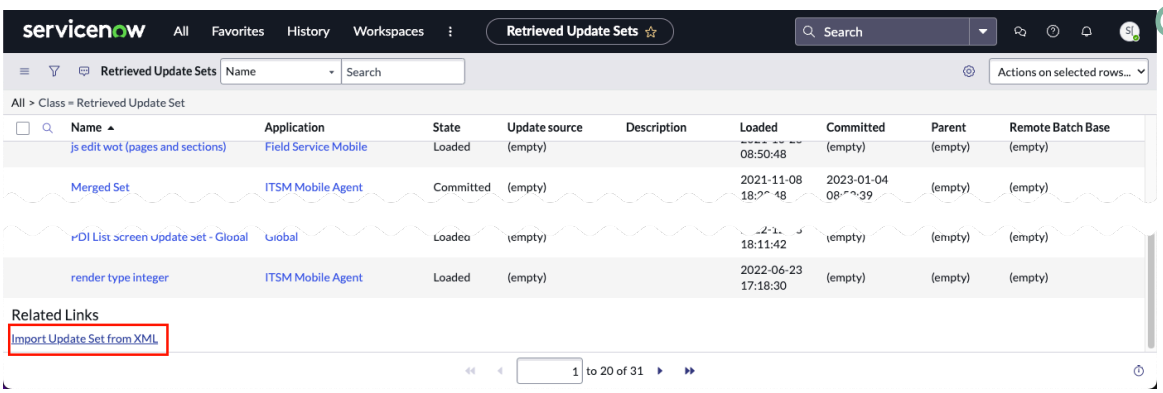
Récupérez l'ensemble de mises à jour en production pour établir la relation de confiance entre les deux instances. Les certificats qui ont été créés pour représenter la confiance dans l'instance approuvée doivent être acceptés dans l'instance de production.

Avant de commencer

Rôles requis : admin, security_admin

Procédure

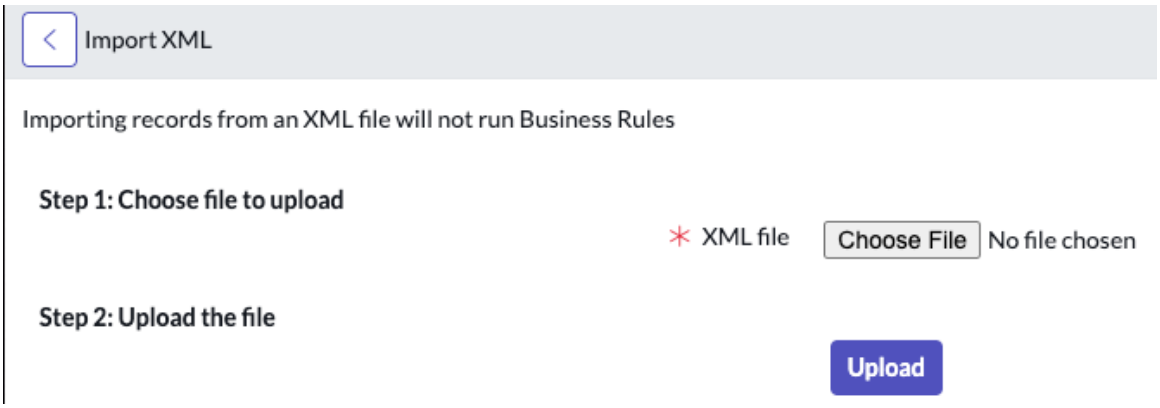
1. Dans l'instance de production, accédez à **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
2. Sélectionnez le bouton **Importer un ensemble de mises à jour à partir d'un fichier XML** dans le coin inférieur gauche de l'écran.



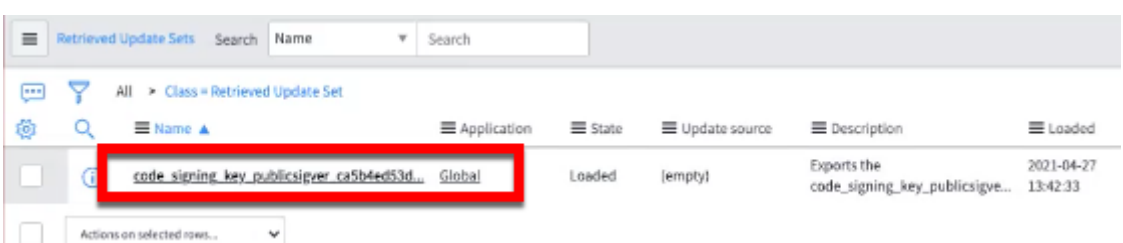
3. Sélectionnez **Choisir un fichier** et parcourez pour sélectionner le fichier XML que vous avez exporté au format Préparer les certificats du cercle de confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

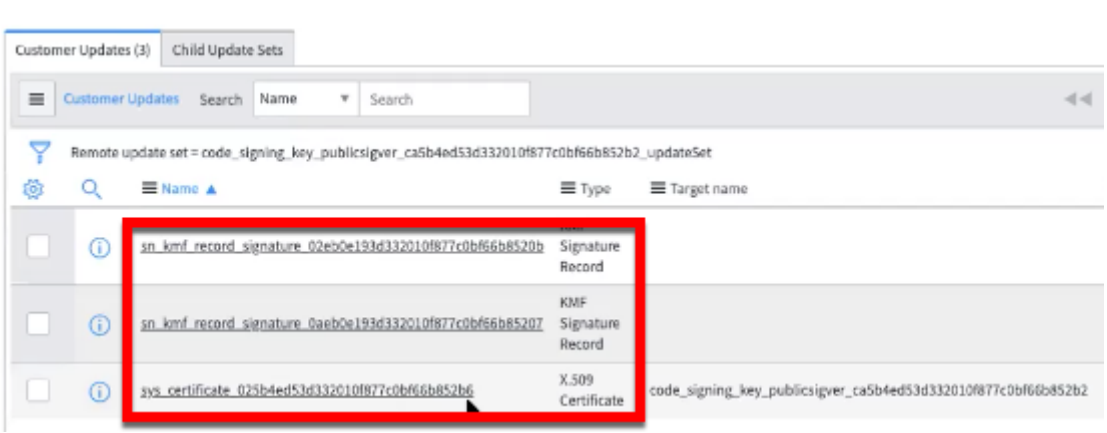


4. Sélectionnez **Charger**.
   L'ensemble de mises à jour de signature de code est ajouté à la table Ensembles de mises à jour récupérés.



Remarque :
Si vous ne voyez pas votre ensemble de mises à jour, filtrez votre liste pour les enregistrements à l'état Chargé, puis triez la liste en fonction du champ **Chargé** .

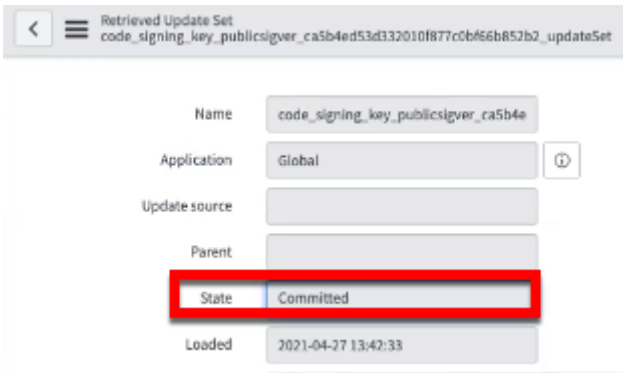
5. Ouvrez l'enregistrement de l'ensemble de mises à jour pour vérifier que la table Mises à jour du client contient les trois enregistrements suivants :
   - Deux KMF enregistrements de signature
   - Certificat X.509



6. Sélectionnez **Aperçu de l'ensemble de mises à jour**.
7. Sélectionnez **Valider l'ensemble de mises à jour**.

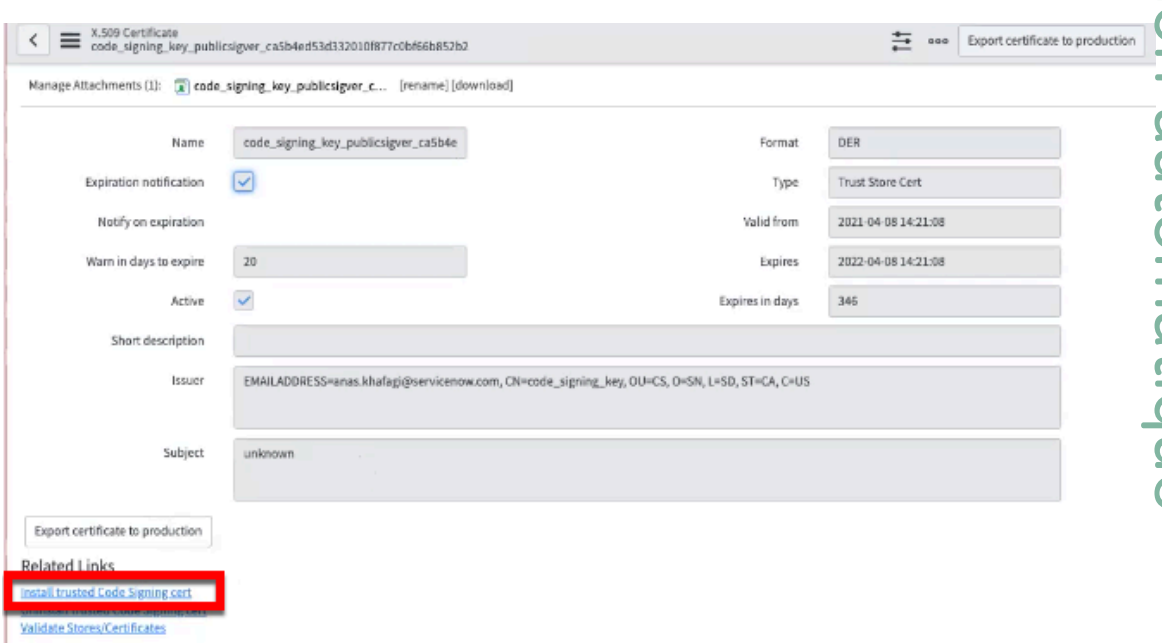
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'état de l'ensemble de mises à jour récupéré est défini sur Validé.

8. Dans le navigateur, saisissez `sn_kmf_record_signature.list` pour ouvrir la liste des **enregistrements de signatures KMF** .
9. Localisez les deux KMF enregistrements de signature.
   Ces enregistrements sont les enregistrements les plus récemment créés où le champ **Objectif de signature KMF** a la valeur `Cercle de confiance`. Vous devrez peut-être ajouter le champ **Créé** à votre liste ou filtrer les enregistrements créés à la date actuelle.
10. Dans le navigateur, saisissez `sys_certificate.list` et ouvrez l'enregistrement avec une valeur **Brève description** de *`code_signing_key`* et une valeur **Type** de certificat `de magasin de confiance`.
11. Sélectionnez **Installer le certificat de signature de code approuvé**.



Le type de certificat est mis à jour vers *`Trusted CodeSigning Cert`*.

> **Important :**
> Répétez ces étapes pour votre deuxième certificat. N'oubliez pas qu'il existe un certificat pour les modules de chiffrement cm_code_attest et cm_code_signing.

Résultats

La relation de confiance est établie entre les instances de confiance et les instances de production. Vous êtes prêt à activer la signature de code. Reportez-vous à la section Activer la signature de code pour terminer les étapes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer la signature de code

Activez la signature de code dans votre instance de non-production de confiance pour identifier les instances de confiance liées à votre instance de production.

Avant de commencer

Rôles requis : security_admin et sn_kmf.crypto_manager ou sn_kmf.admin

Avant d'activer la signature de code, vous devez contacter l'équipe Service et assistance client pour activer le module d'extension Cadre de travail de signature de code [com.glide.code_signing].

Pourquoi et quand exécuter cette tâche

Les tâches de signature de code avec des ensembles de mises à jour signés sont utilisées pour activer ou désactiver la fonctionnalité de signature de code. Il n'existe pas d'autre méthode pour cette fonctionnalité. Ce processus comprend les éléments suivants :

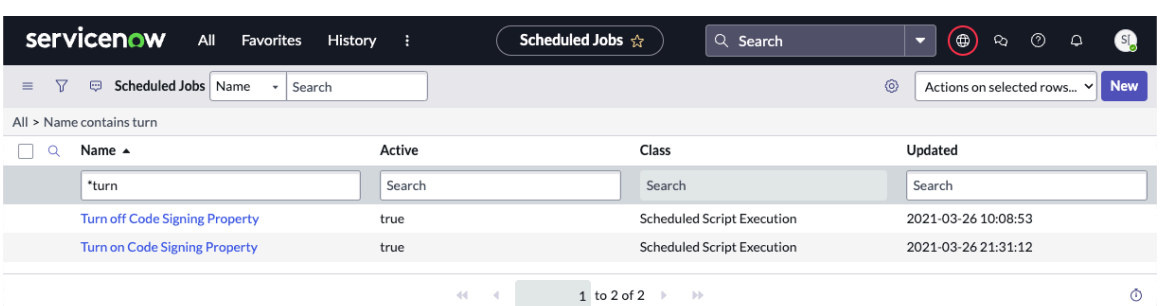
- Créez deux tâches de signature de code dans l'instance approuvée, l'une pour activer la signature de code et l'autre pour désactiver la signature de code.
  - La tâche planifiée **Activer** démarre le processus de validation du code signé par le Serveur MID.
  - La tâche **planifiée Désactiver** arrête la validation du code signé par le MID Server.

> **Remarque :**
> Lorsque vous désactivez la signature de code, la propriété système est marquée comme **faux**, mais la liste d'amis de confiance pour la signature de code est toujours disponible.

- Placer la tâche **Activer la propriété de signature de code** dans un ensemble de mises à jour.
- Mettez le travail en production.
- Utilisez la tâche **Activer la propriété de signature de code** en production si la signature provient d'une instance de confiance après vérification.

Procédure

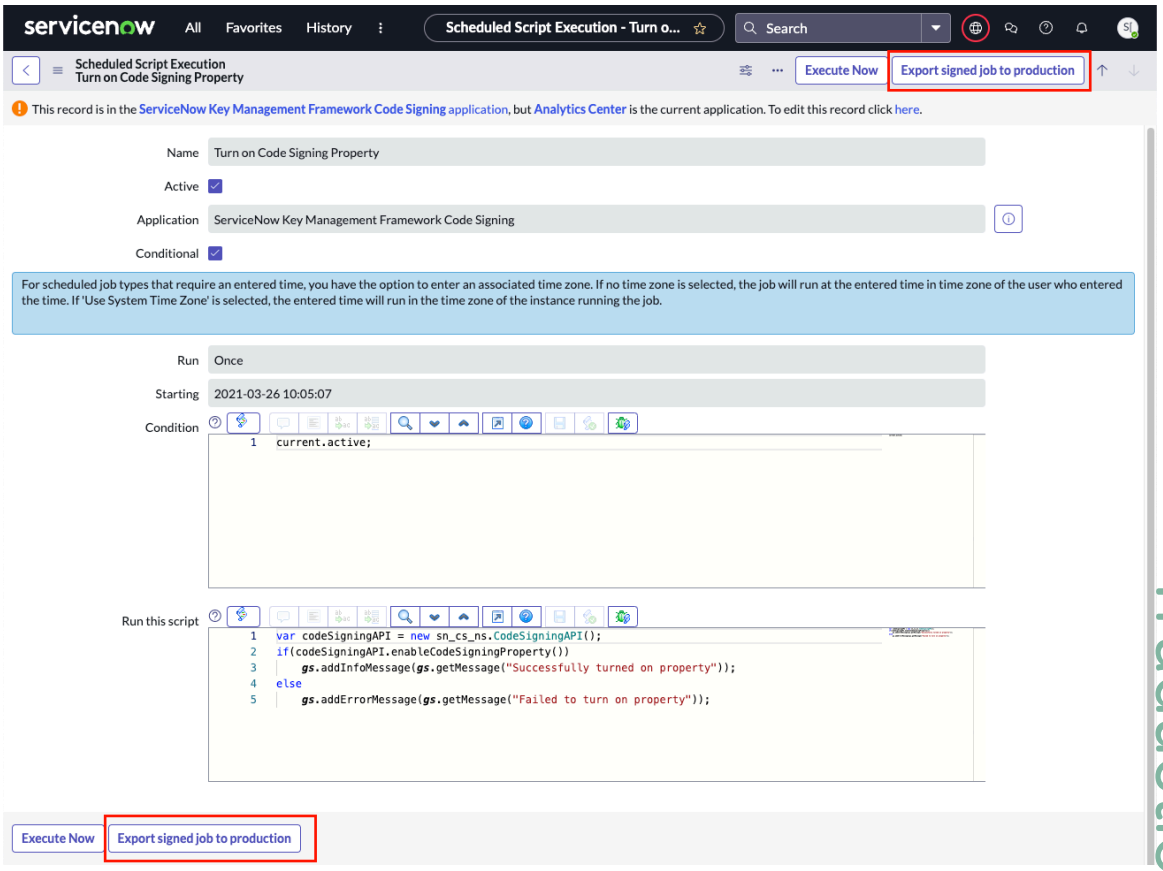
1. Dans votre instance de confiance, accédez à **Tout** > **Définition du système** > **Travaux planifiés**.
2. Recherchez « *Turn » dans le champ de nom.
3. Sélectionnez **Activer la propriété de signature de code**.



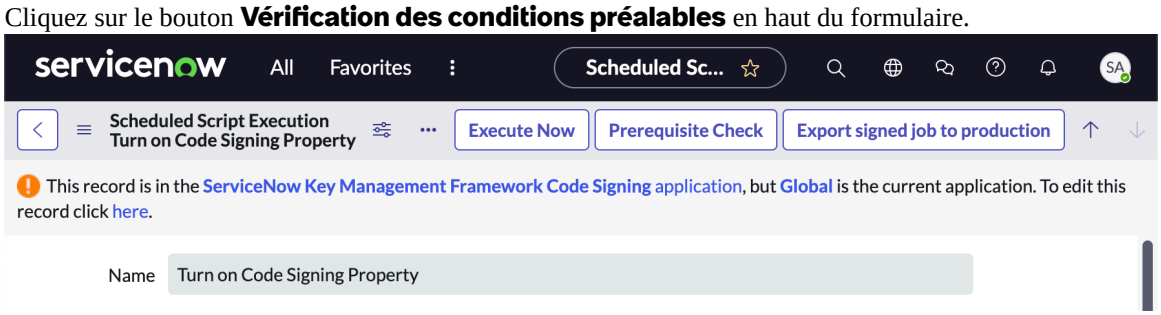
Chargement du formulaire Exécution de script planifiée. Ce formulaire contient des informations permettant d'activer la propriété Signature de code. Les tâches créent des ensembles de mises à jour qui contiennent les tâches et les signatures validées via le processus de signature de code.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Pour exécuter le script immédiatement, signez le certificat, créez l'ensemble de mises à jour et sélectionnez **Exporter la tâche de signature en production**.
   Vous pouvez également configurer le script pour qu'il s'exécute selon un calendrier désigné.
5. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
6. Ouvrez chacun des ensembles de mises à jour de la propriété de signature de code et sélectionnez **Exporter au format XML**.
7. Connectez-vous à l'instance de production.
8. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
9. Sélectionnez le bouton **Importer l'ensemble de mises à jour à partir d'un fichier XML** , puis sélectionnez l'ensemble de mises à jour de la propriété Signature de code.
10. Sélectionnez **Choisir un fichier** , puis chargez et validez les ensembles de mises à jour.
11. Revenez à la liste des travaux planifiés en accédant à **Tout** > **Définition du système** > **Travaux planifiés**.
12. Ouvrez l'enregistrement de tâche **Activer la propriété de signature de code** .
13. Cliquez sur le bouton **Vérification des conditions préalables** en haut du formulaire.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

14. Une fois la vérification des conditions préalables terminée, cliquez sur le bouton **Exécuter maintenant** . La tâche planifiée **Activer la propriété de signature de code** démarre le processus de validation du code signé sur le serveur MID.
15. Dans le navigateur, saisissez sn_kmf_record_signature.list pour ouvrir la liste des **enregistrements de signature KMF** et filtrer les enregistrements dont l'objectif de **signature KMF** est Cercle de confiance. La relation d'approbation a déplacé les tâches et, lorsque les tâches sont utilisées, le processus de vérification de signature s'exécute. Si les tâches, les signatures et les certificats font tous partie du , l'option Signature de Circle of Trustcode avec Circle of Trust peut être activée.
16. Dans le navigateur, saisissez sys_properties.list pour ouvrir la liste des propriétés système.
17. *com_snc_kmf_signature.validation.flag* Recherchez et assurez-vous que la valeur est définie sur **vrai**.
18. Vérifiez qu'une nouvelle propriété *com_snc_kmf_signature.validation.certificate* est répertoriée dans la table.

Propriétés système

com.snc.kmf.signature.validation.certifi...	{"trust_map": {"025b4ed53d332010f877c0bf6...	string	ServiceNow Key Management Framework
com.snc.kmf.signature.validation.flag	true	true | false	Global

Utilisez la Circle of Trust tâche en production pour vérifier la relation de confiance. Aucune tâche directe qui tente de signer du code ne peut être exécutée en production. Pour plus de détails sur les options de configuration, reportez-vous à la section Configuration de la signature de code

Créer des paires de clés et des certificats de signature de code

Créez deux paires de clés pour les certificats signés afin d'établir la confiance entre votre production et les instances approuvées.

Pour établir la confiance entre vos instances, vous devez créer une paire de clés et un certificat pour chacun des modules de chiffrement cm_code_attest et cm_code_signing .

La création de paires de clés et de certificats se fait à l'aide d'un outil cryptographique installé sur votre appareil local, tel que l'outil OpenSSL. Pour plus d'informations sur cet outil, reportez-vous à la section https://www.openssl.org . Si votre organisation utilise d'autres outils cryptographiques, tels que LibreSSL ou GnuTLS, reportez-vous à la documentation de ces produits pour connaître les étapes similaires.

Spécifications de la paire de clés

Les paires de clés que vous créez doivent répondre à ces exigences.

Type	RSA
Longueur de la clé	4096
Algorithme de signature	RSASSA_PKCS1_V1_5_SHA_512

Spécifications du certificat

Les certificats doivent être signés par une autorité de certification publique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Spécifier des règles personnalisées dans le pare-feu ECC

Configurez le pare-feu ECC (External communication Channel) dans votre Serveur MID en spécifiant les règles personnalisées pour autoriser ou rejeter sélectivement le message entrant et remplacer la configuration de signature de code.

Les administrateurs de sécurité peuvent utiliser les balises de pare-feu ECC pour remplacer la configuration de signature de code et autoriser ou rejeter des opérations spécifiques sur Serveur MID. Ces règles personnalisées doivent être spécifiées dans le fichier YAML de l'emplacement situé à l'adresse : agent/boot-config.yaml.

Ces balises sont spécifiques à un protocole. La configuration spécifiée pour la balise parent s'applique à la balise enfant. Par exemple, si le protocole Http est autorisé, les protocoles REST et SOAP sont également autorisés. Ce tableau présente les balises parents et enfants disponibles.

Balise parente	Balise enfant
DNS	
HTTP	• REST • SOAP
DIRECTORY_SERVICES	LDAP
SNMP	
SSH	• SCP • SFTP
JOURNAL SYSTÈME	
WINDOWS	• CIM • POWERSHELL • WMI • WINRM (en anglais seulement)
JAVASCRIPT	
GROOVY	
VCS	GIT
BASES	JDBC
DATA_SOURCES	
INTEGRATION_HUB	
ITOM	• CLOUD_PROVISIONING_GOVERNANCE • DISCOVERY • EVENT_MANAGEMENT

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Balise parente	Balise enfant
	• HEALTH_LOG_ANALYTICS • SERVICE_MAPPING
ORCHESTRATION	

Pour configurer les règles personnalisées :

1. Dans le Serveur MID, identifiez le fichier boot-config-sample.yaml.
2. Renommez le fichier YAML en boot-config.yaml et déplacez le fichier à l'emplacement : agent/boot-config.yaml.
3. Dans le fichier YAML, spécifiez les règles personnalisées et enregistrez les modifications. Un exemple du fichier YAML :

```
security:
  eccFirewall:
    mode: enforcing
    rules:
      - tags: [rest]
        action: accept
      - tags: [soap]
        action: accept
      - tags: [jdbc]
        action: reject
```

4. Redémarrez le Serveur MIDfichier .

Changer la configuration de la racine de confiance

Faites confiance à vos propres certificats et utilisez-les au lieu de vous fier ServiceNow aux certificats de version (par défaut) en modifiant pour utiliser votre racine de confiance (ROT). ServiceNow Les composants tels que les Includes de script, les règles métier, etc., sont signés au moment de la version à l'aide d'une ServiceNow clé de date de génération (le certificat de vérification est le certificat de ServiceNow version).

Modification de la racine de confiance

Pour changer la racine de confiance pour ces signatures d'enregistrements, vous devez suivre le processus de changement de racine de confiance.

- Générez et migrez un nouvel ensemble de signatures pour tous les composants fournis, à l'aide de votre certificat fourni.
- Désactivez la propriété de racine de confiance à l'aide d'une tâche planifiée.

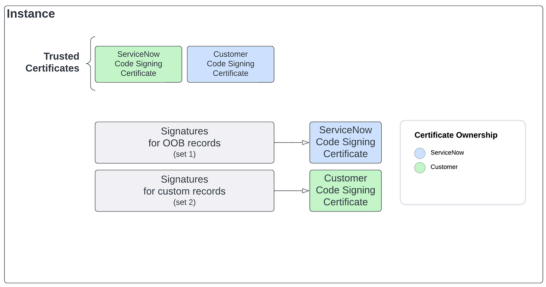
Pour en savoir plus sur ces étapes, consultez Migrer les signatures pour utiliser un certificat client et Désactiver la racine de confiance ServiceNow.

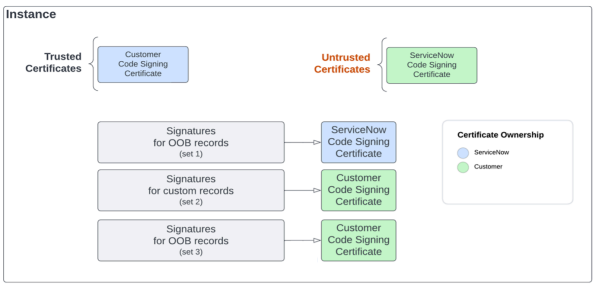
Impact sur le processus de vérification et de génération de signature

Par défaut, les certificats de version de signature de code sont approuvés pendant le processus de vérification de la signature. Une fois cette modification effectuée, votre instance accepte uniquement les signatures de votre propre certificat de signature de code.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.





Propriété ROT définie sur faux (par défaut)	Propriété ROT définie sur vrai
• Lors de la vérification, les signatures avec les certificats de build sont fiables. • Lors de la signature, si vous ne fournissez pas de clés, la clé de signature d'instance est utilisée comme clé de secours. • Le point *api/sn_kmf/signature/certificates* de terminaison REST de signature renvoie ServiceNow les certificats de version de signature de code ainsi que d'autres certificats présents sur l'instance.	• Lors de la vérification, les signatures avec les certificats de version ne sont pas fiables. • Lors de la signature, si vous ne fournissez pas les clés, la signature n'est pas effectuée. • Le point *api/sn_kmf/signature/certificates* de terminaison REST de signature exclut les ServiceNow certificats de build (San Diego, Vancouver PKI, W PKI).

Impact sur votre MID Server

Lorsque la propriété ROT est définie sur false

Si vous choisissez de laisser votre propriété ROT à sa valeur par défaut (false), il n'y a aucun impact sur votre MID Server.

Lorsque la signature de code est activée et que la propriété ROT est définie sur true

- L'API *isTrusted()* renvoie la valeur faux pour les signatures avec un certificat de build.
- L'API *isTrusted()* renvoie la valeur true pour les signatures avec votre certificat.
- L'appel d'API REST pour les certificats exclut les certificats de version.
- Vous pouvez voir des problèmes de Serveur MID, tels que des messages d'échec de validation de signature dans les journaux.

Migrer les signatures pour utiliser un certificat client

Exécutez une tâche de signature pour migrer vos signatures vers une racine de confiance (ROT) client.

Avant de commencer

Rôle requis : admin, security_admin et sn_kmf.cryptographic_manager

La signature de code doit être activée sur vos instances de production et de confiance. Vous pouvez vérifier que la propriété système **com.snc.kmf.signature.validation.flag** est définie sur true.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette procédure fait partie d'une série de procédures pour modifier une racine de confiance client (ROT) sur vos instances. Pour obtenir une vue d'ensemble de ce processus, reportez-vous à la section Changer la configuration de la racine de confiance.

Procédure

1. Connectez-vous à votre instance de production.
2. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés**.
3. Recherchez et ouvrez la **tâche planifiée ROT - Générer un ensemble de mises à jour d'enregistrements pour migrer les signatures à l'aide du certificat client** .
4. En bas du formulaire, sélectionnez **Exécuter maintenant**.
5. Accédez à la **Tout** > **Sécurité de système** > **Tâches de Sécurité** > **Créer**.
6. À l'invite, sélectionnez **Tâche de signature**.
7. Dans le formulaire **Tâche de signature** , renseignez les champs selon vos besoins.

Champ	Valeur
Nom	Créez un nom unique pour votre tâche.
Type	Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Sélectionnez l'ensemble de mises à jour créé lors des étapes précédentes. L'ensemble de mises à jour a un nom qui commence par change_root_of_trust_updateSet.

8. Cliquez avec le bouton droit sur l'en-tête du formulaire et sélectionnez **Enregistrer** pour enregistrer cet enregistrement.
9. Cliquez avec le bouton droit sur l'en-tête du formulaire et sélectionnez **Exporter** > **XML (cet enregistrement)** pour exporter cet enregistrement sous forme de fichier XML.
10. Connectez-vous à votre instance de confiance.
11. Accédez à la **Tout** > **Sécurité de système** > **Tâches de Sécurité** > **Tout**.
12. Cliquez avec le bouton droit sur l'en-tête de liste et sélectionnez **Importer XML**.
13. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé lors des étapes précédentes.
14. Sélectionnez **Charger**.
15. Dans la liste, ouvrez la tâche de sécurité importée.
16. Sélectionnez **Exporter la tâche de signature de code vers la production**.
    Cette action signe la tâche et la place dans un nouvel ensemble de mises à jour que vous pouvez importer dans votre instance de production.

> **Important :**
> Après avoir signé la tâche, vous devez effectuer les étapes suivantes dans un délai de 10 minutes. Si vous dépassez ce délai, vous pouvez resigner la tâche en suivant ces étapes, ce qui crée un autre ensemble de mises à jour signé.

17. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
18. Recherchez l'ensemble de mises à jour créé lors des étapes précédentes.
    Le nom commence par SIGN_UPDATE_SET_updateSet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

19. Sélectionnez **Exporter XML** pour exporter votre ensemble de mises à jour sous forme de fichier XML.
20. Connectez-vous à votre instance de production.
21. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
22. En bas de la liste, sélectionnez **Importer un ensemble de mises à jour à partir du code XML**.
23. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé lors des étapes précédentes.
24. Sélectionnez **Charger**.
25. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**et ouvrez l'ensemble de mises à jour en commençant par SIGN_UPDATE_SET_updateSet.
26. Sélectionnez **Aperçu de l'ensemble de mises à jour**.
27. Une fois l'aperçu terminé, sélectionnez **Valider l'ensemble de mises à jour**.
28. Accédez à la **Tout** > **Sécurité de système** > **Tâches de Sécurité** > **Tout**.
29. Ouvrez la tâche de sécurité importée.
30. Sélectionnez **Démarrer** pour exécuter la tâche de sécurité.

    Une fois la tâche de sécurité terminée, des informations sur l'état de la tâche s'affichent dans le champ **Résumé** .

    Lorsque la tâche est à l'état Terminé, toutes les signatures des enregistrements d'ensembles de mises à jour doivent utiliser le certificat fourni par le client comme certificat de vérification. Vous pouvez le vérifier dans la table Enregistrements de signatures KMF [sn_kmf_record_signature].

Que faire ensuite

Pour poursuivre le processus de configuration de la racine de confiance, reportez-vous à la section Désactiver la racine de confiance ServiceNow.

Désactiver la racine de confiance ServiceNow

Exécutez une tâche planifiée sur votre instance de non-production de confiance pour désactiver la racine de confiance.

Avant de commencer

Rôle requis : admin, security_admin et sn_kmf.cryptographic_manager

La signature de code doit être activée sur vos instances de production et de confiance. Vous pouvez vérifier que la propriété système **com.snc.kmf.signature.validation.flag** est définie sur `true`.

Cette procédure fait partie d'une série de procédures pour passer à une racine de confiance client (ROT) sur vos instances. Pour obtenir une vue d'ensemble de ce processus, reportez-vous à la section Changer la configuration de la racine de confiance.

Procédure

1. Connectez-vous à votre instance de confiance.
2. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés**.
3. Ouvrez la tâche **planifiée Désactiver la racine de confiance ServiceNow** .
4. Sélectionnez **Exporter la tâche signée vers la production**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
6. Recherchez et ouvrez l'ensemble de mises à jour **Désactiver la racine de confiance ServiceNow** .
7. Sélectionnez **Exporter XML** pour exporter votre ensemble de mises à jour sous forme de fichier XML.
8. Connectez-vous à votre instance de production.
9. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
10. En bas de la liste, sélectionnez **Importer un ensemble de mises à jour à partir du code XML**.
11. Dans le formulaire **Importer XML** , sélectionnez **Choisir un fichier** et sélectionnez le fichier XML que vous avez téléchargé lors des étapes précédentes.
12. Sélectionnez **Charger**.
13. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**et ouvrez **l'ensemble de mises à jour Désactiver la racine de confiance ServiceNow** .
14. Sélectionnez **Aperçu de l'ensemble de mises à jour**.
15. Une fois l'aperçu terminé, sélectionnez **Valider l'ensemble de mises à jour**.
16. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés**.
17. Ouvrez la tâche planifiée importée dans l'ensemble de mises à jour.
18. Sélectionnez le bouton **Exécuter maintenant** pour exécuter la tâche.

Résultats

L'exécution de la tâche planifiée définit la propriété ROT sur true. Votre instance est configurée pour utiliser la racine de confiance du client.

Utilisation de la signature de code

Découvrez comment signer des enregistrements, des messages et des pièces jointes pour vérifier l'authenticité et l'intégrité de vos données.

Signer les enregistrements de source de données JDBC dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les sources de données JDBC en activant la signature de code dans les instances de production et de confiance.

Signez les messages REST et SOAP dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les messages REST et SOAP en activant la signature de code dans les instances de production et approuvées.

Signer les flux, les flux secondaires et les actions dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les flux, les flux secondaires et les actions en activant la signature de code dans les instances de production et de confiance.

Signer des enregistrements ou des pièces jointes spécifiques

Créez une tâche de sécurité pour signer des enregistrements ou des pièces jointes spécifiques plutôt que tous les enregistrements ou pièces jointes d'une table.

Outil de signature autonome

Utilisez l'outil de signature autonome pour signer les enregistrements pris en charge dans les applications à ServiceNow l'aide de votre propre clé privée.

Traduction automatique

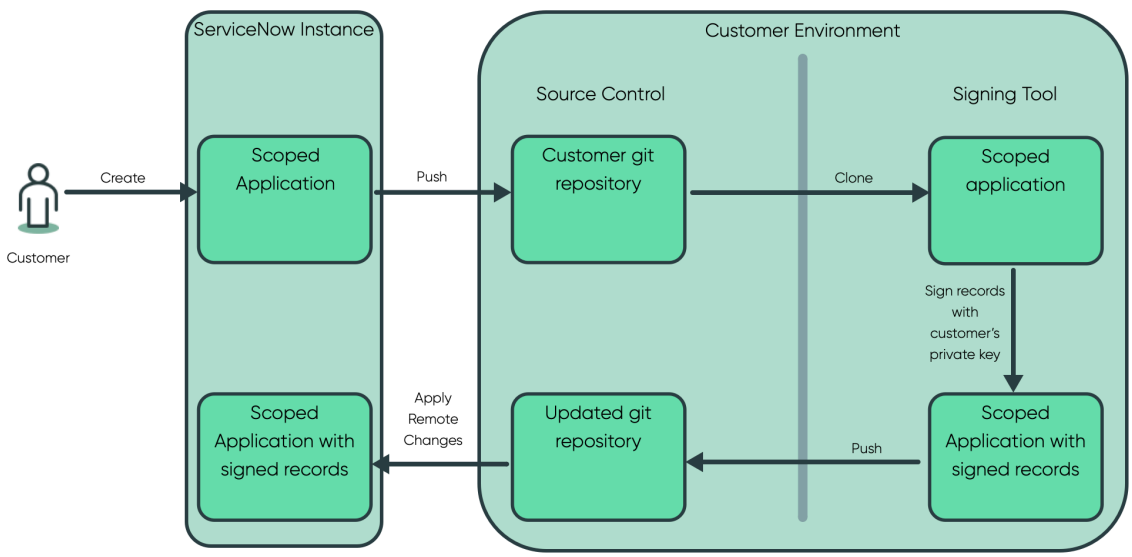
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Outil de signature autonome

Utilisez l'outil de signature autonome pour signer les enregistrements pris en charge dans les applications à ServiceNow l'aide de votre propre clé privée.

Utilisez l'outil de signature pour signer des enregistrements dans ServiceNow les applications. L'outil génère des signatures pour les enregistrements de votre environnement local à l'aide de votre propre clé privée.

Workflow de l'outil de signature



1. Créez ou sélectionnez une application existante ServiceNow avec des enregistrements à signer, tels que des règles métier ou des includes de script.
2. Transférez l'application dans votre référentiel Git, qui réside dans votre environnement.

> **Remarque :**
> Les applications peuvent être synchronisées entre un référentiel Git et votre instance à l'aide de l'intégration de contrôle de source. Pour en savoir plus sur la configuration et l'utilisation de cette intégration, reportez-vous à la section Legacy - Source Control integration .

3. Clonez l'application dans votre environnement local.
4. Utilisez l'outil de signature (également dans votre environnement local) pour signer les enregistrements pris en charge à partir de l'application clonée ServiceNow à l'aide de votre clé privée. L'outil de signature crée des enregistrements de signatures et des enregistrements de certificat X.509 [sys_certificate]. Pour en savoir plus sur l'utilisation de l'outil de signature, reportez-vous à la section Utilisation de l'outil de signature.
5. Poussez l'application mise à jour vers votre référentiel Git.
6. Dans votre instance, importez l'application mise à jour en appliquant les modifications distantes.

Utilisation de l'outil de signature

Découvrez comment utiliser l'outil de signature pour signer les enregistrements pris en charge dans ServiceNow les applications.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur

Pour effectuer ces étapes, vous devez disposer des éléments suivants :

- Une ServiceNow application qui comporte des enregistrements à signer.
- Clé privée pour signer les enregistrements.
- Le *`script signRecords.sh`* dans votre environnement local, avec l'autorisation d'exécution.

> **Important :**
> Le script *`signRecords.sh`* est inclus dans le fichier jar signing-tool, que vous devez demander à ServiceNow Service clientèle .

Procédure

1. Dans votre environnement local, accédez au répertoire contenant le script *`signRecords.sh`* .
2. Utilisez le format de commande suivant pour signer vos enregistrements :

   ```
   ./signRecords.sh -d [Path to the root directory of the ServiceNow Application to Sign] -f [Path to the Keystore file]
   ```

   Par exemple :

   ```
   ./signRecords.sh -d /users/abc/ServiceNow-App-1 -f /users/abc/codesigning.p12
   ```

3. Si vous y êtes invité, entrez le mot de passe du magasin de clés.
   Appuyez sur Entrée s'il n'y a pas de mot de passe.
4. Examinez la sortie pour confirmer une signature réussie.

   ```
   Sep 26, 2022 2:41:09 PM com.snc.java.commands.ACommand start
   INFO: CODESIGN: executing codesigning...
   Sep 26, 2022 2:41:09 PM com.snc.core.codesigning.CodeSignerSupplier get
   INFO: CODESIGN: signing record for documentId: 65e811327702111057416efe7c5a994f
   Sep 26, 2022 2:41:11 PM com.snc.java.commands.ACommand start
   INFO: CODESIGN: codesigning successfully completed!
   ```

   Dans l'exemple de sortie précédent, l'outil de signature a utilisé le fichier de magasin de clés fourni pour signer l'enregistrement. Vous pouvez également voir que :

   - Le script a trouvé un enregistrement pris en charge `65e811327702111057416efe7c5a994f` et l'a signé.
   - Dans le répertoire ServiceNow-App-1, deux enregistrements ont été créés : `sys_certificate.xml` et `sn_kmf_record_signature.xml`.
5. Importez à nouveau l'application mise à jour dans votre instance en appliquant les modifications distantes dans Studio.
   Pour plus d'informations, consultez Legacy - Apply remote changes .

Arguments de l'outil de signature

Découvrez les arguments disponibles pour l'outil de signature.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Arguments de ligne de commande

Argument	Obligatoire	Description
-d	Oui	Répertoire racine du projet à signer. Doit contenir le répertoire de projet (aléatoire 32 caractères alphanumériques), un fichier sn_source_control.properties et un fichier <project_name>.iml
-f	Oui	Chemin d'accès au fichier du magasin de clés.
-a	Non	Alias utilisé pour accéder à une entrée spécifique dans le magasin de clés.
-c	Non	Concaténer les signatures d'enregistrement dans un seul fichier.
-k	Non	Mot de passe permettant d'accéder à la clé stockée dans le magasin de clés. Vous pouvez également saisir ce mot de passe lorsque vous y êtes invité plutôt que dans l'argument.
-o	Non	Signez avec un nouveau certificat à la place de tout fichier sys_cert existant.
-p	Non	Mot de passe permettant d'accéder au magasin de clés s'il possède un mot de passe. Vous pouvez également saisir ce mot de passe lorsque vous y êtes invité plutôt que dans l'argument.
-w	Non	Effacer tous les fichiers d'enregistrement de signature existants.
-h	Non	Affichez ce message d'aide et quittez.

Signer les enregistrements de source de données JDBC dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les sources de données JDBC en activant la signature de code dans les instances de production et de non-production approuvées.

- Établissez Circle of Trust un lien entre les instances de production et les instances approuvées.
- Rôle requis : sécurité_admin

Remarque :

- Serveur MID ne gère pas les sources de données du fichier et, par conséquent, ces sources de données ne sont pas signées par code.
- Les sources de données LDAP ne peuvent pas être signées par code.

Signer les sources de données existantes du type JDBC

Utilisez des ensembles de mises à jour pour apporter des tâches de signature en masse à l'instance de production.

Avant de commencer
Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans l'instance de non-production approuvée, configurez la tâche de signature KMF pour signer les sources de données.

   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.

   b. Cliquez sur **Nouveau**.

   c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Enregistrements de signature en masse**.
Table	Table à partir de laquelle les enregistrements doivent être signés. Sélectionner **la source de données**.

   d. Cliquez sur **Exporter la tâche de signature de code vers la production**.
   Un message de confirmation s'affiche pour indiquer que l'ensemble de mises à jour est signé.

   e. Exportez l'ensemble de mises à jour généré vers un fichier XML.

2. Dans l'instance de production, importez et validez l'ensemble de mises à jour pour récupérer les tâches signées en masse à partir de l'instance de confiance.

   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.

   b. Ouvrez l'ensemble de mises à jour exporté à partir de l'instance approuvée.

   c. Cliquez sur **Démarrer**.
   Un message de confirmation s'affiche pour indiquer que les enregistrements sont signés.

Signer de nouvelles sources de données du type JDBC

Utilisez des ensembles de mises à jour pour apporter l'ensemble de mises à jour signé à l'instance de production.

Avant de commencer

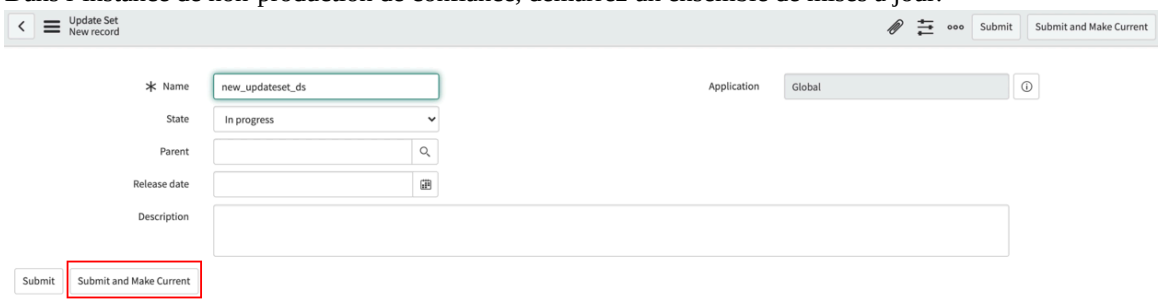
Rôle requis : sn_kmf.cryptographic_manager

Traduction automatique

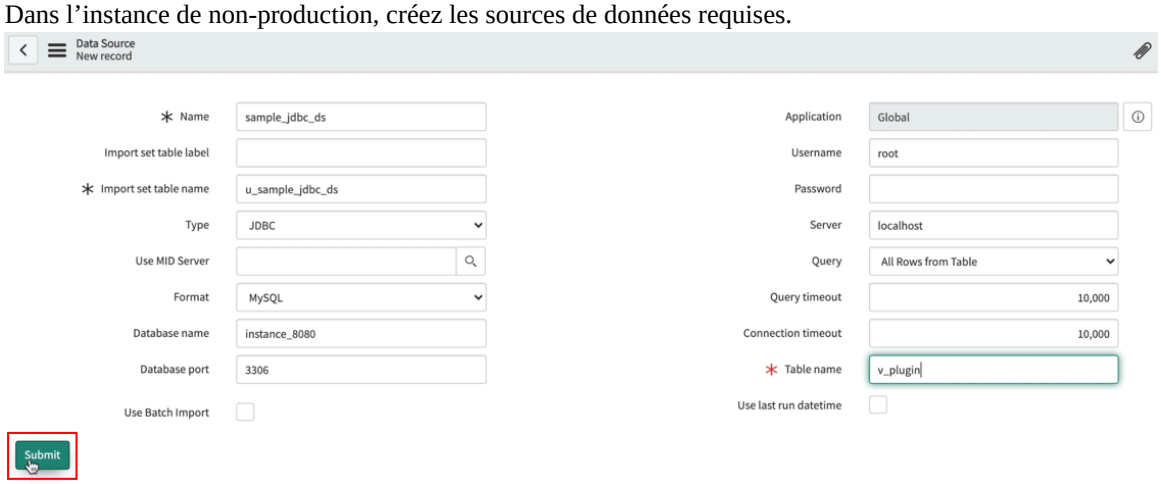
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans l'instance de non-production de confiance, démarrez un ensemble de mises à jour.

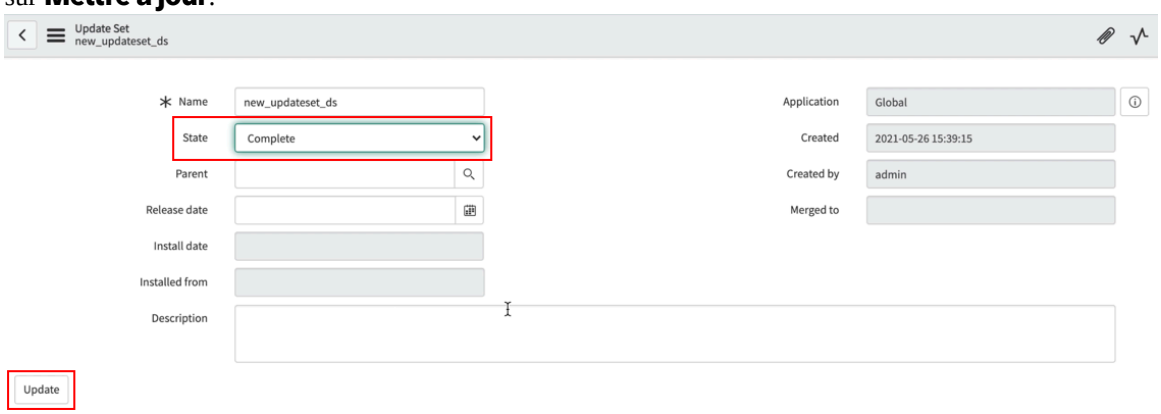


2. Dans l'instance de non-production, créez les sources de données requises.



Les sources de données sont ajoutées à l'ensemble de mises à jour.

3. Dans l'instance de non-production, définissez l'état de l'ensemble de mises à jour sur **Terminé** , puis cliquez sur **Mettre à jour**.



4. Dans l'instance de non-production, signez l'ensemble de mises à jour en créant une tâche de chiffrement.

   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.

   b. Cliquez sur **Nouveau**.

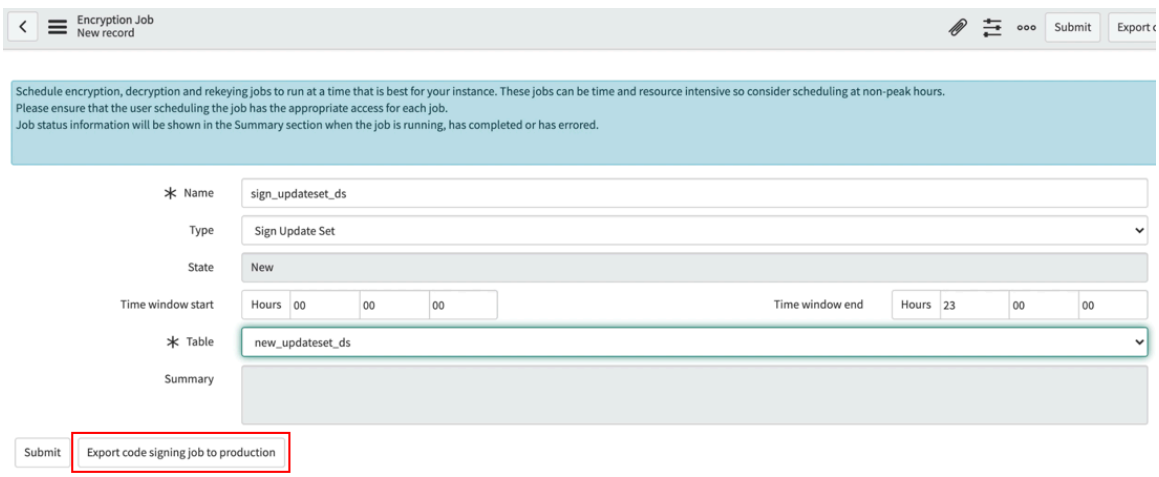
   c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.

Traduction automatique

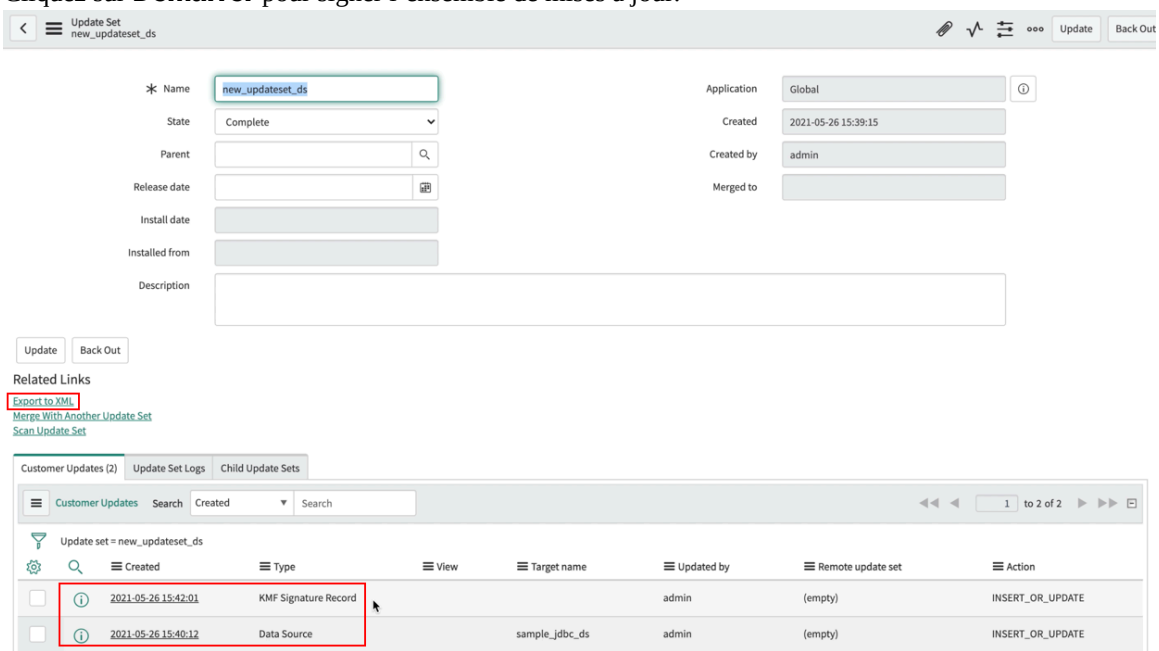
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type	Type de la tâche de chiffrement. Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Ensemble de mises à jour à partir duquel les enregistrements doivent être signés.



d. Cliquez sur **Envoyer**.

e. Cliquez sur **Démarrer** pour signer l'ensemble de mises à jour.



- **Le résumé** est mis à jour et les enregistrements sont signés.
- L'ensemble de mises à jour est mis à jour et inclut la signature.

5. Dans l'instance de non-production, ouvrez l'enregistrement d'ensemble de mises à jour signé et exportez-le au format XML.

6. Dans l'instance de production, importez l'ensemble de mises à jour signé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.

b. Cliquez sur le lien connexe **Importer un ensemble de mises à jour à partir d'un fichier XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance de confiance.
Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
L'ensemble de mises à jour est validé avec succès.

Signez les messages REST et SOAP dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les messages REST et SOAP en activant la signature de code dans les instances de production et de non-production .

Avant de commencer

- Établir Circle of Trust entre les instances de production et de non-production.
- Rôle requis : security_admin

Signer les messages REST et SOAP existants

Signez et validez les messages REST et SOAP existants en activant la signature de code dans les instances de production et de non-production approuvées.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance de confiance, configurez la tâche de signature KMF pour signer les actions d'interface utilisateur.

   a. Accédez à la configuration de signature KMF.

   b. Renseignez ces valeurs sur le formulaire.

Formulaire de configuration de signature KMF

Champ	Description
Nom de la table	Nom de table Glide. Par exemple, sélectionnez **Actions d'interface utilisateur [sys_ui_action].**
Objectif de signature KMF	But de la signature des enregistrements. Sélectionnez **File d'attente ECC**.
Champs de génération de signature	Champs de la source de données que vous souhaitez signer. Si des modifications sont apportées aux valeurs d'un ou de plusieurs de ces champs, la signature générée précédemment devient non valide. Sélectionnez **un nom** et **un script**.
Filtre de génération de signature	Critères de filtre qui doivent être remplis pour signer les enregistrements.
Signer la pièce jointe	Option permettant de signer la pièce jointe dans l'enregistrement Glide.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Clé d'instance	Option permettant d'utiliser la clé d'instance.

c. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.

2. Dans l'instance de confiance, signez les enregistrements requis.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.

b. Cliquez sur **Nouveau**.

c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Enregistrements de signature en masse**.
Table	Table à partir de laquelle les enregistrements doivent être signés. Sélectionnez **Action d'interface utilisateur**.

d. Cliquez sur **Exporter la tâche de signature de code vers la production**.
Deux ensembles de mises à jour signés localement sont créés.

- Un ensemble de mises à jour pour la configuration de l'action d'interface utilisateur.
- Un autre ensemble de mises à jour de la tâche de chiffrement pour exporter la tâche de signature de code.

3. Dans l'instance de confiance, exportez l'ensemble de mises à jour local vers un fichier XML.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.

b. Ouvrez l'ensemble de mises à jour que vous avez créé pour la signature en masse des enregistrements.

c. Cliquez sur le lien connexe **Exporter vers XML** et enregistrez le fichier XML.

4. Dans l'instance de production, importez les ensembles de mises à jour.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.

b. Cliquez sur le lien connexe **Importer un ensemble de mises à jour à partir d'un fichier XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance de confiance.
Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
L'ensemble de mises à jour est validé avec succès.

5. Dans l'instance de production, exécutez la tâche de chiffrement que vous avez créée précédemment dans l'instance approuvée en sélectionnant **Démarrer**.
Un message de confirmation s'affiche indiquant que les enregistrements sont signés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signer de nouveaux messages REST et SOAP

Signez et validez les nouveaux messages REST et SOAP de l'instance approuvée en activant la signature de code dans les instances de production et approuvées.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Dans l'instance de non-production de confiance, démarrez un ensemble de mises à jour.
2. Dans l'instance de non-production approuvée, créez les messages REST ou SOAP requis.
   Les messages sont ajoutés à l'ensemble de mises à jour.
3. Dans l'instance de non-production, définissez l'état de l'ensemble de mises à jour sur **Terminé** , puis cliquez sur **Mettre à jour**.
4. Dans l'instance de non-production, signez l'ensemble de mises à jour en créant une tâche de chiffrement.
   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.
   b. Cliquez sur **Nouveau**.
   c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Ensemble de mises à jour à partir duquel les enregistrements doivent être signés. **Sélectionner Signer un nouvel ensemble de mises à jour REST V2 - 1**.

   d. Cliquez sur **Envoyer**.
   e. Cliquez sur **Démarrer** pour signer l'ensemble de mises à jour.
      - **Le résumé** est mis à jour et les enregistrements sont signés.
      - L'ensemble de mises à jour est mis à jour et inclut la signature.
5. Dans l'instance de non-production, ouvrez l'enregistrement d'ensemble de mises à jour signé et exportez-le au format XML.
6. Dans l'instance de production, importez l'ensemble de mises à jour.
   a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.
   b. Sélectionnez le lien connexe **Importer l'ensemble de mises à jour à partir du XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance approuvée.
   Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
   L'ensemble de mises à jour est validé avec succès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signer les flux, les flux secondaires et les actions dans l'instance de production

Utilisez des ensembles de mises à jour pour signer et valider les flux, les flux secondaires et les actions en activant la signature de code dans les instances de production et de confiance.

- Établissez Circle of Trust un lien entre les instances de production et les instances approuvées.
- Rôle requis : security_admin

Signer le flux, les flux secondaires et les actions existants

Signez et validez le flux, les flux secondaires et les actions existants en activant la signature de code dans les instances de production et de non-production approuvées.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance de confiance, signez les enregistrements de la table d'instance d'étape.
   a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.
   b. Cliquez sur **Nouveau**.
   c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Enregistrements de signature en masse**.
Table	Table à partir de laquelle les enregistrements doivent être signés. Sélectionnez **l'instance d'étape**.

   d. Cliquez sur **Exporter la tâche de signature de code vers la production**.
   Deux ensembles de mises à jour signés localement sont créés.
   - Un ensemble de mises à jour pour la signature KMF.
   - Un autre ensemble de mises à jour de la tâche de chiffrement pour exporter la tâche de signature de code.
2. Dans l'instance de confiance, exportez l'ensemble de mises à jour local vers un fichier XML.
   a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**.
   b. Ouvrez l'ensemble de mises à jour que vous avez créé pour la signature en masse des enregistrements.
   c. Cliquez sur le lien connexe **Exporter vers XML** et enregistrez le fichier XML.
3. Dans l'instance de production, importez le fichier XML.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.

b. Cliquez sur le lien connexe **Importer un ensemble de mises à jour à partir d'un fichier XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance de confiance.
Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
L'ensemble de mises à jour est validé avec succès.

4. Dans l'instance de production, exécutez la tâche de chiffrement que vous avez créée précédemment dans l'instance approuvée.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.

b. Ouvrez la tâche de chiffrement que vous avez créée précédemment dans l'instance approuvée.

c. Cliquez sur **Démarrer** pour démarrer la tâche.
Un message de confirmation s'affiche indiquant que les enregistrements sont signés.

Signer un nouveau flux, des flux secondaires et des actions

Signez et validez les nouveaux flux, flux secondaires et actions en activant la signature de code dans les instances de production et de non-production approuvées.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Dans l'instance de confiance, démarrez un ensemble de mises à jour.
2. Dans l'instance approuvée, créez les flux, flux secondaires ou actions requis et publiez-les.
Les flux, les flux secondaires ou les actions sont ajoutés à l'ensemble de mises à jour.
3. Dans l'instance de confiance, modifiez l'état de l'ensemble de mises à jour sur **Terminé** , puis cliquez sur **Mettre à jour**.
4. Dans l'instance de confiance, signez l'ensemble de mises à jour en créant une tâche de chiffrement.

a. Accédez à la **Sécurité de système** > **Tâches de Sécurité** > **Tout**.

b. Cliquez sur **Nouveau**.

c. Renseignez ces valeurs sur le formulaire.

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement.
Type	Type de la tâche de chiffrement. Sélectionnez **Signer l'ensemble de mises à jour**.
Table	Ensemble de mises à jour à partir duquel les enregistrements doivent être signés.

d. Cliquez sur **Envoyer**.

e. Cliquez sur **Démarrer** pour signer l'ensemble de mises à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Le résumé** est mis à jour et les enregistrements sont signés.
- L'ensemble de mises à jour est mis à jour et inclut la signature.

5. Dans l'instance de confiance, ouvrez l'enregistrement d'ensemble de mises à jour signé et exportez-le au format XML.
6. Dans l'instance de production, importez l'ensemble de mises à jour signé.

   a. Accédez à la **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés**.

   b. Sélectionnez le lien connexe **Importer l'ensemble de mises à jour à partir du XML** pour importer l'ensemble de mises à jour exporté à partir de l'instance approuvée.
   Pour plus d'informations, consultez Importer et valider l'ensemble de mises à jour de démarrage rapide.
   L'ensemble de mises à jour est validé avec succès.

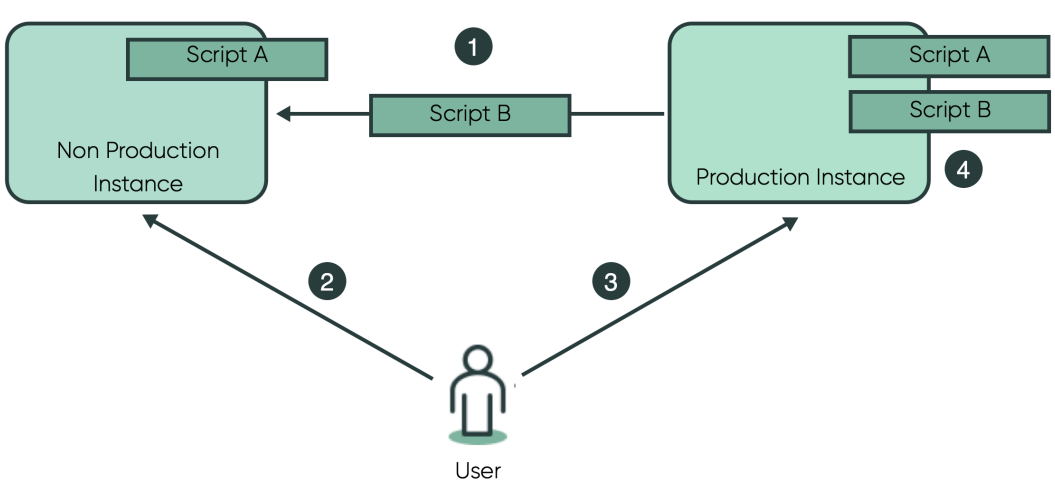
Signer des enregistrements ou des pièces jointes spécifiques

Créez une tâche de sécurité pour signer des enregistrements ou des pièces jointes spécifiques plutôt que tous les enregistrements ou pièces jointes d'une table.

À partir de la Vancouver version, les administrateurs de sécurité peuvent utiliser des tâches de sécurité pour signer des enregistrements spécifiques sur une table plutôt que tous les enregistrements d'une table. Signez des enregistrements spécifiques pour éviter de signer accidentellement un code non révisé.

Ces tâches incluent un fichier journal joint qui est généré à la fin de la tâche de signature. Ce fichier journal contient des informations sur les enregistrements signés et la configuration de signature utilisée.

Processus de signature



Ce diagramme montre un exemple d'utilisation du processus de signature. Dans cet exemple, un script, intitulé Script B , n'existe que sur l'instance de production et doit être importé dans une instance de confiance pour être signé. Le script A existe déjà sur les deux instances, il n'a pas besoin d'être signé. Soit il a déjà été examiné et signé, soit il n'a pas encore été examiné et ne doit pas être signé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Importez l'enregistrement dans votre environnement de confiance.
2. Dans l'instance de confiance, créez une tâche de signature pour signer l'enregistrement. Ce processus est détaillé dans la section Créer une tâche pour signer des enregistrements ou des pièces jointes spécifiques sur une instance de confiance.
3. Importez la tâche de signature signée dans votre instance de production à l'aide d'un ensemble de mises à jour.
4. Dans l'instance de production, exécutez la tâche de signature importée.

Créer une tâche pour signer des enregistrements ou des pièces jointes spécifiques sur une instance de confiance

Signez un enregistrement spécifique ou un groupe d'enregistrements que vous définissez sur une instance de non-production de confiance.

Avant de commencer

Rôle requis : security_admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Tâches de Sécurité** > **Créer**.
2. À **l'invite Quel type de tâche de sécurité voulez-vous créer ?** , sélectionnez **Tâche de signature**. Un nouvel enregistrement **de tâche de signature** s'affiche.
3. Dans le formulaire, renseignez les champs selon vos besoins :

Champs de la tâche de signature

Champ	Description
Nom	Nom descriptif de cette tâche.
Type	Type de tâche de sécurité. Pour signer des enregistrements spécifiques, sélectionnez l'option **Signer des enregistrements spécifiques** . Pour signer des pièces jointes spécifiques, sélectionnez **Signer des pièces jointes spécifiques**.
État	État de cette tâche. Ce champ commence par la valeur **Nouveau**. Ce champ est en lecture seule.
Table	Table contenant les enregistrements ou les pièces jointes que vous souhaitez signer. Si vous signez des pièces jointes, sélectionnez la table contenant des enregistrements auxquels les pièces jointes sont associées, et non la table Pièce jointe [sys_attachment]. **Conseil :** Vérifiez la table d'enregistrement de signature [sn_kmf_record_signature] du cadre de travail de gestion des clés (KMF) pour vous assurer qu'il n'y a pas déjà de signatures pour la table que vous avez sélectionnée.
Filtrer les enregistrements	Conditions de filtre utilisées pour limiter les enregistrements qui s'affichent dans la table **Sélectionner des enregistrements à signer** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner les enregistrements à signer	Liste des enregistrements de la table sélectionnés dans le champ **Table** , limitée par filtre créé dans le champ **Enregistrements de filtre** . Déplacez les enregistrements de la fenêtre **Disponible** vers la fenêtre **Sélectionnée** pour les inclure dans la tâche de signature.
Début de la fenêtre de temps	Début de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécutera après l'heure saisie dans ce champ. Une valeur de temps valide est exprimée en temps universel coordonné sur la base d'une notation temporelle de 24 heures.
Fin de la fenêtre de temps	Fin de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécute avant l'heure saisie dans ce champ. Si la tâche n'est pas encore terminée, elle sera mise en pause et reprendra au prochain début de la fenêtre horaire. L'heure de fin doit être postérieure à l'heure de début. Une valeur de temps valide est exprimée en temps universel coordonné sur la base d'une notation temporelle de 24 heures.
Résumé	Résumé de l'exécution de cette tâche. Ce champ est en lecture seule.

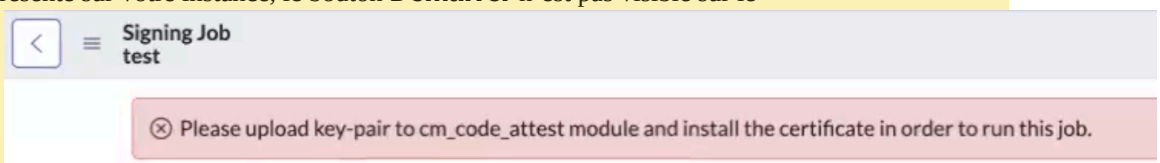
4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
5. En bas du formulaire, sélectionnez **Exporter la tâche de signature de code vers la production**.
   Cette action signe la tâche de signature et elle est prête pour l'exportation.
6. Accédez à la **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour locaux**
7. Recherchez et ouvrez l'ensemble de mises à jour pour votre tâche de signature.
   Dans l'onglet Mises à jour client, vous pouvez voir que cet ensemble de mises à jour inclut la tâche de signature et l'enregistrement de signature.
8. Sélectionnez **Exporter vers XML**.
   Cette action crée un fichier XML contenant votre ensemble de mises à jour sur votre appareil local.
9. Sur votre instance de production, accédez à **Tout** > **Ensembles de mises à jour système** > **Ensembles de mises à jour récupérés** > **.**
10. En bas de la page, sélectionnez **Importer un ensemble de mises à jour à partir du code XML**.
11. Sélectionnez le bouton **Choisir un fichier** , puis sélectionnez le fichier XML créé lors des étapes précédentes.
12. Sélectionnez **Charger**.
    Votre ensemble de mises à jour est chargé et apparaît dans la liste **Ensembles de mises à jour récupérés** .
13. Dans la liste **Ensembles de mises à jour récupérés** , ouvrez l'enregistrement de votre ensemble de mises à jour importé.
14. Sélectionnez le bouton **Aperçu de l'ensemble de mises à jour** .
    Une fois l'aperçu terminé, le bouton **Valider l'ensemble de mises à jour** apparaît.
15. Sélectionnez **Valider l'ensemble de mises à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

16. **Tout** > **Sécurité de système** > **Tâches de Sécurité** > **Tout**.
17. Ouvrez votre tâche de signature.
18. Sélectionnez **Démarrer** pour exécuter la tâche de signature.

> **Avertissement :**
> Si la paire de clés n'a pas été chargée dans votre instance de production, un avertissement s'affiche en haut du formulaire d'enregistrement. Si cette paire de clés n'est pas présente sur votre instance, le bouton **Démarrer** n'est pas visible sur le formulaire.



Que faire ensuite

Une fois terminé, le champ **Résumé** affiche les résultats de la tâche. Un fichier journal est également joint à votre enregistrement de travail de signature nommé « Mass_Sign_Records-<sys_id> ». Examinez cet enregistrement pour plus de détails sur la tâche et une liste de sys_ids pour chaque enregistrement signé.

Référence de signature de code

Les rubriques de référence fournissent des informations supplémentaires pour gérer et résoudre les problèmes liés à la signature de code.

Propriétés installées avec Signature de code

La signature de code ajoute les propriétés suivantes.

Dépannage et accès aux journaux

Accédez à divers journaux pour résoudre les problèmes et identifier les causes des défaillances.

Propriétés installées avec Signature de code

La signature de code ajoute les propriétés suivantes.

Propriété	Type	Description
com.glide.codesigning.expanded.tracking.enabled	true|false	Si la valeur est vrai, la longueur de validation de la pile meta est augmentée pour ecc_queue rubriques répertoriées dans la propriété **com.glide.codesigning.expanded_tracking.topic.list** . **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.glide.codesigning.expanded.tracking.length	Entier	Niveaux de validation de signature de code à produire lorsque la signature de code est activée. La valeur par défaut est de 3.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Type	Description
		Important : Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.glide.codesigning.expanded_tracking.topic_list	Chaîne	Liste séparée par des virgules des rubriques devant faire l'objet d'un suivi accru de la pile meta. **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.glide.codesigning.tracking.agent.validation_exclusion.list	Chaîne	Liste séparée par des virgules des agents ecc_queue pour lesquels la signature de code doit être ignorée
com.glide.codesigning.tracking.debug	true|false	Si la valeur est vrai, la journalisation de débogage pour le suivi de la signature de code est activée.
com.glide.codesigning.tracking.enabled	true|false	Si la valeur est vrai, active le suivi de l'appelant par signature de code. **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.glide.codesigning.tracking.logging.enabled	true|false	Si la valeur est vraie, active la journalisation pour le suivi de la signature de code.
com.glide.codesigning.tracking.unsupported_script_tracking.enabled	true|false	Si la valeur est vrai, les enregistrements ecc_queue insérés via des scripts non pris en charge (si détectés) ne sont pas notarisés. **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.glide.codesigning.tracking.validation.fail_fast	true|false	Si vrai, la vérification de la signature de code échoue au premier échec de validation du script au lieu de vérifier tous les scripts. **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.glide.event_handler.code_signing.tracking	Chaîne	Définit le gestionnaire d'événements qui permet de s'assurer que les clients qui viennent d'activer la signature de code sont

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Type	Description
		configurés pour être aussi sécurisés que possible. **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.glide.web_service_outbound.impl.codesigning.tracking	true|false	Si vrai, active le suivi de signature de code SOAPMessageV2 **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
com.snc.csf.servicenow_root_of_trust.désactivé	true|false	Indique si la fonctionnalité de racine de confiance est active. La valeur par défaut est `faux`, ce qui signifie que ServiceNow les certificats de version sont approuvés. **Important :** Cette propriété ne peut être modifiée qu'à l'aide d'une tâche planifiée signée par un utilisateur ayant les rôles d'administrateur, d'administrateur de sécurité et de gestionnaire KMF. Pour en savoir plus sur la modification de votre racine de confiance, reportez-vous à la section Changer la configuration de la racine de confiance.
com.snc.kmf.signature.validation.optin	true|false	Si la valeur est vrai, active la signature de code sur votre instance. **Important :** Cette propriété ne peut être modifiée que via une requête à Service et assistance client. Pour plus d'informations, consultez KB1205749
glide.jdbcprobeloader.tracking	true|false	Active ou désactive la signature de code pour les sources de données JDBC. **Important :** Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.
glide.rest.codesigning.tracking	true|false	Si la valeur est vrai, active le suivi de signature de code RESTMessageV2.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Type	Description
		Important : Un niveau de sécurité élevé est nécessaire pour modifier cette propriété.

Rôles installés avec Signature de code

La signature de code inclut les rôles suivants.

Administrateur de signature de code [codesigning_admin]

Utilisez le rôle d'administrateur de signature de code pour affecter des rôles codesigning_manager et codesigning_auditor à d'autres utilisateurs.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

Gestionnaire de signature de code [codesigning_manager]

Utilisez le rôle de gestionnaire de signature de code pour créer et mettre à jour la configuration de signature, ainsi que pour créer et exécuter des tâches de signature de code.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Aucun.

Auditeur de signature de code [codesigning_auditor]

Utilisez le rôle d'auditeur de signature de code pour afficher les configurations de signature et les tâches de signature. Le rôle d'auditeur n'a pas d'accès en création ni en écriture aux ressources de signature de code.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

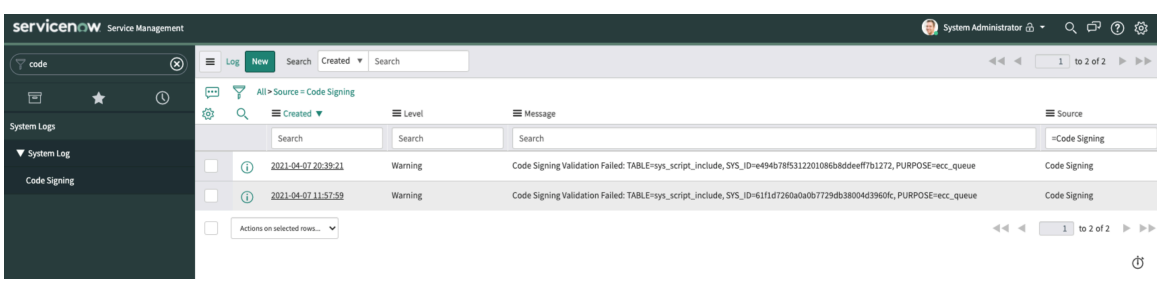
Aucun.

Dépannage et accès aux journaux

Accédez à divers journaux pour résoudre les problèmes et identifier les causes des défaillances.

Journaux de signature de code

Si l'un des enregistrements de file d'attente ECC n'est pas signé par l'API de suivi de signature de code, les messages non signés et les détails requis sont affichés dans le module de signature de code. Accédez à la **Journaux Système** > **Journal système** > **Signature de code** pour accéder à la liste des enregistrements qui ne sont pas approuvés.



Pour des journaux de nœud de débogage supplémentaires, activez *com.glide.codesigning.tracking.debug* et définissez sa valeur sur vrai.

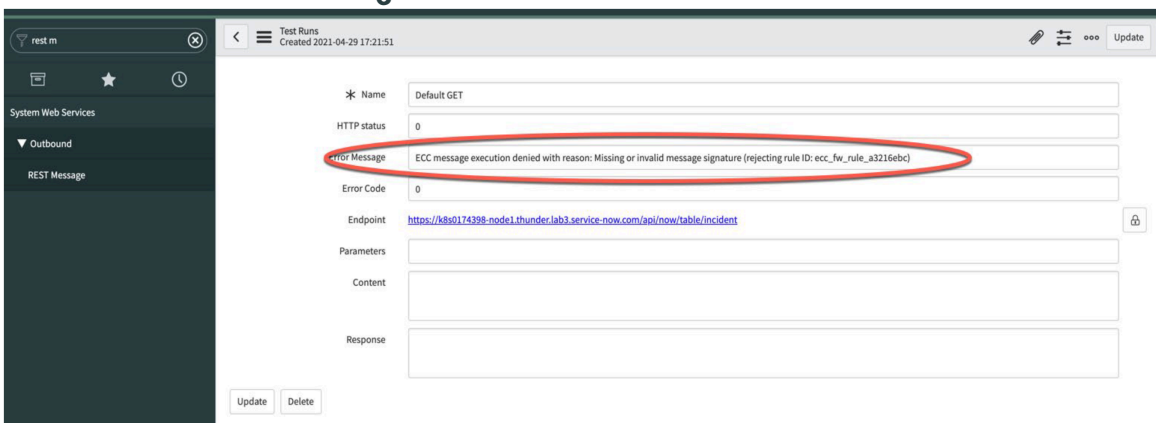
Échec de la validation de la signature du message REST sur Serveur MID

Accédez au message d'erreur relatif à l'échec de validation de la signature en accédant à **Services web du système** > **Sortant** > **Message REST** et l'ouverture de l'enregistrement de message REST requis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

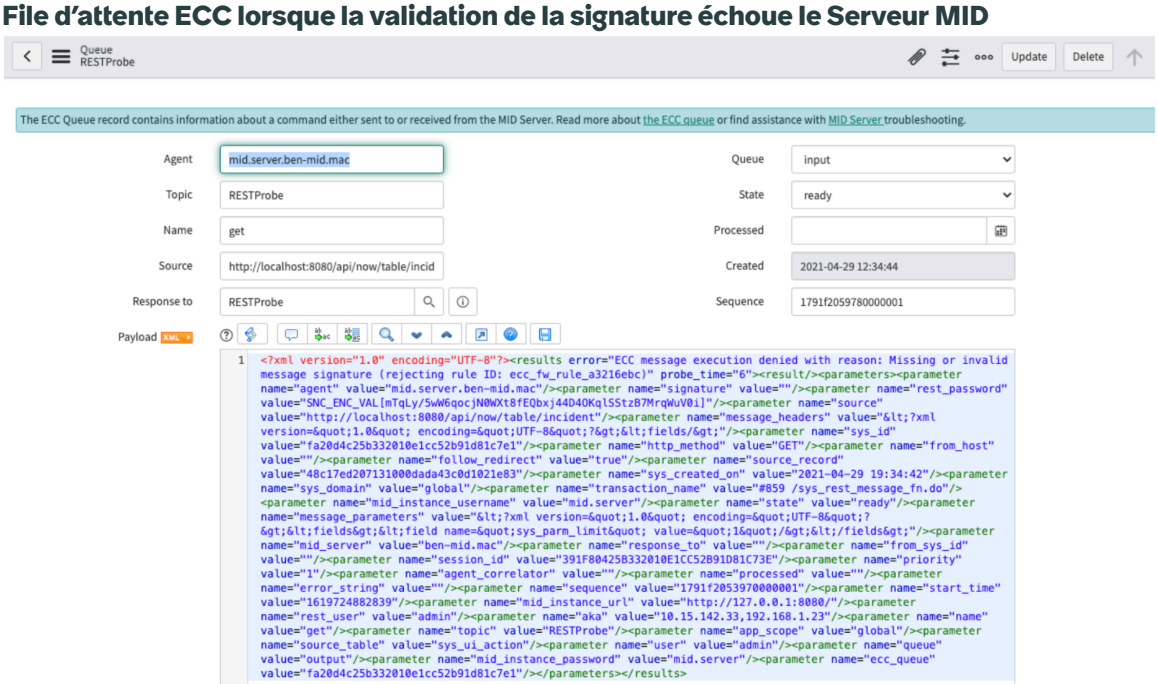
Échec de la validation de la signature sur Serveur MID



Remarque :

Les messages d'erreur associés aux rejets de pare-feu ECC commencent par Exécution du message ECC refusée.

File d'attente ECC lorsque la validation de la signature échoue le Serveur MID



Message d'erreur lorsque le message ECC est bloqué par la règle d'utilisateur



Traduction automatique

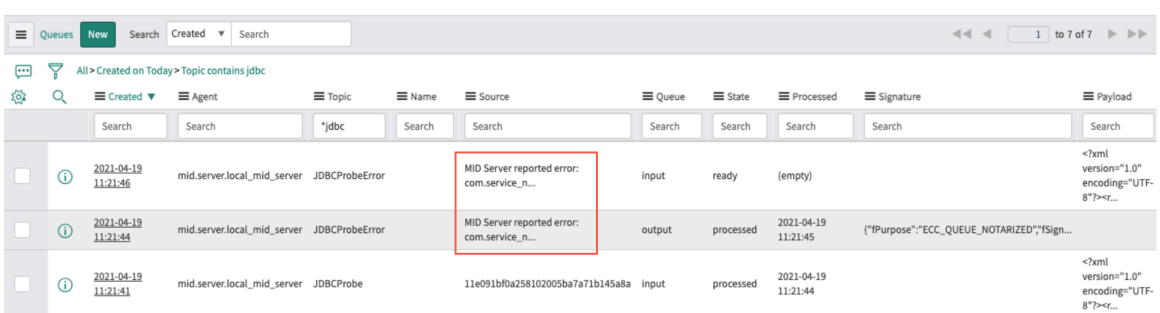
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sonde JDBC

Lorsqu'une source de données JDBC avec une signature non valide ou manquante est exécutée sur un Serveur MID, un message d'erreur contenant les détails requis s'affiche.



Source affiche également les détails du message d'erreur.



Serveur MID Journaux

Pour activer la journalisation détaillée du pare-feu ECC, augmentez le niveau de journalisation en définissant la valeur du paramètre de configuration du serveur MID, `mid.log.level`, sur TRACE. Les journaux détaillés fournissent des informations sur :

- Règles chargées Serveur MID à partir du fichier de configuration de démarrage.
- Trace d'exécution granulaire des règles.
- Règle spécifique en raison de laquelle un message ECC doit être accepté ou rejeté.

Remarque :
Si boot-config.xml n'est pas valide, les Serveur MID échecs de démarrage et les détails de l'échec sont consignés dans les journaux de l'agent MID.

Analyse anti-virus

Utilisez Analyse anti-virus pour protéger votre instance contre les virus que les pièces jointes de fichiers peuvent introduire dans vos enregistrements système, notamment les incidents, les problèmes et les stories.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découvrir l’analyse antivirus



Découvrez la valeur de l’analyse antivirus.

Configurer la protection antivirus



Comprendre comment configurer la protection antivirus.

Résoudre les fichiers infectés



Découvrez ce qu’il faut faire avec les fichiers infectés.

Référence pour l’analyse antivirus



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration de l'analyse antivirus

Utilisez Analyse anti-virus pour protéger votre instance contre les virus que les pièces jointes de fichiers peuvent introduire dans vos enregistrements système, notamment les incidents, les problèmes et les stories.

Analyse anti-virus Analyse les pièces jointes stockées dans votre tableau de pièces jointes [sys_attachment] pour aider à protéger les utilisateurs contre le chargement et le téléchargement de fichiers infectés. Tous les types de documents pris en charge par la plateforme sont analysés par Antivirus Scanning.

Le Protection antivirus module d'extension (com.glide.snap) est activé par défaut sur votre instance. En tant qu'administrateur, vous pouvez désactiver et réactiver la Analyse anti-virus fonctionnalité sur l'ensemble de votre instance d'une simple activation, définir les options de configuration et examiner l'activité antivirus sur l'instance.

Remarque :

- Analyse anti-virus est également disponible pour les clients dans l'environnement Government Community Cloud (GCC) et commercial. Les utilisateurs doivent définir la propriété (com.glide.snap.fed_enable_scan) sur Vrai pour commencer à utiliser cette fonctionnalité.
- Les protocoles de communication HTTP et HTTPS sont pris en charge.
- Les fichiers chiffrés Edge sont exclus de cette analyse.
- Les définitions antivirus sont mises à jour tous les jours.
- Les fichiers d'une taille supérieure à 100 Mo ne sont pas analysés.

Analyse des e-mails et des pièces jointes

Les e-mails entrants sont analysés à la recherche de virus par les filtres de messagerie système, et non par Analyse anti-virus.

Par défaut, seules les pièces jointes attachées à zz_yylive_profile tables sont analysées. Pour analyser d'autres tables ayant un type **de colonne file_attachment** créez la propriété `com.glide.snap.scan.zz_yytables` système et insérez le nom de la table.

Si les noms des tables sont zz_yyincident et zz_yycase, la valeur de la propriété doit être `zz_yyincident,zz_yycase`.

Une fois cette propriété définie, les pièces jointes des tables zz_yyincident et zz_yycase sont analysées.

Scénarios d'analyse

Passez en revue ces scénarios de chargement et de téléchargement pour comprendre comment le système identifie les menaces de sécurité potentielles à partir des fichiers joints à vos enregistrements.

Scénario 1 : charger un fichier

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. L'utilisateur télécharge sans le savoir un fichier infecté dans un enregistrement.
2. Le système analyse le fichier et le met en quarantaine.
3. Le fichier apparaît dans la fenêtre Pièces jointes, où il est marqué comme non disponible.
4. L'utilisateur sélectionne le fichier et le message d'erreur suivant s'affiche : Le fichier Infected_testing.txt n'a pas réussi l'analyse de sécurité. Veuillez supprimer le fichier du INC0000059 de l'enregistrement et réessayer.
5. Le système envoie une notification par e-mail à l'utilisateur et à l'administrateur antivirus.
6. L'utilisateur ferme la fenêtre Pièces jointes et retourne à l'enregistrement. Le fichier infecté s'affiche dans l'en-tête comme indisponible. Exemple : infected_testing123.txtZ [non disponible].

Scénario 2 - Télécharger un fichier

1. L'utilisateur ouvre un enregistrement pour télécharger un fichier qui lui est joint.
2. Ignorant que le fichier est infecté, l'utilisateur le sélectionne pour le téléchargement.
3. Le système analyse le fichier, le place en quarantaine et affiche un message similaire à Le fichier infected_testing123.txt n'a pas réussi l'analyse de sécurité et ne peut pas être téléchargé.
4. L'utilisateur ferme le message et l'écran s'actualise pour indiquer que le fichier n'est pas disponible.
5. Le système envoie une notification par e-mail à l'utilisateur et à l'administrateur antivirus.

Scénario 3 - Télécharger un fichier ZIP

1. Un utilisateur ouvre un enregistrement et télécharge un fichier ZIP qui lui est joint.
2. Le système analyse les fichiers ZIP individuellement.
3. Un fichier ne passe pas l'analyse de sécurité et est marqué comme indisponible. Les fichiers restants sont compressés et téléchargés avec succès.
4. L'utilisateur ouvre le fichier ZIP et voit un fichier « error.txt » en plus du fichier téléchargé avec succès. Ce fichier contient un message d'erreur spécifiant quel fichier n'a pas réussi l'analyse et n'a donc pas été inclus dans le ZIP.
5. L'utilisateur ouvre à nouveau l'enregistrement et constate que le fichier indisponible a été déplacé dans la section **Risques de sécurité potentiels** de la fenêtre Pièces jointes et qu'il ne peut pas être téléchargé.

Configurer Analyse anti-virus

Configurez Analyse anti-virus sur l'ensemble de votre instance et au niveau de la table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : antivirus_admin ou admin

Pourquoi et quand exécuter cette tâche
Analyse anti-virus est actif par défaut dans votre instance, où il analyse automatiquement les pièces jointes pour identifier les fichiers infectés par des virus. Configurez la fonctionnalité en vous assurant que l'analyse est activée sur l'ensemble de votre instance et en identifiant toutes les tables que vous souhaitez exclure de l'analyse.

Procédure
1. Accédez à la **Tout** > **Antivirus** > **Configuration**.
2. Lors de la configuration de la fonctionnalité, tenez compte des éléments suivants.

3. Sélectionnez **Enregistrer**.
4. Excluez les tables de l'analyse antivirus en les ajoutant à la **liste des tables exclues**.
   a. Accéder à la **définition du système** # **au dictionnaire**
   b. Recherchez la table que vous souhaitez exclure de l'analyse et sélectionnez la table dont le type est défini sur collection.
   c. Dans l'onglet **Attributs** , sélectionnez **Nouveau**.
   d. Ajoutez `Exclude_from_antivirus_scan` dans le champ Attributs et entrez `Vrai` dans le champ **Valeur** .
   e. Sélectionnez **Soumettre**.

Résultats
Analyse anti-virus est activé dans votre instance et la **liste des tables exclues de** la page Configuration antivirus est renseignée avec toutes les tables que vous avez exclues de l'analyse.

Examen des fichiers mis en quarantaine

Examinez les pièces jointes mises en quarantaine et prenez des mesures supplémentaires si nécessaire.

Avant de commencer
Rôle requis : antivirus_admin ou admin

Pourquoi et quand exécuter cette tâche
Surveillez vos entrées de fichiers en quarantaine dans la page Quarantaine antivirus à intervalles réguliers pour effectuer l'une des actions suivantes.

Procédure
1. Accédez à la **Tout** > **Antivirus** > **Quarantaine**.
2. Cochez la case en regard de chaque entrée en quarantaine sur laquelle vous souhaitez effectuer une action disponible.
3. Sélectionnez la liste déroulante **Actions sur les lignes sélectionnées** dans la bannière pour choisir l'action à effectuer sur l'entrée en quarantaine de la ligne sélectionnée.

Résultats
Le système demande une confirmation et effectue l'action sélectionnée en fonction de votre entrée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Centre de sécurité de l'instance

Mesures antivirus

Examen de l’activité antivirus

Examinez le journal des activités antivirus qui suit toutes les activités qui se produisent sur les fichiers potentiellement infectés à partir du moment où ils sont découverts et placés en quarantaine.

Avant de commencer

Rôle requis : antivirus_admin ou admin

Pourquoi et quand exécuter cette tâche

Ce journal fonctionne comme un rapport qui capture l’activité de l’antivirus, telle que la détection, la suppression et d’autres événements possibles de fichier mis en quarantaine.

Procédure

1. Accédez à la **Tout** > **Antivirus** > **Activité**.
2. Passez en revue le journal des fichiers mis en quarantaine.
   Vous pouvez afficher les actions effectuées dans la colonne Événement pour chaque fichier mis en quarantaine.

Que faire ensuite

Déterminez les enregistrements que vous souhaitez supprimer, restaurer, télécharger ou conserver dans le journal. Voir Examiner les fichiers mis en quarantaine

Connaître les attributs de dictionnaire pour Analyse anti-virus

Les attributs de dictionnaire modifient le comportement de la table ou de l’élément décrit par l’enregistrement de dictionnaire. En tant qu’administrateur, vous pouvez définir les valeurs des attributs de dictionnaire pour modifier le comportement de la configuration par défaut d’Analyse antivirus.

Attributs de dictionnaire pour Analyse anti-virus

Nom	Valeur	Élément cible	Description
Exclude_from_antivirus_scan	vrai/faux	n’importe quelle table	Si vrai, les pièces jointes de fichier de la table sont exclues de l’analyse antivirus. Reportez-vous à la rubrique Configurer Analyse anti-virus.
Supress_antivirus_email_notification	vrai/faux	n’importe quelle table	Si vrai, arrête d’envoyer des notifications par e-mail générées par la plateforme lorsqu’un fichier potentiellement infecté est identifié.
Suppress_antivirus_ui_notification	vrai/faux	n’importe quelle table	Si vrai, arrête les notifications d’interface utilisateur générées par la plateforme lorsqu’un

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attributs de dictionnaire pour Analyse anti-virus (suite)

Nom	Valeur	Élément cible	Description
			fichier potentiellement infecté est identifié.

Information associée

Altering tables and fields using dictionary attributes

Assainisseur HTML

Supprimez tout code indésirable et protégez-vous contre les problèmes de sécurité tels que les attaques de script site à site en assainissant le balisage HTML dans les champs HTML et les champs HTML traduits.

Explorez l’assainisseur HTML



Découvrez comment fonctionne l’assainisseur HTML.

Configurer l’assainisseur HTML



Configurez l’assainisseur HTML.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer l’assainisseur HTML



Découvrez comment activer l’assainisseur HTML.

Exploration de l’assainisseur HTML

Supprimez tout code indésirable et protégez-vous contre les problèmes de sécurité tels que les attaques de script site à site en assainissant le balisage HTML dans les champs HTML et les champs HTML traduits.

Utilisez l’assainissement HTML pour vous assurer que le contenu HTML de votre instance ne contient pas de contenu potentiellement dangereux. L’assainissement HTML fonctionne en supprimant les balises HTML susceptibles de compromettre votre instance, telles que `<![CDATA[<script>]]>`, `<link>`ou `<embed>` les balises qui peuvent être utilisées pour exécuter des scripts indésirables sur votre instance ou diriger vos utilisateurs vers du contenu indésirable. Les balises sûres qui contrôlent la mise en forme de votre contenu sont préservées. En tant qu’administrateur, vous pouvez personnaliser le contenu supprimé ou conservé. Vous pouvez également contrôler si l’assainissement s’applique à tout le contenu ou uniquement aux champs que vous spécifiez.

L’assainisseur HTML fonctionne en vérifiant la liste d’inclusion intégrée pour le balisage que vous souhaitez toujours conserver. L’assainisseur fournit l’include de script `HTMLSanitizerConfig` que les administrateurs peuvent utiliser pour modifier la liste d’inclusion intégrée. Les éléments peuvent également être ajoutés à la liste d’exclusion pour supprimer le balisage HTML. Le contenu de la liste d’exclusion remplace la liste d’inclusion.

Les types d’éléments suivants peuvent être ajoutés aux listes d’inclusion et d’exclusion :

- Attributs globaux
- Tous les éléments HTML

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Par défaut, les attributs d'URL tels que `href` et src ne prennent en charge que les protocoles suivants :

- `http`
- `https`
- `mailto`
- `données`

Par exemple :

```
<a href="https://community.servicenow.com/community">ServiceNow Community</a>
```

Remarque :
Pour en savoir plus sur la propriété qui contrôle l'utilisation de l'assainisseur HTML, consultez Assainisseur HTML Paramètres de renforcement de la *`glide.html.sanitize_all_fields`* sécurité de l'instance.

Configurer urlAttributes et les protocoles

Vous pouvez configurer urlAttributes et leurs protocoles dans l'include de script **HTMLSanitizer** . Par exemple :

```
HTML_WHITELIST : {
urlAttributes: { "protocols" : [ "file", "notes" ] },
          - -
          - -
    }
```

Étant donné que les `notes` se trouvent dans la liste d'inclusion dans cet exemple, cette URL n'est pas nettoyée :

```
<a title="Lotus"
 href="Notes://
ABC/X575C90019DE33/ABC594DCB76D86EB4925653E0011C4C1/ZZ90B7E2D33964749257EE
A003456FD">Lotus</a></p>
```

Liste d'inclusion par défaut

Remarque :
La liste d'inclusion par défaut est une liste système et n'est pas accessible aux utilisateurs dans l'instance.

```
BUILTIN_HTML_WHITELIST :{

   globalAttributes:{ attribute:["id","class","lang","title","style"],

                          attributeValuePattern:{}},

   label:{ attribute:["for"]},

   font:{ attribute:["color","face","size"]},

   a:{ attribute:["href","nohref","name","shape"]},

   img:{ attribute:["src","name","alt","border","hspace","vspace","align","height","width"},
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
   table:{ attribute:["border","cellpadding","cellspacing","bgcolor","background","align","no
 resize","height","width","summary","frame","rules"]},


 th:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},


 td:
{ attribute:["background","bgcolor","abbr","axis","headers","scope","nowrap","height","width","al
ign","valign","char off","char","colspan","rowspan"]},

   tr:{ attribute:["background","height","width","align","valign","char off","char"]},

   thead:{attribute:["align","valign","char off","char"]},

   tbody:{attribute:["align","valign","char off","char"]},

   tfoot:{attribute:["align","valign","char off","char"]},

   colgroup:{attribute:["align","valign","char off","char","span","width"]},

   col:{attribute:["align","valign","char off","char","span","width"]},

   p:{attribute:["align"]},

   style:{attributeValuePattern:{"type":"text/css"}}

   canvas:{ attribute:["height","width"]},

   details:{ attribute:["open"]},

   summary:{ attribute:["open","valign","char off","char"]},

   button:{ attribute:["disabled","accesskey","type"]},

   form:{},


 input:{ attribute:["size","maxlength","checked","alt","src","type","disabled","readonly","accessk
ey","border","usemap"]},

   select:{ attribute:["disabled","multiple","size"]},

   textarea:{ attribute:["rows","cols","disabled","readonly","accesskey"]},

   option:{ attribute:["disabled","label","selected"]},

   div:{ attribute:["align"]},

   ol:{ attribute:["start","type","square"]},

   ul:{ attribute:["type","square","itemscope","itemtype","itemref"]},

   li:{ attribute:["value","fb__id","itemprop"]},
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
span:{ attribute:["color","size","data-mce-bogus","itemprop","face"]},

br:{ attribute:["clear"]},

h3:{ attribute:["itemprop"]},

html:{ attribute:["xmlns","lang","xml:lang"]},

link:{ attribute:["rel","type","href","charset"]},

meta:{ attribute:["name","content","scheme","charset","http-equiv"]},

pre:{ attribute:["xml:space"]},

noscript:{},  h1:{},  h2:{},  h4:{},  h5:{},  h6:{},

i:{},  b:{},  u:{},  strong:{},  em:{},  small:{},  big:{},

pre:{},  code:{},  cite:{},  samp:{},  sub:{},  sup:{},

strike:{},  center:{},  blockquote:{},  hr:{},  map:{},

dd:{},  dt:{},  dl:{},  fieldset:{},  legend:{}, figure:{},  tt:{},

body:{},  caption:{},  head:{},  title:{},  shape:{},},
```

Configuration de l'assainisseur HTML

Vous devez modifier un include de script pour apporter des changements de configuration à l'assainisseur HTML.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Includes de script**.
2. Ouvrez **HTMLSanitizerConfig**.
3. Pour ajouter des éléments à la liste d'exclusion, utilisez la classe HTML_BLACKLIST.

   Pour ajouter des éléments à la liste d'inclusion, utilisez la classe HTML_WHITELIST.

   Utilisez ce format :

```
HTML_XXXXLIST :{
      globalAttributes :{

         attribute:[attribute-name1,...],
         attributeValuePattern:{ attribute-name2:attribute-value-regex-pattern,...}

      },<html-element-name>:{// Same as Above},----}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *globalAttributes* contient des éléments attribute ou attributeValuePattern qui s'appliquent globalement à tous les éléments HTML.
- *attribute* est une liste d'attributs séparés par des virgules.
- *attributeValuePattern* est un dictionnaire d'attribut pour les paires attribute-value-regex-pattern. Le modèle attribute-value-regex est une expression régulière qui doit correspondre à la valeur de l'attribut.

Example:
Prenons l'exemple suivant :

```
HTML_WHITELIST:{
      globalAttributes:{
         attribute:["id","name"],},
      img:{
         attribute:["style","align"],
         attributeValuePattern:{src:".*jpeg"}},
      iframe:{},}
```

Il ajoute les éléments suivants à la liste d'inclusion :

- ID et nom des attributs globaux. Il s'agit d'une liste de chaînes qui peuvent être appliquées globalement à tous les éléments.
- Élément img dans lequel les attributs sont style et align.
- L'élément img où l'attribut source de l'image est un fichier avec l'extension .jpeg. Il s'agit d'un exemple de modèle d'expression régulière qui correspond à une valeur d'attribut.
- L'élément iframe.

Activation de l'assainisseur HTML

L'assainisseur HTML fournit une propriété permettant d'activer ou de désactiver l'assainisseur pour tous les champs HTML du système.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Par défaut, cette propriété est définie sur true pour les nouvelles instances.

Procédure

1. Dans le filtre de navigation, saisissez sys_properties.list.
2. Définissez les propriétés *glide.html.sanitize_all_fields* et *glide.translated_html.sanitize_all_fields* sur **vrai**.

> **Remarque :**
> Pour en savoir plus sur cette propriété, reportez-vous Assainisseur HTML à la section Paramètres de sécurisation renforcée de la sécurité de l'instance.

Trouble?

Si les propriétés n'existent pas dans la table Propriétés système, vous pouvez les ajouter.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activation de l'assainissement sur les champs individuels

Vous pouvez utiliser des attributs de champ pour activer ou désactiver l'assainisseur sur des champs individuels.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Vous devez d'abord définir la propriété d'assainisseur sur faux, puis activer l'assainisseur pour chaque champ pour n'importe quel formulaire.

Procédure

1. Accédez à la table sys_properties et définissez la *glide.html.sanitize_all_fields* sur **faux**.
   Cela désactive l'assainisseur pour tous les champs HTML du système.
2. Accédez au formulaire qui contient le champ HTML.
3. Cliquez avec le bouton droit sur l'étiquette du champ HTML, puis sélectionnez **Configurer le dictionnaire**.
   Le formulaire Entrée du dictionnaire s'ouvre pour le champ HTML.
4. Entrez l'un des éléments suivants dans le champ Attributs :
   - Pour désactiver l'assainissement, entrez `html_sanitize=false`
   - Pour activer l'assainissement, saisissez `html_sanitize=true`
5. Cliquez sur **Mettre à jour**.
6. Pour activer l'assainisseur HTML pour les champs HTML traduits, définissez la *glide.translated_html.sanitize_all_fields* propriété **sur vrai**.

Activation de la connexion de l'assainisseur HTML

Lorsque l'assainisseur HTML supprime des éléments ou des attributs, ils sont ajoutés au journal système.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Vous pouvez examiner ces éléments atténués en ajoutant /syslog_list.do ?sysparm_query=source%3DHTMLSanitizer à l'URL de votre instance.

Procédure

1. Pour examiner ces éléments nettoyés, ajoutez `/syslog_list.do ?sysparm_query=source %3DHTMLSanitizer` à l'URL de votre instance.
2. Pour activer ou désactiver la connexion, ajoutez la propriété `glide.html_sanitize.discarded_log.enable` aux propriétés système et définissez la valeur sur **vrai** (activé) ou **faux** (désactivé).
   Cette propriété est par défaut définie sur **true**.

Audit

Suivez les modifications d'enregistrement sur les tables activées devant faire l'objet d'un audit. Par défaut, le système suit les modifications apportées aux tables d'incidents, de changements et de problèmes, entre autres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Explorer



Découvrez les fonctionnalités et les valeurs commerciales de l’audit.

Configurer



Découvrez comment configurer l’audit.

Vue



Passez en revue les tables Audit Sys et Changement de relation d’audit.

Référence



En savoir plus sur les ensembles d’histoire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer l'audit

Suivez les modifications d'enregistrement sur les tables activées devant faire l'objet d'un audit. Par défaut, le système suit les modifications apportées aux tables d'incidents, de changements et de problèmes, entre autres.

L'activation de l'audit permet de suivre la création, la mise à jour et la suppression de tous les enregistrements de la table. Si vous souhaitez auditer des champs individuels dans une table, vous pouvez masquer les champs que vous ne souhaitez pas suivre à l'aide d'un attribut de dictionnaire.

Les informations d'audit sont conservées dans les tables suivantes :

- Table d'audit .
- La Connaître les ensembles d'historique table.

⚠ Avertissement :
L'audit des tables système qui reçoivent une grande quantité de trafic, telles que les contextes de workflow [wf_context] ou les alertes de gestion des événements [em_alert], peut avoir un impact sur les performances. Pour cette raison, vous ne pouvez pas auditer la table de em_alert dans son ensemble. Au lieu de cela, auditez les champs d'intérêt sélectionnés. Définissez `audit=true` à la fois sur la table em_alert et sur les champs sélectionnés. Essayez d'auditer le moins de champs possible.

Audit des tables parents et enfants

Les tables ne dérivent pas les marqueurs d'audit des tables auditées parentes ou enfants.

- Par exemple, si vous activez l'audit pour la table Éléments de configuration [cmdb_ci], seuls les CI stockés dans cette table de base sont audités.
- De même, si vous activez l'audit pour la table Ordinateurs [cmdb_ci_computer], seuls les enregistrements CI de l'ordinateur sont audités, y compris les champs de la table Ordinateurs [cmdb_ci_computer] dérivés de la table Éléments de configuration [cmdb_ci].

Audit des tables système

Par défaut, le système n'audite pas la suppression d'un enregistrement des tables système. Pour auditer une table système, ajoutez-la à la liste des tables de la `glide.ui.audit_deleted_tables` liste des propriétés.

Audit des suppressions à partir d'un formulaire ou d'une liste

Par défaut, le système vérifie les suppressions d'enregistrements individuels d'un formulaire. Pour empêcher l'audit, définissez l'attribut `no_audit_delete`de dictionnaire de la table .

Le système audite les suppressions d'une liste **lorsque celui-ci** est sélectionné dans le dictionnaire de table et que la table n'est pas répertoriée dans la `glide.db.audit.ignore.delete` propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Par défaut, la `glide.db.audit.ignore.delete` propriété n'est pas présente dans la table Propriétés système [sys_properties]. Pour modifier la propriété et ses valeurs associées, vous devez d'abord l'ajouter manuellement. Toutefois, lorsqu'il est ajouté manuellement, il remplace les valeurs par défaut suivantes :

```
glide.db.audit.ignore.delete =
sys_mutex,sys_db_cache,sys_lucene_block,sys_lucene_file,sys_lucene_directory,sys_user_preference,sys_aud
cmdb_ci_windows_service, cmdb_sam_sw_install, cmdb_software_instance,
cmdb_sam_sw_usage, sam_sw_counter_detail
```

Pour en savoir plus sur l'ajout de propriétés système, consultez Ajouter une propriété système

Il convient de noter que par défaut, les suppressions d'audit sont activées, que l'enregistrement soit supprimé de la vue de formulaire, de la vue de liste ou via un script/ une tâche planifiée.

Informations auditées

L'audit suit les changements d'enregistrement suivants :

- L'identificateur d'enregistrement unique (sys_id) de l'enregistrement qui a changé
- Champ qui a changé
- Nouvelle valeur du champ
- Ancienne valeur du champ
- Nombre de fois que cet enregistrement et ce champ ont été mis à jour
- Date et heure auxquelles le changement s'est produit
- Utilisateur qui a effectué le changement
- Motif du changement (le cas échéant)
- ID de point de contrôle interne pour l'enregistrement, si celui-ci possède plusieurs versions.

Informations exemptées de l'audit

Certaines mises à jour ne sont pas auditées malgré l'activation de l'audit sur une table. C'est pourquoi vous pouvez voir 132 mises à jour dans l'historique d'un enregistrement, mais seulement sept mises à jour auditées.

L'audit exclut les informations suivantes :

- Mises à jour effectuées par une mise à niveau.
- Les mises à jour sont effectuées par le biais de jeux d'importation.
- Enregistrements dans des tables parentes ou enfants.
- Champs avec l'attribut de dictionnaire no_audit.
- Les tables système ne sont pas répertoriées dans la `glide.ui.audit_deleted_tables` liste des propriétés.
- Champs commençant par le préfixe sys_ (champs système), à l'exception des colonnes sys_class_name et sys_domain_id.
- Les pages de l'interface utilisateur peuvent parfois déclencher des mises à jour d'un enregistrement sans créer de journal d'audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Chaque fois qu'un moniteur d'inactivité touche un enregistrement. Cela vous empêche de voir des centaines de mises à jour répertoriées par rapport à un incident, le bruit noyant les données utiles.
- Modification manuelle des Analyse des performances scores.

Audit d'une table

Pour plus d'informations sur l'audit d'une table, reportez-vous à la section Configuration de l'audit pour une table.

Par défaut, le système suit tous les champs d'une table auditée. Vous pouvez auditer un sous-ensemble de champs dans une table de l'une des deux façons suivantes :

- Vous pouvez activer l'audit pour l'ensemble de la table, puis exclure les champs que vous ne souhaitez pas inclure. Elle est appropriée lorsque vous souhaitez auditer la plupart des champs, mais pas tous, et est appelée *liste d'exclusion*. Pour plus d'informations, consultez Exclusion d'un champ de l'audit (liste d'exclusion).
- Vous pouvez activer l'audit pour la table, mais uniquement pour les champs spécifiés. Elle est appropriée lorsque vous souhaitez auditer uniquement un petit nombre de champs de la table et est appelée *liste d'inclusion*. Pour plus d'informations sur l'inclusion d'un champ à l'aide d'une liste d'inclusion, reportez-vous à la section Inclusion d'un champ de table dans l'audit (liste d'inclusion).

Enregistrements d'audit non annulables

Réduisez les risques que les enregistrements d'audit ne soient pas enregistrés lorsqu'une transaction est annulée avec le nouveau paramètre par défaut.

Des audits ont été définis pour créer un enregistrement immédiatement dans la même transaction que les opérations d'écriture d'enregistrement cible. Si l'enregistrement cible est supprimé, l'audit est quand même créé et conservé sous **le module de suppression d'audit de test NCA** .

Remarque :
Le processus d'audit amélioré est activé par défaut. Si la propriété `glide.db.audit.lazy` est définie sur `true`, le processus d'audit amélioré est désactivé.

Avant la Xanadu publication, si une transaction est annulée, certaines opérations auditables n'étaient pas enregistrées. Cela est dû au fait que la plateforme exécute certaines opérations entre le changement d'enregistrement et son annulation avant la création de l'audit. Désormais, les audits sont créés immédiatement après la modification de l'enregistrement, ce qui réduit les risques qu'une transaction annulée abandonne l'opération avant que l'audit ne soit enregistré.

Les audits sont désormais enregistrés dans le même thread que la transaction. Les audits précédents ont été créés dans un thread d'arrière-plan. Cette modification redéfinit la valeur par défaut de la propriété `glide.db.audit.lazy` de True à False. Cette propriété n'est généralement pas définie dans la table Propriétés, car la majorité des instances commencent à utiliser la nouvelle valeur et le nouveau comportement par défaut. Sur certaines instances, cette propriété peut être déjà présente et définie sur Vrai, ce qui signifie que ces instances ne seront pas en mesure d'utiliser ce changement pour auditer le comportement.

Remarque :
Il est recommandé de supprimer cette propriété pour tirer parti de la mise à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de l'audit pour une table

Vous pouvez activer l'audit de table pour suivre les changements apportés à tout ou partie des champs de la table.

Avant de commencer

Rôle requis : admin.

Remarque :
Les champs chiffrés ne sont pas audités de par leur conception. Ce comportement n'est pas configurable.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Dictionnaire**.
   Le système affiche la liste des entrées du dictionnaire. La liste comprend une ligne pour chaque table ainsi qu'une ligne pour chaque colonne (champ) de la table.
2. Dans la liste des entrées de dictionnaire, recherchez la ligne correspondant à la table que vous souhaitez auditer, par exemple `cmdb_ci_computer`.
   Vous pouvez distinguer la ligne correspondant au tableau lui-même de celle correspondant à une colonne du tableau, en trouvant la ligne avec le nom correct du tableau, une entrée vide **pour le nom** de colonne et un **type** de **collecte**.
3. Sélectionnez l'entrée de dictionnaire pour la table.
   Le système affiche le formulaire d'entrée du dictionnaire.
4. Cochez la case **Audit** .
5. Sélectionnez **Mettre à jour**.

Que faire ensuite

Si vous souhaitez auditer uniquement quelques champs de la table.Activation de l'audit de liste d'inclusion pour une table Si vous souhaitez auditer la plupart des champs, mais en exclure certains, reportez-vous à la section Exclusion d'un champ de l'audit (liste d'exclusion).

Activation de l'audit de liste d'inclusion pour une table

Activez une table pour auditer uniquement les champs que vous désignez explicitement. Cela est utile lorsque vous souhaitez auditer uniquement un petit nombre de champs dans une table auditée.

Avant de commencer

Rôle requis : administrateur
La table doit être activée pour l'audit.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Dictionnaire**.
   Le système affiche la liste des entrées du dictionnaire. La liste comprend une ligne pour chaque table ainsi qu'une ligne pour chaque colonne (champ) de la table.
2. Si nécessaire, personnalisez la vue de liste pour afficher la colonne **Attributs** .
3. Dans la liste des entrées de dictionnaire, recherchez la ligne correspondant à la table que vous souhaitez auditer, par exemple `cmdb_ci_computer`.
   Vous pouvez distinguer la ligne correspondant au tableau lui-même de celle correspondant à une colonne du tableau en trouvant la ligne avec le nom correct du tableau, une entrée vide pour le nom de colonne et un type de *`collection`*.
4. Dans le champ **Attributs** de cette ligne, saisissez *`audit_type=whitelist`*.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite
Désignez les champs que vous souhaitez auditer dans cette table.

Exclusion d'un champ de l'audit (liste d'exclusion)

Empêchez le suivi d'un Now Platform sous-ensemble de champs dans une table auditée en excluant ces champs d'un audit.

Avant de commencer
Rôle requis : administrateur
Pour exclure un champ d'une table de l'audit, vous devez d'abord activer l'audit pour cette table.

Pourquoi et quand exécuter cette tâche
Ajoutez un ensemble de champs à une liste d'exclusion lorsque vous souhaitez auditer la plupart des champs d'une table auditable. Si vous souhaitez auditer uniquement quelques champs, suivez plutôt la procédure de liste d'inclusion .

Remarque :
La désactivation de l'audit sur les champs basés sur le journal peut avoir un impact sur la fonctionnalité des fonctionnalités, telles que le formateur d'activité. Pour plus d'informations, consultez KB0743142 .

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Dictionnaire**.
2. Si nécessaire, personnalisez la vue de liste pour afficher la colonne **Attributs** .
3. Accédez à la ligne correspondant à la table et au champ (colonne) que vous souhaitez exclure de l'audit.
4. Dans la colonne **Attributs** de cette ligne, saisissez `no_audit`.

Inclusion d'un champ de table dans l'audit (liste d'inclusion)

Suivre un sous-ensemble de champs dans une table auditée en ajoutant ces champs à une liste d'inclusion.

Avant de commencer
Rôle requis : administrateur
Pour ajouter des champs dans une table à une liste d'inclusion, vous devez d'abord avoir activé l'audit pour cette table et activé l'audit de la liste d'inclusion pour cette table.

Pourquoi et quand exécuter cette tâche
Ajoutez un ensemble de champs à une liste d'inclusion lorsque vous souhaitez auditer uniquement un petit nombre de champs d'une table auditée. Si vous devez auditer la plupart des champs et n'en exclure que quelques-uns, suivez plutôt la procédure de liste d'exclusion .

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Dictionnaire**.
2. Si nécessaire, personnalisez la vue de liste pour inclure l'affichage de la colonne **Attributs** .
3. Accédez à la table et au champ (colonne) que vous souhaitez ajouter à la liste d'inclusion.
4. Dans le champ **Attributs** , saisissez `audit=true`.

Activer l'audit pour une table système

Les suppressions des tables avec un préfixe sys_ ne sont pas auditées par défaut. Pour suivre les suppressions de ces tables, ajoutez le nom de la table à la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

glide.ui.audit_deleted_tables propriété. L'activation du module d'extension Restaurer les enregistrements supprimés ajoute plusieurs valeurs par défaut à cette propriété.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Propriétés de l'interface utilisateur**.
2. Localisez la **liste des tables système (commençant par « sys_ », séparées par des virgules) qui auront la propriété auditée de suppression** .
3. Ajoutez ou supprimez des noms de tables. Les noms des tables doivent être séparés par des virgules, sans espace.
4. Cliquez sur **Enregistrer**.

Remarque :
Pour plus d'informations sur l'audit, consultez Présentation de la table d'audit système.

Affichage des tables Audit système et Changement de relation d'audit

Le Now Platform suit les insertions et les mises à jour des enregistrements audités dans les tables Audit système (sys_audit) et Changement de relation d'audit (sys_audit_relation).

Les tables d'audit des Now Platform pistes. Pour suivre les tables, cochez la case **Audit** dans l'enregistrement de dictionnaire pour définir la valeur sur vrai. Par défaut, il n'audite pas les enregistrements des tables système, telles que les tables d'ensembles de mises à jour.

Remarque :
Pour éviter les problèmes de performances et les boucles infinies, le système ignore toute règle métier ou workflow déclenché par des insertions dans la table Audit système.

Colonnes de la table d'audit système

Les colonnes suivantes apparaissent dans les enregistrements de la table sys_audit :

Champ	Description
Nom de la table	Table à laquelle l'enregistrement d'audit est destiné (par exemple, « incident »)
Nom de champ	Colonne de la table à laquelle l'enregistrement d'audit est destiné (par exemple, « assigned_to »)
Clé de document	Sys_id (identifiant d'enregistrement unique) de l'enregistrement d'origine associé à l'enregistrement d'audit.
Utilisateur	Nom de l'utilisateur qui a créé le changement. **Remarque :** Certains processus automatisés utilisent le système ou l'utilisateur invité pour appliquer et suivre les changements apportés aux enregistrements. Pour plus d'informations, reportez-vous à la section Utilisateurs système et invités .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Valeur précédente	Ancienne valeur du changement de champ représenté par cet enregistrement de sys_audit. • Champs de référence : valeur de sys_id unique de l'enregistrement changé. • Champs de date et d'heure : Valeur en heure universelle coordonnée (UTC) telle qu'elle est stockée dans la base de données.
Nouvelle valeur	Nouvelle valeur du changement de champ représenté par cet enregistrement sys_audit. • Champs de référence : valeur de sys_id unique de l'enregistrement changé. • Champs de date et d'heure : Valeur en heure universelle coordonnée (UTC) telle qu'elle est stockée dans la base de données.

Fonctionnement de la table Changement de relation d'audit (sys_audit_relation)

La table Audit système [sys_audit] suit les changements apportés aux champs de référence dans les tables qui sont marquées pour l'audit. Cette activité comprend les entrées de champs journal et les jeux d'historique. La table Changement de relation d'audit [sys_audit_relation] suit les changements de relation entre sys_audit enregistrements de table et les tables sources d'où proviennent les enregistrements audités. Il permet également de savoir quand un enregistrement a pu être supprimé.

-
- Chaque fois que vous auditez un enregistrement d'une table, une relation est créée entre les différentes tables d'origine du magasin qui enregistre les données. Ces informations sur la relation sont enregistrées dans les tables sys_history_set, sys_history_line et sys_journal.
- Si vous supprimez un champ associé à un enregistrement de table audité, la table sys_audit_relation enregistre la suppression. En d'autres termes, chaque fois que vous modifiez un enregistrement audité, il supprime d'abord les éléments passés, puis crée une relation dans la table sys_audit_relation avec les nouveaux ID de document.

Connaître les ensembles d'historique

Le système génère automatiquement des enregistrements d'ensemble d'historique selon les besoins à partir de la table d'audit lorsqu'un utilisateur crée un enregistrement ou consulte son historique.

Si un enregistrement se trouve dans une table auditée, son jeu d'historique est généré lorsque l'enregistrement est inséré ou lorsqu'un utilisateur consulte l'enregistrement.

Remarque :
N'utilisez pas d'ensembles d'historique pour générer des rapports.

Plusieurs champs d'informations sont capturés dans l'enregistrement de l'ensemble d'historique, affiché dans la vue de liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'enregistrement de la vue de liste

Champ	Valeur d'entrée
ID	ID de document pour l'enregistrement dont l'historique est en cours d'enregistrement.
Table	Table auditée pour l'enregistrement dont l'historique est en cours d'enregistrement.
Heure de chargement	Temps nécessaire pour générer l'ensemble d'historique.

Champs d'enregistrement de l'historique d'audit

Champ	Valeur d'entrée
Étiquette	Étiquette du champ qui a été modifié.
Ancien	Valeur avant le changement.
Nouveau	Valeur postérieure au changement.
Type	Indique si l'entrée concerne un champ normal, un enregistrement d'e-mail ou un enregistrement de changement de relation.
Numéro de mise à jour	Nombre de fois que ce champ a été modifié. Une valeur de -1 indique quand l'enregistrement a été créé ou supprimé.
Heure de mise à jour	Date et heure du changement. **Remarque :** L'heure de mise à jour des lignes d'historique générées automatiquement ne correspond pas à l'heure de création ou de mise à jour d'un enregistrement dans une situation de traitement spécifique. Lorsque vous affichez un ensemble d'historique d'un enregistrement pour la première fois, un jeu initial d'enregistrements de ligne d'historique est généré automatiquement. Étant donné que les changements de fichier dans une mise à niveau ne sont pas audités, cette incompatibilité de date se produit dans les cas suivants : • Vous affichez un historique défini après qu'un changement a été apporté à un enregistrement, mais • Avant qu'une autre modification ne lui soit apportée lors d'une future mise à niveau.
Noms d'utilisateur	Nom de l'utilisateur qui a créé le changement.

Ensembles d'historique dans une vue de calendrier

Une fois que les jeux d'historique sont actifs, le choix de menu contextuel Historique est rempli à l'aide des informations du jeu d'historique, plutôt qu'à partir de la table sys_audit . Du point de vue de l'utilisateur, les mêmes données historiques sont disponibles dans la même interface utilisateur, mais la façon dont les informations sont stockées est différente.

Étant donné que la vue Historique inclut une vue Calendrier, mais n'utilise pas l'interface de liste normale pour filtrer et interagir avec les enregistrements d'historique, elle permet :

- Recherche et filtrage des données historiques.
- Exportation des données d'historique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affichage des jeux d'historique

Il existe deux façons d'afficher l'ensemble d'historique, accessibles via l'action **Historique** du menu contextuel.

Différences entre les ensembles d'audit et d'historique

Les tables Audit [sys_audit], Jeux d'historique [sys_history_set] et Historique [sys_history_line] stockent les mêmes données, mais elles ont des objectifs différents et gèrent les données différemment.

Table d'audit [sys_audit]

La table Audit [sys_audit] est l'endroit où le système stocke les informations historiques de tous les enregistrements. Ces enregistrements sont destinés à être conservés indéfiniment afin que les administrateurs puissent toujours suivre l'historique des enregistrements audités. À mesure que le nombre d'enregistrements d'audit augmente au fil du temps, il devient plus inefficace d'interroger directement la table d'audit pour obtenir des informations historiques. Il est beaucoup plus efficace d'exécuter des requêtes uniquement sur les plus petits enregistrements de sous-ensemble pour lesquels vous souhaitez réellement afficher des informations historiques.

Historique défini [sys_history_set] table

La table Ensemble d'historique [sys_history_set] identifie les enregistrements particuliers d'une table auditée qui contiennent des informations historiques. La table Historique [sys_history_line] stocke les changements réels apportés aux valeurs de champ qui se sont produits.

- Le système génère automatiquement des enregistrements de l'ensemble d'historique et de l'historique selon les besoins à partir de la table d'audit lorsqu'un utilisateur crée un enregistrement ou demande son historique.
- Plutôt que de contenir un historique complet de tous les changements dans le système, les enregistrements de l'ensemble d'historique et de l'historique ne contiennent qu'un sous-ensemble récent d'informations historiques pour les enregistrements pour lesquels les utilisateurs ont créé ou demandé de telles informations.
- Outre les données d'audit, les jeux d'historique comprennent également les informations définies lors de l'insertion de l'enregistrement, y compris les entrées de champ journal. Les entrées de champ journal que vous créez avant de créer un enregistrement sont traitées de la même manière que les entrées de journal créées au moment de la création de l'enregistrement. Ces entrées de journal apparaissent dans les jeux d'historique avec la même date de création et créées par les données que l'enregistrement associé lui-même.

Le système limite l'ensemble d'historique et les enregistrements d'historique par :

- Demander au nettoyeur de table de supprimer l'historique Définissez les enregistrements qui n'ont pas été mis à jour depuis 30 jours.
- Utilisation de la rotation de table pour alterner entre quatre tables d'historique tous les sept jours. Le système supprime les enregistrements d'historique antérieurs à 28 jours.

Si quelqu'un a besoin d'informations historiques à une date ultérieure, le système peut les régénérer à partir de l'audit des enregistrements sources.

Une fois que le système a généré les enregistrements de l'ensemble d'historique, le choix du menu contextuel **Historique** utilise l'ensemble d'historique plutôt que les enregistrements

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'audit. Du point de vue de l'utilisateur, les mêmes données historiques sont disponibles dans la même interface utilisateur, mais la façon dont les informations sont stockées est différente.

Contrôler l'accès à l'historique

Vous pouvez donner à un rôle l'accès à l'affichage de l'historique des audits en définissant une propriété système.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Système**.
2. Sélectionnez la `glide.history.role` propriété dans la table.
3. Dans le `List of roles (comma-separated) that can access the history of a record`, sélectionnez les rôles d'utilisateur auxquels vous souhaitez donner accès à l'historique.
4. Sélectionnez **Enregistrer**.

Résultats

Toute modification apportée à un champ est omise si un utilisateur sans accès en lecture consulte l'historique d'un enregistrement.

Modifier le nombre d'entrées d'historique

Par défaut, l'historique affiche un maximum de 250 entrées d'historique, mais vous pouvez modifier cette valeur.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Système**.
2. Sélectionnez la propriété `glide.history.max_entries`.
3. Définissez la `Maximum number of field entries displayed in record history, default is 250` valeur avec un nouveau nombre maximal d'entrées à afficher.

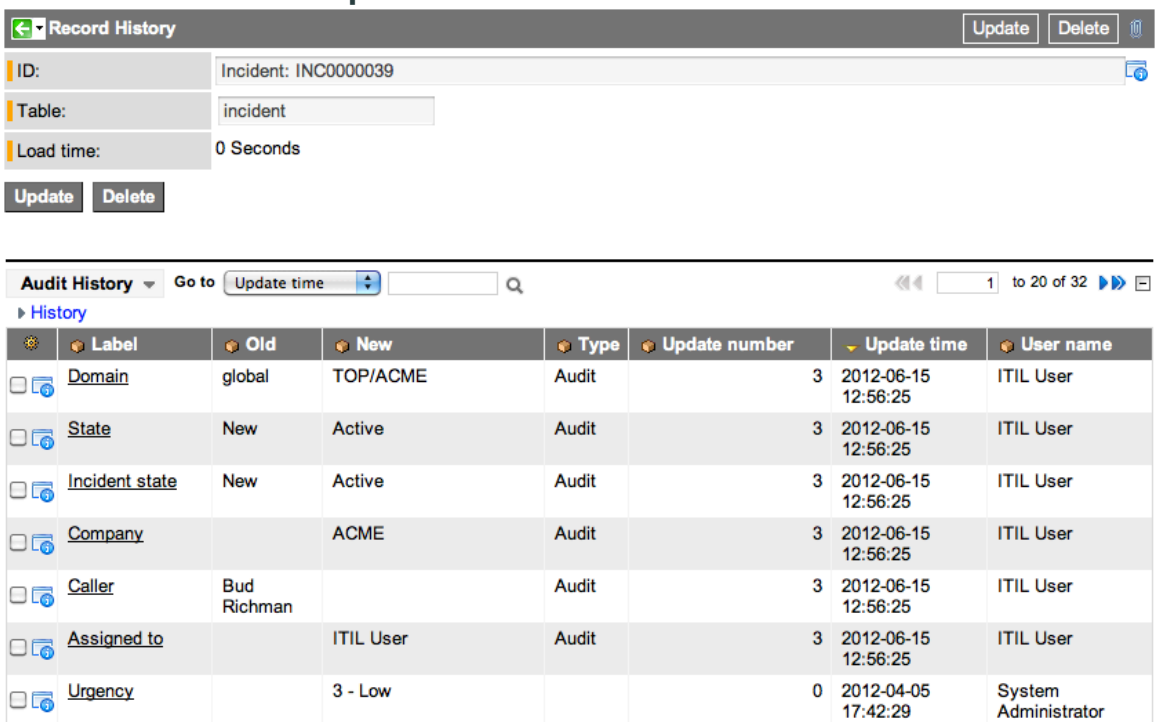
Liste de l'historique

La liste d'historique affiche chaque changement sous la forme d'une ligne à part entière dans la liste des changements.

Traduction automatique

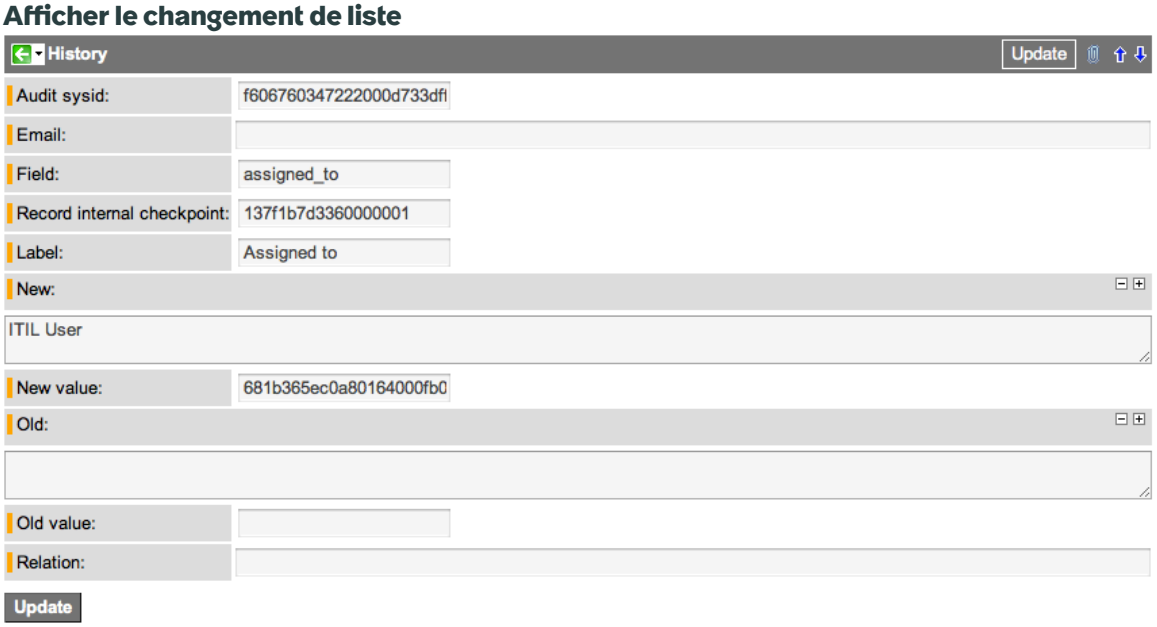
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher la liste de l'historique



Cliquez sur un élément de ligne pour afficher des détails supplémentaires sur le changement.

Afficher le changement de liste



Besoins

Pour afficher une liste d'historique, les conditions suivantes doivent être remplies.

Audit

L'audit de la table doit être activé pour afficher une liste d'historique.

ACL

Par défaut, l'option *Historique de la liste* n'est disponible que pour les utilisateurs disposant du rôle d'utilisateur administrateur. Pour activer cette option pour les non-administrateurs, créez une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

règle ACL personnalisée accordant un accès en lecture à la table Historique des enregistrements [sys_history_set].

Rôles

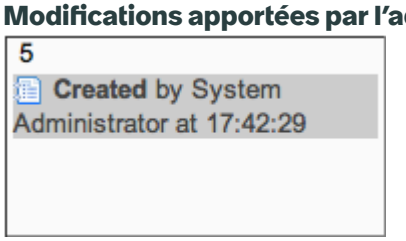
Au moins un des rôles dont dispose l'utilisateur doit être inclus dans la `glide.history.role` propriété, qui inclut le rôle itil par défaut.

Calendrier de l'historique

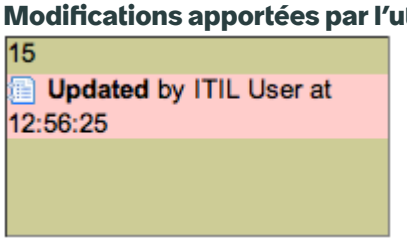
Le calendrier de l'historique indique les jours où l'enregistrement a été changé, la personne qui a effectué le changement et le moment où elle l'a effectué.

Le calendrier historique est trié par numéro de mise à jour. Chaque utilisateur se voit attribuer une couleur afin que vous puissiez savoir en un coup d'œil combien de fois un enregistrement a été modifié par un utilisateur spécifique. Par exemple :

Modifications apportées par l'administrateur système



Modifications apportées par l'utilisateur ITIL

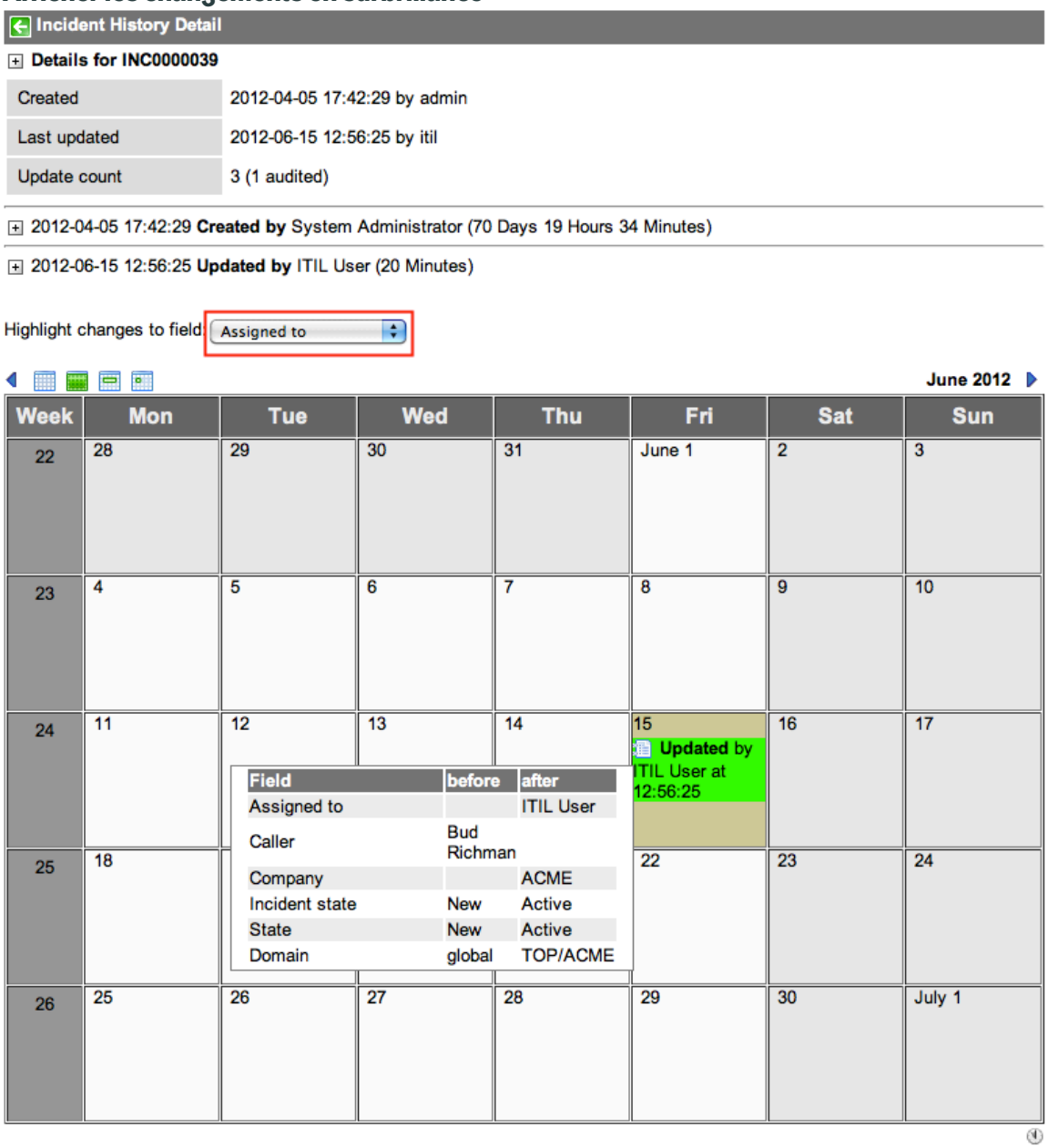


Pour mettre en surbrillance les modifications apportées à un champ particulier, sélectionnez-le dans la zone de sélection **Mettre en surbrillance les modifications apportées au champ** . La sélection d'un champ dans cette zone de sélection modifie le calendrier pour mettre en surbrillance les heures auxquelles ce champ a été modifié. Passez la souris sur le texte de l'un des changements mis en surbrillance pour voir le changement de valeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les changements en surbrillance

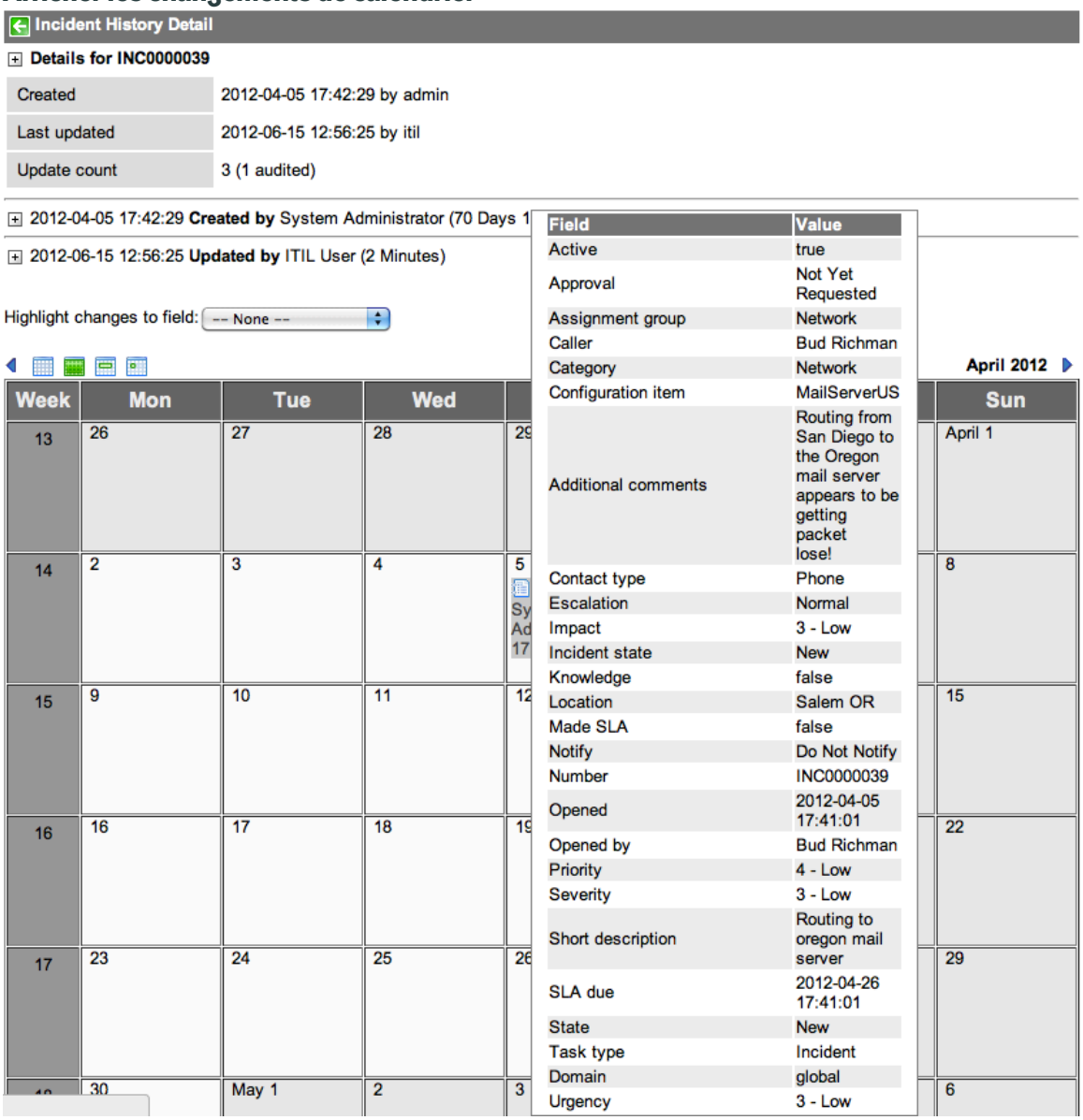


Si vous passez la souris sur l'icône dans une entrée, une fenêtre contextuelle affiche tous les changements de valeur. Il s'agit des mêmes informations qui sont affichées dans la partie supérieure du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les changements de calendrier



Vous pouvez cliquer sur le numéro du jour pour obtenir une vue des changements pour ce jour. Vous pouvez également cliquer sur le numéro de la semaine à gauche pour obtenir une vue de la semaine. Vous pouvez faire défiler d'un mois à l'autre pour afficher les changements.

Chronologie de l'historique

Vous pouvez afficher une chronologie des changements pour un CI et pour ses enregistrements connexes, ses relations, ses bases de référence et les changements proposés pour le CI. Les chronologies sont disponibles pour les CI de la table d'éléments de configuration [cmdb_ci] ou d'un descendant de cette table, si l'audit est activé pour les tables.

Rôle requis : l'ACL de cette vue est basée sur les rôles définis dans la `glide.history.role` propriété système, qui est définie par défaut sur ITIL. En outre, l'utilisateur doit avoir un accès en lecture à la table Ensemble d'historique [sys_history_set], qui par défaut est accordée à l'administrateur.

Vous pouvez ouvrir une chronologie lorsque vous consultez l'historique d'un CI. Vous pouvez spécifier la période, la plage horaire et les propriétés qui sont affichées dans la

Traduction automatique

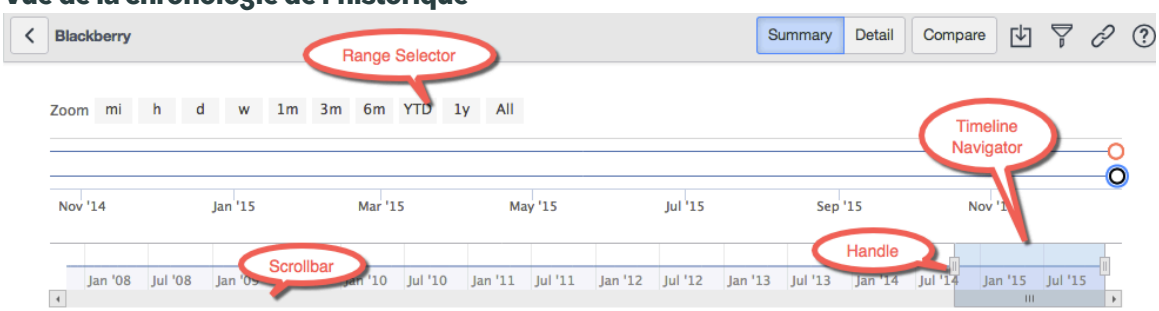
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

chronologie. Vous pouvez afficher ce qui a changé dans un ensemble de changements particulier ou afficher l'ensemble du CI pour mieux résoudre les problèmes. Vous pouvez également afficher une chronologie des modifications apportées aux enregistrements connexes du CI, et exporter et comparer des instantanés du CI à tout moment.

Les changements de CI sont représentés par des bulles de différentes formes et couleurs le long de la chronologie. La forme de chaque bulle représente un type différent de changement et la couleur de chaque bulle indique si le changement est valide ou non valide. Les lignes de base des CI sont représentées par des cercles noirs que vous pouvez survoler pour afficher plus de détails. Cliquez sur **l'icône ?** pour afficher les définitions de forme et de couleur des bulles, et pointez sur une bulle pour afficher les détails du jeu de changements.

Un changement apporté à une relation n'est considéré comme valide que s'il a été appliqué via la gestion des changements. Si le changement a été appliqué via le cadre de travail des changements proposés, il est valide. Pour connaître les étapes de validation supplémentaires, reportez-vous à la section Créer ou modifier un script de validation planifiée .

Vue de la chronologie de l'historique



Bulles de chronologie



Remarque :
Les changements proposés qui n'ont pas de date de début planifiée sont placés à des points temporels futurs.

Navigateur de chronologie

Utilisez les poignées situées aux deux extrémités du navigateur de chronologie pour prolonger ou raccourcir la période affichée.

Vous pouvez faire défiler jusqu'à une autre période de temps en cliquant sur la partie inférieure du navigateur de chronologie, puis en faisant glisser le navigateur vers la gauche ou la droite.

Zoom

Par défaut, la chronologie du dernier mois s'affiche. À côté de l'étiquette **Zoom** au-dessus de la chronologie, vous pouvez sélectionner un autre intervalle de temps. Vous pouvez sélectionner des intervalles allant d'une minute à la période entière des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

S'il y a de nombreux changements de CI au cours de la période, les bulles affichées risquent d'être trop encombrées. Vous pouvez effectuer un zoom avant ou arrière pour étaler les bulles dans l'une ou l'autre des méthodes :

- Modifiez l'intervalle de temps sur la chronologie. Lorsque vous raccourcissez l'intervalle de temps, vous effectuez un zoom avant et lorsque vous allongez l'intervalle de temps, vous effectuez un zoom arrière.
- Sélectionnez la section de la chronologie sur laquelle vous souhaitez zoomer.

Filtre de propriété

Vous pouvez filtrer les bulles qui s'affichent. Par défaut, toutes les bulles sont affichées, représentant les changements apportés à toutes les propriétés du CI. Vous pouvez limiter la vue pour n'afficher que les bulles dans lesquelles les propriétés sélectionnées ont été modifiées et exclure les bulles dans lesquelles seules les propriétés non sélectionnées ont été modifiées.

Les vues **Détail** et **Résumé** mettent en évidence les propriétés dans votre champ d'application de filtre qui ont changé. Les propriétés modifiées sont mises en surbrillance en bleu clair.

Dans la vue **Résumé** , vous pouvez choisir d'inclure toutes les propriétés du CI ou uniquement celles qui ont été modifiées. Si vous choisissez d'afficher toutes les propriétés dans la vue récapitulative, les propriétés modifiées sont répertoriées avant les propriétés inchangées.

Vue de résumé

La vue **Résumé** affiche les instantanés des CI représentés par chaque bulle. Chaque instantané affiche les changements apportés aux champs et relations du CI en fonction de l'ensemble de changements. Il affiche les valeurs anciennes et nouvelles avant et après le changement, ainsi que toutes les relations qui ont été ajoutées ou supprimées.

Utilisez les boutons **>** et **<** des deux côtés de l'écran de l'instantané pour faire défiler les enregistrements d'ensemble de changements suivants et précédents dans l'ordre chronologique.

Vue détaillée

La vue **détaillée** affiche les instantanés du CI qui correspondent aux bulles. Chaque instantané inclut les champs qui se trouvent dans le champ d'application du filtre de propriété, affichant les propriétés qui ont changé avec un arrière-plan bleu clair. Cliquez sur une bulle pour afficher l'instantané du CI correspondant. Les données qui s'affichent sont en lecture seule.

Utilisez les boutons **>** et **<** des deux côtés pour faire défiler les enregistrements d'ensemble de changements suivants et précédents dans l'ordre chronologique.

Afficher la chronologie des changements apportés aux enregistrements connexes

Sur la chronologie des changements d'un enregistrement de CI, vous pouvez également afficher une chronologie des changements pour les enregistrements connexes du CI.

Avant de commencer

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Table cible : l'enregistrement du CI doit se trouver dans la table d'éléments de configuration [cmdb_ci] ou un descendant de cette table.
- Audit : doit être activé pour la table contenant le CI.

Procédure

1. Ouvrez la chronologie du CI.
2. Sélectionnez l'icône **Enregistrements connexes** et sélectionnez les enregistrements connexes dans la **liste des enregistrements connexes** à afficher.
   Cliquez à nouveau sur l'icône Enregistrements connexes pour afficher la chronologie des enregistrements connexes.

Résultats

La chronologie des changements apportés aux enregistrements connexes du CI s'affiche juste au-dessus de la chronologie du CI. Si vous décochez tous les enregistrements connexes, la chronologie des enregistrements connexes est masquée.

Que faire ensuite

Passez le curseur au-dessus d'une bulle de changement sur la chronologie des enregistrements connexes pour afficher les détails du changement, tels que la date et le nombre de propriétés modifiées. Lorsque vous modifiez l'intervalle de temps dans la mise au point, ou que vous effectuez un zoom avant ou arrière, cela affecte simultanément la chronologie du CI et la chronologie des enregistrements connexes.

Exporter un instantané d'un CI

Vous pouvez exporter un instantané d'un CI à partir de sa chronologie.

Avant de commencer

Le CI doit se trouver dans la table d'éléments de configuration [cmdb_ci] ou un descendant de cette table.
L'audit doit être activé pour la table contenant le CI.
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

Vous pouvez exporter un instantané du CI au format XML, PDF (portail) ou PDF (paysage).

Procédure

1. Ouvrez la chronologie du CI.
2. Sélectionnez la bulle correspondant à la période pendant laquelle vous souhaitez exporter un instantané du CI.
3. Cliquez sur l'icône d'exportation ( ).
4. Sélectionnez le format de fichier à utiliser pour l'exportation.
   Vous pouvez télécharger le fichier sur votre système pour le visualiser.

Comparer les instantanés de CI

Vous pouvez comparer les propriétés et les relations d'un CI à deux moments différents de sa chronologie.

Avant de commencer

Le CI doit se trouver dans la table d'éléments de configuration [cmdb_ci] ou un descendant de cette table.
L'audit doit être activé pour la table contenant le CI.
Rôle requis : admin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez la chronologie du CI.
2. Cliquez sur **Comparer**.
3. Sélectionnez une date **de début** et une date **de fin** .
4. Cliquez sur **Comparer**.

Suivi des modifications apportées aux champs de référence

Les administrateurs peuvent suivre les changements apportés aux valeurs d'affichage des champs de référence.

Étant donné que les champs de référence ne stockent qu'une valeur d'ID, le système ne peut normalement auditer les changements que lorsque la valeur d'ID change. Par défaut, le système n'audite pas les changements effectués lorsque la valeur d'affichage d'un champ de référence change.

Considérons la situation suivante. Un utilisateur change son nom de Jane Smith à Jane Miller. Étant donné que le nom d'utilisateur est la valeur d'affichage de la table Utilisateur, toute référence précédente à Jane Smith fait plutôt référence à Jane Miller. Si l'administrateur se contente de mettre à jour le nom de l'enregistrement utilisateur existant, les enregistrements d'audit et d'historique n'afficheront que le nouveau nom Jane Miller. Par défaut, le système ne permet pas de faire la distinction entre les modifications apportées sous le nom d'utilisateur d'origine et celles effectuées avec le nouveau nom d'utilisateur.

Si votre politique d'audit nécessite de suivre les changements de noms d'utilisateur, vous pouvez :

- Créez un nouvel enregistrement d'utilisateur pour le nouveau nom et désactivez l'enregistrement d'utilisateur précédent. Le système conserve les enregistrements d'audit pour l'ancien nom d'utilisateur et crée les enregistrements d'audit futurs avec le nouveau nom d'utilisateur.
- Créez des champs personnalisés et une règle métier pour enregistrer le nom précédent et la date du changement de nom. Le système peut utiliser ces informations pour construire les noms propres dans les enregistrements d'audit et d'historique.

Insertions de suivi

Par défaut, le système ne crée pas d'enregistrements d'audit pour les insertions car, dans une instance classique, les insertions peuvent représenter plus de 80 % de la taille de la table d'audit.

L'absence d'insertions de suivi permet d'améliorer les performances et d'obtenir une table d'audit beaucoup plus petite. Les administrateurs peuvent activer l'audit des insertions en définissant la `glide.sys.audit_inserts` propriété sur *vrai*.

Suivi des relations CI

Les changements apportés à une relation CI (relations CI, relations CI/utilisateur ou relations CI/groupe) apparaissent dans l'historique des éléments des deux côtés de la relation modifiée, que le changement ait été manuel ou résulte de Découverte.

Par exemple, si l'ordinateur alpha a une relation CI utilisé par avec la version bêta de l'ordinateur, l'historique de la version alpha contient un enregistrement de la date à laquelle la relation avec la version bêta a été établie, de même que l'historique de la version bêta contient un enregistrement de la date à laquelle la relation avec la version alpha a été

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

établie. Cet exemple illustre l'historique affiché lorsque des relations CI sont établies, puis que l'une d'entre elles est supprimée :

Historique des relations CI

2008-12-03 10:49:37 **Updated by** Guest (19 Hours 54 minutes ago) - CI Relationship Change

- created 2 Days 2 Hours 51 minutes earlier

Relationship	Before	After
Runs	(relationship added)	Tomcat@tomdmac
Runs	(relationship added)	MySQL Server@tomdmac

2008-12-03 10:49:38 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Disks

2008-12-03 10:49:43 **Updated by** Guest (19 Hours 54 minutes ago) - Mac OS X - Active Connections

2008-12-03 10:50:02 **Updated by** Guest (19 Hours 53 minutes ago)

2008-12-04 06:43:39 **Updated by** Glide Maintenance (just now) - CI Relationship Change

- last activity was 19 Hours 53 minutes earlier
- created 2 Days 22 Hours 45 minutes earlier

Relationship	Before	After
Runs	MySQL Server@tomdmac	(relationship removed)

La puce créée indique la date à laquelle le CI, l'utilisateur ou le groupe a été créé. La dernière puce d'activité fait référence à la date à laquelle les relations ont été modifiées pour la dernière fois. Si vous ne souhaitez pas afficher l'historique des relations CI pour tout ou partie des types de relations CI, vous pouvez désactiver cette option en désactivant l'audit sur les tables de relations CI (Relation CI [cmdb_rel_ci], Type de relation CI/utilisateur [cmdb_rel_user_type] ou Relation de groupe [cmdb_rel_group]).

Paramètres de sécurité élevée

Les paramètres de sécurité élevée désignent plusieurs options de sécurité disponibles dans votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer les paramètres de haute sécurité



Découvrez les fonctionnalités et les valeurs commerciales des paramètres de sécurité élevée.

Activer les paramètres de sécurité élevée



Activez les paramètres de sécurité élevée.

Configurer les paramètres de sécurité élevée



Comprendre comment configurer les paramètres de sécurité élevée.

Traduction automatique

Exploration des paramètres de sécurité élevée

Les paramètres de sécurité élevée désignent plusieurs options de sécurité disponibles dans votre instance.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le module Paramètres de sécurité élevée est activé avec le module d'extension Paramètres de sécurité élevée, qui est actif par défaut sur les nouvelles instances. Si les paramètres de sécurité élevée ne sont pas actifs sur votre instance, consultez Demande d'activation des paramètres de sécurité élevée. Pour en savoir plus sur ce module d'extension, consultez Module d'extension de haute sécurité Paramètres de renforcement de la sécurité de l'instance. Les propriétés de ces types de paramètres de sécurité élevée sont disponibles :

- Valeurs de propriété par défaut : pour renforcer la sécurité de votre plateforme en centralisant tous les paramètres de sécurité critiques en un seul emplacement pour la gestion et l'audit.
- Propriété de refus par défaut : fournit une propriété du gestionnaire de sécurité pour contrôler le comportement de sécurité par défaut pour l'accès à la table.
- Rôle d'administrateur de sécurité : permet d'empêcher la modification des paramètres et des ressources de sécurité clés. Le rôle d'administrateur de sécurité n'est pas hérité par le rôle administrateur et doit être explicitement attribué.
- Privilèges élevés : permet aux utilisateurs ayant le rôle d'administrateur de sécurité d'opérer dans le contexte d'un utilisateur normal et de s'élever à un rôle de sécurité supérieur si nécessaire.
- Contrôles d'accès aux propriétés : permet aux administrateurs de sécurité de définir les rôles requis pour lire et écrire les propriétés.
- Journaux système : sont en lecture seule.
- Règles de contrôle d'accès : contrôlez les données auxquelles les utilisateurs peuvent accéder et la manière dont ils peuvent y accéder.

Remarque :

- Les paramètres de sécurité élevée activent également automatiquement le module d'extension de sécurité contextuelle, s'il n'est pas déjà activé. En outre, Paramètres de sécurité de la plateforme : élevé fournit des paramètres et des fonctionnalités dans le contexte du renforcement de la sécurité de votre instance.
- Le contenu des paramètres de renforcement de la sécurité de l'instance contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans le Now Platform. Pour en savoir plus sur chacune de ces propriétés, reportez-vous à la section Paramètres de la sécurisation pour la sécurité de l'instance.
- Pour en savoir plus sur chacune de ces propriétés, reportez-vous à la section Paramètres de la sécurisation pour la sécurité de l'instance.

Il existe deux façons de définir ou de modifier les propriétés des paramètres de sécurité élevée.

- Accédez à la **Sécurité de système** > **Paramètres de sécurité élevée**.

  Les options de la page Propriétés de sécurité élevée sont **Oui** ou **Non**.

- Accédez à la **sys_properties.list** et recherchez la propriété que vous souhaitez définir ou modifier.

  Les options de la table Propriétés système [sys_properties.list] sont **vrai** ou **faux**.

Contrôle d'accès à la propriété

Deux colonnes supplémentaires sont créées dans la table Propriétés [sys_properties] lorsque les paramètres de sécurité élevée sont actifs :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

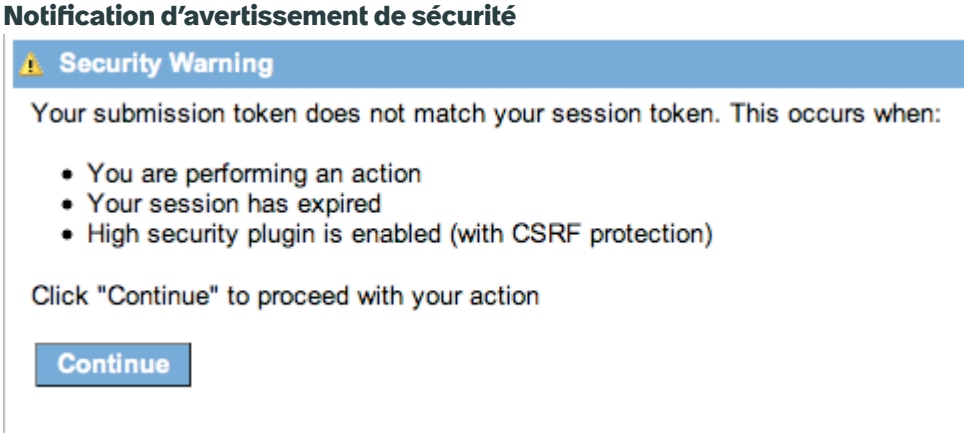
- **read_roles** : liste de noms de rôles, séparés par des virgules, autorisés à lire tous les champs de cette propriété.
- **write_roles** : liste de noms de rôle séparés par des virgules autorisés à écrire/modifier tous les champs de cette propriété.

Les propriétés répertoriées dans la table Propriétés ont **read_roles** d'administrateur et **write_roles** de security_admin. Les utilisateurs disposant du rôle administrateur peuvent afficher et lire les valeurs des propriétés, mais doivent s'élever au rôle security_admin pour les modifier.

Notifications

L'activation des paramètres de sécurité élevée active également les messages d'avertissement de sécurité. Voici un exemple de message qui s'affiche après une approbation.

Notification d'avertissement de sécurité



Propriétés des paramètres de sécurité élevée

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.ui.escape_text	Valeurs XML d'échappement au niveau de l'analyseur de l'interface utilisateur. Empêche les attaques de script de site à site réfléchies et stockées. Cette propriété n'est pas applicable dans Portail de services.	Oui	XML

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	Remarque : Cette propriété est définie sur **vrai** par défaut dans les versions ultérieures Vancouver et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client.		
glide.ui.escape_all_script	Force l'échappement par défaut de toutes les expressions dans Jelly JavaScript <![CDATA[<script type="text/javascript">]]> balises. Applique l'échappement uniquement si l'attribut type de la <![CDATA[<script>balise]]> est vide ou si la valeur est text/javascript, text/ecmascript, application/javascript, application/ecmascript ou application/x-javascript.	Oui dans les nouvelles instances	Échapper à Jelly
glide.ui.rotate_sessions	Effectuez une rotation des	Oui	Rotation des identifiants de session HTTP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	identificateurs de session HTTP pour réduire les vulnérabilités de sécurité. Voir : http://www.owasp.org/index.php/Session_Management#Rota .	**Remarque :** Si vous utilisez le module d'extension SAML 2.0 pour l'authentification unique, définissez cette propriété sur Non. Sinon, cela interfère avec le partage d'informations de session qui a lieu entre l'instance et le fournisseur d'identité.	
glide.ui.secure_cookies	Activer les cookies de session sécurisés : Activez une sécurité par cookie supplémentaire. Si **oui**, la validation stricte des cookies de session est appliquée.	Oui	Cookies de session sécurisés
glide.security.password_reset.uri	Pour mobile Réinitialisation du mot de passe, URL vers laquelle l'utilisateur est redirigé lorsqu'il clique sur le bouton **Mot de passe oublié ?** .		Aucun
glide.security.strict.updates	Vérifiez la sécurité des transactions entrantes lors de la soumission du formulaire (les droits sont toujours vérifiés lors de la création d'un formulaire).	Oui	Double vérification des transactions entrantes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	Remarque : Cette propriété est définie sur **vrai** par défaut dans les versions ultérieures Vancouver et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client.		
glide.security.strict.actions	Vérifiez les conditions des actions d'interface utilisateur avant leur exécution. Normalement, les conditions ne sont vérifiées que pendant le rendu du formulaire.	Oui	Vérifier l'action d'interface utilisateur avant son exécution
glide.security.use_csrf_token	Activez l'utilisation d'un jeton de sécurité pour identifier et valider les demandes entrantes. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête de site à site.	Oui	Jeton anti-CSRF
glide.ui.escape_html_list_field	HTML d'échappement pour les champs HTML d'une vue de liste.	Oui	Échapper au HTML
glide.html.escape_script	Balises JavaScript d'échappement dans les champs HTML.	Oui	Échapper JavaScript

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.ui.forgetme	Décochez la case **Se souvenir de moi** de la page de connexion.	Oui	Supprimer Se souvenir de moi
glide.smtp.auth	Authentifiez-vous auprès du serveur SMTP à l'aide des propriétés du nom d'utilisateur et du mot de passe. **Remarque :** Cette propriété est obsolète.	Oui	Authentification SMTP (obsolète)
glide.script.use.sandbox	Exécutez les scripts générés par le client (AJAXEvaluate et conditions de requête) dans un bac à sable à droits réduits. Si **oui**, seuls les règles métier et les includes de script lorsque la case **Client joignable** est cochée sur **Oui** sont disponibles, et certains appels API centraux sont interdits. Pour plus d'informations, consultez Configuration de la propriété du bac à sable de script.	Oui	Bac à sable pour les scripts générés par le client
glide.soap.strict_security	Appliquez une sécurité stricte sur les demandes SOAP entrantes. Exige que les demandes SOAP entrantes passent par le gestionnaire de sécurité pour l'accès à la table et au champ, et vérifie que les utilisateurs SOAP possèdent les rôles appropriés	Oui	Sécurité stricte des requêtes SOAP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	pour utiliser le service Web.		
glide.basicauth.required.wsdl	Demandez une autorisation pour les demandes WSDL entrantes. **Remarque :** Si vous choisissez de ne pas demander d'autorisation pour les demandes WSDL entrantes, vous devez modifier les règles de contrôle d'accès (ACL) pour permettre aux utilisateurs invités d'accéder au contenu WSDL.	Oui	Autorisation de demande de WSDL
glide.basicauth.required.csv	Exiger l'autorisation de base pour les demandes CSV entrantes .	Oui	Autorisation des demandes de CSV
glide.basicauth.required.excel	Demandez l'autorisation de base pour les demandes Excel entrantes.	Oui	Autorisation des demandes Excel
glide.basicauth.required.importprocessor	Demandez l'autorisation de base pour les demandes d'importation entrantes.	Oui	Autorisation des demandes d'importation
glide.basicauth.required.pdf	Demandez l'autorisation de base pour les demandes PDF entrantes.	Oui	Autorisation de demande de PDF
glide.basicauth.required.rss	Demandez l'autorisation de base pour les demandes RSS entrantes.	Oui	Autorisation de demande de RSS

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.basicauth.required.scriptedprocessor	Demandez l'autorisation de base pour les demandes de script entrantes.	Oui	Autorisation de demande de script
glide.basicauth.required.soap	Demandez l'autorisation de base pour les demandes SOAP entrantes.	Oui	Authentification de base : demandes SOAP
glide.basicauth.required.unl	Demandez l'autorisation de base pour les demandes de déchargement entrantes.	Oui	Autorisation de la demande de déchargement
glide.basicauth.required.xml	Demandez l'autorisation de base pour les demandes XML entrantes.	Oui	Autorisation de demande XML
glide.basicauth.required.xsd	Demandez l'autorisation de base pour les demandes XSD entrantes.	Oui	Autorisation de la demande XSD
glide.cms.catalog_uri_relative	Appliquez des liens relatifs à partir du paramètre URI sur /ess/catalog.do. Si **oui**, seules les URL relatives sont autorisées via la page /ess/catalog.do à l'aide du `uri` paramètre. Si **ce n'est pas le cas**, toutes les URL sont autorisées, ce qui peut permettre la création de liens vers des contenus externes non autorisés.	Oui	Renforcer les liens relatifs
glide.set_x_frame_options	Activez cette propriété pour définir	Oui	X-Frame-Options: SAMEORIGIN

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	l'en-tête de réponse X-Frame-Options sur SAMEORIGIN pour toutes les pages de l'interface utilisateur. L'en-tête de réponse HTTP X-Frame-Options peut être utilisé pour indiquer si un navigateur doit être autorisé à rendre une page dans un <frame> ou <iframe>. Les sites peuvent utiliser cette propriété pour éviter les attaques de détournement de clic en vérifiant que leur contenu n'est pas incorporé dans d'autres sites. https://developer.mozilla.org/en/the_x-frame-options_response_header		
glide.ui.attachment.download_mime_types	Une liste de types MIME de pièce jointe séparés par des virgules qui ne sont pas alignés dans le navigateur. Prévient les attaques par script de site à site. Par exemple, text/html force le téléchargement des fichiers HTML vers le client en tant que pièces jointes plutôt que leur affichage aligné dans le navigateur.	texte/html, image/svg, image/svg+xml	Forcer le téléchargement Types MIME
glide.security.groupby_acl_check	Lorsque cette propriété est activée, les vérifications d'ACL pour les opérations Grouper par sont effectuées	Oui	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	pour les noms de groupe en fonction des données réelles des groupes.		
glide.security.diag_txns_acl	Si **oui**, seul l'utilisateur administrateur ou l'utilisateur à partir de l'adresse IP autorisée peut accéder à `stats.do`, `threads.do` et `replication.do`.	Non	Surveillance des performances (ACL)
glide.ui.security.codetag.allow_script	Autorisez le HTML incorporé (utilisant des balises [code]) pour contenir les balises JavaScript. **Remarque :** Cette propriété est définie sur **vrai** par défaut dans les versions ultérieures Vancouver et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client.	Non	Autoriser le code HTML intégré
glide.script.allow.ajaxevaluate	Activez le processeur AJAXEvaluate. L'appel d'API `AJAXEvaluate` permet au client d'envoyer et d'exécuter des scripts arbitraires sur le serveur.	Non	Activer AJAXEvaluate
glide.login.autocomplete	Autorisez les navigateurs à utiliser la saisie semi-automatique sur les champs de mot de passe	Non	Saisie semi-automatique du champ Mot de passe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
	des formulaires de connexion.		

Les propriétés suivantes sont définies dans la table sys_properties, mais ne sont pas visibles sur la page Paramètres de sécurité élevée.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
com.glide.communications.httpclient.verify_hostname	Vérifiez le nom d'hôte et la chaîne de certification présentés par les hôtes SSL distants. Protégez-vous contre les attaques de l'homme du milieu (MITM). Pour plus d'informations, consultez Configurer un spoke Kubernetes **Remarque :** Cette propriété remplace la propriété com.glide.communications.trustmanager_trust_all.	VRAI	Aucun
glide.basicauth.required.schema	Demandez l'authentification de base pour les demandes de schéma de table entrantes.	VRAI	Aucun
glide.security.csrf_previous.autoriser	Autorisez l'utilisation d'un jeton de sécurité expiré pour identifier et valider les demandes entrantes. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête de site à site.	faux	Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur par défaut	Paramètres de la sécurisation pour la sécurité de l'instance
glide.security.csrf_previous.time_limit	Délai en secondes avant l'expiration d'un jeton de sécurité. Permet de contrôler la durée de validité du jeton CSRF précédent. Lorsque la session utilisateur expire, le jeton de sécurité expire avec elle, sauf si la *glide.security.csrf_previous.allow* propriété est activée et qu'elle se trouve dans la période décrite dans cette propriété. Ce jeton est utilisé pour éviter les attaques de contrefaçon de requête de site à site.	86400 **Remarque :** Valeur en secondes. Équivalent à 1 jour.	Aucun
glide.security.csrf.strict.validation.mode	Applique une validation stricte sur les jetons CSRF afin que les utilisateurs ne puissent pas soumettre à nouveau une demande si le jeton CSRF ne correspond pas.	faux	Validation stricte du CSRF
com.glide.security.check_unapplied_html	Applique le comportement de nettoyage de translated_html champs à un niveau global pour les affectations de champs.	appliquer	Aucun

Configuration de la propriété du bac à sable de script

Activez la propriété de bac à sable de script (*glide.script.use.sandbox*) pour exécuter des scripts générés par le client dans un bac à sable avec des droits restreints.

Il existe deux cas dans le système qui permettent au client d'envoyer des scripts au serveur pour évaluation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Filtres et/ou requêtes : Il est légal d'envoyer un filtre au serveur tel que : assigned_to=javascript :getMyGroups().
- API système : L'appel d'API `AJAXEvaluate` permet au client d'exécuter des scripts arbitraires sur le serveur et de recevoir une réponse.

Si vous activez la propriété de bac à sable de script (`glide.script.use.sandbox`), le script évalué via l'un de ces deux points d'entrée s'exécute dans un bac à sable à droits réduits avec les caractéristiques suivantes :

- Seules les règles métier marquées **client pouvant être appelé** sont disponibles dans le bac à sable.
- Seules les inclusions de script marquées Client **pouvant être appelé** sont disponibles dans le bac à sable.
- Certains appels d'API (en grande partie, mais pas entièrement, ceux traitant d'un accès direct à la base de données) ne sont pas autorisés.
- Les données ne peuvent pas être insérées, mises à jour ou supprimées depuis le bac à sable. Tous les appels à `current.update(),` par exemple, sont ignorés.

Remarque :
Pour en savoir plus sur cette propriété, reportez-vous Bac à sable pour les scripts générés par le client à la section Paramètres de sécurisation renforcée de la sécurité de l'instance.

Ces méthodes ne sont pas autorisées dans les scripts générés par le client lorsque le sandboxing de script est activé.

Méthodes restreintes

Classe	Méthode
GlideRecord	• `deleteMultiple()` • `deleteRecord()` • `getRowCount()` • `insérer()` • `update()` • `updateMultiple()`
GlideSystem (gs)	• `addErrorMessage()` • `addInfoMessage()` • `addMessage()` • `eventQueue()` • `flushMessages()` • `getEscapedProperty()` • `getProperty()` • `log()` • `logError()` • `logWarning()`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Méthodes restreintes (suite)

Classe	Méthode
	• `setProperty()` • `setRedirect()` • `setReturn()` • `workflowFlush()`
Champ d'applicationGlideRecord	• `deleteMultiple()` • `deleteRecord()` • `insérer()` • `update()` • `updateMultiple()`
ScopedGlideSystem (gs)	• `addErrorMessage()` • `addInfoMessage()` • `debug()` • `eventQueue()` • `executeNow()` • `getProperty()` • `getSessionToken()` • `info()` • `setRedirect()`
Date Glide GlideDateTime Heure de Glide	• `add()` • `addDays()` • `addDaysLocalTime()` • `addDaysUTC()` • `addMonthsLocalTime()` • `addMonths()` • `addSeconds()` • `addWeeks()` • `addYears()` • `compareTo()` • `getByFormat()` • `getDate()` • `getDayOfWeek()`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Méthodes restreintes (suite)

Classe	Méthode
	• `getDayOfWeekUTC` • `getDayOfWeekLocalTime()` • `getDayOfMonth()` • `getDayOfMonthLocalTime()` • `getDayOfMonthNoTZ()` • `getDayOfWeek()` • `getDayOfWeekLocalTime()` • `getDayOfWeekUTC()` • `getHourOfDayLocalTime()` • `getHourOfDayUTC()` • `getDaysInMonth()` • `getDaysInMonthUTC()` • `getDaysInMonthLocalTime()` • `getDisplayValueInternal()` • `getDisplayValue()` • `getHourLocalTime()` • `getLocalDate()` • `getLocalTime()` • `getMinutesLocalTime()` • `getMinutesUTC()` • `getMonthLocalTime()` • `getMonthNoTZ()` • `getMonthUTC()` • `getNumericValue()` • `getSeconds()` • `getTime()` • `getTZOffset()` • `getValue()` • `getYear()` • `getUserTimeZone()` • `getWeekOfYearLocalTime()` • `getWeekOfYearUTC()` • `getYearUTC()` • `getYearLocalTime()`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Méthodes restreintes (suite)

Classe	Méthode
	• `isDST()` • `onOrAfter()` • `onOrBefore()` • `setDayOfMonthUTC()` • `setDisplayValue()` • `setMonth()` • `setNumericValue()` • `setTZ()` • `setValue()` • `setValueUTC()` • `subtract()` • `toString()`
GlideSchedule	• `add()` • `isInSchedule()` • `load()` • `quandNext()`

Remarque :
Les méthodes GlideSystem (gs) `log(), logError()` et `logWarning()` peuvent être activées avec le sandboxing des scripts en définissant la `glide.security.sandbox_no_logging` propriété système sur `false`.

Si vous exécutez le système sans activer le sandboxing des scripts, aucune de ces restrictions ne s'applique.

Remarque :
Cette propriété est activée par défaut lorsque vous activez le module d'extension Paramètres de sécurité élevée. N'activez pas cette propriété en dehors du module d'extension.

Activation des paramètres de sécurité élevée

Le module d'extension Paramètres de sécurité élevée est actif par défaut sur toutes les nouvelles instances. S'il n'est pas actif sur votre instance, vous pouvez demander le module d'extension.

Avant de commencer
Rôle requis : aucun

Avant d'activer les paramètres de sécurité élevée sur une instance existante :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

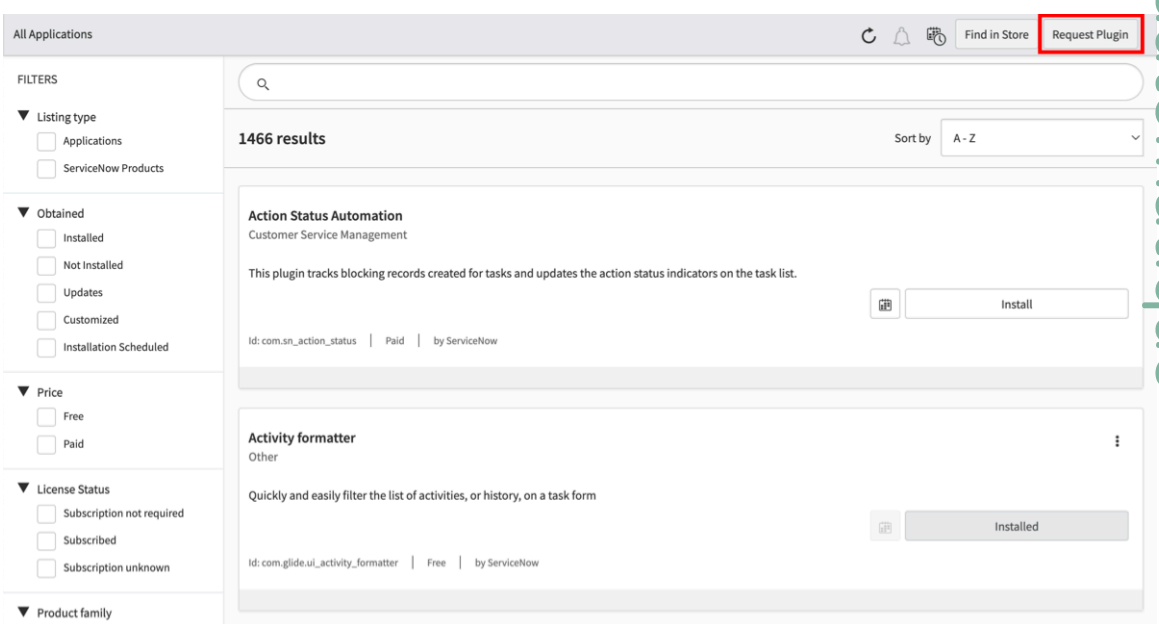
1. Examinez les informations suivantes pour comprendre le nouveau comportement :
   - Règles de la liste de contrôle d'accès
   - Paramètres de sécurité élevée
   - Propriété de refus par défaut
2. Activez le module d'extension sur une instance de non-production. Un clone récent de production est préférable.
3. Testez les fonctionnalités révisées, en particulier les ACL ajoutées et la fonctionnalité de refus par défaut. Continuez à tester jusqu'à ce que le système fonctionne comme prévu. Si les utilisateurs ne peuvent pas accéder aux ressources attendues, assurez-vous qu'ils disposent des rôles et des règles ACL appropriés pour leur accorder l'accès.
4. Créez des ensembles de mises à jour de tous les changements nécessaires afin de pouvoir les appliquer à la production.

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Module d'extension de haute sécurité Paramètres de renforcement de la sécurité de l'instance.

Rôle requis : admin

Procédure

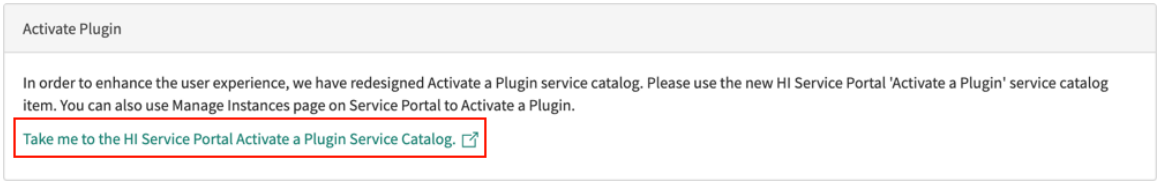
1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

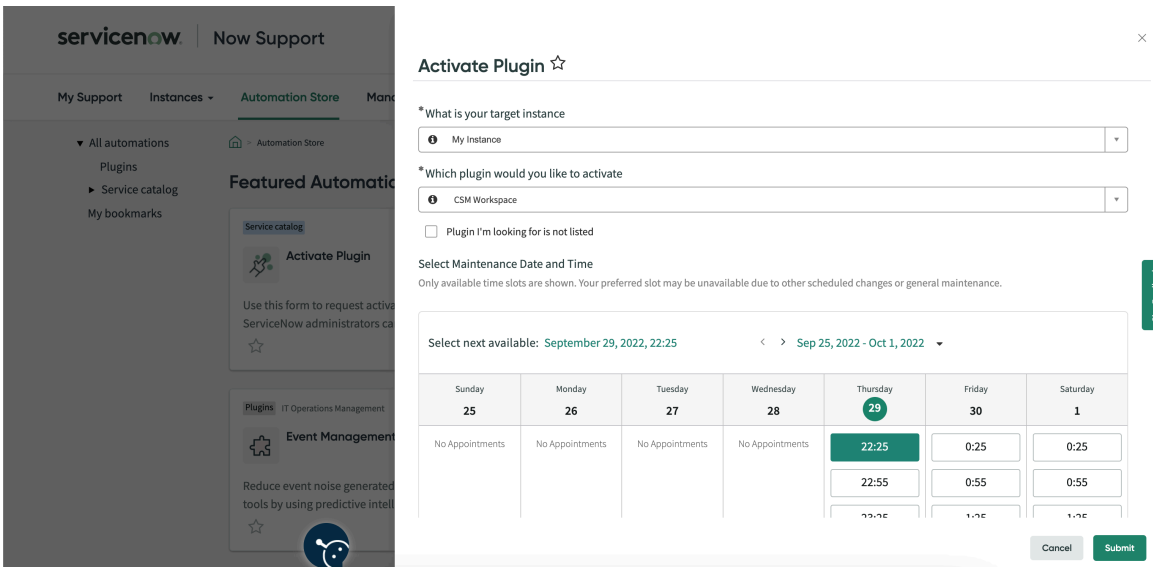
Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Activer le module d'extension



7. Sélectionnez **Envoyer**.
   Pour plus de détails sur la demande d'un module d'extension, consultez l'article Requesting a Plugin from the Service Catalog [KB0751715] de la Now Support Base de connaissances.

VPN (Virtual Private Network)

Utilisez un réseau VPN pour intégrer votre instance à des sources de données externes sur Internet.

Explorez	Activer Activer
	
Découvrez les fonctionnalités et les valeurs commerciales du réseau privé virtuel.	Active le réseau privé virtuel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer



Comprendre comment configurer un réseau privé virtuel.

Explorer le réseau privé virtuel (VPN)

Utilisez un réseau VPN pour intégrer votre instance à des sources de données externes sur Internet.

Mes informations IP

Lors de la configuration d'une intégration qui utilise un protocole chiffré, tel que LDAP (Lightweight Directory Access Protocol) ou HTTPS, il est recommandé d'utiliser Internet comme mécanisme de transport.

Toutefois, il peut y avoir des exigences en matière de sécurité ou d'architecture réseau qui dictent l'utilisation d'une connexion de réseau privé virtuel (VPN) de sécurité du protocole Internet (IPSEC) de site à site entre les centres de données et vos réseaux d'entreprise. Le VPN prend en charge la communication cryptée nécessaire entre l'instance et votre réseau.

Connexions VPN

L'infrastructure ServiceNow VPN utilise des paires de périphériques Cisco Adaptive Security Appliance (ASA) qui servent de points de terminaison VPN.

Le VPN entre l'instance et votre réseau utilise votre matériel réseau existant pour prendre en charge les communications. Il n'est pas nécessaire d'installer une pièce de matériel. Étant donné que chaque client dispose d'une configuration unique, l'instance dispose d'une solution VPN flexible. l'instance a créé des tunnels vers Checkpoint, Juniper, Nortel et d'autres appareils compatibles VPN IPSEC.

Les connexions VPN entre l'instance et votre réseau sont créées pour prendre en charge le flux chiffré de trafic entrant dans votre réseau. Souvent, les intégrations qui utilisent le VPN ne disposent pas de chiffrement dans le cadre du protocole sous-jacent. Par exemple, LDAP sur VPN versus LDAPS sur Internet et HTTP sur VPN versus HTTPS sur Internet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le réseau n'autorise aucune intégration entrante vers ServiceNow ou tout trafic de l'utilisateur final vers ServiceNow de transiter par une connexion VPN. Cette communication restreinte inclut l'accès de l'utilisateur final à la plateforme, l'administration de la plateforme, les intégrations de services Web et d'autres intégrations configurées pour utiliser un serveur MID. Toutes ces communications entrantes vers l'instance doivent être effectuées via Internet à l'aide du protocole HTTPS. Cette configuration fournit un canal de communication chiffré. Le canal de chiffrement, ainsi que le contrôle d'accès IP, répondent aux exigences de sécurité pour ce flux de trafic.

Adresses pour la communication VPN

Pour éviter les conflits ou les chevauchements avec les réseaux internes ServiceNow ou avec d'autres schémas d'adresses IP internes de votre réseau, tout le trafic tunnelisé dans le domaine de chiffrement doit utiliser des adresses autres que RFC-1918 des deux côtés du tunnel.

ServiceNow fournit une adresse IP unique pour la source des requêtes dans votre réseau. Vous devez fournir des adresses NAT (Network Address Translation) non RFC-1918 pour chaque hôte qui s'intègre à votre instance. Ces adresses publiques doivent appartenir à votre organisation. Les adresses tierces ne peuvent pas être utilisées à l'intérieur des tunnels. De plus, le domaine de chiffrement ne doit pas contenir l'adresse IP de l'homologue VPN.

Tunnels redondants

Il existe deux façons de créer une redondance pour vos tunnels :

- En utilisant le même domaine de chiffrement derrière vos deux pairs. C'est la méthode à privilégier.
- Utilisation d'un domaine de chiffrement différent derrière chaque homologue.

Avec la première méthode, vous devez fournir la même adresse NAT derrière chacun de vos homologues pour créer un chemin de connexion à l'aide de cette adresse vers votre serveur. Le chemin d'accès à votre serveur peut être la même machine physique ou un miroir qui fournit des services identiques. Avec cette méthode, votre instance utilisera la même adresse IP pour se connecter à vos serveurs, que votre tunnel primaire ou secondaire soit actif. Si vous avez plus d'un serveur, suivez le même schéma pour vos serveurs supplémentaires. Cette méthode offre le plus de transparence à vos utilisateurs et est recommandée.

La deuxième méthode nécessite une configuration dans votre instance pour assurer la redondance. Lorsque le tunnel est utilisé pour LDAP, par exemple, vous pouvez fournir des serveurs LDAP redondants dans votre instance. Notez que cette méthode nécessite que la connexion au premier serveur LDAP configuré expire avant que l'instance ne tente de se connecter au serveur secondaire. En raison de ce délai supplémentaire, cette solution ne doit être mise en œuvre que si la première option est inaccessible. Notez également que tous les services ne peuvent pas être configurés de manière redondante dans votre instance. Si vous utilisez un tunnel VPN pour autre chose que LDAP et qu'une redondance est requise, vérifiez que votre configuration peut prendre en charge plusieurs adresses ou consultez la première option ci-dessus.

Alternatives à l'utilisation d'un VPN

Ces alternatives offrent un moyen plus simple de connecter votre instance aux ressources des ServiceNow centres de données et offrent un meilleur chiffrement. De plus, vous pouvez éviter tous les problèmes que les temps d'arrêt VPN pourraient causer, tels que rendre votre instance indisponible pour les utilisateurs en cas de problème avec le tunnel VPN.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentification unique et MID Server

Envisagez d'utiliser une combinaison de Single Sign-On (SSO) pour l'authentification et de Serveur MID pour la synchronisation des données utilisateur, plutôt que d'utiliser un VPN pour connecter votre serveur LDAP à votre instance. Pour les intégrations autres que LDAP, envisagez d'utiliser le chiffrement basé sur certificat.

Vous pouvez utiliser l'écouteur LDAP sur un MID Server pour synchroniser votre table utilisateur en temps quasi réel.

L'avantage de cette approche est qu'il n'y a pas de trous de pare-feu, de routes, de tunnels VPN ou d'autres paramètres réseau spéciaux à configurer et à maintenir. La solution SSO/MID-Server est la méthode la plus flexible, la plus sécurisée et la plus rentable pour réaliser l'intégration LDAP complète.

LDAP sur SSL

Une autre alternative à l'utilisation d'un tunnel VPN consiste à configurer LDAP sur SSL (LDAPS) directement sur Internet. Vous pouvez configurer un contrôleur de domaine en lecture seule et verrouiller l'instance dans votre DMZ en utilisant uniquement les adresses source de l'instance et les ports de destination de votre choix. Étant donné que les ports pour LDAP sont configurables dans votre instance, vous pouvez effectuer une traduction d'adresse de port (PAT) si vous le souhaitez. Avec LDAPS, vous contrôlez le certificat qui est téléchargé sur un canal chiffré vers l'instance (reportez-vous à la section Chargement d'un certificat dans une instance). Les paquets ne peuvent pas être chiffrés ou déchiffrés sans le certificat.

L'avantage de cette approche est qu'elle fournit un mécanisme de cryptage et de déchiffrement plus puissant. Un VPN ne peut chiffrer et déchiffrer le trafic entre les deux pairs assis sur Internet qu'avec une clé pré-partagée coordonnée, similaire à un mot de passe. LDAPS fournit un chemin chiffré plus long, de bout en bout, au niveau de la couche applicative et avec un certificat beaucoup plus compliqué qu'une clé pré-partagée utilisée par le tunnel IPSec.

Configuration VPN

À partir du moment où une demande de VPN est soumise, il faut généralement une semaine ou moins pour terminer la version du VPN. Pour prendre en charge les exigences de redondance de votre instance et de votre organisation, un minimum de deux et un maximum de quatre VPN sont provisionnés (du site actif vers votre site actif ou du site actif vers votre site DR, etc.).

Il est recommandé que le domaine de chiffrement soit aussi précis que possible. Idéalement, le domaine de chiffrement inclurait uniquement les hôtes spécifiques requis pour les intégrations. Un grand domaine de chiffrement peut créer des opportunités de divergences de routage (VPN par rapport à Internet).

Pour créer le VPN, l'instance effectue les opérations suivantes :

1. Fournit l'homologue VPN et les adresses d'hôte de chaque centre de données.
2. Crée la connectivité VPN nécessaire à partir de deux centres de données dans votre réseau. Pour prendre en charge les exigences de redondance et de reprise après sinistre (DR), les VPN peuvent être provisionnés à partir de deux centres de données dans deux réseaux.

L'instance ne prend pas en charge la création de plusieurs tunnels VPN dans un réseau client dans le but de se connecter à plusieurs régions géographiques ou filiales. Vous devez effectuer tout routage intersite, distribution du trafic ou mise en forme du trafic au sein de votre propre réseau interne, plutôt que d'avoir plusieurs tunnels VPN.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activation d’un service VPN

Pour toutes les demandes VPN, y compris les provisionnements, les modifications ou les questions d’ordre général, utilisez le formulaire Demande de VPN de Catalogue de services.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à https://support.servicenow.com/now?draw=case.
2. Sélectionnez l’onglet **Automation Store** .
3. Utilisez l’arborescence sur la gauche pour accéder à **Toutes les automatisations** > **Catalogue de services** > **Infrastructure de cloud**.
4. **Sélectionner des demandes VPN**
5. Sélectionnez le type de demande VPN approprié.
6. Répondez aux questions.
   Les questions varient en fonction du type de demande sélectionné.
7. Cliquez sur **Envoyer**.

Résultats
Une fois votre demande soumise, ServiceNow vous travaillerez avec votre ou vos ingénieurs réseau pour tester et valider que le VPN transmet correctement le trafic. Pour vous assurer que vous obtenez une réponse à vos questions en temps opportun, veuillez répondre aux questions relatives au VPN au cours de ce processus.

Configuration d’une adresse pour la communication VPN

Pour éviter les conflits ou les chevauchements avec les réseaux internes ServiceNow ou avec les schémas d’adresses IP internes d’un autre client, l’instance exige que tout le trafic tunnelisé dans le domaine de chiffrement utilise des adresses autres que RFC-1918 des deux côtés du tunnel.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
L’instance fournit une adresse IP unique pour la source des requêtes dans votre réseau.

Procédure

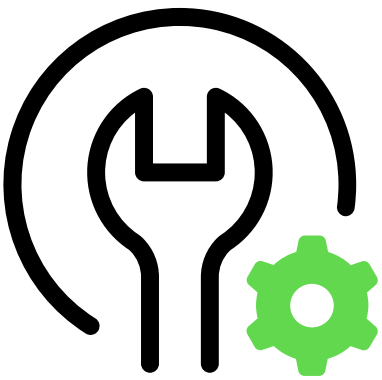
Fournissez des adresses NAT (Network Address Translation) non RFC-1918 pour chaque hôte qui s’intègre à l’instance.

Autres paramètres et ressources de sécurité

Cette section contient les propriétés de sécurité que vous définissez en dehors du centre de sécurité de l’instance, ainsi que d’autres ressources liées à la sécurité.

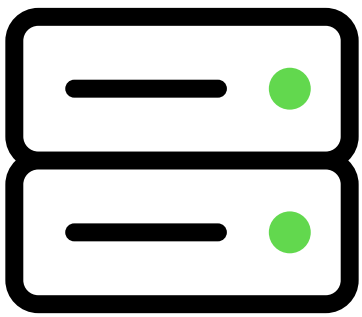
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



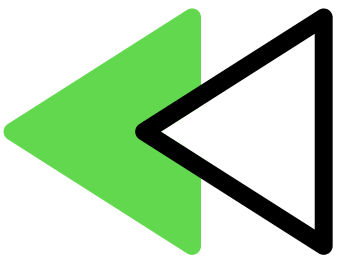
Propriétés système de sécurité

Les paramètres de sécurité fournissent plusieurs propriétés pour contrôler le niveau de sécurité de votre instance.



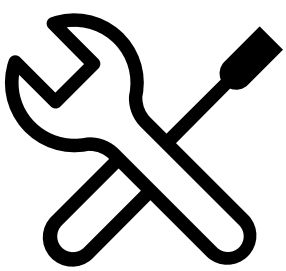
Guide de déploiement du MID Server

Le serveur MID (ServiceNow Management, Integration, and Discovery) est une application Java légère qui s'exécute en tant que service Windows ou démon UNIX sur du matériel standard, notamment des ordinateurs virtuels.



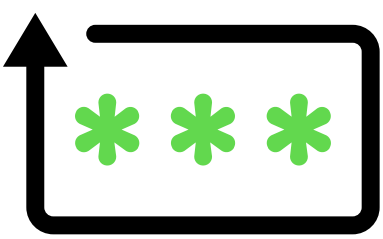
Comportement réversible

Certaines propriétés système sont classées comme « safe_overrides » ou « no_db_override ».



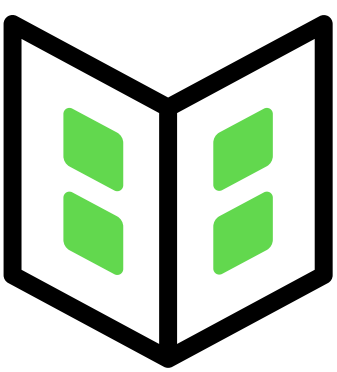
Propriétés de sécurité dépréciées

Ces propriétés de sécurité ont été déconseillées dans les versions précédentes.



Utilisation du contrôle d'accès au contenu JavaScript

Vous pouvez utiliser le contrôle d'accès au contenu JavaScript pour modifier la liste des URL JavaScript tierces bloquées au sein de votre instance.



Autres ressources de sécurisation renforcée

Sources supplémentaires d'informations sur le renforcement des contrôles de sécurité, en lien avec Now Platform.

Traduction automatique

Propriétés des paramètres de sécurité

Les paramètres de sécurité fournissent plusieurs propriétés pour contrôler le niveau de sécurité de votre instance.

Il existe plusieurs façons de définir ou de modifier les propriétés des paramètres de sécurité généraux.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Accédez à la **Propriétés système** > **Sécurité**.

  Les options de la page Sécurité sont **Oui** ou **Non**.

- Accédez à la **sys_properties.list** et recherchez la propriété que vous souhaitez définir ou modifier.

  Les options de la table Propriétés système [sys_properties.list] sont **vrai** ou **faux**.

- Accédez à la **Sécurité de système** > **Centre de sécurité de l'instance**, puis cliquez sur **Sécurisation renforcée**.

  Vous pouvez configurer les paramètres des propriétés de sécurité les plus importantes et les plus critiques. Le contenu des paramètres de renforcement de la sécurité de l'instance contient des descriptions détaillées et des valeurs de conformité pour les propriétés système et les modules d'extension liés à la sécurité dans le Now Platform. Pour en savoir plus sur chacune de ces propriétés, reportez-vous à la section Paramètres de la sécurisation pour la sécurité de l'instance.

⚠ Avertissement :
Lors de l'implémentation de l'une de ces fonctionnalités de sécurité, vous devez tester minutieusement les fonctionnalités avant de les déployer dans une instance de production.

Prise en charge de l'échappement et du script incorporé

glide.ui.security.allow_codetag	Prend en charge l'incorporation du code HTML à l'aide de la balise [code]. Valeur par défaut : oui **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Autoriser le code HTML intégré
glide.ui.security.codetag.allow_script	Permet au HTML incorporé (utilisant des balises [code]) de contenir les balises Javascript. **Remarque :** Cette propriété est définie sur **vrai** par défaut dans les versions ultérieures Vancouver et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client. Pour en savoir plus, voir Autoriser les balises JavaScript dans le HTML intégré.
glide.ui.escape_all_script	Force l'échappement par défaut de toutes les expressions dans Jelly JavaScript `<![CDATA[<script type="text/javascript">]]>` balises. Applique l'échappement uniquement si l'attribut type de la `<![CDATA[<script>balise ]]>` est vide ou si la valeur est `text/javascript`, `text/`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	ecmascript, application/javascript, application/ecmascript ou application/x-javascript. • Valeur par défaut : ○ Instances nouvelles/zbootées : vrai ○ Instances mises à niveau : false • Valeur recommandée : oui **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Échapper à Jelly

Limites et comportement des pièces jointes

com.glide.attachment.max_taille	Définit la taille maximale de la pièce jointe en mégaoctets.
glide.attachment.role	Répertorie les rôles (séparés par des virgules) qui peuvent créer des pièces jointes.
glide.attachment.extensions	Répertorie les extensions de fichier (séparées par des virgules) qui peuvent être jointes à des documents via la boîte de dialogue de pièce jointe. Les extensions ne doivent pas inclure le point (.). Par exemple, xls, xlsx, doc, docx. Laissez vide pour autoriser toutes les extensions. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Restreindre les extensions de fichiers
glide.ui.attachment.force_download_all_mime_types	Force le téléchargement de tous les fichiers en pièce jointe de type MIME (Multipurpose Internet Mail Extensions). Valeur par défaut : • Instances nouvelles/zbootées : oui • Instances mises à niveau : non **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Forcer le téléchargement Types MIME
glide.security.file.mime_type.validation	Active (**Oui**) ou désactive (**Non**) la validation du type MIME pour les pièces jointes de fichiers. Le type MIME est vérifié pendant `glide.attachment.extensions`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	le chargement pour les extensions de fichier configurées via Valeur par défaut : • Instances nouvelles/zbootées : oui • Instances mises à niveau : non **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Restriction sur les types MIME de téléchargement

Chargements du client

Ces propriétés affectent uniquement les chargements des clients. Ils n'affectent pas les pièces jointes.

glide.ui.strict_customer_uploaded_static_content	Lorsque vous définissez cette propriété sur **Oui**, il est possible de restreindre les types de fichiers qui peuvent être téléchargés lorsqu'ils ont été chargés à l'aide de la fonctionnalité Charger un Now Platformfichier du . Utilisé avec `glide.ui.strict_customer_uploaded_content_types` **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Activer les restrictions de téléchargement de fichiers
glide.ui.strict_customer_uploaded_content_types	Lorsque ce paramètre inclut une liste de types de fichiers délimités par des virgules, des fichiers qui ont été chargés à l'aide de la fonctionnalité Charger un fichier de , Now Platformseuls ces types de fichiers peuvent être téléchargés à partir de l'instance. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Spécifier les types de fichiers téléchargeables

Gestionnaire de sécurité et options

glide.security.manager	Gestionnaire de la sécurité.
glide.sm.default_mode	Comportement par défaut du gestionnaire de sécurité en l'absence de tout ACL dans une table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

glide.security.strict.updates	Revérifie la sécurité des transactions entrantes lors de la soumission du formulaire. Les droits sont toujours vérifiés lors de la génération de formulaires. **Remarque :** Cette propriété est définie sur **vrai** par défaut et ne peut pas être modifiée par les administrateurs. Pour un cas d'utilisation où la propriété doit être modifiée, contactez le support client. Pour en savoir plus, voir Double vérification des transactions entrantes.
glide.security.strict.actions	Vérifie les conditions des actions d'interface utilisateur avant leur exécution. Normalement, les conditions ne sont vérifiées que pendant le rendu du formulaire. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Vérifier l'action d'interface utilisateur avant son exécution
glide.security.granular.create	Applique les règles de création sur les nouveaux enregistrements (par opposition aux règles d'écriture, qui peuvent inclure la création et la mise à jour).
glide.security.explain.write.locks	Affiche une explication sur les éléments de formulaire verrouillés.

Cookies

glide.ui.forgetme	Supprime la case à cocher **Se souvenir de moi** de la page de connexion lorsque l'instance utilise des connexions LDAP ou BD. Les sessions connectées actives de l'utilisateur expirent après X minutes d'inactivité, où X est la valeur de la propriété système **glide.ui.session_timeout** . Valeur par défaut : oui (nouvelles instances et instances démarrées par Z) **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Supprimer Se souvenir de moi
glide.ui.secure_cookies	Active les cookies de session sécurisés pour renforcer la sécurité des cookies. Si **oui**, la validation stricte des cookies de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	session est appliquée. Avec les cookies de version 3 activés, des exigences de sécurité supplémentaires sont également appliquées. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Cookies de session sécurisés
glide.secure_cookie.debug	Débogage sécurisé des cookies de session. Sélectionnez cette option pour permettre la journalisation de débogage étendue des opérations de cookies de session sécurisée.

Restrictions de sécurité pour l'exécution de scripts en provenance du client

glide.script.use.sandbox	Exécutez les scripts générés par le client (AJAXEvaluate et conditions de requête) dans un bac à sable à droits réduits. Si activé, seuls les règles métier et les includes de script pour lesquels la case **Client joignable** est cochée sont disponibles, et certains appels d'interface de programmation d'application (API) back-end sont interdits. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Bac à sable pour les scripts générés par le client
glide.script.allow.ajaxevaluate	Active le processeur AJAXEvaluate. **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Activer AJAXEvaluate
glide.script.secure.ajaxgliderecord	Applique des listes de contrôle d'accès de sécurité (ACL) standard aux appels AJAXGlideRecord. Valeur par défaut : oui, pour les instances nouvelles et mises à niveau. (Si **oui**, il ne peut pas être remplacé par **Non**.) **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Activation de la vérification de l'ACL de AJAXGlideRecord

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

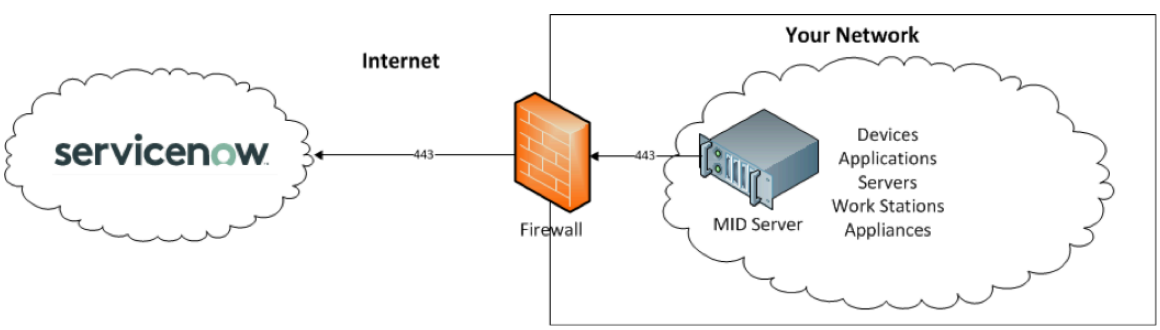
Divers

com.glide.communications.trustmanager_trust_all	Par défaut, l'instance fait confiance à l'autorité de certification (CA) d'un certificat. Garantit que l'instance accepte les certificats auto-émis. Pour valider l'autorité de certification d'un certificat, définissez cette propriété sur **Non** **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Certificat de confiance
glide.outbound.sslv3.disabled	Lorsqu'elle est active, elle force les connexions sortantes d'une instance à utiliser TLS (Transport Layer Security) au lieu de SSL (Secure Sockets Layer). **Remarque :** Paramètres de la sécurisation pour la sécurité de l'instance : Désactivation de SSLv2/SSLv3

Des propriétés supplémentaires sont disponibles pour Paramètres de sécurité élevée.

Guide de déploiement sécurisé de MID Server (renforcement de la sécurité de l'instance)

Le ServiceNow serveur MID (Management, Integration, and Discovery) est une application Java légère qui s'exécute en tant que service Windows ou démon UNIX sur du matériel standard, notamment des ordinateurs virtuels.



Il s'authentifie en toute sécurité auprès de votre instance dans le cloud à l'aide ServiceNow de ses propres identifiants de connexion et facilite la transmission des données avec vos applications, sources de données et services. Plusieurs MID Servers peuvent être déployés dans différents segments du réseau pour offrir une évolutivité supplémentaire.

Tenez compte des facteurs suivants concernant la sécurité de votre MID Server :

Sécurité physique

Sécurisez le matériel physique qui héberge le MID Server ou l'hyperviseur pour les MID Servers virtualisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Placez le matériel dans un endroit sécurisé qui le protège contre tout accès non autorisé.
- Protégez l'accès à cet emplacement à l'aide d'un lecteur de carte électronique et d'une vidéosurveillance.
- Placez le matériel physique dans une cage verrouillée ou un rack avec contrôle d'accès à la clé physique.

Sécurité de l'infrastructure virtuelle

Utilisez la virtualisationavec la flexibilité d'installer plusieurs MID Servers dans des systèmes d'exploitation virtualisés et des réseaux sur du matériel physique partagé.

L'accès à l'hyperviseur et aux consoles de gestion de l'infrastructure virtuelle doit être protégé pour empêcher le clonage non autorisé du MID Server virtualisé :

- Limitez l'accès à l'hyperviseur et aux consoles de gestion de l'infrastructure virtuelle par quelques administrateurs de confiance.
- Autorisez uniquement les connexions au réseau de confiance interne pour la console de gestion, tel que ESX Server et VirtualCenter.
- Utilisez les VLAN pour éviter les attaques réseau.
- Suivez les consignes de sécurité publiées dans les guides de renforcement de la virtualisation des fournisseurs.

Sécurité du système d'exploitation

Découvrez comment le Serveur MID stocke son nom d'utilisateur et son Now Platform mot de passe dans son fichier de configuration, nommé config.xml, pour une authentification sécurisée à l'instance.

Le serveur MID doit être déployé dans un système d'exploitation sécurisé et renforcé pour assurer la protection contre tout accès non autorisé aux informations d'identification :

- Limitez l'accès au système d'exploitation à quelques administrateurs de confiance.
- Surveillez les journaux du système d'exploitation pour détecter tout accès non autorisé, en particulier les tentatives d'accès au fichier config.xml, car ce fichier contient des informations importantes sur la configuration de Serveur MID.
- Installez régulièrement les correctifs de sécurité du système d'exploitation avec les logiciels antivirus les plus récents et mettez régulièrement à jour les définitions antivirus.
- Le serveur MID nécessite un cadre de travail Java actuel pour s'exécuter. Maintenez Java à jour régulièrement.
- Supprimez ou désactivez les services et applications inutiles.
- Installez un pare-feu du système d'exploitation pour limiter l'accès aux ports non autorisés.
- Suivez les consignes de sécurité publiées dans les guides de sécurisation renforcée du système d'exploitation des fournisseurs.

Sécurité réseau

Le MID Server communique sur le port 443 à l'aide du protocole SSL vers l'instance et ne nécessite aucune connexion entrante.

Pour sécuriser correctement votre MID Server dans un réseau, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Installez le serveur MID sur un serveur sécurisé derrière un pare-feu d'entreprise pour vous protéger contre tout accès non autorisé à partir d'Internet.
- Configurez le pare-feu sur le serveur MID pour qu'il n'accepte aucune connexion entrante autre que celles requises pour la gestion d'entreprise du système d'exploitation et du matériel.
- Le système qui héberge le MID Server doit être en mesure d'accéder ServiceNow au site de téléchargement à **install.servicenow.com**.

Remarque :
Cette URL renvoie au site de téléchargement, qui n'est ServiceNow pas accessible à partir de cette rubrique.

L'ordinateur hôte de MID Serve doit être en mesure d'accéder à ce site pour télécharger le package d'installation. Il contacte **install.servicenow.com** toutes les 60 minutes pour voir si une version plus récente est disponible et si c'est le cas, il effectue une mise à niveau automatique. Une mise à niveau de Serveur MID a également lieu lorsque vous mettez à niveau une instance.

Pare-feu

Configurez votre pare-feu pour autoriser le trafic réseau sortant du serveur MID vers votre instance et mettre à niveau automatiquement le serveur.

Pour configurer votre pare-feu, utilisez les exemples de syntaxe suivants :

- `<source IP> VERS <instance_name>.service-now.com SUR LE PORT 443`
- `<source IP> À install.service-now.com SUR LE PORT 443`

Administrer et gérer

Cette section décrit les pratiques de sécurité et les directives pour l'administration et la gestion du serveur MID dans votre environnement.

Créer un compte avec un rôle mid_server

Créez un compte utilisateur dans l'instance qui contient un rôle mid_server.

Lorsque vous créez un compte utilisateur, suivez les instructions suivantes :

- N'utilisez pas de compte administratif dans l'instance pour le Serveur MID.
- Utilisez une longueur et une complexité de mot de passe suffisantes pour le compte de Serveur MID.
- Le mot de passe doit comporter au moins 12 caractères avec des majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Utilisez différents comptes de Serveur MID avec des mots de passe uniques pour différents Serveurs MID dans une instance.
- Utiliser la fonctionnalité de sécurité SOAP stricte pour protéger toutes les tables avec des listes de contrôle d'accès (ACL) en activant *`Enforce strict security on incoming SOAP requests`* dans **Propriétés système** > **Services web**.
- Changez les mots de passe du Serveur MID à la fréquence qui correspond à la politique de mot de passe de votre organisation.

Remarque :
Pour en savoir plus, consultez Créer l'utilisateur de Serveur MID et accorder le rôle .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration d'un MID Server sur un hôte Windows

Lorsque vous installez le Serveur MID sur un hôte Windows, il crée un service Windows. Par défaut, ce service s'exécute en tant que compte système Windows local. Une fois l'installation terminée, remplacez le service Windows nouvellement créé par un compte avec le moins de privilèges requis pour exécuter le Serveur MID sur l'hôte Windows.

1. Accédez à la **Gestion des ordinateurs** > **Services et applications** > **Services**.
2. Cliquez avec le bouton droit sur **Serveur MID ServiceNow**, puis cliquez sur **Propriétés**.
3. Cliquez sur l'onglet **Se connecter** dans la fenêtre contextuelle.
4. Cliquez sur la case d'option en regard de **Ce compte**.
5. Entrez le nom d'utilisateur et le mot de passe appropriés du compte sous lequel le service doit s'exécuter.
6. Cliquez sur **OK**.
7. Dans la fenêtre Services, cliquez avec le bouton droit sur **Serveur MID ServiceNow**, puis cliquez sur **Redémarrer**.
8. Assurez-vous que le MID Server a pu redémarrer et se connecter à l'instance.

Informations d'identification de découverte et d'orchestration Windows

Configurez un compte Windows ou Active Directory local sur les systèmes cibles avec le moins de privilèges nécessaires. Il n'est peut-être pas nécessaire d'utiliser les informations d'identification d'administrateur de domaine.

Les pages de documentation produit suivantes fournissent des conseils sur le type de compte à utiliser et les autorisations requises.

- Informations d'identification Windows
- Sondes Windows et autorisations
- Microsoft Just Enough Administration (JEA) pour Discovery

Informations d'identification de détection et d'orchestration Linux

Utilisez un compte non-root avec des privilèges sudo limités sur les systèmes Linux cibles lors de la découverte et de l'orchestration.

Suivez les instructions suivantes :

- Utilisez une longueur et une complexité de mot de passe suffisantes pour le compte Linux. Le mot de passe doit comporter au moins 12 caractères avec des majuscules, des minuscules, des chiffres et des caractères spéciaux.
- Lors de la configuration des autorisations sudo, les chemins d'accès locaux aux fichiers exécutables binaires peuvent différer en fonction de la distribution Linux que vous exécutez, voir Commandes privilégiées du serveur MID .

Chiffrer les informations d'identification de connexion au MID Server

Par défaut, les informations d'identification de connexion au Serveur MID sont chiffrées dans le fichier config.xml.

Lors de la modification du fichier config.xml et de la fourniture du mot de passe, assurez-vous que l'attribut encrypt="true » existe, à l'aide de la syntaxe suivante :

```
<parameter name="MID.instance.username » value="MIDsrvadmin » />
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

<parameter name="MID.instance.password » encrypt="true » value="$ECUREpassw 0rd"/>

Remarque :
Le chiffrement des informations d'identification de connexion au serveur MID ne remplace pas un hôte de serveur non sécurisé avec une sécurité physique et réseau médiocre. Le mot de passe stocké dans le fichier config.xml est chiffré au premier démarrage du MID Server ou, s'il s'agit d'un MID Server existant, au redémarrage.

Définir la taille minimale du groupe DH sur 2 048 bits

Le National Standard Institute of Technology (NIST) a interdit l'utilisation de la clé Diffie-Hellman (DH) 1024 bits après l'année 2013. Définissez la taille minimale du groupe DH à 2048 bits à la place.

1. Dans l'instance, accédez à **Serveur MID** > **Serveurs**.
2. Cliquez sur le nom du Serveur MID pour lequel vous souhaitez désactiver cette fonctionnalité.
3. Dans la configuration du Serveur MID, cliquez sur le bouton **Nouveau** en regard de Paramètres de configuration.
4. Dans Paramètres de configuration du serveur MID, configurez les paramètres suivants :
   - **Nom de paramètre** mid.ssh.dh_group_length_min
   - **Valeur** 2048

Désactiver le SSL sortant

Vous pouvez désactiver SSLv2 et SSLv3 dans le Now Platformfichier . La définition de cette propriété force le serveur MID à utiliser TLS, en profitant de sa sécurité accrue, lors de l'établissement de connexions sortantes, telles que des demandes REST et SOAP.

1. Dans l'instance, accédez à **Serveur MID** > **Propriétés**.
2. Ajoutez un paramètre de configuration et définissez sa valeur comme suit :
   - **Nom** : glide.outbound.sslv3.disabled
   - **Valeur** : vrai

Désactiver les algorithmes faibles

Vous pouvez désactiver les algorithmes les plus faibles afin que les requêtes adressées à n'importe quel serveur HTTP non compatible TLS 1.2 échouent là où elles fonctionnaient auparavant.

Modifiez le fichier jre/lib/security/java.security dans le dossier de l'agent, en utilisant la syntaxe suivante :

jdk.tls.disabledAlgorithms=SSLv3, TLSv1, TLSv1.1, [autres algos faibles...]

Remarque :
Gardez à l'esprit que ce fichier est écrasé lors de la mise à niveau, vous devez donc avoir un processus en place pour réactualiser ce fichier après chaque mise à niveau.

Les utilisateurs de Powershell doivent consulter leur Windows administrateur pour obtenir de l'aide afin de désactiver les versions inférieures de TLS. Pour savoir quelles versions de TLS sont utilisées dans PowerShell, utilisez la commande [enum] ::GetNames([Net.SecurityProtocolType]).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comportement réversible

Certaines propriétés système sont classées comme « safe_overrides » ou « no_db_override ».

Remplacement sécurisé

Les valeurs de ces propriétés ne peuvent pas être modifiées une fois modifiées (elles ne sont pas réversibles).

Remarque :
Les administrateurs ne sont pas en mesure de renommer ou de supprimer la propriété de remplacement sécurisé.

Attribut	Catégorie
Refus par défaut	Contrôle d'accès
Activation de la vérification de l'ACL de AJAXGlideRecord	Contrôle d'accès
Protection de la vie privée sur les includes de script pouvant être appelés par le client comprend	Contrôle d'accès
Bac à sable pour les scripts générés par le client	Validation de l'entrée
Remplacement du mode de collecte (obsolète)	Liste d'inclusion de sécurité

Aucun remplacement de base de données

Les valeurs existantes de ces propriétés ne peuvent pas être modifiées ou remplacées.

Attribut	Catégorie
Activer les restrictions de téléchargement de fichiers	Pièces jointes

Propriétés de sécurité déconseillées

Ces propriétés de sécurité ont été déconseillées dans les versions précédentes.

Remplacement du mode de collecte (obsolète)

La *glide.whitelist.manager.collection_mode.override* propriété a été conçue pour fournir une rétrocompatibilité pour les instances hautement personnalisées. Il utilisait des appels de packages qui ont été créés sur une version antérieure à Calgary et qui ont depuis été dépréciés.

En savoir plus

Attribut	Description
Nom de la propriété	*glide.whitelist.manager.collection_mode.override*
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut	Description
Objectif	La désactivation de la propriété Mode de collection comble la faille de sécurité qui existe lors de l'importation d'appels de package Java dans une instance.
Valeur recommandée	faux
Impact fonctionnel	(Faible) Il ne devrait pas y avoir d'impact tant que les résultats de la section 10.6 sont examinés et approuvés. Pour garantir le bon fonctionnement de l'instance, testez les changements dans un environnement de non-production avant le déploiement dans l'environnement de production
Risque de sécurité	Les appels d'API côté client (élevés) qui entraînent la récupération de données ou l'accès à des objets sur le serveur sont considérés comme dangereux du point de vue de la sécurité. Validez-les pour l'autorisation et la restriction d'accès aux objets sensibles.

Authentification SMTP (obsolète)

Propriété *glide.smtp.auth* désignée si un serveur SMTP doit exiger des entrées d'authentification de nom d'utilisateur et de mot de passe.

En savoir plus

Attribut	Description
Nom de la propriété	glide.smtp.auth
Type de configuration	Propriétés système (/sys_properties_list.do)
Configurer dans le centre de sécurité de l'instance	Non
Objectif	Applique l'authentification SMTP
Valeur recommandée	VRAI
Impact fonctionnel	(Élevé) Cette remédiation impose une authentification au serveur de messagerie externe avant que le contenu ne soit remis sous la forme d'un e-mail. Si l'automatisation est configurée pour fournir du contenu d'e-mail, il peut y avoir un impact jusqu'à ce que vous définissiez la propriété et fournissiez un nom d'utilisateur/mot de passe approprié pour l'accès au serveur de messagerie.
Risque de sécurité	(Faible) Activez l'authentification SMTP avant d'envoyer le contenu au serveur de messagerie externe. L'authentification doit toujours avoir lieu avant que les transactions n'aient lieu vers/depuis l'instance.
Références	Propriétés d'e-mail

Utilisation du contrôle d'accès au contenu JavaScript

Si vous avez effectué une mise à niveau, vous pouvez utiliser le contrôle d'accès au contenu JavaScript pour modifier la liste des URL JavaScript tierces bloquées au sein de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Si vous êtes un client mis à niveau, vous disposez d'un accès en lecture et en écriture à la table.

Si vous êtes un nouveau client, tous les enregistrements sont masqués. Contactez ServiceNow® le support pour obtenir de l'aide.

Rôle requis : administrateur

Procédure

1. Dans le navigateur d'application, recherchez `sys_js_content_provider_rule.list`.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Règle du fournisseur de contenu JavaScript

Champ	Description
Actif	Option qui, lorsqu'elle est sélectionnée, la règle devient active. Lorsque cette option est décochée, si aucune autre règle ne correspond, l'URL **du chemin d'accès** est admise.
Chemin d'accès	URL absolue vers un fichier JavaScript. **Remarque :** Chaque chemin a quatre variantes. Par exemple, le chemin d'accès `/scripts/lib/jquery/jquery-1.8.2.min.js` bloque les URL suivantes : ○ /scripts/lib/jquery/jquery-1.8.2.min.js ○ /scripts/lib/jquery/jquery-1.8.2.min.jsx ○ /lib/jquery/jquery-1.8.2.min.js ○ /lib/jquery/jquery-1.8.2.min.jsx
Action	Option pour ○ **Refuser** : le serveur renvoie une réponse **404 introuvable** pour l'URL du **chemin d'accès** ou l'une de ses variantes. ○ **Autoriser** : le serveur renvoie le contenu du fichier pour l'URL du **chemin d'accès** ou l'une de ses variantes. ○ **Redirection** : le serveur renvoie le contenu d'un autre fichier comme spécifié dans le champ Chemin d'accès de la redirection.
Application	Option qui spécifie le champ d'application de la règle. **Global** est la valeur par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Cette fonctionnalité ne dépend pas du périmètre/de l'application ou du domaine.
Chemin de redirection	Champ qui clarifie le chemin d'accès vers lequel la redirection. Lorsque **l'action** est définie sur **Rediriger**, le contenu de cette URL est proposé à une demande d'URL du **chemin d'accès** .

4. Cliquez sur **Envoyer**.

Autres ressources de sécurisation renforcée

Vous trouverez ci-dessous d'autres sources d'information sur le renforcement des contrôles de sécurité en ce qui concerne le Now Platform.

Ressource	Description
Portail de test de sécurité	Portefeuille des services de sécurité sur HI
KB0538598	Test d'intrusion de l'application client | Politique et procédure
KB0546756	Désactivation de l'accès public au système de gestion du contenu (CMS)
KB0550071	ServiceNow, Inc. Examen du contrôle d'accès à l'instance
KB0550613	Identification et activation des restrictions d'adresse IP
KB0550828	Auditer et examiner les transactions GlideAjax
KB0550837	Rattrapage du sandboxing de script
KB0551031	Rattrapage de sécurité pour l'interface utilisateur de réinitialisation du mot de passe
KB0552835	Rattrapage pour les comptes d'utilisateurs de démonstration
KB0529232	ServiceNow, Inc. Surveillance : vue d'ensemble et aperçu
KB0564232	Utilisation de ServiceNow, Inc. l'application Mobile avec authentification externe
Sécurité et risque	ServiceNow, Inc. Communauté

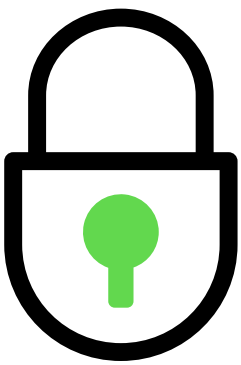
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Confidentialité de la plateforme

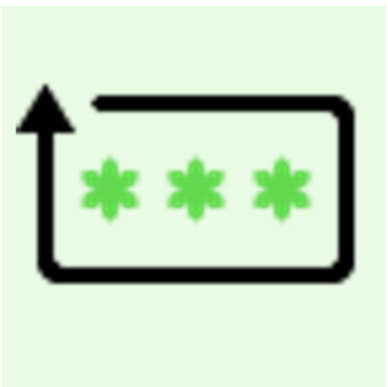
La confidentialité vous permet de masquer la date sensible sur l'instance.

Confidentialité des données



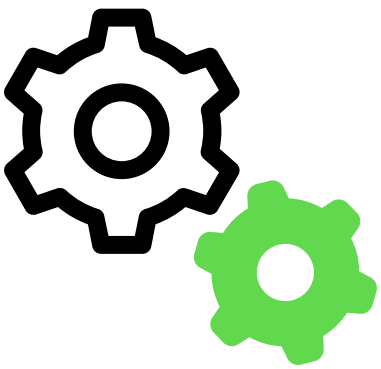
Utilisez Data Privacy pour classer les données sensibles et supprimer les informations à caractère personnel (PII) des données utilisateur dans une instance de production et anonymiser les données dans les instances de non-production.

Détection de données



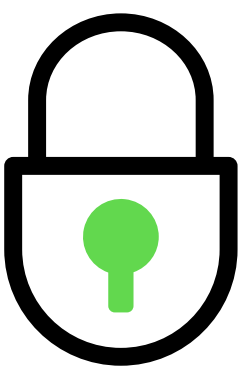
Utilisez la détection de données pour identifier les données sensibles au sein d'une instance afin de classer, protéger ou générer des rapports.

Classification des données



Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez administrer différentes classes de données ou analyser visuellement l'état actuel de différents types de données au sein de l'instance.

Anonymisation des données



L'anonymisation des données permet de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

transformer facilement les données afin qu'elles ne soient pas identifiables et de les rendre plus conformes à la réglementation en matière de confidentialité des données.

Confidentialité des données

Utilisez Data Privacy pour classer les données sensibles et supprimer les informations à caractère personnel (PII) des données utilisateur dans une instance de production et anonymiser les données dans les instances de non-production. Une fois anonymisées, les données utilisateur ne sont plus considérées comme des informations privées réglementées.

Explorez la confidentialité des données



En savoir plus sur la confidentialité des données.

Configurer Confidentialité des données



Découvrez comment configurer Confidentialité des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles dans la confidentialité des données



Obtenir des détails sur les rôles dans Confidentialité des données.

Fonctionnalités avancées de Confidentialité des données



Découvrez les fonctionnalités avancées de Confidentialité des données.

Traduction automatique

Exploration de la confidentialité des données

Utilisez Data Privacy pour classer les données sensibles et supprimer les informations à caractère personnel (PII) des données utilisateur dans une instance de production et anonymiser les données dans les instances de non-production. Une fois anonymisées, les données utilisateur ne sont plus considérées comme des informations privées réglementées.

Explique l'importance de la confidentialité des données et les mesures que les entreprises peuvent prendre pour protéger les informations sensibles par le biais de la classification et de l'anonymisation. À l'aide de l'application de stockage Confidentialité des données, nous donnons une vue d'ensemble du tableau de bord principal et des options.

Les développeurs doivent utiliser les données des instances de non-production pour s'assurer que leurs implémentations fonctionnent comme prévu. Bien que l'importation de données à partir de votre instance de production soit un moyen utile de simuler la production, elle présente un risque pour la sécurité. Les administrateurs peuvent utiliser la confidentialité des données pour fournir aux développeurs des données qui ne contiennent pas d'informations privées afin qu'ils puissent travailler en toute sécurité dans un environnement de non-production.

Classification des données

Identifiez et classez vos données sensibles selon des critères prédéfinis déterminés par le niveau de sensibilité des types de données dans votre instance. Les niveaux de sensibilité des données aident à déterminer comment chaque type de données classifiées doit être traité. Plusieurs classes prédéfinies sont fournies avec la confidentialité des données au niveau de base. Utilisez la section de classification de Confidentialité des données pour

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

étiqueter et regrouper les données au sein de votre instance. Ajoutez des classes, affichez la structure des classes de données et classez les données. Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur.

Explique comment classer les données à l’aide de l’application de stockage Confidentialité des données

Anonymisation des données utilisateur

En tant qu’administrateur, vous décidez s’il faut anonymiser toutes les informations pour tous les utilisateurs ou pour un sous-ensemble d’utilisateurs. Lorsqu’elles sont anonymisées, les données des enregistrements des utilisateurs sélectionnés sont remplacées par des valeurs randomisées ou des valeurs que vous définissez. Lors du remplacement des valeurs, il est possible de conserver la structure des données à l'aide de diverses techniques.

Explique comment anonymiser des données à l’aide de l’application de stockage Confidentialité des données

Options de confidentialité des données

- Confidentialité des données (classique): utilisez d’abord l’application de classification des données pour regrouper vos données par type, à l’aide de classifications de données prédéfinies ou définies par l’utilisateur. Créez ensuite des techniques et des tâches de confidentialité des données pour anonymiser les informations PII.
- Confidentialité des données (App Store) : classez et anonymisez vos données à partir de l’application de confidentialité des données.

Considérations

- Seules les données classifiées peuvent être anonymisées. Pour plus d’informations sur les classes de données et la classification, consultez Classification des données (classique) ou Classification des données App Store.
- Les informations PII dans les journaux et autres données d’audit ne sont pas anonymisées.
- Seules les données structurées peuvent être anonymisées. Les données non structurées, telles que les champs de journal, les commentaires, les pièces jointes et les autres champs où un texte partiel peut représenter des informations PII ne sont pas anonymisées. Consultez Types de champs pris en charge pour l’anonymisation pour plus d'informations.
- Les intégrations avec des systèmes d’authentification unique (SSO) peuvent resynchroniser les informations utilisateur à partir de leurs systèmes sources de vérité. Il n’y a pas de mécanisme en place pour assurer la permanence de la dépersonnalisation des données sys_user. Pour plus d’informations sur l’administration et la sys_users utilisateurs, reportez-vous à la section Administration des utilisateurs .

Séparation de domaine et confidentialité des données

La confidentialité des données n’est pas prise en charge de Séparation de domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Aucun

- Le champ Domaine peut être présent dans les tables de données, mais il n'existe aucune logique métier pour gérer les données.
- Ce niveau n'est pas considéré comme étant séparé par domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Information associée

Séparation de domaine pour les fournisseurs de services

Types de champs pris en charge pour l'anonymisation

Vérifiez quels types de champs sont pris en charge lors de l'anonymisation des données.

Remarque :
Tous les types de champs qui ont été classifiés ne sont pas disponibles pour l'anonymisation.

Certains types de champs à risque élevé sont désactivés par défaut, comme indiqué dans la table. Pour plus d'informations sur les champs, consultez Types de champs .

Types de champs pris en charge pour l'anonymisation

Type de champ	Disponible par défaut
audio	Non
condition	Non
condition_string	Non
currency	Oui
décimal	Oui
due_date	Oui
flotter	Oui
glide_date	Oui
glide_date_time	Oui
glide_duration	Non
glide_time	Oui
html	Non
icône	Non
entier	Oui
ip_addr	Non
ip_address	Non
journal	Oui
journal_input	Oui
journal_list	Oui
Entier long	Oui
name_values	Non
percent_complete	Non
phone_number_e164	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de champ	Disponible par défaut
price	Oui
chaîne	Oui
string_full_utf8	Oui
translated_html	Non
translated_text	Non
URL	Non
user_image	Non
vidéo	Non
wiki_text	Non

Rôles Confidentialité des données

La confidentialité des données ajoute ces rôles.

Administrateur de la confidentialité des données

Le rôle d'administrateur de Confidentialité des données est un rôle administrateur utilisé pour créer des techniques et des politiques de confidentialité des données.

Administrateur de la confidentialité des données [data_privacy_admin]

Contient des rôles

Aucun

Affecté à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Évitez d'affecter ce rôle à vos utilisateurs lorsque des rôles plus ciblés sont disponibles.

Pour affecter le rôle « Administrateur de la confidentialité des données », élevez l'utilisateur au rôle d'administrateur de sécurité afin d'ajouter le rôle.

Auditeur de la confidentialité des données

L'auditeur de confidentialité des données est un rôle en lecture seule utilisé pour afficher les enregistrements de confidentialité des données.

Auditeur de la confidentialité des données [data_privacy_auditor]

Contient des rôles

Aucun

Affecté à des groupes

Aucun

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Abonnement

Non

Élevé

Non

Considérations

Aucun

Processeur de clone Confidentialité des données

Les utilisateurs ayant le rôle de processeur clone Confidentialité des données peuvent créer et exécuter des tâches de confidentialité des données de classe de données.

Processeur de clone de confidentialité des données [data_privacy_clone_processor]

Contient des rôles

Aucun

Affecté à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Aucun

Processeur de confidentialité des données

Les utilisateurs ayant le rôle de processeur de confidentialité des données créent et exécutent des tâches de confidentialité des données sur la table utilisateur [sys_user].

Sous-traitant de la confidentialité des données [data_privacy_processor]

Contient des rôles

Aucun

Affecté à des groupes

Aucun

Abonnement

Non

Élevé

Oui

Considérations

Aucun

Confidentialité des données (classique)

Confidentialité des données (Classic) est disponible en tant que version familiale. Les dernières mises à jour de la famille ont été publiées lors du lancement de Tokyo.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer la confidentialité des données (classique)

Vous pouvez activer le module d'extension de confidentialité des données (com.glide.data_privacy) si Platform Security vous disposez du rôle administrateur. Cette application inclut des données de démonstration et installe les applications et modules d'extension associés ServiceNow® Store , le cas échéant.

Avant de commencer

La confidentialité des données nécessite un abonnement distinct du reste du Now Platformfichier .

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Lorsque vous achetez un abonnement, certains modules d'extension sont activés automatiquement. Si un module d'extension acheté n'est pas activé automatiquement, vous pouvez l'activer manuellement à partir de la liste Toutes les applications de votre instance.

Remarque :
Avant d'acheter un abonnement, vous pouvez évaluer Data Privacy (Classic) et Data Discovery avec une période d'essai de 30 jours. Après l'expiration de votre période d'essai, vous ne serez plus en mesure de découvrir des données ou d'exécuter des tâches d'anonymisation sans licence.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec Confidentialité des données :

- Modules d'extension
- Rôles
- Tables

Pour plus d'informations, consultez Composants installés avec Confidentialité des données (classique).

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Recherchez le module d'extension Confidentialité des données (com.glide.data_privacy) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée.

Composants installés avec Confidentialité des données (classique)

Découvrez les composants installés avec le module d'extension Confidentialité des données (com.glide.data_privacy).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables installées

Table	Description
Tâche fédérée Confidentialité des données [dp_federated_job]	Tâches fédérées pour la confidentialité des données
Tâche Confidentialité des données [dp_job]	Tâches Confidentialité des données
Tâche Confidentialité des données [dp_job_summary]	Résumés des tâches de confidentialité des données
Technique Confidentialité des données [dp_technique]	Techniques de confidentialité des données
Lien de référence primaire [dp_primary_reference]	Liens de référence primaires
Technique de champ classé pour la confidentialité [dp_field_technique]	Techniques de champs classifiés pour la confidentialité des données
Configuration de la confidentialité [dp_configuration]	Configurations de Confidentialité des données
Configuration de la technique de confidentialité [dp_technique_with_params]	Techniques de confidentialité des données
Paramètre de la technique de confidentialité [dp_technique_with_parameter]	Techniques de confidentialité des données avec des paramètres
Valeur de paramètre de la technique de confidentialité [dp_technique_with_parameter_value]	Valeurs de paramètres utilisées dans les techniques de confidentialité des données avec des paramètres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de la confidentialité des données (classique)

Découvrez comment créer des techniques et des politiques de confidentialité des données, et comment créer et exécuter des tâches de confidentialité des données.

Techniques de confidentialité des données

Les techniques de confidentialité des données sont des options que vous sélectionnez pour déterminer comment vos données sont anonymisées. Vous devez créer une technique de confidentialité des données à référencer dans la tâche de confidentialité des données. Reportez-vous à la section Créer une configuration de technique de confidentialité des données pour associer une technique de confidentialité à une **configuration de technique de confidentialité** associée.

Politiques de confidentialité des données

Configurez une politique de confidentialité des données pour spécifier quelles techniques de confidentialité des données sont utilisées lors de l'anonymisation de vos données. Consultez Créer une politique de confidentialité des données pour en savoir plus.

Tâches Confidentialité des données

Les tâches de confidentialité des données utilisent tous ces composants pour anonymiser vos données. Pour en savoir plus sur ces métiers, reportez-vous à la section Configurer une tâche de confidentialité des données.

Créer une configuration de technique de confidentialité des données

Créez une configuration de technique de confidentialité des données pour personnaliser la façon dont la confidentialité des données anonymise vos données.

Avant de commencer
Rôle requis : data_privacy_admin et admin

Procédure

1. Élevez-vous au rôle **data_privacy_admin** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Configuration de la technique de confidentialité**.
3. Cliquez sur **Nouveau**.
4. Dans le champ **Nom** , entrez un nom pour la configuration de votre technique de confidentialité.
5. Dans le champ **Technique de confidentialité** , sélectionnez une technique de confidentialité.

Techniques de confidentialité des données

Technique	Description
Aucune action	Cette technique est un espace réservé. Il ne modifie pas les champs lorsqu'il est sélectionné.
Remplacement aléatoire	Cette technique échange les valeurs avec des valeurs générées de façon aléatoire. Les données chaîne et numéro peuvent utiliser cette technique.
Remplacement sélectif	Cette technique remplace sélectivement les données de chaîne. Tous les caractères entre les index de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Technique	Description
	début et de fin de l'entrée sont remplacés par le caractère que vous choisissez. Vous pouvez spécifier des caractères à exclure du masquage : ○ start_index : la technique masque les données commençant par le caractère spécifié. Si ce champ est laissé vide, le masquage commence par le premier caractère. ○ end_index : la technique masque les données du début de la chaîne jusqu'au caractère spécifié. Si ce champ est laissé vide, le masquage se termine au dernier caractère. ○ exclude_char : définissez un caractère à exclure du masquage. ○ replacement_char : définissez un caractère utilisé pour le masquage. Si aucun n'est fourni, les astérisques (*) sont utilisés par défaut.
Remplacement statique	Cette technique échange les valeurs avec des valeurs statiques. Les données chaîne, numéro et date peuvent utiliser cette technique : ○ date_time_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss. ○ date_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj. ○ number_value : remplacez les valeurs de nombres par ce nombre. ○ string_value : remplacez les valeurs de chaîne par ce texte.
Supprimer	Cette technique supprime les valeurs et les remplace par des valeurs vides (nulles).

Remarque :
La valeur précédemment prise en charge **Remplacer** est déconseillée et renommée **Remplacement-Déconseillé** et ne doit pas être utilisée.

6. Cliquez avec le bouton droit sur l'en-tête, puis cliquez sur **Enregistrer** dans le menu contextuel.
   Une fois l'enregistrement enregistré, la liste **Valeurs paramétrées de confidentialité** s'affiche.
7. Utilisez les enregistrements de la liste **Valeurs paramétrées de confidentialité** pour personnaliser la configuration de votre technique de confidentialité des données.
   Les valeurs paramétrées disponibles dépendent de la technique de confidentialité que vous avez sélectionnée. Il n'existe aucune valeur paramétrée pour les techniques **Aucune action** et **Supprimer** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeurs paramétrées de confidentialité pour le remplacement sélectif

Valeur de paramètre de la technique de confidentialité	Description	Valeur par défaut
char_to_replace	Caractère à utiliser lors du remplacement de valeurs à l'aide d'un remplacement sélectif.	*
end_index	La technique masque les données du début de la chaîne jusqu'au caractère spécifié. S'il n'est pas renseigné, le masquage se termine au dernier caractère.	(Vide)
exclude_char	Caractère pour ignorer le masquage. Un seul caractère peut être utilisé dans cette valeur. Si plusieurs caractères sont saisis, le premier caractère est utilisé.	(Vide)
start_index	La technique masque les données commençant par le caractère spécifié.	1

Valeurs paramétrées de confidentialité pour remplacer

Valeur de paramètre de la technique de confidentialité	Description	Valeur par défaut
date_time_value	Remplacez les valeurs de date et d'heure par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss.	1988-11-11 10:10:10
date_value	Remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj.	1988-11-11
number_value	Remplacez les valeurs de nombres par ce nombre.	1234567
preserve_data_length	Définissez la valeur **sur vrai** pour préserver la longueur des données. Les données dépersonnalisées auront la même longueur que les données d'origine.	VRAI
string_value	Remplacez les valeurs de chaîne par ce texte.	TEXT123
use_random_generated_value	Définissez la valeur **sur vrai** pour remplacer les données par des valeurs générées de façon aléatoire. Seules les données de chaîne et de numéro peuvent être remplacées par des valeurs	faux

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur de paramètre de la technique de confidentialité	Description	Valeur par défaut
	aléatoires. Cette option remplace les valeurs statiques.	

8. Cliquez sur **Enregistrer**.

Créer une politique de confidentialité des données

Configurez une politique de confidentialité des données pour spécifier quelles techniques de confidentialité des données sont utilisées lors de l'anonymisation de vos données.

Avant de commencer

La configuration de confidentialité des données définit les tables, sys_user et autres, ainsi que les colonnes à dépersonnaliser, en fonction du cas d'utilisation, et spécifie les types paramétrés des techniques à utiliser lors de l'anonymisation des données.

Remarque :
Pour terminer une configuration de confidentialité, vous devez d'abord configurer une technique de confidentialité des données. Consultez Créer une configuration de technique de confidentialité des données pour plus d'informations.

Rôle requis : data_privacy_admin et admin

Procédure

1. Élevez-vous au rôle **data_privacy_admin** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données (classique)** > **Configuration de la politique de confidentialité**.
3. Sélectionnez **Nouveau**.
4. Dans le champ **Nom** , saisissez un nom pour la configuration de votre politique de confidentialité.
5. Dans le champ **Classe de données** , sélectionnez la classe de données à utiliser avec cette politique.
   Les politiques de confidentialité des données ne peuvent s'appliquer qu'aux données classifiées. Pour plus d'informations sur la classification des données, consultez Classification des données.
   Après avoir sélectionné une classe de données, les listes **Techniques de champ classé confidentialité** et **Liens de référence primaires de confidentialité** s'affichent sur le formulaire.
6. **Facultatif :** Sélectionnez **Appliquer à toutes les données de la classe** pour appliquer l'anonymisation à toutes les données de la classe de données choisie.
   Si vous ne sélectionnez pas ce champ, les utilisateurs de votre processeur de confidentialité des données peuvent choisir les utilisateurs à anonymiser lors de la création de tâches de confidentialité des données. Si vous sélectionnez ce champ, cette option n'est pas disponible.
   - **Appliquer lors du clonage** : cette option devient disponible. Lorsque cette option est sélectionnée, la configuration de confidentialité s'exécute pendant le clone de confidentialité des données.
   - **Ordre d'application** : une tâche de confidentialité des données pour la configuration Postclone avec un ordre d'application plus élevé peut commencer avant une autre tâche avec un ordre inférieur.

   Important :
   Évitez de créer plusieurs politiques de confidentialité des données avec le même ordre d'application, car l'ordre de traitement qui en résultera pour celles ayant le même ordre sera incohérent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. **Facultatif :** Sélectionnez **Prend en charge la restauration** pour activer la possibilité de désanonymiser les données à partir d'une tâche de confidentialité des données.
   Consultez Restaurer une tâche de confidentialité des données pour plus d'informations.
   Après avoir sélectionné **Prendre en charge la restauration** lors de la création d'une tâche de confidentialité des données, l'option de restauration de la tâche devient disponible.
8. Sélectionnez l'onglet **Techniques de champ classé pour la confidentialité** pour afficher la liste **des techniques de champ classées pour la confidentialité** .
9. Sélectionnez une entrée dans le champ **Table** pour ouvrir le champ **Configuration de la technique de confidentialité** pour chaque entrée de liste.
   La liste **Techniques de champ classifiées pour la confidentialité** affiche toutes les données à anonymiser dans la classe de données sélectionnée. Pour chacune de ces entrées, vous devez sélectionner une technique de confidentialité à appliquer.
10. Sélectionnez une **configuration de technique de confidentialité** à appliquer.

> **Important :**
> Si vous n'anonymisez pas une entrée, sélectionnez la technique **DoNothing** plutôt que de laisser l'entrée vide. Les politiques avec des valeurs vides dans le champ Configuration de la **technique de confidentialité** ne peuvent pas s'exécuter lorsqu'elles sont utilisées dans des tâches de confidentialité des données.

11. Sélectionnez **Soumettre** ou **Enregistrer** pour enregistrer l'enregistrement.

Que faire ensuite
Configurer une tâche de confidentialité des données.

Configurer une tâche de confidentialité des données

Configurez une tâche de confidentialité des données sur votre instance de production pour utiliser des données rendues anonymes sur votre instance de non-production pour les tâches d'utilisateur et de classe de données.

Avant de commencer
La tâche de confidentialité des données prend en charge deux cas d'utilisation de désidentification :

- Données sensibles d'sys_users spécifiques
- Données sensibles d'une classe de données particulière.

Rôle requis : data_privacy_processor et admin

Procédure

1. Élevez-vous au rôle **data_privacy_processor** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Tâche Confidentialité des données**.
3. Dans la liste des tâches Confidentialité des données, cliquez sur **Nouveau**.
4. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de tâche Confidentialité des données

Champ	Description
Nom	Nom de la tâche.
Description	Description de la tâche.
Configuration de la confidentialité	La configuration de la politique de confidentialité à utiliser pour cette tâche. Pour en savoir plus sur les configurations de la politique de confidentialité, reportez-vous à la section Créer une politique de confidentialité des données.
Utilisateurs	Sélectionnez les utilisateurs ou le groupe d'utilisateurs à anonymiser dans cette tâche. Jusqu'à 1 000 utilisateurs d'un groupe peuvent être traités. **Remarque :** Ce champ s'affiche uniquement lorsque la condition de politique de confidentialité sélectionnée exige une sélection d'enregistrements utilisateur.
Essai	Exécutez la tâche en tant que test. Aucun enregistrement n'est affecté lors de l'exécution de cette tâche. Les résultats s'affichent dans le champ **Résumé** comme si la tâche avait été exécutée. **Remarque :** **L'exécution d'essai** doit être désactivée lors de la configuration d'une tâche de confidentialité des données avec restauration. Consultez Restaurer une tâche de confidentialité des données pour en savoir plus.
État	État de la tâche de confidentialité des données : ○ **Prêt à planifier** : état par défaut pour les nouvelles tâches. ○ **Restauration en cours** : la tâche a été définie pour restaurer l'anonymisation. ○ **Restauration terminée** : la restauration de la tâche d'anonymisation s'est terminée avec succès. Un champ en lecture seule.
Estimer le nombre d'enregistrements	Nombre estimé d'enregistrements affectés par cette tâche. Un champ en lecture seule.
Résumé	Champ en lecture seule qui affiche les résultats de la tâche lorsque vous l'exécutez.
Début de la fenêtre de temps	Début de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécutera après l'heure saisie dans ce champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Une valeur de temps valide est exprimée en Temps universel coordonné sur la base d'une notation temporelle de 24 heures.
Fin de la fenêtre de temps	Fin de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécute avant l'heure saisie dans ce champ. Si la tâche n'est pas encore terminée, la tâche sera mise en pause et reprendra au prochain début de la fenêtre horaire. L'heure de fin doit être postérieure à l'heure de début. Une valeur de temps valide est exprimée en Temps universel coordonné sur la base d'une notation temporelle de 24 heures.

5. Cliquez avec le bouton droit dans l'en-tête du formulaire et sélectionnez **Enregistrer** dans le menu contextuel.
   Une fois l'enregistrement enregistré, les boutons **Planifier la tâche** et **Supprimer la tâche** s'affichent.
6. Cliquez sur **Planifier la tâche** pour exécuter votre tâche.
   La tâche s'exécute entre les heures sélectionnées dans les champs Début de la **fenêtre** de temps et Fin de la **fenêtre de temps** . Si la tâche n'est pas terminée pendant la fenêtre d'heure de début et de fin, la tâche se poursuivra au prochain début de la fenêtre de temps.

   Remarque :
   Une tâche ne peut être exécutée qu'une seule fois, même si **l'option Essai** est sélectionnée. Pour exécuter à nouveau la même tâche, créez une tâche de confidentialité des données à l'aide des mêmes valeurs de champ.

7. **Facultatif :** Choisissez l'une des fonctions suivantes :
   - **Annuler la tâche** : annule la tâche de confidentialité des données.
   - **Pause** : met en pause la tâche et l'enregistrement de restauration, si la restauration a été sélectionnée. Un message d'avertissement s'affichera après une période d'expiration de trois jours pour les contextes de restauration. Consultez Restaurer une tâche de confidentialité des données pour en savoir plus.
   - **Reprise** : redémarre une tâche en pause. La restauration n'est pas prise en charge pour les tâches qui reprennent si elles sont mises en pause. Annuler la tâche et créer une tâche de confidentialité des données. L'enregistrement utilise un contexte de restauration non expiré.

Restauration des tâches de confidentialité des données

Les changements de base de données sont capturés pour des actions telles que des tâches et des scripts afin que les changements puissent être annulés. Restaurez une tâche de confidentialité des données lorsqu'une erreur humaine anonymise par inadvertance des informations utilisateur incorrectes. La restauration annualise les données de la tâche de confidentialité des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble

- La restauration est limitée à quelques jours, en fonction de la durée d'expiration configurée du RollbackContext du nouveau RollbackType *REDACT*. Après l'expiration du RollbackContext associé à une tâche de confidentialité des données, la fonction de restauration n'est plus disponible pour cette tâche.
  - Un contexte de restauration issu de la désanonymisation est enregistré pendant trois jours par défaut.
  - Le délai d'expiration par défaut peut être défini sur une valeur supérieure à un par l'administrateur de la confidentialité des données dans le **RollbackContext** du nouveau **RollbackType** *REDACT*. Définissez la valeur dans la propriété `glide.rollback.expiration_days_redact`système Glide . Consultez Roll back and delete recovery .

    Pour en savoir plus sur l'ajout ou la création d'une propriété système, reportez-vous à la section Add a system property .

    pour plus d'informations.
- La restauration est disponible pour les tâches de confidentialité des données qui sont à l'état Terminé, Annulé ou Erreur.
- Un contexte de restauration est créé pour chaque tâche de désanonymisation sys_user réussie configurée avec une politique de confidentialité des données sur laquelle la prise en charge de la restauration est activée. Il peut y avoir au maximum un contexte de restauration par tâche de confidentialité des données.

Restaurer une tâche de confidentialité des données

Restaurez une tâche de confidentialité des données sur votre instance de non-production qui utilise des données rendues anonymes de votre instance de production à un état antérieur à la désidentification d'une tâche de classe de données ou d'utilisateur.

Avant de commencer

Rôle requis : data_privacy_admin ou data_privacy_processor, et admin

Procédure

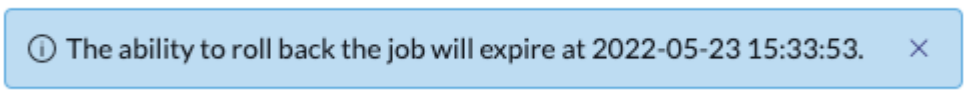
1. Accéder au **rôle data_privacy_processor** ou **data_privacy_admin** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Tout** > **Sécurité de système** > **Confidentialité des données** > **Tâche Confidentialité des données**.

   Remarque :
   Au préalable, une configuration de politique de confidentialité des données prenant en charge la restauration doit être créée. Créer une politique de confidentialité des données.
3. Créez une tâche de confidentialité des données et sélectionnez une configuration de confidentialité qui prend en charge la restauration.
   Consultez Configurer une tâche de confidentialité des données.
4. Planifiez la tâche d'anonymisation des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Une fois le travail exécuté, les données sont anonymisées pour la configuration sélectionnée.
- Un message s'affiche dans la tâche pour informer du délai d'expiration. Pendant la période d'expiration, vous avez la possibilité d'annuler la tâche.



5. Élevez-vous au rôle **data_privacy_processor** .
6. Ouvrez la tâche de confidentialité des données à restaurer.
7. Sélectionnez **Restaurer** pour désanonymiser les données.

Clone de confidentialité des données

Au fur et à mesure que les données client sont clonées d'une source vers une instance cible, généralement de la production à la non-production, les données sensibles sont anonymisées sur l'instance cible.

Un administrateur de la confidentialité des données configure des politiques post-clonage. Une fois le script post-clonage terminé sur l'instance cible, les utilisateurs voient les données anonymisées et n'ont pas accès aux données d'origine. Les administrateurs de la confidentialité des données peuvent configurer des politiques de désidentification à appliquer à l'instance cible lors du clonage afin de s'assurer que l'instance cible ne contiendra pas de données sensibles d'origine. Un ordre est spécifié pour la politique par rapport aux autres politiques à exécuter.

Remarque :
Le clonage de confidentialité des données est disponible sur les instances auto-hébergées.

Le clone de confidentialité des données possède les attributs supplémentaires suivants :

- Le module d'extension Confidentialité des données crée le script de post-clone à exécuter sur l'instance cible.
- Les tâches de confidentialité des données créées pour la configuration PostClone peuvent s'exécuter en parallèle si elles n'impliquent pas les mêmes tables.
- Une tâche de confidentialité des données pour la configuration Postclone avec un ordre d'application plus élevé peut commencer avant une autre tâche d'ordre inférieur, si la tâche d'ordre supérieur n'implique aucune table liée à une autre tâche d'ordre inférieur.
- Avec le module d'extension Confidentialité des données, les tables de confidentialité des données se trouvent par défaut dans l'ensemble de tables Conservateurs de données clones.
- Toute tentative d'ajout d'une table de confidentialité des données (dp_[table]) aux tables d'exclusion de clones recevra un avertissement, cette table ne doit pas être exclue.

Configurer la demande de clone Confidentialité des données

L'intégration du clone Confidentialité des données est configurée à l'aide d'un script PostClone pour créer et exécuter des tâches de confidentialité des données pour les politiques configurées sur la cible. Après avoir exécuté le script, les utilisateurs verront les données anonymisées et n'auront pas accès aux données d'origine.

Avant de commencer
Rôle requis : data_privacy_clone_processor, data_privacy_admin et admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Activez le module d'extension de confidentialité des données (com.glide.data_privacy) sur l'instance source.
   Le module d'extension ne peut être installé que par Service et assistance client.
   Le script PostClone de confidentialité des données est installé.
2. Élevez-vous au rôle **data_privacy_admin** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.
3. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Configuration de la politique de confidentialité**.
4. Créez une configuration de politique de confidentialité.
   Sélectionnez **Appliquer à tous dans la classe de données** et **Appliquer lors du clonage**.
   Consultez Créer une politique de confidentialité des données pour plus d'informations.
5. Sauvegardez les configurations de confidentialité des données.
6. En tant qu'administrateur de la confidentialité des données, soumettez une demande de clone.

Résultats

Le script PostClone s'exécute sur l'instance cible et le script PostClone crée un enregistrement de tâche fédérée sur la confidentialité des données sur l'instance cible. La tâche fédérée crée et exécute une tâche de confidentialité des données pour chaque politique post-clone, dans l'ordre de l'application, sur l'instance cible.La source de sauvegarde est clonée vers l'instance cible. Le script PostClone Confidentialité des données crée et exécute des tâches de confidentialité des données pour les politiques configurées sur l'instance cible.

Le processeur clone de confidentialité des données élevé peut se connecter à l'instance cible et surveiller l'état de la tâche fédérée post-clonage sur les dp_federated_job.list et dp_job.list.

Confidentialité des données

L'application de stockage Confidentialité des données est une actualisation Next Experience pour la classification et la confidentialité des données avec une apparence et une convivialité modernes. L'application de stockage de confidentialité des données est prise en charge dans Utah et les versions ultérieures.

La confidentialité des données est composée de plusieurs composants : vue d'ensemble, classification et anonymisation.

Vue d'ensemble

Utilisez la section Vue d'ensemble comme point de départ pour gérer vos données et la conformité à la confidentialité des données. Consultez Vue d'ensemble de la confidentialité des données pour en savoir plus.

Classification

La classification des données est le processus d'organisation des données en catégories qui facilitent leur récupération, leur tri et leur stockage pour une utilisation ultérieure. L'utilisation d'un système de classification permet de se concentrer sur les exigences de la politique de confidentialité et de sécurité. Classer les données à utiliser pour l'anonymisation. Pour plus d'informations sur les classes de données et la classification, reportez-vous à la section Classification des données.

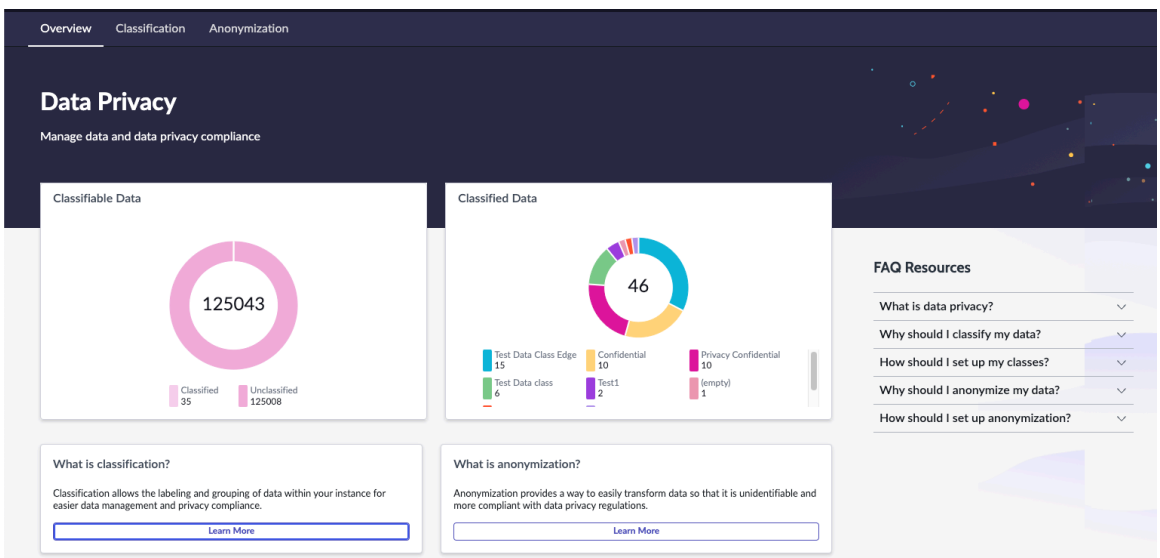
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d’ensemble de la confidentialité des données

La page d’accueil Vue d’ensemble est un point de départ pour gérer vos données et la conformité à la confidentialité des données.

Le tableau de bord Vue d’ensemble signale l’état actuel des classifications de données et des tâches d’anonymisation au sein de votre instance. Vous pouvez afficher vos données avec le tableau de bord Vue d’ensemble pour voir la quantité de données pouvant être classifiées, les classes de données disponibles, la quantité de données dans chaque classe et un état général des tâches d’anonymisation. Les données classifiées sont divisées en différentes catégories. La sélection d’une sous-catégorie dans l’un ou l’autre des graphiques ajoutera ou supprimera la catégorie du graphique global et ajustera les nombres.



Données classifiables

Affiche le nombre total d’enregistrements de données dans l’instance qui peuvent être classifiés. Ce nombre est ventilé entre le nombre total de données classifiées et le nombre total de données non classifiées. Cela donne aux administrateurs un aperçu rapide des opportunités de classification potentielles.

Données classifiées

Affiche le nombre total d’enregistrements de données de l’instance qui ont été classifiés. Ce nombre est réparti en nombre total de données classifiées pour chaque classe de données affectée. Cela permet de comprendre rapidement la quantité de données qui ont été classifiées dans chaque domaine.

Tâches d'anonymisation

Affiche les tâches de confidentialité des données actuellement en cours de traitement des tâches qui se sont terminées sur votre instance de non-production pour les tâches d’utilisateur et de classe de données.

En savoir plus

Les sections **En savoir plus** fournissent un aperçu rapide de la compréhension de la classification et de l’anonymisation, ainsi qu’un moyen facile de démarrer le processus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ressources de la FAQ

Accédez aux ressources d'apprentissage du produit sur la classification ou l'anonymisation pour plus d'informations sur la façon de commencer à sécuriser votre instance avec la confidentialité des données.

Activer la confidentialité des données

La confidentialité des données inclut la classification et l'anonymisation des données et est installée à partir du ServiceNow Storefichier .

Avant de commencer

Pour utiliser l'anonymisation des données, la confidentialité des données (classique) doit d'abord être activée avec l'autorisation ServiceNow Coffre-fort . Consultez Activer la confidentialité des données (classique) pour plus d'informations.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Applications système** > **Toutes les applications disponibles** > **Tout** > **Confidentialité des données**.
2. Utilisez les critères de filtre et la barre de recherche pour trouver l'application.

   Vous pouvez rechercher l'application à l'aide de son nom ou de son ID. Si vous ne trouvez pas l'application que vous recherchez, vous devrez peut-être la demander auprès du ServiceNow Store.

   Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et pour obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique. Pour obtenir des informations sur les notes de publication cumulatives pour toutes les applications publiées, consultez les ServiceNow Storenotes de publication relatives à l'historique des versions .
3. Sélectionnez une version de la liste et sélectionnez **Installer**.

   La boîte de dialogue Installer qui s'affiche répertorie toutes les dépendances installées avec votre application.
4. Si vous y êtes invité, suivez les liens vers le ServiceNow Store afin d'obtenir des autorisations supplémentaires pour les dépendances.
5. **Facultatif :** Si des données de démonstration sont disponibles et que vous souhaitez les installer, cochez la case **Charger les données de démonstration**.

   (Optional) Les données de démonstration comprennent des exemples d'enregistrements décrivant les fonctionnalités des applications pour les cas d'utilisation fréquents. Chargez les données de démonstration lors de la première installation de l'application sur une instance de développement ou de test.

   > **Important :**
   > Les données de démonstration ne sont pas disponibles pour un chargement ultérieur si vous ne les chargez pas lors de l'installation.
6. Sélectionnez **Installer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Classification des données

Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez administrer différentes classes de données ou analyser visuellement l'état actuel de différents types de données au sein de l'instance.

Data Classification Active la prise en charge de :

- Visibilité sur les types de données hébergées sur des Now Platform instances.
- Conformité aux lois sur la protection de la vie privée et respect des exigences réglementaires pour des secteurs tels que les services financiers et la fabrication de dispositifs médicaux.

Classifications des données

La classification des données est un processus autonome dans lequel vous appliquez manuellement des classifications de données aux entrées de dictionnaire existantes dans n'importe quelle table. Consultez Data dictionary tables pour plus d'informations.

- Vous classez les données comme vous le jugez approprié pour votre entreprise et vous pouvez modifier les classes de données disponibles si nécessaire.
- Lorsque vous classez des données, vous pouvez utiliser les classifications de données prédéfinies ou créer les vôtres. Bien que l'utilisation de classifications de données prédéfinies soit facultative, il est conseillé de le faire comme point de départ. Ces classifications de données prédéfinies sont incluses dans les données de démonstration que vous pouvez installer dans votre instance.
- Si vous créez vos propres classifications de données, vous pouvez également concevoir un système hiérarchique hiérarchique hiérarchique avec des classifications de données parentes et enfants.

Remarque :
Data Classification prend en charge Séparation de domaine, et la table data_classification elle-même est séparée par processus. Consultez Séparation de domaine et Data Classification pour plus d'informations.

Cas d'utilisation

Le Règlement général sur la protection des données (RGPD) est un règlement de l'Union européenne dont l'objectif est de permettre aux individus de contrôler leurs propres données personnelles. Vous pouvez utiliser des classifications de données, telles que les informations personnellement identifiables, pour identifier où les données personnelles sont stockées dans votre instance. En appliquant les mécanismes de sécurité appropriés pour protéger ces données personnelles contre les fuites, votre organisation répond aux exigences du RGPD.

Si vous stockez des informations sur vos clients dans le Now Platform, utilisez le code de classification des informations personnellement identifiables (PII) si nécessaire pour suivre les données soumises à la réglementation des lois locales sur la protection de la vie privée.

Vous pouvez appliquer une classification de données restreinte aux colonnes de la table Employés qui stockent des informations sensibles sur les employés, telles que les numéros de sécurité sociale (SSN). Les administrateurs et les auditeurs peuvent ensuite utiliser le tableau de bord Vue d'ensemble pour confirmer que vous avez affecté des classifications de données aux colonnes correctes. Ils peuvent également afficher les détails de classification pour des types d'informations restreints.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer des classifications des données

Créez vos propres classifications de données définies par l'utilisateur dans la table [data_classification] que vous pouvez ensuite affecter à des colonnes spécifiques dans des tables spécifiques. Créez de nouvelles classes de données pour démarrer le processus de classification.

Avant de commencer
Rôle requis : data_classification_admin, admin

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Confidentialité des données** > **Classification**.
2. Sélectionnez **+Ajouter une classe de données**.

> **Remarque :**
> Plusieurs classes de données sont incluses dans le système de base.

3. Renseignez les champs du formulaire.

Champ	Description
Nom de classe	Nom de la classification des données.
Classe parent	Nom de la classification de données parente à laquelle cette classification de données est subordonnée. Laissez le champ vide si cette classification de données n'est pas un enfant d'une classification de données parente.
Description	Description de la classification des données.

4. Cliquez sur **Envoyer**.
   La nouvelle classe de données est ajoutée. Si la classe de données est enfant, elle sera répertoriée sous le parent dans la barre de navigation de gauche.

Classifier des données

Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Affectez des classifications de données à des colonnes spécifiques de la table Dictionnaire [sys_dictionary]. Lorsque vous affectez des classifications de données, cela crée des entrées dans la table Classe de données du dictionnaire [m2m_dictionary_dataclass], que vous pouvez ensuite passer en revue dans le tableau de bord Vue d'ensemble.

Avant de commencer
Rôle requis : data_classification_admin, admin

Procédure

1. Sélectionnez **Nouveau** pour affecter les données d'une table à classer.
2. Sélectionnez la classe de données dans la liste déroulante.
3. Sélectionnez les enregistrements reflétant les tables et les colonnes à classer.
   Choisissez des lignes supplémentaires à afficher par page dans le tableau pour simplifier la localisation d'un tableau particulier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Classifier les données**.
   Les données sont classées sous le nom de classification dans la table Données classifiées.
5. Affichez ou exportez les données au format Excel, CSV, JSON ou PDF.
   Choisissez de télécharger les données dans le format choisi ou de les recevoir par e-mail.

Anonymisation en temps réel

Utilisez la politique d'anonymisation en temps réel (RTA) pour anonymiser les entrées de données en temps réel.

Vue d'ensemble RTA

Les utilisateurs créent une politique RTA via la page Politiques d'anonymisation. Des colonnes des tables cibles peuvent être sélectionnées pour RTA, après quoi des modèles de données actifs sont utilisés et leurs stratégies appliquées à toutes les entrées d'enregistrement valides aux colonnes ciblées pour RTA. Si une entrée correspond à un modèle de données actif, sa technique d'anonymisation associée sera utilisée pour l'anonymisation.

Conseil :
Si vous devez modifier la technique d'anonymisation, reportez-vous à la section Configurer Détection de données les modèles.

Échecs d'anonymisation en temps réel

En cas d'échec d'une politique RTA, vous pouvez examiner son état à l'aide de la Échecs d'anonymisation en temps réel table.

Échecs d'anonymisation en temps réel

Examinez les défaillances d'anonymisation (RTA) en temps réel.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Confidentialité des données (classique)**.
2. Passez en revue les défaillances RTA dans la table.

Titre de champ	Description
Colonne de table	Colonne de table dans laquelle la défaillance s'est produite.
Cause de la défaillance	Catégorie de la cause des défaillances.
Détails de la raison de la défaillance	Description brève résumant la cause de la défaillance.
Configuration de la confidentialité	La configuration de confidentialité RTA qui a échoué.
Enregistrement	L'enregistrement spécifique qui a échoué.
Nom de la table	Table dans laquelle l'échec s'est produit.
Horodatage	Heure de la défaillance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détection de données

Permet Détection de données d'identifier les données sensibles au sein d'une instance, telles que les informations de carte de crédit, les e-mails ou les numéros de sécurité sociale.

Explorer la détection de données



En savoir plus sur la découverte de données.

Configurer la détection de données



Obtenez de l'aide pour configurer la détection de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles dans la détection de données



En savoir plus sur les rôles dans la découverte de données.

Résultats de détection de données



Examinez les résultats de détection de données.

Traduction automatique

Explorer Détection de données

Permet Détection de données d'identifier les données sensibles au sein d'une instance, telles que les informations de carte de crédit, les e-mails ou les numéros de sécurité sociale.

Détection de données Exécute un ensemble de tâches défini par l'utilisateur sur un ensemble de tables. Les tâches recherchent et signalent des informations sensibles pour examen sur le Détection de données tableau de bord. Une tâche planifiée utilise automatiquement tous les modèles de données actifs et les tables cibles lorsqu'elle s'exécute.

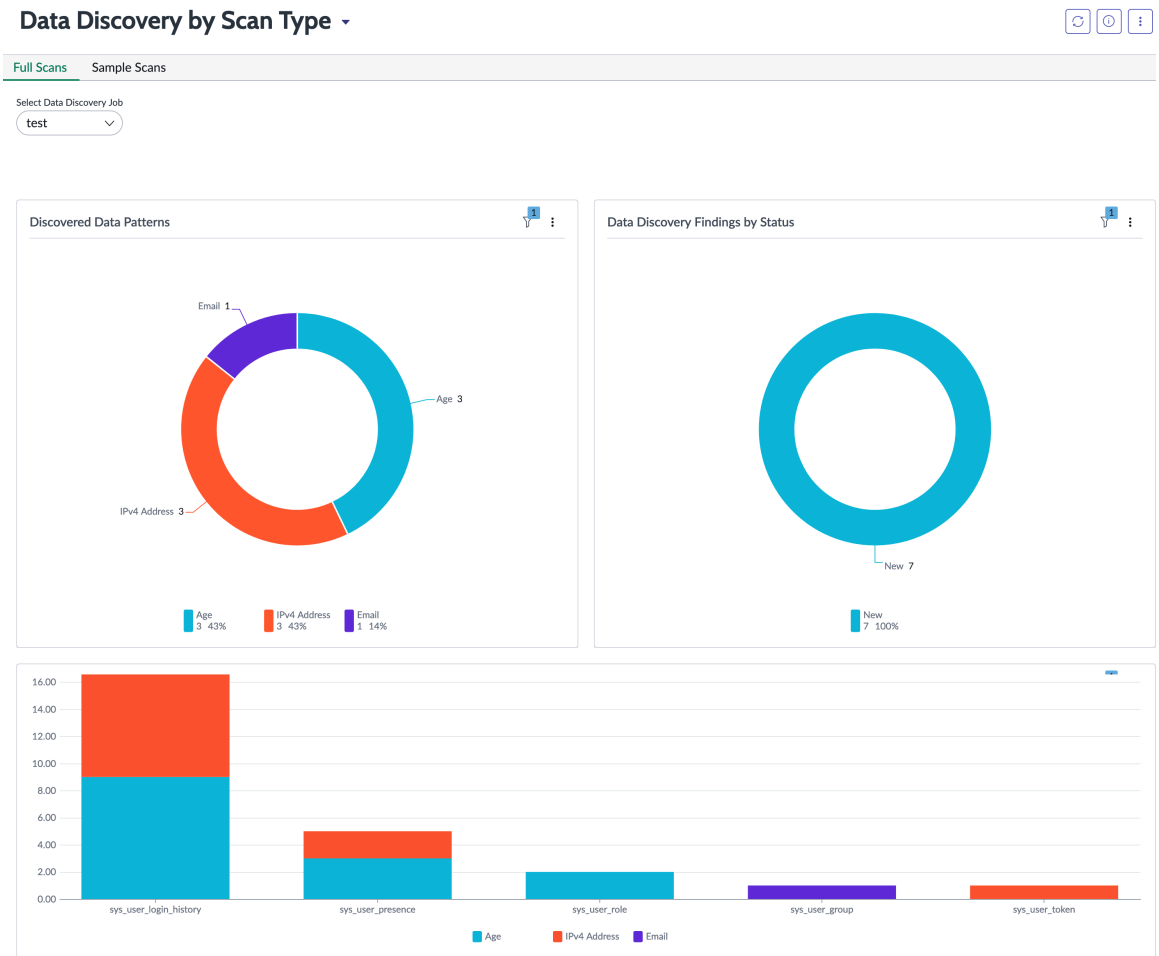
Détection de données inclut également des rôles préalloués avec différents niveaux d'accès aux données.

Accéder au tableau de bord Détection de données

Accédez à la **Tout** > **Sécurité de système** > **Détection de données (classique)** > **Tableau de bord** pour afficher le tableau de bord et passer en revue les Détection de données résultats de votre tâche actuelle.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tableau de bord de Détection de données



Modèles de données détectés

Conseil :
Sélectionnez un enregistrement pour afficher plus d'informations et prendre des mesures supplémentaires avec les résultats. Voir Détection de données Résultats des tâches pour en savoir plus.

Le graphique Schémas de données détectés affiche le nombre et le pourcentage de schémas de données actuellement détectés. Sélectionnez une section pour effectuer des actions supplémentaires.

Résultats de détection de données par état

Le graphique Résultats de détection de données passe en revue le nombre et le pourcentage de modèles de données actuellement détectés en fonction de leur état.

Tables détectées

Les tables détectées mettent en évidence les tables dans lesquelles se trouvent les données actuellement détectées et leur modèle de données.

Colonnes avec données détectées

La section Colonnes avec données détectées passe en revue les données actuellement détectées par colonne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer Détection de données

L’application s’installe Détection de données , ainsi que les applications et modules d’extension connexes ServiceNow® Store , le cas échéant.

Avant de commencer

La détection de données nécessite un abonnement distinct du reste du Now Platformfichier .

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Lorsque vous achetez un abonnement, certains modules d'extension sont activés automatiquement. Si un module d'extension acheté n'est pas activé automatiquement, vous pouvez l'activer manuellement à partir de la liste Toutes les applications de votre instance.

Remarque :

Avant d'acheter un abonnement, vous pouvez évaluer la fonctionnalité sur une instance de non-production sans frais en la demandant auprès du Now Support Catalogue de services.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec la découverte de données :

- Rôles
- Tables

Pour plus d’informations sur les rôles et les tables installés, consultez Détection de données rôles et Modèles de données par défaut.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Recherchez le module d’extension Détection de données (sn_data_discovery) à l’aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Classer les données dans Détection de données la page Résultats

Classez les données sensibles trouvées par toutes les tâches réussies via Détection de données les résultats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôles requis : data_discovery_admin

Une tâche doit terminer une exécution réussie avant que les données de résultat puissent apparaître comme étant classifiées.

Pourquoi et quand exécuter cette tâche
La Détection de données page Conclusions affiche toutes les entrées de données qui ont été trouvées par une tâche. La page Conclusions vous permet d'examiner les entrées et de les associer à une classification.

Procédure

1. Accédez à la **Sécurité de système** > **Détection de données (classique)** > **Résultats de détection de données**.
2. Sélectionnez l'entrée que vous souhaitez classer.
3. Dans la Détection de données liste Résultats, sélectionnez **Classer**.
4. Sélectionnez les classes de données que vous souhaitez associer aux entrées de table.
5. Sélectionnez **Classifier**.

Détection de données Emplois

Détection de données Examine vos informations ciblées à l'aide de modèles de données définis par l'utilisateur et de tables cibles.

Détection de données fonctionne en planifiant d'abord une tâche dans la section **Tâche de détection de données** . Lorsqu'une tâche planifiée s'exécute, tous les modèles de données actifs sont recherchés dans les tables cibles actuelles. Pour plus d'informations sur la création et la configuration d'une Détection de données tâche, reportez-vous à la section Configurer une Détection de données tâche.

Remarque :
Les travaux d'analyse d'échantillons analysent jusqu'à 10 000 enregistrements par table et par modèle.

Avertissement :
Si une tâche est exécutée deux fois dans un court laps de temps, le nombre de lignes numérisées peut renvoyer 0 pour la deuxième exécution.

Détection de données Modèles de données

La section **Schémas de données** affiche tous les modèles de données actuels, actifs et inactifs. Un modèle de données est une expression régulière utilisée pour mettre en correspondance des données sensibles. Pour plus d'informations sur l'accès et la configuration des modèles de données, reportez-vous à la section Configurer Détection de données les modèles. La section **Modèles de données actifs** affiche uniquement les modèles actifs. Les modèles inactifs n'apparaissent pas.

Tables cibles

La section **Tables cibles** répertorie toutes les tables qui peuvent être traitées pour une tâche. Pour accéder aux tables cibles, sélectionnez **Tables cibles**.

Les tables suivantes ne sont pas prises en charge :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sr
- sysx (en anglais seulement)
- v
- sh$
- syslog
- UA
- Analyse d'utilisation
- Ecc
- cloner
- jrobin
- papa
- sla_repair_log
- analyse
- Gcf
- fm_log
- journal
- np$
- sn_data_discovery
- dp_configuration
- dp_federated_job
- dp_field_technique
- dp_job
- dp_job_summary
- dp_primary_reference
- dp_technique
- data_classification
- m2m_dictionary_dataclass

Traduction automatique

Configuration granulaire

L'outil de configuration granulaire permet des contrôles plus spécifiques et affinés pour détecter les données sensibles dans une table. Cependant, il existe des différences clés dans son fonctionnement par rapport à un travail de découverte de données traditionnel. Une configuration granulaire analyse uniquement les colonnes spécifiées d'une table à des fins de détection, en signalant ses résultats par enregistrement. Les actions des résultats de l'analyse des configurations granulaires, appelés résultats granulaires, sont spécifiées par enregistrement et le rôle data_privacy_admin doit être anonymisé.

Configurer une Détection de données tâche

Configurez une Détection de données tâche et examinez l'état des tâches en cours. Une Détection de données tâche définit quand un modèle est exécuté sur une table cible.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : data_discovery_admin

Procédure

1. Accédez à la **Sécurité de système** > **Détection de données (classique)** > **Tâche de détection de données**.
2. Dans la Détection de données liste Tâches, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Champs de Détection de données tâche.

Détection de données Champs de tâches

Champ	Description
Nom	Nom de la tâche.
Description	Description de la tâche.
Type d'analyse	Nombre d'entrées à analyser. Les états possibles sont les suivants : ○ **Exemple** : analyse 10 000 entrées. ○ **Complet** : analyse toutes les entrées.
Contexte	Détails de la tâche sur les modèles analysés, les entrées de tables cibles touchées et le temps écoulé.
État	État de la Détection de données tâche. Les états possibles sont les suivants : ○ **Prêt à planifier** : état par défaut pour les nouvelles tâches. ○ **Planifié** : l'exécution de la tâche est planifiée. ○ **En cours** : la tâche est activement en cours d'exécution. ○ **Terminé** : l'exécution de la tâche s'est terminée avec succès. ○ **Erreur** : la tâche a cessé de s'exécuter en raison d'une erreur. ○ **Annulé** : la tâche a été annulée. ○ **En pause** : la tâche est en pause.
Résumé	Affiche les résultats de la tâche une fois que vous l'avez exécutée.
Date de démarrage	Définit la date de début de la tâche.
Début de la fenêtre de temps	Début de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécutera après l'heure saisie dans ce champ. L'heure saisie dans le champ de **début de la fenêtre horaire** doit se situer avant l'heure saisie dans le champ de fin de la **fenêtre** horaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Une valeur de temps valide est exprimée en temps universel coordonné sur la base d'une notation temporelle de 24 heures.
Fin de la fenêtre de temps	Fin de la fenêtre de temps pour exécuter cette tâche. La tâche s'exécute jusqu'à l'heure saisie dans ce champ. Si la tâche n'est pas terminée cette fois-ci, la tâche se met en pause et reprend au prochain début de la fenêtre horaire. L'heure saisie dans le champ de **fin de la fenêtre** horaire doit être postérieure à l'heure saisie dans le champ de début de la **fenêtre horaire** . **Remarque :** Une valeur de temps valide est exprimée en temps universel coordonné sur la base d'une notation temporelle de 24 heures.

4. Sélectionnez **Soumettre**.
   Les boutons **Planifier une tâche** et **Mettre à jour** s'affichent.
5. Sélectionnez **Planifier une tâche** pour exécuter votre tâche.
   La tâche s'exécute entre les heures sélectionnées dans les champs Début de la **fenêtre** de temps et Fin de la **fenêtre de temps** . Si la tâche n'est pas terminée pendant la fenêtre d'heure de début et de fin, la tâche se poursuivra au prochain début de la fenêtre de temps.
6. **Facultatif :** Choisissez l'une des fonctions suivantes :
   - **Annuler la tâche** : annule la tâche.
   - **Pause** : met la tâche en pause.
   - **Reprise** : redémarre une tâche en pause.

Configurer Détection de données les modèles

Configurez un Détection de données modèle et passez en revue les modèles actuels. Un Détection de données modèle définit l'expression régulière utilisée pour mettre en correspondance des données avec une table cible.

Avant de commencer

Rôle requis : data_discovery_admin

Procédure

1. Accédez à la **Sécurité de système** > **Détection de données** > **Tous les modèles de données**.
2. Dans la Détection de données liste Modèle, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Champs de la Détection de données tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détection de données Champs de tâches

Champ	Description
Périmètre interne	Champ d'application du modèle.
Description	Description de la tâche.
Nom	Nom du modèle de données.
Application	Périmètre d'application du modèle.
Expression	Expression régulière utilisée pour découvrir le modèle de données. **Remarque :** La longueur de l'expression doit être inférieure à 1 000 caractères.
Mot clé (facultatif)	Un mot spécifique (ou des mots séparés par une virgule) à rechercher autour d'une expression. Doit être utilisé avec **la proximité des mots clés** **Remarque :** Un mot clé peut être utilisé pour rechercher un contexte supplémentaire pour un modèle. Par exemple, l'utilisation d'un mot-clé peut aider à faire la différence entre une date de naissance et une date d'embauche, étant donné qu'elles ont le même format MM/JJ/AA.
Proximité du mot clé (facultatif)	À quelle distance de l'expression rechercher des mots-clés. Doit être utilisé avec **le mot clé** **Remarque :** La valeur par défaut est 30, limite supérieure de 64

4. Sélectionnez **Soumettre**.
   - Le bouton **Test** vous permet de tester votre expression régulière avant de soumettre la liste de modèles de données.

Le modèle de données doit être défini comme actif pour être utilisé avec les travaux planifiés.

5. Accédez à la **Sécurité de système** > **Détection de données** > **Schémas de données actifs**.
6. Dans la Détection de données liste Modèle actif, sélectionnez **Modifier**.
7. Sélectionnez la liste de modèles dans **Listes disponibles** et déplacez-la vers **Listes sélectionnées**.

Modèles de données par défaut

Examinez les expressions régulières de modèle de données par défaut incluses dans Détection de données. Ces modèles de données par défaut peuvent être utilisés pour filtrer les entrées de table en vue d'une classification ultérieure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici les modèles par défaut disponibles pour la découverte de données.

Nom	Description	Expression régulière	Mots clés	Exemples
Âge	L'âge d'une personne entre 0 et 99 ans	\b([0-9][1-9][0-9]| 1[012][0-9])\b	âge	**Correspondant** 24 **Ne correspondant pas** • 103 • -2
Date de naissance	Date de naissance au format JJ/MM/AAAA	\b[0-3] ? [0-9]/ [0-3]? [0-9]/(?:[0-9] {2})? [0-9] {2}\b	date de naissance, date de naissance, date de naissance	**Correspondant** • 06/18/2012 • 1/1/19
E-mail	Adresse e-mail standard	\b[\w !#$ %&'*+/= ?'{|} ~^-]+(?:\. [\w !# $%&'*+/= ?'{|} ~^-]+)*@(?:[a-zA-Z0-9-]+\.) +[a-zA-Z]{2,6}\b		**Correspondant** • johndoe@emailserver.com • historyprofessor@college **Ne correspondant pas** • notanemail.com • bademail@.org (en anglais seulement)
Numéro d'identification du véhicule	Un numéro d'identification du véhicule (NIV)	\b[A-HJ-NPR-Z0-9] {17}\b		**Correspondant** AHUYA31581L000000
Adresse IP	Adresse IP standard	**IP à 4 chiffres** \b(?: (?:25[0-5]| 2[0-4] [0-9]| [01]? [0-9] [0-9]?) \.) {3} (?:25[0-5]| 2[0-4] [0-9]| [01]? [0-9] [0-9]?) \b		**IP à 4 chiffres correspondant** 102.28.46.103 **IP à 6 chiffres correspondant** 914b :d45a :61ea :6346:59bc :30

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description	Expression régulière	Mots clés	Exemples
		IP à 6 chiffres \b(((?:[0-9A-Fa-f]{1,4}(?::[0-9A-Fa-f]{1,4})*) ?) ::((?:[0-9A-Fa-f]{1,4}(?::[0-9A-Fa-f]{1,4})*) ?))|((?:[0-9a-fA-F]{1,4}:){7}[0-9a-fA-F]{1,4})\b		
Carte de crédit - Visa	Numéro de carte de crédit Visa	\b4[0-9]{12}(?:[0-9]{3}) ?\b		**Correspondant** 4444434342424242
Carte de crédit - American Express	Numéro de carte de crédit American Express	\b3[47][0-9]{13}\b		**Correspondant** 378225246366005
Carte de crédit : Mastercard	Numéro de carte de crédit Mastercard	\b(?:5[1-5][0-9]{2}|222[1-9]|22[3-9][0-9]|2[3-6][0-9]{2}|27[01][0-9]|2720)[0-9]{12}\b		**Correspondant** 5555444455554444
Carte de crédit - Diners Club	Numéro de carte de crédit Diners Club	\b3(?:0[0-5]|[68][0-9])[0-9]{11}\b		**Correspondant** 3056930009020004
Carte de crédit : Discover	Numéro de carte de crédit Discovery	\b6(?:011|5[0-9]{2})[0-9]{12}\b		**Correspondant** 6011025690875424
Carte de crédit - CCV	Numéro de sécurité de la carte de crédit	\b[0-9]{3,4}\b	CVV, code de vérification, code de sécurité	**Correspondant** 124
Carte de crédit : date d'expiration	Expiration de la carte de crédit au format MM/AAAA	\b(([1-9])|(0[1-9]|1[0-2]))\/ ? ([0-9]{4}|[0-9] {2}) \b	Expiration,exp	**Correspondant** • 02/2027 • 04/23

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Description	Expression régulière	Mots clés	Exemples
				Ne correspondant pas 03/9
USA - Numéro de sécurité sociale	Numéro de sécurité sociale du citoyen américain	\b(?! 666|000|9\d{2})\d{3}-(?! 00)\d{2}-(?! 0{4})\d{4}\b		**Correspondant** 001-22-111
États-Unis - Numéro de téléphone	Numéro de téléphone aux États-Unis **⚠ Avertissement :** N'utilise pas l'indicatif d'appel des États-Unis.	\b\(?([0-9] {3})\)? [-.]? ([0-9]{3})[-.]? ([0-9]{4})\b		**Correspondant** 2065550199 **Ne correspondant pas** 1 555 238 0199
États-Unis - Numéro de passeport	Numéro de passeport américain à 9 chiffres	\b[a-zA-Z0-9]\\d{8}\b		**Correspondant** 770022122
États-Unis - ID contribuable	Numéro d'identification du contribuable américain	\b(9\d{2})([\-] ?)([7]\d|8[0-8]) ([\-]?)(\d{4})\b		**Correspondant** 927 70 5828
États-Unis – État de Californie Numéro de permis de conduire	État de Californie, États-Unis Numéro de permis de conduire	\b[a-zA-Z]\d{7}\b		**Correspondant** A0002144
USA – Banque Numéro d'acheminement	Numéro d'acheminement bancaire américain (ABA)	\b((0[0-9])|(1[0-2])|(2[1-9])|(3[0-2])|(6[1 à 9])|(7[0-2])|80)([0-9]{7})\b		**Correspondant** 125210305

Configurer Détection de données la table cible

Ajoutez des tables cibles à utiliser dans Détection de données les tâches. Seules les tables cibles seront analysées pour les modèles de données.

Avant de commencer

Rôle requis : data_discovery_admin

Pourquoi et quand exécuter cette tâche

Lorsqu'une Détection de données tâche est exécutée, elle s'exécute sur toutes les tables cibles avec tous les modèles actifs.

Procédure

1. Sélectionner **Sécurité de système** > **Détection de données (classique)** > **Tables cibles**.
2. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez votre table cible dans le champ **Nom de table** .
4. Sélectionnez **Soumettre**.

Activer les tâches parallèles pour Détection de données

Utilisez des tâches parallèles pour réduire le temps d'exécution de votre Détection de données tâche.

Avant de commencer
Rôle requis : administrateur

Procédure
Exécute par défaut Détection de données les tâches à l'aide d'un seul thread. Plusieurs threads peuvent être activés pour Détection de données des analyses complètes.

1. Dans le filtre de navigation, saisissez `sys_properties.list`.
2. Créer la propriété `com.glide.data_discovery.max_concurrent_item_workers`
3. Vérifiez que le **type** est un nombre entier.
4. **Important :**
   Il est recommandé de commencer avec un petit nombre de travailleurs par nœud (2 ou 3).

   Entrez le nombre d'agents de tâches parallèles dans le champ **Valeur** jusqu'à 5.

Détection de données rôles

Vous pouvez affecter Détection de données des rôles pour limiter l'accès des utilisateurs à certains types de données.

Administrateur de détection de données [sn_data_discovery.data_discovery_admin]

Affichez, créez et modifiez des modèles de données et les tâches connexes.

- Modèles de données :
  - Créer
  - Lecture
  - Mettre à jour
  - Supprimer
- Modèles de données actifs :
  - Supprimer
  - Lecture
- Emplois:
  - Créer
  - Lecture
  - Mettre à jour
  - Supprimer

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Calendrier
- Pause
- Reprendre
- Annuler

- Tables cibles :
  - Créer
  - Lecture
  - Écriture
- Configuration granulaire :
  - Créer
  - Lecture
  - Mettre à jour
  - Supprimer
- Résultats granulaires :
  - Créer
  - Lecture
  - Actions

Remarque :
Les utilisateurs dotés de ce rôle ne peuvent effectuer que l'action ignorer

Contient des rôles

Liste des rôles contenus dans le rôle.

- data_classification_auditor
- data_classification_admin
- sn_data_discovery.data_discovery_api_processor

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Ce rôle est automatiquement attribué aux administrateurs lors de l'installation du produit.

Remarque :
Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

Auditeur de détection de données [sn_data_discovery.data_discovery_auditor]

Lire des modèles de données et des tables cibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lire des modèles de données
- Lire des modèles de données actifs
- Lire les Détection de données tâches
- Lire les tables cibles
- Examiner la configuration granulaire
- Examiner les résultats granulaires

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Aucun.

Administrateur de classification des données [data_classification_admin]

Lisez les modèles de données, les tâches de détection et la table data_classification lorsqu'un résultat de modèle spécifique activé est classifié.

Contient des rôles

Le rôle Classification de données contient la liste des rôles contenus dans le rôle data_classification_auditor.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Remarque :
Pour plus d'informations sur le rôle administrateur de classification des données, reportez-vous à Installation des données de démonstration du module d'extension Data Classification.

Détection de données Résultats des tâches

La Détection de données page Résultats affiche les détails des données trouvées par une tâche. Vous pouvez utiliser la page Résultats pour examiner les résultats d'une tâche et commencer à classer les données.

La Détection de données page Conclusions affiche les détails suivants après une tâche terminée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
Entrée du dictionnaire	Colonne de la table cible où se trouvaient les données
Table	Table cible où les données ont été trouvées
Modèle de données	Modèle de données utilisé pour trouver les données
Nombre de correspondances de modèles de données	Nombre d'entrées de données qui correspondent au modèle de données
Nombre total d'analyses de lignes	Nombre de lignes numérisées pendant la tâche
Pourcentage de lignes correspondantes	Pourcentage de lignes dans la table cible qui correspondent au modèle de données
Détection de données Travail	Tâche utilisée sur la table cible
Statut	État de l'entrée

Une fois que vous avez exécuté une Détection de données tâche, les résultats affichent l'état Nouveau. Si aucune action n'est nécessaire, vous pouvez ne pas toucher aux données, ce qui définit automatiquement l'état sur Ignoré. Sinon, vous pouvez classer les données, par exemple en créant des classifications de données définies par l'utilisateur, pour préparer l'anonymisation des données à l'aide de l'outil Data Classification .

Résultats granulaires

Les utilisateurs peuvent sélectionner l'action **Suivre les résultats granulaires** pour utiliser la page afin de prendre des Résultats granulaires mesures sur des enregistrements détectés spécifiques. Consultez Résultats granulaires pour plus d'informations.

Protections disponibles

Sélectionnez le bouton **Protections disponibles** pour examiner un service de contrôle des entrées, l'état, les notes et le dernier enregistrement. À partir de Xanadu cette fonctionnalité, seul Chiffrement au niveau des colonnesfichier .

Les services Protecton sont également accessibles à partir du tableau de bord. Pour en savoir plus sur le tableau de bord, Détection de donnéesreportez-vous à la section .

Consolider les résultats

Les résultats des travaux peuvent être consolidés à l'aide du bouton **Consolider les résultats** . Les résultats de tâches partagés entre deux tâches distinctes seront ensuite consolidés sous la tâche la plus récente exécutée.

Remarque :
Seules les tâches d'analyse complète terminées peuvent être consolidées

Classer les données dans la page des résultats des Détection de données tâches

Classez les données directement à Détection de données partir de la page de résultats d'une tâche.

Avant de commencer
Rôle requis : data_discovery_admin et admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une tâche doit terminer une exécution réussie avant que les données de résultat puissent apparaître comme étant classifiées.

Procédure

1. Accéder à **Sécurité de système** > **Détection de données** > **Tâche de détection de données**.
2. Sélectionnez l'entrée que vous souhaitez classer.
3. Dans la Détection de données liste Résultats, sélectionnez **Classer**.
4. Sélectionnez les classifications de données que vous souhaitez associer aux entrées de table.
5. Sélectionnez **Classifier**.

Détection de données Types de données pris en charge

Vérifier quels types de champs sont pris en charge lors de l'utilisation de Détection de données.

Remarque :
Tous les types de champs qui ont été classifiés ne sont pas disponibles pour Détection de données.

Certains types de champs à risque élevé sont désactivés par défaut, comme indiqué dans la table. Pour plus d'informations sur les champs, consultez Types de champs .

Types de champ pris en charge pour la découverte de données

Type de champ	Disponible par défaut
audio	Non
condition	Non
condition_string	Non
currency	Oui
décimal	Oui
due_date	Oui
flotter	Oui
glide_date	Oui
glide_date_time	Oui
glide_duration	Non
glide_time	Oui
html	Non
icône	Non
entier	Oui
ip_addr	Non
ip_address	Non
journal	Oui
journal_input	Oui
journal_list	Oui

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type de champ	Disponible par défaut
Entier long	Oui
name_values	Non
percent_complete	Non
phone_number_e164	Oui
price	Oui
chaîne	Oui
string_full_utf8	Oui
translated_html	Non
translated_text	Non
URL	Non
user_image	Non
vidéo	Non
wiki_text	Non

Numérisation avec configuration granulaire

L'analyse granulaire peut être utilisée pour analyser des colonnes de table spécifiques à des fins de détection. Les tâches traditionnelles Détection de données analysent l'ensemble de la table pour découvrir des données, tandis que l'analyse granulaire cible des colonnes spécifiques de la table, offrant ainsi plus de contrôle sur le processus de découverte

Avant de commencer

Rôle requis : admin, sn_data_discovery_admin, data_privacy_admin

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Détection de données (classique)** > **Configuration granulaire**.
2. Dans la liste **Configurations granulaires** , sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire **Champs de configuration granulaire** .

Champs de configuration granulaire

Champ	Description
Entrée du dictionnaire	Colonne à analyser.
Table	Table à analyser.
Étiquette de colonne	Étiquette de colonne à analyser
Point de début de l'analyse	Les données sensibles ne seront détectées que le jour et après le début de l'analyse.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si le point de départ de l'analyse est laissé vide, toutes les entrées de la colonne seront analysées. Si le point de début de l'analyse est modifié, l'analyse sera réinitialisée pour démarrer à partir de l'horodatage nouvellement configuré.
Actif	Cochez cette case pour activer la configuration granulaire.

4. Sélectionnez **Soumettre**.
   Les enfants des tables extensibles peuvent être sélectionnés pour la configuration.
5. **Facultatif :** Sélectionnez la configuration granulaire pour la table parente, sélectionnez **Sélectionner les tables enfants** , puis sélectionnez les tables enfants pour l'analyse.

Résultats

La colonne spécifique de la table cible sera analysée pour détection. L'analyse granulaire utilise les modèles de **données des modèles de données actifs**. Vous pouvez examiner les résultats et effectuer des actions à l'adresse suivante : **Tout** > **Sécurité de système** > **Détection de données (classique)** > **Résultats granulaires**. Consultez Résultats granulaires pour plus d'informations.

Résultats granulaires

Les résultats granulaires peuvent être examinés à l'aide de l'outil Résultats granulaires.

Examen des résultats granulaires

Les résultats granulaires sont utilisés pour examiner jusqu'à 500 résultats provenant de configurations granulaires. Lorsqu'il y a 500 résultats, l'analyse des configurations granulaires est mise en pause jusqu'à ce qu'une action soit effectuée.

Étiquette de colonne	Description
Enregistrement	Enregistrement détecté.
Table	Table parente de l'enregistrement.
Colonne	Colonne de l'enregistrement où des informations sensibles ont été découvertes.
Modèles de données	Modèle utilisé pour détecter l'enregistrement.
Action	Action à effectuer sur les résultats. Sélectionnez cette option pour modifier **Important :** Le rôle data_privacy_admin est requis pour effectuer l'action Anonymiser sur un enregistrement. **Revue**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette de colonne	Description
	L’enregistrement est en attente de révision. Celle-ci est affectée aux nouvelles découvertes granulaires. **Ignorer** Aucune action ne sera effectuée sur l’enregistrement **Anonymiser** L’enregistrement est anonymisé.
Statut	État de l’enregistrement. **Nouveau** État affecté au résultat lors du premier signalement **Traité** Lorsque l’action choisie par l’utilisateur a été appliquée avec succès au résultat **Remarque :** Les résultats traités sont stockés pendant 3 jours dans la table des résultats granulaires avant d’être supprimés **Revue manuelle** Lors de l’application, l’action choisie par l’utilisateur a échoué. **Avertissement :** Les résultats de l’examen manuel doivent être supprimés par les utilisateurs après avoir pris les mesures appropriées.

Avertissement :
La restauration n'est pas prise en charge pour l'anonymisation déclenchée à partir des résultats granulaires.

Data Classification

Regroupez les données par type à l'aide de classifications de données prédéfinies ou définies par l'utilisateur. Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez administrer différentes classes de données ou analyser visuellement l'état actuel de différents types de données au sein de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Explorer la classification des données



En savoir plus sur la classification des données.

Configurer la classification des données



Créez et configurez vos propres classes de données.

Référence pour la classification des données



Découvrez comment la classification des données fonctionne avec les données de démonstration.

Analyser les classifications des données



Apprenez à analyser les classifications de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration de la classification des données

Explorez la classification des données.

Data Classification Active la prise en charge de :

- Visibilité sur les types de données hébergées sur des Now Platform instances.
- Conformité aux lois sur la protection de la vie privée et respect des exigences réglementaires pour des secteurs tels que les services financiers et la fabrication de dispositifs médicaux.

Classifications des données

La classification des données est un processus autonome dans lequel vous appliquez manuellement des classifications de données aux entrées de dictionnaire existantes dans n'importe quelle table. Consultez Data dictionary tables pour plus d'informations.

- Vous classez les données comme vous le jugez approprié pour votre entreprise et vous pouvez modifier les classes de données disponibles si nécessaire.
- Lorsque vous classez des données, vous pouvez utiliser les classifications de données prédéfinies ou créer les vôtres. Bien que l'utilisation de classifications de données prédéfinies soit facultative, il est conseillé de le faire comme point de départ. Ces classifications de données prédéfinies sont incluses dans les données de démonstration que vous pouvez installer dans votre instance. Pour en savoir plus, consultez Installation des données de démonstration du module d'extension Data Classification et Composants installés avec Data Classification des données de démonstration.
- Si vous créez vos propres classifications de données, vous pouvez également concevoir un système hiérarchique hiérarchique hiérarchique avec des classifications de données parentes et enfants.

Tableau de bord de vue d'ensemble

Utilisez le tableau de bord Vue d'ensemble pour comprendre comment vos tables de données actuelles sont mappées à différentes classifications de données. Vous pouvez également analyser la façon dont vos utilisateurs mondiaux, régionaux et internationaux peuvent avoir besoin d'approches différentes de la classification des données, en ce qui concerne l'utilisation ou l'accès aux données. Vous pouvez également personnaliser le contenu et la mise en page du tableau de bord de vue d'ensemble pour répondre à vos besoins.

Pour apprendre à utiliser les API scriptées et REST disponibles pour appliquer les métadonnées de classification aux processus, workflows et applications existants, consultez les rubriques suivantes :

- Classification des données : REST API
- DCManager - Global
- ScopedDCManager - Dans le champ d'application

Remarque :
Data Classification prend en charge Séparation de domaine, et la table data_classification elle-même est séparée par processus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cas d'utilisation

Le Règlement général sur la protection des données (RGPD) est un règlement de l'Union européenne dont l'objectif est de permettre aux individus de contrôler leurs propres données personnelles. Vous pouvez utiliser des classifications de données, telles que les informations personnellement identifiables, pour identifier où les données personnelles sont stockées dans votre instance. En appliquant les mécanismes de sécurité appropriés pour protéger ces données personnelles contre les fuites, votre organisation répond aux exigences du RGPD.

Si vous stockez des informations sur vos clients dans le Now Platform, utilisez le code de classification des informations personnellement identifiables (PII) si nécessaire pour suivre les données soumises à la réglementation des lois locales sur la protection de la vie privée. Lorsque vous installez des données de démonstration, ce code de classification est automatiquement appliqué à certains champs sensibles de sécurité dans la table Utilisateur [sys_user]. Pour en savoir plus, consultez :

- Composants installés avec Data Classification des données de démonstration
- Affectation de classifications de données à des entrées de dictionnaire

Vous pouvez appliquer une classification de données restreinte aux colonnes de la table Employés qui stockent des informations sensibles sur les employés, telles que les numéros de sécurité sociale (SSN). Les administrateurs et les auditeurs peuvent ensuite utiliser le tableau de bord Vue d'ensemble pour confirmer que vous avez affecté des classifications de données aux colonnes correctes. Ils peuvent également afficher les détails de classification pour des types d'informations restreints.

Installation des données de démonstration du module d'extension Data Classification

Lors de la mise à niveau ou de l'installation Xanadu (et versions ultérieures), le module d'extension Data Classification (com.glide.data_classification) est automatiquement activé. Toutefois, vous devez installer manuellement les données de démonstration fournies avec le module d'extension. Il comprend plusieurs classifications de données prédéfinies importantes et affecte également l'une d'entre elles à des colonnes de table Utilisateur [sys_user] spécifiques dans votre instance.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Que vous installiez des données de démonstration ou non, le module d'extension activé Data Classification ajoute les rôles d'utilisateur suivants dans votre instance :

- data_classification_admin : peut gérer tous les aspects de l'application, y compris la configuration et l'affectation Data Classification de la classification des données.
- data_classification_auditor : peut auditer Data Classification les affectations de code effectuées aux tables et colonnes des utilisateurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :
Avis concernant l'utilisation par les clients :

Toutes les décisions relatives à la mise en œuvre de cette application sont à la seule discrétion du Client. Les clients reconnaissent et acceptent que l'utilisation de l'application n'engage en rien ServiceNow à se conformer à une loi ou à une réglementation, et que toute suggestion, langage, champ ou classification prêt à l'emploi fourni avec l'application ne constitue pas un avis juridique de la part de ServiceNow.

Les clients demeurent seuls responsables du respect de leurs obligations légales en vertu de la législation applicable, y compris (mais sans s'y limiter) la protection des données, les exigences de sécurité et les lois sur la confidentialité, et sont responsables de la configuration et de la modification nécessaires à cette application, y compris (mais sans s'y limiter) les modèles, pour répondre aux exigences des clients.

Procédure

1. Accédez à la **Applications système** > **Toutes les applications disponibles** > **Tout**.
2. Trouvez le module d'extension Data Classification à l'aide des critères de filtre et de la barre de recherche. Un message Installé s'affiche une fois que vous avez localisé le module d'extension.
3. Cliquez sur l'icône avec trois points verticaux, puis sélectionnez **Réparer** pour accéder à la boîte de dialogue Activer le module d'extension.
4. Sélectionnez **Charger les données de démonstration**, puis cliquez sur **Réparer**.

Composants installés avec Data Classification des données de démonstration

Lorsque vous installez les données de démonstration incluses dans le module d'extension Data Classification (com.glide.data_classification), plusieurs types de composants sont installés dans votre instance. Ces composants comprennent des classifications de données prédéfinies et des affectations de code pour des colonnes d'utilisateur [sys_user} spécifiques.

Classifications des données installées

Classification des données	Description
Confidentiel	Données sensibles qui, si elles étaient compromises, pourraient avoir un impact négatif sur les opérations.
Interne	Données internes non destinées à être divulguées publiquement.
Informations personnellement identifiables	Également connu sous le nom de PII. Données qui pourraient potentiellement être utilisées pour identifier une personne en particulier.
Public	Données qui peuvent être librement divulguées au public.
Restreint	Des données d'entreprise hautement sensibles qui, si elles étaient compromises, pourraient exposer l'organisation à des risques financiers ou juridiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Data Classification Affectations

Table	Colonne affectée	Classification des données affectée
sys_user	code postal	Informations personnellement identifiables
sys_user	first_name	Informations personnellement identifiables
sys_user	E-mail	Informations personnellement identifiables
sys_user	city	Informations personnellement identifiables
sys_user	middle_name	Informations personnellement identifiables
sys_user	rue	Informations personnellement identifiables
sys_user	mobile_phone	Informations personnellement identifiables
sys_user	last_name	Informations personnellement identifiables
sys_user	pays	Informations personnellement identifiables
sys_user	sexe	Informations personnellement identifiables
sys_user	name	Informations personnellement identifiables
sys_user	photo	Informations personnellement identifiables
sys_user	État	Informations personnellement identifiables
sys_user	home_phone	Informations personnellement identifiables

Création de classifications des données

Créez vos propres classifications de données définies par l'utilisateur dans la Data Classification table [data_classification] que vous pouvez ensuite affecter à des colonnes spécifiques dans des tables spécifiques.

Avant de commencer

Rôle requis : data_classification_admin, admin

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Classification des données** > **Classes de données**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire.

Champ	Description
Nom de classification	Nom de la classification des données.
Description	Description de la classification des données.
Parent	Nom de la classification de données parente à laquelle cette classification de données est subordonnée. Laissez le champ vide si cette classification de données n'est pas une classification de données parent à enfant.
Application	Périmètre de l'application pour cette classification des données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Si cette classification de données doit être une classification de données parent à enfant, cliquez sur **Nouveau**.
   Si vous ne souhaitez pas créer de classifications de données enfants, ignorez cette étape.
5. Renseignez les champs du formulaire.

Titre

Champ	Description
Nom de classification	Nom de la classification des données enfants.
Description	Description de la classification des données enfants.
Parent	Nom de la classification de données parente à laquelle cette classification de données est subordonnée. Laissez le champ vide si cette classification de données n'est pas une classification de données parent à enfant.
Application	Périmètre de l'application pour cette classification de données enfants.

6. Cliquez sur **Envoyer**.

Affectation de classifications de données à des entrées de dictionnaire

Affectez des classifications de données à des colonnes spécifiques de la table Dictionnaire [sys_dictionary]. Lorsque vous affectez des classifications de données, cela crée des entrées dans la table Classe de données du dictionnaire [m2m_dictionary_dataclass], que vous pouvez ensuite passer en revue dans le tableau de bord Vue d'ensemble.

Avant de commencer

Rôle requis : data_classification_admin et admin

Procédure

1. Dans la fenêtre Navigator (Navigateur), saisissez `sys_dictionary.list`.
2. Dans Entrées de dictionnaire, sélectionnez chacun des éléments auxquels vous souhaitez affecter des classifications de données spécifiques.
3. Après avoir sélectionné les éléments, cliquez **sur Actions sur les lignes sélectionnées**, puis sélectionnez **Classer**.

> **Remarque :**
> Pour effacer les classifications de données précédemment affectées pour les éléments de dictionnaire sélectionnés, vous pouvez sélectionner **Effacer la classification**.

4. Lorsque la boîte de dialogue Affecter à la classe de données s'affiche, sélectionnez les classifications de données que vous souhaitez affecter aux éléments de dictionnaire sélectionnés, puis cliquez sur **Classer**.

> **Avertissement :**
> Cela remplacera toutes les classifications existantes pour les éléments de dictionnaire sélectionnés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez sélectionner plusieurs classifications de données selon vos besoins.

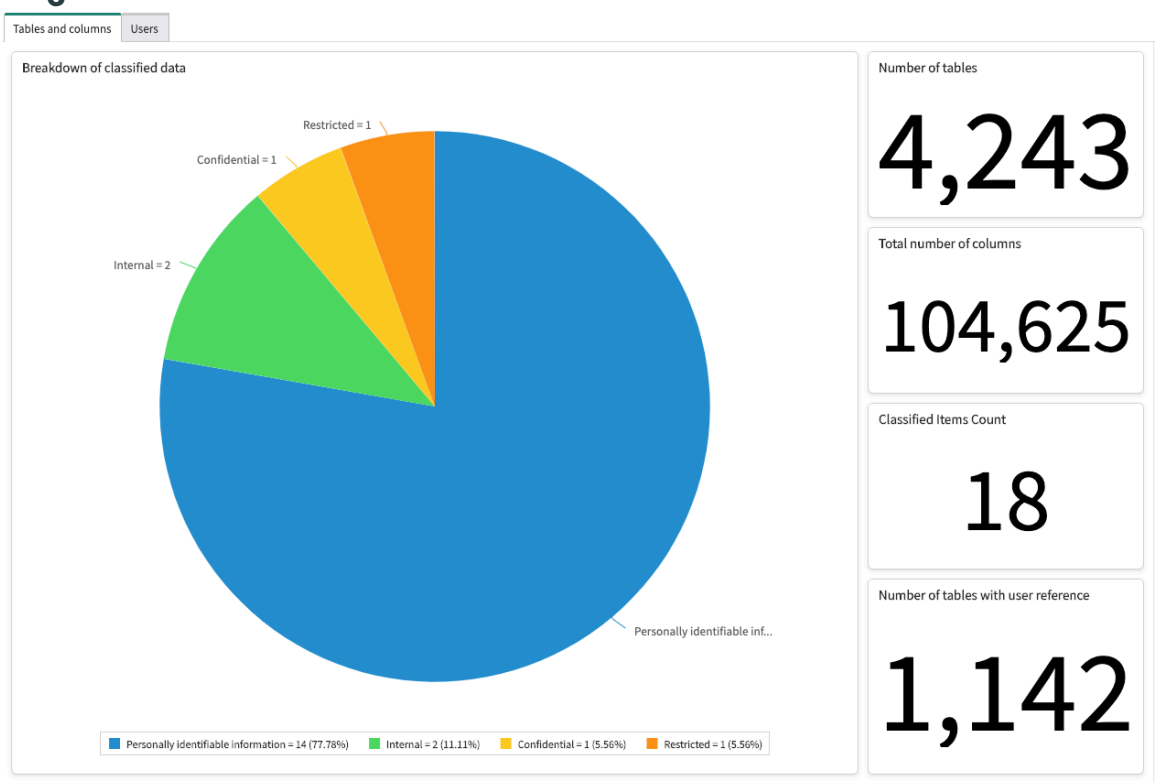
Consultez Data dictionary tables pour plus d'informations.

Analyser les classifications de données à l'aide du tableau de bord Vue d'ensemble

Le tableau de bord Vue d'ensemble signale l'état actuel des classifications de données au sein de votre instance et la façon dont vos utilisateurs sont répartis par emplacement.

Si vous disposez d'un rôle d'administrateur de classification des données ou d'auditeur, vous pouvez visualiser la sensibilité actuelle des données d'instance, ce qui contribue à renforcer la sécurité et la conformité aux lois sur la confidentialité. En utilisant le champ Emplacement dans les enregistrements utilisateur, les administrateurs mappent les utilisateurs dans différentes régions où les réglementations en matière de confidentialité diffèrent.

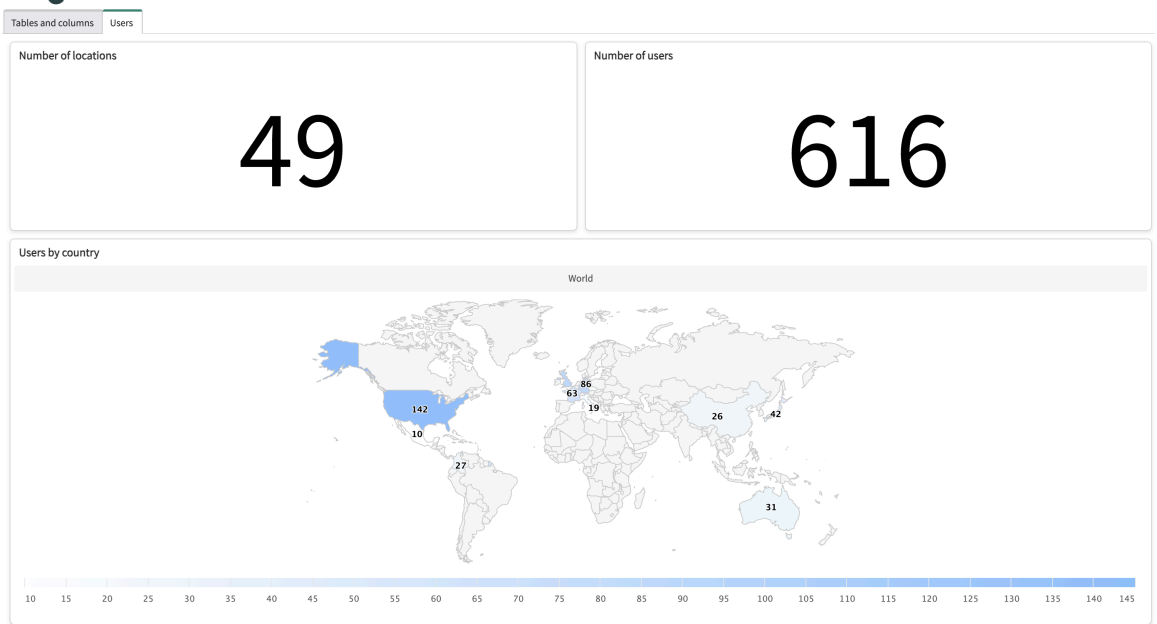
Onglet Tables et colonnes



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Onglet Utilisateurs



Rôles Now Platform requis

- data_classification_admin : administre tous les aspects de l'application, y compris la classification des données, la configuration et l'affectation Data Classification .
- data_classification_auditor : audite les affectations de Data Classification codes.

Cas d'utilisation

Pour obtenir des exemples supplémentaires sur la façon dont différentes personnes de votre organisation utilisent ce tableau de bord, reportez-vous à la section Cas d'utilisation dans Data Classification.

Utilisateur	Utilisation du tableau de bord
data_classification_admin	Confirmez que vous avez affecté des classifications de données aux champs corrects de votre instance.
data_classification_auditor	Auditez la sénilité et la sécurité des données dans votre instance.

Rapports

Titre	Type	Table source	Description
Répartition des données classées	Couronne	m2m_dictionary_dataclass	Fournit une répartition des classifications de données d'instance, par classe de données, total affiché au centre.
Nbre total de tables	Score unique	sys_dictionary	Nombre total de tables de données dans l'ensemble du dictionnaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Titre	Type	Table source	Description
Colonnes Total	Score unique	sys_dictionary	Nombre total de colonnes de données classées dans l'ensemble du dictionnaire.
Colonnes de référence des utilisateurs	Score unique	sys_dictionary	Nombre total de colonnes de référence utilisateur dans le dictionnaire.
Nombre d'emplacements de l'utilisateur	Score unique	sys_user	Nombre total d'emplacements distincts trouvés pour les utilisateurs
Nombre d'utilisateurs	Score unique	sys_user	Nombre total d'enregistrements utilisateur dans votre instance.
Utilisateurs par pays	Carte	sys_user	Répartition des enregistrements d'utilisateurs par pays.

Séparation de domaine et Data Classification

L'application Séparation de domaine est prise en charge pour Data Classification . Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Amélioré

- Inclut les niveaux **Basique** et **Standard**.
- Le processus piloté par les données permet aux clients du fournisseur de service de modifier la logique métier basée sur des cas d'utilisation définis. Ces configurations sont basées sur l'interface utilisateur et sont sécurisées de sorte que les configurations d'un client ne peuvent pas en affecter une autre.
- Les locataires de l'instance doivent être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) pour eux-mêmes. Cette logique et ces paramètres sont attendus pour un fonctionnement normal de l'application.

Exemple de cas d'utilisation : les locataire-clients d'un environnement partagé doivent être en mesure de modifier la matrice d'impact, d'urgence ou de priorité pour définir la priorité au sein de leur domaine.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Comment fonctionne Séparation de domaine dans Data Classification

Pour Séparation de domaine, l'application utilise la séparation de processus pour la Data Classification table [sys_data_classification]. Pour la table Dictionary-Data Class [m2m_dictionary_dataclass], elle utilise la séparation des données. Pour en savoir plus sur la séparation des données et des processus, consultez Explication de Séparation de domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Séparation de domaine pour les fournisseurs de services

Anonymisation des données

L'anonymisation permet de transformer facilement les données afin qu'elles ne soient pas identifiables et de les rendre plus conformes à la réglementation en matière de confidentialité des données.

Les administrateurs peuvent effectuer le processus d'anonymisation dans les instances de production et de non-production. La confidentialité des données peut être utilisée dans les instances de production pour anonymiser des utilisateurs. L'anonymisation des classes de données ne doit être utilisée qu'avec des instances de non-production. Cette conservation garantit que certaines données, telles que les adresses e-mail ou les adresses physiques, sont remplacées par des versions au format similaire, mais anonymisées.

Les administrateurs peuvent également utiliser l'anonymisation dans le cadre de leurs processus de droit à l'oubli (RTBF) du Règlement général sur la protection des données (RGPD) pour anonymiser les informations des utilisateurs. Consultez https://gdpr-info.eu/art-17-gdpr/ pour plus d'informations.

Utilisez la section d'anonymisation de Confidentialité des données pour créer et afficher des politiques et des techniques de confidentialité, et pour effectuer une affectation en bloc de confidentialité. Affichez toutes les tâches, avec la description, la politique de confidentialité utilisée et l'état. Pour accéder à la section d'anonymisation, un administrateur doit d'abord accéder aux rôles data_privacy_admin et data_privacy_processor.

Techniques d'anonymisation

Les techniques d'anonymisation sont des options que vous sélectionnez pour déterminer comment vos données sont anonymisées. Vous devez créer une technique d'anonymisation à référencer dans la tâche d'anonymisation. Reportez-vous à la section Créer des techniques d'anonymisation pour associer une technique de confidentialité à une **configuration de technique d'anonymisation** associée.

Politiques d'anonymisation

Configurez une politique d'anonymisation pour spécifier les techniques de confidentialité des données utilisées lors de l'anonymisation de vos données. Voir pour Créer des politiques d'anonymisation plus de détails.

Tâches d'anonymisation

Les tâches d'anonymisation utilisent tous ces composants pour anonymiser vos données. Pour en savoir plus sur ces métiers, reportez-vous à la section Créer une tâche d'anonymisation.

Créer des techniques d'anonymisation

Créez une configuration de technique de confidentialité des données pour personnaliser la façon dont la confidentialité des données anonymise vos données.

Avant de commencer
Rôle requis : data_privacy_admin et admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Élevez-vous au rôle **data_privacy_admin** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
3. Sélectionnez **Afficher les techniques**.
   Il existe plusieurs techniques prédéfinies disponibles pour la sélection.

Technique	Description
Remplacement sélectif	Cette technique remplace sélectivement les données de chaîne. Tous les caractères entre les index de début et de fin de l'entrée sont remplacés par le caractère que vous choisissez. Vous pouvez spécifier des caractères à exclure du masquage : ○ start_index : la technique masque les données commençant par le caractère spécifié. Si ce champ est laissé vide, le masquage commence par le premier caractère. ○ end_index : la technique masque les données du début de la chaîne jusqu'au caractère spécifié. Si ce champ est laissé vide, le masquage se termine au dernier caractère. ○ exclude_char : définissez un caractère à exclure du masquage. ○ replacement_char : définissez un caractère utilisé pour le masquage. Si aucun n'est fourni, les astérisques (*) sont utilisés par défaut.
Remplacement statique	Cette technique échange les valeurs avec des valeurs statiques. Les données chaîne, numéro et date peuvent utiliser cette technique : ○ date_time_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss. ○ date_value : remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj. ○ number_value : remplacez les valeurs de nombres par ce nombre. ○ string_value : remplacez les valeurs de chaîne par ce texte. ○ number_type : accepte un nombre entier
Remplacement aléatoire	Cette technique échange les valeurs avec des valeurs générées de façon aléatoire. Les données chaîne et numéro peuvent utiliser cette technique.
Supprimer	Cette technique supprime les valeurs et les remplace par des valeurs vides (nulles).
Aucune action	Cette technique est un espace réservé. Il ne modifie pas les champs lorsqu'il est sélectionné.
Remplacement sélectif par X	Transforme les données de chaîne et remplace sélectivement les caractères sensibles par la lettre X. **Remarque :** Technique par défaut pour les modèles de données dans Explorer Détection de données.
Anonymisation du modèle de données	Annuise uniquement les modèles de données détectés dans des champs de données non structurés tout en conservant le contexte sous-jacent intact.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Technique	Description
	Remarque : Les paramètres de cette technique d'anonymisation du modèle de données de référence sont définis dans Explorer Détection de données.

4. Sélectionnez **Ajouter une technique personnalisée**, si vous n'utilisez pas une technique prédéfinie.
5. Renseignez les champs du formulaire **Personnaliser une technique** .

Champ 1	Description
Technique de base	Sélectionnez une technique prédéfinie, car les techniques personnalisées sont basées sur les techniques prédéfinies.
Nom de la technique	Donnez un nom à la technique.
Description de la technique	Entrez une description de la technique.

6. Sélectionnez **Suivant**.
7. Entrez les paramètres de la technique.
   Les valeurs paramétrées disponibles dépendent de la technique de confidentialité que vous avez sélectionnée. Il n'existe aucune valeur paramétrée pour les techniques **Aucune action** et **Supprimer** .

Valeurs paramétrées de confidentialité pour les techniques de base

Technique de base	Valeur de paramètre de la technique de confidentialité	Description	Valeur par défaut
Remplacement sélectif	end_index	La technique masque les données du début de la chaîne jusqu'au caractère spécifié. S'il n'est pas renseigné, le masquage se termine au dernier caractère.	(Vide)
Remplacement sélectif	exclude_char	Caractère pour ignorer le masquage. Un seul caractère peut être utilisé dans cette valeur. Si plusieurs caractères sont saisis, le premier caractère est utilisé.	(Vide)
Remplacement sélectif	replacement_char	Caractère à utiliser lors du remplacement de valeurs à l'aide d'un remplacement sélectif.	Un astérisque (*) est utilisé si aucune autre valeur n'est saisie.
Remplacement sélectif	start_index	La technique masque les données commençant par le caractère spécifié.	Si ce champ est laissé vide, le masquage

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Technique de base	Valeur de paramètre de la technique de confidentialité	Description	Valeur par défaut
			commence au premier caractère.
Remplacement statique	date_time_value	Remplacez les valeurs de date et d'heure par cette date. Utilisez le format aaaa-MM-jj HH :mm :ss.	1988-11-11 10:10:10
Remplacement statique	date_value	Remplacez les valeurs de date par cette date. Utilisez le format aaaa-MM-jj.	1988-11-11
Remplacement statique	number_value	Remplacez les valeurs de nombres par ce nombre.	1234567
Remplacement statique	string_value	Remplacez les valeurs de chaîne par ce texte.	TEXT123
Remplacement aléatoire	preserve_data_length	Définissez la valeur **sur vrai** pour préserver la longueur des données. Les données dépersonnalisées auront la même longueur que les données d'origine.	Vrai

8. Sélectionnez **Créer une technique personnalisée**.
   Votre technique personnalisée est ajoutée aux techniques d'anonymisation.

Que faire ensuite

Reportez-vous à la section Créer des politiques d'anonymisation pour configurer une politique d'anonymisation afin de spécifier les techniques utilisées lors de l'anonymisation de vos données.

Créer des politiques d'anonymisation

Configurez une politique d'anonymisation pour spécifier les techniques utilisées lors de l'anonymisation de vos données.

Avant de commencer

La configuration de confidentialité des données définit les tables, sys_user et autres, ainsi que les colonnes à dépersonnaliser, en fonction du cas d'utilisation, et spécifie les types paramétrés des techniques à utiliser lors de l'anonymisation des données.

Remarque :
Pour terminer une configuration de confidentialité, vous devez d'abord configurer une technique de confidentialité des données. Consultez Créer des techniques d'anonymisation pour en savoir plus.

Rôle requis : data_privacy_admin et admin

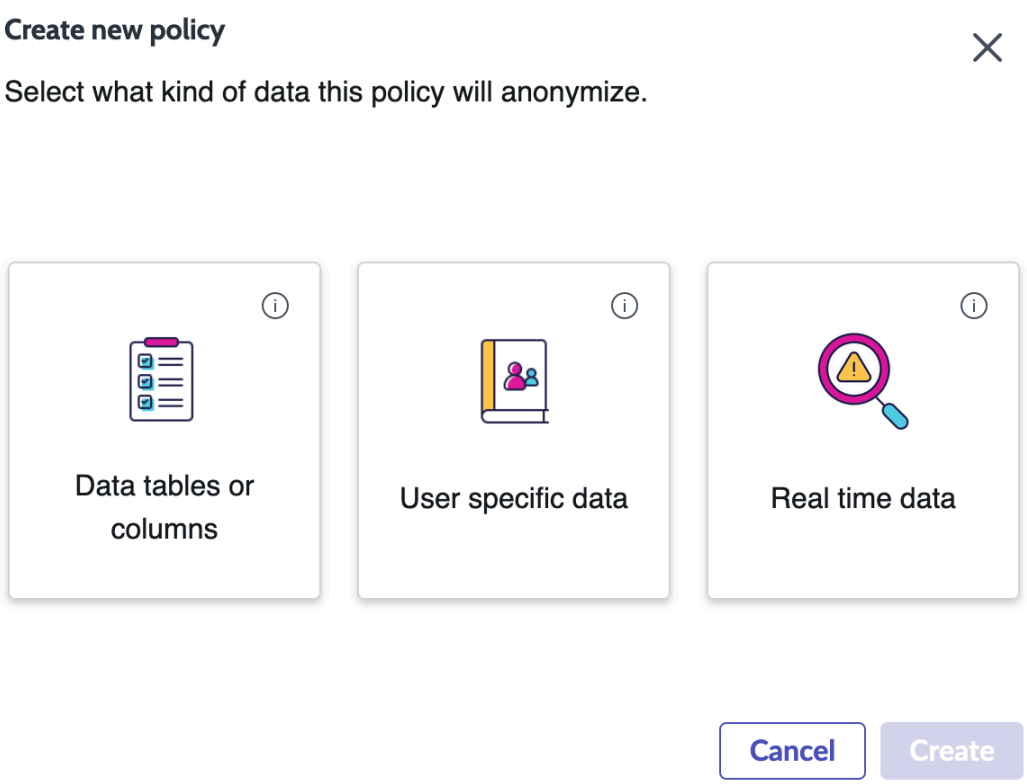
Procédure

1. Élevez-vous au rôle **data_privacy_admin** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
   Toutes les politiques d'anonymisation s'affichent. Des politiques publiées sont disponibles pour planifier la tâche d'anonymisation.
3. Sélectionnez **Créer une nouvelle politique**.
4. Sélectionnez cette option pour anonymiser **les tables ou colonnes de données**, **les données spécifiques à l'utilisateur** ou **les données en temps réel**.



Type de données	Description
Tables ou colonnes de données	Les enregistrements qui correspondent à la politique de données sont anonymisés.
Données spécifiques à l'utilisateur	Sélectionnez un ensemble d'utilisateurs ou de groupes d'utilisateurs à anonymiser.
Données en temps réel	Anonymisez les entrées en temps réel pour un ensemble de colonnes.

Les politiques de confidentialité des données ne peuvent s'appliquer qu'aux données classifiées. Pour plus d'informations sur la classification des données, reportez-vous à la section Classification des données.

5. Sélectionnez **Créer**.
   Des étapes séquentielles sont requises pour finaliser la politique, **définir les détails**et **affecter des techniques**. **Sélectionner la référence de l'utilisateur** est également requis lors de la définition de la politique pour les données spécifiques à l'utilisateur.
6. Définissez les détails de la nouvelle politique d'anonymisation.

Traduction automatique

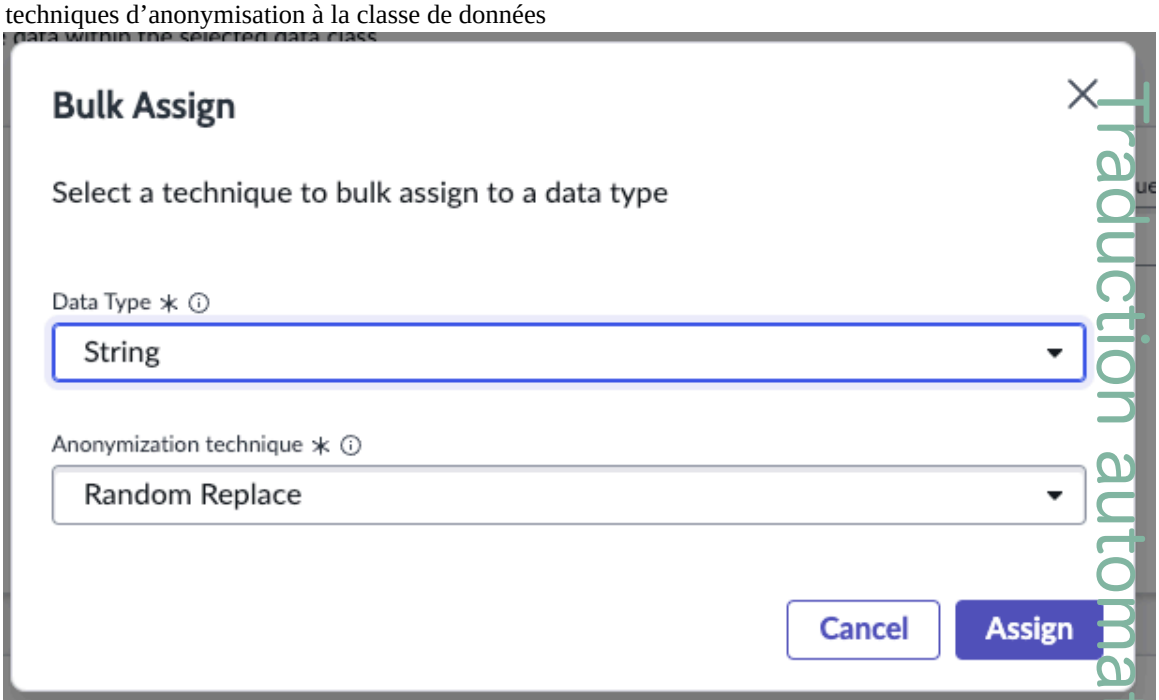
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

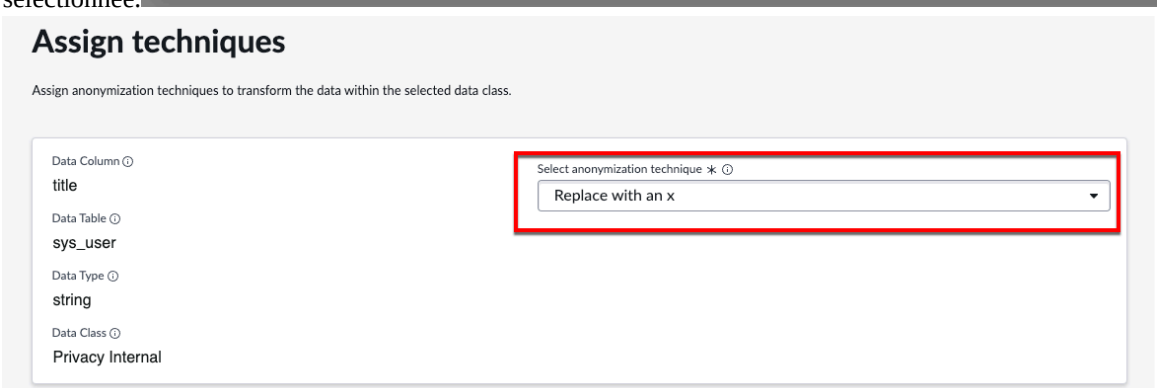
- Entrez le nom de la politique dans le champ **Nom** et la description de la politique dans le champ **Description** .
- Dans le champ **Classe de données** , sélectionnez la classe de données à utiliser avec cette politique.

Remarque :
Si vous n'anonymisez pas une entrée, sélectionnez la technique **DoNothing** plutôt que de laisser l'entrée vide. Les politiques avec des valeurs vides dans le champ Configuration de la technique de confidentialité ne peuvent pas s'exécuter lorsqu'elles sont utilisées dans des tâches de confidentialité des données.

Après avoir sélectionné une classe de données, le formulaire Affecter des techniques s'affiche pour chaque enregistrement renvoyé pour la classe de données définie.

7. Affectez des techniques d'anonymisation à la classe de données sélectionnée.





8. **Facultatif :** Saisissez les tables enfants à analyser.
Les tables enfants du parent sont anonymisées. Si une table n'a pas d'enfants, cette option n'est pas disponible.

Avertissement :
Une tâche parente échouera si une tâche enfant échoue.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. **Facultatif :** Si l'option Anonymisation du modèle de données est sélectionnée, sélectionnez la technique d'anonymisation à utiliser.
10. **Facultatif :** Définissez l'ordre des modèles de données.
11. **Facultatif :**

    Conseil :
    Utilisez la fonction **de test** pour tester des exemples d'entrées. Vous pouvez examiner les mesures à partir des résultats, telles que le temps d'analyse, le résultat et les modèles détectés.

    Sélectionnez le bouton **Test** pour tester la stratégie.

12. **Important :**
    Toutes les tables doivent avoir une entrée sys_dictionary correcte.

    Sélectionnez **Enregistrer**.
13. Sélectionnez **Publier** pour mettre à jour la politique d'anonymisation pour la planification et revenir aux politiques d'anonymisation.

    Remarque :
    Seules les politiques publiées peuvent être utilisées pour la planification des tâches d'anonymisation.

Que faire ensuite
Créer une tâche d'anonymisation.

Configurer l'anonymisation des données Cloner la demande

L'intégration du clone Confidentialité des données est configurée à l'aide d'un script PostClone pour créer et exécuter des tâches de confidentialité des données pour les politiques configurées sur la cible. Après avoir exécuté le script, les utilisateurs verront les données anonymisées et n'auront pas accès aux données d'origine.

Avant de commencer
Le script PostClone de confidentialité des données est installé avec l'activation du module d'extension de confidentialité des données (com.glide.data_privacy). Consultez Activer la confidentialité des données pour en savoir plus.

Rôle requis : data_privacy_clone_processor, data_privacy_admin et admin

Procédure
1. Activez le module d'extension de confidentialité des données (com.glide.data_privacy) sur l'instance source.
   Le script PostClone de confidentialité des données est installé.
2. Élevez-vous au rôle **data_privacy_admin** .
   Pour plus d'informations sur l'élévation de rôle, consultez Élever à un rôle privilégié.
3. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
4. Sélectionnez **Créer une nouvelle politique**.
   Consultez Créer des politiques d'anonymisation pour en savoir plus.
5. Sélectionnez **des tables ou des colonnes de données**.
6. Sélectionnez **Créer**.
7. Saisissez un nom et sélectionnez une classe de données.
8. Sélectionnez cette option pour **activer la politique pendant le clonage**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Sélectionnez l’ordre de la politique à exécuter s’il existe plusieurs politiques de clonage.
   Une tâche de confidentialité des données pour la configuration Postclone avec un ordre d’application plus élevé peut commencer avant une autre tâche d’ordre inférieur, si la tâche d’ordre supérieur n’implique aucune table liée à une autre tâche d’ordre inférieur.
10. Sélectionnez **Continuer**.
11. Terminez la configuration de la politique et publiez-la.
12. Sauvegardez les configurations de confidentialité des données.
13. Planifiez la tâche d’anonymisation.
    Pour en savoir plus, reportez-vous à la rubrique Créer une tâche d’anonymisation.
14. En tant qu’administrateur de la confidentialité des données, soumettez une demande de clone.

Résultats

Le script PostClone s’exécute sur l’instance cible et le script PostClone crée un enregistrement de tâche fédérée sur la confidentialité des données sur l’instance cible. La tâche fédérée crée et exécute une tâche de confidentialité des données pour chaque politique post-clone, dans l’ordre de l’application, sur l’instance cible.La source de sauvegarde est clonée vers l’instance cible. Le script PostClone Confidentialité des données crée et exécute des tâches de confidentialité des données pour les politiques configurées sur l’instance cible.

Le processeur clone de confidentialité des données élevé peut se connecter à l’instance cible et surveiller l’état de la tâche fédérée post-clonage sur les dp_federated_job.list et dp_job.list.

Créer une tâche d’anonymisation

Configurez une tâche de confidentialité des données sur votre instance de production pour utiliser des données rendues anonymes sur votre instance de non-production pour les tâches d’utilisateur et de classe de données.

Avant de commencer

La tâche de confidentialité des données prend en charge deux cas d’utilisation de désidentification :

- Données sensibles d’sys_users spécifiques
- Données sensibles d’une classe de données particulière.

Rôle requis : data_privacy_processor et admin

Procédure

1. Élevez-vous au rôle **data_privacy_processor** .
   Pour plus d’informations sur l’élévation de rôle, consultez Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Confidentialité des données** > **Anonymisation**.
3. Dans une stratégie d’anonymisation, sélectionnez **Planifier la tâche** pour que la politique soit utilisée dans la tâche.
   Une politique doit être à l’état Publié afin de planifier une tâche d’anonymisation.

> ⚠ **Avertissement :**
> Les tâches d’anonymisation sont très destructrices et ne peuvent être inversées qu’en cas de restauration. Vérifiez toutes les informations, telles que les enregistrements et la table traitée, avant de planifier une tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Renseignez les champs du formulaire.

Champs de tâche Confidentialité des données

Champ	Description
Politique utilisée	Nom en lecture seule de la configuration de politique de confidentialité sélectionnée à utiliser pour cette tâche. Modifiez la politique pour afficher des informations supplémentaires sur la politique. Pour en savoir plus sur les configurations de la politique de confidentialité, reportez-vous à la section Créer des politiques d'anonymisation.
Description de poste	Description de la tâche.
Heure de début	Début de l'heure d'exécution de cette tâche dans **HH :MM :SS**.
Heure de fin	Fin de la fenêtre de temps pour exécuter cette tâche dans **HH :MM :SS**. L'heure de fin doit être postérieure à l'heure de début. La tâche s'exécute avant l'heure saisie dans ce champ. Si la tâche n'est pas encore terminée, la tâche sera mise en pause et reprendra au prochain début de la fenêtre horaire.
Essai	Exécutez la tâche en tant que test. Aucun enregistrement n'est affecté lors de l'exécution de cette tâche. Les résultats sont affichés dans la liste **Tâches** , comme si la tâche avait été exécutée. **Remarque :** **L'exécution d'essai** doit être désactivée lors de la configuration d'une tâche de confidentialité des données avec restauration. Consultez Restauration des tâches de confidentialité des données pour en savoir plus.
Type de sélection de l'utilisateur	Sélectionnez les utilisateurs ou les groupes à anonymiser.
Sélectionner des utilisateurs/groupes	Sélectionnez un ensemble spécifique d'utilisateurs ou de groupes à anonymiser dans cette tâche. Prend en charge jusqu'à un maximum de 1 000 utilisateurs. **Remarque :** Ce champ obligatoire s'affiche uniquement lorsque la condition de politique de confidentialité sélectionnée exige une sélection d'enregistrements utilisateur.

Traduction automatique

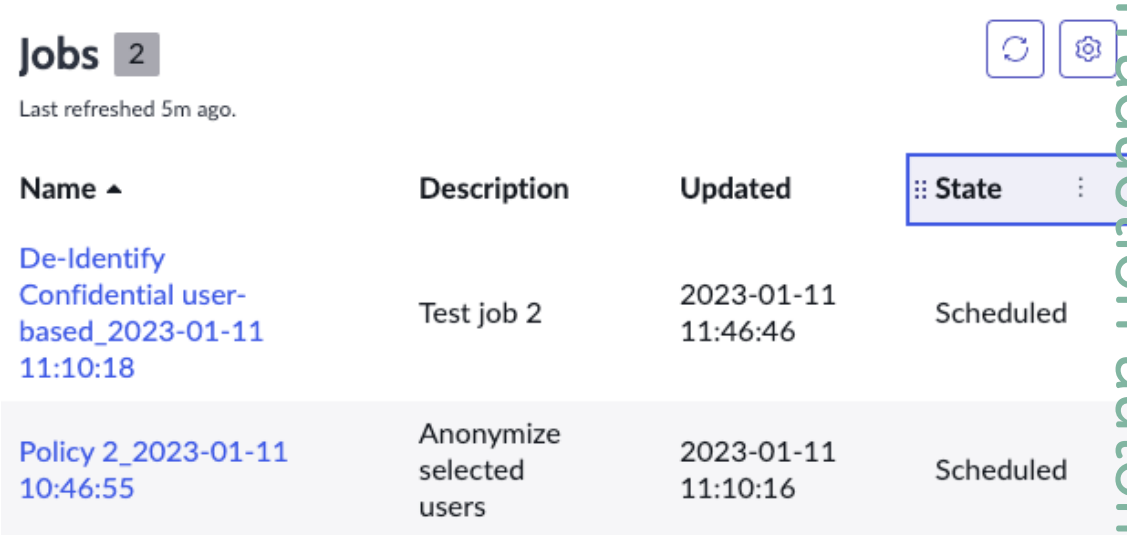
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Important :**
   Toutes les tables doivent avoir une entrée de sys_dictionary correcte avant la planification et pendant sa tâche.

Sélectionnez **Planifier la tâche** sur le formulaire pour placer l'anonymisation dans la file d'attente des tâches.
La tâche s'exécute entre les heures sélectionnées dans les champs **Heure de début** et **Heure de fin** . Si la tâche n'est pas terminée pendant la fenêtre d'heure de début et de fin, la tâche se poursuivra au prochain début de la fenêtre de temps.

Remarque :
Une tâche ne peut être exécutée qu'une seule fois, même si **l'option Essai** est sélectionnée. Pour exécuter à nouveau une tâche basée sur la même politique, sélectionnez **Planifier la tâche** et remplissez le formulaire en utilisant les mêmes valeurs de champ.

La tâche est répertoriée dans le volet



Emplois .

Champ	Description
Nom	Nom de la tâche d'anonymisation.
Description	Description de la tâche d'anonymisation.
Date de mise à jour	Date et heure de la dernière mise à jour de la tâche.
État	État de la tâche de confidentialité des données : ○ **Planifié** : état par défaut pour les nouvelles tâches. ○ **Terminé** : la tâche a anonymisé avec succès les données sélectionnées. ○ **Annulé** : la tâche a été annulée manuellement. ○ **Erreur** : un problème est survenu lors de l'enregistrement de la tâche. Replanifiez la tâche ou créez une nouvelle tâche. Il peut y avoir des problèmes avec la configuration si l'erreur persiste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Restauration en cours** : la tâche a été définie pour restaurer l'anonymisation. ○ **Restauration terminée** : la restauration de la tâche d'anonymisation s'est terminée avec succès. Un champ en lecture seule.

6. Sélectionnez une tâche dans le volet **Tâches** pour ouvrir le résumé de la tâche.
   Une fois qu'une tâche est planifiée, les boutons **Annuler la tâche** et **Pause** apparaissent dans le résumé de la tâche.

Champs supplémentaires pour les travaux planifiés

Champ	Description
Estimer le nombre d'enregistrements	Nombre estimé d'enregistrements que cette exécution d'essai affecte avant d'être exécutée. Un champ en lecture seule
Nombre total d'enregistrements de données traités	Nombre total d'enregistrements de données individuels affectés par cette tâche. Un champ en lecture seule.
Nombre total de tables de données traitées	Nombre total de tables de données traitées par cette tâche. Un champ en lecture seule.
Temps restant pour la restauration	Le temps restant pendant lequel une tâche d'anonymisation des données terminée peut être restaurée et désanonymiser les données. Un champ en lecture seule.
Nombre total d'utilisateurs traités	Nombre total d'enregistrements d'utilisateurs individuels affectés par cette tâche. Un champ en lecture seule.
Annuler le travail	Sélectionnez cette option pour annuler la tâche d'anonymisation. Cette option doit être sélectionnée avant l'heure de début de la tâche. Lorsque cette option est sélectionnée, l'état de la tâche est mis à jour sur *Annulé*.
Pause	Sélectionnez cette option pour mettre en pause la tâche et restaurer l'enregistrement, si la restauration a été sélectionnée. Un message d'avertissement s'affichera après une période d'expiration de trois jours pour les contextes de restauration. Cette option doit être sélectionnée après l'heure de début de la tâche et avant l'heure de fin de la tâche. Lorsque cette option est sélectionnée, l'état de la tâche est mis à jour sur *En pause*.
Reprendre	Redémarre une tâche en pause. La restauration n'est pas prise en charge pour les tâches qui reprennent si elles sont mises en pause. Annuler la tâche et créer une tâche de confidentialité des données. L'enregistrement utilise un contexte de restauration non expiré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Lorsque cette option est sélectionnée, l'état de la tâche est mis à jour sur *Planifié*.
Exporter	Télécharge un fichier .PDF contenant les détails de la tâche de confidentialité des données.

Activer les tâches parallèles pour l'anonymisation des données

Utilisez des tâches parallèles pour réduire le temps d'exécution de votre tâche d'anonymisation.

Avant de commencer

Rôle requis : administrateur

Procédure

Par défaut, les tâches d'anonymisation basées sur la classe de données et l'utilisateur s'exécutent à l'aide d'un seul thread. Plusieurs threads peuvent être activés pour les tâches basées sur la classe de données et l'utilisateur. De plus, les tâches fédérées utilisées lors du clonage utilisent des tâches parallèles avec 3 workers par défaut.

1. Dans le filtre de navigation, saisissez sys_properties.list.
2. Créer la propriété com.glide.data_privacy.max_parallel_workers
3. **Facultatif :** Pour ajuster le nombre d'agents parallèles de tâche fédérés, modifiez la propriété dp.max_concurrent_clone_item_workers .
4. Vérifiez que le **type** est un nombre entier.
5. **Important :**
   Il est recommandé de commencer avec un petit nombre de travailleurs par nœud (2 ou 3).

   Entrez le nombre d'agents de tâches parallèles dans le champ **Valeur** jusqu'à 5.

Traduction automatique

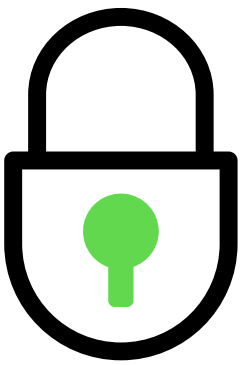
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Chiffrement

Protégez vos données sensibles et restez en conformité avec les exigences et les normes réglementaires.

Key Management Framework



Utilisez le (KMF) pour personnaliser et gérer entièrement la

Key Management Framework

façon dont les opérations de chiffrement sont effectuées sur votre

[qa: BEGIN review][End]

instance.

Certificats

Utilisez des certificats pour établir des connexions sécurisées et valider les signatures.

Chiffrement au niveau des colonnes

Utilisez Chiffrement au niveau des colonnes (CLE) pour autoriser et refuser l'accès aux données chiffrées en fonction du rôle de l'utilisateur. Chiffrement au niveau des colonnes inclut la gestion des clés de base à l'aide de modules de chiffrement.

Chiffrement au niveau des colonnes – Entreprise

Utilisez Chiffrement au niveau des colonnes (CLE) pour autoriser et refuser l'accès aux données chiffrées en fonction du rôle de l'utilisateur. Chiffrement au niveau des colonnes inclut la gestion des clés de base à l'aide de modules de chiffrement.

Chiffrement dans le cloud

Chiffrez votre base de données d'instance à l'aide du chiffrement de blocs, ainsi que d'une gestion des clés améliorée.

Ensemble d'autorisations Chiffrement de la plateforme

Effectuez une mise à niveau vers Chiffrement au niveau des colonnes à usage illimité Entreprise, Chiffrement dans le cloud et Chiffrement de base de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chiffrement complet du disque (FDE)	Chiffrement Edge	Chiffrement de la base de données
Le chiffrement intégral du disque applique le chiffrement à l'ensemble du système de stockage au sein du serveur de base de données uniquement. Parce qu'il s'agit du seul composant de stockage des données client.	Chiffre les données sensibles dans les locaux de votre entreprise avant d'envoyer les données sur Internet à votre [qa: BEGIN review][End] instance ServiceNow. Les données restent chiffrées au repos sur l'instance.	Chiffrez toutes les données stockées en temps réel, offrant une protection des données en ligne et hors ligne sans perte de fonctionnalité.

Key Management Framework

Le chiffrement est une procédure cryptographique qui convertit le texte brut en texte chiffré pour contrôler la divulgation d'informations.

Vue d'ensemble

ServiceNow La gestion des clés comprend les activités impliquant la manipulation des clés cryptographiques et des paramètres de sécurité associés au cours du cycle de vie des clés de bout en bout et constitue un contrôle efficace basé sur les directives 800-57 du National Institute of Standards and Technology (NIST).

Le chiffrement est utilisé pour convertir des chaînes de caractères en texte brut en texte chiffré, qui reste indéchiffrable sans accès à la bonne clé. Les avantages du chiffrement en matière de sécurité découlent de la combinaison d'algorithmes solides et d'une gestion des clés de qualité.

Le chiffrement de toutes les informations peut ne pas être nécessaire pour toutes les données et augmenterait considérablement le temps de traitement en raison du grand nombre de données prises en charge dans toutes les applications. Lorsque vous déterminez que le chiffrement est nécessaire pour les données, les options suivantes Now Platform sont disponibles :

Premiers pas

Comprendre le Cadre de gestion des clés (KMF)	Comprendre le Cadre de gestion des clés (KMF)	Actions de gestion des clés
	L'API [qa: BEGIN review][End] /UX (KMF) vous permet de personnaliser et de gérer entièrement la manière dont	Afficher, gérer et faire pivoter les clés cryptographiques

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	les opérations de chiffrement sont effectuées sur votre [qa: BEGIN review][End] instance.	

Informations sur l'activation

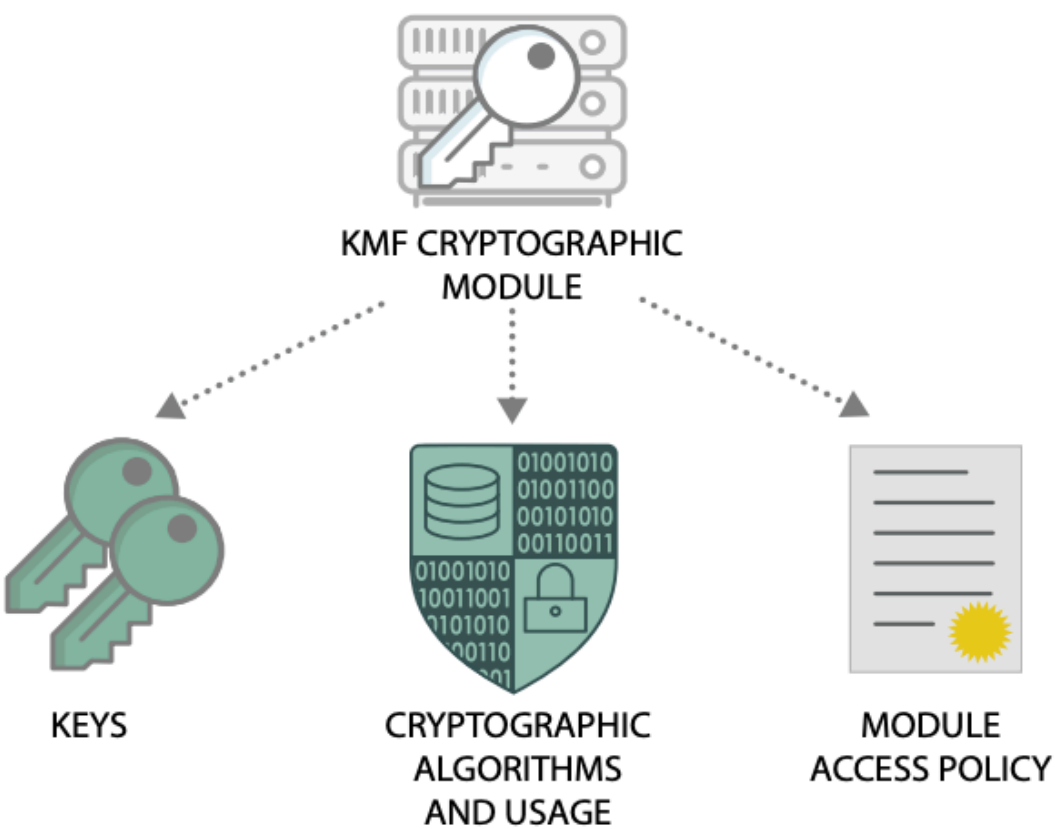
L'offre ServiceNow groupée d'abonnements Chiffrement de la plateforme est une autorisation commerciale de groupe qui inclut Entreprise de Chiffrement au niveau des colonnes, Chiffrement dans le cloudet Chiffrement de base de données.

Entreprise de Chiffrement au niveau des colonnes est la licence illimitée de Chiffrement au niveau des colonnes. Le Chiffrement au niveau des colonnes module d'extension Enterprise est disponible avec l'activation du module d'extension com.glide.now.platform.encryption. Pour plus d'informations, consultez Gestion des clés et chiffrement par lot d'abonnements.

Explorer le cadre de gestion des clés

L'API/UX Key Management Framework (KMF) vous permet de personnaliser et de gérer entièrement la manière dont les opérations de chiffrement sont effectuées sur votre instance. KMF fournit une interface sécurisée et complète pour les services de gestion des clés cryptographiques côté instance.

Vue d'ensemble du cadre de travail de gestion des clés



Ce graphique vous montre les composants qui composent le KMF.

Modules de chiffrement KMF

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les modules cryptographiques sont la pièce maîtresse du KMF. Chaque module de chiffrement sur votre instance définit une méthode de chiffrement pour un cas d'utilisation spécifique. Pour en savoir plus sur ces modules, reportez-vous à la section Vue d'ensemble du module de chiffrement.

Clés

Les clés cryptographiques sont des chaînes de caractères utilisées en cryptographie. Lorsqu'ils sont utilisés avec un algorithme cryptographique, ils peuvent coder ou décoder des données cryptographiques. Ces clés sont utilisées par vos modules cryptographiques. Vous pouvez choisir d'utiliser une clé générée ou de charger votre propre clé fournie par le client avec Chiffrement au niveau des colonnes d'entreprise. Pour en savoir plus sur les clés, reportez-vous à la section Clés de niveau instance dans Key Management Framework.

Algorithmes de chiffrement

Les algorithmes cryptographiques sont des procédures informatiques qui utilisent une clé cryptographique pour coder ou décoder vos données. Ces algorithmes sont définis par la configuration de spécification de chiffrement sur votre instance.

Politiques d'accès au module

Les politiques d'accès aux modules sont des mécanismes de contrôle d'accès appliqués aux modules de chiffrement pour définir des contrôles au niveau de l'instance. Ces politiques déterminent les conditions dans lesquelles l'accès est accordé ou refusé aux modules cryptographiques. Pour plus d'informations, consultez Vue d'ensemble de la politique d'accès au module.

Workflow du cadre de travail de gestion des clés

1. Affectez KMF des administrateurs, qui peuvent à leur tour affecter d'autres KMF rôles.
2. Configurez vos paramètres de chiffrement de champ pour sélectionner soit ServiceNow les clés fournies, soit vos propres clés fournies par le client (CSK) pour le chiffrement.
3. Créez des modules de chiffrement pour définir les mécanismes utilisés pour les opérations de chiffrement.
4. Créez une spécification cryptographique, dans laquelle vous définissez un algorithme de chiffrement et générez une clé.
5. Créez des politiques d'accès au module qui déterminent dans quels contextes vos données peuvent être chiffrées ou déchiffrées.
6. Créez une politique de cycle de vie du module de chiffrement. Ces politiques imposent des limites aux modules de chiffrement au niveau de l'instance, telles que la durée de validité de la clé. Ces stratégies peuvent protéger les modules cryptographiques en limitant leur exposition.

Pour plus d'informations sur ces processus, reportez-vous à la section Actions de gestion des clés.

Principaux avantages du cadre de travail de gestion

Avantage	Fonctionnalité	Utilisateurs
Protégez vos données sensibles et propriétaires.	Gestion du chiffrement et des clés	Tout
Maintenir la conformité avec les directives NIST 800-57 . Ces directives sont fournies par le National Institute of Standards and Technology pour réduire les risques de cybersécurité pour vos réseaux et vos données.	Gestion du chiffrement et des clés	Administrateurs de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantage	Fonctionnalité	Utilisateurs
Utilisez le cadre de travail de gestion des clés pour générer, charger, afficher et gérer vos clés de chiffrement. Utilisez la rotation des clés pour une rotation manuelle ou programmée de vos clés afin d'augmenter la sécurité.	Key Management Framework	Administrateurs de sécurité

Offre groupée d'abonnements pour Encryption and Key Management

Grâce à la gestion des clés, le chiffrement au niveau des colonnes est mis à niveau sans frais supplémentaires par rapport aux modules de chiffrement hautement configurables. Vous avez également la possibilité de passer à la licence d'utilisation illimitée. Abonnez-vous à la nouvelle offre groupée d'autorisations de chiffrement, Chiffrement de la plateforme, qui comprend Entreprise de Chiffrement au niveau des colonnes et Chiffrement dans le cloud.

Fonctionnalités de chiffrement au niveau des colonnes

Le chiffrement au niveau des colonnes avec modules de chiffrement est inclus gratuitement dans votre instance et inclut la gestion des clés NIST 800-57 avec les éléments suivants pris en charge :

- ServiceNow Les clés gérées sont prises en charge (les clés fournies par le client ne sont pas prises en charge).
- L'accès aux modules de chiffrement est uniquement basé sur les rôles.
- Rotation manuelle illimitée des clés.
- Cinq modules de chiffrement au maximum peuvent exister à la fois.
- Il peut exister un maximum de cinq politiques d'accès aux modules à un moment donné.
- Les types de champs existants sont pris en charge. (Les nouveaux types de champs créés dans les versions ultérieures ne seront pas pris en charge dans la version non entreprise.)
- La prise en charge de l'API peut être utilisée en fonction de l'accès au rôle.
- Audit des actions de chiffrement.
- Visite guidée Chiffrement au niveau des colonnes.

ServiceNow Fonctionnalités du groupe Chiffrement de la plateforme

Le groupe Chiffrement de la plateforme ajoute les fonctionnalités et offres suivantes :

- Chiffrement au niveau des colonnes – Entreprise :
  - Clés fournies par le client.
  - Rotation automatique des clés.
  - Prise en charge des types de champs avancés et mises à jour futures.

    Remarque :
    La prise en charge des types de champs étendus inclut les types **de champs Journal**, **Liste de journaux**, **Entrée de journal** et **HTML et Traduit (Champ/Texte/HTML).**

  - Prise en charge avancée des pièces jointes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L’accès au module de chiffrement peut être accordé avec une politique d’accès au module basée sur les éléments suivants :
  - Utilisateur système
  - Script
  - Périmètres d’application spécifiques
- Modules de chiffrement et politiques d’accès aux modules illimités.
- Importer une clé à partir d’un service Web.
- Définissez une date de rotation future pour les clés de chiffrement.

- Chiffrement dans le cloud avec la gestion des clés.

Informations supplémentaires

Pour en savoir plus sur la gestion des clés, reportez-vous Comprendre le cadre de gestion des clésà .

Comprendre le cadre de gestion des clés

L’API Key Management Framework /UX (KMF) vous permet de personnaliser et de gérer entièrement la manière dont les opérations de chiffrement sont effectuées sur votre ServiceNow instance. Le ServiceNow Key Management Framework fournit une interface sécurisée et complète pour les services de gestion des clés cryptographiques côté instance.

Conformément aux directives NIST 800-57 , KMF fournit les fonctionnalités suivantes :

- Séparation des tâches avec des rôles dédiés à la gestion et aux opérations cryptographiques, à l’audit et à l’intégration
- Les modules de chiffrement permettent de configurer des spécifications de chiffrement à des fins de chiffrement et des types de clés uniques
  - Clé symétrique : chiffrement et déchiffrement, encapsulation et désencapsulation de clés, et authentification
  - Clé asymétrique : génération et vérification de signatures numériques, chiffrement et déchiffrement, encapsulation et désencapsulation de clés
- Gestion du cycle de vie des clés pour générer, faire tourner, révoquer et suspendre les clés, y compris la prise en charge de plusieurs états de cycle de vie clés
- Mise en application des contrôles d’accès avec des politiques d’accès aux modules, garantissant que l’accès est accordé uniquement aux modules de chiffrement tels que configurés dans les politiques.
- Protection des clés : Racine de confiance (RoT) matérielle FIPS (Federal Information Processing Standard) 140-2-L3, infrastructure à clé publique (PKI), hiérarchie de clés et chiffrement de l’enveloppe
- Audit qui inclut les statistiques d’utilisation clés

Activation de KMF

KMF est actif par défaut.

Remarque :
KMF ne prend pas en charge Séparation de domaine, mais peut être utilisé avec des instances sur site.

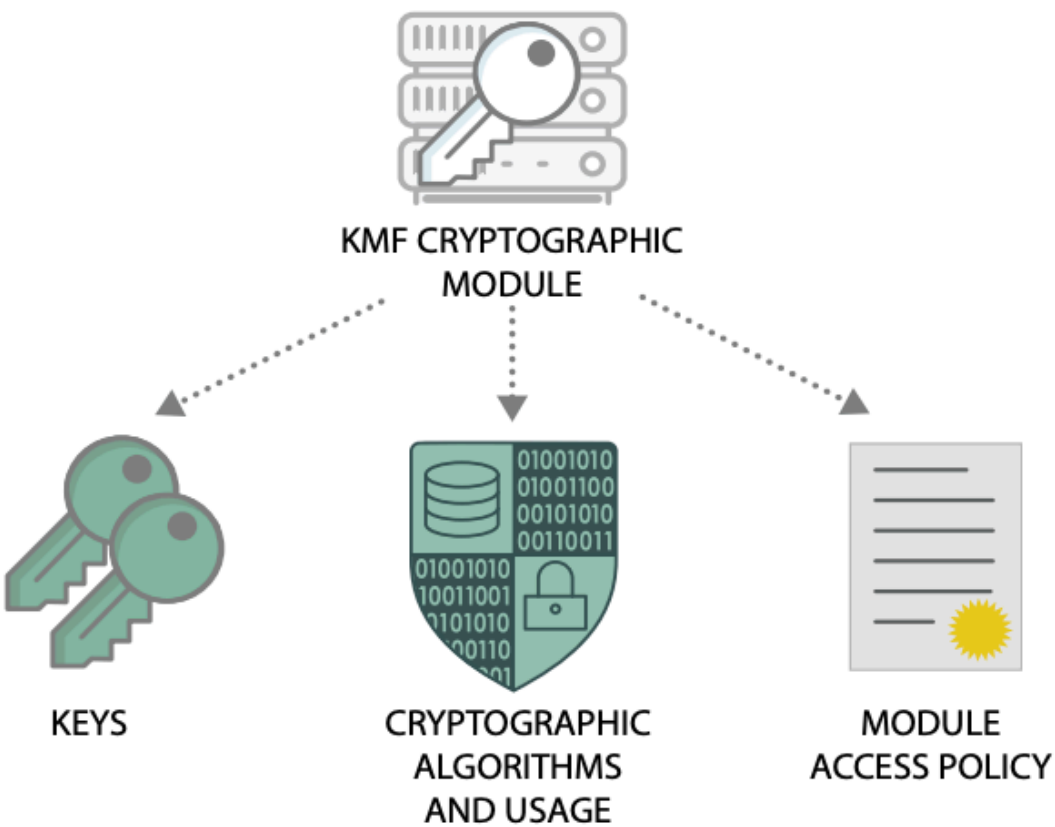
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnement de KMF

Ce graphique vous montre les composants qui composent KMF :

- Les modules cryptographiques sont utilisés pour définir la méthode de chiffrement.
- La spécification cryptographique est une configuration qui définit un algorithme pour le chiffrement.
- La spécification vous permet également de définir la clé du module, une ServiceNow clé ou votre propre clé fournie par le client.
- Une politique d'accès aux modules est une politique au niveau de l'instance qui régit les conditions dans lesquelles l'accès est accordé ou refusé aux modules cryptographiques.



Pour plus d'informations sur KMF, commencez par Vue d'ensemble du module de chiffrement.

Key Management Framework (KMF) introduit des rôles spécifiques pour les configurations liées au module de chiffrement et à la gestion des clés. Seuls les administrateurs KMF peuvent affecter des utilisateurs à d'autres rôles KMF. Consultez Rôles installés avec Key Management Framework pour plus d'informations.

Pour plus d'informations sur l'infrastructure de chiffrement qui succède à CLE, reportez-vous à la section Chiffrement au niveau des colonnes – Entreprise.

Vue d'ensemble du module de chiffrement

Les modules cryptographiques sont la pièce maîtresse de (KMF). Ils définissent les mécanismes cryptographiques spécifiques utilisés pour les opérations cryptographiques pour un cas d'utilisation donné.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un module de chiffrement applique le mécanisme de chiffrement de votre choix à un cas d'utilisation que vous définissez. Par exemple, si vous souhaitez sécuriser les données de votre application RH avec un AES-CBC avec une clé symétrique de 256 bits, vous pouvez créer un module à cet effet.

Les modules cryptographiques prennent également en charge la gestion du cycle de vie des clés. Vous pouvez créer et faire pivoter vos clés cryptographiques, et définir votre méthode de chiffrement. Les modules de chiffrement sont composés des composants suivants :

Spécification cryptographique

Définit les aspects de votre module, y compris son objectif de chiffrement et les algorithmes à utiliser.

Clés cryptographiques

Clé que votre module utilise pour coder ou décoder des données cryptographiques. Il peut s'agir d'une clé générée par votre instance ou d'une clé fournie par le client que vous créez et chargez.

Politiques d'accès au module

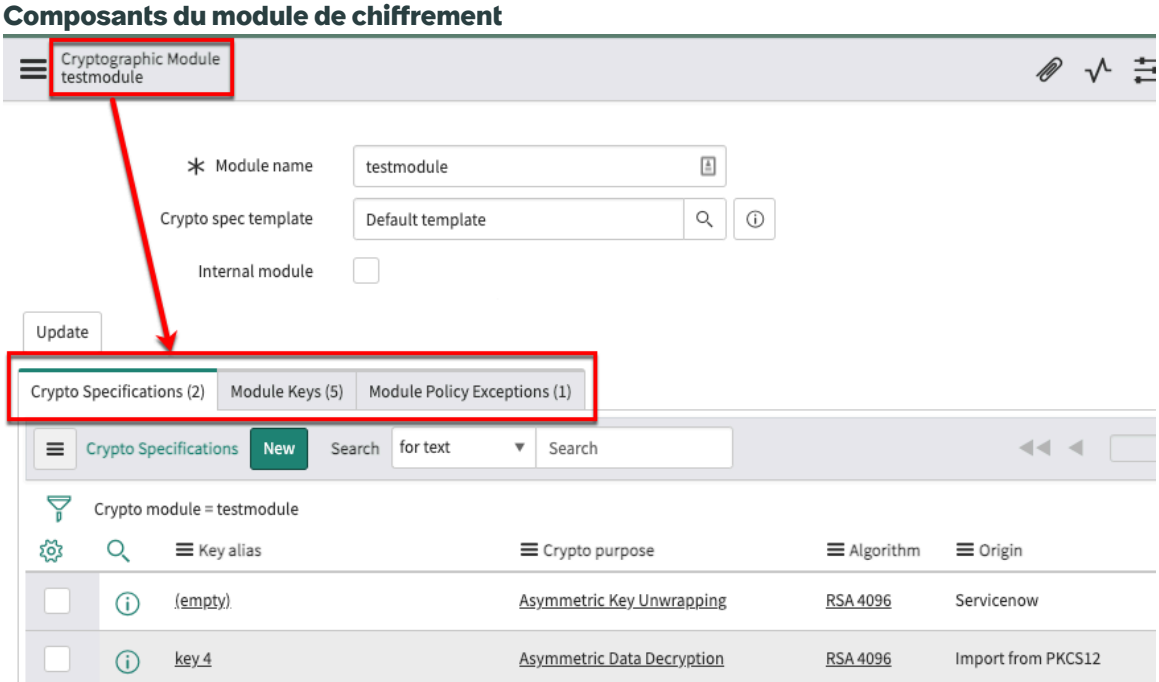
Les politiques d'accès aux modules sont les mécanismes de contrôle d'accès qui limitent le chiffrement ou le déchiffrement des données.

Exceptions de politique du module

Un mécanisme de contrôle pour définir des exceptions à une politique d'accès de module.

L'écran suivant montre ces composants de haut niveau dans un module de chiffrement :

Composants du module de chiffrement



Pour en savoir plus sur la création de modules de chiffrement, reportez-vous à la section Créer un module cryptographique.

Vue d'ensemble de la politique d'accès au module

Les politiques d'accès aux modules sont les contrôles d'accès que vous appliquez à vos modules de chiffrement pour définir des contrôles au niveau de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politiques d’accès au module

Les politiques d’accès aux modules sont introduites avec le Key Management Framework (KMF) dans le système de base.

Remarque :
Un abonnement est requis pour utiliser cette Entreprise de Chiffrement au niveau des colonnes fonctionnalité. Pour plus d’informations, reportez-vous à Entreprise de Chiffrement au niveau des colonnesla section Activer Chiffrement au niveau des colonnes – Entreprise .

Les politiques d’accès aux modules étendent les désignations basées sur les rôles fournies avec les modules de chiffrement. Les politiques d’accès aux modules peuvent être basées sur les éléments suivants :

- Basique (périmètre)
- Rôle
- Utilisateur système
- Script
- Resource Exchange

Remarque :
Consultez Échange de ressources du cadre de travail de gestion des clés pour en savoir plus.

Dans un module cryptographique, vous devez configurer les politiques d’accès au module appropriées pour allouer l’accès aux données chiffrées. Sans une politique d’accès au module associée à un module cryptographique, les données chiffrées ne sont pas visibles par les utilisateurs et les champs et colonnes associés dans les listes s’affichent vides.

Dans cette image, l’absence d’une politique d’accès au module sur le champ Brève description chiffré masque le contenu à tous les utilisateurs accédant à la table Incident. Avec une politique d’accès au module en place, les utilisateurs ayant le rôle autorisé sont en mesure de voir les données chiffrées.

Brèves descriptions chiffrées avec et sans politiques d’accès au module



Remarque :
Les données de la colonne apparaissent également vides pour les utilisateurs qui ne disposent pas du rôle correct spécifié dans la politique d’accès du module.

Reportez-vous à pour la Créer une politique d’accès au module configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politiques de génération automatique

Les politiques de génération automatique sont automatiquement générées par le système en fonction de la politique d'accès au module par défaut définie pour le module de chiffrement donné. Il s'agit de politiques de niveau global qui sont générées et appliquées si aucune politique de niveau granulaire n'est définie lorsque le système ou le script tente d'accéder au module de chiffrement donné.

Important :

Les règles de stratégie de génération automatique ne sont pas appliquées aux types de travaux planifiés ou aux modules de chiffrement de champ (modules dont le module parent est Chiffrement au niveau des colonnes).

Clés de niveau instance dans Key Management Framework

L'architecture Key Management Framework (KMF) introduit une structure clé construite dans un souci de sécurité. À l'aide d'un module de sécurité matériel (HSM), KMF utilise le chiffrement d'enveloppe pour s'assurer que toutes les clés de plateforme gérées KMF sont protégées par une chaîne de clés. Les clés de chiffrement des données client (CDEK) créées par KMF sont également incluses.

Au niveau de l'instance, KMF définit plusieurs clés qui sont utilisées en interne à des fins de chiffrement variables tout au long du Now Platform.

Le chiffrement d'enveloppe est la pratique consistant à chiffrer une clé avec une autre clé. La figure suivante fournit un exemple de chiffrement d'enveloppe. Ici, les CDEK sont cryptés par l'enveloppe par l'IKEK, qui à son tour est une enveloppe cryptée par l'IRK, qui est finalement une enveloppe cryptée par le RK. Étant donné que l'IRK n'est accessible que par le HSM, l'IKEK doit être téléchargé pour le déchiffrement.

Cette table fournit des exemples d'un sous-ensemble de clés client/d'application disponibles qui sont gérées et protégées par KMF.

Clé	Emplacement	Description
Clé racine (RK)	Modèle de sécurité matériel (HSM)	Clé racine utilisée pour déchiffrer l'IRK.
Clé racine d'instance (IRK)	HSM	Clé unique à votre instance qui est utilisée pour chiffrer l'enveloppe de plusieurs clés internes d'instance.
Clé HMAC d'instance (IHK)	Instance	Unique par instance, l'IHK est utilisé en interne à des fins de code d'authentification de message basé sur le hachage (HMAC). L'IHK permet de garantir l'authenticité et l'intégrité des clés de module et est encapsulé soit dans KeySecure, soit dans le magasin de clés de fichier.
Clé de chiffrement de clé d'instance (IKEK)	Instance	L'IKEK englobe les clés du module et est encapsulé soit sur KeySecure, soit sur le magasin de clés de fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Clé	Emplacement	Description
Clé de chiffrement asymétrique d'instance (IAEK)	Instance	Clé unique à votre instance qui est utilisée en interne à des fins de chiffrement asymétrique. L'IAEK est utilisé pour transmettre des messages confidentiels entre une instance pendant ou Réplication de données d'instance l'approbation Key Exchange du consommateur.
Clé de signature d'instance (ISK)	Instance	Une clé unique à votre instance qui est utilisée en interne à des fins de signature.
Password2 (PW2)	Instance	Avec KMF, la clé des PW2 champs est entièrement gérée par KMF.
Clé de chiffrement des données client (CDEK)	Instance	Les clés de chiffrement créées sont KMF cryptées par enveloppe par l'IKEK.
Réplication de données d'instance (IDR) Clé de chiffrement des données (DEK)	Instance	Clés de chiffrement spécifiques utilisées pour le processus IDR.

Objectif cryptographique, algorithmes et informations clés

Les spécifications cryptographiques peuvent être adaptées à un objectif cryptographique spécifié, couvrant à la fois les opérations cryptographiques asymétriques et symétriques basées sur des clés. La sélection d'un objectif cryptographique offre d'autres choix, à savoir un ensemble d'algorithmes pris en charge et de configurations de longueur de clé.

Finalités cryptographiques, algorithmes et informations clés

Objectif de chiffrement	Algorithme	Informations clés
Déchiffrement asymétrique des données	RSA	Asymétrique : clé 2 048 bits, 3 072 bits et 4 096 bits
Chiffrement asymétrique des données	RSA	Asymétrique : clé 2 048 bits, 3 072 bits et 4 096 bits
Désencapsulation de clé asymétrique	RSA	Asymétrique : clé 2 048 bits, 3 072 bits et 4 096 bits
Encapsulation de clé asymétrique	RSA	Asymétrique : clé 2 048 bits, 3 072 bits et 4 096 bits
Génération de signature	RSA	Asymétrique : clé 2 048 bits, 3 072 bits et 4 096 bits
Vérification de signature	RSA	Asymétrique : clé 2 048 bits, 3 072 bits et 4 096 bits
Authenticité symétrique	HMAC	Symétrique : clé 256 bits, 384 bits et 512 bits
Chiffrement/déchiffrement symétrique des données*	AES-CBC *	Symétrique – clé 128 bits, 192 bits, 256 bits
	AES-CFB (en anglais seulement)	
	AES-OFB	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Finalités cryptographiques, algorithmes et informations clés (suite)

Objectif de chiffrement	Algorithme	Informations clés
	AES-CTR (en anglais seulement)	
	AES-GCM **	
Encapsulation/désencapsulation de clé symétrique*	AES-CBC *	Symétrique – clé 128 bits, 192 bits, 256 bits
	AES-CFB (en anglais seulement)	
	AES-OFB	
	AES-CTR (en anglais seulement)	
	AES-GCM **	

* AES-CBC prend en charge les options de préservation de l'égalité. Entreprise de Chiffrement au niveau des colonnes utilise AES-CBC.

** AES-GCM intègre l'intégrité des données.

La configuration de ces paramètres est décrite dans Créer un module cryptographiquela section .

États du cycle de vie des clés du cadre de travail de gestion des clés

KMF prend en charge plusieurs états du cycle de vie des clés cryptographiques grâce à l'application d'actions autorisées spécifiques. Par exemple, seules les clés dont l'état est actif peuvent être entièrement utilisées aux fins de chiffrement prévues. Le tableau suivant fournit plus de détails sur les différents états clés du cycle de vie.

État ou action du cycle de vie de la clé	Description
Actif	Il ne peut y avoir qu'une seule clé active pour une spécification cryptographique donnée dans un module cryptographique.
Compromis	Plusieurs clés peuvent exister à l'état compromis pour être révoquées dans une spécification cryptographique donnée dans un module cryptographique. Toute clé active ou suspendue peut être déplacée vers un état compromis. Les clés compromises ne peuvent pas être utilisées pour générer de nouveaux contenus, tels que le chiffrement ou la signature, mais peuvent toujours être utilisées pour identifier l'objectif du contenu existant, tel que le déchiffrement ou la vérification.
Désactivé	Toute clé active peut être désactivée. Il peut y avoir plusieurs clés à l'état désactivé pour une spécification cryptographique donnée dans un module cryptographique. Par exemple, lorsque la clé est tournée, la clé active actuelle est désactivée. Les clés désactivées ne peuvent pas être utilisées pour générer de nouveaux contenus, tels que le chiffrement et la signature, mais peuvent toujours

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État ou action du cycle de vie de la clé	Description
	être utilisées pour identifier les objectifs du contenu existant, tels que le déchiffrement ou la vérification. **Remarque :** Les clés compromises et révoquées sont traitées comme des clés désactivées.
Détruit	Lorsqu'une clé est détruite, le matériel de clé est définitivement supprimé et ne peut plus être utilisé à des fins cryptographiques. Toute clé désactivée peut être détruite à l'aide de l'automatisation du cycle de vie lorsqu'elle n'a pas été utilisée dans le délai configuré. Il peut y avoir plusieurs clés à l'état détruit pour une spécification cryptographique donnée dans un module cryptographique. **Avertissement :** Les données associées à une clé détruite ne sont plus accessibles, il convient donc de faire preuve d'une extrême prudence lors de l'exécution d'une action de destruction de clé.
Généré	Plusieurs clés peuvent exister à l'état généré pour une spécification cryptographique donnée dans un module cryptographique. Une clé générée peut être passée à un état actif lorsqu'aucune clé active n'existe pour la spécification de chiffrement donnée. La première clé générée est automatiquement activée. **Remarque :** Si vous choisissez de générer une nouvelle clé, alors une nouvelle clé est générée et rendue active même s'il existe des clés à l'état généré pour la spécification de chiffrement donnée.
Renouvelé	Une clé active ayant une date d'expiration peut être renouvelée autant de fois que nécessaire pour étendre la période de cycle de vie de la clé. **Remarque :** La différence entre la date d'activation et la date d'expiration est calculée et la date d'expiration est reportée de cette durée par rapport au jour actuel.
Reprendre	L'action d'interface utilisateur est disponible sur les clés suspendues pour les ramener à un état actif lorsqu'aucune autre clé active n'existe pour la spécification de chiffrement donnée.
Révoqué	Toute clé active ou suspendue peut être passée à l'état révoqué. Les clés révoquées ne peuvent pas être utilisées pour générer du nouveau contenu, par exemple pour le chiffrement ou la signature, mais elles peuvent tout de même être utilisées pour identifier l'objectif du contenu existant, par exemple à des fins de déchiffrement ou de vérification. Plusieurs clés à l'état révoqué peuvent exister pour une spécification cryptographique donnée dans un module cryptographique.
Pivoté	La rotation des clés entraîne la désactivation de la clé active actuelle et la activation d'une autre clé. Sélectionnez la nouvelle clé active parmi les suivantes :

Traduction automatique

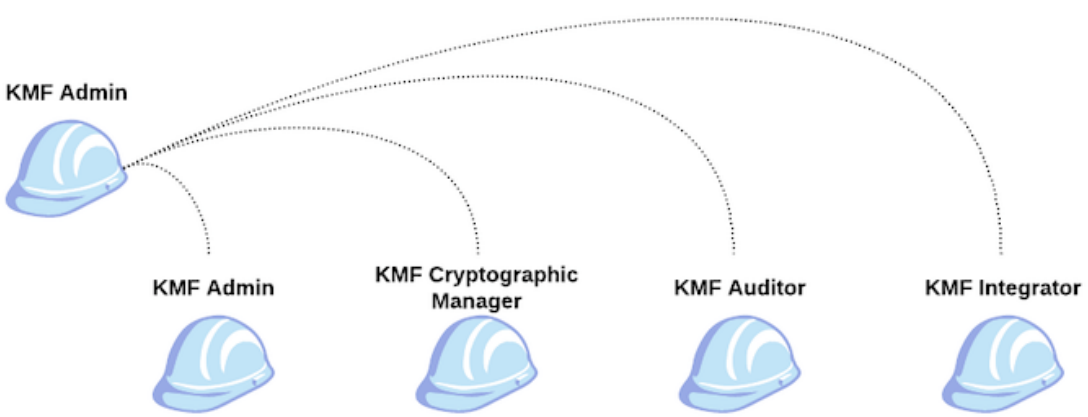
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

État ou action du cycle de vie de la clé	Description
	• Génération d'une nouvelle clé. • Pointez vers une clé importée existante. N'importe quelle clé active peut être pivotée.
Suspendu	Il peut y avoir plusieurs clés à l'état suspendu pour une spécification cryptographique donnée dans un module cryptographique. Lorsque la clé est suspendue, elle peut être reprise et réaffectée à un état actif lorsqu'aucune autre clé active n'existe pour cette spécification cryptographique.

Rôles installés avec Key Management Framework

Le Key Management Framework (KMF) introduit des rôles spécifiques pour les configurations liées au module cryptographique et à la gestion des clés.

Important :
Pour affecter le rôle administrateur KMF, vous devez disposer des rôles administrateur, security_admin et sn_kmf_admin. Utilisez le rôle administrateur KMF pour affecter d'autres rôles KMF. Pour plus d'informations sur l'affectation des rôles KMF, reportez-vous à la section Affecter KMF des rôles.



Administrateur KMF [sn_kmf.admin]

Affecte des rôles à d'autres utilisateurs pour effectuer des opérations autour de ServiceNow Key Management Framework.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Considérations particulières

Important :
Évitez d'accorder un rôle administrateur lorsque des rôles plus spécialisés sont disponibles.

- Ce rôle est affecté via le processus illustré à la section Affecter KMF des rôles.
- Vous devez disposer de ce rôle pour affecter des rôles KMF et vous pouvez en outre exécuter toutes les options du gestionnaire de chiffrement KMF.

Gestionnaire de chiffrement KMF [sn_kmf.cryptographic_manager]

Créez, lisez et mettez à jour les opérations sur les modules cryptographiques (association des clés à l'utilisation cryptographique et aux configurations d'algorithmes) et les politiques d'accès aux modules. En outre, les gestionnaires cryptographiques KMF peuvent effectuer des opérations de gestion des clés (générer, rotation, révoquer) et de cycle de vie.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Aucun.

Auditeur cryptographique KMF [sn_kmf.cryptographic_auditor]

Affichez les informations du module de chiffrement, les métadonnées clés et les détails relatifs au cycle de vie, ainsi que les informations sur la politique d'accès au module (MAP).

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Aucun.

Intégrateur cryptographique KMF [sn_kmf.cryptographic_integrator]

Intégrez Key Management Framework des keystores ou des systèmes externes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Aucun.

Opérateur de chiffrement KMF [sn_kmf.cryptographic_operator]

Partie de l'accès au cycle de vie de la ServiceNow Key Management Framework clé : renouvellement, rotation, révocation.

Contient des rôles

Liste des rôles contenus dans le rôle.

Aucun.

Groupes

Liste des groupes auxquels ce rôle est affecté par défaut.

Aucun.

Considérations particulières

Aucun.

Affecter KMF des rôles

Affectez KMF des rôles aux administrateurs, qui peuvent à leur tour affecter d'autres KMF rôles.

Avant de commencer
Rôle requis : admin et security_admin

Vous devez vous élever au rôle security_admin avant de lui affecter le KMF rôle administrateur. Pour obtenir des instructions, consultez Élever à un rôle privilégié

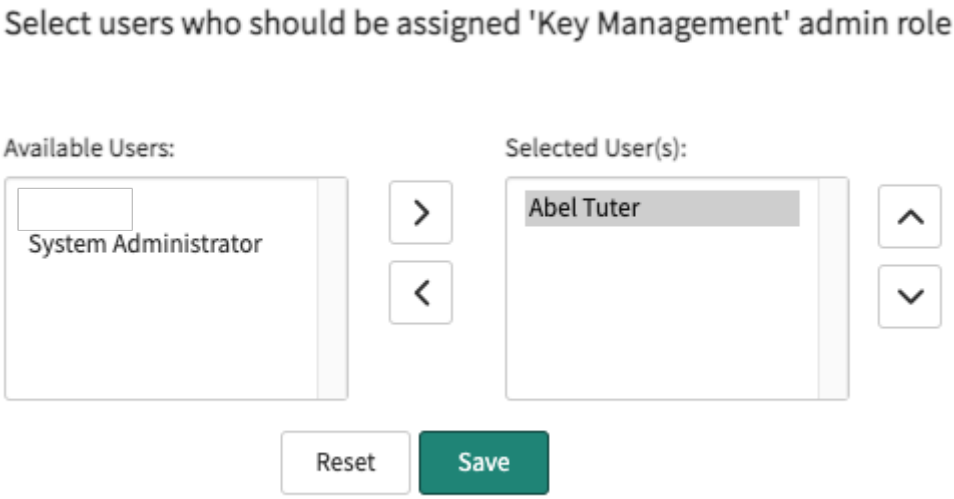
Procédure

1. Élevez-vous au rôle d'administrateur de sécurité.
2. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur que vous souhaitez nommer KMF administrateur.
3. Vérifiez que l'utilisateur dispose déjà des rôles administrateur et security_admin.
   Si ce n'est pas le cas, sélectionnez **Modifier** sous la liste connexe Rôles et ajoutez des _admin **d'administration** et **de sécurité**.
4. Accédez à la **Sécurité de système** > **Administration de la gestion de clés**.

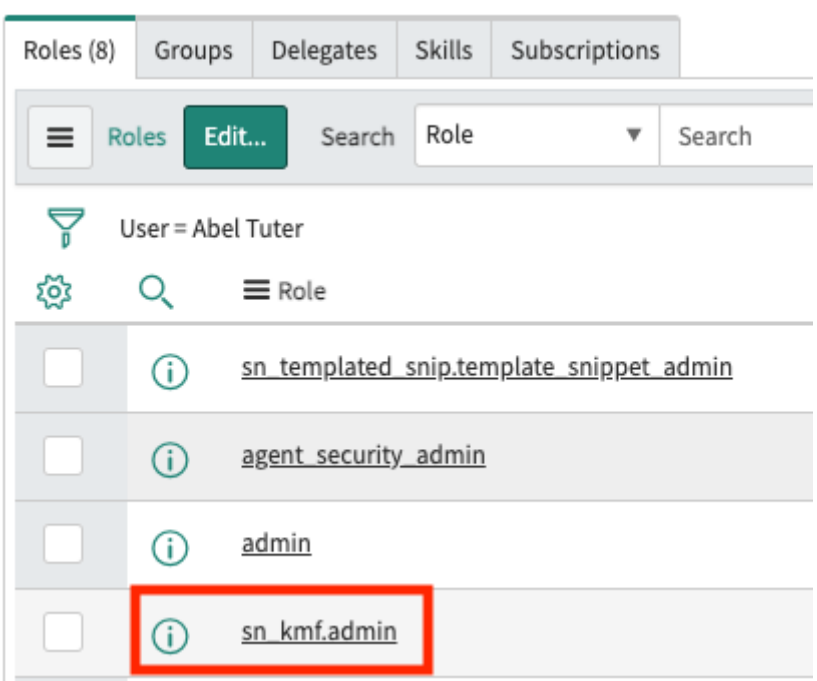
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez l'utilisateur que vous souhaitez nommer KMF administrateur dans la colonne **Utilisateurs disponibles** et déplacez-le vers la colonne **Utilisateur(s) sélectionné(s).**



6. Sélectionnez **Enregistrer**.
7. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur auquel vous venez de conférer le rôle sn_kmf.admin.
   L'utilisateur dispose du rôle sn_kmf.admin dans la liste connexe **Rôles** et peut affecter d'autres rôles KMF.



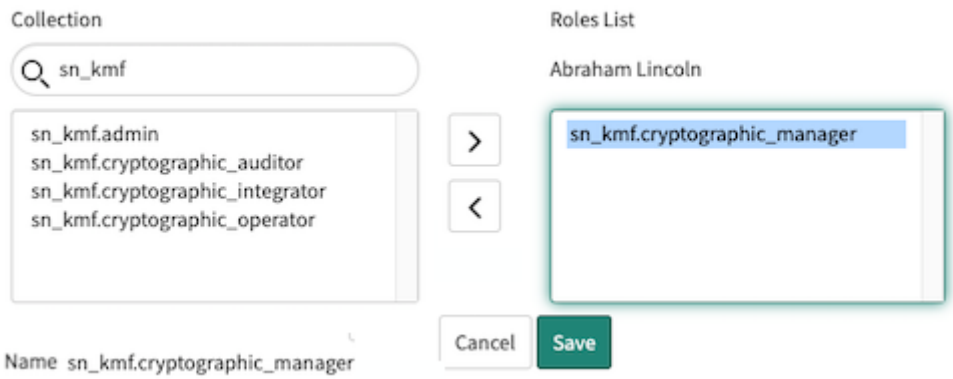
Que faire ensuite

Si vous disposez du rôle administrateur KMF, procédez comme suit pour affecter d'autres rôles KMF :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Accédez à la **Administration utilisateurs** > **Utilisateurs** et sélectionnez l'utilisateur auquel vous souhaitez confier un autre rôle KMF, tel que Gestionnaire de chiffrement KMF.
2. Dans la liste connexe **Rôles** , sélectionnez Modifier, puis sélectionnez les rôles KMF que vous souhaitez affecter aux utilisateurs. Tous les rôles KMF commencent par `sn_kmf`.



Configurer les paramètres de chiffrement de champ pour sélectionner le type de clé

Configurez vos paramètres de chiffrement de champ pour utiliser ServiceNow les clés fournies ou vos propres clés fournies par le client (CSK) pour le chiffrement sur Now Platform.

Avant de commencer

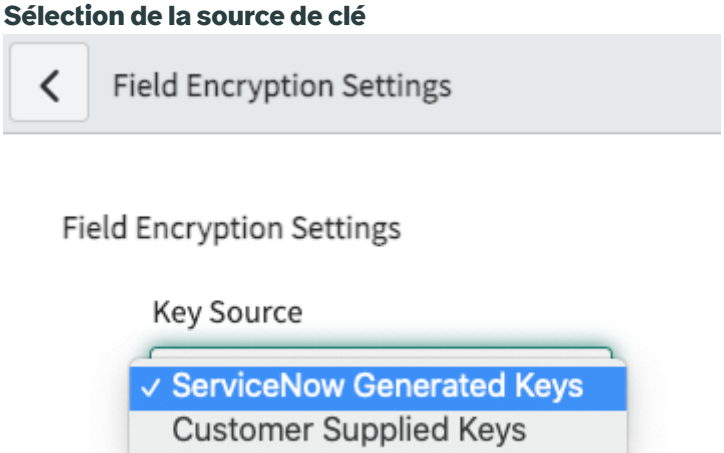
Les clés fournies par le client ne sont prises en charge qu'avec Entreprise de Chiffrement au niveau des colonnes.

Rôle requis : sn_kmf.cryptographic_manager et security_admin

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Paramètres de Chiffrement de champ**.
2. Dans les paramètres de chiffrement de champ, sélectionnez **Clés générées par ServiceNow** ou **Clés fournies par le client** dans la liste Source de **clés** .

Sélection de la source de clé



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette option remplace la propriété com.glide.encryption.cle_kmf.key_source par **Clés générées par ServiceNow** ou **Clés fournies par le client**.

3. Sélectionnez **Enregistrer**.

Que faire ensuite

- Si vous utilisez vos propres clés fournies par le client, reportez-vous à la section Utilisation des clés fournies par le client avec Chiffrement au niveau des colonnes – Entreprise.
- Si vous utilisez les ServiceNow clés fournies, commencez à créer votre module cryptographique. Consultez Créer un module cryptographique.

Créer un module cryptographique

Créez un module de chiffrement pour définir les mécanismes utilisés pour les opérations de chiffrement. Une fois le module créé, vous créez une spécification cryptographique, dans laquelle vous définissez un algorithme de chiffrement et générez une clé.

Avant de commencer

Si vous fournissez vos propres clés, reportez-vous à Configurer et charger votre clé fournie par le clientla section .

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Cette procédure décrit les options disponibles dans KMF le système de base de la ServiceNow plate-forme. Entreprise de Chiffrement au niveau des colonnes La fonctionnalité n'est disponible que lorsque le module d'extension `com.glide.now.platform.encryption` est actif. Pour Activer Chiffrement au niveau des colonnes – Entreprise plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes. Consultez Créer un module cryptographique pour Chiffrement au niveau des colonnes.

Remarque :
Les enregistrements du module de chiffrement [sys_kmf_crypto_module] ne peuvent pas être supprimés.

Procédure

1. Accédez à la **Tout** > **Gestion des clés** > **Modules de chiffrement** > **Créer**.
2. Renseignez les champs suivants du formulaire :

Champs du module de chiffrement

Champ	Description
Nom du module	Chaîne alphanumérique à référencer lors de l'exécution de scripts.
Modèle de spécification de chiffrement	Sélectionnez le modèle **par défaut** à utiliser pour créer le module cryptographique, car il contient des mappages d'algorithmes pris en charge pour les spécifications cryptographiques.
Valeur de la politique d'accès au module par défaut	○ S'appuyer sur le système par défaut : ○ Refuser ○ Trace

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Résultat réel de la politique d'accès au module	Rejeter ou suivre, en fonction de la valeur de politique par défaut ou de la valeur sélectionnée lors de la création de la politique d'accès au module.
Nom	Nom du module de chiffrement précédé du nom du périmètre de l'application.
État du cycle de vie du module de chiffrement	Le cycle de vie fait référence à la création, à l'utilisation et à la désactivation d'un module cryptographique. Défini sur **Brouillon** initialement lors de la configuration. Lors de l'utilisation du module, définissez ce champ sur **Publié**. Le modèle par défaut est automatiquement défini sur Publié.

3. Sélectionnez **Soumettre**.

⚠ Avertissement :

Pour les utilisateurs de l'assistance de chiffrement héritée :

Si vous utilisez la version non entreprise de Chiffrement au niveau des colonnes, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

Cette insertion dépasse le nombre de limites des modules publiés de Chiffrement au niveau des colonnes autorisées avec le produit d'abonnement. L'abonnement Entreprise à Chiffrement au niveau des colonnes est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

Une fois l'envoi réussi, votre module de chiffrement est répertorié dans la table Modules de chiffrement. Le système ajoute le champ d'application au nom pour éviter tout conflit avec d'autres applications incluses dans le périmètre. Par exemple, si vous avez créé un module avec le nom `my_crypto_module` dans le périmètre de l'application global, le nom est enregistré comme `global.my_crypto_module`.

Que faire ensuite

Créer une spécification cryptographique

.

Créer une spécification cryptographique

Après avoir créé un module cryptographique, créez une spécification cryptographique pour définir les algorithmes du module.

Avant de commencer

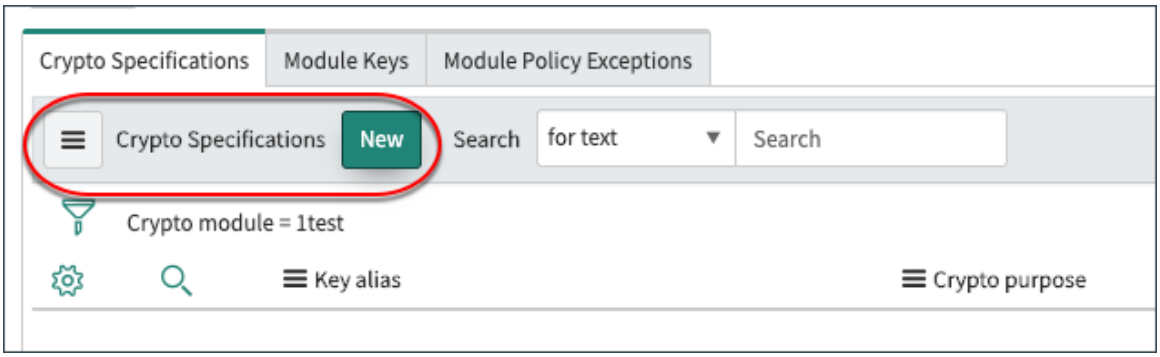
Rôle requis : sn_kmf.cryptographic_manager

Procédure

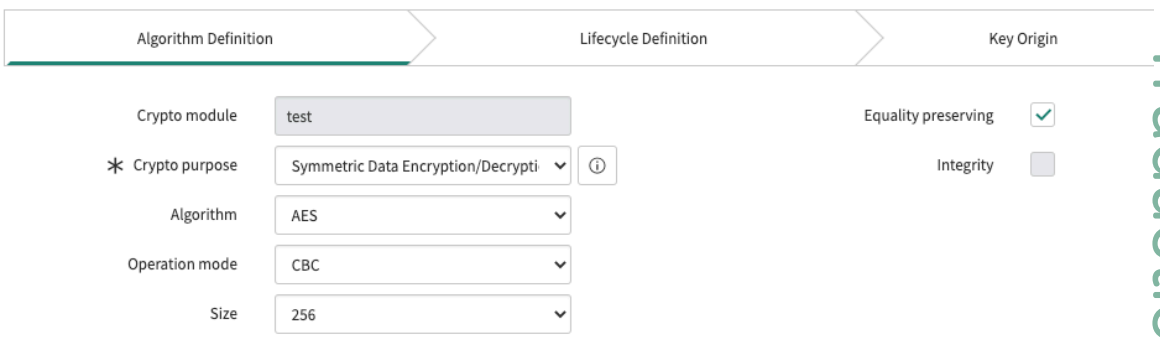
1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tout**.
2. Sélectionnez le module de chiffrement pour définition afin d'ouvrir les options de configuration.
3. Dans l'onglet **Spécifications de chiffrement** , cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Remplissez le formulaire de définition de l'algorithme.
   Consultez Objectif cryptographique, algorithmes et informations clés pour en savoir plus.



L'écran de définition de l'algorithme s'ouvre. Sélectionnez les options de la génération de clés. Répétez cette étape pour générer plusieurs clés pour le module de chiffrement sélectionné.

Champs de définition d'algorithme

Champ	
Module de chiffrement	Lecture seule. Le nom du module de chiffrement sélectionné s'affiche.
Objectif de chiffrement	Sélectionnez l'objectif de ce module. Par exemple, vous pouvez l'utiliser pour le chiffrement de données, la génération de signatures ou l'emballage de clés. Les algorithmes disponibles s'ajustent en fonction de l'objectif de chiffrement sélectionné. Consultez Objectif cryptographique, algorithmes et informations clés pour en savoir plus.
Algorithme	Type d'algorithme utilisé pour atteindre l'objectif de chiffrement. L'algorithme contrôle également l'origine de la clé. S'ajuste automatiquement en fonction de l'objectif de chiffrement sélectionné. Objectif cryptographique, algorithmes et informations clés pour plus de détails.
Mode d'opération	Ce champ peut s'afficher en fonction de l'objectif de chiffrement sélectionné.
Taille	Sélectionnez la taille de bits.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	
Hachage	Ce champ devient disponible en fonction de l'algorithme sélectionné.
Préservation de l'égalité	Active le chiffrement non déterministe. Cette option s'affiche lorsque vous sélectionnez **Chiffrement/déchiffrement symétrique des données** avec **AES** et en mode **CBC (Cipher Block Chaining).** La sélection de cette option signifie que si les mêmes données sont chiffrées à nouveau, les données codées sont les mêmes à chaque fois. Le chiffrement non déterministe ne prend pas en charge le filtrage d'une liste de données chiffrées à l'aide d'opérateurs de comparaison d'égalité.
Intégrité	Le mode de fonctionnement GCM assure l'intégrité.

5. Cliquez sur **Suivant**.
   La spécification de chiffrement est répertoriée dans la table Cycle de vie de la clé en fonction des algorithmes sélectionnés.

Que faire ensuite

Effectuez l'une des opérations suivantes :

- Sélectionnez une entrée dans la table Cycle de vie de la clé pour définir le comportement du cycle de vie de la clé. Consultez Configurer les états clés du cycle de vie pour en savoir plus sur la définition du cycle de vie de la clé.
- Cliquez sur **Suivant** pour créer une clé cryptographique. Reportez-vous à l'une des tâches suivantes pour la génération de clés :
  - Générer une clé cryptographique ServiceNow.
  - Configurer les propriétés des clés fournies par le client.
  - Importer la paire de clés d'encapsulation/de désencapsulation.

Configurer les états clés du cycle de vie

Après avoir créé une spécification de chiffrement, vous pouvez configurer les actions de cycle de vie pour les clés dans votre instance.

Avant de commencer

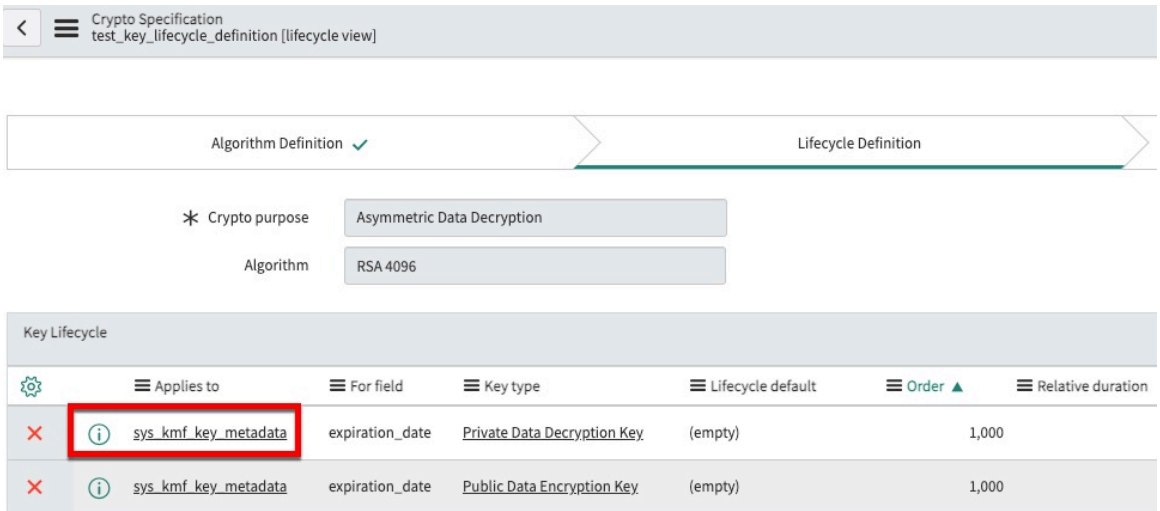
Rôle requis : sn_kmf.admin

Procédure

1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tout**.
2. Sélectionnez le module de chiffrement pour configurer le cycle de vie d'une clé.
3. Cliquez sur un alias de clé dans l'onglet Spécifications de chiffrement.
   Le formulaire de définition de l'algorithme s'ouvre pour la clé sélectionnée.

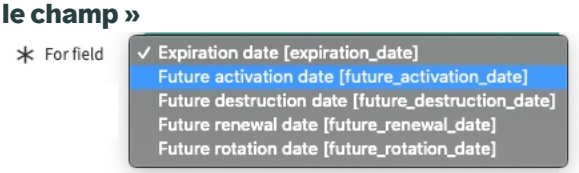
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



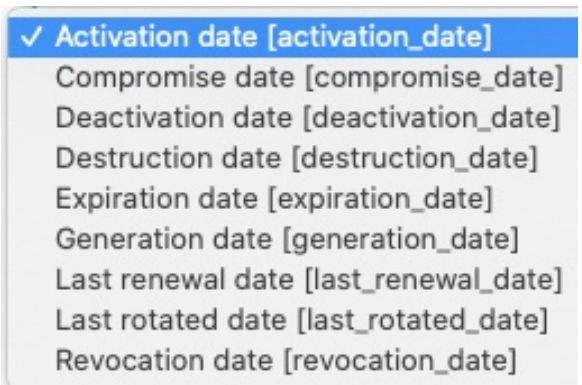
4. Cliquez sur **Suivant**.
   Le modèle de cycle de vie du champ se charge. Les valeurs de cycle de vie de la clé par défaut sont créées en fonction des algorithmes sélectionnés pour la spécification de chiffrement définie.
5. Sélectionnez un cycle de vie de clé dans la colonne **S'applique à de l'étape** Définition du cycle de vie de la spécification de chiffrement.

Champs du cycle de vie de la clé

Champ	Description
Concerne	Clé sélectionnée à laquelle le cycle de vie s'applique.
Pour le champ	Sélectionnez le type de contrôle de la clé à laquelle le cycle de vie s'applique. **Gestion du cycle de vie des clés Valeurs « Pour le champ »** 
Type	Indiquez si l'évaluation du cycle de vie de la clé est une valeur relative ou une valeur absolue : ○ **Relative** : entrez une valeur qui dépend d'autres entrées de données dans le système, telles que la génération de clés, l'activation et la désactivation. ○ **Absolu** : entrez une valeur exacte, telle qu'une date.
Valeur par défaut du cycle de vie	Lecture seule. Affiche une valeur si elle est définie.
Ordre	Entrez la séquence dans laquelle traiter l'état du cycle de vie de la clé pour la spécification de chiffrement.
Type de durée relative	Durée du cycle de vie : **années**, **mois** ou **jours**.
Durée relative	Nombre d'années, de mois ou de jours de validité de la clé.
Opération relative	**Avant**ou **après**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Relatif à	Champ par rapport auquel la durée est relative. S'affiche si une durée ou une opération relative est sélectionnée. 

Générer une clé cryptographique ServiceNow

Suivez cette procédure pour charger et configurer une ServiceNow clé cryptographique afin de chiffrer les données sensibles.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Les gestionnaires de chiffrement ont le choix d'utiliser ServiceNow les clés fournies ou leurs propres clés fournies par le client (CSK) pour le chiffrement sur le Now Platform fichier .Entreprise de Chiffrement au niveau des colonnes Pour plus d'informations sur CSK, reportez-vous à la section Configurer les propriétés des clés fournies par le client.

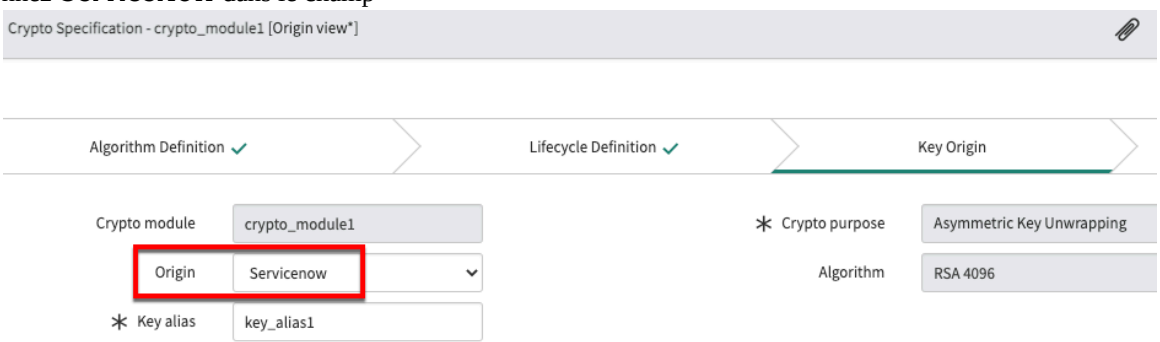
Procédure

1. Définissez les paramètres de chiffrement de champ pour utiliser les clés générées par ServiceNow. Consultez Configurer les paramètres de chiffrement de champ pour sélectionner le type de clé pour en savoir plus.
2. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tout**.
3. Sélectionnez le module de chiffrement correspondant pour ouvrir la page des détails du module de chiffrement.
4. Cliquez sur la ligne de l'entrée de l'alias de clé dans l'onglet Spécifications de chiffrement.
   Si aucune clé n'a encore été générée, le champ alias de la clé est vide.
5. Cliquez sur **Suivant** pour accéder à l'onglet Origine de la clé des composants de spécification de chiffrement.
   L'onglet Définition du cycle de vie s'affiche avec la table Cycle de vie de la clé et peut être révisé ou modifié.
   Consultez Configurer les états clés du cycle de vie pour en savoir plus.

Traduction automatique

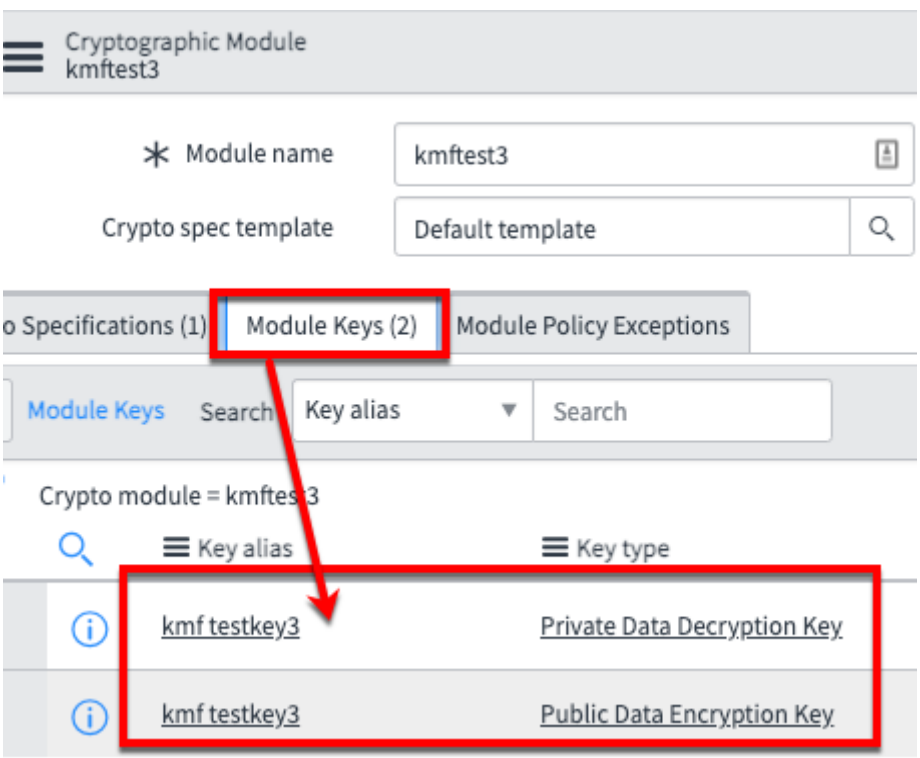
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Sélectionnez **ServiceNow** dans le champ



Origine.
Ce champ varie en fonction des paramètres de chiffrement de champ de l'étape 1 et de l'algorithme sélectionné. Pour utiliser une clé importée, reportez-vous à la section Importer la paire de clés d'encapsulation/de désencapsulation. Vérifiez Configurer les propriétés des clés fournies par le client si vous utilisez votre propre clé.

7. Entrez un nom convivial pour l'alias de clé.
8. Cliquez sur **Suivant** pour accéder à l'onglet Création de clé.
9. Cliquez sur **Générer la clé**.
   Une fois la clé générée, le formulaire du module de chiffrement se recharge pour afficher la spécification de chiffrement.
10. Cliquez sur l'onglet **Clés de module** pour afficher les clés.
    Les informations sécurisées pour la clé seront stockées dans l'onglet Clés de module avec le nombre de clés qui existent pour la spécification de chiffrement.



11. Sélectionnez une clé pour effectuer des actions de gestion des clés. Consultez Actions de gestion des clés pour en savoir plus.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une politique d’accès au module

Créez des politiques d’accès au module pour limiter le chiffrement ou le déchiffrement des données.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Pourquoi et quand exécuter cette tâche

Chiffrement au niveau des colonnes (CLE) prend en charge les politiques d’accès au module basées sur les rôles et des options de configuration supplémentaires deviennent disponibles avec la fonctionnalité (CLE_Ent).

- Configurez l’opération cryptographique spécifique dans les politiques d’accès au module pour les modules cryptographiques qui prennent en charge les opérations symétriques. Par exemple, un utilisateur peut être autorisé à chiffrer des données, mais pas à les déchiffrer.
- Définissez une valeur de politique d’accès au module par défaut par module de chiffrement.
- Associez les versions de script où les modifications apportées au script sont suivies et invalidez la politique de script, offrant ainsi une meilleure sécurité pour les politiques d’accès aux modules de type script.

CLE_Ent cette fonctionnalité est disponible avec un abonnement payant. Consultez la rubrique pour connaître les fonctionnalités et options prises en charge disponibles avec chaque offre. Pour plus d'informations, consultez Entreprise de Chiffrement au niveau des colonnes.

Remarque :
Le comportement par défaut des politiques d’accès au module (MAP) est Rejeter pour empêcher tout accès non autorisé, sauf s’il est explicitement déclaré dans les enregistrements MAP.

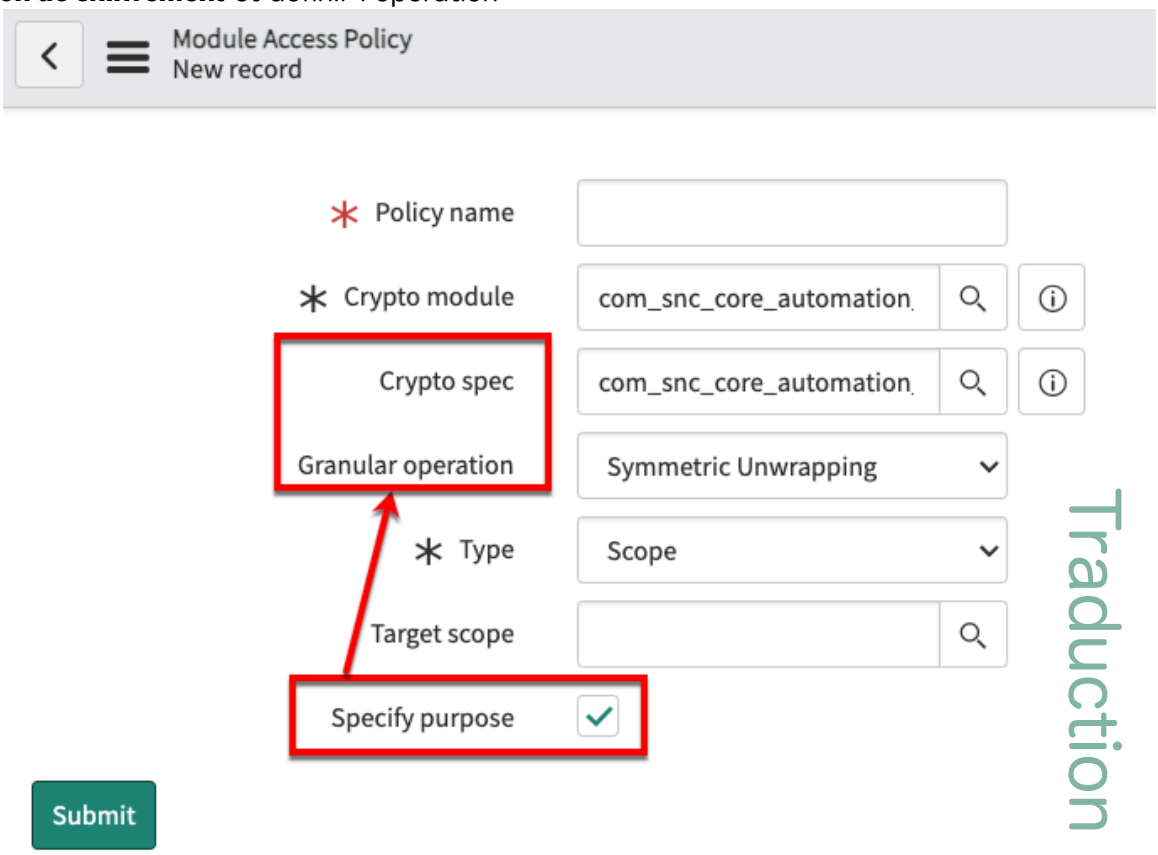
Procédure

1. Accédez à la **Tout** > **Gestion des clés** > **Politiques d'accès au module** > **Tous**.
   Si vous ne créez pas de module cryptographique configuré pour le chiffrement/déchiffrement symétrique des données, une politique d’accès au module générée automatiquement est créée et répertoriée dans la table.
2. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sélectionnez **Spécifier l'objectif** pour choisir une **spécification de chiffrement** et définir l'opération **granulaire**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Avec des spécifications cryptographiques pour le chiffrement/déchiffrement symétrique des données et l'encapsulation/désencapsulation symétrique, le champ **Opération granulaire** est disponible si vous cochez la case **Spécifier l'objectif** .



3. Renseignez le formulaire.

Champs Politiques d'accès au module

Champ	Description
Nom de la politique	Donnez un nom à la politique.
Module de chiffrement	Cliquez sur l'icône de recherche ( ) pour sélectionner un module.
Spécification du chiffrement	Sélectionnez ou créez une nouvelle spécification cryptographique lors de la génération de la politique d'accès au module. Ce champ devient disponible lorsque la case **Spécifier l'objectif** est cochée.
Opération granulaire	Sélectionnez l'objectif de chiffrement pour la spécification de chiffrement. Les valeurs disponibles dépendent du type de spécification de chiffrement sélectionné. Voir pour plus de détails sur les objectifs de cryptographie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Type	○ **Périmètre** : contrôle l'accès par périmètre de l'application. ○ **Utilisateur système** : autorise l'accès des utilisateurs système aux modules de chiffrement. ○ **Script** : contrôler l'accès par script. Voir pour plus d'informations ○ **Rôle** : contrôle l'accès par rôle d'utilisateur. ○ **Échange de ressources** : contrôlez l'accès à l'aide du Resource Exchangefichier . Consultez pour plus d'informations. **Remarque :** Seul le type de rôle est pris en charge avec Chiffrement au niveau des colonnes. Tous les autres types sont disponibles avec Entreprise de Chiffrement au niveau des colonnes.
Périmètre cible	Le champ est visible en tant qu'identificateur pour le type de **champ d'application** . Fait référence à la fonctionnalité de la politique. Sélectionnez les applications dans le menu de recherche. **Remarque :** Le périmètre cible n'est pas pris en charge et ne peut être défini qu'avec Entreprise de Chiffrement au niveau des colonnes
Rôle cible	Le champ est visible en tant qu'identificateur pour le type **de rôle** . Rôle auquel cette politique s'applique.
Table de scripts Script cible	Ces champs s'affichent lorsque vous sélectionnez **Script** comme type. Le champ est visible en tant qu'identificateur pour le type de **script** . Sélectionnez une table à laquelle cette politique s'applique. Document auquel cette politique s'applique. Sélectionnez le **nom** de la table, puis le document connexe de la politique. La première fois qu'un script appelle un module cryptographique, l'accès au module est refusé et le développeur reçoit une erreur. Cette erreur donne au propriétaire du module la possibilité d'accorder ou de refuser l'accès au module.
Échange de ressources : ○ Spécification du chiffrement ○ Type d'approbation ○ Hôte de l'instance cible	Ces options s'affichent lorsque vous sélectionnez le type. Resource Exchange est pris en charge à la fois par KMF et par lorsque le module parent est **column_level_encryption**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Sélectionnez la spécification de chiffrement, ponctuelle ou récurrente, ainsi que l'URL de l'instance cible. Consultez pour plus d'informations.
Emprunt d'identité	Dans les politiques d'accès au module basées sur les rôles, les utilisateurs peuvent accéder à des données chiffrées à l'aide d'une session d'emprunt d'identité. Lorsque des utilisateurs, tels que des administrateurs, empruntent l'identité d'autres utilisateurs, ces politiques d'accès au module permettant l'emprunt d'identité sont appliquées.
Spécifier l'objectif	Sélectionnez cette option pour activer/désactiver le champ de spécification de chiffrement en tant que champ disponible pour la politique.
Actif	Sélectionnez cette option pour activer la politique.
Résultat	Sélectionnez l'une des options suivantes : ○ **StrictReject** rejette l'accès en toutes circonstances. ○ **Le rejet** rejette **l'accèsà ce** module de chiffrement à moins qu'une autre politique ne leur accorde l'accès. ○ **Suivre** pour autoriser l'accès et surveiller l'utilisation du module.

4. Sélectionnez **Soumettre**.

⚠ Avertissement :

Pour les utilisateurs de l'assistance de chiffrement héritée :

Si vous utilisez la version non entreprise de Chiffrement au niveau des colonnes, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

Cette insertion dépasse le nombre de limites des modules publiés de Chiffrement au niveau des colonnes autorisées avec le produit d'abonnement. L'abonnement Entreprise à Chiffrement au niveau des colonnes est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

5. Sélectionnez le nom de politique associé au module de chiffrement que vous souhaitez examiner.
Utilisation de la politique d'accès au module de type de script :

Une politique d'accès au module est générée automatiquement en fonction du paramètre d'accès par défaut lors de l'exécution du script. Le nom du module est précédé d'AutoGen-. Par exemple, le module Module-TestPolicy est répertorié en tant que AutoGen-Module-TestPolicy dans la colonne Nom de la politique.

Le formulaire Politique d'appelant de chiffrement répertorie la politique d'appelant que vous avez sélectionnée. Le champ Champ d'application cible spécifie le champ d'application du script qui tente d'utiliser le module. Voir pour plus d'informations.

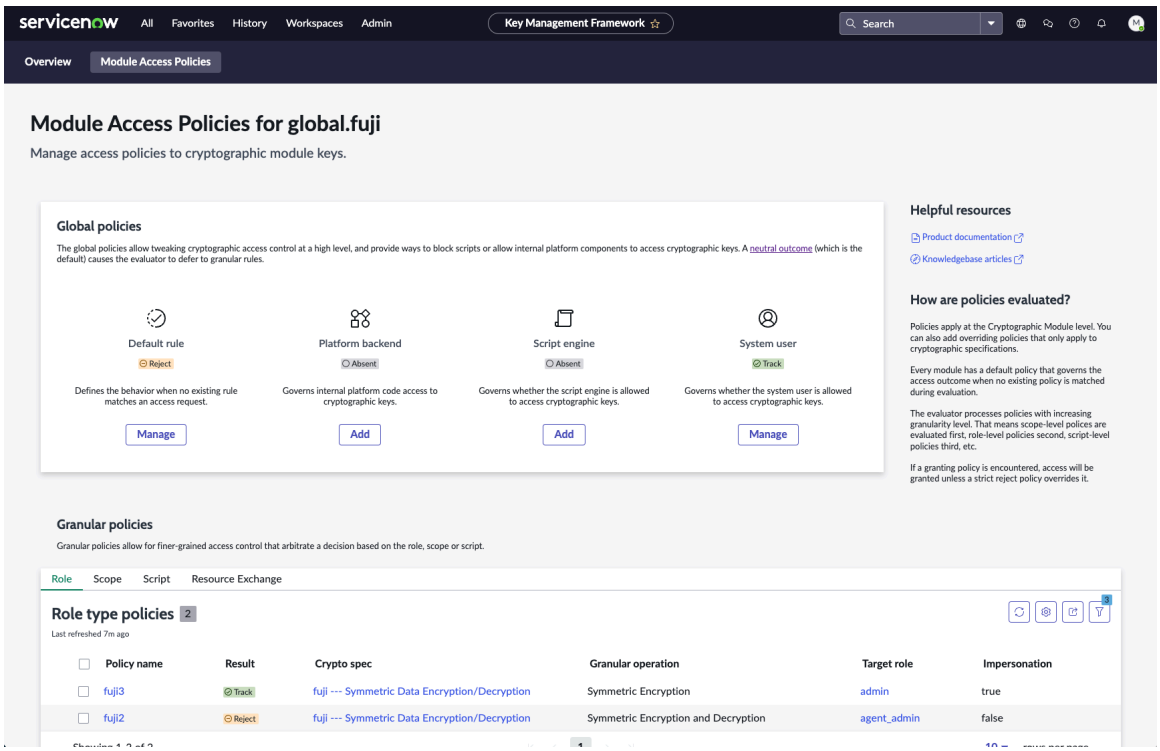
Remarque :
Cinq politiques d'accès au module au maximum sont autorisées avec Chiffrement au niveau des colonnes. Reportez-vous à la section pour les options de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Visualisation de la politique d'accès au module

Utilisez la visualisation de la politique d'accès au module pour afficher toutes les informations pertinentes du module de chiffrement sur une seule page d'interface utilisateur.



Les administrateurs de Key Management Framework et les gestionnaires de chiffrement peuvent utiliser la page de l'interface utilisateur de politique d'accès au module, afficher tous les mécanismes de contrôle d'accès associés à un seul module cryptographique. Utilisez les informations collectées sur cette page d'interface utilisateur pour déterminer rapidement qui a accès aux informations chiffrées sur votre instance.

Les utilisateurs disposant des `sn_kmf.admin` rôles ou `sn_kmf.cryptographic_manager` peuvent accéder à la page d'interface utilisateur de visualisation de la politique d'accès au module en naviguant vers **Tout** > **Gestion des clés** > **Modules de chiffrement** > **Tout**.

Étiquettes des résultats

Les politiques d'accès aux modules contiennent un champ **Résultat** qui détermine s'il convient d'accorder l'accès au module de chiffrement sélectionné. La page d'interface utilisateur affiche une étiquette sur les éléments de la page d'interface utilisateur en fonction de la valeur de ce champ.

Étiquette de l'interface utilisateur	Valeur de champ de résultat	Définition
Track	`Track` ou `Allow`	L'accès est accordé à tous les utilisateurs, y compris les scripts.

Traduction automatique

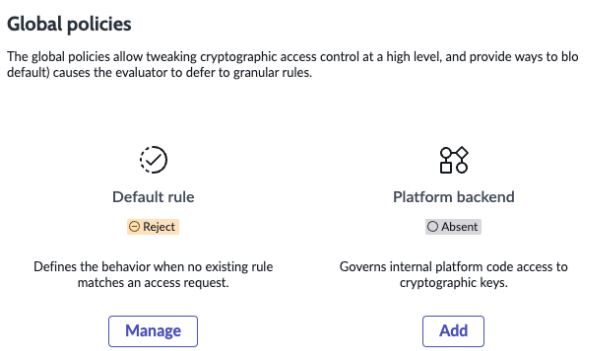
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette de l’interface utilisateur	Valeur de champ de résultat	Définition
Reject	`Reject`	L’accès est refusé sauf si une politique d’accès au module de suivi est trouvée.
StrictReject	`StrictReject`	Accès refusé.
Absent	`N/A`	La politique d’accès au module n’existe pas sur l’instance. L’accès est refusé à tous.

Politiques globales

Utilisez la section **Stratégies globales** pour passer en revue les politiques d’accès au module qui contrôlent l’accès au niveau de la plateforme.

Sélectionnez le bouton **Gérer** sous l’une des politiques pour accéder à cet enregistrement de politique. Si la politique n’existe pas, un bouton **Ajouter** s’affiche sous cette entrée. Sélectionnez le bouton **Ajouter** pour accéder à un nouvel enregistrement de politique dans lequel vous pouvez définir la politique.



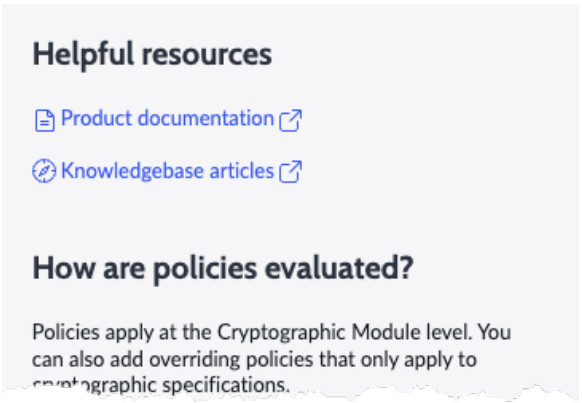
Politique	Définition
Règle par défaut	La politique de règle par défaut définit le comportement lorsqu’aucune règle existante ne correspond à une demande d’accès.
Back-end de la plateforme	La stratégie back-end de la plateforme régit l’accès du code interne de la plateforme aux clés de chiffrement.
Moteur de script	La politique du moteur de script détermine si le moteur de script est autorisé à accéder aux clés de chiffrement.
Utilisateur système	La politique d’utilisateur système détermine si l’utilisateur système est autorisé à accéder aux clés de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ressources utiles

Utilisez la section **Ressources utiles** pour trouver des liens vers la documentation produit, des articles de la base de connaissances pertinents et une brève description de la façon dont les politiques d'accès aux modules sont évaluées sur la plateforme. Pour en savoir plus sur la façon dont les stratégies d'accès aux modules sont évaluées, reportez-vous à Débogueur de politique d'accès au module.

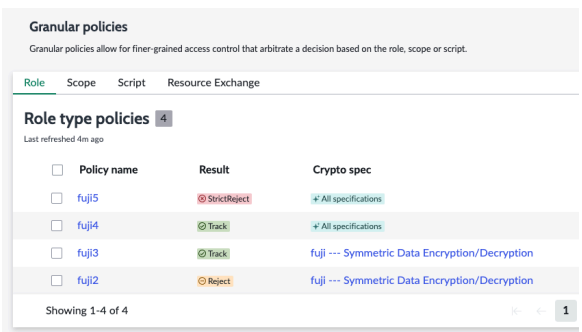


Politiques granulaires

Utilisez la section **Politiques granulaires** pour afficher les listes des politiques d'accès au module, séparées par type de politique. Utilisez les onglets au-dessus de la liste pour sélectionner une catégorie de politique à afficher.

- Rôle
- Périmètre
- Champ d'application et domaine (si Séparation en domaines est actif)
- Script
- Échange de ressources (si le module de chiffrement est un sous-module Password2 ou Chiffrement au niveau des colonnes)
- Identité (si Gestion des secrets Enterprise est active)

Par défaut, chaque liste affiche uniquement les stratégies actives. Utilisez l'icône de filtre pour changer le filtre par défaut de la liste.

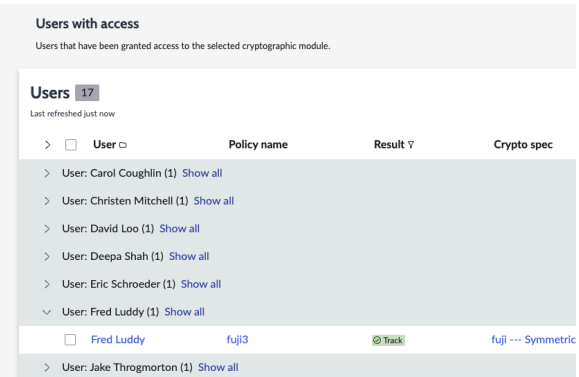


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisateurs ayant accès

Utilisez la section **Utilisateurs avec accès** pour afficher une liste de tous les utilisateurs ayant accès au module de chiffrement sélectionné. La liste est regroupée par utilisateur, car un seul utilisateur peut avoir plusieurs rôles qui accordent l'accès à un module cryptographique.

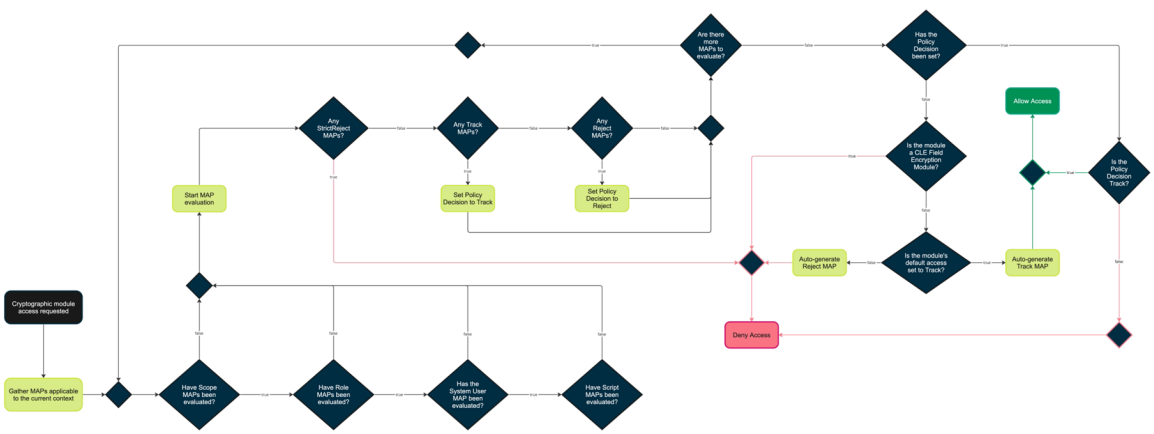


Débogueur de politique d'accès au module

Utilisez le débogueur de politique d'accès au module pour examiner les informations de connexion et comprendre pourquoi vos utilisateurs ont ou n'ont pas accès à un contexte de chiffrement.

Les politiques d'accès aux modules (MAP) définissent des contrôles au niveau de l'instance pour l'accès aux modules de chiffrement. Les appelants (par exemple, un utilisateur ou un script) ont besoin d'un accès explicite afin d'utiliser un module de chiffrement pour le chiffrement et le déchiffrement. Il n'est pas toujours clair quels MAP sont évalués lorsque les appelants tentent d'accéder à un module cryptographique. Utilisez le débogueur pour voir quelles politiques sont évaluées lorsqu'un appelant tente d'accéder à un module de chiffrement et savoir pourquoi l'accès est accordé ou non.

Cet organigramme montre comment votre instance évalue les demandes d'accès à un module cryptographique.



Contrôler l'accès aux journaux de débogage

L'accès aux journaux de débogage d'accès au module est déterminé par rôle. Les utilisateurs disposant des `sn_kmf.admin` rôles et `sn_kmf.cryptographic_manager` ont toujours accès au débogueur. Accordez l'accès à d'autres rôles à l'aide de la `glide.kmf.module_access_policies.debugger.authorized.roles` propriété système. La valeur de cette propriété est une liste séparée par des virgules des rôles qui accèdent aux journaux de débogage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer ou désactiver le débogueur

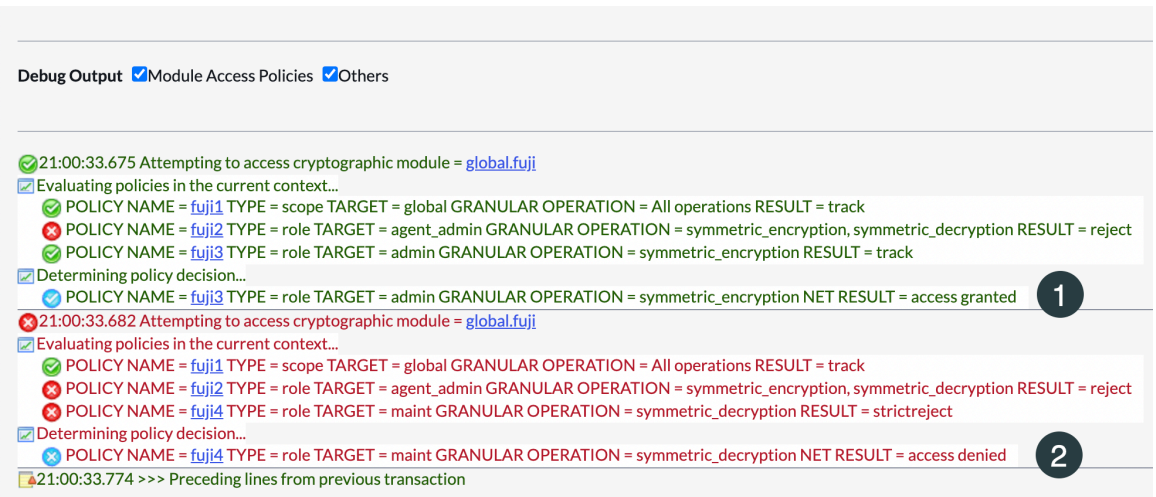
Pour activer les messages de journalisation de débogage pour les politiques d'accès au module, accédez à **Tout** > **Diagnostics** > **Débogage de session** > **Débogage pour les politiques d'accès au module** > **.**

Lorsque vous avez terminé le débogage, vous pouvez désactiver les messages de journalisation en accédant à **Tout** > **Diagnostics** > **Débogage de session** > **Désactiver tout** > **.**

Accéder aux journaux

Après avoir activé le débogage, accédez à une page qui déclenche une évaluation MAP pour afficher les journaux de débogage MAP. Les messages de débogage s'affichent en bas de la page.

Conseil :
Vous pouvez utiliser l'emprunt d'identité pour dépanner l'accès d'autres utilisateurs. Pour en savoir plus sur l'emprunt d'identité, reportez-vous à la section Impersonating users . Pour afficher les journaux de débogage du point de vue d'un autre utilisateur, assurez-vous que le champ **Emprunt d'identité** de vos politiques d'accès `role` au module est défini sur **vrai**.



Dans cet exemple, un appelant appelle deux demandes d'accès au module de chiffrement global.fuji . Un chiffrement symétrique, qui est accordé, et un déchiffrement symétrique, qui a été refusé.

Comprendre les entrées de journal

Les informations de débogage sont structurées à l'aide de ce format.

1. Cette première ligne affiche le module cryptographique qui reçoit la demande d'accès.
2. Les lignes entre la première et la dernière ligne affichent les MAP évaluées dans l'ordre dans lequel elles ont été évaluées et incluent leur nom, leur type, leur cible, leur opération granulaire et leur résultat.
3. La dernière ligne affiche la décision de politique (le cas échéant) et le résultat de l'accès net pour l'appelant (si l'appelant bénéficie ou non de l'accès).

Chaque ligne commence par une icône qui indique le type de message.

Traduction automatique

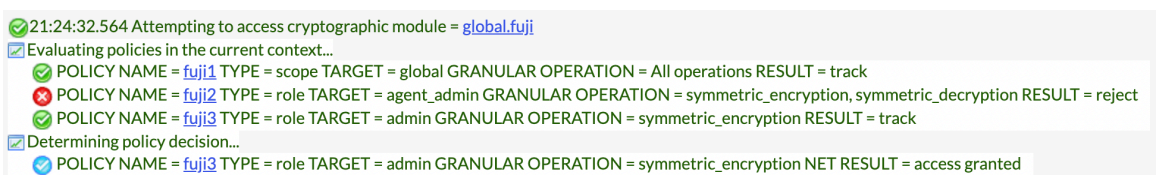
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Icônes de messages

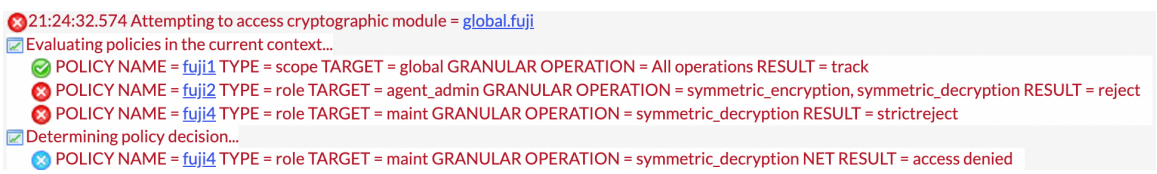
Icône	Type du message
	Message d'information
	La politique d’accès au module accorde l’accès
	La politique d’accès au module refuse l’accès
	L’appelant bénéficie d’un accès
	L’accès est refusé à l’appelant
	Aucune politique d’accès au module à évaluer

Exemples de journal de débogage

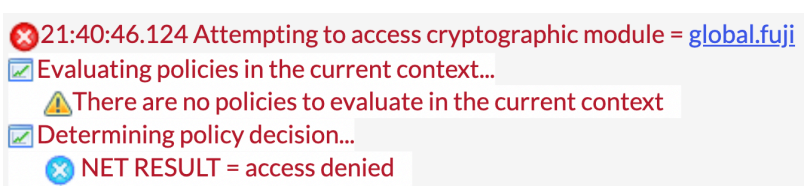
Message d’accès accordé



Message de refus d’accès



Accès refusé (aucune politique d’accès au module à évaluer



Accès refusé (privilèges insuffisants)



Créer une politique de cycle de vie du module de chiffrement

Créez une politique de cycle de vie des modules de chiffrement pour imposer des limites aux modules de chiffrement, telles que la durée de validité de la clé. Créez des politiques pour protéger les modules cryptographiques en limitant leur exposition.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Une politique de cycle de vie de module de chiffrement est une politique au niveau de l’instance. Plus une clé cryptographique est exposée, plus elle est susceptible d’être compromise. Protégez les clés en limitant la durée d’utilisation des clés et les personnes qui peuvent les utiliser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les fonctionnalités suivantes régissent les modules de chiffrement :

- Les politiques d'instance définissent les limites de l'instance. Par exemple, si vous spécifiez dans une stratégie d'instance que la date d'expiration ne doit jamais être postérieure à plus de deux ans après la date d'activation, vous ne pouvez pas utiliser les règles de cycle de vie pour définir une date d'expiration de cinq ans après la date d'activation.

- Les modèles de cycle de vie des instances vous permettent de définir différentes politiques pour différentes clés. Les modèles offrent des règles de cycle de vie par défaut pour les modules de chiffrement afin qu'ils n'aient pas à être recréés pour chaque module. Par exemple, vous pouvez définir des dates d'expiration différentes pour les clés de chiffrement de données symétriques et pour les clés d'encapsulation de clé publique.

- Les règles de cycle de vie affectent directement les clés. Par exemple, si vous spécifiez dans les règles de cycle de vie que la date d'expiration doit être deux ans après la date d'activation, les clés expireront deux ans après la date d'activation.

Procédure

1. Accédez à la **Tout** > **Gestion des clés** > **Politiques de cycle de vie** > **Politiques d'instance**.
2. Sélectionner **Nouveau**.
3. Renseignez le formulaire.

   Champs Politiques de cycle de vie cryptographique

Que faire ensuite

Si vous souhaitez ajouter des exceptions à cette politique de cycle de vie au niveau du module, reportez-vous à la section Créer des exceptions de politique de cycle de vie du module.

Créer des exceptions de politique de cycle de vie du module

Créez une exception de politique de module pour changer la politique de cycle de vie d'une clé au niveau du module d'une instance. La ou les exceptions s'appliquent uniquement à ce module et non à l'instance entière. Par exemple, si l'administrateur a configuré des clés symétriques pour qu'elles soient limitées à un an au niveau de l'instance, une exception peut être faite au niveau du module pour qu'elles soient de deux ans.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager et sn_kmf.admin

Procédure

1. Accédez à la **Tout** > **Gestion des clés** > **Modules de chiffrement Tout**.
2. Sélectionnez le module de chiffrement qui utilisera les exceptions de politique.
3. Dans la table Module de chiffrement, sélectionnez l'icône **Exceptions de politique du module** onglet.
4. Cliquer sur **Nouveau**.
5. Renseignez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs Exceptions de politique de module

Champ	Description
Module de chiffrement	Lecture seule, nom du module sélectionné.
Concerne	La clé spécifiée est renseignée automatiquement.
Type de clé	Sélectionnez le type de clé, car les politiques d'exception sont liées à une clé spécifique. Plusieurs politiques d'exception peuvent être créées par module de chiffrement.
Condition de la politique	Choisissez les conditions admissibles dans la liste déroulante et complétez les critères de contrainte supplémentaires.
Nouveaux critères	Sélectionnez des conditions de politique supplémentaires, au besoin.
Résultat	Sélectionnez **Rejeter** pour rejeter l'utilisation de la clé ou **Suivre** pour autoriser son utilisation lorsque les critères sont remplis.

6. Cliquer sur **Soumettre** à retourner à la table Module de chiffrement.

Actions de gestion des clés

L'une des principales fonctionnalités de KMF est de fournir la possibilité de gérer les clés, telles que la révocation ou la rotation des clés. KMF sécurise correctement les données sensibles avec les matériaux de chiffrement et les opérations de cycle de vie les plus récents.

Le tableau suivant fournit un résumé des principales opérations et actions de gestion du cycle de vie. L'objectif du module de chiffrement est appliqué aux données avec la configuration du module de chiffrement et n'a aucun impact sur les données.

Action de gestion des clés	Description
Générer la clé	Génère une nouvelle clé pour le module de chiffrement donné. Une première clé générée est définie sur `active`.
Faire pivoter la clé	Désactive la clé actuelle et en génère une nouvelle. La nouvelle clé de module est définie sur actuelle (active).
Révoquer la clé	Marque la clé actuelle et l'état du cycle de vie comme révoqués. Le module de chiffrement génère automatiquement une nouvelle clé sur les nouvelles données et définit l'état de la clé sur actif. Révoqué signifie que la clé n'est plus utilisée pour le chiffrement. Cependant, il peut toujours être utilisé pour le décryptage. Vous ne pouvez pas détruire une clé.
Suspendre la clé	Marque la clé actuelle comme suspendue. Reprenez manuellement la clé suspendue ou révoquez la clé suspendue pour générer une nouvelle clé de module avant d'utiliser à nouveau le module cryptographique.
Reprendre la clé	Marque une clé suspendue comme clé active.
Renouveler la clé	Prolonge la durée de vie de la clé actuelle. Le bouton **Renouveler** est disponible dans les cas suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action de gestion des clés	Description
	• Le rôle de gestionnaire de chiffrement vous est affecté. • L'état du cycle de vie est marqué soit **Actif, soit Renouvelé**. • Une date d'expiration est définie dans la définition du cycle de vie du module.

Afficher et gérer les clés

Examinez l'état de n'importe quelle clé pour déterminer d'autres actions clés, telles que le renouvellement, la rotation, la suspension, la désactivation ou la destruction d'une clé actuelle.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tout** > **Gestion des clés** > **Modules de chiffrement** > **Tout**.
2. Sélectionnez un module cryptographique.

   Le formulaire du module de chiffrement <module-name> s'affiche.
3. Dans l'onglet Clés de module, sélectionnez l'alias de clé pour examiner l'état de la clé sur le formulaire de cycle de vie <nom de clé>.
4. Passez en revue le formulaire, car tous les champs sont en lecture seule.

Cycle de vie cryptographique Champs clés

Champ	Description
Date de création	Affiche la date à laquelle la clé a été générée.
Date d'activation	Affiche la date à laquelle la clé a été activée.
Dernière date de renouvellement	Affiche la date du dernier renouvellement de la clé.
Date de la dernière rotation	Affiche la date de la dernière rotation de la clé.
Date de désactivation	Affiche la date à laquelle la clé a été désactivée.
Date de destruction	Affiche la date à laquelle la clé a été détruite.
État du cycle de vie de la clé	Affiche l'état clé du cycle de vie.
Prochaine date d'activation	Affiche la date future d'activation de clé.
Prochaine date de renouvellement	Affiche la date de renouvellement de clé future.
Prochaine date de rotation	Affiche la date future pour la rotation de clés.
Prochaine date de destruction	Affiche la date future à laquelle la clé est détruite.
Date d'expiration	Affiche la date d'expiration de la clé.

5. Pour effectuer une action sur la clé, sélectionnez l'une des options suivantes pour qu'elle prenne effet immédiatement :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Révoquer la clé**: sélectionnez cette option pour désactiver la clé et générer une nouvelle clé. Entrez la raison pour laquelle vous révoquez la clé.
- **Faire pivoter la clé**: sélectionnez cette option pour désactiver la clé actuelle et générer une nouvelle clé à sa place. La nouvelle clé est répertoriée dans la table Clé de module et le numéro de version de clé est incrémenté de 1. Voir pour plus de détails.
- **Suspendre la clé**: sélectionnez cette option pour désactiver la clé actuelle.
- **Reprendre la clé** : sélectionnez cette option pour marquer une clé suspendue comme clé active. Cette option n'est disponible qu'après la suspension de la clé active.

Faire pivoter les clés

Pour plus de sécurité, vous pouvez alterner vos clés cryptographiques selon un calendrier prédéterminé. La rotation de clé consiste à mettre hors service une clé de chiffrement et à remplacer cette ancienne clé par la génération d'une nouvelle clé cryptographique.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

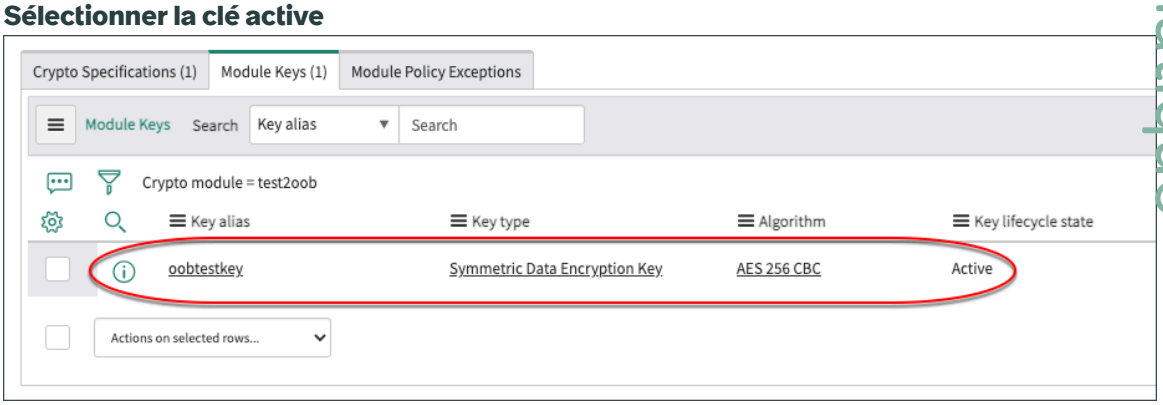
Pourquoi et quand exécuter cette tâche

Les modules de chiffrement, contrairement aux contextes de chiffrement, prennent en charge une nouvelle saisie des enregistrements pour un nouveau chiffrement avec une nouvelle clé. Ce qui suit montre comment effectuer manuellement une opération de rotation de clé sur un module cryptographique.

Procédure

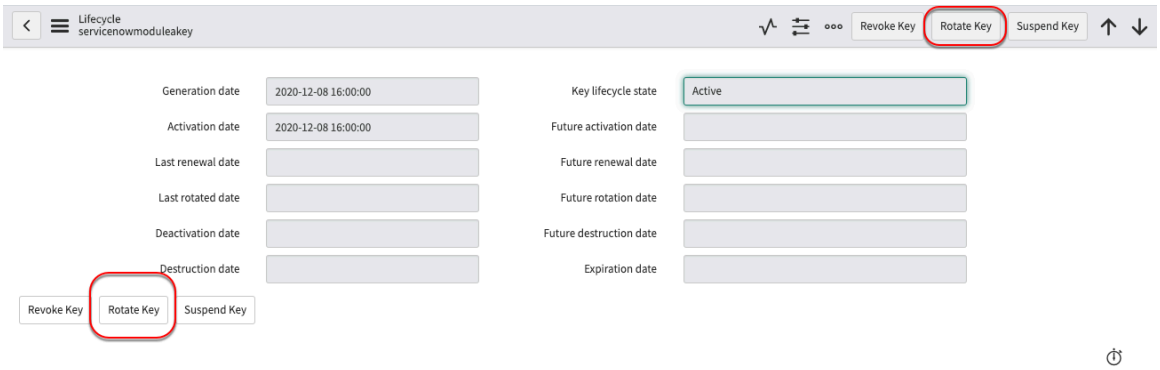
1. Accédez à la **Gestion des clés** > **Modules de chiffrement** > **Tout**.
2. Sélectionnez le module de chiffrement pour la rotation de clé.
3. Dans l'onglet **Clés de module** , sélectionnez la touche Active.

Sélectionner la clé active

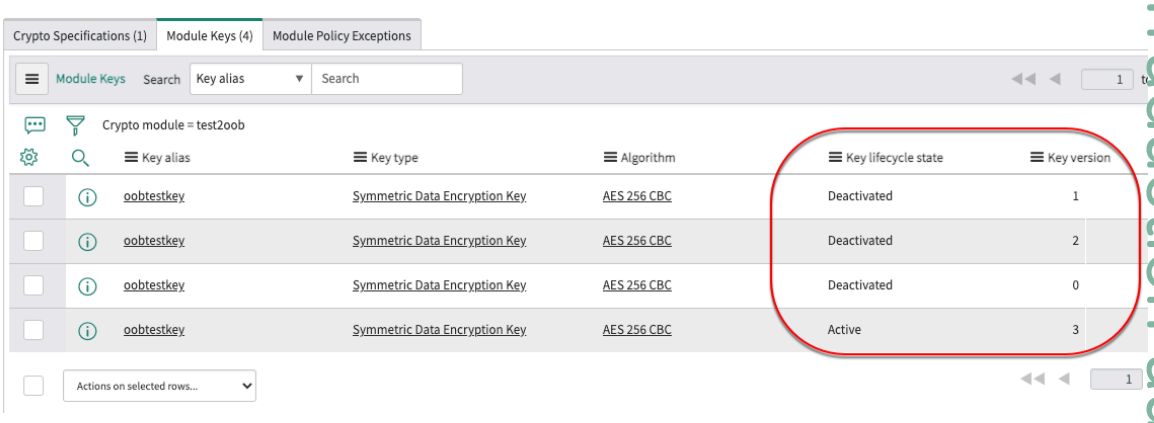


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez **Faire pivoter la clé**.
   L'état du cycle de vie clé devient « Désactivé ». Les champs **Dernière date de rotation**, **Date de désactivation** et **Version de clé** sont mis à jour.
5. Retourner à **Module de chiffrement** > **Clés de module**.



Il y a une clé de module supplémentaire répertoriée dans la table. La touche nouvellement tournée devient « Active » et la dernière touche est « Désactivée ».

Importer une clé à partir d'un service Web

Chargez en toute sécurité une clé client externe sur votre instance à l'aide de l'option Importer une clé à partir d'un service Web (par exemple, l'API REST de clé). Les clés publiques symétriques et asymétriques peuvent être importées dans un module cryptographique ciblé KMF .

La clé à importer (la clé cible) doit être chiffrée avec une clé d'encapsulation avant d'être téléchargée dans le module de chiffrement cible de l'instance. Cette clé d'encapsulation est le composant public d'une paire de clés publique/privée, qui doit être présente sur l'instance. La clé est une condition préalable avant que la clé cible encapsulée puisse être chargée via l'importation à partir des services Web.

Ces deux procédures distinctes (importation de la paire de clés encapsulée et importation de la clé cible encapsulée à partir d'un service Web) sont détaillées dans la documentation suivante. Cette paire de clés doit être générée et chargée pour être disponible dans le module de chiffrement d'importation de clé interne de l'instance.

Remarque :
Cet exemple utilise OpenSSL pour la génération de clés et de certificats, et l'outil de test d'API Postman pour afficher l'utilisation de l'API REST. Remplacez d'autres outils comparables en fonction des besoins de votre entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importer la paire de clés d'encapsulation/de désencapsulation

Configurez Key Management Framework les paramètres d'importation avant d'importer une clé.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Cet exemple utilise OpenSSL pour la génération de clés et de certificats. Remplacez d'autres outils comparables en fonction des besoins de votre entreprise.

Procédure

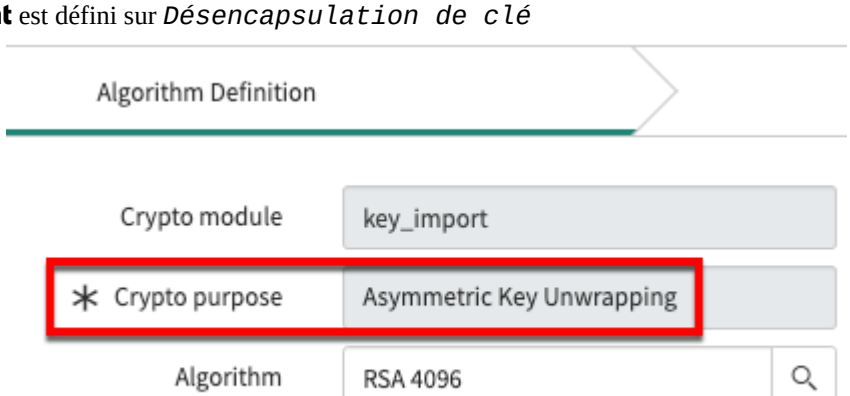
1. Dans votre environnement local, utilisez le terminal pour créer un certificat.
   Par exemple : `openssl req -x509 -sha256 -nodes -days 365 -newkey rsa :4096 -keyout wrapping_private.key -out wrapping_public.crt`

   Ce certificat est un composant public qui contient une clé. Le certificat est utilisé pour encapsuler une clé symétrique AES.

2. Dans votre environnement local, utilisez le terminal pour créer un magasin de clés contenant un certificat public (avec la clé d'encapsulation) et une clé de désencapsulation privée.
   Par exemple :`openssl pkcs12 -export -in wrapping_public.crt -inkey wrapping_private.key -name « wrapping_key_alias » -out wrapping_keystore.p12`

3. Sur votre instance, accédez à **Tout** > **Gestion des clés** > **Paramètres d'importation** > **Paramètres d'importation de clé**.

4. Dans la section Définition de l'algorithme, vérifiez que **l'objectif de chiffrement** est défini sur *`Désencapsulation de clé asymétrique`*.



5. Sélectionnez un algorithme approprié qui s'aligne sur le matériau de clé asymétrique pour le magasin de clés importé.
   Consultez Objectif cryptographique, algorithmes et informations clés pour plus d'informations.

6. Sélectionnez **Suivant**.

7. Dans la section **Définition du cycle de vie** , sélectionnez **Suivant** pour continuer.

8. Dans la section Origine de la **clé** , sélectionnez **Importer à partir de PKCS12** ou **Importer à partir de BCFKS** dans le champ **Origine** .

   Remarque :
   Si vous utilisez l'exemple de magasin de clés de l'étape 1, sélectionnez **Importer à partir de PKCS12**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Entrez un **alias de clé** pour identifier la clé.
   Cet alias doit correspondre à l'alias de clé (ou « nom convivial ») spécifié lors de la génération du certificat ou du magasin de clés à charger. En reprenant l'exemple ci-dessus, ce serait `wrapping_key_alias`.
10. Sélectionnez **Suivant**.
    La section **Création de clé** inclut un lien **Importer la clé** , qui affiche une boîte de dialogue permettant de charger le magasin de clés. En poursuivant l'exemple, il s'agirait de `wrapping_keystore.p12`.

Importer une clé encapsulée à partir d'un service Web

Chargez votre clé encapsulée dans un module de chiffrement à l'aide de la fonctionnalité d'importation de clé à partir du service Web. L'exemple utilise une clé symétrique. Des étapes similaires peuvent être utilisées pour importer une clé asymétrique.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager (configuration du module), sn_kmf.cryptographic_operator (authentification de base de l'opération REST)

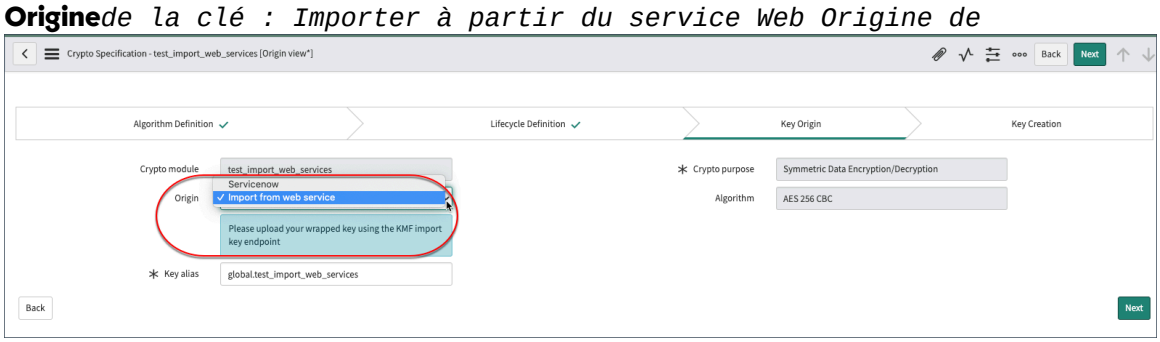
Pourquoi et quand exécuter cette tâche

KMF L'accès au point de terminaison de la clé d'importation est requis pour terminer le processus d'importation de la clé.

Cet exemple utilise OpenSSL pour générer des clés et des certificats. Vous pouvez remplacer d'autres outils comparables en fonction de vos besoins.

Procédure

1. À l'aide du terminal de votre appareil local, encapsulez votre clé symétrique à l'aide de la clé d'encapsulation de clé publique du module d'importation de clés.
   Par exemple : `openssl pkeyutl -encrypt -pubin -inkey public_wrapping_key.pem -in symmetric_key.bin -pkeyopt rsa_padding_mode :oaep -pkeyopt rsa_oaep_md :sha256 -out wrapped_symmetric_key.txt`
   Cet exemple crée un fichier de clé encapsulé nommé `wrapped_symmetric_key.txt`.
2. Créez un module cryptographique à lier à l'API.
   Voir ou pour plus d'informations.
3. Ajoutez une spécification cryptographique avec les sélections suivantes.
   - **Objectif du chiffrement** : *`Cryptage/déchiffrement symétrique des données`*.
   - **Origine***`de la clé : Importer à partir du service Web Origine de`*



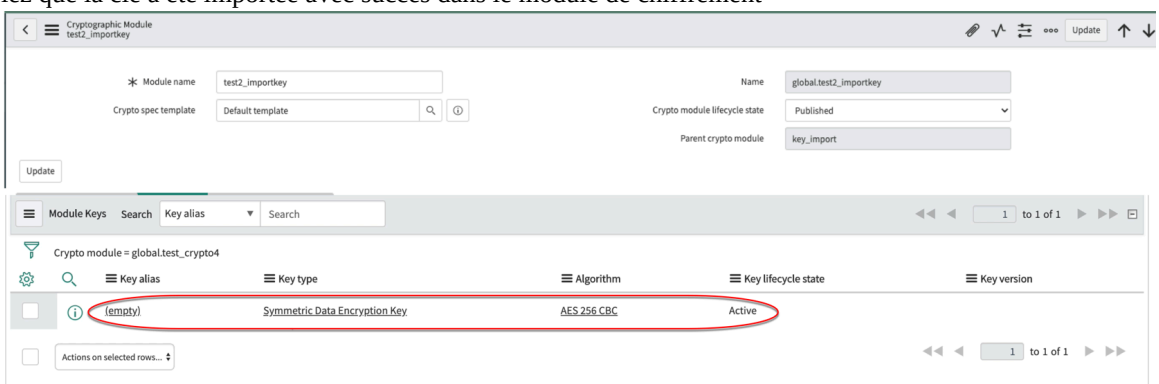
   Voir ou pour plus d'informations.
4. Exécutez une *`demande HTTP POST`* à importer à partir d'un point de terminaison REST de service Web.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’importation réussie de la clé publique entraîne l’envoi d’un message de réponse HTTP avec `l’état 200`.

5. Vérifiez que la clé a été importée avec succès dans le module de chiffrement ciblé.



Intégrité de Key Management Framework

Accédez à des informations sur l’état de santé sur demande pour le Key Management Framework. Les erreurs d’avertissement et de dysfonctionnement sont accompagnées d’un message détaillé.

Avant de commencer

Rôle requis : auditeur sn_kmf_cryptographic ou sn_kmf_admin ou sn_kmf_cryptographic_manager

Pourquoi et quand exécuter cette tâche

Chaque composant de l’est Key Management Framework décrit et signale les états et les couleurs suivants :

- Vert/Opérationnel : le composant est opérationnel, aucune erreur à signaler.
- Gris/Désactivé : le composant est inactif, par conséquent aucune vérification de l’intégrité n’est effectuée.
- Jaune/Dégradé : Avertissement, le composant fonctionne, mais des retards/problèmes transitoires sont susceptibles de se produire.
- Rouge/Dysfonctionnement : une erreur fatale empêche le composant de fonctionner, ce qui est susceptible de provoquer des pannes partielles.

Les composants peuvent inclure des sous-composants avec des rapports individuels et leur propre état d’intégrité a un impact sur le parent comme suit :

- Si tous les sous-composants sont inactifs, le parent s’affiche comme inactif. Les sous-composants inactifs n’ont pas d’impact sur la santé de leurs parents.
- Si un ou plusieurs sous-composants sont dégradés ou fonctionnent mal, l’intégrité du parent apparaît comme dégradée.
- Si tous les sous-composants sont signalés comme défectueux, le parent signale également comme défectueux.

Pour plus d’informations sur les sous-composants, reportez-vous à la section Clés de niveau instance dans Key Management Framework.

Remarque :
Les contrôles d’intégrité s’exécutent toutes les 15 secondes. Actualisez la page d’intégrité pour réexécuter le rapport.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Gestion des clés** > > **Diagnostics**.
2. Passez en revue les informations suivantes sur l'état de santé :

Informations de diagnostic

Catégorie	Détails
Clé sécurisée	Vérifie si le chiffrement est en cours de tentative.
Magasin de clés de fichier	Vérifie si une tentative d'extraction de clé racine d'instance (IRK) se produit. **Remarque :** Le magasin de clés de fichier est une alternative hors connexion à Key Secure utilisée pour les instances sur site et les instances de développeur.
GlideEncrypter	Vérifie si un module de chiffrement au niveau de l'instance GlideEncrypter, une spécification et une clé sont présents. **Remarque :** GlideEncrypter est un composant scriptable qui permet le chiffrement transparent des champs et d'autres utilisations de Password2 chiffrement héritées via le Key Management Frameworkfichier .
Clé de chiffrement de clé d'instance (IKEK)	Vérifie si la clé peut être extraite du magasin de clés de fichier ou de KeySecure.
Clé HMAC d'instance	Vérifie si la clé peut être extraite du magasin de clés de fichier ou de KeySecure.
PKI du coffre-fort	Vérifie la connectivité du coffre-fort pour vérifier si la clé de chiffrement asymétrique d'instance (IAEK) et la clé de signature d'instance (ISK) sont utilisables et peuvent être extraites du coffre-fort.
EJBCA PKI	Vérifie la connectivité LDAP pour vérifier si IAEK et ISK sont utilisables et peuvent être extraits du cache et LDAP.
PKI d'instance	Vérifie la présence d'une clé dans le magasin de clés de fichier et KeySecure, ainsi que si le certificat est présent et correspond à la clé symétrique. **Remarque :** L'instance PKI n'est disponible que sur les instances d'un centre de ServiceNow données.

Pour obtenir de l'aide sur le dépannage, contactez Service et assistance client.

Préparer votre instance pour la dépréciation de GlideEncrypter

Utilisez un script d'analyse d'instance pour rechercher et supprimer les appels d'API GlideEncrypter sur votre instance. La suppression de ces appels est une étape nécessaire pour déconseiller le chiffrement 3DES sur votre instance.

Avant de commencer

Rôle requis : administrateur

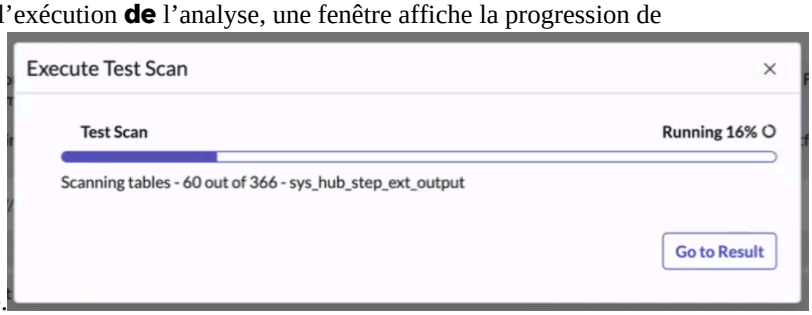
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'obsolescence de l'API GlideEncrypter est prévue à partir de la version Zurich de ServiceNow. La suppression des appels GlideEncrypter de votre script est également une étape nécessaire avant de déprécier le chiffrement 3DES sur votre instance.

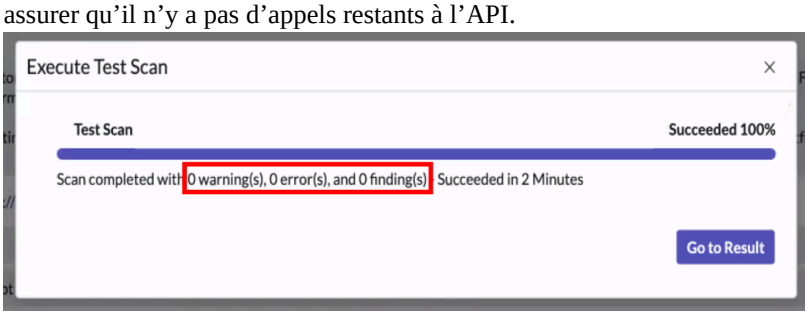
Procédure

1. Accédez à la **Tout** > **Instance Scan** > **Suites**.
2. Dans la liste **Suites** , sélectionnez **GlideEncrypter pour identifier les enregistrements avec des utilisations GlideEncrypter**
3. Dans l'enregistrement **Suites** , sélectionnez **GlideEncrypter pour identifier les enregistrements avec des utilisations GlideEncrypter** à partir de la liste connexe **Vérifications** .
   La **vérification du type de colonne** s'affiche. Cet enregistrement contient une description de la vérification, ainsi que des informations et des liens sur la façon de mettre à jour les enregistrements trouvés par la vérification.
4. Dans l'enregistrement **Vérification du type de colonne** , sélectionnez **Tester la vérification** pour exécuter l'analyse.
   Pendant l'exécution **de** l'analyse, une fenêtre affiche la progression de l'analyse.



Remarque :
Cette analyse vérifie uniquement les enregistrements qui ont été créés ou modifiés par le client.

5. Lorsque l'analyse est terminée, sélectionnez **Accéder au résultat** pour afficher l'enregistrement **du résultat de l'analyse** .
   Dans l'enregistrement **des résultats de l'analyse** , la liste **des conclusions de l'analyse** affiche une liste des enregistrements sur votre instance qui utilisent l'API **GlideEncrypter** .
6. Sélectionnez le champ **Nombre** de la liste **Conclusions de l'analyse** pour accéder à un enregistrement.
7. Modifiez tous les scripts dans l'enregistrement qui utilisent l'API **GlideEncrypter** .
   Pour plus d'informations sur les alternatives à **GlideEncrypter**, consultez Alternatives aux API GlideEncrypter déconseillées .
8. Après avoir supprimé les appels **GlideEncrypter** de vos scripts, exécutez à nouveau l'analyse pour vous assurer qu'il n'y a pas d'appels restants à l'API.



Que faire ensuite

Déconseiller l'utilisation de 3DES par GlideEncrypter pour les champs password2

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déconseiller l'utilisation de 3DES par GlideEncrypter pour les champs password2

Déconseiller l'utilisation de la norme de chiffrement 3DES par GlideEncrypter sur votre instance. Assurez-vous que votre instance utilise la norme AES (Advanced Encryption Standard) plus sécurisée exclusivement pour le chiffrement et le déchiffrement de vos données Password2.

À partir de Rome, les données password2 sont protégées à l'aide de , Key Management Frameworkqui utilise l'algorithme AES (Advanced Encryption Standard) plus moderne. Toutefois, certaines configurations et secours dans la logique password2 peuvent toujours utiliser l'algorithme 3DES pour le chiffrement et le déchiffrement.

Dans cette Vancouver version, les administrateurs peuvent choisir de déconseiller entièrement l'algorithme 3DES. Une fois cette modification effectuée, votre instance utilise le chiffrement AES exclusivement pour toutes les tâches de chiffrement et de déchiffrement relatives aux données password2. Ce changement offre une meilleure sécurité d'instance que le chiffrement 3DES et est nécessaire pour rester conforme au NIST.

Considérations avant l'obsolescence

Transfert des données password2 entre les instances

Lors du transfert de textes chiffrés password2 vers d'autres instances, vous devez vous assurer que cette option KMF Key Exchange est activée entre les instances source et cible. Cette configuration garantit que les clés utilisées pour chiffrer les textes password2 sont disponibles sur les deux instances pour déchiffrer les textes chiffrés password2. Avant de déconseiller 3DES, prenez en compte les cas d'utilisation suivants qui peuvent avoir un impact sur les données password2 entre les instances.

- Si vous avez des applications sur votre instance qui utilisent des données password2, assurez-vous qu'elles KMF Resource Exchange sont installées sur cette instance. KMF Resource Exchange Garantit que les clés de niveau instance utilisées pour chiffrer les données password2 sur l'instance source sont disponibles sur les instances cibles pour le déchiffrement. Pour plus d'informations, consultez Échange de ressources du cadre de travail de gestion des clés.
- Si vous prévoyez d'exporter des données password2 via XML ou des sources de données, assurez-vous que l'instance cible est KMF Key Exchange activée. Cette configuration garantit que les clés au niveau de l'instance utilisées pour chiffrer les données password2 sur l'instance source sont disponibles sur les instances cibles pour le déchiffrement. Pour en savoir plus sur cette configuration, reportez-vous à la section Échange de clés du cadre de travail de gestion de clés.

> **Important :**
> Les exemples ci-dessus sont des scénarios plus courants, mais si vous utilisez d'autres moyens pour transférer du texte chiffré password2 entre des instances, vous devez configurer KMF Resource Exchange pour vous assurer que l'instance cible peut déchiffrer les données password2.

Passage à une version antérieure d'une instance après l'obsolescence de 3DES

Ce qui suit s'applique uniquement aux instances dont les champs password2 ont des longueurs d'entrée supérieures à 125 caractères et dont vous avez déjà déconseillé le chiffrement 3DES.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour passer à une version antérieure à une instance afin de la publier avant le clonage d'instance Vancouver , procédez comme suit avant de lancer le clone.

1. Vérifiez si la conservation des données est configurée pour préserver les données du champ password2.
2. Si c'est le cas, contactez ServiceNow le support technique avant de demander un clone. Dans le champ **Motif** , utilisez « Cloner les conditions préalables à la prise en charge de password2 ».

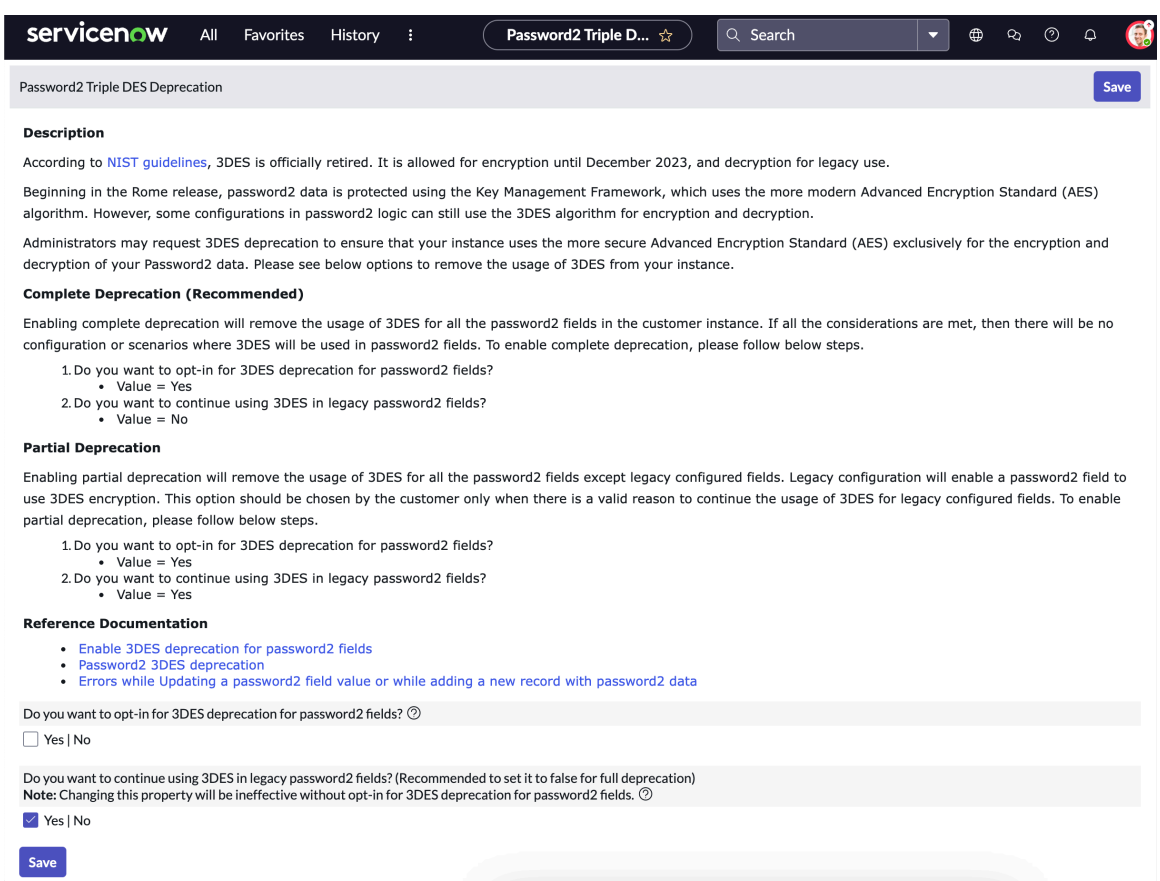
Champs password2 hérités

Votre instance utilise le chiffrement 3DES pour convertir les données password2 en données (pré-Rome)password2 héritées. Après l'obsolescence du chiffrement 3DES, cette option n'est plus disponible. Si vous avez toujours besoin de cette fonctionnalité, demandez l'obsolescence partielle (voir les détails dans la section suivante).

Comment déconseiller 3DES

Une fois que vous avez examiné les cas d'utilisation précédents, activez l'obsolescence partielle ou totale en fonction de vos besoins. Pour l'une ou l'autre option, vous pouvez accéder au formulaire pour contrôler l'obsolescence en accédant à **Tout** > **Sécurité de système** > **Conformité de la sécurité** > **Obsolescence de Triple DES Password2**.

Important :
Vous devez vous élever au rang d'administrateur de sécurité pour voir le module **de conformité de sécurité** et effectuer ces étapes. Pour obtenir plus de détails sur ce processus, voir Élever à un rôle privilégié.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le formulaire de **dépréciation de Triple DES de Password2** contient des informations sur le processus d'obsolescence complète et partielle de 3DES. Sélectionnez les options d'obsolescence totale ou **partielle, puis sélectionnez Enregistrer**.

Dépréciation complète

L'activation de l'obsolescence complète supprime l'utilisation de 3DES pour tous les champs password2 dans votre instance. Si toutes les conditions préalables sont remplies, il n'y a pas de configuration ou de scénarios où 3DES est utilisé dans les champs password2.

Pour activer l'obsolescence complète :

- Sélectionnez **Voulez-vous accepter l'obsolescence 3DES pour les champs password2 ?**
- **Voulez-vous continuer à utiliser 3DES dans les champs password2 hérités ?**

Dépréciation partielle

L'activation de l'obsolescence partielle supprime l'utilisation de 3DES pour tous les champs password2, à l'exception des champs configurés hérités. Les champs password2 de configuration hérités continuent d'utiliser le chiffrement 3DES. Sélectionnez cette option uniquement si vous devez continuer à utiliser 3DES pour les champs configurés hérités.

Pour activer l'obsolescence partielle :

- Sélectionnez **Voulez-vous accepter l'obsolescence 3DES pour les champs password2 ?**
- Sélectionnez **Voulez-vous continuer à utiliser 3DES dans les champs password2 hérités ?**

Après l'obsolescence de GlideEncrypter

Une fois le processus de dépréciation terminé, les informations suivantes s'appliquent à votre instance.

- Les champs password2 prennent toujours en charge le déchiffrement (mais pas le chiffrement) des données chiffrées 3DES.
- Les données chiffrées 3DES existantes dans les champs password2 restent telles quelles jusqu'à ce que la valeur du champ soit mise à jour par un utilisateur ou un workflow.
- Toute mise à jour de la valeur d'un champ password2 supprime le texte chiffré 3DES et le remplace par le texte chiffré à KMF l'aide d'AES.
- Dans certains cas, votre instance peut afficher une erreur lors de l'enregistrement des données de mot de passe :

  Action abandonnée : la valeur du mot de passe ne peut pas être enregistrée en raison d'un problème technique. Veuillez consulter KB1296997 pour obtenir de l'aide.

  Si cette erreur s'affiche, reportez-vous aux informations d'assistance de l'article KB1296997 de la base de connaissances.

Échange de ressources du cadre de travail de gestion des clés

ServiceNow® Resource Exchange est une KMF fonctionnalité qui vous permet d'échanger des ressources entre les instances de manière sécurisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Terminologie

Lorsque vous utilisez le Resource Exchange, reportez-vous à la terminologie suivante :

Resource Exchange Terminologie

Nom	Description
Resource Exchange	Processus d'échange de ressources entre les instances
Key Exchange (KE)	Processus d'échange de clés sur des instances.
Instance de la source de clé (source de clé)	L'instance qui possède les clés.
Instance cible clé (cible clé)	L'instance qui demande les clés.

Vue d'ensemble

Resource Exchange utilise les API cryptographiques pour assurer la confidentialité, l'intégrité, l'authentification KMF et la non-répudiation. Actuellement, Resource Exchange prend en charge la Key Exchange fonctionnalité. Consultez Échange de clés du cadre de travail de gestion de clés pour plus d'informations.

Échange de clés du cadre de travail de gestion de clés

KMF Key Exchange est une fonction de sous-ensemble de KMF Resource Exchange. Key Exchange Transfère en toute sécurité des données chiffrées sur plusieurs instances.

Vue d'ensemble de Key Exchange

Key Exchange Transfère en toute sécurité les clés entre les instances.

KMF Key Exchange fournit aux clients un moyen sécurisé d'échanger KMF des clés entre les instances. Un cas d'utilisation de l'application est le processus de clonage de données. Avec Key Exchange, les clés de module de chiffrement sont copiées lors du clonage de données des KMF composants. Les modules cryptographiques, les spécifications clés des modules et les politiques d'accès aux modules sont inclus dans le processus de clonage. Le transfert des clés n'est pas inclus.

Utiliser Key Exchange

Les administrateurs qui utilisent KMF le chiffrement au niveau des colonnes peuvent Key Exchange utiliser pour cloner les clés entre les instances de production lors de l'exécution du clonage de données. Dans le clonage de données, l'administrateur/ KMF gestionnaire cryptographique peut effectuer les opérations suivantes :

- Échangez toutes les clés vers les autres instances.
- Échangez des clés particulières une fois ou périodiquement à l'autre instance.
- Envoyer des demandes à la demande de l'instance cible à l'instance source clé.
- Échangez les clés de la source vers la cible pour une nouvelle saisie du texte chiffré.
  - Gérez le délai d'expiration de la demande avec la possibilité de supprimer des clés ou de rejeter la demande d'échange de clé si la demande a expiré.
  - Une fois la demande terminée et la clé importée, la clé utilisée sera définie comme expirée et horodatée.
  - Retapez le texte chiffré sur l'instance cible qui a été chiffrée avec les clés de la source.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modes pris en charge

Key Exchange prend en charge plusieurs modes au niveau de la spécification de chiffrement du module de chiffrement :

Mode	Description
Automatique (aucune configuration, comportement par défaut)	Toutes les clés sont envoyées automatiquement pendant le processus de clonage des données sans configuration supplémentaire.
Configurable (configuration unique)	L'administrateur configure les clés à envoyer pendant le processus de clonage des données.
Manuel (personne dans la boucle)	L'administrateur envoie une demande sur demande sur l'instance cible à la source. La demande doit être approuvée par un administrateur sur l'instance source de clé.
Renouvellement de saisie (demande automatisée)	L'administrateur sélectionne l'option de renouvellement de saisie pendant le processus de configuration du clonage.

Configurer l'échange de clés

Key Management Framework (KMF) génère des demandes automatiques d'échange de clés pour les modules de chiffrement pris en charge lors de la nouvelle installation ou de la mise à niveau de l'instance. Gère la clé de chiffrement des données localement pour l'instance.

Avant de commencer

Un module de chiffrement avec une clé doit être créé dans les instances cible et source avant d'utiliser Key Exchange.

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Key Exchange Les demandes sont lancées à partir de l'instance cible.

L'échange de clés automatique est actif par défaut lors du clonage d'une instance, où la propriété est clonée vers l'instance cible. En plus de KMF, configurez les propriétés système pour gérer la façon dont les clés sont traitées pendant un clone d'instance :

- **Désactiver l'échange automatique de clés :** Définissez la propriété sur **false** pour les `glide_encryption.auto_key_exchange.enabled` demandes de clone récurrentes.
- **Envoyer des demandes d'échange de clé automatique** : définissez cette propriété sur **vrai**.

> **Important :**
> La propriété système de base est définie sur **vrai** par défaut, ce qui signifie que l'échange de clés automatique est activé lors du clonage d'une instance. Cette valeur doit être définie sur **faux** si vous utilisez la Retaper le texte chiffré avec l'échange de clés fonctionnalité d'échange de clés récurrente ou la fonctionnalité Récurrente. Consultez la rubrique Procédure pas à pas récurrente de l'échange de clés pour en savoir plus.

Procédure

1. Accédez à la **Tout** > **Gestion des clés** > **Demandes d'échange de ressources** > **Nouveau**.
2. Renseignez les champs du formulaire.

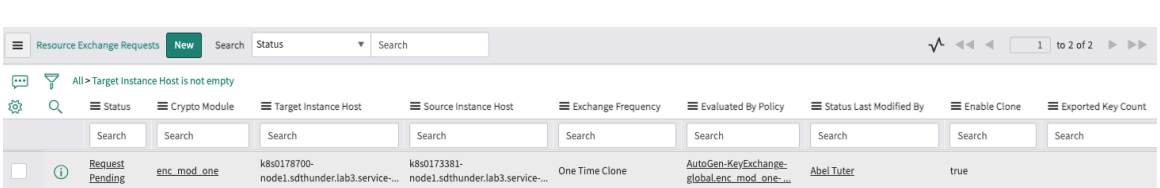
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Resource Exchange Champs du formulaire de demande

Nom	Description
Fréquence d'échange	○ **Adhoc** : envoie des demandes de l'instance cible clé à l'instance source. Entrez le sys_id d'instance et les informations d'hôte pour la source. Non pris en charge avec le renouvellement de clé de l'échange de clés. ○ **Clone unique** : échange unique des clés des spécifications de chiffrement source vers l'instance cible. ○ **Clone récurrent** : échangez les clés des spécifications de chiffrement source sélectionnées vers l'instance cible sur un clone récurrent défini.
<Source or Target> sys_id d'instance	○ **Adhoc** : saisissez le sys_id de l'instance source à laquelle vous souhaitez demander les clés. ○ **Clone unique**, **clone récurrent** : saisissez le sys_id de l'instance cible qui envoie les demandes. **Conseil :** Saisissez `stats.do` dans le navigateur d'application pour localiser l'ID d'instance.
<Source or Target> Hôte d'instance	Entrez l'emplacement d'hôte ou le nom de l'instance source ou cible. **Conseil :** Par exemple , `instanceA.service-now.com`
Spécifications de chiffrement	Les clés de la spécification de chiffrement dans un module de chiffrement définissent les clés à cloner. Pour les demandes de clone ponctuelles et récurrentes, votre instance crée automatiquement une politique d'accès au module **d'échange de ressources** . Vous n'avez pas besoin de configurer une stratégie manuellement. **Remarque :** Sélectionnez l'icône Rechercher à l'aide d'une liste (icône pour parcourir les spécifications de chiffrement disponibles.
Activer le renouvellement de saisie après l'importation de la clé	Option permettant d'activer le renouvellement de saisie automatique.

3. Sélectionnez **Soumettre**.
   En cas de réussite, une confirmation s'affiche en haut du formulaire. La table Demandes est mise à jour avec une entrée Demande **en attente** dans l'instance source et dans l'instance cible. Ouvrez l'enregistrement de la demande pour afficher l'état de la demande, le nombre de clés importées et le nombre total de clés sur l'hôte cible ou source.

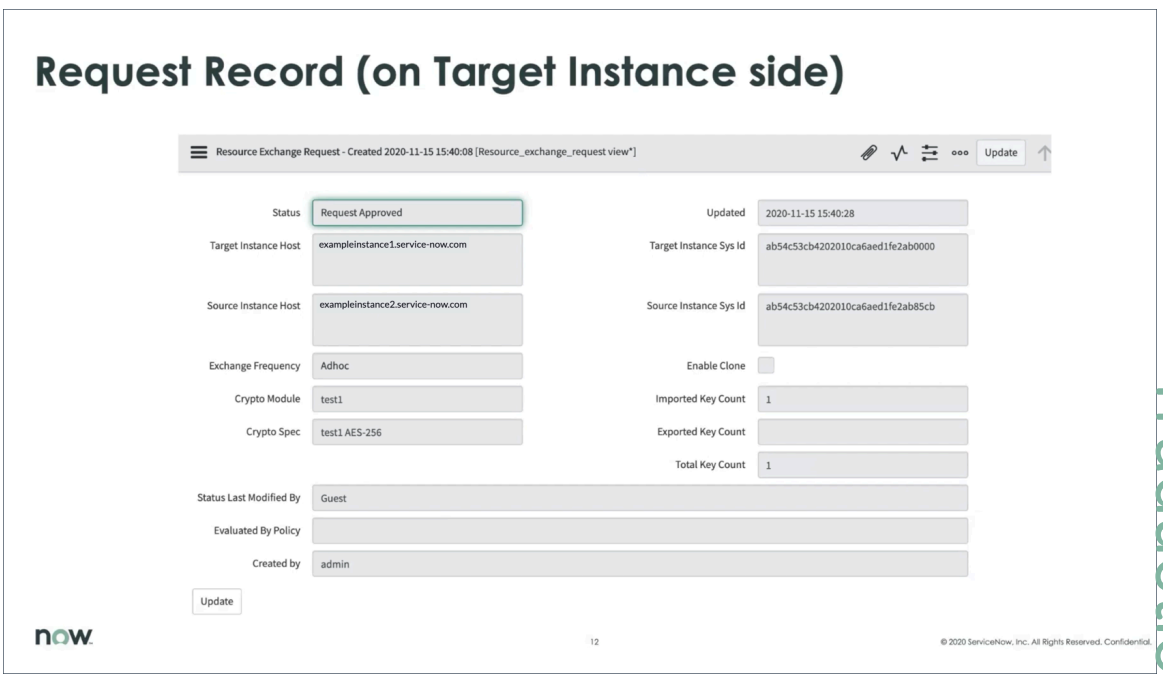


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. La demande en attente est acceptée dans l'instance source pour terminer l'échange.

   Au moment du clonage, la politique d'accès au module sur l'instance source est appelée pour approuver automatiquement la demande et envoyer les clés à la cible nouvellement clonée.



Résultats
Après une tentative d'échange de clé, votre instance de non-production met à jour la `protected.script.values.kmf.rekeyed` propriété système. Cette propriété est visible dans la table Propriétés système [sys_properties] après une tentative d'échange de clé. Si le chiffrement à l'aide de la clé échangée réussit, cette propriété a la valeur **vrai**. Dans le cas contraire, la propriété a la valeur **false**. Si la valeur est définie sur faux, l'instance tente à nouveau de chiffrer le lendemain.

Retaper le texte chiffré avec l'échange de clés

Resource Exchange prend en charge la nouvelle saisie du texte chiffré sur l'instance cible qui a été chiffrée avec des clés de la source. L'activité de nouvelle saisie est suivie dans le cycle de vie de la clé.

Vue d'ensemble

Les administrateurs qui utilisent KMF le chiffrement au niveau des colonnes peuvent l'utiliser Key Exchange pour renouvellement de clé cryptographique entre les instances de production lors de l'exécution du clonage de données. Une clé active doit d'abord être disponible sur l'instance cible pour le renouvellement de saisie, car le renouvellement de saisie nécessite une clé active. Une tâche de chiffrement est automatiquement créée et exécutée par le système pour faire pivoter et retaper la clé source et chiffrer à nouveau le texte chiffré.

Permet Key Exchange d'effectuer les actions suivantes :

- Définissez un délai d'expiration pour le renouvellement de saisie.

  Si la demande a expiré, la demande est rejetée et la clé est supprimée.

Traduction automatique

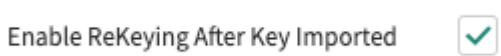
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Automatisez la nouvelle saisie du texte chiffré avec les clés des instances sources.

  Une nouvelle clé de chiffrement clonée est utilisée pour chiffrer à nouveau le texte chiffré sur l'instance cible.

- L'objectif de renouvellement de clé est défini pendant le processus de clonage et est automatisé dans le cadre du clone.
- L'activité de nouvelle saisie est suivie dans l'onglet **Clé de modules** du module de chiffrement. Accédez à l'état du cycle de vie de la clé et à la version de la clé pour l'activité clé. Consultez Faire pivoter les clés pour plus d'informations.

Configurez un Key Exchange et cochez la case **Activer le renouvellement de saisie après l'importation de la clé** pour l'activation. Consultez Configurer l'échange de clés pour en savoir plus.



Procédure pas à pas récurrente de l'échange de clés

Utilisez cette procédure pas à pas pour configurer un échange de clés récurrent dans votre instance à l'aide de et Resource Exchange.

Avant de commencer

Rôles requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Cet exemple montre comment une instance cible demande des clés à une instance hôte.

- Avant de pouvoir effectuer cette procédure, vous devez cloner une instance. Reportez-vous à la section Clone système pour plus d'informations.
- **Échange de clés automatique** : la propriété `glide_encryption.auto_key_exchange.enabled` système de base est **true** par défaut, ce qui signifie que l'option Automatique est activée lors du clonage d'une instance. La propriété est clonée sur l'instance cible.
- Désactivez l'option Automatique en définissant la propriété sur **faux**.

Procédure

1. Sur l'instance source, créez un module de chiffrement ou accédez à un module de chiffrement existant à l'aide de column_level_encryption et configurez les configurations de champs chiffrés pour le chiffrement de texte chiffré pour Key Exchange.
   Voir et pour plus de détails.

   a. Assurez-vous que les clés ont été générées dans le module de chiffrement.

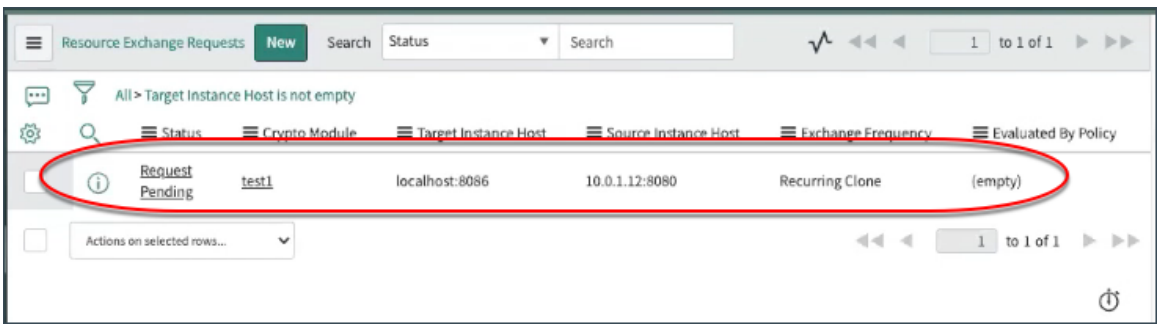
   Remarque :
   Votre instance crée automatiquement une politique d'accès au module lors de l'exécution de la demande de clone.

2. À partir de l'instance clonée, accédez à **Gestion des clés** > **Demandes d'échange de ressources** > **Nouveau**.
3. Remplissez le formulaire et sélectionnez **Clone récurrent** comme fréquence d'échange.

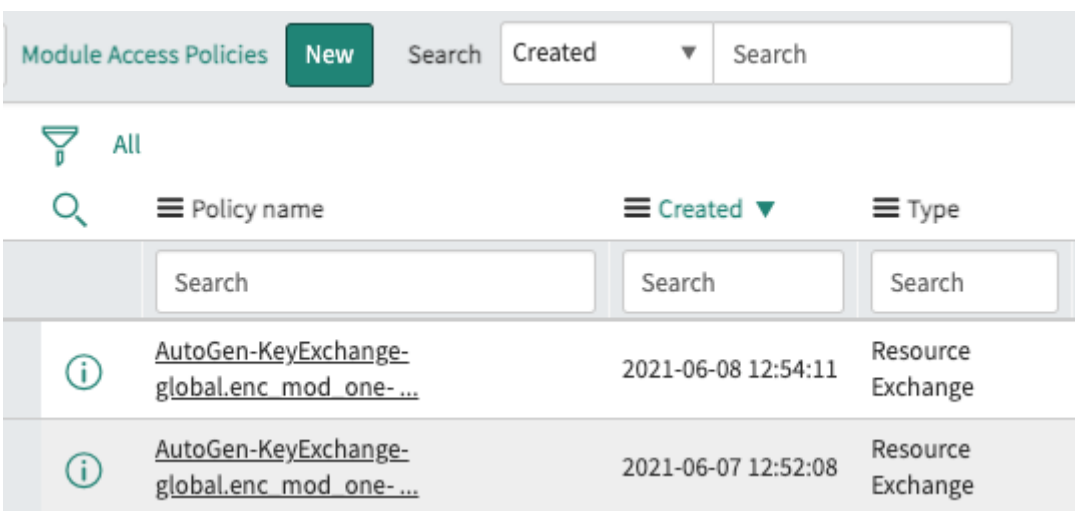
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. À partir de l'instance cible du clone, accédez à **Gestion des clés** > **Demandes d'échange de ressources**.
   La demande de l'instance hôte est affichée dans la table.



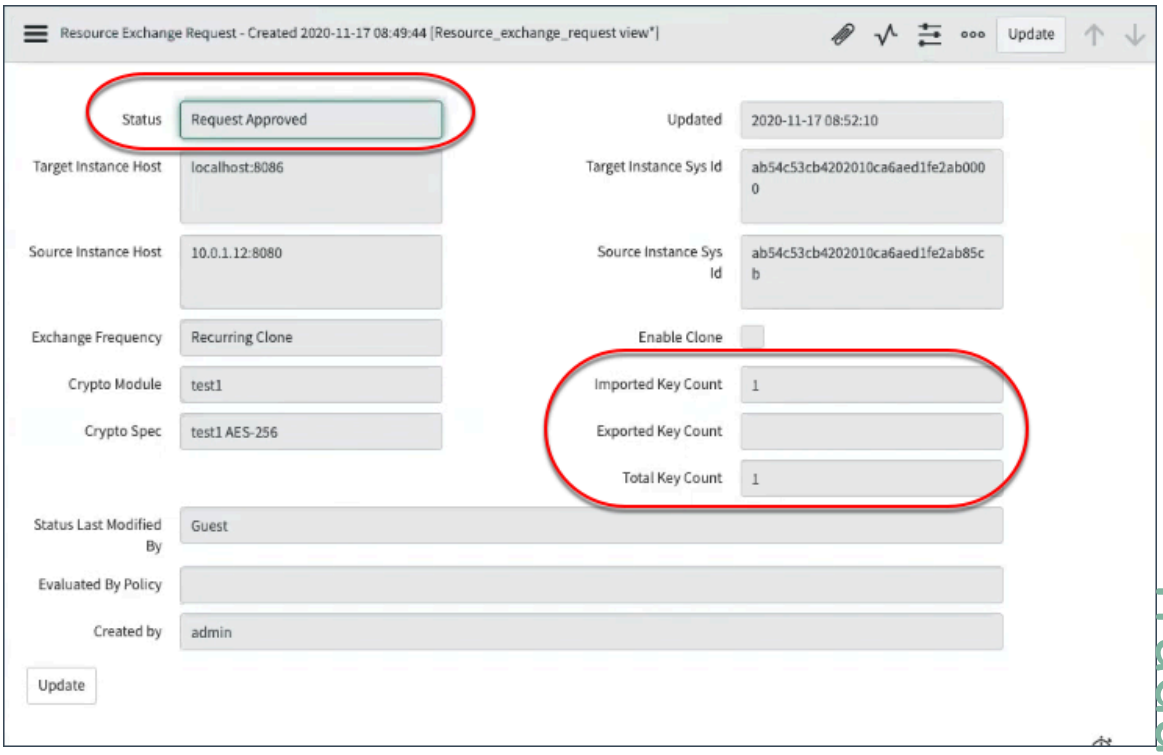
Important :
Pour les demandes de clone ponctuelles et récurrentes, votre instance crée automatiquement une politique d'accès au module. Vous n'avez pas besoin de configurer une stratégie manuellement. Au moment du clonage, cette politique sur l'instance source est invoquée pour approuver automatiquement la demande et envoyer les clés à la cible nouvellement clonée.



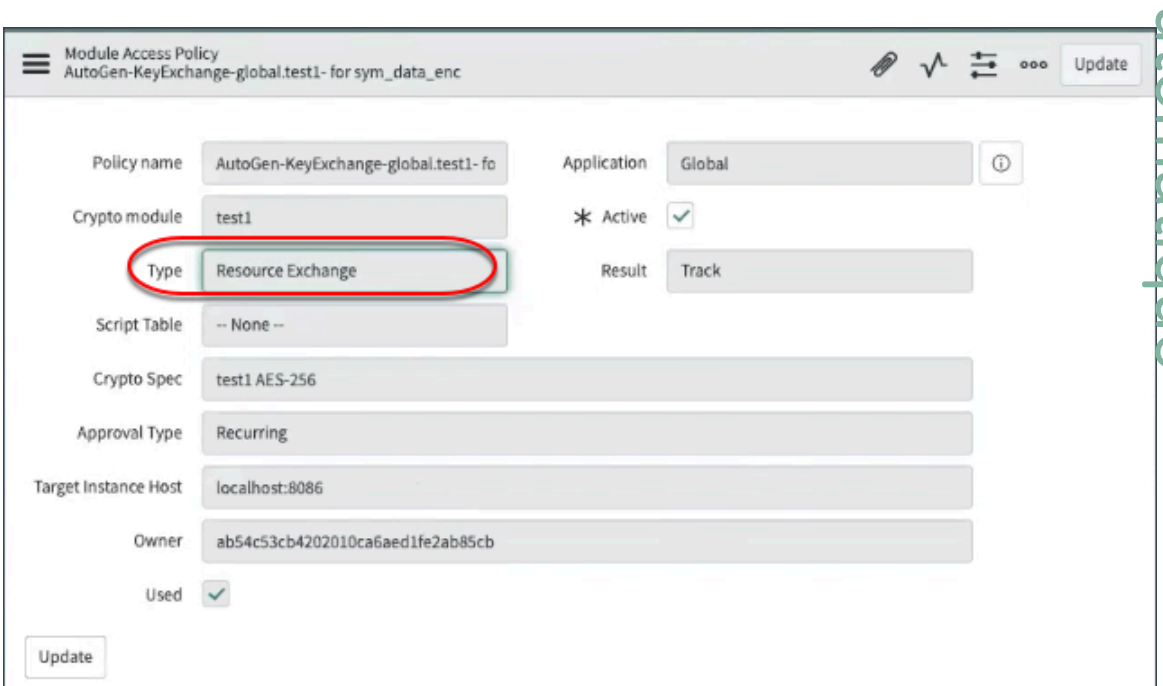
Dans le formulaire Demandes, l'état est mis à jour sur **Demande approuvée** et le champ **Nombre de clés importées** apparaît sur l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Retournez à l'instance hôte.
6. Affichez l'enregistrement de la demande pour afficher le nombre de clés exportées.
7. Affichez l'enregistrement de la politique d'accès au module pour voir que le **type** est Resource Exchange.



Remarque :
Resource Exchange Prend également en charge la nouvelle saisie du texte chiffré sur l'instance cible. Voir pour plus de détails.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Après une tentative d'échange de clé, votre instance de non-production met à jour la `protected.script.values.kmf.rekeyed` propriété système. Cette propriété est visible dans la table Propriétés système [sys_properties]. Si le chiffrement à l'aide de la clé échangée réussit, cette propriété a la valeur **vrai**. Dans le cas contraire, la propriété a la valeur **false**. Si la valeur est définie sur faux, votre instance tente à nouveau de chiffrer le lendemain.

Sécurité de l'infrastructure

Utilisez les outils de sécurité de l'infrastructure pour créer, charger et gérer les certificats que votre instance utilise pour chiffrer le trafic du client vers le serveur.

Le module d'extension Sécurité de l'infrastructure fournit les outils que vous pouvez utiliser pour gérer les chiffrements et les certificats TLS (Transport Layer Security). Votre instance utilise TLS pour chiffrer le trafic entre le client et votre serveur.

Sélectionnez les chiffrements utilisés sur votre instance

À l'aide **de la page TLS**, les administrateurs peuvent configurer les chiffrements de centre de données à utiliser sur leur instance, ainsi que sélectionner l'ordre dans lequel les chiffrements sont essayés.

Générez et chargez vos propres certificats

Utilisez les outils de sécurité de l'infrastructure pour générer vos propres demandes de signature de certificat, qui peuvent être signées par l'autorité de certification de votre choix. Ensuite, vous pouvez utiliser les outils pour charger le certificat signé dans l'équilibreur de charge de votre instance.

Surveillez l'état de vos chiffrements et certificats

Utilisez les pages **Paramètres TLS** et **Paramètres SYOC** pour afficher l'état des modifications que vous avez apportées à vos chiffrements et certificats.

Installer le module d'extension Infrastructure Security

Installez le module d'extension Paramètres de sécurité de l'infrastructure ServiceNow (com.glide.infrastructure_security) pour commencer à utiliser ces fonctionnalités. Pour en savoir plus sur l'activation d'un module d'extension, consultez Activer un module d'extension .

Après avoir installé le module d'extension, activez la fonctionnalité Sign Your Own Security (SYOC) en définissant la `sn_infra_sec.syoc.enabled` propriété système sur vrai.

Remarque :
Si la `sn_infra_sec.syoc.enabled` propriété n'est pas disponible sur votre instance, vous devez la créer. Pour obtenir des détails sur ce processus, consultez Add a system property .

Générer une demande de signature de certificat

Utilisez la page Générer une signature de certificat (CSR) pour créer une demande de signature de certificat afin de prendre en charge les certificats signés par le client pour votre équilibreur de charge d'instance.

Avant de commencer
Rôle requis : administrateur

Le module d'extension Sécurité de l'infrastructure (com.glide.infrastructure_security) doit être installé pour effectuer ces étapes. VoirSécurité de l'infrastructure pour plus de détails sur ce plugin.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d’informations sur l’utilisation d’URL personnalisées avec , reportez-vous à ServiceNowla section Définir une URL personnalisée comme URL d’instance.

Procédure

1. Accédez à la **Tout** > **Paramètres de sécurité de l'infrastructure** > **Générer un CSR**.
2. Ajoutez un ou plusieurs domaines à votre demande.
   a. Sélectionnez le bouton **Ajouter** sous l’en-tête **Domaines** .
   b. Dans la fenêtre contextuelle, saisissez le domaine et sélectionnez **OK**.
   c. Répétez ces étapes autant de fois que nécessaire pour ajouter d’autres domaines.

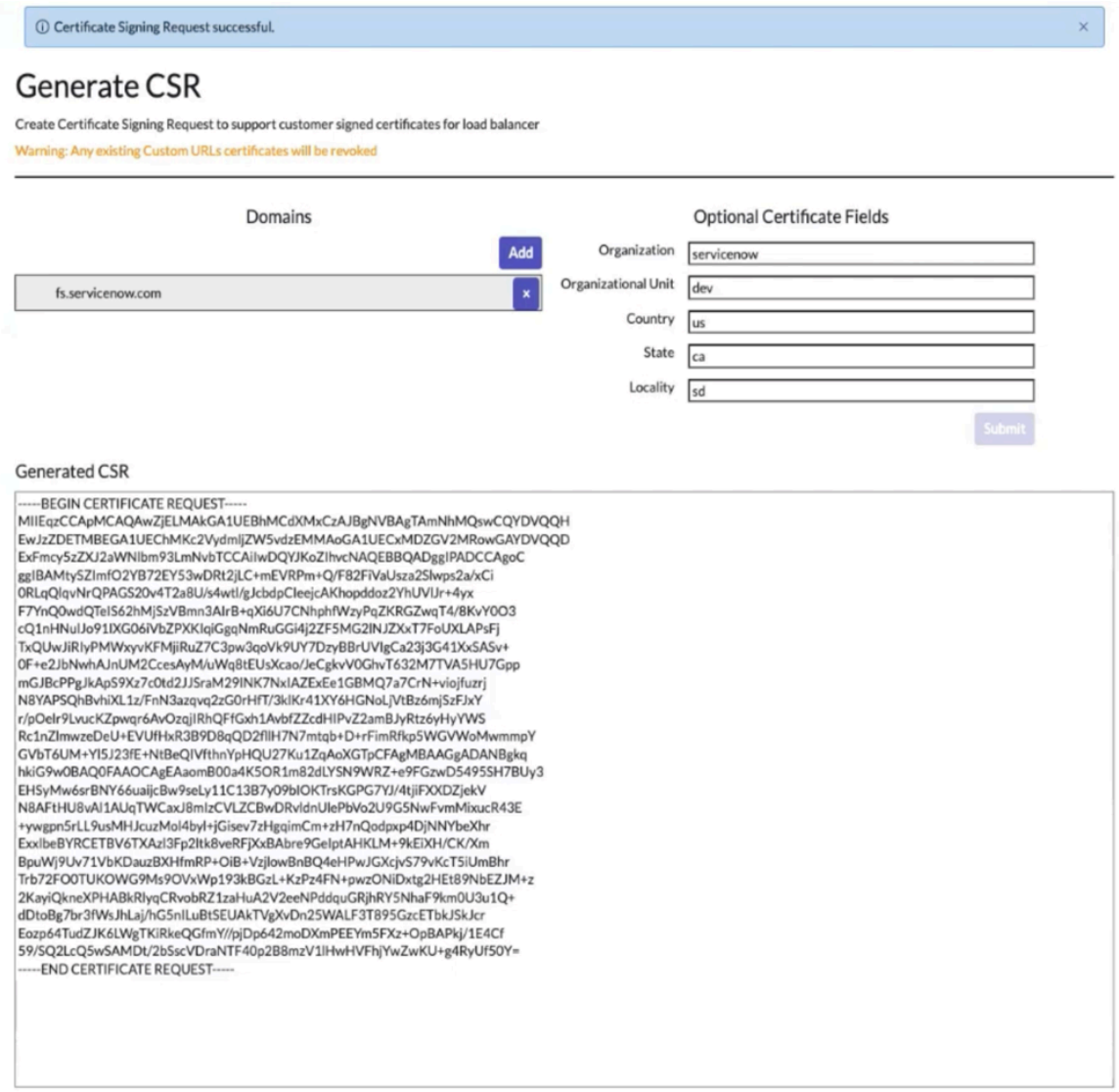
   Remarque :
   Les domaines peuvent être supprimés en sélectionnant le bouton X à gauche de chaque entrée de domaine.
3. Saisissez les informations que vous souhaitez inclure dans votre demande dans les **champs de certificat facultatifs**.
4. Sélectionnez **Soumettre**.

Avertissement :
Vous ne pouvez pas soumettre une demande pendant qu’une autre demande est en cours de génération. Si ce problème se produit, l’erreur « Ressource en conflit » s’affiche. Pour traiter, annulez la demande actuelle ou attendez que la demande actuelle soit traitée avant d’en soumettre une autre.

Après avoir sélectionné **Soumettre**, votre instance générera la demande de signature de certificat. La demande s’affiche dans le champ **CSR généré** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Copiez le contenu du champ **CSR généré** .

Chiffrement Password2 avec Key Management Framework (KMF)

Pris en charge par le Key Management Framework, utilisez le type de champ (chiffré dans 2 Password2 sens) pour chiffrer et déchiffrer des champs personnalisés avec la séparation des tâches, la protection des clés et la gestion du cycle de vie. Il fonctionne conformément aux directives NIST 800-57 et offre une protection FIPS 140-2-L3.

Password2 est un champ de texte qui stocke les mots de passe avec un chiffrement bidirectionnel. Le chiffrement bidirectionnel stocke les mots de passe sous la forme d'une valeur chiffrée sécurisée qui peut être déchiffrée dans l'instance.

Conseil :
À partir de la version, les Vancouver administrateurs peuvent déconseiller le chiffrement 3DES sur les champs password2 en faveur de la nouvelle norme AES (Advanced Encryption Standard). Pour plus de détails, voir Déconseiller l'utilisation de 3DES par GlideEncrypter pour les champs password2.

Activation

Password2 La fonctionnalité est active par défaut. Il est contrôlé par la `glide.kmf.encrypter.enabled` propriété, qui est définie sur **true** pour toutes les

Traduction automatique

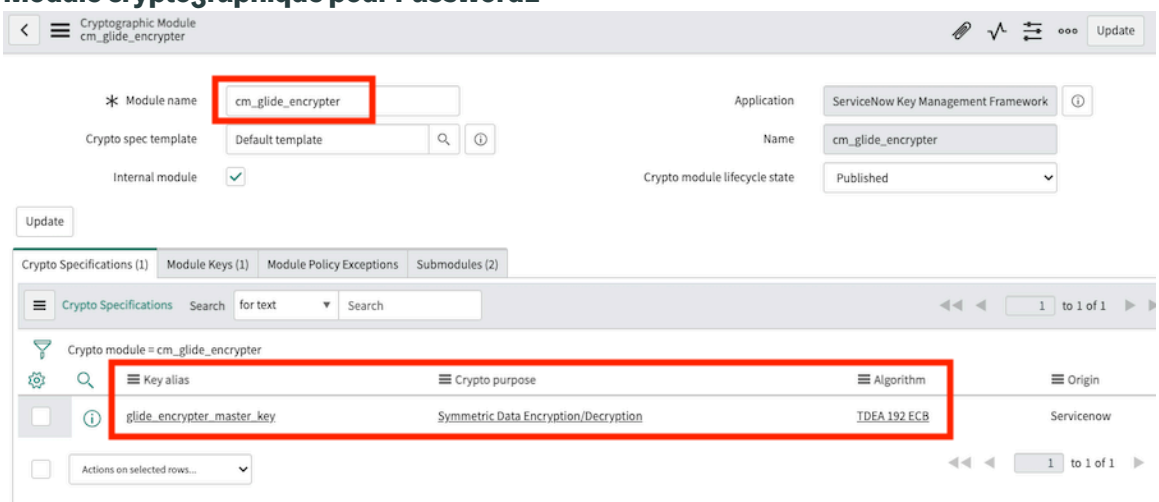
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

nouvelles instances et mises à niveau. Vous n'avez pas besoin d'activer Entreprise de Chiffrement au niveau des colonnes pour utiliser Password2.

Mode de fonctionnement de Password2

Le Key Management Framework fournit un module de chiffrement parent du système de base **cm_glide_encrypter**. Ce module fournit une spécification cryptographique et une clé qui permet de déchiffrer les champs hérités Password2 .

Module cryptographique pour Password2



Ce module cm_glide_encrypter peut avoir des sous-modules, chacun ayant sa propre clé de module et ses propres spécifications. Si un sous-module est présent avec le même périmètre d'application que l'application dans laquelle se trouve le Password2 champ, le système utilise le sous-module. Par exemple, si une table de l'application ServiceNow® Service clientèle comporte un sous-module et que vous écrivez des informations dans un Password2 champ d'une table du périmètre de Service clientèle l'application, le processus de chiffrement appelle le Service clientèle sous-module. Le processus utilise également la clé de ce sous-module pour le chiffrement et le déchiffrement avec une clé de chiffrement AES 256 GCM unique. Un sous-module par périmètre de l'application est autorisé. Le module parent n'est pas toujours utilisé pour le champ d'application global. Généralement, les nouveaux champs utilisent instance_level_glide_encrypter.

Remarque :
Vous ne pouvez pas créer vos propres sous-modules dans Xanadu. Des sous-modules sont fournis dans divers modules d'extension d'application sur le Now Platformfichier . Vous pouvez faire pivoter les clés sur les sous-modules, mais pas sur le module cm_glide_encrypter parent.

Séparation de domaine et clients sur site

KMF Password2 ne prend pas en charge Séparation de domaine. Vous pouvez l'utiliser Password2 avec des instances sur site.

L'héritage Password2 et l'actuel Password2

En Xanadu, le champ existant Password2 a été mis à niveau.

La mise en œuvre actuelle de Password2:

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilise les directives d'encapsulation Key Management Framework de clés NIST 800-57 et fournit une protection FIPS 140-2-L3 pour l'ensemble de la hiérarchie de clés.
- Inclut des options permettant de créer des sous-modules dédiés et uniques KMF Password2 pour des applications spécifiques, en fournissant un contrôle via le périmètre de l'application. Chaque sous-module possède sa propre clé de chiffrement AES 256 GCM.

Champs Password2 dans les scripts

Lorsque vous accédez à Password2 des champs avec un script, exécutez le script sous le même champ d'application que le champ d'application de la table. Utilisez setDisplayValue() pour chiffrer Password2 les valeurs et getDecryptedValue() pour déchiffrer et lire la valeur.

Remarque :
N'utilisez pas l'API GlideEncrypter() sur Password2 les champs.

Cet exemple de script vous montre comment chiffrer my@Password dans la colonne password2 de la table « table_xyz ».

```
var  gr =  new GlideRecord('table_xyz');
gr.setDisplayValue('pwd2column_name', 'my@Password');
gr.insert();
```

Important :
Vous ne pouvez pas utiliser l'API setValue() pour le Password2 champ.

Cet exemple de script vous montre comment déchiffrer le même champ pour récupérer la valeur :

```
var  gr =  new GlideRecord('table_xyz');
gr.query();
gr.next();
var ge=gr.getElement('pwd2column_name');
var ged1 = ge.getDecryptedValue();
```

Important :
L'API getDecryptedValue() n'est pas incluse dans le périmètre. Il est disponible dans le monde entier.

1. Lorsque vous chiffrez des données dans un Password2 champ, le système détermine le périmètre de l'application où réside le Password2 champ.
2. Le système recherche ensuite un sous-module du module parent **cm_glide_encrypter** ayant le même champ d'application que l'application si la propriété est définie sur *true*.

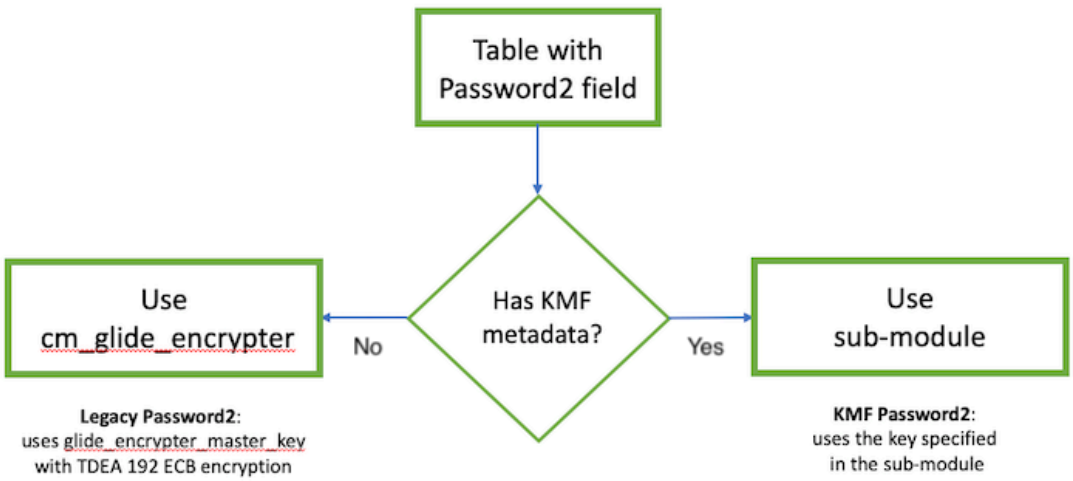
   Remarque :
   Si un sous-module ayant le même champ d'application est présent, il utilise la spécification et la clé du sous-module pour effectuer le chiffrement.

Cette illustration explique comment votre instance déchiffre les données dans Password2 les champs :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Flux de déchiffrement Password2



KMF Password2 Tâche de migration

Une tâche de migration est fournie aux clients effectuant une mise à niveau à partir de versions précédentes. Il prend les données chiffrées avec un chiffrement hérité Password2 et les chiffre à nouveau avec la clé d'une KMF Password2 clé de sous-module. Le rechiffrement s'applique uniquement aux tables avec Password2 des champs dans les périmètres de l'application qui ont également des sous-modules créés pour ce périmètre. Par exemple, un champ hérité Password2 dans **XYZ_example'application** (avec **XYZ_example** périmètre de l'application) n'est chiffré à nouveau que si un sous-module pour le périmètre de l'application **XYZ_example** existe sous le module parent cm_glide_encrypter.

Les KMF Password2 clés de chiffrement du sous-module sont protégées (enveloppe chiffrée) dans la KMF hiérarchie des clés.

Certificats

Votre instance a besoin de certificats pour établir des connexions sécurisées et valider les signatures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les principales fonctionnalités et la valeur commerciale des certificats.

Configurer



Planifiez vos configurations de base.

Charger



Planifiez et configurez l’application.

Traduction automatique

Exploration des certificats

Votre instance a besoin de certificats pour établir des connexions sécurisées et valider les signatures.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les certificats sont utilisés pour des fonctionnalités telles que :

- LDAPS (en anglais seulement)
- Outbound web service mutual authentication
- Sécurité des services Web
- MID Server

Pour utiliser un certificat, vous devez générer ou acheter un certificat pour le serveur ou le client sécurisé et le charger sur une instance.

Certificats LDAP

Un certificat SSL est nécessaire pour que l'instance établisse une connexion LDAP sur SSL (protocole LDAPS) avec un serveur LDAP.

L'instance accepte deux types de certificats LDAP :

Certificat	Type	Requis pour
Certificat du serveur LDAP	Tout type pris en charge	Toutes les configurations LDAP
Certificat client LDAP	Type de magasin de clés Java	Authentification réciproque

S'il existe plusieurs certificats de serveur, l'instance teste chaque certificat de serveur à tour de rôle jusqu'à ce que le serveur LDAP autorise la connexion. Si vous utilisez plusieurs serveurs LDAP, assurez-vous d'inclure le certificat SSL pour chaque serveur LDAP.

L'authentification réciproque exige que le client présente un certificat en plus du serveur. Si votre serveur LDAP nécessite une authentification réciproque, vous devez également fournir le certificat client de votre serveur LDAP dans un certificat de type magasin de clés Java.

Critères de certification

Un certificat valide doit répondre aux critères suivants :

- Le certificat peut avoir une taille de clé allant jusqu'à 2048 bits.
- Le certificat doit avoir l'une des extensions de fichier suivantes :

Extension	Description
DER	Le format *Distinguished Encoding Rules* est une syntaxe binaire de transfert de messages. Ce format prend également en charge le fichier . CER et . Extensions de fichiers CRT.
Régie de l'énergie	Extensions de fichier de certificat pour les certificats utilisant le format Distinguished Encoding Rules.
Tube cathodique	Extensions de fichier de certificat pour les certificats utilisant le format Distinguished Encoding Rules.
PEM	Le format *Privacy Enhanced Mail* est un certificat DER codé en base 64 placé entre les chaînes de texte « -----BEGIN CERTIFICATE----- » et « -----END CERTIFICATE----- ».

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Certificat de confiance

Par défaut, votre instance ne fait confiance qu'aux certificats issus d'une autorité de certification (CA) reconnue dans la machine virtuelle Java (JVM). Les certificats autosignés et signés par l'entreprise ne sont pas fiables.

Remarque :
Pour en savoir plus sur les propriétés qui affectent l'utilisation des certificats, consultez Communications sécurisées Paramètres de renforcement de la sécurité de l'instance.

Génération d'un certificat client LDAP

Générez un certificat client LDAP pour l'authentification réciproque à l'aide d'OpenSSL. Le résultat final est un certificat PKCS#12 stocké dans un magasin de clés Java.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Consultez la documentation OpenSSL pour plus d'informations sur la génération de certificats. Ces étapes supposent que vous avez accès à OpenSSL.

Entrez ces commandes dans une interface de ligne de commande.

Procédure

1. Générez un certificat client auto-signé.

   Example
   Par exemple, cette commande crée un certificat client test1-cert.crt basé sur la clé privée test1-key.key.

   ```
   openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout test1-key.key -out
    test1-cert.crt
   ```

2. Convertissez à la fois le fichier de certificat et la clé privée en PKCS#12 (un fichier avec une extension .pfx ou .p12).

   Example
   Par exemple, cette commande convertit le certificat client et la clé privée en un certificat PKCS#12 appelé test1-certificate.pfx.

   ```
   openssl pkcs12 -export -out test1-certificate.pfx -inkey test1-key.key -in test1-cert.crt
   ```

3. Générez le magasin de clés Java et importez-y le fichier pkcs12.

   Example
   Par exemple, cette commande importe le certificat dans le magasin de clés Java test1.jks.

   ```
   keytool -importkeystore -srckeystore test1-certificate.pfx -srcstoretype PKCS12
    -destkeystore test1.jks
   ```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Chargez le certificat dans le fichier keystore (`test1.jks`) vers l'instance.

> **Remarque :**
>
> Si vous chargez vers une instance sur site à l'aide d'un certificat avec l'extension .jks et que vous recevez un message d'erreur indiquant « Aucun certificat valide trouvé pour traiter le chargement de l'application », utilisez plutôt un certificat avec l'extension .pfx.

Que faire ensuite

Chargement d'un certificat dans une instance

Génération d'un certificat de serveur

Vous pouvez utiliser keytool pour générer un nouveau fichier de magasin de clés Java, créer une demande de signature de certificat (CSR) et importer la clé privée, la paire de certificats publics et les certificats signés dans le magasin de clés.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Consultez la documentation de l'outil de clés Java pour plus d'informations sur la génération de clés et de CSR.

Entrez ces commandes dans une interface de ligne de commande :

Procédure

1. Générez un magasin de clés Java et une paire de clés.

   Example

   Par exemple, cette commande crée un magasin de clés appelé my.keystore et génère une clé privée appelée mydomain dans le magasin de clés.

   ```
   keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
   ```

2. Générez une CSR pour un magasin de clés Java existant.

   Example

   Par exemple, cette commande génère une CSR appelée mydomain.csr ou la clé mydomain.

   ```
   keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
   ```

3. Importez un certificat *d'autorité de certification* (CA) racine ou intermédiaire dans le magasin de clés Java.

   Example

   Par exemple, cette commande importe le certificat CA pour Thawte. Cette commande suppose que Thwate est l'autorité de certification qui a signé la CSR.

   ```
   keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
   ```

4. Importez un certificat primaire signé dans le magasin de clés Java.

   Example

   Par exemple, cette commande importe le certificat signé mydomain.crt dans le magasin de clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

5. Chargez le certificat dans le fichier keystore (my.keystore) vers l'instance.

Que faire ensuite

Chargement d'un certificat dans une instance

Chargement d'un certificat dans une instance

Ajoutez un certificat à l'instance à partir du module Certificats.

Charger un certificat dans une instance

Chargez un certificat dans une instance.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Lorsqu'un certificat est mis à jour sur le serveur ADFS, vous devez également charger un certificat mis à jour sur l'instance.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Certificats**.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire.
4. Sélectionnez **Soumettre**.

   Lors du téléchargement, le module extrait et affiche les propriétés en lecture seule du certificat dans les champs suivants :

   - Date de début de validité
   - Date d'expiration
   - Émetteur
   - Objet de la certification

5. Sélectionnez **Valider les magasins/certificats** pour vérifier si le certificat est correct.
   Si l'instance rencontre des erreurs avec le certificat ou le magasin de clés, elle affiche un message d'erreur.

Chargement d'un certificat de serveur approuvé

En chargeant le certificat de serveur approuvé du fournisseur de service, l'instance s'assure qu'elle se connecte à un service valide et sécurisé.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

L'instance valide les appels de service Web sortants à l'aide du certificat fourni par le fournisseur de service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Créez un enregistrement de certificat de type **Certificat de magasin de confiance**.
2. Effectuez l'une des actions suivantes :
   - Joindre le certificat au format DER du fournisseur de service.
   - Copiez et collez le certificat au format PEM du fournisseur de service dans le champ **Certificat PEM** .

Chiffrement au niveau des colonnes

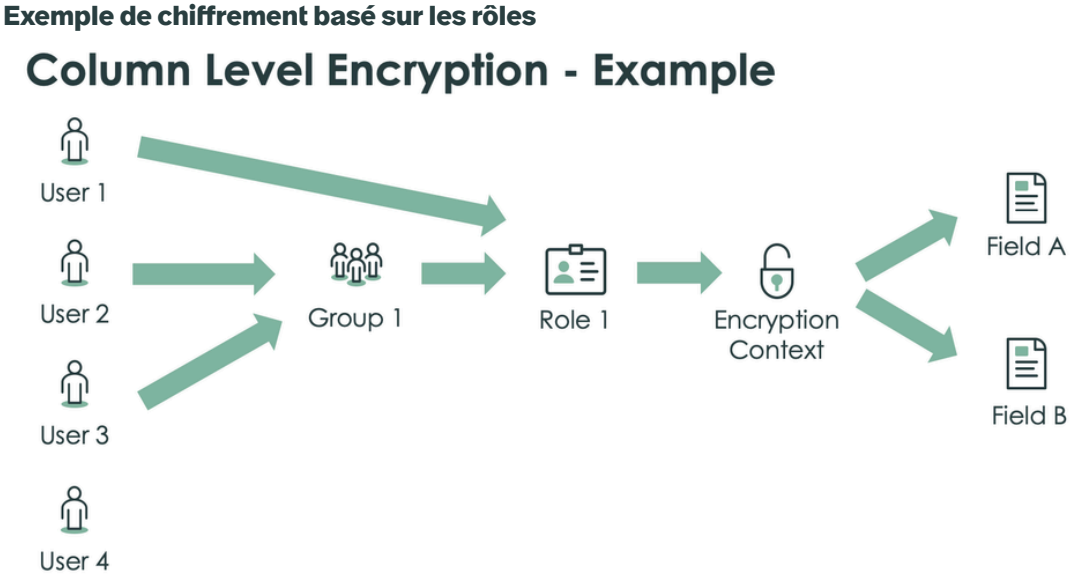
Le chiffrement au niveau des colonnes (CLE) autorise et refuse l'accès aux données chiffrées en fonction du rôle de l'utilisateur. Chiffrement au niveau des colonnes inclut la gestion des clés de base à l'aide de modules de chiffrement.

Vue d'ensemble

Avec le chiffrement au niveau des colonnes, vous pouvez chiffrer des colonnes de données spécifiques au sein de vos tables, au lieu de chiffrer l'intégralité de la table ou de la base de données. Utilisez cette méthode pour vous assurer que vos données sensibles restent protégées sans avoir besoin de chiffrer une table entière. La possibilité de chiffrer uniquement les parties de vos tables qui en ont besoin permet de réduire le temps passé à chiffrer et à déchiffrer les données.

CLE accorde l'accès aux données chiffrées en fonction du rôle d'un utilisateur. En raison de cette approche, les utilisateurs doivent être associés à un rôle pour afficher les données chiffrées par CLE. Les utilisateurs peuvent être associés directement à un rôle ou affectés à un groupe associé à un rôle. Cette approche basée sur les rôles simplifie le processus consistant à s'assurer que vos données sont visibles uniquement par les utilisateurs qui en ont besoin.

Exemple de chiffrement basé sur les rôles



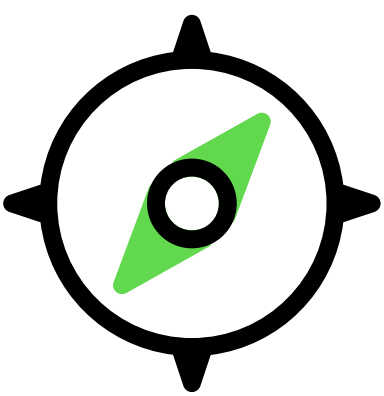
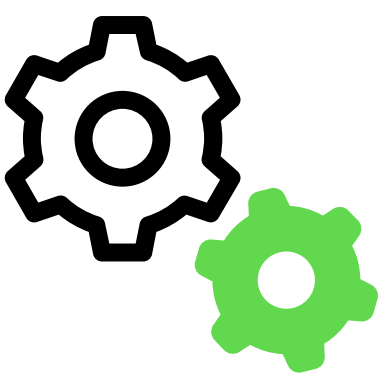
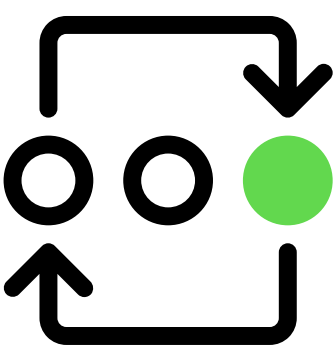
Dans cet exemple, vous pouvez voir quatre utilisateurs tenter d'accéder aux données stockées dans deux champs d'un formulaire. Ces champs sont chiffrés par un contexte de chiffrement, qui n'est accessible qu'aux utilisateurs associés à un rôle spécifique (rôle 1).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'utilisateur 1 est membre du rôle 1, qui fournit l'accès au module de chiffrement 1. L'utilisateur 1 peut voir le contenu des champs A et B.
- L'utilisateur 2 et l'utilisateur 3 sont membres du groupe 1. Le groupe 1 est membre du rôle 1, qui permet à tous les membres du groupe 1 d'accéder au module de chiffrement 1 et permet aux utilisateurs 2 et 3 de voir le contenu des champs A et B.
- L'utilisateur 4 n'est membre d'aucun groupe ou rôle et n'a pas accès au module de chiffrement 1. L'utilisateur 4 note l'accès au champ A ou au champ B. L'utilisateur 4 ne voit pas non plus ces champs sur un formulaire. Dans une vue de liste, ces champs sont visibles, mais les valeurs doivent être vides.

Premiers pas

Explorer	Configurer	Utiliser
		
Découvrez les avantages des éditions Standard et Enterprise de Chiffrement au niveau des colonnes.	Découvrez comment activer et configurer Chiffrement au niveau des colonnes, et gérer la migration à partir de la prise en charge du chiffrement	Utiliser le chiffrement au niveau des colonnes pour gérer l'accès aux données chiffrées sur vos instances

Dépannage et demande d'aide

- Forum des développeurs de la communauté ServiceNow
- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client

Explorer Chiffrement au niveau des colonnes

En savoir plus sur Chiffrement au niveau des colonnes.

Vue d'ensemble de Chiffrement au niveau des colonnes

Le chiffrement au niveau des colonnes (CLE) est une fonctionnalité du système de base qui permet le chiffrement des données stockées dans une instance à l'aide d'AES128 ou AES256.

CLE vous permet de chiffrer les champs de base de données sélectionnés et les fichiers stockés à l'aide de contextes de chiffrement. Dans ces contextes, vous définissez ce qui est

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

chiffré, choisissez l'algorithme à utiliser et fournissez la clé de chiffrement, qui est stockée dans votre instance.

Une fois le contexte créé, vous pouvez l'associer à un rôle d'utilisateur. Les utilisateurs affectés à ce rôle, soit directement, soit par l'intermédiaire d'un groupe, peuvent accéder aux données chiffrées.

Étant donné que CLE base l'accès aux données sur l'affectation de rôles, il est important de savoir comment administrer les rôles sur votre instance. Pour plus d'informations, consultez Managing roles .

Workflow Chiffrement au niveau des colonnes

Avantages de Chiffrement au niveau des colonnes

Avantage	Fonctionnalité	Rôles requis
Configurez l'accès à vos données chiffrées en fonction des rôles d'utilisateur affectés.	Accès basé sur les rôles aux données chiffrées	Administrateur de sécurité
Protégez vos données à l'aide d'AES (Advanced Encryption Standard). Vous pouvez choisir d'utiliser les algorithmes de chiffrement AES-128 ou AES-256.	Chiffrement AES	Administrateur de sécurité
Créez jusqu'à 5 modules et politiques d'accès aux modules (MAP) à l'aide de la version standard de CLE. Les MAP élargissent l'accès basé sur les rôles pour permettre de prendre en compte les éléments suivants : • Utilisateurs système • Scripts • Échange de ressources KMF CLE Enterprise prend en charge des MAP supplémentaires.	Prise en charge d'un maximum de 5 modules et politiques d'accès au module (MAP)	Administrateur de sécurité
Chiffrez les types de champs courants à l'aide de la version standard de CLE. CLE Enterprise prend en charge des types de champs supplémentaires.	Chiffrement pour le texte de chaîne, les champs Date et Date/heure, les pièces jointes et les URL	Administrateur de sécurité
Choisissez entre un chiffrement standard et un chiffrement préservant l'égalité. Lorsqu'il est activé, le chiffrement préservant l'égalité garantit que la valeur chiffrée d'un champ est la même lorsque la valeur du champ reste la même. Ce type de chiffrement permet des comparaisons d'égalité et des opérations de regroupement par sur un champ. **Remarque :** Le chiffrement non déterministe n'est pas pris en charge.	Prise en charge du chiffrement préservant l'égalité	Administrateur de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantage	Fonctionnalité	Rôles requis
Utilisez les API getDisplayValue() et setDisplayValue() pour renvoyer des valeurs en clair et insérer des données chiffrées pour les champs chiffrés.	API getDisplayValue() et setDisplayValue()	Administrateur de sécurité, développeur

Avantages de Chiffrement au niveau des colonnes pour l'entreprise

Chiffrement au niveau des colonnes Enterprise s'appuie sur le cadre de travail CLE existant et fournit ces fonctionnalités supplémentaires après l'achat d'un abonnement.

Avantage	Fonctionnalité	Rôles requis
Chiffrez les types de champs supplémentaires.	Prise en charge de types de champs supplémentaires : • HTML • Journal • Traduit	Administrateur de sécurité
CLE Enterprise prend en charge plus de 5 modules et politiques d'accès aux modules pour offrir plus d'options d'accès aux données sécurisées.	Prise en charge de modules et de MAP supplémentaires	Administrateur de sécurité
Les clés d'un coffre à clés peuvent faire l'objet d'une rotation selon un calendrier automatisé que vous configurez. L'utilisation de la rotation automatique des clés peut améliorer la sécurité tout en réduisant les frais administratifs.	Rotation automatique des clés configurable	Administrateur de sécurité
Gérez le cycle de vie complet de vos clés de chiffrement des données. En option, vous pouvez échanger en toute sécurité des clés de chiffrement de données générées au sein de votre environnement.	Clés fournies par le client	Administrateur de sécurité
Les clés éphémères sont des clés cryptographiques qui sont générées à chaque exécution d'un processus cryptographique. Ces clés sont d'autant plus sécurisées qu'elles sont générées pour être utilisées dans une seule session.	Clés cryptographiques éphémères	Administrateur de sécurité
Les API setDisplayValue() et setDisplayValue() mises à jour peuvent insérer des données chiffrées pour les champs chiffrés.	Mise à jour des API getDisplayValue() et setDisplayValue()	Administrateur de sécurité, développeur

Visite guidée Chiffrement au niveau des colonnes

La visite guidée donne un bref aperçu de la configuration de Chiffrement au niveau des colonnes (CLE) nécessaire pour chiffrer des champs de table ou des pièces jointes. Les étapes de création de modules de chiffrement de champ, de politiques d'accès au module et de configurations de champs chiffrés sont également abordées. La visite guidée comprend des liens vers la documentation détaillée et le cours ServiceNow University Vue d'ensemble de Chiffrement au niveau des colonnes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

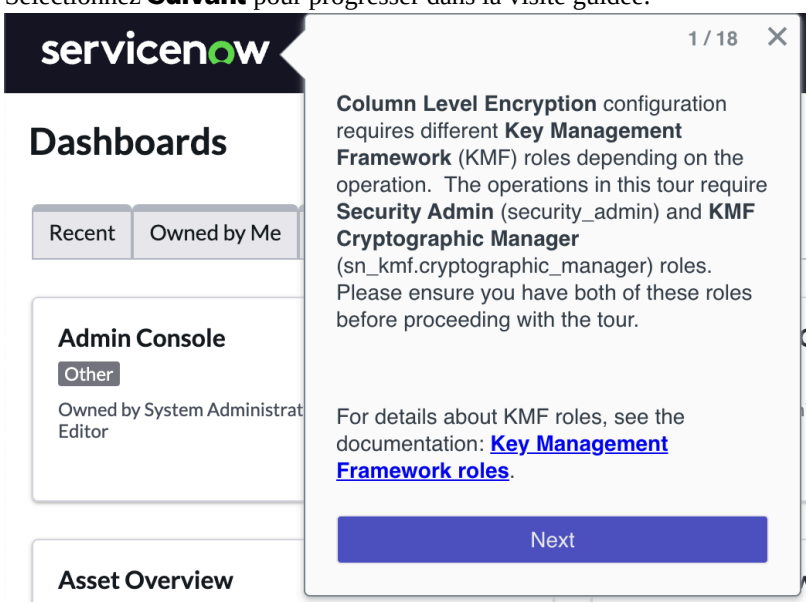
Avant de commencer

Rôle requis : sn_kmf.crypto_manager ou security_admin

Remarque :
La visite guidée n'est pas encore disponible lorsqu'elle Next Experience est activée.

Procédure

1. Accédez à la page d'interface utilisateur **$pa_dashboards_overview.do** sur votre instance.
   Par exemple : `http://yourcompany.servicenow.com/nav_to.do?uri=%2F$pa_dashboards_overview.do` remplacez `votresociété` par le nom de votre instance.
2. Ouvrez l'icône **Afficher l'aide** ( ) dans le coin supérieur gauche.
3. Sélectionnez **Faire une visite guidée** en bas de la barre latérale.
4. Sélectionnez **Suivant** pour progresser dans la visite guidée.



Configuration de Chiffrement au niveau des colonnes

Découvrez comment activer et configurer Chiffrement au niveau des colonnes, et gérer la migration à partir de la prise en charge du chiffrement.

Activation

Chiffrement au niveau des colonnes

Le module d'extension Chiffrement au niveau des colonnes (com.glide.encryption) ne nécessite pas d'abonnement et peut être activé sur votre instance par un administrateur. Pour en savoir plus sur l'installation du module d'extension, reportez-vous à la section Activate a plugin .

Chiffrement au niveau des colonnes – Entreprise

Chiffrement au niveau des colonnes - Entreprise est une version améliorée de Chiffrement au niveau des colonnes, qui nécessite un abonnement.

- Pour en savoir plus sur le produit, reportez-vous à la section Chiffrement au niveau des colonnes – Entreprise.
- Pour plus d'informations sur l'installation de Chiffrement au niveau des colonnes Enterprise, reportez-vous à la section Activer Chiffrement au niveau des colonnes – Entreprise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Migration à partir de la prise en charge du chiffrement

Utilisez les travaux planifiés pour migrer vos clés et données chiffrées de la prise en charge du chiffrement héritée vers Entreprise de Chiffrement au niveau des colonnes. Pour en savoir plus sur ce processus, consultez l'adresse Migration vers Chiffrement au niveau des colonnes – Entreprise

Modifier les paramètres de chiffrement de la pièce jointe

Améliorez la sécurité en empêchant les utilisateurs de joindre des fichiers non chiffrés. Pour plus de détails, consultezEmpêcher les utilisateurs de joindre des fichiers non chiffrés.

Activer Chiffrement au niveau des colonnes – Entreprise

Avec un abonnement à Entreprise de Chiffrement au niveau des colonnes, un administrateur peut activer le module d'extension com.glide.now.platform.encryption.

Avant de commencer

Rôle requis : administrateur

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Le chargé de clientèle peut faire en sorte que le module d'extension soit activé sur les instances de production et de non-production de votre organisation, en général en quelques jours à peine.

Pourquoi et quand exécuter cette tâche

L'activation du module d'extension Entreprise de Chiffrement au niveau des colonnes (com.glide.now.platform.encryption) apporte les modifications suivantes à votre instance :

- Le module d'extension Encryption Support (com.glide.encryption) est également activé.

  Remarque :
  Le Key Management Framework module d'extension (com.glide.kmf.global) est déjà actif par défaut.

- La propriété glide_encryption.set_value_support_cle.disabled est définie sur **faux**, ce qui active la fonctionnalité SetValue. La prise en charge de SetValue permet aux API setDisplayValue() et setValue() de prendre en charge les données chiffrées. Il permet également à getDisplayValue() et getValue() de renvoyer des valeurs en texte clair.
- Deux travaux planifiés sont activés :
  - **autoKeyMigration** : migre les clés de contexte de chiffrement vers les clés de Key Management Framework module de chiffrement (KMF).
  - **autoDataMigration** : migre les données que vous avez déjà chiffrées pour utiliser la clé de KMF module de chiffrement.

  Les administrateurs peuvent modifier le moment d'exécution de ces travaux planifiés et les mettre en pause ou les redémarrer à tout moment.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Recherchez le module d'extension *`Platform Encryption - com.glide.now.platform.encryption`* à l'aide des critères de filtrage et de la barre de recherche. Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Installer**, puis sur **Activer** dans la boîte de dialogue Activer le module d'extension.

> **Remarque :**
> Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Migration vers Chiffrement au niveau des colonnes – Entreprise

Les travaux planifiés migrent vos clés et données chiffrées de la prise en charge du chiffrement vers Entreprise de Chiffrement au niveau des colonnes.

Vous pouvez passer en revue les travaux planifiés en accédant à **Sécurité de système** > **Paramètres de sécurité élevée** > **Tâches de Sécurité**:

- **autoKeyMigration** : migre les clés de contexte de chiffrement vers les clés de Key Management Framework module de chiffrement (KMF).
- **autoDataMigration** : migre les données que vous avez déjà chiffrées pour utiliser la clé de KMF module de chiffrement.

Vous pouvez modifier le moment d'exécution de ces travaux planifiés et les mettre en pause ou les redémarrer à tout moment.

Vérifiez que les configurations de champs chiffrés utilisent vos clés de module nouvellement migrées en accédant à **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**. Recherchez les éléments suivants :

- Le champ **Méthode** est **Module unique**.
- Le champ **Module de chiffrement** est rempli avec le nom du module de chiffrement que le système crée automatiquement. Vous pouvez consulter ce module et la politique d'accès au module, qui sont tous deux actifs et publiés.

Chiffrement au niveau des colonnes Clones Enterprise et système

Si Chiffrement au niveau des colonnes Enterprise est installé sur votre instance, une nouvelle clé de chiffrement du module de chiffrement de champ est automatiquement générée sur l'instance de clone cible dans le cadre du processus de clonage. Ces clés sont générées pour tous les modules auxquels l'utilisateur a accès et qui n'ont pas déjà de clé.

Pour cette raison, deux clés de chiffrement de module peuvent être présentes dans les modules de chiffrement de champ sur l'instance de clone cible :

- Une clé de chiffrement de module actif. Il s'agit de la nouvelle clé générée après le clone, tant que le module est accessible à l'utilisateur et qu'il n'a pas de clés antérieures.
- Une clé de module de chiffrement désactivée (à partir du transfert automatisé d'échange de clés)

  La clé de chiffrement du module actif est utilisée pour chiffrer les données insérées selon les besoins sur l'instance de clone cible. Le module désactivé est utilisé pour déchiffrer les données existantes qui ont été clonées dans le cadre du clone système.

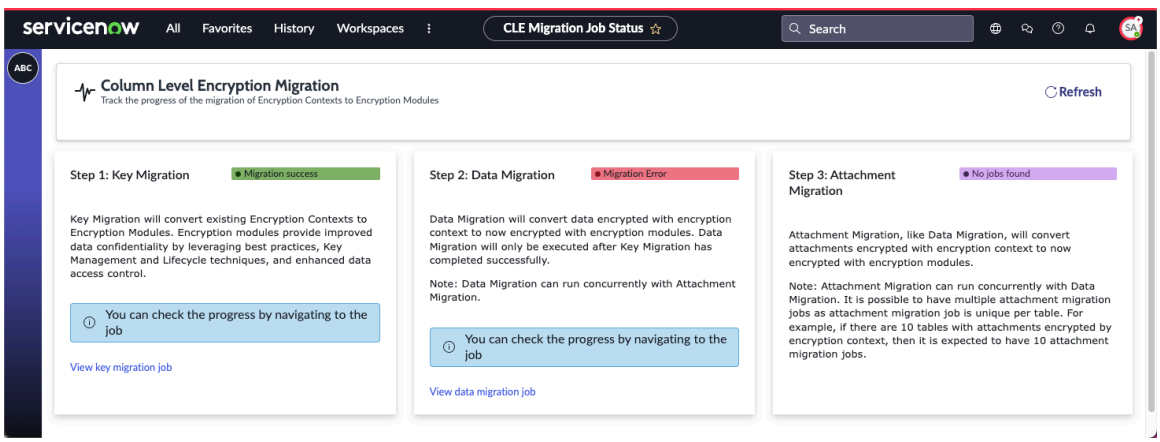
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour utiliser une clé unique afin de déchiffrer et de chiffrer toutes les données, vous pouvez exécuter une tâche de renouvellement de saisie de module. Pour plus d'informations sur les tâches de renouvellement de saisie des modules, consultez Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse.

Page d'état de la migration de Chiffrement au niveau des colonnes

Utilisez la page État de la migration pour suivre la migration des contextes de chiffrement vers les modules de chiffrement.

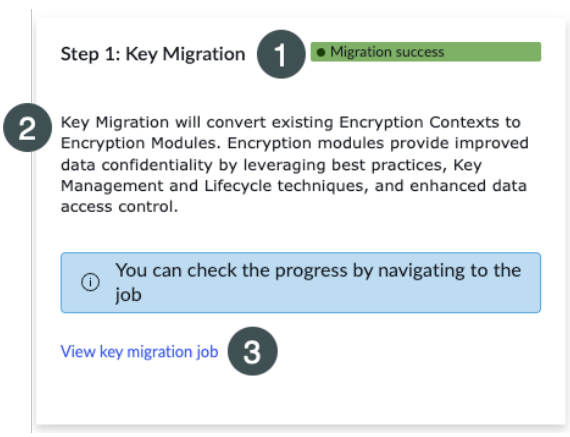


La Chiffrement au niveau des colonnes page Migration affiche l'état des étapes impliquées dans la migration des contextes de chiffrement vers les modules de chiffrement. Chacune des trois sections affiche l'état d'une étape spécifique du processus.

Cartes de sections de page

La page contient trois cartes représentant les étapes de la progression de la migration. Ces cartes affichent :

- (1) L'état de l'étape en cours. Cet état indique si l'étape s'est terminée avec succès ou s'il n'y a aucune tâche à traiter.
- (2) Une description de l'étape énumérée.
- (3) Un lien vers l'enregistrement de tâche de chiffrement [sys_mass_encryption_job] pertinent.



Empêcher les utilisateurs de joindre des fichiers non chiffrés

Modifiez la propriété com.glide.encryption.enable_attachment_key_ui pour empêcher vos utilisateurs ayant accès à une clé de module de chiffrement de joindre des pièces jointes non chiffrées.

Avant de commencer
Rôle requis : security_admin

Vous devez vous élever au rôle security_admin effectuant ces étapes. Pour obtenir des instructions, consultez Élever à un rôle privilégié

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, les utilisateurs qui ont accès à une clé de module de chiffrement peuvent charger des pièces jointes non chiffrées. Utilisez la `com.glide.encryption.enable_attachment_key_ui` propriété système pour modifier ce comportement.

Lors de l'attachement, vos utilisateurs voient un sélecteur d'interface utilisateur sur les enregistrements qui ont une configuration de champs chiffrés multi-modules. Lorsque cette propriété est définie sur faux, les utilisateurs ne voient plus d'option permettant de ne pas chiffrer une pièce jointe.

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Toutes les propriétés**.
2. Dans la liste des propriétés système, recherchez et ouvrez la propriété système.
3. Définissez la **valeur** de la propriété sur faux.

Utilisation du chiffrement au niveau des colonnes

Utilisez le chiffrement au niveau des colonnes pour gérer l'accès aux données chiffrées sur vos instances.

Information associée

- Créer un module cryptographique pour Chiffrement au niveau des colonnes
- Utilisation de plusieurs modules de chiffrement
- Créer une spécification cryptographique pour Chiffrement au niveau des colonnes
- Configurer des algorithmes avancés pour Chiffrement au niveau des colonnes – Entreprise
- Configurer les propriétés des clés fournies par le client
- Chiffrer les champs et les pièces jointes
- Exemples d'Enterprise de Chiffrement au niveau des colonnes

Créer un module cryptographique pour Chiffrement au niveau des colonnes

Créez un module de chiffrement au niveau des colonnes pour définir les mécanismes utilisés pour les opérations de chiffrement.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf_admin, security_admin, admin

Pourquoi et quand exécuter cette tâche

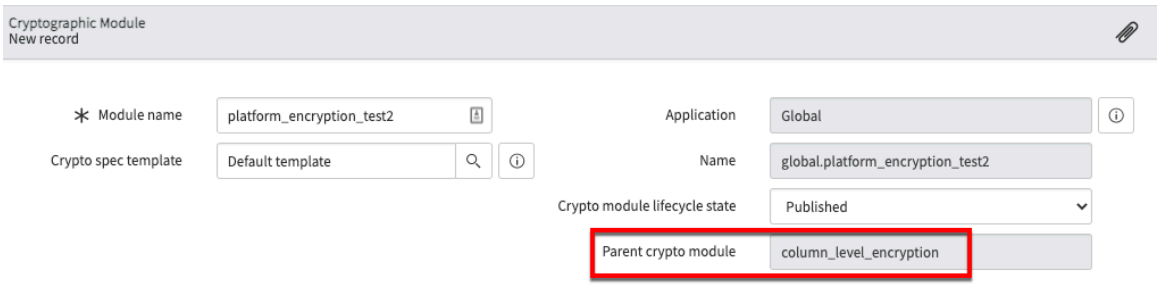
Cette procédure décrit les options disponibles avec Chiffrement au niveau des colonnes (CLE) avec le système de base et les options de configuration supplémentaires qui deviennent disponibles avec Entreprise de Chiffrement au niveau des colonnes la fonctionnalité Entreprise de Chiffrement au niveau des colonnes (CLE_Ent). est disponible avec un abonnement payant. Consultez la rubrique Offre groupée d'abonnements pour Encryption and Key Management pour connaître les fonctionnalités et options prises en charge disponibles avec chaque offre. Pour Activer Chiffrement au niveau des colonnes – Entreprise plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Modules de chiffrement de champ** > **Nouveau**.



2. Renseignez les champs du formulaire.

Formulaire du module de chiffrement

Champ	Description
Nom du module	Chaîne alphanumérique à référencer lors de l'exécution de scripts.
Modèle de spécification de chiffrement	Modèle par défaut utilisé pour créer le module de chiffrement qui contient des mappages de nombreux objectifs de chiffrement par rapport aux spécifications de chiffrement et aux algorithmes recommandés.
Application	Le périmètre de l'application sélectionnée.
Nom	Le nom du module de chiffrement est ajouté avant le nom du périmètre de l'application pour éviter tout conflit avec d'autres applications du périmètre lors de la création du module. Par exemple, si vous avez créé un module avec le nom `my_crypto_module` dans le périmètre de l'application global, le nom est enregistré comme `global.my_crypto_module`.
État du cycle de vie du module de chiffrement	Le terme *cycle de vie* désigne la création, l'utilisation et la désactivation d'un module cryptographique. Défini sur **Brouillon** initialement lors de la configuration. Lors de l'utilisation du module, définissez sur **Publié**. Le modèle par défaut est automatiquement défini sur **Publié**.
Module de chiffrement parent	Le parent est renseigné automatiquement comme **column_level_encryption**.

3. Cliquez sur **Envoyer**.

Une fois l'envoi réussi, votre module de chiffrement est répertorié dans la table Modules de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avertissement :

Pour les utilisateurs de l'assistance de chiffrement héritée :

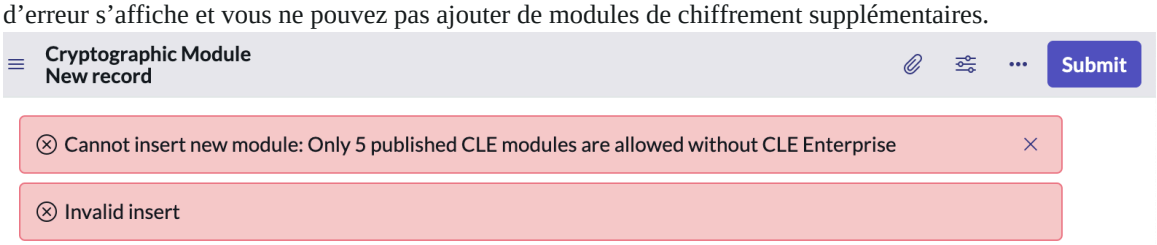
Si vous utilisez la version non entreprise de Chiffrement au niveau des colonnes, vous êtes limité à cinq modules. Si vous avez dépassé cette limite, vous recevez l'avertissement suivant :

Cette insertion dépasse le nombre de limites des modules publiés de Chiffrement au niveau des colonnes autorisées avec le produit d'abonnement. L'abonnement Entreprise à Chiffrement au niveau des colonnes est requis pour les modules supplémentaires. Veuillez contacter l'équipe de votre compte.

Une spécification cryptographique par défaut est créée avec l'objectif de chiffrement défini sur Symmetric Data Encryption/Decryption et l'algorithme en tant qu'AES 256 CBC. Sélectionnez l'algorithme pour les mises à jour.

4. Pour ouvrir les options de configuration, cliquez sur le module de chiffrement nouvellement créé.

Remarque :
Cinq modules de chiffrement au niveau des colonnes au maximum sont autorisés avant la mise à niveau vers Entreprise de Chiffrement au niveau des colonnes. Un message d'erreur s'affiche et vous ne pouvez pas ajouter de modules de chiffrement supplémentaires.



Que faire ensuite

Créer une spécification cryptographique pour Chiffrement au niveau des colonnes.

Utilisation de plusieurs modules de chiffrement

Plusieurs modules de chiffrement permettent de chiffrer les données avec plusieurs modules de chiffrement. Si chaque module a sa propre politique d'accès basée sur un rôle, par exemple, les utilisateurs ayant des rôles différents peuvent chiffrer les données sur la même table, mais ils peuvent toujours être empêchés de visualiser les données chiffrées les uns des autres.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Pourquoi et quand exécuter cette tâche

Remarque :
Seul le chiffrement sur les colonnes prend en charge plusieurs modules. Ce n'est pas le cas du chiffrement des pièces jointes. Le chiffrement en masse n'est pas disponible lors de l'utilisation de la méthode des modules de chiffrement multiples.

Vous ne pouvez pas modifier un champ à l'aide de plusieurs modules de chiffrement pour utiliser un seul module de chiffrement.

Le champ est chiffré par le module de chiffrement du premier utilisateur à saisir des données. Étant donné que le module de chiffrement est défini pour chaque enregistrement, les champs d'une liste peuvent avoir différents modules de chiffrement. Au sein d'un seul enregistrement, le champ ne peut être chiffré que par un seul module.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Créez plusieurs modules de chiffrement et une politique d'accès pour chacun d'eux.

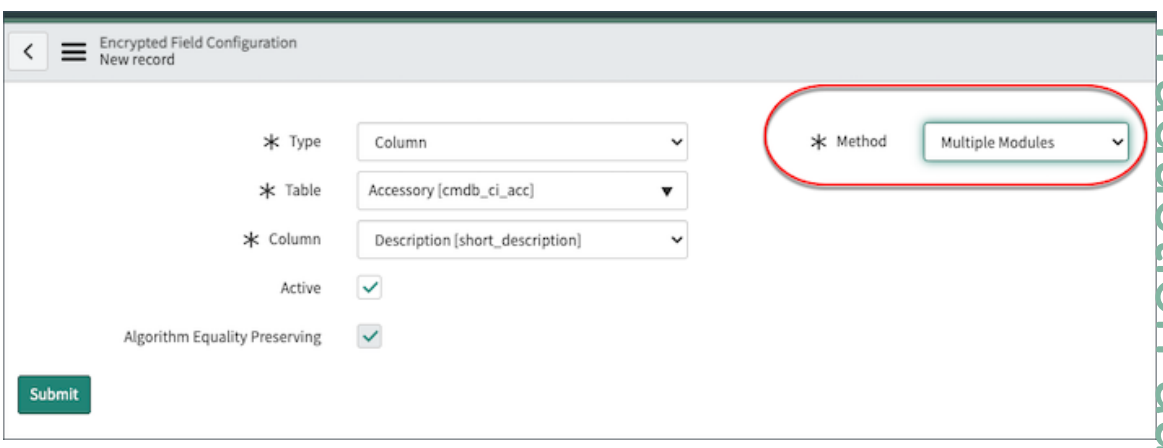
   Assurez-vous d'accorder différents rôles aux différents modules de chiffrement par le biais des politiques d'accès.

2. Accédez à la **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**.

   Si vous avez besoin de plus d'informations sur les configurations des champs chiffrés, reportez-vous à la section Définir des configurations de champs chiffrés.

3. Dans le champ **Type** , vous devez sélectionner **Colonne**.
   Le chiffrement des pièces jointes ne prend pas en charge plusieurs modules.

4. Sélectionnez **plusieurs modules** dans le champ **Méthode** .



5. Sélectionnez la **table** et la **colonne** de la table que vous souhaitez chiffrer.

6. Cliquez sur **Envoyer**.

Résultats

Les données nouvellement créées pour le champ spécifié sont chiffrées avec la clé du module correspondant. Lorsqu'un utilisateur ayant le rôle spécifié dans la politique d'accès du module A écrit dans la table spécifiée, les données sont chiffrées avec la clé du module A. Seuls les utilisateurs ayant le même rôle peuvent lire les données.

Example:

Pour chiffrer la colonne Brève description de la table Incident. Vous devez procéder comme suit :

1. Créez deux modules de chiffrement A et B.

2. Pour chaque module, créez une politique d'accès au module.

   Pour le module A, donnez accès aux utilisateurs disposant d'un rôle RH. Pour le module B, donnez un accès aux utilisateurs disposant d'un rôle de vente.

3. Créez un enregistrement de configuration de champ chiffré en spécifiant la colonne Brève description dans la table Incident et assurez-vous de sélectionner **plusieurs modules** dans le champ **Méthode** .

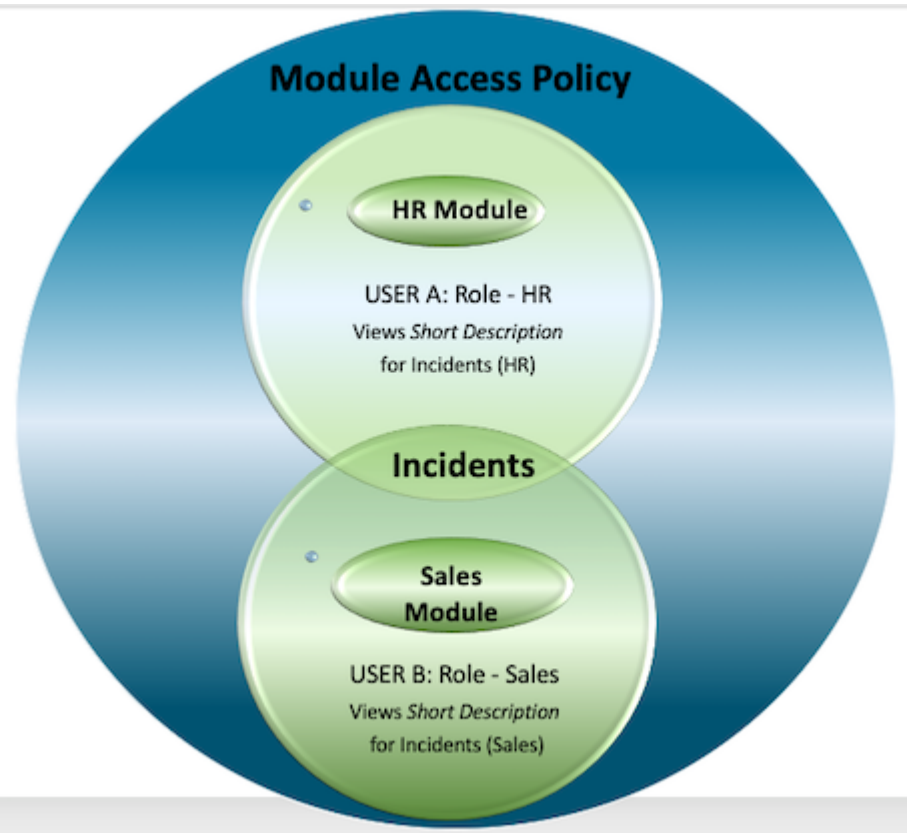
4. Faites en sorte que deux utilisateurs, l'un ayant le rôle RH (utilisateur A) et l'autre ayant le rôle commercial (utilisateur B), créent un incident avec une brève description, puis demandent aux deux utilisateurs d'examiner la liste des incidents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La description brève de l'incident créé par l'utilisateur disposant du rôle RH est chiffrée par la clé du module A. De même, la brève description de l'incident créé par l'utilisateur disposant du rôle commercial est chiffrée par la clé du module B.

Bien que tous les utilisateurs disposant des rôles RH et Ventes aient accès aux incidents, seul un utilisateur disposant du rôle RH peut déchiffrer et afficher la brève description de ces incidents créés par l'utilisateur A, qui avait le rôle RH. De même, seuls les utilisateurs disposant du rôle commercial peuvent déchiffrer et afficher les brèves descriptions des incidents créés par l'utilisateur B, qui avait le rôle commercial.



Créer une spécification cryptographique pour Chiffrement au niveau des colonnes

Après avoir créé un module de chiffrement, accédez à la spécification de chiffrement correspondante pour définir l'algorithme.

Avant de commencer

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf_admin et security_admin ou admin

Pourquoi et quand exécuter cette tâche

Cette procédure décrit les options disponibles avec Chiffrement au niveau des colonnes (CLE) avec le système de base et les options de configuration supplémentaires qui deviennent disponibles avec Entreprise de Chiffrement au niveau des colonnes la fonctionnalité Entreprise de Chiffrement au niveau des colonnes (CLE_Ent). Cette fonctionnalité est disponible avec un abonnement payant. Consultez la rubrique Offre groupée d'abonnements pour Encryption and Key Management pour connaître les fonctionnalités et options prises en charge disponibles avec chaque offre. Pour Activer Chiffrement au niveau des colonnes – Entreprise plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Une spécification cryptographique est créée par le système lorsque vous créez un module cryptographique pour le chiffrement au niveau des colonnes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

.

Procédure

1. Accédez à la **Sécurité de système** > **Modules de chiffrement de champ** > **Tout**.
2. Sélectionnez le module de chiffrement pour ouvrir les options de configuration.
   Les informations sur le module de chiffrement sont affichées en haut de l'écran. Une spécification de chiffrement symétrique de chiffrement/déchiffrement des données est créée automatiquement avec un algorithme AES 256 CBC.
3. Sélectionnez la spécification de chiffrement dans la table pour ouvrir la définition de l'algorithme.
   Pour Entreprise de Chiffrement au niveau des colonnes reportez-vous à la section Configurer des algorithmes avancés pour Chiffrement au niveau des colonnes – Entreprise.
4. Cliquez sur **Suivant** pour accéder au cycle de vie de la clé.

Que faire ensuite

Effectuez l'une des opérations suivantes :

- Sélectionnez une entrée dans la table Cycle de vie de la clé pour définir le comportement du cycle de vie de la clé. Consultez Configurer les états clés du cycle de vie pour en savoir plus sur la définition du cycle de vie de la clé.
- Cliquez sur **Suivant** pour créer une clé cryptographique. Pour obtenir des détails sur ce processus, consultez Générer une clé cryptographique ServiceNow.

Configurer des algorithmes avancés pour Chiffrement au niveau des colonnes – Entreprise

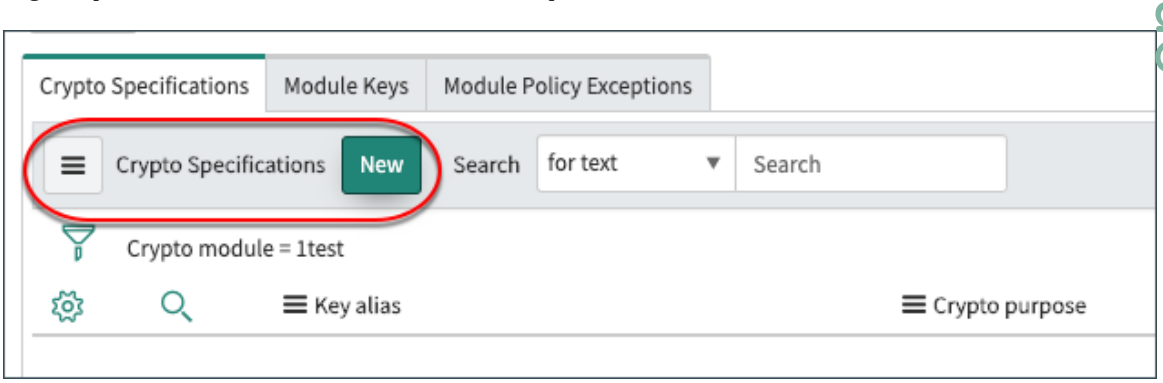
Créez une spécification cryptographique pour définir l'algorithme d'un module cryptographique. Personnalisez les spécifications de chiffrement avec des options avancées disponibles pour Entreprise de Chiffrement au niveau des colonnes.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Dans l'onglet **Spécifications de chiffrement (#),** cliquez sur **Nouveau**.



2. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de définition d'algorithme

Champ	Description
Module de chiffrement	Le nom du module de chiffrement sélectionné est renseigné.
Objectif de chiffrement	La valeur est **Chiffrement/déchiffrement symétrique des données** pour Entreprise de Chiffrement au niveau des colonnes.
Algorithme	La valeur est **AES** pour Entreprise de Chiffrement au niveau des colonnes.
Mode d'opération	La valeur est **CBC** pour Entreprise de Chiffrement au niveau des colonnes.
Taille	Les valeurs possibles sont **256** et **128**. **Remarque :** La taille 256 bits est la plus sécurisée pour le chiffrement et est utilisée pour le chiffrement/déchiffrement symétrique des données pour Entreprise de Chiffrement au niveau des colonnes.
Préservation de l'égalité	Option permettant d'activer le chiffrement déterministe. **Remarque :** La sélection de cette option signifie que la valeur chiffrée d'un champ doit être la même lorsque la valeur du champ reste la même. Option permettant d'activer le **chiffrement/déchiffrement symétrique des données** avec **AES** en mode **CBC (Cipher Block Chaining).**
Intégrité	Option permettant d'assurer l'intégrité de l'opération GCM et ne s'applique pas aux Entreprise de Chiffrement au niveau des colonnes fonctionnalités.

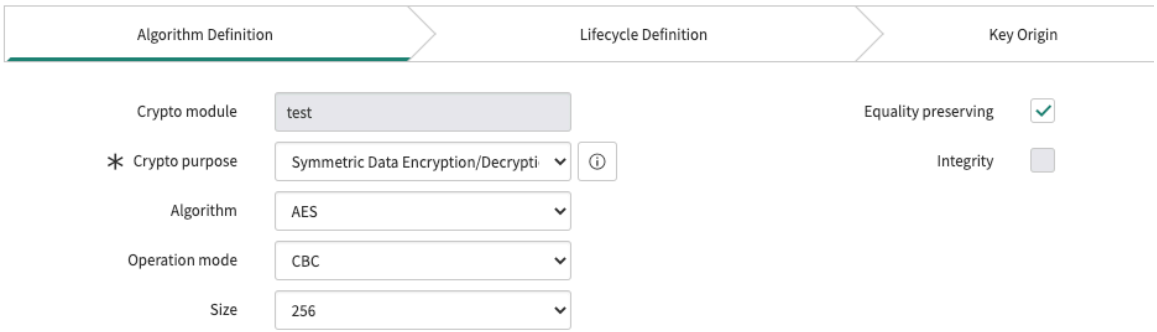
3. Cliquez sur **Envoyer**.

L'exemple suivant montre le chiffrement AES CBC-256. Lorsque Entreprise de Chiffrement au niveau des colonnes la valeur est active et que le module parent est column_level_encryption, seul le chiffrement/déchiffrement symétrique des données AES CBC-256 s'applique en

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

tant qu'objectif de chiffrement. Consultez Objectif cryptographique, algorithmes et informations clés pour en savoir plus.



Que faire ensuite

Effectuez l'une des opérations suivantes :

- Sélectionnez une entrée dans la table Cycle de vie de la clé pour définir le comportement du cycle de vie de la clé. Consultez Configurer les états clés du cycle de vie pour en savoir plus sur la définition du cycle de vie de la clé.
- Cliquez sur **Suivant** pour créer une clé cryptographique. Reportez-vous à l'une des tâches suivantes pour la génération de clés :
  - Générer une clé cryptographique ServiceNow.
  - Configurer les propriétés des clés fournies par le client.
  - Importer la paire de clés d'encapsulation/de désencapsulation.

Utilisation des clés fournies par le client avec Chiffrement au niveau des colonnes – Entreprise

Vous pouvez utiliser votre propre clé fournie par le client au lieu des clés générées par le ServiceNow® système.

Important :
Ces rubriques ne s'appliquent qu'aux instances utilisant Entreprise de Chiffrement au niveau des colonnes, qui n'est disponible qu'avec le module d'extension `com.glide.now.platform.encryption` . Consultez Activer Chiffrement au niveau des colonnes – Entreprise pour plus d'informations sur l'obtention de ce module d'extension.

Avec Chiffrement au niveau des colonnes Entreprise, vous pouvez utiliser vos propres clés pour le chiffrement. Les administrateurs ont le choix d'utiliser ServiceNow® les clés fournies ou vos propres clés fournies par le client (CSK) pour le chiffrement sur le Now Platformfichier .

Important :
Pour utiliser l'option de clé fournie par le client, vous devez disposer de votre propre clé cryptographique.

Une fois que vous avez votre clé, vous pouvez l'utiliser sur vos instances en suivant ces étapes.

1. **Configurer les propriétés des clés fournies par le client**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il existe trois propriétés système qui définissent la taille, l'algorithme de remplissage et la période de validité de la paire de clés RSA encapsulée. Examinez ces propriétés et ajustez leurs valeurs si la valeur par défaut ne correspond pas à vos besoins.

2. **Encapsuler votre clé fournie par le client**

   Utilisez un outil cryptographique pour encapsuler votre clé, comme OpenSSL pour encapsuler la clé symétrique à utiliser pour le chiffrement avec la clé publique téléchargée.

Configurer et charger votre clé fournie par le client

Chargez votre clé emballée fournie par le client et configurez le module de chiffrement pour commencer à utiliser votre clé pour le chiffrement sur votre instance.

Configurer les propriétés des clés fournies par le client

Si le module d'extension est activé, vous pouvez utiliser les propriétés système pour définir le remplissage des clés, la taille de la Entreprise de Chiffrement au niveau des colonnes paire de clés éphémères et la période de validité de vos clés fournies par le client.

Entreprise de Chiffrement au niveau des colonnes avec la gestion des clés vous permet de gérer le cycle de vie complet de vos clés de chiffrement des données. En option, vous pouvez échanger en toute sécurité des clés de chiffrement de données générées au sein de votre environnement.

Chiffrement de plateforme avec gestion des clés vous permet de gérer le cycle de vie complet de vos clés de chiffrement des données. En option, vous pouvez échanger en toute sécurité des clés de chiffrement de données générées au sein de votre environnement.

Propriétés système pour définir les attributs de paire de clés

Lorsque vous fournissez votre propre clé, vous devez l'envelopper avec la clé publique RSA. Trois propriétés définissent la taille, l'algorithme de remplissage et la période de validité de la paire de clés RSA encapsulée :

- *glide.kmf.ephemeral_key.key_padding* Contrôle le schéma de remplissage de clé pour la clé éphémère. Le schéma par défaut est OAEP SHA256, mais SHA1 est également pris en charge.
- *glide.kmf.ephemeral_key.key_size* Contrôle la taille de clé de la paire de clés éphémères. La valeur par défaut est de 4096 bits, mais 2048 bits sont également pris en charge.
- *glide.kmf.ephemeral_key.key_validity_period* Définit la période de validité de la paire de clés éphémères. La valeur par défaut est de deux heures.

Une fois la clé de chiffrement des données importée dans l'instance, une clé d'encapsulation sécurisée protège les nouvelles clés de module sur l'instance. La clé d'encapsulation est une clé de chiffrement de clé d'instance (IKEK) générée par un module de sécurité matériel (HSM) sur SafeNet KeySecure. Pour plus de détails, reportez-vous à la section Clés de niveau instance dans Key Management Framework Types de clés.

Poursuivez vers Encapsuler votre clé fournie par le client.

Encapsuler votre clé fournie par le client

Encapsulez la clé symétrique à utiliser pour le chiffrement avec la clé publique téléchargée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Remarque :
Cette procédure décrit les options disponibles avec KMF le système de base et les options à utiliser avec Entreprise de Chiffrement au niveau des colonnes la fonctionnalité. Entreprise de Chiffrement au niveau des colonnes La fonctionnalité n'est disponible que lorsque le module d'extension `com.glide.now.platform.encryption` est actif. Pour Activer Chiffrement au niveau des colonnes – Entreprise plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Certaines des étapes décrites dans ce document nécessitent l'utilisation d'un outil de chiffrement installé sur votre appareil local. Les exemples de cette tâche utilisent l'outil OpenSSL. Pour plus d'informations sur cet outil, reportez-vous à la section https://www.openssl.org . Si vous utilisez d'autres outils cryptographiques, tels que LibreSSL ou GnuTLS, reportez-vous à la documentation de ces produits pour connaître les étapes similaires.

- Modifiez les propriétés facultatives qui contrôlent la taille, l'algorithme de remplissage et la période de validité de la clé. Consultez Configurer les propriétés des clés fournies par le client.
- Vous devez disposer de votre clé symétrique (. BIN) pour le chiffrement.

Important :
Votre clé doit être au format binaire. Si un autre format est utilisé, la validation d'un jeton a échoué. Veuillez attacher à nouveau le jeton non modifié.Un message d'erreur s'affiche.

- Vous devez disposer d'un outil cryptographique pour encapsuler votre clé. Cet exemple utilise OpenSSL 1.1.

Rôle requis : sn_kmf.cryptographic_manager ou sn_kmf.admin

Procédure

1. Accédez à la **Tout** > **Key Management Framework** > **Modules de chiffrement** > **Tout**.
2. Sélectionnez le module de chiffrement que vous avez créé pour la clé fournie par le client dans la liste connexe Spécifications de chiffrement.
3. Vous serez dirigé vers l'étape **de création de clé** .
4. Si vous n'avez pas encore téléchargé la clé d'encapsulation, cliquez sur le lien pour télécharger le fichier `token_publickey<id>.zip` et l'enregistrer au même emplacement que votre clé.

   Remarque :
   Ne renommez pas le fichier `token_publickey<id>` téléchargé.

5. Décompressez le fichier sur votre réseau local.
   Le fichier zip contient deux fichiers, un jeton d'importation et une clé publique . Certificat PEM .
   Encapsulez votre clé symétrique avec la clé publique pour la chiffrer.
6. Copiez le nom du fichier `token_publickey` dans votre presse-papiers.
7. À partir d'une ligne de commande, utilisez le nom du fichier `token_publickey` copié pour ouvrir le dossier des fichiers décompressés en tant qu'espace réservé pour la clé enveloppée.
8. Modifiez ce script en remplaçant les exemples par les noms de vos fichiers de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
"downloads user.name$ cd token_publickey_<token>
openssl pkeyutl -encrypt -pubin -inkey publickey_<keyname>.PEM
-in <keyname.bin>
-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt
 rsa_oaep_md:sha<128 or 256> "
```

Passez en revue les commandes d'emballage de clé dans le tableau suivant pour plus d'informations.

Commandes d'emballage de clé

Directions	Commande	Exemple
Ouvrez le répertoire de fichiers dans lequel vous avez téléchargé le jeton d'encapsulation.	`cd`	token_publickey123456789 CD
Collez le nom de la clé publique. Certificat PEM .	`openssl pkeyutl -encrypt -pubin -inkey`	publickey_586798643ffff. PEM
Collez le nom de votre clé ici.	`-in`	mykey.bin
Entrez la commande <-out> et spécifiez si la clé est 128 bits ou 256 bits.	`-out wrapped_key_material -pkeyopt rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256`	N/A

9. Exécutez la commande.
   Un message système affiche `token_publickey_<numéro de clé>`. La clé sera générée et un fichier *`wrapped_key_material`* ajouté au répertoire.
10. Chargez la clé emballée.

Que faire ensuite

Retournez à Configurer et charger votre clé fournie par le client pour charger votre clé enveloppée.

Configurer et charger votre clé fournie par le client

Vous pouvez utiliser votre propre clé fournie par le client au lieu des clés générées par le ServiceNow® système.

Avant de commencer

Rôles requis : security_admin, sn_kmf.cryptographic_manager

Si vous ne fournissez PAS vos propres clés, vous n'avez pas besoin d'effectuer cette procédure. Pour créer un module cryptographique avec ServiceNow® des clés, accédez à Créer un module cryptographique ou Créer un module cryptographique pour Chiffrement au niveau des colonnes.

Remarque :
Cette procédure ne s'applique qu'aux Entreprise de Chiffrement au niveau des colonnes fonctionnalités. Consultez Activer Chiffrement au niveau des colonnes – Entreprise pour plus d'informations.

Important :
Vous ne pouvez pas révoquer une clé fournie par le client.

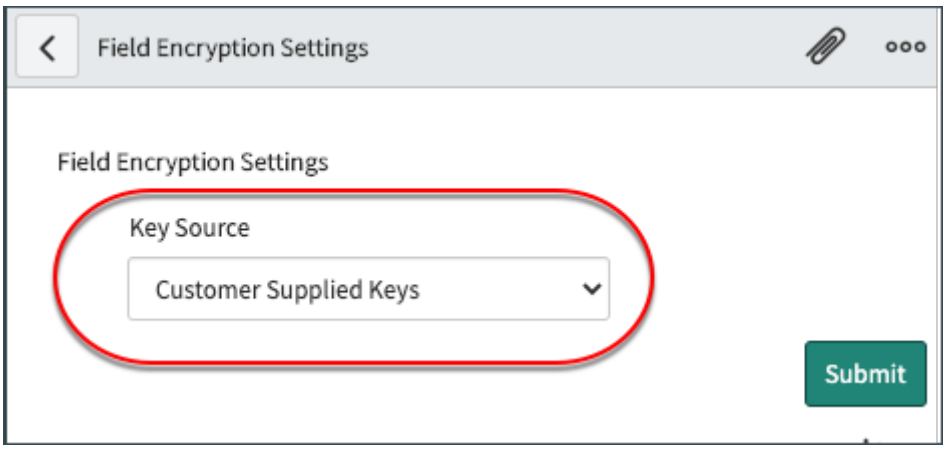
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

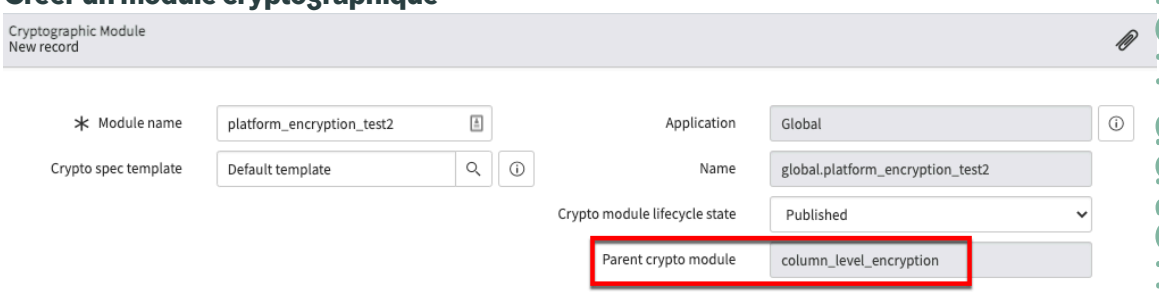
1. Accédez à la **Tout** > **Sécurité de système** > **Paramètres de Chiffrement de champ** et vérifiez que **l'option Clés fournies par le client** est sélectionnée.

Sélection de la source de clé



2. Sélectionnez **Soumettre**.
3. Retourner à **Sécurité de système** > **Modules de chiffrement de champ** > > **Créer**.

Créer un module cryptographique



4. Renseignez le formulaire Module de chiffrement comme suit :

Champs du module de chiffrement

Champ	Description
Nom du module	Entrez un nom pour le module.
Modèle de spécification de chiffrement	Le modèle de chiffrement par défaut est sélectionné.
Nom	Se remplit automatiquement en fonction du nom du module et ajoute le champ d'application au nom pour garantir quelle application est appliquée. Dans ce cas, le périmètre global est appliqué.
État du cycle de vie du module de chiffrement	Sélectionner **Publié** pour activer le module de chiffrement.

Traduction automatique

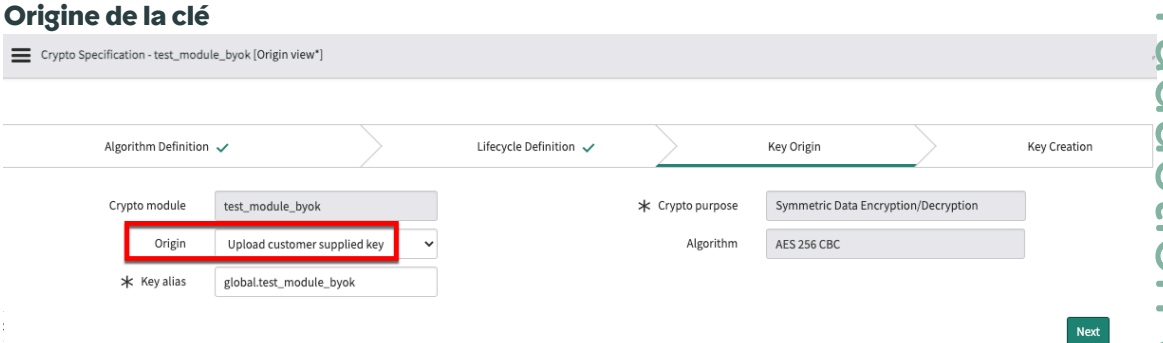
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Module de chiffrement parent	Le **column_level_encryption** de module parent est sélectionné automatiquement lors de l'utilisation des clés et des modules de chiffrement fournis par le client.

5. Sélectionnez **Soumettre**.
6. Sélectionnez le module de chiffrement nouvellement créé dans la table.
   Dans la liste connexe **Spécifications de chiffrement** , sélectionnez l'alias de clé généré automatiquement avec l'algorithme AES 256 CDB.

   Le système remplit automatiquement l'objectif de chiffrement et l'algorithme pour CLE et passe à l'étape **d'origine** de la clé.
7. Notez que Télécharger la **clé fournie par le client** est l'origine et que l'alias de **clé** est déjà renseigné.

Origine de la clé

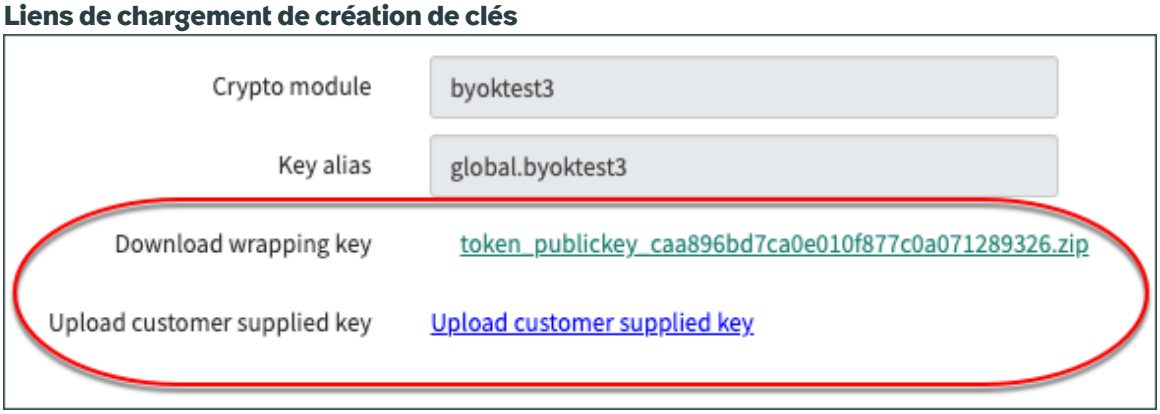


8. Sélectionnez **Suivant** pour passer à l'étape **de création de clé** .

   Il y a deux liens :

   - **Télécharger la clé encapsulée** télécharge la clé dans un fichier zip contenant un jeton d'importation et un certificat de clé publique. Fichier PEM . Utilisez le jeton d'importation pour vérifier que l'encapsulation de clé est correcte conformément aux spécifications de sécurité de l'instance. Utilisez le certificat de clé publique . Fichier PEM pour envelopper votre clé fournie par le client en toute sécurité avant de la charger avec le jeton.
   - **Télécharger la clé fournie par le client** ouvre l'explorateur de fichiers pour sélectionner le jeton et la clé chiffrée que vous avez encapsulés.

Liens de chargement de création de clés

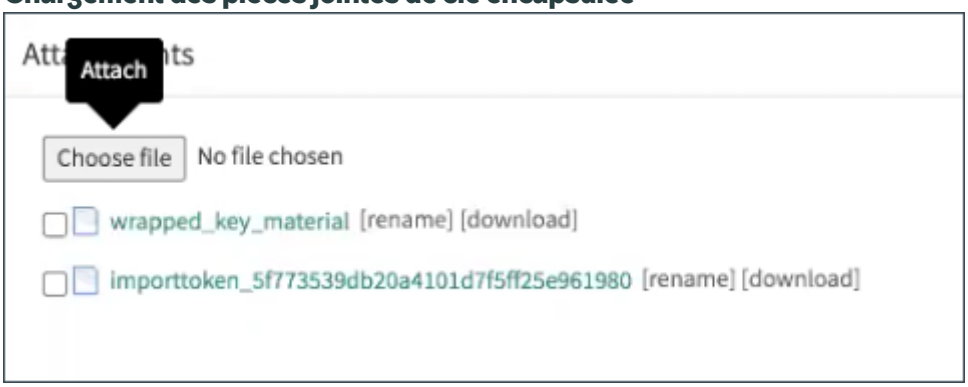


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Sélectionnez **Télécharger la clé d'encapsulation** pour enregistrer le jeton.
   Enregistrez le jeton au même emplacement de destination que celui où la clé est enregistrée sur votre système.
   Ne renommez pas le jeton téléchargé.
10. Exécutez la commande BYOK sur un terminal pour envelopper la clé.
    Pour plus d'informations, référez-vous à Encapsuler votre clé fournie par le client.
11. Sélectionnez **Télécharger la clé fournie par le client**.
12. Sélectionnez **Parcourir** pour sélectionner les deux fichiers, la clé enveloppée et le fichier de jeton.
    La fenêtre Pièces jointes affiche les deux fichiers.

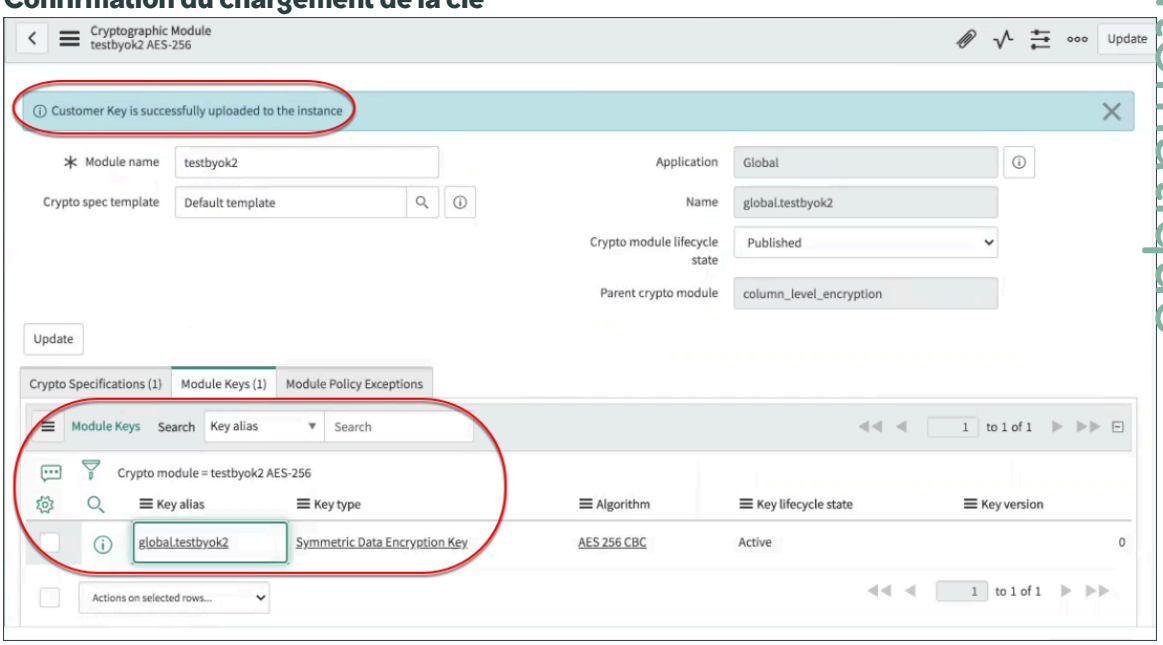
Chargement des pièces jointes de clé encapsulée



Sélectionnez un fichier à supprimer et à recharger, si nécessaire.

13. Sélectionnez **OK**.
    Vous revenez à l'écran Module cryptographique. Un message de confirmation s'affiche pour le chargement réussi de la clé client. La clé est également répertoriée dans la liste connexe des clés de module.

Confirmation du chargement de la clé



Que faire ensuite

Maintenant que vous avez terminé la configuration de votre module de chiffrement avec votre clé fournie par le client, passez à Créer une politique d'accès au module

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chiffrer les champs et les pièces jointes

Après avoir créé vos modules de chiffrement, créez des configurations de champs chiffrés et indiquez s'il faut chiffrer un champ d'une table ou chiffrer les pièces jointes.

Comment chiffrer des champs

Remarque :
Les champs chiffrés ne sont pas audités de par leur conception. Ce comportement n'est pas configurable.

1. Spécifier la source de clé : clés générées par le système ou clés fournies par votre client (Apporter votre propre clé) dans **Sécurité de système** > **Paramètres de Chiffrement de champ**.
2. Après avoir spécifié la source de clé, créez un nouveau module de chiffrement ou utilisez un module de chiffrement existant. Commencez par Créer un module cryptographique pour obtenir des instructions.

   Remarque :
   Si vous utilisez des clés fournies par le client, suivez les instructions des sections Créer un module cryptographique pour Chiffrement au niveau des colonnes et Configurer les propriétés des clés fournies par le client.

3. Créez une configuration de champ chiffré, dans laquelle vous spécifiez la table sur laquelle le chiffrement est effectué et la colonne de la table ou les pièces jointes de la table à chiffrer. Voir Définir des configurations de champs chiffrés pour commencer.

Remarque :
Reportez-vous à cette section Exemples d'Enterprise de Chiffrement au niveau des colonnes qui illustre comment chiffrer des champs et des pièces jointes à l'aide de clés fournies par le client.

Définir des configurations de champs chiffrés

Configurez les tables, colonnes ou pièces jointes que le système chiffre à l'aide d'un module de chiffrement préconfiguré.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager et security_admin ou élever le rôle au rang d'administrateur de sécurité.

Pourquoi et quand exécuter cette tâche
Assurez-vous que vous êtes dans le périmètre de l'application correct afin de pouvoir voir les tables de ce périmètre.

Seuls les utilisateurs ayant accès au module de chiffrement utilisé dans cette configuration peuvent lire les données dans la colonne de table chiffrée ou accéder à la pièce jointe.

- Si un utilisateur dispose d'un accès en écriture mais pas d'un accès en lecture, le champ s'affiche en mode de modification et les données saisies s'affichent sous forme d'astérisques.
- Si un utilisateur dispose d'un accès en lecture mais pas d'un accès en écriture, le champ affiche les données déchiffrées en mode lecture seule.
- Si un utilisateur dispose de tous les accès, les deux fonctionnalités de lecture/écriture sont disponibles dans le champ chiffré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voir Créer un module cryptographique ou Créer un module cryptographique pour Chiffrement au niveau des colonnes pour commencer.

Important :

Après avoir chiffré une colonne, toute nouvelle donnée insérée dans la colonne est chiffrée automatiquement. Toutefois, les données qui existaient dans la colonne avant que le chiffrement ne soit actif ne sont pas automatiquement chiffrées.

Pour chiffrer des données qui existaient avant le chiffrement de la colonne, vous devez exécuter une tâche de chiffrement en masse distincte. Pour en savoir plus sur le chiffrement en masse, consultez Exécuter le chiffrement ou le déchiffrement en masse.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés** > **Nouveau**.
2. Sélectionnez **Nouveau**.
3. Renseignez le formulaire.

Champ	Description
Type	**Colonne** pour chiffrer une colonne de table ou **Pièce jointe** pour chiffrer toutes les pièces jointes d'une table. Les types de données chiffrées sont les suivants : ○ Texte de chaîne (UTF-8 complet) ○ Pièces jointes ○ Date, Date/Heure : **Remarque :** Vous pouvez créer des configurations de champs chiffrés pour chiffrer les champs Date et Date/Heure existants. Vous pouvez ajouter une nouvelle configuration de chiffrement à une table parente uniquement. Vous ne pouvez pas ajouter une nouvelle configuration de chiffrement à une table enfant. ○ URL ○ Entreprise de Chiffrement au niveau des colonnes prend également en charge les types de champs suivants : ▪ HTML ▪ Journal ▪ Traduit
Table	Table dont les champs ou les pièces jointes doivent être chiffrés.
Colonne	Colonne (champ) à chiffrer si **vous avez sélectionné** colonne comme type.
Actif	Sélectionnez cette option pour marquer la configuration comme active. Désélectionnez si la configuration n'est pas encore utilisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Module de chiffrement	Module de chiffrement auquel la configuration des champs chiffrés s'applique.
Méthode	Sélectionnez **Module unique** pour définir la configuration des champs dans un module. Sélectionnez **plusieurs modules** pour un accès basé sur les rôles qui s'étend sur plusieurs modules de chiffrement. **Module unique** Utilisez cette option pour chiffrer toutes les pièces jointes à l'aide d'un seul module. Vos utilisateurs doivent accéder à ce module, sinon ils ne sont pas en mesure de charger des pièces jointes. **Modules multiples** Utilisez cette option pour permettre aux utilisateurs de choisir un module lors du chargement des pièces jointes. Les utilisateurs ayant accès à au moins un module peuvent sélectionner un module à utiliser pour le chiffrement. Les utilisateurs n'ayant pas accès au module peuvent télécharger des pièces jointes non chiffrées.
Chiffrement de l'algorithme : conservation [Lecture seule]	Indique si le module de chiffrement que vous avez sélectionné est déjà configuré pour prendre en charge le chiffrement non déterministe. Cela signifie que si les mêmes données sont chiffrées plus d'une fois, le cryptage est différent à chaque fois.

4. Sélectionnez **Soumettre**.

Accès aux scripts pour les modules de chiffrement

Des scripts peuvent être exécutés pour accéder à une politique de module de chiffrement à des fins de chiffrement.

Pour Key Management Framework, les politiques peuvent être basées sur des scripts. Lorsqu'une politique d'accès est déclenchée pour l'accès aux scripts, le script back-end peut exécuter les actions de politique du module à partir du script.

Les modules de chiffrement peuvent prendre en charge un ou plusieurs objectifs de chiffrement, tels que le déchiffrement asymétrique des données et le déchiffrement symétrique des données. Chaque finalité cryptographique nécessite la génération d'une clé de chiffrement et la définition d'une finalité cryptographique.

Lors de l'exécution d'une demande de script de chiffrement, prenez en compte les éléments suivants :

- La finalité de chiffrement référencée doit être définie dans le module de chiffrement.
- Une clé générée active doit exister pour le module de chiffrement.
- Le type de politique d'accès au module doit être défini sur **script**.

Vérifier la version du script

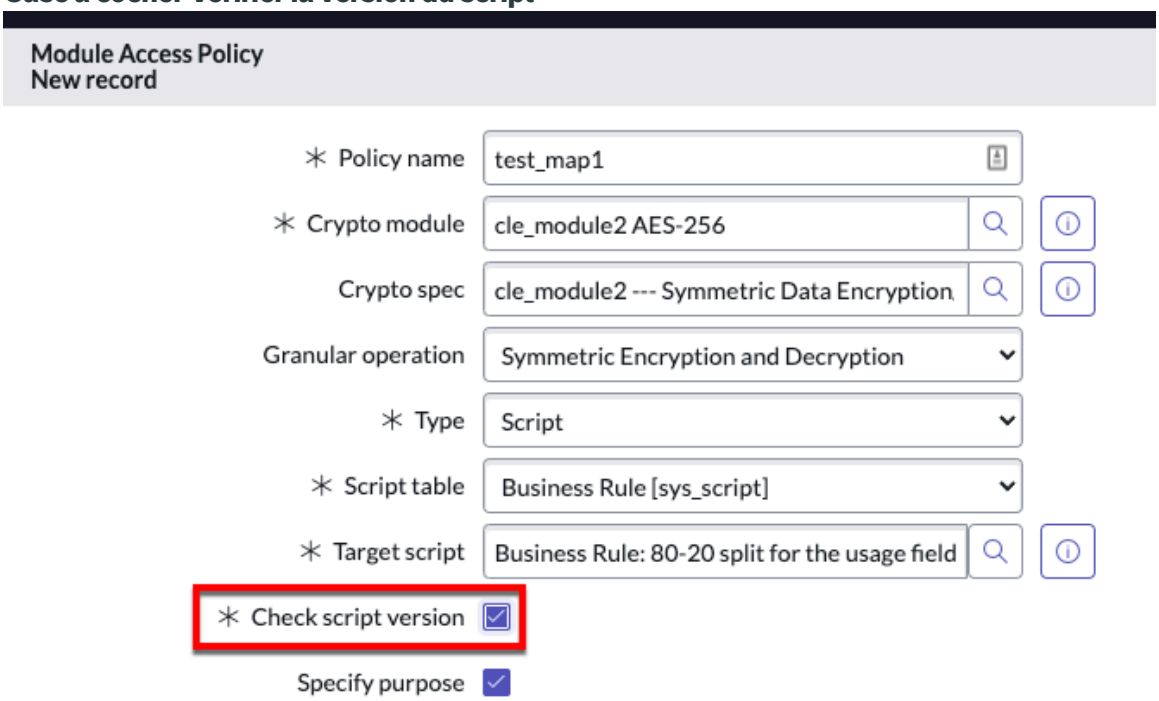
Lors de la création d'une politique d'accès au module définie sur le type de script, une option est disponible pour valider l'intégrité de la version de script à laquelle vous accédez. Seule la version affectée du script est autorisée à accéder aux modules de chiffrement. Lorsque la case **Vérifier la version du script** est cochée dans la politique d'accès au module,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à chaque fois que le script est exécuté, le système effectue une comparaison de version. Si le script a été modifié, l'utilisateur en est informé.

Case à cocher Vérifier la version du script



Configurer l'accès des scripts aux données chiffrées

Exécuter un script pour exécuter la politique du module de chiffrement à des fins de chiffrement. Un accès spécifique en lecture (déchiffrer/désencapsuler) ou en écriture (chiffrer, encapsuler) peut être défini en fonction de la granularité opérationnelle de la politique d'accès du module.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager

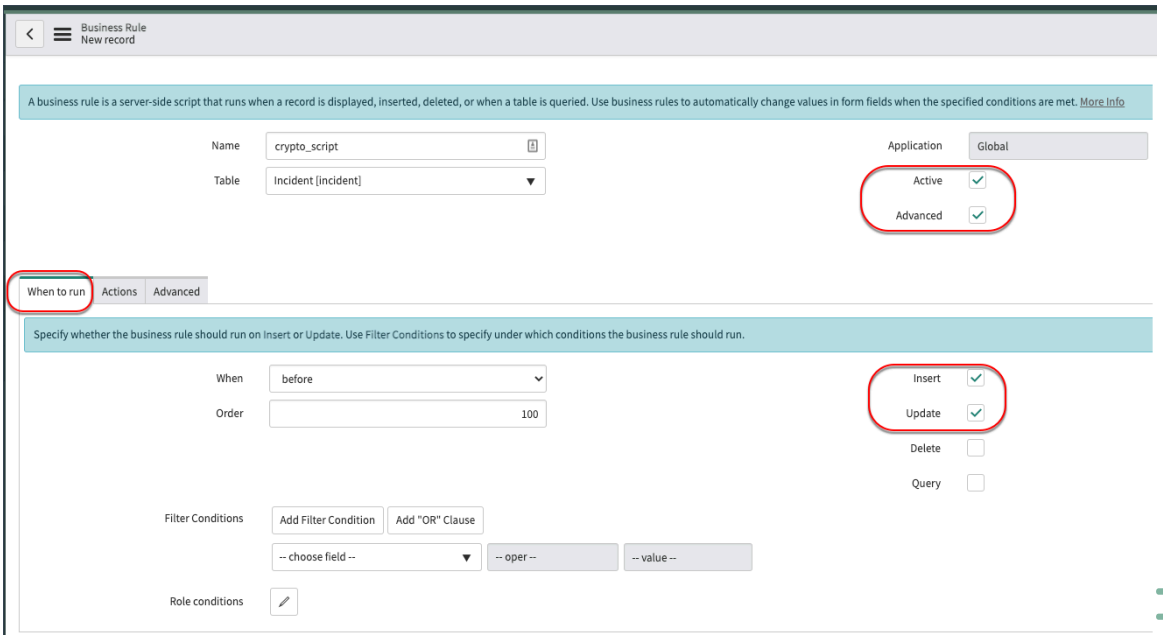
Pourquoi et quand exécuter cette tâche
Les règles métier et les includes de script sont des exemples d'utilisation. Cette procédure utilise un script pour les règles métier.

Procédure

1. Créez un module cryptographique avec l'algorithme de chiffrement/déchiffrement symétrique des données. Consultez Créer un module cryptographique pour plus de détails. L'accès spécifique aux données ou à la pièce jointe est contrôlé par une politique d'accès au module ayant les caractéristiques suivantes :
   - Chiffrement symétrique : le script est capable de chiffrer les données, mais ne peut pas les déchiffrer.
   - Déchiffrement symétrique : le script est capable de déchiffrer les données chiffrées téléchargées ou les pièces jointes, mais ne peut pas chiffrer les données ou les pièces jointes.
   - Chiffrement et déchiffrement symétriques : le script est capable de chiffrer et de déchiffrer des données ou des pièces jointes.
2. Accédez à la **Définition du système** > **Règles métier**.
3. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Remplissez le formulaire dans l'onglet **Quand exécuter** et entrez le script dans l'onglet **Avancé** :

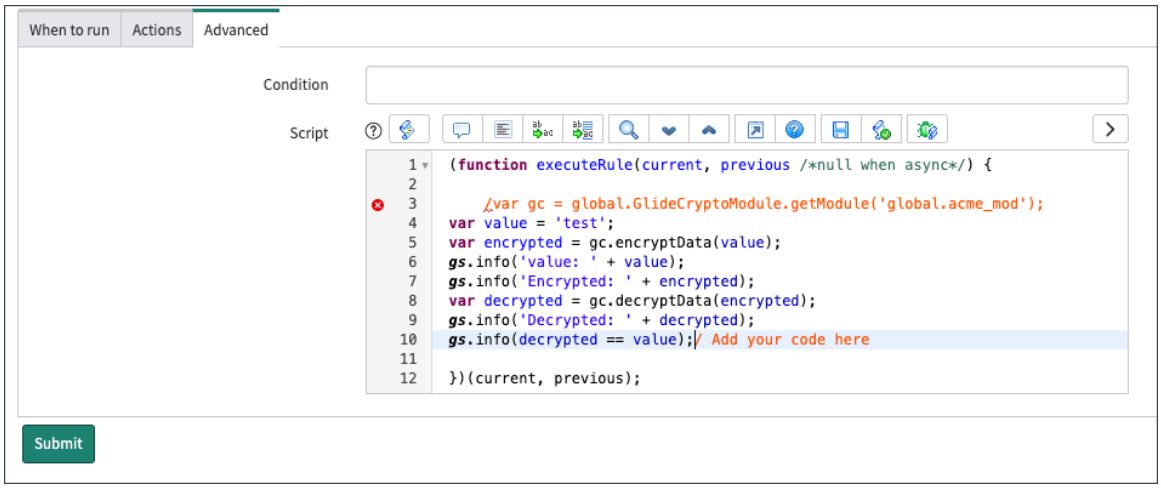
Champs de règle métier

Champ	Description
Nom	Saisissez un nom pour la règle métier.
Table	Sélectionnez **Incident [incident]** dans la liste déroulante.
Application	**Global** est sélectionné par défaut.
Actif	Marquez la règle comme **active.**
Avancés	Cochez cette case pour afficher les options avancées.
Onglet Quand exécuter	Dans l'onglet **Quand exécuter** , activez les champs **Insérer** et **Mettre à jour** .

Onglet Avancé	Dans l'onglet **Avancé** , collez le texte de script suivant à la ligne 3 :
	`//`
	`var gc =`
	`global.GlideCryptoModule.getModule('global.acme_mod');`
	`var value = 'test';`
	`var encrypted = gc.encryptData(value);`
	`gs.info('value: ' + value);`
	`gs.info('Encrypted: ' + encrypted);`
	`var decrypted = gc.decryptData(encrypted);`
	`gs.info('Decrypted: ' + decrypted);`
	`gs.info(decrypted == value);`
	Remarque : Pour plus d'informations, reportez-vous à l'image « Onglet Règles métier avancées ».

Traduction automatique

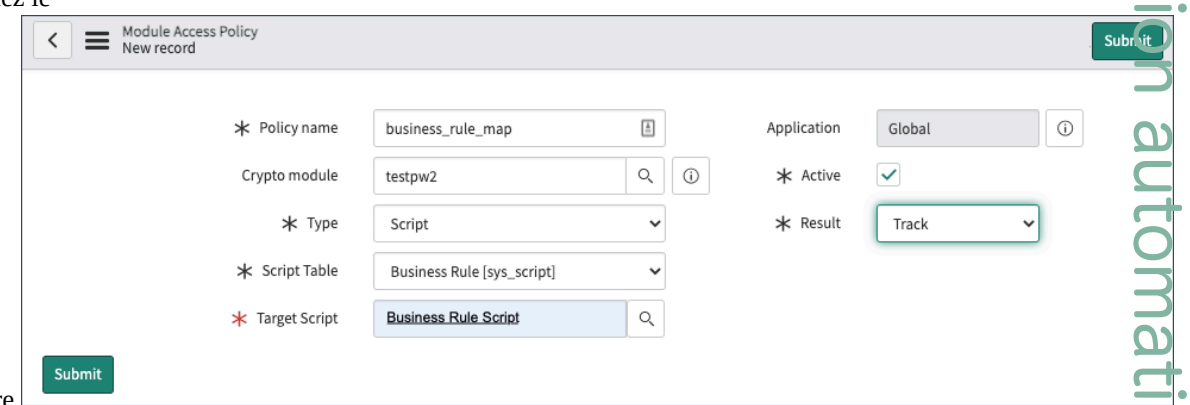
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Envoyer**.
6. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tous**.

> **Remarque :**
> Pour en savoir plus, reportez-vous à Créer une politique d’accès au modulela section .

7. Cliquez sur **Nouveau**.
8. Renseignez le formulaire.



Champs Politiques d’accès au module

9. Cliquez sur **Envoyer**.
   La politique d’accès au module pour le script est maintenant disponible dans le système.

Afficher les demandes d’utilisation du module de chiffrement refusées

Affichez les modules de chiffrement qui rejettent les demandes de chiffrement effectuées par les scripts en raison de mécanismes de chiffrement non pris en charge.

Avant de commencer
Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche
Les modules de chiffrement peuvent prendre en charge un ou plusieurs objectifs de chiffrement, tels que le déchiffrement asymétrique des données et le déchiffrement symétrique des données. Les données chiffrées ne sont accessibles que sur la base de la politique d’accès du module. Si un script tente d’utiliser un module de chiffrement à des fins non définies dans le module, le script ne peut pas accéder aux données chiffrées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

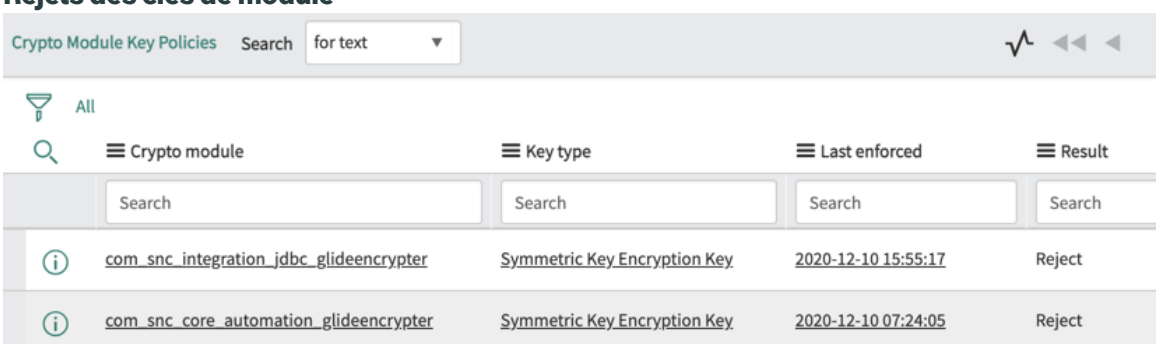
Dans l'exemple suivant, un objectif de chiffrement a été affecté à un module de chiffrement, mais aucune clé n'a jamais été générée pour celui-ci.

Procédure

Accédez à la **Tout** > **Gestion des clés** > **Politiques de clé de module** > **Rejets des clés de module**.

Une liste des modules de chiffrement qui ont rejeté des demandes s'affiche ainsi que la clé de chiffrement utilisée dans le script correspondant.

Rejets des clés de module



Remarque :
Si un script différent tente d'utiliser le même module de chiffrement avec le même type de clé, la valeur des dernières mises à jour **appliquées** . Une autre ligne n'est pas générée.

Dans cet exemple, à 2020-02-10_15:55:17, le premier module a rejeté une demande car la clé du module1 est compromise. À 2020-02-10_07:24:05, le deuxième module a rejeté une demande car la clé du deuxième module est suspendue.

Pour accorder aux scripts l'autorisation d'utiliser le module de chiffrement lors de leur prochaine exécution, créez une politique d'accès au module pour le chiffrement des scripts. Pour plus d'informations, référez-vous à Configurer l'accès des scripts aux données chiffrées.

Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse

Planifiez l'exécution des tâches de chiffrement, de déchiffrement et de nouvelle saisie au moment le plus approprié pour vous.

Avant de commencer

Les tâches de chiffrement, de déchiffrement et de nouvelle saisie peuvent demander beaucoup de temps et de ressources, envisagez donc de les planifier en dehors des heures de pointe. Assurez-vous également que l'utilisateur qui planifie la tâche dispose de l'accès approprié pour chaque tâche.

Rôle requis : sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Le chiffrement et le déchiffrement en masse sont également disponibles à partir du formulaire Configurations des champs chiffrés. Consultez les Exécuter le chiffrement ou le déchiffrement en masse pour obtenir les instructions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Paramètres de sécurité élevée** > **Tâches de Sécurité**.
2. Cliquez sur **Nouveau**.
3. Remplissez le formulaire de planification.

Champ	Description
Nom	Nom de la tâche de chiffrement, de déchiffrement ou de nouvelle saisie.
Type	Type de tâche : ○ **Contexte de migration des clés vers le module :** Migration en masse des clés de contexte de chiffrement vers les modules de chiffrement, y compris la création d'enregistrements de politiques d'accès au module pour les contrôles d'accès sur les modules de chiffrement ○ **Contexte de migration des données vers le module** : migre les données chiffrées par Contextes de chiffrement vers les modules de chiffrement ○ **Pièce jointe de déchiffrement en masse**:D chiffre toutes les pièces jointes chiffrées dans les enregistrements pour une seule table que vous définissez dans le champ **Table** . ○ **Pièce jointe de chiffrement en masse** : chiffre toutes les pièces jointes des enregistrements pour une seule table que vous définissez dans le champ **Table** . ○ **Module de chiffrement en masse** : chiffre toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ ○ **Module de déchiffrement en masse** : déchiffre toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ avec module unique. ○ **Module multiple de déchiffrement en masse** : déchiffre toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ avec un module multiple. ○ **Renouvellement de saisie du module** : chiffre à nouveau toute valeur préexistante dans la colonne/le champ défini utilisé dans la configuration de chiffrement de champ à l'aide de la clé active actuelle pour le module. ○ **Migrer le contexte de pièce jointe vers le module** : chiffre toute pièce jointe préexistante dans la table définie dans la configuration de Chiffrement de champ. Toute pièce jointe précédemment chiffrée avec un contexte est à nouveau chiffrée avec le module.
État	L'état initial de la tâche est Nouveau. Une fois que la tâche a été exécutée comme prévu, l'état est mis à jour en conséquence.
Début de la fenêtre de temps	Heure de début de la tâche au format 24 heures.
Fin de la fenêtre	Heure de fin de la tâche au format 24 heures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
de temps	
Table	Table à chiffrer ou à déchiffrer.
Champ	Champ à chiffrer ou à déchiffrer.
Résumé	Informations sur l'état de la tâche lorsque la tâche est en cours d'exécution, est terminée ou présente des erreurs.

Remarque :
En raison de la surcharge du système, vous devez planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse pour qu'elles s'exécutent en dehors des heures de pointe. Le Now Platform exécute la tâche entre le **début** et la fin de la **fenêtre de temps**. Si la tâche n'est pas terminée au cours d'une fenêtre de traitement, elle se poursuit pendant la fenêtre de traitement spécifiée suivante jusqu'à ce que tout le traitement soit terminé.

4. Cliquez sur **Envoyer**.
5. Après avoir planifié une tâche, vous pouvez effectuer les actions suivantes.
   - Cliquez sur **Annuler la tâche** pour annuler une tâche en cours d'exécution.
   - Cliquez sur **Démarrer** pour démarrer une tâche immédiatement.
   - Cliquez sur **Mettre à jour** pour enregistrer toutes les modifications apportées au calendrier de tâche.
   - Cliquez sur **Supprimer** pour supprimer la tâche planifiée.

Exécuter le chiffrement ou le déchiffrement en masse

Vous pouvez exécuter le chiffrement en masse sur les configurations de chiffrement, ainsi qu'un déchiffrement en masse pour déchiffrer les valeurs précédemment chiffrées.

Avant de commencer
Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche
Vous pouvez également créer des travaux planifiés pour le chiffrement et le déchiffrement en masse. Consultez les Planifier des tâches de chiffrement, de déchiffrement et de nouvelle saisie en masse pour obtenir les instructions.

Le chiffrement et le déchiffrement en masse ne sont disponibles que lorsqu'une configuration de champ chiffré utilise le module de chiffrement unique. Le déchiffrement de masse est disponible pour les méthodes de cryptage uniques et multiples.

Remarque :
Vous ne devez exécuter le chiffrement et le déchiffrement en masse que pendant les heures creuses, car les opérations demandent beaucoup de temps et de ressources.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Chiffrement de champ** > **Configurations des champs chiffrés**.
2. Ouvrez la configuration du champ chiffré pour le champ que vous souhaitez chiffrer ou déchiffrer en masse.
3. Sous Liens connexes, sélectionnez une option disponible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Planifier la tâche de déchiffrement en masse**
- **Planifier la tâche de chiffrement en masse**

4. Confirmez votre sélection dans la boîte de dialogue.

Résultats

En cas d'exécution d'un chiffrement en masse, toutes les valeurs sont chiffrées avec le module de chiffrement défini dans l'enregistrement de configuration du champ chiffré. En cas d'exécution d'un déchiffrement en masse, seuls les champs chiffrés avec un module de chiffrement auquel vous avez accès sont déchiffrés.

Exemples d'Enterprise de Chiffrement au niveau des colonnes

Ces exemples vous guident dans le chiffrement des champs et des pièces jointes à l'aide des clés fournies par le client.

Procédure pas à pas de chiffrement de champ

Cette procédure pas à pas vous montre comment chiffrer un champ dans votre instance à l'aide Entreprise de Chiffrement au niveau des colonnes du Key Management Framework (KMF). Il vous montre également comment utiliser votre propre clé.

Avant de commencer

Remarque :
Cette procédure ne s'applique qu'aux Entreprise de Chiffrement au niveau des colonnes fonctionnalités. Pour Activer Chiffrement au niveau des colonnes – Entreprise plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Rôle requis : admin ou security_admin

Remarque :
security_admin s'agit d'un rôle privilégié, pour plus de détails sur l'utilisation des rôles privilégiés, voir Élever au rang de rôle privilégié

Pourquoi et quand exécuter cette tâche

Cette procédure pas à pas commence par une instance dans laquelle vous avez déjà créé et chargé votre clé cryptographique personnelle. Vous pouvez utiliser la clé, mais cet exemple utilise une clé fournie par le ServiceNow client.

Une fois la clé stockée dans un module de chiffrement, vous pouvez commencer à configurer les champs de votre instance, tels que les numéros de salaire ou de sécurité sociale, dont l'accès est limité par certains utilisateurs. Dans la configuration du champ chiffré, spécifiez quel personnel autorisé peut accéder aux données sensibles.

Cette tâche illustre deux scénarios. Par exemple, le champ **Brève description** d'un incident est chiffré pour les utilisateurs qui ne sont pas autorisés à afficher les données sensibles.

Les pièces jointes peuvent également être chiffrées et visibles uniquement par les utilisateurs qui y ont accès, ou par tous les utilisateurs qui ne sont pas empêchés de consulter les données. Reportez-vous à la rubrique Procédure pas à pas du chiffrement des pièces jointes pour chiffrer une pièce jointe.

Procédure

1. Assurez-vous que cette Entreprise de Chiffrement au niveau des colonnes option est activée.
2. Créez un module de chiffrement pour column_level_encryption.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

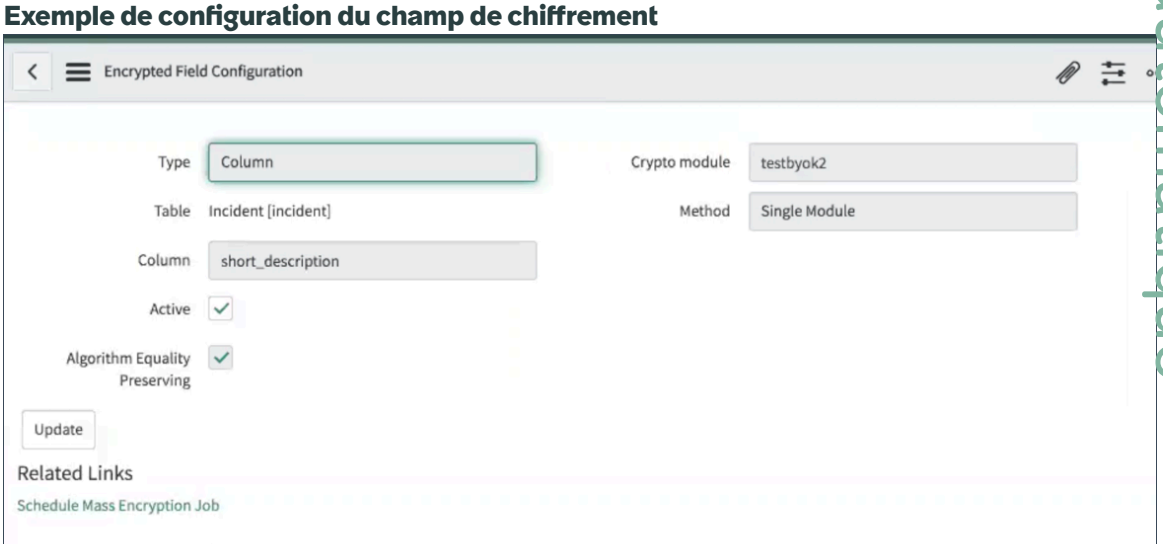
Voir Créer un module cryptographique pour Chiffrement au niveau des colonnes Créer un module cryptographique pour plus d'informations.

3. Accédez à la **Sécurité de système** > **Configurations des champs chiffrés**.
4. Cliquez sur **Nouveau**.
5. Renseignez les champs du formulaire.

Formulaire de configuration des champs chiffrés

Champ	Description
Type	**La colonne** est requise pour utiliser votre clé personnelle.
Table	Table qui stocke les informations sensibles. Pour cet exemple, sélectionnez **Incident [incident].**
Colonne	Colonne, ou informations spécifiques, qui représentent la date sensible à chiffrer. Pour cet exemple, sélectionnez **short_description**.
Actif	Option permettant de marquer **Actif** pour utiliser la configuration du champ.
Préservation de l'égalité des algorithmes	L'option est automatiquement sélectionnée.
Module de chiffrement	Module que vous avez créé à utiliser avec la clé personnelle.
Méthode	L'option **Module unique** permet d'appliquer les politiques à un module. **Plusieurs modules** est utilisé pour appliquer les politiques à plusieurs modules.

Exemple de configuration du champ de chiffrement



6. Cliquez sur **Envoyer**.

Établissez une politique d'accès au module pour affecter l'accès au module cryptographique. Consultez Créer une politique d'accès au module pour plus d'informations.

7. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > > **Créer** > **.**
8. Renseignez les champs du formulaire.

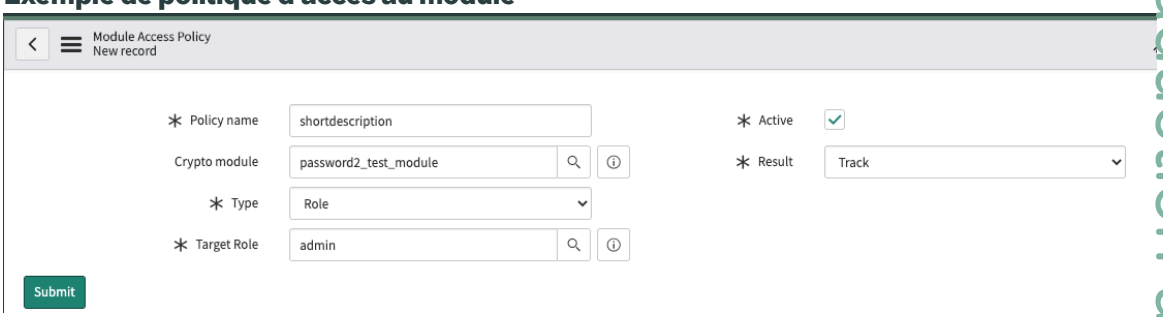
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de politique d'accès au module

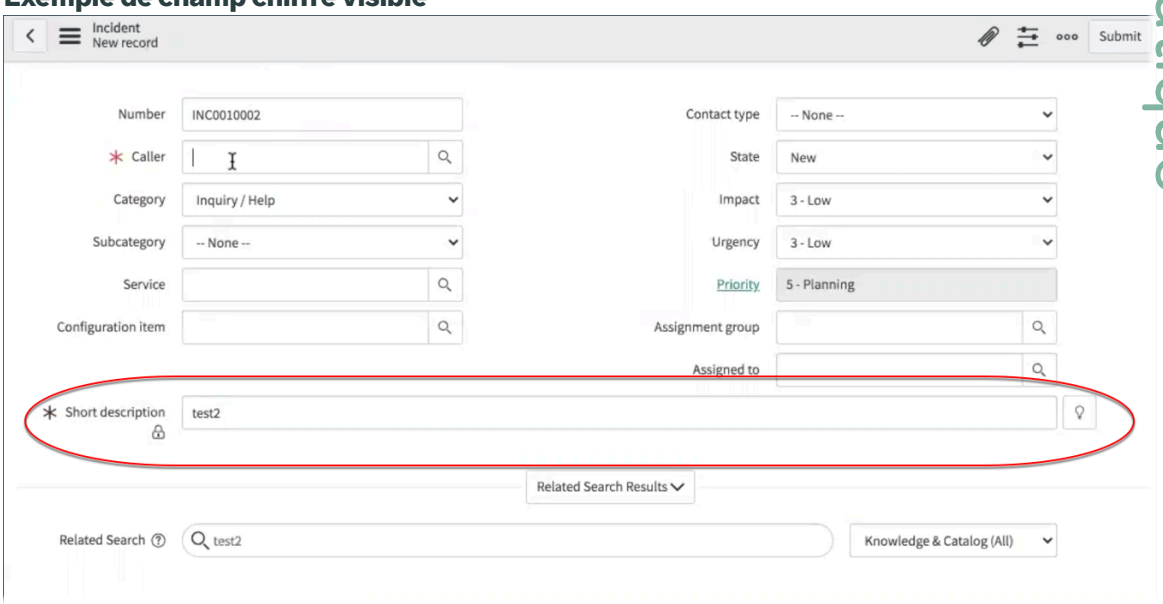
Champ	Description
Nom de la politique	Nom de la politique, par exemple description brève.
Module de chiffrement	Module de chiffrement que vous avez créé pour chiffrer votre clé.
Type	Type de désignation d'accès pour la politique de chiffrement. Utilisez **Rôle** pour accorder l'accès au champ chiffré uniquement aux utilisateurs disposant du rôle affecté.
Rôle cible	Le rôle qui a accès au champ chiffré. Pour cet exemple, sélectionnez **Administrateur**.
Actif	Option permettant d'activer la politique d'accès au module.
Résultat	L'option **Suivre**permet d'accéder au champ pour le rôle sélectionné. (Pour limiter l'accès à ce champ pour le rôle sélectionné, sélectionnez **Rejeter** ou**Rejeter strict**.)

Exemple de politique d'accès au module



9. Cliquez sur **Envoyer**.
10. En tant qu'utilisateur disposant du rôle sn_kmf.admin, accédez à **Incident** > **Nouveau**.

Exemple de champ chiffré visible



Vous pouvez maintenant afficher le champ Brève description en fonction de la configuration de politique d'accès au module.

Traduction automatique

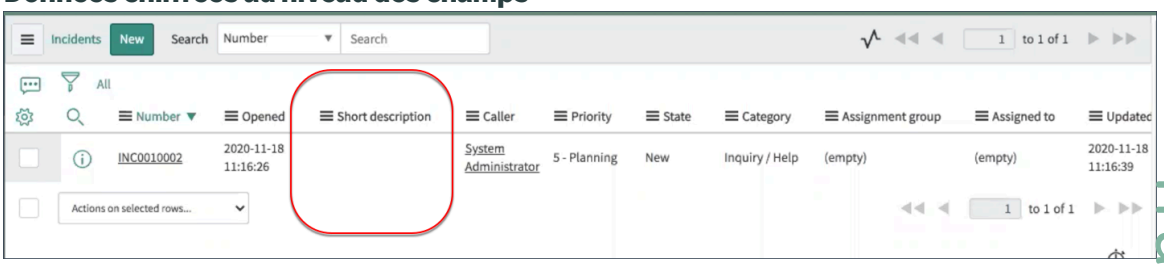
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le rôle sn_kmf.admin a obtenu l'accès utilisateur au champ chiffré Description brève en définissant la politique d'accès au module sur **Suivre**. Remarquez l'icône de cadenas ( ) sous le nom du champ indiquant que le champ est un champ chiffré.

Vous pouvez maintenant accéder au module **Incidents** en tant qu'utilisateur final pour tester la configuration des champs chiffrés.

11. Connectez-vous en tant qu'utilisateur pour ne pas pouvoir afficher les données chiffrées dans le champ configuré.

Données chiffrées au niveau des champs



Lorsque vous accédez au numéro d'incident, les données de la brève description ne sont pas visibles.

Résultats
Vous avez utilisé avec succès votre clé symétrique pour contrôler l'accès à un champ spécifique à l'aide de Entreprise de Chiffrement au niveau des colonnes.

Procédure pas à pas du chiffrement des pièces jointes

Cette procédure pas à pas vous montre comment chiffrer une pièce jointe dans votre instance à l'aide Entreprise de Chiffrement au niveau des colonnes du Key Management Framework (KMF). Il vous montre également comment utiliser votre propre clé.

Avant de commencer

Remarque :
Cette procédure ne s'applique qu'aux Entreprise de Chiffrement au niveau des colonnes fonctionnalités. Pour Activer Chiffrement au niveau des colonnes – Entreprise plus d'informations sur l'obtention de Entreprise de Chiffrement au niveau des colonnes.

Rôle requis : gestionnaire de chiffrement KMF

Pourquoi et quand exécuter cette tâche
Cette procédure pas à pas commence avec une instance dans laquelle vous avez déjà créé et téléchargé votre clé cryptographique fournie par le client. Vous pouvez utiliser la clé, mais cet exemple utilise une clé fournie par le ServiceNow® client.

Chargez des pièces jointes confidentielles dans votre instance et limitez l'accès de certains utilisateurs. Utilisez la configuration des champs chiffrés pour spécifier quel personnel autorisé peut accéder aux données sensibles.

Nous vous montrons comment chiffrer des pièces jointes pour qu'elles ne soient visibles que par les utilisateurs qui y ont accès, ou pour tous les utilisateurs qui ne sont pas empêchés de consulter les données. Dans cet exemple, nous limitons la possibilité pour un certain rôle d'accéder à une pièce jointe dans le module **Incidents** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Bien que vous puissiez utiliser plusieurs modules avec chiffrement de colonne, le chiffrement des pièces jointes doit utiliser des modules uniques.

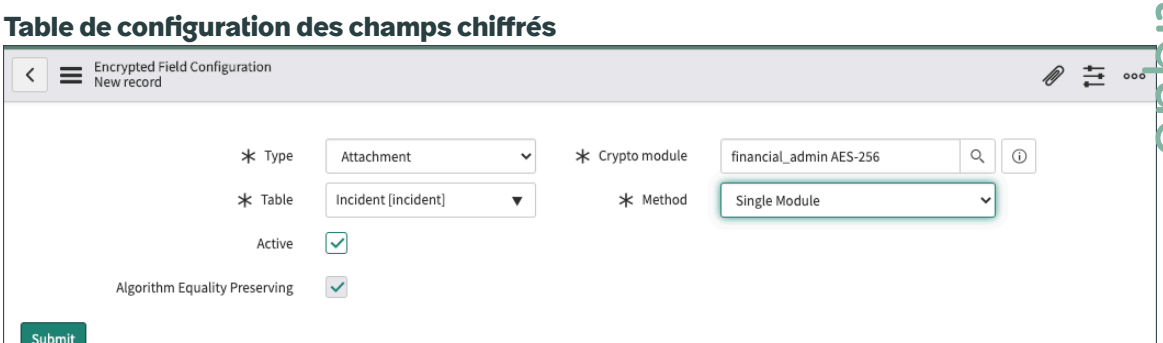
Procédure

1. Assurez-vous que cette Entreprise de Chiffrement au niveau des colonnes option est activée.
2. Créez un module cryptographique.
   Consultez Créer un module cryptographique pour Chiffrement au niveau des colonnes pour plus d'informations.
3. Accédez à la **Sécurité de système** > **Configurations des champs chiffrés**.
4. Cliquez sur **Nouveau**.
5. Complétez le formulaire :

Champs de configuration des champs chiffrés

Champ	Description
Type	Sélectionnez **Pièce jointe** pour utiliser votre clé personnelle pour chiffrer une pièce jointe à partir de la **table** sélectionnée. Pour cet exemple, sélectionnez **Incident**.
Table	Sélectionnez la table pour accéder aux informations sensibles. Pour cet exemple, sélectionnez **Incident [incident].**
Actif	Marquez **comme actif** pour pouvoir utiliser la configuration du champ.
Préservation de l'égalité des algorithmes	Lorsque vous sélectionnez le chiffrement au niveau des colonnes, ce champ est visible en fonction de la table sélectionnée.
Module de chiffrement	Sélectionnez le module que vous avez créé pour l'utiliser avec la clé personnelle.
Méthode	L'option **Module unique** permet d'appliquer les politiques à un module. **Plusieurs modules** est utilisé pour appliquer les politiques à plusieurs modules.

Table de configuration des champs chiffrés



6. Cliquez sur **Envoyer**.

Établissez une politique d'accès au module pour affecter l'accès au module cryptographique. Reportez-vous à Créer une politique d'accès au module pour plus d'informations.

7. Accédez à la **Gestion des clés** > **Politiques d'accès au module** > **Tout**.
8. Cliquez sur **Nouveau**.

Traduction automatique

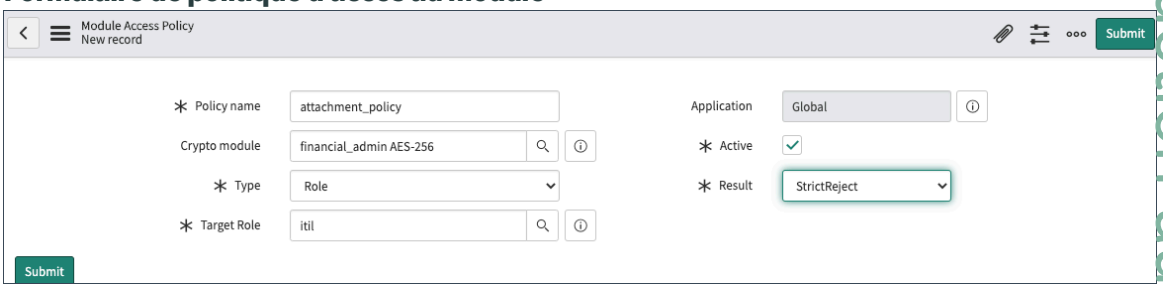
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Complétez le formulaire :

Champs de politique d'accès au module

Champ	Description
Nom de la politique	Saisissez un nom pour la politique, par exemple « Politique en matière de pièces jointes ».
Module de chiffrement	Sélectionnez le module de chiffrement que vous avez créé pour chiffrer votre clé.
Type	Sélectionnez **Rôle** pour restreindre l'accès au champ chiffré des utilisateurs disposant du rôle affecté.
Rôle cible	Sélectionnez le rôle qui n'aura pas accès au champ chiffré. Pour cet exemple, sélectionnez **itil**.
Actif	Cochez cette case pour pouvoir utiliser la politique d'accès au module.
Résultat	Sélectionnez **Rejet strict** pour contrôler l'accès à la pièce jointe à partir du rôle sélectionné. (Pour accorder l'accès au rôle sélectionné, sélectionnez **Suivre**.)

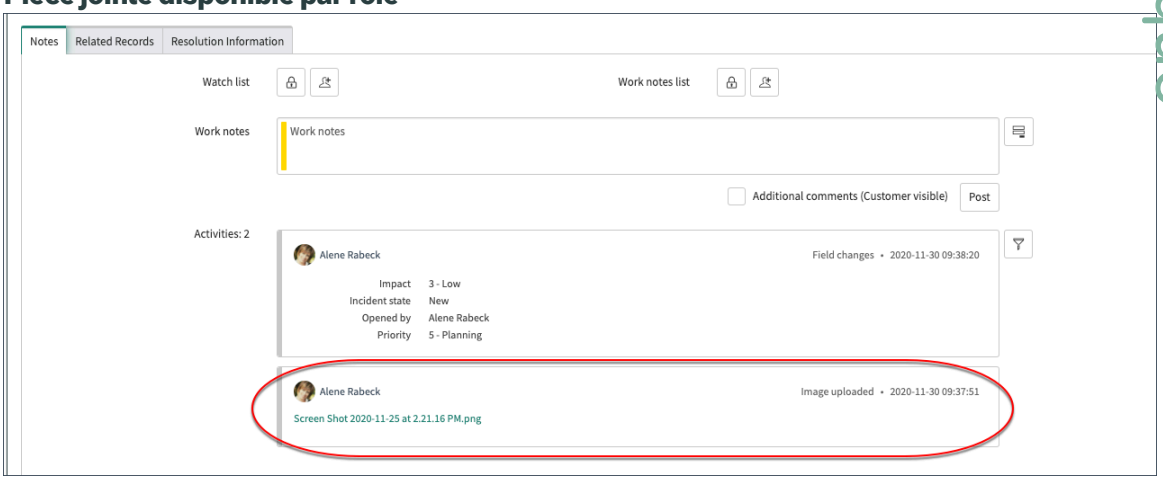
Formulaire de politique d'accès au module



10. Cliquez sur **Envoyer**.

11. En tant qu'administrateur ou en tant que personne qui a créé l'incident, accédez à **Incidents** et ajoutez une pièce jointe aux **activités** dans la liste connexe **Notes** .

Pièce jointe disponible par rôle



12. Connectez-vous en tant qu'utilisateur ayant restreint l'accès à la pièce jointe chiffrée.

13. Ouvrez l'incident et faites défiler jusqu'à la section **Activités :** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le lien permettant d'ouvrir la pièce jointe n'est pas accessible aux utilisateurs disposant du rôle restreint.

14. Vous avez maintenant utilisé avec succès votre clé fournie par le client pour contrôler l'accès à une pièce jointe spécifique à l'aide du chiffrement au niveau des colonnes.

Chiffrement au niveau des colonnes – Entreprise

Entreprise de Chiffrement au niveau des colonnes (CLE) utilise le Key Management Framework (KMF) pour vous permettre de personnaliser et de gérer la façon dont les champs et les pièces jointes sont chiffrés et déchiffrés sur votre instance. Un abonnement est requis pour utiliser Entreprise de Chiffrement au niveau des colonnes.

Important :
Cette rubrique couvre la version d'entreprise de Chiffrement au niveau des colonnes. Pour plus d'informations sur la version standard de CLE ou pour connaître les différences entre les deux versions, reportez-vous à la section Explorer Chiffrement au niveau des colonnes.

Entreprise de Chiffrement au niveau des colonnesrepose sur Chiffrement au niveau des colonnes (CLE) et utilise la et sa prise en charge complète des fonctions de gestion des clés. Entreprise de Chiffrement au niveau des colonnes assure la Key Management Framework protection des clés et la gestion du cycle de vie des clés pour le chiffrement des champs au niveau de l'application. Toutes les clés sont protégées par une hiérarchie d'encapsulation des clés enracinée dans les modules de sécurité matériels (HSM) FIPS 140-2-L3.

Entreprise de Chiffrement au niveau des colonnes vous donne la possibilité de gérer la façon dont les champs pris en charge sont chiffrés et déchiffrés conformément aux pratiques NIST 800-57 . Il utilise également la version la plus récente du chiffrement au niveau des champs, y compris l'intégration pour une protection et une gestion appropriées des clés.

Plus précisément, Entreprise de Chiffrement au niveau des colonnes utilise les KMF modules de chiffrement, ce qui vous permet de mieux contrôler le chiffrement côté serveur. KMF Assure une protection appropriée des clés de chiffrement des données à l'aide de la hiérarchie des clés et du chiffrement de l'enveloppe. Votre instance chiffre les données via des modules de chiffrement que vous configurez. Vous pouvez créer une politique d'accès pour chaque module, puis configurer les spécifications cryptographiques et les politiques d'accès et contrôler le contrôle de la gestion du cycle de vie des clés.

Entreprise de Chiffrement au niveau des colonnes prend en charge les politiques d'accès au module basées sur :

- Périmètre
- Rôle
- Script
- Échange de ressources
- Utilisateur système

Consultez Créer une politique d'accès au module pour plus d'informations.

Remarque :
Pour en savoir plus sur les fonctionnalités prises en charge de Chiffrement au niveau des colonnes et savoir comment mettre à niveau et s'abonner à l'autorisation Entreprise de Chiffrement au niveau des colonnes , reportez-vous à Offre groupée d'abonnements pour Encryption and Key Management.

Traduction automatique

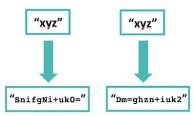
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Termes de chiffrement

Terme	Description
Gestion des clés 	Prise en charge de la gestion des clés Le Cadre de gestion des clés (CGM) est fondamental Entreprise de Chiffrement au niveau des colonnes . Bénéficiez des options suivantes : • Gestion du cycle de vie des clés. • Rotation des clés. Consultez Faire pivoter les clés pour en savoir plus. • Protection des clés et génération de clés avec les modules de sécurité matériels (HSM) FIPS 140-2-L3. • Séparation des rôles et des tâches. • Transfert sécurisé des clés de chiffrement des données entre les instances, telles que les instances de production et de non-production. • Clés fournies par le client (CSK) avec emballage de clés. • Chiffrement non déterministe. • Chiffrement/déchiffrement de masse. • Audit de l'accès/de l'utilisation des clés. Consultez Comprendre le cadre de gestion des clés pour en savoir plus.
Clé fournie par le client 	Prise en charge des clés fournies par le client L'un Entreprise de Chiffrement au niveau des colonnes des plus grands avantages est que vous pouvez utiliser vos propres clés pour le chiffrement. Les administrateurs ont le choix d'utiliser ServiceNow les clés fournies ou vos propres clés fournies par le client (CSK) pour le chiffrement sur le Now Platform®fichier . Vous pouvez également gérer le cycle de vie des clés et décider quand les révoquer, les faire pivoter et les désactiver. Une fois que vous avez activé les clés fournies par le client et créé un module de chiffrement, vous téléchargez un jeton et une clé éphémère publique. Vous utilisez le jeton et la clé publique pour encapsuler votre clé, puis la charger dans l'instance. Pour utiliser les clés fournies par le client, reportez-vous aux sections Configurer les paramètres de chiffrement de champ pour sélectionner le type de clé et Utilisation des clés fournies par le client avec Chiffrement au niveau des colonnes – Entreprise .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Terme	Description
Chiffrement au niveau des colonnes 	Prise en charge du chiffrement de champ et du chiffrement de pièce jointe Le chiffrement de champ et le chiffrement de pièce jointe utilisent tous deux des modules cryptographiques et des politiques d'accès via des configurations de champs chiffrés. Le formulaire Configuration des champs chiffrés permet de choisir un type de chiffrement de *colonne* ou de *pièce jointe* . Pour plus d'informations et connaître les types de champs pris en charge, consultez la rubrique Définir des configurations de champs chiffrés
Chiffrement non déterministe 	Prise en charge du chiffrement non déterministe Entreprise de Chiffrement au niveau des colonnes Prend en charge le chiffrement *non déterministe* pour une sécurité renforcée. Si le système crypte les mêmes données plus d'une fois, les textes chiffrés sont différents à chaque fois. Le chiffrement non déterministe est disponible avec le chiffrement AES avec Cipher Block Chaining (CBC). Vous pouvez activer cette fonctionnalité via l'option Préservation de l'égalité à l'étape Définition de l'algorithme de la spécification cryptographique. Créez une spécification cryptographique pour un module de chiffrement et définissez un algorithme pour le chiffrement et générez la clé. Reportez-vous à la rubrique Créer un module cryptographique pour définir les mécanismes utilisés pour les opérations de chiffrement et pour plus d'informations sur l'activation du chiffrement non déterministe.
Resource Exchange 	Resource Exchange Entreprise de Chiffrement au niveau des colonnes clé d'instance en instance de manière sécurisée à l'aide des API de chiffrement pour garantir la confidentialité, l'intégrité KMF , l'authentification et la non-répudiation. Resource Exchange est une KMF fonctionnalité qui vous donne la possibilité d'échanger des ressources entre les instances de manière sécurisée. Consultez Échange de ressources du cadre de travail de gestion des clés pour en savoir plus.

Remarque :
Si vous choisissez de ne pas activer Entreprise de Chiffrement au niveau des colonnes, vous pouvez toujours utiliser le chiffrement au niveau des colonnes. Voir Explorer Chiffrement au niveau des colonnes pour plus d'informations.

Entreprise de Chiffrement au niveau des colonnes prend en charge les clients sur site. Il ne prend pas en charge Domain Separation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Prise en charge de modules et de politiques d'accès aux modules supplémentaires

La version standard de est limitée à cinq modules et stratégies d'accès Chiffrement au niveau des colonnes au module (MAP). Entreprise de Chiffrement au niveau des colonnes prend en charge un plus grand nombre de modules et de MAP.

Informations sur les champs pris en charge

Les types de champs suivants peuvent être chiffrés :

- Pièces jointes
- Date
- Date/Heure
- E-mail
- HTML
- Journal
- Entrée de journal
- Liste de journaux
- Téléphone
- Texte de chaîne
- Champ traduit
- HTML traduit
- Texte traduit
- URL

Chiffrement de la pièce jointe

Chiffrement des pièces jointes par défaut

Les clients qui utilisent le chiffrement au niveau des colonnes ont des pièces jointes chiffrées par défaut dans les tables dont le type de configuration de champ chiffré (EFC) actif est *.Attachment*

Ce chiffrement par défaut défini par la configuration EFC signifie que les administrateurs n'ont pas besoin de déclarer manuellement qu'une pièce jointe doit être chiffrée lors du chargement pour ces tables.

Les administrateurs peuvent empêcher les utilisateurs de joindre des fichiers non chiffrés

Pour plus de détails, voir Empêcher les utilisateurs de joindre des fichiers non chiffrés.

Désactiver le chiffrement par défaut

Si vous ne souhaitez pas que les pièces jointes soient chiffrées par défaut en fonction de la configuration EFC, vous pouvez désactiver cette option en contactant l'assistance ServiceNow .

Pour désactiver cette fonctionnalité, créez un ticket de support avec ServiceNow support et incluez cette déclaration dans un commentaire sur l'enregistrement du ticket :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

« Je [nom du client] comprends que je demande ServiceNow la désactivation d'une bonne pratique de sécurité recommandée pour les pièces jointes, et que [l'entreprise cliente] assume tout risque supplémentaire lié à la configuration et à l'utilisation de pièces jointes non chiffrées dans l'application ServiceNow . »

Prise en charge de l'API

Entreprise de Chiffrement au niveau des colonnes met à jour les API setDisplayValue() et setValue() afin qu'elles puissent insérer des données chiffrées pour les champs chiffrés. Il permet également à getDisplayValue() et getValue() de renvoyer des valeurs en clair.

Le script suivant illustre ces changements d'API lorsque la brève description de l'incident est chiffrée :

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Lorsque vous utilisez getValue() pour obtenir du texte chiffré, votre script ne renvoie plus le texte chiffré. Votre script renvoie le texte en clair, en supposant que l'utilisateur a accès au module de chiffrement. getValue() renvoie le texte chiffré pour les utilisateurs qui n'ont pas accès au module cryptographique.

Chiffrement dans le cloud avec la gestion des clés

ServiceNow® Chiffrement dans le cloud offre un stockage chiffré pour la base de données à l'aide du chiffrement par blocs, ainsi qu'une gestion des clés améliorée. Chiffrement dans le cloud est disponible avec le ServiceNow® Lot d'abonnements Chiffrement de la plateforme.

Chiffrement dans le cloud Offre:

- Séparation des tâches.
- Rotation des ServiceNow clés gérées.
- Option Clés gérées par le client.

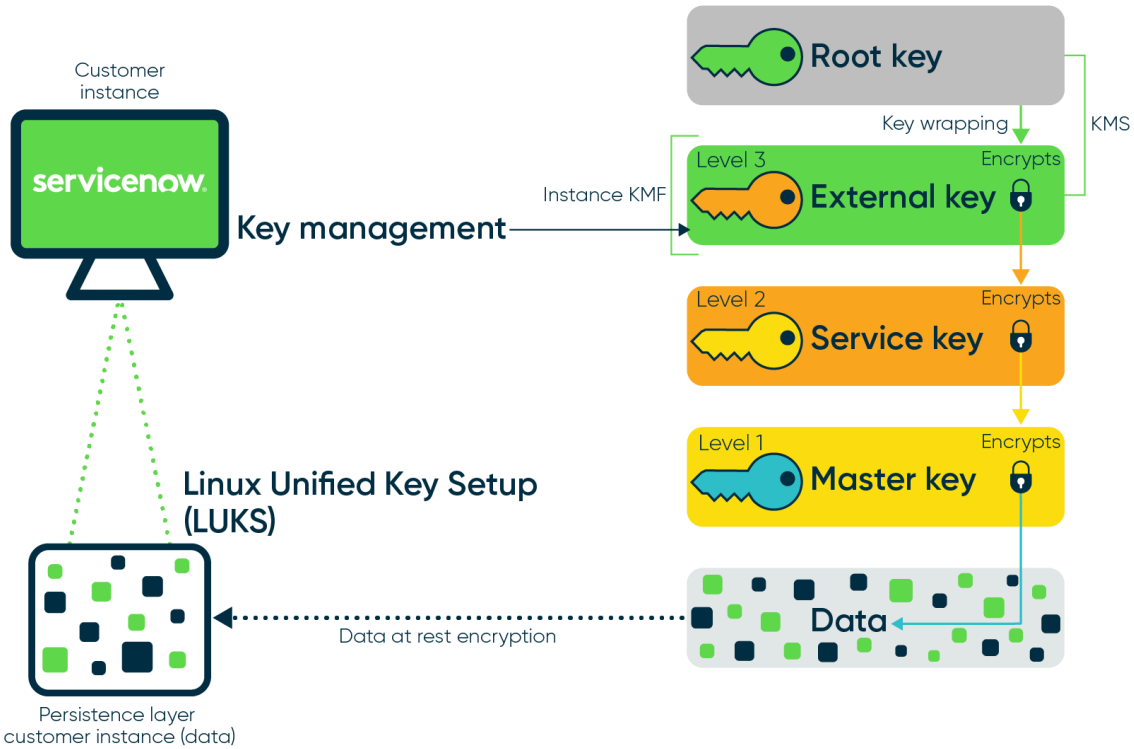
Remarque :
Envisagez cette option si votre organisation exige que vous utilisiez du matériel clé généré par vos propres outils ou bibliothèques cryptographiques, un système de gestion des clés d'entreprise ou un module de sécurité matériel (HSM). Consultez Opérations de gestion des clés pour en savoir plus.

Le diagramme suivant montre comment Chiffrement dans le cloud cela fonctionne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vue d'ensemble de Chiffrement dans le cloud



Le Chiffrement dans le cloud module de gestion des clés se compose des sous-modules suivants :

- Opérations de gestion des clés :
  - Accédez à la liste des clés.
  - Effectuez des opérations de rotation de clés.
  - Retirer la clé gérée par le client.
- Transactions de gestion des clés :

  Référencez toutes les transactions qui se sont produites pour les clés qui ont été utilisées.

  Utilisez votre propre clé gérée par le client pour le chiffrement.

Dans certaines circonstances, vous pouvez opter pour une demande de retrait de clé lorsque vous utilisez une clé gérée par le client. Pour ce faire, vous devez obtenir une licence pour la référence SKU complémentaire facultative Retrait et réapprovisionnement de Chiffrement cloud, puis demander à un membre de l'équipe d'activer Service et assistance client la fonctionnalité de retrait de clé.

L'option Paramètres de la politique de contrôle du quorum devient disponible lorsque la fonction de retrait est activée, sinon le module n'est pas visible dans le menu. Cette fonctionnalité ne peut être activée que lors de l'utilisation de clés gérées par le client. Cette politique permet de configurer les paramètres concernant le quorum lorsque la fonctionnalité de retrait est activée. Pour en savoir plus sur cette fonctionnalité, reportez-vous à la section Politique de contrôle du quorum.

Chiffrement dans le cloud prend en charge les instances de production et de non-production pour les bases de données MariaDB et RaptorDB. Cloud Encryption est pris en charge dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commercial ServiceNow Cloud, Government Customer Cloud (GCC) pod 101 et ServiceNow Protected Platform – Australia (SPP-AU).

Gestion des licences et activation Chiffrement dans le cloud

Pour en savoir plus sur la gestion des licences Chiffrement dans le cloud, reportez-vous à la section Offre groupée d'abonnements pour Encryption and Key Management.

Pour les clients sous licence disposant de nouvelles instances, la nouvelle mise en service d'instance inclura Chiffrement dans le cloud.

Pour les clients sous licence disposant d'instances existantes, pour demander le déplacement d'une instance vers Chiffrement dans le cloud, suivez les instructions de la KB1117369 . Vous devez disposer du rôle d'administrateur des clients ou des partenaires pour demander à l'élément de Catalogue de services d'activer Chiffrement dans le cloud sur votre instance. L'activation de cette fonctionnalité nécessite une fenêtre de maintenance d'une heure.

Interface utilisateur de Chiffrement dans le cloud

Lorsque Chiffrement dans le cloud est activé, l'interface utilisateur de Chiffrement dans le cloud est visible par l'utilisateur security_admin lorsque celui-ci dispose du rôle sn_kmf.admin.

Pour accéder à l'interface utilisateur de Chiffrement dans le cloud, recherchez **Gestion des clés de chiffrement dans le cloud** dans la barre de navigation. Accédez à la section **Opérations de gestion de clés** pour afficher des informations sur les clés de chiffrement, telles que les détails de la clé active et si Chiffrement dans le cloud est activé pour l'instance.

Opérations de gestion des clés

Le sous-module Opérations de gestion des clés permet d'afficher et de gérer toutes les clés de chiffrement utilisées avec ServiceNow Chiffrement dans le cloud.

Prise en main de Chiffrement dans le cloud

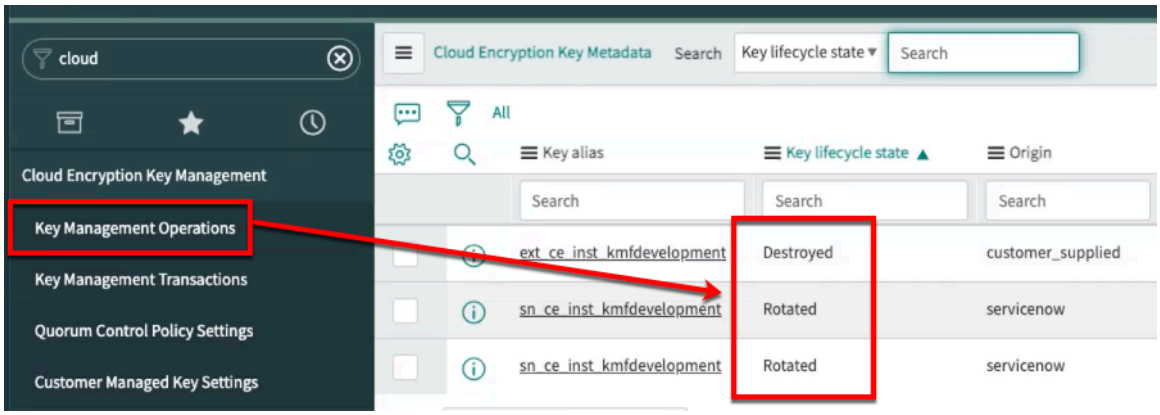
États du cycle de vie de la clé

Il n'y a qu'une seule clé active dans le système à un moment donné. Lorsque vous sélectionnez une clé, vous accédez à l'activité correspondant à la clé sélectionnée, comme les clés qui ont été tournées ou retirées et l'horodatage correspondant.

L'état du cycle de vie de la clé se met à jour en fonction de l'opération de gestion des clés effectuée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Voir Faire pivoter une clé gérée par ServiceNow ou Faire pivoter une clé gérée par le client pour plus de détails.

Remarque :
Le processus de rotation des clés peut prendre jusqu'à 20 minutes.

Faire pivoter une clé gérée par ServiceNow

Effectuez une rotation de la clé gérée active Chiffrement dans le cloud ServiceNow .

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Important :
Si vous utilisez des clés gérées par le client, reportez-vous à la section Faire pivoter une clé gérée par le client.

Procédure

1. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
   La Chiffrement dans le cloud liste des métadonnées clés se charge. Toutes les clés utilisées dans votre instance sont répertoriées. Une seule clé peut être active à la fois.

   Si vous accédez au module pour la Chiffrement dans le cloud première fois, les entrées de clés seront disponibles après une rotation de clés initiale. Une ServiceNow clé gérée est l'option par défaut dans le système.

2. Sélectionnez la clé active dans la table.
   La table Définition de clé s'affiche avec des informations générales sur la clé que vous ServiceNow avez générée.

3. Sélectionnez le bouton **Faire pivoter la clé** .
   Une notification s'affiche avec la possibilité de continuer la rotation des clés ou d'annuler l'opération.

4. Sélectionnez **OK** pour faire pivoter la touche.
   Un message de confirmation s'affiche en haut de la page Définition de clé.

5. Revenez à l'écran Opérations de gestion des clés pour actualiser la table Métadonnées de clés Chiffrement dans le cloud .
   Les entrées sont répertoriées pour la clé active actuelle et la clé en cours de génération pour tourner à la place de la clé active actuelle. Consultez la rubrique États du cycle de vie des clés du cadre de travail de gestion des clés pour connaître les différents états disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La clé active est répertoriée avec une version de clé de `0` et la clé générée a une version de `1`.

6. Ouvrez l'entrée de la clé d'origine pour afficher les transactions de gestion des clés.
   Pour plus d'informations, consultez Transactions de gestion des clés pour plus d'informations.
   La clé précédemment active, version `0`, mise à jour vers l'état de cycle de vie de la clé `Tourné` et la nouvelle clé, version `1` , est `Active`.

Préparer votre clé gérée par le client

Suivez ces étapes pour préparer votre clé gérée par le client en vue de son chargement sur votre instance.

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Pourquoi et quand exécuter cette tâche

Pour une clé gérée par le client, vous pouvez utiliser n'importe quelle bibliothèque cryptographique ou HSM pour générer votre clé. Cette clé doit être une clé AES 256 bits et être encapsulée par un certificat d'encapsulation de chiffrement dans le cloud avec un schéma de chiffrement RSAES_OAEP_SHA_256.

Remarque :

Si vous choisissez d'utiliser l'outil de chiffrement OpenSSL pour générer votre clé, la version OpenSSL doit être la version 1.1.1x ou ultérieure.

Si vous créez et encapsulez votre clé gérée par le client à l'aide Windowsde , vous devez générer la clé encapsulée via des applications de prise en charge du shell Bash telles que Git Bash.

Procédure

1. Générez une valeur aléatoire à utiliser comme clé symétrique AES-256 bits à l'aide d'OpenSSL.

   Par exemple, en utilisant openSSL, vous pouvez générer cette clé avec la commande `openssl rand 32` .

   Pour des raisons de compatibilité, votre clé symétrique doit comporter les attributs suivants :

Attribut	Valeur
Type de clé	Clé symétrique basée sur un algorithme AES (Advanced Encryption Standard).
Taille de la clé	256 bits (32 octets)
Besoin d'encapsulation de clé	○ Algorithme de chiffrement RSA ○ Remplissage de chiffrement asymétrique optimal (OAEP) ○ Fonction de hachage SHA-256 (RSAES_OAEP_SHA_256) ○ Codé à l'aide de l'algorithme Base64

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Enregistrer la clé dans un fichier.
   Par exemple, la commande `openSSL openssl rand 32 > plaintext_key.bin` génère une clé de 32 octets et l'enregistre dans un fichier nommé `plaintext_key.bin`.

   Important :
   Enregistrez ce fichier en toute sécurité pour référence ultérieure. Cette clé est enveloppée avec la clé publique pour le chargement.

3. Extrayez la clé publique du fichier de certificat d'encapsulation téléchargé à partir de votre instance :

   ```
   openssl x509 -pubkey -noout -in wrapping_cert.pem > public_key.pem
   ```

   Remarque :
   Reportez-vous à la section pour plus d'informations sur le téléchargement du certificat d'enrubannage.

4. Encapsulez la clé générée avec la clé publique téléchargée avec le certificat d'encapsulation à l'aide de l'algorithme RSAES_OAEP_SHA_256 :

   ```
   cat plaintext_key.bin | openssl pkeyutl -encrypt -inkey public_key.pem -pubin -pkeyopt
   rsa_padding_mode:oaep -pkeyopt rsa_oaep_md:sha256 | openssl base64 -A -out
   wrapped_key.txt
   ```

   Un fichier spécifié sur cette commande contient une clé encapsulée gérée par le client qui peut être fournie à SN pour le processus CMK.

Basculer entre ServiceNow et les clés gérées par le client

Basculez entre une clé gérée par le client ou une clé gérée pour une ServiceNow utilisation dans ServiceNow Chiffrement dans le cloud.

Par défaut, votre instance est configurée pour utiliser ServiceNow des clés gérées et ServiceNow la génération de clés de chiffrement est active. Toutefois, les administrateurs peuvent choisir d'utiliser des clés gérées par le client. Ils peuvent aussi choisir de revenir aux ServiceNow clés gérées.

Faire pivoter une clé gérée par le client

Faites pivoter votre clé gérée par le client vers votre instance après avoir encapsulé votre clé gérée par le client pour Chiffrement dans le cloud.

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
   La liste des **métadonnées de Clé de chiffrement dans le cloud** se charge. Toutes les clés qui ont été utilisées dans votre instance sont répertoriées.
2. Dans la liste **des métadonnées de Clé de chiffrement dans le cloud** , ouvrez l'enregistrement de votre clé active.
   Si vous avez plusieurs clés, sélectionnez la clé dont **l'état de cycle de vie** de la clé est `Actif`. Il n'y a qu'une seule clé active sur votre instance.
3. Dans l'enregistrement de définition de clé, sélectionnez le bouton **Faire pivoter la clé** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la fenêtre **Télécharger la clé gérée par le client** , procédez comme suit.

   a. Sélectionnez **Télécharger le certificat d'encapsulation**.
   Le `public_certificate.... Le fichier ZIP` est téléchargé sur votre ordinateur local et est utilisé pour encapsuler votre clé gérée par le client.

   > **⚠ Avertissement :**
   > Évitez les problèmes potentiels liés au certificat en téléchargeant le certificat d'encapsulation chaque fois que vous alternez ou basculez vers une clé gérée par le client.

   b. Sélectionnez **Parcourir** pour charger votre clé gérée par le client, puis localisez et sélectionnez votre clé de chiffrement encapsulée.
   Pour choisir un autre fichier, sélectionnez-le, puis sélectionnez **Supprimer**.

   c. Fermez la fenêtre Pièces jointes.

   d. Sélectionnez **OK** pour charger votre clé.
   Si la clé est au bon format, un message de confirmation s'affiche, sinon un message d'erreur s'affiche. Le fichier de clé est joint à l'enregistrement de définition de clé.

   Dans la table Transactions de gestion des clés, les étapes de téléchargement et de chargement des clés sont répertoriées. Consultez la rubrique Transactions de gestion des clés pour plus de détails sur les étapes de demande.

5. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés** pour afficher la liste des clés.
   Dans la liste des clés, vous pouvez voir un nouvel enregistrement pour votre clé gérée par le client. Cette nouvelle clé a une valeur **d'origine** de **customer_supplied** et est à l'état **Actif** . Votre clé précédente était dans l'état **Pivoté** .

Basculer vers une clé gérée par le client

Utilisez votre clé gérée par le client pour ServiceNow Chiffrement dans le cloud.

Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Pour passer à une clé gérée par le client, vous devez disposer d'une clé gérée par le client encapsulée prête à être chargée dans le cadre de ces étapes. Pour en savoir plus sur la préparation de cette clé en vue du chargement, reportez-vous à la section Préparer votre clé gérée par le client. Après avoir téléchargé votre clé, ce processus lancera une rotation de clés vers votre nouvelle clé.

Procédure

1. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
2. Dans la liste **des métadonnées de Clé de chiffrement dans le cloud** , ouvrez l'enregistrement de votre clé active.
   Si vous avez plusieurs clés, sélectionnez la clé dont **l'état de cycle de vie** de la clé est Actif. Il n'y a qu'une seule clé active sur votre instance.
3. Dans la section **Liens connexes** du formulaire, sélectionnez le lien **Basculer vers la clé gérée par le client** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans la boîte **de dialogue Basculer vers la clé gérée** par le client, sélectionnez le bouton **Télécharger la clé gérée** .
5. Dans la boîte de dialogue **Télécharger la clé gérée par le client, procédez** comme indiquées.

   a. Sélectionnez **Télécharger le certificat d'encapsulation**.

   > **Avertissement :**
   > Évitez les problèmes potentiels liés au certificat en téléchargeant le certificat d'encapsulation chaque fois que vous alternez ou basculez vers une clé gérée par le client.

   b. Sélectionnez **Parcourir**, puis suivez les instructions pour sélectionner et télécharger votre clé à partir de votre appareil.

   c. Sélectionnez **Basculer vers la clé gérée par le client**.

   Une demande est générée par l'instance pour basculer vers votre clé gérée par le client. Dans le formulaire actuel, vous pouvez voir que **l'état du cycle de vie** de la clé active d'origine est passé à **Pivoté**.
6. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés** pour afficher la liste des clés.
   Dans la liste des clés, vous pouvez voir un nouvel enregistrement pour votre clé gérée par le client. Cette nouvelle clé a une valeur **d'origine** de **customer_supplied** et est à l'état **Actif** .

Résultats

Votre instance utilise maintenant votre clé gérée par le client pour ServiceNow Chiffrement dans le cloud.

> **Important :**
> Assurez-vous qu'une copie de votre clé de chiffrement est toujours disponible dans un emplacement sécurisé pour les opérations de gestion des clés. Sans cette clé, votre instance risque d'être rendue inaccessible.

Basculer vers une clé gérée par ServiceNow

Basculer d'une clé gérée par le client vers une clé gérée pour ServiceNow Chiffrement dans le cloud.

Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés**.
2. Dans la liste **des métadonnées de Clé de chiffrement dans le cloud** , ouvrez l'enregistrement de votre clé active.
   Si vous avez plusieurs clés, sélectionnez la clé dont **l'état de cycle de vie** de la clé est Actif. Il n'y a qu'une seule clé active sur votre instance.
3. Dans la section **Liens connexes** du formulaire, sélectionnez le lien **Basculer vers la clé gérée par ServiceNow** .
4. Dans la boîte **de dialogue Basculer vers la clé gérée par ServiceNow** , sélectionnez le bouton **Basculer vers la clé gérée par ServiceNow** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une demande est générée par l'instance pour passer à une ServiceNow clé gérée. Dans le formulaire actuel, vous pouvez voir que **l'état du cycle de vie** de la clé active d'origine est passé à **Pivoté**.

5. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Opérations de gestion des clés** pour afficher la liste des clés.
   Dans la liste des clés, vous pouvez voir un nouvel enregistrement pour une ServiceNow clé gérée. Cette nouvelle clé a une valeur **d'origine** de **ServiceNow** et est à l'état **Actif** .

Planifier la rotation de clé

Définissez un calendrier pour la rotation automatique de vos ServiceNow clés gérées. Ce processus met automatiquement hors service une clé de chiffrement et remplace l'ancienne clé par une clé cryptographique nouvellement générée. Si vous utilisez une clé gérée par le client, ce calendrier peut vous rappeler de faire pivoter manuellement vos clés personnalisées.

Avant de commencer

Rôle requis : sn_kmf.admin

Procédure

1. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Paramètres de rotations de clés planifiées**.
2. Cochez la case **Activer la rotation de clés planifiée** .
3. Renseignez les champs restants en fonction de vos besoins professionnels.

Paramètres de rotations de clés planifiées

Champ	Description
Nombre de mois entre les rotations de clés (maximum de 60 mois)	Nombre de mois entre les rotations de clés. Cette valeur est 12 par défaut et peut avoir un maximum de 60 mois.
Jour de la semaine pour effectuer la rotation de clés	Jour de la semaine où la rotation de clés est effectuée.
Heure de la journée à laquelle effectuer la rotation de clés	Heure de la journée à laquelle la rotation de clés est effectuée.
Date et heure de la prochaine rotation de clés	Date et heure de la prochaine rotation de clés planifiée. Cette valeur n'est pas modifiable directement et est automatiquement calculée en fonction de vos choix.
Nombre de jour avant la rotation de clés pour envoyer un rappel (maximum de 15 jours)	Nombre de jours avant la date de votre rotation de clés que votre instance envoie des notifications.
Les notifications par e-mail sont envoyées à la liste suivante de vos administrateurs de sécurité approuvés	Liste des utilisateurs qui reçoivent des notifications pour la rotation de clés. **L'administrateur système** figure sur cette liste par défaut.

4. Sélectionnez **Soumettre**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après avoir sélectionné Soumettre, vous pouvez voir une notification en haut du formulaire. Les notifications confirment votre rotation de clés et le calendrier des notifications.

⚠ Avertissement :

Chaque rotation de clés planifiée possède une signature unique, qui garantit l'intégrité d'une tâche et détecte toute modification non autorisée. La signature d'une tâche planifiée est unique sur chaque instance. Lors du clonage d'une tâche de rotation de clés planifiée d'une instance source A vers une instance cible B, la tâche planifiée sur l'instance B échoue à la validation de signature. Dans ce cas, vous pouvez recréer la signature en désélectionnant puis en cochant à nouveau la case **Activer la rotation de clés planifiée** . Pour plus de détails sur ce problème, voir KB1247113 .

Retirer une clé gérée par le client

Une fois que la fonctionnalité de retrait de clé gérée par le client est activée, une opération de retrait devient disponible dans la page Opérations de gestion de clés. Les opérations de retrait de clé et d'approbation du quorum peuvent également être gérées.

Avant de commencer

Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Cette section s'applique uniquement si vous disposez d'une licence de retrait et de réapprovisionnement par chiffrement dans le cloud, un module complémentaire facultatif de Chiffrement dans le cloud.

Procédure

1. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > > **Opérations de gestion des clés**.
2. Sélectionnez la clé gérée par le client active dans la table.
   La table Définition de clé s'affiche avec des informations générales sur votre clé client. Une fonction de retrait de la touche est maintenant disponible.
3. Sélectionnez la **clé de retrait** pour déclencher le processus de retrait.

⚠ Avertissement :

Un message d'avertissement Retirer la clé s'affiche. Le retrait de la clé déclenche l'arrêt de votre instance jusqu'à ce qu'une opération de restauration soit effectuée avec la clé retirée.

DANGER :
Vous ne pouvez effectuer une opération de restauration qu'avec la même clé qui a été retirée. Si vous souhaitez passer à une autre clé, vous devez le faire après avoir restauré la clé qui a été retirée.

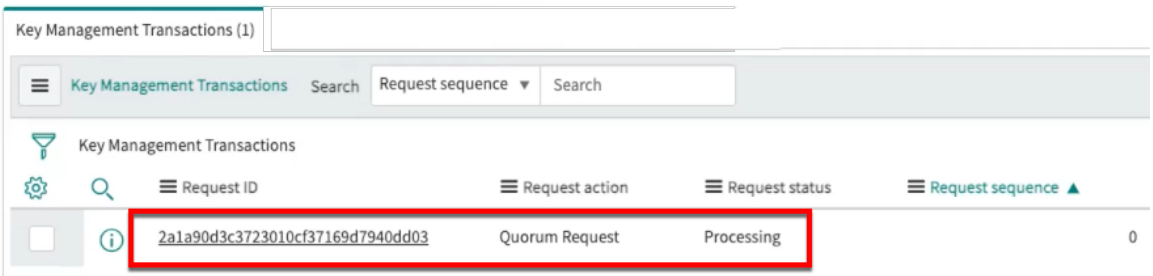
Si la clé gérée par le client retirée n'est pas restaurée dans le délai de ServiceNow conservation des sauvegardes (voir la procédure opérationnelle standard (pour plus d'informations), les sauvegardes de votre base de données d'instance ne seront plus accessibles. Les données de sauvegarde perdues de cette manière ne sont pas récupérables.

4. Sélectionnez **OK** pour retirer la clé.
   Sélectionnez **Annuler** en cas de doute sur la fonction de retrait de clé.
   Vous revenez à l'écran Définition de clé et un message de confirmation s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Actualisez la page Définition de clé pour afficher la demande de retrait en attente.



Si la politique de contrôle du quorum a été activée, le workflow d'approbation doit être terminé pour terminer le retrait de clé. Consultez Gérer le contrôle du quorum pour en savoir plus.

Réapprovisionner une clé gérée par le client

Une fois qu'une opération de retrait de clé est terminée, votre clé gérée par le client doit être réapprovisionnée dans votre instance.

Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Remarque :
Cette section s'applique uniquement si vous disposez d'une licence de retrait et de réapprovisionnement de Cloud Encryption.

Procédure

1. Accéder à Now Support et accéder à **Catalogue de services** > **Catalogue** > **Gestion de l'instance** > **Restauration d'instance : réapprovisionnement de la clé gérée**.
2. Cliquez sur **Demander**.
3. Dans la fenêtre **Restauration d'instance - Clé gérée de réapprovisionnement** , sélectionnez votre instance dans la liste déroulante **Sélectionner une instance** .
4. Téléchargez le certificat d'encapsulation en cliquant sur le texte du **certificat d'enrubannage** .

Avertissement :
Vous devez télécharger un nouveau certificat d'encapsulation chaque fois que vous alternez ou chargez une clé gérée par le client.

5. Préparez votre clé pour le chargement.
   Pour obtenir des détails sur ce processus, consultez Préparer votre clé gérée par le client.
6. Dans la section **Étape 4** , cliquez sur **Parcourir et charger** pour charger votre clé enveloppée à partir de votre appareil local.
   Une fois votre clé téléchargée, vous pouvez voir la clé sous **Téléchargé sous le fichier avec succès**. Si vous devez télécharger à nouveau la clé, cliquez sur **Supprimer le fichier** et téléchargez à nouveau votre clé comme décrit dans les étapes précédentes.
7. Cliquez sur **la touche Rotation** pour terminer le réapprovisionnement.

Politique de contrôle du quorum

La politique de contrôle du quorum spécifie le nombre minimal d'approbations requises parmi le nombre total d'approbateurs sélectionnés pour atteindre le quorum pour le retrait des clés gérées par le client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

⚠ Avertissement :
Vous devez signer un addendum légal pour activer la fonctionnalité de retrait de clé. L'option Paramètres de la politique de contrôle du quorum est disponible lorsque la fonction de retrait est activée, sinon le module n'est pas visible dans le menu de l'application. Après le retrait de la clé, votre instance n'est plus disponible tant que la clé de chiffrement n'est pas réapprovisionnée et qu'elle n'est pas de nouveau active.

Dans certaines circonstances, vous voudrez peut-être créer un retrait de clé. Vous devez d'abord demander la fonctionnalité de retrait de clé à partir de Service et assistance client.

La politique de contrôle du quorum spécifie le nombre minimal d'approbations requises parmi le nombre total d'approbateurs sélectionnés pour atteindre le quorum pour le retrait des clés gérées par le client. Par exemple, il y a un total de cinq approbateurs, mais seulement quatre approbations sont nécessaires pour atteindre le quorum. Lorsque quatre approbations sont obtenues, la demande de retrait est traitée et la clé retirée.

Chaque fois qu'une opération de retrait est effectuée dans un groupe activé pour l'approbation du quorum, un workflow pour l'approbation du quorum est déclenché. Une notification par e-mail est envoyée à tous les utilisateurs qui peuvent accorder l'approbation. Les tâches sont également générées dans les comptes des approbateurs, qu'ils voient sur le tableau de bord lorsqu'ils se connectent à leur ServiceNow compte.

Les utilisateurs peuvent accorder des approbations à partir de l'instance, de l'e-mail ou de la page Opérations de gestion des clés. L'opération de retrait de clé est bloquée jusqu'à ce que le quorum soit atteint.

Une fois le nombre minimal d'approbateurs atteint, le quorum est atteint et le retrait de clé se déclenche. Le retrait est effectué et consigné, y compris les noms des utilisateurs qui ont approuvé la demande.

Reportez-vous à la section Configurer les paramètres des politiques de contrôle du quorum pour plus de détails sur la configuration.

Configurer les paramètres des politiques de contrôle du quorum

Pour configurer les paramètres des politiques de contrôle du quorum, procédez comme suit.

Avant de commencer

Rôles requis : sn_kmf.admin

Pourquoi et quand exécuter cette tâche

⚠ Avertissement :
Vous devez signer un addendum légal pour activer la fonctionnalité de retrait de clé. L'option Paramètres de la politique de contrôle du quorum devient disponible lorsque la fonction de retrait est activée, sinon le module n'est pas visible dans le menu de l'application. Après le retrait de la clé, votre instance n'est plus disponible tant que la clé de chiffrement n'est pas à nouveau active.

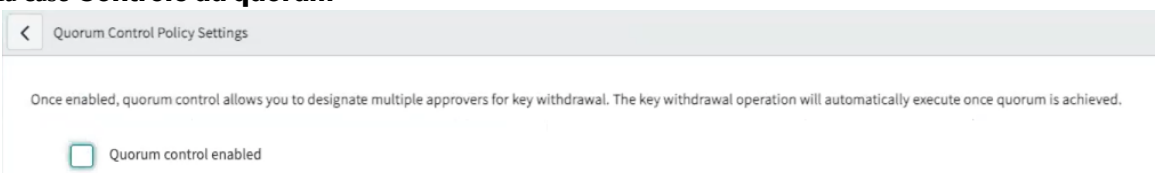
Procédure

1. Demandez la fonctionnalité de retrait de clé à partir de Service et assistance client.
2. Accédez à la **Gestion de clé de chiffrement dans le cloud** > **Paramètres des politiques de contrôle du quorum**.

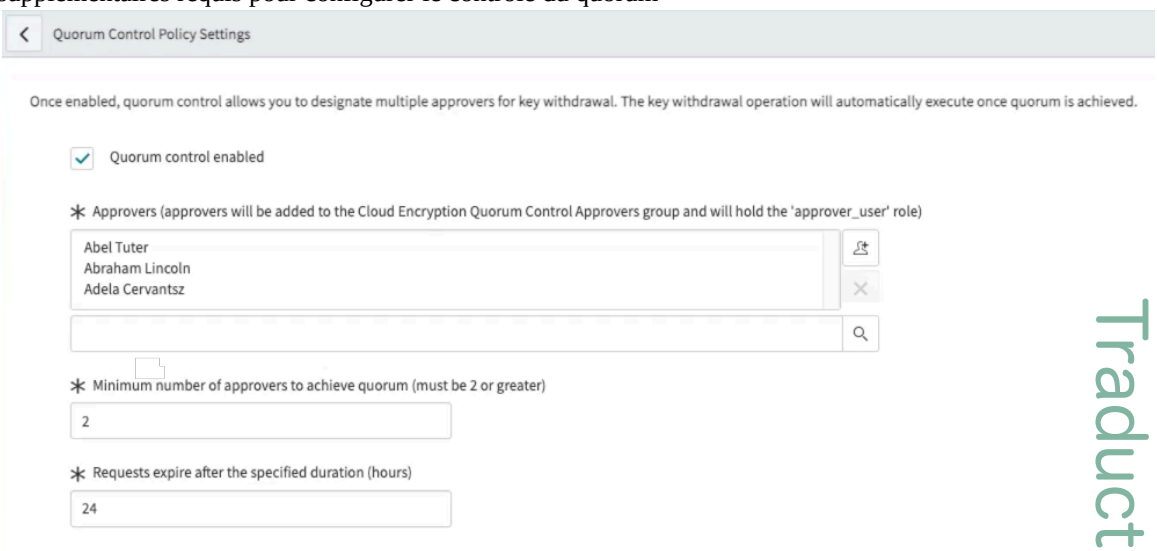
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cochez la case **Contrôle du quorum**



activé .
Les champs supplémentaires requis pour configurer le contrôle du quorum



apparaissent.

4. Renseignez les champs pour remplir le formulaire.

5. Cliquez sur **Envoyer**.
Un message de confirmation s’affiche.

Que faire ensuite

Les actions de retrait sont disponibles dans Opérations de gestion des clés.

Gérer le contrôle du quorum

Une fois qu’un workflow d’opération de retrait est déclenché, les actions de quorum peuvent être gérées à partir de la page Opérations de gestion des clés. L’opération de retrait de clé est bloquée jusqu’à ce que le quorum soit atteint.

Avant de commencer

Rôle requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

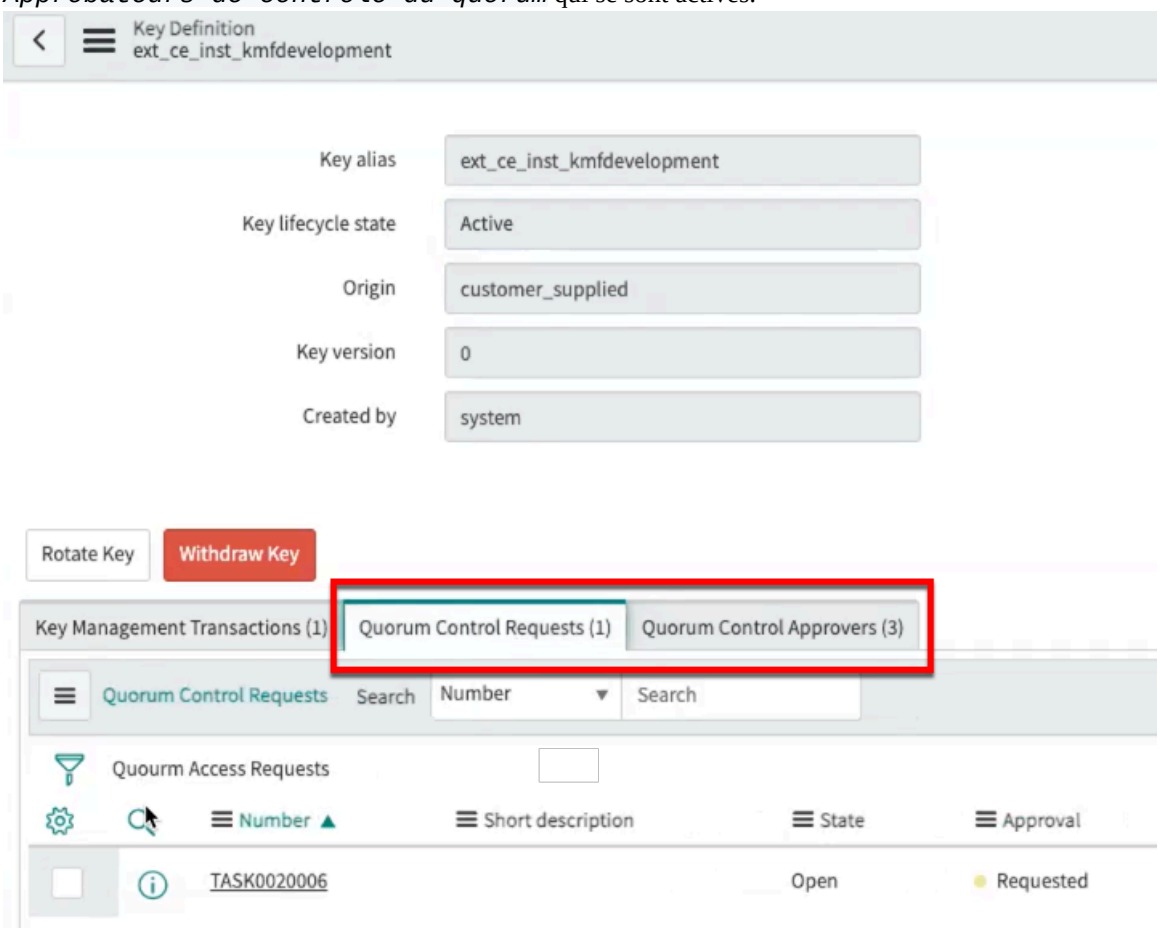
Lorsque le quorum a été approuvé ou rejeté, le demandeur du retrait de clé reçoit un e-mail indiquant si le quorum a été atteint ou refusé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Effectuez les étapes de retrait d'une clé gérée par le client trouvée dans Opérations de gestion des clés.
2. Affichez les *onglets Demandes de contrôle* du *quorum et Approbateurs de contrôle du quorum* qui se sont activés.

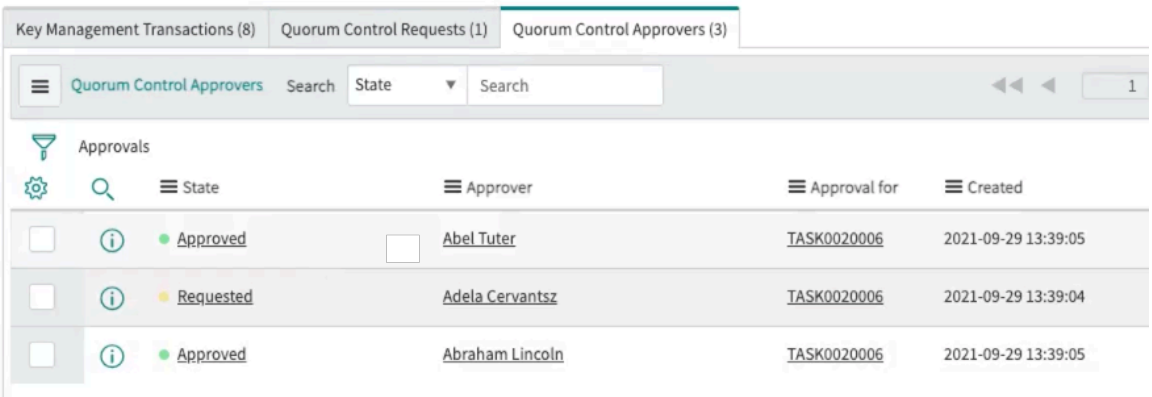


3. Ouvrez le **Demandes de contrôles du quorum** pour afficher la demande réelle qui est créée.
   - État :
     - Ouvert : l'action de retrait de clé est en attente que le quorum soit atteint.
     - Fermé terminé : le quorum a été atteint et aucune autre action ne peut être effectuée sur cette demande de quorum particulière.
   - Approbation:
     - Demandé : des e-mails d'approbation ont été envoyés et le workflow a été déclenché pour atteindre le quorum.
     - Approuvé : la clé sera retirée et l'instance sera arrêtée.
     - Refusé : la demande de quorum est annulée et aucune autre action n'est entreprise avec cette demande. Une nouvelle demande de retrait sera nécessaire pour retirer la clé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Ouvrez l'onglet Approbateurs de contrôle du quorum pour afficher la liste des approbateurs et l'état de la demande d'approbation.



État :

- Demandé : l'approbateur n'a pas encore donné suite à la demande d'approbation.
- Approuvée : la demande a été approuvée à partir de l'e-mail ou de la page d'approbations.

5. Sélectionnez l'onglet **Transactions de gestion des clés** pour afficher la progression de l'étape de demande pour le retrait de clé.
   - Étape 0 - Demande de quorum : demande de quorum réelle. La demande de quorum doit être complétée afin de déclencher les étapes de retrait de clés.
   - Étape 1 - Retrait de la clé : L'étape de retrait de la clé. Celui-ci est composé des étapes deux à sept.
   - Étape 2 - Request_preparation : crée une demande de déclenchement, d'emballage et de rotation.
   - Étape 3 - request_integrity_check : valide que la demande est légitime et sécurisée.
   - Étape 4 - request_validation : valide qu'il y a une demande en cours et qu'une seule demande de rotation peut être traitée à la fois.
   - Étape 5 - hsm_key_delete : Effectue l'appel à KeySecure pour supprimer la clé active.
   - Étape 6 - key_metadata_withdraw : convertit l'état du cycle de vie des métadonnées de clé actives en « détruit ».
   - Étape 7 - post_withdraw : effectue un appel pour arrêter l'instance.

Traduction automatique

Approuver ou refuser une demande de contrôle du quorum

Approuvez ou refusez une demande de contrôle du quorum des transactions de gestion des clés.

Pourquoi et quand exécuter cette tâche

Lorsqu'une demande de quorum a été créée, le nombre minimal d'approbations est requis par les membres. Une fois qu'un workflow d'opération de retrait est déclenché, les actions de quorum peuvent être gérées à l'aide de plusieurs méthodes. Les utilisateurs peuvent accorder des approbations à partir de la page Opérations de gestion des clés, de Mes approbations dans l'instance ou directement à partir de l'e-mail de demande. L'opération de retrait de clé est bloquée jusqu'à ce que le quorum soit atteint.

Cette procédure décrit comment approuver ou refuser une demande de quorum à partir de la page Opérations de gestion des clés.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Procédure

1. Accédez à la **Tout** > **Gestion de clé de chiffrement dans le cloud** > **Transactions de gestion des clés** > **Approbateurs de contrôle de quorum**.
2. Sélectionnez votre nom d'utilisateur dans la table.
3. Approuvez ou refusez la demande.

Approuver ou refuser une demande de quorum

Lorsqu'une demande de quorum a été créée, le nombre minimal d'approbations est requis par les membres. Une fois qu'un workflow d'opération de retrait est déclenché, les actions de quorum peuvent être gérées à l'aide de plusieurs méthodes. Les utilisateurs peuvent accorder des approbations à partir de la page Opérations de gestion des clés, de **Mes approbations** dans l'instance ou directement à partir de l'e-mail de demande. L'opération de retrait de clé est bloquée jusqu'à ce que le quorum soit atteint.

Avant de commencer
Rôles requis : sn_kmf.admin ou sn_kmf.cryptographic_manager

Transactions de gestion des clés

Le sous-module Transactions de gestion des clés affiche toutes les transactions qui ont eu lieu pour les clés dans votre ServiceNow instance.

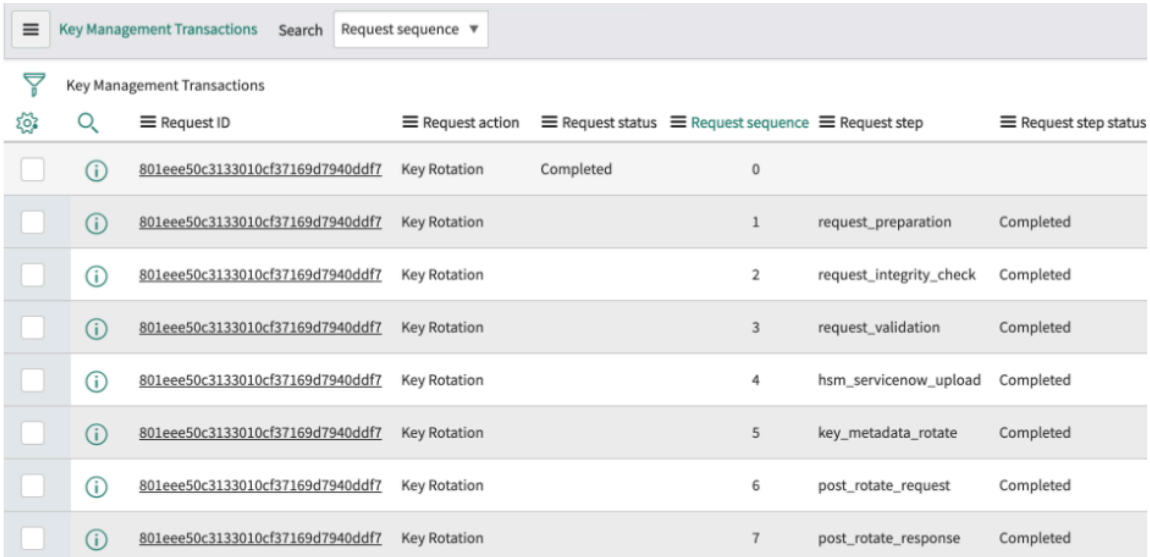
- Une transaction clé est définie par les éléments suivants :
  - Composé de plusieurs étapes de demande.
  - Un *`ID de demande`* unique est partagé pour toutes les étapes de la demande.
  - L'étape initiale, la séquence de demande 0, d'une transaction fournit l'état actuel de la transaction globale.

    Comme le montre l'image ci-dessous, l'étape initiale 0 a un *`état de demande`* global Terminé.
- Les éléments suivants peuvent être identifiés pour la transaction par l'étape de demande individuelle :
  - L'ordre de chaque étape d'une transaction peut être identifié par le numéro de séquence de l'étape.
  - L'état de chaque transaction est visible à travers l'état de l'étape de demande.
  - Si des étapes au-delà de l'étape initiale échouent, la transaction globale a l'état Échoué. Si toutes les étapes sont terminées, le statut de la transaction est également terminé.

L'écran suivant est un exemple du type d'informations qui s'affichent avec une ServiceNow rotation de touches.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le tableau suivant répertorie les informations de champ disponibles sur la page Transactions de gestion des clés.

Transactions de gestion des clés

Champ	Description
ID de demande	ID unique généré par le système pour l'action en cours d'exécution Un ID de demande est partagé pour toutes les étapes de la demande.
Action de demande	Affiche l'action de l'opération clé en cours d'exécution.
État de la demande	• Traitement : une demande a été saisie, mais n'est pas encore terminée. • Terminée : la demande a été effectuée avec succès. • Échec : un problème s'est produit et le processus n'est pas terminé. **Remarque :** Contactez Service et assistance client et fournissez le numéro de demande à l'endroit où la défaillance s'est produite.
Alias de la clé	Entrée alphanumérique.
État du cycle de vie de la clé	Voir États du cycle de vie des clés du cadre de travail de gestion des clés pour les définitions.
Origine	• ServiceNow clé • Clé gérée par le client
Version de la clé	Lorsqu'une clé tourne, le numéro de version augmente.
Séquence de demande	Affiche l'ordre dans lequel une demande est traitée dans le système.
Étape de demande	Affiche si une étape est en cours de traitement dans le système pendant la rotation des clés. La quantité et le contenu des étapes varient en fonction du type d'opération clé effectuée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Transactions de gestion des clés (suite)

Champ	Description
	1. request_preparation : crée une demande de déclenchement, d'emballage et de rotation. 2. request_integrity_check : valide que la demande est légitime et sécurisée. 3. request_validation : valide qu'il y a une demande en cours et qu'une seule demande de rotation peut être traitée à la fois. 4. attachment_process : extrait le matériel clé encapsulé de la pièce jointe. (Étape supplémentaire lors de la rotation d'une clé gérée par le client.) 5. hsm_<type de clé>_upload : télécharge le matériel de clé encapsulée vers le HSM, KeySecure. 6. key_metadata_rotate : génère les nouvelles métadonnées de clé. 7. post_rotate_request : envoie une demande pour effectuer la rotation de clés. 8. post_rotate_response : réponse pour effectuer la rotation de clés en fonction de la demande de l'instance client. **Remarque :** Indiquez l'étape de demande pour Service et assistance client analyser la progression de l'état au cas où une étape de demande ne se terminerait pas.
État de l'étape de la demande	• Terminé : la rotation est réussie. • Échec : échec de la rotation. **Remarque :** Indiquez l'étape de demande pour Service et assistance client analyser la progression de l'état au cas où une étape de demande ne se terminerait pas.

Journalisation de Chiffrement dans le cloud

En savoir plus sur les options de journalisation pour Chiffrement dans le cloud.

Tables de journalisation de Chiffrement dans le cloud

Utilisez ces tables pour trouver les informations de connexion relatives aux transactions Chiffrement dans le cloud sur votre instance.

Table	Description
Métadonnées de Chiffrement dans le cloud [dare_key_metadata]	Les métadonnées de Chiffrement dans le cloud capturent les métadonnées clés de gestion du cycle de vie. Sur cette table, vous trouverez des informations clés sur le cycle de vie, l'état et la version. Cette table est mise à jour après chaque opération clé.
Transactions de gestion des clés [dare_key_request]	Transactions de gestion des clés capture les informations sur les transactions de gestion des clés. Sur cette table, vous pouvez trouver la journalisation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	de chaque étape d'une transaction. La table enregistre toute information d'erreur pour une transaction dans le champ de **message d'erreur** .
Audits sys[sys_audit]	La table Audits système capture, insère et met à jour tous les enregistrements audités sur votre instance. Dans cette table, vous trouverez les changements apportés aux enregistrements sur votre instance, la date à laquelle ces changements ont été apportés et le compte d'utilisateur à l'origine de ce changement.

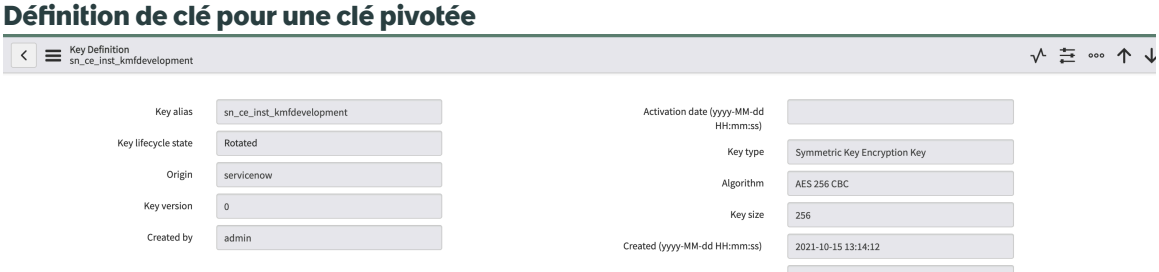
Surveiller les opérations de rotation des clés

Utilisez la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata] pour rechercher des informations sur le cycle de vie de votre clé. Dans ce tableau, vous trouverez des informations telles que l'origine, la date d'activation, l'état et la version de vos clés.

Utilisez la table Transactions de gestion des clés [dare_key_request] pour surveiller les transactions des opérations clés. Dans ce tableau, vous trouverez toutes les demandes relatives à vos clés, y compris l'état, l'état et l'étape du processus dans laquelle la demande se trouve. Les demandes terminées sont conservées sur cette table avec l'état **Terminé** .

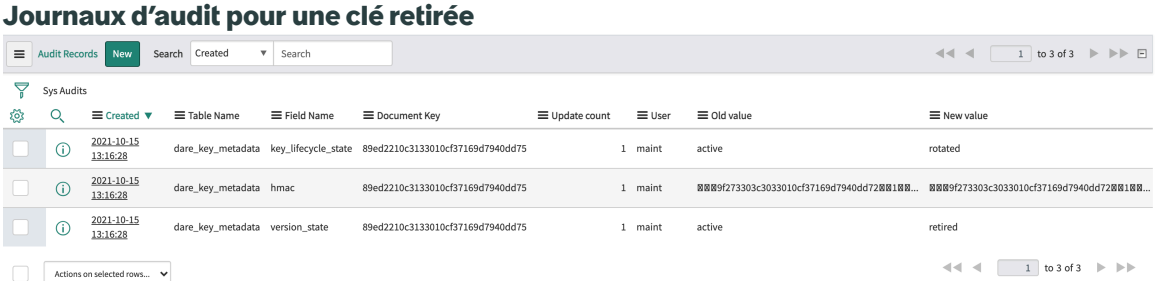
Cet exemple montre une opération de rotation de clés. Au cours de cette opération, l'état de l'ancien cycle de vie de la clé passe d'Actif à Pivoté, et l'état de la version passe d'Actif à Mis hors service.

Définition de clé pour une clé pivotée



En examinant la table Audits système[sys_audit], les administrateurs peuvent voir les modifications apportées aux enregistrements dans la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata]. Les administrateurs peuvent voir quels enregistrements ont été mis à jour et quand. Les entrées du journal enregistrent également le champ qui a été modifié, ainsi que l'ancienne et la nouvelle valeur.

Journaux d'audit pour une clé retirée

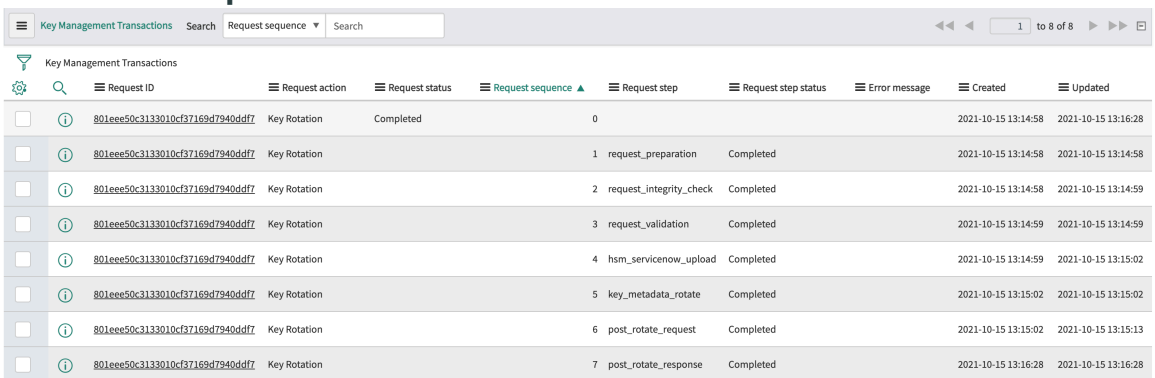


Les administrateurs peuvent afficher les enregistrements sur la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata]. Dans les enregistrements d'audit ci-dessous, l'état de la demande est passé de En cours de traitement à Terminé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journaux d'audit pour une clé retirée



Key Management Transactions | Search: Request sequence | Search | 1 to 8 of 8

Key Management Transactions

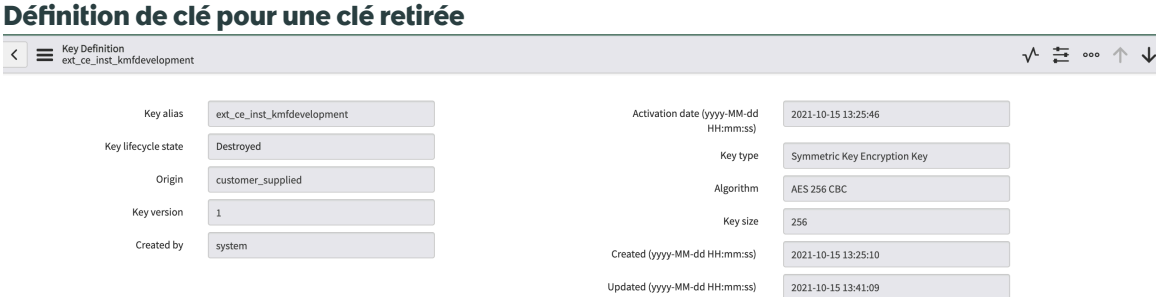
Request ID	Request action	Request status	Request sequence	Request step	Request step status	Error message	Created	Updated
801eee50c3133010cf37169d7940ddf7	Key Rotation	Completed	0				2021-10-15 13:14:58	2021-10-15 13:16:28
801eee50c3133010cf37169d7940ddf7	Key Rotation		1	request_preparation	Completed		2021-10-15 13:14:58	2021-10-15 13:14:58
801eee50c3133010cf37169d7940ddf7	Key Rotation		2	request_integrity_check	Completed		2021-10-15 13:14:58	2021-10-15 13:14:59
801eee50c3133010cf37169d7940ddf7	Key Rotation		3	request_validation	Completed		2021-10-15 13:14:59	2021-10-15 13:14:59
801eee50c3133010cf37169d7940ddf7	Key Rotation		4	hsm_servicenow_upload	Completed		2021-10-15 13:14:59	2021-10-15 13:15:02
801eee50c3133010cf37169d7940ddf7	Key Rotation		5	key_metadata_rotate	Completed		2021-10-15 13:15:02	2021-10-15 13:15:02
801eee50c3133010cf37169d7940ddf7	Key Rotation		6	post_rotate_request	Completed		2021-10-15 13:15:02	2021-10-15 13:15:13
801eee50c3133010cf37169d7940ddf7	Key Rotation		7	post_rotate_response	Completed		2021-10-15 13:16:28	2021-10-15 13:16:28

Journalisation des opérations de retrait de clés

Les informations de connexion lors du retrait des clés sont stockées dans la table Audits [sys_audit]. Ces informations de connexion contiennent des informations sur qui a initié le retrait de clé et quand le retrait a eu lieu.

Cet exemple montre une opération de retrait de clé. Au cours de cette opération, l'état du cycle de vie de la clé est mis à jour, passant de « Généré » à « Actif », puis « Détruit ». La version de clé est mise à jour de Inconnue à Active, puis à Retirée.

Définition de clé pour une clé retirée

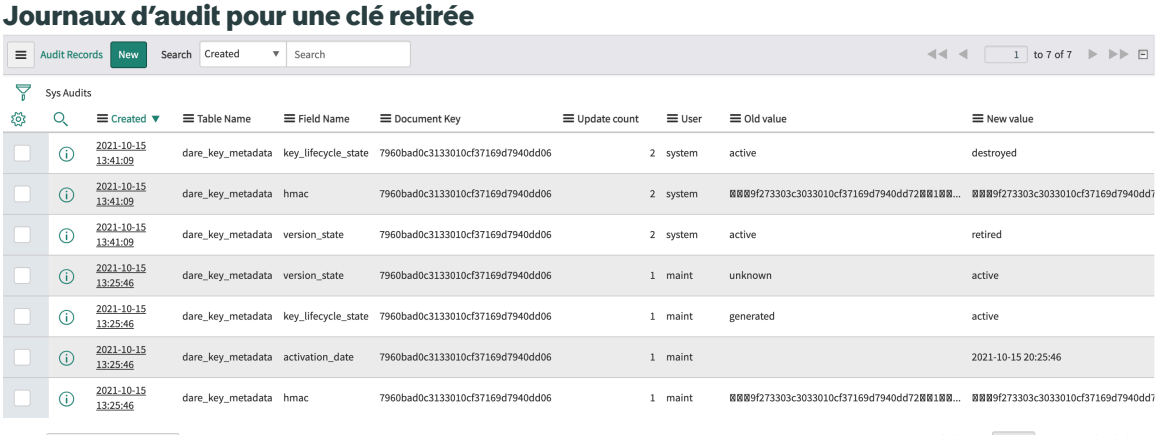


Key Definition
ext_ce_inst_kmfdevelopment

Key alias	ext_ce_inst_kmfdevelopment	Activation date (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:25:46
Key lifecycle state	Destroyed	Key type	Symmetric Key Encryption Key
Origin	customer_supplied	Algorithm	AES 256 CBC
Key version	1	Key size	256
Created by	system	Created (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:25:10
		Updated (yyyy-MM-dd HH:mm:ss)	2021-10-15 13:41:09

En examinant la table Audits Sys[sys_audit], les administrateurs peuvent modifier la table Métadonnées de clé de chiffrement dans le cloud [dare_key_metadata].

Journaux d'audit pour une clé retirée



Audit Records | New | Search: Created | Search | 1 to 7 of 7

Sys Audits

Created	Table Name	Field Name	Document Key	Update count	User	Old value	New value
2021-10-15 13:41:09	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	2	system	active	destroyed
2021-10-15 13:41:09	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	2	system	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7
2021-10-15 13:41:09	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	2	system	active	retired
2021-10-15 13:25:46	dare_key_metadata	version_state	7960bad0c3133010cf37169d7940dd06	1	maint	unknown	active
2021-10-15 13:25:46	dare_key_metadata	key_lifecycle_state	7960bad0c3133010cf37169d7940dd06	1	maint	generated	active
2021-10-15 13:25:46	dare_key_metadata	activation_date	7960bad0c3133010cf37169d7940dd06	1	maint		2021-10-15 20:25:46
2021-10-15 13:25:46	dare_key_metadata	hmac	7960bad0c3133010cf37169d7940dd06	1	maint	▯▯▯9f273303c3033010cf37169d7940dd72▯▯1▯▯...	▯▯▯9f273303c3033010cf37169d7940dd7

Actions on selected rows... | 1 to 7 of 7

Détection de sabotage

Utilisez la détection d'altération pour améliorer la sécurité en détectant les changements non autorisés de vos paramètres de contrôle du quorum.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Traduction automatique

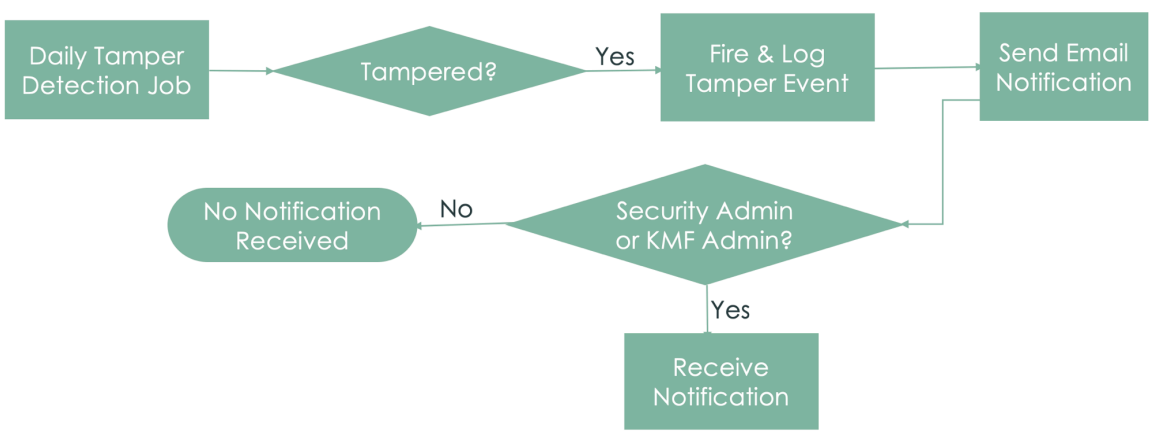
Processus de détection d'inviolabilité

Lorsqu'elle est activée, la détection d'altération valide vos paramètres de contrôle du quorum en vérifiant toute modification non autorisée (altération). La détection de falsification utilise le code d'authentification de message basé sur le hachage (HMAC).

1. Lorsqu'un paramètre est modifié ou créé, votre instance crée un HMAC. Le HMAC est basé sur la valeur de l'enregistrement de paramètre (dare_property).
2. Chaque fois que votre instance utilise ces paramètres, la détection de falsification les valide à l'aide du HMAC.
3. Si le paramètre est validé avec succès, il peut être utilisé par la plateforme, sinon il ne le peut pas.

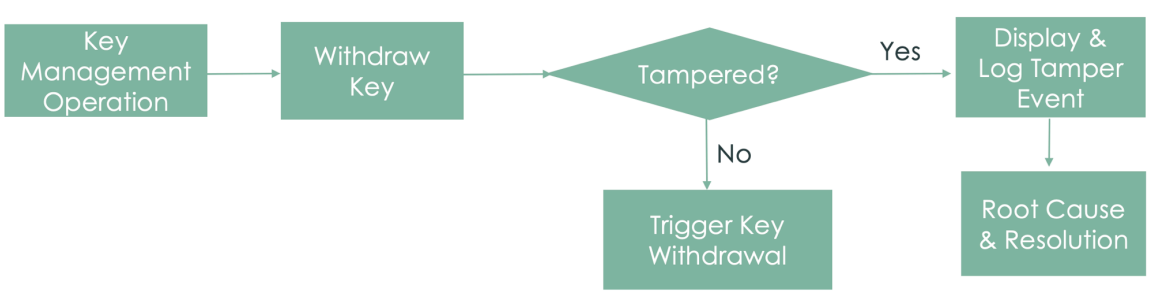
La détection de falsification s'exécute quotidiennement sur votre instance

La détection d'altération vérifie l'altération de vos paramètres à l'aide d'une tâche planifiée quotidienne et signale les échecs de validation dans vos journaux de nœud et de sécurité. La détection de falsification envoie une notification aux administrateurs Security et KMF en cas d'échec de validation.



La détection de falsification s'exécute avant d'exécuter un retrait de clé

La détection d'effraction valide également vos propriétés lorsque vous demandez un retrait de clé. Si vos paramètres ne passent pas la validation, le retrait de clé ne s'exécute pas. Dans ce cas, vous devez résoudre tous les problèmes de validation avant que le retrait de clé puisse avoir lieu.



Identification de l'altération

La détection de falsification met à jour vos journaux en cas d'échec de validation.

Si la détection d'altération ne parvient pas à valider l'un de vos paramètres de contrôle du quorum, ces défaillances s'affichent dans vos journaux de nœud et de sécurité. L'entrée de journal inclut la sys_id de l'enregistrement des paramètres (dare_property) qui n'a pas été validé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

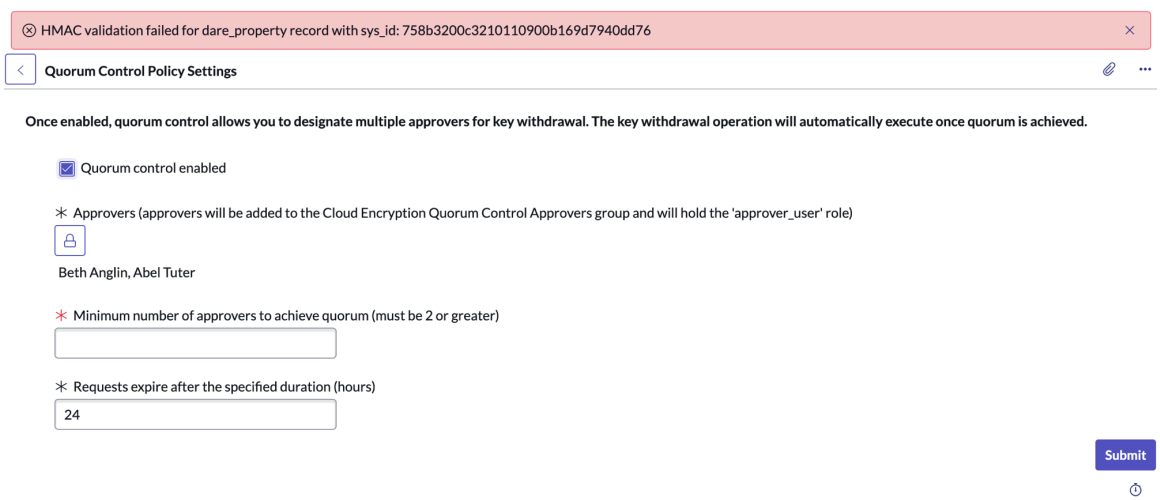
```
2022-06-28 13:45:46 (582) Default-thread-5
 B6FAC1F6C3D01110CF37169D7940DD6E txid=231c4d72c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 776e3200c3210110900b169d7940dd76 failed HMAC validation

2022-06-28 13:47:35 (264) Default-thread-8
 B6FAC1F6C3D01110CF37169D7940DD6E txid=8e8cc972c310 SEVERE
 HMAC_VALIDATION_FAILED:The dare_property record with sys_id:
 758b3200c3210110900b169d7940dd76 failed HMAC validation
```

La connexion affiche des informations similaires à ces exemples en cas d'échec de validation. Les validations réussies n'apparaissent pas dans les journaux.

La détection de falsification affiche un message d'avertissement sur la page des paramètres de contrôle du quorum

Si la validation d'un paramètre de contrôle du quorum échoue, un avertissement s'affiche lorsque vous consultez la page des paramètres de la politique de contrôle du quorum sur votre instance. L'avertissement inclut la sys_id de l'enregistrement des paramètres (dare_property) dont la validation a échoué.



La détection d'altération envoie des notifications aux utilisateurs disposant des `Security Admin` rôles et `KMF Admin`

Si la détection d'altération ne parvient pas à valider l'un de vos paramètres de contrôle du quorum, vos administrateurs de sécurité et KMF reçoivent une notification similaire à cet exemple.

Subject: IMPORTANT: Cloud Encryption Properties Tampering Detected

The following list of Cloud Encryption properties appear to have been tampered.
Contact ServiceNow support for additional information and how to correct this issue.

Tampered properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

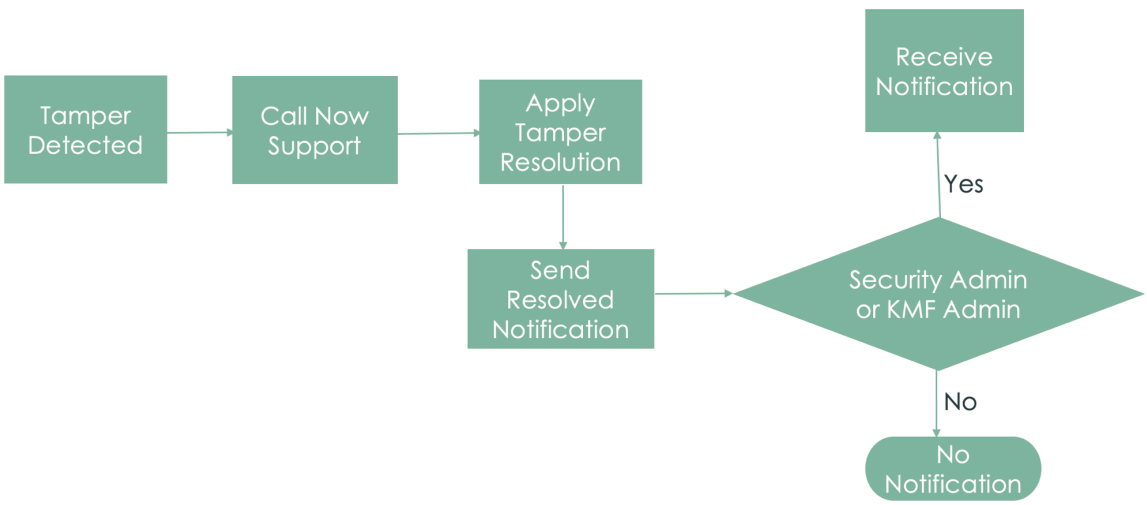
Ref:MSG0000109_q5pzYMS7hcgHXAoUhipc

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résolution des problèmes d'altération avec ServiceNow assistance

Important :
Les échecs de validation de la détection des falsifications ne peuvent être résolus qu'avec l'aide de l'assistance ServiceNow .



Si la détection de sabotage ne parvient pas à valider l'un de vos paramètres de contrôle du quorum, contactez ServiceNow le support pour obtenir de l'aide afin de résoudre le problème. Une fois qu'un agent d'assistance a résolu l'échec de validation, les administrateurs de sécurité et KMF reçoivent une notification indiquant que le problème a été résolu.

Subject: IMPORTANT: Cloud Encryption Properties Reset

At your request, ServiceNow support has reset the following list of Cloud Encryption properties to their default values.
If you did not request this action, contact ServiceNow support immediately.

Reset properties:
com.glide.dare_key_mgmt.quorum.approvers(903a3212c3210110cf37169d7940dda8)

Ref:MSG0000116_0HAz8U1r59OmppqV8ysg

Chiffrement intégral du disque

Le chiffrement complet du disque (FDE) applique le chiffrement à l'ensemble du système de stockage au sein du serveur de base de données uniquement, car il s'agit du seul composant de stockage des données client. FDE ne protège que contre la perte physique ou le vol des périphériques de stockage. Lorsque des serveurs de disques chiffrés sont mis sous tension et fournissent des données, le chiffrement n'offre aucune protection supplémentaire.

Chiffrement intégral du disque

Le chiffrement complet du disque peut être pertinent pour les organisations fortement réglementées ServiceNow , mais peut ajouter des coûts importants au déploiement d'un client. Les mesures mises en place pour ServiceNow atténuer la perte ou le vol des appareils de stockage peuvent également être un facteur dans son choix.

Du point de Now Platform vue, toutes les données sont déchiffrées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les environnements commerciaux utilisent le chiffrement complet du disque (FDE) avec du matériel ou des périphériques de stockage validés FIPS 140 qui sont en cours de validation, ainsi qu'une option matérielle dédiée moyennant des ServiceNow frais supplémentaires. FDE s'applique au matériel lui-même, et fournit donc un chiffrement au repos pour toutes les données stockées dans chaque instance qui vous est attribuée.

Pour plus de détails sur la sélection des options matérielles FDE et dédiées, contactez votre ServiceNow représentant.

Chiffrement Edge

ServiceNow® Chiffrement Edge ™ chiffre les données sensibles dans les locaux de votre entreprise avant de les envoyer sur Internet à votre ServiceNow instance (chiffrées à la volée), où elles restent chiffrées au repos.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de Chiffrement Edge.

Plan

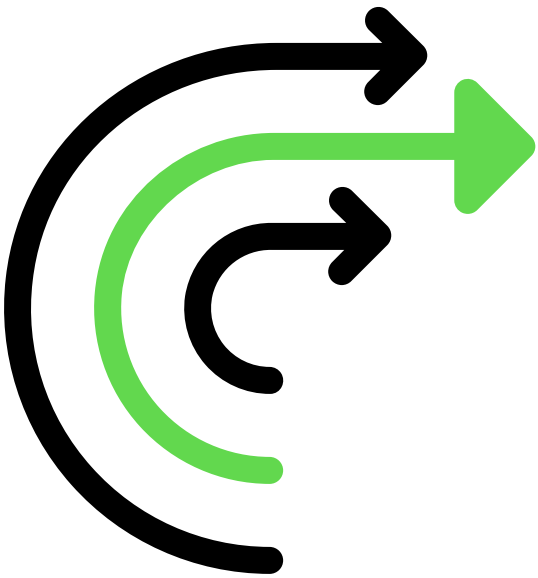


Découvrez comment planifier Chiffrement Edge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Installer



Installez Chiffrement Edge.

Mise à niveau de Chiffrement Edge

Référence de mise à niveau



Savoir comment mettre à niveau Chiffrement Edge.

Configurer



Découvrez comment configurer Chiffrement Edge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer Chiffrement Edge

Chiffrement Edge est un système de chiffrement réseau qui réside sur votre réseau et qui chiffre et déchiffre les données sensibles lorsqu'elles transitent entre votre centre de données et le ServiceNow cloud.

Qu'est-ce que Chiffrement Edge ?

Également appelé chiffrement « côté client », Edge exige que tout le trafic utilisateur bidirectionnel passe par des proxys conservés sur votre infrastructure. Vous avez un contrôle total sur la gestion de vos clés, car celles-ci sont stockées dans votre proxy sur votre infrastructure. Ils Now Platform ne peuvent pas déchiffrer votre texte chiffré pour accéder à vos clés.

Cette Chiffrement Edge fonctionnalité est une option payante supplémentaire qui vous permet de contrôler le chiffrement de bout en bout de la gestion de vos données et clés. Chiffrement Edge utilise une application proxy, fournie et installée par ServiceNow vous au sein de votre propre réseau. Cette application proxy tokenise les modèles de données spécifiés ou chiffre les champs de chaîne, les champs de date, les champs de date/heure et les données de pièce jointe avant qu'ils ne soient envoyés de votre environnement à votre instance. L'application proxy déchiffre également les mêmes données, encore une fois uniquement au sein de votre propre réseau, à l'aide de clés stockées uniquement sur votre propre réseau.

Les clés de chiffrement et la configuration appropriées existent uniquement sur le proxy Edge au sein de votre réseau et ne sont pas visibles par ServiceNow. Les données sont cryptées à partir du moment où elles quittent votre environnement et ne sont décryptées qu'à la récupération. À aucun moment, les données ne sont accessibles en clair par ServiceNow les systèmes ou le personnel.

Qui utilise Chiffrement Edge

Seul un utilisateur connecté à l'instance via un serveur proxy sur votre réseau peut afficher des données chiffrées en texte clair. De même, seul un utilisateur security_admin connecté à une instance via un serveur proxy de votre réseau peut configurer et administrer Chiffrement Edge.

Étant donné que le serveur proxy réside dans votre réseau, vous possédez et gérez les clés de chiffrement, et elles ne sont jamais envoyées à l'instance. Par conséquent, n'affiche ServiceNow jamais de données sensibles en texte clair.

En plus de la configuration du proxy Edge et de la gestion des règles, vous êtes responsable des exigences habituelles d'exploitation d'un serveur au sein de votre environnement (y compris l'hébergement, le routage, la sauvegarde, la configuration DNS, etc.) pour activer et prendre en charge vos proxys Edge.

Chiffrement et tokenisation

Chiffrement Edge prend en charge à la fois le chiffrement (via des configurations de chiffrement) et la tokenisation (via des schémas de chiffrement) comme moyen de protéger vos informations sensibles.

Configurations de chiffrement

Vous pouvez chiffrer des champs individuels à l'aide de configurations de chiffrement. Chiffrement Edge prend en charge les clés de chiffrement AES 128 bits et AES 256 bits. Chiffrement Edge Prend en charge les types de chiffrement standard, préservant l'égalité et préservant l'ordre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Outre les pièces jointes, vous pouvez chiffrer les types de champs suivants :

- Date
- E-mail
- Date/Heure
- HTML
- Adresse IP
- Journal
- Entrée de journal
- Texte de plusieurs lignes
- Texte sur ligne unique
- Chaîne
- URL

Remarque :

Si un champ Journal marqué pour chiffrement est ajouté au flux d'activité, toutes les entrées d'utilisateur dans ce champ sont chiffrées dans le flux d'activité.

Les caractères codés sur plusieurs octets dans les types de champs pris en charge peuvent être chiffrés.

Vous pouvez également chiffrer les types de variables de catalogue de services suivants :

- Types de chaînes
  - Texte sur ligne unique
  - Texte de plusieurs lignes
  - Texte sur ligne unique large
- Date
- Date/Heure
- URL
- E-mail
- HTML
- Adresse IP

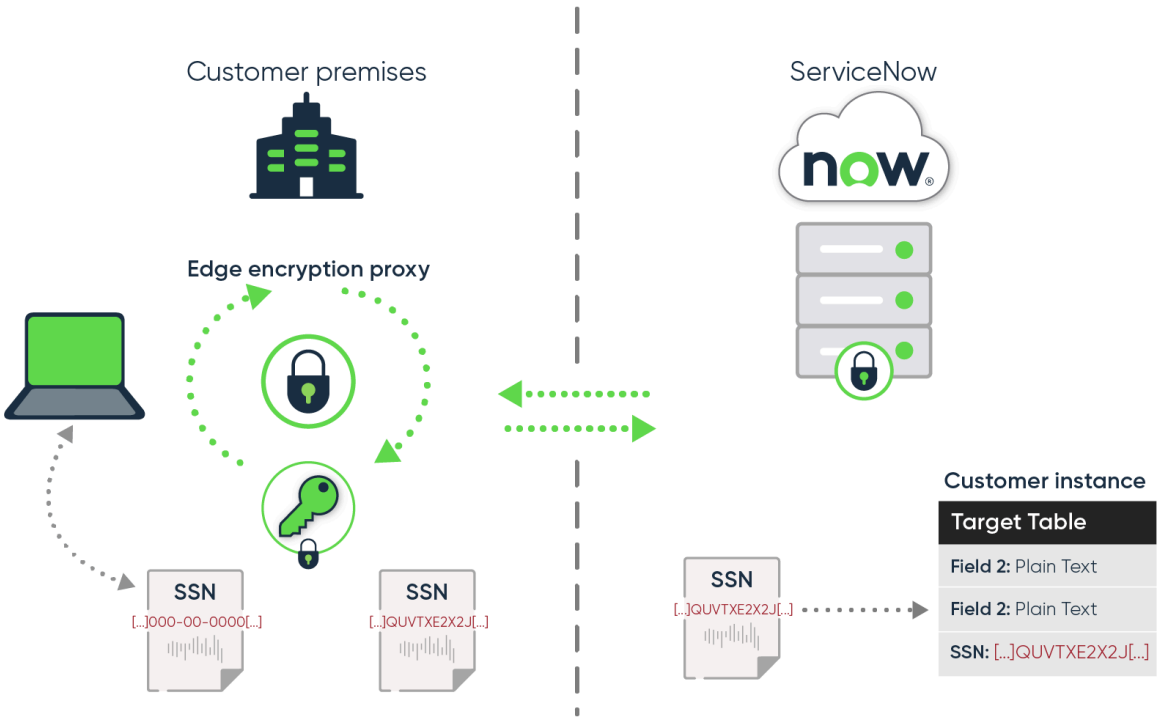
Schémas de chiffrement

Vous pouvez utiliser des schémas de chiffrement pour tokeniser des chaînes qui correspondent à des schémas réguliers, tels que les numéros de sécurité sociale et de carte de crédit. Bien que les configurations de chiffrement doivent être la principale méthode de chiffrement, utilisez des modèles de chiffrement en complément pour sécuriser les informations sensibles trouvées en dehors des champs chiffrés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le Chiffrement Edge serveur proxy nécessite une base de données MySQL dans votre réseau uniquement s'il utilise un cryptage préservant l'ordre ou des schémas de chiffrement. Les valeurs en texte clair sont stockées dans la base de données proxy de votre réseau. Pour cette raison, il est essentiel que vous sécurisiez et sauvegardez régulièrement votre base de données proxy. Pour des recommandations, reportez-vous à la section Composants de Chiffrement Edge.



Chiffrement Edge on the Now Platform

Chiffrement Edge agit comme une passerelle entre votre navigateur et votre ServiceNow instance. Le trafic provenant de votre navigateur passe par la passerelle avant d'être acheminé vers l'instance ServiceNow . La passerelle, à son tour, est configurée pour chiffrer les données sortantes qui sont marquées pour chiffrement. Le trafic entrant est déchiffré via la passerelle et l'utilisateur final voit du texte clair dans le navigateur. L'avantage de cette implémentation du point de vue du contrôle de sécurité est que le chiffrement et la gestion des clés sont gérés en externe à partir de ServiceNow.

Avantages et inconvénients

Comme pour Entreprise de Chiffrement au niveau des colonnes le chiffrement au niveau des colonnes, Chiffrement Edge il impose certaines limitations fonctionnelles au sein d'une instance en raison de la sécurité supplémentaire. Toutefois, le proxy Edge local fournit également des fonctionnalités supplémentaires relatives au tri par rapport au chiffrement au niveau des colonnes.

Avantages:

- Chiffrement Edge Fournit un contrôle absolu sur les personnes qui voient vos informations et empêche les violations de données.
- Les informations restent sur votre serveur proxy et ne quittent jamais votre réseau sans cryptage.
- Les informations sont chiffrées en transit, avant même qu'elles n'atteignent l'instance ServiceNow .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous détenez et gérez toutes vos propres clés de chiffrement. Personne d'autre, pas même ServiceNow le personnel, ne peut accéder à vos clés.
- Vous pouvez choisir la force de l'algorithme de cryptage : AES-128 ou AES-256.
- Chiffrement Edge inclut la possibilité de chiffrer le texte de chaîne, les champs de date et de date/heure, les pièces jointes, les URL et les journaux.
- Chiffrement Edge fournit le chiffrement standard, la préservation de l'égalité et la préservation de l'ordre des données au repos au sein de la base de données et de l'instance.
- Les règles de chiffrement vous permettent d'écrire des scripts personnalisés qui indiquent précisément au serveur proxy ce qu'il doit chiffrer et où placer ces informations chiffrées dans l'instance. Ces scripts sont utiles lorsque la structure des données ne correspond pas exactement à l'instance ServiceNow .
- Les schémas de chiffrement vous permettent de tokeniser des informations telles que les mots de passe.

Contre:

- Chiffrement Edge nécessite un saut de réseau supplémentaire via le cluster de proxys Edge et un traitement supplémentaire, ce qui peut ajouter un délai au trafic. Le délai de traitement supplémentaire de l'application Chiffrement Edge est négligeable par rapport au saut de réseau.
- La gestion de vos propres clés de chiffrement peut s'avérer complexe et prendre beaucoup de temps.
- Vous pouvez gérer un maximum de deux clés, sans possibilité de définir des clés différentes pour différents sous-ensembles de colonnes/données, ou pour différents rôles, et ainsi de suite
- Chiffrement Edge a pour effet secondaire que le serveur ou la plate-forme ne peut pas décrypter les données pour effectuer une manipulation des données déchiffrées. Par conséquent, les fonctionnalités et le traitement des données sur le Now Platform peuvent être limités lors du chiffrement des colonnes avec Chiffrement Edge.

À savoir avant de commencer

Étant donné que le chiffrement et la tokenisation modifient la nature de vos données, Chiffrement Edge ils peuvent affecter d'autres processus d'instance. Avant d'utiliser Chiffrement Edge, examinez attentivement l'impact sur votre instance.

Étant donné que le serveur proxy est installé et maintenu sur votre réseau, Chiffrement Edge il nécessite une administration et une gestion réseau. Passez en revue la configuration réseau requise pour garantir une implémentation fluide.

Passez en revue les rubriques suivantes pour comprendre l'impact de Chiffrement Edge sur votre instance :

- Planification pour Chiffrement Edge
- Configuration requise pour Chiffrement Edge
- Dimensionnement de votre environnement Edge Encryption
- Calculer la taille de la base de données de conservation de l'ordre et de la création de jetons
- Chiffrement Edge Limitations
- Gestion des clés pour Chiffrement Edge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composants de Chiffrement Edge

Chiffrement Edge est composé du serveur proxy qui s'exécute sur un serveur de votre réseau et du module d'extension Chiffrement EdgeChiffrement Edge qui doit être installé sur votre ServiceNow instance. Si vous utilisez des types ou des modèles de chiffrement préservant l'ordre, une base de données proxy doit également être installée sur votre réseau.

Application proxy

Lorsque vous passez par le Chiffrement Edge serveur proxy, le module d'extension Chiffrement Edge vous permet de spécifier les champs, les modèles et les pièces jointes qui doivent être chiffrés. Vous pouvez également gérer des règles de chiffrement pour chiffrer des demandes spécifiques et planifier des tâches de chiffrement en masse.

Serveur proxy

Le Chiffrement Edge serveur proxy utilise des règles de chiffrement pour identifier dans une requête HTTP ce qui doit être chiffré, le cas échéant, et le chiffre avant de transmettre la demande à l'instance. Pour le déchiffrement, le Chiffrement Edge serveur proxy examine les réponses HTTP pour toutes les données chiffrées et les déchiffre avant de renvoyer la réponse au client. Pour que ce déchiffrement se produise, toutes les requêtes et réponses HTTP doivent passer par le Chiffrement Edge serveur proxy. Ces requêtes HTTP incluent toutes les requêtes provenant d'un navigateur, ainsi que toutes les requêtes SOAP ou REST.

Base de données proxy

Si vous utilisez un chiffrement préservant l'ordre ou des schémas de chiffrement, vos serveurs proxy s'appuient sur une base de données MySQL située sur votre réseau. Tous les serveurs proxy de votre réseau doivent utiliser la même base de données.

La base de données proxy contient ces tables.

Tables de bases de données proxy

Nom	Description
db_id	ID unique de base de données
edge_token_map	Données du modèle de chiffrement
token_map	Données de chiffrement préservant l'ordre

Sauvegarde de votre base de données proxy

Étant donné que les modèles de chiffrement reposent sur la tokenisation, les valeurs en texte clair sont stockées dans votre base de données proxy. En cas de perte de la base de données, les valeurs en clair ne peuvent pas être restaurées. Il est essentiel que vous mainteniez des sauvegardes régulières. Pour éviter la perte de données, sauvegardez votre base de données proxy conformément aux ServiceNow recommandations.

- Sauvegardez votre base de données toutes les 24 heures.
- Conservez les fichiers journaux binaires de base de données MySQL pendant au moins deux jours. Une fois qu'une sauvegarde a été restaurée, utilisez le journal binaire pour régénérer toutes les données perdues depuis la sauvegarde la plus récente.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chiffrement Edge Clientèle

Chiffrement Edge utilise trois clients pour informer l'instance que le proxy est en cours d'exécution, synchroniser les demandes entre le proxy et l'instance et transmettre toutes les demandes de l'utilisateur final à l'instance après tout chiffrement potentiel.

Client	Description
Client Intervalle de mise à jour/KeepAlive	En charge d'envoyer une demande à l'instance ServiceNow toutes les 5 secondes pour faire savoir à l'instance que ce proxy est actif et en cours d'exécution. Les demandes pilotent le champ last_response_on sur la table proxy Edge et, par conséquent, déterminent l'état du proxy. Si votre système rencontre des problèmes pour envoyer les demandes, ou si la demande ou le traitement de la demande est retardé, l'instance peut marquer le proxy comme ne répondant pas, même si les autres clients (y compris celui du trafic utilisateur) sont en cours d'exécution. Ce client contrôle également l'état en ligne du proxy sur l'instance. La *edgeencryption.proxy.keepalive.interval* propriété contrôle le taux d'interrogation pour ce client. La valeur par défaut est 5 (secondes).
Client d'interrogation/synchronisation	En charge de diverses demandes que le proxy envoie à l'instance pour synchronisation sur la configuration Chiffrement Edge (par exemple, la table, la colonne ou la pièce jointe à chiffrer, les clés, les tâches, les règles et les modèles de tokenisation). La *edgeencryption.config.poll.interval* propriété contrôle le taux d'interrogation pour ce client. **⚠ Avertissement :** Ne modifiez pas ce paramètre. La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de synchronisation lors de la mise à jour des paramètres Chiffrement Edge sur l'instance.
Client de trafic par défaut/utilisateur	Pour tout le reste, ce client gère toutes les demandes de l'utilisateur final et les transfère à l'instance ServiceNow après tout chiffrement potentiel. Ce client gère également les réponses de l'instance et les transmet à l'utilisateur final après tout déchiffrement potentiel.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des clés pour Chiffrement Edge

Vous êtes responsable de la fourniture et de la gestion des clés de chiffrement utilisées par Chiffrement Edge.

Cette rubrique fait référence aux clés du Chiffrement Edge produit. Si vous recherchez des informations sur le cadre de travail de gestion de clés, qui peut être utilisé avec Chiffrement au niveau des colonnes, consultez Cadre de travail de gestion de clés.

Lors de l'obtention et de la création de clés de chiffrement pour prendre en charge les types de chiffrement utilisés par Chiffrement Edge, tenez compte des éléments suivants :

- Indique s'il faut utiliser AES 128 bits ou AES 256 bits. Vous devez définir une clé de chiffrement AES 128 bits par défaut, même si elle n'est pas utilisée.
- Indique s'il faut utiliser le système de fichiers, Java KeyStore ou Enterprise Key Management (EKM).
- Quand alterner les clés de chiffrement.
- Quand et si utiliser une tâche de chiffrement en masse pour chiffrer à nouveau les données à l'aide de la nouvelle clé

Avant de supprimer une clé des fichiers de configuration du proxy et du magasin de clés, il est essentiel de déchiffrer toutes les données sur l'instance qui utilise la clé. Pour ce faire, ajoutez une nouvelle clé de chiffrement et planifiez une tâche de rotation de clés en masse.

Magasins de clés

Chiffrement Edge prend en charge les types de stockage de clés suivants.

Magasin de fichiers

Les clés sont stockées dans un fichier dans un système de fichiers accessible par le Chiffrement Edge proxy. Les clés de chiffrement stockées dans un fichier ne sont pas chiffrées, il est donc de votre responsabilité de protéger ces fichiers.

Java KeyStore

Les clés sont stockées dans le KeyStore JCEKS de Java. Un magasin de clés Java est protégé par un mot de passe, il est donc plus sûr que le stockage des clés dans un fichier dans le magasin de fichiers. Un seul magasin de clés Java peut stocker plusieurs clés, et les clés sont identifiées par un alias de clé, ce qui facilite la gestion de plusieurs clés.

Gestion des clés d'entreprise (EKM)

Les clés sont stockées et récupérées à l'aide des systèmes de gestion des clés SafeNet KeySecure ou Unbound Technology.

Le Chiffrement Edge proxy est livré avec le fichier Java JCEKS KeyStore nommé keystore.jceks dans le répertoire keystore . Ce fichier keystore contient la clé publique utilisée pour valider les ServiceNow règles de chiffrement signées par ServiceNow.

Remarque :
Si vous utilisez un magasin de clés autre que le KeyStore Java JCEKS du système de base, vous devez importer la clé publique dans votre magasin de ServiceNow clés. L'alias de clé publique est *servicenow*.

En plus des clés de chiffrement, le KeyStore Java JCEKS est utilisé pour stocker la paire de clés RSA pour signer numériquement la configuration de chiffrement et les règles de chiffrement stockées dans l'instance, ainsi que le certificat numérique que le Chiffrement Edge proxy utilise pour établir une connexion sécurisée avec les navigateurs et tout autre client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gestion des versions de clé SafeNet pour Chiffrement Edge

Utilisez la gestion des versions de clés SafeNet pour simplifier le changement des clés. Au lieu de créer un alias pour chaque nouvelle clé, la gestion des versions de clés SafeNet conserve le même alias et incrémente la version.

Vous devez configurer la gestion des versions de clé dans SafeNet avant de pouvoir configurer la gestion des versions de clé SafeNet sur le serveur proxy Edge.

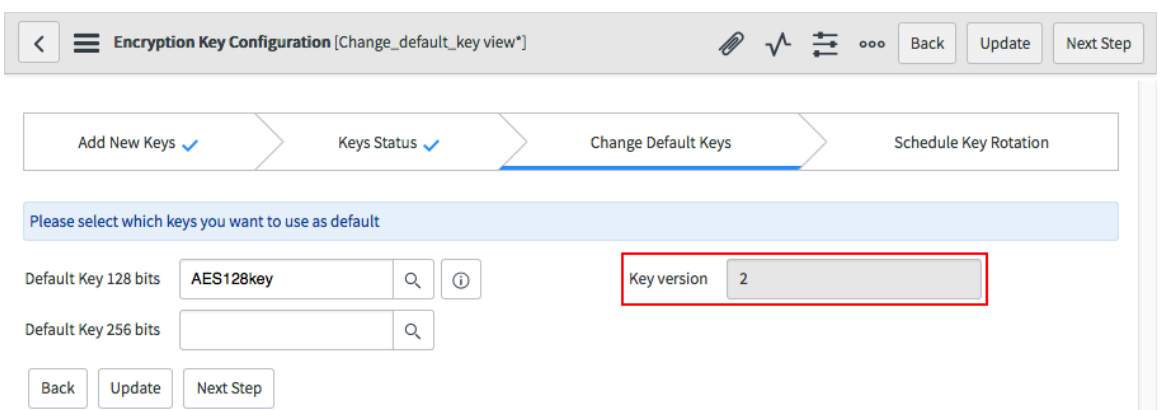
Remarque :

Les proxys Edge installés avant la London version prennent en charge les clés SafeNet, mais pas la gestion des versions des clés SafeNet. Si vous utilisez par erreur une clé versionnée sur un ou plusieurs Kingston versions antérieures, lorsque vous effectuez une mise à niveau vers une version antérieure ou ultérieure London , le proxy ou une London version ultérieure détecte ce problème et, pour éviter toute perte de données potentielle, le proxy ne démarre pas.

Vous devez d'abord planifier une tâche de rotation de clé en masse ou une tâche de rotation de clé unique pour remplacer l'ancienne clé versionnée SafeNet par une clé non versionnée, puis créer une nouvelle clé versionnée SafeNet, si nécessaire. Cette nouvelle clé versionnée peut être utilisée en toute sécurité avec le proxy ou une London version ultérieure, et vous pouvez redémarrer le proxy.

Configuration de la clé de chiffrement

Si vous utilisez des clés versionnées SafeNet, la section Modifier les clés par défaut du formulaire Configuration de la clé de chiffrement inclut de nouveaux champs pour la **version de clé** des clés 128 bits et 256 bits par défaut. **Les** champs de version de clé sont grisés et ne peuvent pas être modifiés.



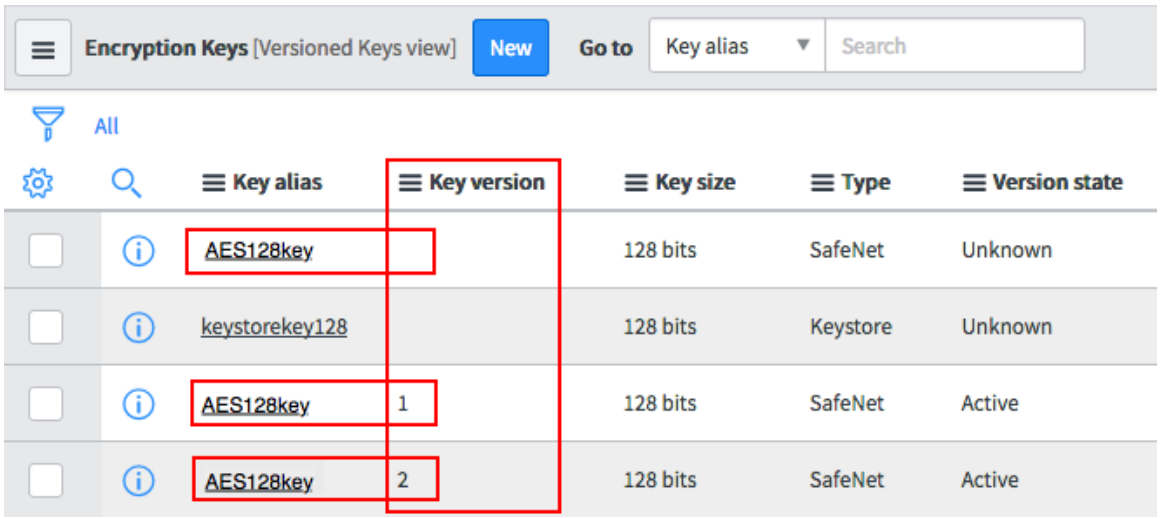
Pour connaître les procédures, reportez-vous à la section Configurer les clés de chiffrement sur l'instance.

Clés versionnées

Si vous utilisez des clés versionnées SafeNet, lorsque vous accédez à **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Toutes les clés**, les clés versionnées incluent la **version Key**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Un numéro de version n'apparaît pas pour les entrées initiales que vous effectuez dans la section Modifier les clés par défaut du formulaire Configuration de la clé de chiffrement. Lorsque le serveur proxy demande une clé à SafeNet, le système ajoute une nouvelle ligne pour l'alias et ajoute la **version** de la clé.

Dans l'exemple ci-dessus, **AES128key** est répertorié trois fois :

- La première liste, sans version de **clé** indiquée, est l'entrée initiale.
- La deuxième liste, avec **1** dans la colonne Version de la **clé** , est la première version de la clé renvoyée par SafeNet.
- La troisième liste, avec **2** dans la colonne Version de la **clé** , est la deuxième version de la clé renvoyée par SafeNet.
- Au fur et à mesure que d'autres versions de la clé sont renvoyées à partir de SafeNet, de nouvelles lignes sont ajoutées pour enregistrer la **version de la clé** actuellement utilisée.

Configurations et schémas de chiffrement

Avec Chiffrement Edge, vous pouvez chiffrer des champs et tokeniser des chaînes.

Configurations de chiffrement

Vous pouvez chiffrer des champs individuels à l'aide de configurations de chiffrement. Chiffrement Edge prend en charge les clés de chiffrement AES 128 bits. Si les fichiers de politique de juridiction de force illimitée de Java Cryptography Extension (JCE) sont installés, Chiffrement Edge prend en charge les clés de chiffrement AES 256 bits pour chaque type de chiffrement. Chiffrement Edge prend en charge les types suivants de configurations de chiffrement.

Chiffrement standard

La valeur chiffrée d'un champ est différente chaque fois que le champ est chiffré, même si la valeur du champ reste la même. Le chiffrement standard est la forme de chiffrement la plus robuste. Les champs utilisant le chiffrement standard ne peuvent pas être triés, regroupés ou filtrés.

Chiffrement préservant l'égalité

La valeur chiffrée d'un champ est la même lorsque la valeur du champ reste la même. Prend en charge les comparaisons d'égalité et les opérations de regroupement par sur un champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque le chiffrement préservant l'égalité est sélectionné pour un champ qui contient déjà des données, l'exécution d'une action Grouper par sur le champ peut ne pas regrouper les champs avec la même valeur si l'un est chiffré et l'autre non.

Chiffrement préservant l'ordre

Utilise des jetons et le chiffrement pour sécuriser les données de votre base de données proxy. Prend en charge les comparaisons d'égalité, le regroupement par opérations et la possibilité de trier les données. Le type de chiffrement préservant l'ordre n'est pris en charge que si une base de données MySQL est configurée pour le Chiffrement Edge serveur proxy.

Remarque :
Lorsque vous utilisez le chiffrement préservant l'ordre et que la base de données proxy est en panne, des mises à jour peuvent être effectuées sur les champs à l'aide du chiffrement préservant l'ordre. Toutefois, l'ordre de tri ne sera pas correct lorsque vous tenterez de trier les données en fonction de ces champs. Les groupes ne fonctionneront pas non plus comme prévu. Lorsque la base de données proxy est à nouveau opérationnelle, planifiez une tâche de réparation de jeton de commande pour réparer les jetons manquants.

Types de chiffrement

Les types de chiffrement suivants sont répertoriés dans la catégorie Qualité de sécurité décroissante.

Type de chiffrement	Description
AES 256 standard	Les champs ne peuvent pas être filtrés, triés ou comparés.
AES 128 standard	Les champs ne peuvent pas être filtrés, triés ou comparés.
Préservation de l'égalité AES 256	Les champs peuvent être filtrés à l'aide de comparaisons d'égalité.
Préservation de l'égalité AES 128	Les champs peuvent être filtrés à l'aide de comparaisons d'égalité.
Conservation de l'ordre AES 256	Les champs peuvent être triés et le filtrage de comparaison d'égalité peut être utilisé. Nécessite l'utilisation d'une base de données MySQL dans votre réseau.
Conservation de l'ordre AES 128	Les champs peuvent être triés et le filtrage de comparaison d'égalité peut être utilisé. Nécessite l'utilisation d'une base de données MySQL dans votre réseau.

Schémas de chiffrement

Vous pouvez sécuriser les données sensibles trouvées dans des chaînes à l'aide de modèles de chiffrement. Une fois qu'un modèle de chiffrement est stocké et activé, le Chiffrement Edge serveur proxy identifie les chaînes qui correspondent au modèle dans les demandes. Une fois localisée, la chaîne de texte clair est stockée dans la base de données proxy et remplacée sur l'instance par un jeton. Utilisez des schémas de chiffrement pour tokeniser des chaînes qui correspondent à des schémas réguliers tels que les numéros de sécurité sociale et de carte de crédit. Bien que nous recommandions que les configurations de chiffrement soient la principale méthode de chiffrement, utilisez des modèles de chiffrement en complément pour localiser et sécuriser les informations sensibles qui se trouvent en dehors des champs chiffrés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le Chiffrement Edge serveur proxy nécessite une base de données MySQL dans votre réseau uniquement s'il utilise un cryptage préservant l'ordre ou des schémas de chiffrement. Les valeurs en texte clair sont stockées dans la base de données proxy de votre réseau. Pour cette raison, il est essentiel que vous sécurisiez et sauvegardez régulièrement votre base de données proxy. Pour des recommandations, reportez-vous à la section Composants de Chiffrement Edge.

Information associée

Chiffrer les champs à l'aide de configurations de chiffrement

Tokeniser des chaînes à l'aide de schémas de chiffrement

Installé avec Chiffrement Edge

Chiffrement Edge installe les tables pour stocker les données liées au chiffrement, les propriétés système pour configurer le comportement par défaut et le rôle edge_encryption à administrer Chiffrement Edge.

Tables installées avec Chiffrement Edge

Chiffrement Edge ajoute les tables suivantes.

Configuration de Chiffrement Edge [sys_encryption_configuration]

Contient des champs chiffrés et des tables pour lesquelles les pièces jointes sont chiffrées.

Règle Chiffrement Edge [sys_encryption_rule]

Contient un enregistrement pour chaque règle. Une règle a un nom, la condition lorsqu'elle est utilisée, un script et un champ d'ordre.

Journal d'insertion invalide Chiffrement Edge [sys_edge_encryption_invalid_insert_log]

Contient les messages de journal créés pour les tentatives d'enregistrement de données non chiffrées dans un champ chiffré.

Proxy Chiffrement Edge [sys_encryption_proxy]

Contient des informations sur l'application proxy de chiffrement.

Type de chiffrement du proxy Edge [sys_proxy_encryption_type]

Utilisé pour activer et désactiver les types de chiffrement sur le formulaire de chiffrement.

Exécution de la tâche de chiffrement [sys_encryption_job_execution]

Prend en charge les tâches de chiffrement en masse.

Bloc d'exécution de la tâche de chiffrement [sys_encryption_job_execution_chunk]

Prend en charge les tâches de chiffrement en masse.

Tâche de chiffrement planifiée [sysauto_encryption_job]

Répertorie les travaux planifiés pour le chiffrement, le déchiffrement, la rotation de clé, la réparation des jetons de commande et la récupération de base de données.

Configuration de la clé de chiffrement [sys_encryption_key_configuration]

Répertorie les clés de chiffrement par défaut.

Clé de chiffrement [sys_encryption_key]

Répertorie les clés disponibles et les attributs de clé.

Clé de chiffrement de proxy [sys_encryption_proxy_key]

Répertorie les clés de chiffrement de proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés installées avec Chiffrement Edge

Chiffrement Edge ajoute les propriétés suivantes.

Remarque :
Pour ouvrir la table Propriétés système [sys_properties], saisissez `sys_properties.list` dans le filtre de navigation.

glide.edge.pattern.disallowed.chars

Une liste de caractères qui ne sont pas autorisés dans les modèles.

- **Type** : chaîne d'une liste de valeurs séparées par des virgules
- **Emplacement** : table Propriétés système [sys_properties]

glide.edge.pattern.min.size

Taille minimale du modèle autorisée. Autoriser des modèles plus petits signifie trouver plus de correspondances, ce qui augmente les frais généraux.

- **Type** : nombre
- **Valeur par défaut** : 5
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.logging.destination

Emplacement où les messages sont consignés.

- **Type** : chaîne
- **Valeur par défaut** : fichier
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.journalisation.verbosité

Niveau de journalisation à utiliser.

- **Type** : chaîne
- **Valeur par défaut** : info
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.encryption.proxy.buildtag

Version du proxy enregistrée auprès de votre instance.

- **Type** : chaîne
- **Emplacement** : table Propriétés système [sys_properties]

sn_edge_encryption.cleartext.allowed

Si vrai, autorise l'enregistrement de texte clair dans un champ chiffré. Cela se produit lorsqu'un utilisateur accède à l'instance sans passer par le Chiffrement Edge proxy. Lorsque la valeur est définie sur false, le système empêche l'enregistrement du texte clair dans un champ chiffré.

- **Type** : booléen
- **Valeur par défaut** : faux
- **Emplacement** : table Propriétés système [sys_properties]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Planification pour Chiffrement Edge

La mise en œuvre réussie de nécessite de la planification et de Chiffrement Edge la préparation.

Répondez aux questions suivantes à l'étape de la planification.

- Quels champs doivent être chiffrés ?
- Quels types de chiffrement doivent être utilisés ?
- Combien de Chiffrement Edge proxys sont nécessaires ? Consultez la section Dimensionnement de votre environnement Edge Encryption pour connaître les recommandations et les éléments à prendre en considération.
- Si un type de chiffrement ou des schémas de chiffrement préservant l'ordre doivent être utilisés, où se trouve la base de données MySQL ?
- Quel système de gestion des clés doit être utilisé ?

Les administrateurs système, les administrateurs réseau et les membres de l'équipe de sécurité ont différentes tâches à accomplir pour la mise en œuvre Chiffrement Edgede .

- Les administrateurs système doivent avoir le rôle d'administrateur de sécurité. L'administrateur système doit :
  - Téléchargez l'application Chiffrement Edge proxy.
  - Configurez un Chiffrement Edge compte d'utilisateur que les proxys utiliseront pour se connecter à l'instance. Le rôle edge_encryption doit être affecté à l'utilisateur.
  - Configurez les clés de chiffrement et définissez les clés par défaut.
  - Configurez Chiffrement Edge sur l'instance.
  - Planifiez des tâches de chiffrement.
  - Moniteur Chiffrement Edge.
  - Créez et modifiez des règles de chiffrement.
- Votre administrateur réseau doit :
  - Installez l'application Chiffrement Edge proxy.
  - Connaître les adresses réseau des serveurs proxy et la base de données proxy utilisée pour le chiffrement préservant l'ordre et les modèles de chiffrement.
  - Installez la base de données proxy à utiliser pour le chiffrement préservant l'ordre et les modèles de chiffrement.
  - Démarrez et arrêtez les applications proxy.
  - Effectuer la gestion des clés de chiffrement.
  - Déterminez comment mapper les utilisateurs aux applications proxy de chiffrement. Cela peut être fait avec des paramètres DNS ou des règles de routage, et est spécifique à chaque réseau.
  - Gérez plusieurs serveurs proxy.
  - Configurez les pools d'équilibreurs de charge et leurs paramètres.
- Votre administrateur de sécurité doit déterminer les types de chiffrement à affecter à chaque champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration requise pour Chiffrement Edge

Vous pouvez exécuter l'application proxy sur des serveurs ou des ordinateurs virtuels Chiffrement Edge fonctionnant sous les systèmes d'exploitation Microsoft Windows ou Linux. Pour des performances optimales, assurez-vous que votre configuration répond à ces exigences.

Configuration requise pour Java

L'ordinateur hôte sur lequel l'installation ou l'exécution du Chiffrement Edge serveur proxy doit gérer une version prise en charge de Java. Les versions prises en charge actuelles sont Java 11.0.6 ou ultérieure dans la série de versions 11.x

Remarque :
Java 8 n'est plus pris en charge à partir de cette Utah version. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 11 avant d'essayer d'installer la Utah version du Chiffrement Edge proxy.

Remarque :
Java n'autorise pas automatiquement un nombre illimité de clés de force. Vous devez spécifiquement activer l'utilisation du cryptage AES 256 bits.

Prise en charge d'OpenJDK

Il prend en charge la version 11 d'OpenJDK Now Platform .

Configuration minimale du serveur proxy

Un serveur proxy nécessite la configuration minimale suivante :

- 4 Go de RAM par serveur proxy (6 Go sont recommandés pour la plupart des déploiements).

  Remarque :
  L'hôte du serveur proxy nécessite au moins 1 Go de RAM de plus que le serveur proxy. L'hôte du serveur proxy a besoin de 1 Go supplémentaire pour les services du système d'exploitation. Par exemple, si vous configurez un serveur proxy pour qu'il utilise 4 Go de RAM, vous devez installer au moins 5 Go de RAM sur l'hôte du serveur proxy.

  Étant donné que le serveur proxy nécessite au moins 4 Go de mémoire, les JRE 32 bits et les systèmes d'exploitation 32 bits ne sont plus pris en charge à partir de la London version.

- Processeur de 3 GHz ou plus (processeur à 4 cœurs préféré pour des performances optimales).
- Plusieurs serveurs proxy derrière un équilibreur de charge. Le nombre de serveurs proxy dont vous avez besoin dépend du nombre de nœuds d'application, du nombre d'utilisateurs simultanés et du nombre de serveurs nécessaires pour le basculement. Consultez Dimensionnement de votre environnement Edge Encryption pour plus d'informations.
- Possibilité d'exécution simultanée avec d'autres services, en fonction de l'utilisation du serveur et de la disponibilité des ressources.

Systèmes pris en charge par le serveur proxy

Les systèmes suivants sont pris en charge :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Système pris en charge	Description
Éditions Windows Server 2012, 2012-R2, 2016 et 2019	• Ordinateurs virtuels ou matériel physique • Systèmes 64 bits
Linux	• Ordinateurs virtuels ou matériel physique • Systèmes 64 bits Sur les systèmes Linux 64 bits, vous devez installer la bibliothèque GNU C 32 bits (glibc). La commande d'installation pour CentOS est `yum install glibc.i686`.

Besoins de version du serveur proxy

Synchronisez la version de votre Chiffrement Edge proxy avec la version de votre ServiceNow instance (même version majeure, par exemple Tokyo). Pour éliminer les temps d'arrêt pendant le processus de mise à niveau, le Chiffrement Edge proxy est rétrocompatible. Cependant, il est important de mettre à niveau dès que possible pour éviter de s'assurer que les utilisateurs peuvent accéder à de nouvelles fonctionnalités et à des corrections de bogues importantes.

Besoins de connexion au serveur proxy

Le serveur proxy qui exécute l'application doit être en mesure de communiquer avec les Chiffrement Edge machines de votre réseau. Assurez-vous que le serveur proxy dispose des privilèges réseau suivants :

Privilège réseau	Description
Accès par pare-feu	Configurez tous les pare-feu entre le serveur proxy et les périphériques clients pour autoriser une connexion. Si votre réseau utilise une zone démilitarisée (DMZ) pour ajouter une couche de sécurité supplémentaire à votre réseau local (LAN) et si vos protocoles de sécurité réseau limitent l'accès des ports de l'intérieur du réseau à la zone DMZ, vous devrez peut-être déployer un serveur proxy sur une machine dans la zone DMZ.
Accès au réseau	Configurez chaque client pour permettre au serveur proxy de s'y connecter. Si la sécurité réseau vous empêche de configurer de nouvelles machines capables de se connecter aux clients, installez le serveur proxy sur une machine existante disposant de privilèges de connexion.
Accès à l'instance	Assurez-vous que le serveur proxy dispose d'un accès réseau à l'instance. Assurez-vous de configurer le réseau de serveurs proxy pour autoriser le trafic sur le port TCP 443.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Privilège réseau	Description
Compte réseau	Installez le serveur proxy avec un administrateur local ou de domaine.

Configuration système requise pour la conservation des commandes et la tokenisation des bases de données

Le chiffrement et les schémas de chiffrement préservant l'ordre nécessitent que vous configuriez une base de données Oracle MySQL pour le Chiffrement Edge serveur proxy. Le chiffrement préservant l'ordre permet d'appliquer directement n'importe quelle opération de comparaison sur des données chiffrées, sans avoir à déchiffrer les données au préalable. Les schémas de chiffrement vous permettent de remplacer les schémas de chaîne par des jetons (tokenisation) avant qu'ils ne soient envoyés et stockés dans la base de données. En raison de la taille de la base de données MySQL, utilisez un serveur proxy dédié pour exécuter la base de données de préservation de l'ordre et de tokenisation.

La configuration minimale requise pour le système de base de données est la suivante :

Base de données MySQL	Besoin
Version	Base de données MySQL versions 5.7 et 8.0 **Remarque :** Les versions 5.5 et 5.6 de MySQL ne sont plus testées et ont atteint la fin du support.
Systèmes d'exploitation	Systèmes 64 bits
Processeur	Processeur de 2 GHz ou plus (processeur à 4 cœurs préféré pour des performances optimales)
RAM	16 Go
Disque	SAN (Storage Area Network) ou stockage local (RAID 10 recommandé)
Taille	Déterminé par le nombre d'enregistrements potentiels multiplié par la taille de l'enregistrement. Voir Calculer la taille de la base de données de conservation de l'ordre et de la création de jetons.
Configuration	Grappe haute disponibilité. Si vous n'êtes pas sûr de la configuration de votre serveur MySQL, contactez MySQL pour obtenir des informations de configuration.

Dimensionnement de votre environnement Edge Encryption

Choisir le nombre de serveurs proxy pour votre environnement est une tâche importante. Tenez compte du nombre d'utilisateurs, des besoins de redondance et de la latence acceptable.

Redondance

Maintenez des serveurs proxy redondants en cas de défaillance matérielle. Les serveurs proxy doivent être situés derrière un équilibreur de charge pour fournir un chemin fonctionnel à tous les utilisateurs si un serveur proxy n'est pas accessible. Au minimum, assurez-vous que deux serveurs proxy sont toujours disponibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Taille

La taille fait référence au nombre de serveurs proxy nécessaires pour éviter la latence supplémentaire produite par le chiffrement des données. En fonction de l'utilisation, vous pouvez réduire la latence en ajoutant des serveurs proxy supplémentaires. Par exemple, si des chiffrements en masse réguliers sont exécutés, ajoutez des serveurs proxy supplémentaires pour gérer la charge, ou exécutez les chiffrements en masse lorsque la charge utilisateur est faible. De plus, le matériel sur lequel s'exécute le serveur proxy influence les performances et la latence. Les serveurs proxy s'exécutant sur du matériel doté de processeurs plus rapides, de plus de processeurs et de plus de RAM ont un débit plus élevé que les systèmes plus lents et limités.

Les instructions suivantes supposent que votre serveur proxy fonctionne avec au moins la configuration matérielle minimale requise. Pour déterminer le nombre de serveurs proxy :

- Envisagez de configurer un serveur proxy pour deux nœuds d'application sur l'instance.
- Pour la redondance, configurez au moins deux serveurs proxy derrière un équilibreur de charge.
- Ajoutez un serveur proxy supplémentaire pour chaque tranche de 500 utilisateurs simultanés.
- En fonction de la redondance souhaitée, ajoutez des serveurs proxy supplémentaires pour le basculement.

Par exemple, pour une instance avec 2 000 utilisateurs, vous devez avoir au moins cinq serveurs proxy derrière un équilibreur de charge. Ce calcul inclut un serveur proxy pour 500 utilisateurs, avec un serveur proxy supplémentaire pour le basculement. Déterminez à l'avance quand vous approcherez d'un seuil de 500 utilisateurs et placez un autre serveur proxy dans le pool d'équilibreurs de charge.

Équilibreurs de charge

Pour équilibrer les demandes et améliorer le délai de réponse du serveur, répartissez les serveurs proxy dans un pool d'équilibreurs de charge. Configurez les équilibreurs de charge pour utiliser la méthode du « minimum de connexions ». Cette méthode connecte les requêtes au serveur proxy ayant le moins de connexions actives, empêchant ainsi la surcharge d'un seul proxy.

Utilisation du processeur

Étant donné que le chiffrement et la tokenisation des données sont des opérations gourmandes en ressources processeur, les pics de CPU lors du chiffrement des données sont normaux et attendus. Lorsque l'utilisation du processeur est supérieure à 80 % pendant plusieurs minutes à la fois, cela signifie probablement que le serveur proxy a trop de travail à faire. Lorsque cela se produit, la latence augmente pendant la période où l'utilisation du processeur est élevée. Si la latence persiste, l'ajout d'un autre serveur proxy peut aider à réduire la latence.

Mémoire

Le serveur proxy doit disposer d'un minimum de 4 Go de RAM (6 Go recommandés). Définissez les limites de mémoire initiales et supérieures du serveur proxy sur les paramètres recommandés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Calculer la taille de la base de données de conservation de l'ordre et de la création de jetons

Si vous utilisez un chiffrement préservant l'ordre ou des modèles de chiffrement, déterminez la taille de votre base de données MySQL en multipliant le nombre d'enregistrements potentiels par la taille de l'enregistrement.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Utilisez une machine dédiée pour exécuter la base de données de conservation de l'ordre et de tokenisation. N'exécutez pas la base de données sur le même matériel que le serveur proxy.

Procédure

1. Déterminez le nombre potentiel d'enregistrements qui pourraient inclure des champs chiffrés avec un chiffrement préservant l'ordre.
   a. Multipliez le nombre de configurations de chiffrement à l'aide du chiffrement préservant l'ordre par le nombre d'enregistrements auxquels chaque configuration est appliquée.
   b. Pour permettre la croissance, multipliez le résultat par trois.
2. Multipliez le résultat de l'étape 1 par 1 536.
   1 536 est la taille moyenne d'un enregistrement en octets.
3. Si vous utilisez des modèles de chiffrement, effectuez les étapes 1 et 2 pour les enregistrements tokenisés et ajoutez le résultat au total.

Résultats

La valeur calculée est la taille recommandée en octets pour votre base de données de conservation des commandes et de tokenisation.

Chiffrement Edge Limitations

Chiffrement Edge a un impact sur les fonctions du système. Évaluez soigneusement l'impact du chiffrement d'un champ.

Restrictions de type de champ

Vous pouvez chiffrer uniquement les types de champs suivants :

- Date
- E-mail
- Date/Heure
- HTML
- Adresse IP
- Journal
- Entrée de journal
- Texte de plusieurs lignes
- Texte sur ligne unique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Chaîne
- URL

Vous ne pouvez pas chiffrer les types de champs suivants :

- Champs de choix
- Champs virtuels
- Champs dans les tables système, à l'exception de certains champs dans sys_user
- Champs système dans les tables
- Champs numériques ou champs associés à un schéma de numérotation automatique
- Tout autre type de champ non répertorié ci-dessus

Restrictions supplémentaires :

- Lorsqu'un champ Journal est chiffré, le bouton **Publier** est inactif, même s'il existe plusieurs champs Journal et qu'un seul de ces champs est chiffré.
- Les champs chiffrés ne sont pas disponibles dans les zones **Aller à** et dans les filtres d'en-tête.
- Lorsque vous chiffrez des champs utilisés comme index, vous ne pouvez utiliser que des types de chiffrement préservant l'ordre et l'égalité. Les champs indexés ne peuvent pas être chiffrés à l'aide du type de chiffrement standard.

Pour plus d'informations, reportez-vous à la rubrique Types de champs .

Restrictions de filtrage et de recherche

Chiffrement standard

Lorsque vous sélectionnez un champ de chaîne, de date, de date/heure ou d'URL avec une configuration de champ chiffré standard comme opérande de gauche dans un filtre, aucune option de filtrage n'est disponible.

Chiffrement préservant l'égalité

Lorsque vous sélectionnez un champ de chaîne, de date, de date/heure ou d'URL avec une configuration de champ chiffré préservant l'égalité comme opérande gauche dans un filtre, les opérateurs suivants sont disponibles :

- **est**
- **n'est pas**
- **est vide**
- **n'est pas vide**

Chiffrement préservant l'ordre

Lorsque vous sélectionnez un champ de chaîne avec une configuration de champ chiffré préservant l'ordre comme opérande de gauche dans un filtre, les opérateurs suivants sont disponibles, en plus de **est**, **n'est pas**, **est vide** et **n'est pas vide** :

- **supérieur à**
- **inférieur à**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous sélectionnez un champ Date ou Date/Heure avec une configuration de champ chiffrée préservant l'ordre comme opérande de gauche dans un filtre, les opérateurs suivants sont disponibles, en plus de **est**, **n'est pas**, **est vide** et **n'est pas vide** :

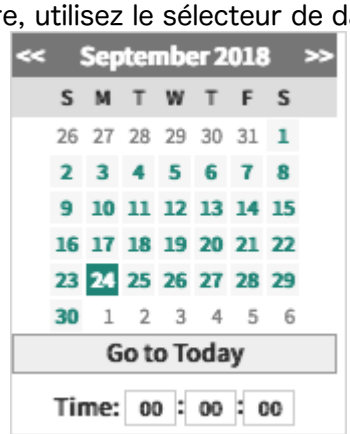
- **après**
- **avant**
- **après ou le**
- **avant ou le**

Sélecteurs de date et de date/heure

Pour les champs Date, utilisez le sélecteur de date pour spécifier la date :



Pour les champs Date/heure, utilisez le sélecteur de date et d'heure pour spécifier la date et l'heure :



Filtres de condition de liste

Les options **Afficher la correspondance** et **Filtrer sont** prises en charge dans les listes. Seules les correspondances exactes sont renvoyées ou filtrées.

Remarque :
L'ajout de champs chiffrés dans les filtres de condition est pris en charge dans les scripts tels que les politiques d'interface utilisateur et les règles métier.

Restrictions de configuration

Restrictions et comportement des configurations de chiffrement :

- Une fois que vous avez ajouté un champ à la Chiffrement Edge table de configuration, vous ne pouvez pas supprimer l'enregistrement de configuration. Si vous ne souhaitez plus qu'un champ soit chiffré, désactivez l'enregistrement dans la Chiffrement Edge table de configuration et planifiez une tâche de chiffrement pour déchiffrer les données.
- Si un champ d'une table parente est marqué comme étant chiffré, le champ est également chiffré dans toutes les tables héritées. Par exemple, si le champ **Brève description** de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

table Tâche est chiffré, le contenu du champ **Brève description** de la table Incident est chiffré.

- Si un champ hérité d'une table parente est marqué pour être chiffré, le champ de la table parente ne peut pas être chiffré. Par exemple, si la **brève description** de la table Incident est marquée comme étant chiffrée, la **brève description** de la table Tâche ne peut pas être chiffrée. Dans cet exemple, vous pouvez chiffrer la **brève description** dans la table Problème.
- Lorsqu'un champ avec une configuration de chiffrement définie est exporté vers n'importe quel format, la sortie inclut des valeurs chiffrées, même lorsqu'elle est exportée via le serveur proxy.
- Vous ne pouvez pas importer de données dans un champ avec une configuration de chiffrement définie.
- Vous ne pouvez pas chiffrer les champs Date et Date/Heure hérités. Les champs Date ou Date/Heure hérités d'une table parente ne sont pas répertoriés dans la liste déroulante **Champ de colonne** , et vous ne pouvez pas créer de configurations de chiffrement de date ou de date/heure pour ces champs.
- Vous pouvez chiffrer un champ Chaîne ou URL uniquement à partir d'une table parente ou d'une table enfant, mais pas des deux.

Restrictions d'instance

Impact de l'utilisation Chiffrement Edge sur l'instance :

- La logique back-end ne peut pas traiter les données chiffrées. Lorsque l'instance contient des données chiffrées, toute règle métier, tout script principal ou toute fonctionnalité back-end qui repose sur l'évaluation des données dans le champ chiffré ne s'exécute pas correctement.

  Remarque :
  Les données chiffrées à l'aide d'un chiffrement préservant l'égalité ou l'ordre passent toujours les contrôles d'équivalence lorsqu'elles sont comparées à une valeur chiffrée identique.

- Étant donné que le traitement des e-mails passe directement des systèmes de messagerie à l'instance et ne peut pas passer par le proxy Edge, les données envoyées par e-mail ne peuvent pas être chiffrées ou déchiffrées par le proxy Edge.
  - Les données et les pièces jointes des e-mails entrants ne sont pas chiffrées.
  - Les données et les pièces jointes des e-mails sortants restent chiffrées et ne peuvent pas être déchiffrées.
- Les scripts exécutés sur le serveur ne peuvent pas modifier les données chiffrées.
- La recherche globale n'est pas prise en charge. Étant donné que la recherche globale tente de rechercher à la fois des données chiffrées et en texte clair, les résultats peuvent ne pas être ceux attendus.
- Les données chiffrées ne peuvent pas être copiées-collées dans un enregistrement dont le champ n'est pas chiffré.
- Selon le type de chiffrement sélectionné, la fonctionnalité de l'interface utilisateur pour les champs chiffrés est réduite. Par exemple, la possibilité de comparer, de regrouper, de trier et de rechercher peut être impactée. En règle générale, plus le chiffrement sélectionné est fort, plus les fonctionnalités sont réduites.
- À l'exception de Java KeyStore, SafeNet et Unbound Technology, aucune gestion de clé de chiffrement logicielle ou matérielle tierce n'est prise en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Bien que plusieurs serveurs proxy connectés à une seule instance soient pris en charge, la gestion et la surveillance des clusters de proxy de chiffrement ne sont pas disponibles. Chaque proxy doit être géré séparément.
- Les configurations système telles que la charge de travail et le nombre de champs chiffrés peuvent avoir un impact sur les performances des champs chiffrés.
- Le Chiffrement Edge serveur proxy ne peut se connecter qu'à une seule instance.
- Si votre instance utilise une base de données Oracle et que le champ Chaîne que vous marquez pour chiffrement est supérieur à 2 925 caractères, ce champ ne peut pas être trié même si le chiffrement de préservation de l'ordre est sélectionné.
- Si votre instance utilise une base de données Oracle, Unicode AL32UTF8 est le seul jeu de caractères pris en charge.
- Les données chiffrées ne peuvent pas être utilisées dans les rapports.
- Chiffrement Edge ne peut pas être utilisé avec Data Archiving.

Installation de Chiffrement Edge

Vous pouvez installer un Chiffrement Edge proxy manuellement ou à l'aide du programme d'installation Chiffrement Edge interactif.

Configuration requise pour Java

L'ordinateur hôte sur lequel l'installation ou l'exécution du Chiffrement Edge serveur proxy doit gérer une version prise en charge de Java. Les versions prises en charge actuelles sont Java 11.0.6 ou ultérieure dans la série de versions 11.x

Remarque :
Java 8 n'est plus pris en charge à partir de cette Utah version. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 11 avant d'essayer d'installer la Utah version du Chiffrement Edge proxy.

Installation du serveur proxy

L'installation Chiffrement Edge comprend les étapes suivantes.

- Installez l'application Chiffrement Edge proxy sur un serveur de votre réseau à l'aide du programme d'installation interactif ou du programme d'installation manuel.
- Générez la paire de clés RSA pour les configurations de chiffrement de signature numérique et les règles de chiffrement.
- Installez Java Cryptography Extension (JCE) si vous prévoyez d'utiliser le chiffrement AES 256.
- Si vous utilisez une connexion SSL sécurisée, procurez-vous un certificat de serveur et importez-le dans le Java KeyStore.
- Configurez votre magasin de clés et votre clé de chiffrement.
- Si des types ou des modèles de chiffrement préservant l'ordre doivent être utilisés, configurez une base de données MySQL sur une machine de votre réseau.
- Définissez les propriétés souhaitées. Les propriétés se trouvent dans le fichier de configuration edgeencryption.properties .
- Spécifiez qu'un serveur proxy est une source approuvée afin de Chiffrement Edge pouvoir traiter les demandes provenant de ce serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accès au serveur proxy

Une fois l'installation terminée, pointez le navigateur de chaque utilisateur vers un Chiffrement Edge proxy à l'aide du format d'URL : <host> :<port>. Les valeurs sont déterminées par les propriétés d'hôte et de port dans le fichier edgeencryption.properties .

À titre d'exemple avec les valeurs suivantes :

Propriété	Exemple de valeur
edgeencryption.proxy.host	hostname.mycompany.com
edgeencryption.proxy.http.port	8081

Un client accèdera au serveur proxy à l'adresse suivante : http://hostname.mycompany.com:8081/.

Remarque :
Les paramètres DNS et les règles de routage peuvent être utilisés. Les valeurs d'hôte et de port sont déterminées par votre administrateur réseau.

Demander Chiffrement Edge

Le Chiffrement Edge module d'extension (com.glide.edgeencryption) est disponible sous forme d'abonnement distinct.

Avant de commencer

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Le chargé de clientèle peut faire en sorte que le module d'extension soit activé sur les instances de production et de sous-production de votre organisation, en général en quelques jours à peine.

Si vous n'avez pas de chargé de clientèle, si vous décidez de retarder l'activation après l'achat ou si vous souhaitez évaluer le produit sur une instance de sous-production sans frais, suivez ces étapes.

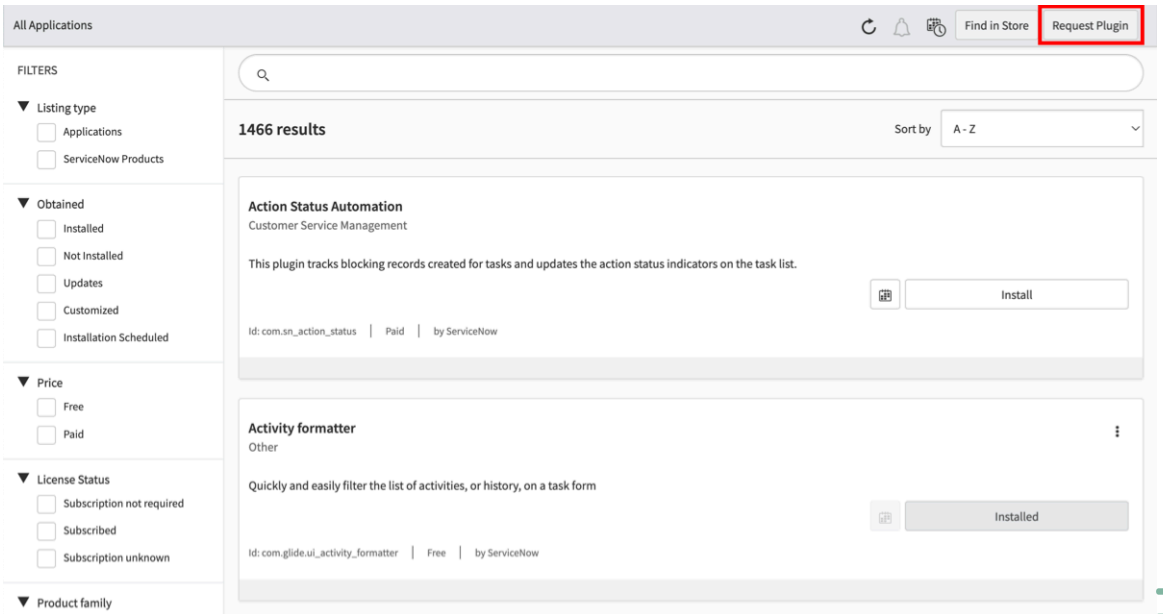
Rôle requis : aucun

Procédure

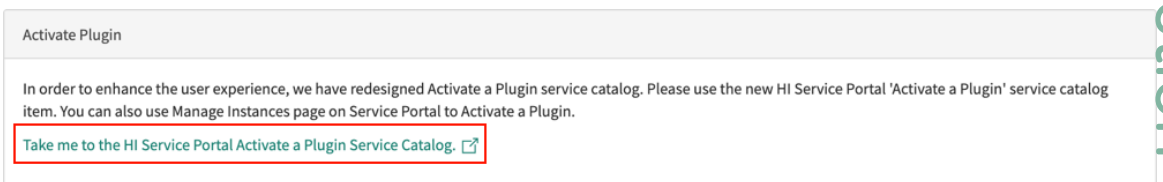
1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.

Traduction automatique

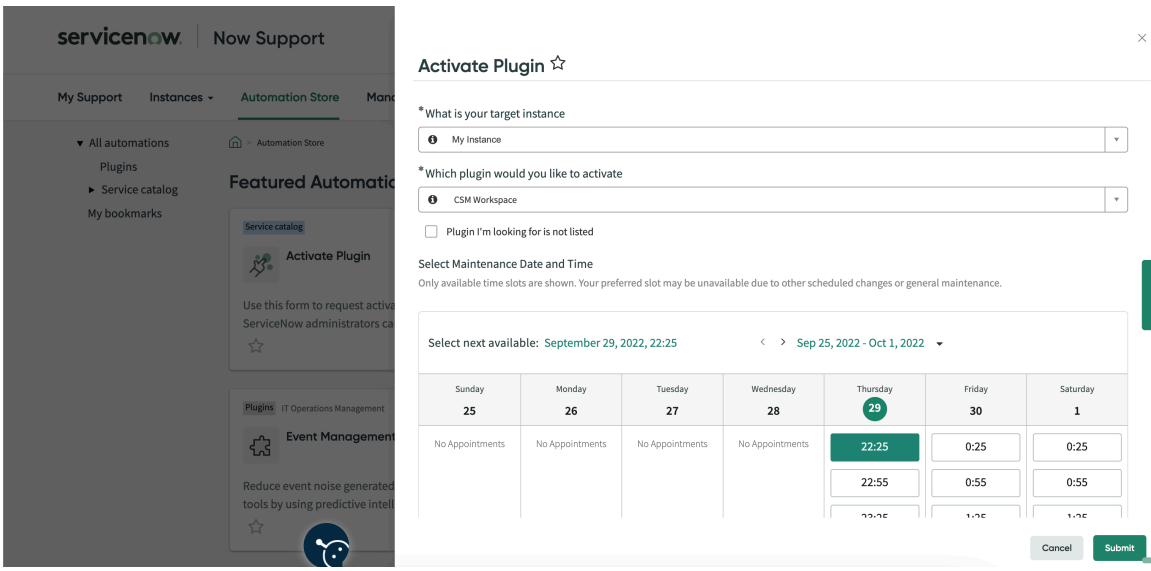
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



7. Sélectionnez **Envoyer**.
   Pour plus de détails sur la demande d'un module d'extension, consultez l'article Requesting a Plugin from the Service Catalog [KB0751715] de la Now Support Base de connaissances.

Configurer un compte d'utilisateur Chiffrement Edge

Les Chiffrement Edge proxys se connectent à l'instance en tant qu'utilisateur pour obtenir et mettre à jour les informations de configuration de chiffrement. Créez un compte d'utilisateur à cet effet et attribuez le rôle edge_encryption à l'utilisateur.

Avant de commencer

Le Chiffrement Edge module d'extension doit être installé avant de pouvoir affecter le rôle.

Rôle requis : admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sur votre ServiceNow instance, créez un compte d'utilisateur à utiliser par les Chiffrement Edge applications proxy.
2. Affectez le rôle edge_encryption à l'utilisateur.

Télécharger le serveur proxy Chiffrement Edge

Téléchargez l'application du Chiffrement Edge serveur proxy à partir de votre instance, puis copiez le fichier sur chaque ordinateur qui doit exécuter le Chiffrement Edge serveur proxy.

Avant de commencer

Avant de commencer cette procédure, le module d'extension Chiffrement Edge doit être installé et activé sur votre instance.

Remarque :
Le Chiffrement Edge proxy est officiellement pris en charge uniquement sur Oracle JRE.

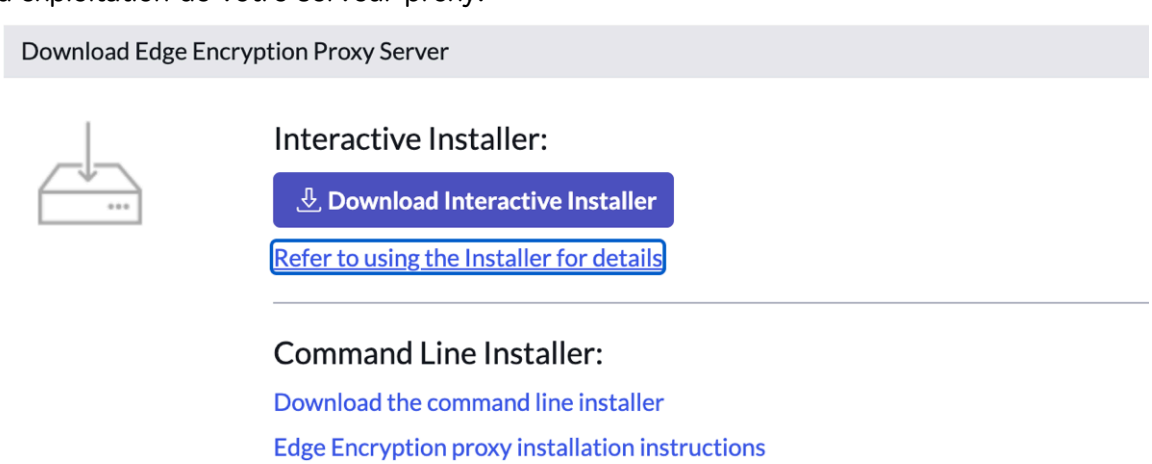
Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Installation et téléchargements** > **Téléchargements**.
2. Pour utiliser le programme d'installation interactif, cliquez sur **Télécharger le programme d'installation interactif**.

   Si vous installez manuellement le serveur proxy, sélectionnez la version du système d'exploitation de votre serveur proxy.



Remarque :
Étant donné que le serveur proxy nécessite au moins 4 Go de mémoire pour fonctionner, les JRE 32 bits et les systèmes d'exploitation 32 bits ne sont plus pris en charge à partir de la Washington DC version.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Copiez le programme d'installation sur chaque ordinateur qui doit exécuter le Chiffrement Edge serveur proxy.

Remarque :
Si vous installez manuellement le Chiffrement Edge serveur proxy, copiez le fichier ZIP sur chaque ordinateur qui doit exécuter le Chiffrement Edge serveur proxy.

Que faire ensuite

Après avoir téléchargé le programme d'installation Chiffrement Edge , Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation interactif. En cas d'installation manuelle, Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation de ligne de commande.

Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation interactif

Installez le Chiffrement Edge serveur proxy sur un ordinateur Windows ou Linux à l'aide du programme d'installation interactif.

Avant de commencer

Remarque :
SafeNet KeyLes fichiers de magasin de clés sécurisés ne sont pas pris en charge par le programme d'installation Chiffrement Edge . Pour utiliser un magasin de clés SafeNet KeySecure, Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation de ligne de commande.

Le Chiffrement Edge module d'extension doit être installé et activé sur votre instance avant de commencer cette procédure. Assurez-vous que la version 11.0.6 ou ultérieure de Java est installée sur l'ordinateur exécutant le programme d'installation Chiffrement Edge .

Rôle requis :

- security_admin sur votre ServiceNow instance
- administrateur local ou de domaine sur un hôte Windows
- utilisateur de service avec accès complet au système de fichiers sur un hôte Linux

Pourquoi et quand exécuter cette tâche

Après l'installation d'un nouveau serveur proxy, vous pouvez exécuter à nouveau le programme d'installation pour effectuer des tests afin de détecter les problèmes d'une installation ou de modifier les paramètres actuels. Vos options incluent :

- **Installer nouveau** : installez un nouveau serveur proxy.
- **Vérifier l'installation** : effectuez des tests pour détecter et résoudre les problèmes d'une installation précédente.
- **Réinstaller l'élément existant** : effectuez des tests pour détecter et corriger les problèmes dans une installation précédente et affichez ou modifiez les paramètres existants.

Remarque :
Si vous installez le serveur proxy sur une machine Linux sur un port privilégié (port 80 ou 443), vous devez exécuter le programme d'installation en tant qu'utilisateur root avec un accès complet au système de fichiers. Pour restreindre l'accès au système de fichiers après l'installation du serveur proxy, vous pouvez utiliser la fonctionnalité SetUID dans le programme d'installation proxy. Pour activer cette fonctionnalité, lancez le programme d'installation en tant que root ou sudo root. Lorsque le programme d'installation vous y invite, indiquez le nom d'utilisateur et le groupe d'utilisateurs d'un utilisateur sans privilèges. Le serveur proxy s'installera avec les privilèges du système de fichiers de l'utilisateur donné. Vous pouvez ignorer cette étape pour continuer l'installation par défaut avec les privilèges root.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Utilisez le programme d'installation pour installer plusieurs proxys pour votre instance sur plusieurs machines, en veillant à ce que les critères suivants s'appliquent :

- Tous les proxys doivent avoir les mêmes clés de chiffrement et la même paire de clés RSA utilisée pour signer numériquement les configurations et les règles de chiffrement.
- La clé de chiffrement doit être la clé par défaut configurée sur l'instance.
- Lorsqu'une base de données proxy est configurée dans le cadre de l'installation, tous les proxys doivent utiliser la même base de données proxy.

  Vous aurez peut-être besoin d'une base de données proxy pour le chiffrement préservant l'égalité, le chiffrement préservant l'ordre ou la création de jetons. Si vous n'utilisez aucune de ces fonctionnalités, vous n'avez pas besoin d'une base de données proxy.

Que faire ensuite

Pour utiliser NVDA, un lecteur d'écran de technologie d'assistance conçu pour lire les applications Java accessibles conçues pour les utilisateurs de clavier, consultez Configurer un hôte Windows 64 bits pour utiliser NVDA 32 bits avec des applications Java .

Après avoir installé le Chiffrement Edge serveur proxy, définissez la limite de mémoire initiale et la limite supérieure de mémoire du serveur proxy.

Installer le serveur proxy (programme d'installation Chiffrement Edge interactif)

Installez le Chiffrement Edge proxy sur un ordinateur Windows ou Linux.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Téléchargez le programme d'installation du serveur proxy Chiffrement Edge.
2. Ouvrez le programme d'installation du Chiffrement Edge proxy.

   Remarque :
   En cas d'installation sur un ordinateur Windows, vous devez exécuter le programme d'installation en tant qu'administrateur.

   a. Pour exécuter le programme d'installation en tant qu'administrateur sur un ordinateur Windows, cliquez avec le bouton droit de la souris sur l'invite de commande et sélectionnez **Exécuter en tant qu'administrateur**.

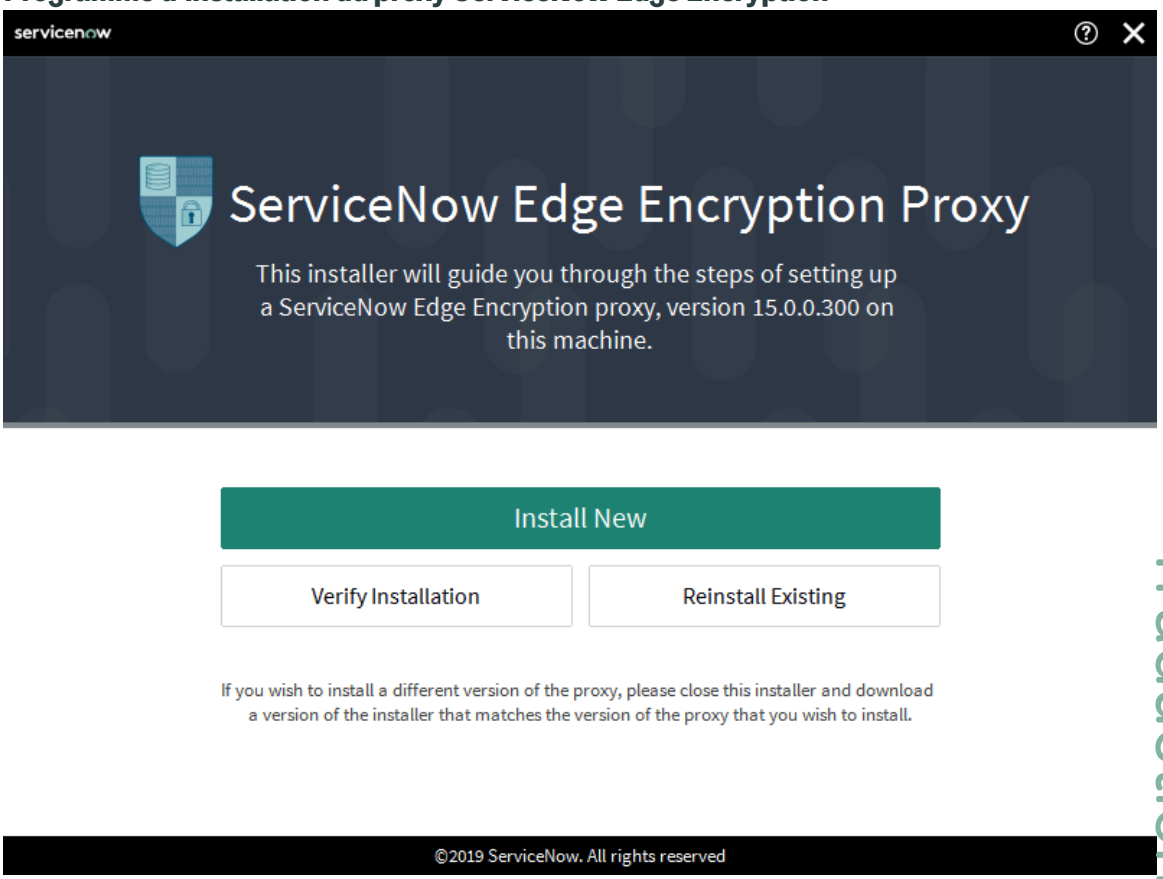
   b. À partir de la ligne de commande, accédez au répertoire qui contient le fichier .jar téléchargé.

   c. Exécutez la commande suivante : `java -jar <nom de fichier>.jar`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Programme d'installation du proxy ServiceNow Edge Encryption



Traduction automatique

3. Pour installer un nouveau serveur proxy, sélectionnez **Installer nouveau**.
   Si un proxy est déjà installé, vous pouvez exécuter le programme d'installation pour :
   - **Vérifier l'installation** : effectuez des tests pour détecter et résoudre les problèmes d'une installation précédente.
   - **Réinstaller l'élément existant** : effectuez des tests pour détecter et corriger les problèmes dans une installation précédente et affichez ou modifiez les paramètres existants.
4. Configurez **l'emplacement d'installation et l'instanceServiceNow cible**.

   a. Cliquez sur **Parcourir** pour sélectionner un emplacement d'installation ou entrez manuellement un chemin d'installation.

   b. Entrez l'URL de l'instance cible ServiceNow .
   Incluez le protocole et le numéro de port.

   Example
   `https://example.servicenow.com:443`

   c. Saisissez le nom d'utilisateur et le mot de passe d'un utilisateur ayant le rôle edge_encryption sur l'instance cible ServiceNow .

5. Cliquez sur **Suivant**.
6. Configurez les **paramètres de connexion** et les **paramètres de proxy**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Description
Hôte proxy	Nom de domaine complet de l'ordinateur sur lequel vous installez le serveur proxy. **Remarque :** Cliquez sur **Détecter le nom de domaine complet (Detect FQDN)** pour rechercher le nom de domaine complet de l'ordinateur et remplir automatiquement le champ **Proxy Host (Hôte proxy)**. Avec le port, cette propriété définit l'URL utilisée par le client pour accéder au serveur proxy.
Port HTTP	Port sur le proxy pour la communication HTTP.
Port HTTPS	Port sur le proxy de la communication HTTPS.
Nom du proxy	Nom du proxy et du service. Le nom du proxy doit être unique.
Intervalle d'interrogation du proxy	Intervalle d'interrogation en secondes. Avec le paramètre par défaut, il faut 5 secondes au proxy pour être informé des modifications de la configuration de chiffrement. Plus les valeurs sont grandes, plus l'instance met de temps à détecter les proxys mis en ligne. **Remarque :** La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de détection lors de la mise en ligne d'un proxy.
Intervalle d'envoi de ping de conservation de connexion active au proxy	Durée, en secondes, entre les pings émis par le proxy vers l'instance. Des pings sont émis périodiquement pour vérifier la connectivité entre le proxy et l'instance. La valeur par défaut est de 10. La valeur minimale est 5.

Traduction automatique

7. Cliquez sur **Installer**.
   Le Chiffrement Edge serveur proxy s'installe. L'installation peut prendre quelques minutes.

Configurer la protection des propriétés CyberArk

Vous pouvez également configurer la protection des propriétés CyberArk pour stocker Chiffrement Edge en toute sécurité les mots de passe dans un coffre-fort numérique centralisé et sécurisé.

Avant de commencer
Rôle requis : administrateur

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Vous devez acheter et configurer CyberArk AIM (Application Identity Management) avant de pouvoir configurer les paramètres de connexion CyberArk et les informations d'identification protégées pour un serveur proxy. Dans le cadre de l'installation du client AIM, le fichier JavaPasswordSDK.jar est installé dans le répertoire d'installation du client AIM. Le coffre-fort CyberArk est installé sur un serveur renforcé indépendant, et les clients AIM permettent un accès sécurisé à ce serveur.

Remarque :
Vous devez installer le client CyberArk AIM sur chaque ordinateur hôte sur lequel un proxy Edge est installé.

Dans le programme d'installation d'Edge, vous devez spécifier l'emplacement du fichier JavaPasswordSDK.jar pour configurer la connexion CyberArk au proxy Edge. Vous devez également entrer d'autres valeurs que vous avez définies lors de l'installation du client AIM.

La configuration du stockage des mots de passe CyberArk est facultative. Si vous ne souhaitez pas configurer le stockage des mots de passe CyberArk, cliquez sur **Ignorer** les écrans CyberArk.

Procédure

1. Sur la page Connexion CyberArk du programme d'installation, entrez les paramètres de Chiffrement Edge connexion CyberArk.

Paramètres de connexion CyberArk

Paramètre	Description
Chemin d'accès à PasswordSDK.jar	Le chemin vers le fichier JavaPasswordSDK.jar installé sur l'ordinateur Windows hôte pendant la configuration de CyberArk.
ID d'application	**L'ID de l'application** saisi lors de la configuration de CyberArk.
Nom sûr	Le **nom de sécurité** saisi lors de la configuration de CyberArk.

2. Cliquez sur **Suivant**.
3. Sur la page Informations d'identification protégées de CyberArk du programme d'installation, saisissez les informations d'identification à protéger par CyberArk.
   - Pour utiliser un seul nom d'informations d'identification pour tous les mots de passe protégés, cochez la case **Appliquer un nom d'informations d'identification à toutes les informations d'identification** , saisissez le nom des informations d'identification et cliquez sur **Appliquer**.
   - Saisissez le nom de l'identifiant pour un ou plusieurs des champs suivants. Les noms d'informations d'identification sont les noms d'utilisateur saisis pour les clés SSH lors de la configuration de CyberArk.

Informations d'identification protégées par CyberArk

Paramètre	Description
Utilisateur de Chiffrement Edge	Nom d'informations d'identification CyberArk d'un utilisateur de Chiffrement Edge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Description
Magasin de clés de signature	Nom d'informations d'identification CyberArk du magasin de clés de signature.
Magasin de clés de certificat HTTPS	Nom d'informations d'identification CyberArk pour le magasin de clés de certification HTTPS.
Magasin de clés de chiffrement	Nom d'informations d'identification CyberArk du magasin de clés de chiffrement.
Base de données	Nom d'informations d'identification CyberArk du magasin de clés de base de données.
Magasin de clés de certificat HTTPS SafeNet	Nom d'informations d'identification CyberArk pour le magasin de clés de certification HTTPS SafeNet.
Serveur SafeNet	Le nom d'informations d'identification CyberArk pour le serveur SafeNet.
Transférer le proxy	Le nom d'informations d'identification CyberArk du proxy direct.

4. Cliquez sur **Suivant**.

Configurer la clé de signature

Configurez la clé de signature après l'installation du serveur proxy via le programme d'installation proxy Chiffrement Edge .

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La clé de signature signe les modifications apportées aux configurations et aux propriétés par le serveur proxy. La clé de signature doit être une paire de clés RSA asymétrique dans un KeyStore JCEKS.

Remarque :
En cas d'installation de plusieurs proxys, chaque proxy doit utiliser la même clé de signature.

Procédure

1. Sur la page Clé de signature du programme d'installation, sélectionnez le magasin de Chiffrement Edge clés sur l'ordinateur hôte pour stocker la clé de signature.
   - **Créer un magasin de clés Java** : saisissez l'emplacement du répertoire, le nom et le mot de passe du nouveau magasin de clés.
   - **Utiliser le magasin de clés existant** : entrez l'emplacement et le mot de passe du fichier de magasin de clés.
2. Cliquez sur **Suivant**.
3. Sélectionnez ou créez une clé de signature.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Nouvelle clé** : créez une clé de signature pour ce proxy.
- **Utiliser la clé existante** : utilisez une paire de clés RSA du magasin de clés sélectionné.
- **Importer une clé existante** : importez une paire de clés RSA à partir d'un magasin de clés différent. Accédez au fichier du magasin de clés, saisissez le mot de passe du magasin de clés et sélectionnez l'alias de clé. Fournir un nouvel alias pour la clé.

4. Cliquez sur **Suivant**.

Configurer le certificat HTTPS

Pour permettre aux clients de se connecter au serveur proxy à l'aide Chiffrement Edge d'une connexion SSL sécurisée, importez le certificat HTTPS dans le serveur proxy.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Le Chiffrement Edge proxy fournit le certificat HTTPS aux clients qui tentent de se connecter.

Procédure

1. Sur la page Certificat HTTPS du programme d'installation, sélectionnez le magasin de Chiffrement Edge clés pour stocker le certificat.
   - **Créer un magasin de clés Java** : saisissez l'emplacement du répertoire, le nom et le mot de passe du nouveau magasin de clés.
   - **Utiliser le magasin de clés existant** : entrez l'emplacement et le mot de passe du fichier de magasin de clés.
2. Cliquez sur **Suivant**.
3. Sélectionnez ou importez un certificat.
   L'alias de clé est l'alias donné pour le certificat.
   - **Utiliser le certificat existant** : utilisez un certificat existant dans le magasin de clés sélectionné.
   - **Importer à partir d'un fichier ou d'un magasin de clés** : importez un certificat à partir d'un autre magasin de clés ou d'un fichier .cer. Accédez au magasin de clés ou au fichier .cer, saisissez le mot de passe et sélectionnez l'alias. Vous devez fournir un nouvel alias pour le certificat.
4. Cliquez sur **Suivant**.

Configurer la clé de chiffrement AES 128 bits

Après avoir configuré le certificat HTTPS via le programme d'installation Chiffrement Edge du proxy, configurez la clé de chiffrement AES 128 bits pour chiffrer vos données.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
La clé de chiffrement est soit un fichier texte brut dans le répertoire `/keys` , soit une clé secrète dans un magasin de clés. Si vous utilisez un magasin de clés pour vos clés de chiffrement AES 128 bits et AES 256 bits, ils doivent tous les deux utiliser le même magasin de clés.

Si vous mettez à jour un certificat SSL sur un serveur proxy Edge, reportez-vous à la rubrique Mettre à jour le certificat SSL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sélectionnez l’emplacement de la clé de chiffrement.
2. Cliquez sur **Suivant**.
3. Sélectionnez ou créez la clé de chiffrement.
4. Cliquez sur **Suivant**.
5. Configurez la clé sur l’instance en fonction des exigences définies dans votre programme d’installation. Pour configurer la clé sur l’instance, accédez à l’instance et définissez une clé par défaut. Voir Configurer les clés de chiffrement sur l’instance. Assurez-vous que l’alias, la taille et le type de clé correspondent aux exigences définies dans le programme d’installation.

Besoins de clés par défaut



6. Une fois la clé configurée sur l’instance, revenez au programme d’installation et cliquez sur **Suivant**.

Configurer la clé de chiffrement AES 256 bits

Après avoir configuré la clé AES 128 bits via le programme d’installation du proxy Edge, vous pouvez éventuellement configurer une clé de chiffrement AES 256 bits pour chiffrer vos données.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

La clé de chiffrement est soit un fichier texte brut dans le répertoire /keys , soit une clé secrète dans un magasin de clés. Si vous utilisez un magasin de clés pour vos clés de chiffrement AES 128 bits et AES 256 bits, les deux clés doivent utiliser le même magasin de clés. Si vous ne souhaitez pas configurer de clé de chiffrement AES 256 bits, sélectionnez **Ignorer** pour continuer l'installation du serveur proxy.

Si vous mettez à jour un certificat SSL sur un serveur proxy Edge, reportez-vous à la rubrique Mettre à jour le certificat SSL.

Procédure

1. Sélectionnez l'emplacement de la clé de chiffrement.
2. Sélectionnez **Suivant**.
3. Sélectionnez ou créez la clé de chiffrement.
4. Sélectionnez **Suivant**.
5. **Facultatif :** Si vous souhaitez utiliser le chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.
6. Pour utiliser le chiffrement AES 256 bits, vous devez également configurer la clé de chiffrement AES 256 bits par défaut sur l'instance.

   Pour ce faire, accédez à l'instance et définissez une clé par défaut. Consultez Configurer les clés de chiffrement sur l'instance. Assurez-vous que l'alias, la taille et le type de clé correspondent aux exigences définies dans le programme d'installation.
7. Une fois la clé configurée sur l'instance, revenez au programme d'installation et sélectionnez **Suivant**.

Mettre à jour le certificat SSL

Lors de la mise à jour d'un certificat SSL sur un serveur proxy Edge, vous devez supprimer l'ancien.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Lors de la mise à jour du certificat SSL sur le serveur proxy Edge, vous devez également supprimer l'ancien certificat. Si vous ne le faites pas, l'ancien certificat (sous la forme d'un alias dans le fichier KeyStore) continue d'être utilisé même si le serveur proxy Edge est configuré pour utiliser le nouveau certificat.

Procédure

1. Sur le serveur proxy Edge, répertoriez les entrées dans le Java KeyStore :

   ```
   keytool -list -keystore keystore.jceks -storetype jceks -storepass MY_SUPER_PASSWORD
   ```
2. Supprimer l'ancien certificat SSL :

   ```
   keytool -delete -alias MY_OLD_ALIAS -keystore keystore.jceks -storetype jceks -storepass
    MY_SUPER_PASSWORD
   ```
3. Ajoutez le nouveau certificat SSL dans le Java KeyStore.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la base de données proxy Chiffrement Edge

Si vous utilisez des types de chiffrement ou des modèles de chiffrement préservant l'ordre, vous pouvez éventuellement configurer les propriétés de la Chiffrement Edge base de données proxy.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Pour utiliser des types de chiffrement ou des modèles de chiffrement préservant l'ordre, une base de données MySQL en cours d'exécution sur votre réseau est obligatoire. Cette tâche connecte le proxy à la base de données, mais elle n'installe ni ne configure la base de données.

Remarque :
En cas d'utilisation de plusieurs serveurs proxy, tous les serveurs proxy doivent utiliser la même base de données proxy. Les valeurs saisies dans le programme d'installation doivent être les mêmes pour tous les serveurs proxy.

Procédure

1. Confirmez ou modifiez l'URL de la base de données, qui correspond à l'emplacement de la base de données proxy.
2. Dans le champ **Nom** , entrez le nom de la base de données proxy.
   La valeur par défaut est `edgeencryption`.
3. Entrez le nom d'utilisateur et le mot de passe pour accéder à la base de données proxy.
4. Cliquez sur **Suivant**.

Lancer le serveur proxy Chiffrement Edge

Une fois qu'un Chiffrement Edge proxy est installé et configuré, vous pouvez le démarrer à partir du programme d'installation.

Avant de commencer
Rôle requis : administrateur

Procédure

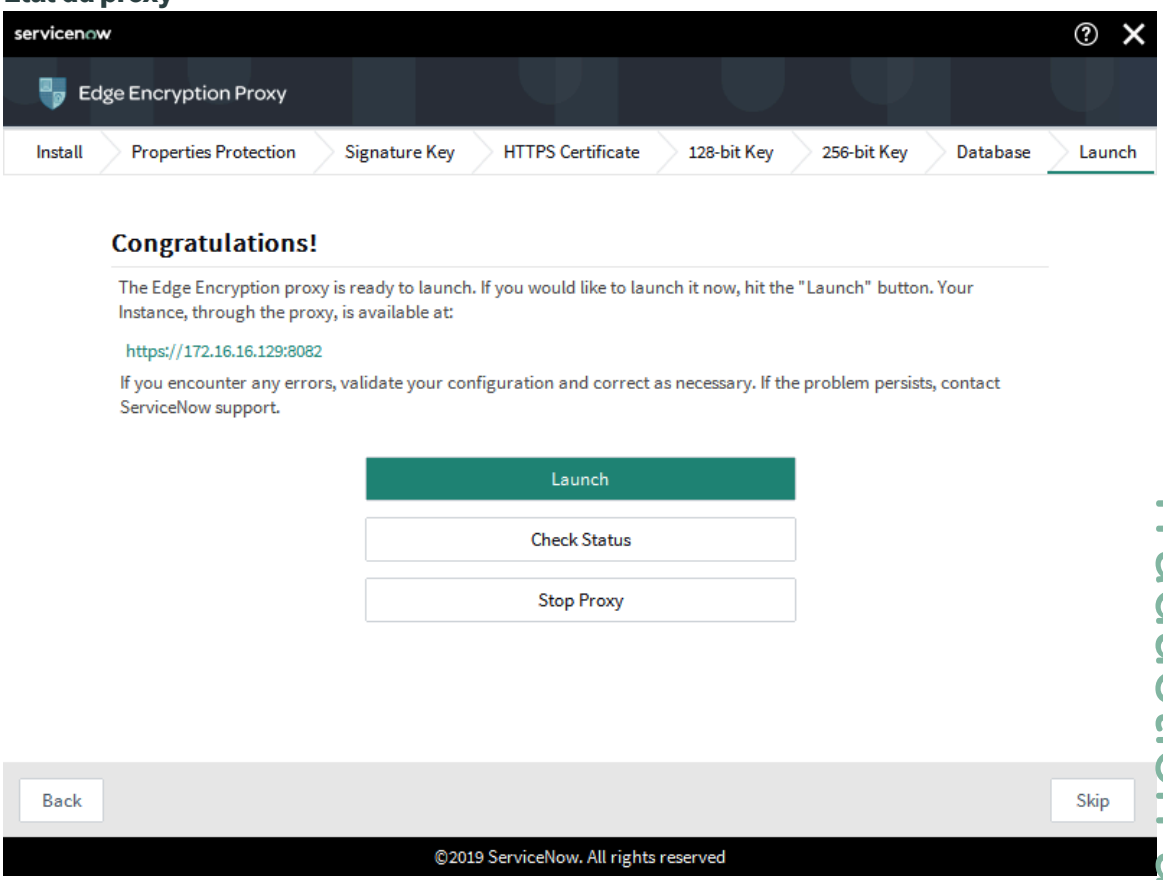
1. Après avoir configuré les clés sur l'instance et configuré la base de données proxy, revenez au programme d'installation Chiffrement Edge proxy et cliquez sur **Lancer**.
2. Si un problème est détecté ou pour vérifier l'état de votre serveur proxy, vous pouvez cliquer sur **Vérifier l'état** pour vérifier que le proxy est en cours d'exécution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un message affiche l'état du proxy.

État du proxy



Que faire ensuite

Après l'installation réussie du serveur proxy, Définir la limite de mémoire initiale et la limite supérieure de mémoire du serveur proxy.Chiffrement Edge

Vérifier et résoudre les problèmes liés à l'installation du serveur proxy Chiffrement Edge

Une fois votre Chiffrement Edge proxy installé, vous pouvez vérifier l'installation pour localiser les problèmes ou démarrer et arrêter le proxy.

Avant de commencer

Rôle requis : administrateur

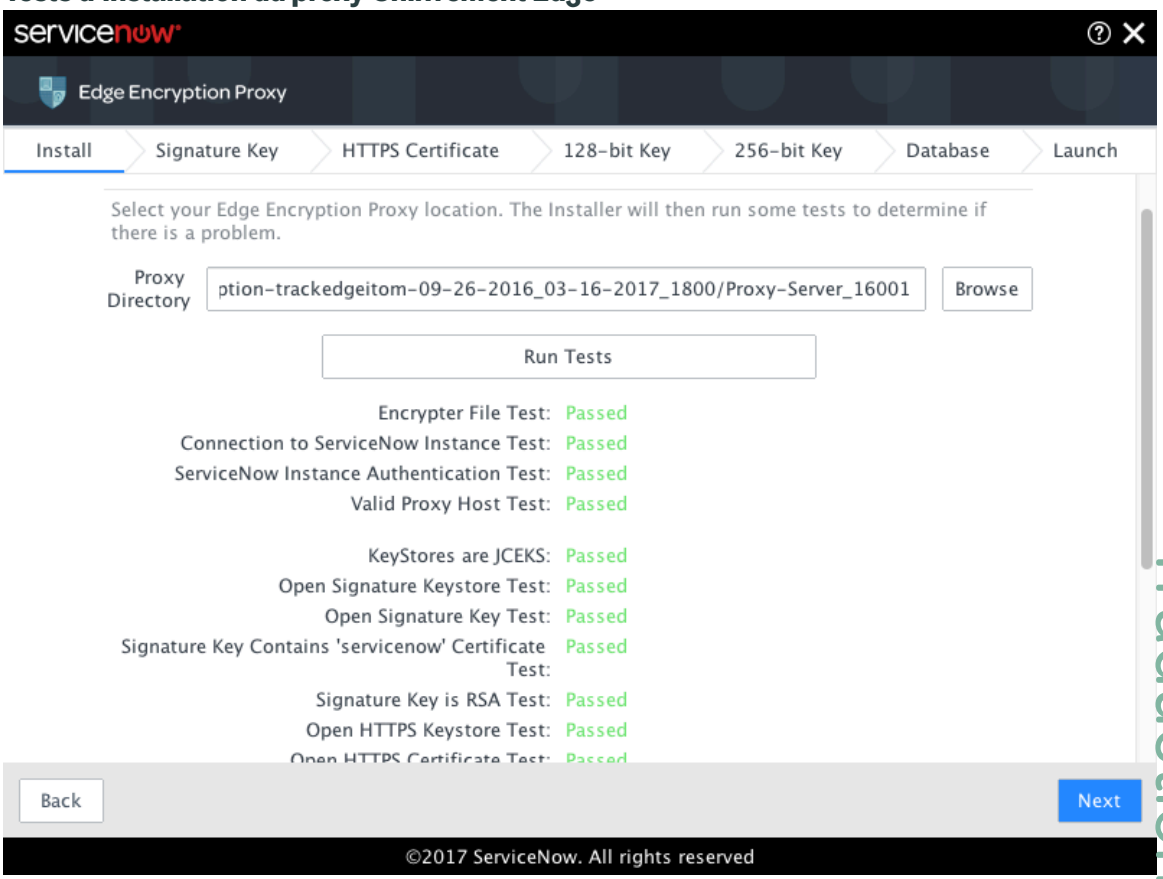
Procédure

1. Ouvrez le programme d'installation du Chiffrement Edge proxy.
2. Sélectionnez **Vérifier l'installation**.
3. Cliquez sur **Répertoire proxy** et sélectionnez le répertoire proxy.
4. Cliquez sur **Exécuter les tests**.
   Les résultats des tests s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tests d'installation du proxy Chiffrement Edge



5. Cliquez sur **Suivant**.
   Si un problème est rencontré, vous pouvez passer par le programme d'installation pour corriger la configuration. Si aucun problème n'est rencontré, le programme d'installation passe à la page **de lancement** . Vous pouvez vérifier l'état du proxy, arrêter le proxy ou démarrer le proxy à partir de la page **Lancer** .

Installer le serveur proxy Chiffrement Edge à l'aide du programme d'installation de ligne de commande

Installez manuellement plusieurs Chiffrement Edge serveurs proxy sur votre réseau.

Avant de commencer

Rôles requis : security_admin sur votre ServiceNow instance et administrateur local sur l'ordinateur hôte.

Si des types ou des modèles de chiffrement préservant l'ordre doivent être utilisés, configurez une base de données MySQL sur une machine de votre réseau si elle n'est pas déjà présente.

Remarque :
Si vous utilisez des clés de chiffrement Unbound Technology avec Chiffrement Edge, installez le serveur proxy à l'aide du programme d'installation de ligne de commande sur la machine cliente Unbound. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client de technologie Unbound.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Tout d'abord, configurez un serveur proxy unique Chiffrement Edge . Une fois que votre premier serveur proxy est en cours d'exécution, ajoutez des serveurs proxy supplémentaires pour une instance afin de garantir un environnement optimal. Reportez-vous à la rubrique Dimensionnement de votre environnement Edge Encryption pour déterminer le nombre de serveurs proxy supplémentaires nécessaires.

Installer le serveur proxy Chiffrement Edge (programme d'installation de ligne de commande)

Installez un Chiffrement Edge proxy sur un ordinateur Windows ou Linux 64 bits.

Avant de commencer

Rôle requis : administrateur

La version Java 11.0.6 ou ultérieure de la série de versions 11.x est requise pour exécuter le programme d'installation.

Pourquoi et quand exécuter cette tâche

Installez le Chiffrement Edge serveur proxy sur une machine de votre réseau à l'aide de la commande appropriée pour votre machine cible. Si vous installez le Chiffrement Edge serveur proxy sur un ordinateur Windows, vous devez également installer le serveur proxy en tant que service Windows.

Lorsque vous mettez à niveau le serveur proxy Chiffrement Edge, le système sauvegarde l'ancien proxy dans le répertoire backup.dist-upgrade-<timestamp> sous le répertoire d'installation actuel. Le répertoire de sauvegarde est généré lors du processus de mise à niveau et stocke les anciennes informations de proxy.

Lorsque vous exécutez une mise à niveau via la ligne de commande, un dist-upgrade.log peut être généré dans le répertoire dans lequel la commande s'exécute. Le dist-upgrade.log contient des journaux pour le processus de mise à niveau.

En cas d'échec de la mise à niveau, le système crée un répertoire failed-backup.dist-upgrade-<timestamp> . En outre, les journaux/wrapper.log dans le répertoire proxy d'origine peuvent également contenir des informations sur les défaillances.

Procédure

1. Créez le répertoire d'installation.
2. Téléchargez le fichier d'archive Chiffrement Edge proxy dans le répertoire d'installation.
3. Ouvrez le terminal et accédez au répertoire d'installation.

> **Remarque :**
> En cas d'installation sur un ordinateur Windows, vous devez démarrer l'invite de commande Windows avec les privilèges d'administrateur.

4. Exécutez cette commande pour la machine cible et modifiez les variables en fonction de votre configuration :
   `java -jar edgeencryption-<version>-all.jar -m install -n <ProxyName> --instancehost <host> -p <InstancePort> --protocol https`

Option	Variable	Description
aucun	version	Numéro de version du Chiffrement Edge proxy utilisé pour effectuer l'opération en cours.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Variable	Description
-m	Mode	Opération ou mode d'exécution (installation ou mise à niveau).
-n	Nom du proxy	Nom de l'instance du proxy de chiffrement. Utilisez un ProxyName unique pour pouvoir identifier des instances de proxy spécifiques.
--instancehost	hôte	Le nom d'hôte de votre instance ServiceNow (par exemple, mycompany.service-now.com).
-p	Port d'instance	Port de votre instance. Lorsque le protocole est https, le port est normalement 443.
--protocole	protocol	Protocole utilisé pour accéder à votre instance ServiceNow (généralement https).

Remarque :
Ne copiez pas et ne collez pas de commandes à partir du navigateur. Parfois, des opérations de copier/coller provoquent le collage de caractères inattendus sur la machine cible et entraînent une exécution incorrecte de la commande. Il est préférable de taper la commande à la main en utilisant la documentation comme référence.

Pour afficher l'écran d'aide, exécutez cette commande sans arguments : `java -jar edgeencryption-<version>-all.jar`

5. En cas d'installation sur un ordinateur Windows, installez le Chiffrement Edge proxy en tant que service Windows.

   a. **Facultatif :** Modifiez le nom du service en ouvrant le fichier conf/wrapper.conf sur le nouveau proxy et en définissant les propriétés dans la table suivante.

Propriété	Description
wrapper.ntservice.name	Nom unique du Chiffrement Edge service proxy.
wrapper.ntservice.displayname	Chiffrement Edge Nom d'affichage du service proxy.
wrapper.ntservice.description (facultatif)	Description du serveur proxy.

   Si cette étape n'est pas effectuée, le Chiffrement Edge service proxy est installé sous le nom **de Chiffrement Edge**.

   b. Enregistrez et fermez le fichier.

   c. Ouvrez l'invite de commande Windows et cd pour ServerName_port/bin.

   d. Exécutez edgeencryption.bat installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Le répertoire ProxyName_port est créé dans le répertoire courant. Le fichier edgeencryption.properties est mis à jour avec les valeurs hôte, port et protocole de la ligne de commande.

Créer et configurer la paire de clés RSA pour la signature numérique

Créez une paire de clés RSA que le serveur proxy peut utiliser pour créer la signature numérique pour signer les modifications apportées aux propriétés et à la configuration de chiffrement.

Avant de commencer
Rôle requis : administrateur

Pour générer et valider la signature numérique, une paire de clés RSA doit être générée et stockée dans le magasin de clés Java JCEKS et chaque proxy doit être configuré pour utiliser cette paire de clés. Générez une paire de clés de chiffrement à l'aide de la commande keytool.

Pour utiliser l'utilitaire keytool avec un proxy installé sur SElinux (CentOS), vous devez activer le chargement des bibliothèques partagées à partir du répertoire proxy java-installation. Pour ce faire, exécutez la commande suivante en tant que root.

```
chcon -R -t texrel_shlib_t proxy_install_dir/java/jre /lib
```

Vous devez utiliser la version Java 1.8 de l'utilitaire keytool. Une copie de l'utilitaire se trouve dans <proxy install dir>java/jre/bin/keytool.

Procédure

1. Accédez au répertoire KeyStore dans le répertoire de téléchargement proxy.
2. Changez le mot de passe par défaut.

   Le mot de passe par défaut est *changeme*.

   ```
   keytool -keystore keystore.jceks -storetype jceks -storepasswd -new <newpassword>
   ```

3. Créer une paire de clés de chiffrement.

   Remarque :
   N'entrez pas de mot de passe pour la clé lorsque l'utilitaire keytool vous en demande un.

   Entrez cette commande sur une seule ligne.

   ```
   keytool -genkeypair -alias <key alias> -keyalg rsa -keystore keystore.jceks
   -storetype jceks -storepass <keystore password> -keysize 2048
   ```

4. Mettez à jour le fichier de propriété du proxy de chiffrement (edgeencryption.properties).

   a. Accédez au répertoire <installation>/conf/ .

   b. Ouvrez le fichier edgeencryption.properties .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Saisissez les propriétés de la signature numérique.

Ces propriétés doivent être les mêmes pour tous les proxys.

5. Enregistrez et fermez le fichier edgeencryption.properties .

Importer et configurer le certificat pour une connexion SSL sécurisée

Pour utiliser une connexion SSL sécurisée, importez un certificat de serveur et ajoutez-le au Java KeyStore.

Avant de commencer
Rôle requis : administrateur

Vous devez obtenir le certificat du serveur et la clé privée correspondante avant de l'ajouter au magasin de clés Java.

Procédure

1. Générez une demande de signature de certificat (CSR) à l'aide de la commande openssl .

```
openssl req -newkey rsa:2048 -keyout PRIVATEKEY.key -out MYCSR.csr
```

2. Envoyez votre CSR (MYCSR.csr dans l'exemple ci-dessus) à votre autorité de certification pour qu'elle la fasse signer.
3. Créez un magasin de clés P12 à importer à l'aide de la commande openssl .

```
openssl pkcs12 -export -in MYSIGNEDCERT.pem -inkey PRIVATEKEY.key -name shared >
 MY_SERVER.p12
```

4. Stockez votre certificat et votre clé privée dans un fichier jceks.

```
keytool -importkeystore -destkeystore keystore.jceks -deststoretype jceks -srckeystore
 MY_SERVER.p12 -srcstoretype pkcs12 -alias MYALIAS
```

L'alias, représenté dans l'exemple par MYALIAS , peut avoir n'importe quelle valeur. Vous utiliserez cet alias dans la propriété edgeencryption.proxy.https.cert.alias dans le fichier edgeencryption.properties situé dans le dossier <répertoire d'installation>/conf/ .

5. Arrêtez et redémarrez le proxy Edge.

Remarque :
Lors d'un redémarrage, le serveur proxy est hors ligne pendant une courte période. La durée est déterminée par votre environnement et le temps nécessaire pour arrêter et redémarrer le service proxy.

Configurer un magasin de clés et des clés de chiffrement

Configurez le magasin de clés et les clés de chiffrement utilisés par le Chiffrement Edge serveur proxy.

Avant de commencer
Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Déterminez soigneusement le type de magasin de clés approprié à utiliser en fonction des besoins de votre organisation.

Magasin de clés pris en charge	Description
Magasin de fichiers	Les clés sont stockées dans un fichier dans un système de fichiers auquel le Chiffrement Edge serveur proxy accède. Étant donné que les clés de chiffrement stockées dans un fichier ne sont pas chiffrées, il est de votre responsabilité de protéger ces fichiers.
Java KeyStore	Un magasin de clés Java : ○ Stocke les clés dans un magasin de clés Java JCEKS. ○ Est protégé par mot de passe et plus sécurisé que le stockage des clés dans un fichier dans le système de fichiers. ○ Peut stocker plusieurs clés. Un alias de clé représente chaque clé, ce qui facilite la gestion de plusieurs clés. Le Chiffrement Edge proxy est livré avec le fichier Java JCEKS KeyStore nommé keystore.jceks dans le répertoire keystore . Ce fichier keystore contient la clé publique utilisée pour valider les ServiceNow règles de chiffrement signées par ServiceNow.
Gestion des clés d'entreprise (EKM)	**SafeNet KeySecure** Les clés sont stockées et récupérées avec la gestion des clés SafeNet KeySecure. Vous devez obtenir une licence auprès de Gemalto , télécharger les bibliothèques et installer le magasin de clés SafeNet KeySecure sur une machine hôte de votre réseau avant de configurer le magasin de clés sur le Chiffrement Edge serveur proxy. **Technologie Unbound** La clé de chiffrement encodée en base64 est stockée sous forme de fichier texte sur le Chiffrement Edge serveur proxy. L'implémentation de la technologie Unbound (anciennement Dyadic Security) conserve le contrôle de la clé d'encapsulation. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client de technologie Unbound.

Remarque :
Si vous utilisez un magasin de clés autre que le KeyStore Java JCEKS du système de base, vous devez importer la clé publique dans votre magasin de ServiceNow clés. L'alias de clé publique est `servicenow`.

2. Configurez le magasin de clés et les clés de chiffrement dans votre réseau local.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer un magasin de clés Java KeyStore

Vous pouvez utiliser un magasin de clés Java KeyStore pour stocker les clés de chiffrement.

Avant de commencer

Rôle requis : administrateur

Vous devez utiliser la version Java 1.8 de l'utilitaire keytool. Une copie de l'utilitaire se trouve dans <répertoire d'installation proxy>/java/jre/bin/keytool.

Pourquoi et quand exécuter cette tâche

Le Chiffrement Edge proxy est livré avec le fichier Java JCEKS KeyStore nommé keystore.jceks dans le répertoire keystore . Ce fichier keystore contient la clé publique utilisée pour valider les ServiceNow règles de chiffrement signées par ServiceNow.

Procédure

1. Configurez les propriétés du keystore.
   a. Accédez au répertoire <installation>/conf/ .
   b. Ouvrez le fichier edgeencryption.properties .
   c. Entrez les propriétés du Java KeyStore.
2. Enregistrez et fermez le fichier edgeencryption.properties .

Que faire ensuite

Après avoir configuré le KeyStore Java, Créer des clés de chiffrement à l'aide de l'outil de clés Java KeyStore.

Créer des clés de chiffrement à l'aide de l'outil de clés Java KeyStore

Vous pouvez utiliser l'outil clé fourni avec la distribution de proxy de chiffrement pour créer des clés de chiffrement AES 128 bits et AES 256 bits.

Avant de commencer

Rôle requis : administrateur

Vous devez utiliser la version Java 1.8 de l'utilitaire keytool. Une copie de l'utilitaire se trouve dans <répertoire d'installation proxy>/java/jre/bin/keytool.

Pour en savoir plus sur l'utilitaire keytool, consultez la documentation Java SE .

Pourquoi et quand exécuter cette tâche

Remarque :
Le KeyStore Java exige que le nom de l'alias (nom de la clé, alias de la clé) utilise des lettres minuscules et des chiffres.

Procédure

1. Accédez au répertoire du magasin de clés, <répertoire d'installation>/keystore/.
2. Pour créer la clé de chiffrement, exécutez l'une des commandes suivantes.

Remarque :
Si vous choisissez d'exécuter ces commandes à partir d'un répertoire autre que le répertoire keystore, *c'est-à-dire* que vous avez ignoré l'étape précédente, vous devez modifier l'option -keystore pour inclure le chemin d'accès de votre répertoire actuel au répertoire keystore. Par exemple, si vous vous trouvez dans le répertoire <installation>\bin , l'option serait -keystore .. /keystore/keystore.jceks.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
AES 128	`keytool -genseckey -alias 128bitkey -keyalg aes -keysize 128 -keystore keystore.jceks -storetype jceks`
AES 256	`keytool -genseckey -alias 256bitkey -keyalg aes -keysize 256 -keystore keystore.jceks -storetype jceks`

Vous ajoutez l'alias sur l'instance lorsque vous affectez des clés par défaut.

Remarque :
Le mot de passe de clé doit être identique au mot de passe de magasin de clé.

Configurer un magasin de clés SafeNet KeySecure

Si vous utilisez un magasin de clés SafeNet, copiez un ensemble de bibliothèques dans le répertoire de distribution proxy.

Avant de commencer
Rôle requis : administrateur

Vous devez installer et configurer le magasin de clés SafeNet avant d'effectuer cette étape. Obtenir une licence auprès de Thales afin de télécharger les bibliothèques.

Remarque :
Pour la version 8.12 d'IngrianNAE, vous devez également télécharger le fichier commons-collections.jar

Pourquoi et quand exécuter cette tâche
Remarque :
Sous Linux, les chemins d'accès aux fichiers utilisent une barre oblique (/).

Procédure

1. Accédez au répertoire <installation>/conf/ , puis ouvrez le fichier edgeencryption.properties .
2. Saisissez les propriétés du magasin de clés SafeNet.

Remarque :
Vous pouvez configurer le magasin de clés SafeNet avec l'authentification par nom d'utilisateur/mot de passe ou l'authentification par certificat client, mais pas une combinaison des deux.

Example

Exemple d'un magasin de clés SafeNet utilisant l'authentification par nom d'utilisateur et mot de passe.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_truststore
edgeencryption.nae.keystore.password = password
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
edgeencryption.nae.user = safenet_user
edgeencryption.nae.password = safenet_password
```

Example

Exemple d'un magasin de clés SafeNet utilisant l'authentification par certificat client. Cette méthode d'authentification élimine la nécessité de stocker le nom d'utilisateur et le mot de passe du serveur SafeNet dans le fichier de propriétés.

```
edgeencryption.nae.retries = 3
edgeencryption.nae.enabled = true
edgeencryption.nae.server = url
edgeencryption.nae.port = 9000
edgeencryption.nae.protocol = ssl
edgeencryption.nae.keystore.path = keystore/safenet_clientcert
edgeencryption.nae.keystore.password = password
edgeencryption.nae.client.certificate = cert_name
```

3. Ajoutez ou créez une clé dans le magasin de clés SafeNet.
   Vous ajoutez le nom de la clé (alias) à l'instance lorsque vous affectez des clés par défaut.
4. Enregistrez et fermez le fichier edgeencryption.properties .

Surclassement de Kingston ou une version antérieure vers London ou une version supérieure

Si vous utilisez un serveur NAE SafeNet pour le stockage des clés avec Edge, avant de mettre à niveau le proxy à partir d'un London serveur ProtectApp ou d'un Kingston niveau inférieur, vous devez copier les fichiers JAR ProtectApp du client Gemalto SafeNet et ajouter de nouvelles propriétés.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Remarque :
Sous Linux, les chemins d'accès aux fichiers utilisent une barre oblique (/).

Procédure

1. Copiez les fichiers suivants du <répertoire d'installation>/lib vers le répertoire <installation>/nae :
   - commons-collections<version>.jar
   - ingrianlog4j-api-<version>.jar
   - ingrianlog4j-core-<version>.jar
   - ingrianNAE-<version>.jar
2. Sur la version actuelle (non mise à niveau) du proxy, mettez à jour le fichier <répertoire d'installation>/conf/edgeencryption.properties en ajoutant les deux propriétés suivantes :
   - *edgeencryption.ekm.provider.classname* = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider
   - *edgeencryption.thirdparty.vendor.library.path* = <chemin du répertoire vers le répertoire dans lequel vous avez copié les fichiers jar à l'étape 1>

     Remarque :
     edgeencryption.thirdparty.vendor.library.path pour Java 11.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Enregistrez les changements.
4. Procédez à la mise à niveau vers London ou une version supérieure.

Configurer Unbound Clés technologiques

Utilisez les clés Unbound Technology (anciennement Sécurité dyadique) en Chiffrement Edge stockant la clé de chiffrement encodée en base64 sous forme de fichier texte sur le Chiffrement Edge serveur proxy et en fournissant l'alias de clé d'encapsulation. L'implémentation d'Unbound Technology conserve le contrôle de la clé d'encapsulation.

Avant de commencer

Rôle requis : security_admin

Dans votre implémentation de la technologie Unbound, identifiez à la fois la clé encapsulée et la clé encapsulée. Utilisez l'algorithme RSA/ECB/OAEPWITHSHA-256ANDMGF1PADDING pour l'emballage et le remplissage. Exportez la clé enveloppée au format texte codé en base64. Enregistrez le fichier à l'aide de l'alias de la clé comme nom sans extension de fichier.

Remarque :
Si vous utilisez des clés de chiffrement Unbound Technology avec Chiffrement Edge, installez le serveur proxy à l'aide du programme d'installation de ligne de commande sur la machine cliente Unbound. Le Chiffrement Edge serveur proxy doit s'exécuter sur le même ordinateur que le client de technologie Unbound.

Procédure

1. Ajoutez la clé de chiffrement encapsulée au format texte codé en base64 dans le répertoire <proxy-installation-directory>/keys .
   Le nom du fichier doit être l'alias de la clé sans extension de fichier.
2. Mettez à jour le fichier edgeencryption.properties .
   a. Accédez au répertoire <proxy-installation-directory>/conf .
   b. Ouvrez le fichier edgeencryption.properties .
   c. Entrez les propriétés du magasin de fichiers et définissez la valeur de *edgeencryption.keyfile.directory* to keys.

      Cette propriété demande au serveur proxy de rechercher la clé de chiffrement dans le répertoire <Java-home-directory>/keys .

      Pour plus d'informations sur Chiffrement Edge les propriétés, consultez Propriétés du serveur proxy Chiffrement Edge.

   d. Supprimez les commentaires des propriétés de la configuration du fournisseur Dyadic et définissez la valeur de l'alias de clé d'encapsulation *edgeencryption.ekm.provider.rsa.wrapping.key.alias* dans votre implémentation Unbound.
   e. Enregistrez et fermez le fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Ajoutez l'alias de la clé de chiffrement à l'instance. L'alias de clé de chiffrement est le nom de fichier de la clé de chiffrement encapsulée ajoutée au répertoire <proxy-installation-directory>/keys . Par exemple, si le fichier du répertoire est nommé myunboundkey, ajoutez ce nom au champ Alias de **clé** . Reportez-vous à Configurer les clés de chiffrement sur l'instance.

Créer une clé de chiffrement stockée dans un fichier

Vous pouvez utiliser un simple fichier texte comme magasin de clés. Chaque fichier contient une seule clé de chiffrement.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Cette étape crée à la fois le stockage de clé et la clé de chiffrement.

Remarque :
Le nom du fichier de clé doit correspondre à l'alias de clé spécifié dans la table des clés de chiffrement de l'instance. Voir Configurer les clés de chiffrement sur l'instance.

Procédure

1. Créez un fichier dans le dossier /keys du répertoire d'installation du serveur proxy.
2. Ajoutez la clé de chiffrement au fichier.

Option	Description
AES 128	Placez la clé de chiffrement, exactement 16 octets, dans le fichier.
AES 256	Placez la clé de chiffrement, exactement 32 octets, dans le fichier.

3. Mettez à jour le fichier edgeencryption.properties .
   a. Accédez au répertoire <installation>/conf/ .
   b. Ouvrez le fichier edgeencryption.properties .
   c. Entrez les propriétés du magasin de fichiers.
   d. Enregistrez et fermez le fichier.

Configurer les clés de chiffrement sur l'instance

Chiffrement Edge Fournit les outils permettant de gérer les clés de chiffrement sans mettre le proxy hors ligne.

Avant de commencer

Rôle requis : security_admin

Avant de configurer de nouvelles clés de chiffrement sur l'instance :

1. Créez la clé de chiffrement.
2. Mettez la nouvelle clé à la disposition de tous les proxys de chiffrement. Copiez le fichier ou le fichier Java KeyStore vers chaque proxy, ou assurez-vous que chaque proxy a accès au KeyStore Java ou à l'appareil de gestion des clés d'entreprise (EKM).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Les alias de clés doivent être uniques. Chaque alias de clé doit avoir la même taille et le même type de clé sur chaque proxy, sinon la clé ne peut pas être affectée comme valeur par défaut.

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Configurer les clés.**.
2. Dans la section Ajouter de nouvelles clés du formulaire, procédez comme suit pour ajouter une nouvelle clé.

   Important :
   Si vous utilisez des clés versionnées SafeNet, une colonne supplémentaire s'affiche pour la **version de clé**. La **version de la clé** ne peut pas être modifiée. Cliquez sur le lien **Récupérer les dernières versions de clés** dans les liens connexes pour récupérer la dernière version de chaque clé à partir du proxy Edge.

   Les lignes de la liste marquées d'un **X** dans la colonne de gauche peuvent être supprimées. Les clés qui ont été utilisées par défaut ou dont **l'état** est **Disponible** ne peuvent pas être supprimées.

   a. Double-cliquez sur la ligne indiquant **Insérer une nouvelle ligne.**

   b. Dans la zone d'édition, saisissez un nom pour la clé, puis cochez la coche.

      Les alias clés sont des lettres minuscules et des chiffres. Les lettres majuscules sont remplacées par des lettres minuscules lorsque vous cliquez sur **Mettre à jour**. Les alias de clés doivent être uniques.

      Remarque :
      Si vous utilisez des clés technologiques Unbound, ajoutez l'alias de clé de chiffrement. L'alias de clé de chiffrement est le nom de fichier de la clé de chiffrement encapsulée ajoutée au répertoire <proxy-installation-directory>/keys . Par exemple, si le fichier du répertoire est nommé myunboundkey, ajoutez ce nom au champ Alias de **clé** .

   c. Sur la même ligne, double-cliquez dans la colonne Taille de la **clé** .

   d. Dans la zone de sélection, sélectionnez une taille de clé, **128 bits** ou **256 bits**, puis cochez la case.

   e. Sur la même ligne, double-cliquez dans la colonne **Type** .

   f. Dans la zone de sélection, sélectionnez un type de clé, **soit Fichier**, **Keystore**, **SafeNet** ou **Unbound**, puis cochez la case.

   g. Lorsque vous avez terminé d'ajouter des clés, cliquez sur **Étape suivante**.
   Vous devez spécifier un alias, une taille de clé et un type de clé pour chaque clé avant de continuer.

3. Dans la section État des clés du formulaire, vérifiez **l'état** de la clé et assurez-vous qu'elle est **disponible**.
4. Lorsque la clé est **disponible**, cliquez sur **Étape suivante**.
   Cette opération peut prendre quelques minutes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous utilisez des clés versionnées SafeNet, une colonne supplémentaire s'affiche pour la **version de clé**. La **version de la clé** ne peut pas être modifiée.

L'instance suit l'état de chaque clé de chiffrement disponible pour n'importe quel proxy. Lorsqu'une clé est disponible sur tous les proxys, son état devient **Disponible**. Si l'état ne change pas après quelques minutes, vérifiez que la clé est disponible sur tous les proxys. Si l'état reste **indisponible**, un ou plusieurs des proxys ne possèdent pas la clé.

États des clés de chiffrement

États	Description
Disponible	Tous les proxys en ligne ont la clé.
Non disponible	Il s'agit d'une nouvelle clé et les proxys ne l'ont pas encore chargée, ou au moins un proxy n'a pas réussi à la charger.

5. Dans la section Changer les clés par défaut du formulaire, effectuez l'une des actions suivantes :
   - Tapez l'alias de clé.
   - Cliquez sur l'icône de loupe et sélectionnez un alias.

   Remarque :
   En cas d'utilisation de clés versionnées SafeNet, un champ supplémentaire s'affiche pour la **version de clé**. La **version de la clé** est grisée et ne peut pas être modifiée. Choisissez uniquement la version de clé la plus récente. Si vous choisissez une version antérieure, le message suivant s'affiche lorsque vous cliquez sur **Mettre à jour** ou **sur Étape suivante**.

   ```
   One of the default keys chosen is not the latest version available for the key. Please use the latest version.
   ```

   Si les clés par défaut ne correspondent pas aux dernières versions des clés SafeNet, un lien **Mettre à jour les clés par défaut vers la dernière version** s'affiche dans les liens connexes. Cliquez sur le lien pour mettre à jour les clés par défaut afin d'utiliser la dernière version.

6. Dans la section Planifier la rotation de clé du formulaire, planifiez une tâche de rotation de clé en masse ou une tâche de rotation de clé unique pour chiffrer les données existantes à l'aide de la nouvelle clé de chiffrement.

   Si vous n'exécutez pas de tâche de rotation de clé en masse ou de clé unique, les données existantes restent chiffrées avec l'ancienne clé jusqu'à ce que vous accédiez à nouveau aux données.

Configurer des propriétés supplémentaires dans le fichier de propriétés de Chiffrement Edge

Après avoir installé le serveur proxy dans votre réseau et configuré votre magasin de Chiffrement Edge clés et vos clés, configurez les propriétés supplémentaires Chiffrement Edge .

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Ouvrez le fichier <répertoire d'installation>/conf/edgeencryption.properties et configurez les propriétés de serveur proxy suivantes Chiffrement Edge :
   - Propriétés (instance) de la cible
   - Propriétés du compte utilisateur
   - Propriétés de proxy
   - Si vous utilisez des types de chiffrement ou des modèles de chiffrement préservant l'ordre, configurez les propriétés de la base de données proxy
   - Texte clair et propriétés IV statiques
2. Enregistrez et fermez le fichier.

Configurer un proxy web

Si votre réseau utilise un proxy Web, vous pouvez configurer le Chiffrement Edge proxy pour qu'il utilise le proxy Web.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Si votre réseau n'utilise pas de proxy Web, laissez les propriétés du proxy Web dans le fichier de configuration commentées.

Le Chiffrement Edge serveur proxy prend en charge la connexion HTTP et l'authentification de base avec le proxy Web.

Procédure

1. Accédez au répertoire <installation>/conf/ .
2. Ouvrez le fichier edgeencryption.properties .
3. Configurez les propriétés du proxy web.
4. Enregistrez et fermez le fichier edgeencryption.properties .
5. Si le proxy web utilise un certificat de serveur spécifique au client, ajoutez ce certificat à la JVM utilisée par le Chiffrement Edge serveur proxy pour établir la confiance entre le proxy web et le Chiffrement Edge serveur proxy.
   a. Utilisez la commande `cd` pour accéder à <répertoire personnel Java>/jre/lib/security/cacerts
   b. Exécutez la commande : `keytool -keystore cacerts -importcert -alias <chooseAlias> -file <certificateFile>`

Définir la limite de mémoire initiale et la limite supérieure de mémoire du serveur proxy

Définissez la limite de mémoire initiale et la limite supérieure de mémoire pour spécifier la quantité de mémoire que le serveur proxy peut consommer. Définissez ces limites pour éviter les problèmes de performances de votre Chiffrement Edge implémentation.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

À titre indicatif, définissez la limite de mémoire initiale et la limite supérieure de mémoire sur la même valeur. Sur n'importe quel ordinateur, allouez 2 Go de mémoire physique au système d'exploitation. Allouez ensuite le reste de la mémoire physique au tas à l'aide des propriétés de limite de mémoire initiale et de limite de mémoire de limite supérieure. Par exemple, sur un ordinateur doté de 8 Go de mémoire, allouez 2 Go au système d'exploitation et allouez les 6 Go restants (6 144 m) à la mémoire initiale et à la mémoire de limite supérieure.

Important :
Si votre Chiffrement Edge serveur proxy est en cours d'exécution, vous devez arrêter et redémarrer le serveur proxy après avoir mis à jour ces propriétés.

Procédure

1. Dans le répertoire de votre serveur proxy, ouvrez <install dir>/conf/wrapper.conf.
2. Pour définir la limite de mémoire initiale, ajoutez la ligne suivante à la fin du fichier :

```
wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m
```

Définissez <number> sur le prochain <number> disponible dans la séquence des propriétés wrapper.java.additional.<number> définies dans le fichier wrapper.conf .

Example

Par exemple, vous disposez de la liste suivante des propriétés wrapper.java.additional.<number> :

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Le <nombre> maximal dans la liste ci-dessus est **de 2**. Lorsque vous ajoutez la ligne wrapper.java.additional.<number>=-Xms<min_memory_in_MB>m , définissez <number> sur **3**, le numéro disponible suivant.

Important :
Ne laissez pas d'espaces dans la séquence de numérotation.

Définissez <min_memory_in_MB> sur le nombre de mégaoctets de mémoire restant après avoir alloué 2 Go de mémoire au système d'exploitation.

3. Définissez la limite supérieure de mémoire de limite.
Étant donné qu'aucune limite supérieure de mémoire n'est définie dans le système de base, le serveur proxy peut utiliser toute la mémoire disponible. Si d'autres services sont en cours d'exécution sur le serveur, vous pouvez définir la limite supérieure de mémoire de limite.

Ajoutez la ligne suivante à la fin du fichier :

wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m

Définissez <number> sur le prochain <number> disponible dans la séquence des propriétés wrapper.java.additional.<number> définies dans le fichier wrapper.conf .

Example

Par exemple, vous disposez de la liste suivante des propriétés wrapper.java.additional.<number> :

```
wrapper.java.additional.1=
wrapper.java.additional.2=
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le <nombre> maximal dans la liste ci-dessus est **de 2**. Lorsque vous ajoutez la ligne wrapper.java.additional.<number>=-Xmx<max_memory_in_MB>m , définissez <number> sur **3**, le nombre disponible suivant.

Remarque :
Ne laissez pas d'espaces dans la séquence de numérotation.

Définissez <max_memory_in_MB> sur le nombre de mégaoctets de mémoire restant après avoir alloué 2 Go de mémoire au système d'exploitation.

4. Enregistrez et fermez le fichier.

Example: Exemple : définition des limites de mémoire initiales et supérieures de la limite de mémoire du serveur proxy

```
wrapper.java.additional.1 = -Djava.io.tmpdir=../tmp
wrapper.java.additional.2 = -Dcloudedge.home.dist=..
# must ensure UTF8 encoding when running on Windows
wrapper.java.additional.3 = -Dfile.encoding=UTF8
# additional properties for heap settings
wrapper.java.additional.4 = -Xms6144m
wrapper.java.additional.5 = -Xmx6144m
```

Que faire ensuite

Démarrer le proxy Chiffrement Edge.

Démarrer le proxy Chiffrement Edge

Une fois qu'un Chiffrement Edge proxy est installé et configuré, vous pouvez le démarrer à partir de la ligne de commande.

Avant de commencer

Rôle requis : administrateur

Avant de démarrer le proxy de chiffrement, vérifiez les points suivants :

- Le Chiffrement Edge module d'extension est activé dans l'instance.
- Le fichier edgeencryption.properties sur cet ordinateur a été configuré.
- Si vous utilisez un type de chiffrement ou des modèles de chiffrement préservant l'ordre, la base de données proxy est en cours d'exécution.

Remarque :
La première fois que vous configurez le fichier edgeencryption.properties ou que vous modifiez les propriétés, vous ne souhaitez peut-être pas définir la propriété de chiffrement du mot de passe. Après avoir vérifié que tout fonctionne, vous pouvez définir la propriété de chiffrement du mot de passe, arrêter le proxy, puis le redémarrer.

Procédure

1. Exécutez le serveur proxy.

Option	Description
Sur un ordinateur Linux	**a.** CD à ServerName_port **b.** Exécuter ./startup.sh

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Sur un ordinateur Windows	En tant qu'administrateur, procédez comme suit à partir de la ligne de commande : **a.** CD vers ServerName_port/bin **b.** Exécuter edgeencryption.bat démarrage

2. Vérifiez le journal sur le serveur proxy pour vérifier que le proxy est en cours d'exécution.

Brouiller les mots de passe dans le fichier de propriétés

Grisez les mots de passe dans le fichier edgeencryption.properties pour pouvoir partager le fichier de propriétés sans révéler les mots de passe en texte clair.

Avant de commencer
Rôle requis : administrateur

Assurez-vous que le Chiffrement Edge serveur proxy est configuré et exécuté avec succès avant de définir cette propriété. Avant de définir cette propriété, Arrêter le proxy Chiffrement Edge.

Pourquoi et quand exécuter cette tâche
La définition de cette propriété peut rendre difficile le débogage des problèmes de connexion et d'accès lors du démarrage initial. Définissez cette propriété uniquement dans les environnements de production une fois que le proxy a été configuré et testé avec succès.

Procédure

1. Accédez au répertoire <installation>/conf/ .
2. Dans le répertoire conf , créez un fichier texte contenant une chaîne ou une phrase complexe qui peut être utilisée comme phrase de passe que le proxy utilise pour brouiller les mots de passe dans le fichier edgeencryption.properties .
   Cette phrase de passe doit être une phrase aléatoire et complexe qui n'est pas liée aux mots de passe eux-mêmes.
3. Ouvrez le fichier edgeencryption.properties .
4. Définissez la propriété de chiffrement du mot de passe.
5. Enregistrez et fermez le fichier edgeencryption.properties .

Que faire ensuite
Après avoir défini cette propriété, vous pouvez Démarrer le proxy Chiffrement Edge.

Ajouter manuellement un proxy supplémentaire

Une fois que le premier Chiffrement Edge proxy est correctement configuré et testé, vous pouvez configurer des proxys supplémentaires sur un ordinateur Linux ou Windows. Il n'est pas recommandé d'installer plusieurs proxys sur la même machine.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Ajoutez des serveurs proxy supplémentaires sur des machines supplémentaires pour garantir un environnement optimal. Reportez-vous à la rubrique Dimensionnement de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

votre environnement Edge Encryption pour déterminer le nombre de proxys supplémentaires nécessaires.

Remarque :
Assurez-vous que tous les proxys ont les mêmes clés de chiffrement et la même paire de clés RSA utilisées pour signer numériquement la configuration de chiffrement et les règles de chiffrement. Si une base de données proxy a été configurée dans le cadre de l'installation, tous les proxys doivent utiliser la même base de données proxy.

Procédure

1. Installez le proxy à l'aide de la commande appropriée.
   Pour plus d'informations, consultez Installer le serveur proxy (programme d'installation Chiffrement Edge interactif).
2. Copiez toutes les clés de chiffrement et le fichier `edgeencryption.properties` du premier proxy vers le nouveau proxy.
   Les clés de chiffrement peuvent se trouver dans le magasin de clés proxy, dans le répertoire `/keys` ou dans un magasin de clés SafeNet KeySecure.
3. Ouvrez le fichier `edgeencryption.properties` sur le nouveau proxy.
4. Modifiez les propriétés suivantes :

Propriété	Description
`edgeencryption.proxy.name`	Nom unique du serveur proxy
`edgeencryption.proxy.host`	Le nom du serveur, l'adresse IP ou le nom de domaine complet de l'ordinateur sur lequel fonctionne le proxy.
`edgeencryption.proxy.http.port`	Port sur le proxy pour la communication HTTP. Doit être unique dans tous les processus de l'ordinateur.
`edgeencryption.proxy.https.port`	Port sur le proxy de la communication HTTPS. Doit être unique dans tous les processus de l'ordinateur.

5. Si vous installez le serveur proxy sur un ordinateur Windows, vous devez modifier le nom du service. en ouvrant le fichier `conf/wrapper.conf` sur le nouveau proxy et en ajoutant les propriétés listées dans le tableau suivant.

   Remarque :
   Vous devez effectuer cette étape avant de lancer le serveur proxy.

Propriété	Description
`wrapper.ntservice.name`	Nom unique du Chiffrement Edge service proxy.
`wrapper.ntservice.displayname`	Chiffrement Edge Nom d'affichage du service proxy.
`wrapper.ntservice.description` (Facultatif)	Description du serveur proxy.

6. Enregistrez et fermez le fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Lancez le proxy à l'aide de la commande appropriée.
   Pour plus d'informations, consultez Démarrer le proxy Chiffrement Edge.

Authentifier un Chiffrement Edge serveur proxy

Spécifiez qu'un serveur proxy est une source approuvée afin de Chiffrement Edge pouvoir traiter les demandes provenant de ce serveur proxy.

Avant de commencer

Si un serveur proxy n'est pas authentifié, le journal de la console comprend le message suivant :

```
WARN This Edge Encryption proxy has not yet been authenticated by the instance.
Please navigate to the matching Proxy record on your ServiceNow instance and authenticate it.
```

Si vous tentez d'accéder au proxy, vous recevez le message suivant : Ce site est inaccessible.

Pour maintenir le proxy dans un état opérationnel pendant le processus de mise à niveau, l'authentification n'est requise qu'une fois la mise à jour du proxy réussie.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Proxys**.
2. Sélectionnez le proxy et cliquez sur **Authentifier**.

Résultats

Le proxy passe de **Non authentifié** à **En attente** puis **Authentifié.** L'état passe de **Non authentifié** à **En attente** lorsque vous démarrez l'authentification. Lorsque l'authentification est terminée, l'état passe de **En attente** à **Authentifié,** et vous pouvez accéder au proxy et Chiffrement Edge accepter les demandes du proxy.

Remarque :
Si vous arrêtez et redémarrez le proxy, celui-ci reste **authentifié** et redémarre avec succès.

Arrêter le proxy Chiffrement Edge

Vous pouvez arrêter un Chiffrement Edge proxy à partir de la ligne de commande.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Arrêtez le serveur proxy.

Option	Description
Sur un ordinateur Linux	Exécuter `./shutdown.sh`
Sur un ordinateur Windows	Exécuter `edgeencryption.bat arrêt` Pour supprimer le service Windows, exécutez `edgeencryption.bat supprimer`

2. Vérifiez le journal sur le serveur proxy pour vérifier que le proxy s'est arrêté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Désinstaller le proxy Chiffrement Edge sur Linux

Vous pouvez désinstaller le Chiffrement Edge proxy. Si vous mettez à niveau le proxy, il n'est pas nécessaire d'arrêter et de désinstaller la version actuelle.

Avant de commencer

Rôle requis : administrateur

Vous devez avoir accès à l'ordinateur qui exécute le Chiffrement Edge proxy.

Pourquoi et quand exécuter cette tâche

Avant d'arrêter le Chiffrement Edge proxy, assurez-vous qu'aucun utilisateur n'est connecté à l'instance qui utilise le proxy.

Le proxy de chiffrement s'exécutant sous Linux fonctionne comme un processus unique. Vous pouvez terminer ce processus pour prendre en charge des tâches telles que le redéploiement du proxy de chiffrement vers un autre ordinateur hôte, la mise à jour de la version du proxy, la mise à jour de la version Java ou la modification du nom unique du proxy de chiffrement lors du déploiement du proxy de chiffrement sur plusieurs serveurs proxy.

Procédure

1. Vous pouvez enregistrer le fichier edgeencryption.properties avant de supprimer le répertoire de distribution.
2. Exécutez le script `shell shutdown.sh` .
3. Vérifiez le journal sur le serveur proxy pour vérifier que le serveur proxy est arrêté.
4. Supprimez les fichiers dans le dossier de distribution.

Désinstaller le proxy Chiffrement Edge sous Windows

Vous pouvez désinstaller le Chiffrement Edge proxy. Si vous mettez à niveau le proxy, il n'est pas nécessaire d'arrêter et de désinstaller la version actuelle.

Avant de commencer

Rôle requis : administrateur

Vous devez avoir accès à l'ordinateur qui exécute le Chiffrement Edge proxy.

Avant d'arrêter le Chiffrement Edge proxy, assurez-vous qu'aucun utilisateur n'est connecté à l'instance qui utilise le proxy.

Procédure

1. Vous pouvez enregistrer le fichier edgeencryption.properties avant de supprimer le répertoire de distribution.
2. Exécuter `edgeencryption.bat arrêt`
3. Exécuter `edgeencryption.bat supprimer`
4. Vérifiez le journal sur le serveur proxy pour vérifier que le serveur proxy est arrêté.
5. Supprimez les fichiers dans le dossier de distribution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer l'authentification unique (SSO) de plusieurs fournisseurs avec Chiffrement Edge

Configurez la SSO de plusieurs fournisseurs pour permettre la connexion via l'URL du serveur proxy ou l'URL Chiffrement Edge de l'instance. Si vous implémentez l'authentification unique (SSO) de plusieurs fournisseurs avec Chiffrement Edge l'authentification unique activée, certains utilisateurs devront peut-être se connecter à votre instance via le Chiffrement Edge serveur proxy, tandis que d'autres non.

Avant de commencer

- Activez le module d'extension Intégration - Programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).
- Activez le module d'extension Chiffrement Edge (com.glide.edgeencryption) et assurez-vous qu'un ou plusieurs serveurs proxy sont configurés sur votre réseau.
- Déterminez l'URL du Chiffrement Edge serveur proxy auquel les utilisateurs se connecteront à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs. Pour déterminer l'URL d'un Chiffrement Edge serveur proxy, reportez-vous à la section Installation de Chiffrement Edge.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

L'utilisateur qui se connecte doit utiliser l'URL appropriée pour se connecter, soit en utilisant le proxy Edge, soit en utilisant non le proxy Edge.

- Si vous acheminez tous les utilisateurs via le Chiffrement Edge serveur proxy, configurez votre enregistrement d'identification de fournisseur et définissez l'URL du serveur proxy dans les champs **Page d'accueil de ServiceNow**, **ID d'entité/Émetteur** et **URI d'audience** .
- Pour acheminer certains utilisateurs via le serveur proxy et d'autres utilisateurs vers l'instance, créez deux enregistrements d'identification du fournisseur. Les deux enregistrements utilisent la même valeur dans le champ **URL du fournisseur d'identité** . Toutefois, l'un des enregistrements passe par le serveur proxy, tandis que l'autre est acheminé vers l'instance.
  - Connexion via le nom de l'instance : https://<nom d'instance>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id de l'enregistrement IdP pour le proxy non Edge
  - Se connecter via le proxy Edge : https://<nom d'hôte Edge> :<port>/login_with_sso.do ?glide_sso_id=<sys_id de l'enregistrement IdP pour le proxy Edge

Procédure

1. Activer la duplication des URL des fournisseurs d'identité dans les enregistrements des fournisseurs d'identité.
   Une contrainte unique empêche la duplication de l'URL du fournisseur d'identité dans deux enregistrements de fournisseur d'identité différents. Vous pouvez activer la duplication de l'URL du fournisseur d'identité dans plusieurs enregistrements IdP en définissant un champ sur faux.
   a. Accédez à la **Définition du système** > **Dictionnaire**.
   b. Ouvrez l'enregistrement de définition pour le champ **IdP** de dans la table Fournisseurs d'identité [saml2_update1_properties].
   c. Configurez le formulaire pour ajouter le champ **Unique** .
   d. Assurez-vous que la valeur du champ **Unique** est définie sur **faux**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
3. Créez deux enregistrements de fournisseur d'identité pour le même fournisseur d'identité : l'un à l'aide de l'URL d'instance et l'autre à l'aide de l'URL du Chiffrement Edge serveur proxy.
   Pour créer un enregistrement de fournisseur d'identité, consultez Créer un fournisseur d'identité externe.

   a. Pour l'URL du Chiffrement Edge serveur proxy, remplissez le formulaire à l'aide de ces valeurs.

Champ	Valeur
URL du fournisseur d'identité	Importé à partir des métadonnées IdP.
ServiceNow Page d'accueil	URL de la page d'accueil de votre serveur proxy. Par exemple : https://<nom d'hôte proxy> :<port>/navpage.do
ID d'entité/Émetteur	https://<nom d'hôte proxy> :<port>
URI de l'audience	https://<nom d'hôte proxy> :<port>

   b. Cliquez sur **Envoyer**.

   c. Pour l'URL d'instance, remplissez le formulaire à l'aide de ces valeurs.

Champ	Valeur
URL du fournisseur d'identité	Importé à partir des métadonnées IdP.
ServiceNow Page d'accueil	https://<instance>.service-now.com/navpage.do
ID d'entité/Émetteur	https://<instance>.service-now.com/navpage.do
URI de l'audience	https://<instance>.service-now.com/navpage.do

   d. Cliquez sur **Envoyer**.

4. **Facultatif :** Si vous utilisez plusieurs fournisseurs d'identité, modifiez la sortie d'installation de l'authentification unique (SSO) à fournisseurs multiples.

   a. Accédez à la **Définition du système** > **Sorties d'installation**.
   Le système affiche la liste actuelle des sorties d'installation.

   b. Ouvrez la sortie d'installation **de l'authentification unique (SSO) à fournisseurs multiples** .

   c. Recherchez l'instruction suivante dans le champ **Script** .

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
   var idpRecord = this.getIdPRecord(request);
   if (idpRecord) {
      SSO_Helper.debug("IdP found based on SAML response: " +
idpRecord.getUniqueValue());
      return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    }
}
```

d. Remplacez l'instruction par le code suivant.

```
var samlResponseTxt = request.getParameter("SAMLResponse");
if (!GlideSession.get().isLoggedIn() && GlideStringUtil.notNil(samlResponseTxt)) {
  /* // You have two profiles that use the same IdP entity id it cannot use
  // the IdP issuer / entity id from the response otherwise it may result in the
  // wrong IdP profile. IdP initiated login will not work
  var idpRecord = this.getIdPRecord(request);
  if (idpRecord) {
    SSO_Helper.debug("IdP found based on SAML response: " +
idpRecord.getUniqueValue());
    return new SSO_Helper(idpRecord.getUniqueValue(), false, null, true);
    }*/
  return new SSO_Helper(null, true);
  }
```

Remarque :
La connexion initiée par l'IdP ne fonctionne pas dans cette configuration.

e. Cliquez sur **Mettre à jour**.

5. **Facultatif :** Si vous utilisez plusieurs sociétés, configurez les utilisateurs pour la SSO de plusieurs fournisseurs et mettez à jour les sys_id de l'enregistrement du fournisseur d'identité en fonction de l'utilisateur.

   (Optional) Pour plus d'informations, consultez Configurer les utilisateurs pour l'authentification unique (SSO) de plusieurs fournisseurs.

   - Pour configurer un utilisateur pour qu'il se connecte via le Chiffrement Edge serveur proxy, utilisez la sys_id de l'enregistrement du fournisseur d'identité qui utilise l'URL du Chiffrement Edge serveur proxy.
   - Pour configurer la connexion d'un utilisateur à l'instance, utilisez la sys_id de l'enregistrement du fournisseur d'identité qui utilise l'URL de l'instance.

URL de connexion

URL	Destination de connexion
https://<nom d'hôte proxy> :<port>/ login_with_sso.do ?glide_sso_id=<sys_id de l'enregistrement IdP pour l'URL du serveur proxy>	Se connecte via le serveur proxy.
https://<nom d'instance>.service-now.com/ login_with_sso.do?glide_sso_id=<sys_id de l'enregistrement IdP pour l'URL d'instance>	Se connecte via l'instance.

Propriétés du serveur proxy Chiffrement Edge

Le fichier de configuration edgeencryption.properties situé dans le dossier <installation directory>/conf/ contient les propriétés utilisées pour configurer votre environnement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez redémarrer le serveur proxy après avoir apporté des modifications aux propriétés du serveur proxy.

Texte clair et propriétés IV statiques

Chiffrement Edge.Client.Affecté.Connu.Texte clair	Effacer le texte pour permettre à l'instance de vérifier que tous les proxys utilisent les mêmes clés. Au démarrage, le proxy chiffre le texte en clair et envoie le texte chiffré à l'instance. L'instance ne connaît pas le texte clair et les clés ne lui sont pas envoyées. Cette propriété doit être la même pour tous les proxys.
edgeencryption.encrypter.static.iv	Static IV (vecteur d'initialisation) utilisé dans le chiffrement préservant l'égalité et la préservation de l'ordre. Cette propriété doit être la même pour tous les proxys et doit être exactement de 16 octets (16 caractères ASCII).

Propriétés de Signature numérique

edgeencryption.proxy.signature.keystore.path	Chemin d'accès et nom de fichier Java KeyStore.
edgeencryption.proxy.signature.keystore.password	Mot de passe. Le mot de passe par défaut est <changeme>. Changez le mot de passe après avoir installé le Java KeyStore.
edgeencryption.proxy.signature.keystore.keyalias	Alias de clé indiqué comme argument -alias lors de la génération de la paire de clés RSA.

Propriété du magasin de fichiers

edgeencryption.keyfile.directory	Le répertoire spécifie l'emplacement de stockage des fichiers clés. Si vous utilisez le magasin de clés Java KeyStore ou un magasin de clés SafeNet KeySecure, laissez cette propriété en commentaire. Exemple : `edgeencryption.keyfile.directory=keys` Si vous utilisez des clés de technologie non liées, retirez le commentaire de cette propriété et définissez la valeur sur le répertoire des clés.

Propriétés de configuration générales

edgeencryption.config.poll.interval	Intervalle d'interrogation en secondes. Le paramètre par défaut signifie qu'il faut 5 secondes au proxy pour apprendre les modifications de la configuration de chiffrement. Plus les valeurs sont grandes, plus l'instance met de temps à détecter un proxy hors ligne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	⚠ Avertissement : Ne changez pas cette propriété. La modification du paramètre par défaut de l'intervalle d'interrogation du proxy peut entraîner des retards de détection lors de la mise en ligne d'un proxy.
edgeencryption.rules.dir	Dossier dans lequel les règles de chiffrement sont stockées sur le proxy.
edgeencryption.encryption.order_preserving.cache.enable	Le paramètre détermine si la mise en cache est utilisée pour prendre en charge les types de chiffrement préservant l'ordre.
edgeencryption.encryption.order_preserving.cache.size	Taille maximale du cache, en octets.
edgeencryption.jobs.concurrency	Nombre maximal de tâches de chiffrement en masse qui peuvent s'exécuter simultanément sur ce proxy.
edgeencryption.jobs.requests_per_second	Nombre de demandes de tâches HTTP par seconde pouvant être envoyées à l'instance par ce proxy.
edgeencryption.attachments.request.timeout.seconds	Délai de la demande de chargement de pièce jointe en secondes.
edgeencryption.request.buffer.size	Taille d'une demande de chiffrement. Si une demande de chiffrement est supérieure à cette taille, l'excédent est enregistré sur le disque. **⚠ Avertissement :** Ne changez pas cette propriété.
edgeencryption.httpclient.request.buffer.size	Taille de la demande client. Si la demande client est supérieure à cette taille, l'excédent est enregistré sur le disque. **⚠ Avertissement :** Ne changez pas cette propriété.
edgeencryption.httpclient.header.size	Taille de l'en-tête de demande/réponse. • Valeur minimale : 8K • Valeur maximale : 32K **⚠ Avertissement :** Ne changez pas cette propriété.
edgeencryption.proxy.idle.timeout	Délai, en secondes, après lequel une transaction expire. Valeur par défaut : 300 (secondes)
edgeencryption.proxy.keepalive.interval	Durée, en secondes, entre les pings émis par le proxy vers l'instance. Des pings sont émis périodiquement pour vérifier la connectivité entre le proxy et l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

	• Valeur par défaut : 10 (secondes) • Valeur minimale : 5 (secondes)
edgeencryption.register.retry.count	Nombre maximal de fois que le proxy envoie un ping à l'instance pour essayer de s'inscrire. Valeur par défaut : 0 (aucune limite)
edgeencryption.tokenization.exclusion.list	Les schémas de chiffrement ne peuvent pas tokeniser les chaînes trouvées dans ces champs.

Propriétés du KeyStore Java

edgeencryption.keystore.path	Chemin d'accès au KeyStore Java. Si vous utilisez un magasin de fichiers ou un magasin de clés SafeNet KeySecure, laissez cette propriété en commentaire. Exemple : `edgeencryption.keystore.path = keystore/keystore.jceks`
edgeencryption.keystore.password	Mot de passe utilisé par le proxy pour se connecter au KeyStore Java. Si vous utilisez un magasin de fichiers ou un magasin de clés SafeNet KeySecure, laissez cette propriété en commentaire.

Propriétés de journalisation

Les propriétés de journalisation se trouvent dans le fichier lo4gj2.properties qui se trouve dans le répertoire <installation>/conf/ . Ces propriétés ne sont modifiées qu'à des fins de dépannage ou si l'assistance ServiceNow vous le demande. Pour plus d'informations, reportez-vous à la rubrique Comment augmenter la journalisation de débogage pour le proxy Chiffrement Edge .

Propriétés du keystore d'appareil NAE

edgeencryption.nae.retries	Nombre de nouvelles tentatives à effectuer.
edgeencryption.nae.enabled	Le paramètre indique si un périphérique NAE est disponible.
edgeencryption.nae.server	Nom du serveur NAE.
edgeencryption.nae.port	Port utilisé par le serveur NAE.
edgeencryption.nae.protocol	Protocole utilisé par le serveur NAE.
edgeencryption.nae.keystore.path	Chemin d'accès au magasin de clés sur le serveur NAE.
edgeencryption.nae.keystore.password	Mot de passe de magasin de clés NAE.
edgeencryption.nae.username	Nom d'utilisateur à utiliser pour s'authentifier avec l'appareil NAE.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

edgeencryption.nae.password	Mot de passe à utiliser pour s'authentifier avec l'appareil NAE.
edgeencryption.nae.client.certificate	Certificat situé dans le magasin de clés sur le serveur NAE. Définissez cette propriété pour qu'elle s'authentifie à l'aide d'un certificat au lieu d'un nom d'utilisateur et d'un mot de passe.

Propriété du mot de passe

edgeencryption.encrypter.properties.password	Nom du fichier dans le dossier `conf` qui contient une chaîne utilisée dans un processus sécurisé pour brouiller les mots de passe dans le fichier `edgeencryption.properties` . **Remarque :** Nom du fichier dans le dossier `conf` qui contient une chaîne utilisée dans un processus sécurisé pour brouiller les mots de passe dans le fichier `edgeencryption.properties` .

Propriétés de proxy

edgeencryption.proxy.host	Nom du serveur, adresse IP ou nom de domaine complet de l'ordinateur exécutant le proxy. Avec le port, cette propriété définit l'URL utilisée par le client pour accéder au serveur proxy.
edgeencryption.proxy.name	Nom du proxy. Doit être unique pour chaque proxy.
edgeencryption.proxy.http.port	Port sur le proxy pour la communication HTTP.
edgeencryption.proxy.https.port	Port sur le proxy de la communication HTTPS.

Propriété verrouillée de configuration de proxy

edgeencryption.proxy.locked	Si la valeur est vrai, le proxy n'accepte pas les changements de configuration ou de règle de chiffrement de l'instance. Définissez cette propriété sur l'instance de production une fois que toutes les configurations et règles de chiffrement sont finalisées.

Propriétés de la base de données proxy

edgeencryption.db.url	Emplacement de la base de données proxy. Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance.
edgeencryption.db.utilisateur	Nom d'utilisateur permettant d'accéder à la base de données proxy. Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

edgeencryption.db.mot de passe	Mot de passe permettant d'accéder à la base de données proxy. Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance.
edgeencryption.db.name	Nom de la base de données proxy. Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance. La valeur par défaut de cette propriété est `edgeencryption`.
edgeencryption.db.bootstrap.file	Fichier d'amorce pour la base de données proxy. Le fichier est relatif au répertoire `sql/` . Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance. **⚠ Avertissement :** Dans des circonstances normales, ne modifiez pas ce paramètre.

Propriétés de performances du serveur proxy

Les propriétés de performances du serveur proxy ne sont pas présentes dans le fichier de configuration par défaut. Pour modifier les valeurs par défaut, vous devez ajouter les propriétés et redémarrer le serveur proxy. Pour plus d'informations, consultez Diagnostics et performances d'Edge Encryption.

edgeencryption.stat.collection.enabled	Active la collecte des statistiques utilisées par le Chiffrement Edge tableau de bord des performances du serveur proxy. Valeur par défaut : true Ajoutez cette propriété et définissez la valeur sur faux pour désactiver la collecte des statistiques utilisées par le Chiffrement Edge tableau de bord des performances du serveur proxy.
edgeencryption.stat.collection.interval	Intervalle en secondes pendant lequel le Chiffrement Edge serveur proxy collecte des statistiques. La valeur ne peut pas être inférieure à 30 secondes. Valeur par défaut : 30 (secondes)

Propriétés du certificat SSL

Redémarrez votre proxy si vous modifiez la valeur d'une propriété de certificat SSL. Le système utilise la paire de clés HTTPS au démarrage pour établir la connexion du serveur proxy et déterminer comment le proxy répond aux demandes du client.

edgeencryption.proxy.https.cert.alias	Alias du certificat fourni par le serveur proxy aux clients qui se connectent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

edgeencryption.proxy.https.keystore.path	Chemin d’accès au magasin de clés qui contient le certificat HTTPS.
edgeencryption.proxy.https.keystore.password	Mot de passe du magasin de clés qui contient le certificat HTTPS.

Propriétés (instance) de la cible

edgeencryption.target.host	Nom d’hôte de l’instance. Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance. Cette propriété est définie lors de l’installation du proxy. Par exemple, instancename.servicenow.com
edgeencryption.target.port	Port d’instance. Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance. Cette propriété est définie lors de l’installation du proxy.
edgeencryption.target.protocol	Protocole d’instance. Elle doit être identique pour tous les proxies de chiffrement qui se connectent à la même instance. Cette propriété est définie lors de l’installation du proxy. Les options incluent : • http • https

Non lié Propriétés du fournisseur de technologie

edgeencryption.ekm.provider.classname	Nom de classe interne pour l’implémentation. **⚠ Avertissement :** Ne changez pas cette propriété.
edgeencryption.thirdparty.vendor.library.path	Chemin d’accès au fichier JAR de l’API Unbound sur l’ordinateur client Unbound.
edgeencryption.ekm.provider.rsa.wrapping.key.alias	Alias de clé d’encapsulation dans l’implémentation d’Unbound Technology. Elle doit être la même pour tous les proxys.

Propriétés du compte utilisateur

edgeencryption.target.username	Nom d’utilisateur utilisé par le proxy pour se connecter à l’instance. L’utilisateur doit avoir le rôle edge_encryption. Voir Configurer un compte d’utilisateur Chiffrement Edge.
edgeencryption.cible.mot de passe	Mot de passe utilisé par le proxy pour se connecter à l’instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de proxy web

edgeencryption.webproxy.host	Nom ou adresse IP du proxy Web.
edgeencryption.webproxy.port	Port sur le proxy web.
edgeencryption.webproxy.user	Nom d'utilisateur utilisé pour se connecter au proxy web. Si votre proxy web n'utilise pas l'authentification, laissez cette propriété en commentaire.
edgeencryption.webproxy.password	Mot de passe à utiliser pour se connecter au proxy web. Si votre proxy web n'utilise pas l'authentification, laissez cette propriété en commentaire.

Propriétés de chiffrement de proxy déconseillées

edgeencryption.encrypter.default.key128

Spécifie le nom de la clé AES 128 actuelle. Une clé AES 128 doit être disponible même si elle n'est pas utilisée. Elle doit être la même pour tous les proxys.

Effectuez la maintenance de ces clés sur l'instance.

edgeencryption.encrypter.default.key256

Spécifie le nom de la clé AES 256 actuelle. Elle doit être la même pour tous les proxys.

Effectuez la maintenance de ces clés sur l'instance.

edgeencryption.encrypter.key

Spécifie le nom de clé pour chaque clé et est utilisé pour spécifier les clés par défaut. Il s'agit de l'alias de clé intégré aux métadonnées qui est inclus avec chaque élément chiffré et qui, par conséquent, est stocké sur l'instance. Le nom de la clé doit être en minuscules.

edgeencryption.encrypter.type

Spécifie le type de système de magasin de clés de chiffrement.

edgeencryption.encrypter.file

Spécifie le chemin d'accès et le nom de fichier du fichier texte associé à la clé.

edgeencryption.encrypter.password

Spécifie le mot de passe pour accéder au magasin de clés.

Intégration de CyberArk au serveur proxy Edge

Utilisez CyberArk pour stocker les mots de passe dans un coffre-fort numérique centralisé et sécurisé afin de sécuriser les mots de passe qui étaient auparavant stockés en texte clair et sécurisés par l'accès aux fichiers, ou qui étaient auparavant chiffrés via un deuxième fichier.

CyberArk AIM (Application Identity Management) empêche tout accès non autorisé en éliminant les mots de passe codés en dur et visibles. AIM stocke les mots de passe dans un coffre-fort numérique sur un serveur renforcé indépendant, où les mots de passe sont représentés comme des justificatifs d'identité numériques. Les clients AIM (les serveurs proxy Edge) utilisent les informations d'identification numériques de CyberArk et accèdent au serveur indépendant pour récupérer les mots de passe sécurisés. Aucun mot de passe n'est stocké sur les serveurs proxy Edge ou dans l'instance.

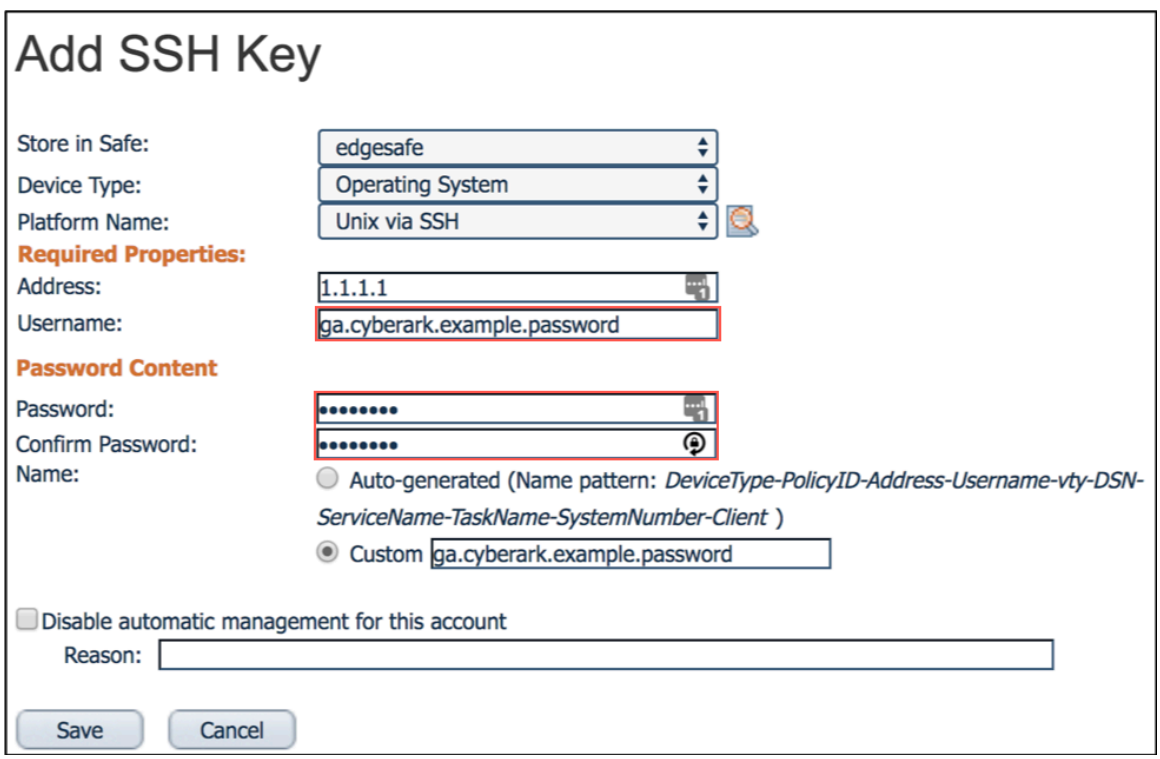
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification du coffre-fort numérique CyberArk

Vous devez acheter et configurer CyberArk avant de pouvoir configurer l'intégration de CyberArk au serveur proxy Edge.

Pour ajouter des informations d'identification à CyberArk (qui sont lues par le proxy Edge), définissez le nom de **la plateforme** des informations d'identification sur **Unix via SSH** et **assurez-vous** de créer un **nom** d'informations d'identification **personnalisé** ou de noter le **nom** des informations d'identification généré automatiquement. Lorsque vous configurez le proxy Edge pour utiliser ces informations d'identification, le serveur proxy fait correspondre ce **nom** d'informations d'identification au paramètre du proxy.



Chaque entrée d'informations d'identification contient un **mot de passe** en cours de sécurisation, ainsi qu'un **nom** d'informations d'identification utilisé par une application pour accéder à ce mot de passe.

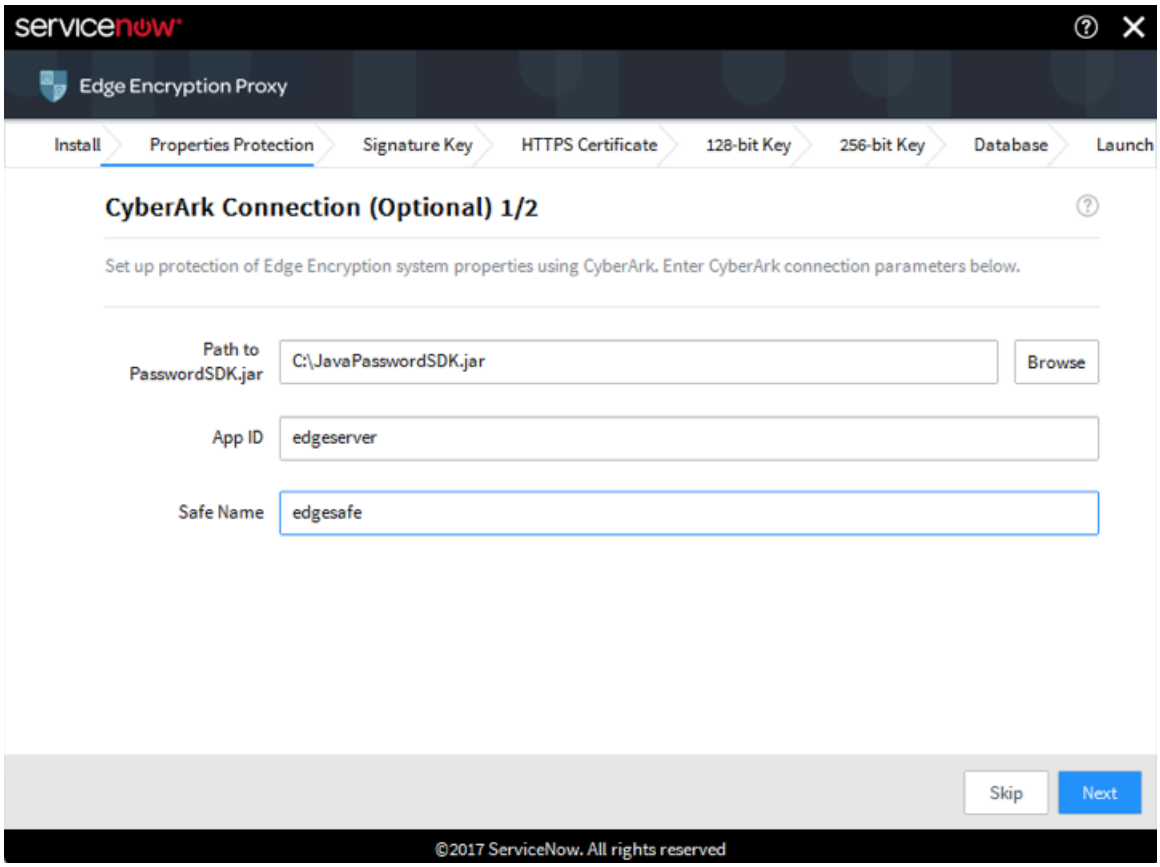
Remarque :
Les informations d'identification CyberArk ne sont pas des clés de chiffrement.

Ajout de CyberArk lors de l'installation d'un proxy Edge

Le programme d'installation du proxy inclut une nouvelle page de configuration pour une intégration CyberArk. Cette page est facultative si vous ne souhaitez pas inclure CyberArk lors de l'installation de votre proxy avec le programme d'installation du proxy. Vous pouvez également installer et configurer manuellement l'intégration de CyberArk dans le fichier de configuration.

Traduction automatique

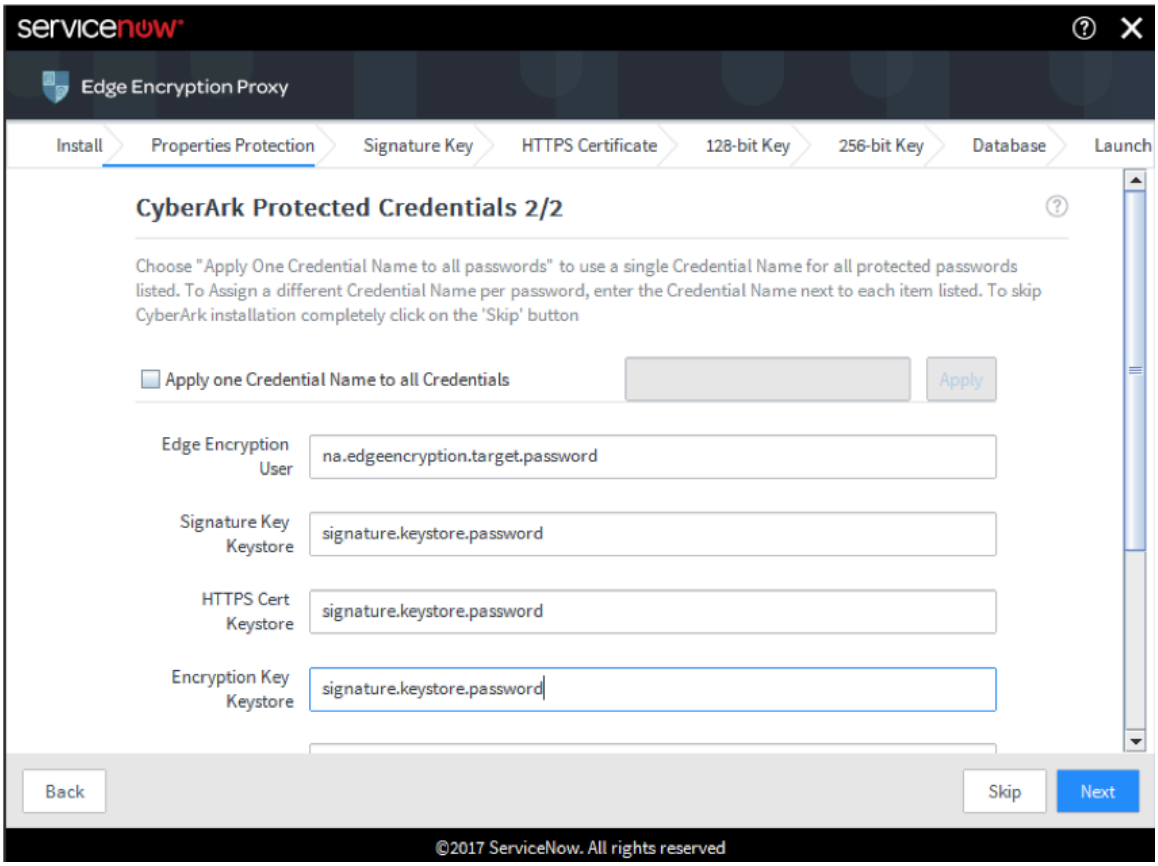
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Le programme d'installation proxy comprend également une nouvelle page pour les informations d'identification protégées par CyberArk. Cette page permet de configurer différentes propriétés à l'aide d'un seul ou de plusieurs noms d'informations d'identification. Cette page est facultative si vous ne souhaitez pas inclure CyberArk lors de l'installation de votre proxy avec le programme d'installation du proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Protection par mot de passe CyberArk

Tout champ de mot de passe dans le programme d'installation proxy Edge dont les informations d'identification CyberArk sont configurées dans le coffre-fort CyberArk et spécifiées sur la page Informations d'identification protégées de CyberArk du programme d'installation est grisé et contient le message Protégé par CyberArk.

Utilisation d'un équilibreur de charge avec le serveur proxy Edge

Vous pouvez utiliser un équilibreur de charge pour équilibrer la charge sur les serveurs proxy dans votre configuration de proxy Chiffrement Edge. Si l'équilibreur de charge et les serveurs proxy utilisent des ports différents, spécifiez le nom d'hôte et le port HTTPS de l'équilibreur de charge pour permettre aux utilisateurs d'afficher les réponses sur leur navigateur.

Important :
Tous les environnements de production doivent inclure au moins deux serveurs proxy Edge Encryption pour la redondance.

Traitement des demandes en bordure sans équilibreur de charge

Si vous n'utilisez pas d'équilibreur de charge, une demande est traitée comme décrit ci-dessous.

1. L'utilisateur émet une requête à partir d'un navigateur.
2. Le navigateur envoie la demande au serveur proxy Edge.
3. Le serveur proxy envoie la demande à l'instance ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. L'instance ServiceNow renvoie la réponse au serveur proxy.
5. Le serveur proxy ajoute son propre numéro de port dans l'en-tête de réponse avant de renvoyer la réponse au navigateur de l'utilisateur.

La demande est terminée avec succès, car l'utilisateur peut afficher la réponse du serveur proxy au numéro de port spécifié dans l'en-tête de réponse.

Traitement des demandes en bordure avec un équilibreur de charge

Toutefois, si vous utilisez un équilibreur de charge, le navigateur de l'utilisateur communique directement avec l'équilibreur de charge, et non avec le serveur proxy. Une demande est traitée comme décrit ci-dessous.

Remarque :
L'exemple suivant utilise 1025 comme numéro de port du serveur proxy.

1. L'utilisateur émet une requête à partir d'un navigateur.
2. Le navigateur envoie la demande à une adresse IP virtuelle (VIP) d'équilibreur de charge, également appelée serveur virtuel.
3. L'adresse IP virtuelle est configurée pour pointer vers le serveur proxy (par exemple, 10.2.200.148:1025), de sorte que l'équilibreur de charge transfère la demande au serveur proxy.
4. Le serveur proxy envoie la demande à l'instance ServiceNow.
5. L'instance ServiceNow renvoie la réponse au serveur proxy.
6. Le serveur proxy réécrit l'en-tête d'emplacement dans la réponse avec les valeurs configurées dans les propriétés de risk-servicenow.dev.echonet :1025.
   - **Hôte** : edgencryption.proxy.host
   - **Port HTTP** : edgeencryption.proxy.http.port
   - **Port HTTPS** : edgeencryption.proxy.https.port
7. Le serveur proxy transfère la réponse à l'équilibreur de charge avec l'en-tête d'emplacement pointant vers le port du serveur proxy.

Le résultat varie selon que l'équilibreur de charge et les serveurs proxy utilisent ou non le même port.

- Si l'équilibreur de charge et les serveurs proxy utilisent le même port, la demande aboutit, car l'utilisateur reçoit la réponse du même port identifié dans l'en-tête de réponse.
- Si l'équilibreur de charge et les serveurs proxy utilisent des ports différents, la demande échoue car le navigateur de l'utilisateur communique uniquement avec l'équilibreur de charge, mais la réponse est sur le serveur proxy.

Solution

Vous pouvez résoudre le problème en utilisant simplement l'équilibreur de charge et tous les serveurs proxy Edge sur le même port, mais ce n'est pas une solution idéale. Une meilleure solution consiste à permettre au système de savoir quel port l'équilibreur de charge utilise.

Les propriétés suivantes permettent au serveur proxy Edge de réacheminer les messages de réponse vers l'équilibreur de charge si le serveur proxy et l'équilibreur de charge utilisent des ports différents.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- *edgeencryption.proxy.rewrite.location.host* Spécifie le nom d'hôte utilisé pour accéder à ServiceNow via l'équilibreur de charge.
- *edgeencryption.proxy.rewrite.location.https.port* spécifie le port HTTPS utilisé pour accéder à ServiceNow via l'équilibreur de charge.

Configurer l'équilibreur de charge

Si l'équilibreur de charge et les serveurs proxy utilisent des ports différents, spécifiez le nom d'hôte et le port HTTPS de l'équilibreur de charge pour permettre aux utilisateurs d'afficher les réponses sur leur navigateur.

Avant de commencer

Rôles requis :

- administrateur local ou de domaine sur un hôte Windows
- utilisateur de service avec accès complet au système de fichiers sur un hôte Linux

Procédure

1. Connectez-vous à l'hôte du serveur proxy en tant qu'administrateur, administrateur de domaine ou utilisateur de service.
2. Accédez au répertoire d'installation du proxy Edge et sélectionnez conf/edgeencryption.properties.
3. Définissez les propriétés suivantes :

Propriété	Description
edgeencryption.proxy.rewrite.location.host	Si votre configuration Edge inclut un équilibreur de charge pour équilibrer la charge entre les serveurs proxy, réécrit les réponses à l'équilibreur de charge afin que les demandes puissent être terminées. ○ Si un équilibreur de charge existe dans la configuration du proxy, spécifiez le nom d'hôte utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ Facultatif : s'il n'y a pas d'équilibreur de charge dans la configuration du proxy, vous pouvez définir cette valeur sur le nom d'hôte utilisé par le serveur proxy.
edgeencryption.proxy.rewrite.location.https.port	Si votre configuration Edge inclut un équilibreur de charge pour équilibrer la charge entre les serveurs proxy, spécifie le port HTTPS utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ S'il existe un équilibreur de charge dans la configuration, spécifiez le port HTTPS utilisé pour accéder à ServiceNow via l'équilibreur de charge. ○ Facultatif : s'il n'y a pas d'équilibreur de charge dans la configuration, vous pouvez définir cette valeur sur le port HTTPS utilisé par le serveur proxy.

4. Enregistrez le fichier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultats
Les demandes peuvent être terminées, car les utilisateurs peuvent désormais afficher les réponses sur leur navigateur.

Mise à niveau de Chiffrement Edge

Les mises à niveau d'instance et les mises à niveau de serveur proxy nécessitent une attention particulière dans un Chiffrement Edge environnement.

Mises à niveau d'instance

Les mises à niveau d'instance dans un environnement Chiffrement Edge nécessitent de la prudence pour s'assurer que les contrôles Edge fonctionnent correctement après la mise à niveau de l'instance.

Lors d'une mise à niveau d'instance, vous ne devez pas ajouter, modifier ou supprimer les éléments suivants :

- Configurations de Chiffrement Edge
- Règles de Chiffrement Edge
- Schémas de tokenisation Edge Encryption
- Travaux planifiés Chiffrement Edge
- Configurations de la clé de chiffrement Edge
- Mises à niveau planifiées de Chiffrement Edge
- Configurations IP de la liste de refus de Chiffrement Edge

Toute tâche planifiée en cours d'exécution pendant la mise à niveau de l'instance ne se terminera pas. Pour terminer la tâche interrompue, réexécutez la tâche une fois l'instance mise à niveau. Lorsque vous replanifiez la tâche, le traitement qui s'est produit avant la mise à niveau de l'instance n'est pas perdu et la tâche continue de traiter uniquement les données qui n'ont pas encore été traitées.

Mises à niveau des serveurs proxy

Planifiez une mise à niveau de proxy pour permettre à l'instance de mettre à niveau le Chiffrement Edge serveur proxy ou mettez à niveau manuellement le serveur proxy à tout moment.

⚠ Avertissement :
Pour une mise à niveau sous Windows, vous pouvez rencontrer des problèmes de verrouillage de fichiers et la mise à niveau peut échouer. Pour que la mise à niveau réussisse, aucun fichier ne doit être ouvert dans le répertoire d'installation. De plus, il ne doit pas y avoir de shell existant dans le répertoire d'installation. En particulier, si vous démarrez le proxy à partir de la ligne de commande (via `bin \edgeencryption.bat install/start`) alors qu'il se trouve dans le répertoire d'installation, vous devez fermer ce shell ou le déplacer hors du répertoire d'installation par la suite. Aucun fichier sous le répertoire d'installation ne doit être ouvert par un éditeur ou par une autre application.

Bibliothèques tierces

Les bibliothèques tierces, telles que Gemalto, sont perdues lors des mises à niveau des serveurs d'instance et des serveurs proxy si elles sont conservées dans le même répertoire. Vous pouvez effectuer ce qui suit pour empêcher la perte de bibliothèques tierces lors des mises à niveau :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Ajoutez manuellement la propriété suivante à edgeencryption.properties :

   `edgeencryption.ekm.provider.classname = com.snc.edgeencryption.encryption.CloudEdgeNaeKeyProvider`

2. Ajoutez la propriété d'emplacement de la *`edgeencryption.thirdparty.vendor.library.path`* bibliothèque fournisseur et définissez-la sur `/chemin/vers/jars`.

   Par exemple :

   `edgeencryption.thirdparty.vendor.library.path = /app/servicenow/libs`

3. Copiez les fichiers JAR SafeNet dans ce chemin d'accès.

Une fois que vous avez installé les bibliothèques tierces en dehors de l'installation Chiffrement Edge , elles ne sont plus perdues lors des mises à niveau.

Mises à niveau planifiées

Important :
Pendant ServiceNow les mises à niveau d'instance, mettez également à niveau la version de votre serveur proxy pour qu'elle s'aligne sur la version de votre instance et réduise les risques de problèmes de compatibilité.

Planifiez une mise à niveau pour permettre à l'instance de mettre à niveau le serveur proxy à l'heure planifiée. Cette fonctionnalité est disponible par défaut après la mise à niveau. Une mise à niveau planifiée inclut les événements suivants :

1. Le serveur proxy vérifie auprès de l'instance s'il existe une nouvelle version disponible pour la mise à niveau. Les nouvelles versions sont généralement disponibles lorsque l'instance est mise à niveau.
2. L'administrateur reçoit une notification lors de la connexion lorsqu'une nouvelle version du serveur proxy est disponible.
3. L'administrateur peut planifier une mise à niveau du serveur proxy Chiffrement Edge pour chaque serveur proxy.

   Remarque :
   Seuls les utilisateurs disposant du rôle security_admin peuvent créer un calendrier de mise à niveau via le serveur proxy.

4. Une fois la mise à niveau planifiée, le serveur proxy effectue automatiquement la mise à niveau à l'heure planifiée. Pendant la mise à niveau, le serveur proxy n'est hors ligne que pendant une courte période.

   Remarque :
   Étant donné que le serveur proxy redémarre pendant la mise à niveau, il est hors ligne pendant une courte période. La durée est déterminée par votre environnement et le temps nécessaire pour arrêter et redémarrer le service proxy.

5. Lors de la mise à niveau planifiée, un nouveau répertoire proxy est créé et vos fichiers de configuration sont copiés dans le nouveau répertoire. Les nouvelles propriétés sont écrites dans votre fichier de propriétés existant. Les fichiers ou répertoires suivants dans votre ancien répertoire proxy sont copiés dans le nouveau répertoire proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Répertoire /conf
- Répertoire /keys
- Répertoire /keystore
- fichier java/jre/lib/security/cacerts

Par conséquent, vos clés, magasins de clés, paramètres et certificats sont conservés.

Remarque :
Seuls les fichiers ci-dessus sont copiés dans le nouveau répertoire proxy. Les autres fichiers personnalisés dans le répertoire du serveur proxy ne sont pas conservés lors d'une mise à niveau planifiée. Le fichier journal de mise à niveau se trouve dans le répertoire proxy d'origine dans le dossier suivant : <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Prérequis pour la mise à niveau planifiée

Avant de planifier une mise à niveau pour un proxy Chiffrement Edge, vérifiez les points suivants :

1. La variable d'environnement *JAVA_HOME* pointe vers une installation Java sur l'ordinateur qui se trouve en dehors de la structure de répertoires du proxy Chiffrement Edge.
2. La variable d'environnement *JAVA_HOME* pointe vers une installation Java à la version 1.8_u144 ou supérieure.
3. Le *-Djava.io.tmpdir* paramètre dans le fichier wrapper.conf du proxy Chiffrement Edge pointe vers un répertoire qui se trouve en DEHORS de la structure de répertoire du proxy Chiffrement Edge et le proxy dispose d'autorisations de lecture/écriture/exécution sur le répertoire. Si vous le souhaitez, vous pouvez commenter entièrement le paramètre afin que Java utilise son emplacement tmp par défaut.

Mises à niveau manuelles

Au lieu de créer un calendrier de mise à niveau, vous pouvez mettre à niveau manuellement chaque serveur proxy via la ligne de commande. Voir Mettre à niveau manuellement un serveur proxy Chiffrement Edge s'exécutant sous Linux ou Mettre à niveau manuellement un serveur proxy Chiffrement Edge s'exécutant sous Windows.

État de la version du proxy

Vous pouvez facilement identifier si un serveur proxy est obsolète en accédant à **Configuration de Chiffrement Edge** > **Proxys** > **Tout**. L'état de votre version de proxy est indiqué dans la colonne **Version de proxy** par les couleurs suivantes :

Vert

Votre serveur proxy est à jour.

Jaune

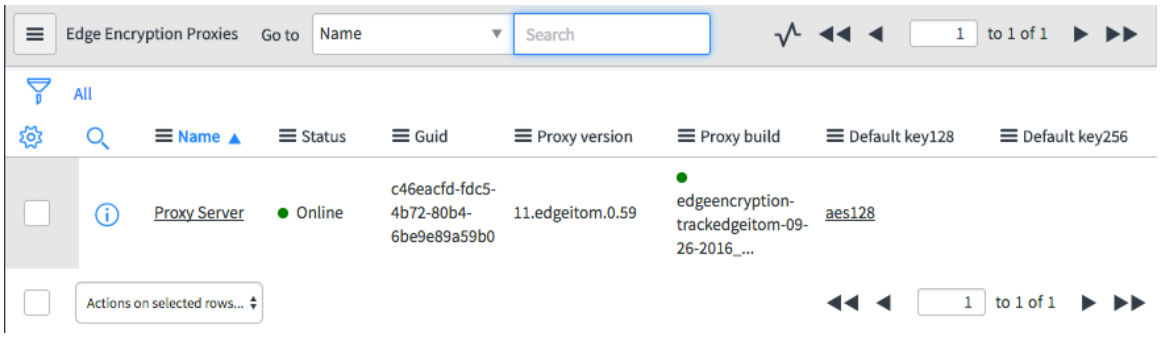
Votre serveur proxy n'est pas à jour et une mise à niveau est nécessaire.

Orange

Nous n'avons pas pu procéder à la mise à niveau. Votre serveur proxy revient à l'ancienne version pour s'assurer qu'il n'y a pas de temps d'arrêt.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Résoudre un échec de la mise à niveau d'un proxy planifié

Lorsqu'une mise à niveau de proxy planifiée échoue, le serveur proxy revient à la version depuis laquelle vous effectuez la mise à niveau. Toutes les données, clés et fichiers de configuration d'origine sont conservés. Ce processus peut prendre plusieurs minutes. Contactez-nous Service et assistance client pour garantir la réussite de la mise à niveau.

Pour déterminer la raison de l'échec, vous pouvez vérifier la **raison de l'échec** dans le calendrier de mise à niveau. En outre, le répertoire d'installation de la mise à niveau ayant échoué est conservé afin que les fichiers journaux soient disponibles pour le dépannage.

Remarque :
Avant de supprimer des répertoires proxy supplémentaires, vérifiez toujours quel répertoire est à jour en examinant les fichiers journaux. Si les fichiers journaux présentent une activité récente, le proxy est peut-être connecté à votre instance.

Si la mise à niveau d'un proxy programmée échoue à plusieurs reprises, vous pouvez mettre à niveau manuellement votre serveur proxy. Consultez Mettre à niveau manuellement un serveur proxy Chiffrement Edge s'exécutant sous Linux et Mettre à niveau manuellement un serveur proxy Chiffrement Edge s'exécutant sous Windows.

Configuration minimale requise pour Java

L'ordinateur hôte sur lequel l'installation ou l'exécution du Chiffrement Edge serveur proxy doit gérer une version prise en charge de Java. Les versions prises en charge actuelles sont Java 11.0.6 ou ultérieure dans la série de versions 11.x

Remarque :
Java 8 n'est plus pris en charge à partir de cette Utah version. Mettez à niveau votre environnement avec le Chiffrement Edge proxy vers Java 11 avant d'essayer d'installer la Utah version du Chiffrement Edge proxy.

Si vous utilisez un chiffrement AES 256 bits avec Java 8 mise à jour 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte de serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d'effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de stratégie de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Environnements mixtes de versions proxy

Bien qu'il ne soit pas recommandé d'utiliser un environnement exécutant d'anciennes versions du serveur proxy avec des versions à jour du serveur proxy, il est possible de le prendre en charge si tous les serveurs proxy appartiennent à la même famille de versions que votre instance. Par exemple, si vous disposez d'une instance sur la Xanadu version,

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

votre environnement prend en charge les serveurs proxy à partir de n'importe quel Xanadu correctif ou correctif logiciel. Cependant, les limitations suivantes s'appliquent.

- Si un serveur proxy prend en charge des fonctionnalités qu'un autre proxy ne prend pas en charge, vous constaterez un comportement incohérent, selon le serveur proxy utilisé.
- Si un serveur proxy n'est pas à jour, il se peut qu'il n'inclue pas les améliorations de sécurité récentes.

Si un serveur proxy d'une version précédente est enregistré avec une version plus récente de l'instance, vous recevrez régulièrement des notifications indiquant que le serveur proxy est obsolète. Pour garantir un environnement optimal et sécurisé, ServiceNow il est recommandé de toujours mettre à niveau votre serveur proxy vers la version la plus récente du logiciel pris en charge par votre instance.

Planifier une mise à niveau du serveur proxy Chiffrement Edge

Créez un calendrier de mise à niveau pour permettre à l'instance de mettre à niveau un serveur proxy obsolète.

Avant de commencer

Pour planifier une mise à niveau, vous devez être connecté à votre instance via le serveur proxy.
Si vous utilisez un chiffrement AES 256 bits avec Java 8 mise à jour 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte de serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d'effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de stratégie de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Une fois la mise à niveau planifiée, le serveur proxy effectue automatiquement la mise à niveau à l'heure planifiée. Pendant la mise à niveau, le serveur proxy n'est hors ligne que pendant une courte période.

Remarque :
Étant donné que le serveur proxy redémarre pendant la mise à niveau, il est hors ligne pendant une courte période. La durée est déterminée par votre environnement et le temps nécessaire pour arrêter et redémarrer le service proxy.

Lors de la mise à niveau planifiée, un nouveau répertoire proxy est créé et vos fichiers de configuration sont copiés dans le nouveau répertoire. Les nouvelles propriétés sont écrites dans votre fichier de propriétés existant. Les fichiers ou répertoires suivants dans votre ancien répertoire proxy sont copiés dans le nouveau répertoire proxy.

- Répertoire /conf
- Répertoire /keys
- Répertoire /keystore
- fichier java/jre/lib/security/cacerts

Par conséquent, vos clés, magasins de clés, paramètres et certificats sont conservés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Seuls les fichiers ci-dessus sont copiés dans le nouveau répertoire proxy. Les autres fichiers personnalisés dans le répertoire du serveur proxy ne seront pas conservés lors d'une mise à niveau planifiée. Le fichier journal de mise à niveau se trouve dans le répertoire proxy d'origine dans le dossier suivant : <original-proxy-directory>/tmp/upgrade-wrapper/bin.

Si plusieurs serveurs proxy ne sont pas à jour, vous devez planifier une mise à niveau pour chaque serveur proxy individuellement.

Remarque :
Évitez d'héberger plusieurs serveurs proxy sur la même machine. Toutefois, si votre environnement inclut cette configuration, ne planifiez pas les mises à niveau vers plusieurs proxys sur le même ordinateur en même temps.

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Proxys** > **Calendriers de mise à niveau**.
2. Cliquez sur **Nouveau**.
3. Complétez le formulaire.

Formulaire de calendrier de mise à niveau du proxy Chiffrement Edge

Champ	Description
Serveur proxy	Le serveur proxy est en cours de mise à niveau.
Version cible	Version vers laquelle vous mettez à niveau votre serveur proxy. Cette valeur est en lecture seule et définie sur la version de proxy la plus récente disponible pour votre instance.
Heure de début planifiée	Date et heure de début de la mise à niveau.
Actifs	Indique si la mise à niveau planifiée est active. Si ce champ n'est pas sélectionné, la mise à niveau n'est pas effectuée aux date et heure planifiées.
États	L'état de la mise à niveau. Cette valeur est en lecture seule. Les états possibles sont les suivants : ○ En attente ○ En cours d'exécution ○ Terminé ○ Échoué

4. Cliquez sur **Envoyer**.

Que faire ensuite

La durée moyenne d'une mise à niveau est inférieure à 15 minutes. Une fois la mise à niveau exécutée, vous pouvez examiner les détails de la mise à niveau pour en savoir plus. Si votre mise à niveau a échoué, examinez le **motif de l'échec** pour déterminer les étapes suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Détails de mise à niveau

Champ	Description
À partir de la version	La version à partir de laquelle le serveur a été mis à niveau.
Vers la version	Version vers laquelle le serveur a été mis à niveau.
Heure de début réel	Heure à laquelle la mise à niveau a commencé.
Heure de fin	Heure à laquelle la mise à niveau a pris fin.
Cause de la défaillance	Motif de l'échec de la mise à niveau.

Mettre à niveau manuellement un serveur proxy Chiffrement Edge s'exécutant sous Linux

Mettre à jour un proxy fonctionnant sous Linux.

Avant de commencer

Si vous utilisez un chiffrement AES 256 bits avec Java 8 mise à jour 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte de serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d'effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de stratégie de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Rôle requis : administrateur local ou security_admin sur l'ordinateur hôte

Procédure

1. Téléchargez le fichier d'archive Chiffrement Edge proxy-update dans le répertoire d'installation.
   a. Accédez à la **Configuration de Chiffrement Edge** > **Installation et téléchargements** > **Téléchargements**
   b. Sélectionnez le lien **Télécharger le programme d'installation de ligne de commande** .
   c. Lorsque le téléchargement commence, sélectionnez votre répertoire d'installation comme emplacement de téléchargement.
2. Accédez au répertoire d'installation.
3. Exécutez la commande suivante :

```
java -jar edgeencryption-dist-<version>-linux-x86-64.jar -m dist-upgrade -c <répertoire proxy>
```

Option	Description
Répertoire proxy	Répertoire du répertoire d'installation où le proxy a été initialement installé. Ce répertoire est créé par l'installation.

Si vous souhaitez afficher l'écran d'aide, exécutez cette commande sans arguments : `java -jar edgeencryption-dist-<version>-linux-x86-64.jar`

Un nouveau répertoire proxy est créé avec un horodatage actuel. Une sauvegarde de l'ancien répertoire proxy est conservée sous la forme backup.dist-upgrade_timestamp dans le nouveau répertoire d'installation du

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

proxy. L'ancien proxy s'arrête et le nouveau proxy démarre. Toutes les connexions/transactions ouvertes sur l'ancien serveur proxy sont terminées.

4. Vérifiez le journal du proxy dans le nouveau répertoire et l'instance pour vérifier que le nouveau proxy est en cours d'exécution.

Mettre à niveau manuellement un serveur proxy Chiffrement Edge s'exécutant sous Windows

Mettre à jour un proxy en cours d'exécution sous Windows.

Avant de commencer

Si vous utilisez un chiffrement AES 256 bits avec Java 8 mise à jour 141 (8u141) ou une version antérieure, vous devez installer les fichiers de stratégie de juridiction Java Cryptography Extension (JCE) en les copiant dans le répertoire de base Java système de chaque Chiffrement Edge hôte de serveur proxy. Ajoutez ces fichiers au dossier <Java-home-directory>/jre/lib/security avant d'effectuer une mise à niveau planifiée ou manuelle. Pour installer les fichiers de stratégie de chiffrement AES 256 bits, reportez-vous à la section Configurer la clé de chiffrement AES 256 bits.

Rôle requis : administrateur local ou security_admin sur l'ordinateur hôte

Procédure

1. Téléchargez le fichier d'archive Chiffrement Edge proxy-update dans le répertoire d'installation.
   a. Accédez à la **Configuration de Chiffrement Edge** > **Installation et téléchargements** > **Téléchargements**
   b. Sélectionnez le lien **Télécharger le programme d'installation de ligne de commande** .
   c. Lorsque le téléchargement commence, sélectionnez votre répertoire d'installation comme emplacement de téléchargement.
2. Démarrez le programme de terminal cmd Windows avec des privilèges d'administrateur.
3. Accédez au répertoire d'installation.
4. Exécutez la commande suivante :

```
java -jar edgeencryption-dist-<version>-all.jar -m dist-upgrade -c <répertoire proxy>
```

Option	Description
Répertoire proxy	Répertoire du répertoire d'installation où le proxy a été initialement installé. Ce répertoire est créé par l'installation.

Si vous souhaitez afficher l'écran d'aide, exécutez cette commande sans arguments : `java -jar edgeencryption-dist-<version>-all.jar`

Un nouveau répertoire proxy est créé avec un horodatage actuel. Une sauvegarde de l'ancien répertoire proxy est conservée sous la forme backup.dist-upgrade_timestamp dans le nouveau répertoire d'installation du proxy. L'ancien proxy s'arrête et le nouveau proxy démarre. Toutes les connexions/transactions ouvertes sur l'ancien serveur proxy sont terminées.

5. Vérifiez le journal du proxy dans le nouveau répertoire et l'instance pour vérifier que le proxy a été mis à jour et qu'il est en cours d'exécution.

Restaurer une mise à niveau du serveur proxy Chiffrement Edge

Si la mise à niveau d'un proxy échoue, vous pouvez revenir à la version antérieure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Si une mise à niveau échoue lors de l'utilisation de la fonctionnalité de mise à niveau planifiée dans la Xanadu version, le serveur proxy revient automatiquement à l'ancienne version. L'ancien serveur proxy est stocké tel quel dans un répertoire de sauvegarde.

Si vous souhaitez restaurer une mise à niveau manuelle, vous pouvez suivre ces étapes.

Procédure

1. Arrêtez le proxy.
2. Supprimez le nouveau répertoire proxy.
3. Renommez le répertoire de sauvegarde avec le nom du proxy.
   Le répertoire de sauvegarde se trouve dans le répertoire d'installation du proxy avec le nom <nom du proxy>_backup
4. Démarrez le proxy.
5. Vérifiez le journal du proxy et l'instance pour vérifier que le proxy est en ligne.

Configuration de Chiffrement Edge

Une fois le serveur proxy installé et en cours d'exécution, effectuez la Chiffrement Edge gestion Chiffrement Edge via le serveur proxy.

Vous devez effectuer toutes les étapes avant Installation de Chiffrement Edge de créer des configurations de chiffrement et des schémas de chiffrement sur l'instance.

Remarque :
Pour accéder à la Chiffrement Edge configuration, vous devez vous connecter via le serveur proxy et vous élever au rôle security_admin.

Rotation des clés de chiffrement

Effectuez la rotation de la clé de chiffrement à partir de l'instance. Ajoutez une nouvelle clé, modifiez l'affectation de clé par défaut, puis planifiez une rotation de clés en masse ou une rotation de clés uniques.

Avant de définir une clé de chiffrement comme clé par défaut, mettez la clé à la disposition de chaque proxy. Cela garantit que les proxys disposent de la clé pour chiffrer les données lorsque la clé est affectée comme clé par défaut. Tous les proxys doivent avoir accès à une clé pour que cette clé puisse être affectée comme clé par défaut.

Avertissement :
Avant de supprimer une clé du proxy, configurez et exécutez une tâche de rotation de clé en masse pour vous assurer qu'aucune donnée sur l'instance n'utilise la clé. Si des informations sont toujours chiffrées avec cette clé, vous ne pouvez pas les déchiffrer après avoir supprimé la clé.

Comportement de filtrage et de tri en bordure

Chaque fois que vous modifiez des clés par défaut, assurez-vous d'effectuer une rotation de clés (en masse ou une rotation de clés uniques). Sinon, vous risquez d'obtenir des résultats inattendus lors du tri et du filtrage des enregistrements. Imaginons par exemple le scénario suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. Vous créez des enregistrements chiffrés à l'aide d'une clé de chiffrement.
2. Vous créez une nouvelle clé et la définissez par défaut.
3. Vous créez un nouvel ensemble d'enregistrements chiffrés à l'aide de la nouvelle clé de chiffrement.

Si vous filtrez par un champ chiffré lorsque vous êtes connecté via le proxy Edge, tous les enregistrements peuvent ne pas être filtrés correctement ou des enregistrements peuvent apparaître de manière inattendue. Le filtre fonctionne uniquement pour les enregistrements chiffrés à l'aide de la clé par défaut actuelle. Les enregistrements chiffrés à l'aide de la clé par défaut précédente apparaissent toujours dans la vue de liste.

Si vous triez par un champ chiffré lorsque vous êtes connecté via le proxy Edge, vous voyez deux groupes d'enregistrements avec le même texte lisible par l'homme dans le champ chiffré.

Planifier une tâche de rotation de clé unique

Planifiez une tâche pour trouver les données chiffrées à l'aide d'un alias de clé spécifié, puis chiffrez à nouveau les données avec la clé de chiffrement par défaut actuelle. Les données sont déchiffrées avant d'être chiffrées à nouveau avec la clé par défaut.

Avant de commencer

Rôle requis : security_admin

Avant de planifier cette tâche, mettez à jour la clé par défaut dans **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Définir les clés par défaut**.

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la rotation de clé unique**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Rotation de clé unique**.
Clé	Entrez la clé à mettre hors service. Vérifiez que cette clé n'est plus la clé par défaut dans **Configuration de Chiffrement Edge** > **Configuration de la clé de chiffrement** > **Définir les clés par défaut**.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Non disponible lors de l'exécution d'une rotation de clés unique.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ dans la table d'audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Ce champ est en lecture seule et actif. Pour en savoir plus sur les champs audités, reportez-vous à la rubrique Audit.
Estimer le nombre	Nombre maximal estimé d'enregistrements audités à traiter. Non disponible lors de l'exécution d'une rotation de clés unique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
d'enregistrements d'audit maximal	
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
L'estimation du nombre d'enregistrements n'est pas prise en charge lors du traitement des champs audités.

Planifier une tâche de rotation de clés en masse

Planifiez une tâche pour trouver les données chiffrées avec une clé précédente, puis chiffrez à nouveau les données avec les clés de chiffrement par défaut actuelles. Les données sont déchiffrées avant d'être chiffrées à nouveau avec la clé par défaut actuelle.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la rotation de clés en masse**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Mass Key Rotation (Rotation des clés en masse)**.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Non disponible lors de l'exécution d'une rotation de clés en masse.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ dans la table d'audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Ce champ est en lecture seule et actif. Pour en savoir plus sur les champs audités, reportez-vous à la rubrique Audit.
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Non disponible lors de l'exécution d'une rotation de clés en masse.
Actifs	Décochez cette case pour désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
   L'estimation du nombre d'enregistrements n'est pas prise en charge lors du traitement des champs audités.

Planifier une tâche de rotation de clé de pièce jointe

Planifiez une tâche pour trouver des pièces jointes chiffrées à l'aide d'un alias de clé spécifié, puis chiffrez à nouveau les pièces jointes avec la clé de chiffrement par défaut actuelle. La pièce jointe est déchiffrée avant d'être chiffrée à nouveau avec la clé par défaut.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la rotation clé des pièces jointes**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Rotation clé de la pièce jointe**.
Actifs	Décochez la case si vous souhaitez désactiver cette tâche.
Table	Selectionner une table.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Nombre d'enregistrements estimé.**
5. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Chiffrer les champs à l'aide de configurations de chiffrement

Chiffrez les champs en créant des configurations de chiffrement.

Pour configurer Chiffrement Edge, vous devez être connecté à l'instance via le proxy. Testez tous les changements sur une instance de non-production avant de les appliquer à l'instance de production.

Définir des clés de chiffrement

Après avoir configuré un ou plusieurs proxys et une clé de chiffrement par défaut, l'instance vérifie que les clés sont disponibles pour tous les proxys. Vous ne pouvez pas faire d'une clé de chiffrement la clé par défaut à moins que tous les proxys ne disposent de la clé. Une fois qu'une clé par défaut est définie, vous pouvez créer des configurations de chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Affecter les champs et les pièces jointes à chiffrer

Affecter des champs et des pièces jointes à chiffrer signifie affecter un type de chiffrement au champ ou à la pièce jointe. Avant de marquer un champ comme chiffré, évaluez les problèmes suivants.

- Déterminez les fonctionnalités système qui pourraient être impactées.
- Examinez tous les scripts pour vérifier l'utilisation du champ.
- Apportez les ajustements souhaités à la taille du champ. Une fois qu'un champ a été configuré pour le chiffrement, la taille du champ ne peut pas être modifiée.

Le marquage d'un champ à chiffrer augmente la taille du champ pour stocker les données chiffrées. Le processus d'augmentation de la taille du champ peut prendre beaucoup de temps, en fonction du nombre d'enregistrements dans la table.

Prise en charge de l'API

Chiffrement au niveau des colonnes met à jour les API `setDisplayValue()` et `setValue()` afin qu'elles puissent insérer des données chiffrées pour les champs chiffrés. Il permet également à `getDisplayValue()` et `getValue()` de renvoyer des valeurs en clair.

Le script suivant illustre ces changements d'API lorsque la brève description de l'incident est chiffrée :

```
var gr = new GlideRecord('incident'); //creates a new incident
gr.setValue('short_description','test123'); //sets the value to test123
var sys_ID = gr.insert(); //inserts the record in the Incident table.
gs.info(gr.getValue('short_description')); //displays the unencrypted value
```

Lorsque vous utilisez `getValue()` pour obtenir du texte chiffré, votre script ne renvoie plus le texte chiffré. Votre script renvoie le texte en clair, en supposant que l'utilisateur a accès au module de chiffrement. `getValue()` renvoie le texte chiffré si l'utilisateur n'a pas accès au module cryptographique.

Créer une configuration de chiffrement de champ

Sélectionnez les champs à chiffrer et identifiez le type de chiffrement.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Créer**.
2. Renseignez le formulaire.

Champ	Description
Table	Table qui contient le champ à chiffrer.
Type	Indique s'il faut chiffrer une colonne de table ou des pièces jointes pour la table. **Sélectionner une colonne**.
Colonne	Champ à chiffrer. S'affiche uniquement lorsque le **type** est **Colonne**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Seuls les champs Chaîne, Date, Date/heure, Journal, Entrée de journal et URL sont pris en charge. ○ **Champs de chaîne et d'URL** : vous pouvez ajouter une configuration de chiffrement à une table parente ou à une table enfant. ○ **Champs Date et Date/Heure** : vous pouvez ajouter une configuration de chiffrement à une table parente uniquement. Vous ne pouvez pas ajouter une nouvelle configuration de chiffrement à une table enfant. **Remarque :** Selon le nombre d'enregistrements affectés par les champs Date et Date/Heure que vous chiffrez, la création de la configuration de chiffrement peut prendre jusqu'à quelques minutes. Veillez à créer la configuration de chiffrement pour les champs Date et Date/Heure lorsque le volume de transactions sur l'instance est faible.
Type de chiffrement	Le type de chiffrement à utiliser.

Remarque :
Une combinaison spécifique de table et de champ ne peut avoir qu'une seule configuration active à la fois.

3. Cliquez sur **Envoyer**.

Que faire ensuite
Après avoir ajouté l'enregistrement de configuration de chiffrement, vous pouvez créer une tâche de chiffrement pour chiffrer les données existantes. Si vous n'exécutez pas de tâche de chiffrement, Edge chiffre les données existantes la prochaine fois que les données sont modifiées. Pour plus de détails, voir Planifier une tâche de chiffrement.

Créer une configuration de chiffrement de variable

Sélectionnez les variables de catalogue de services à chiffrer et identifiez le type de chiffrement.

Avant de commencer
Rôle requis : security_admin

Procédure
1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Configuration de chiffrement de variable**.
2. Dans la liste **Configurations des variables de Chiffrement Edge** , cliquez sur **Nouveau**.
3. Renseignez le formulaire.

Champ	Description
Variable	La variable à chiffrer.
Type de chiffrement	Le type de chiffrement à utiliser.

4. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Après avoir ajouté l'enregistrement de configuration de chiffrement, vous pouvez créer une tâche de chiffrement pour chiffrer les données existantes. Si vous n'exécutez pas de tâche de chiffrement, Edge chiffre les données existantes la prochaine fois que les données sont modifiées. Pour plus de détails, voir Planifier une tâche de chiffrement.

Désactiver une configuration de chiffrement

Après avoir configuré un champ ou les pièces jointes d'une table à chiffrer, vous pouvez arrêter le chiffrement en désactivant la configuration de chiffrement. Après la désactivation du chiffrement, vous pouvez exécuter une tâche de déchiffrement pour les champs ou une tâche de déchiffrement de pièce jointe pour les pièces jointes afin de supprimer les données chiffrées de l'instance.

Avant de commencer

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

⚠ Avertissement :
La désactivation d'une configuration de chiffrement ne supprime pas l'enregistrement de chiffrement et le type de chiffrement ne peut pas être modifié.

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de Chiffrement Edge** > **Tout**.
   La liste **des configurations de Chiffrement Edge** s'affiche.
2. Cliquez sur la configuration de chiffrement à désactiver.
   Le formulaire **Configuration de Chiffrement Edge** s'affiche.
3. Cliquez sur la case **Actif** .
   La case **Actif** n'est pas claire.
4. Cliquez sur **Mettre à jour**.
   La liste **des configurations de Chiffrement Edge** s'affiche.

Que faire ensuite

Vous pouvez exécuter une tâche de déchiffrement ou de chiffrement de pièce jointe pour déchiffrer les données sur l'instance. Si vous n'exécutez aucune tâche, les données chiffrées sont déchiffrées la prochaine fois qu'elles sont modifiées.

Planifier une tâche de chiffrement

Vous pouvez planifier une tâche pour rechercher et chiffrer des données non chiffrées dans un champ spécifié, à l'aide de la clé de chiffrement par défaut configurée pour le champ. Si vous ne créez pas de tâche de chiffrement après avoir configuré un champ pour le chiffrement, seules les nouvelles valeurs sont chiffrées.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tout** afin de créer une tâche pour un champ ou **Configuration de Chiffrement Edge** > **Configuration de chiffrement de variable** pour créer une tâche pour une variable.
2. Cliquez sur le champ pour lequel vous souhaitez planifier une tâche de chiffrement.
3. Sous **Liens connexes**, cliquez sur Planifier une **tâche de chiffrement en masse**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le formulaire **de tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. La partie inférieure du formulaire affiche les enregistrements de toutes les exécutions de tâches précédentes.

4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Type de travail	Sélectionnez **Chiffrement**.
Table	Selectionner une table.
Colonne	Sélectionnez une colonne.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Se remplit après avoir sélectionné **Estimer le nombre d'enregistrements**.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ dans la table d'audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Pour en savoir plus sur les champs audités, reportez-vous Audità .
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Se remplit après avoir sélectionné **Estimer le nombre d'enregistrements**. Ce champ n'est visible que lorsque **l'option Traiter les enregistrements historiques** est sélectionnée. **Remarque :** L'estimation peut être supérieure au nombre réel d'enregistrements traités.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Planifier une tâche de déchiffrement

Vous pouvez planifier une tâche pour déchiffrer les données dans un champ chiffré, afin de stocker les données claires dans l'instance.

Avant de commencer

Remarque :
Vous devez marquer l'enregistrement de chiffrement du champ comme inactif (décochez la case **Actif**) pour exécuter la tâche de déchiffrement.

Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tout** afin de créer une tâche pour un champ ou **Configuration de Chiffrement Edge** > **Configuration de chiffrement de variable** pour créer une tâche pour une variable.
2. Cliquez sur le champ que vous souhaitez déchiffrer.
3. Sous **Liens connexes**, cliquez sur **Planifier une tâche de déchiffrement en masse**.

   Le formulaire **de tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. La partie inférieure du formulaire affiche les enregistrements des exécutions de tâches précédentes.
4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Déchiffrement**.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Table	Selectionner une table.
Colonne	Sélectionnez une colonne.
Estimer le nombre d'enregistrements	Nombre total estimé d'enregistrements à traiter. Se remplit après avoir sélectionné **Estimer le nombre d'enregistrements**.
Traiter les enregistrements historiques	Sélectionnez cette option pour traiter les enregistrements historiques dans la table Audit si le champ est audité. Lors du chiffrement des enregistrements historiques d'un champ dans la table d'audit, les nouvelles valeurs et les anciennes valeurs sont chiffrées. Pour en savoir plus sur les champs audités, reportez-vous Audità .
Estimer le nombre d'enregistrements d'audit maximal	Nombre maximal estimé d'enregistrements audités à traiter. Se remplit après avoir sélectionné **Estimer le nombre d'enregistrements**. Ce champ n'est visible que lorsque **l'option Traiter les enregistrements historiques** est sélectionnée. **Remarque :** L'estimation peut être supérieure au nombre réel d'enregistrements traités.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Chiffrer les pièces jointes à l'aide du chiffrement standard

Vous pouvez chiffrer les pièces jointes pour des tables spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Toutes les pièces jointes d'une table utilisent le même type de chiffrement. Les pièces jointes chiffrées ne sont pas recherchées lors d'une recherche de texte. Seuls les types de chiffrement standard sont autorisés pour les pièces jointes. Les types de chiffrement Préservation de l'ordre ou préservation de l'égalité ne sont pas autorisés.

Pour une session contournant le Chiffrement Edge proxy :

- Sur un enregistrement dont le chiffrement des pièces jointes est activé :
  - L'utilisateur peut voir qu'il existe des pièces jointes et des noms de pièces jointes.
  - L'utilisateur ne peut pas ajouter de nouvelles pièces jointes.
- Sur un enregistrement sans chiffrement des pièces jointes activé :
  - L'utilisateur peut ouvrir et télécharger les pièces jointes existantes.
  - L'utilisateur peut ajouter de nouvelles pièces jointes.

Pour une session utilisant le proxy de chiffrement, l'utilisateur peut ouvrir et télécharger des pièces jointes existantes et ajouter de nouvelles pièces jointes.

Configurer le chiffrement des pièces jointes

Sélectionnez les tables dont les pièces jointes doivent être chiffrées et identifiez le type de chiffrement.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Configurations de Chiffrement Edge** > **Créer**.
2. Renseignez les champs du formulaire comme il convient.

Configuration de Chiffrement Edge

Champ	Description
Table	Sélectionnez une table dont les pièces jointes doivent être chiffrées.
Type	Indique s'il faut chiffrer une colonne de table ou des pièces jointes pour la table. Sélectionnez **Pièce jointe**.
Colonne	Champ de table à chiffrer. Ce champ s'affiche lorsque le **Type** est **Colonne** et non lorsque le **Type** est **Pièce jointe**.
Type de chiffrement	Le type de chiffrement à utiliser. Pour les pièces jointes, seuls l'AES128 standard et l'AES256 standard sont autorisés.

3. Cliquez sur **Envoyer**.

Que faire ensuite

Une fois l'enregistrement de chiffrement ajouté, vous pouvez créer une tâche de chiffrement des pièces jointes pour chiffrer les pièces jointes existantes. Si vous n'exécutez aucune tâche de chiffrement de pièce jointe, le système chiffre les nouvelles pièces jointes lorsque vous les joignez.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous marquez `l'attribut edge_encryption_clear_attachment_allowed` comme **Vrai** dans l'entrée Dictionnaire de collecte de la table, les pièces jointes non chiffrées sont ajoutées à une table à l'aide de Chiffrement Edge pour chiffrer les pièces jointes. Si vous activez cet attribut, vous devez configurer une tâche de chiffrement des pièces jointes afin que toutes les pièces jointes non chiffrées ajoutées soient chiffrées.

Planifier une tâche de chiffrement des pièces jointes

Vous pouvez planifier une tâche pour rechercher et chiffrer toutes les pièces jointes non chiffrées pour une table spécifiée, à l'aide de la clé de chiffrement par défaut configurée pour la table.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tout**.
2. Cliquez sur la table pour laquelle vous souhaitez planifier une tâche de chiffrement.
3. Sous **Liens connexes**, cliquez sur Planifier une **tâche de chiffrement en masse**.

   Le formulaire **de tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. La partie inférieure du formulaire affiche les enregistrements des exécutions de tâches précédentes.
4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Type de travail	Sélectionnez **Chiffrement des pièces jointes**.
Table	Selectionner une table.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Planifier une tâche de déchiffrement de pièce jointe

Vous pouvez planifier une tâche pour déchiffrer toutes les pièces jointes chiffrées pour une table spécifiée, afin de stocker les pièces jointes effacées dans l'instance.

Avant de commencer

Remarque :
Vous devez marquer l'enregistrement de chiffrement de la table comme inactif (décochez la case **Actif**) avant l'exécution de la tâche de déchiffrement, sinon rien ne se passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tout**.
2. Cliquez sur la table contenant les pièces jointes que vous souhaitez déchiffrer.
3. Sous **Liens connexes**, cliquez sur **Planifier la tâche de déchiffrement en masse des pièces jointes**.

   Le formulaire **de tâche de chiffrement planifiée** s'affiche avec tous les champs renseignés. La partie inférieure du formulaire affiche les enregistrements des exécutions de tâches précédentes.
4. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Déchiffrement des pièces jointes**.
Actifs	Décochez la case si vous souhaitez désactiver cette tâche.
Table	Selectionner une table.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

5. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
6. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.
7. Pour exécuter immédiatement la tâche, cliquez sur **Exécuter maintenant**.

Modifier le type de chiffrement d'un champ ou d'une pièce jointe

Vous pouvez modifier le type de chiffrement d'un champ ou d'une pièce jointe en sélectionnant un nouveau type de chiffrement dans l'enregistrement de configuration de chiffrement existant. Une combinaison spécifique de table et de champ ne peut avoir qu'une seule configuration active à la fois.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Configuration de Chiffrement Edge** > **Configurations de chiffrement** > **Tout**.
   La liste **des configurations de Chiffrement Edge** s'affiche.
2. Ouvrez l'enregistrement pour modifier la configuration de chiffrement.
3. Cliquez sur la liste déroulante **Type de chiffrement** et sélectionnez un nouveau type de chiffrement.

Remarque :
Pour les pièces jointes, seuls l'AES128 standard et l'AES256 standard sont autorisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Si nécessaire, exécutez une tâche de chiffrement ou de chiffrement des pièces jointes .
   Il n'est pas nécessaire d'exécuter une tâche de chiffrement. Si vous n'exécutez pas de tâche de chiffrement, le champ ou la pièce jointe sera chiffré à l'aide du nouveau type de chiffrement lors de la prochaine modification du champ ou de la pièce jointe.

Tokeniser des chaînes à l'aide de schémas de chiffrement

Vous pouvez remplacer les modèles de chaîne par des jetons avant qu'ils ne soient envoyés et stockés dans l'instance.

Avant de commencer

Pour utiliser des modèles de chiffrement, vous devez installer et configurer une base de données MySQL sur votre réseau. Il s'agit de la même base de données que celle utilisée pour le chiffrement préservant l'ordre. Pour créer ou modifier des schémas de chiffrement, vous devez être connecté à l'instance via le proxy.

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Vous pouvez utiliser des modèles de système de base ou créer vos propres modèles. Les modèles du système de base sont des modèles avancés. Les schémas de chiffrement incluent les limitations suivantes.

- Un modèle composé uniquement de caractères alphabétiques n'est pas autorisé.
- La taille minimale du modèle est de cinq caractères. Vous pouvez modifier ce paramètre à l'aide d'une propriété système.
- Les quantificateurs * et + sont interdits dans les modèles de chiffrement.
- Les schémas de chiffrement correspondent à des mots complets, et non à des parties de chaînes intégrées dans une chaîne plus grande. Les mots sont définis par des espaces et des caractères qui ne peuvent pas être inclus dans un modèle.
- Si la même chaîne est envoyée plusieurs fois à l'instance, elle est remplacée par le même jeton.
- La recherche de texte sur les correspondances exactes est prise en charge. La chaîne de requête est échangée avec un jeton lorsqu'elle est envoyée à l'instance, la recherche est effectuée sur les jetons et lorsque les résultats de la recherche sont renvoyés au serveur proxy, les jetons sont remplacés par du texte clair. Les fonctionnalités telles que la radicalisation ne sont pas prises en charge.

Lorsque vous utilisez des modèles, le texte clair ne quitte jamais votre réseau. Lorsque le serveur proxy correspond à un modèle dans une requête envoyée à l'instance, le proxy remplace la chaîne par un jeton de même taille. Le jeton est envoyé à l'instance au lieu de la chaîne de texte clair. Lorsque la réponse est envoyée depuis l'instance au serveur proxy, le proxy remplace le jeton par la chaîne. Lorsqu'elle est affichée via le serveur proxy, la chaîne s'affiche sous forme de texte clair.

Remarque :
Les modèles de chiffrement des champs chiffrés ne sont pas vérifiés.

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Schémas de chiffrement** > **Créer**.
   Vous pouvez également accéder à **Schémas avancés** pour activer ou modifier un modèle préconfiguré.
2. Saisissez le nom du modèle.
3. Définissez le **type d'entrée du modèle de bordure**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Élémentaire	Une série de types de caractères. Dans l'onglet **En trée de modèle de base** , cliquez sur **Ajouter** et sélectionnez un type de caractère. **L'exemple de modèle** affiche le modèle au fur et à mesure que des caractères sont ajoutés. Cliquez sur **Nouveau bloc** pour déplacer le caractère suivant vers la ligne suivante. Cela vous permet de regrouper des carac–tères dans un motif long. Cliquez sur **X** pour supprimer le dernier ca–ractère du modèle.
Avancé	Une expression RegEx Java. Si l'option Avancé est sélectionnée, vous ne pouvez pas redéfinir le type d'entrée sur De base. Dans le champ **Sample match (Exemple de correspondance**), saisissez un exemple de modèle pour tester l'expression Reg–Ex. Dans le champ **Modèle** , entrez une ex–pression RegEx Java. Cliquez sur **Valider** pour vérifier que l'expression correspond au modèle d'échantillon.

Le type d'entrée définit la façon dont vous allez entrer le modèle. Cela n'a pas d'incidence sur la façon dont le modèle est utilisé.

4. Cliquez sur **Envoyer**.

Réparer ou récupérer des données chiffrées préservant l'ordre

Si vous disposez du rôle security-admin, vous pouvez planifier des tâches exécutées par le proxy pour réparer ou récupérer les champs qui utilisent le chiffrement préservant l'ordre Chiffrement Edge .

Planifiez les tâches pour :

- Jetons d'ordre de réparation.
- Recréez la base de données proxy.

L'exécution de ces tâches peut être une opération chronophage qui peut avoir un impact sur les Chiffrement Edge performances du proxy. Planifiez ces tâches à un moment où aucun utilisateur ou un nombre minimal d'utilisateurs n'utilisent le système, par exemple à minuit le week-end.

Planifier une tâche de réparation de jeton de commande

Vous pouvez planifier une tâche pour rechercher et réparer les champs dans lesquels le jeton de commande est manquant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche
Utilisez ces tâches pour réparer des champs individuels dans une table ou pour réparer tous les champs à l'aide du chiffrement préservant l'ordre. Exécutez cette tâche lorsque la base de données proxy a été hors ligne pendant l'exécution de l'instance, ce qui entraîne la conservation de l'ordre des champs pour lesquels il manque des jetons de commande.

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la réparation des jetons de commande**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Saisissez un nom descriptif.
Type de travail	Sélectionnez **Commander la réparation du jeton**.
Tous les champs	Cochez cette case pour réparer toutes les tables.
Table	Selectionner une table.
Colonne	Sélectionnez une colonne.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de la tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher un nombre estimé d'enregistrements à mettre à jour, cliquez sur **Nombre d'enregistrements estimé.**

Planifier une tâche de récupération de base de données proxy

Exécutez cette tâche lorsque la base de données proxy a perdu des données. Cette tâche recherche tous les enregistrements qui ont été chiffrés avec un jeton (type de chiffrement préservant l'ordre) et les envoie au proxy afin que la base de données du proxy puisse être reconstruite.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Maintenance** > **Planifier la récupération de la base de données**.
2. Renseignez les champs du formulaire comme il convient.

Champ	Valeur
Nom	Entrez un nom descriptif pour cette tâche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur
Type de travail	Sélectionnez **Récupération de base de données**.
Actifs	Décochez cette case si vous souhaitez désactiver cette tâche.
Exécution	Sélectionnez la période entre les exécutions de tâches.
En cours de démarrage	Entrez la date et l'heure de la première exécution de cette tâche.

3. Cliquez sur l'icône de menu dans l'en-tête du formulaire et sélectionnez **Enregistrer**.
4. Pour afficher une estimation du nombre d'enregistrements à mettre à jour, cliquez sur **Estimer le nombre d'enregistrements**.

Configurer la liste de refus d'adresse IP

Empêcher une adresse IP de votre réseau d'envoyer des demandes à votre instance

Avant de commencer

Rôle requis : security_admin

Étant donné que le Chiffrement Edge serveur proxy réside dans votre réseau, il peut faire l'objet d'analyses de vulnérabilité par votre logiciel réseau. Pour empêcher le scanner d'adresses IP ou d'autres demandes d'être transférés à votre ServiceNow instance, vous pouvez ajouter des adresses IP, des plages d'adresses IP ou des masques de réseau à une liste de refus. Toute connexion au serveur proxy à partir d'une adresse sur liste de refus est interrompue et n'est pas transmise à votre instance.

Pour placer une adresse IP sur une liste de refus, vous devez être connecté à votre instance via le serveur proxy.

Important :
Assurez-vous de bien comprendre la topologie de votre réseau avant d'ajouter des adresses IP à votre réseau à une liste de refus. Si une adresse IP est ajoutée à la liste de refus, tout utilisateur possédant cette adresse IP ne peut pas accéder au Chiffrement Edge serveur proxy.

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Maintenance** > **Liste de refus des adresses IP**.
   La vue de listes Encryption Proxy IP Denylists [edge_encryption_ip_blacklist] s'ouvre.
2. Cliquez sur **Nouveau**.
3. Complétez le formulaire.

Champ	Description
Serveur proxy	Le Chiffrement Edge serveur proxy qui n'est pas autorisé à transférer des demandes provenant d'adresses figurant sur la liste de refus.
Adresse IP, plage d'adresses IP ou masque réseau	Les demandes provenant de cette adresse IP, de cette plage ou de ce masque réseau ne sont pas transmises à votre ServiceNow instance. Exemples de valeurs : ○ Adresse IP : 10.10.10.5 ○ Plage IP : 10.10.10.1-15 ○ Masque réseau : 10.10.10.0/24

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Vous pouvez utiliser des adresses IPv4 ou IPv6
Actif	Indique si l'enregistrement est actif ou non. Seules les adresses IP des enregistrements actifs ne peuvent pas envoyer de demandes à l'instance.
Description	Description de l'enregistrement de liste de refus.

4. Cliquez sur **Envoyer**.
5. Répétez ces étapes pour tous les autres proxys pour lesquels une adresse IP doit être refusée.

Résultats

Le Chiffrement Edge serveur proxy met fin à toute connexion à partir d'adresses IP, de plages ou de masques réseau figurant sur la liste de refus et ne peut pas transmettre la demande à l'instance.

Chiffrer les données à partir d'un créateur d'enregistrement

Configurez votre Chiffrement Edge serveur proxy pour autoriser les insertions à partir d'un créateur d'enregistrement en créant des règles de chiffrement à partir de l'enregistrement du créateur d'enregistrement.

Avant de commencer

Rôle requis : security_admin

Les créateurs d'enregistrements permettent aux utilisateurs finaux de créer des enregistrements basés sur des tâches, tels que des enregistrements d'incidents, à Catalogue de services partir du et Portail de services. Si un créateur d'enregistrement tente d'insérer des données dans un champ marqué pour chiffrement, un message d'insertion non valide s'affiche et les données ne sont pas enregistrées dans le champ.

Le chiffrement de données provenant d'un créateur d'enregistrement nécessite une configuration de chiffrement définie pour le champ cible. Vérifiez que vous avez créé une configuration de chiffrement pour le champ et la table cibles avant de créer une règle de chiffrement à partir d'un créateur d'enregistrement. Voir Créer une configuration de chiffrement de champ. Pour chiffrer des pièces jointes à partir d'un créateur d'enregistrement, Configurer le chiffrement des pièces jointes.

Procédure

1. Connectez-vous à votre instance via le Chiffrement Edge serveur proxy.
2. Accédez à la **Catalogue de services** > **Définitions de catalogues** > **Créateurs d'enregistrements**.
3. Créez un enregistrement de créateur d'enregistrement ou ouvrez un enregistrement de créateur d'enregistrement existant.
4. Sous **Liens connexes**, sélectionnez **Créer une règle de chiffrement Edge**.
   Deux règles de chiffrement inactives sont automatiquement créées pour chiffrer les données envoyées par le créateur d'enregistrement au champ marqué pour chiffrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règle de chiffrement	Description
<RecordProducerName>	Règle créée pour traiter les paramètres POST à partir de et Catalogue de services mapper les variables aux champs de l'instance.
<RecordProducerName>JSON	Règle créée pour traiter une charge utile JSON à partir de et Portail de services mapper les variables aux champs de l'instance.

5. Activez les règles de chiffrement nécessaires créées par le créateur d'enregistrement.

   a. Accédez à la **Configuration de Chiffrement Edge** > **Règles** > **Tout**.

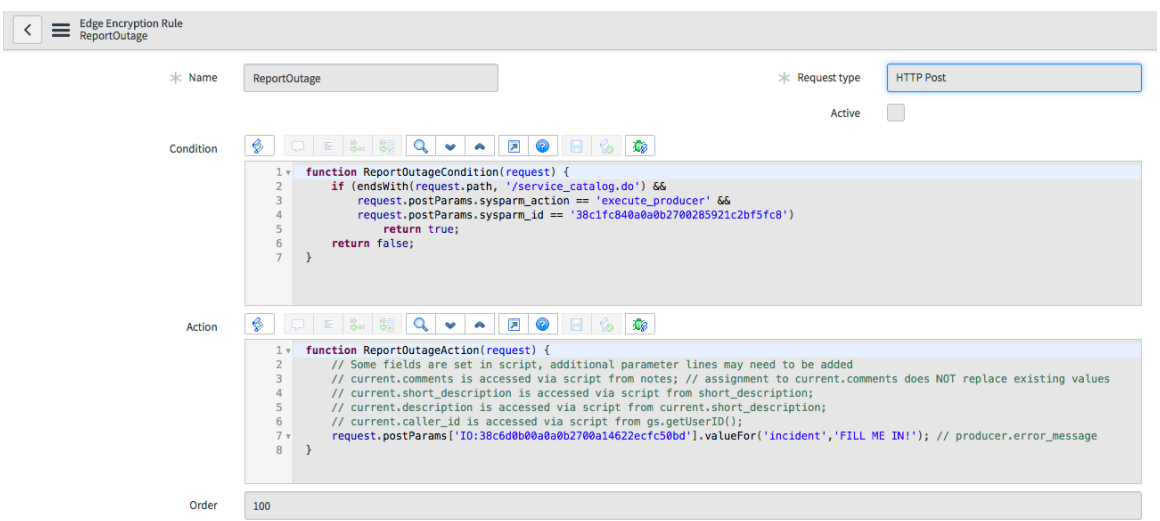
   b. Selon l'endroit où le créateur d'enregistrement sera utilisé, ouvrez la règle de chiffrement associée créée par le créateur d'enregistrement et sélectionnez le marqueur **Actif** .
   Si vous utilisez le créateur d'enregistrement dans le Catalogue de services, activez la règle de chiffrement <RecordProducerName >. Si vous utilisez le créateur d'enregistrement dans , Portail de servicesactivez la règle de chiffrement <RecordProducerName>JSON.

6. **Facultatif :** Examinez le champ **Action** de règle de chiffrement et ajoutez tous les noms de champs ou instructions nécessaires.

   (Optional) Si un créateur d'enregistrement mappe directement une variable à un champ d'une table, la règle de chiffrement mappe automatiquement la variable au champ correct. Toutefois, si une variable est mappée indirectement par le biais de divers scripts sur la plateforme, vous devrez peut-être mettre à jour les règles pour mapper chaque variable au champ approprié.

   Example

   (Optional) La règle de chiffrement ci-dessous a été créée à partir du créateur d'enregistrement Signaler une panne et traite les paramètres POST à partir du Catalogue de services pour mapper les variables aux champs de l'instance. Remplacez « RENSEIGNEZ-MOI » par le champ cible.

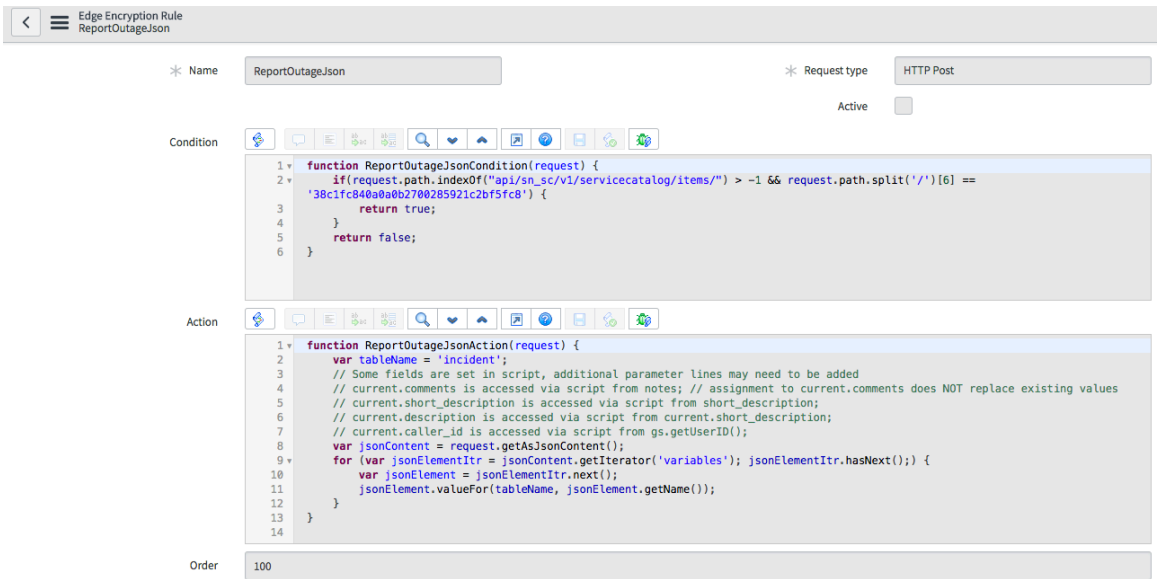


   La règle de chiffrement ci-dessous a été créée à partir du créateur d'enregistrement Signaler une panne et traite une charge utile JSON à partir du Portail de services pour

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

mapper les variables aux champs de l'instance. Ajoutez des instructions supplémentaires pour mapper toutes les variables scriptées aux champs cibles.



Lorsque la charge utile du créateur d'enregistrement est examinée, l'élément error_message contient la valeur du champ short_description. En ajoutant l'instruction suivante, vous pouvez mapper la variable scriptée error_message au champ short_description.

```
if (jsonElement.getName() == 'error_message')
      jsonElement.valueFor(tableName, 'short_description');
```

La valeur du champ **Action** devient :

```
function ReportOutageJsonAction(request) {
 var tableName = 'incident';
 // Some fields are set in script, additional parameter lines may need to be added
 // current.comments is accessed via script from notes; // assignment to current.comments
 does NOT replace existing values
 // current.short_description is accessed via script from short_description;
 // current.description is accessed via script from current.short_description;
 // current.caller_id is accessed via script from gs.getUserID();
 var jsonContent = request.getAsJsonContent();
 for (var jsonElementItr = jsonContent.getIterator('variables'); jsonElementItr.hasNext();) {
  var jsonElement = jsonElementItr.next();
  if (jsonElement.getName() == 'error_message')
   jsonElement.valueFor(tableName, 'short_description');
            } else {
        jsonElement.valueFor(tableName, jsonElement.getName());
 }
}
```

Résultats

Les deux règles de chiffrement permettent au créateur d'enregistrement d'insérer des valeurs dans les champs marqués pour chiffrement à partir de ou Catalogue de servicesPortail de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir une règle de chiffrement personnalisée

Il peut être nécessaire d'identifier et de chiffrer les informations sensibles dans les requêtes HTTP sur le chemin vers votre instance. Vous pouvez écrire des règles de chiffrement pour identifier, interpréter et chiffrer les données dans de telles demandes, en mappant les champs de la demande aux noms de table-champ sur votre instance.

Qu'est-ce qu'une règle de chiffrement ?

Les règles de chiffrement sont des scripts exécutés sur le serveur proxy pour mapper les champs d'une Chiffrement Edge demande aux champs d'une table sur votre ServiceNow instance. Une règle de chiffrement indique au serveur proxy comment chiffrer les Chiffrement Edge données dans des charges utiles personnalisées.

Remarque :
Les règles de chiffrement ne prennent en charge qu'ECMAScript 3 et les versions antérieures.

Quand utiliser des règles personnalisées

Un ensemble de règles de chiffrement est inclus dans le module d'extension Chiffrement Edge . Ces règles gèrent de nombreux cas d'utilisation de la plateforme principale, tels que :

- Modification d'un champ à partir du formulaire de modification de liste
- Mettre à jour un enregistrement à partir du formulaire d'enregistrement
- Gestion du service Web direct
- Traitement des données de l'interface de programmation (API) de l'application REST

Les applications créées à l'aide de formulaires et de listes standard doivent fonctionner sans règles de chiffrement personnalisées.

Si vous développez des scripts qui contiennent des données qui doivent être chiffrées, créez des règles de chiffrement pour trouver et mapper ces données à des noms table-champ Glide. Par exemple :

- Processeurs avec script
- Services Web basés sur un script
- API REST, interfaces utilisateur ou scripts Ajax basés sur un script

Format d'une règle de chiffrement

Les règles comprennent trois parties :

- **Condition** : identifie le type de demande.
- **Action** : mappe les champs de la demande aux champs d'une table, en chiffrant les valeurs qui sont mappées aux champs avec des configurations de chiffrement définies.
- **Ordre** : priorité de la règle. La règle de priorité la plus basse avec une condition satisfaite est la seule règle qui s'exécute. Comme les règles métier, les règles vont du plus bas au plus haut.

À l'exception des demandes de pièces jointes, les demandes HTTP sont évaluées par le Chiffrement Edge serveur proxy. Le Chiffrement Edge serveur proxy évalue toutes les conditions de règle de chiffrement par ordre de priorité jusqu'à ce que toutes les conditions retournent la valeur faux ou qu'une condition renvoie la valeur vrai. Lorsqu'une

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

condition renvoie vrai, l'action est exécutée sur la demande et le résultat est transmis à l'instance. Aucune autre condition n'est évaluée. Par conséquent, les conditions de règle de chiffrement doivent être aussi spécifiques que possible. Une règle générique peut être évaluée comme vraie pour une demande censée être traitée par une autre règle, ce qui entraîne le traitement de la demande par une action incorrecte. Si une condition générique est inévitable, la règle doit être marquée d'une valeur d'ordre élevé afin que des règles plus spécifiques soient évaluées en premier.

Instructions pour la création de règles de chiffrement

La création de règles de chiffrement efficaces et optimisées peut réduire le temps de traitement de la validation des scripts.

Règle générale : Lorsque les règles deviennent longues, faites de votre mieux pour minimiser le nombre de blocages et séparez-les dans la mesure du possible. Idéalement, les règles personnalisées devraient s'appliquer à des cas d'utilisation spécifiques, plutôt que d'englober plusieurs cas, avec des instructions ifs ou switch dans le script d'action.

1. Divisez les règles dans la mesure du possible. Par exemple :
   - Créez différentes règles pour différentes tables et assurez-vous que chaque règle ne s'exécute que sur sa table respective.
   - Créez des règles différentes pour chaque créateur d'enregistrement que vous ciblez, ou au moins pour chaque sous-ensemble de créateurs d'enregistrement. Au lieu d'une règle ciblant des dizaines de sys_ids, vous pouvez créer plusieurs règles différentes ciblant des sous-ensembles plus petits de créateurs d'enregistrements, ou même créer une règle par sys_id.

     Remarque :
     La création de plusieurs règles nécessite plus de maintenance. La contrepartie est que plusieurs règles plus simples peuvent être validées plus efficacement que des règles plus longues et plus complexes.

2. Minimisez le nombre de blocs. Étant donné que le moteur de traitement analyse chaque bloc lors de l'évaluation des scripts, un grand nombre de blocs entraîne des retards dans la validation. Par exemple :
   - Remplacez tous les blocs if par une recherche de tableau, et remplacez tous les blocs de la recherche de tableau par un seul bloc if .
   - Combinez les blocs if chaque fois qu'il est possible de les regrouper.

API de règles de chiffrement

Les règles de chiffrement sont écrites en JavaScript et utilisent Chiffrement Edge des API pour localiser et chiffrer les informations sensibles dans le corps d'une demande. L'API utilise des expressions similaires à xPath pour naviguer dans le contenu JSON et XML.

Chiffrement Edge Les API traitent la demande hors du flux au fur et à mesure qu'elle est écrite dans le flux de sortie. L'analyse de flux permet aux règles de chiffrement d'être performantes sur le réseau. Cependant, la récupération et l'analyse du contenu du corps plusieurs fois peuvent entraîner des résultats inattendus. Pour annuler ce problème potentiel, les demandes doivent être traitées par l'action en une seule passe.

Lors de la création de règles de chiffrement, vous ne pouvez pas utiliser les API Glide, les includes de script, les règles métier ou tout autre paramètre global tel que `actuel`. Étant donné que les règles sont créées pour les objets HTTP, un objet `de requête` globale est disponible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lors de la création de règles de chiffrement, vous ne pouvez pas utiliser les API du gestionnaire de liste d'autorisation ou des applications incluses dans le périmètre.

Gestion des erreurs

Si une condition ou une action de règle de chiffrement lève une exception, consultez le journal du proxy pour obtenir des informations de dépannage.

Inspecter la demande du client

Avant de créer une règle de chiffrement personnalisée, vous devez déterminer le format de la demande client entrant dans le Chiffrement Edge serveur proxy.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Étant donné que les règles de chiffrement itèrent sur les demandes des clients et déterminent ce qui doit être chiffré, le cas échéant, vous devez comprendre le type de demande pour lequel vous créez une règle. Le format de la demande client détermine la structure de votre règle de chiffrement et les API disponibles pour une utilisation dans la règle.

Procédure

1. Inspectez la demande du client.

   Selon la source de la demande, les outils suivants sont disponibles pour inspecter la demande et déterminer le format.

Source de la demande	Outils disponibles
Navigateur client	Utilisez la console développeur de votre navigateur pour inspecter la demande du client. Voici quelques exemples d'outils utiles : ○ Moniteur réseau Firefox ○ Panneau réseau Chrome
Source tierce/externe	Utilisez un analyseur de protocole HTTP pour inspecter la demande. Voici quelques exemples d'outils utiles : ○ Requin filaire ○ HTTP Scoop Vous pouvez également utiliser la documentation de la source externe pour déterminer le format de la demande.

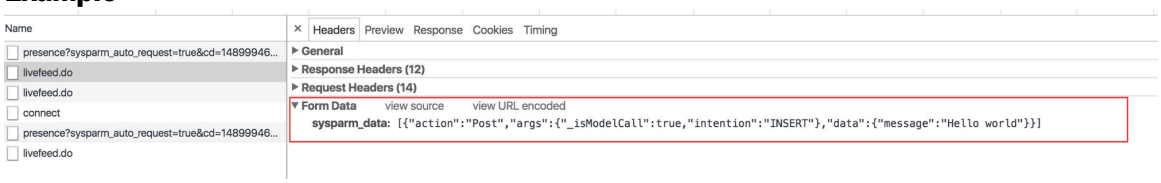
2. À partir de la demande du client, inspectez le paquet et déterminez :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La méthode de demande du client
- Adresse URL de la demande
- Les paramètres d'URL
- Les paramètres de l'auto-test de démarrage (No POST), le cas échéant
- Le format du corps de la demande, s'il est inclus

Example



Résultats
L'inspection de la demande permet de comprendre les champs que vous devez filtrer et itérer dans votre règle de chiffrement. Pour comprendre les champs de l'objet de *`la demande`* , reportez-vous à la section request.

Créer une règle de chiffrement

Les règles de chiffrement sont utilisées par le proxy pour trouver le contenu des requêtes HTTP qui doit être chiffré.

Avant de commencer
Rôle requis : security_admin
Avant de créer une règle de chiffrement, vous devez Inspecter la demande du client déterminer le format.

Pourquoi et quand exécuter cette tâche
Pour créer ou modifier des règles de chiffrement, vous devez être connecté à l'instance via un proxy de chiffrement.

Procédure

1. Accédez à la **Tout** > **Configuration de Chiffrement Edge** > **Règles** > **Créer**.
2. Dans la zone **Nom** , saisissez un nom.
3. Dans le **champ Type de demande**, sélectionnez une méthode HTTP.
   - **HTTP Post**
   - **HTTP Get**
   - **Put HTTP**
   - **Correctif HTTP**
   - **HTTP Delete**

   Remarque :
   Les instances préalables n'autorisentJakarta que les méthodes **HTTP Get** et **HTTP Post** .
4. Dans la zone **Condition** , entrez une instruction JavaScript définissant à quel moment la règle doit s'exécuter.
5. Dans la zone **Action** , entrez une fonction JavaScript à exécuter lorsque la condition est vraie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la zone **Ordre** , entrez la priorité relative de la règle.
7. Cliquez sur **Envoyer** ou enregistrez le formulaire.

Conditions de la règle de chiffrement

Les conditions de la règle de chiffrement déterminent si la règle doit être exécutée.

Une condition de règle de chiffrement doit renvoyer la valeur true si la règle doit gérer la requête HTTP ; sinon, elle doit retourner false.

Lorsque vous créez votre condition, gardez à l'esprit qu'une seule règle est exécutée par demande. Par conséquent, la condition doit être aussi générale ou spécifique que nécessaire pour fonctionner dans les circonstances prévues.

Remarque :
Soyez prudent lorsque vous effectuez des vérifications du contenu de l'état. Des vérifications excessives peuvent être coûteuses pour le serveur proxy et entraîner une latence accrue lors du traitement de demandes complexes.

La condition peut utiliser le type de méthode, le type de contenu, le chemin d'accès URL ou n'importe quel paramètre de chaîne de requête d'URL pour déterminer si la règle doit gérer la demande. La condition a accès à ces champs via l'objet request . Avant de créer une condition de règle de chiffrement, assurez-vous d'avoir inspecté la demande du client et d'avoir compris les conditions requises pour déclencher la règle.

Remarque :
Pour créer des règles efficaces, envisagez des moyens simples d'exclure les demandes que vous ne souhaitez pas voir évaluées par une règle. Construisez votre condition pour qu'elle retourne d'abord la valeur faux pour ces demandes. Cette méthode augmente les performances et achemine rapidement la demande vers la règle appropriée.

Objets de règles de chiffrement et API sont disponibles pour les conditions de règle de chiffrement.

Exemple utilisant path et postParams

```
/*This condition checks if the request coming in has a path ending in
"/sample_processor.do" and if a post parameter exists in that request called myPostParam */

function SampleCondition(request) {
  if (endsWith(request.path, "/sample_processor.do") && request.postParams.myPostParam) {
     return true;
  }
  return false;
}
```

Exemple utilisant urlParams et contentType

```
/* This condition checks if a url parameter exists in the query called
myUrlParam and if the content type contains 'xml'
(if so, you can expect the body to be an XML payload).
Then, it checks if the xml payload contains myXmlTag */

function SampleCondition2(request) {
  if (request.urlParams.myUrlParam && request.contentType.indexOf('xml') > -1 &&
 request.xmlContains('myXmlTag')) {
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    return true;
  }
 return false;
}
```

Actions de règle de chiffrement

Une règle de chiffrement mappe les champs d'une demande client aux champs d'une table de votre instance et identifie les champs marqués pour chiffrement.

Une action de règle de chiffrement s'exécute uniquement lorsque la condition de règle de chiffrement renvoie la valeur vrai. Une règle de chiffrement identifie les données à chiffrer dans la charge utile de votre demande. Étant donné que la règle itère sur le contenu de l'objet de la demande, vous devez comprendre la forme et la structure du corps de votre demande et déterminer ce qui, dans la demande, doit être chiffré. Les données à chiffrer peuvent se trouver à l'intérieur :

- Paramètre POST ou URL.
- Contenu JSON ou XML dans un paramètre POST ou URL.
- Une charge utile JSON .
- Une charge utile XML .

Avant d'écrire une action de règle de chiffrement, assurez-vous de :

- Inspecter la demande du client.
- Identifiez où se trouvent les données sensibles dans l'objet de la demande .
- Déterminez le nom de champ et de table dans lequel insérer des données, ou découvrez comment les extraire dynamiquement de la demande.

Objets de règles de chiffrement et API sont disponibles pour les actions et conditions de la règle de chiffrement.

Objets de règles de chiffrement et API

Utilisez les API de règles de chiffrement pour analyser et chiffrer les valeurs des demandes transitant par le Chiffrement Edge serveur proxy vers l'instance.

Les API disponibles pour votre règle de chiffrement dépendent du format de l'objet de la demande. Par exemple, si le paramètre contentType de l'objet de demande est XML, vous pouvez utiliser la méthode pour API XML analyser et chiffrer les valeurs de la charge utile. Après avoir déterminé le type d'objet dans votre demande, vous pouvez créer une règle de chiffrement à l'aide des API disponibles.

Les API de règles de chiffrement sont disponibles dans les scripts d'action et de condition de règle de chiffrement.

request

L'objet *de demande* est un objet global disponible dans les Chiffrement Edge scripts de règle, d'action et de condition.

L'objet *request* est un objet JavaScript qui représente la demande client entrant sur le Chiffrement Edge serveur proxy. Vous devez créer votre règle de chiffrement pour analyser l'objet de *la demande* , mapper les valeurs de *l'objet de la demande* aux champs d'une table sur l'instance et chiffrer toutes les données sensibles dans l'objet de *la demande* .

L'objet de *demande* inclut les attributs et données suivants de la demande client :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'objet de demande

Champ	Description
chemin d'accès	La partie chemin d'accès de l'URL.
requestMethod (en anglais seulement)	OBTENIR, PUBLIER, METTRE, CORRIGER, SUPPRIMER.
Type de contenu	Le champ d'en-tête Content-Type.
urlParams	Les paramètres de la chaîne de requête. Cela peut également être évalué à une chaîne de caractères.
postParams (en anglais)	S'il s'agit d'une publication de formulaire, elle contient les paramètres de publication.

demande : getAsJsonContent()

Renvoie la demande sous la forme d'un objet itérable de type `JsonNode`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle si le corps de la demande est une charge utile JSON valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de `la demande` .

Une fois la demande renvoyée en tant qu'objet `JsonNode` , vous pouvez utiliser la méthode pour API JSON itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	La demande en tant que `JsonNode` itérable.

demande : getAsXmlContent()

Renvoie le contenu de la demande en tant qu'objet itérable de type `XMLContent`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle si le corps de la demande est une charge utile XML valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de `la demande` .

Une fois que la requête est renvoyée en tant qu'objet `XMLContent` , vous pouvez utiliser la API XML méthode pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renvoie

Type	Description
XMLContent	La demande en tant qu'objet itérable de type `XMLContent`.

demande : XMLContains(chemin d'accès de la chaîne)

Renvoie la valeur true si le chemin d'accès donné existe dans les DOM XML.

Cette méthode n'est disponible que si le corps de la demande est une charge utile XML valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de `la demande` .

Paramètres

Nom	Type	Description
chemin d'accès	Chaîne	XPath que vous recherchez.

Renvoie

Type	Description
Booléen	Indique si le chemin d'accès donné existe dans le DOM XML.

API de paramètres POST et URL

Les paramètres POST et URL sont accessibles en tant que propriétés de l'objet de `la demande` à l'aide de request.postParams et request.urlParams.

Vous pouvez accéder à n'importe quel paramètre unique en tant que propriété des objets `parents postParams` et `urlParams` en appelant request.postParams.myParam. Tout paramètre accessible de cette manière est un objet de la classe `sous-jacente ParameterValue`. Toutes les API de cette classe peuvent être appelées sur n'importe quel paramètre.

Après avoir inspecté la demande client, il peut être nécessaire d'accéder aux valeurs de paramètres de l'objet de la `demande` et de les chiffrer. Selon les données de la demande client, vous pouvez chiffrer des valeurs et les mapper aux champs de l'instance de plusieurs façons.

Chiffrer la valeur d'une table et d'un champ connus

Si vous connaissez le nom de la table d'instance et du champ qui contiendront les données chiffrées, vous pouvez les définir explicitement dans la règle de chiffrement. Par exemple, vous savez peut-être que la demande sera traitée sur l'instance pour créer un incident et vous souhaitez chiffrer le paramètre **de texte** dans le champ de description. Dans ce cas, vous pouvez créer l'action suivante.

```
function SampleAction1() {
   request.postParams.text.valueFor('incident', 'description');
}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chiffrer la valeur d'une table et d'un champ définis dynamiquement

Si, à l'inverse, vous ne connaissez pas le nom du champ que les données chiffrées rempliront, vous pouvez les définir dynamiquement à l'aide de **tableName** et **fieldName**.

L'exemple ci-dessous traite une demande générique susceptible de stocker des données dans différentes tables de tâches (par exemple, incident, problème et change_request) sur l'instance.

```
function SampleAction2() {
   var tableName = request.urlParams.table;
   for (var parameter in request.postParams) {
      var currentParam = request.postParams[parameter];
      var fieldName = currentParam.toString();
      if (fieldName == 'text') {
         currentParam.valueFor(tableName, 'description')
      } else {
         currentParam.valueFor(tableName, fieldName);
      }
   }
}
```

Cette action :

- Obtient la table de destination à partir des paramètres d'URL.
- Itère sur les paramètres de l'URL.
- Demande au serveur proxy de chiffrer tout paramètre d'URL dont le Chiffrement Edge nom correspond à un champ marqué pour chiffrement.
- Recherche un paramètre spécifique appelé *`texte`* et demande Chiffrement Edge au proxy de chiffrer la valeur en fonction de la configuration de chiffrement pour le champ de description dans la table d'incident.

Dans cet exemple, la méthode valueFor() n'effectue en fait aucun chiffrement. Au lieu de Chiffrement Edge cela, la méthode demande au serveur proxy de vérifier si la paire table/champ dans l'objet de la requête est marquée pour le chiffrement avec une configuration de chiffrement et, le cas échéant, de la chiffrer.

Chiffrer JSON ou XML dans un paramètre

Un paramètre POST ou URL peut inclure du contenu JSON ou XML. Dans ce cas, vous pouvez traiter le contenu à l'intérieur du paramètre, itérer sur les valeurs et chiffrer les champs requis. Dans cet exemple, le **tableName** est toujours accessible à partir d'un paramètre POST, mais la valeur du champ est l'objet JSON **data**.

```
function SampleAction3() {
   var tableName = request.postParams.table;
   var data = request.postParams.data;
   var dataIterator = data.getAsJsonContent().iterator();
   while (dataIterator.hasNext()) {
      var jsonElement = dataIterator.next();
      var fieldName = jsonElement.getName();
      if (fieldName == 'text') {
         jsonElement.valueFor(tableName, 'description');
      } else {
         jsonElement.valueFor(tableName, fieldName);
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    }
  }
}
```

Exemple d'une action de règle de chiffrement qui traite XML dans un paramètre POST.

```
function SampleAction4() {
  var tableName = request.postParams.table;
  var data = request.postParams.data;
  var dataIterator = data.getAsXmlContent().getIteratorOverAllChildren();
  while (dataIterator.hasNext()) {
    var jsonElement = dataIterator.next();
    var fieldName = jsonElement.getName();
    if (fieldName == 'text') {
      jsonElement.valueFor(tableName, 'description');
    } else {
      jsonElement.valueFor(tableName, fieldName);
    }
  }
}
```

Chiffrer une requête

Il se peut que vous rencontriez une requête codée dans un paramètre de la demande client qui contient des données sensibles. Pour faire correspondre un champ d'une requête à une valeur chiffrée dans la base de données de l'instance, vous devez créer une règle de chiffrement qui demande au proxy de vérifier si un champ de la requête est marqué pour le chiffrement. La méthode encodedQueryFor() analyse une requête codée dans une table donnée et vérifie si des champs de la requête ont des configurations de chiffrement.

Dans cet exemple, la règle itère sur les paramètres à la recherche du paramètre **de filtre** , qui est censé être une requête codée Glide.

```
function SampleAction5() {
  var tableName = request.urlParams.table;
  for (var parameter in request.postParams) {
    var currentParam = request.postParams[parameter];
    var fieldName = currentParam.toString();
    if (fieldName == 'filter') {
      currentParam.encodedQueryFor(tableName);
    } else {
      currentParam.valueFor(tableName, fieldName);
    }
  }
}
```

Par exemple, si la valeur du **filtre** est : `short_description=Mes informations sensibles^numéro=INC000056^catégorie=Panne`, la requête deviendra `short_description=<Chiffré(Mes informations sensibles)>^numéro=INC000056^catégorie=Panne` sur l'instance.

ParameterValue : toString()

Convertit la valeur du paramètre POST ou URL en chaîne.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	La valeur du paramètre sous forme de chaîne.

ParameterValue : getAsJsonContent()

Renvoie la demande sous la forme d'un objet itérable de type `JsonNode`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle si le corps de la demande est une charge utile JSON valide. Si vous n'êtes pas sûr du format inclus dans le corps de la demande, vérifiez le champ contentType sur l'objet de `la demande` .

Une fois la demande renvoyée en tant qu'objet `JsonNode` , vous pouvez utiliser la méthode pour API JSON itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	La demande en tant que `JsonNode` itérable.

ParameterValue : getAsXmlContent()

Renvoie le contenu de la demande en tant qu'objet itérable de type `XMLContent`.

Cette méthode n'est disponible que dans une Chiffrement Edge règle. Cette méthode suppose que le corps de la demande est une charge utile XML valide. Vous pouvez vérifier le contentType pour vous en assurer.

Une fois que la requête est renvoyée en tant qu'objet `XMLContent` , vous pouvez utiliser la API XML méthode pour itérer sur l'objet et chiffrer les champs.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
XMLContent	La demande en tant qu'objet itérable de type `XMLContent`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ParameterValue : encodedQueryFor(String tableName)

Spécifie que la valeur de l'élément est une requête codée sur la table spécifiée.

L'appel de cette fonction sur un paramètre indique au proxy que la valeur du paramètre est une chaîne de requête codée pour la table spécifiée. Le proxy analyse la requête codée et chiffre les champs de la requête codée qui doivent être chiffrés.

Paramètres

Nom	Type	Description
tableName	Chaîne	Table sur laquelle vous attendez que la requête s'exécute.

Renvoie

Type	Description
nul	

ParameterValue : valueFor(String tableName, String fieldName)

Spécifie que la valeur de l'élément est mappée au champ spécifié dans la table spécifiée.

L'appel de cette méthode sur une valeur d'élément indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Nom du champ.

Renvoie

Type	Description
nul	

API XML

Les API XML peuvent être utilisées après l'appel `getAsXmlContent()` sur l'objet de `requête` ou sur une propriété `ParameterValue` .

Lorsque vous utilisez des API XML pour écrire votre règle de chiffrement, vous pouvez suivre un format général :

1. Appelez `getAsXmlContent()` sur l'objet de `demande` ou la propriété `ParameterValue` . Cela renvoie un objet itérable de la classe sous-jacente `XMLContent` .
2. Appelez `getIterator()` ou `getIterator(String xPath)` sur l'objet `XMLContent` . Cela renvoie un objet `XMLElementIterator` qui peut être utilisé pour itérer sur des éléments XML.
3. Appelez la méthode `hasNext()` sur l'objet `XMLElementIterator` pour déterminer si un autre élément est disponible.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Appelez `next()` sur l'objet `XMLElementIterator` pour retourner l'élément XML suivant. Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`
5. Appelez `valueFor(String tableName, String fieldName)` sur l'élément XML. Cette méthode indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré.

Remarque :
Pour déterminer si vous souhaitez appeler `valueFor(String tableName, String fieldName)` sur un élément XML, vous pouvez utiliser la méthode `getName()` pour renvoyer le nom de l'élément.

Mappage vers une table-champ connue sur l'instance

Dans cet exemple, la charge utile XML sera traitée sur l'instance pour insérer des enregistrements dans la table d'incident. Le champ Description renseignera les short_description sur l'incident.

```
<data>
   <record>
      <name>'Test Record 1'</name>
      <description>'Test Record 1 Description'</description>
      <tag>critical</tag>
   </record>
   <record>
      <name>'Test Record 2'</name>
      <description>'Test Record 2 Description'</description>
      <tag>security</tag>
   </record>
</data>
```

L'action de règle de chiffrement suivante peut s'appliquer :

```
function sampleXmlAction1() {
   var xmlContent = request.getAsXmlContent();
   // This loop iterates over all description tags that match the given path
   var xmlElementIterator = xmlContent.getIterator('data/record/description');
   while (xmlElementIterator.hasNext()) {
      var xmlElement = xmlElementIterator.next();
      xmlElement.valueFor('incident', 'short_decription');
   }
}
```

Cette action parcourt les balises **de description** et demande au serveur proxy de chiffrer les valeurs et de les insérer dans incident.short_description sur l'instance.

Remarque :
Cette règle trouve toutes les balises **de description** dans toutes les balises **d'enregistrement** dans la charge utile XML. S'il n'y a qu'une seule occurrence d'une balise à chiffrer, la règle utilise toujours la structure xPath et l'itérateur. Cependant, il n'itère qu'une seule fois dans la boucle.

Mappage vers une table-champ inconnue sur l'instance

Dans cet exemple, la règle itère sur les balises **d'enregistrement** , mais ne sait pas quelles balises attendre dans la balise **d'enregistrement** . La seule chose que l'on sait est que les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

balises contenues dans les balises **d'enregistrement** correspondent aux noms des colonnes spécifiées dans le paramètre URL de la table.

La règle spécifie également que, si la table est incidente, les données de la balise **de description** doivent être chiffrées et stockées dans le champ short_description de l'instance.

```
function sampleXmlAction2() {
   var xmlContent = request.getAsXmlContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var xmlElementIterator = xmlContent.getIterator('data/record');
   while (xmlElementIterator.hasNext()) {
      encryptFieldsInRecord(xmlElementIterator.next());
   }
}
function encryptFieldsInRecord(xmlElement) {
   //Then, iterate over all tags representing fields in the table
   var fieldIterator = xmlElement.getIteratorOverAllChildren();
   while (fieldIterator.hasNext()) {
      var field = fieldIterator.next();
      var fieldName = childElement.getName();
      //if table is incident, then description is encrypted for the short_description field
      if (tableName == 'incident' && fieldName == 'description') {
         field.valueFor(tableName, 'short_description');
      } else {
         //if table is not incident, ask the proxy to check if the given field is encrypted for the
 given table
         field.valueFor(tableName, fieldName);
      }
   }
}
```

Dans la fonction `encryptFieldsInRecord()`, la méthode `valueFor()` est appelée sur une table et un champ qui sont affectés dynamiquement en fonction de la demande. Même si les noms de table et de champ peuvent changer, la règle demande au proxy de vérifier si le champ de la table doit être chiffré en fonction des configurations de chiffrement définies.

Si le champ n'est pas configuré pour le chiffrement, ou si la balise ne correspond pas à un champ de la table, le proxy ignore cette balise. Si la balise correspond à un champ marqué pour chiffrement, le Chiffrement Edge serveur proxy chiffre la valeur.

Utilisation d'une requête codée

Dans cet exemple, toutes les balises ont l'attribut **filter** , qui indique si la balise contient une requête codée.

```
<data>
   <record>
      <name filter="false">'Test Record 1'</name>
      <description filter="false">'Test Record 1 Description'</description>
      <query filter="true">category=1^name=edge</query>
   </record>
   <record>
      <name filter="false">'Test Record 2'</name>
      <description filter="false">'Test Record 2 Description'</description>
      <query filter="true">category=2^severity=3</query>
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
  </record>
</data>
```

L'action de règle de chiffrement suivante peut s'appliquer :

```
function sampleXmlAction3() {
  var xmlContent = request.getAsXmlContent();
  var tableName = request.urlParam.table;
  // This first iterator will iterate over all record elements
  var xmlElementIterator = xmlContent.getIterator('data/record');
  while (xmlElementIterator.hasNext()) {
     encryptFieldsInRecord(xmlElementIterator.next());
  }
}
function encryptFieldsInRecord(xmlElement) {
  //this time we want to iterate over all tags representing fields in the table
  var fieldIterator = xmlElement.getIteratorOverAllChildren();
  while (fieldIterator.hasNext()) {
     var field = fieldIterator.next();
     var fieldname = childElement.getName();
     //let's look at the filter attribute, if true, then encrypt as encoded query
     if (field.getAttributeValue('filter') == 'true') {
        field.encodedQueryFor(tableName);
     } else {
        //if it is false then check if the field should be encrypted
        field.valueFor(tableName, fieldName);
     }
  }
}
```

Si la valeur de l'attribut de **filtre** est vraie, la règle demande au serveur proxy de chiffrer les valeurs de la requête codée. Si la valeur est faux, la règle demande au proxy de vérifier si le champ doit être chiffré.

XMLContent

Objet global qui fournit des méthodes pour itérer sur le contenu XML.

Vous pouvez accéder à un objet *`XMLContent`* en appelant getAsXmlContent() sur un objet de *`requête`* .

Pour accéder aux données XML d'un paramètre POST ou URL, appelez request.postParams.<parameter name>.getAsXmlContent() ou request.urlParams.<parameter name>.getAsXmlContent().

XMLContent : getIterator()

Renvoie un objet *`XMLElementIterator`* pour le contenu XML.

Paramètres

Nom	Type	Description
Aucun		

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet `XMLContent` .

XMLContent : getIterator(String xPath)

Renvoie un objet `XMLElementIterator` pour le contenu XML en fonction du paramètre spécifié.

Paramètres

Nom	Type	Description
xPath	Chaîne	Expression de type xPath qui spécifie où commencer dans l'objet `XMLContent` .

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet `XMLContent` .

XMLElementIterator

Fournit des méthodes pour itérer sur des éléments XML.

Vous obtenez un objet `XMLElementIterator` en appelant la méthode `getIterator()` de la classe `XMLContent` .

XMLElementIterator : hasNext()

Détermine s'il existe un autre élément disponible.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Booléen	Vrai si un autre élément est disponible.

XMLElementIterator : next()

Renvoie l'élément suivant dans l'itérateur.

Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`

Paramètres

Nom	Type	Description
Aucun		

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Renvoie

Type	Description
XMLElement	L'élément XML suivant.

XMLElement

Fournit des méthodes pour l'itération via des éléments XML et le mappage de valeurs aux champs d'une table.

Vous obtenez un objet `XMLElement` en appelant la méthode `next()` d'un objet `XMLElementIterator` .

XMLElement - getIterator(String xPath)

Renvoie un objet `XMLElementIterator` pour l'élément XML en fonction du paramètre spécifié.

Paramètres

Nom	Type	Description
xPath	Chaîne	Expression de type xPath qui spécifie où commencer dans l'objet `XMLElement` .

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet `XMLElement` .

XMLElement : getIteratorOverAllChildren()

Renvoie un objet `XMLElementIterator` qui inclut tous les sous-éléments de l'élément XML en fonction du paramètre spécifié.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
XMLElementIterator	Objet qui peut être utilisé pour itérer sur des éléments de l'objet `XMLElement` .

XMLElement - valueFor(String tableName, String fieldName)

Spécifie que la valeur de l'élément est mappée au champ spécifié dans la table spécifiée.

L'appel de cette méthode sur une valeur d'élément indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré. Si les noms de table et de champ sont inconnus, vous pouvez appeler la méthode `valueFor()` sur une table et un champ qui sont affectés dynamiquement en fonction de la demande.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Nom du champ.

Renvoie

Type	Description
nul	

XMLElement : encodedQueryFor(String tableName)

Spécifie que la valeur de l'élément est une requête codée pour la table spécifiée.

L'appel de cette fonction sur un élément indique au proxy que la valeur de l'élément est une chaîne de requête codée pour la table spécifiée. Le proxy analyse la requête codée et chiffre les champs de la requête codée qui doivent être chiffrés.

Paramètres

Nom	Type	Description
tableName	Chaîne	Table sur laquelle vous attendez que la requête s'exécute.

Renvoie

Type	Description
nul	

XMLElement : getName()

Renvoie le nom de l'élément.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	Nom de l'élément.

XMLElement : getAttributeValue(attribut String)

Renvoie la valeur de l'attribut spécifié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres

Nom	Type	Description
attribut	Chaîne	Nom d'attribut.

Renvoie

Type	Description
Chaîne	La valeur de l'attribut.

API JSON

Les API JSON peuvent être utilisées après avoir appelé `getAsJsonContent()` sur l'objet de `la demande` ou sur une propriété `ParameterValue` .

Lorsque vous utilisez des API JSON pour écrire votre règle de chiffrement, vous pouvez suivre un format général :

1. Appelez `getAsJsonContent()` sur l'objet de `la demande` . Cela renvoie un objet itérable de la classe sous-jacente `JsonNode` .
2. Appelez `iterator()` ou `getIterator(String xPath)` sur l'objet `JsonNode` . Cela renvoie un objet `JsonNodeIterator` qui peut être utilisé pour itérer sur les nœuds de l'objet JSON.
3. Appelez la méthode `hasNext()` sur l'objet `JsonNodeIterator` pour déterminer si un autre élément est disponible.
4. Appelez `next()` sur l'objet `JsonNodeIterator` pour retourner l'élément JSON suivant. Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`
5. Appelez `valueFor(String tableName, String fieldName)` sur l'élément JSON. Cette méthode indique au proxy que la valeur de cet élément est mappée au champ spécifié dans la table spécifiée. Le proxy vérifie ensuite si le champ doit être chiffré.

> **Remarque :**
> Pour déterminer si vous souhaitez appeler `valueFor(String tableName, String fieldName)` sur un élément JSON, vous pouvez utiliser la méthode `getName()` pour renvoyer le nom de l'élément.

Mappage vers une table-champ connue sur l'instance

Dans cet exemple, la charge utile JSON est traitée sur l'instance pour insérer des enregistrements dans la table d'incidents. Le champ Description renseigne les short_description sur l'incident.

```
{
   data: {
      records: [
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
            "tag": "security"
         },
         {
            "name": "Test Record 1",
            "description": "Test Record 1 Description",
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
            "tag": "security"
         }],
      "query": "assigned_to=3D4860165813e63a00d00abd322244b092^category=vulnerability"
   },
   "source": "10.11.13.14"
}
```

La règle suivante peut s'appliquer :

```
function sampleJsonAction1() {
   var jsonContent = request.getAsJsonContent();
   // This loop iterates over all description elements in the records array
   var jsonNodeIterator = jsonContent.getIterator('/data/records/description');
   while (jsonNodeIterator.hasNext()) {
      var jsonNode = jsonNodeIterator.next();
      jsonNode.valueFor('incident', 'short_decription');
   }
}
```

Cette action parcourt les nœuds **de description** et demande au serveur proxy de chiffrer les valeurs et de les insérer dans incident.short_description sur l'instance.

Remarque :
Cette règle trouve tous les nœuds **de description** dans la charge utile JSON. S'il n'y a qu'une seule occurrence d'un nœud à chiffrer, la règle utilise toujours la structure xPath et l'itérateur. Cependant, il n'itère qu'une seule fois dans la boucle.

Mappage vers une table-champ inconnue sur l'instance

Dans cet exemple, la règle itère sur les **enregistrements**, mais n'est pas sûre des nœuds à attendre. La seule chose que l'on sait, c'est que pour chaque objet des **enregistrements**, les nœuds correspondent aux noms des colonnes spécifiées dans le paramètre URL de la table.

La règle spécifie également que, si la table est incidente, les données du nœud **de description** doivent être chiffrées et stockées dans le champ short_description de l'instance.

```
function sampleJsonAction2() {
   var jsonContent = request.getAsJsonContent();
   var tableName = request.urlParam.table;
   // This first iterator will iterate over all record elements
   var jsonNodeIterator = jsonContent.getIterator('data/records');
   while (jsonNodeIterator.hasNext()) {
         encryptFieldsInRecord(jsonNodeIterator.next());
   }
}
function encryptFieldsInRecord(jsonNode) {
   //this time we want to iterate over all nodes
   var fieldIterator = jsonNode.iterator();
   while (fieldIterator.hasNext()) {
         var field = fieldIterator.next();
         var fieldname = childElement.getName();
         if (fieldName == 'description') {
            field.valueFor(tableName, 'short_description');
         } else {
            field.valueFor(tableName, fieldName);
         }
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    }
}
```

Dans la fonction *encryptFieldsInRecord(),* la méthode *valueFor()* est appelée sur une table et un champ qui sont affectés dynamiquement en fonction de la demande. Même si les noms de table et de champ peuvent changer, la règle demande au proxy de vérifier si le champ de la table doit être chiffré en fonction des configurations de chiffrement définies.

Si le champ n'est pas configuré pour le chiffrement ou si le nom du nœud ne correspond pas à un champ de la table, le proxy ignore ce nœud. Si le nom du nœud correspond à un champ marqué pour chiffrement, le proxy chiffre la valeur.

Utilisation d'une requête codée

```
function sampleJsonAction3() {
    var jsonContent = request.getAsJsonContent();
    var tableName = request.urlParam.table;
    // This first iterator will iterate over all record elements
    var jsonNodeIterator = jsonContent.getIterator('data');
    while (jsonNodeIterator.hasNext()) {
        var jsonNode = jsonNodeIterator.next();
        if (jsonNode.getName() == 'records')
            encryptRecors(jsonNodeIterator.next());
        else if (jsonNode.getName() == 'query')
            jsonNode.encodedQueryFor(tableName);
    }
}
function encryptRecords(jsonNode) {
    //we iterate over all fields in the node
    var recordIterator = jsonNode.iterator();
    while (recordIterator.hasNext()) {
        encryptFieldsInRecord(recordIterator.next());
    }
}
function encryptFieldsInRecord(jsonNode) {
    //this time we want to iterate over all nodes
    var fieldIterator = jsonNode.iterator();
    while (fieldIterator.hasNext()) {
            var field = fieldIterator.next();
            var fieldname = childElement.getName();
            field.valueFor(tableName, fieldName);
    }
}
```

Dans cet exemple, la règle itère sur les **données**. Au fur et à mesure qu'il trouve des **enregistrements**, il exécute la même logique que dans le deuxième exemple, en itérant sur les champs de chaque nœud. Lorsqu'il trouve le nœud de **requête** , il appelle *encodedQueryFor()* pour chiffrer les valeurs qui doivent être chiffrées dans la requête.

Nœud JSON

Objet global qui fournit des méthodes pour itérer sur le contenu JSON.

Vous pouvez accéder à un objet *JsonNode* en appelant getAsJsonContent() sur un objet de *demande* .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous accédez au contenu JSON à partir d'un paramètre POST ou URL en appelant request.postParms.<parameter name>.getAsJsonContent() ou request.urlParms.<parameter name>.getAsJsonContent().

JSONNode : getIterator(String xPath)

Renvoie un objet *JSONNodeIterator* pour le contenu JSON.

Cette méthode ne peut être utilisée que sur le nœud racine, mais peut être utilisée pour parcourir profondément l'objet JSON. Les traversées suivantes doivent utiliser la méthode *iterator().*

Paramètres

Nom	Type	Description
xPath	Chaîne	Une expression xPath.

Renvoie

Type	Description
Itérateur JsonNodeItérateur	Objet qui peut itérer sur les nœuds de l'objet JSON.

JSONNode : itérateur()

Renvoie un objet *JsonNodeIterator qui itère* sur tous les nœuds enfants du nœud actuel.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Itérateur JsonNodeItérateur	Objet qui peut itérer sur les nœuds de l'objet JSON.

JsonNode : getAsString()

Renvoie la valeur du nœud actuel sous forme de chaîne.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	La valeur actuelle du nœud.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

JsonNode : getAsString(String propertyName)

Renvoie la valeur de chaîne de la propriété spécifiée.

Paramètres

Nom	Type	Description
propertyName	Chaîne	Nom de la propriété.

Renvoie

Type	Description
Chaîne	Valeur de la propriété.

JsonNode : getName()

Renvoie le nom du nœud JSON actuel.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Chaîne	Nom du nœud JSON actuel.

JsonNode : valueFor(String tableName, String fieldName)

Spécifie que la propriété JSON est mappée au champ spécifié dans la table spécifiée.

L'appel de cette méthode sur une propriété JSON indique au proxy que la valeur de cette propriété est mappée au champ spécifié dans la table spécifiée. Le proxy décide ensuite si le champ doit être chiffré. Si les noms de table et de champ sont inconnus, vous pouvez appeler la méthode `valueFor()` sur une table et un champ qui sont affectés dynamiquement en fonction de la demande.

Paramètres

Nom	Type	Description
tableName	Chaîne	Le nom de la table.
Fieldname	Chaîne	Nom du champ.

Renvoie

Type	Description
nul	

JsonNode : encodedQueryFor(String tableName)

Spécifie que la valeur de la propriété JSON est une requête codée pour la table spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'appel de cette fonction sur un nœud JSON indique au proxy que la valeur est une chaîne de requête codée pour la table spécifiée. Le proxy analyse la requête codée et chiffre les valeurs des champs de la requête codée qui doivent être chiffrés.

Paramètres

Nom	Type	Description
tableName	Chaîne	Table sur laquelle vous attendez que la requête s'exécute.

Renvoie

Type	Description
nul	

Itérateur JsonNodeItérateur

Vous obtenez un objet `JsonNodeIterator` en appelant les méthodes `getIterator()` ou `iterator()` de la classe `JsonNode` .

JsonNodeIterator : hasNext()

Détermine s'il existe une autre propriété disponible.

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Booléen	Vrai si une autre propriété est disponible.

JsonNodeIterator : next()

Renvoie la propriété suivante dans l'itérateur.

Vous ne pouvez pas appeler `next()` sans appeler `d'abord hasNext().`

Paramètres

Nom	Type	Description
Aucun		

Renvoie

Type	Description
Nœud JSON	Le prochain `JsonNode`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

print(message de chaîne)

Imprime un message dans le fichier journal de la couche : <répertoire du serveur proxy>/logs/wrapper_<date>.log.

Cette méthode n'est disponible que dans un script d'action Chiffrement Edge de règle.

Paramètres

Nom	Type	Description
message	Chaîne	Message à écrire dans le fichier journal de la couche

Renvoie

Type	Description
nul	

Mots clés interdits

Le Chiffrement Edge proxy valide les scripts de règle de chiffrement avant d'enregistrer la règle. De nombreux mots clés JavaScript ne sont pas autorisés dans les scripts de règle de chiffrement.

Mots clés interdits

Mot clé
__DIR__
__LIME__
__LIGNE__
__parent__
__proto__
Erreur
Eval
getClass
getPrototypeOf
Java
JavaScript
javafx
JavaImporter
charger
loadWithNewGlobal (en anglais seulement)
nouveau
Packages
Objet

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mots clés interdits (suite)

Mot clé
prototype
Exp reg
setPrototypeOf (en anglais seulement)
ce
jeter

Attributs du dictionnaire Chiffrement Edge

Ajoutez des attributs de dictionnaire aux tables et aux champs pour contrôler leur fonctionnement avec Chiffrement Edge.

Pour définir un attribut de dictionnaire sur true, vous devez saisir `attribute=true` dans le champ **Attributs** . Pour ajouter un attribut de dictionnaire à un enregistrement, reportez-vous à Altering tables and fields using dictionary attributes .

Chiffrement Edge exclu [edge_encryption_excluded]

Détermine si le champ est exclu du chiffrement.

Lorsque la valeur est définie sur `vrai`, le champ ou la table ne peut pas être chiffré. Lorsqu'elle est définie sur `faux`, le champ peut être chiffré.

- Valeur : vrai/faux
- Élément cible : champ ou table
- Valeur par défaut : false

Chiffrement Edge activé [edge_encryption_enabled]

Détermine si le champ est éligible au chiffrement via une configuration de chiffrement.

Lorsqu'elle est définie sur `vrai`, le champ est éligible pour le chiffrement. Lorsqu'elle est définie sur `faux`, le champ n'est pas éligible au chiffrement. Étant donné que cet attribut est utilisé par le système et ne peut pas être modifié, il n'est pas affiché pour l'utilisateur.

Remarque :
Cet attribut n'indique pas qu'un champ est chiffré et ne déclenche aucune logique de chiffrement sur le champ. Au contraire, l'attribut détermine la possibilité que le champ soit chiffré par un utilisateur.

- Valeur : vrai/faux
- Élément cible : champ
- Valeur par défaut : true pour les champs de type chaîne

Texte clair de Chiffrement Edge autorisé [edge_encryption_clear_text_allowed]

Détermine si les scripts côté serveur peuvent ajouter des données non chiffrées à une chaîne chiffrée dans le champ pour les actions utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

effectuées via le serveur proxy, ou tout script automatisé côté serveur, tel que les travaux planifiés.

Lorsque la valeur est définie sur `vrai`, l'ajout de données est autorisé. Lorsque la valeur est définie sur `faux`, l'ajout de données n'est pas autorisé.

- Valeur : vrai/faux
- Élément cible : champ
- Valeur par défaut : faux

Séparation de domaine et Chiffrement Edge

Séparation de domaine est pris en charge dans des circonstances limitées avec Chiffrement Edge. Chiffrement Edge permet de chiffrer des données depuis l'environnement du client grâce à l'utilisation de configurations, de règles et de clés spécifiques définies sur le Chiffrement Edge proxy. Le proxy ne prend pas en charge le Chiffrement Edge domaine et ne peut pas prendre en charge les paramètres spécifiques au domaine. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Aucun

- Le champ Domaine peut être présent dans les tables de données, mais il n'existe aucune logique métier pour gérer les données.
- Ce niveau n'est pas considéré comme étant séparé par domaine.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Comment fonctionne Séparation de domaine dans Chiffrement Edge

Chiffrement Edge peut être utilisé lorsque des clés, des configurations et des règles spécifiques au domaine ne sont pas requises.

Information associée

Séparation de domaine pour les fournisseurs de services

Intégration des données avec Chiffrement Edge

Pour intégrer des données tierces à une instance à l'aide Chiffrement Edgede , vous devez acheminer les données via le Chiffrement Edge serveur proxy à l'aide d'intégrations prises en charge. Les intégrations prises en charge utilisent des règles de chiffrement du système de base qui mappent les données de chaque charge utile aux champs d'une table.

Charger des données dans des champs marqués pour chiffrement

Chiffrement Edge ne prend pas en charge l'importation ou l'exportation de données depuis Excel, CSV, XML ou d'autres types de fichiers vers ou depuis des champs avec des configurations de chiffrement définies.

ODBC driver

Chiffrez les demandes et interrogez les données via le Chiffrement Edge serveur proxy à l'aide du pilote ODBC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour en savoir plus : Intégration du pilote ODBC de Chiffrement Edge

MID Server

Vous pouvez configurer l'acheminement des Serveur MID données via un Chiffrement Edge serveur proxy. Cependant, certaines restrictions s'appliquent.

Pour en savoir plus : Intégration du MID Server de Chiffrement Edge

Services Web REST/SOAP

Utilisez les services Web REST/SOAP pour mettre à jour ou récupérer des données d'enregistrement via le Chiffrement Edge serveur proxy.

En savoir plus : Services Web

Service Web JSONv2

Utilisez les API de service Web JSONv2 pour mettre à jour ou récupérer les données d'enregistrement via le Chiffrement Edge serveur proxy. Les règles de chiffrement du système de base prennent en charge les API de récupération et de modification des données.

- Pour insérer un seul enregistrement à l'aide de l'API de modification de données, utilisez les méthodes `insert()` ou `insertMutiple()`.
- Pour insérer plusieurs enregistrements à l'aide de l'API de modification de données, utilisez la méthode `insertMultiple()`.

En savoir plus : JSONv2 Web Service

Pour chiffrer les données provenant d'intégrations tierces personnalisées non répertoriées ci-dessus, créez des règles de chiffrement personnalisées. Voir Définir une règle de chiffrement personnalisée.

Charger les pièces jointes aux enregistrements marqués pour chiffrement

Les pièces jointes peuvent être téléchargées dans des tables avec chiffrement de pièce jointe configuré à l'aide des services Web REST et SOAP.

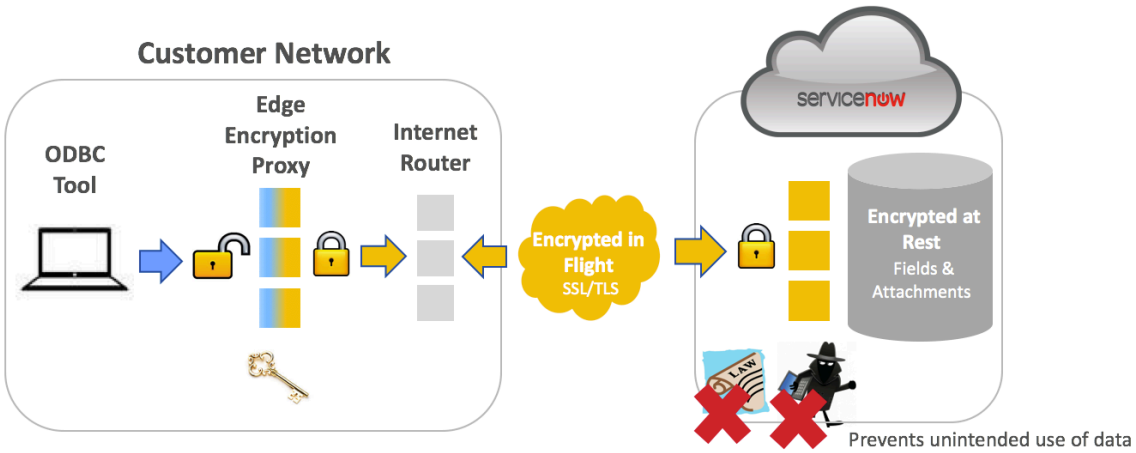
Intégration du pilote ODBC de Chiffrement Edge

Configurez votre pilote ODBC pour interroger les données chiffrées par Chiffrement Edge. Le Chiffrement Edge serveur proxy chiffre les demandes de pilote ODBC vers l'instance ServiceNow lorsqu'il Chiffrement Edge est intégré au pilote ODBC.

Les réponses chiffrées de l'instance sont déchiffrées via le Chiffrement Edge serveur proxy avant d'être transmises au pilote ODBC de votre réseau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pour une intégration réussie, le pilote ODBC doit faire confiance au certificat du Chiffrement Edge serveur proxy. Si le certificat du Chiffrement Edge serveur proxy est signé par une autorité de certification approuvée par le pilote ODBC, le Chiffrement Edge serveur proxy est automatiquement approuvé. Toutefois, si une autorité de certification approuvée par le pilote ODBC n'a pas signé le certificat du Chiffrement Edge serveur proxy, vous devez importer le certificat auto-signé dans le magasin de confiance ODBC.

Importer un certificat auto-signé dans le magasin de confiance ODBC

Si une autorité de certification approuvée par le pilote ODBC n'a pas signé le certificat du Chiffrement Edge serveur proxy, vous devez importer un certificat auto-signé dans le magasin de clés de confiance ODBC. Vous pouvez exporter le certificat à partir Chiffrement Edge du serveur proxy et l'importer dans le magasin de confiance ODBC.

Avant de commencer
Rôle requis : administrateur

Pour déterminer si une autorité de certification approuvée par le pilote ODBC a signé le certificat du Chiffrement Edge serveur proxy, exécutez la commande suivante dans le répertoire keystore du répertoire personnel proxy pour afficher une liste des autorités de certification approuvées par le pilote ODBC :

```
keytool -keystore "<ODBC directory>\ip\Java\jre\lib\security\cacerts" -list
```

Remarque :

Dans la plupart des cas, le client se connecte aux proxys par le Chiffrement Edge biais d'un équilibreur de charge, de sorte que le certificat serait le certificat configuré dans l'équilibreur de charge.

Dans le cas où il n'y a pas d'équilibreur de charge entre le client et le serveur proxy Edge, le certificat est le certificat présenté par le proxy Edge et est configuré dans le *`edgeencryption.properties`* fichier.

```
edgeencryption.proxy.https.port = 9090
edgeencryption.proxy.https.keystore.path = keystore/keystore
edgeencryption.proxy.https.keystore.password = password
edgeencryption.proxy.https.cert.alias = jetty
```

Pour plus d'informations sur la modification des propriétés, consultez Configurer des propriétés supplémentaires dans le fichier de propriétés de Chiffrement Edge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez au répertoire du magasin de clés dans le répertoire de base du proxy.
2. Vérifiez le magasin de clés pour le certificat auto-signé.
   a. Pour vérifier le magasin de clés correspondant au certificat, vous pouvez exécuter la commande suivante pour répertorier tous ses éléments.

      ```
      keytool -list -keystore keystore.jceks -storetype jceks -v
      ```

   b. Localisez l'alias de clé dans la liste des éléments.
3. À l'aide de l'alias de clé, exportez le certificat vers un fichier .cer.

   ```
   keytool -export -alias <key alias> -keystore keystore.jceks -storetype jceks -rfc -file <file name>.cer
   ```
4. Accédez à votre répertoire de magasin de confiance ODBC : ODBC\ip\Java\jre\lib\security\cacerts.
5. Importez le certificat dans votre magasin de clés de confiance ODBC.

   ```
   keytool -keystore cacerts -importcert -alias $<key alias> -file <file name>.cer
   ```

Définir les propriétés du pilote ODBC

Définissez les propriétés du pilote ODBC pour acheminer les demandes via le Chiffrement Edge serveur proxy.

Avant de commencer

Rôle requis : administrateur

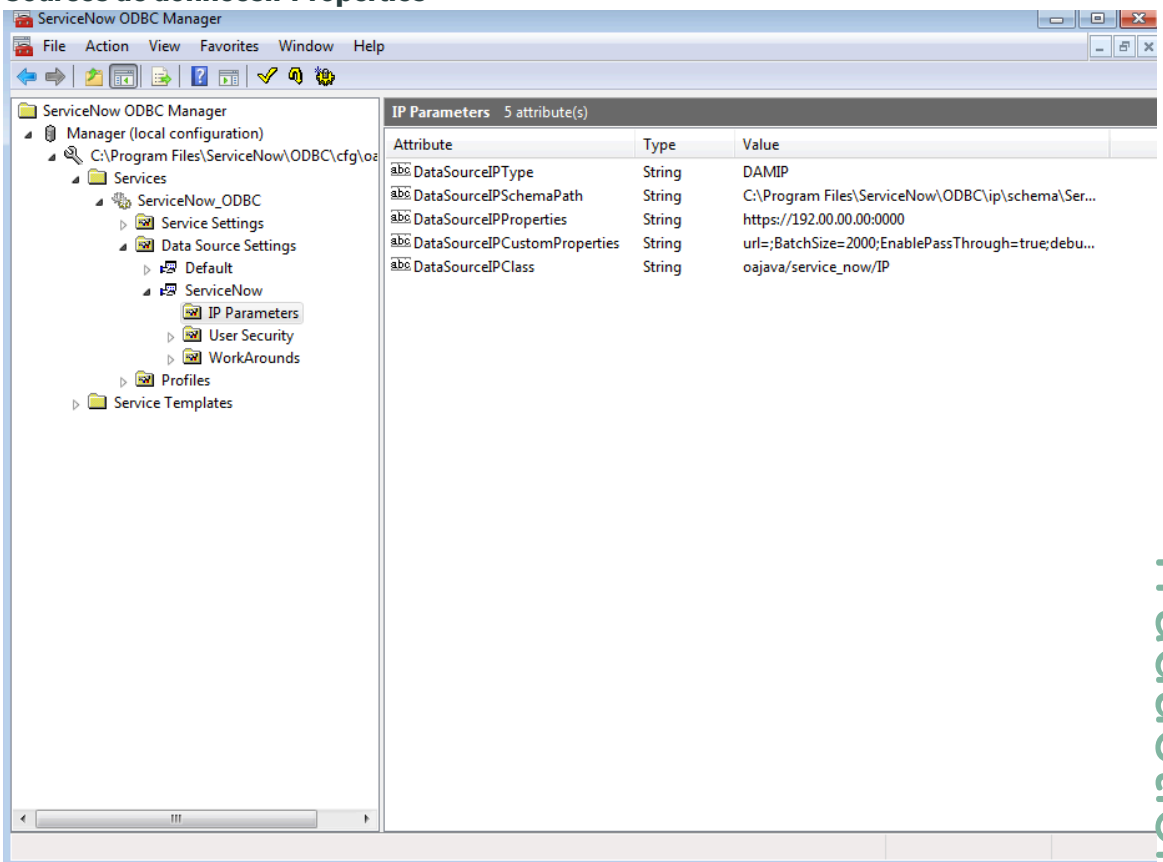
Procédure

1. Sous Windows, accédez à **Début** > **Programmes** > **Console de gestion ODBC ServiceNow**.
2. Développez la racine de l'arborescence de la console comme suit : Gestionnaire ODBC ServiceNow \Gestionnaire\<emplacement d'installation>\Services\ServiceNow_ODBC\Paramètres de source de données\ServiceNow\Paramètres IP.
3. Double-cliquez sur l'attribut **DataSourceIPProperties** .
4. Remplacez la **valeur** par l'URL de votre serveur proxy Chiffrement Edge, par exemple https://<adresse IP> :<port>

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sources de donnéesIPProperties



5. Cliquez sur **OK**.

Que faire ensuite

Le pilote ODBC est maintenant configuré pour acheminer les demandes vers l'instance via le Chiffrement Edge serveur proxy.

Intégration du MID Server de Chiffrement Edge

Configurez le pour acheminer les Serveur MID données via un Chiffrement Edge serveur proxy.

Lorsqu'il Serveur MIDest intégré au , le Chiffrement Edge serveur proxy agit comme le Serveur MIDpoint de terminaison de . Le Chiffrement Edge serveur proxy chiffre et déchiffre ensuite les données transmises entre l'instance et le ServiceNowServeur MIDfichier .

Limitations lors de l'intégration au MID Server

Lorsque Serveur MID les données sont configurées pour transiter par le Chiffrement Edge serveur proxy, les limitations suivantes s'appliquent :

- Le chiffrement des champs de file d'attente ECC n'est pas pris en charge.
- Les données chiffrées ne peuvent pas être utilisées avec Découverte ou Mappage des services.

Pointez le serveur MID vers le serveur proxy Chiffrement Edge

Pour transmettre des Serveur MID données via le Chiffrement Edge serveur proxy, mettez à jour le Serveur MID fichier de configuration pour pointer vers Serveur MID le Chiffrement Edge serveur proxy.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Lors de la configuration du Serveur MID passage via le Chiffrement Edge serveur proxy, vous ne pouvez pas utiliser les propriétés du proxy web dans le Serveur MID fichier de configuration pour acheminer le trafic via le Chiffrement Edge serveur proxy vers votre instance. Au lieu de Serveur MIDcela, vous devez définir le Chiffrement Edge serveur proxy comme point de terminaison de .

Procédure

1. Accédez à votre répertoire local Serveur MID et ouvrez le fichier config.xml .
2. Recherchez l'élément `<parameter name="url » value="https ://YOUR_INSTANCE.service-now.com » />` et remplacez la propriété value par l'URL de votre Chiffrement Edge serveur proxy.
   Par exemple, http://hostname.mycompany.com:8081
   Cette étape demande Serveur MID au serveur proxy de transmettre le Chiffrement Edge trafic au serveur proxy plutôt qu'à l'instance. À son tour, le Chiffrement Edge serveur proxy chiffre tous les champs nécessaires et transmet la charge utile à l'instance.
3. Enregistrez et fermez le fichier.
4. S'il est en cours d'exécution, redémarrez le Serveur MIDfichier .

Diagnostics et performances d'Edge Encryption

Surveillez les Chiffrement Edge tendances des performances du serveur proxy et analysez les erreurs générées par le Chiffrement Edge serveur proxy.

Performances du proxy Edge

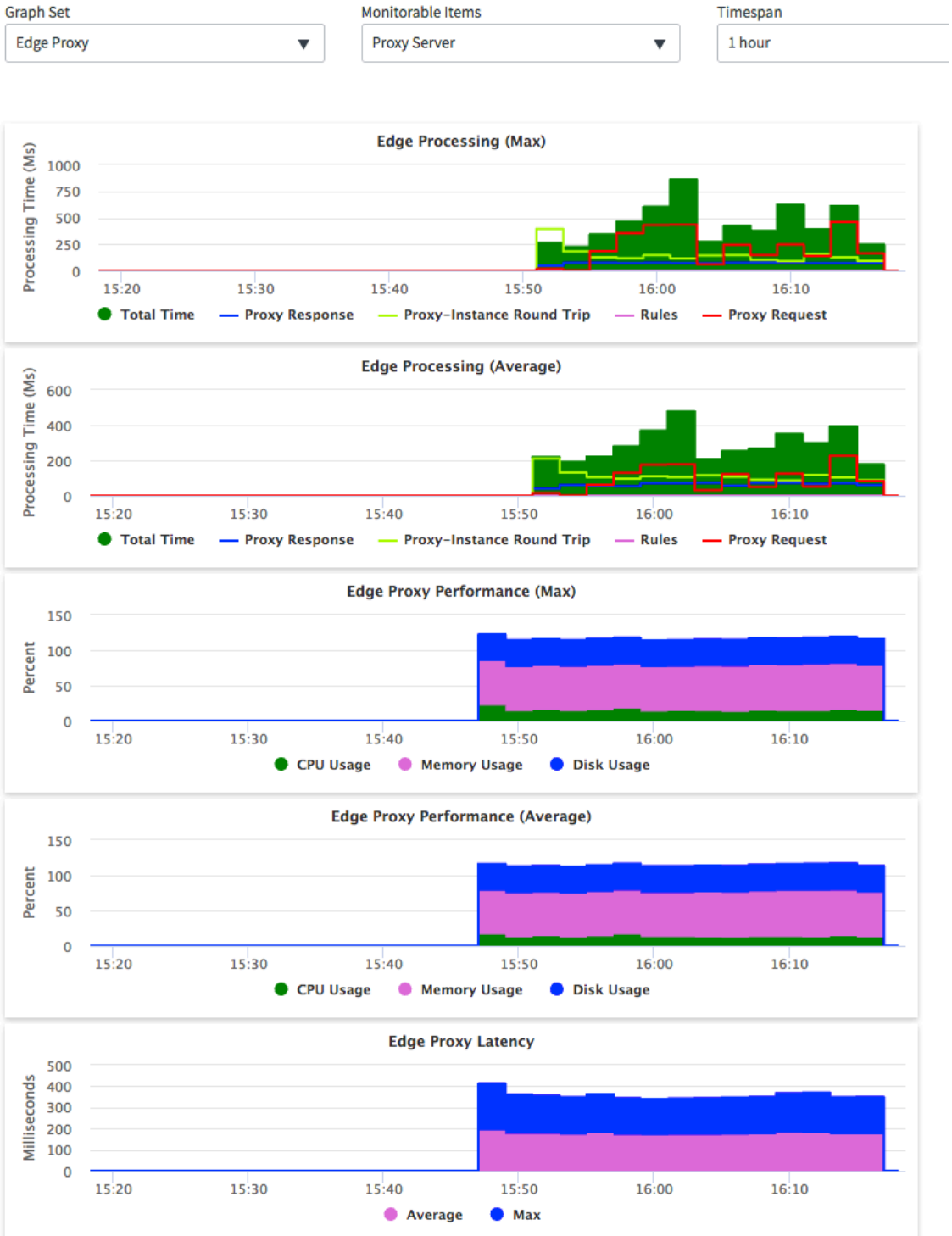
Affichez les principales Chiffrement Edge tendances des performances des serveurs proxy à l'aide du graphique du proxy Edge défini sur la page d'accueil ServiceNow des performances. Les tendances surveillées sont les suivantes :

- Délais de réponse maximaux et moyens entre le client, le serveur proxy et l'instance.
- Utilisation du processeur, de l'espace disque et de la mémoire de l'ordinateur hôte.
- Latence réseau maximale et moyenne entre le serveur proxy et l'instance ServiceNow .

Remarque :
Chiffrement Edge Les serveurs proxy avec des noms en double ne signalent pas les tendances de performance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Traitement Edge (max et moyen)

Délai maximum et moyen, en millisecondes, de traitement d'une demande. Ces points de données sont des tendances générales dans le temps.

- **Temps total** : temps nécessaire pour que le serveur proxy reçoive une demande d'un client et envoie une réponse. Ce point de données est la somme des points de données suivants.
- **Réponse du proxy** : délai de traitement par le serveur proxy d'une réponse de l'instance.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Aller-retour proxy-instance** : temps écoulé entre le serveur proxy et envoie une demande à l'instance et reçoit une réponse. Inclut la latence du réseau entre le serveur proxy et l'instance, ainsi que le temps passé par l'instance à traiter la demande.
- **Règles** : délai accordé au serveur proxy pour évaluer une demande à l'aide de règles de chiffrement définies.
- **Demande proxy** : délai de traitement d'une demande client par le serveur proxy et son transfert à l'instance.

Performances du proxy Edge (maximales et moyennes)

Pourcentage maximal et moyen de ressources utilisées sur l'ordinateur hôte.

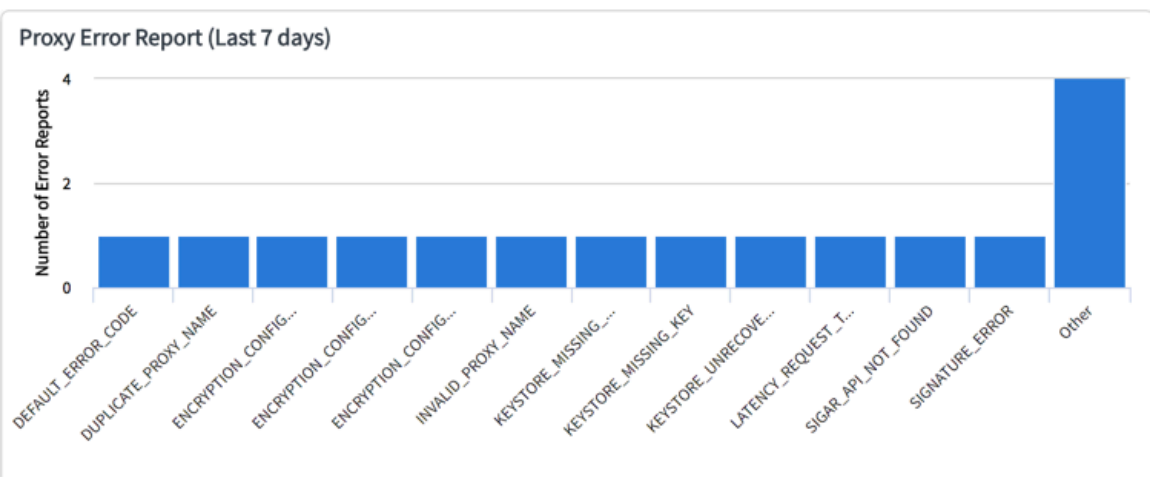
- Utilisation du processeur
- Utilisation de la mémoire
- Utilisation du disque

Latence du proxy Edge

Latence réseau maximale et moyenne en millisecondes à un moment donné. La latence est déterminée par le temps d'aller-retour d'un serveur proxy pour envoyer un simple ping à l'instance et recevoir une réponse.

Rapports d'erreurs de proxy

Accédez à la **Configuration de Chiffrement Edge** > **Diagnostics et dépannage** > **Rapports d'erreurs de proxy** Pour afficher toutes les erreurs de serveur proxy collectées au cours des sept derniers jours.



Les erreurs sont collectées sur une période d'une minute. Chaque minute, un rapport d'erreur est généré. L'axe vertical affiche le nombre de rapports d'erreur au cours des sept derniers jours qui incluent chaque erreur. Par exemple, même si l'erreur DEFAULT_ERROR_CODE est générée plusieurs fois au cours d'une période de rapport d'une minute, la barre de DEFAULT_ERROR_CODE n'atteindra qu'une seule fois sur l'axe **Nombre de rapports d'erreurs** .

À partir de cette vue, vous pouvez :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Cliquez sur la barre de code d'erreur de chaque proxy pour afficher le rapport sur une seule erreur pour chaque serveur proxy. À partir de cette vue, vous pouvez cliquer à nouveau sur la barre pour afficher le texte d'erreur dans la Chiffrement Edge table Stat proxy [edge_encryption_stat]. Suivez les liens dans le texte d'erreur pour afficher plus d'informations et les étapes de rattrapage possibles.
- Cliquez sur **Autre** pour afficher la deuxième page du rapport d'erreurs.

Remarque :
Si vous avez plusieurs serveurs proxy portant le même nom, une seule erreur DUPLICATE_PROXY_NAME s'affiche dans le rapport d'erreur de proxy. Aucune autre erreur n'est signalée pour les serveurs proxy avec des noms en double. Si vous rencontrez cette erreur, assurez-vous que tous les serveurs proxy ont des noms uniques.

Ressources de surveillance supplémentaires

L'instance suit tous les proxys de chiffrement. Chaque Chiffrement Edge serveur proxy s'enregistre au démarrage. L'instance est notifiée lorsque :

- Un nouveau Chiffrement Edge serveur proxy démarre.
- Un Chiffrement Edge serveur proxy est intentionnellement arrêté.

Si un Chiffrement Edge serveur proxy tente de s'enregistrer auprès d'une instance qui n'est Chiffrement Edge pas installée, le proxy ne démarre pas.

Tous les fichiers de configuration de chiffrement sont audités. Les enregistrements supprimés sont audités sur tous les fichiers de configuration de chiffrement. Les enregistrements d'audit sont placés dans la table sys_audit. Pour afficher l'historique d'un enregistrement de configuration spécifique, affichez l'enregistrement, puis cliquez sur **Historique** > **Liste** dans le menu. La tâche de chiffrement en masse n'est pas auditée.

Utilisez les ressources supplémentaires suivantes pour surveiller vos serveurs proxy.

Table	Description
Tentatives d'insertion non valides [sys_edge_encryption_invalid_insert_log]	Liste des tentatives d'enregistrement des données suivantes dans des champs chiffrés : • Données non chiffrées. • Données qui ne proviennent pas d'un Chiffrement Edge proxy. L'instance rejette puis consigne toute tentative d'enregistrement de ces données. Si vous disposez du rôle security-admin, vous pouvez afficher les journaux dans la liste Tentatives d'insertion non valides.
Échecs de tâches [sys_encryption_job_execution]	Liste des tâches qui ne se sont pas exécutées correctement.
Journaux système	L'instance recherche périodiquement les messages provenant de chaque serveur proxy enregistré. Si un serveur proxy n'a pas envoyé de message dans le délai requis, une erreur est enregistrée. Le message du journal contient des informations sur le proxy de chiffrement et la dernière fois que le proxy a envoyé un ping à l'instance. Si l'instance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table	Description
	détermine qu'aucun des proxys de chiffrement n'est en ligne, elle consigne un message. Ces messages sont ajoutés au journal système.

Désactiver ou réduire la collecte de statistiques du proxy Edge

Empêchez le serveur proxy d'envoyer Chiffrement Edge des statistiques Edge Proxy Graph Set à la page d'accueil ServiceNow Performance ou réduisez la fréquence de collecte des statistiques.

Avant de commencer
Rôle requis : admin ou security_admin

Pourquoi et quand exécuter cette tâche
En ajoutant des propriétés dans le fichier de configuration edgeencryption.properties , vous pouvez :

- Désactivez l'ensemble de graphiques du proxy Edge.
- Modifiez l'intervalle pendant lequel les statistiques sont collectées par le Chiffrement Edge serveur proxy. Par défaut, les statistiques sont collectées toutes les 30 secondes.

Procédure

1. Dans le répertoire d'installation de votre serveur proxy, ouvrez le fichier de configuration edgeencryption.properties situé dans le dossier <installation directory>/conf/ .
2. Ajoutez l'un des Propriétés du serveur proxy Chiffrement Edgefichiers .
3. Redémarrez le serveur proxy.

Augmenter la journalisation de débogage pour le Chiffrement Edge proxy

Augmentez le niveau de journalisation pour interpréter les journaux et déboguer les problèmes avec le proxy.

Il existe actuellement trois options pour augmenter la journalisation du débogage dans le Chiffrement Edge proxy. Augmentez le niveau de journalisation pour déboguer les problèmes, fournissez au support technique des informations pour examiner le problème avec l'avantage d'instructions de journal plus détaillées.

Selon le problème en cours de débogage, configurez la journalisation du débogage de l'une des trois façons suivantes :

- Problèmes de débogage autres que la connectivité SSL
- Journalisation des mesures de minutage des demandes via le proxy
- Débogage des problèmes de connectivité SSL entre le proxy Chiffrement Edge et l'instance

Pour tous les tickets de débogage, vous pouvez afficher et interpréter les journaux dans les vôtres ou ouvrir un incident pour obtenir une interprétation de ServiceNow l'assistance technique fournissant la description du problème et la façon dont il est reproduit.

Problèmes de débogage avec l'application autre que la Chiffrement Edge connectivité SSL

Cette méthode vous permet de déboguer les problèmes liés à l'application Chiffrement Edge , sans arrêter ni redémarrer le proxy. Ces étapes augmentent le niveau de journalisation et aident à résoudre le problème de la cause première avec des instructions de journal plus détaillées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Remarque :
Les modifications apportées au fichier $proxy_installation_location/conf/log4j2.properties sont prises en charge par le proxy dans un délai d'environ 60 secondes après que vous ayez effectué vos modifications. Vous n'avez pas besoin de redémarrer les proxys.

Procédure

1. Dans le fichier $proxy_installation_location/conf/log4j2.properties , recherchez la ligne suivante.

```
logger.edge.level=info
```

2. Remplacez la ligne ci-dessus par ce qui suit :

```
logger.edge.level=debug
```

3. Enregistrez le changement.
   La prise d'effet du changement peut prendre jusqu'à 60 secondes, mais cela ne nécessite pas de redémarrage du proxy.
4. Reproduisez votre problème.
5. Recherchez les instructions du journal de débogage liées à l'application dans le fichier $proxy_installation_location/logs/edgeencryption.log ;.

Résultats
Une fois la propriété modifiée, vous pouvez voir des détails supplémentaires dans votre fichier $proxy_installation_location/logs/edgeencryption.log . Lorsque vous avez terminé le débogage, rétablissez la modification apportée au fichier $proxy_installation_location/conf/log4j2.properties .

Journalisation des mesures de minutage des demandes via le proxy

Activez la journalisation des mesures de synchronisation pour ajouter une instruction de mesure pour chaque demande traitée par le Chiffrement Edge proxy. Chacun de ces enregistrements de journal de mesures de minutage contient des informations utiles sur la demande, telles que les délais de traitement et la règle de chiffrement utilisée.

Avant de commencer
Rôle requis : administrateur

Remarque :

Les paramètres de journalisation supplémentaires sont ajoutés au fichier $proxy_installation_location/conf/log4j2.properties . Les modifications apportées sont prises en charge par le proxy dynamiquement dans un délai d'environ une minute après que les modifications apportées au fichier ont été apportées, de sorte que vous n'avez pas besoin de redémarrer les proxys.

Procédure

1. Modifiez le fichier $proxy_installation_location/conf/log4j2.properties en ajoutant les lignes suivantes à la fin du fichier

```
appender.timinglog.type=RollingFile
appender.timinglog.name=TimingLog
appender.timinglog.fileName=../logs/edgenetwork.log
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
appender.timinglog.filePattern=../logs/$
${date:yyyy-MM}/edgenetwork-%d{yyyy-MM-dd-HH}-%i.log.gz
appender.timinglog.layout.type=PatternLayout
appender.timinglog.layout.pattern=%d [%t] %-5p %m%n
appender.timinglog.policies.type=Policies
appender.timinglog.policies.size.type=SizeBasedTriggeringPolicy
appender.timinglog.policies.size.size=500MB
appender.timinglog.strategy.type=DefaultRolloverStrategy
appender.timinglog.strategy.max=4

logger.timing.name=com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache
logger.timing.level=debug
logger.timing.additivity=false
logger.timing.appenderRef.rolling.ref=TimingLog
```

2. Enregistrez le fichier.

Résultats

Une fois le fichier log4j.properties enregistré, les types de messages suivants s'affichent dans le fichier journal $proxy_installation_location/logs/edgenetwork.log pour connaître les délais réseau.

```
2022-07-21 12:56:15,783 [qtp1971991758-7700] DEBUG
 com.snc.edgeencryption.metrics.EdgeEncryptionTimingMetricCache -
 request_uri=/api/now/ui/presencesysparm_auto_request=true&cd=1658433375754
 request_method=POST client_request_received="2022-07-21 12:56:15,015"
 proxy_request_processing_time=6 all_rules_processing_time=0
 rule_executed="REST JSON" rule_execution_time=1 proxy_instance_round_trip=14
 proxy_response_processing_time=1 total_time_from_proxy=21 reponse_code=201
 glide_user=SCv3_1:BAz1ZK7ee9XoroG2nvMlixHpgTvsT4fY2bwQvnH2WdU=:y5HGsTTqo3Pjq6
G0xk4LoazCwCiWRJk4/6SpbXuBzqg=:6816f79cc0a8016401c5a33be04be441
 jsessionid_suffix=037A66
```

Les valeurs des messages du journal sont les suivantes :

```
request_uri: The URI being requested

request_method: The HTTP method being used, for example, GET, POST, PUT, PATCH,
 DELETE

client_request_received: The timestamp noting when the HTTP client request arrived at the
 Edge proxy

proxy_request_processing_time: How long the Edge proxy took to process the request in
 milliseconds

all_rules_processing_time: Total time it took to execute all of the Edge Encryption rules for the
 request in milliseconds

rule_executed: The name of the encryption rule that was executed

rule_execution_time: How long it took to execute listed rule_executed in milliseconds

proxy_instance_round_trip: The time from when the Edge proxy sent the request to the instance
 until the instance sent the response and was received by the edge proxy in milliseconds
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

proxy_response_processing_time: How long the Edge proxy took to process the response in milliseconds

total_time_from_proxy: The total time from when the Edge proxy received the request from the client and returned the response to the client in milliseconds

response_code: HTTP response code

glide_user: The glide_user cookie value

jsessionid_suffix: The JSession cookie suffix associated with the request

Déboguer les problèmes de connectivité SSL entre le Chiffrement Edge proxy et l'instance

Utilisez cette méthode pour déboguer les problèmes de connectivité SSL entre le proxy et votre instance, tels que les Chiffrement Edge échecs d'accès à l'instance via le proxy. Ces étapes augmentent la journalisation et aident à trouver les instructions de journal détaillées.

Avant de commencer
Rôle requis : administrateur

Remarque :
Le débogage de connectivité SSL n'est pertinent que lors de la résolution des problèmes de type de connectivité TLS. Dans la pratique, ce n'est pas courant et rarement nécessaire.

Procédure

1. Arrêtez le serveur proxy.
2. Ajoutez la ligne suivante au fichier $proxy_installation_location/conf/wrapper.conf, qui est une propriété de démarrage Java :

   ```
   wrapper.java.additional.<next available number in sequence> = -Djavax.net.debug=all
   ```

   Par exemple :

   ```
   For example: wrapper.java.additional.4 = -Djavax.net.debug=all
   ```

3. Enregistrez le changement et redémarrez le serveur proxy.
4. Reproduisez votre problème de connectivité.

Résultats
Après avoir reproduit le problème, les instructions du journal de débogage liées à l'échange SSL se trouvent dans le fichier $proxy_installation_location/logs/wrapper_<current date>.log . Lorsque vous avez terminé le débogage. Vous pouvez supprimer ou commenter à distance la connexion supplémentaire en supprimant ou en commentant la ligne créée lors des étapes précédentes.

Chiffrement de la base de données

ServiceNow® propose des méthodes de chiffrement de base de données (DBE) et de chiffrement complet du disque pour les clients ayant des obligations légales en matière de protection des données qui peuvent nécessiter une protection au repos pour toutes les données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :
À partir de cette Washington DC version, Database Encryption ne sera plus disponible. Chiffrement dans le cloud est la solution de remplacement pour le chiffrement des données au repos. Pour plus d'informations, voir Chiffrement dans le cloud avec la gestion des clés

Explorer



Découvrez les principales fonctionnalités et la valeur commerciale de Database Encryption.

Demande



En savoir plus sur la façon de demander la rotation de clé de base de données.

Référence



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le chiffrement de base de données avec commutateur contrôlé par le client (DBE-CCS) est une solution de chiffrement qui chiffre toutes les données au repos lorsqu'elles ne sont pas utilisées dans la base de données.

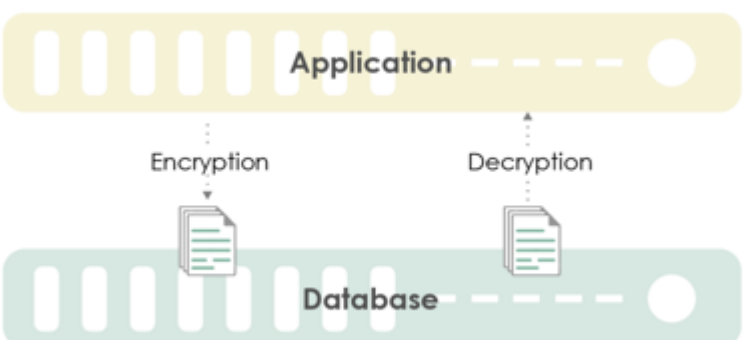
Exploration du chiffrement de base de données

ServiceNow® propose des méthodes de chiffrement de base de données (DBE) et de chiffrement complet du disque pour les clients ayant des obligations légales en matière de protection des données qui peuvent nécessiter une protection au repos pour toutes les données.

Important :
À partir de cette Washington DC version, Database Encryption ne sera plus disponible. Chiffrement dans le cloud est la solution de remplacement pour le chiffrement des données au repos. Pour plus d'informations, voir Chiffrement dans le cloud avec la gestion des clés

Le chiffrement de la base de données permet de protéger toutes les données avec le chiffrement symétrique AES-256, que la base de données soit en ligne ou hors ligne. Du point de Now Platform vue, toutes les données sont déchiffrées.

- Database Encryption prend en charge toutes les données stockées à chiffrer en temps réel, offrant une protection des données en ligne et hors ligne sans perte de fonctionnalité.
- Le chiffrement complet du disque protège les données hors ligne en cas de perte ou de vol du disque.



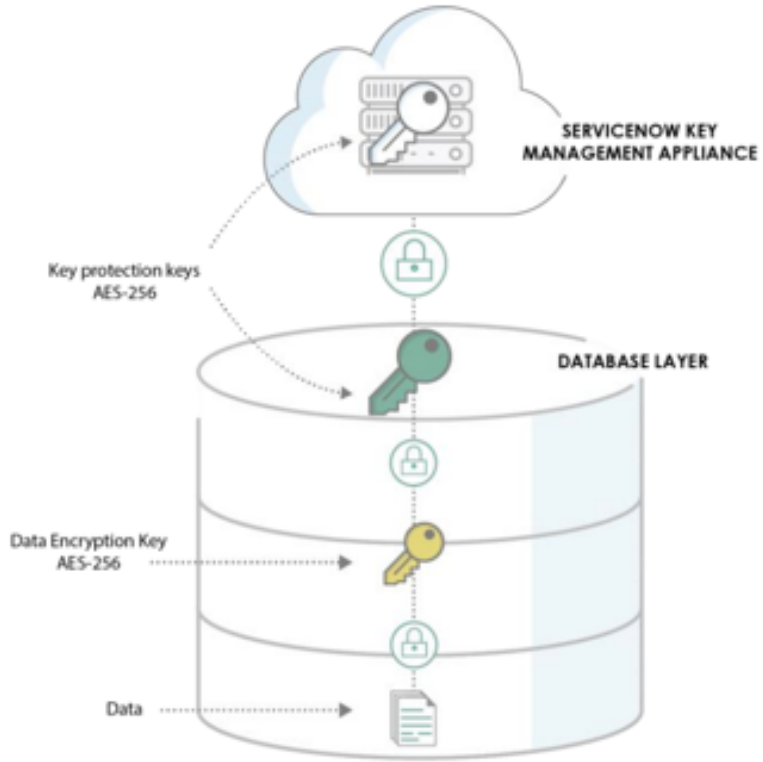
Avec le chiffrement de base de données, toutes les données stockées sont chiffrées et les enregistrements ou tables individuels sont déchiffrés en mémoire lors de l'accès. Les données nouvelles ou modifiées sont chiffrées lorsqu'elles sont saisies dans une table et les fichiers journaux d'activité associés (BIN, REDO, UNDO et Error) sont également chiffrés.

Database Encryption est transparent pour les utilisateurs, sans perte de fonctionnalité. Lors de l'utilisation de cette fonctionnalité, toutes les instances sont chiffrées, ainsi que le trafic de réplication et les sauvegardes. Le clonage d'instance est toujours disponible avec un impact mineur sur les performances pour l'utilisation du chiffrement de base de données jusqu'à 5 %. Les instances nouvelles et existantes sur les versions prises en charge peuvent Now Platform tirer parti du chiffrement de base de données.

Comme illustré, ServiceNow stocke et gère les clés à l'aide d'une hiérarchie de clés à trois niveaux :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



1. Une clé AES-256 spécifique au client est créée par le moteur de base de données et utilisée pour chiffrer les données.
2. Une deuxième clé AES-256 spécifique au client est créée par le moteur de base de données et est utilisée pour protéger la clé de premier niveau.
3. Une troisième clé AES-256 est créée et stockée dans les dispositifs de gestion des clés validés FIPS 140 dans les centres de ServiceNow données. Cette clé protège la clé de deuxième niveau et est unique par instance client.

Il Now Platform prend également en charge le chiffrement de la base de données avec un commutateur fourni par le client, DBE avec CCS. Il s'agit d'une solution de chiffrement qui chiffre toutes les données au repos lorsqu'elles ne sont pas utilisées dans la base de données. Il utilise un cryptage AES standard de l'industrie sans impact sur les fonctionnalités. La base de données chiffre les données au fur et à mesure qu'elles sont écrites sur le disque et les déchiffre au fur et à mesure qu'elles sont lues à partir du disque. Cela signifie que les applications disposent toujours des données dans un état non chiffré pour exécuter la logique et les fonctions nécessaires sans impact.

Remarque :
Le chiffrement de la base de données n'est pas pris en charge pour les instances sur site.

Si vous utilisez vos propres clés pour le chiffrement de la base de données, reportez-vous à la section Chiffrement de la base de données avec commutateur contrôlé par le client.

Demande de rotation de clé de base de données

Effectuez une rotation de la clé de base de données une fois par an ou selon les besoins en soumettant une demande d'assistance.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Important :
À partir de cette Washington DC version, Database Encryption ne sera plus disponible. Chiffrement dans le cloud est la solution de remplacement pour le chiffrement des données au repos. Pour plus d'informations, voir Chiffrement dans le cloud avec la gestion des clés

Pourquoi et quand exécuter cette tâche

La rotation de clé a lieu la nuit dans les 24 heures précédant la date d'expiration et n'interrompt pas le service de l'instance.

Remarque :
Actuellement, la rotation de clés n'est disponible que dans les ServiceNow environnements commerciaux, Government Community Cloud (GCC), France et Singapour.

Procédure

Contact Service et assistance client pour demander l'une des actions de rotation clés suivantes :

- Inscrivez-vous pour effectuer une rotation de clés annuelle sur toutes les instances désignées.
- Obtenir un rapport historique des trois dernières rotations clés contenant les éléments suivants :
  - Nom d'instance
  - Nom et version de la clé.
  - Dates et heures de rotation.
- Planifiez une rotation de clés anticipée en dehors de la rotation annuelle planifiée.

Chiffrement de la base de données avec commutateur contrôlé par le client

Le chiffrement de base de données avec commutateur contrôlé par le client (DBE-CCS) est une solution de chiffrement qui chiffre toutes les données au repos lorsqu'elles ne sont pas utilisées dans la base de données.

Vue d'ensemble

Le chiffrement de la base de données avec commutateur contrôlé par le client utilise le cryptage AES standard de l'industrie, sans impact sur les fonctionnalités. La base de données chiffre les données au fur et à mesure qu'elles sont écrites sur le disque et déchiffrées par la base de données au fur et à mesure qu'elles sont lues à partir du disque. Les applications disposent toujours des données dans un état non chiffré pour exécuter la logique et les fonctions nécessaires.

DBE-CCS utilise une technologie native de la base de données, souvent appelée Tablespace Encryption ou Transparent Data Encryption. Pour plus d'informations sur la technologie, consultez le site Web MariaDB sous « Chiffrement de l'espace de table ».

DBE-CCS vous demande de configurer un point de terminaison de service REST HTTPS qui fournit périodiquement la clé secrète de l'instance ServiceNow . Le point de terminaison CCS renvoie ensuite la clé secrète du client chiffrée avec la clé publique de l'instance de base de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Point de terminaison de client

> **Important :**
> Votre organisation est seule responsable de la configuration et de la maintenance de votre point de terminaison CCS. La spécification de point de terminaison client est fournie dans KB0789788 .

Un ServiceNow partenaire technologique, Fortanix, est à votre disposition pour mettre en œuvre votre point de terminaison client à votre place. Contactez directement le partenaire technologique pour plus de détails sur l'intégration. Pour plus d'informations, reportez-vous à la section Utilisation de Fortanix Data Security Manager avec ServiceNow .

Prise en charge de plusieurs ServiceNow versions

> **Important :**
> Database Encryption est une offre d'infrastructure payante indépendante de la version. Elle peut être appliquée à n'importe quelle version prise en charge, ainsi qu'à des instances nouvelles ou existantes.

Autres références

Reportez-vous à ces références pour plus d'informations sur DBE avec CCS :

Référence	Description
KB0993681	Architecture du commutateur contrôlé par le client de chiffrement de base de données
KB0789788	Guide d'implémentation pour DBE avec CCS

> **Remarque :**
> Pour accéder aux articles de la base de connaissances, vous devez d'abord vous authentifier dans Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Gestion des accès

Gestion d’accès vous permet d’accéder à l’instance ServiceNow® en toute sécurité.

Accès zéro confiance



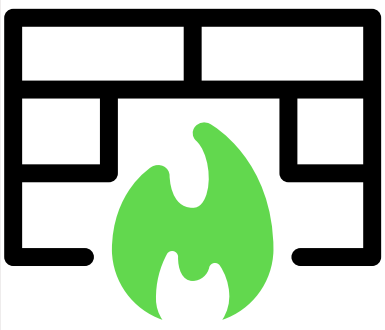
L’accès zéro confiance garantit que tous les accès aux applications et aux données sont accordés sur la base du moindre privilège, uniquement après vérification de l’identité de l’utilisateur et évaluation des risques.

Séparation en domaines



Avec la plateforme ServiceNow, les fournisseurs de services peuvent accélérer l’intégration de leurs clients, respecter la conformité et protéger leurs données à l’aide de Domain Separation.

Authentification



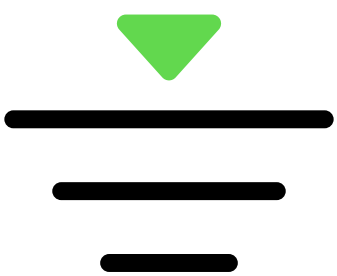
L’authentification de ServiceNow valide l’identité d’un utilisateur qui accède à une instance, puis autorise l’utilisateur à utiliser les fonctionnalités qui correspondent au rôle ou à la fonction de l’utilisateur.

ACL



Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Filtration des données



Utilisez la filtration des données pour contrôler l'accès aux tables et aux enregistrements en fonction des attributs d'objet lors de l'exécution de requêtes de lecture.

Rôles de sécurité



Les rôles de sécurité offrent une sécurité supplémentaire : chaque utilisateur doit avoir au moins un rôle afin que l’instance puisse distinguer les utilisateurs internes des utilisateurs externes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connexions et informations d'identification



Les informations d'identification et de connexion sont nécessaires pour accéder à un ordinateur ou à un appareil réseau pour Découverte, Mappage des services et Gestion cloud, ou pour travailler avec Orchestration.

Contrôle d'accès ServiceNow



Le module d'extension SNC Access Control vous permet de contrôler quels employés du service clientèle et du support technique peuvent accéder à votre instance, et quand.

Accès zéro confiance

L'accès zéro confiance (ZTA) est un modèle de sécurité qui suppose qu'aucun utilisateur ou appareil n'est approuvé par défaut.

Explorer



Activer



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découvrez les fonctionnalités et la valeur commerciale de l’accès Zero Trust.

Découvrez comment activer l’accès Zero Trust.

Configurer



Configurez l’accès zéro confiance.

Référence – Propriétés



En savoir plus sur les propriétés de l’accès Zero Trust.

Traduction automatique

Exploration de l’accès zéro confiance

L’accès zéro confiance (ZTA) est un modèle de sécurité qui suppose qu’aucun utilisateur ou appareil n’est approuvé par défaut.

ZTA garantit que tous les accès aux applications et aux données sont accordés sur la base du moindre privilège, uniquement après vérification de l’identité de l’utilisateur et évaluation des risques.

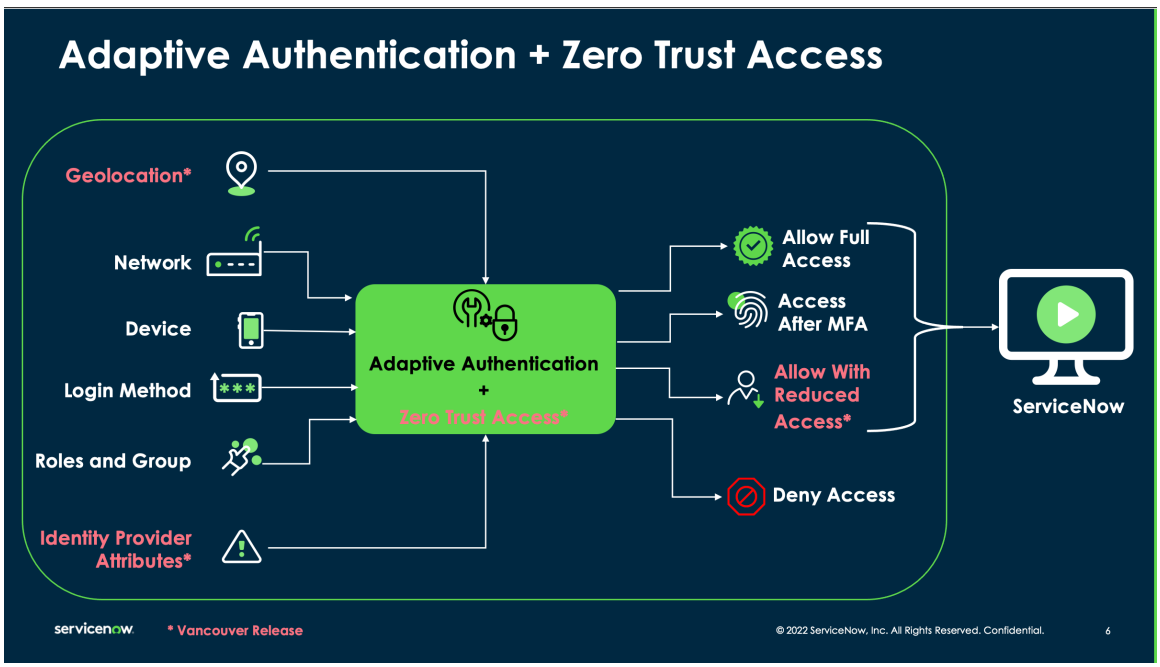
Zéro confiance : accès à la session basé sur des politiques

ServiceNow Zero Trust : accès à la session basé sur des règles (Accès à la session) permet aux organisations de réduire dynamiquement les privilèges des utilisateurs dans une session Web en fonction de divers facteurs, notamment l’adresse IP, l’emplacement, la méthode d’authentification, le rôle de l’utilisateur, le groupe, l’utilisateur disposant de la MFA et les attributs partagés par le fournisseur d’identité (IDP). Cela peut aider à protéger les organisations contre les accès non autorisés et les violations de données, même lorsque des utilisateurs hautement privilégiés accèdent aux applications à partir d’appareils ou d’emplacements non approuvés.

Zéro confiance : accès à la session basé sur des politiques

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Elle permet aux administrateurs de sécurité de réduire ou de limiter l'accès des utilisateurs à une session en fonction de l'adresse IP, de l'emplacement, des attributs du fournisseur d'identité et des attributs de l'utilisateur à l'aide de politiques d'authentification adaptative.



Remarque :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- L'accès à la session ne prend pas en charge les intégrations.
- L'accès à la session n'a aucun impact si le rôle réduit ou limité n'est pas affecté à un utilisateur. Dans ce cas, il n'y a aucun changement apporté à la session de connexion. L'utilisateur continue d'accéder à l'instance avec les privilèges affectés.
- L'accès à la session n'a aucun impact lorsque l'utilisateur est déjà connecté à l'instance et que l'administrateur configure la politique simultanément. L'utilisateur doit se déconnecter de la session pour que la politique soit efficace.
- L'accès à la session n'a aucun impact lorsque l'utilisateur se trouve dans un réseau de confiance et passe ultérieurement à un VPN (changement d'emplacement ou de réseau) au cours d'une session.
- L'accès à la session est appliqué au moment de la connexion. Tout changement des paramètres de risque pendant la session n'entraîne pas de réduction de l'accès. Par exemple, si un utilisateur passe d'un réseau d'entreprise à un réseau non approuvé après avoir établi la session, l'accès ne sera pas réduit, sauf s'il se déconnecte et se reconnecte.

Cas d'utilisation

Voici quelques-uns des cas d'utilisation de l'accès Zero Trust :

- Réduisez les privilèges en fonction du risque associé à la session. Par exemple, un utilisateur ayant un rôle de prestataire se connectant en dehors du réseau approuvé peut être configuré pour avoir uniquement le rôle de demandeur pour la session.
- Réduisez l'accès en fonction de la réponse IdP pour une session utilisateur, si l'utilisateur utilise un appareil non approuvé. Pour plus d'informations, consultez Configurer l'attribut IdP pour l'accès à la session.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Cette relégation de rôle garantit que l'utilisateur n'a pas d'autres privilèges existants dans une session. Lorsque l'utilisateur se connecte à partir d'un réseau approuvé, tous les privilèges existants sont affectés pour une session.

Plusieurs conditions IP et plusieurs affectations de rôle ou de groupe peuvent être définies dans le cadre de la politique.

Accès zéro confiance - Mobile

Vous pouvez utiliser la stratégie Accès zéro confiance - Accès à la session dans la stratégie d'authentification adaptative pour réduire les rôles ou privilèges d'une session particulière sur mobile.

Accès zéro confiance : l'accès à la session mobile peut être activé en activant **glide.authenticate.session_access.mobile.enabled** dans la table des propriétés système.

Pour utiliser l'accès zéro confiance : accès à la session mobile avec les attributs IdP, vous pouvez configurer le champ **glide.authenticate.session_access.mobile.refresh_token_interval** . Cela permet aux administrateurs de contrôler efficacement l'accès à la session en fonction du jeton d'actualisation.

Pour plus d'informations, consultez Configure Zero Trust Access for mobile .

Activation de l'accès zéro confiance

Activez la stratégie de `com.snc.zero_trust_session_access` d'accès à la **session Zero Trust : basé sur des politiques** pour permettre aux administrateurs de sécurité de réduire ou de limiter l'accès des utilisateurs à une session en fonction de l'adresse IP, de l'emplacement, des attributs du fournisseur d'identité et des attributs de l'utilisateur à l'aide de politiques d'authentification adaptative.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module **d'extension Zero Trust - Policy Based Session Access** (`com.snc.zero_trust_session_access`).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration du rôle d'accès à la session

Configurez l'accès à la session pour réduire l'accès des utilisateurs dans une session en fonction de l'adresse IP, de l'emplacement, des attributs du fournisseur d'identité et des attributs de l'utilisateur à l'aide de politiques d'authentification adaptative.

Avant de commencer
Rôle requis : security_admin

Remarque :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- L'accès à la session ne prend pas en charge les intégrations.
- L'accès à la session n'a aucun impact si le rôle réduit ou limité n'est pas affecté à un utilisateur. Dans ce cas, il n'y a aucun changement apporté à la session de connexion. L'utilisateur continuera d'accéder à l'instance avec les privilèges qui lui ont été affectés.
- L'accès à la session n'a aucun impact lorsque l'utilisateur est déjà connecté à l'instance et que l'administrateur configure la politique simultanément. L'utilisateur doit se déconnecter de la session pour que la politique soit efficace.
- L'accès à la session est appliqué au moment de la connexion. Tout changement des paramètres de risque pendant la session n'entraîne pas de réduction de l'accès. Par exemple, si un utilisateur passe d'un réseau d'entreprise à un réseau non approuvé après avoir établi la session, l'accès ne sera pas réduit, sauf s'il se déconnecte et se reconnecte.

Procédure

1. Accédez à la **Tout** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.
2. Pour créer une configuration de rôle d'accès à la session, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire :

Configuration du rôle d'accès à la session

Champ	Description
Nom	Nom de la configuration
Description	Brève description de la configuration.
Politique	Choisissez la politique d'authentification adaptative. Utilisez l'icône de recherche pour afficher la liste des politiques.
Action	**Supprimez les rôles** ou **limitez-les aux rôles**. ○ **Supprimer** rôles : lorsque l'utilisateur configuré se connecte, la liste des rôles fournie dans la liste de rôles ou de groupes est supprimée pour la session. ○ **Limiter aux rôles** : lorsque l'utilisateur configuré se connecte, seuls les rôles sélectionnés sont fournis à l'utilisateur et tous les autres rôles sont supprimés pour la session.

Traduction automatique

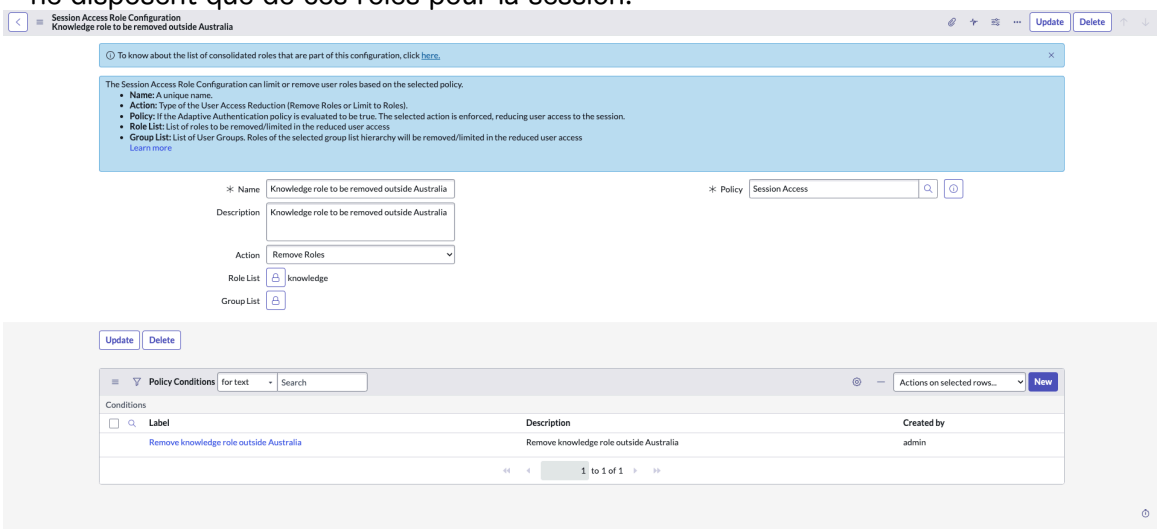
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Liste de rôles	Choisissez des rôles dans la liste des rôles.
Liste de groupes	Choisissez les rôles dans la liste de groupes que vous souhaitez supprimer ou limiter à l'utilisateur.

4. Sélectionner, **soumettre**.

   La connexion des utilisateurs en fonction des pays configurés est la suivante :

   - Dans **Supprimer les rôles**, les utilisateurs des pays configurés avec les rôles sélectionnés n'ont plus ces rôles pour la session.
   - Dans **Limiter aux rôles**, les utilisateurs des pays configurés avec les rôles sélectionnés ne disposent que de ces rôles pour la session.



   Pour en savoir plus sur la suppression ou la limitation des rôles pour une session expliquée à l'aide d'un exemple de cas d'utilisation, reportez-vous à la section Tutoriel : Utiliser l'accès zéro confiance.

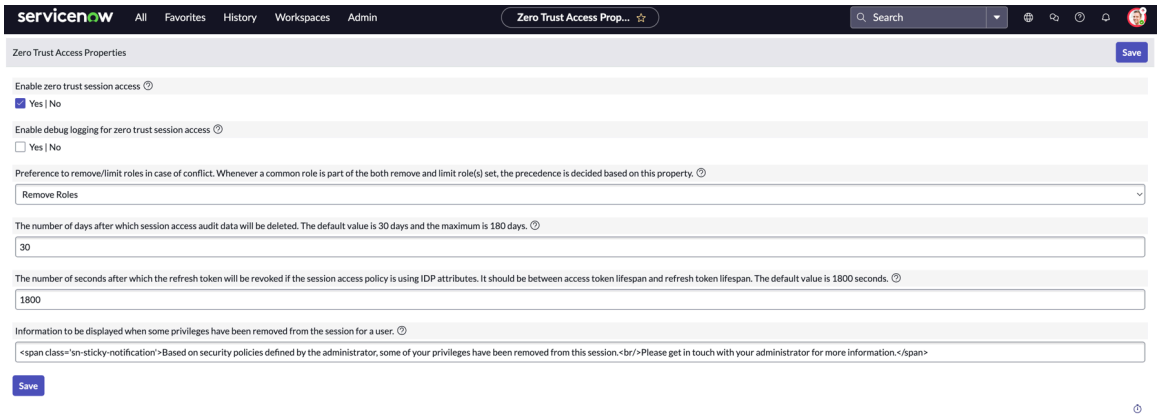
Propriétés système d'accès Zero Trust

Utilisez les propriétés système pour activer et personnaliser l'accès zéro confiance afin de répondre à vos exigences de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés



Propriétés système d'accès Zero Trust

Propriété	Description
Activer l'accès Zero Trust à la session	Option qui permet aux administrateurs d'utiliser la fonctionnalité d'accès à la session Zero Trust. Par défaut, la valeur est faux.
Activer la journalisation de débogage pour l'accès à la session Zero Trust	Option permettant d'activer la journalisation de débogage pour l'accès à la session Zero Trust.
Préférence pour supprimer/limiter les rôles en cas de conflit. Chaque fois qu'un rôle commun fait partie d'un ou de plusieurs rôles de suppression et de limite définis, la priorité est définie en fonction de cette propriété.	**Supprimer des rôles** ou **limiter les rôles**
Nombre de jours après lesquels les données d'audit d'accès à la session sont supprimées. La valeur par défaut est de 30 jours et la valeur maximale de 180 jours.	Par défaut, il est de 30 jours.
Nombre de secondes après lesquelles le jeton d'actualisation est révoqué si la politique d'accès à la session utilise des attributs IdP. Il doit être compris entre la durée de vie du jeton d'accès et la durée de vie du jeton d'actualisation. La valeur par défaut est de 1 800 secondes.	Par défaut, il s'agit de 1800 secondes.
Informations à afficher lorsque certains privilèges ont été supprimés de la session pour un utilisateur.	Description que vous souhaitez afficher à vos utilisateurs concernant la limitation ou la suppression des privilèges. Description de l'exemple : Selon les politiques de sécurité définies par l'administrateur, certains de vos rôles ont été supprimés de cette session. Veuillez contacter votre administrateur pour plus d'informations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

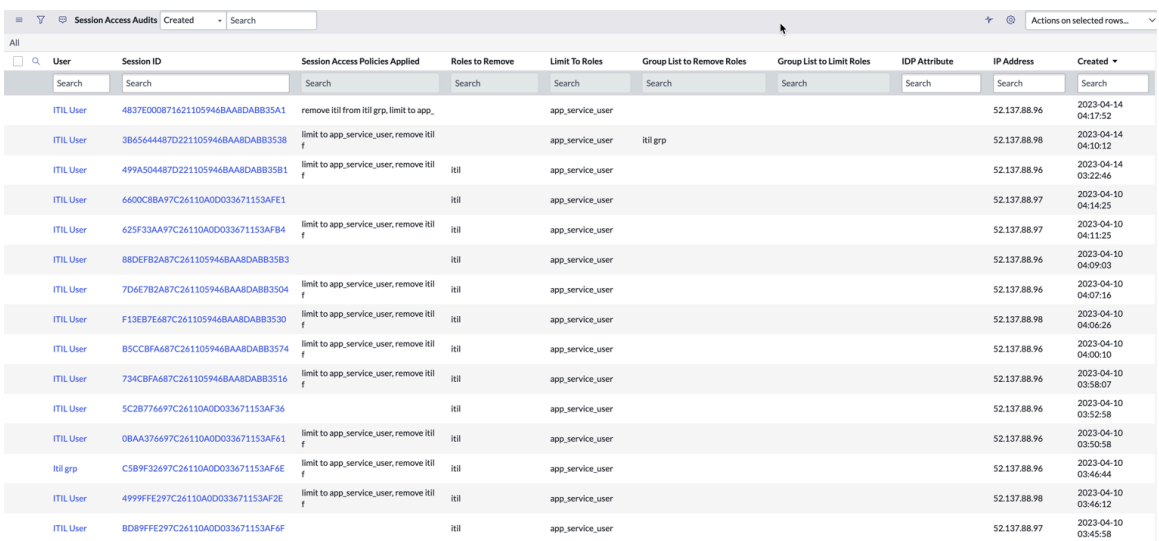
Audits d'accès à la session

Les audits d'accès à la session affichent les journaux d'accès à la session et les informations relatives à la session d'un utilisateur.

Audits

L'audit d'accès à la session affiche les informations d'audit comme suit :

Remarque :
Utilisez la propriété `glide.authenticate.session_access.log_audit_event` pour renseigner les informations de l'audit.



Audits d'accès à la session

Champ	Description
Utilisateur	Détails de l'utilisateur.
ID de session	Détails de la session affichés sous la forme d'un ID unique.
Client mobile	Les détails du client mobile. **ServiceNow Agent** (Now Agent) et **ServiceNow Request** (Now Mobile).
Politiques d'accès à la session appliquées	Politique d'accès à la session appliquée.
Rôles à supprimer	Rôles qui ont été supprimés de l'utilisateur lors de la connexion.
Limiter aux rôles	Rôles qui étaient limités à l'utilisateur lors de la connexion.
Liste de groupes pour supprimer les rôles	Informations sur le groupe qui a supprimé des rôles pour l'utilisateur.
Liste de groupes pour limiter les rôles	Informations sur le groupe qui dispose de rôles limités pour l'utilisateur.
Client mobile	Détails de l'utilisateur connecté via un mobile avec un accès réduit ou supprimé.
Attribut IdP	L'IDP qui a été utilisé pour cette session.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Audits d'accès à la session (suite)

Champ	Description
Adresse IP	Détails de l'adresse IP utilisée par l'utilisateur pour se connecter.
Créé	Détails de la date et de l'heure de l'enregistrement d'utilisateur créé.

Tutoriel : Utiliser l'accès zéro confiance

Procédure d'utilisation de la fonctionnalité d'accès zéro confiance avec un cas d'utilisation de bout en bout.

Avant de commencer
Rôle requis : security_admin

Activez la **propriété Activer l'accès à la session**.

Remarque :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- L'accès à la session ne prend pas en charge les intégrations.
- L'accès à la session n'a aucun impact si le rôle réduit ou limité n'est pas affecté à un utilisateur. Dans ce cas, il n'y a aucun changement apporté à la session de connexion. L'utilisateur continuera d'accéder à l'instance avec les privilèges qui lui ont été affectés.
- L'accès à la session n'a aucun impact lorsque l'utilisateur est déjà connecté à l'instance et que l'administrateur configure la politique simultanément. L'utilisateur doit se déconnecter de la session pour que la politique soit efficace.
- L'accès à la session est appliqué au moment de la connexion. Tout changement des paramètres de risque pendant la session n'entraîne pas de réduction de l'accès. Par exemple, si un utilisateur passe d'un réseau d'entreprise à un réseau non approuvé après avoir établi la session, l'accès ne sera pas réduit, sauf s'il se déconnecte et se reconnecte.

L'accès à la session est une fonctionnalité qui permet aux administrateurs de réduire ou de restreindre dynamiquement un ensemble de rôles pour l'utilisateur, lorsque celui-ci tente de se connecter à l'instance à partir de différents environnements, par exemple une connexion à partir d'un réseau non approuvé, une connexion à partir d'un autre appareil, etc.

L'accès à la session peut être contrôlé par la politique créée et l'action sélectionnée lors de l'exécution de la configuration. Voici quelques-uns des scénarios :

- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Supprimer les rôles**, les rôles sélectionnés et les rôles enfants associés sont supprimés pour l'utilisateur lorsqu'il tente de se connecter à l'instance.
- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Limiter aux rôles**, seuls les rôles sélectionnés et leurs rôles enfants associés sont affectés à l'utilisateur lorsqu'il tente de se connecter à l'instance.

La procédure suivante explique une configuration de bout en bout de la configuration de l'accès à la session en fonction de laquelle le rôle est limité à l'utilisateur qui se connecte à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'instance. De même, vous pouvez également supprimer des rôles en sélectionnant l'option **Supprimer les rôles** lors de la configuration.

Procédure

1. Accédez à la **Tout** > **Accès à la session** > **Configurations du rôle d'accès à la session**.
2. Sur la page Configurations des rôles d'accès à la session, sélectionnez **Nouveau**.
3. Pour limiter tout rôle de l'utilisateur, renseignez les champs suivants du formulaire :
   - Nom
   - Description
   - Politique
   - Action
   - Liste de rôles
   - Liste de groupes

   a. Choisissez **Limiter aux rôles** pour limiter les rôles de l'utilisateur.
   Par exemple, **itil**.

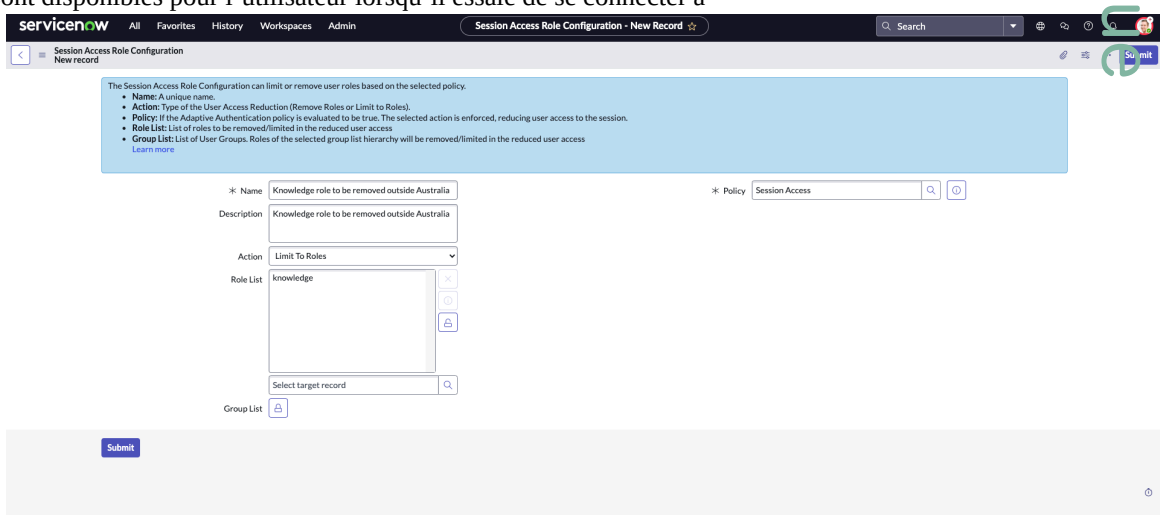
   b. Choisissez un rôle de **la base de connaissances** dans la liste des rôles.

   c. Choisissez la **politique**.

   Vous pouvez créer la politique d'accès à la session à l'aide de politiques d'authentification et de critères de filtre (rôle, groupe, adresse IP, emplacement) avec des entrées et des conditions de politique.

   Utilisez la politique dans la configuration de l'accès à la session. Par exemple, vous souhaitez limiter le rôle (connaissances) à l'utilisateur qui se connecte en dehors de l'emplacement (Australie).

   d. Choisissez Action comme **Limiter aux rôles**.
   Si la politique est définie sur true, seuls les rôles sélectionnés et leurs rôles enfants associés sont disponibles pour l'utilisateur lorsqu'il essaie de se connecter à l'instance.



Traduction automatique

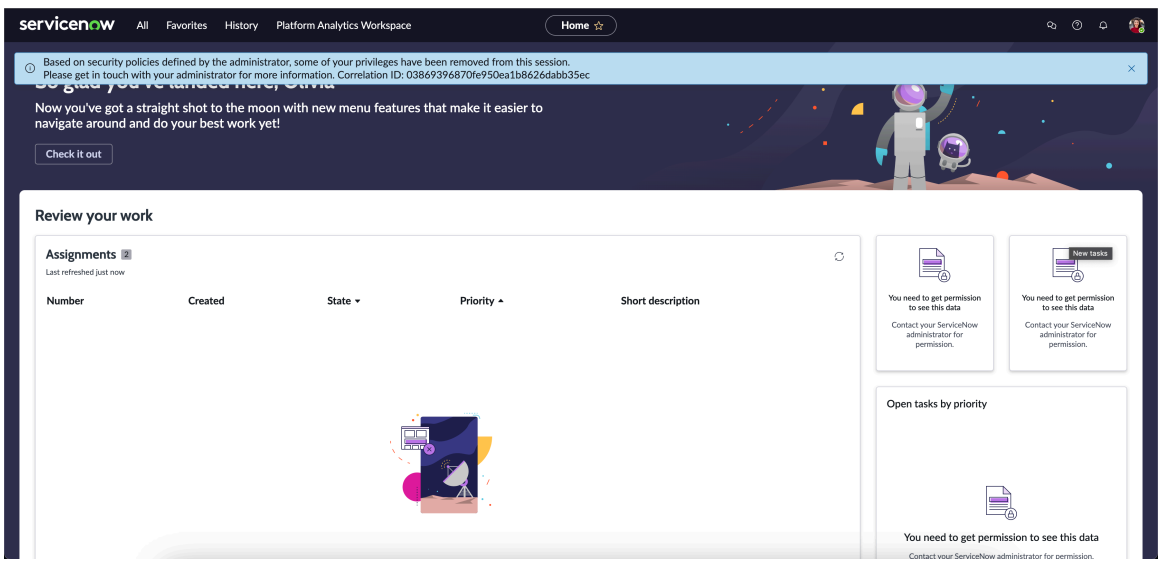
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Sélectionnez **Soumettre**.

De même, vous pouvez choisir le groupe dans la liste des groupes pour restreindre ou supprimer des rôles pour les utilisateurs au sein du groupe.

Lorsque l'utilisateur se connecte à l'instance en dehors de l'Australie, seuls le rôle **Knowledge** et ses rôles enfants associés sont affectés pour la session journalisée et les autres rôles de l'utilisateur sont restreints.

Après s'être connecté, l'utilisateur s'affiche avec le message d'erreur suivant sur la plateforme dans sa section de profil :



L'utilisateur peut contacter les administrateurs et fournir l'ID de corrélation pour enquête.

Remarque :
L'ID de corrélation est l'sys_id de l'enregistrement d'audit correspondant dans la table d'audit d'accès à la session.

Configurer l'attribut IdP pour l'accès à la session

Utilisez l'attribut de fournisseur d'identité (IDP) créé à partir de la réponse SAML (Security Assertion Markup Language) pour supprimer ou restreindre l'accès de session utilisateur à l'instance.

Avant de commencer

Rôle requis : security_admin

Activez la **propriété Activer l'accès à la session**.

Remarque :
Pour utiliser la configuration du rôle d'accès à la session, vous devez élever votre rôle à `security_admin`.

L'accès à la session peut être contrôlé par la politique créée et l'action sélectionnée lors de l'exécution de la configuration. Voici quelques-uns des scénarios :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Supprimer les rôles** ainsi que l'entrée et la condition de l'attribut IdP, les rôles sélectionnés et les rôles enfants associés sont supprimés pour l'utilisateur lorsqu'il tente de se connecter à l'instance.
- Si la politique est définie sur vrai et que l'action des rôles est définie sur **Limiter aux rôles** ainsi que l'entrée et la condition de l'attribut IdP, seuls les rôles sélectionnés et leurs rôles enfants associés sont affectés à l'utilisateur lorsqu'il tente de se connecter à l'instance.

La procédure suivante montre les étapes à suivre pour configurer l'attribut IdP à partir de la réponse SAML, une entrée de politique, pour contrôler l'accès à la session.

Procédure

1. Accédez à la **Tout** > **Accès à la session** > **Configurations du rôle d'accès à la session**.
2. Sur la page Configurations des rôles d'accès à la session, sélectionnez **Nouveau**.
3. Pour supprimer un rôle de l'utilisateur, renseignez les champs suivants du formulaire :
   - Nom
   - Description
   - Politique
   - Action
   - Liste de rôles
   - Liste de groupes

   a. Choisissez **Supprimer les rôles** pour supprimer les rôles de l'utilisateur.
   Par exemple : **itil**.

   b. Choisissez le rôle **itil** dans la liste des rôles.

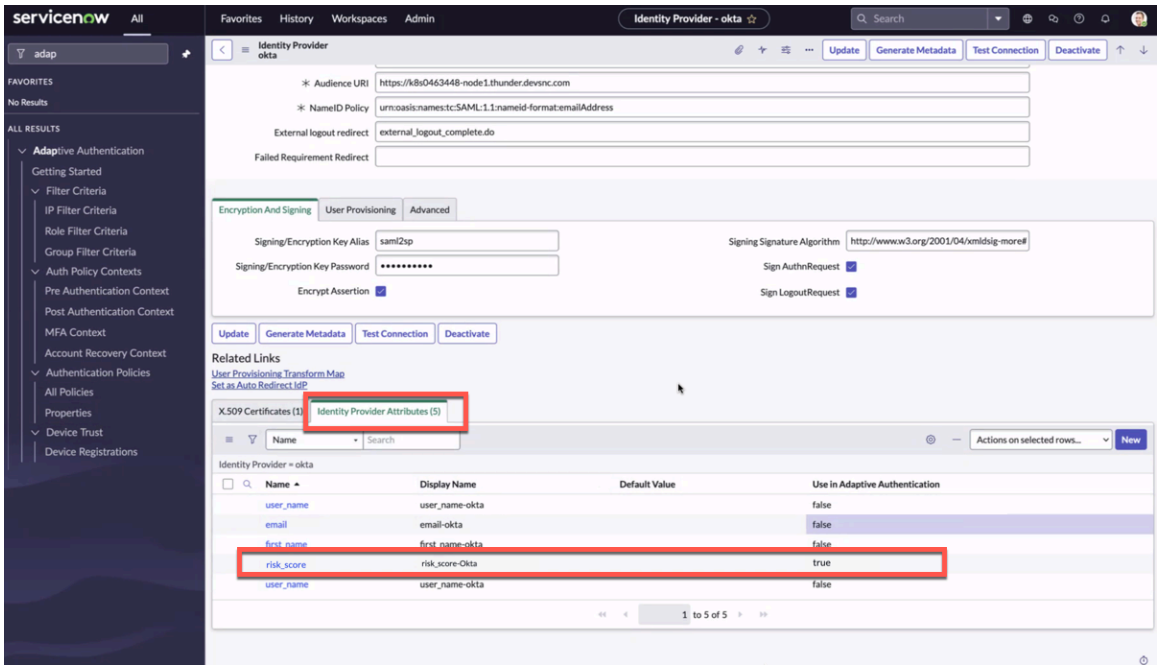
   c. Choisissez la **politique**.
   Pour en savoir plus sur la création de politiques à l'aide de différents critères de filtre à l'aide de la création de politiques d'authentification adaptative, reportez-vous à la section Critère de filtre.

   d. Choisissez Action en tant que supprimer les rôles.
   Si la politique est définie sur vrai et que l'action des rôles est définie sur **Supprimer les rôles**, les rôles sélectionnés sont supprimés pour l'utilisateur lorsqu'il tente de se connecter à l'instance.

   e. Dans l'entrée Politique, créez l'entrée Politique et la Condition de politique.
   Par exemple :
   - **Entrée de politique** : attribut de score de risque d'Okta (IDP).
   - **Conditions de politique** : score de risque de 60 à 80 en tant que condition.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Selon cette configuration, lorsque la valeur de l'attribut de score de risque d'Okta (IdP) dépasse 80, l'utilisateur n'est pas authentifié avec les rôles (**employé**) et ses rôles enfants qui ont été supprimés de l'instance, l'utilisateur est uniquement authentifié avec les autres rôles affectés. Si le score de risque est compris entre 60 et 80, l'utilisateur est authentifié auprès de l'instance disposant de tous les rôles.

Pour plus d'informations sur la création d'une politique de contexte de post-authentification avec des entrées et une condition de politique, reportez-vous à la section Contexte post-authentification.

Remarque :
Si la propriété **Activer l'accès à la session** est inactive, la configuration de l'accès à la session ne restreint ni ne supprime les rôles de l'utilisateur.

f. Sélectionnez **Soumettre**.

Accès zéro confiance pour mobile

L'accès zéro confiance (ZTA) est un modèle de sécurité qui suppose qu'aucun utilisateur ou appareil n'est approuvé par défaut.

Vous pouvez utiliser la stratégie Accès zéro confiance - Accès à la session dans la stratégie d'authentification adaptative pour réduire les rôles ou privilèges d'une session spécifique dans Mobile pour les utilisateurs.

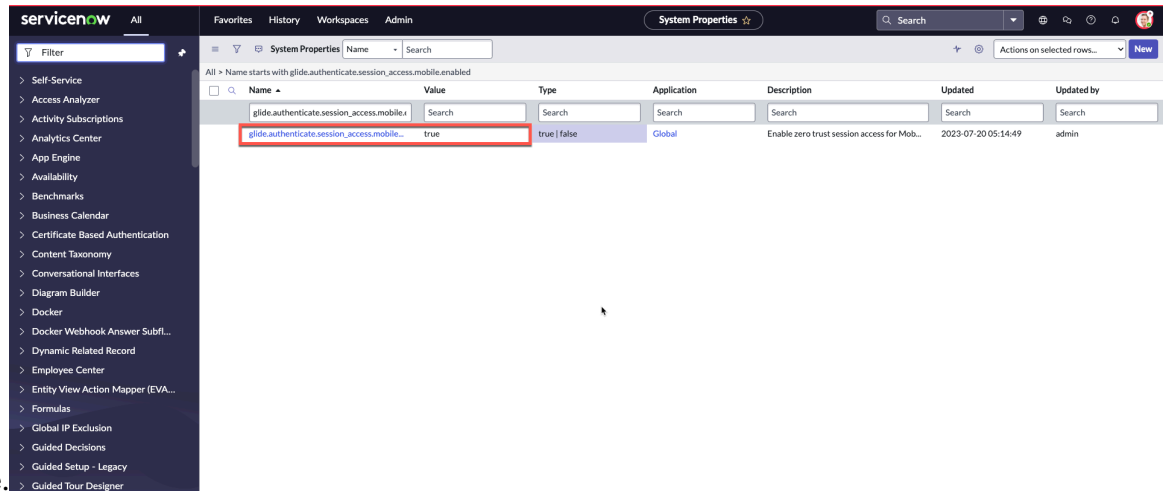
Pour activer l'accès zéro confiance sur mobile, vous devez effectuer les tâches suivantes :

- Les configurations d'accès à la session ne peuvent être effectuées qu'avec security_admin rôle. Vous devez élever votre rôle à security_admin.
- Activez la politique de com.snc.zero_trust_session_access**d'accès à la session Zero Trust : basée sur des politiques**.

Traduction automatique

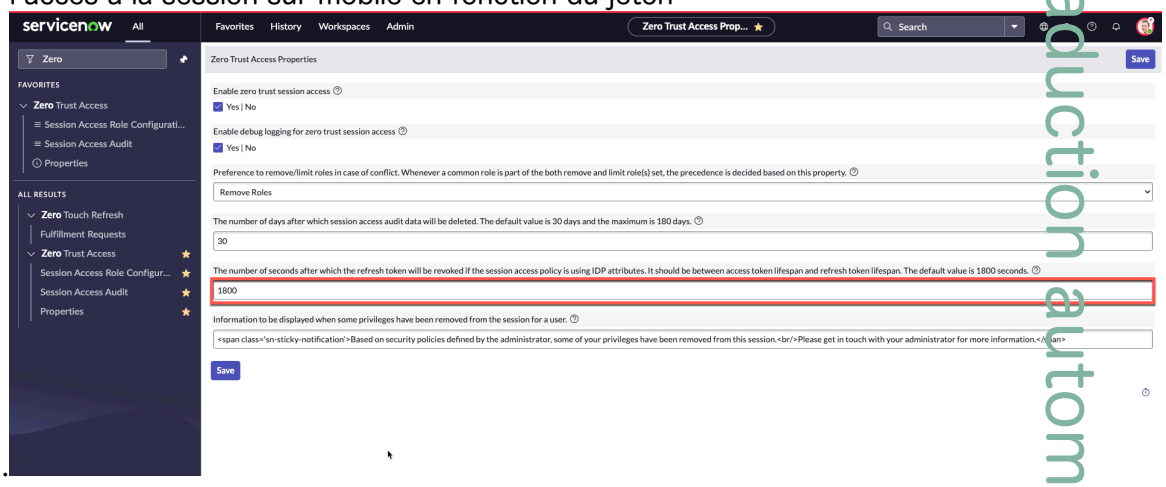
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez le **glide.authenticate.session_access.mobile.enabled** à partir de la table des propriétés



système.

- Configurez le champ **glide.authenticate.session_access.mobile.refresh_token_interval** pour contrôler l'accès à la session sur mobile en fonction du jeton



d'actualisation.

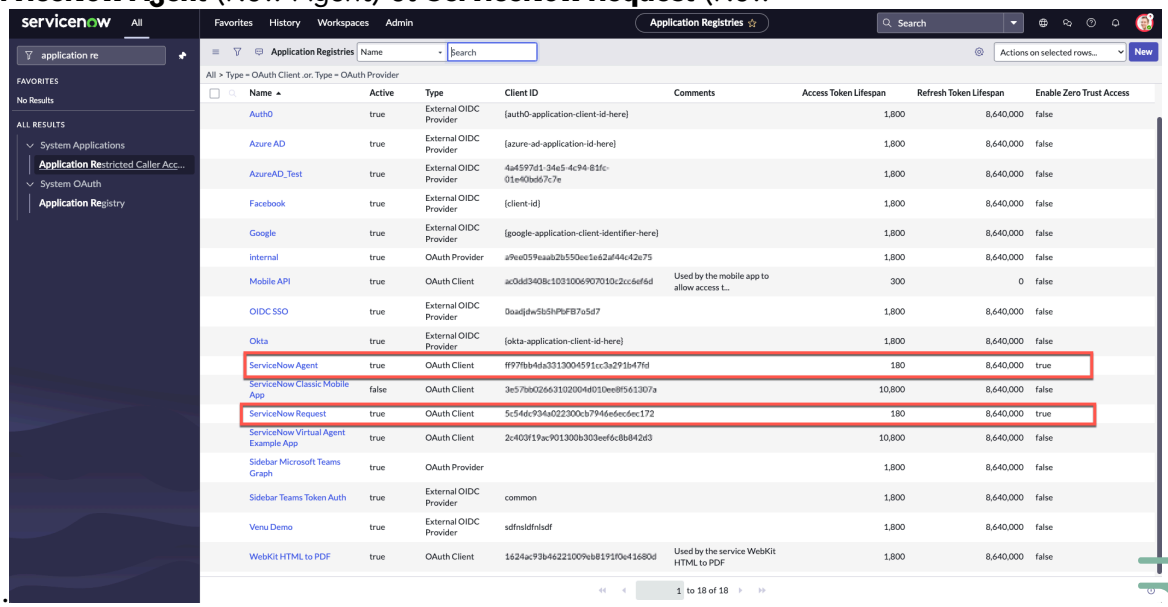
> **Remarque :**
> Vous devez configurer les secondes de jeton d'actualisation lors de l'utilisation d'un IdP pour les connexions à l'application mobile. Par défaut, les utilisateurs sont déconnectés des applications mobiles après 1 800 secondes (30 minutes).

- L'option Activer l'accès zéro confiance est activée sous **Registres d'application** pour l'application cliente mobile (client OAuth). Dans ce

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

cas, **ServiceNow Agent** (Now Agent) et **ServiceNow Request** (Now Mobile).



- Configurez le rôle d’accès à la session pour réduire ou supprimer les rôles pour la connexion des utilisateurs en fonction des entrées et des conditions de la politique. Pour en savoir plus sur la configuration, reportez-vous à la section Configuration du rôle d’accès à la session.

La configuration évalue la connexion pour réduire ou supprimer les rôles des utilisateurs qui accèdent à votre ServiceNow® instance en fonction des filtres et des conditions de politique. Pour plus d'informations, consultez Configure Zero Trust Access for mobile .

Domain Separation pour les fournisseurs de services

Grâce à la plateforme ServiceNow, les fournisseurs de services peuvent offrir à leurs clients une intégration plus rapide, assurer le respect de la conformité et protéger leurs données à l'aide de Domain Separation. Vous pouvez séparer les données, les processus et les rapports clients en groupes logiques appelés domaines. Les fournisseurs de services déterminent qui peut afficher tel ou tel contenu et y accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Explorer



En savoir plus sur Séparation de domaine.

Configurer



Configurez Séparation de domaine.

Référence



Obtenir des détails sur Séparation de domaine.

Analyser



En savoir plus sur l’analyse de Séparation de domaine

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer la séparation de domaine

Avec Séparation de domaine, vous pouvez séparer les données, les processus et les tâches administratives en domaines logiquement définis.

Séparation de domaine est la solution idéale pour les clients qui :

- Nécessité d'appliquer la ségrégation absolue des données entre les entités d'entreprise (séparation des données).
- personnalisent les définitions des processus business et les interfaces utilisateur pour chaque domaine (administration déléguée) ;
- conservent certains processus globaux et des générations de rapports globaux dans une seule instance.
- Séparez les données entre les fournisseurs de service, les clients, les partenaires ou les sous-organisations.
- Présenter des différences de processus mineures ou modérées entre les clients.

Séparation de domaine par rapport à des instances distinctes

Bien que Domain Separation fournisse une prise en charge partagée, le partage est toujours contenu dans une seule instance. Certaines données, propriétés et processus globaux sont partagés dans tous les domaines. Par exemple, le fait que le système *se souvienne de moi* sur la page de connexion du système est global et ne peut pas être spécifié par domaine.

Si vous avez besoin d'une séparation complète et totale de toutes les propriétés système et que vous n'avez pas besoin de rapports globaux ou de processus globaux, des instances distinctes constituent la meilleure option.

Séparation des données

Les membres d'un domaine ne voient que les données contenues dans leur domaine ou les domaines enfants qui se trouvent plus bas dans la hiérarchie de domaine. Par défaut, tous les utilisateurs et tous les enregistrements sont membres du domaine global, sauf si un administrateur les affecte à un domaine particulier. Une fois que vous avez affecté un utilisateur ou un enregistrement à un domaine, l'instance compare le domaine de l'utilisateur au domaine de l'enregistrement pour déterminer si l'utilisateur peut afficher l'enregistrement.

Les applications ServiceNow sont définies avec les niveaux de prise en charge incrémentielle suivants. Ces niveaux sont basés sur la perspective des cas d'utilisation et des profils réels.

Séparation des données : les locataires ne voient que les données qu'ils ont l'autorisation de voir. Les locataires peuvent avoir accès à d'autres données de locataire, mais ne peuvent pas interroger les données des locataires s'ils n'y ont pas accès.

Séparation de l'interface utilisateur : prend en charge une expérience spécifique au locataire pour les éléments de l'interface utilisateur tels que les vues, les listes, les étiquettes, et autres.

Séparation de la logique métier : vous pouvez créer des politiques système spécifiques au locataire, telles que des notifications par e-mail, des règles métier, des scripts clients, une politique d'interface utilisateur et des actions d'interface utilisateur.

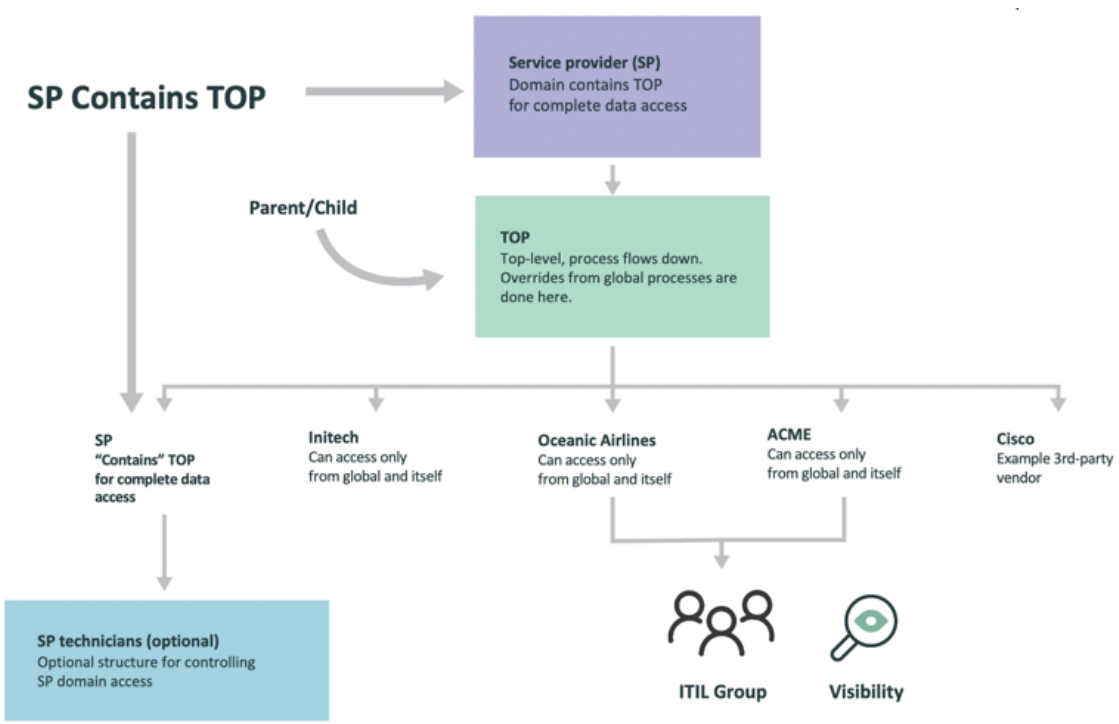
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modélisation hiérarchique : imbriqué multi-tenant afin que les locataires parents puissent accéder aux ressources des locataires enfants. La logique métier pour les locataires parents s'exécute automatiquement pour les locataires enfants et peut être remplacée à n'importe quel niveau.

Intelligence entre locataires (champ d'application de domaine) : gère automatiquement les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires qui ont accès à des données de locataire supplémentaires.

En général, les données définies à un niveau supérieur de la hiérarchie de domaine ne sont pas visibles aux niveaux inférieurs de la hiérarchie.



Migration du chemin de domaine

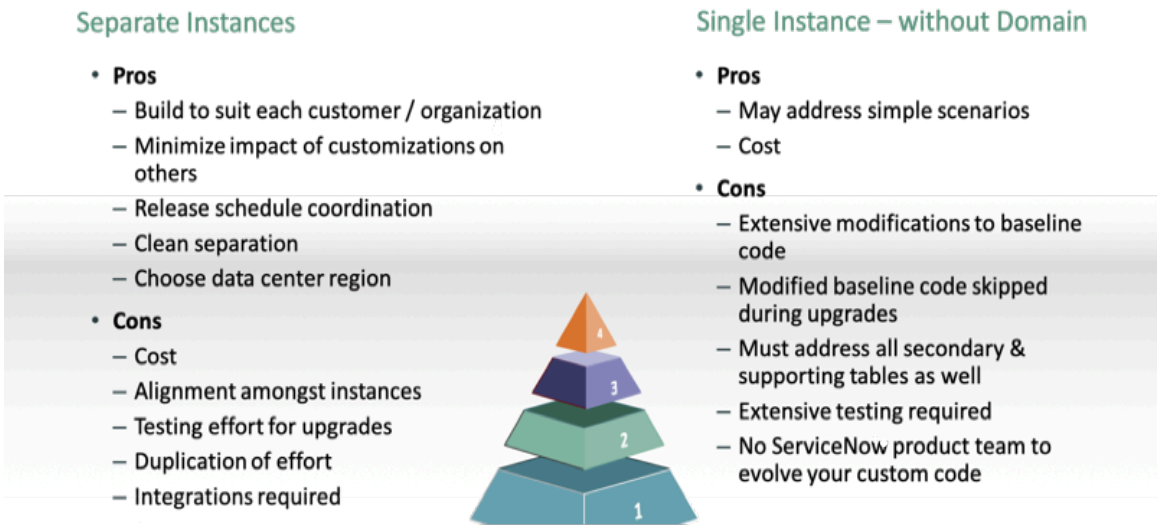
Les chemins de domaine sont utilisés pour tous les clients. La numérotation de domaine n'est pas utilisée. Service et assistance client peut vous aider dans la mise à niveau.

Alternatives à Domain Separation

Les instances distinctes constituent une alternative courante à la séparation de domaine. Cela offre un grand degré de flexibilité pour répondre aux exigences des clients et des parties prenantes avec peu ou pas d'impact sur les autres.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



⚠ Avertissement :
Avant d'activer Séparation de domaine, consultez votre représentant pour vérifier qu'elle est adaptée à votre environnement. Séparation de domaine ajoute un niveau de surcharge d'administration. Bien qu'il puisse être désactivé, il ne peut pas être supprimé d'une instance.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Module d'extension Domain Separation

Configuration pouvant être déléguée à des clients internes ou externes

L'application Séparation de domaine est conçue pour donner ServiceNow® aux fournisseurs de services (SP) la possibilité de configurer les services qu'ils proposent à leurs clients. Il n'est pas conçu pour permettre à ses clients d'administrer ces services eux-mêmes, à l'exception de quelques domaines détaillés dans cette rubrique.

Vue d'ensemble

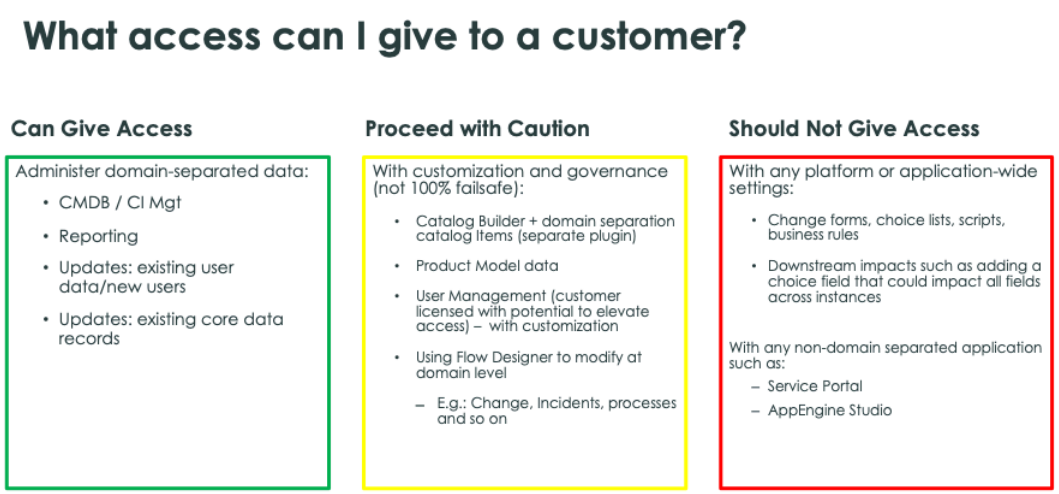
Les clients SP peuvent gérer eux-mêmes en toute sécurité les données contenues dans leur domaine qui n'affectent pas la gestion des licences ou d'autres clients. Par exemple, un client peut créer des rapports ou gérer des éléments de configuration en toute sécurité, mais il n'est pas sûr pour lui de personnaliser des champs, des choix, des règles métier et d'autres processus qui peuvent avoir un impact sur d'autres clients sur la même instance.

Les ServiceNow rôles d'administration du système de base et leurs contrôles d'accès sur la ServiceNow plateforme sont conçus pour une seule équipe d'administration par instance. Par exemple, le rôle domain_admin est accordé à l'une des ressources du SP pour gérer tous les paramètres de domaine de l'instance et pour créer de nouveaux domaines. Pour toutes les tâches d'administration spécifiques à un domaine, le SP doit créer de nouveaux rôles « administrateur client » et de nouveaux contrôles d'accès si nécessaire pour accorder un accès spécifique à ses clients.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'image suivante est une vue d'ensemble des fonctions d'administration courantes dans différentes catégories de ce qui peut être fait en toute sécurité pour un client.



Traduction automatique

Peut donner accès

Exemples :

- Gestion des données CI dans la CMDB
- Création de rapport
- Mises à jour des données utilisateur existantes ou des nouveaux utilisateurs sans rôle
- Met à jour les enregistrements de données de base existants tels que le département, le groupe, l'emplacement, le centre de coûts ou les nouveaux groupes sans rôle, ainsi que les nouveaux départements/centres de coûts/emplacements.

Procédez avec prudence

Exemples :

- Éléments de catalogue : pour créer des éléments de catalogue spécifiques au client qui peuvent être mis à jour par le client, deux options peuvent être utilisées conjointement : Séparation de domaine pour les éléments de catalogue (Séparation de domaine et Catalogue de services) permet au propriétaire de l'instance de créer des éléments dans le domaine du client. Le propriétaire de l'instance peut créer un rôle pour permettre aux clients de mettre à jour des champs fiables tels que le prix, la description et les images. Le générateur de catalogue (nouveau dans la version Quebec) donne à l'équipe d'administration du SP la possibilité de créer des modèles d'éléments qui peuvent être distribués en toute sécurité aux clients pour créer de nouveaux éléments au sein de leur domaine à partir d'une expérience d'interface utilisateur prescriptive.
- Gestion des utilisateurs/groupes : la création d'un rôle « administrateur client » qui peut créer et modifier des enregistrements d'utilisateurs est sécurisée, mais l'ajout et la suppression de rôles peuvent affecter la sécurité et la gestion des licences. Il n'y a aucun moyen dans le système de base de subdiviser les rôles qu'un client peut accorder en toute sécurité. Il en va de même pour la création et la modification de groupes. Bien que le groupe lui-même puisse être modifié, l'ajout ou la soustraction des rôles doit être contrôlé.
- Flow Designer : ServiceNow Studio de workflow est l'outil de création utilisé pour créer un processus (workflow) pour les tables. Le rôle flow_designer donne aux clients un accès

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sans script pour créer des flux. Ils peuvent lire et cloner tous les flux dans les domaines au-dessus d'eux dans la hiérarchie. Ils peuvent créer et modifier des flux dans leur domaine. Cependant, cela ne peut pas se faire en vase clos. Toute personne pouvant influer sur le processus doit être ajoutée à l'équipe d'administration globale pour la gouvernance afin que les processus ne s'annulent pas les uns les autres et ne provoquent pas d'autres conflits.

Ne pas donner accès

Il est utile de comprendre comment fonctionnent les champs de choix pour comprendre pourquoi seule l'équipe d'administration SP devrait les gérer.

- Structure d'un champ de choix : les valeurs de champ de choix sont stockées dans la table sys_choice et regroupées en fonction de la table, du domaine et de la langue.

  Par exemple, le champ **État** d'une tâche est disponible pour toutes les tables qui étendent une tâche. Cela signifie que chaque table peut avoir ses propres valeurs, ces valeurs peuvent être multipliées par domaine, et les valeurs de domaine peuvent être multipliées par langue.

  Toutes les valeurs **d'État** dans toutes les tables, domaines et langues sont considérées comme les valeurs du champ **État** .

- Fonctionnement des changements apportés aux champs de choix : lorsqu'un champ de choix est mis à jour, une charge utile est créée avec toutes les valeurs de ce champ (tables, domaines, langues). Lorsque vous installez cette charge utile sur une instance, toutes les valeurs existantes du champ sont supprimées et les nouvelles valeurs sont chargées. Cela permet de s'assurer qu'il n'y a pas d'entrées en double ou de valeurs restantes qui ne sont plus valides.

  Pour cette raison, il est impossible de donner à un client dans une instance séparée par domaine la possibilité de mettre à jour directement les champs de choix, car cela affecterait l'ensemble de l'instance. En outre, vous ne pouvez pas mettre à jour les choix directement dans une instance de production, car tout ensemble de mises à jour importé qui affecte ce champ écraserait les choix existants. Dans certains cas, les champs de choix peuvent être à l'origine de processus eux-mêmes, qui s'interrompraient si un client modifiait ces champs.

Pour en savoir plus, consultez :

- Exploring user administration
- Créer une règle ACL
- Parcours d'apprentissage du fournisseur de service sur NowLearning
- Domain Separation pour les fournisseurs de services
- Concepts des fournisseurs de services
- Prise en charge de l'application pour Domain Separation
- Notes de version de Domain Separation

Affectation de domaine

Par défaut, Séparation de domaine ajoute un champ de domaine aux tables et à leurs extensions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez également étendre Séparation de domaine à toutes les nouvelles tables que vous créez en ajoutant un champ **sys_domain** à la définition de dictionnaire de la table. Par défaut, le domaine système uniquement sépare les tables de plateforme et d'application de base de référence, le cas échéant.

> **⚠ Avertissement :**
> ServiceNow ne recommande pas l'utilisation de tables de plateforme de séparation par domaine (toute table comportant le préfixe sys_, comme les tables Entrée de dictionnaire [sys_dictionary] et Remplacement d'entrée de dictionnaire [sys_dictionary_override]), car elle peut produire des résultats inattendus.

Un seul domaine est affecté à chaque enregistrement.Ce domaine est stocké dans le champ **sys_domain**.Par défaut, plusieurs tables ont la colonne **sys_domain** et sont déjà séparées par domaine.

La valeur du champ **sys_domain** contient le domaine affecté à l'enregistrement par l'un des éléments suivants :

- Société à laquelle l'utilisateur appartient
- Règle métier lors de la création d'un enregistrement
- Module utilisé lors de la création d'un enregistrement
- Modèle de formulaire utilisé lors de la création d'un enregistrement
- Domaine de l'enregistrement parent
- Domaine affecté à Enregistrement utilisateur
- Domaine de l'utilisateur qui le crée

Le système empêche les tables suivantes d'être séparées par domaine :

- Contrôle d'accès [sys_security_acl]
- Script include [sys_script_include]
- Propriétés système [sys_properties]
- Entités de la liste d'exclusion/d'inclusion de sécurité [sys_security_restricted_list]
- Entrée de dictionnaire [sys_dictionary]
- Contournement d'entrée de dictionnaire [sys_dictionary_override]

Affectation d'utilisateurs à des sociétés

Les administrateurs peuvent rapidement affecter des utilisateurs à un domaine en les affectant à une société. Une fois que les utilisateurs sont affectés à un domaine, les enregistrements héritent automatiquement du domaine de l'utilisateur.

Par exemple, l'affectation de Bow Ruggeri à la société ACME l'affecte automatiquement au domaine ACME. L'affectation de Don Goodliffe à la société Initech l'affecte automatiquement au domaine Initech. Tous les enregistrements qu'ils créent sont automatiquement ajoutés au domaine approprié.

Utilisation des règles métier pour affecter des domaines

Les administrateurs peuvent utiliser une règle métier pour définir automatiquement une valeur de domaine lors de la création d'un enregistrement. La règle métier doit définir une valeur dans le champ **sys_domain** . Les administrateurs doivent s'assurer qu'il existe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

une colonne **sys_domain** disponible pour la table de l'enregistrement. Pour en savoir plus, reportez-vous Pratiques recommandées de séparation de domaine pour les fournisseurs de servicesà .

Utilisation de modules pour affecter des domaines

Les administrateurs peuvent utiliser le paramètre URL **sysparm_domain** pour affecter automatiquement de nouveaux enregistrements à un domaine particulier à partir d'un module. Les administrateurs doivent créer un module avec une valeur **d'argument** de : `sysparm_domain=sys_ID de domaine`.

Utilisation des modèles de formulaire pour affecter des domaines

Les administrateurs peuvent utiliser un modèle de formulaire pour affecter automatiquement de nouveaux enregistrements à un domaine particulier. Les administrateurs doivent ajouter le champ **sys_domain** au formulaire et sélectionner une valeur de domaine. Par exemple, si vous définissez le champ **sys_domain** sur **domaine TOP/ACME** affecte automatiquement tous les enregistrements de ce modèle au domaine TOP/ACME.

Héritage de domaine sur les tables

Par défaut, les enregistrements connexes héritent du domaine de l'enregistrement parent. Par exemple :

- Un enregistrement de tâche de changement hérite du domaine de l'enregistrement de demande de changement parent.
- Un enregistrement de problème hérite du domaine de l'enregistrement d'incident parent.

Affectation automatique de domaines en fonction des domaines d'utilisateurs

Si aucune autre condition de domaine ne s'applique, un enregistrement hérite automatiquement du domaine de l'utilisateur qui le crée.

Domaines de visibilité et domaines contient

Les domaines de visibilité contrôlent ce qu'un utilisateur ou un groupe d'utilisateurs spécifique peut voir. Les domaines « contient » contrôlent ce qu'un domaine entier d'utilisateurs peut voir.

Domaines de visibilité

L'élément « Domaines de visibilité » détermine si les utilisateurs d'un domaine peuvent accéder aux enregistrements d'un autre domaine. Associez cet élément aux enregistrements de l'utilisateur [sys_user] et du groupe [sys_user_group] dans les listes connexes de ces enregistrements. Les groupes accordent à leurs membres les domaines de visibilité du groupe. Lorsqu'un utilisateur quitte un groupe, il perd les domaines de visibilité du groupe. L'attribution aux utilisateurs d'un domaine de visibilité accorde tous les droits sur les enregistrements de ce domaine en fonction des règles ACL (liste de contrôle d'accès).

Un domaine de visibilité :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Il s’agit d’une relation utilisateur-domaine explicitement accordée.
- N’est pas un domaine enfant.
- N’est pas contrôlé par la sélection dans le sélecteur de domaine. Les utilisateurs ayant accès à un domaine de visibilité voient toujours les données de ce domaine et de ses domaines enfants.

Remarque :
Il n’est pas recommandé d’utiliser des domaines de visibilité de manière excessive. Bien que la visibilité soit une méthode permettant aux utilisateurs d’accéder aux enregistrements, il est préférable d’utiliser des domaines contains pour un contrôle plus robuste.

Contient les domaines

Normalement, les relations parent-enfant définissent la hiérarchie du domaine. Un domaine contient vous permet de relier des domaines selon les besoins, indépendamment des relations parent-enfant. Toutefois, les domaines contains n’accordent de visibilité qu’aux données de domaine. Les processus ne sont pas affectés par les relations de contenu.

A contient le domaine :

- Il s’agit d’une relation de domaine à domaine plusieurs-à-plusieurs.
- Peut avoir des domaines enfants. Lorsqu’un domaine est sélectionné, vous pouvez voir les données de ce domaine et de ses enfants.
- Est contrôlé par la sélection dans le sélecteur de domaine.

Remarque :
Lorsque vous ouvrez l’enregistrement de domaine, le champ d’application est défini sur le domaine de cet enregistrement, de sorte que vous ne pouvez voir que les domaines enfants. Choisissez **Activer/désactiver le champ d’application de domaine** dans le menu pour remplir la liste connexe.

Exemple de domaine contient

Lorsque le domaine d’accueil d’un utilisateur est A et que le domaine A contient les domaines B et C, ils deviennent tous des domaines de pairs. Cela signifie que l’utilisateur voit les données des domaines A, B et C lorsqu’il se trouve dans son domaine d’accueil A. Si les utilisateurs changent de domaine avec le sélecteur de domaine pour le domaine B, ils ne voient que les données du domaine B. Lorsque les utilisateurs interagissent directement avec un enregistrement du domaine B ou du domaine C, ils ne voient que les données de ce domaine.

Exemple de domaine de visibilité

En utilisant la visibilité de domaine, si Don Goodliffe se trouve dans le domaine Base de données et que Bow Ruggeri est dans le domaine Réseau et qu’aucun incident ne se trouve dans le domaine global, Don ne peut pas accéder aux incidents de Bow en raison de la séparation des données.

Hériter de domaines de visibilité en fonction de l’appartenance au groupe

Si vous définissez la table de domaines sur la table Groupe [sys_user_group], les utilisateurs peuvent hériter de domaines de visibilité en fonction de leur appartenance au groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Contient des requêtes et un accès au domaine

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Champ d'application de domaine

Le champ d'application de domaine définit ce à quoi les utilisateurs peuvent et ne peuvent pas accéder.

Chaque utilisateur dispose de deux champs d'application de domaine lors de l'établissement d'une session dans une instance séparée par domaine.

- *Le champ d'application* de la session est défini lors de l'établissement de la session sur le domaine répertorié dans l'enregistrement utilisateur de l'utilisateur. Les utilisateurs peuvent modifier manuellement le champ d'application de leur session à partir du sélecteur de domaine.
- *Le champ d'application de l'enregistrement* utilise le domaine de l'enregistrement et est actif lors de l'affichage du formulaire d'un enregistrement.

Par défaut, le champ d'application de l'enregistrement a priorité sur le champ d'application de la session afin que les utilisateurs des domaines de niveau supérieur respectent les données et les contraintes de processus de chaque enregistrement. Toutefois, ces utilisateurs peuvent choisir d'élargir ou de réduire le champ d'application de domaine pour afficher ou masquer les données d'autres domaines. Par exemple, un utilisateur dans le domaine du fournisseur de service (SP) a également une visibilité sur les domaines enfants tels que le domaine ACME. Lors de l'examen d'un enregistrement d'incident à partir du domaine ACME, l'utilisateur peut choisir d'élargir le champ d'application de domaine pour afficher les valeurs du domaine SP ou de réduire le champ d'application de domaine pour afficher uniquement les valeurs d'enregistrement qui correspondent au domaine ACME de l'enregistrement.

Remarque :
Les utilisateurs ont toujours accès aux données des domaines qui leur ont été explicitement accordés par la visibilité du domaine.

Les utilisateurs ayant le rôle d'utilisateur domain_expand_scope peuvent sélectionner le champ d'application de domaine à partir de l'action d'interface utilisateur **Basculer le champ d'application de domaine** sur le formulaire. Lorsque le champ d'application de l'enregistrement est activé, cliquez sur l'action d'interface utilisateur pour l'étendre au champ d'application de la session et afficher toutes les données disponibles en fonction du domaine de l'utilisateur et des domaines enfants. Lorsque le champ d'application de la session est en vigueur, cliquez sur l'action d'interface utilisateur pour le réduire afin de le réduire et de n'afficher que les données qui correspondent au domaine de l'enregistrement actuel.

Remarque :
Un enregistrement n'affiche pas l'action d'interface utilisateur permettant d'activer/désactiver le champ d'application de domaine si l'enregistrement se trouve dans le domaine global ou si le domaine de l'utilisateur correspond au domaine de l'enregistrement.

Enregistrer la sélection de valeurs dans d'autres domaines

Les utilisateurs qui peuvent afficher plusieurs domaines ont la possibilité de sélectionner des valeurs d'enregistrement à partir d'un domaine différent du domaine de l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, les agents Service Desk travaillant pour un fournisseur de service peuvent vouloir s'affecter certains incidents pour résoudre des problèmes au nom de leurs clients. Dans ce cas, le champ **Affecté à** de l'incident peut contenir un utilisateur du domaine SP, même si l'enregistrement d'incident lui-même est associé à un domaine enfant tel que ACME.

La sélection d'une valeur d'enregistrement à partir d'un autre domaine ne modifie pas le domaine de l'enregistrement. L'enregistrement conserve son domaine d'origine. Lorsqu'un utilisateur consulte un enregistrement avec des valeurs provenant de plusieurs domaines, la visibilité du domaine de l'utilisateur détermine ce qu'il voit.

Sélection de valeur d'enregistrement

Lorsque ces conditions sont remplies	L'utilisateur a accès à ces éléments d'interface utilisateur
L'utilisateur a accès au domaine de l'enregistrement actuel référencé dans un champ.	L'utilisateur peut : • Voir la valeur d'affichage du champ de référence. Par exemple, voit le nom d'utilisateur dans le champ **Affecté à** . • Affichez l'enregistrement connexe à partir de l'icône de référence. Par exemple, affiche l'enregistrement de l'utilisateur dans le champ **Affecté à** . • Sélectionnez les valeurs dans n'importe quel domaine visible. Par exemple, peut sélectionner des utilisateurs à partir des domaines SP et ACME.
L'utilisateur n'a pas accès au domaine de l'enregistrement actuel référencé dans un champ.	L'utilisateur peut : • Ne pas afficher les valeurs d'affichage du champ de référence. (C'est le cas si Séparation de domaine a été activé dans Madrid ou dans les versions ultérieures et que l'utilisateur n'a pas accès au domaine de cet enregistrement.) • Sélectionnez uniquement des valeurs dans le domaine de l'enregistrement. Par exemple, ne peut sélectionner que des utilisateurs du domaine ACME.

Domaines et sociétés associées

Avec Séparation de domaine, vous pouvez appliquer en cascade les modifications que vous apportez à un enregistrement d'entreprise, au domaine et à d'autres enregistrements associés à l'entreprise.

Par défaut, le système affecte automatiquement les utilisateurs au même domaine que leur entreprise. Par exemple, tous les utilisateurs de la société ACME deviennent automatiquement membres du domaine TOP/ACME.

Remarque :
Les utilisateurs disposant du rôle administrateur peuvent modifier leurs propres enregistrements utilisateur et, par conséquent, changer de domaine. Les fournisseurs de services peuvent désactiver l'administration déléguée ou configurer un processus d'approbation pour vérifier que l'utilisateur a besoin du rôle administrateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous modifiez le domaine d'une société, l'instance modifie automatiquement le domaine des enregistrements associés suivants pour qu'il corresponde au nouveau domaine de la société.

- Emplacements
- Départements
- Groupes
- Utilisateurs

Remarque :
L'instance ne modifie pas automatiquement le domaine des enregistrements pour lesquels vous avez coché la case **Domaine géré** .

Désactivation du domaine et entreprises associées

Lorsque vous désactivez un domaine, l'instance effectue automatiquement les actions suivantes.

- Désactive toutes les sociétés du domaine.
- Empêche tous les utilisateurs affectés à la société inactive de se connecter.

Remarque :
Lorsqu'un utilisateur d'une société inactive tente de se connecter, il voit un message d'erreur similaire à Entreprise inactive - votre accès à cette instance n'est pas autorisé.

Par exemple, si vous désactivez le domaine ACME à partir des exemples de données, l'instance désactive également la société ACME et les trois exemples d'utilisateurs sont verrouillés.

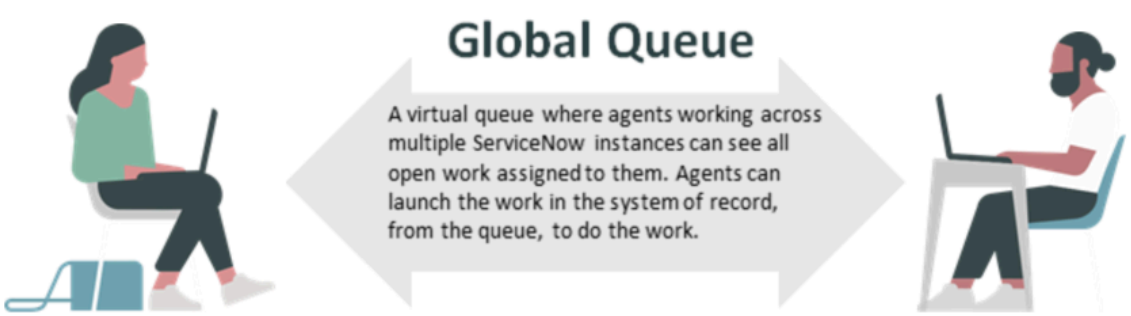
Concepts pour les prestataires de services

Ces concepts fonctionnent avec les fonctionnalités de la plateforme existante ServiceNow pour vous aider à résoudre les cas d'utilisation courants.

File d'attente globale v.2

Le concept de file d'attente globale fournit une vue virtuelle unique des tâches qui résident dans plusieurs instances. Le concept crée une application personnalisée pour fournir une vue de prestataire du travail qui réside dans plusieurs instances sans avoir à répliquer des tâches ou des données.

Vue d'ensemble



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les fournisseurs de services dont les agents travaillent sur des tâches à partir de plusieurs systèmes ont tendance à réintégrer les données dans une instance centrale, ou une « chaise pivotante » entre les instances. Bien que cette méthode puisse être appropriée dans certains cas, elle peut être coûteuse et prendre du temps à construire et à entretenir. Cette méthode expose également le fournisseur à d'éventuelles considérations d'audit et d'exigences en matière de données, telles que le Règlement général sur la protection des données (RGPD) dans tous les cas où les données se trouvent désormais.

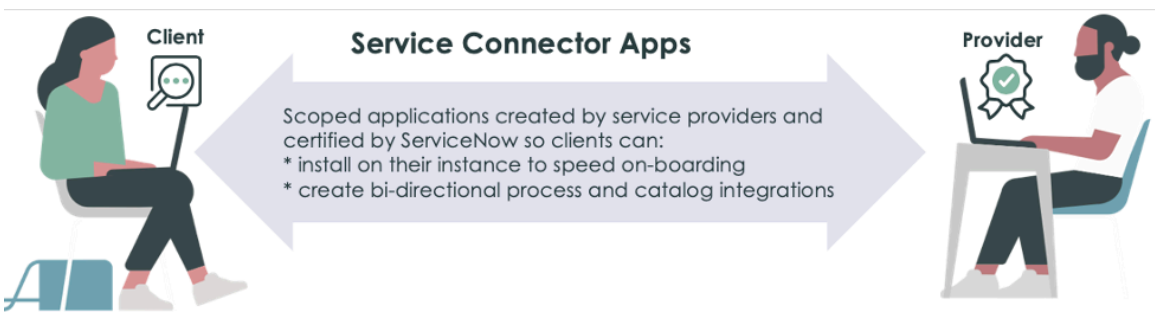
La file d'attente globale v.2 est une alternative : avec cette méthode, les agents peuvent voir les données qui leur sont affectées à partir d'une seule instance sans que les données souveraines ne persistent sur l'instance à laquelle ils sont connectés. Par exemple, dans les cas où les clients ont des exigences en matière de résidence des données, mais autorisent l'accès à des agents d'autres pays, le fournisseur peut utiliser un service d'assistance « follow the sun » à l'aide de la file d'attente globale v.2.

Pour en savoir plus sur la preuve de concept Global Queue v.2 , consultez le ServiceNow site Knowledge.

Remarque :
Dans la version Quebec, la preuve de concept de la file d'attente globale a été mise à niveau vers la file d'attente globale v. 2.

Connecteur fournisseur de service

L'application Connecteur fournisseur de services est une conception de référence pour la création d'une ServiceNow application de stockage que vos clients peuvent utiliser pour s'intégrer à vos systèmes. Les applications des fournisseurs de services vous aident à accélérer l'intégration et à créer des intégrations standardisées.



Avantages des connecteurs de service

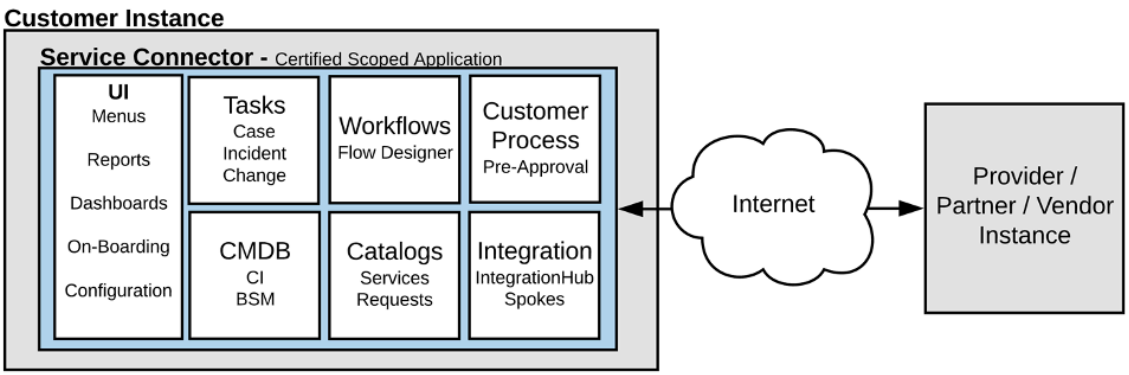
Lorsque les fournisseurs de services (vendeurs, fournisseurs, partenaires) publient des connecteurs, l'intégration des clients est plus rapide, ce qui signifie une facturation plus rapide. Les instances intégrées augmentent la productivité, augmentent la visibilité dans l'écosystème ServiceNow et offrent des avantages au programme de partenariat. Les avantages spécifiques sont les suivants :

- Élimine les intégrations personnalisées, y compris le coût des services requis pour les fournir et les maintenir.
- Les services sont définis par les fournisseurs au sein de leurs ServiceNow instances et éliminent la complexité et le coût des intégrations personnalisées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Les flux de travail et les demandes du catalogue peuvent être synchronisés, les processus et les approbations du client précédant les processus du fournisseur, afin que les clients puissent suivre leurs propres processus.
- Toutes les données créées ou modifiées (par exemple, les CI) pour le client sur l'instance du fournisseur peuvent être synchronisées dans l'instance du client pour leur visibilité et leur utilisation dans les processus.



Fonctionnalités principales

Fonctionnalité	Description
Interface utilisateur	Un connecteur de service doit inclure au minimum les composants d'interface utilisateur suivants : • Rapports/Tableaux de bord : les rapports et tableaux de bord prédéfinis par profil améliorent la visibilité. • Menu et modules – Le client doit être en mesure de trouver l'application via le fournisseur de menu descriptif **XYZ Services**. • Rôles : chaque connecteur nécessite des rôles d'utilisateur et d'administrateur pour garantir que l'accès peut être contrôlé par le client. Par exemple, « x_snc_xyz_user » ou « x_snc_xyz_admin ». • Intégration : une intégration rapide est essentielle à une bonne expérience utilisateur et doit être incluse via un playbook, une configuration guidée ou un élément de catalogue de sorte qu'aucun service professionnel ne soit requis pour que le client soit en direct. (Des services professionnels sont disponibles, mais l'intégration peut être réalisée sans eux). • Configuration – Les points de données doivent être intégrés dans les processus pour tenir compte de la majeure partie de la configuration de processus normale

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnalité	Description
	qu'un client doit réaliser. Cela permet d'éliminer autant que possible les services professionnels. • Documentation – Une documentation complète augmente la satisfaction du client et la facilité d'utilisation. • Intégration de l'assistance ou informations de contact : le client a besoin d'un moyen facile de rester en contact avec le fournisseur de services pour tout problème, question ou demande.
Tâches	Utilisez l'application pour que les tâches, telles que les incidents, les tickets, les changements, les problèmes, etc., doivent être prédéfinies dans le connecteur. Ces intégrations sont conçues en utilisant Studio de workflow et Hub d'intégration pour garantir le plus haut niveau de résilience et de performance.
CMDB	La synchronisation des données de base, telle que les CI requis pour des processus ITIL appropriés, doit être synchronisée entre les instances du fournisseur et du client.
Workflows	Tous les flux de travail doivent être conçus de Studio de workflow manière à garantir la résilience et les performances.
Catalogues	Le catalogue du fournisseur auquel le client effectue la demande doit être inclus dans l'application en tant que catalogue de production d'enregistrements. La demande générée par l'élément dans l'instance du client doit être liée électroniquement aux instances du fournisseur. Les workflows du fournisseur tiennent la demande à jour et la resynchronisent avec l'instance du client.
Processus clients	Tout mécanisme de synchronisation des demandes avec l'instance du fournisseur doit permettre aux processus client d'interagir avec les demandes avant qu'elles ne soient envoyées à l'instance du fournisseur. Pendant le traitement du fournisseur, les approbations peuvent être envoyées à l'instance du client selon les besoins.
Intégration	Les intégrations doivent être conçues en utilisant Studio de workflow et Hub d'intégration pour garantir le plus haut niveau de résilience et de performance.

Composants possibles que vous pouvez inclure dans un connecteur de service

Composant	Description
Réplication de données d'instance (IDR)	Lorsque l'objectif est la réplication :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composant	Description
	• Peut être utilisé pour l'intégration de processus, mais peut être trop rigide en fonction de la complexité logique d'intégration basée sur la transition d'état • Pour en savoir plus, consultez Réplication de données d'instance
Centre d'intégration	Lorsque l'intégration des processus est l'objectif : • Plus facile à injecter au milieu d'un processus, dans le cadre d'une étape complexe ou conditionnelle au milieu d'un flux • Pour en savoir plus, consultez Centre d'intégration
File d'attente de travail globale (virtuelle)	Lorsque l'objectif est la fédération de tâches et que le stockage des données en externe n'est pas acceptable : • Utilisé lorsque les agents travaillent sur plusieurs ServiceNow instances et ont besoin de voir tout le travail ouvert qui leur est affecté • Les lignes renvoyées doivent être limitées à moins de 1 000 • Pour en savoir plus, reportez-vous à la section File d'attente de travail globale
Tables distantes	Lorsque l'objectif est d'utiliser des données externes sans stockage : • Utilisé pour connecter une instance à des sources tierces ou, à une autre instance, pour récupérer des données externes et éventuellement les mettre en cache dans la mémoire. Les données sont traitées comme une table dans l'instance à des fins de lecture seule telles que regrouper, trier, regrouper et filtrer. • Pour en savoir plus, reportez-vous à la rubrique Récupération de données externes à l'aide de tables et de scripts distants
Concepteur de flux	Quand la conception des processus est l'objectif • Utilisé pour automatiser les processus dans un environnement de conception unique. Les propriétaires de processus peuvent utiliser le langage naturel pour automatiser les approbations, les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Composant	Description
	tâches, les notifications et les opérations d'enregistrement sans codage. • Pour en savoir plus, reportez-vous à la rubrique Flow Designer .

Pour en savoir plus sur la preuve de concept du connecteur de service , consultez le ServiceNow site Knowledge.

Installé avec Séparation de domaine

Plusieurs composants de la plateforme sont ajoutés ou modifiés avec Séparation de domaine.

Rôles

Rôle	Description
domain_admin	Peut créer, modifier et supprimer des domaines.

Ajouts aux champs [sys_domain]

Le champ sys_domain est ajouté aux tables suivantes :

Tables avec le champ sys_domain

Tables
sys_attachment
sys_user_has_role
sys_group_has_role
sys_email
sys_user_group
core_company
cmn_location
cmn_department
sys_gauge
sys_report
kb_feedback
sysapproval_approver
sys_user_grmember

Champ de la table de tâches

Les extensions MSP ajoutent un champ task_for à la table Tâche. Ce champ de référence fait référence à la table Utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options pour le type de groupe

Les extensions MSP ajoutent plusieurs nouvelles options par défaut au champ type de la table Groupe. Ajoutez ou mettez à jour ces types selon vos besoins pour prendre en charge vos domaines.

Tables
Sécurité
Prise en charge
Visibilité

Règles métier

Nom	Table	Description
Domaine : activer/ désactiver	core_company	Active le domaine connexe si au moins une de ses sociétés est active. Désactive le domaine connexe si toutes les sociétés associées sont inactives.
Domaine : Société en cascade	core_company	Synchronise le domaine d'une entreprise avec ses utilisateurs, groupes, départements et emplacements.
Domaine : Cascade Domaine : E-mail	sys_email	Synchronise le domaine d'un e-mail avec ses pièces jointes.
Domaine : Cascade Domaine : Groupe	sys_user_group	Synchronise le domaine d'un groupe avec ses rôles hérités (enregistrements sys_group_has_role).
Domaine : Cascade Domaine : Connaissances	kb_knowledge	synchronise le domaine d'un article de la base de connaissances avec ses commentaires connexes.
Domaine : Cascade Domaine : Tâche	tâche	Synchronise le domaine avec les tâches connexes pour wf_context, wf_executing, wf_history, pièces jointes, e-mails, task_sla et son workflow, sysapproval_approver et son workflow, et sysapproval_group et son workflow.
Domaine : Cascade Domaine : Utilisateur	sys_user	Synchronise le domaine d'un utilisateur avec ses enregistrements d'appartenance à un groupe (sys_user_grmember) et de rôle (sys_user_has_role).
Domaine : Cascade Domaine : Version	wf_workflow_version	Synchronise les domaines avec les versions de workflow associées pour wf_activity et wf_transition.
Domaine : désactiver les sociétés	domain	Désactive les sociétés liées si un domaine est désactivé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Table	Description
Domaine : Par défaut : Tâche	tâche	Définit le domaine de tâche en fonction de la tâche pour le domaine de l'utilisateur. Si ce domaine est global, définit le domaine sur Par défaut à la place.
Domaine : Par défaut : Utilisateur	sys_user	Définit le domaine d'un utilisateur par défaut si le domaine aurait été global autrement.
Domaine : interdire l'enregistrement du domaine global	domain	Empêche la création d'un domaine avec le nom global.
Domaine : remplacer la copie	sys_app_application	Lorsqu'une application est remplacée pour un domaine, crée une copie de ses modules pour la nouvelle application.
Domaine : remplacer la copie	sys_data_policy2	Lorsqu'une politique de données est remplacée pour un domaine, crée une copie de ses règles de politique de données pour la nouvelle politique de données.
Domaine : remplacer la copie	sys_gauge	Lorsqu'une jauge est remplacée pour un domaine, crée une copie de son nombre de jauges pour la nouvelle jauge.
Domaine : remplacer la copie	sys_ui_action	Lorsqu'une action d'interface utilisateur est remplacée pour un domaine, crée une copie de ses vues d'action d'interface utilisateur pour la nouvelle action d'interface utilisateur.
Domaine : remplacer la copie	sys_ui_list_control_embedded	Lorsqu'un contrôle de liste incorporé est remplacé pour un domaine, crée une copie de ses scripts client et serveur pour le nouveau contrôle de liste incorporé.
Domaine : remplacer la copie	sys_ui_policy	Lorsqu'une politique d'interface utilisateur est remplacée pour un domaine, crée une copie de ses actions de politique d'interface utilisateur pour la nouvelle politique d'interface utilisateur.
Domaine : Définir Domaine : Approbations	sysapproval_approver	Définit le domaine en fonction de celui de l'enregistrement en cours d'approbation.
Domaine : Définir Domaine : Pièce jointe	sys_attachment	Définit le domaine en fonction du domaine de l'enregistrement parent.
Domaine : Définir Domaine : CMDB_CI	cmdb_ci	Définit le domaine d'un CI sur celui de sa société.
Domaine : ensemble Domaine : département	cmn_department	Définit le domaine d'un département sur celui de sa société.
Domaine : ensemble	domain	Définit le domaine d'un domaine sur lui-même.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Table	Description
Domaine : domaine : domaine		
Domaine : Définir Domaine : E-mail	sys_email	Définit le domaine en fonction du domaine de l'enregistrement parent. L'enregistrement parent d'un e-mail est l'enregistrement spécifié dans le champ d'instance.
Domaine : Définir Domaine : Commentaire	kb_feedback	Définit le domaine d'un commentaire de la base de connaissances sur celui de son article de la base de connaissances.
Domaine - Ensemble Domaine - Groupe	sys_user_group	Définit le domaine d'un groupe sur celui de sa société.
Domaine - Définir Domaine - Approbations de groupe	sysapproval_group	Définit le domaine en fonction de celui de l'enregistrement en cours d'approbation.
Domaine - Définir Domaine - Rôle de groupe	sys_group_has_role	Définit le domaine d'un rôle de groupe sur celui de son groupe.
Domaine - Ensemble Domaine - Emplacement	cmn_location	Définit le domaine d'un emplacement sur celui de sa société.
Domaine - Définir Domaine - SLA de tâche	task_sla	Définit le domaine d'un SLA de tâche sur celui de sa tâche.
Domaine : Ensemble Domaine : Utilisateur	sys_user	Définit le domaine d'un utilisateur sur celui de sa société.
Domaine - Définir Domaine - Rôle de l'utilisateur	sys_user_has_role	Définit le domaine d'un rôle d'utilisateur sur celui de son utilisateur.
Domaine : ensemble Domaine : Historique de l'activité WF	wf_history	Définit le domaine de l'historique de l'activité du workflow en fonction du domaine du contexte de workflow parent.
Domaine - Définir Domaine - Contexte WF	wf_context	Définit le domaine de contexte du workflow en fonction du domaine de l'enregistrement référencé, s'il en a un.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Table	Description
Domaine : ensemble Domaine : activité d'exécution WF	wf_executing	Définit le domaine de l'activité d'exécution du workflow en fonction du domaine du contexte de workflow parent.
Domaine - Définir la tâche pour - Changement	demande de changement	Lors de la conversion d'un ticket en demande de changement, définit le champ Demandé par sur la valeur Tâche du ticket.
Domaine - Définir la tâche pour - Incident	incident	Lors de la conversion d'un ticket en incident, définit le champ Appelant sur Tâche du ticket pour valeur.
Domaine : valider par défaut	domain	Garantit que la case Par défaut est cochée sur un seul domaine.
Domaine : valider le domaine primaire	domain	Garantit que la case Primaire est cochée dans un seul domaine.
Règles métier installées avec le module d'extension Domain Support		
Modifier l'ensemble de domaine	sys_dictionary	Définit l'ensemble de domaines sur le domaine actuel.
Propriétés de prise en charge du domaine	sys_properties	Définit les propriétés système pour qu'elles correspondent à la méthode de requête de domaine (chemins de domaine ou numérotation de domaine).

Scripts clients

Script client	Description
Domaine : définir la société et l'emplacement (sys_script)	Surveille les changements dans le champ Appelant de l'incident. Si les champs d'entreprise et d'emplacement n'ont pas déjà de valeur, le script ajoute ces informations à partir de l'enregistrement de l'appelant. Si les champs d'entreprise et d'emplacement ont déjà une valeur, le script conserve les valeurs existantes.
Script désactivé	
(BP) Définir l'emplacement sur l'utilisateur	Surveille le champ d'emplacement de l'incident et définit le champ d'emplacement sur l'emplacement de l'appelant.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Prise en charge par les applications pour Domain Separation

De nombreuses ServiceNow applications prennent en charge Séparation de domaine dans le système de base, mais pas toutes. Certaines applications prises en charge incluent des

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

limitations sur les données et les paramètres administratifs qui peuvent être séparés par domaine. Ces définitions délimitent les niveaux de prise en charge de Domain Separation du point de vue des cas d'utilisation réels et des personnes qui les utilisent.

Niveaux de prise en charge de Domain Separation

ServiceNow Les applications qui prennent en charge Séparation de domaine peuvent uniquement prendre en charge la séparation des données et le routage des données, disposer d'une séparation avancée de la logique métier ou prendre en charge l'administration au niveau du locataire (client) de l'application. ServiceNow Les applications sont définies avec les niveaux de prise en charge incrémentielle suivants.

Basic	Standard	Enhanced
• Data is domain-separated • Logic exists to ensure proper data routing, caching, rollups, and aggregations • Global configuration operational for multiple tenants	• Application properties are domain-aware as needed • Business logic can be domain-separated by the instance owner per tenant	• Data-driven process enables failsafe configuration by tenants through the UI to drive business logic

Aucune prise en charge

- Le champ Domaine peut être présent dans les tables de données, mais il n'existe aucune logique pour gérer les données.
- Ce niveau n'est pas considéré comme étant séparé par domaine.

Élémentaire

- Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de services (SP) de l'application.
- Dans l'application, l'interface utilisateur, les clés de cache, les rapports, les déploiements, les agrégations et autres utilisent tous un domaine au moment de l'exécution de la production.
- Le propriétaire de l'instance doit pouvoir configurer l'application pour qu'elle fonctionne sur plusieurs locataires.

Exemple de cas d'utilisation : lorsqu'un SP utilise la messagerie instantanée pour répondre au message d'un locataire-client, le client doit pouvoir voir la réponse du SP.

Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : les processus peuvent être créés ou modifiés par client par le fournisseur de services (SP). Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de cas d'utilisation : un administrateur doit être en mesure de rendre les commentaires obligatoires lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Amélioré

- Inclut les niveaux **Basique** et **Standard**.
- Le processus piloté par les données permet aux clients du fournisseur de service de modifier la logique métier basée sur des cas d'utilisation définis. Ces configurations sont basées sur l'interface utilisateur et sont sécurisées de sorte que les configurations d'un client ne peuvent pas en affecter une autre.
- Les locataires de l'instance doivent être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) pour eux-mêmes. Cette logique et ces paramètres sont attendus pour un fonctionnement normal de l'application.

Exemple de cas d'utilisation : les locataire-clients d'un environnement partagé doivent être en mesure de passer à la matrice d'impact, d'urgence ou de priorité pour définir la priorité au sein de leur domaine.

Remarque :
Domaine effectif (*)

Parfois, une fonctionnalité ou une application de plateforme peut prendre en charge efficacement les cas d'utilisation SP, même sans le cadre de travail du domaine. Si tel est le cas, les cas d'utilisation doivent détailler sa prise en charge de la séparation de domaine. Un astérisque (*) après le niveau de support indique ce type de configuration.

Fonctionnalité prise en charge	Élémentaire	Standard	Amélioré
La colonne Domaine est présente pour les tables d'application du système de base.	●	●	●
La configuration spécifique à un domaine est gérée par le propriétaire de l'instance.	●	●	●
Les domaines de locataire peuvent gérer leurs propres données d'application.		●	●
Les propriétés de l'application sont sensibles au domaine en cas de besoin.		●	●
Les processus et la logique métier peuvent être séparés par domaine par le propriétaire de l'instance.		●	●
La logique métier et les processus peuvent être administrés par le domaine du locataire.			●

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Niveaux de prise en charge par application

Suite de produits	Application	Niveau de prise en charge
Hyperautomation and low-code	App Engine Studio	Aucune prise en charge
	Automation Center	Élémentaire
	Concentrateur de l'automatisation robotisée des processus (RPA)	Élémentaire
	Table Builder	Élémentaire
	Management Center du moteur de développement d'application	Aucune prise en charge
	Exploring decision tables	Standard
	Intégration de la planification des ressources de l'entreprise	Aucune prise en charge
	Exploration de personnalisation du progiciel de ressource de l'entreprise	Aucune prise en charge
	Générateur d'IU Next Experience	Élémentaire
Gestion du service clientèle	Communities	Aucune prise en charge
	Gestion du service clientèle	Élémentaire
	Gestion des mises en production	Basique*
	Order Management pour Customer Service Management	Élémentaire
	Post-Sales Support	Élémentaire
	Domain separation in Workforce Optimization for Customer Service	Élémentaire
DevOps	Domain separation and DevOps Change Velocity	Aucune prise en charge
	Domain separation and DevOps Config	
Gestion des services aux employés	HR Service Delivery	Basique*
	Santé et sécurité	Élémentaire
	Legal Service Delivery	Élémentaire
	Gestion des services de procurement (PSM)	Aucune prise en charge
	Safe Workplace Suite	Voir le site d'application pour connaître les niveaux de prise en charge des applications individuelles
	Connecteur de recherche SharePoint Online	Élémentaire
	Demande universelle	Élémentaire
	Tâche universelle	Élémentaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Optimisation de la main d'œuvre pour RH	Élémentaire
Gestion environnementale, sociale et de gouvernance	Gestion environnementale, sociale et de gouvernance	Élémentaire
Field Service Management	Field Service Management	Élémentaire
Gouvernance, risque et conformité	Business Continuity Management	Élémentaire
	Gouvernance, risque et conformité (GRC)	Élémentaire
	Operational Resilience	Élémentaire
Produits spécifiques à chaque secteur		
•Financial Services	Financial Services Card Operations	Élémentaire
	Financial Services Deposit Operations	Élémentaire
	Financial Services Payment Operations	Élémentaire
	Entretien intelligent en cas de fraude	
	Gestion des services d'assurance de dommages	
	Gestion des services d'assurance-vie	
	Réclamations d'assurance	
	Financial Services Know Your Customer	
	Services financiers Opération de crédit	
	Processeur de document de services financiers	Élémentaire
• Santé et sciences de la vie	Support EMR	Élémentaire
	Gestion des services de santé et de sciences de la vie Core	Élémentaire
	Gestion avant la visite	Élémentaire
	Services de soutien aux patients	Élémentaire
	Vaccine Administration Management	Élémentaire
• Production industrielle	Industrial Process Manager	Standard
	Operational Technology Manager	Standard
	Operational Technology Vulnerability Response	Standard
	Operational Technology Manager	Standard
IT Asset Management	Cloud Insights	Aucune prise en charge
	Hardware Asset Management	Amélioré

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Gestion des actifs logiciels	Amélioré
	Enterprise Asset Management	Standard
Strategic Porfolio Management	Agile Development	Basique*
	Alignment Planner Workspace	Élémentaire
	Application Portfolio Management	Élémentaire
	Cost Management	Aucune prise en charge
	Gestion de la demande	Élémentaire
	Gestion financière	Aucune prise en charge
	Investment Funding	Élémentaire
	Project Portfolio Management	Basique*
	Gestion des mises en production	Basique*
	Scaled Agile Framework (SAFe)	Basique*
	Test Management	Basique*
	Cadre de travail des objectifs	Élémentaire
IT Operations Management	Cloud Provisioning and Governance	Élémentaire
	Agent Client Collector	Élémentaire
	Discovery	Standard
	Event Management	Élémentaire
	Espace de travail pour l'exploitation des services pour ITOM	Élémentaire
	Analyse de santé du journal	Élémentaire
	Analyse des mesures	Élémentaire
	Service Mapping	Élémentaire
	Évaluation de la migration vers le cloud	Élémentaire
	Bibliothèque d’actions	Aucune prise en charge
	Cloud Configuration Governance	Aucune prise en charge
	Tag Governance	Élémentaire
	Facturation d'Analyse des coûts du cloud	Aucune prise en charge
	Cloud Provisioning and Governance : Google Cloud	Élémentaire
	Mise en service et gouvernance du cloud Terraform	Élémentaire
	Espace de travail pour l’exploitation dans le cloud	Élémentaire
	Découverte dans le cloud	Standard

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
IT Service Management	Benchmarks	Aucune prise en charge
	Gestion des changements	Élémentaire
	Coaching	Élémentaire
	Gestion de l'amélioration continue	Élémentaire
	Gestion des contrats	Aucune prise en charge
	Ligne de dépense	Aucune prise en charge
	Incident Communications Management	Standard
	Gestion des incidents	Standard
	Facilities Service Management	Standard
	Gestion des incidents	Standard
	Planification d'astreinte	Standard
	Gestion des actifs	Élémentaire
	Problem Management	Standard
	Approvisionnement	Standard*
	Catalogue de produits	Standard
	Gestion des requêtes	Standard
	Catalogue de services	Standard
	Service Level Management	Élémentaire
	Gestion des portefeuilles de services	Basique*
	Opérations pour la fiabilité des sites	Basique*
	Panne de tâche	Élémentaire
	Domain separation and Vendor Management Workspace	Aucune prise en charge
	Walk-up Experience	Élémentaire
Configuration et navigation Mobile	Mobile	Élémentaire
Now Intelligence	Tableaux de bord	Élémentaire
	Performance Analytics	Amélioré
	Process Optimization	Élémentaire
	Reporting	Élémentaire
	User Experience Analytics	Élémentaire
La Now Platform	, Administration , Studio du moteur de développement d’application , Options de Now Platform , Interface utilisateur	
	Domain separation and Agent Chat	Standard
	Affectation de travail avancée	Standard

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	AI Search	Les recherches respectent les restrictions de domaine des enregistrements indexés
	App Engine Studio	Aucune prise en charge
	Gestion des applications	Aucune prise en charge
	Évaluations	Standard
	Automated Test Framework	Standard*
	Fonctions vocales ServiceNow	
	Signature de code	Support de base
	Contextual Search	Standard
	Configuration Management (CMDB)	Standard
	Système de gestion du contenu	Aucune prise en charge
	Informations d'identification et connexions	Standard
	Certification des données	Basique*
	Classification des données	Amélioré
	Confidentialité des données	Aucune prise en charge
	Gestion des données	Basique*
	Développement délégué	Aucune prise en charge
	Dependency Views	Élémentaire
	Services documentaires	Aucune prise en charge
	Dynamic Translation	Élémentaire
	Edge Encryption	Support de base
	Chiffrement au niveau des colonnes	Aucune prise en charge
	Chiffrement au niveau des colonnes – Entreprise	Aucune prise en charge
	Chiffrement dans le cloud avec gestion des clés	Support de base
	Normalisation de champ	Aucune prise en charge
	Flow Designer	Standard*
	Configuration guidée	Aucune prise en charge
	Domain separation and Integration Hub	Standard*
	Intégrations avec des applications et des sources de données tierces	Basique + Standard
	Knowledge Management	Standard
	Service de messagerie Hermes	Aucune prise en charge

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Documents gérés	Aucune prise en charge
	MetricBase	Élémentaire
	Compréhension de la lessification naturelle	Basique + Standard
	Notifications	Standard
	Pilote ODBC	Basique*
	Orchestration	Standard*
	Password Reset	Standard
	Sécurité de la plateforme	Page de destination Séparation de domaine
	Confidentialité des données	Aucune prise en charge
	Intelligence prédictive	Standard
	Déclencheurs proactifs	Élémentaire
	Process Automation Designer	Élémentaire
	Tables distantes	Aucune prise en charge
	Calendriers	Élémentaire
	Débogueur de script	Élémentaire
	Suggestions de recherche	Aucune prise en charge
	Service Portal	Aucune prise en charge
	Domain separation and Sidebar	Standard
	Flux d'états	Aucune prise en charge
	Subscription Management	Basique*
	Gestion des enquêtes	Basique*
	Intelligence des tâches	Aucune prise en charge
	Domain separation and Time Card	Basique*
	UI Builder	Standard
	Agent virtuel	Élémentaire
	Visual Task Boards	Élémentaire
	Services Web	Standard*
	Workflow	Standard*
	Espace de travail	Standard
Security Operations	Configuration Compliance	Standard
	Gestion des données de configuration	Élémentaire
	IBM QRadar Offense Ingestion	Élémentaire
	Intégration de l'ingestion d'alerte de l'API Microsoft Graph Security	Élémentaire

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suite de produits	Application	Niveau de prise en charge
	Security Incident Response	Standard
	Threat Intelligence	Standard
	Vulnerability Response	Standard
Service Management	Facilities Service Management	Standard
	Planned Maintenance	Standard*
	Déclencheurs proactifs	Élémentaire
	Éditeur de code NOW	Aucune prise en charge
	Optimisation de la main d'œuvre pour ITSM	Élémentaire
	Vendor Management Workspace	Élémentaire

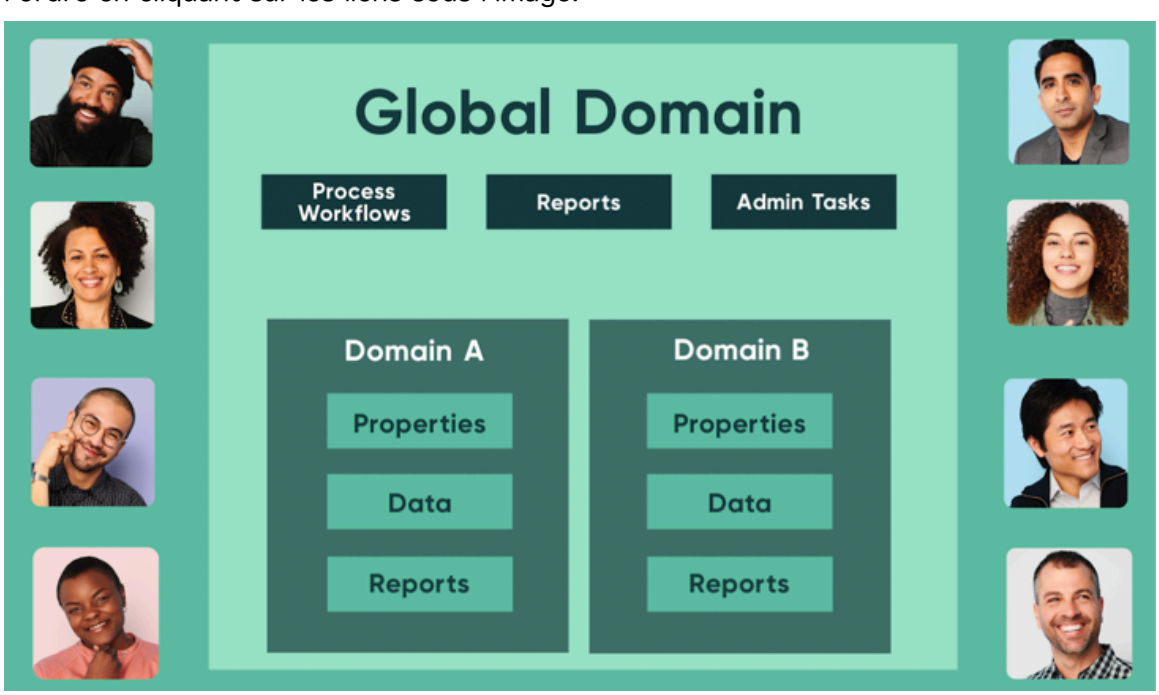
Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Vous pouvez créer, implémenter et gérer Séparation de domaine pour vos applications et services.

Informations de base sur les domaines

Avec Séparation de domaine (également connue sous le nom d'architecture ServiceNow de plateforme mutualisée), vous pouvez séparer les données d'application, l'interface utilisateur et la logique métier dans une instance client unique qui prend en charge la modélisation hiérarchique avec l'intelligence entre locataires. La logique métier décrit la façon dont Séparation de domaine est configurée et les règles qui affectent la configuration.

Avant de vous lancer dans l'aventure de Domain Separation, voici quelques bonnes pratiques à suivre. Sélectionnez les rubriques comme vous le souhaitez ou suivez-les dans l'ordre en cliquant sur les liens sous l'image.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explication de Séparation de domaine

Avec Séparation de domaine, vous pouvez séparer les données d'application, l'interface utilisateur et la logique métier, telles que les règles ou les workflows, dans une seule instance client. La séparation de ces éléments en domaines logiquement définis prend en charge des hiérarchies spécifiques pour tous les clients qui utilisent vos applications.

Informations de base sur les domaines

Séparation de domaine, également connue sous le nom d'architecture ServiceNow de plateforme mutualisée, ajoute une surcharge considérable à la gestion d'une instance. Cependant, si vous utilisez Séparation de domaine correctement, cela peut améliorer l'efficacité, renforcer la sécurité et augmenter les performances des instances de vos clients.

Vous ne pouvez pas séparer certaines normes et propriétés globales, telles que les propriétés système et le schéma de table, par locataire.

Avant de commencer à séparer des domaines, lisez les instructions suivantes.

Ce que vous pouvez faire avec Séparation de domaine

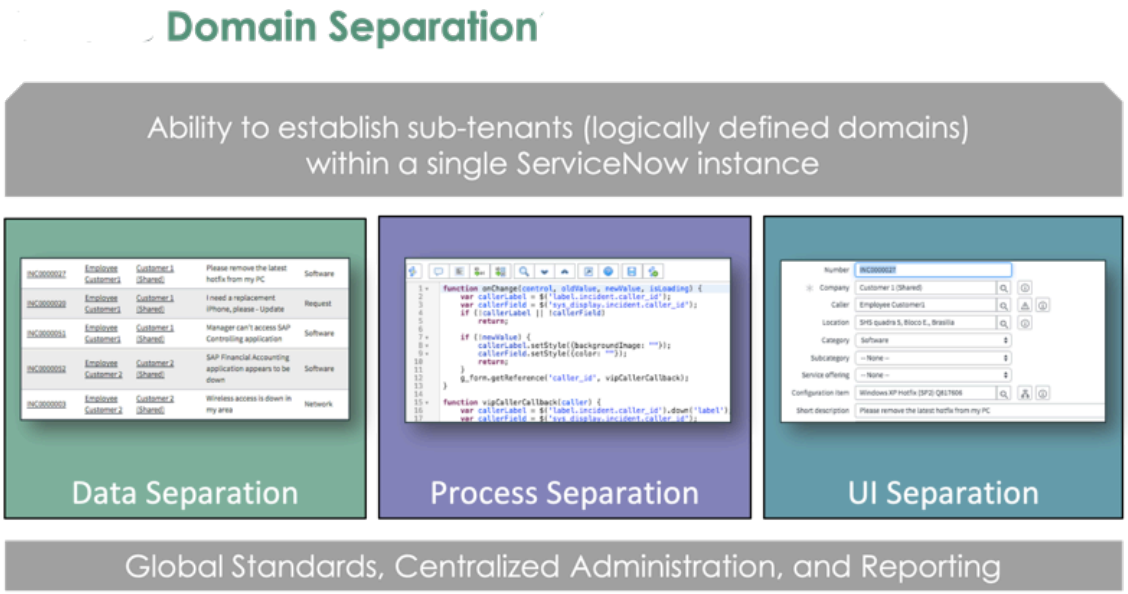
- Séparation des données : permet aux locataires du domaine de voir uniquement les données pour lesquelles ils ont l'autorisation. Les locataires peuvent avoir accès à d'autres données de locataire, mais ne peuvent pas interroger les données de locataire auxquelles ils n'ont pas accès.
  - Lorsque vous mettez à jour des enregistrements de données, ils ne génèrent pas d'enregistrements d'ensembles de mises à jour.
  - Les utilisateurs, y compris les comptes clients utilisés pour les intégrations, ne voient que les données dans les domaines auxquels ils ont l'autorisation d'accéder.
  - Les clients, les agents et les prestataires voient les données relatives aux clients et aux organisations qu'ils prennent en charge.
- Séparation de l'interface utilisateur : prend en charge une expérience spécifique au locataire pour les éléments d'interface utilisateur tels que les vues, les listes, les étiquettes, et ainsi de suite.
  - Vous pouvez remplacer l'interface utilisateur basée sur un navigateur, y compris les menus d'application, les listes, les formulaires et les tableaux de bord. Vous pouvez également les personnaliser pour un domaine ou un ensemble de domaines spécifique tout en préservant votre logique de processus de base.
  - Les fournisseurs de services peuvent modifier la marque affichée et les éléments d'interface utilisateur pour répondre aux besoins individuels des clients.
- Séparation de la logique métier : crée des politiques système spécifiques au locataire, telles que les notifications par e-mail, les règles métier, les scripts clients, la politique d'interface utilisateur et les actions d'interface utilisateur.
- Modélisation hiérarchique : imbrique vos locataires multiples afin que les locataires parents puissent accéder aux ressources des locataires enfants. La logique métier pour les locataires parents s'exécute automatiquement pour les locataires enfants, que vous pouvez remplacer à n'importe quel niveau.
- Intelligence entre locataires : gère automatiquement les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires ayant accès à des données de locataire supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Domain Separation en un coup d'œil

Le graphique suivant montre la division des données, le processus et la séparation de l'interface utilisateur. Ces concepts sont abordés en profondeur dans la section Pratiques recommandées.



Architecture du domaine

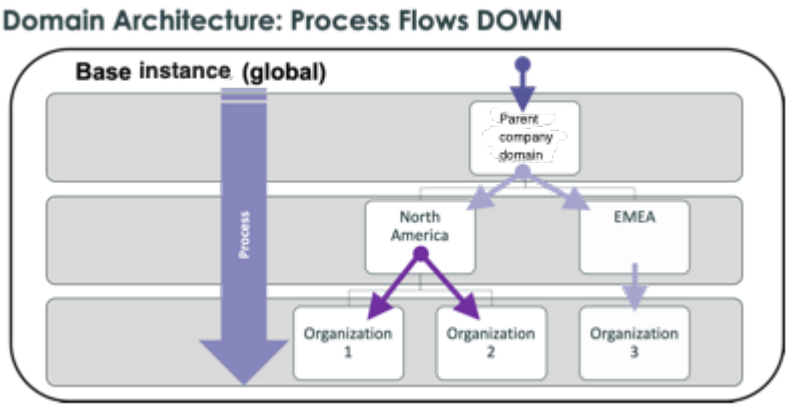
Les enregistrements utilisateur se voient attribuer une valeur de domaine qui représente le domaine d'origine de l'utilisateur. Les utilisateurs n'ont pas accès aux données dans les domaines parents, les domaines pairs ou les domaines dans d'autres branches de la hiérarchie.

Consultez la section Contient des requêtes et un accès au domaine pour connaître les options avancées permettant d'accorder une visibilité de domaine supplémentaire.

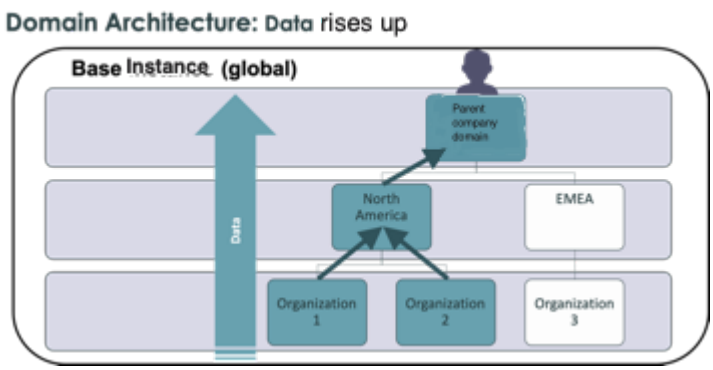
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le diagramme suivant montre comment le processus d'architecture se déroule jusqu'aux



domaines enfants.



Proposition de valeur de Domain Separation

Avec Séparation de domaine, les fournisseurs de services peuvent disposer d'une architecture d'instance mutualisée qui fournit des offres de manière efficace et sécurisée à leurs clients. Des normes de processus universelles solides, une conception de processus axée sur les données, une gouvernance stricte et une administration centralisée contribuent à maximiser ces avantages.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantages de Domain Separation

Les locataires d'un domaine bénéficient d'un retour sur investissement rapide, de frais administratifs réduits et de l'exploitation des services aux entreprises fournis par les propriétaires d'instances.

Voici un aperçu rapide de ces avantages.

Propriétaire de l'instance	Locataires de domaines
Productivité des employés du fournisseur de service	Sécurité accrue
Seuls les deltas de processus maintenus	Processus et fonctionnalités prédéfinis
Efficacité de l'administration	Réduction du personnel requis
Moins d'intégrations clients	Une intégration plus rapide
Mise à niveau et évolutivité	Exploitation des dernières versions
Ségrégation des données	Services fournis par le propriétaire de l'instance
Rapports globaux	

Définition de Séparation de domaine

Avec Séparation de domaine (également connue sous le nom d'architecture de plateforme mutualisée), vous pouvez séparer les données d'application, l'interface ServiceNow® utilisateur et la logique métier dans une instance client unique qui prend en charge la modélisation hiérarchique avec l'intelligence inter-locataire (client).

Propriétés de Domain Separation

Les applications séparées ServiceNow par domaine sont définies avec les propriétés suivantes :

Séparation des données

Permet aux clients de voir uniquement les données pour lesquelles ils ont l'autorisation. Les clients peuvent avoir accès à d'autres données client, mais ne peuvent pas interroger les données client s'ils n'y ont pas accès.

Séparation de l'interface utilisateur

Prend en charge une expérience spécifique au client pour les éléments d'interface utilisateur tels que les vues, les listes, les étiquettes, etc.

Séparation de logique métier

Prend en charge les politiques système spécifiques au client telles que les notifications par e-mail, les règles métier, les scripts clients, la politique d'interface utilisateur et les actions d'interface utilisateur.

Modélisation hiérarchique

Prend en charge la mutualisation imbriquée afin que les locataires parents (clients) puissent accéder aux ressources client enfant. La logique métier pour les clients parents s'exécute automatiquement pour les clients enfants et peut être remplacée à n'importe quel niveau.

Connaissance inter-clients (champ d'application de domaine)

Gère automatiquement les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires qui ont accès à des données de locataire supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Hiérarchies Domain Separation

Créez une hiérarchie lorsque vous définissez une architecture de domaine afin de suivre vos processus et workflows.

Exemples de hiérarchies Domain Separation

Le diagramme suivant est un bon point de départ pour définir l'architecture de domaine. Il montre la relation entre les domaines TOP et inférieurs et comment le processus, les données et les règles métier ont un impact sur les domaines parent et enfant.

- Dans l'exemple suivant, TOP est un domaine de processus. Il ne doit jamais contenir d'utilisateurs. À la place, TOP doit contenir les nouveaux processus que les propriétaires d'instances développent et les remplacements vers ces processus à partir du domaine global.
- Seul le fournisseur de service (SP) a accès au domaine par défaut. Ce domaine ne contient jamais d'utilisateurs actifs. Il contient uniquement les données « perdues » que vous devez réaffecter au domaine approprié.

  Remarque :
  Lorsque les données ne sont pas affectées à un domaine spécifique, elles se déplacent vers le domaine par défaut. Elles sont alors temporairement « perdues » et doivent être affectées au domaine approprié.

- Les tâches et les utilisateurs sans domaine sont placés automatiquement dans le domaine par défaut lorsque vous créez ou mettez à jour des domaines. Vous pouvez remplacer cette action en effaçant l'option **Par défaut** sur cet enregistrement ou en sélectionnant l'option **Par défaut** sur un autre enregistrement de domaine. Si vous n'avez pas encore défini de domaine par défaut, les tâches et les utilisateurs sans domaine se déplacent vers le domaine global.
  - Ne déplacez pas les données entre les domaines lorsque vous utilisez l'instance.
  - Si des données finissent dans le domaine par défaut, cela signifie que vous avez un problème de configuration ou de procédure à résoudre.

Vous ne voyez pas le mot « Global » dans ce diagramme car il n'y a pas de domaine global. N'oubliez pas que « global » se traduit par l'absence d'un domaine dans un enregistrement.

Par exemple, lorsqu'une table n'a aucun champ de domaine, cela signifie qu'elle contient tous les enregistrements globaux. Lorsqu'une table possède un champ de domaine, cela signifie que tout enregistrement sans domaine est un domaine global.

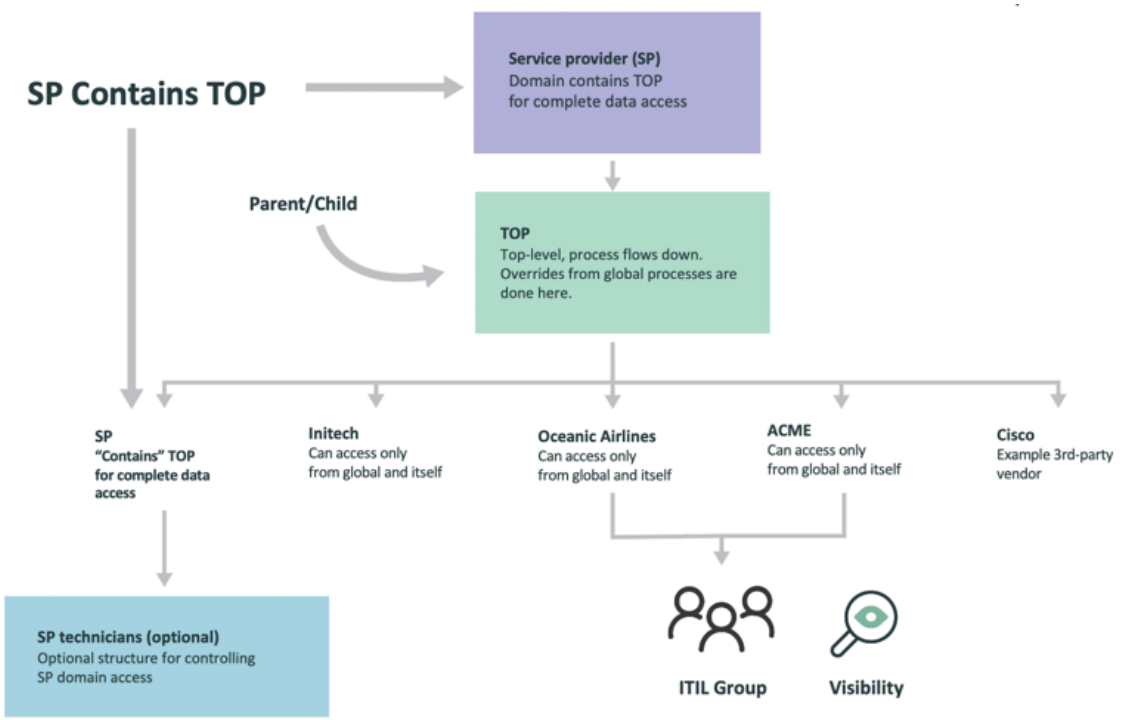
Le mot « global » se trouve dans le champ Domaine. Il y est placé automatiquement lorsque l'enregistrement n'a pas de domaine.

Les enregistrements globaux sont disponibles pour tous les utilisateurs de l'instance, sauf s'ils sont restreints par des configurations de sécurité.

- Utilisez le domaine par défaut pour vous assurer que les enregistrements ne finissent pas dans le domaine global sur des tables qui ne doivent jamais avoir d'enregistrements globaux.
- Les propriétaires d'instances doivent ensuite trier les enregistrements dans le domaine par défaut et les déplacer vers le domaine approprié.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Hiérarchies de domaines

- Parent/Child (Parent/enfant) : processus et données affectés
  - Conception basée sur un flux de processus.
  - N'oubliez pas que les domaines parent peuvent accéder à toutes les données des domaines enfant.
- Domaine « Contains » : seules les données sont affectées. Par exemple, l'ajout d'un SP dans le TOP Contains du diagramme n'entraîne pas l'exécution des processus du SP dans le domaine TOP et dans les domaines vers le bas.
  - Accorde des droits d'accès aux données aux personnes de groupes qui ont besoin d'un accès dédié à certains domaines.
  - Contient des causes ou des conditions à ajouter aux requêtes de base de données qui peuvent entraîner des problèmes de performance avec des ensembles de données et de domaines volumineux.
- Visibility (Visibilité) : hiérarchie qui est toujours visible par les utilisateurs une fois que vous fournissez l'accès. Seules les données sont affectées, et non les processus.
  - Accorde l'accès aux données d'un domaine à un autre domaine qui n'avait pas cet accès lors de la création de la hiérarchie parent-enfant.
  - Permet aux utilisateurs de voir toutes les données dans les domaines pour lesquels ils ont une visibilité d'accès, tout le temps, quel que soit l'enregistrement sur lequel ils travaillent.

> **Remarque :**
> Utilisez cette option avec parcimonie, car la visibilité peut entraîner un accès complet que vous n'avez peut-être pas l'intention d'accorder.

Principes de base de la définition d'une hiérarchie des domaines

Cas d'utilisation avec et sans restriction pour la séparation de domaines.

Traduction automatique

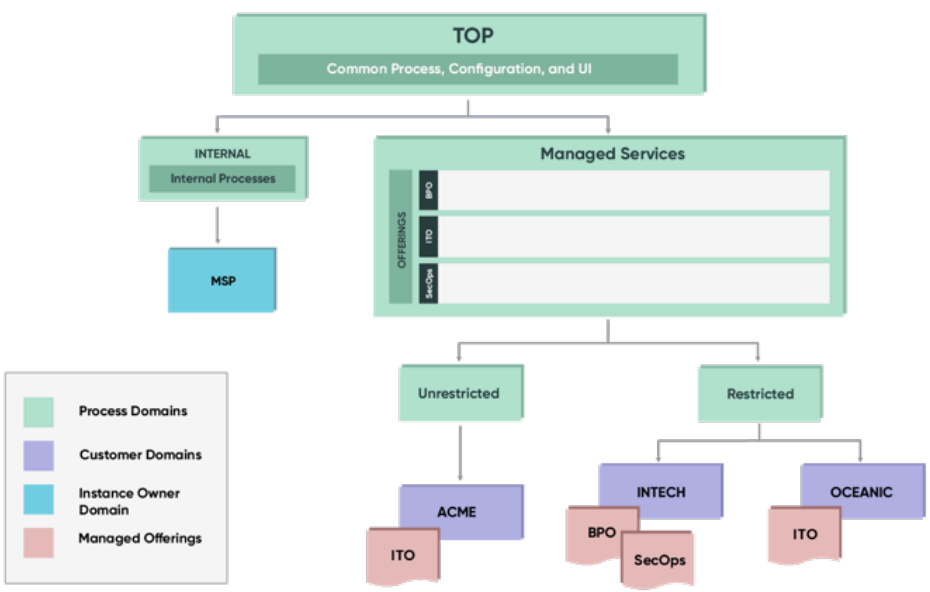
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

De nombreux SP ont des clients qui déclarent implicitement que l'accès à leurs domaines doit être fortement réglementé, ce qui restreint l'utilisation de la fonction « contains » dans le domaine TOP. Le diagramme suivant explique comment atténuer cette réglementation en divisant les domaines en domaines avec restriction (Restricted) et sans restriction (Unrestricted).

1. Les clients se trouvent dans un « vertical » spécifique de la hiérarchie de séparation de domaines Cela signifie qu'ils n'utilisent que des processus définis dans leur domaine et tous les domaines parent au-dessus du leur dans la hiérarchie. Tous les processus définis dans les domaines qui ne sont pas dans leur hiérarchie parent-enfant linéaire ne s'appliquent pas.

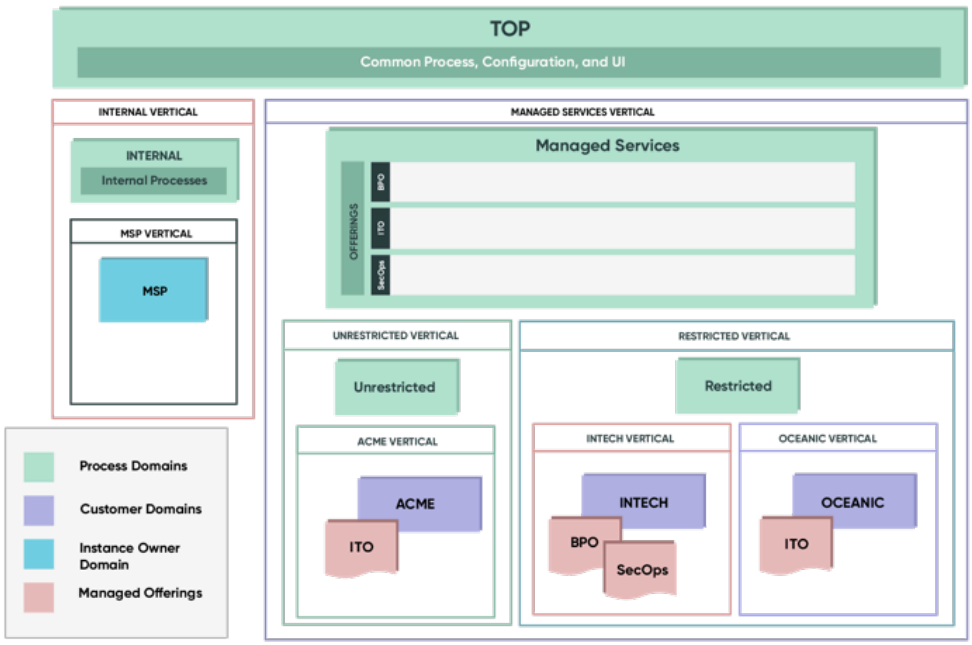
   Remarque :
   Les clients ou « locataires » sont des entités qui sont séparées les unes des autres, contrairement aux départements ou aux unités business, qui se partagent les ressources entre elles.

2. Les super verticaux (restreints, services de gestionnaire, etc.) sont autorisés tant que les clients n'appartiennent qu'à l'un d'eux.
3. Les services, produits ou offres qui doivent être disponibles horizontalement pour tous les clients ne sont pas définis dans des hiérarchies de domaines distinctes.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Voici quelques cas d'utilisation :

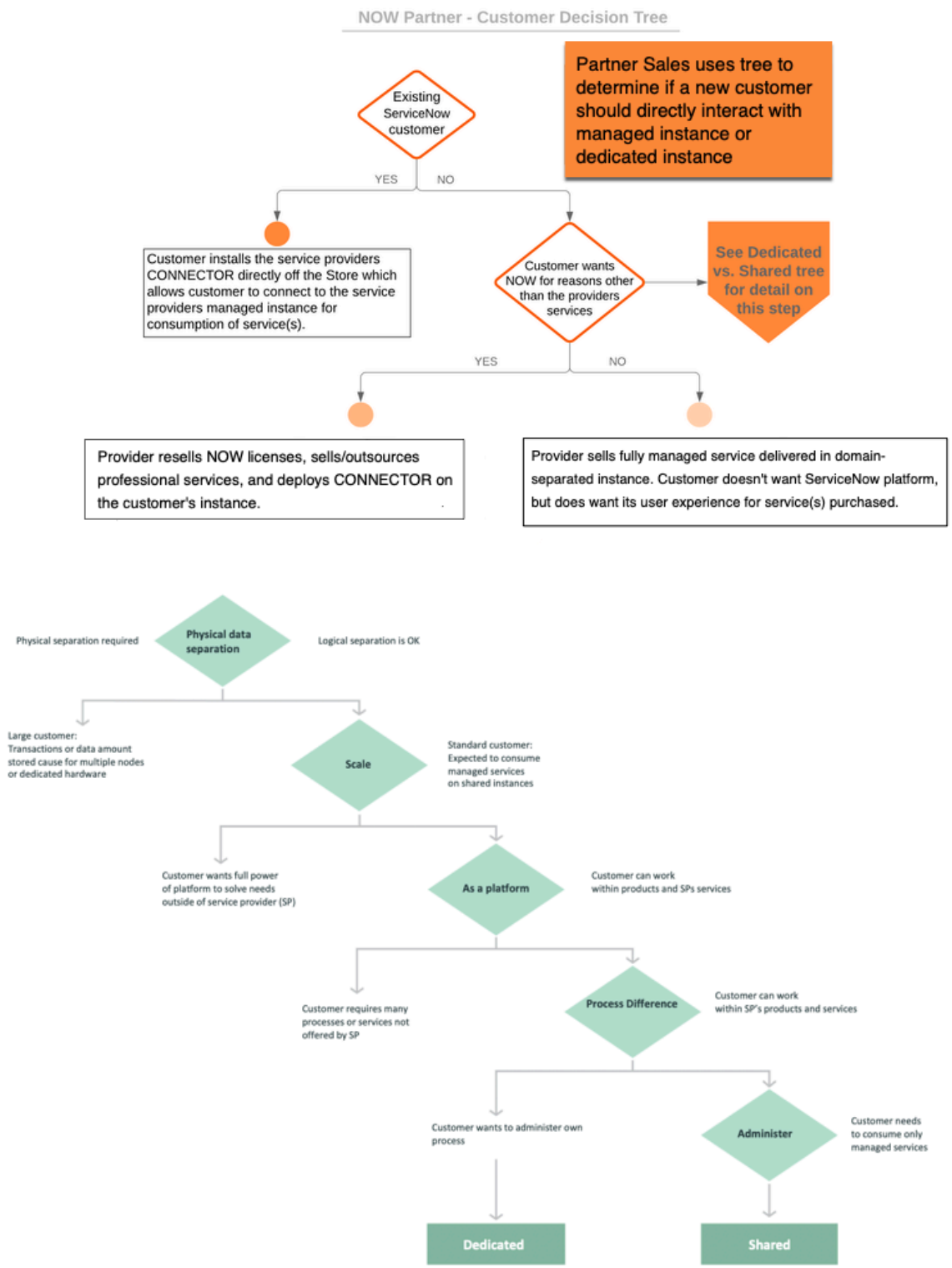
- Sous TOP, vous pouvez créer deux domaines, *Unrestricted* (Sans restriction) et *Restricted* (Avec restriction).
  - Placez les clients et leurs domaines qui n'ont pas de visibilité SP sous Unrestricted.
  - Placez les clients et leurs domaines qui ont cette exigence sous Restricted.
- Les administrateurs système peuvent alors utiliser les fonctions « contains » et « visibility » de manière efficace et ciblée.
  - Appliquez « contains » à Unrestricted pour qu'un seul « contains » puisse accorder une visibilité à la plupart des clients.
  - Appliquez la visibilité de domaine à des domaines spécifiques selon les besoins à l'aide de « groupes de visibilité de domaine ».

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Arborescences des décisions client

Le diagramme suivant montre comment choisir le modèle de hiérarchie qui vous convient. Vous pouvez choisir des hiérarchies distinctes, hybrides ou partagées, en fonction des processus et des fonctionnalités souhaités dans vos structures de domaine.



Pour en savoir plus sur l'architecture des hiérarchies, consultez Architecture de référence du fournisseur de services.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

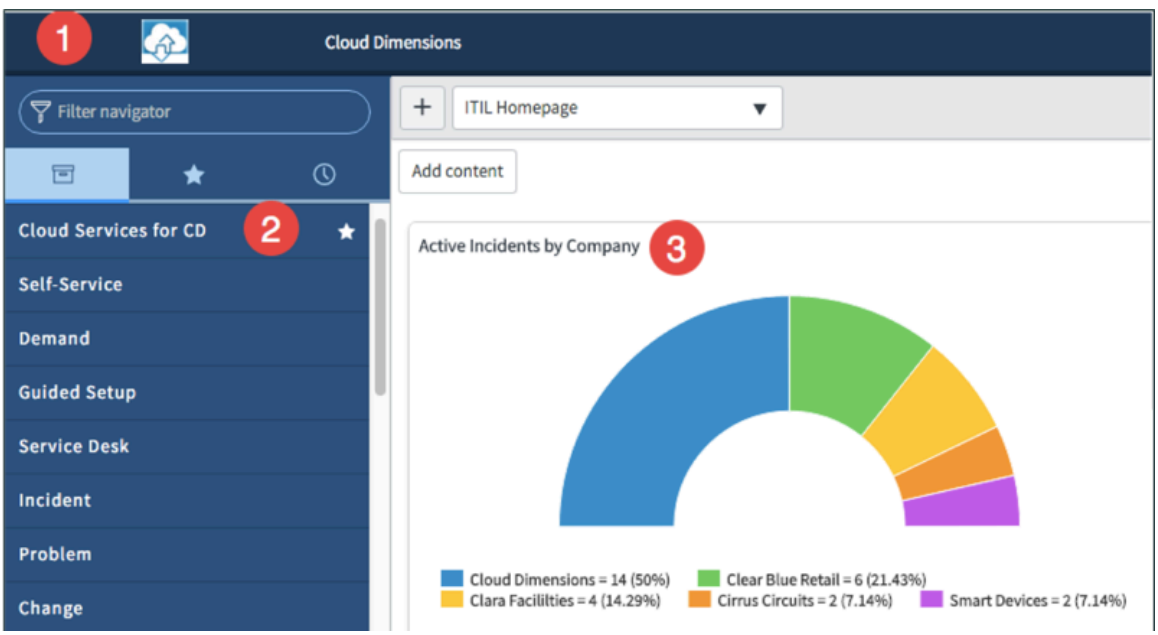
Traduction automatique

Séparation de contexte et de domaine

Le contexte de la session d'un utilisateur détermine les processus, les données et l'interface utilisateur lorsque l'utilisateur parcourt les vues de listes, les pages d'accueil, les rapports et les articles de la base de connaissances. Le contexte est déterminé par les processus que vous créez, les règles métier que vous définissez, vos workflows et d'autres facteurs.

Contexte de la session de l'utilisateur

De nombreux facteurs déterminent le contexte d'une session utilisateur, tels que les profils d'utilisateurs, les groupes, les critères de société, etc. Dans le diagramme suivant, vous voyez que les incidents créés par une entreprise font partie du contexte.



Dans cet exemple, l'utilisateur dispose d'un domaine d'accueil Cloud Dimensions.

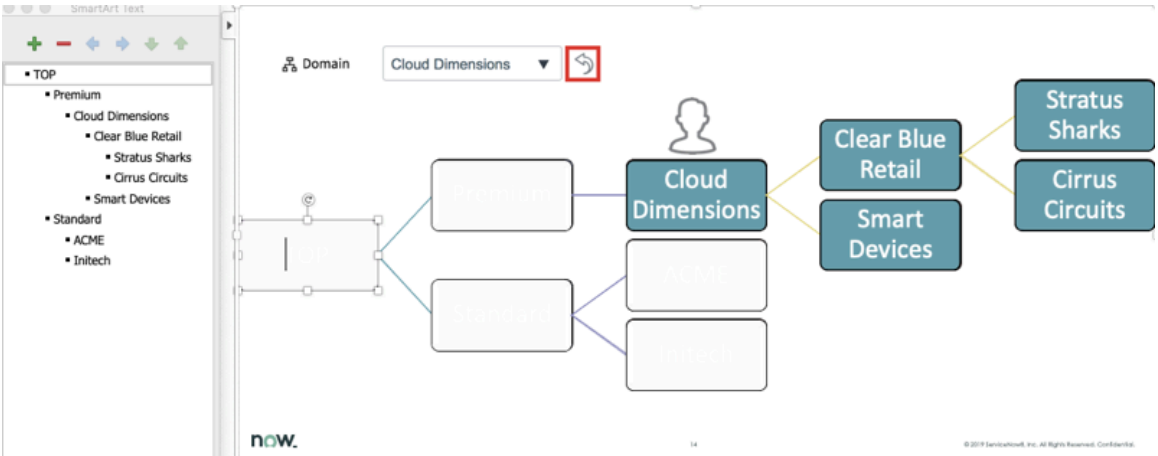
1. La marque reflète les paramètres du domaine Cloud Dimensions et de l'enregistrement de société.
2. Le navigateur d'application affiche les éléments qui sont hérités des domaines de niveau supérieur, ainsi que les modules qui sont définis dans le domaine Cloud Dimensions.
3. Les pages d'accueil et les données de liste reflètent les données visibles par l'utilisateur. Ces données sont basées sur le contexte de la session de l'utilisateur. Dans ce cas, l'utilisateur dans le domaine Cloud Dimensions peut voir les données dans Cloud Dimensions, les domaines enfants et le domaine global.

Début du contexte de la session de l'utilisateur dans le domaine d'accueil

Dans le schéma suivant, vous pouvez voir les éléments du contexte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'administrateur système définit les domaines d'accueil des utilisateurs sur leurs enregistrements utilisateur. En règle générale, le domaine d'accueil d'un utilisateur est défini sur le même domaine que le domaine de sa société. Lorsque l'utilisateur se connecte, le sélecteur de domaine se définit automatiquement sur le domaine d'accueil de l'utilisateur. Les utilisateurs peuvent revenir à leur domaine d'origine à tout moment en cliquant sur l'icône flèche dans le sélecteur de domaine.

La liste du sélecteur de domaine inclut les domaines situés dans le contexte de la session de l'utilisateur. Les utilisateurs peuvent limiter davantage le contexte de leur session en sélectionnant des domaines enfants à l'aide du sélecteur.

Le contexte de la session utilisateur inclut le domaine d'accueil de l'utilisateur et tous les domaines enfants. Cet ensemble de domaines dans le contexte de la session de l'utilisateur est ajouté automatiquement à chaque requête envoyée à la base de données. De cette façon, les résultats sont limités aux données de ces domaines et aux données globales. Ce processus est intégré dans le code compilé qui n'est pas accessible.

Les comptes de service utilisés pour les intégrations ont également un contexte de session utilisateur. Il existe un contexte utilisateur et un contexte d'enregistrements, chacun avec ses propres données dans son propre domaine. Ces contextes affectent les intégrations. Les requêtes de base de données (enregistrements) sont limitées de la même manière que les utilisateurs interactifs (utilisateurs), ce qui signifie qu'elles fonctionnent normalement mais sont limitées par les contraintes que le développeur a configurées.

Pour en savoir plus sur d'autres méthodes d'ajout de domaines au contexte de la session d'un utilisateur, consultez Architecture de référence du fournisseur de services.

Contexte d'enregistrement

Lorsqu'un utilisateur explore des enregistrements individuels, le contexte de l'enregistrement est activé. Le contexte d'enregistrement détermine les éléments d'interface utilisateur et les processus à appliquer à l'enregistrement.

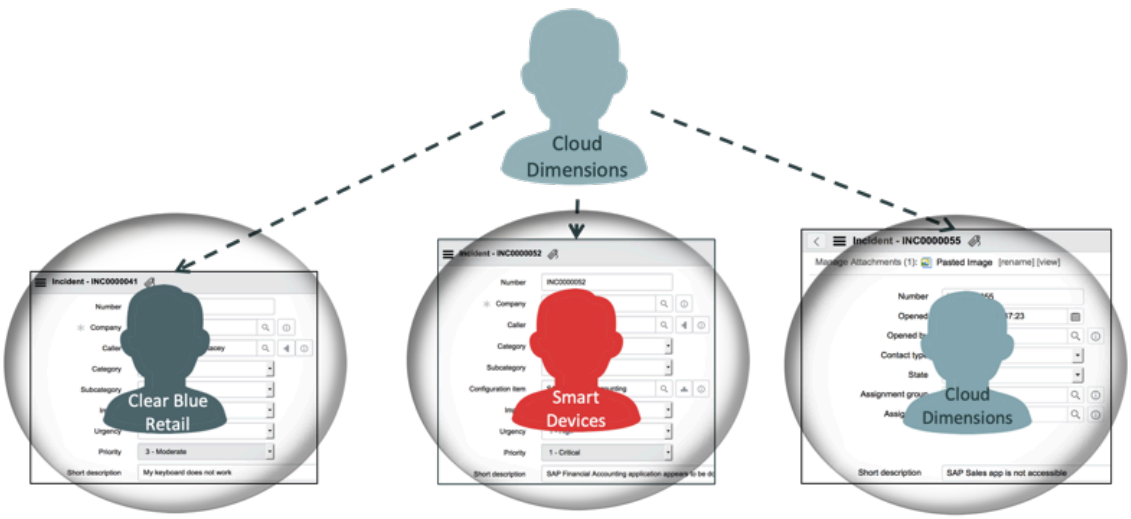
Le domaine d'un enregistrement dicte le processus, les données et la disponibilité des éléments d'interface utilisateur au sein de l'enregistrement.

Remarque :

- Le contexte d'enregistrement persiste même si le domaine de l'utilisateur change.
- Les utilisateurs peuvent afficher les enregistrements simultanément dans plusieurs onglets de navigateur, tout en conservant leur propre contexte d'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

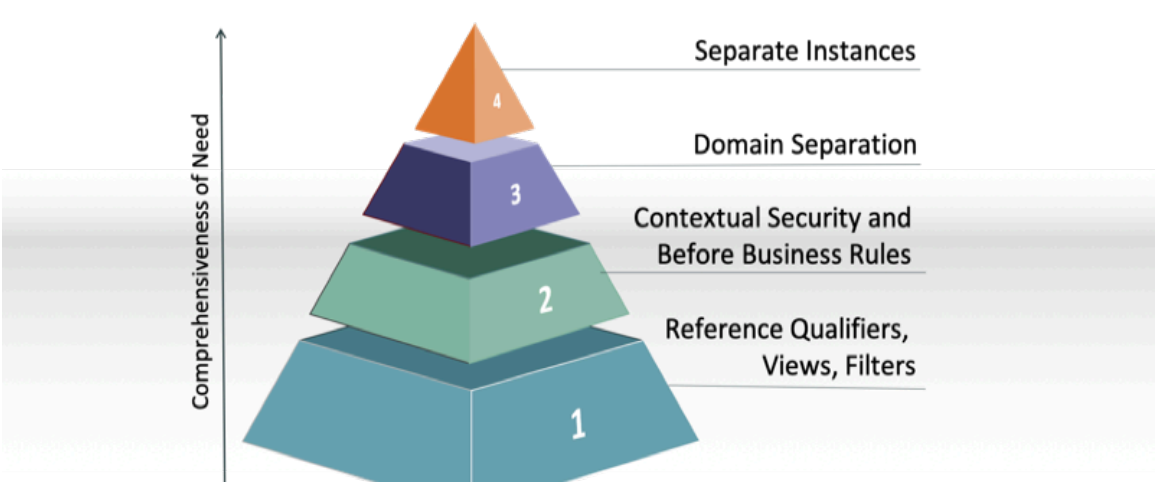


Ségrégation et sécurisation des données avec Domain Separation

Vous pouvez séparer et sécuriser les données sur la ServiceNow plateforme de plusieurs façons, en fonction des besoins de votre client.

Ségrégation des données de plusieurs façons

Le diagramme suivant montre quatre façons de séparer les données. Vous pouvez utiliser des instances distinctes, la séparation de domaine, la sécurité contextuelle et les règles métier, ainsi que l'architecture de référence elle-même pour séparer les données.



Vous pouvez séparer les données de ces quatre façons :

1. Personnalisation de l'architecture de référence avec des qualificatifs et des filtres afin que les départements et les groupes d'une entreprise puissent se concentrer sur leur propre travail. En séparant les données entre ces départements ou groupes, un département ou un groupe ne peut pas voir les enregistrements d'un autre département ou groupe.
2. Ajout de règles métier de sécurité contextuelle et Before Query comme couches de sécurité supplémentaires pour se prémunir contre les violations de données. Consultez Séparation de contexte et de domaine et Avant les règles métier de requête pour en savoir plus sur Séparation de domaine et les règles métier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Ajouter un niveau de sécurité supplémentaire dans une entreprise en utilisant la séparation de domaine. Les données de chaque requête de base de données sont limitées aux données visibles dans un domaine avant l'exécution de la sécurité contextuelle et des règles métier.
4. Utilisation d'instances distinctes pour séparer les données au niveau de la couche de base de données et d'application.

Les instances distinctes, la séparation de domaine, la sécurité contextuelle et les règles métier, ainsi que l'architecture de référence sont des moyens de séparer les données. Ces quatre voies sont liées les unes aux autres, comme l'indique la flèche d'exhaustivité des besoins dans le diagramme. La façon dont chaque couche interagit avec les autres couches dépend de la façon dont vous configurez votre configuration Séparation de domaine.

Toutes les organisations n'exigent pas la séparation de domaine. Vous pouvez trouver d'autres alternatives, telles que des instances distinctes ou une instance unique sans domaine. Pour en savoir plus sur ces alternatives, reportez-vous à la section Évaluation de la nécessité d'une séparation de domaine.

Intelligence entre locataires

Une architecture mutualisée est l'instance unique desservant plusieurs locataires. Les données, les métadonnées, la logique métier et le contexte de traitement pour les locataires sont automatiquement traités avec l'accès aux données de locataire supplémentaires.

Locataires uniques et multiples

Instance à locataire unique

Vous êtes client ServiceNow , vous avez acheté les licences, et c'est à vous de décider quels services vous voulez. Vous pouvez effectuer une mise à niveau quand vous le souhaitez, voir des aperçus de toutes les nouvelles fonctionnalités et configurer votre instance immédiatement. Le fait d'être un locataire unique présente les avantages et les restrictions suivants :

- Vous avez des coûts initiaux et des frais administratifs plus élevés, mais vous avez plus de liberté pour remodeler et agrandir.
- Vous avez des coûts plus élevés pour obtenir et maintenir le personnel d'administration de l'instance et de l'approvisionnement. Bien que vous soyez libre d'aménager l'environnement au besoin, vous devez vous conformer aux ServiceNow pratiques et aux normes recommandées.

Instance à locataires multiples

Quelqu'un d'autre est propriétaire de l'instance, éventuellement un fournisseur de service avec plusieurs clients. Ils effectuent une mise à niveau quand ils le souhaitent et mettent de nouveaux services sur l'instance lorsqu'ils le souhaitent. Si vous êtes client d'un fournisseur de services, vous êtes probablement sur son instance parce que vous vouliez ce qu'il propose. Les locataires multiples présentent les avantages et les restrictions suivants :

- Un personnel centralisé gère les configurations, les intégrations et les mises à niveau.
- Le propriétaire de l'instance fournit des services supplémentaires.
- Les locataires de domaine ont des coûts initiaux moins élevés pour utiliser la ServiceNow plate-forme, ont des coûts mensuels moins élevés parce qu'ils

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

la partagent avec de nombreux locataires et n'ont pas besoin d'employer du personnel pour administrer l'environnement.

- Avantages partagés à partir de demandes ou de changements initiés par d'autres locataires.

Alternatives à Domain Separation

Vous pouvez utiliser une instance distincte comme alternative à Séparation de domaine pour vos clients. Une instance distincte vous offre la flexibilité nécessaire pour répondre aux exigences de séparation des données au sein des groupes et des départements d'une organisation avec peu ou pas d'impact sur les autres.

Instances distinctes

Avantages et inconvénients des instances distinctes

Instance distincte	Instance unique : sans domaine
Avantages	**Avantages**
Conçu pour répondre aux besoins de chaque client/organisation	Peut s'adresser à des scénarios simples
Minimiser l'impact de la personnalisation sur les autres	Coût
Coordination du calendrier de mise en production	**Contre**
Séparation nette	Modifications importantes du code de base de référence
Choisir la région CENTRE DE DONNÉES	Code du système de base modifié ignoré pendant les mises à niveau
Contre	Doit également s'adresser à toutes les tables secondaires et de support
Coût	Des tests approfondis sont requis
Alignement des instances	Aucune équipe produit pour ServiceNow faire évoluer votre code personnalisé
Effort de test pour les mises à niveau	
Duplication des efforts	
Intégrations requises	

Vous pouvez chronométrer les mises à niveau et les versions séparément pour chaque instance. Toutefois, si vous choisissez d'utiliser des instances distinctes, vous devez effectuer une coordination importante avec d'autres personnes qui administrent les instances. En configurant une instance avec une sécurité contextuelle, des vues de formulaire, des qualificatifs de référence, des filtres et des conditions robustes, vous n'avez pas besoin d'utiliser Séparation de domaine dans votre entreprise.

Une instance distincte vous permet de traiter la séparation des données et des processus, mais vos propriétaires d'instances doivent gérer et suivre les personnalisations étendues requises pour des instances distinctes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Séparation de contexte et de domaine

Architecture de référence du fournisseur de services

Évaluation de la nécessité d'une séparation de domaine

Vous constaterez peut-être que Séparation de domaine ne fonctionne pas toujours pour les organisations de vos clients. Il est préférable que vous basiez votre décision d'opter pour la séparation de domaine en examinant les besoins de vos clients.

Évaluation de la nécessité d'une séparation de domaine

Motifs de séparation de domaine

Ces facteurs peuvent vous aider à choisir Séparation de domaine pour les organisations de vos clients :

- Vos clients ont un alignement modéré des processus et des exigences générales de la plateforme.
- Vos clients prévoient de travailler sur des tâches en tant que prestataires plutôt qu'en tant que demandeurs.
- Vos clients ont un accord contractuel qui exige que les enregistrements de données soient isolés, mais votre propriétaire d'instance a déterminé que le besoin peut être pris en compte ailleurs dans la configuration.
- Les propriétaires de l'instance de votre société possèdent des entités entières qui fonctionnent comme des organisations physiquement distinctes et ne partagent pas de données, mais la génération de rapports complète est toujours requise. Des domaines distincts permettraient la visibilité des données lorsqu'ils sont configurés correctement.

Raisons pour lesquelles il n'y a pas de séparation de domaine

Ces facteurs peuvent indiquer des raisons pour lesquelles les organisations de vos clients pourraient ne pas vouloir configurer Séparation de domaine :

- Vos clients veulent administrer leur environnement, en avoir la pleine propriété et définir la feuille de route pour l'expansion.
- Vos clients exigent que les données et les processus au niveau physique ou de la base de données soient complètement isolés.

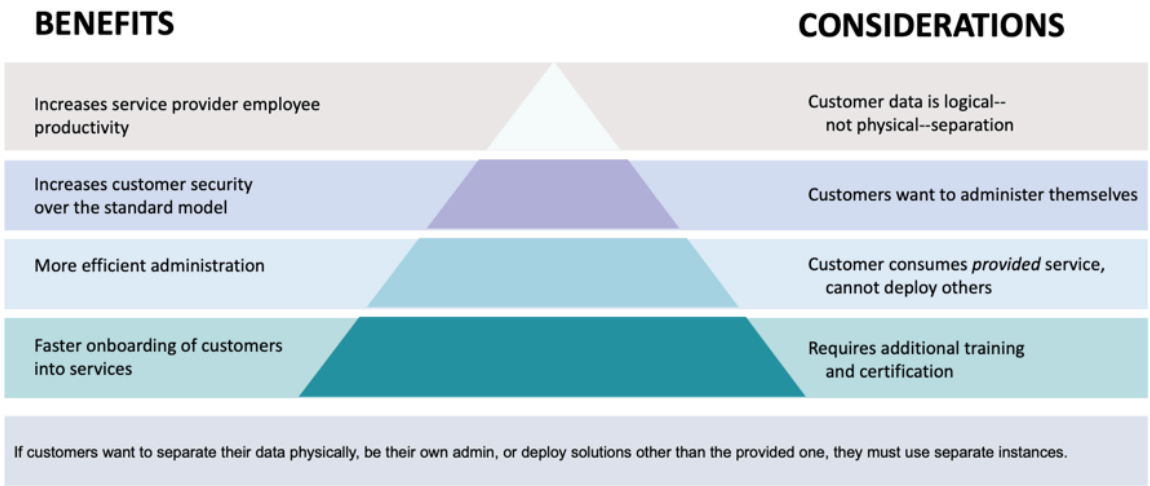
Remarque :

Les instances séparées par domaine contiennent une base de données partagée, ce qui réduit l'exigence d'isolement.

- Les départements de l'organisation de vos clients souhaitent isoler les enregistrements. (Des contrôles d'accès peuvent suffire.)
- Vos clients veulent tous leurs propres processus, règles métier et workflows.
- La culture d'entreprise est celle de la non-collaboration entre les organisations de vos clients.
- Vos clients interagissent avec la plateforme en tant qu'utilisateurs finaux uniquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

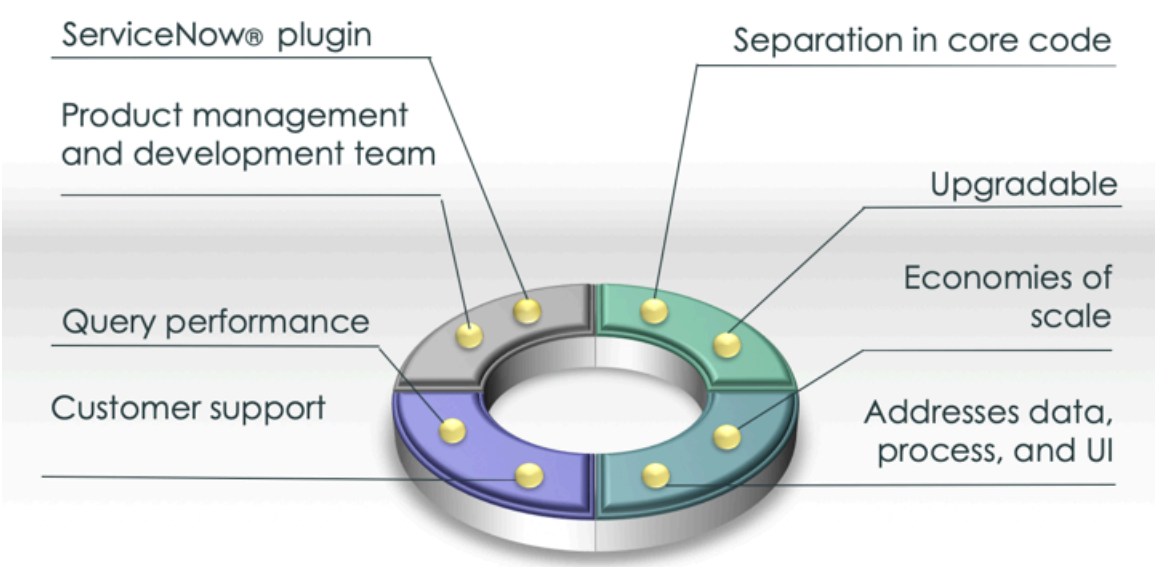


Avantages de Domain Separation

La séparation de domaine peut être plus efficace pour les organisations de vos clients que toute autre méthode de séparation des données entre les groupes et les départements.

Les avantages de Domain Separation en un coup d'œil

Vous pouvez activer Séparation de domaine à l'aide d'un module d'extension ServiceNow dont les fonctionnalités sont intégrées à la plateforme principale. La configuration de domaines distincts est gérée par un chef de produit assisté d'une équipe de développement. Des améliorations et des correctifs pour la fonctionnalité Séparation de domaine sont inclus dans ServiceNow les versions et prêts à être utilisés par les clients. Pour obtenir de l'aide concernant Séparation de domaine, les propriétaires de votre instance peuvent utiliser Service et assistance client des ressources, telles que le Portail de services .



Fonctionnement d'une requête de base de données avec Séparation de domaine

L'utilisation de requêtes de base de données avec séparation de domaine dans les applications de vos clients les aide à protéger leurs données. Ces requêtes accélèrent ensuite les processus de configuration et de construction.

Traduction automatique

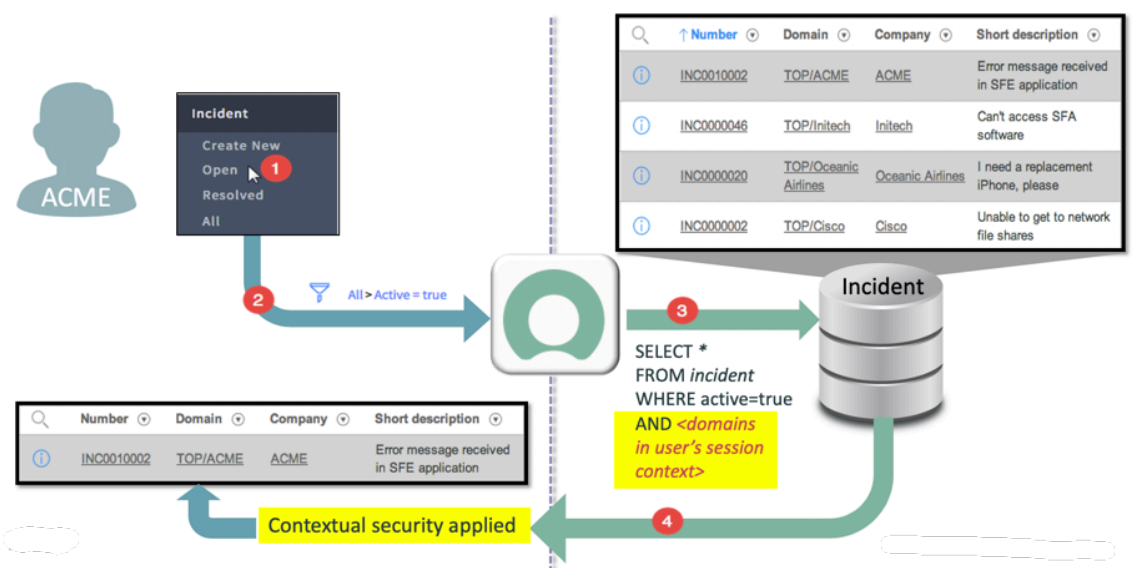
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment Domain Separation protège les données

Dans la figure suivante, la table Incident [incident] possède un champ de domaine hérité de la tâche de l'incident. Lorsque ce champ de domaine s'affiche, vous savez que les enregistrements de la table peuvent avoir des affectations de domaine.

Lorsque les utilisateurs se connectent, leur domaine d'accueil apparaît avec l'ensemble des domaines auxquels ils peuvent accéder. C'est ce qu'on appelle le contexte de la session de l'utilisateur. Pour plus d'informations sur les contextes de session, reportez-vous à la section Séparation de contexte et de domaine.

Requête de base de données avec séparation de domaine



1. Dans un navigateur, l'utilisateur de l'une des sociétés, Acme, sélectionne le module Incidents ouverts pour afficher tous les incidents où actif = vrai.
2. Le filtre active=true est soumis à l'application.
3. L'application envoie ensuite une requête à la base de données en ajoutant une clause WHERE à active=true. La clause WHERE limite les enregistrements d'incidents qui sont renvoyés aux enregistrements qui se trouvent dans le domaine de l'utilisateur ou aux domaines auxquels l'utilisateur peut accéder. Seuls les enregistrements de ces domaines sont renvoyés à l'application pour traitement.
4. La sécurité contextuelle est appliquée, ce qui limite davantage les données renvoyées à l'utilisateur. Les enregistrements d'incidents apparaissent dans la liste Incidents ouverts.

Remarque :

Lorsque vous appliquez la sécurité contextuelle, vous limitez les données qui sont renvoyées à l'utilisateur. Ces limites protègent d'autres contenus que vous ne souhaitez peut-être pas que les utilisateurs voient.

Pour en savoir plus sur la sécurité contextuelle, reportez-vous à la section Séparation de contexte et de domaine.

Remarque :

Cette logique de traitement s'applique à toutes les requêtes adressées à la base de données, y compris celles qui sont déclenchées à l'aide d'intégrations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveaux de prise en charge de Domain Separation

Choisissez parmi trois catégories pour la séparation de domaine d'une application pour les organisations de vos clients.

Les applications qui prennent en charge Séparation de domaine peuvent prendre en charge la séparation des données et le routage des données uniquement, disposer d'une séparation avancée de la logique métier ou prendre en charge l'administration de l'application au niveau du locataire (client). Ces définitions définissent les niveaux de prise en charge du point de vue des cas d'utilisation réels et des personnes qui les implémentent.

Niveaux de prise en charge incrémentielle ServiceNow



Niveau	Type	Résumé
Aucune prise en charge		• Le champ Domaine peut exister dans les tables de données, mais il n'existe aucune logique métier pour gérer les données. • Ce niveau n'est pas considéré comme étant séparé par domaine.
Élémentaire	Gestion des données client	• Logique métier : garantit que les données parviennent au bon domaine pour les cas d'utilisation du fournisseur de services de l'application. • Dans l'application, l'interface utilisateur, les clés de cache, la génération de rapports, les déploiements, les agrégations, etc., tous prennent en compte les propriétés du domaine au moment de l'exécution. • Les propriétaires de votre instance doivent être en mesure de configurer l'application pour qu'elle fonctionne normalement sur plusieurs locataires. Cas d'utilisation : lorsqu'un fournisseur de service utilise la messagerie instantanée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau	Type	Résumé
		pour répondre au message d'un client, le client doit pouvoir voir la réponse.
Standard	Gestion des processus clients	• Inclut le niveau Basique • Logique métier : les processus peuvent être créés ou modifiés par client par le fournisseur de services. Les cas d'utilisation reflètent la façon dont l'application est utilisée par plusieurs clients fournisseurs de services dans une seule instance. • Les propriétaires de votre instance doivent être en mesure de configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par client pour l'application spécifique. Cas d'utilisation : l'administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un client, mais pas pour un autre client.
Amélioré	Configuration autogérée par le client	• Inclut les niveaux basique et standard • Permet aux clients du fournisseur de service de modifier la logique métier basée sur des cas d'utilisation définis. Ces configurations sont basées sur l'interface utilisateur et sont sécurisées de sorte que les configurations d'un client ne peuvent pas affecter un autre client. • Les clients de l'instance doivent être en mesure de configurer eux-mêmes la logique métier et les paramètres de données MVP. Cas d'utilisation : le client d'un environnement partagé doit être en mesure d'apporter des modifications en fonction de l'impact, de l'urgence ou de la priorité au sein d'un domaine.
Domaine effectif*		Dans certains cas, une fonctionnalité ou une application de plateforme peut prendre en charge les cas d'utilisation du fournisseur de service même si le cadre de travail du domaine n'est pas utilisé. Les cas d'utilisation doivent être détaillés pour prendre en charge Séparation de domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Niveau	Type	Résumé
		Un astérisque (*) après le niveau de support indique ce type de configuration. Cas d'utilisation : avant la version New York, il n'y avait pas de prise en charge de domaine, Catalogue de services mais les propriétaires d'instances pouvaient configurer des catalogues et des éléments distincts pour chaque locataire dans une instance séparée par domaine à l'aide de critères d'utilisateur. Il en résultait que chaque locataire pouvait utiliser Catalogue de services à un niveau standard.

Pour afficher toutes les applications répertoriées par niveau de prise en charge, reportez-vous à la section Prise en charge par les applications pour Domain Separation.

Résumé

Séparation de domaine est un cadre de travail que vous devez utiliser pour que vos applications soient conscientes de ses clients.

Tenez compte des options du cadre de travail de domaine, des cas d'utilisation d'entreprise de vos applications, des profils et de la façon dont ils utilisent l'application avant de pouvoir utiliser le cadre de travail pour rendre votre application prise en charge.

Architecture de référence du fournisseur de services

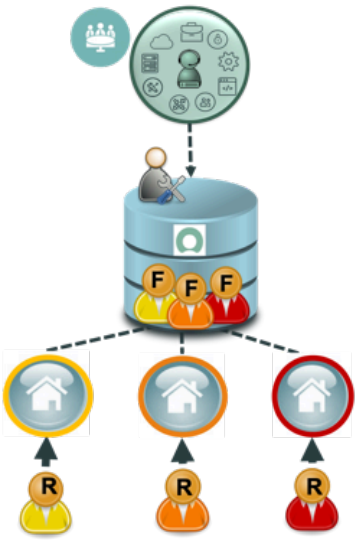
Vos clients peuvent accéder aux services du fournisseur de services (SP) à l'aide d'un portail conçu pour qu'ils atteignent leur instance séparée par domaine.

Attributs de base de l'architecture de référence du fournisseur de services

- Vous n'affectez pas de prestataires à un domaine. Au lieu de cela, vous les partagez entre les domaines. Il est donc plus difficile d'auditer le nombre de prestataires que vous avez par domaine.
- Vous pouvez partager et exploiter l'administration de domaine. Cela signifie qu'il n'y a pas de frais généraux et que vous pouvez optimiser les licences.
- Le nombre d'utilisateurs sur l'instance peut changer lorsque vous obtenez un nouveau client. Un nouveau client peut entraîner des dizaines, voire des centaines de milliers de nouveaux utilisateurs sur le système. Le nombre total d'utilisateurs est pratiquement illimité dans un environnement partagé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- SP customers access SP services via a portal to the SP Domain Separated instance
- SP uses ServiceNow shared instance(s) to manage their service delivery
- SP could have a shared instance per region to support data sovereignty requirements

Legend:

Centralized governance at the SP

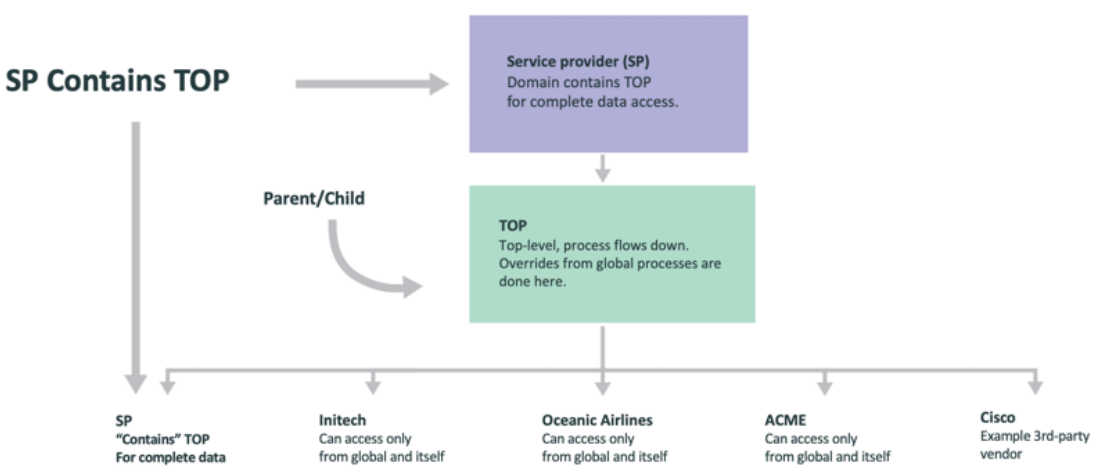
Centralized administration at the SP. Shared business requirements and configurations

Both SP and customer fulfillers on one instance

Customer requesters on each instance

Le portail des services du fournisseur de services est dédié ou partagé avec l'instance partagée du fournisseur de services. Les fournisseurs de services utilisent ServiceNow des instances partagées pour gérer leur prestation de services.

Hiérarchie de référence pour les instances séparées par domaine



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison de l'architecture de référence du fournisseur de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

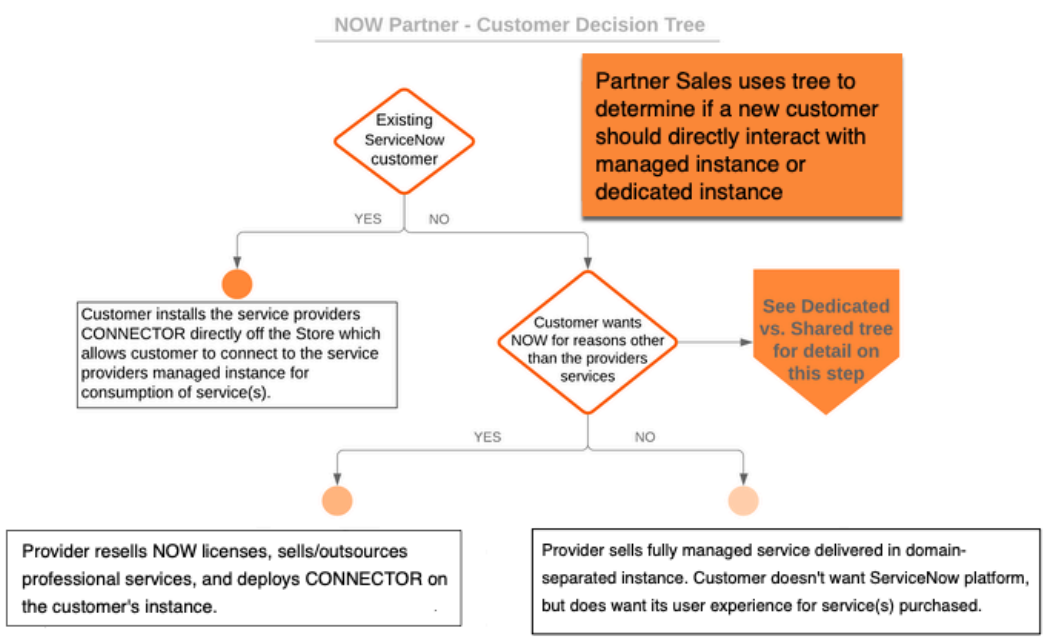
Architecture de référence du fournisseur de service Arbres de décision

Vous pouvez utiliser des arborescences de décision et un tableau comparatif pour déterminer si un nouveau client doit être ajouté à une instance partagée ou à sa propre instance dédiée.

Arborescences de décision

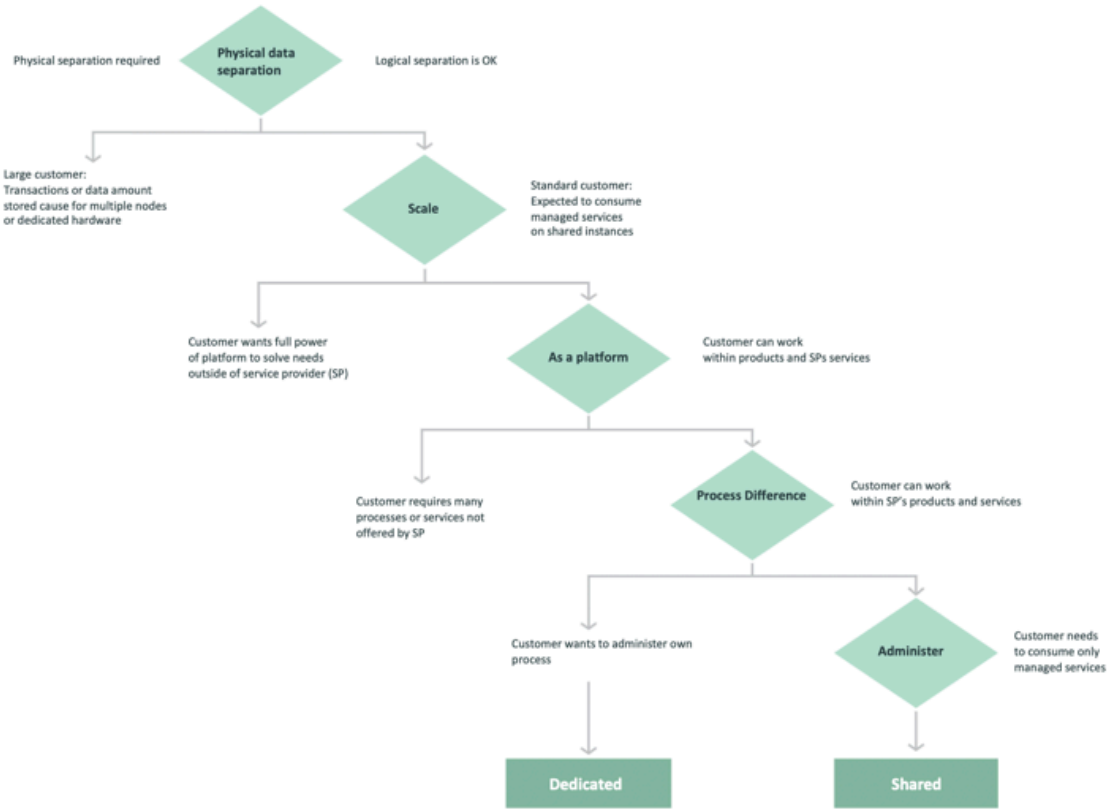
Utilisez ces arborescences de décision pour aider vos clients à décider s'ils doivent utiliser une instance gérée ou dédiée.

Arbre de décision du client



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comparaison de l'architecture de référence du fournisseur de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

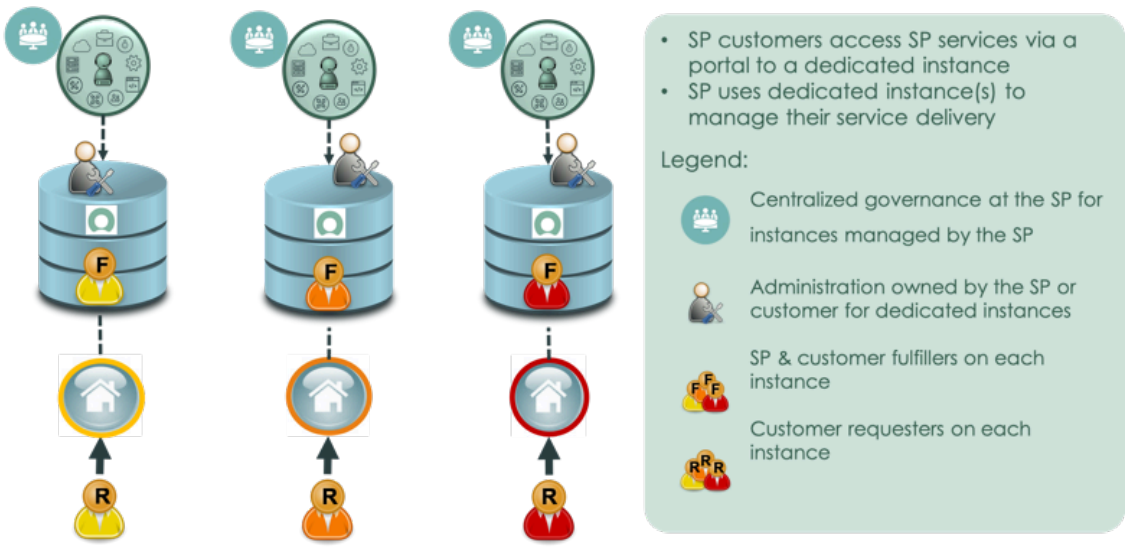
Architecture de référence du fournisseur de service pour les instances dédiées

Les clients des fournisseurs de services (SP) peuvent accéder aux services SP à l'aide d'un portail vers une instance dédiée. Les fournisseurs de services utilisent ces instances dédiées pour gérer leur prestation de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Instances dédiées



Attributs

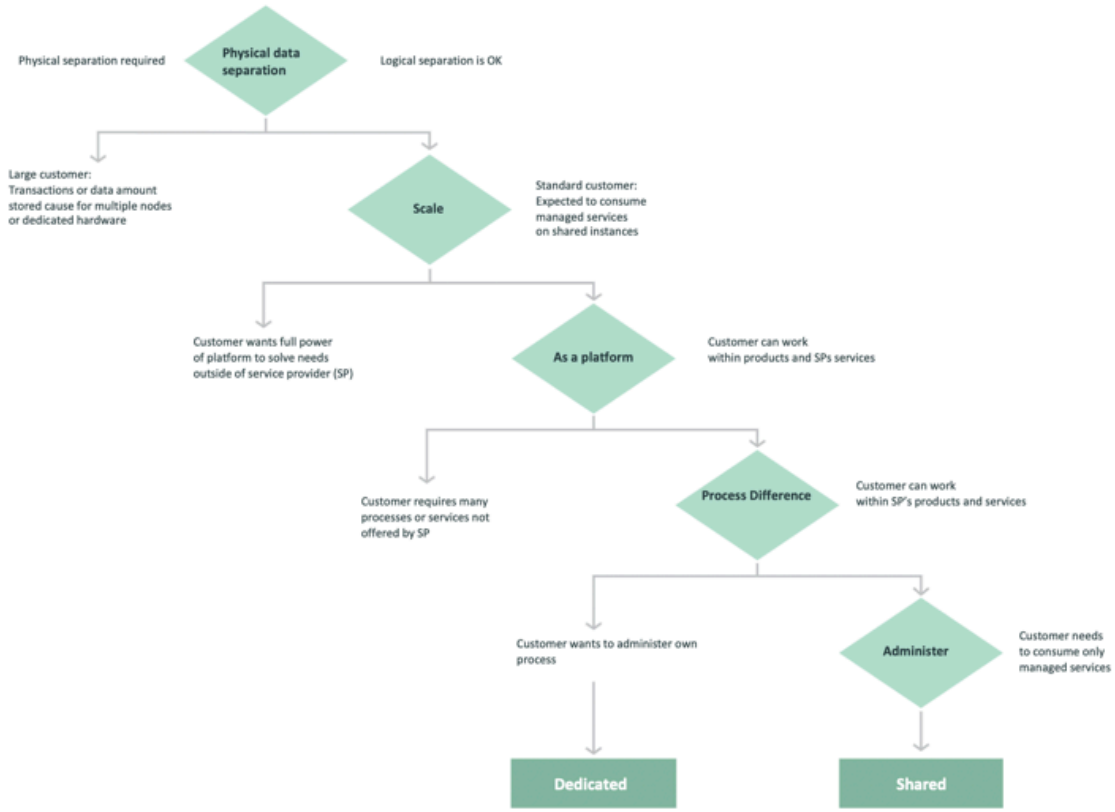
- Les instances dédiées nécessitent que vous disposiez d'une administration et d'équipes dédiées distinctes. Vous avez besoin de plusieurs licences pour les administrateurs et les développeurs qui se connectent à plusieurs instances.
- Chaque instance dispose d'un nombre limité de demandeurs et de prestataires. Lorsque vous obtenez un nouveau client, vous devez vous procurer une instance basée sur la taille et l'échelle de l'entreprise du client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Instance partagée

Instance dédiée ou partagée



Comparaison de l'architecture de référence du fournisseur de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

Architecture de référence du fournisseur de services pour hybride

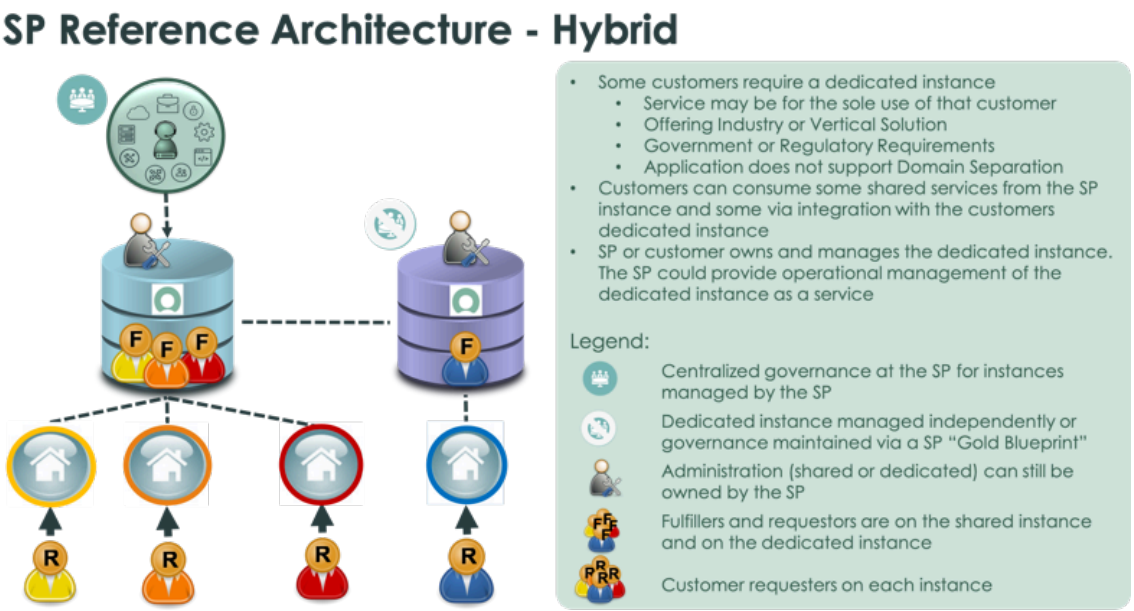
Utilisez l'architecture de référence du fournisseur de services hybrides (SP) pour obtenir une solution personnalisée. Vos clients ont besoin d'une instance dédiée pour un service spécifique. Ils peuvent toujours utiliser l'instance SP partagée pour d'autres services, mais cela nécessite l'intégration de chaque instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture hybride

Votre client peut être responsable de la livraison directe de ce service supplémentaire. Vous devez créer une solution hybride avec plusieurs attributs que votre client doit fournir.



Attributs

- Vous pouvez partager et exploiter l'administration de l'instance. Cela signifie qu'il n'y a pas de frais généraux et que vous pouvez optimiser les licences.
- S'il existe une nouvelle instance pour un environnement décentralisé, l'équipe de programme est responsable et financée en conséquence en tant qu'utilisateurs administrateurs dédiés pour cette instance. Dans un environnement centralisé où toutes les instances découlent d'un plan, vous avez besoin de licences d'administration en double.
- Vous n'affectez pas de prestataires à un domaine. Au lieu de cela, vous pouvez les partager entre les domaines.
- Si un client partage à la fois un environnement partagé et un environnement dédié, il a besoin d'un prestataire dans les deux environnements. Cela signifie plus de travail pour chaque équipe, car les processus pour les instances partagées et dédiées nécessitent un travail différent pour chaque instance.
- Le nombre d'utilisateurs sur l'instance peut changer lorsque vous obtenez un nouveau client. Un nouveau client peut entraîner des dizaines, voire des centaines de milliers de nouveaux utilisateurs sur le système. Le nombre total d'utilisateurs est pratiquement illimité dans un environnement partagé.
- Chaque instance dispose d'un nombre limité de demandeurs et de prestataires. Lorsque vous obtenez un nouveau client, vous devez vous procurer une instance basée sur la taille et l'échelle de l'entreprise du client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

servicenow

Comparaison de l'architecture de référence du fournisseur de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

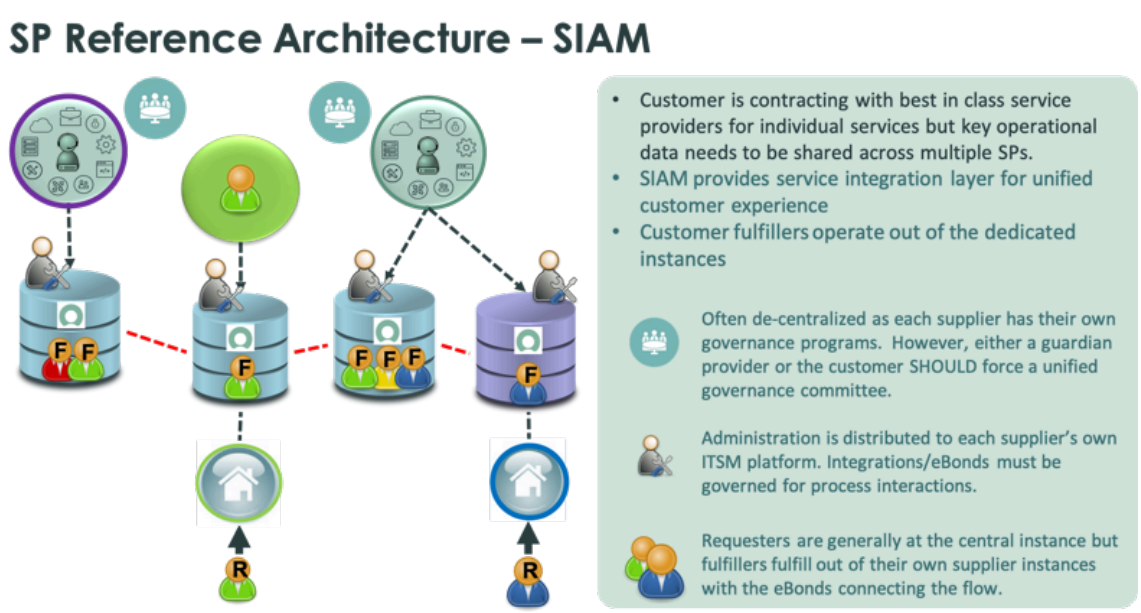
Architecture de référence du fournisseur de services pour Service Integration and Management (SIAM)

L'architecture Service Integration and Management SIAM (Service Integration and Management) pour le fournisseur de services (SP) intègre des services pour une expérience client unifiée.

Attributs de l'architecture SIAM

- Les clients accèdent aux services SP sur un portail dédié ou partagé à l'instance partagée SP.
- Les fournisseurs utilisent ServiceNow des instances partagées pour gérer leur prestation de services.

L'architecture SIAM en un coup d'œil



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comparaison de l'architecture de référence du fournisseur de services

Standalone (SA)		Multi-Tenant (MT)		Hybrid (MT+SA)		SIAM (Multi-Vendor)	
Platform as a Service	Enterprise scale	Processes simplified	Cost reduction	Managed Services (MT)	Custom Services (SA)	Service Integration	Multi-supplier governance
Customer wants full power of platform to Solve own needs outside those offered by SP.	Large customer: Transactions or data amount stored cause for multiple nodes or dedicated hardware.	Global governance & admin for business use case & process can be developed & maintained on the instance. Best when used w/ minor-to-moderate process differences among customers or sub-entities.	Lower administration, transaction, & onboarding costs, & ongoing operational costs for resources & licensing. Faster onboarding = more revenue.	Standardized re-usable services. procedures. processes, & resources delivered on a single ServiceNow instance to multiple Customers.	Services for sole use of customer, offerings specific to industry or vertical solutions, government, or regulatory requirements, applications that do not support Domain Separation.	Multiple best in class Service providers for individual services bringing together tooling, reporting, SLAs, strategy, & design for unified customer experience.	Unified governance across all providers to ensure organization requirements are met & that all providers cooperate on behalf of the customer.

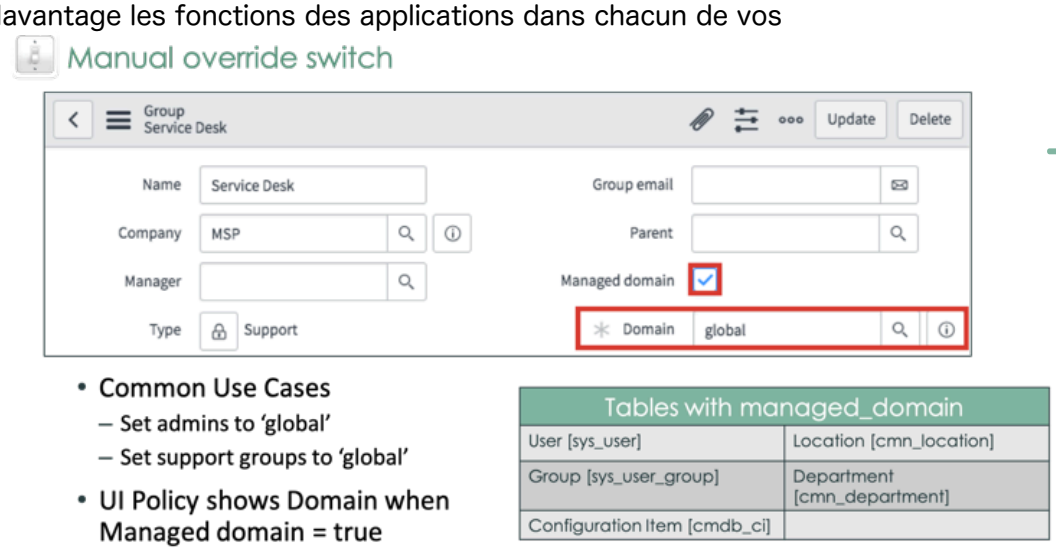
Termes de séparation de domaine

ServiceNow Une instance vous permet d'améliorer l'efficacité, de renforcer la sécurité et d'augmenter les performances de vos organisations clientes. Il est utile de comprendre certains des termes les plus courants lorsque vous créez vos configurations.

Domaine géré

Dans un domaine géré, le champ **Domaine géré** permet aux administrateurs de domaine de sélectionner manuellement un domaine pour l'utilisateur, le groupe, le département, l'emplacement ou l'enregistrement de CI, plutôt que d'utiliser le domaine affecté automatiquement à partir de l'enregistrement de société.

Si vous souhaitez modifier ces propriétés, vous pouvez les remplacer pour personnaliser davantage les fonctions des applications dans chacun de vos



domaines.

Tables des processus

Dans les tables de processus, si vous voyez une valeur dans le champ **Remplacements [sys_overrides],** un enregistrement de remplacement de processus existe. Cela signifie que l'administration déléguée, qui permet aux administrateurs de définir des stratégies

Traduction automatique

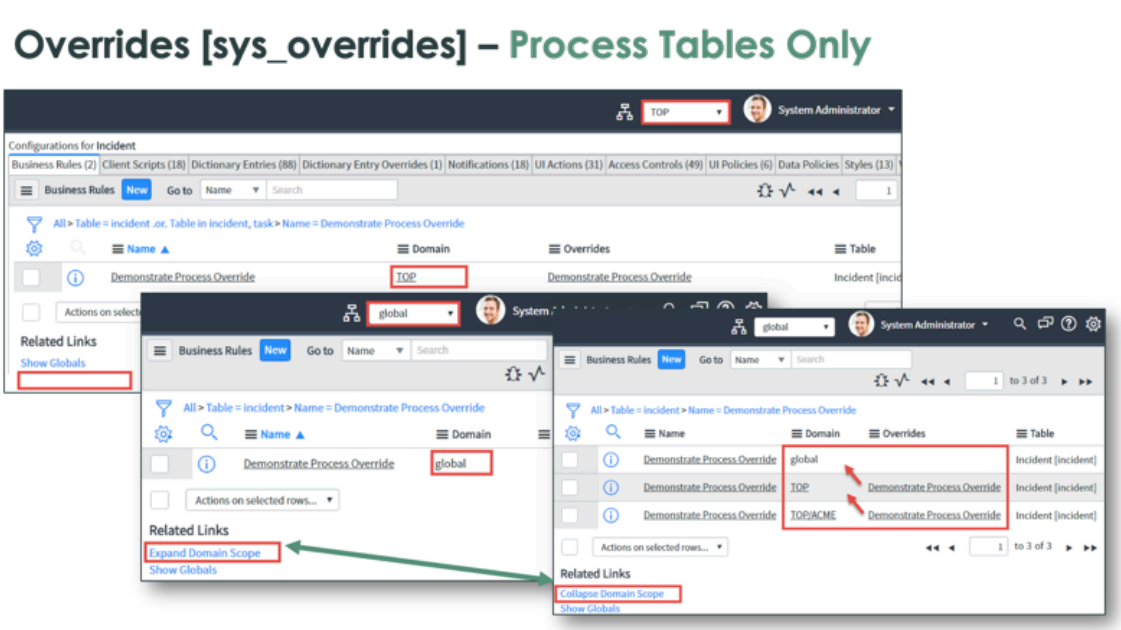
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

spécifiques à un domaine, est en vigueur. Les administrateurs dans le domaine global peuvent utiliser le lien connexe **Développer/Réduire le champ d'application de domaine** pour afficher les enregistrements de remplacement.

Remarque :
Les rapports sont séparés en domaines et contiennent un champ **Remplacements** . Pour afficher tous les rapports du domaine global, utilisez le lien connexe **Élargir le champ d'application de domaine** .

Lorsque vous affichez des tables de processus à partir d'un domaine, seuls les enregistrements de processus pertinents pour le domaine sélectionné s'affichent. Lorsque vous affichez une table de processus à partir du domaine global, le lien connexe **Étendre le champ d'application de domaine** s'affiche pour vous permettre de voir tous les enregistrements de processus, y compris les remplacements. Pour afficher à nouveau uniquement les enregistrements de processus pertinents pour global, utilisez le lien connexe **Réduire le champ d'application de domaine** .

La fonctionnalité de champ d'application de domaine n'est utilisée que pour les tables de processus et entraîne un décalage de la visibilité des données sur la table dans la direction opposée. Par exemple, un enregistrement dans le domaine parent peut être vu dans l'enfant, mais un parent ne peut pas voir un enregistrement enfant. Cela permet au processus de s'écouler vers les domaines enfants.



Types de domaines

Différents types de domaines peuvent vous aider à organiser vos processus et vos données, ainsi que leur fonctionnement dans l'application ou la fonctionnalité.

Domaine client

Dans le domaine du client se trouve l'interface utilisateur, ainsi que le processus qui contrôle la façon dont les données sont utilisées.

Le domaine ACME dans l'image suivante est un domaine client.

Domaine du processus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous créez des processus pour définir la façon dont les données sont utilisées et ce qu'elles font dans le domaine. Ces processus doivent comporter les attributs suivants :

- Processus et paramètres d'interface utilisateur spécifiques pour un ensemble de domaines
- Pas de données de base d'aucune sorte (telles que des données utilisateur spécifiques).
- Le domaine TOP dans l'image suivante est un domaine de processus.

Domaine de données

Le domaine de données contient des données pertinentes pour plusieurs clients. Ces données peuvent être partagées sans partager les domaines clients réels. Chaque client dispose de son propre domaine de données et peut y accéder.

Remarque :

Ce type de domaine n'est pas courant et peut entraîner des problèmes de performances s'il est surutilisé. Consultez un architecte SP avant utilisation.

Exemple : le domaine peut contenir des tâches avec lesquelles ACME, Cisco et le SP doivent tous interagir.

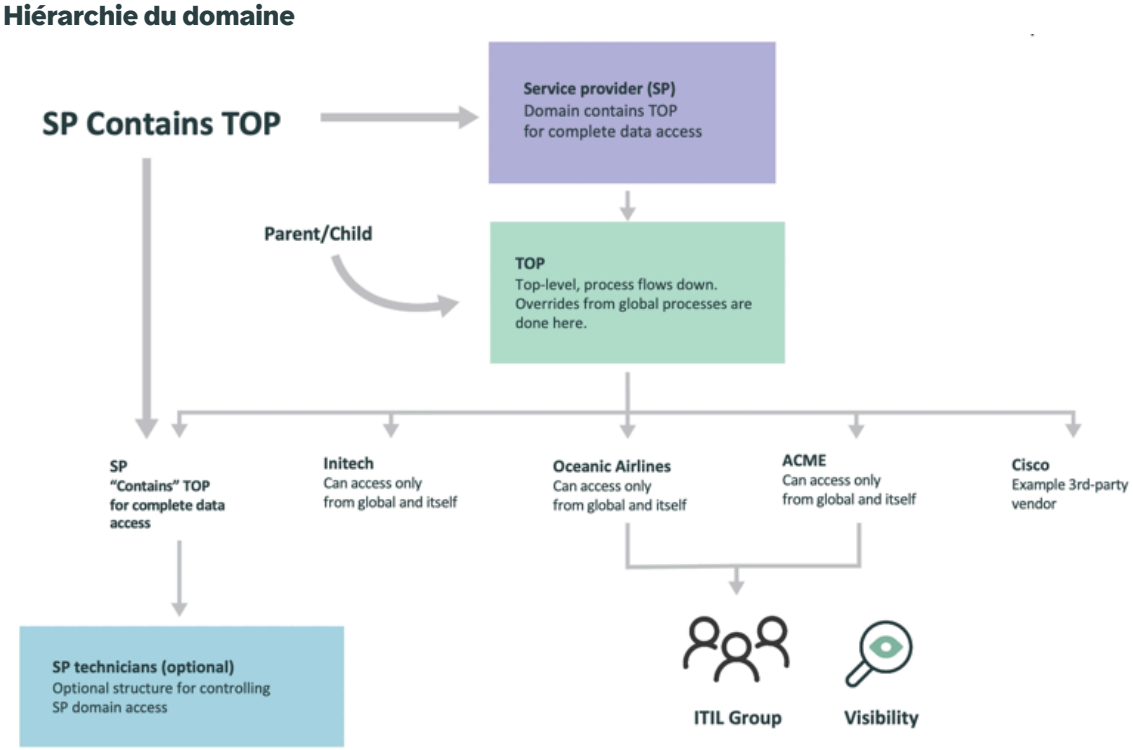
Le domaine par défaut dans l'image suivante est un domaine de données.

Données utilisateur

Les données de l'enregistrement utilisateur n'appartiennent jamais au domaine global ou à aucun domaine de processus. Les utilisateurs sont principalement créés dans les domaines clients et peuvent parfois être créés dans les domaines de données.

Les comptes administrateur sont spéciaux, car ils ne doivent pas être utilisés comme des utilisateurs quotidiens de l'instance et doivent être dans le domaine global pour faciliter les fonctions administratives.

Hiérarchie du domaine



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Listes, administrateur, processus global

Listes

Dans le domaine global, si vous cliquez avec le bouton droit sur l'étiquette d'un champ de choix, sélectionnez **Configurer les choix**, puis ajoutez un nouveau choix, le choix est automatiquement transmis à toutes les listes spécifiques au domaine pour ce champ. Si la nouvelle option est marquée comme **sélectionnée**, elle est ajoutée comme active. Si la nouvelle option est marquée comme **disponible**, elle est ajoutée comme inactive.

Administration des instances

Les administrateurs du propriétaire de l'instance doivent gérer la création, la modification et la maintenance de tous les processus normaux dans une instance séparée par domaine. Les gestionnaires de domaine individuels peuvent gérer certaines parties des processus pilotés par les données. Les types de gestionnaires de domaine gèrent l'administration des utilisateurs, les appartenances aux groupes de support et les emplacements, ou gèrent les applications conçues avec l'administration des locataires à l'esprit.

Processus/paramètres globaux

Vous pouvez créer et gérer les processus qui affectent le domaine global ainsi que définir les paramètres. Ces propriétés sont communes à tous les utilisateurs d'une instance séparée par domaine.

Exemples : propriétés système, contournements de dictionnaire, `sys_documentation` (étiquettes de champs), modèle de données (classes, types de CI, etc.), tables et champs [sys_dictionary] (accès restreint), indexation (index de texte et base de données), ACL, sorties d'installation, actions entrantes, pages publiques et intercepteurs.

Séparer par domaine une table personnalisée

Vous devrez peut-être créer des tables personnalisées dans des domaines distincts. Cette rubrique couvre à la fois la procédure et le concept de séparation par domaine d'une table personnalisée.

1. Créer un champ sys_domain

> **Remarque :**
> Si une table système ou une table n'a pas été séparée par domaine par le module d'extension Domain Separation, il est préférable de ne pas la séparer par domaine.

Utilisez ces points comme guide pour créer un champ sys_domain.

- Créez un champ en tant que *`domain_id`* type.
  - Nom de colonne : sys_domain
  - Autres attributs : définis automatiquement
- Le Sys_domain_path est créé automatiquement.

Le nom de colonne **sys_domain** est réservé dans le Now Platform, ce qui signifie que le système le reconnaît et applique automatiquement le type de champ et les attributs appropriés pour vous. Cette configuration automatique crée également un champ **sys_domain_path** correspondant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Définissez le nom de colonne `sur sys_domain` plutôt que d'utiliser l'étiquette.
- Séparation de domaine n'est pas approprié pour toutes les tables. En général, si une table fait partie de l'instance de base et que cette table ne possède pas de champ **sys_domain** , vous devez laisser cela ainsi.

Un champ **sys_domain** est créé automatiquement lorsque vous créez un champ de type domain_id portant le nom « sys_domain ».

2. Ajouter une règle métier pour définir le domaine

Sans règles métier

Le domaine est défini sur le domaine actuel de l'utilisateur qui crée l'enregistrement.

Avec des règles métier

Le domaine est affecté à l'aide d'une logique scriptée, généralement basée sur le champ Entreprise.

En plus d'un `champ sys_domain`, les tables personnalisées ont besoin d'une règle métier similaire à **Domaine – Définir domaine – Tâche**pour définir la valeur du champ Domaine. En outre, vous aurez besoin **de Domaine – Par défaut – Tâche**, qui déplace les enregistrements sans domaine vers le domaine par défaut si la première règle ne parvient pas à affecter un domaine.

Dans la table des tâches, examinez les règles métier pour le domaine. Portez une attention particulière au champ Commande. La priorité d'exécution est donnée par le champ Ordre de faible à élevée.

La première règle qui s'exécute, **Domaine – Définir le domaine – Tâche**, tente de définir le domaine de l'enregistrement en fonction du domaine de la société de l'enregistrement.

Si la première règle ne parvient pas à trouver un domaine approprié, la deuxième règle, **Domaine – Par défaut – Tâche**, s'exécute. Cette règle définit le domaine de l'enregistrement sur le domaine par défaut.

Enfin, si le domaine d'un enregistrement de tâche change, la règle métier **Domaine – Cascade Domaine – Tâche** modifie le domaine sur tous les enregistrements associés à la tâche, tels que les workflows, les mesures, les SLA et les pièces jointes.

3. Ajouter une règle métier en cas d'échec de l'étape 2

Si la règle métier initiale ne parvient pas à définir un domaine et que le domaine est toujours vide ou global, une deuxième règle métier s'exécute. Cette règle examine le champ `task_for` qui est basé sur le champ de l'appelant ou du `requested_for` . Cette règle vérifie si vous pouvez définir le domaine de l'enregistrement en fonction du domaine de l'utilisateur. Dans le cas contraire, la règle métier définit le domaine par défaut.

Voici un exemple de script pour la règle métier :

```
/* essentially
If (task_for is set)
  set the domain to the user's domain
ELSE
  set the domain to the default domain
*/
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Domaine – domaine en cascade – tâche

Les tâches peuvent avoir de nombreuses tables connexes qui fonctionnent ensemble pour atteindre les objectifs business. Ces enregistrements connexes comprennent le workflow, le SLA, les approbations, les pièces jointes et les e-mails. Si le domaine d'une tâche change, le domaine des enregistrements connexes doit également changer afin qu'ils restent visibles par les utilisateurs du nouveau domaine.

Cette règle en cascade est généralement déclenchée lorsque vous effacez les enregistrements du domaine par défaut.

Les enregistrements connexes pour un domaine en cascade contenus dans le script sont affichés de la même manière que l'exemple :

```
/*
* Keep domains in sync w/related records for:
* workflow context
* workflow history
* approver tables and related workflows
* attachments
* emails
*/
```

Personnalisation des propriétés et des thèmes de domaine

Vous pouvez personnaliser les propriétés et les thèmes de l'entreprise de vos clients dans les domaines que vous avez configurés. La personnalisation permet à leurs instances de s'adapter à l'apparence générale de leur entreprise.

Personnalisation des thèmes et logos de l'entreprise

Dans l'enregistrement de société, vous pouvez personnaliser des thèmes de conception et des logos spécifiques pour chaque société.

Personnaliser le domaine

Par défaut, lorsque le module d'extension du fournisseur de service est installé, les règles métier standard contenues dans les tables principales font que le domaine de l'enregistrement est défini sur le domaine de la société qui est associée à l'enregistrement. La société peut contrôler les tables telles que Tâche, Utilisateur, Groupe, Emplacement, Département, etc.

Avec toutes ces tables, à l'exception de la table Tâche, vous pouvez remplacer le domaine dans lequel un enregistrement est créé. Cela vous donne plus d'options de personnalisation.

Gestion de Domain Separation pour des utilisations spécifiques

Vous pouvez configurer des domaines distincts pour les notifications par e-mail et personnaliser les propriétés du catalogue, des tables, des utilisateurs, des groupes et des vues. Cela vous permet d'offrir un comportement plus spécifique dans chaque domaine, ce qui donne à vos clients plus de flexibilité.

E-mails

Vous pouvez utiliser des domaines distincts pour les notifications par e-mail et les remplacements. Lorsque vous utilisez des domaines distincts pour les notifications, vous pouvez effectuer un contournement basé sur le domaine de l'enregistrement joint uniquement, et non sur le domaine entier de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Catalogue de services

Catalogue de services est maintenant séparé par domaine afin que vos clients puissent voir le catalogue et y accéder. Les éléments sont traités en tant que conditions OU lorsque plusieurs éléments sont utilisés. Les fournisseurs de services doivent gérer eux-mêmes les catégories et les éléments afin qu'ils correspondent spécifiquement à leurs propres critères.

Utilisateurs et groupes

Utilisez uniquement des comptes d'administrateur dans le domaine global, car les administrateurs doivent avoir accès à tous les domaines. Effectuez tous vos tests d'application à partir d'un domaine réel, et non dans le domaine global. Les remplacements ne sont pas traités correctement dans le domaine global. Les administrateurs doivent également recevoir des comptes d'utilisateur en production s'ils doivent utiliser l'application.

Utilisation des champs

Il y a plusieurs points à prendre en compte lorsque vous travaillez avec des champs. Portez une attention particulière à ces champs, car ils peuvent avoir de nombreuses variantes qui affectent vos configurations.

Listes

Il existe des listes personnelles, globales et de domaines, ainsi que plusieurs vues de chacune.

Formulaires

Il existe des listes globales et de domaines, ainsi que plusieurs vues de chacun.

Une base de données

Tous les champs que vous créez existent pour tous les utilisateurs, dans une seule base de données. Tenez compte de l'impact global avant d'en créer un.

Remarque :
Les scripts ACL ne peuvent pas empêcher un champ d'être affiché dans une liste, car ils ne s'exécutent pas. Vous pouvez ajouter une ACL LECTURE pour masquer un champ aux utilisateurs si l'ACL est uniquement basée sur les rôles.

Création de tables

Lorsque vous créez une table, vous devez ajouter un `champ sys_domain` ou `sys_overrides` . Toute table contenant des données auxquelles les utilisateurs de votre instance doivent accéder a besoin du champ `sys_domain` . Les tables qui étendent ou prennent en charge des processus et qui doivent descendre vers des domaines enfants ont également besoin du champ `sys_domain` .

Configuration de Séparation de domaine avec le sélecteur de domaine

Utilisez le sélecteur de domaine à bon escient et n'oubliez pas l'approche 80/15/5 afin de ne pas trop personnaliser et d'impacter les performances de votre instance.

Vérifiez votre domaine avant d'apporter des modifications

Le sélecteur de domaine rassemble tous les domaines dans une liste parmi laquelle vous pouvez faire votre choix.

Si votre session expire et même si vous n'êtes pas déconnecté, votre session rebascule sur le domaine de votre enregistrement utilisateur. Vous perdez également tous les rôles élevés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en même temps. Dans ce cas, votre sélecteur de domaine peut toujours afficher le dernier domaine que vous avez sélectionné si le cadre supérieur de la liste n'a pas été rechargé. Pour cette raison, vous devez recharger complètement votre liste si vous avez été absent de l'instance pendant un certain temps.

Configuration au domaine TOP ou au domaine global

Séparation de domaine fonctionne mieux lorsque vous fournissez des services à des clients qui sont pour la plupart standard dans leur configuration et leur définition des utilisateurs et des groupes. Plus vous personnalisez et créez des solutions « ponctuelles », plus vous créez une marge d'erreur. Lorsque vous créez vos processus et votre logique métier, toutes les variations doivent se trouver dans des propriétés qui fonctionnent automatiquement pour chaque client. Bien que les processus puissent toujours être ajustés selon les besoins, soyez très prudent lorsque vous décidez quand et dans quelle mesure créer une configuration unique pour un seul client.

Vous devez utiliser une approche « 80-15-5 » dans la configuration de vos domaines afin d'éviter une marge de personnalisation trop importante, et donc des erreurs.

- Approche recommandée pour la configuration :
  - **80 %** ou plus **Standard**
  - **15 %** ou plus **paramétrique**
  - **Configuration** de moins de **5 %**
- Déterminez si un changement suggéré doit être une propriété globale ou configurable.
- Ne construisez pas trop en ajoutant de plus en plus de personnalisation qui doit être gérée. Au lieu de cela, procédez comme suit :
  - Commencez par les fonctionnalités du système de base et vérifiez toutes les lacunes avant d'apporter des modifications.
  - Recherchez des solutions sans code.
  - Utilisez des scripts côté serveur, créez des API modulaires et intégrez des propriétés séparées par domaine.
  - Si vous devez utiliser un script client, utilisez uniquement ServiceNow des API. Limitez les appels « synchrones » (ceux qui vont et viennent du client au serveur, aussi appelés AJAX).
  - Écrivez tous les scripts de manière logique pour qu'ils restent simples et efficaces. Appliquer des examens par les pairs des changements de code et assurez-vous que tout le monde respecte les instructions Pratiques recommandées de séparation de domaine pour les fournisseurs de services de cette section.

Considérations relatives aux performances de Domain Separation

Lorsque vous configurez Séparation de domaine dans votre application et vos services, assurez-vous de prendre en compte le nombre et les propriétés des domaines que vous créez. Un trop grand nombre de domaines avec beaucoup de propriétés peut avoir un impact sur les performances de votre instance.

Limitation des domaines à forte propriété

Vous pouvez créer autant de domaines que nécessaire, mais assurez-vous de ne pas créer de domaines inutiles sur l'instance. Pondérer trop de domaines sur l'instance avec un grand nombre de propriétés peut avoir un impact sur les performances de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce n'est pas le nombre de domaines qui a un impact sur les performances, mais plutôt ce qu'ils contiennent. Trop de propriétés peuvent ralentir le sélecteur de domaine, ce qui ralentit ensuite l'expérience utilisateur globale de vos clients. Si vous chargez le sélecteur de domaine et que vous avez déjà un grand nombre de domaines avec beaucoup de propriétés, le sélecteur de domaine doit charger tous les domaines avant de vous donner le contrôle de la session. Ce processus peut entraîner une panne où vous ne pouvez accéder à rien sur l'instance tant que le sélecteur de domaine n'a pas terminé. Avant de créer de nouveaux domaines, accédez à la hiérarchie des domaines sous **Administrateur de domaine** > **Carte de domaine** et assurez-vous que vous avez réellement besoin de créer un nouveau domaine ou si une hiérarchie de domaines existante peut fonctionner.

Utilisation Interface utilisateur principale du sélecteur de domaine

Le sélecteur de référence de domaine est disponible dans Interface utilisateur principale. Avec le sélecteur de référence, vous ne chargez pas tous les domaines à la fois, mais le domaine est recherché lorsque vous commencez à entrer le nom de votre domaine dans le sélecteur de domaine.

Activez le sélecteur de référence de domaine en procédant comme Interface utilisateur principale suit :

1. Dans le navigateur d'application, saisissez `sys_properties.list`.
2. Définissez la propriété *`glide.ui.domain_reference_picker.enabled`* sur true.
3. Actualisez le navigateur.

Remarque :
Ne chargez pas un grand nombre de domaines (plus de 30) via l'intégration ou des jeux d'importation sans effectuer d'abord des tests, sinon vous risquez de faire tomber votre instance.

Configurer des hiérarchies de domaines

Vous pouvez éviter les ralentissements et les impacts sur les performances de votre instance en connaissant le fonctionnement des hiérarchies de domaines et en les configurant correctement.

En fonction de la hiérarchie des domaines, les utilisateurs ont accès aux données de leur domaine d'accueil et de tous les domaines enfants. Le processus s'écoule vers les domaines enfants et les données remontent.

Apportez des modifications à la hiérarchie de domaine existante uniquement lorsque cela est nécessaire. Lorsque vous mettez à jour le domaine parent d'un domaine, le système rétablit le domaine parent avec tous ses domaines enfants qui modifient la hiérarchie de domaine. Lorsque la hiérarchie de domaines est mise à jour, le système déclenche une mise à jour en cascade sur toutes les tables associées aux domaines pour les enregistrements créés sur ce domaine. Par conséquent, un grand nombre de tables de support doivent également être mises à jour.

Pour les mêmes raisons, même si vous devez changer la hiérarchie de domaine, ne faites jamais de mise à jour en masse. Imaginez le nombre de requêtes que le système doit exécuter pour modifier la hiérarchie de domaine. Faites toujours une mise à jour par petits lots. Avant de commencer le lot de mises à jour suivant, assurez-vous que les enregistrements de demande de travail de domaine (DWR) sont traités. Les DWR sont des rapports qui affichent s'il y a des erreurs après que vous avez modifié la hiérarchie de domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suivi des enregistrements DWR

Dans la table syslog_domain, recherchez une entrée d'information dans la colonne Message pour **l'exécution du DWR terminée.** pour confirmer que le DWR est terminé.

Vérification des journaux de domaine pour les erreurs et avertissements

Consultez les journaux de domaine pour rechercher des erreurs ou des avertissements dans vos processus de chemin de domaine et vos configurations hiérarchiques.

Vous pouvez trouver les journaux de domaine dans la table Journal de domaine [syslog_domain]. Lorsque la hiérarchie de domaine est mise à jour, le système déclenche une tâche planifiée pour recalculer les chemins de domaine. La table des journaux de domaine capture les résultats.

Recherchez les erreurs et les avertissements dans ce tableau. Après avoir examiné cette table, vous devez résoudre ces erreurs et exécuter à nouveau le validateur de chemin de domaine.

Dans cet exemple de journal, le système a détecté dix enregistrements orphelins dans la table sys_ui_list. Les erreurs dans ces enregistrements doivent être corrigées pour que le chemin de domaine puisse s'exécuter correctement.

Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again.	com.glide.domain.validator
Error	10 records detected in 'sys_ui_list' that are not in any existing domain and Domain Paths. Fix the domain value in these records & run validator again. Entries causing the error are as follows:sys_id:1d13ae40470002007f47563dbb9a7170, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:22e34b23470002007f47563dbb9a718c, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:4c85fa809f233100fc6cd4b4232e706b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:94648b23470002007f47563dbb9a711b, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a0844b23470002007f47563dbb9a71ef, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:a95ff2c09f233100fc6cd4b4232e7096, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:bd25f4719f233100fc6cd4b4232e70da, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:c1263e809f233100fc6cd4b4232e70f6, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:d8a72c45475002007f47563dbb9a71bb, sys_domain:11722b01473231007f47563dbb9a7154 sys_id:e4c3ce39eb10020045e1a5115206fea0, sys_domain:60e014f69f013100fbf01f80a57fcf00	com.glide.domain.validator

Pour en savoir plus sur les erreurs de séparation par domaine, reportez-vous à Résoudre les erreurs de Domain Separation.

Importance du domaine par défaut

L'organisation de vos domaines est un élément crucial du processus de séparation de domaine. Si vous ne définissez pas de domaine par défaut, les nouvelles tâches et les enregistrements d'utilisateurs sont transférés vers le domaine global. Tout le monde peut voir les enregistrements dans le domaine global, ce qui signifie que les données peuvent être vues alors qu'elles ne sont pas censées l'être.

Lorsque vous définissez le domaine par défaut, ses enregistrements ne sont visibles par aucun utilisateur autre qu'un administrateur.

Remarque :
L'accès par défaut peut être modifié en donnant aux utilisateurs une visibilité sur le domaine par défaut ou le domaine parent.

Vous devez toujours définir un domaine par défaut pour les enregistrements de domaine sur votre instance. Le domaine par défaut est l'endroit où le système affecte automatiquement les enregistrements de tâches et d'utilisateurs qui ne sont pas déjà affectés à un domaine.

Lorsque vous créez un domaine par défaut à partir de l'écran Administration de domaine, ajoutez le nom par défaut dans le champ **Nom** pour le différencier des autres domaines. Cochez la case **Par défaut** pour l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conservez régulièrement les enregistrements que vous créez dans le domaine par défaut et déplacez-les vers les domaines appropriés. Si les enregistrements s'affichent souvent dans le domaine par défaut, vous devrez peut-être en chercher la raison. Idéalement, vous devez vous assurer que tous les enregistrements sont créés dans leurs domaines appropriés (et non dans les domaines globaux ou par défaut).

Contient des requêtes et un accès au domaine

Utilisez une requête « contient » uniquement dans des cas particuliers, par exemple lorsque des utilisateurs ou des groupes ont besoin de voir les données d'un domaine auquel ils n'ont pas accès, mais que vous ne voulez pas déplacer ces utilisateurs vers un domaine. La création d'un domaine « contient » et d'un accès utilisateur ou groupe pour un domaine doit être une exception, uniquement en cas d'absolue nécessité.

« Contient » est une relation de domaine à domaine qui est plusieurs-à-plusieurs et n'a aucun effet sur le flux de processus. Si vous créez un grand nombre de relations de domaine « contient » ou si vous fournissez un accès large, vous générerez des requêtes avec trop de conditions OU. Les conditions de salle d'opération sont lentes et ont un impact sur les performances de votre instance. Au lieu d'utiliser trop de relations « contient », configurez votre hiérarchie de domaines comme suit :

Exemple de requête

```
SELECT ... FROM task task0 ignore index(number) WHERE task0.`sys_class_name`
= 'incident' AND (task0.`sys_domain_path` = '/' OR task0.`sys_domain_path` LI
KE '!!$/!!(/%' OR task0.`sys_domain_path` LIKE '!!$/!!$/!!&/%') ORDER BY task
0.`number` DESC limit 0,20
```

Avant de déplacer des utilisateurs vers un domaine, assurez-vous qu'ils doivent vraiment avoir accès à ce domaine. Pesez les avantages et les limites. La requête ci-dessus ne concerne qu'une seule relation contient. Si vous avez un domaine qui contient un autre domaine, et que ce domaine est le parent d'un certain nombre d'autres domaines, vous aurez beaucoup plus de conditions OU. Lorsque vous créez une carte de domaine, veillez à ne pas impacter les performances de votre instance.

Chemins de domaine Méthode de requête

Vous pouvez créer des requêtes efficaces avec des chemins de domaine.

Utilisez des chemins de domaine au lieu de la mise en file d'attente de domaine (sys_domain) ou de la numérotation de domaine. Les requêtes qui utilisent des chemins de domaine sont beaucoup plus rapides que la mise en file d'attente ou la numérotation.

Chemins de domaine est la méthode de requête par défaut pour les instances qui ont activé Séparation de domaine.

Si vous souhaitez vérifier la méthode de requête sur votre instance, recherchez les propriétés système suivantes dans le tableau de bord de l'administrateur :

- *If domain path is enabled*: dans la table Propriétés système, vous voyez glide.sys.domain.provider=domain_paths et glide.sys.domain.paths.installed=true.
- *If domain path is not enabled*: dans la table Propriétés système, vous voyez glide.sys.domain.provider != domain_paths,glide.sys.domain.paths.installed=false

Requêtes lentes et débogage SQL

Le débogage SQL et les requêtes lentes peuvent vous aider à résoudre les problèmes de lenteur dans une instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous déboguez une instance, vous pouvez activer le débogage SQL pour rechercher les requêtes lentes ou rechercher les requêtes lentes en consultant la table Requêtes lentes [sys_query_pattern] en accédant à **Diagnostics du système > Stats > Requêtes lentes**. Cette table stocke toutes les requêtes lentes de l'instance.

Lorsque vous effectuez une recherche dans la table, recherchez les requêtes qui contiennent des domain_path pour déterminer si les requêtes lentes sont dues au chemin de domaine de votre instance.

Si vous trouvez des requêtes lentes, essayez d'analyser pourquoi elles sont lentes.

Raisons courantes de la lenteur des requêtes

- Une requête comporte trop de conditions OU (pour plus d'informations, reportez-vous à la section Contient des requêtes et un accès au domaine). Dans la hiérarchie de domaine, placez l'utilisateur ou un domaine à un niveau hiérarchique où contient ou visibilité n'est pas nécessaire.
- La méthode de requête n'est pas la méthode de requête du chemin de domaine (pour plus d'informations, voir Chemins de domaine Méthode de requête) : Si vous n'utilisez pas la méthode de requête du chemin de domaine, contactez Service et assistance client.
- Une requête nécessite qu'une base de données soit indexée afin que vous puissiez voir rapidement ce qu'il y a dans la base de données. Si vous pouvez identifier la requête lente, exécutez le « plan d'explication » pour voir s'il existe des options d'indexation disponibles. Le « plan d'explication » est une fonction de SQL qui montre la requête et ce qui se passe avec elle.

Avant les règles métier de requête

Vous pouvez utiliser une règle métier Avant requête pour faciliter la prise en charge de la ségrégation des données sur une instance. ServiceNow Les applications qui prennent en charge Séparation de domaine peuvent uniquement prendre en charge la séparation des données et le routage des données, disposer d'une séparation avancée de la logique métier ou prendre en charge l'administration au niveau du locataire (client) de l'application.

Une règle métier Avant requête est un code supplémentaire que vous utilisez pour prendre en charge la ségrégation des données dans des environnements séparés par domaine.

Avertissement :
N'utilisez pas la règle métier Avant requête à la place du module d'extension Séparation de domaine. Cette règle métier n'empêche pas les fuites de données de manière aussi sécurisée que le module d'extension.

Utilisation de la règle métier Avant requête pour la ségrégation des données

Vous pouvez utiliser la règle métier Avant requête avec ségrégation des données dans les situations suivantes :

- Lorsque Séparation de domaine n'est pas pris en charge par une ServiceNow application et que vous devez accorder ou restreindre l'accès aux tables ou aux lignes à un ou plusieurs clients non internes en dehors de l'organisation fournisseur de service.

Remarque :
Avant de commencer le développement, contactez ServiceNow le support client au sujet de la feuille de route de l'application pour ce produit. Des améliorations de la prise en charge du domaine peuvent être prévues pour les versions à venir.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Lorsqu'une table est séparée par domaine, mais que l'accès à ses lignes doit être accordé ou restreint en fonction de certaines conditions qui s'appliquent uniquement à un ensemble de domaines dans le système.

Remarque :
Par exemple, un client dans le domaine X a plusieurs fournisseurs qui prennent en charge ce domaine et ces fournisseurs ont un accès pour voir uniquement les enregistrements qui leur sont affectés.

Points à prendre en compte avant de créer des règles métier Avant requête

Vous pouvez scripter les règles métier Avant requête pour empêcher l'accès aux tables parent et enfant en fonction d'une combinaison d'informations utilisateur, d'appartenances à des groupes, de sociétés, de rôles ou de conditions de champ spécifiques à un enregistrement. Avant la requête Les règles métier sont placées dans des domaines distincts et créées pour s'appliquer globalement, à une branche spécifique d'une hiérarchie de domaine.

- Dans la mesure du possible, créez des règles métier Avant requête dans la partie la plus basse possible de la hiérarchie de domaine, afin que la règle ne s'exécute que pour les utilisateurs auxquels elle s'applique.
- Sachez qu'il existe des scénarios dans le système dans lesquels des règles métier peuvent ne pas s'exécuter ou où une interaction déclenchée par l'utilisateur peut ne pas déclencher l'exécution d'une règle métier. Par exemple, une règle métier ne s'exécute pas si vous avez désactivé les cartes de transformation pour lesquelles Exécuter les règles métier est désactivé ou si vous avez des scripts pour lesquels le workflow est désactivé.
- Renseignez toujours le champ de condition pour spécifier quand la règle s'exécute. Par exemple, vous pouvez spécifier si la règle métier s'applique uniquement à certains fournisseurs d'un domaine.

Avertissement :
Lors de la conception et du codage de règles métier (en particulier les règles métier de requête), limitez les clauses OR et les recherches dans les champs non indexés. Trop de clauses OU et de recherches dans des champs non indexés peuvent ralentir les requêtes ou affecter les performances de votre instance.

- Utilisez les règles métier Avant requête uniquement lorsque cela est nécessaire. Un trop grand nombre de règles de requête Before peut affecter les performances de votre instance.

Avant requête Les règles métier s'exécutent avant les listes de contrôle d'accès (ACL) et sont généralement plus performantes. Cela est particulièrement vrai si l'on limite les résultats renvoyés aux utilisateurs des environnements de fournisseur de services (SP) qui ont accès à plusieurs domaines du système.

Remarque :
Le filtrage des données est transparent (contrairement aux ACL) pour les utilisateurs qui ne voient pas le message Sécurité des données restreint lors de l'interaction avec les données.

Quand ne pas utiliser les règles métier et ACL Avant requête

Soyez prudent lorsque vous utilisez des règles métier et des ACL Avant requête pour séparer les données client. En utilisant à la fois des règles métier et des ACL, vous créez des personnalisations que vous devez ensuite gérer. Les personnalisations peuvent potentiellement entraîner des problèmes de performances. Vos équipes de développement doivent créer des processus pour s'assurer qu'ils ne cassent pas le système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Séparation de domaine assure à la fois évolutivité et gouvernance avec la méthode de requête de chemin de domaine actuelle (v3), qui est un cadre de travail largement pris en charge. Les ServiceNow équipes de la plateforme et de l'application sont responsables de la maintenance du framework, déchargeant ainsi le client.

Pour les entreprises comptant de nombreux clients, dans de nombreux cas, l'utilisation excessive des requêtes Before et des ACL peut entraîner une mauvaise exécution des requêtes de base de données.

Comment la séparation de domaine est-elle activée ?

Vous pouvez activer Séparation de domaine à l'aide d'un module d'extension ServiceNow . Un chef de produit, épaulé par une équipe de développement, gère les fonctionnalités. Des améliorations et des correctifs pour la fonctionnalité Séparation de domaine sont inclus dans ServiceNow les versions. Les propriétaires d'instances peuvent consulter Service et assistance client des ressources, telles que , à l'adresse pour https://support.servicenow.com obtenir de Portail de servicesl'aide sur la séparation de domaine.

Éviter le chemin de domaine dans les scripts

Les chemins de domaine peuvent entraîner la modification ou même la rupture des valeurs de votre script, c'est pourquoi ne les utilisez pas dans les scripts.

Votre script ne doit pas dépendre du chemin de domaine, car si vous modifiez la hiérarchie de domaine, le chemin de domaine est recalculé et sa valeur change. Lorsque cela se produit, vos scripts sont inutiles ou peuvent générer des erreurs ou se panner. La meilleure stratégie est de ne pas écrire vos scripts en fonction de chemins de domaine.

Utilisez le champ **sys_domain** dans vos scripts plutôt que de dépendre du chemin de domaine. Si vous modifiez la hiérarchie de domaine, le chemin de domaine est recalculé et sa valeur change, ce qui peut rendre vos scripts inutiles, générer des erreurs ou les interrompre. Recherchez les règles métier du système de base, qui utilisent le champ **sys_domain** , pour obtenir des idées avant de créer vos propres scripts.

La ServiceNow plateforme ne capture pas les valeurs sys_domain_path dans un ensemble de mises à jour afin d'éviter les problèmes liés aux différences dans la hiérarchie de domaine pour chaque instance. Par conséquent, vous devez valider la hiérarchie de domaines après avoir importé un ensemble de mises à jour pour vous assurer que les valeurs du chemin de domaine de vos enregistrements sont correctes.

Pour en savoir plus sur les chemins de domaine, consultez Demander Séparation de domaine et Centre Séparation en domaines.

Affectations de domaines

La façon dont vous affectez un domaine a un impact sur la valeur du champ sys_domain. Les affectations contiennent des conceptions et des propriétés commerciales qui affectent le fonctionnement de l'application dans chaque domaine.

Valeur du champ sys_domain

La valeur du champ **sys_domain** contient le domaine affecté à l'enregistrement par l'un des éléments suivants :

- Société à laquelle l'utilisateur appartient
- Règle métier utilisée lors de la création de l'enregistrement
- Module utilisé lors de la création de l'enregistrement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Modèle de formulaire utilisé lors de la création de l'enregistrement
- Domaine de l'enregistrement parent
- Domaine affecté à l'enregistrement utilisateur
- Domaine de l'utilisateur qui le crée

Assurez-vous que vos stratégies et conceptions d'affectation de domaine sont bien documentées et testées afin de créer des enregistrements au fur et à mesure que ces stratégies et conceptions sont insérées dans le domaine approprié. De cette façon, vous pouvez voir les propriétés de chaque domaine si vous avez besoin de les dupliquer ou de les modifier.

Séparation de domaine et le module d'extension Gestion du service client (CSM)

Pour un résultat optimal, soyez conscient du fonctionnement des propriétés du module d'extension CSM . Lorsque le module d'extension est activé, vous pouvez voir l'état de vos enregistrements dans vos domaines.

Les propriétaires d'instances doivent nous contacter Service et assistance client pour activer la *csm_auto_account_domain_generation* propriété.

Remarque :
Cette propriété système de base se trouve dans la table des propriétés système et est disponible après l'activation des modules d'extension CSM.

Fonction de la propriété

Chaque fois qu'un nouveau compte est créé dans l'application Customer Service, un domaine est créé et placé sous le domaine TOP. Si le champ parent du formulaire de compte est renseigné et qu'un nouvel enregistrement est inséré, ce compte devient un sous-domaine du parent.

Que se passe-t-il si cette propriété n'est pas vraie et que le domaine est activé ?

Les nouveaux enregistrements de compte dans un environnement séparé par domaine sont automatiquement placés dans le domaine par défaut.

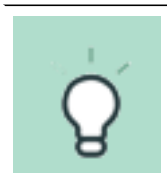
Dans la barre d'en-tête, vous pouvez voir l'état des enregistrements avec le module d'extension activé.

Aide de Domain Separation

Assistance supplémentaire avec Domain Separation

Vidéo de présentation de Domain Separation

Explorer, apprendre, développer



Pratiques recommandées

Trucs et astuces pour créer et développer judicieusement votre structure de domaine



Niveaux de prise en charge par application

Votre application est-elle prise en charge pour Domain Separation ? Consultez les niveaux de prise en charge et les cas d'utilisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

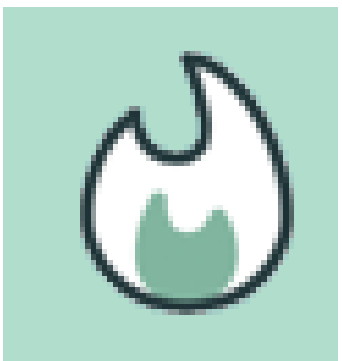
Concepts pour les prestataires de services

Concepts qui fonctionnent avec la ServiceNow plateforme pour vous aider à résoudre les cas d'utilisation courants



Classes

- Pour les développeurs : ServiceNow Site développeur Séparation de domaine
- Pour les fournisseurs de services : Séparation de domaine pour les fournisseurs de services (connexion ServiceNow University requise)



Suite Safe Workplace et Séparation de domaine

ServiceNow Les applications Safe Workplace vous aident à rouvrir vos lieux de travail et à soutenir la santé et la sécurité de vos employés après des urgences et des pandémies telles que la COVID-19. La suite dispose de nombreuses applications pour aider votre organisation à se mobiliser, à récupérer et à se reconstruire.



Configuration et administration

- Mises à niveau
- Demander Séparation de domaine
- Créer un domaine
- Configuration pouvant être déléguée à des clients internes ou externes



Dépannage

- Rechercher des articles sur une erreur connue dans le portail d'erreurs connues
- Contact Service et assistance client
- Poser des questions ou y répondre dans la communauté

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration et administration de Domain Separation

La configuration de Séparation de domaine implique de demander l'activation d'un module d'extension, de définir des options et d'affecter des utilisateurs et des enregistrements à des domaines.

Pour configurer Séparation de domaine, procédez comme suit :

1. Demander Séparation de domaine
2. Créer un domaine
3. Ajouter un champ de domaine à une table

Vous pouvez également effectuer ces tâches administratives de base sur les domaines :

- Activer ou désactiver un domaine
- Afficher les relations du domaine
- Élargir le champ d'application de domaine
- Créer une liste de choix spécifique à un domaine

Consultez Administration avancée de Domain Separation la liste des tâches à effectuer après la configuration de Séparation de domaine et l'administration de base.

Demander Séparation de domaine

Toutes les fonctionnalités de prise en charge du domaine sont activées à l'aide d'un module **d'extension appelé Domain Support - Domain Extensions Installer**. Les administrateurs peuvent demander l'activation de ce module d'extension.

Avant de commencer

Pour acheter un abonnement, contactez votre chargé de clientèle ServiceNow. Le chargé de clientèle peut faire en sorte que le module d'extension soit activé sur les `com.glide.domain.msp_extensions.installer` instances de production et de sous-production de votre organisation, en général en quelques jours à peine.

Si vous n'avez pas de chargé de clientèle, si vous décidez de retarder l'activation après l'achat ou si vous souhaitez évaluer le produit sur une instance de sous-production sans frais, suivez ces étapes.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Si le module d'extension Domain Support - Domain Extensions Installer est déjà actif, le contenu du module d'extension Domain Support - Domain Extensions Installer n'est pas installé pour éviter tout conflit potentiel avec une implémentation existante.

Séparation de domaine remplace Séparation de l'entreprise. À partir de la version Helsinki, le module d'extension Séparation de l'entreprise ne peut plus être activé. Toutefois, si Séparation de l'entreprise est déjà actif lorsque vous activez Séparation de domaine, les deux modules d'extension sont actifs en même temps. Vous pouvez contrôler l'état d'activation de séparation de l'entreprise avec la `glide.db.separation.field` propriété.

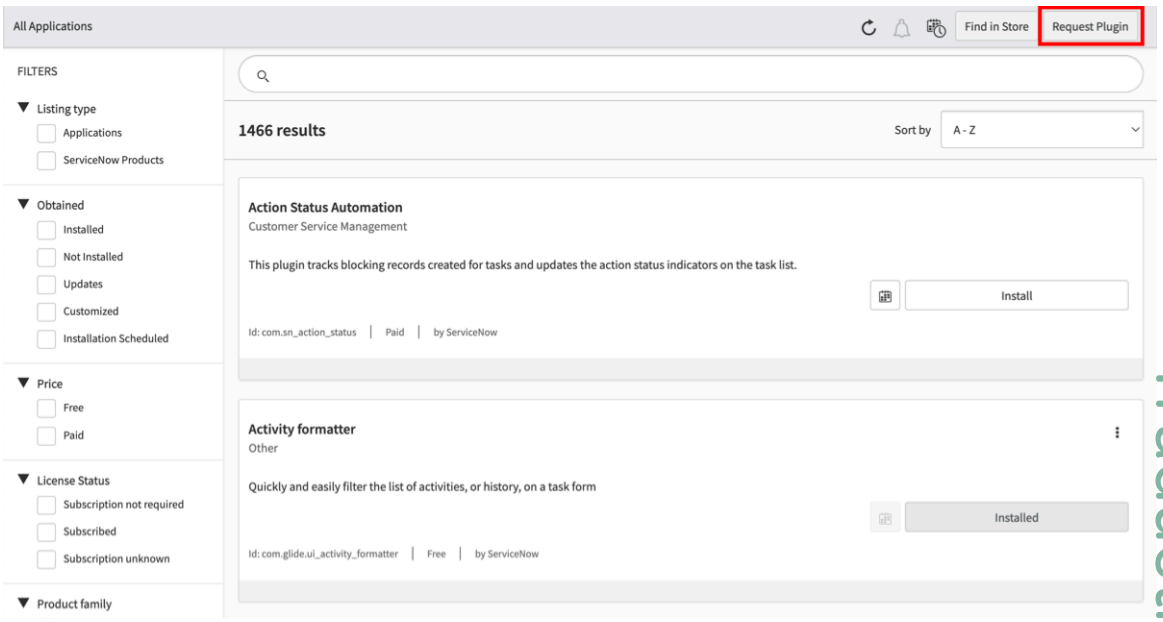
Remarque :
Les chemins de domaine sont utilisés pour tous les clients sur Helsinki et les versions ultérieures. La numérotation de domaine n'est plus utilisée. Service et assistance client peut vous aider dans la mise à niveau.

Traduction automatique

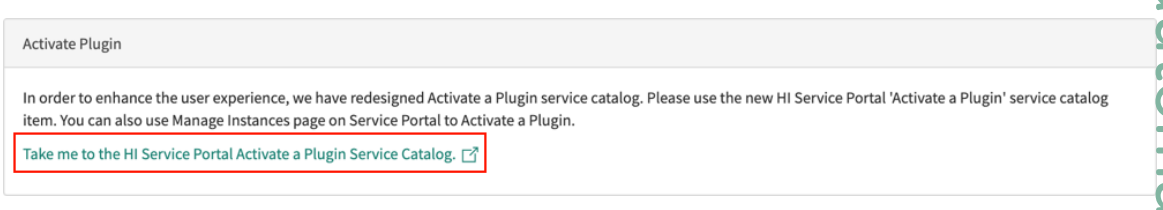
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer.

Traduction automatique

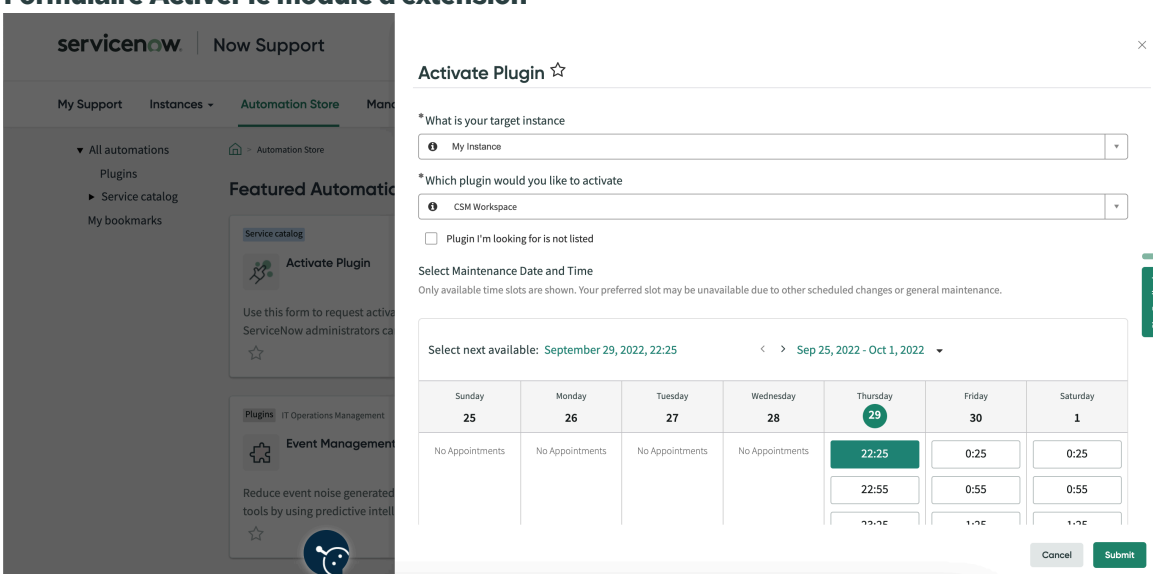
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



7. Sélectionnez **Envoyer**.
   Pour plus de détails sur la demande d'un module d'extension, consultez l'article Requesting a Plugin from the Service Catalog [KB0751715] de la Now Support Base de connaissances.

Résultats

L'activation du module d'extension du programme d'installation de domaine active ces fonctionnalités :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Séparation de domaine est basée sur la table Domaine [sys_domain].
- L'administration déléguée permet à chaque domaine d'avoir une politique distincte.
- Tous les enregistrements font partie du domaine global.
- Le domaine de l'utilisateur actuel détermine le domaine à utiliser lors de l'affichage ou de l'utilisation d'un enregistrement dans un domaine différent.

Information associée

Module d'extension Domain Separation

Module d'extension Domain Separation

Le module d'extension Domain Support - Domain Extensions Installer active plusieurs fonctionnalités et propriétés de séparation de domaine à la fois. Ce module d'extension est généralement appelé module d'extension Séparation de domaine.

Pratique recommandée pour l'activation du module d'extension Domain Separation

Dans le cadre du développement de Domain Separation, les administrateurs doivent demander l'activation de ce module d'extension. Pour de meilleurs résultats, activez le module d'extension Séparation de domaine au début du processus de développement, de préférence avant l'activation de tout autre module d'extension.

Important :
Demandez l'activation du module d'extension Domain Extensions Installer (com.glide.domain.msp_extensions.installer) avant d'activer Domain Separation (module d'extension com.snc.pa.domain_support).

Si vous activez Séparation de domaine vers la fin de l'implémentation ou une fois qu'une ServiceNow instance a été mise en service, les performances et le processus de votre application sont à risque. Sur les instances établies, en fonction de la façon dont les choses ont été structurées lors du développement, le risque pour la plateforme et sa facilité d'utilisation peut être élevé. Pour en savoir plus sur le processus de séparation par domaine, reportez-vous à la section Explorer la séparation de domaine.

Par exemple, lorsque le module d'extension Séparation de domaine est activé, la colonne **Domaine** (sys_domain) est ajoutée à la table des tâches et tous les enregistrements existants sont automatiquement placés dans **global**. Pour utiliser un script afin d'affecter tous les enregistrements dans les domaines appropriés, une hiérarchie parent/enfant établie est requise. Ces types d'actions scriptées risquent d'entraîner la corruption ou la perte de données, ainsi que d'éventuels temps d'arrêt de la production à mesure que de grandes quantités de données sont déplacées. Une grande partie du code de la plate-forme est également placée dans **global**, comme les règles métier, les scripts clients, les vues de formulaire et les workflows.

Si un client crée du code ou modifie le code, il existe un risque pour les performances et la convivialité de ServiceNow la plateforme. Avec ce type d'approche, les propriétaires d'instances pourraient retarder considérablement leur implémentation ou subir de longs temps d'arrêt.

Fonctionnalités du module d'extension Domain Separation

Ces fonctionnalités sont activées lorsque vous activez le module d'extension :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Séparation de domaine est basée sur la table Domaine [sys_domain].
- L'administration déléguée permet à chaque domaine d'avoir une politique distincte.
- Tous les enregistrements font partie du domaine global.
- Le domaine de l'utilisateur actuel détermine le domaine à utiliser lors de l'affichage ou de l'utilisation d'un enregistrement dans un domaine différent.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Propriétés système du domaine et préférences utilisateur

Les administrateurs ont accès aux propriétés et aux préférences utilisateur qui contrôlent le champ d'application de domaine.

Propriétés

Les nouvelles activations de Séparation de domaine restreignent automatiquement le champ d'application de domaine au domaine de l'enregistrement pour toutes les données ou tous les processus associés. Lorsque l'utilisateur affiche un enregistrement dans un formulaire, les données connexes de l'enregistrement (telles que le sélecteur de référence et les données de liste connexe) et les processus appliqués (tels que les règles métier et les scripts clients) sont limités au champ d'application de domaine de l'enregistrement. Si des enregistrements sont présents dans plusieurs onglets, chaque onglet possède son propre champ d'application de domaine en fonction de l'enregistrement ouvert dans cet onglet. Les propriétés suivantes limitent le champ d'application de domaine au domaine de l'enregistrement et au domaine de la session en cours de l'utilisateur.

Propriétés système du domaine

Propriété	Détails
glide.sys.domain.use_record_domain_for_processes	Limite le champ d'application de domaine au domaine de l'enregistrement pour tous les processus. Cette propriété ne s'applique pas aux règles métier. Les règles métier sont toujours traitées à partir de l'enregistrement de domaine. • *Type* : vrai | faux • *Valeur par défaut* : vrai • *Emplacement* : table Propriétés système [sys_properties]
glide.sys.domain.use_record_domain_for_data	Limite le champ d'application de domaine au domaine de l'enregistrement pour toutes les données. • *Type* : vrai | faux • *Valeur par défaut* : vrai dans les nouvelles activations de domaines à partir de Fuji (les mises à niveau à partir d'instances

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés système du domaine (suite)

Propriété	Détails
	antérieures à Fuji n'ont pas cette propriété dans la table) • *Emplacement* : table Propriétés système [sys_properties]

Lorsque la propriété ou la `glide.sys.domain.use_record_domain_for_processesglide.sys.domain.use_record_domain_for_` propriété est définie sur **true**, les propriétés suivantes ne sont pas utilisées, quel que soit leur paramètre :

- `glide.sys.domain.use_record_domain`
- `glide.sys.domain.use_record_domain_for_client_scripts`
- `glide.sys.domain.domain_change_notify`
- `glide.sys.domain.no_change_roles`

Pour obtenir la liste complète des propriétés, reportez-vous à la section Propriétés système disponibles .

Remarque :

Dans les nouvelles activations de Séparation de domaine à partir de la version Jakarta, le domaine de session détermine les règles métier exécutées sur la table de domaine. Dans les versions précédentes, les règles métier exécutées sur la table de domaine étaient définies en fonction de la hiérarchie du domaine nouvellement créé. Ce comportement est modifié par la `glide.sys.domain.skip_domain_insert_businessrules` propriété. Définir cette propriété sur vrai améliore considérablement les performances d'insertion de domaine.

Propriétés du champ d'application de domaine pour les règles métier exécutées sur la table de domaine

Propriété	Détails
glide.sys.domain.skip_domain_insert_businessrules	Spécifie le champ d'application de domaine pour les règles métier exécutées sur la table de domaine. Dans les nouvelles activations de Séparation de domaine, la propriété par défaut est true et les règles métier sont déterminées par le domaine de session. Dans les implémentations existantes, la valeur par défaut de la propriété est false et les règles métier sont déterminées par la hiérarchie du domaine nouvellement créé. • *Type* : vrai | faux • *Valeur par défaut* : vrai dans les nouvelles activations de domaines à partir de Jakarta. False dans les implémentations existantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés du champ d'application de domaine pour les règles métier exécutées sur la table de domaine (suite)

Propriété	Détails
glide.sys.domain.skip_non_global_businessrule_if_nodomain	Garantit que seules les règles bus.rules du domaine global sont exécutées lors de l'utilisation de queryNoDomain() ou lorsque la table n'est pas séparée par domaine, de sorte que vous pouvez ignorer toute autre règle métier • *Type* : vrai | faux • Définir la propriété sur false restaure l'ancien comportement et ne s'aligne pas sur ServiceNow® les pratiques recommandées. • Recommandé : séparez vos tables par domaine ; Essayez toujours d'utiliser le domaine de l'enregistrement plutôt que le domaine de la session.

Préférences utilisateur

En outre, les administrateurs d'utilisateurs peuvent définir les préférences utilisateur suivantes globalement ou par utilisateur :

Préférences utilisateur pour le champ d'application de domaine

Préférence	Catégorie	Mis à jour par	Détails
glide.domain.session_scope	Domaine	Administrateur uniquement	Si la valeur est vraie, définit le champ d'application par défaut sur le domaine de la session de l'utilisateur plutôt que sur le domaine de l'enregistrement. Si la valeur est définie sur false, le champ d'application par défaut est le domaine de l'enregistrement. Les utilisateurs disposant du rôle d'utilisateur domain_expand_scope peuvent toujours modifier le champ d'application de domaine selon leurs besoins. • **Type** : vrai | faux • **Valeur par défaut** : faux
glide.domain.session_scope_notification	Domaine	Administrateur uniquement	Si la valeur est « vrai », affiche un repère visuel indiquant que les valeurs d'enregistrement incluent un champ d'application de domaine étendu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Préférences utilisateur pour le champ d'application de domaine (suite)

Préférence	Catégorie	Mis à jour par	Détails
			Si la valeur est définie sur false, la notification est masquée. • **Type** : vrai | faux • **Valeur par défaut** : true

Information associée

Propriétés de l'application Séparation de domaine

Créer un domaine

Vous pouvez créer un domaine en créant un enregistrement dans la table [domain].

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Lors de la création d'un nouveau domaine, gardez à l'esprit les points suivants :

- Un seul domaine peut être le domaine par défaut.
- Un seul domaine peut être le domaine principal.

Procédure

1. Accédez à la **Tout** > **Administrateur de domaine** > **Domaines**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs nécessaires (voir tableau).
4. Cliquez sur **Envoyer**.

Champs de formulaire de domaine

Champ	Description
Nom	Entrez un nom unique pour le domaine.
Type	Sélectionnez un type de domaine qui décrit le domaine. Par défaut, les types de domaines sont *Fournisseur*, *Client* et *MSP*. Vous pouvez également ajouter vos propres choix.
Primaire	Cochez la case si ce domaine doit être le domaine de niveau supérieur dans la hiérarchie. Le domaine de niveau supérieur n'a que des domaines enfants et aucun domaine parent.
Par défaut	Indiquez si ce domaine doit être le domaine par défaut de votre hiérarchie.
Parent	Sélectionnez le nom du domaine placé plus haut dans la hiérarchie qui contient ce domaine. Ce champ doit avoir une valeur pour que le domaine apparaisse sur la carte de domaine.
Actif	Cochez la case pour rendre le domaine disponible à l'utilisation. Vous devez sélectionner cette option pour que ce domaine apparaisse sur la carte de domaine.
Description	Entrez une description pour le domaine.

Chaque enregistrement de domaine peut également avoir plusieurs enregistrements connexes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sociétés
- Contient les domaines
- Contenu par

Que faire ensuite

Pour modifier la hiérarchie de domaine, accédez à la liste connexe Contient les domaines et sélectionnez les enregistrements de domaine qui sont les domaines enfants (contenus) de la relation contient.

Utiliser par défaut un domaine

Définition d'un domaine comme domaine auquel le système affecte automatiquement les enregistrements de tâches et d'utilisateurs qui ne sont pas déjà affectés à un domaine.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Remarque :
Si vous ne définissez pas de domaine par défaut, les nouvelles tâches et enregistrements utilisateur sont placés dans le domaine global.

Procédure

1. Accédez à la **Tout** > **Administrateur de domaine** > **Domaines**.
2. Ouvrez le domaine que vous souhaitez utiliser par défaut, par exemple, Principal.
3. Configurez la mise en page du formulaire pour ajouter le champ **Par défaut** .
4. Cochez la case **Par défaut**.
5. Cliquez sur **Mettre à jour**.

Gérer manuellement le domaine pour des enregistrements particuliers

Par défaut, le système attribue automatiquement un domaine en fonction de l'enregistrement de société de l'utilisateur. Dans certains cas, cependant, les administrateurs de domaine souhaitent gérer manuellement le domaine auquel appartient un enregistrement particulier.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Le champ **Domaine géré** permet aux administrateurs de domaine de sélectionner manuellement un domaine pour l'enregistrement d'utilisateur, de groupe, de département, d'emplacement ou de CI, plutôt que d'utiliser le domaine affecté automatiquement à partir de l'enregistrement de société. Le champ **Domaine géré** est disponible sur ces types d'enregistrements.

- Enregistrements utilisateur
- Enregistrements de groupe
- Enregistrements du département

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Enregistrements des emplacements
- Enregistrements de CI

Procédure

1. Accédez à l'enregistrement que vous souhaitez gérer manuellement.
2. Cochez la case **Domaine géré** .
3. Dans le champ **Domaine** , sélectionnez le domaine de l'enregistrement.
4. Cliquez sur **Mettre à jour**.

Si vous désactivez la case à cocher Domaine **géré** , le champ **Domaine** est masqué et l'enregistrement utilise la valeur de domaine de la société de l'enregistrement.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Tables séparées de domaine

Vous pouvez voir en un coup d'œil quelles tables sont séparées par domaine dans votre instance grâce à la fonctionnalité Tables séparées par domaine.

Vue d'ensemble

Utilisez la fonctionnalité Tables séparées par domaine pour voir quelles tables sont séparées par domaine. Commencez à saisir « domaine » dans le filtre **Tout** pour accéder aux **tables séparées par domaine** dans le volet de navigation de gauche.

Vous pouvez filtrer cette vue pour afficher ou supprimer des noms de colonnes afin de rechercher certaines propriétés ou attributs inclus dans vos tables. Il existe deux types de tables qui s'affichent dans la liste :

- Tables qui ont une colonne explicite `sys_domain` présente, où le nom de **colonne** affiche `sys_domain` la valeur dans la liste.
- Tables qui utilisent l'attribut pour dériver Séparation `domain_master` de domaine à partir d'un enregistrement référencé, où la colonne **Attributs** inclut la `domain_master=ref-field-value` valeur.

Lorsque vous utilisez les sélections Afficher la correspondance ou Filtrer dans le menu Nom de colonne, vous pouvez afficher ces deux types de tables.

Visionneuse de remplacement de domaine

La visionneuse de remplacement de domaine vous permet de voir et de gérer tous les remplacements de processus à la fois sur l'ensemble de l'instance.

Vue d'ensemble

Plutôt que de créer une recherche élaborée pour les remplacements dans vos scripts, vous pouvez utiliser la visionneuse de remplacement de domaine pour les trouver rapidement. Commencez à saisir « domaine » dans le filtre **Tout** pour accéder à la **visionneuse de remplacement de domaine** dans le volet de navigation de gauche.

Le sélecteur de table de la visionneuse de remplacement de domaine affiche une liste des tables contenant uniquement des remplacements d'enregistrement, ainsi qu'un nombre de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

remplacements dans cette table. Une fois que vous avez sélectionné une table, une liste de tous les enregistrements parents avec remplacements est renvoyée. Vous pouvez afficher rapidement tous les **enregistrements parents**, le **domaine** de l'enregistrement parent et un **nombre** de remplacements pour chaque enregistrement.

La sélection **de la vue remplace** charge un nouvel onglet dans lequel tous les remplacements, y compris l'enregistrement parent, s'affichent dans la vue de liste standard. Sélectionnez une table dans la liste déroulante pour afficher tous les enregistrements et remplacements. Sélectionnez **Afficher les remplacements** sur un enregistrement pour afficher tous les remplacements spécifiques à l'enregistrement.

Remarque :
Seules les tables avec remplacements sont répertoriées.

Pour plus d'informations, consultez Créer des remplacements de propriétés séparées par domaine .

Activer ou désactiver un domaine

Lorsque vous activez ou désactivez un domaine, l'état d'activation se répercute sur les sociétés du domaine.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Lorsque vous activez un enregistrement de société, Séparation de domaine active automatiquement le domaine associé de la société. Par exemple, si vous activez la société ACME, vous activez également le domaine TOP/ACME.

Procédure

1. Accédez à l'enregistrement du domaine.
2. Décochez ou sélectionnez la case **Actif** .
3. Cliquez sur **Mettre à jour**.

Avertissement :
Ne supprimez pas de domaines. Désactivez les domaines dont vous n'avez plus besoin au lieu de les supprimer.

Ajouter un champ de domaine à une table

En tant qu'administrateur, séparez par domaine une table personnalisée en y ajoutant un champ sys_domain.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Remarque :

N'ajoutez pas de domaines aux tables système de base.

Procédure

1. Accédez à la vue de liste de la table.
   Par exemple, tapez <table name>.list dans le filtre de navigation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Cliquez avec le bouton droit sur l'en-tête de liste et sélectionnez **Configurer** > **Mise en page de la liste**.
3. Dans la section **Créer un champ** , entrez `sys_domain` comme **Nom** et ID de `domaine` comme **Type**.
4. Cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer**.

Remarque :

Tout autre moyen de créer un champ ajoute un préfixe **u_** au nom de colonne. Mais avec le champ de domaine, le système crée automatiquement le champ sans le préfixe **u_** . Vous pouvez utiliser la fonctionnalité suivante comme raccourci : Chaque fois que vous créez un champ **sys_domain**, nommez-le **sys_domain** et laissez le type de champ tel quel. Le système définit automatiquement le type de champ sur **ID de domaine** et l'étiquette de champ sur **Domaine**, ce qui vous permet d'économiser quelques clics.

L'ajout de domaines aux tables du système de base nécessite des tests approfondis, des mises à jour et l'ajout d'une nouvelle logique prohibitifs. De plus, dans de nombreux cas, le code source n'est pas accessible au client.

Afficher les relations du domaine

La carte de domaine offre aux administrateurs de domaine une représentation en lecture seule des domaines actifs sur l'instance et de la façon dont ils sont liés les uns aux autres.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Toutes les cartes de domaine doivent avoir un domaine défini comme domaine principal. En outre, chaque domaine de la carte de domaine doit répondre aux critères suivants :

- Le champ **Parent** doit être renseigné (le domaine primaire est la seule exception à cette règle).
- La case **Actif** doit être cochée.

La carte de domaine ne dessine pas de relations de domaine pour les domaines qui ne répondent pas aux critères de mappage.

Procédure

1. Accédez à la **Tout** > **Administrateur de domaine** > **Carte de domaine**.
2. Cliquez sur les icônes plus (**+**) ou moins (**-**) sur les en-têtes de domaine pour afficher ou masquer les sous-domaines.

Sélectionner un domaine principal

Le domaine principal indique le domaine de niveau supérieur sur la carte de domaine.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Le domaine principal ne peut pas avoir de domaine parent et doit avoir au moins un domaine enfant. Il ne peut y avoir qu'un seul domaine principal à la fois. Si vous

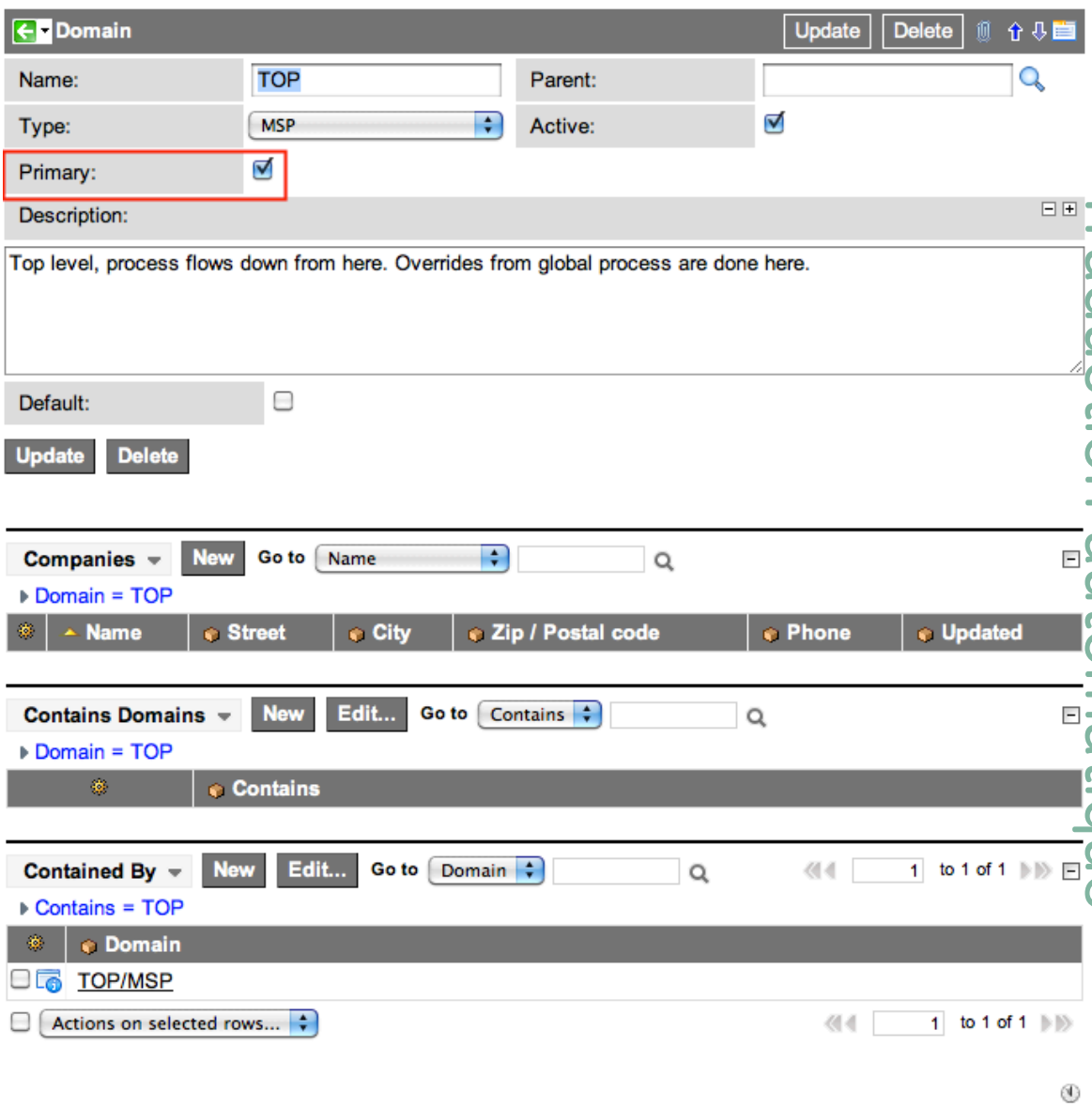
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sélectionnez un autre domaine comme domaine principal, il remplace le domaine principal précédent.

Procédure

1. Accédez à la **Tout** > **Administrateur de domaine** > **Domaines**.
2. Sélectionnez le domaine que vous souhaitez utiliser comme domaine principal, par exemple, TOP.
3. Sélectionnez la case à cocher **Primaire** .
4. Cliquez sur **Mettre à jour**.



Traduction automatique

Créer des relations contenues entre les domaines

Créez une relation « contient » entre les domaines pour modifier la hiérarchie de domaine.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

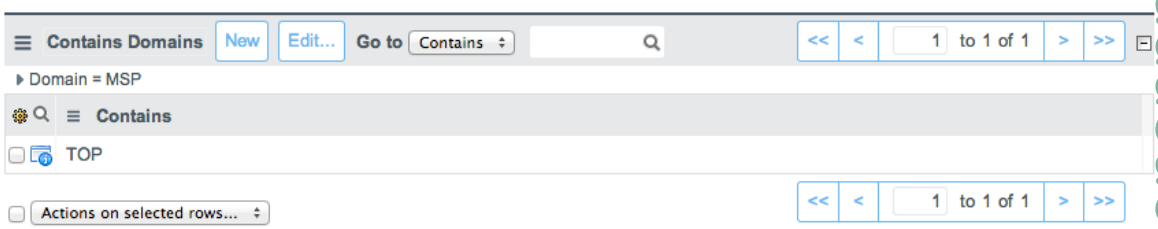
Les domaines d'une relation contient héritent des paramètres du domaine conteneur. Le domaine conteneur permet aux utilisateurs de voir les données du domaine contenu ainsi

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que n’importe lequel de ses enfants. Les processus ne sont pas affectés par une relation d’inclusion.

Procédure

1. Accédez à la table du domaine.
2. Sélectionnez l’enregistrement de domaine qui est le domaine parent (conteneur) de la nouvelle relation contient.
3. Basculez le champ d’application de domaine pour basculer entre le champ d’application de la session et le champ d’application de l’enregistrement, si nécessaire.
4. Dans la liste connexe Contient des domaines, cliquez sur **Modifier**.
5. Sélectionnez les enregistrements de domaine qui constituent les domaines enfants (contenus) de la relation contenue.
   Seuls les domaines enfants apparaissent par défaut lorsque le sélecteur de domaine est défini sur Global. Basculez le champ d’application de domaine pour voir tous les domaines.
6. Cliquez sur **Enregistrer**, puis sur **Mettre à jour**.



Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Élargir le champ d'application de domaine

Par défaut, lorsqu’un utilisateur du domaine global affiche une table contenant une **colonne sys_overrides** , il ne voit que les enregistrements du domaine global. Lorsqu’un administrateur du domaine global affiche une table de processus, il ne voit que les enregistrements qui se trouvent dans cette table de processus.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Remplacez la *glide.sys.restrict_global_domain_processes* propriété par **true**.
2. Pour afficher les enregistrements de tous les domaines, cliquez sur **Développer le champ d’application de domaine** sous Liens connexes.
3. Pour revenir à l’affichage des enregistrements du domaine global uniquement, cliquez sur **Réduire le champ d’application de domaine**.

Ajouter des domaines à une liste de domaines de visibilité

L’ajout d’un domaine de visibilité permet à un utilisateur ou à un groupe de voir et éventuellement de modifier les enregistrements d’un autre domaine, quelle que soit l’appartenance normale de l’utilisateur ou du groupe au domaine.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

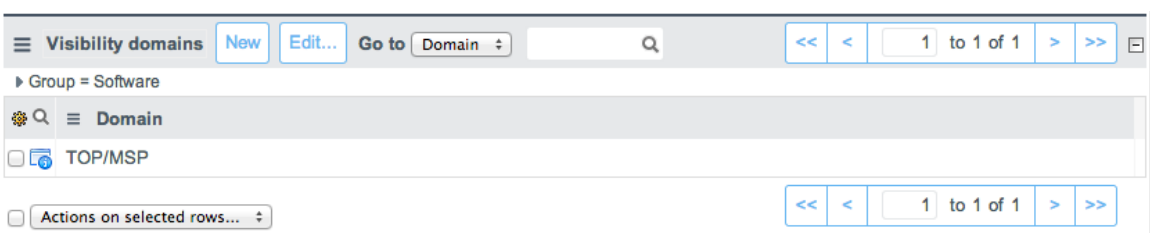
Pourquoi et quand exécuter cette tâche

Il est préférable d'affecter des domaines de visibilité à tous les membres d'un groupe plutôt que de les accorder à des utilisateurs individuels.

Remarque :
L'ajout d'un domaine de visibilité ne modifie pas les exigences de règles de contrôle d'accès à une table ou à un enregistrement.

Procédure

1. Accédez à la table de groupe.
2. Sélectionnez le groupe auquel vous souhaitez attribuer des domaines de visibilité.
3. Ajoutez la liste connexe **Domaines de visibilité** au formulaire.
4. Dans la liste connexe **Domaines de visibilité** , cliquez sur **Modifier**.
5. Sélectionnez les enregistrements de domaine que vous souhaitez que le groupe ou le domaine voie.
6. Cliquez sur **Enregistrer**, puis sur **Mettre à jour**.



Attribuer des domaines de visibilité à un utilisateur individuel

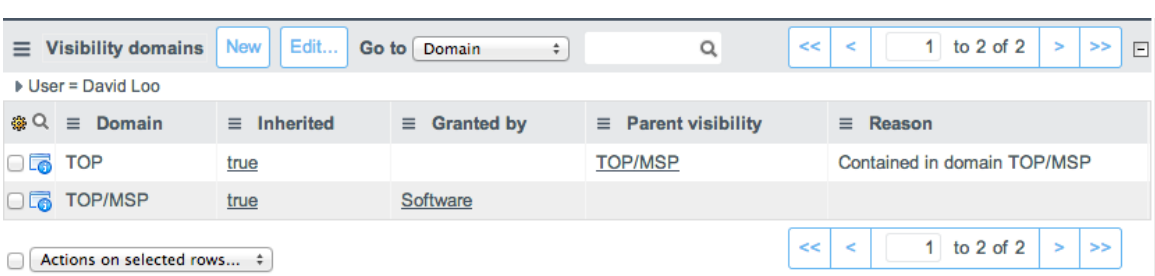
Bien qu'il soit possible d'ajouter des domaines de visibilité pour des utilisateurs spécifiques sur le formulaire Utilisateur, il est préférable de les ajouter uniquement via des groupes. Contrôle les autorisations et l'accès en cas de changement de service ou de départ de l'entreprise.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateur**.
2. Sélectionnez l'utilisateur auquel vous souhaitez attribuer des domaines de visibilité.
3. Ajoutez la liste connexe **Domaines de visibilité** au formulaire.
4. Dans la liste connexe Domaines de visibilité, cliquez sur **Modifier**.
5. Sélectionnez les domaines dont vous souhaitez que l'utilisateur voie les enregistrements.
6. Cliquez sur **Enregistrer**, puis sur **Mettre à jour**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La liste incorporée Domaine de visibilité contient les champs suivants.

Champ	Description
Domaine	Domaine visible par le groupe ou l'utilisateur.
Hérité	Le domaine est hérité de la visibilité du domaine ou d'un domaine parent.
Accordé par	Nom du groupe qui a accordé la visibilité du domaine.
Visibilité du parent	Nom du domaine parent et utilisé pour le regroupement des enregistrements. Si l'enregistrement parent est supprimé, tous les enregistrements ayant le même parent sont également supprimés.

Créer une liste de choix spécifique à un domaine

Les administrateurs peuvent configurer des listes de choix de sorte qu'elles contiennent des entrées spécifiques à un domaine particulier.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Sélectionnez le domaine dans le sélecteur de domaine dans lequel le choix doit être ajouté.
2. Cliquez avec le bouton droit sur le champ de choix que vous souhaitez personnaliser et sélectionnez **Configurer les choix**.
3. Mettez à jour ou ajoutez des choix.
4. Poussez les changements par le biais du processus de changement normal tel que les ensembles de mises à jour.

Remarque :
Les administrateurs doivent s'assurer que les choix sont uniques dans les domaines afin d'éviter toute confusion administrative dans le domaine global.

Si un administrateur ajoute un nouveau choix à partir du domaine global, les utilisateurs des domaines situés plus bas dans la hiérarchie voient ce nouveau choix à la fin de leur liste de choix actuelle. Si le nouveau choix n'est pas actif au niveau global, il est alors disponible pour les utilisateurs du domaine via **Configurer les choix** , mais ne s'affiche pas comme un choix actif.

Administration avancée de Domain Separation

Les administrateurs peuvent afficher des informations sur Séparation de domaine, identifier les problèmes potentiels et modifier les paramètres de configuration.

Vous pouvez effectuer ces tâches administratives avancées sur les domaines :

- Utiliser les menus de sélection de domaine
- Afficher les relations du domaine

Utiliser les menus de sélection de domaine

L'instance propose une sélection de domaine via deux formats de menu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Sélecteur de domaine : fournit une liste déroulante simple des domaines disponibles.
- Sélecteur de référence de domaine : active un champ de référence qui offre un filtrage et une fonctionnalité de saisie semi-automatique et de saisie automatique. Utilisez ce format pour les listes plus longues.

L'emplacement de ces sélecteurs et la procédure permettant de les afficher ou de les masquer diffèrent selon la version de l'interface utilisateur.

Activer les menus de sélection de domaine dans Interface utilisateur principale

L'affichage du sélecteur de domaine dans Interface utilisateur principale active le sélecteur de domaine par défaut. Après avoir activé le sélecteur de domaine, vous pouvez ajouter une propriété système pour activer le sélecteur de référence de domaine.

Avant de commencer

Remarque :
Séparation de domaine (module d'extension com.snc.pa.domain_support) est requis pour activer le sélecteur de référence de domaine.

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Procédure

1. Cliquez sur l'icône d'engrenage dans l'en-tête.
2. Dans l'onglet Général, cliquez sur **Afficher le sélecteur de domaine dans le commutateur d'en-tête** .
   Le sélecteur de domaine apparaît dans l'en-tête Interface utilisateur principale .
3. **Facultatif :** Activez le sélecteur de référence de domaine.

   Remarque :
   L'activation du sélecteur de référence de domaine supprime l'option globale de la liste. Pour revenir à votre domaine d'origine, cliquez sur la flèche de retour en regard du champ de référence. Les utilisateurs administrateurs peuvent cliquer sur la flèche de retour pour revenir au domaine global.

   a. Saisissez `sys_properties.list` dans Application Navigator.
   b. Si ce n'est pas déjà fait, ajoutez la propriété `glide.ui.domain_reference_picker.enabled` et définissez la valeur sur **true**.
   c. Actualisez le navigateur.
   Le sélecteur de référence de domaine apparaît dans l'en-tête Interface utilisateur principale .

Restreindre l'accès au sélecteur de domaine

Utilisez une propriété système pour restreindre l'accès au sélecteur de domaine dans Interface utilisateur principale et Next Experience.

Avant de commencer
Rôle requis : administrateur

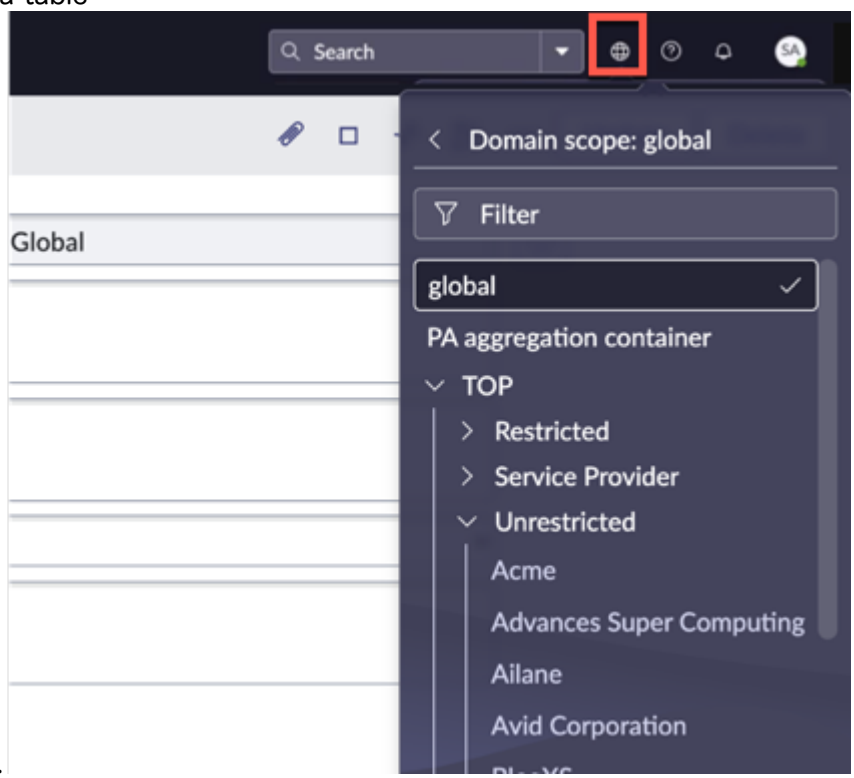
Pourquoi et quand exécuter cette tâche
Par défaut, les utilisateurs disposant du rôle ITIL et des rôles qui incluent le rôle ITIL (tels que l'administrateur) peuvent accéder au sélecteur de domaine dans Next Experience. Vous pouvez accorder l'accès à d'autres rôles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

en les ajoutant à la propriété ou restreindre les rôles en les supprimant. Il est recommandé de limiter le rôle aux administrateurs uniquement.

Les administrateurs peuvent accorder l'accès aux utilisateurs en créant une propriété système dans la table sys_properties.



Procédure

1. Ouvrez la table Propriétés système [sys_properties].
2. Ajoutez cette propriété : `glide.ui.polaris.domain_picker.role`
3. Configurez la valeur de la propriété sous la forme d'une liste de rôles séparés par des virgules : **admin, itil**. Pour en savoir plus, consultez Configurer les sélecteurs Next Experience

Propriétés de l'application Séparation de domaine

Le module d'extension Séparation de domaine dispose de deux nouvelles tables pour donner aux fournisseurs de services plus de flexibilité dans la personnalisation de leurs applications qui utilisent Séparation de domaine. Il s'agit de la table Propriétés de l'application système [sys_application_property] et de la table Valeur de propriété de l'application système [sys_application_property_value].

Les nouvelles tables offrent plus d'options

Avec les applications de fournisseur de services (SP), certaines actions peuvent varier en fonction du domaine. Toutefois, la ServiceNow® table Propriétés système du système de base [sys_properties] n'est pas séparée par domaine, elle ne répond donc pas aux exigences des applications qui utilisent Séparation de domaine.

Chaque client SP peut souhaiter personnaliser ses applications différemment. Auparavant, les fonctionnalités pouvant être personnalisées n'étaient définies que sous la forme d'une seule valeur globale. Les développeurs d'applications ont besoin d'une table plus flexible. Vous pouvez désormais modifier votre application sans avoir à créer de code à chaque fois que vous souhaitez ajouter ou modifier la fonctionnalité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Comment fonctionnent les remplacements dans les nouvelles tables

Les développeurs utilisent généralement la ServiceNow table Propriétés système [sys_properties] pour créer diverses fonctions dans les applications. Si vous souhaitez développer une application pour qu'elle se comporte différemment dans différents domaines, vous devez la personnaliser vous-même.

Dans la version Paris, la nouvelle table Propriétés de l'application [sys_application_property] simplifie cette personnalisation. Au lieu d'aller directement à la table Propriétés système pour une valeur, la table des propriétés de l'application va d'abord à la table Application système. Cette nouvelle table stocke maintenant la logique dont vous avez besoin pour configurer votre application. S'il trouve une propriété dans la nouvelle table, il utilise ce contenu. Si aucune information n'est contenue dans cette table, elle passe à la table des propriétés système de base.

Lorsque vous configurez la prise en charge de Séparation de domaine, vous pouvez ajouter une logique de domaine à cette nouvelle table Propriétés de l'application. Cette table peut contenir des propriétés qui n'existent pas dans la table Propriétés système. Vous pouvez également ajouter des propriétés à la table de configuration qui peuvent remplacer n'importe quelle propriété que vous sélectionnez dans la table Propriétés système.

Par exemple, supposons que vous souhaitiez configurer une application avec une fonctionnalité Premier jour de la semaine. Parfois, vous voudrez peut-être que le premier jour de la semaine soit le dimanche. Dans d'autres cas, vous voudrez peut-être que le premier jour de la semaine soit le lundi. Dans la table du système de base, il se peut qu'il n'y ait qu'une seule option Jour 1, qui est le dimanche. Avec la nouvelle table, vous pouvez stocker une autre propriété, ce qui fait que le Jour 1, le dimanche, et un domaine enfant, le lundi.

Cette figure montre comment le système tire les propriétés de la table Propriétés de l'application avant d'accéder à la table Propriétés système [sys_properties].



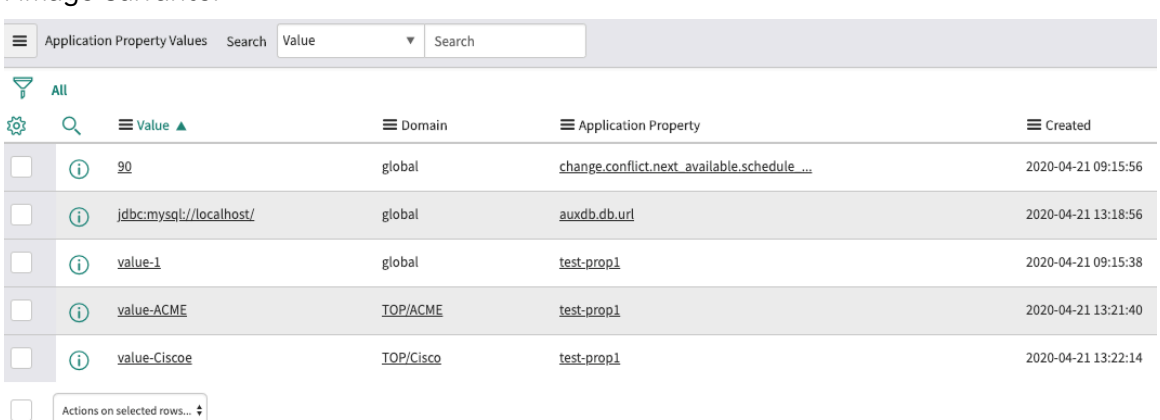
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnement des applications incluses dans le périmètre dans la nouvelle table

La nouvelle table Propriétés de l'application est prise en charge dans les applications incluses dans le périmètre. Le nom de la propriété de l'application, similaire au nom de la propriété système, est unique, ce qui signifie qu'il est précédé du nom du périmètre s'il n'est pas global. Le périmètre d'une application a une incidence sur votre configuration. Le champ d'application peut déterminer quel jour 1 est défini comme dimanche et lequel comme lundi. Vous pouvez utiliser la même propriété, mais la personnaliser de sorte que Jour 1, Dimanche soit le domaine parent et Jour 1, Lundi soit le domaine enfant. Dans la nouvelle table, il y a à la fois une colonne de domaine et une colonne de champ d'application, afin que vous puissiez définir ces propriétés pour chacune.

Vous pouvez utiliser la vue Étendre le champ d'application de domaine dans la table sys_application_property_value pour afficher tous les remplacements, comme illustré dans l'image suivante.



Remarque :

Si ces tables ne sont pas disponibles, assurez-vous d'avoir activé le module d'extension Domain Extension Installer (com.glide.domain.msp_extensions.installer).

Nouvelles tables de propriétés d'application

La nouvelle table Propriétés de l'application système [sys_application_property] contient les champs suivants :

- name
- description
- type (choix de chaîne, vrai|faux, nombre entier, fuseau horaire, couleur, etc.)
- default_value
- Propriété (référence à sys_properties)
- usage_notes
- read_roles
- write_roles
- Clé unique : (nom)

La nouvelle table Valeur de propriété d'application système [sys_application_property_value] contient les champs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- sys_application_property (réf. à sys_application_property)
- sys_domain
- sys_overrides
- valide
- Clé unique : (sys_application_property, sys_domain)

Nouvelles API

Les nouvelles API sont également prises en charge dans les applications incluses dans le périmètre. Les propriétés d'application séparées par domaine ont des API distinctes. L'API GlideApplicationProperty dispose de deux nouvelles méthodes scriptables, disponibles dans les applications globales et incluses dans le périmètre. Consultez GlideApplicationProperty - Scoped, Global pour en savoir plus sur ces nouvelles API.

Information associée

Pratiques recommandées de séparation de domaine pour les fournisseurs de services

Outil de migration de domaine

Utilisez l'outil de migration de domaine pour déplacer un client d'un environnement séparé par domaine vers sa propre instance dédiée.

Module d'extension Domain Migration Tool

Le module d'extension Domain Migration Tool (com.glide.domain.migration_tool) simplifie la tâche de déplacement d'un client d'un environnement séparé par domaine vers une instance dédiée plus flexible. Les clients peuvent souhaiter migrer vers une instance distincte pour tirer davantage parti des Now Platform options. Bien que le module d'extension Séparation de domaine soit installé, les propriétés de séparation des données et des processus sont désactivées.

Remarque :
Vous devez demander une instance clonée et demander l'activation du module d'extension Outil de migration de domaine avant de pouvoir l'utiliser.

L'outil de migration de domaine s'exécute uniquement si la séparation des données et des processus est activée dans l'instance séparée par domaine :

- La `glide.sys.domain.partitioning` propriété de données doit être définie sur **true**.
- La `glide.sys.domain.delegated_administration` propriété de processus doit être définie sur **true**.

Fonction de l'outil de migration

- Automatise une grande partie du processus de migration, en particulier le nettoyage des données.
- Migre l'instance séparée par domaine vers une nouvelle instance dédiée.
- Supprime les données de l'instance dédiée.

Remarque :
L'outil ne supprime pas les données globales, dans le domaine cible ou dans des domaines de données supplémentaires (si spécifié).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Réduit les données de processus ou, s'il ne peut pas les réduire, supprime les données de processus
- Conserve les enregistrements de processus visibles par le domaine cible
- Met à jour les tables spéciales sys_choice, sys_ui_list et sys_ui_related_list
- Nettoie les enregistrements ajoutés par les modules d'extension Domain Separation :
  - Règles métier
  - Actions d'interface utilisateur
  - Travaux planifiés
  - Sorties d'installation
  - Modules de navigation
- Désactive Séparation de domaine et supprime les domaines de l'instance clonée :
  - Définit ces propriétés sur **false** dans l'instance clonée :
    - *`glide.sys.domain.partitioning`*
    - *`glide.sys.domain.delegated_administration`*
    - *`glide.sys.domain.enabled`*
  - Supprime tous les domaines, à l'exception du domaine cible et de tous les domaines de données supplémentaires spécifiés.
- Met à jour le champ **État** dans la table domain_migration_tool_status.

État individuel des tables

Statut	Description
En attente	État par défaut des tables séparées par domaine pendant la migration. Les tables doivent être migrées, mais la migration n'a pas encore démarré.
Échec	Défaillance du niveau de la table. Si le processus de migration s'est terminé avec des erreurs, cet état indique quelles tables présentent des erreurs.
En cours d'exécution	État de la table actuellement en cours de migration. Une seule table peut avoir cet état et est en cours de migration.
Réussi	État des tables qui ont migré avec succès.
Terminé avec succès	Le processus de migration s'est terminé sans erreur.
Terminé avec erreurs	Le processus de migration s'est terminé avec des erreurs.

- Consigne la progression et l'état à syslog_domain

  La source est **MigrationTool** pour toutes les entrées de journal associées à la migration.
  - Consigne chaque table de données et le nombre de tables de données restantes
  - Consigne chaque table de processus et les enregistrements du domaine qui sont actuellement désactivés ou supprimés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce que l'outil de migration ne fait pas

- Cloner l'instance
- Créer une autre instance séparée par domaine
- Migrer les enregistrements (données ou processus) si les propriétés de séparation des données ou des processus sont désactivées avant d'exécuter l'outil
- Modifier les données sur l'instance source
- Supprimer les données globales, dans le domaine cible ou dans des domaines de données supplémentaires (si spécifié)

Ce que vous devez faire après avoir exécuté l'outil

L'outil de migration de domaine automatise la suppression des données en dehors des domaines souhaités (le domaine cible, tous les domaines de données supplémentaires et le domaine global). Vous devez évaluer toutes les configurations restantes pour vous assurer qu'elles sont appropriées et qu'elles fonctionnent pour votre instance dédiée. Par exemple, si vous avez une règle métier qui définit le champ Domaine sur les enregistrements, vous pouvez désactiver cette règle métier, car elle n'a plus d'utilité.

Migrer une instance séparée par domaine vers une instance dédiée

Déplacez un client d'un environnement séparé par domaine vers son propre environnement d'instance dédié.

Avant de commencer

Rôle requis : security_admin et admin

Procédure

1. Élever au rôle de security_admin.
   Consultez Élever à un rôle privilégié pour en savoir plus.
2. Accédez à la **Tout** > **Administrateur de domaine** > **Outil de migration de domaine**.
   Accès également avec **domain_migration_tool_status.list**.
3. Cliquez sur **Nouveau**.
4. Complétez le formulaire.

Champ	Description
Domaine cible	Spécifiez le domaine utilisé pour le processus et les données que vous souhaitez migrer. Seul le domaine cible est conservé, aucun de ses enfants, sauf indication contraire dans le champ **Domaines de données supplémentaires** .
Domaines de données supplémentaires	Vous pouvez également spécifier tous les domaines de données supplémentaires que vous souhaitez migrer. Si vous souhaitez migrer le domaine cible et tous ses enfants, vous devez spécifier tous les enfants.

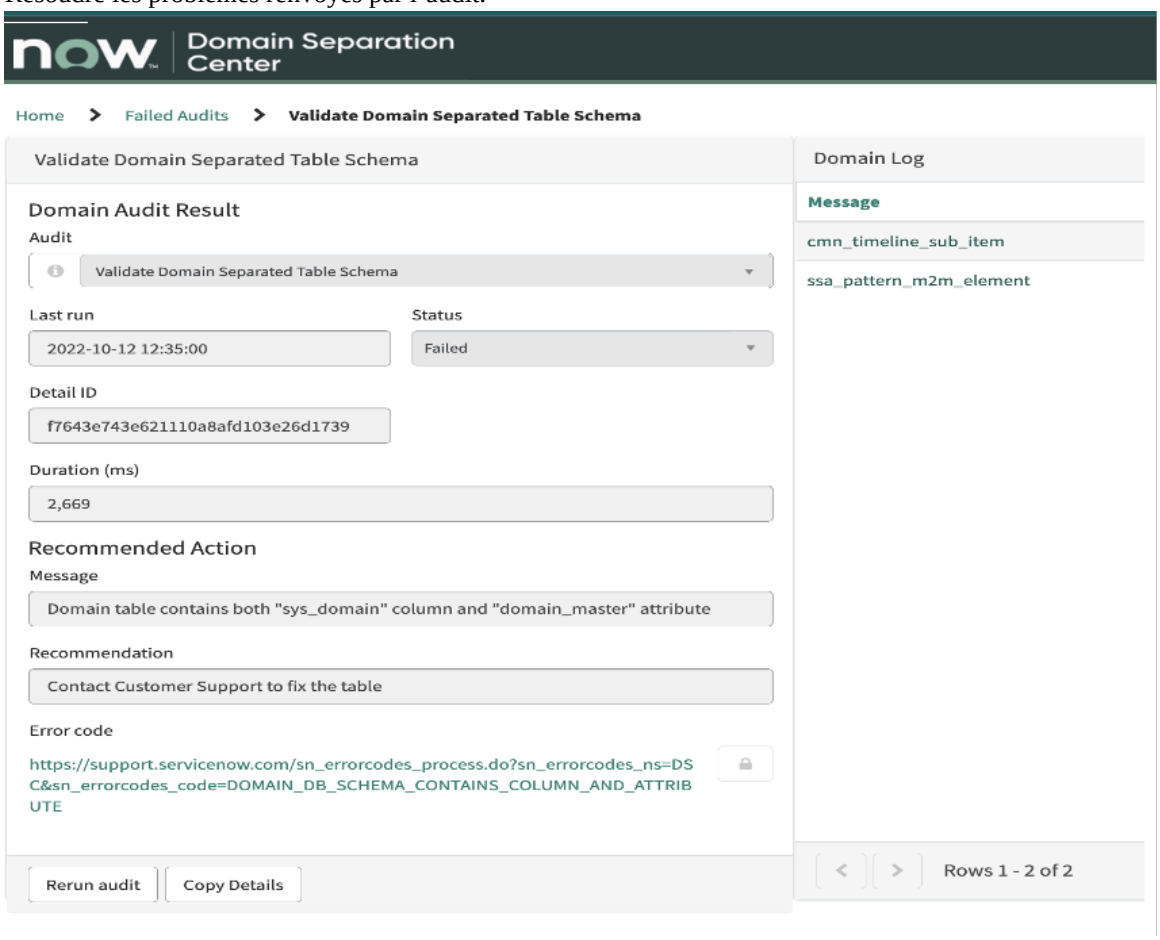
5. Sélectionnez **Soumettre**.
6. Ouvrez le formulaire que vous venez de soumettre.
7. Accédez à la **Tout** > **Centre Séparation en domaines** > **Configurer des audits** .
   Consultez Centre Séparation en domaines pour plus d'informations.
8. Définissez l'audit **Valider le schéma de table séparée par domaine** sur **Actif** et affectez un calendrier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il s’agit d’un audit de domaine de précaution visant à prévérifier l’intégrité du schéma des tables séparées par domaine. Cela vous permet de corriger les erreurs avant d’exécuter la migration.

9. **Exécutez le calendrier d’audit** qui inclut le schéma.
   Consultez Exécuter les audits immédiatement pour en savoir plus.
10. Résoudre les problèmes renvoyés par l’audit.

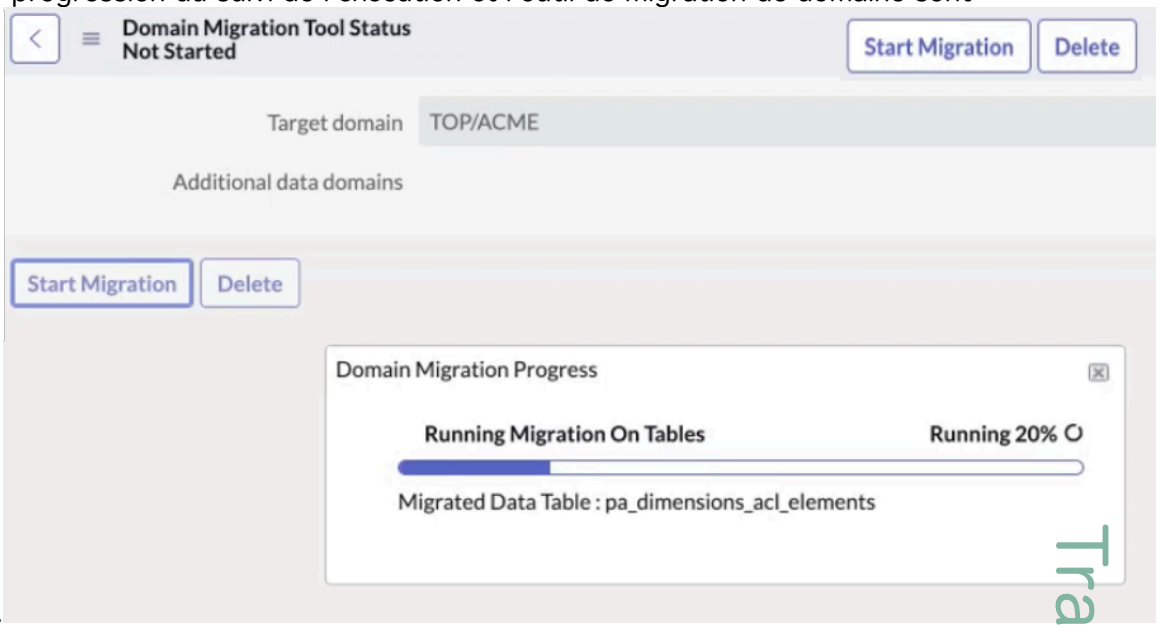


11. Sélectionnez **Démarrer la migration**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- La barre de progression du suivi de l'exécution et l'outil de migration de domaine sont déclenchés.



- La table de migration progressive actuelle s'affiche avec le pourcentage total de tables correctement migrées.
- Table dans laquelle toutes les tables séparées par domaine sont enregistrées avec l'état de migration, le nombre total d'enregistrements dans chaque table et le nombre d'enregistrements migrés.
- Le nombre de tables où la migration a échoué est également enregistré.
- **L'état** est mis à jour au fur et à mesure que l'outil exécute ses fonctions.
- La migration de domaine est toujours en cours d'exécution en arrière-plan si vous fermez la barre de progression. Accédez à la table `sys_execution_tracker` et recherchez **Migration en cours d'exécution sur les tables** pour vérifier que le processus de migration s'exécute en arrière-plan.

L'état de l'outil de migration de domaine affiche les champs suivants :

Champs d'état de l'outil de migration de domaine

Champ	Description
Statut	Affiche l'état de la migration. ○ **Migration des tables de données...** : état en cours. ○ **Migration réussie** : état mis à jour après une migration réussie. ○ **Une mauvaise configuration est observée sur l'une des tables séparées par domaine** : Indique un échec de la migration des données. Une erreur de schéma a été trouvée, la migration ne démarre pas. Exécuter l'audit **Valider le schéma de table séparée par domaine**. L'audit échouera et affichera les tables qui ne suivent pas la norme de schéma. ○ **Terminé avec des erreurs dans les tables de revisite** : le nombre de tables pour traiter la migration de schéma est répertorié. Localisez les défaillances dans le nombre de tables de revisite et résolvez les problèmes de schéma.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

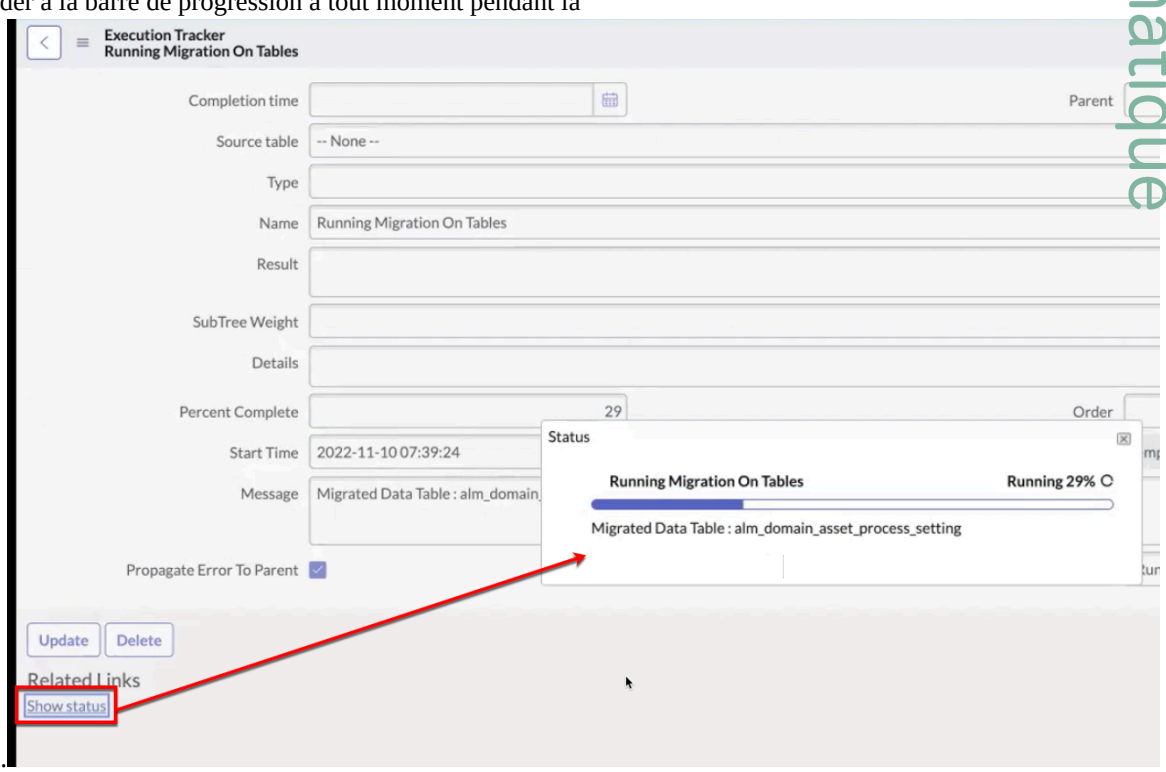
Champ	Description
	○ **Échec de la migration de domaine pour les tables...** : les enregistrements non cibles doivent être supprimés manuellement des tables ayant échoué. ○ **Terminé avec succès** : lorsque toutes les tables ont migré.
Domaine cible	Domaine cible sélectionné pour la migration.
Domaines de données supplémentaires	Renseigné si plusieurs domaines de migration ont été sélectionnés.
Nombre des tables de revisite	Ce champ est renseigné uniquement si la migration d'une table échoue. S'il n'y a pas d'échecs, ce nombre est égal à zéro. Dans ce cas, les tables seront revisitées pour retenter la migration. En l'absence d'échecs, il n'est pas nécessaire de revoir les tables ou de retenter la migration.
Table de progression actuelle	Affiche le nom de la table actuellement en cours de migration. Une fois la migration réussie, ce champ sera vide.

12. Sélectionnez le lien **Cliquez ici** sur la page État de l'outil de migration de domaine pour ouvrir le suivi des exécutions.



Vous pouvez également accéder à la table *sys_execution_tracker* et rechercher **Migration en cours d'exécution sur les tables** pour vérifier que le processus de migration s'exécute en arrière-plan.

13. Sélectionnez **Afficher l'état** dans la section Liens connexes pour accéder à la barre de progression à tout moment pendant la migration.



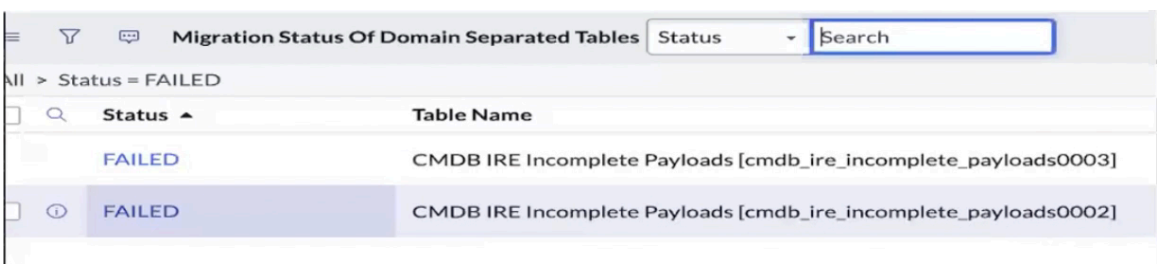
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

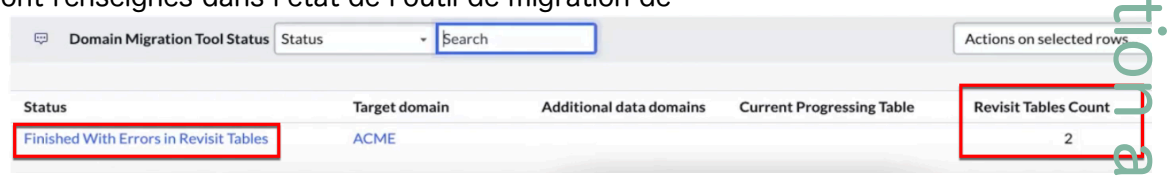
En cas d'échec de la vérification du schéma d'une table, l'état global de la migration des tables séparées par domaine est **défini sur** **Échec**.



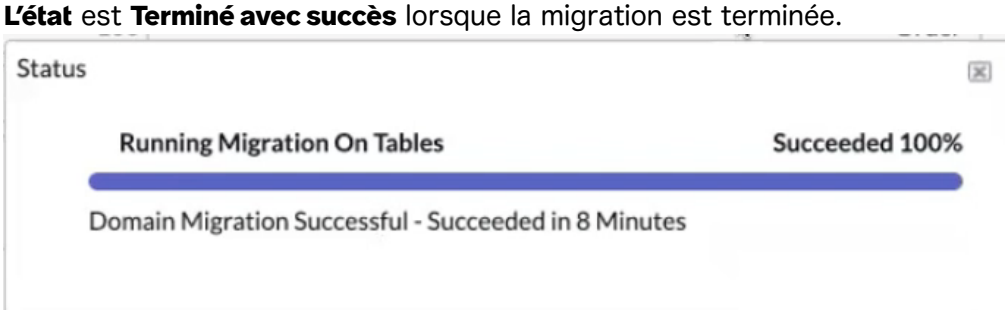
Il y aura des entrées **d'échec** pour chaque table correspondante.



Le reste de la migration se poursuit et un résumé de toutes les tables ayant échoué ainsi que le nombre total de **tables de revisite** sont renseignés dans l'état de l'outil de migration de domaine.



L'état est **Terminé avec succès** lorsque la migration est terminée.



Administration des processus

L'administration des processus permet aux administrateurs de définir des stratégies spécifiques à un domaine.

Les politiques définies plus bas dans la hiérarchie de domaine remplacent les politiques définies plus haut dans la hiérarchie de domaine. Dans un domaine, les administrateurs peuvent définir des versions spécifiques au domaine de ces stratégies et paramètres globaux :

- Scripts clients
- Politiques système
- Noms des applications et des modules

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rôles d'application
- Filtres de module

⚠ Avertissement :
Tous les utilisateurs ayant le rôle administrateur bénéficient d'un accès spécial à l'ensemble des fonctionnalités, fonctions et données système, car les administrateurs peuvent remplacer les règles ACL et subir avec succès toutes les vérifications de rôles. Accordez ce privilège avec soin.

Lorsque les utilisateurs disposent du rôle **administrateur** , toutes les politiques de l'instance sont disponibles, quel que soit le domaine affecté. Ils peuvent entrer un domaine spécifique, puis seules les politiques de ce domaine ou d'une politique supérieure sont visibles et traitées lors d'une transaction pertinente. Lorsqu'un administrateur modifie une politique qui se trouve dans un domaine supérieur ou dans le domaine global, le système crée automatiquement un nouvel enregistrement pour le domaine actuel de cet administrateur. Elle ne modifie pas l'enregistrement de politique, d'application ou de module d'origine. Ce nouvel enregistrement remplace l'original.

Pour apporter des changements à une politique dans un domaine de niveau inférieur, accédez à ce domaine et modifiez la politique. Cette approche crée l'enregistrement de politique dans votre domaine qui remplace l'enregistrement de politique de niveau supérieur d'origine.

Ne modifiez pas la politique de niveau supérieur, puis le champ **Domaine** de cette politique. Cette approche ne crée pas d'enregistrement de politique dans votre domaine de niveau inférieur et ne conserve pas non plus l'enregistrement de politique pour le domaine de niveau supérieur.

Le champ **sys_overrides** indique qu'une politique, une application ou un module d'un niveau inférieur dans la hiérarchie remplace un enregistrement d'un niveau supérieur. Le système définit automatiquement ce champ lorsqu'un administrateur tente de modifier une politique, une application ou un module appartenant à un autre domaine placé plus haut dans la hiérarchie.

Plutôt que de modifier l'enregistrement de niveau supérieur, la tentative de mise à jour est modifiée en un encart et le champ **sys_overrides** est défini pour indiquer la politique, l'application ou le module de niveau supérieur en cours de remplacement. Plus tard, lorsque les enregistrements d'une transaction pertinente sont chargés, la politique, l'application ou le module spécifique au domaine de remplacement est utilisé à la place de l'original.

Domaines pour l'administration des processus

Par défaut, l'administration des processus utilise toujours le domaine de l'enregistrement pour déterminer les politiques à appliquer.

Le domaine de l'enregistrement a priorité sur le domaine de l'utilisateur. Si le domaine de l'enregistrement ne contient aucune politique, l'administration déléguée recherche les politiques se situant au niveau immédiatement supérieur de la hiérarchie de domaine. La recherche de politiques de domaine se poursuit dans la hiérarchie des domaines jusqu'à atteindre le domaine global. S'il n'y a pas de politiques de domaine plus bas dans la hiérarchie de domaine, l'administration des processus utilise les politiques pour le domaine global.

Par exemple, Fred Luddy est un utilisateur du domaine Acme qui peut voir les enregistrements dans les domaines enfants des domaines enfants Acme : Atlanta, Acme : San Diego et Acme : NY. Lorsque cet utilisateur ouvre un enregistrement dans le domaine Acme : San Diego, l'administration des processus vérifie d'abord les politiques dans le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

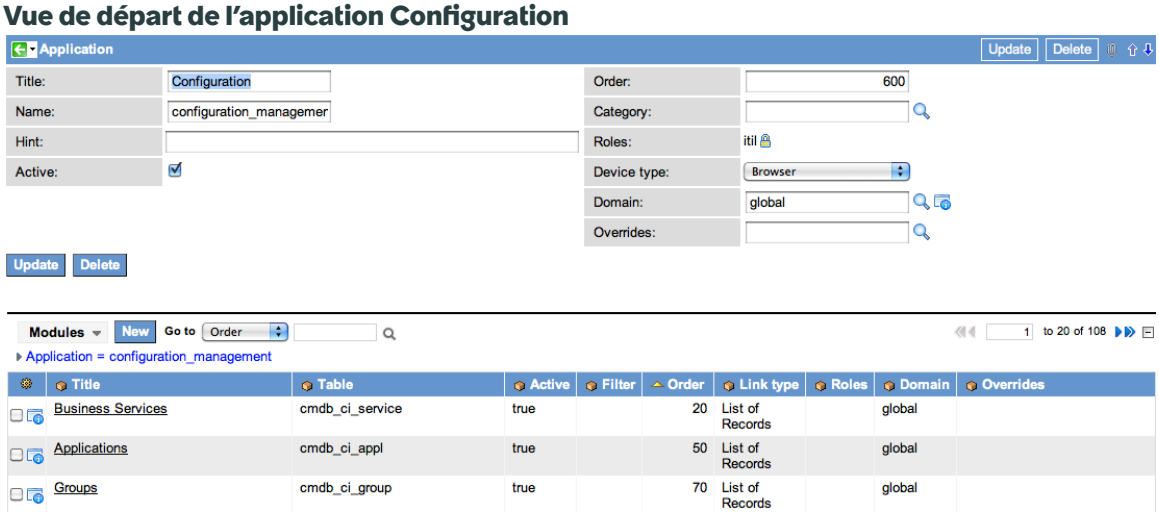
domaine Acme : San Diego. S'il n'y a pas de politiques à ce niveau de la hiérarchie du domaine, l'administration des processus recherche les politiques du domaine ACME. Si aucune politique n'est disponible dans le domaine ACME, l'administration des processus utilise les politiques de domaine globales, car il n'existe aucun autre domaine placé plus haut dans la hiérarchie de domaine.

Exemple d'administration de processus avec des applications spécifiques à un domaine

L'exemple suivant illustre l'administration des processus avec des applications et des modules spécifiques au domaine.

En tant qu'administrateur du domaine Oceanic, David Loo décide de personnaliser l'application Configuration. Pour commencer, David passe en revue les modules disponibles dans le module d'application Configuration.

Vue de départ de l'application Configuration



David décide de renommer l'application de configuration en CMDB et d'autoriser le rôle inventory_admin à voir l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de modifications spécifiques à un domaine de l'application de configuration

Applications | New | Go to Title | 1 to 20 of 46

All > Active = true > Device type != Mobile

Title	Active	Order	Roles	Name	Domain	Overrides
Asset Management	true	900	asset	asset	global	
BSM Map	true		admin itil	bsm_map	global	
Change	true	400	itil	change_management	global	
CMDB	true	600	itil inventory_admin	configuration_management	Database	configuration_management
Content Management	true		content_admin	cms	global	
Contract Management	true	1,000	asset contract_manager	asset_contracts	global	
Domain Admin	true		domain_admin	domain_admin	global	
ECC	true		admin	ecc	global	
Homepage Admin	true		admin	home	global	
Incident	true	200	itil	incident_management	global	
Instance Clone	true		clone_admin	instance_clone	global	
Knowledge Base	true	800	knowledge	km	global	
Metrics	true		itil_admin metric_admin	metrics	global	
MID Server	true		admin	MID	global	
Organization Management	true	875	asset	organization_management	global	
Problem	true	300	itil	problem_management	global	
Reports	true	1,100	itil	reports	global	
SAML 2 Single Sign-on	true		admin	saml_2_single_sign_on	global	
SAML Single Sign-on	true		admin	SAML Single Sign-on	global	

Activate | Deactivate | Actions on selected rows... | 1 to 20 of 46

Ensuite, David décide de modifier l'application Incident en activant le module **Ouvert - dans « Nouveau » état** et en ajoutant un nouvel élément de filtre pour afficher les incidents ouverts dans la catégorie Océanique.

Exemples de modifications spécifiques à un domaine du module État Ouvert - « Nouveau »

Module | = Required field | Update | Delete

Title:	Open - in "New" state	Link type:	List of Records
Table:	Incident [incident]	View name:	
Order:	200	Roles:	
Application:	incident_management		
Hint:			
Active:	☑		
Image:			

Filter:

	Incident state	is	New
and	Active	is	true
and	Category	is	Database

Arguments:

```
incident_state=1^active=true
```

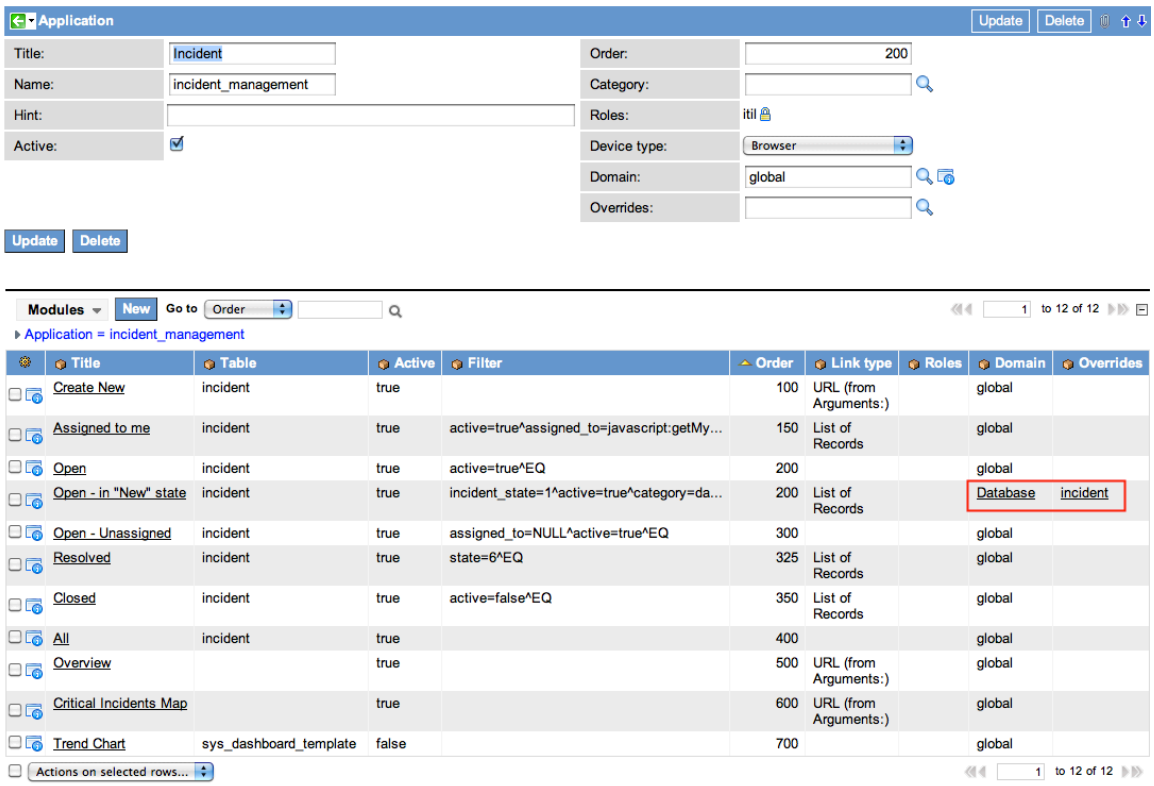
Update | Delete

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

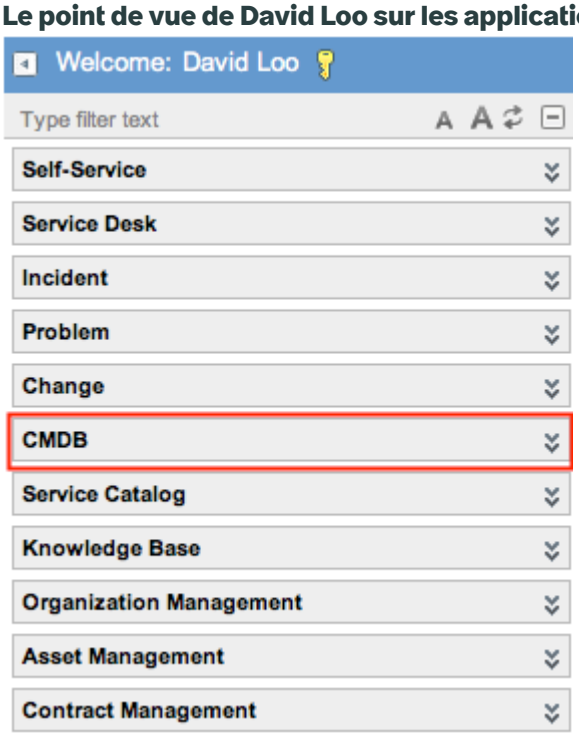
Cela crée une nouvelle entrée de module dans l'application plutôt que de remplacer le module existant dans le domaine global.

Vue spécifique au domaine de l'application Incident



Si un autre administrateur d'un autre domaine, comme Fred Luddy, se connecte et consulte l'application de configuration, les paramètres du domaine global s'affichent.

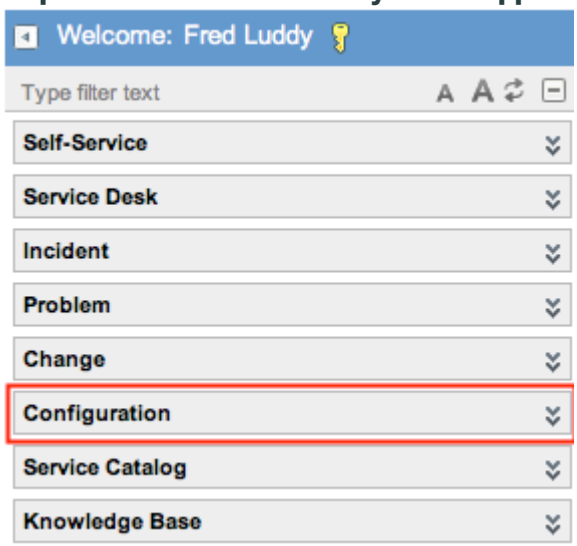
Le point de vue de David Loo sur les applications



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le point de vue de Fred Luddy sur les applications



Activer la connexion de domaine documentée et les messages de débogage

Le journal de domaine et les messages de débogage vous permettent de résoudre les erreurs de configuration de domaine.

Avant de commencer

Rôle requis : administrateur

Assurez-vous d'être l'instance la plus récente pour des performances optimales.

Procédure

1. Dans le centre Séparation en domaines, accédez à **Administrateur de domaine**.
2. Cliquez sur **Configurer le centre du domaine**.
3. Pour **Activer la journalisation de domaine détaillée**, cochez la case **Oui** .
4. Cliquez sur **Mettre à jour**.

Afficher un message de domaine en temps réel

Vous pouvez afficher les messages de domaine en temps réel à partir des journaux système.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Activer la connexion de domaine documentée : accédez à **Tout** > **Administrateur de domaine** > **Centre Séparation en domaines** > **Configurer le centre du domaine** > **Active la journalisation des détails du domaine** > **Oui** (ou définissez la propriété glide.sys.domain.verbose sur **Vrai**).
2. Accédez à la **Diagnostics du système** > **Débogage de session** > **Autoriser tout**.
   Étant donné qu'il s'agit d'une révision en temps réel, il n'est pas nécessaire de laisser la session de débogage s'exécuter avant de vérifier les fichiers journaux.
3. Accédez à la console de débogage de session pour afficher les journaux détaillés du domaine système.
4. Recherchez la requête de texte par rapport à la table.

   Cette requête recherche les messages du journal au format suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
08:36:43.974: [Domain Paths] Query against table incident restricted by domain values
 [Database Atlanta[db53580b0a0a0a6501aa37c294a2ba6b],
Database[287ee6fea9fe198100ada7950d0b1b73],
Database San Diego[db53a9290a0a0a650091abebccf833c6], global, NY
 DB[5f74727dc0a8010e01efe33a251993f9]]
```

Dans cet exemple, l'utilisateur qui consulte la table Incident a vu uniquement les enregistrements qui correspondaient aux domaines de base de données Base de données Atlanta, Base de données, Base de données San Diego, global et NY.

Afficher un message de domaine historique

Affichez l'historique des messages de domaine dans le fichier journal pour résoudre les problèmes de Séparation de domaine.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Activer la connexion de domaine documentée : accédez à **Tout** > **Administrateur de domaine** > **Centre Séparation en domaines** > **Configurer le centre du domaine** > **Active la journalisation des détails du domaine** > **Oui** (ou définissez la propriété glide.sys.domain.verbose sur **Vrai**).
2. Accédez à la **Diagnostics du système** > **Débogage de session** > **Autoriser tout**.
3. Laissez la session de débogage s'exécuter pendant un certain temps, par exemple un jour, avant de vérifier les fichiers journaux.
4. Accédez à la **Journaux Système** > **Utilités** > **Téléchargement du fichier journal de nœud**.
5. Ouvrez l'enregistrement du jour que vous souhaitez afficher.
   Les fichiers journaux utilisent le format de nommage localhost_log.<aa-mm-jj>.txt.
6. Cliquez sur le lien connexe **du journal de téléchargement** .
7. Ouvrez le fichier journal téléchargé dans un éditeur de texte et recherchez les messages journaux au format suivant :

   Requête par rapport à la table Incident restreint par valeurs de domaine [global, Logiciel[8a4dde73c6112278017a6a4baf547aa7]]

   Dans cet exemple, un utilisateur a uniquement vu les enregistrements de la table Incident qui correspondaient aux domaines global et logiciel.

Résoudre les erreurs de Domain Separation

Si vous rencontrez des problèmes de séparation de domaine, consultez cette liste de solutions.

Erreur ou symptôme	Solution
Un sys_id de domaine pointe vers un domaine inexistant	Cette erreur se produit lorsqu'un enregistrement de données, tel qu'un enregistrement d'utilisateur ou de tâche, a une valeur de colonne sys_domain dont le sys_id n'existe pas dans la table de domaine actuelle. Il est possible que le sys_id de domaine ait été supprimé accidentellement ou qu'il fasse référence à une table de domaines précédente si vous avez modifié la table de domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreur ou symptôme	Solution
	Pour corriger l'erreur, ouvrez une liste pour la table contenant l'erreur, filtrez sur la valeur de sys_domain non valide. Ensuite, entrez manuellement la valeur de sys_domain correcte ou supprimez-la. **Remarque :** Vous pouvez avoir des sys_ids de domaine non valides dans n'importe quelle table qui fait référence à la table de domaine. Par exemple, des ID de domaine non valides peuvent se produire dans les tables Domaine de visibilité utilisateur [sys_user_visibility], Domaine de visibilité de groupe [sys_user_group_visibility] et Domaine contenu [domain_contains].
Un chemin de domaine ou un numéro de domaine sys_id pointe vers le mauvais domaine	Cette erreur se produit lorsqu'une requête de numéro de domaine ou de chemin de domaine n'est pas synchronisée avec le nom de domaine réel. Cette erreur peut se produire avec des numéros de domaine lorsque l'ajout de domaines nécessite une renumérotation ou lors de la conversion des numéros de domaine en chemins de domaine. Pour corriger l'erreur, vérifiez les résultats dans le Centre Séparation en domainesfichier . Si l'erreur persiste, vous pouvez modifier manuellement la valeur des colonnes sys_domain_path ou sys_domain_number pour pointer vers le domaine approprié.
L'arborescence du domaine est corrompue	Cette erreur se produit s'il existe une série de relations de domaine qui créent une boucle infinie entre les domaines. Pour corriger l'erreur, ouvrez une liste pour la table Domaine et modifiez manuellement les valeurs contenues dans le domaine pour éviter de former une boucle.

Centre Séparation en domaines

Auditez régulièrement vos domaines pour révéler des problèmes.

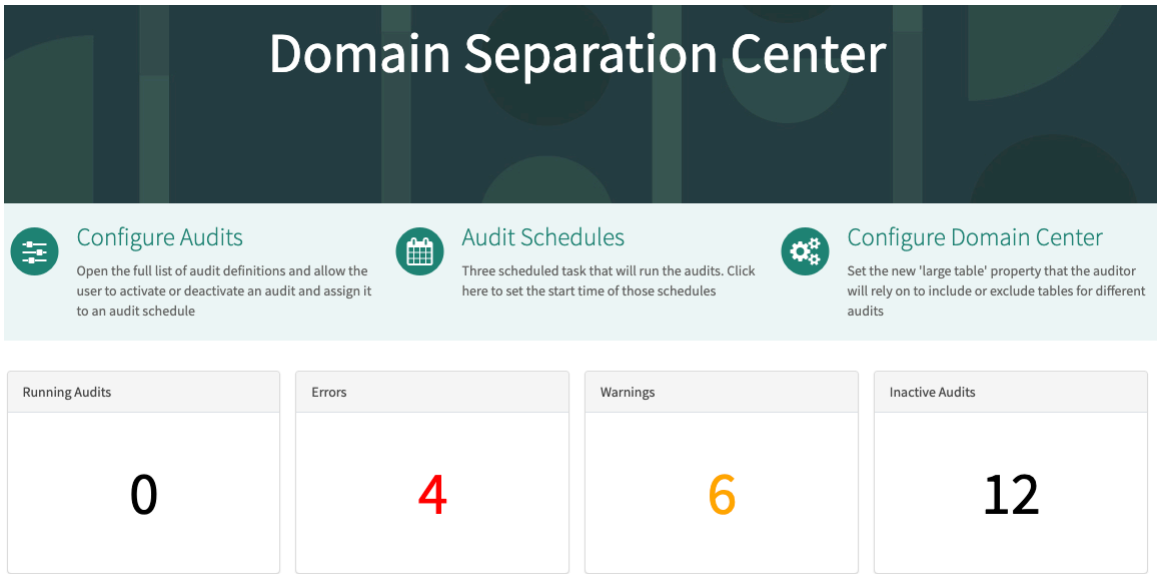
Vue d'ensemble

Le centre Séparation en domaines est un tableau de bord dans lequel vous pouvez planifier et configurer des audits pour tous les domaines stockés dans votre table domain_audit_definition. Le tableau de bord vous permet d'examiner les résultats d'audit et d'analyser plus en détail les erreurs et avertissements liés au domaine. Vous pouvez trouver le tableau de bord du centre Séparation en domaines à l'adresse <ServiceNow-instance-name>/domaincenter.

Le centre Séparation en domaines fournit de nombreux audits. Vous ne pouvez pas créer le vôtre. Vous pouvez toutefois configurer la fréquence à laquelle ils s'exécutent. Les audits s'exécutent sur tous les domaines stockés dans la table domain_audit_definition.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configurer des audits

Vous pouvez configurer si un audit est actif et à quelle fréquence il s'exécute.

1. Dans le centre Séparation en domaines, sélectionnez **Configurer les audits**.

   La page **Configurer les audits** s'affiche.

2. Configurez chaque audit que vous souhaitez rendre actif. Les audits sont désactivés par défaut.
   a. Sélectionnez un audit.
   b. Cochez la case **Actif** pour activer l'audit.
   c. Spécifiez la fréquence d'exécution de l'audit dans le champ **Fréquence** .

      Le centre Séparation en domaines exécute tous les audits marqués à la même fréquence et en même temps. Ne sélectionnez pas **Quotidien** pour les audits exécutés sur de grandes tables.

   d. Répétez ces étapes pour chaque audit que vous souhaitez activer.
3. Sélectionnez **Enregistrer**.

Calendriers d'audits

Configurez un ou plusieurs audits à exécuter quotidiennement, hebdomadairement ou mensuellement. Le planificateur spécifie les jours et les heures d'exécution de ces audits. Tous les audits avec la même fréquence de planification s'exécutent séquentiellement, en commençant par l'heure que vous configurez.

1. Dans le centre Séparation en domaines, sélectionnez **Calendriers d'audit**.

   La page **Calendrier d'audit** s'affiche.

2. Configurez les calendriers d'audit.
   a. Sélectionnez un nom de calendrier.
   b. Spécifiez l'heure de la journée à laquelle effectuer l'audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les unités de temps sont mesurées avec l'horloge de 24 heures, c'est-à-dire que 14 est égal à 14 heures.

c. Pour les calendriers hebdomadaires, sélectionnez le jour de la semaine pour exécuter l'audit, où 1 est le dimanche.

d. Pour les planifications mensuelles, sélectionnez le jour du mois pour exécuter l'audit.

e. Répétez la procédure pour les autres horaires.

3. Sélectionnez **Enregistrer** pour enregistrer les changements de configuration.
4. Sélectionnez **Exécuter maintenant** pour exécuter tous les audits planifiés à la fréquence indiquée en haut du volet droit, par exemple, si le titre du volet est **Calendrier d'audit de domaine : quotidien**, tous les audits qui s'exécutent quotidiennement sont exécutés.

Pour afficher l'état d'un audit en cours d'exécution, dans le centre Séparation en domaines, sélectionnez le numéro dans la zone **Audits en cours** .

Exécuter les audits immédiatement

En règle générale, les audits s'exécutent comme prévu. Vous pouvez toutefois exécuter tous les audits sur commande.

1. Dans le centre Séparation en domaines, sélectionnez **Calendriers d'audit**.

   La page **Calendrier d'audit** s'affiche.

2. Sélectionnez le nom du calendrier d'audit que vous souhaitez exécuter ; par exemple Quotidien, Hebdomadaire ou Mensuel.
3. Sélectionnez **Exécuter maintenant**.

Pour afficher l'état d'un audit en cours d'exécution, dans le centre Séparation en domaines, sélectionnez le numéro dans la zone **Audits en cours** .

Configurer le centre Séparation en domaines

1. Dans le centre Séparation en domaines, sélectionnez **Configurer le centre du domaine**.
2. Sur la page **Configurer le centre de domaine** , pour **Active la journalisation de domaine détaillée**, sélectionnez **Oui** pour stocker des journaux détaillés qui aident à diagnostiquer les problèmes liés au domaine. Une journalisation détaillée peut entraîner des problèmes de performances.

   Ces journaux font référence aux journaux côté serveur de la table syslog_domain. Pour plus d'informations sur l'affichage des journaux, consultez Afficher les audits avec des avertissements et des défaillances.

3. Dans la zone de liste double, sélectionnez et déplacez tous vos grands tableaux dans la colonne **Sélectionné** .

   Les audits quotidiens ne doivent pas s'exécuter sur de grandes tables. Les noms de table grisés dans la colonne **Sélectionné** sont volumineux et ne peuvent pas être déplacés vers la colonne **Disponible** .

4. Sélectionnez **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les audits avec des avertissements et des défaillances

Sur le tableau de bord, les **erreurs** et **avertissements fournissent des** informations détaillées sur les audits qui ont rencontré des problèmes. Les journaux associés à Séparation de domaine résident sur votre serveur dans la table syslog_domain.

1. Dans le centre Séparation en domaines, sélectionnez le nombre dans la zone **Erreurs** ou **avertissements** .

   La page **Erreurs** ou **Avertissements** s'affiche respectivement.

2. Sélectionnez l'un des audits de la liste.

   La page affiche des informations détaillées sur les problèmes liés à l'audit que vous avez sélectionné. Les messages dans **Détails du résultat d'audit** font référence aux valeurs de la table syslog_domain pour les audits de table qui ont révélé des erreurs ou des avertissements.

3. Pour afficher les journaux sur le serveur qui fournissent des informations sur les audits d'avertissement ou d'erreur :
   a. Copiez la valeur **d'ID de détail** dans le panneau de gauche d'un avertissement ou d'une erreur.
   b. Dans le navigateur de filtre de HI, saisissez *`syslog_domain.do`*.

      La page Journal de domaine s'affiche.

   c. Dans le champ de recherche **Source** , entrez `=<Detail-ID >` (pas d'espace après le signe égal), par exemple, =f6a00fd29a85b300a9503a81b9169678.

      La page Journal de domaine affiche uniquement les journaux associés à l'audit avec l'ID de détail que vous avez spécifié. Chaque ligne de la table spécifie un enregistrement différent dans lequel l'audit a trouvé des problèmes. Notez que le champ **Message** de cette page correspond aux valeurs affichées dans la colonne **Message** du Centre de services de domaine. Le format du message correspond au type d'audit.

4. Sélectionnez :
   - **Réexécuter l'audit : réexécutez** un audit pour voir s'il rencontre toujours un avertissement ou une erreur.
   - **Désactiver l'audit** : désactive un audit.
   - **Copier les détails** : permet de copier les détails de l'audit dans le presse-papiers.

Afficher les audits en cours et en attente

Les audits actifs s'exécutent périodiquement ou sont mis en file d'attente pour s'exécuter, comme prévu. Vous pouvez afficher leur état au fur et à mesure qu'ils s'exécutent.

1. Sélectionnez le nombre dans la zone **Audits en cours** pour afficher les audits en cours d'exécution ou en attente d'exécution.

   La page **Audits en cours d'exécution** s'affiche.

2. Sélectionnez un audit pour plus d'informations à son sujet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les audits inactifs

1. Sélectionnez le nombre dans la zone **Audits inactifs** .

   La page **Audits inactifs** affiche tous les audits actuellement désactivés.

2. Sélectionnez l'un des audits pour afficher plus d'informations à son sujet.
3. Pour activer un audit, cochez la case **Actif** et utilisez le champ **Fréquence** pour spécifier la fréquence d'exécution de l'audit.
4. Sélectionnez **Mettre à jour**.

Configurer le centre Séparation en domaines

Spécifiez quelles tables des domaines sont volumineuses et si vous souhaitez une journalisation détaillée.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Vous pouvez planifier des audits à exécuter sur une base quotidienne, hebdomadaire ou mensuelle. Les audits exécutés sur de grandes tables peuvent prendre beaucoup de temps. Pour cette raison, évitez d'exécuter des audits quotidiennement sur de grandes tables. Le lancement d'un nouvel audit sur un audit dont l'exécution prend plus d'une journée peut avoir des conséquences négatives.

Une journalisation détaillée peut fournir de meilleures informations sur les problèmes détectés lors des audits, mais peut entraîner des problèmes de performance.

Procédure

1. Dans le centre Séparation en domaines, sélectionnez **Configurer le centre du domaine**.
   La page Configurer le centre du domaine s'affiche.
2. Sélectionner **Oui** pour **Active la journalisation détaillée du domaine**, afin de stocker des journaux détaillés qui aident à diagnostiquer les problèmes liés au domaine.
   Ces journaux font référence aux journaux côté serveur dans la table Journal de domaine [syslog_domain]. Pour plus d'informations sur l'affichage des journaux, consultez la section Afficher les audits avec des avertissements et des défaillances.
3. Dans la liste, déplacez toutes vos grandes tables dans la colonne **Sélectionné** .
   Les audits quotidiens ne doivent pas s'exécuter sur de grandes tables. Les noms de table grisés dans la colonne **Sélectionné** sont volumineux et ne peuvent pas être déplacés vers la colonne **Disponible** .
4. Sélectionnez **Mettre à jour**.
5. Si vous avez des tables volumineuses qui ne doivent jamais faire l'objet d'un audit, définissez la `com.glide.domain.audit.big_tables.additional` propriété système sur une liste de ces noms de tables séparés par des virgules.

Configurer des audits

Configurez si un audit est actif et à quelle fréquence il s'exécute.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur **Configurer les audits**.
   T s'affiche.
2. Sur la page Configurer les audits, configurez chaque audit que vous souhaitez rendre actif.
   Les audits sont désactivés par défaut.
   a. Cliquez sur un audit.
   b. Cochez la case **Actif** pour activer l'audit.
   c. Spécifiez la fréquence d'exécution de l'audit dans le champ **Fréquence** .
      Le centre Séparation en domaines exécute tous les audits marqués à la même fréquence et en même temps.
      Ne sélectionnez pas **Quotidien** pour les audits exécutés sur de grandes tables.
   d. Répétez les étapes a à c pour chaque audit que vous souhaitez activer.
3. Cliquez sur **Enregistrer**.

Planifier les audits

Spécifiez l'heure et le jour d'exécution des audits.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Vous avez configuré un ou plusieurs audits à exécuter quotidiennement, hebdomadairement ou mensuellement. Le planificateur spécifie les jours et les heures d'exécution de ces audits. Tous les audits avec la même fréquence de planification s'exécutent séquentiellement à partir de l'heure que vous configurez.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur **Calendriers d'audit**.
   La page Calendrier d'audit s'affiche.
2. Configurez les calendriers d'audit.
   a. Cliquez sur le nom d'un calendrier.
   b. Spécifiez l'heure de la journée à laquelle effectuer l'audit.
      Les unités de temps utilisent l'horloge de 24 heures (c'est-à-dire que 14 est égal à 14 heures).
   c. Pour les calendriers hebdomadaires, sélectionnez le jour de la semaine pour exécuter l'audit, où 1 est le dimanche.
   d. Pour les planifications mensuelles, sélectionnez le jour du mois pour exécuter l'audit.
   e. Répétez la procédure pour les autres horaires.
3. Cliquez sur **Enregistrer** pour enregistrer les changements de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. **Facultatif :** Cliquez sur **Exécuter maintenant** pour exécuter tous les audits planifiés à la fréquence indiquée en haut du volet droit.
   Par exemple, si le titre du volet est **Calendrier d'audit de domaine : quotidien**, **exécuter maintenant** exécute immédiatement tous les audits planifiés pour s'exécuter quotidiennement.

Que faire ensuite
Pour afficher l'état d'un audit en cours d'exécution, dans le Centre Séparation en domaines, cliquez sur le numéro dans la zone **Audits en cours** .

Exécuter les audits immédiatement

En règle générale, les audits s'exécutent comme prévu. Vous pouvez toutefois exécuter tous les audits sur commande.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Vous ne pouvez pas exécuter manuellement des audits individuels. Vous pouvez toutefois exécuter tous les audits configurés avec la même fréquence de planification. Par exemple, vous pouvez exécuter tous les audits qui sont configurés pour s'exécuter quotidiennement.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur **Calendriers d'audit**.
2. Cliquez sur le nom du calendrier d'audit que vous souhaitez exécuter (par exemple, Quotidien, Hebdomadaire ou Mensuel).
3. Cliquez sur **Exécuter maintenant**.

Que faire ensuite
Pour afficher l'état d'un audit en cours d'exécution, dans le Centre Séparation en domaines, cliquez sur le numéro dans la zone **Audits en cours** .

Afficher les audits avec des avertissements et des erreurs

Le centre Séparation en domaines fournit des détails sur les erreurs et avertissements d'audit.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Sur le tableau de bord du centre Séparation en domaines, les **erreurs** et **avertissements fournissent des** informations détaillées sur les audits qui ont rencontré des problèmes. Les journaux associés à Séparation de domaine résident sur votre serveur dans la table syslog_domain. Les erreurs sont des problèmes qui nécessitent une attention immédiate. Les avertissements n'entraînent pas d'échecs mais présentent les meilleures pratiques, par exemple, ne pas rendre le nom de domaine trop long.

Procédure

1. Dans le centre Séparation en domaines, cliquez sur le numéro dans la zone **Erreurs** ou **avertissements** .
   La page **Erreurs** ou **avertissements** s'affiche.
2. Cliquez sur l'un des audits de la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La page affiche des informations détaillées sur les problèmes liés à l'audit que vous avez sélectionné. Les messages dans **Détails du résultat d'audit** font référence aux valeurs de la table syslog_domain sur le serveur pour les audits de table qui ont révélé des erreurs ou des avertissements.

3. Pour afficher les journaux sur le serveur qui fournissent des informations sur les audits d'avertissement ou d'erreur :

   a. Copiez la valeur **d'ID de détail** dans le panneau de gauche d'un avertissement ou d'une erreur.

   b. Sur l'instance exécutant le centre Séparation en domaines, saisissez *`syslog_domain.list`* dans le **navigateur de filtre**.
   La page Journal de domaine s'affiche.

   c. Dans le champ de recherche de la colonne **Source** , saisissez `=<Detail-ID >` (pas d'espace après le signe égal), par exemple, `=f6a00fd29a85b300a9503a81b9169678`.
   La page Journal de domaine affiche uniquement les journaux associés à l'audit avec l'ID de détail que vous avez spécifié. Chaque ligne de la table spécifie un enregistrement différent dans lequel l'audit a trouvé des problèmes. Notez que le champ **Message** de cette page correspond aux valeurs affichées dans la colonne **Message** du Centre de services du domaine. Les informations contenues dans le message correspondent au type d'audit.

4. **Facultatif :** Sélectionnez l'une des options suivantes :
   - **Réexécuter l'audit** : réexécutez un audit pour voir s'il rencontre toujours un avertissement ou une erreur.
   - **Désactiver l'audit** : permet de désactiver un audit.
   - **Copier les détails** : permet de copier les détails de l'audit dans le presse-papiers.

Afficher les résultats en cours et en attente

Vous pouvez afficher les audits en cours et en attente pour voir leur état.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Les audits actifs s'exécutent périodiquement ou sont mis en file d'attente pour s'exécuter, comme prévu. Vous pouvez afficher leur état au fur et à mesure qu'ils s'exécutent.

Procédure

1. Cliquez sur le nombre indiqué dans la zone **Audits en cours d'exécution** pour afficher les audits en cours d'exécution ou en attente d'exécution.
   La page Audits en cours d'exécution s'affiche.
2. Cliquez sur un audit en cours ou en attente pour afficher des informations à son sujet.

Afficher les audits inactifs

Vous pouvez afficher tous les audits inactifs au même endroit et les activer éventuellement.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

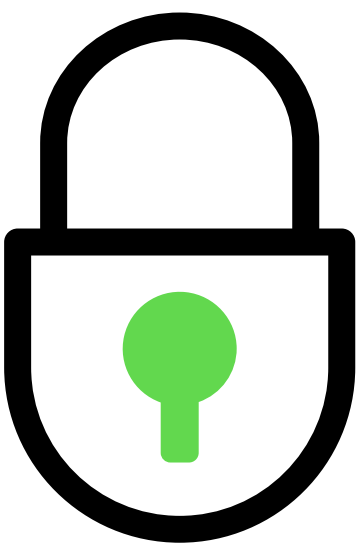
Procédure

1. Cliquez sur le nombre indiqué dans la zone **Audits inactifs** .
   La page Audits inactifs affiche tous les audits actuellement désactivés.
2. Cliquez sur l'un des audits pour afficher plus d'informations à son sujet.
3. **Facultatif :** Activez un audit en cochant la case **Actif** et en spécifiant la fréquence d'exécution de l'audit dans le champ **Fréquence** .
4. Cliquez sur **Mettre à jour**.

Authentification

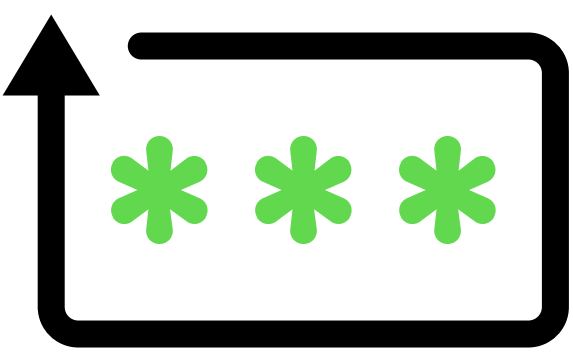
ServiceNow®L'authentification de valide l'identité d'un utilisateur qui accède à une instance, puis autorise l'utilisateur à accéder aux fonctionnalités qui correspondent au rôle ou à la fonction de l'utilisateur.

Premiers pas



Authentification unique (SSO) de plusieurs fournisseurs

Nom d'utilisateur et mot de passe configurés dans les fournisseurs d'identité, qui ont un compte d'utilisateur correspondant dans la base de données.

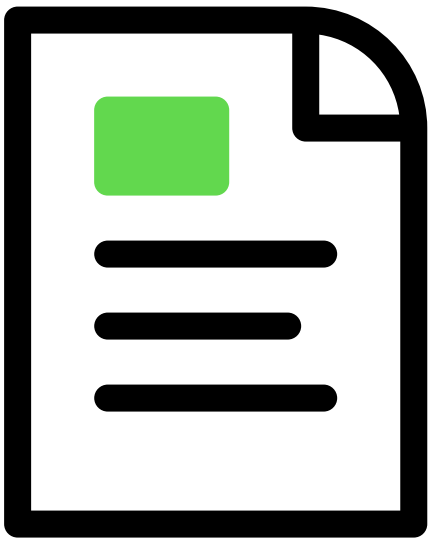


OAuth entrant et sortant

L'authentification basée sur OAuth valide l'identité du client qui tente d'établir une confiance dans le système à l'aide d'un protocole d'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



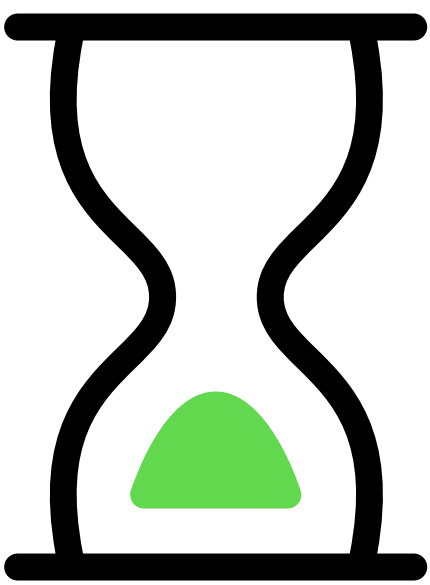
Politique d'accès API

La politique d’accès d’API définit les autorisations et l’accès à une API qui peuvent être contrôlés par le biais d’une politique.



Authentification du jeton Digest

Le nom d’utilisateur et le secret dans la table exécutent une opération de hachage spécifique à l’utilisateur, par exemple SHA1, SHA 256 ou MD5. Cette valeur doit être ajoutée dans le cadre du suffixe d’URL, qui fonctionne sur le paramètre de requête.



Authentification temporelle limitée

Configurer l’authentification basée sur les liens sur le

ServiceNow

ServiceNow. Le lien configuré peut être partagé avec l’utilisateur par e-mail ou SMS. L’utilisateur peut utiliser ces liens pour se connecter à l’instance.



Authentification multifacteur (MFA)

La MFA vous permet de fournir un deuxième niveau d’authentification qui inclut l’utilisation d’un code secret provenant d’une application d’authentification, d’une clé matérielle, d’un authentificateur biométrique, d’un SMS ou d’un e-mail.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



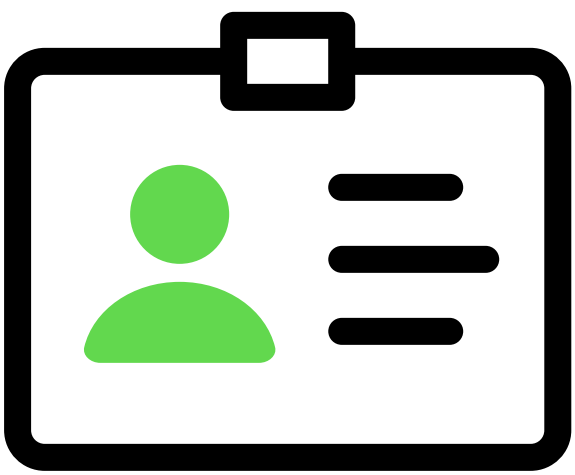
Authentification basée sur certificat

Certificats codés PEM uniques mappés aux utilisateurs au lieu du nom d'utilisateur et du mot de passe pour l'authentification basée sur certificat.



Auto-inscription

Utilisez l'auto-inscription des utilisateurs externes pour intégrer un grand volume d'utilisateurs externes à votre instance.



LDAP

Intégration à un répertoire LDAP (Directory Access Protocol) léger pour rationaliser le processus de connexion de l'utilisateur

Vous pouvez utiliser plusieurs méthodes différentes pour authentifier les utilisateurs. Les informations d'identification de l'utilisateur sont mises en correspondance avec différentes informations d'identification enregistrées pour chaque méthode.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le Okta module d'extension SSO est obsolète.
- Pour en savoir plus sur les propriétés de sécurité qui affectent le traitement des autorisations, consultez Contrôle d'accès dans les paramètres de renforcement de la sécurité de l'instance.
- Vous pouvez utiliser l'authentification SAML et Digest via l'application SSO de plusieurs fournisseurs.

Authentification adaptative

Utilisez le cadre de travail de la politique d'authentification adaptative pour appliquer des contrôles d'authentification contextuelle aux bons utilisateurs au bon moment. L'authentification adaptative utilise des politiques d'authentification pour évaluer les demandes d'authentification, puis pour refuser ou autoriser l'accès à votre instance en fonction des conditions de politique spécifiées.

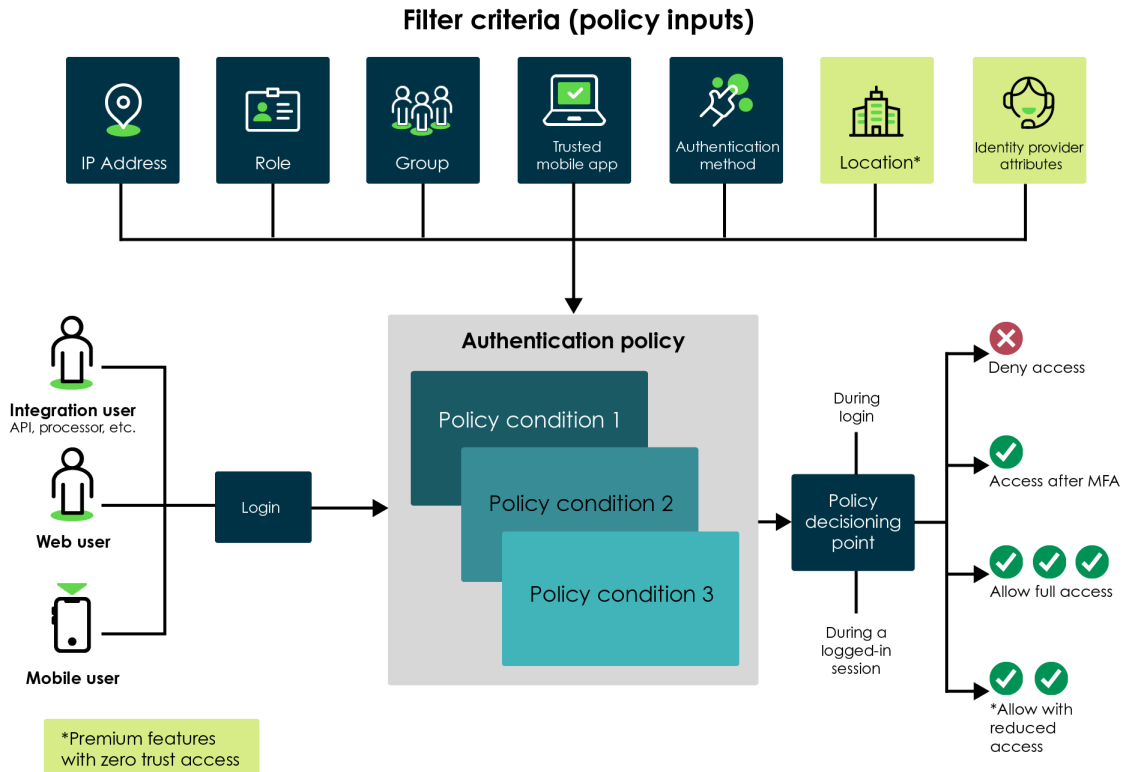
Utilisez des politiques et des contextes d'authentification adaptative pour restreindre l'accès des utilisateurs et des API à votre instance en fonction de critères tels que l'adresse IP, le rôle de l'utilisateur et le groupe d'utilisateurs. Vous pouvez configurer les politiques d'authentification intégrées en fonction de vos exigences de sécurité.

Par exemple, un administrateur peut configurer le pour autoriser les `Allow Access Policy` connexions uniquement par des utilisateurs dans une plage approuvée d'adresses IP et qui sont membres d'un rôle spécifique. Lorsqu'elle `Post-authentication context`est affectée au , la politique d'accès refuse l'accès à partir d'adresses IP non approuvées.

Pour définir un message personnalisé dans la langue de votre instance, vous devez ajouter la paire clé/valeur dans sys_ui_message.list et mettre à jour l'enregistrement sys_ui_message . Lorsque vous vous connectez avec un mot de passe incorrect, le message personnalisé dans la langue préférée s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Composants d'authentification adaptative

Politiques d'authentification

Les politiques d'authentification évaluent les demandes d'authentification en fonction des conditions de politique spécifiées et autorisent ou refusent l'accès en fonction du résultat de l'évaluation des conditions de politique. Par exemple, l'accès n'est autorisé que si toutes les conditions de politique spécifiées dans la **politique d'accès** sont définies sur vrai.

Les politiques d'authentification utilisent les informations fournies par les critères de filtre pour les comparer aux conditions de la politique afin de déterminer s'il convient d'accorder l'accès à l'instance. Par exemple, un critère de filtre fournit l'adresse IP d'un utilisateur et une condition de politique détermine si cette adresse se trouve dans la plage spécifique avant d'accorder l'accès. Pour en savoir plus sur les politiques d'authentification, consultez Politiques d'authentification.

Contextes de politique d'authentification

Les contextes des politiques d'authentification définissent comment et quand les politiques sont appliquées pendant le processus de connexion. Le contexte de pré-authentification s'exécute avant que l'écran de connexion ne s'affiche pour l'utilisateur. Le contexte de post-authentification s'exécute une fois que l'utilisateur a entré ses informations d'identification. Pour utiliser une politique, celle-ci doit être affectée à un contexte de politique. Pour plus de détails sur ces contextes, reportez-vous à la section Contextes de politique d'authentification.

Critère de filtre

Les critères de filtre (également appelés entrées de politique) sont utilisés comme entrées pour les conditions de politique. Les conditions de politique utilisent ces entrées pour vérifier et répondre aux exigences des demandes d'authentification. Ces entrées fournissent des informations telles

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que le rôle de l’utilisateur, la plage IP et le fournisseur d’identité. Pour en savoir plus sur les critères de filtrage, reportez-vous à la section Critère de filtre.

Propriétés d’authentification

Utilisez les propriétés d’authentification pour contrôler si l’authentification adaptative est active sur votre instance. Vous pouvez également utiliser des propriétés pour activer le débogage et définir la messagerie que les utilisateurs voient lorsque l’accès est bloqué. Pour en savoir plus sur ces propriétés, reportez-vous à la section Configurer les propriétés d’Authentification adaptative.

Politiques d’accès REST API

Vous pouvez utiliser les critères de filtre de l’infrastructure d’authentification adaptative pour restreindre l’accès aux API REST entrantes ServiceNow . Pour plus d'informations, consultez Politiques d’accès REST API.

Séparation de domaine et Authentification adaptative

L’authentification adaptative est prise en charge sur les instances séparées par domaine au niveau de la condition de politique d’authentification. Les conditions de politique affectent le domaine dans le champ **Domaine** des enregistrements [sys_domain]. Les conditions de politique dans le domaine global affectent tous les domaines.

Événements d'authentification adaptative

Vous pouvez utiliser la table des événements d’authentification adaptative pour connaître les événements qui se sont produits spécifiquement pour la fonctionnalité d’authentification adaptative. Pour plus d'informations, consultez Événements d'authentification adaptative.

Activer Authentification adaptative

Vous pouvez activer le module d’extension Authentification adaptative (com.snc.adaptive_authentication) pour Authentification adaptative si vous disposez du rôle administrateur.

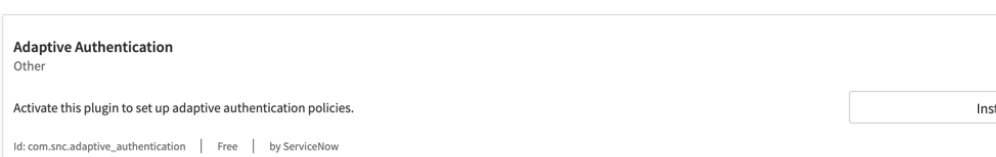
Avant de commencer

Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module **d’extension Authentification adaptative** (com.snc.adaptive_authentication).



Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Que faire ensuite
Configurez vos politiques d'authentification pour appliquer des contrôles d'authentification contextuelle sur votre instance.

Une fois vos stratégies configurées. Activez l'authentification adaptative à l'aide de la politique **Activer la politique d'authentification** . Pour en savoir plus sur les propriétés d'Authentification adaptative, reportez-vous à la section Configurer les propriétés d'Authentification adaptative.

Critère de filtre

Les critères de filtre (également appelés entrées de politique) sont utilisés comme entrées pour les conditions de politique afin de vérifier et de répondre aux exigences d'une demande d'authentification.

Utilisez des critères de filtre pour fournir des politiques d'authentification des informations telles que l'adresse IP, les rôles ou les groupes d'un utilisateur. Ajoutez ces critères dans la section Conditions de la **politique** de vos polices.

Sept types de critères de filtre sont utilisés dans l'authentification adaptative. Vos politiques d'authentification peuvent utiliser un ou plusieurs de ces critères pour évaluer les demandes d'authentification.

Types de critères de filtre

Type	Description
Critère de filtre d'adresses IP	Utilisez les critères de filtre d'adresses IP pour filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. Les formats IPv4 et IPv6 sont pris en charge.
Critère de filtre de rôle	Utilisez des critères de filtre de rôle pour filtrer les utilisateurs en fonction de leurs rôles.
Critères de filtre de groupe	Utilisez les critères de filtre de groupe pour filtrer les utilisateurs en fonction du groupe d'utilisateurs auquel l'utilisateur appartient.
Critère de filtrage de la localisation	Utilisez les critères de filtrage d'emplacement pour filtrer les utilisateurs en fonction de l'emplacement de l'utilisateur.
Critères de filtre d'attributs du fournisseur d'identité	Utilisez les attributs de fournisseur d'identité reçus de la réponse SAML de l'IdP comme critères de filtrage pour l'authentification.

Critères génériques

Outre les types répertoriés précédemment, il existe quatre critères de filtre génériques. Ces critères n'apparaissent pas dans votre navigateur de filtre, mais vous pouvez les sélectionner tout en ajoutant des entrées de politique à vos politiques d'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de critères de filtre génériques

Type	Description
Schéma d'authentification	Utilisez cette fonction pour filtrer en fonction du schéma d'authentification de l'utilisateur. Ce critère est un type de choix avec deux options : • Nom d'utilisateur et mot de passe, qui désignent une connexion locale • SSO, qui désigne une connexion basée sur plusieurs SSO (SAML, OIDC ou Digest). **Remarque :** Ce critère de filtre n'est disponible que lorsque le module d'extension **Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs** [com.snc.integration.sso.multi.installer] est installé.
Fournisseur d'identité	Utilisez cette propriété pour filtrer en fonction du fournisseur d'identité de l'utilisateur. Utilisez en même temps que les critères du schéma d'authentification pour avoir un contrôle granulaire sur le processus de connexion. Ce critère est une référence à la table **Fournisseurs d'identité** [sso_properties]. **Remarque :** Ce critère de filtre n'est disponible que lorsque le module d'extension **Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs** [com.snc.integration.sso.multi.installer] est installé.
MFA basée sur les rôles	Utilisez cette propriété pour filtrer en fonction de la fonctionnalité MFA basée sur les rôles. Ce critère est un critère de filtre de type booléen qui indique si la MFA basée sur les rôles est activée pour l'utilisateur.
MFA basé sur l'utilisateur	Utilisez cette option pour filtrer en fonction de la fonctionnalité MFA basée sur l'utilisateur. Ce critère est un critère de filtre de type booléen qui indique si la MFA basée sur l'utilisateur est activée pour l'utilisateur.
Application mobile de confiance	Filtre d'application mobile approuvé permettant d'activer l'accès à l'instance à partir de l'application mobile.

Filtre d'adresses IP

Utilisez des critères de filtre IP pour filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. Les formats IPv4 et IPv6 sont pris en charge.

Les critères de filtre IP vous permettent de filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une adresse spécifique ou à une plage d'adresses.

Créer des critères de filtre IP

Les critères de filtre IP vous permettent de filtrer les utilisateurs en fonction des adresses IP de l'utilisateur. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une adresse spécifique ou à une plage d'adresses.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

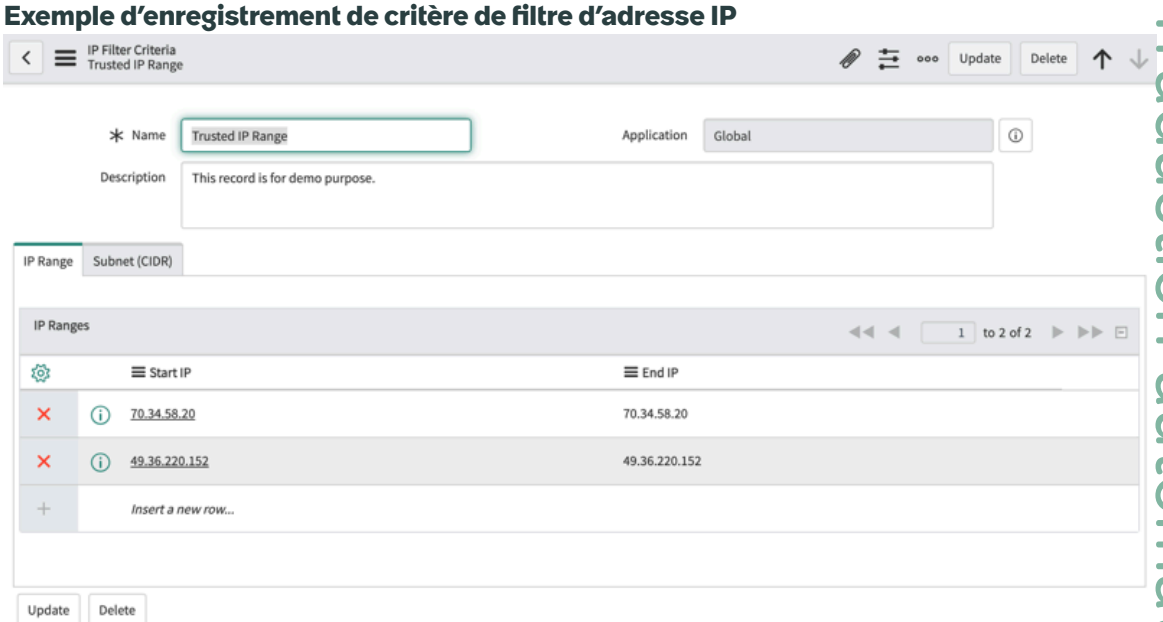
Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Critère de filtre** > **Critère de filtre d'adresses IP**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtre d'adresses IP

Champ	Description
Nom	Nom permettant d'identifier le réseau IP.
Description	Brève description du réseau IP.
Application	Périmètre de l'application.

Exemple d'enregistrement de critère de filtre d'adresse IP



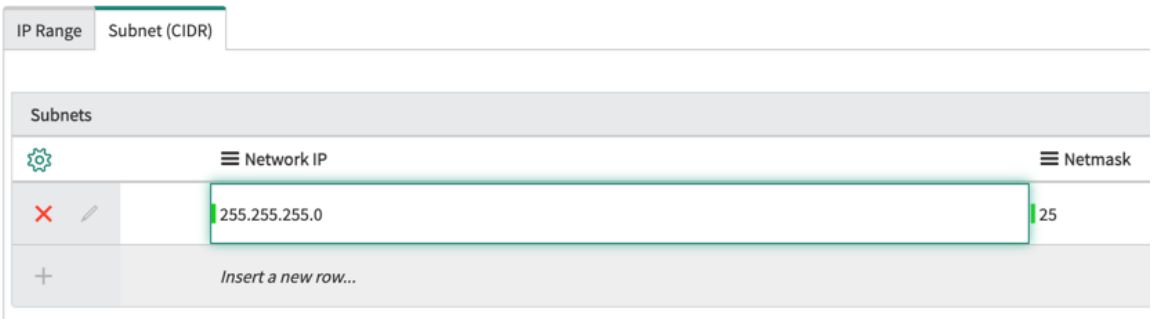
4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
5. Dans l'onglet **Plage IP** , double-cliquez sur **Insérer une nouvelle ligne**.
   Vous pouvez saisir une seule adresse IP ou plusieurs plages d'adresses IP. Par exemple, pour une plage d'adresses IP, entrez `192.0.2.0` dans la colonne **Adresse IP de début** et `192.0.2.255` dans la colonne **Adresse IP de fin** .

> **Remarque :**
> Pour une seule adresse IP, assurez-vous de saisir la même adresse IP dans les colonnes **Adresse IP de début** et **Adresse IP de fin** . Lorsque vous entrez une adresse IP dans la colonne **Adresse IP de début** , laissez la colonne **IP de fin** vide, puis enregistrez l'enregistrement. La colonne **Adresse IP de fin** est renseignée automatiquement avec la même adresse **IP de début** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans l'onglet **Sous-réseau (CIDR),** double-cliquez sur **Insérer une nouvelle ligne**. Entrez l'adresse IP réseau et le masque réseau au format CIDR (Classless Inter-Domain Routing). Par exemple, entrez 255.255.255.0 comme adresse IP réseau et 25 comme masque réseau.



Filtre de rôle

Utilisez des critères de filtre de rôle pour filtrer les utilisateurs en fonction de leurs rôles.

Les critères de filtre de rôle vous permettent de filtrer les utilisateurs en fonction des rôles. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une liste de rôles d'utilisateur.

Créer un critère de filtre de rôle

Les critères de filtre de rôle vous permettent de filtrer les utilisateurs en fonction des rôles. Vous pouvez configurer une politique d'authentification pour autoriser ou refuser l'accès à une liste de rôles d'utilisateur.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Critère de filtre** > **Critère de filtre de rôle**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

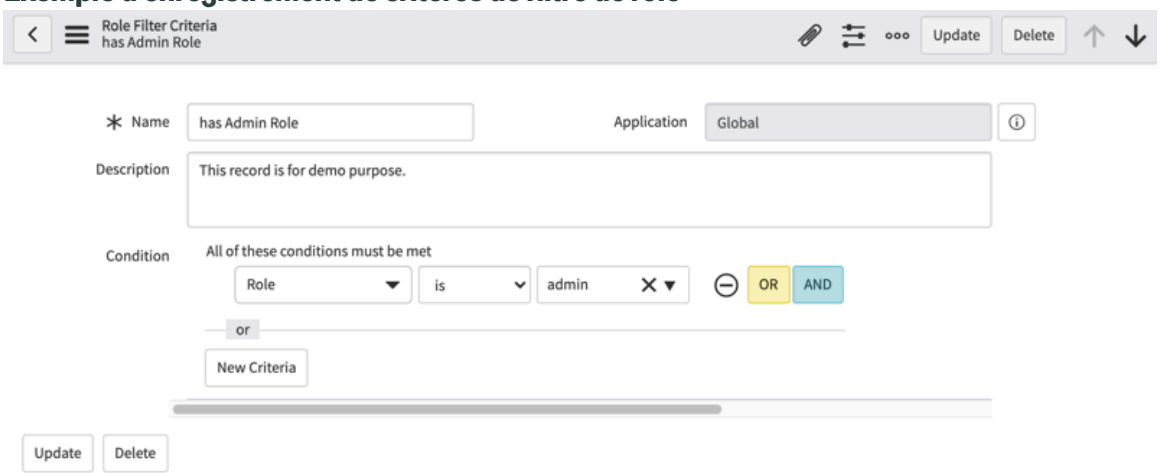
Formulaire Critères de filtre de rôle

Champ	Description
Nom	Nom permettant d'identifier le rôle.
Application	Périmètre de l'application.
Description	Brève description du rôle.

Traduction automatique

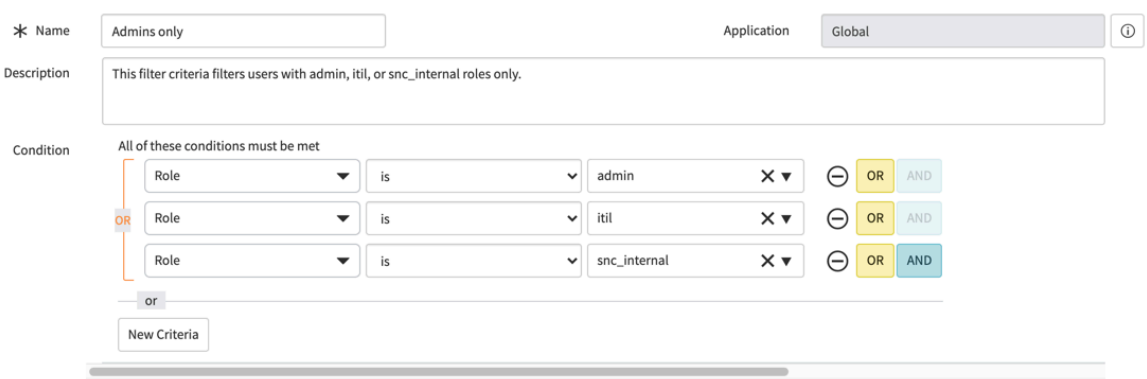
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'enregistrement de critères de filtre de rôle



4. Dans la **section Rôles pour les critères**, double-cliquez sur **Insérer une nouvelle ligne**.
5. Créez une condition pour un rôle spécifique à l'aide du Créateur de conditions.
   Par exemple, vous pouvez créer une condition qui autorise uniquement les utilisateurs ayant des rôles administrateur, itil ou snc_internal. Pour plus d'informations sur Générateur de conditions, consultez Créer une instruction de condition à l'aide du générateur de conditions .

   Remarque :
   Actuellement, la remontée pas à pas n'est pas prise en charge dans les critères de filtre de rôle.



Filtre de groupe

Utilisez les critères de filtre de groupe pour filtrer les utilisateurs en fonction du groupe d'utilisateurs auquel l'utilisateur appartient.

Les critères de filtre de groupe autorisent ou refusent l'accès des utilisateurs en fonction du groupe d'utilisateurs auquel ils appartiennent.

Créer un critère de filtre de groupe

Les critères de filtre de groupe autorisent ou refusent l'accès des utilisateurs en fonction du groupe d'utilisateurs auquel ils appartiennent.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

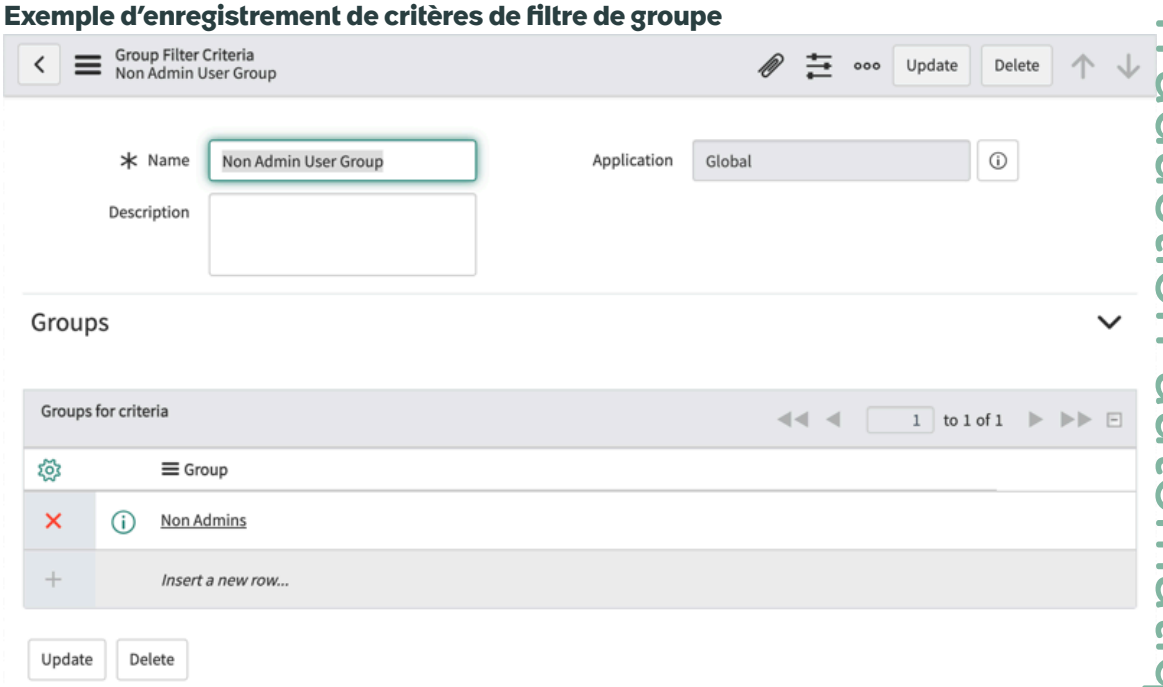
Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Critère de filtre** > **Critères de filtre de groupe**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Critères de filtre de groupe

Champ	Description
Nom	Nom identifiant le groupe.
Description	Brève description du groupe.
Application	Périmètre de l'application.

Exemple d'enregistrement de critères de filtre de groupe



4. Dans l'onglet **Groupe pour les critères** , double-cliquez sur **Insérer une nouvelle ligne**.
5. Cliquez sur , recherchez et sélectionnez un groupe d'utilisateurs.
6. Cliquez sur l'icône .

Filtre d'emplacement

Les critères de filtre d'emplacement peuvent être utilisés comme entrée de filtre pour les utilisateurs en fonction de l'emplacement de l'utilisateur.

Le filtre d'emplacement est un critère de filtre que les administrateurs peuvent utiliser lors de l'élaboration des politiques d'authentification en fonction de l'emplacement physique de l'appareil.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Les critères de filtre d'emplacement sont un module d'extension payant qui nécessite une licence.
- L'instance doit être sur ADCv2. Si l'instance n'est pas sur ADCv2, les informations d'emplacement de l'utilisateur ne sont pas disponibles.

Les critères de filtrage d'emplacement vous permettent d'effectuer les actions suivantes :

- Agir en tant qu'entrée de politique Agir pour les conditions de politique afin de vérifier et de satisfaire aux exigences d'authentification.
- Offrez la possibilité de créer des politiques d'authentification adaptatives en fonction du **pays**.
- Autorisez ou non l'accès d'instance à une zone géographique donnée.
- Utilisez la politique de pré-authentification ou de post-authentification basée sur l'emplacement géographique pour :
  - Empêcher l'accès en provenance de pays sanctionnés, en dehors d'une région étroitement contrôlée par la confidentialité, à la discrétion de l'entreprise.
  - Autorisez l'accès aux zones uniquement dans les limites de la zone de confidentialité applicable et à la discrétion de l'entreprise.
  - Configurer la liste d'autorisation basée sur le pays pour l'authentification.

Cas d'utilisation

Voici quelques-uns des cas d'utilisation des critères de filtrage d'emplacement pour l'authentification adaptative :

- Bloquez l'accès à l'instance à partir d'un pays.
- Autorisez l'accès à l'instance uniquement à partir d'un pays particulier.
- Appliquer l'authentification renforcée ou MFA pour se connecter en fonction du pays.
- Réduisez ou limitez les rôles de l'utilisateur en fonction du pays.
- Les critères de filtre d'emplacement peuvent être utilisés pour la MFA, l'accès zéro confiance (ZTA), le contexte de pré-authentification et le contexte de post-authentification.

Identification de l'emplacement

Les services de localisation permettant d'identifier l'emplacement de l'utilisateur sont fournis par un service tiers - MaxMind.

L'emplacement de l'utilisateur est identifié via le VPN, à partir de l'en-tête x-forwarded-for. S'il n'y a pas d'en-tête renseigné par le service, seule l'adresse IP VPN (emplacement) est affichée en tant qu'emplacement utilisateur.

Remarque :

Si des emplacements incorrects s'affichent après la configuration du filtre d'emplacement, consultez l'article de la base de connaissances pour résoudre les problèmes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer l’accès en fonction de l’emplacement

Activez **l’option Zéro confiance : accès basé sur l’emplacement** (com.snc.zero_trust_location_access) pour permettre aux administrateurs de configurer des politiques d’authentification adaptative en fonction de l’emplacement de l’utilisateur.

Avant de commencer
Rôle requis : administrateur

- Module d’extension dépendant : Adaptive Authentication
- Type de module d’extension : payant et nécessitant une licence.
- L’instance doit être sur ADCv2. Si l’instance n’est pas sur ADCv2, les informations d’emplacement de l’utilisateur ne sont pas disponibles.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d’extension**Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Créer un critère de filtre d’emplacement

Utilisez les critères de filtre d’emplacement pour filtrer l’entrée pour l’authentification des utilisateurs en fonction de l’emplacement de l’utilisateur.

Avant de commencer
Rôle requis : administrateur

Module d’extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Propriété : activez la propriété d’authentification adaptative.

Remarque :
Les administrateurs ne peuvent créer la politique basée sur les filtres d’emplacement que si l’emplacement est disponible pour la session utilisateur actuelle.

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Critère de filtre** > **Critère de filtrage d'emplacement**.
2. Sélectionnez **Nouveau**.

Traduction automatique

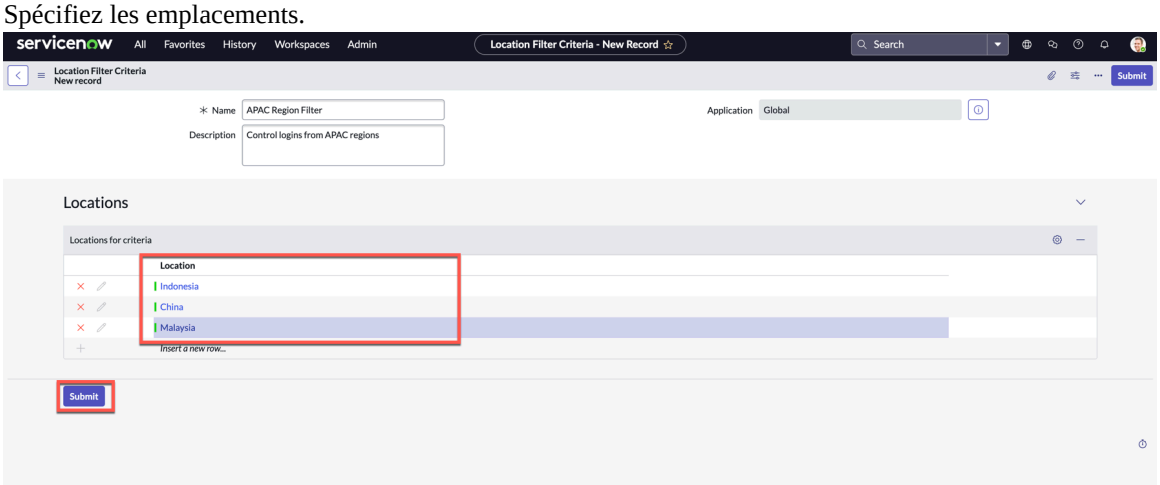
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Renseignez ces champs du formulaire.

Formulaire Critères de filtrage d'emplacement

Champ	Description
Nom	Nom permettant d'identifier les critères.
Description	Brève description des critères.
Application	Périmètre de l'application.

4. Dans les sections **Emplacements** , sous l'onglet Emplacements pour les critères, double-cliquez pour **insérer une nouvelle ligne**.
5. Spécifiez les emplacements.



6. Sélectionnez **Soumettre**.

Didacticiel : Utiliser les critères de filtre d'emplacement

Décrit les étapes à suivre pour utiliser les critères de filtrage d'emplacement dans la politique d'authentification et restreindre l'accès aux utilisateurs en fonction de l'emplacement.

Avant de commencer
Rôle requis : administrateur

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Propriété : activez la propriété d'authentification adaptative.

Remarque :
Les administrateurs ne peuvent créer la politique basée sur les filtres d'emplacement que si l'emplacement est disponible pour la session utilisateur actuelle.

La procédure suivante décrit comment créer et utiliser les critères de filtrage d'emplacement dans une politique d'authentification.

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Critère de filtre** > **Filtre d'emplacement**.
2. Sélectionnez **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

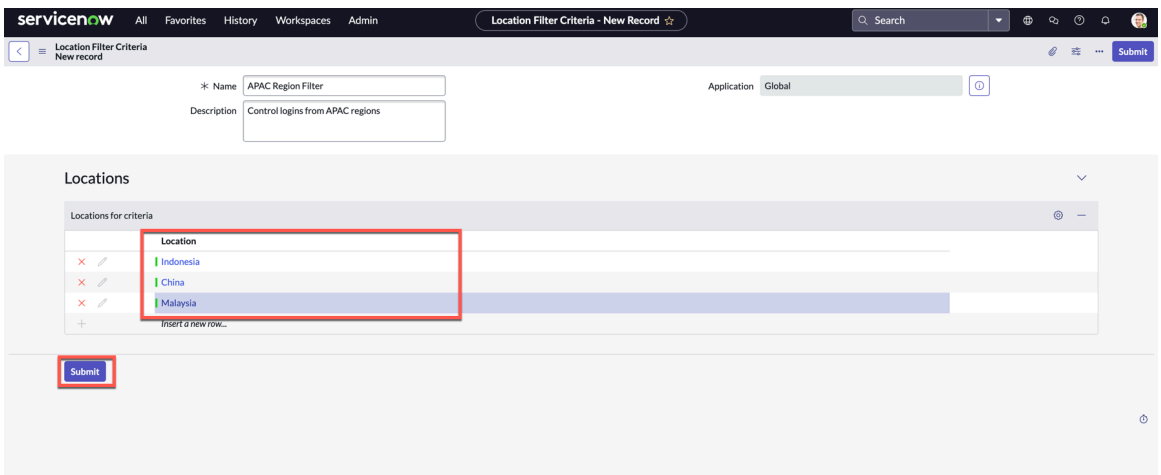
3. Renseignez ces champs du formulaire.

Formulaire Critères de filtrage d'emplacement

Champ	Description
Nom	Nom permettant d'identifier les critères.
Description	Brève description des critères.
Application	Périmètre de l'application.

4. Dans les sections **Emplacements** , sous l'onglet Emplacements pour les critères, double-cliquez pour **insérer une nouvelle ligne**.
5. Spécifiez les emplacements.

   Par exemple, utilisez certaines régions APAC pour contrôler les connexions des utilisateurs venant d'APAC.



   En fonction des critères définis dans l'exemple, vous pouvez contrôler les connexions à partir de l'Indonésie, de la Chine et de la Malaisie pour votre instance.

6. Sélectionnez **Soumettre**.
7. Utilisez les critères de filtre créés dans l'un des contextes d'authentification (Pré, Post, MFA) et d'accès à la session.

   Pour en savoir plus sur la configuration basée sur le contexte d'authentification et l'accès à la session, consultez :

   - Filtre d'emplacement dans le contexte de pré-authentification
   - Filtre d'emplacement dans le contexte de post-authentification
   - Filtre d'emplacement dans le contexte MFA
   - Filtre d'emplacement pour l'accès à la session

   Vous pouvez utiliser l'ID de propriété : message d'erreur à afficher à l'utilisateur en cas d'échec de la connexion en raison d'une défaillance de la politique d'authentification (glide.auth.policy.ui.error.message) pour personnaliser le message d'erreur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser le filtre d'emplacement dans le contexte de pré-authentification

Utilisez les critères de filtrage d'emplacement créés dans le contexte de pré-authentification.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Créez un filtre d'emplacement avec les pays dans lesquels vous souhaitez restreindre l'accès aux utilisateurs en fonction de l'emplacement. Pour plus d'informations, consultez Créer un critère de filtre d'emplacement.

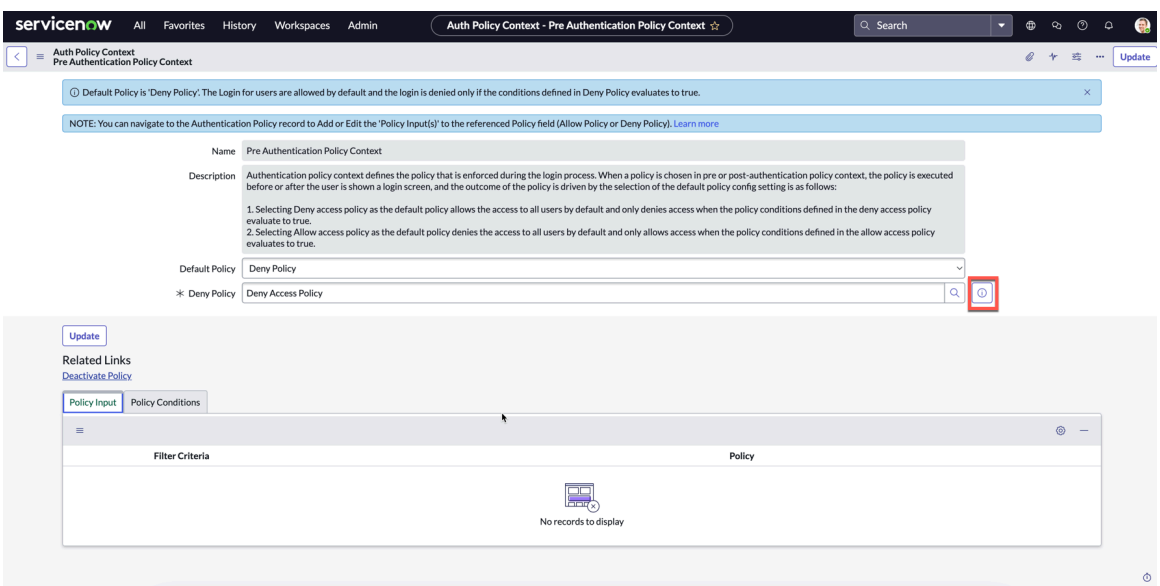
Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Contexte de la politique d'authentification** > **Contexte de pré-authentification**.

   Lorsqu'une politique est choisie dans le contexte de la politique de pré-authentification :

   - La sélection de la politique de refus d'accès comme politique par défaut autorise l'accès à tous les utilisateurs par défaut et ne refuse l'accès que lorsque les conditions de politique définies dans la politique de refus d'accès sont évaluées comme vraies.
   - La sélection de la politique d'autorisation d'accès comme politique par défaut refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions de politique définies dans la politique d'autorisation d'accès sont évaluées comme vraies.

   L'exemple montre comment restreindre les connexions à partir des emplacements spécifiés. Vous pouvez choisir Refuser l'accès et la politique associée (Refuser l'accès) comme politique de pré-authentification et spécifier les entrées et conditions de la politique.



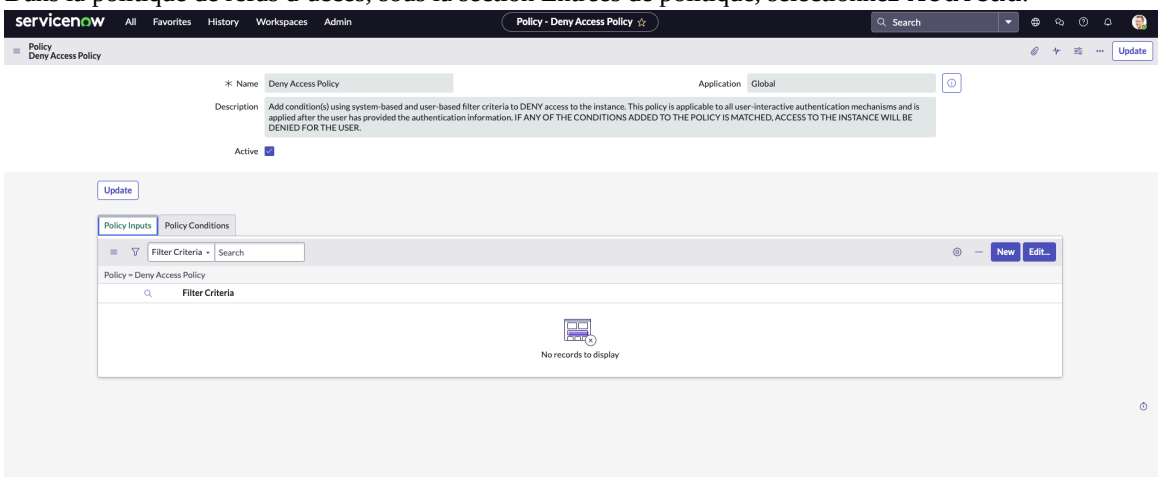
2. Sélectionnez l'icône d'informations pour ouvrir l'enregistrement **de politique de refus** .

> **Remarque :**
> L'exemple décrit dans cette tâche est **Refuser la politique**. Vous pouvez également utiliser **la politique d'autorisation** et définir les conditions en conséquence pour contrôler les connexions.

Traduction automatique

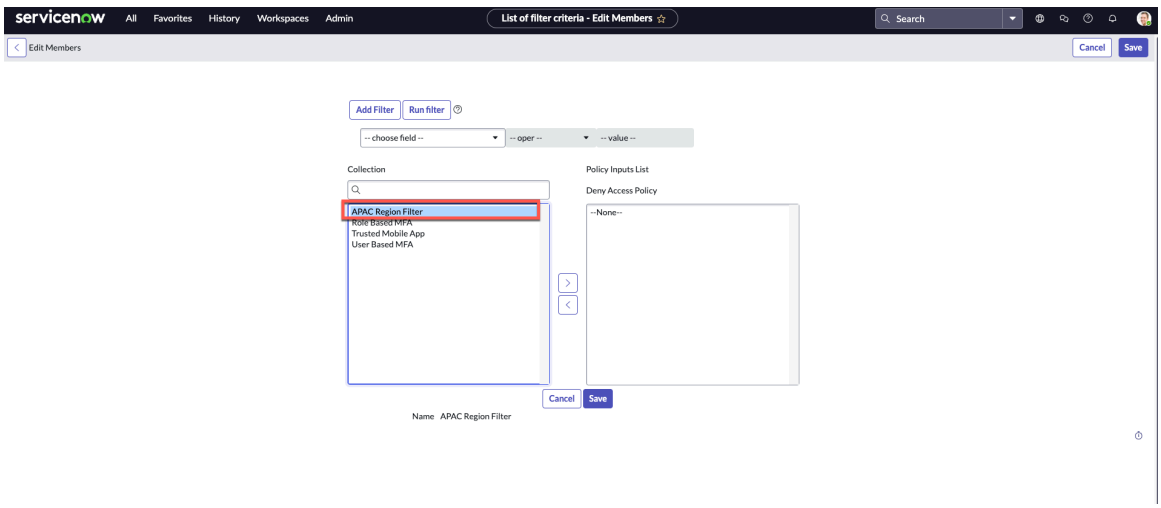
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Dans la politique de refus d'accès, sous la section Entrées de politique, sélectionnez **Nouveau**.



4. Ajoutez l'entrée Filtre d'emplacement et **enregistrez**.

Par exemple, Région APAC.



Le filtre est ajouté en tant **qu'entrées de politique**.

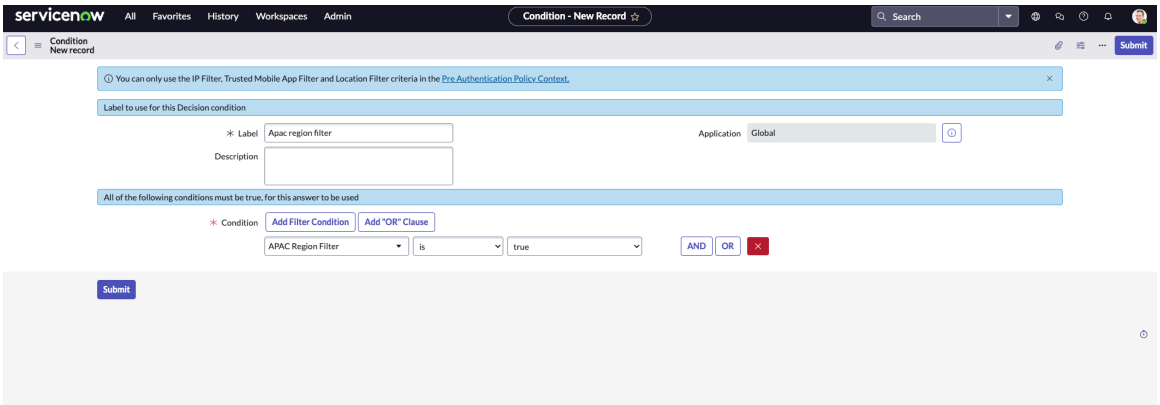
5. Sélectionnez l'onglet Conditions de la politique, puis sélectionnez **Nouveau**.



6. Dans la page Conditions, fournissez l'étiquette, les conditions, puis définissez-les sur vrai.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

- Dans cet exemple, la sélection de true comme condition implique que l'utilisateur qui se connecte à partir des régions configurées ne pourra pas se connecter à l'instance.
- Si la condition est définie sur false, seuls les utilisateurs des régions configurées peuvent se connecter à l'instance et les autres utilisateurs ne peuvent pas se connecter à l'instance.

7. Sélectionnez **Soumettre**.
   Les utilisateurs qui sélectionnent le lien d'instance et se connectent à partir des pays configurés verront s'afficher un message d'erreur concernant le refus d'accès (message d'erreur configuré par leurs administrateurs sur la page des propriétés de la politique).

Utiliser le filtre d'emplacement Contexte de post-authentification

Utilisez les critères de filtrage d'emplacement créés dans le contexte de post-authentification.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

Créez un filtre d'emplacement avec les pays dans lesquels vous souhaitez restreindre l'accès aux utilisateurs en fonction de l'emplacement. Pour plus d'informations, consultez Créer un critère de filtre d'emplacement.

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Contexte de la politique d'authentification** > **Contexte de post-authentification**.

   Lorsqu'une politique est choisie dans le contexte de la politique de post-authentification :

   - La sélection de la politique de refus d'accès comme politique par défaut autorise l'accès à tous les utilisateurs par défaut et ne refuse l'accès que lorsque les conditions de politique définies dans la politique de refus d'accès sont évaluées comme vraies.
   - La sélection de la politique d'autorisation d'accès comme politique par défaut refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions de politique définies dans la politique d'autorisation d'accès sont évaluées comme vraies.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

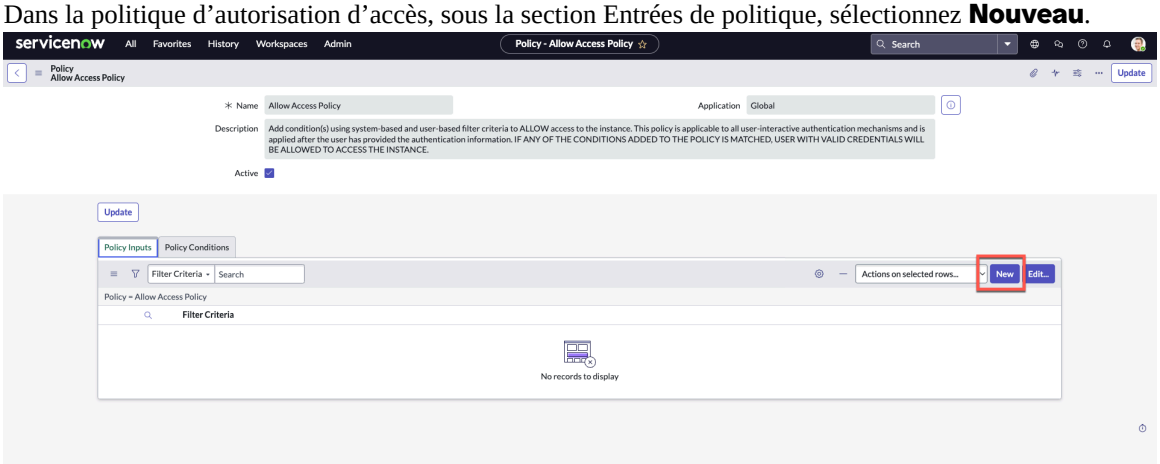
L’exemple montre comment configurer des utilisateurs ITIL avec une condition pour accéder uniquement à l’instance à partir de l’emplacement spécifié (États-Unis). Et les utilisateurs ITIL ne peuvent pas se connecter depuis d’autres pays.

Une fois que les utilisateurs ont fourni leurs informations d’identification sur la page de connexion. Vous pouvez choisir Autoriser l’accès et la politique associée (Autoriser l’accès) comme politique de post-authentification et spécifier les entrées et conditions de politique.

2. Sélectionnez l’icône d’informations pour ouvrir l’enregistrement **Autoriser la politique** .

> **Remarque :**
> L’exemple décrit dans cette tâche est **Autoriser la politique**. Vous pouvez également utiliser la **stratégie de refus** et définir les conditions en conséquence pour contrôler les connexions.

3. Dans la politique d’autorisation d’accès, sous la section Entrées de politique, sélectionnez **Nouveau**.



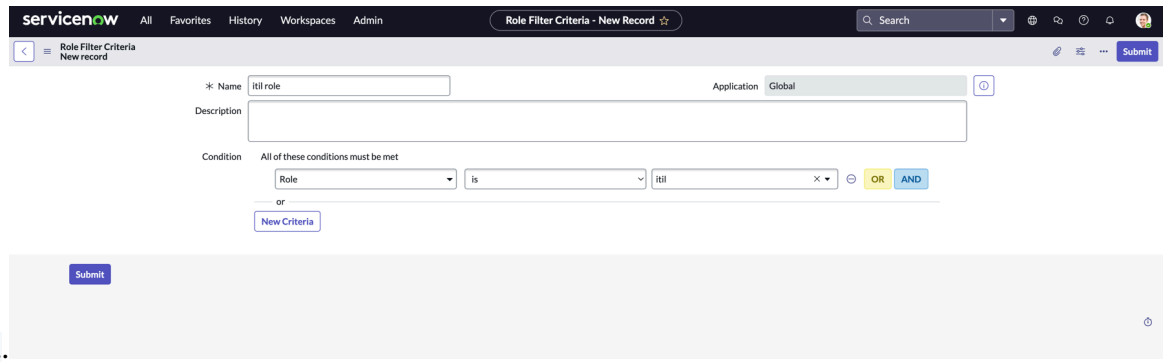
4. Ajoutez les critères de filtre de rôle et les critères de filtre d’emplacement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

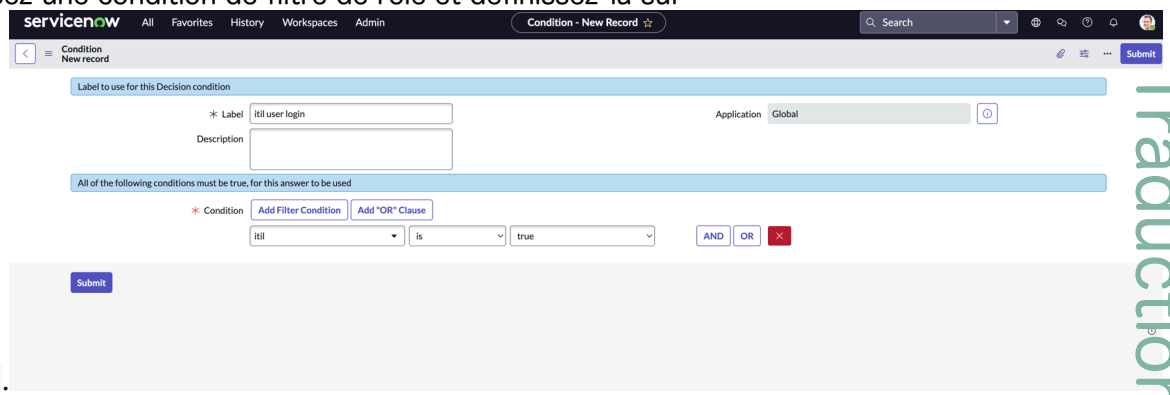
a. Ajout d'un rôle Critères de filtre :

- Créer un rôle Filtrer l'entrée au format



ITIL.

- Créez une condition de filtre de rôle et définissez-la sur



vrai.

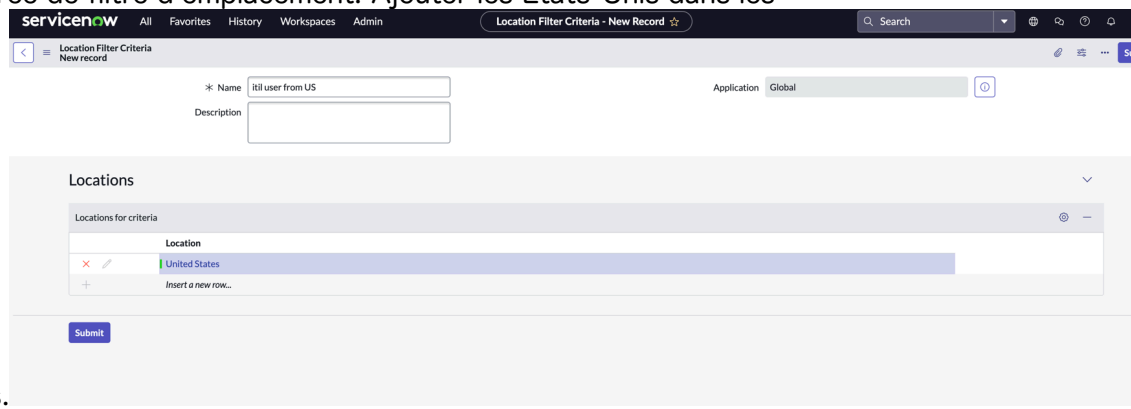
Pour en savoir plus sur la création de critères de filtre de rôle, reportez-vous à la section Créer un critère de filtre de rôle.

b. Ajout de critères de filtre d'emplacement :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Créer une entrée de filtre d’emplacement. Ajouter les États-Unis dans les emplacements.



- Créez une condition de filtre d’emplacement et définissez-la sur vrai.



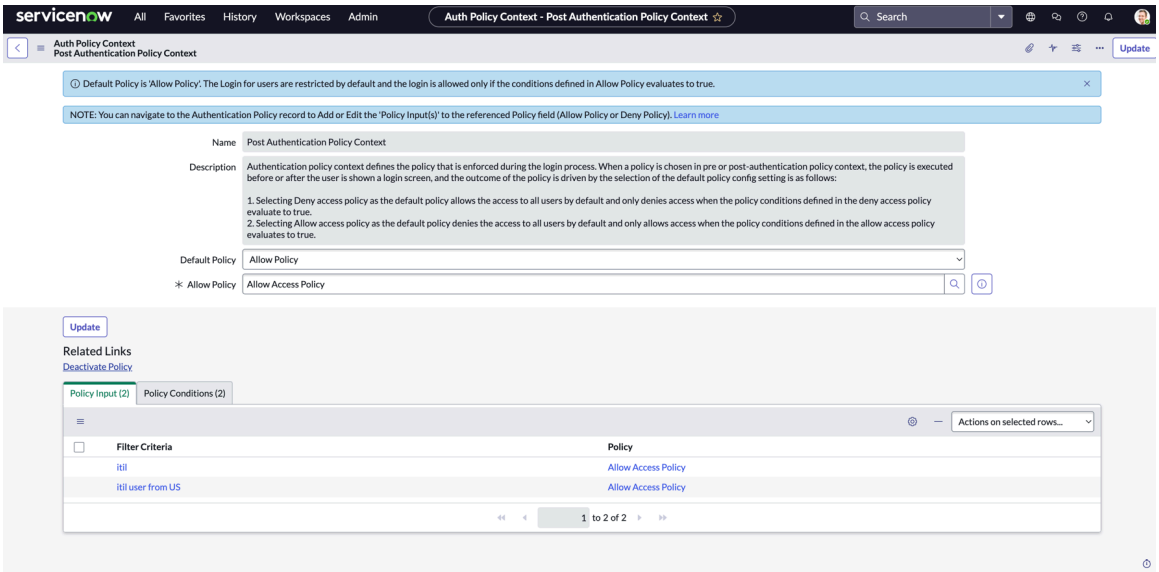
Pour en savoir plus sur la création de critères de filtre de rôle, reportez-vous à la section Créer un critère de filtre d’emplacement.

La politique d’autorisation d’accès affiche les entrées et conditions de politique créées lors des étapes précédentes :

- Entrées de politique : itil, utilisateur itil des États-Unis
- Conditions de la politique : connexion de l’utilisateur itil, condition de l’utilisateur itil à partir des États-Unis.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

- Dans cet exemple, la sélection de true comme condition implique que les utilisateurs ITIL qui se connectent à partir du pays configuré (États-Unis) sont en mesure de se connecter à l'instance.
- Si la condition est définie sur faux, les utilisateurs ITIL du pays configuré (États-Unis) ne pourront pas se connecter à l'instance et les autres utilisateurs ne pourront pas se connecter à l'instance.

5. Sélectionnez **Soumettre** ou **Mettre à jour** pour mettre à jour le contexte de post-authentification.
   Les utilisateurs ITIL qui sélectionnent le lien d'instance, spécifient leurs informations d'identification, puis se connectent en dehors du pays configuré (États-Unis) voient s'afficher un message d'erreur concernant le refus d'accès (message d'erreur configuré par leurs administrateurs sur la page des propriétés de la politique).

Utiliser le filtre d'emplacement dans le contexte MFA

Utilisez les critères de filtrage d'emplacement créés dans le contexte MFA.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

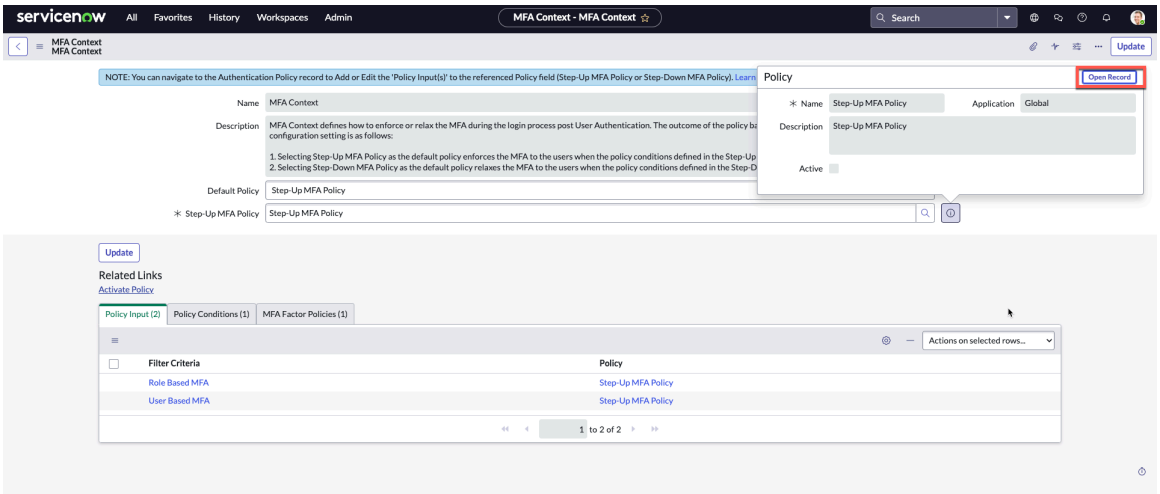
La procédure suivante décrit comment créer un filtre d'emplacement avec les pays dans lesquels vous souhaitez configurer l'authentification MFA comme deuxième facteur d'authentification auprès des utilisateurs en fonction de l'emplacement.

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Contexte de la politique d'authentification** > **Contexte MFA**.
2. Sur la page **contextuelle MFA** , sélectionnez l'icône **Informations sur la politique MFA ascendante** et ouvrez l'enregistrement.

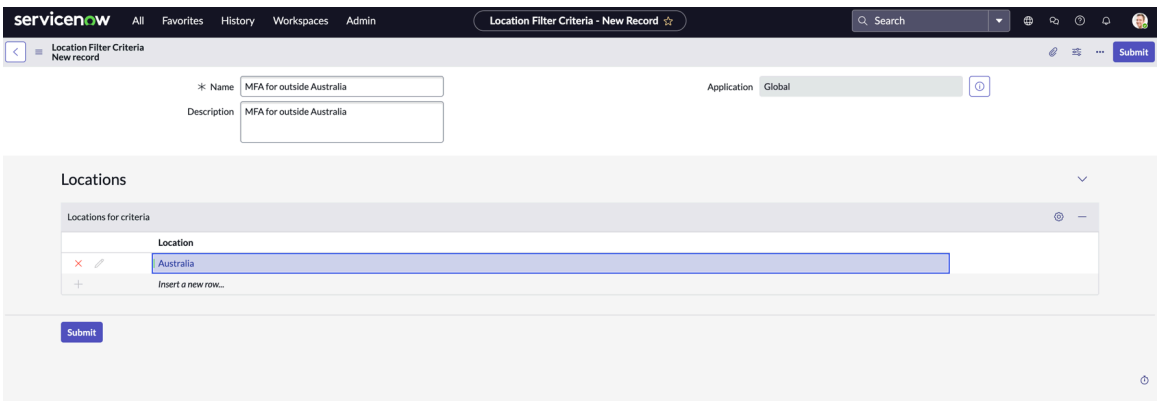
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

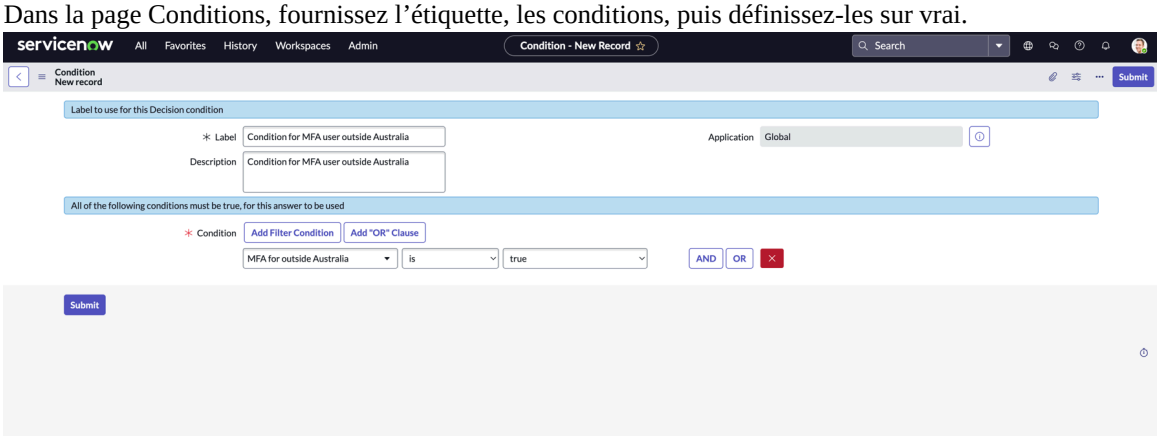


3. Sur la page Politique MFA ascendante, sous l'onglet Entrées de politique, sélectionnez **Nouveau**.
4. Ajoutez l'entrée Filtre d'emplacement et **soumettez**.

   Par exemple, vous souhaitez afficher la MFA pour les utilisateurs qui se connectent à l'instance en dehors de l'Australie.



5. Sur la page Politique MFA ascendante, sélectionnez l'onglet Conditions de politique, puis sélectionnez **Nouveau**.
6. Dans la page Conditions, fournissez l'étiquette, les conditions, puis définissez-les sur vrai.



7. Sélectionnez **Soumettre**.
8. Sur la page Politique MFA ascendante, activez la politique MFA si elle est **désactivée**.
9. Sélectionnez **Mettre à jour** pour mettre à jour la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les utilisateurs en dehors du pays configuré (Australie) sélectionnant le lien d'instance, en spécifiant leurs informations d'identification ; s'affichera avec l'écran MFA pour fournir les informations d'identification du deuxième facteur permettant de se connecter à l'instance.

Utiliser le filtre d'emplacement pour l'accès à la session

Utilisez les critères de filtrage d'emplacement créés dans Accès à la session pour réduire les rôles en fonction de l'emplacement de l'utilisateur.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : **Zero Trust - Location Based Access** (com.snc.zero_trust_location_access).

La procédure suivante explique comment créer un filtre d'emplacement avec les pays pour lesquels vous souhaitez supprimer ou limiter les rôles aux utilisateurs en fonction de l'emplacement.

Procédure

1. Accédez à la **Tout** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.
2. Pour créer une configuration de rôle d'accès à la session, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire :

Configuration du rôle d'accès à la session

Champ	Description
Nom	Nom de la configuration
Description	Brève description de la configuration.
Politique	Choisissez la politique d'accès. Utilisez l'icône de recherche pour afficher la liste des politiques. **Remarque :** Vous devez ajouter l'entrée et les conditions du filtre d'emplacement en ouvrant l'enregistrement de la politique.
Action	**Supprimez les rôles** ou **limitez-les aux rôles**. ○ **Supprimer les rôles** : lorsque l'utilisateur configuré est connecté, la liste des rôles fournie dans la liste de rôles ou de groupes est supprimée pour la session connectée. ○ **Limiter aux rôles** : lorsque l'utilisateur configuré est connecté, seuls les rôles sélectionnés lui sont fournis et tous les autres rôles sont supprimés pour la session connectée.
Liste de rôles	Choisissez le rôle dans la liste des rôles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Liste de groupes	Choisissez le rôle dans la liste des groupes.

4. Sélectionner, **soumettre**.

   La connexion des utilisateurs en fonction des pays configurés est la suivante :

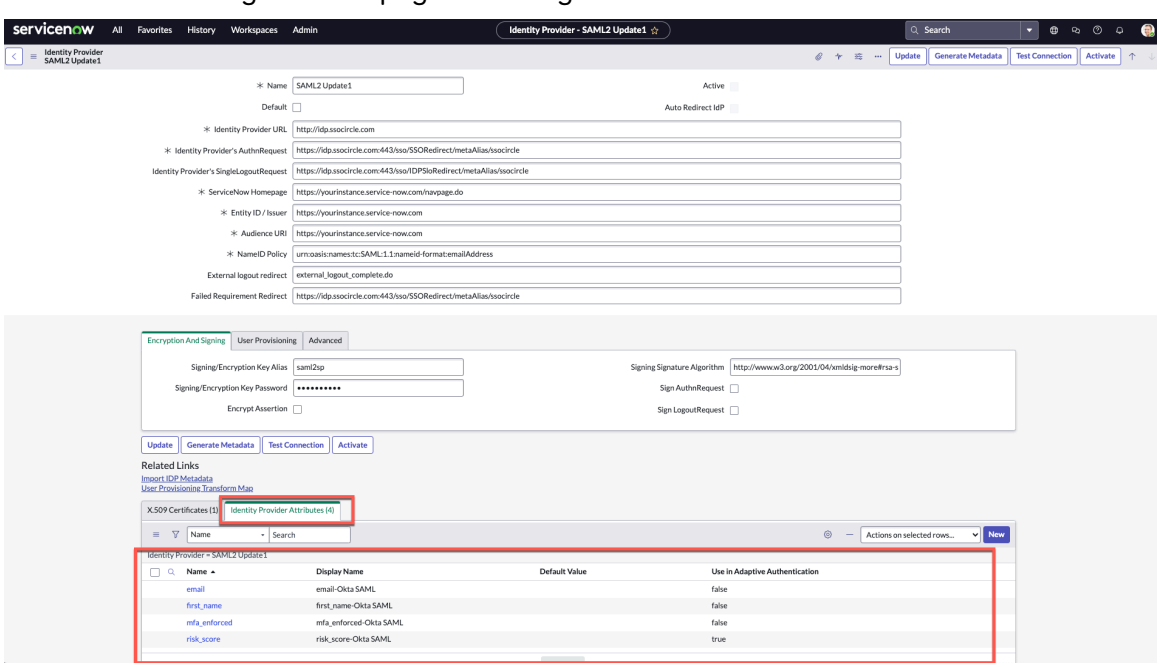
   - Si **l'option Supprimer les rôles**, les utilisateurs des pays configurés dans le filtre d'emplacement seront supprimés avec les rôles configurés pour la session.
   - Si **l'option Limiter aux rôles** est activée, les utilisateurs des pays configurés dans le filtre d'emplacement ne disposent que des rôles configurés pour la session.

   Pour en savoir plus sur la suppression ou la limitation des rôles d'une session, reportez-vous à la section Tutoriel : Utiliser l'accès zéro confiance.

Filtre d'attributs du fournisseur d'identité

Utilisez les attributs de fournisseur d'identité reçus de la réponse SAML (Security Assertion Markup Language) du fournisseur d'identité (IdP) comme critères de filtre pour l'authentification.

Pour extraire tous les attributs d'un IdP via la réponse SAML, vous devez effectuer un test de connexion avec l'IdP. Une fois la connexion de test réussie, les attributs sont ajoutés dans un nouvel onglet sur la page de configuration du fournisseur d'identité.



Vous pouvez également ajouter des attributs en sélectionnant **Nouveau** dans la section Attributs du fournisseur d'identité et utiliser ces attributs pour Authentification adaptative en la définissant sur vrai.

Les **attributs du fournisseur d'identité sont affichés** avec les détails suivants :

Formulaire Critères de filtrage d'emplacement

Champ	Description
Nom	Nom d'attribut fourni par le fournisseur d'identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Critères de filtrage d'emplacement (suite)

Champ	Description
Nom d'affichage	Le nom d'affichage est le nom détaillé utilisé pour les critères de filtre. **Remarque :** Vous pouvez fournir un nom lisible en tant que nom d'affichage, dans certains cas, le nom d'affichage fourni par les fournisseurs d'identité est long et non lisible.
Valeur par défaut	La valeur par défaut est utilisée pour l'évaluation des critères de filtre au cas où l'attribut serait manquant dans la réponse SAML.
Utiliser dans Authentification adaptative	Option permettant d'utiliser l'attribut dans l'authentification adaptative.

Remarque :
Le nom et le nom d'affichage des attributs renseignés à partir de l'IdP Azure sont limités à des caractères en raison de la longueur du nom de l'attribut.

Vous pouvez également ajouter de nouveaux attributs en sélectionnant **Nouveau** dans la section **Attributs des fournisseurs d'identité** .

Si l'utilisation dans Authentification adaptative est définie sur true, l'attribut sélectionné est ajouté en tant que critère de filtre dans les critères de filtre génériques. Par exemple, **risk_score** défini sur vrai. Un nouveau filtre a été créé pour la page Critères de filtre génériques.

Utiliser l'attribut du fournisseur d'identité comme critère de filtre

Utilisez l'attribut fournisseur d'identité (IDP) de la réponse SAML (Security Assertion Markup Language) comme critère de filtre pour la politique d'authentification.

Avant de commencer
Rôle requis : administrateur

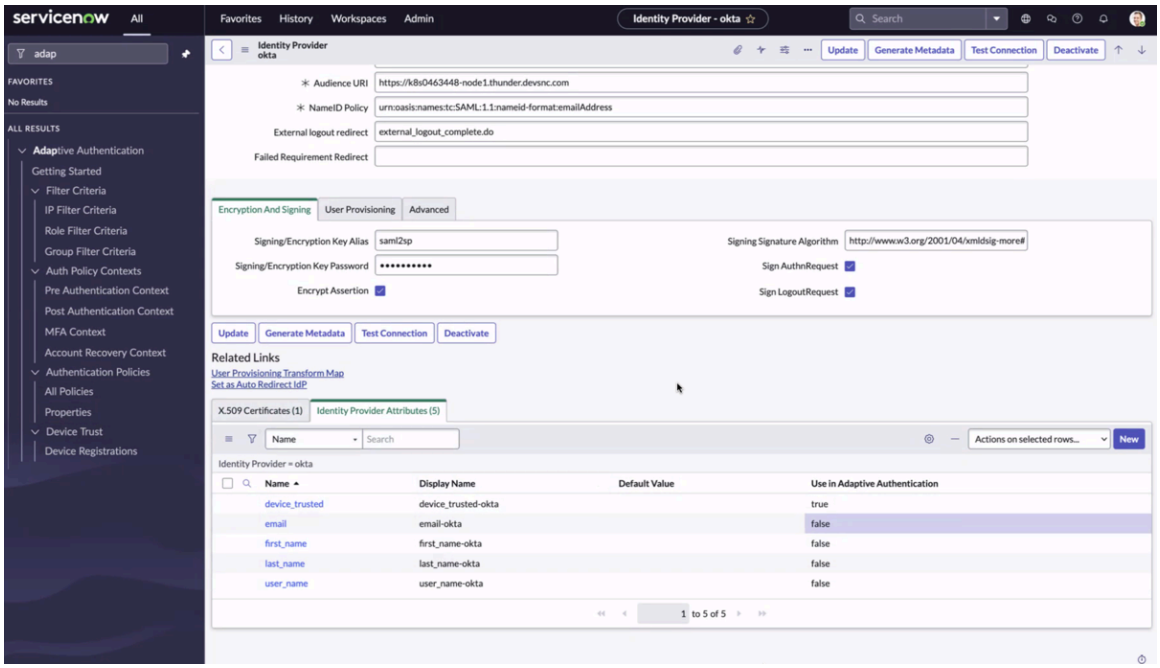
Vous pouvez créer une politique d'accès à la session en utilisant le contexte de la politique (pré-authentification, post-authentification, authentification multifacteur) et des critères de filtre (rôle, groupe, IP, emplacement) avec des entrées et des conditions de politique.

La procédure suivante montre les étapes à suivre pour configurer l'attribut IdP de la réponse SAML en tant qu'entrée de politique pour contrôler l'authentification dans le **contexte de post-authentification**, le **contexte d'authentification multifacteur (MFA)** et **Zéro confiance : accès à la session basé sur des politiques**.

Les attributs IdP Okta sont présentés dans la capture d'écran suivante. Vous devez définir l'utilisation dans l'authentification adaptative sur vrai pour l'utiliser dans le **contexte de post-authentification**, dans le **contexte d'authentification multifacteur (MFA)** et dans les politiques **d'accès à la session Zero Trust : basées sur des politiques** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Les politiques de post-autorisation, MFA, Zero Trust : accès à la session basé sur des politiques s'exécutent une fois que les utilisateurs ont entré les informations d'identification ou la réponse SSO.

Procédure

1. Utilisation de l'attribut IdP dans le contexte de la politique de post-authentification.
   Exemple : configuration pour activer les connexions à partir des attributs IdP Okta si l'appareil est approuvé.

   a. Accédez à la **Tout** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de la politique de post-authentification.**.

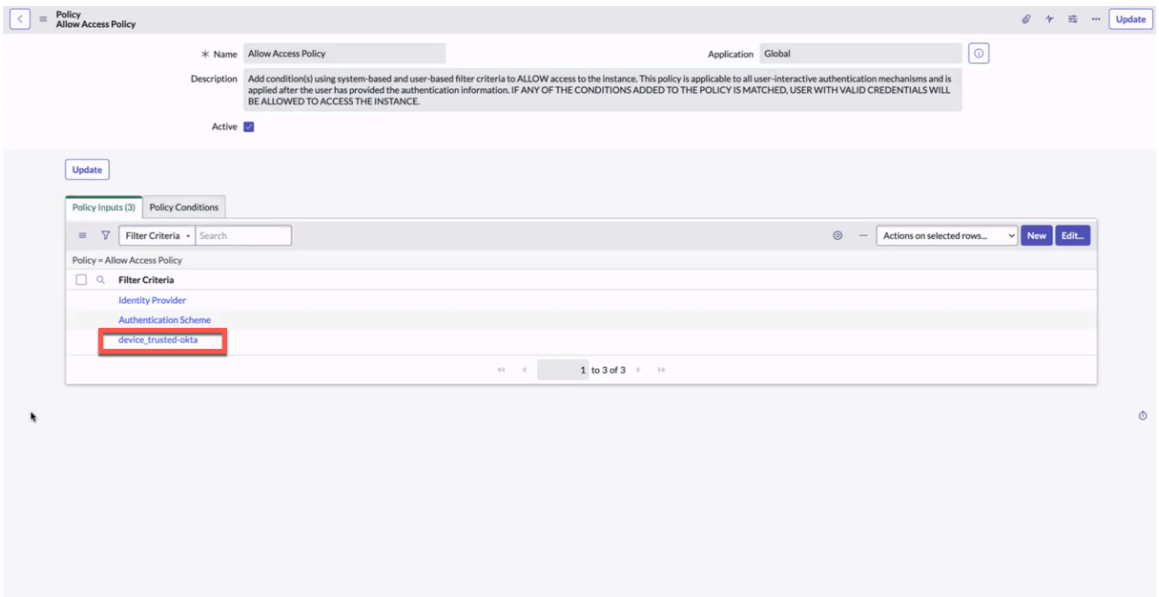
   b. Sélectionnez **Autoriser la politique** et ouvrez l'enregistrement de la politique.

   c. Dans l'entrée Politique, créez l'entrée Politique et la Condition de politique.

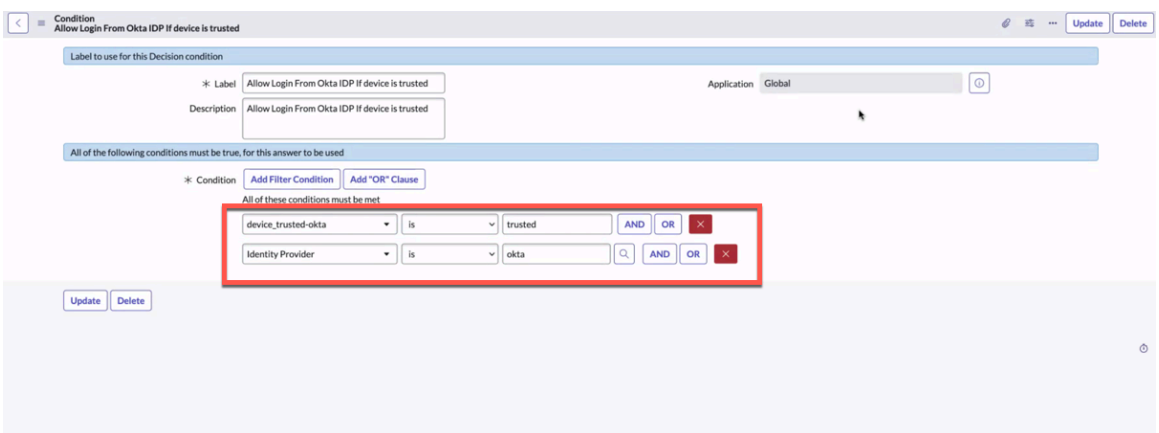
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Entrée de politique** : ajoutez **device_trusted-okta**.



- **Conditions de la politique** : **device_trusted-okta** est approuvé et **le fournisseur d'identité** est okta.



Selon cette configuration, lorsque l'appareil est approuvé par Okta (IdP), l'utilisateur est authentifié auprès de l'instance.

Pour en savoir plus sur la création d'un contexte de post-authentification avec une politique et une condition, reportez-vous à la section Contexte post-authentification.

2. Utilisation de l'attribut IdP dans le contexte de la politique de MFA.
Exemple : configuration permettant d'activer la MFA à partir des attributs IdP Okta si l'appareil n'est pas approuvé.

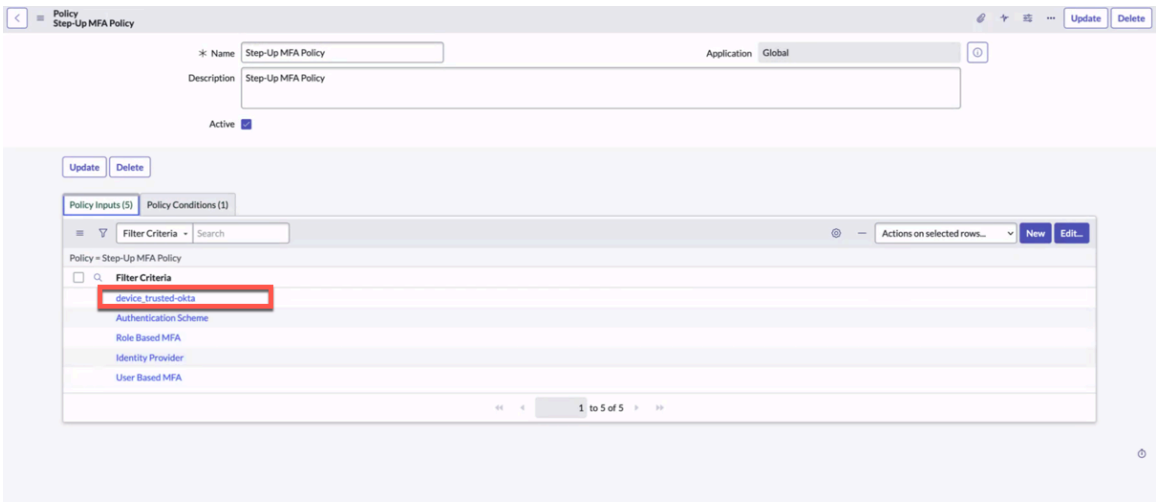
a. Accédez à la **Tout** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de la politique d'authentification MFA.**.

b. Dans l'entrée Politique, créez l'entrée Politique et la Condition de politique.

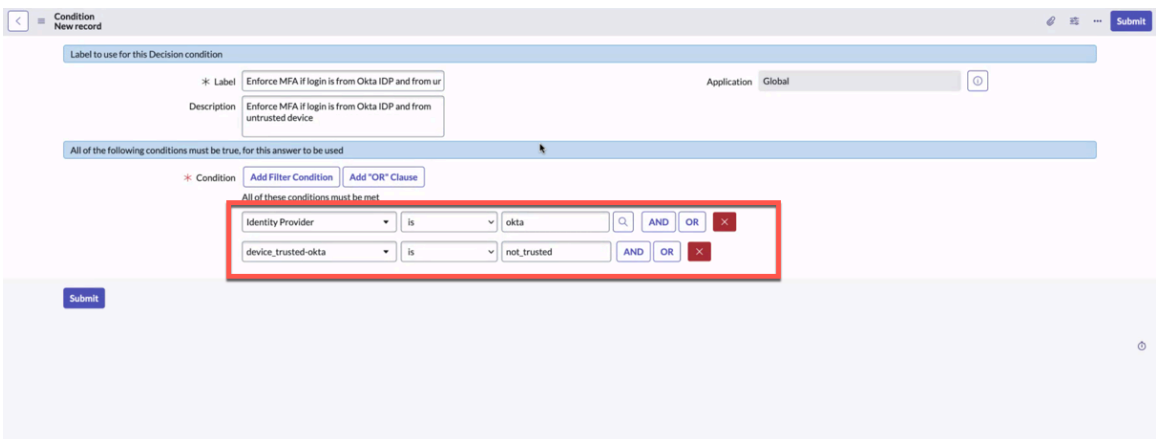
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Entrée de politique** : ajoutez **device_trusted-okta**.



- **Conditions de la politique** : **device_trusted-okta** est `not_trusted` et **le fournisseur d'identité** est `okta`.



Selon cette configuration, lorsque l'appareil n'est pas approuvé par Okta (IdP), l'utilisateur affiche une authentification à deuxième facteur pour se connecter à l'instance.

Pour plus d'informations sur la création d'un contexte MFA avec une politique et une condition, reportez-vous à la section Contexte MFA (Multi-Factor Authentication).

3. Utilisation de l'attribut IdP dans l'accès à la session Zero Trust : basé sur des politiques.
Exemple : configuration pour réduire le privilège du rôle `ITIL` à partir des attributs IdP Okta si l'appareil n'est pas approuvé.

a. Accédez à la **Tout** > **Accès zéro confiance** > **Configurations du rôle d'accès à la session**.

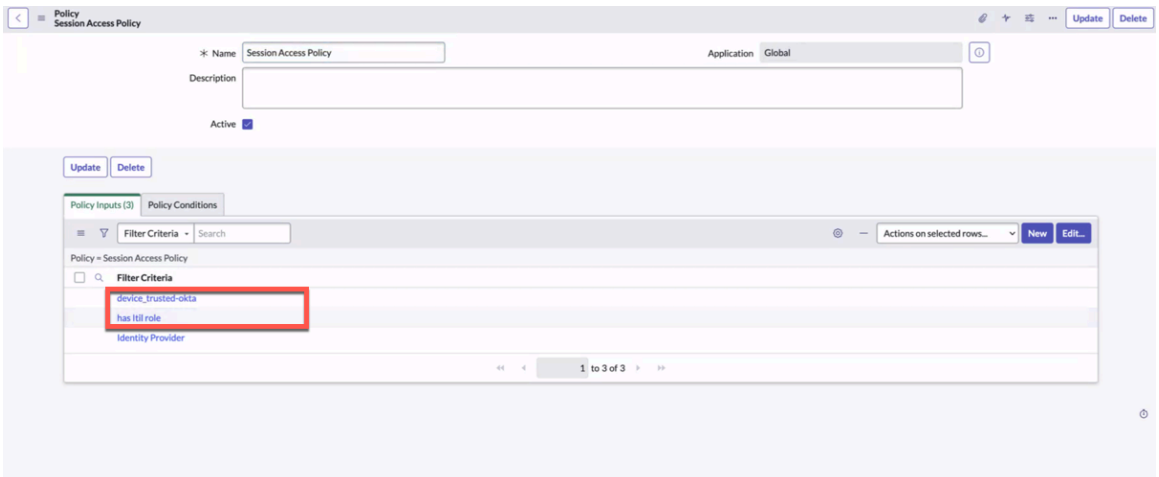
b. Créez une configuration du rôle d'accès à la session.

c. Dans l'entrée Politique, créez l'entrée Politique et la Condition de politique.

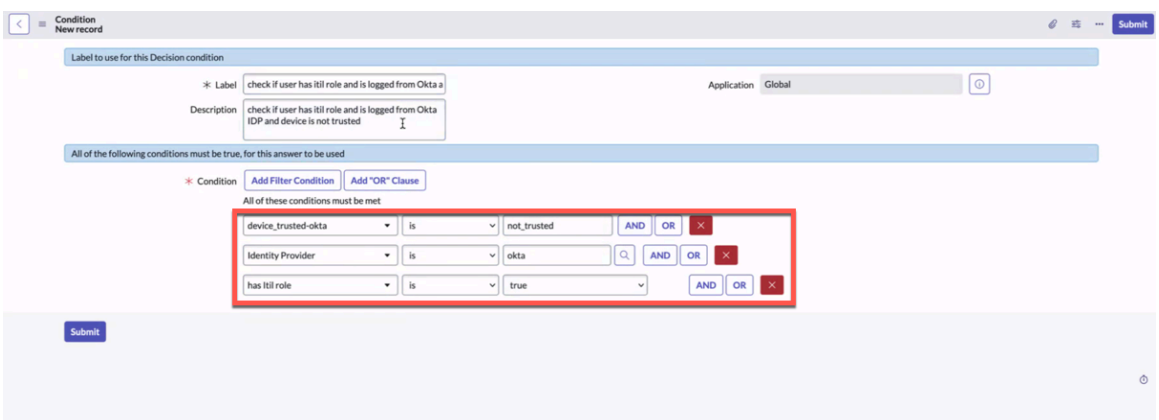
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Entrée de politique** : ajouter **device_trusted-okta** et **dispose du rôle itil**.



- **Conditions de la politique** : **device_trusted-okta** est `not_trusted`, **le fournisseur d'identité** est `okta` et **a le rôle itil** est `vrai`.



Sur la base de cette configuration, lorsque l'utilisateur ITIL utilise un appareil qui n'est pas approuvé par Okta (IdP), les privilèges de l'utilisateur sont réduits pour la session connectée.

Pour plus d'informations sur la création d'un accès à la session Zéro confiance - basé sur des politiques avec une politique et une condition, reportez-vous à la section Accès zéro confiance.

Contextes de politique d'authentification

Utilisez les contextes de politique d'authentification pour déterminer comment et quand votre instance applique les politiques d'authentification.

Les contextes d'authentification définissent comment et quand une stratégie est appliquée pendant le processus de connexion. Affectez une politique à un contexte de politique pour définir des entrées et des conditions concernant la façon dont votre instance gère l'authentification.

Contexte de pré-authentification

Dans le contexte de la pré-autorisation, les politiques s'exécutent lorsqu'un utilisateur accède pour la première fois à l'instance, avant qu'un écran de connexion ne s'affiche. Vous pouvez utiliser le contexte de pré-autorisation pour autoriser ou refuser l'accès avant

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que vos utilisateurs soient invités à entrer des informations d'identification de connexion en fonction de la politique que vous avez sélectionnée. Étant donné que ces politiques évaluent avant qu'un utilisateur ne saisisse des informations, elles ne peuvent pas prendre en compte des critères tels que les rôles ou les groupes d'un utilisateur.

Pour plus de détails sur ce contexte, reportez-vous à Contexte de pré-authentification.

Contexte post-authentification

Dans le contexte de post-autorisation, les politiques s'exécutent une fois que les utilisateurs ont entré leurs informations d'identification ou leur réponse SSO. Votre instance autorise ou refuse l'accès en fonction de la politique que vous avez sélectionnée. Étant donné que vos utilisateurs se sont identifiés à l'aide de leurs identifiants de connexion, la politique peut utiliser les informations utilisateur pour déterminer s'ils doivent accorder l'accès.

Pour plus de détails sur ce contexte, reportez-vous à Contexte post-authentification.

Contexte MFA (Multi-Factor Authentication)

Les politiques affectées au contexte MFA définissent s'il faut appliquer la MFA pendant le processus de connexion. L'application de la MFA par votre instance dépend de la configuration des politiques dans ce contexte. Pour plus de détails sur ce contexte, reportez-vous à Contexte MFA (Multi-Factor Authentication).

Contexte de récupération de compte

Les administrateurs peuvent configurer la récupération de compte (ACR) pour effectuer des activités de récupération telles que le traitement d'une erreur de configuration SSO ou de certificats expirés. Pour utiliser la récupération de compte, vous devez enregistrer au moins un compte administrateur en tant qu'utilisateur de récupération de compte. L'authentification unique ne peut pas être activée sur votre instance tant qu'au moins un compte n'est pas configuré. Pour plus d'informations sur le contexte qui peut être défini, reportez-vous à la section Contexte de récupération de compte.

Contexte de validation de la session

Le contexte de validation de session peut être utilisé avec le cadre de travail des politiques d'authentification adaptative. Le cadre de travail utilise des politiques d'authentification pour évaluer les demandes d'authentification (session), puis pour refuser ou autoriser l'accès en fonction des conditions de la politique. Pour plus d'informations, consultez Contexte de validation de la session.

Politique par défaut

Dans le contexte de la politique, vous pouvez définir une politique par défaut dans le champ **Politique par défaut** . Cette valeur par défaut définit la façon dont votre instance répond au résultat de votre politique. Les options de stratégie par défaut disponibles sont déterminées par le contexte que vous utilisez. Vous trouverez des détails sur ces options dans les documents décrivant ces contextes individuels.

Contexte de pré-authentification

Le contexte de la politique de pré-authentification définit comment et quand une politique est appliquée pendant le processus de connexion. La politique utilisée dans ce contexte s'exécute avant que vos utilisateurs ne voient un écran de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrement de contexte de pré-authentification

Dans le contexte de la pré-autorisation, les politiques s'exécutent lorsqu'un utilisateur accède pour la première fois à l'instance, avant qu'il ne voie un écran de connexion.

Vous pouvez utiliser le contexte de pré-authentification pour autoriser ou refuser l'accès avant que vos utilisateurs soient invités à fournir des informations d'identification de connexion en fonction de la politique que vous avez sélectionnée. Étant donné que ces politiques évaluent avant qu'un utilisateur ne saisisse des informations, elles ne peuvent pas prendre en compte des critères tels que les rôles ou les groupes d'un utilisateur.

Utilisez les champs de l'enregistrement de contexte de la politique de pré-authentification pour définir la façon dont votre instance utilise votre politique.

Formulaire de contexte de pré-authentification

Champ	Description
Nom	Nom du contexte de la politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Autoriser la politique** Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions évaluées par la politique sélectionnées dans le champ **Autoriser la politique** sont vraies. **Refuser la politique** Permet l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions que la politique sélectionnée dans le champ **Refuser la politique** sont évaluées comme vraies.
Autoriser la politique	La politique utilisée pour ce contexte s'applique. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	La politique utilisée pour ce contexte s'applique. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Remarque :

Vous ne pouvez utiliser que les critères Filtre IP, Filtre d'application mobile de confiance et Filtre d'emplacement dans le contexte de la politique de pré-authentification.

Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et conditions de la politique sélectionnées dans le champ Autoriser la **politique** ou Refuser la **politique** . Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier votre politique, accédez à la politique à l'aide de l'icône de référence ( ) en regard du champ **Autoriser la politique** ou **Refuser la politique** .

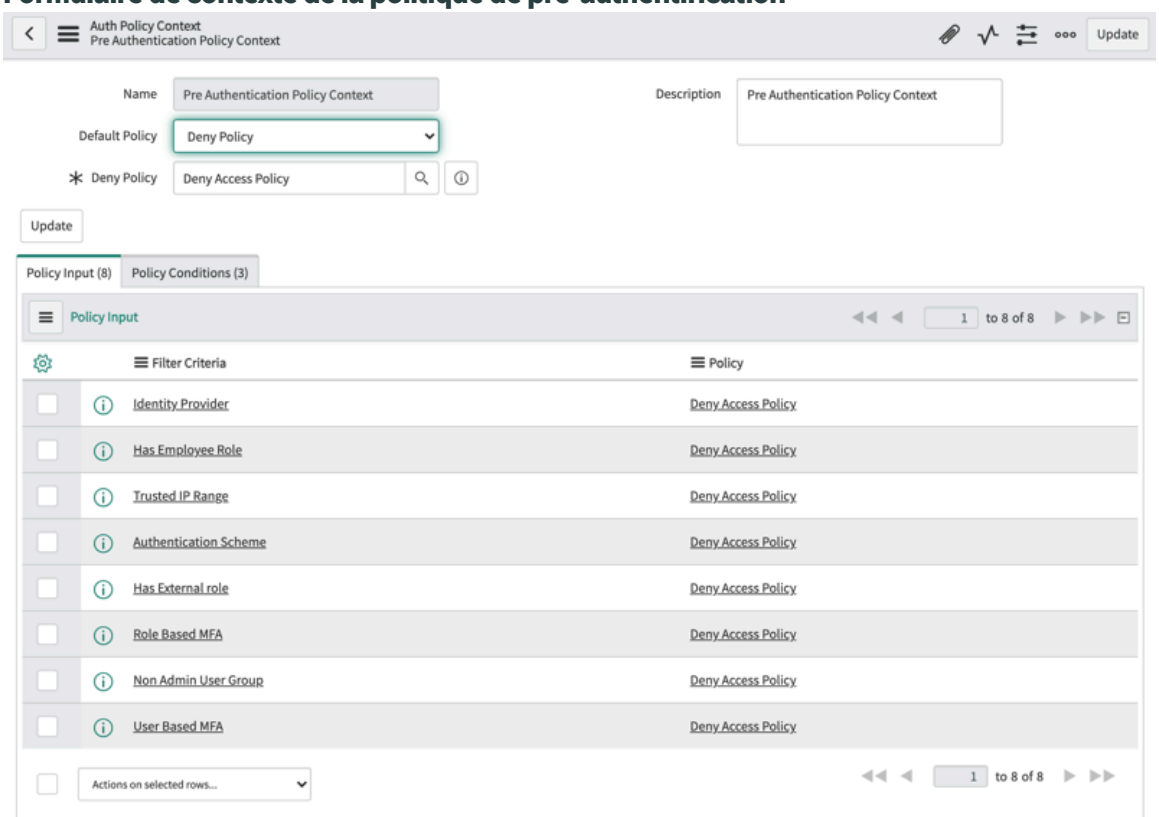
Cet exemple montre un enregistrement de contexte de politique de pré-authentification configuré pour refuser l'accès par défaut. Le contexte utilise une politique appelée **stratégie de refus d'accès**. Cette politique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

comporte un ensemble d'entrées et de conditions qui s'affichent dans les onglets **Entrée de politique** et **Condition de politique** .

Formulaire de contexte de la politique de pré-authentification



Contexte post-authentification

Le contexte de politique de post-authentification définit comment et quand une politique est appliquée pendant le processus de connexion. La politique utilisée dans ce contexte s'exécute une fois que vos utilisateurs ont vu un écran de connexion.

Enregistrement de contexte post-authentification

Dans le contexte de post-autorisation, les politiques s'exécutent une fois que les utilisateurs ont entré leurs informations d'identification ou leur réponse SSO. Votre instance autorise ou refuse l'accès en fonction de la politique que vous avez sélectionnée. Étant donné que vos utilisateurs se sont identifiés à l'aide de leurs informations d'identification de connexion, la politique peut utiliser des informations utilisateur telles que le rôle ou le groupe pour déterminer s'il convient d'accorder l'accès.

Utilisez les champs de l'enregistrement de contexte de la politique post-authentification pour définir la façon dont votre instance utilise votre politique.

Formulaire de contexte post-authentification

Champ	Description
Nom	Nom du contexte de la politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de contexte post-authentification (suite)

Champ	Description
	Autoriser la politique Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions évaluées par la politique sélectionnées dans le champ **Autoriser la politique** sont vraies. **Refuser la politique** Permet l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions que la politique sélectionnée dans le champ **Refuser la politique** sont évaluées comme vraies.
Autoriser la politique	La politique utilisée pour ce contexte s'applique. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	La politique utilisée pour ce contexte s'applique. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Entrées et conditions de la politique

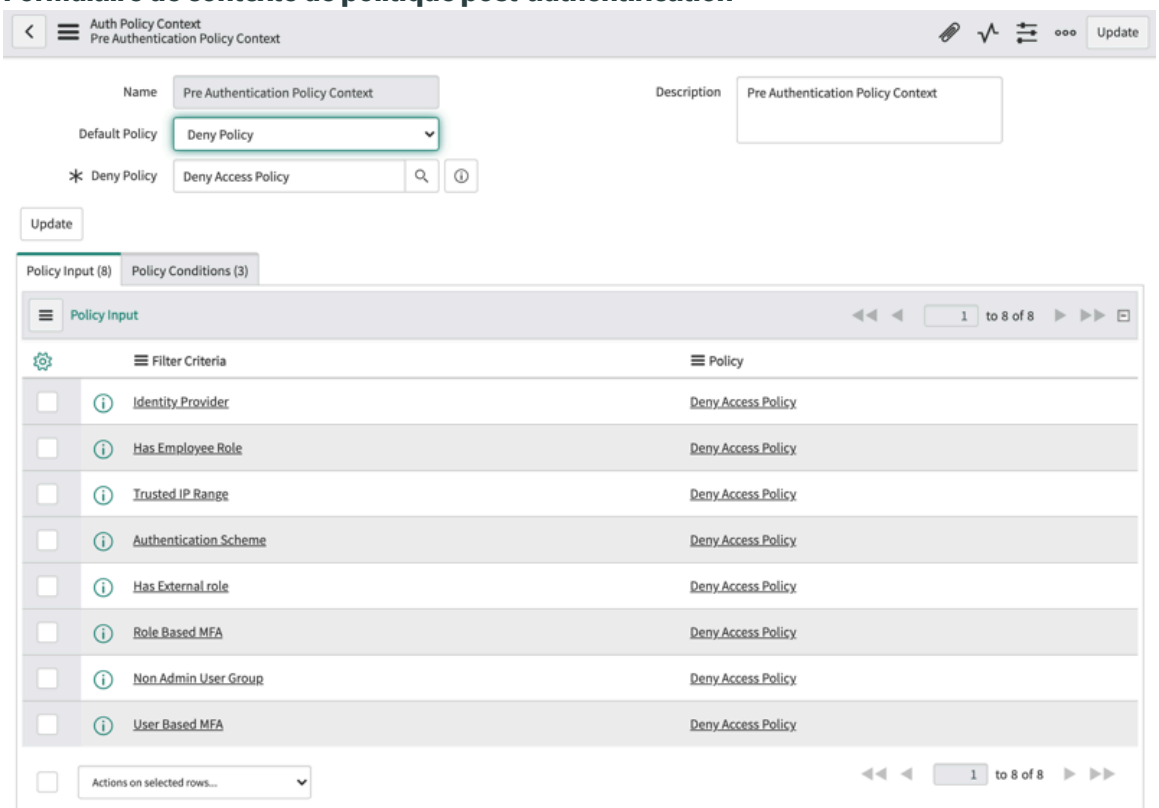
Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et conditions de la politique sélectionnées dans le champ Autoriser la **politique** ou Refuser la **politique** . Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier les paramètres de votre politique, accédez à la politique à l'aide de l'icône de référence (ⓘ) en regard du champ **Autoriser la politique** ou **Refuser la politique** .

Cet exemple montre un enregistrement de contexte de politique de post-authentification configuré pour refuser l'accès par défaut. Le contexte utilise une politique appelée **stratégie de refus d'accès**. Cette politique comporte un ensemble d'entrées et de conditions qui s'affichent dans les onglets **Entrée de politique** et **Condition de politique** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de contexte de politique post-authentification



Contexte MFA (Multi-Factor Authentication)

Le contexte de la politique MFA (Multi-Factor Authentication) utilise une politique pour définir comment et quand la MFA est appliquée pendant le processus de connexion.

Enregistrement de contexte MFA

Le contexte de la politique MFA (Multi-Factor Authentication) définit si vos utilisateurs doivent fournir une deuxième forme d'authentification lors de la connexion. Ce contexte ne refuse pas l'accès à votre instance comme les politiques de post-authentification et de pré-authentification. La politique que vous sélectionnez dans ce contexte est prioritaire sur les configurations basées sur les utilisateurs ou les rôles pour l'authentification multifacteur.

Pour accéder au contexte MFA, accédez à **Tout** > **Authentification multifacteur** > **Contexte MFA**.

Utilisez les champs de l'enregistrement de contexte de la politique post-authentification pour définir la façon dont votre instance utilise votre politique.

Remarque :

- Si la politique par défaut est Politique **de MFA ascendante**, les utilisateurs s'affichent avec l'authentification multifacteur si la politique configurée dans la **politique de MFA ascendante** est évaluée comme vrai. La politique a priorité sur la configuration basée sur l'utilisateur ou le rôle.
- MFA avec connexion SSO n'est disponible que si la propriété glide.authenticate.mfa.with.multisso.enabled est définie sur vrai.
- Vous pouvez accéder à l'enregistrement Politique d'authentification pour ajouter ou modifier les « entrées de politique » au champ de politique référencé (**Politique de MFA ascendante** ou **Politique de MFA descendante**).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de contexte MFA

Champ	Description
Nom	Nom du contexte de la politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Politique MFA ascendante** Applique la MFA aux utilisateurs lorsque les conditions de politique définies dans le champ **Politique de MFA ascendante** sont évaluées comme vraies. **Politique MFA descendante** Applique la MFA par défaut. La MFA n'est pas appliquée uniquement lorsque les conditions de politique définies dans le champ **Politique de MFA descendante** sont évaluées comme vraies.
Politique MFA ascendante	La politique utilisée pour ce contexte s'applique. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Politique MFA ascendante**.
Politique MFA descendante	La politique utilisée pour ce contexte s'applique. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Politique MFA descendante**.

Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et conditions de la politique sélectionnée dans le champ **Politique MFA ascendante** ou **Politique MFA descendante** . Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier les paramètres de votre politique, accédez à la politique à l'aide de l'icône de référence ( ) en regard du champ **Politique MFA ascendante** ou **Politique MFA descendante** .

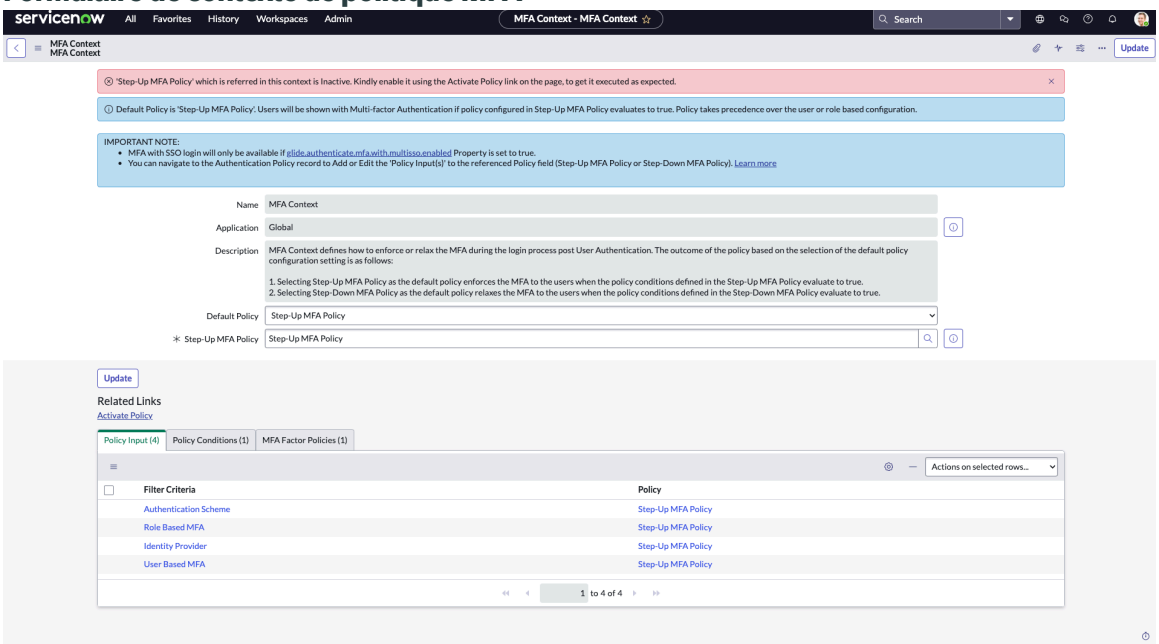
Remarque :
Les conditions de politique peuvent être créées à partir d'ici, mais comme bonne pratique, il est recommandé d'ajouter de nouvelles conditions de politique à partir de la page de politique.

Cet exemple montre un enregistrement de contexte MFA configuré à l'aide d'une politique MFA ascendante. Cette politique par défaut signifie que MFA n'est appliquée que lorsque les conditions définies dans la politique sont évaluées comme vraies. Le contexte utilise une politique appelée **politique MFA ascendante**.
Cette politique comporte un ensemble d'entrées et de conditions qui s'affichent dans les onglets **Entrée de politique** et **Condition de politique** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de contexte de politique MFA



Contexte de récupération de compte

Le contexte de récupération de compte utilise une politique pour définir comment et quand la récupération de compte peut être établie.

Les administrateurs peuvent afficher et modifier ce contexte et sa politique associée en accédant à **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Contexte de récupération de compte**.

> **Remarque :**
> Par défaut, la politique est **définie sur Autoriser la politique**. La connexion pour les utilisateurs est limitée par défaut et la connexion n'est autorisée que si les conditions définies dans la **politique d'acceptation** sont évaluées comme vraies.

Utilisez les champs dans l'enregistrement de contexte de récupération de compte pour définir la façon dont votre instance utilise la politique.

Formulaire de contexte de récupération de compte

Champ	Description
Nom	Nom du contexte de la politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez une option parmi les suivantes : • Autoriser la politique • Refuser la politique
Autoriser la politique	Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

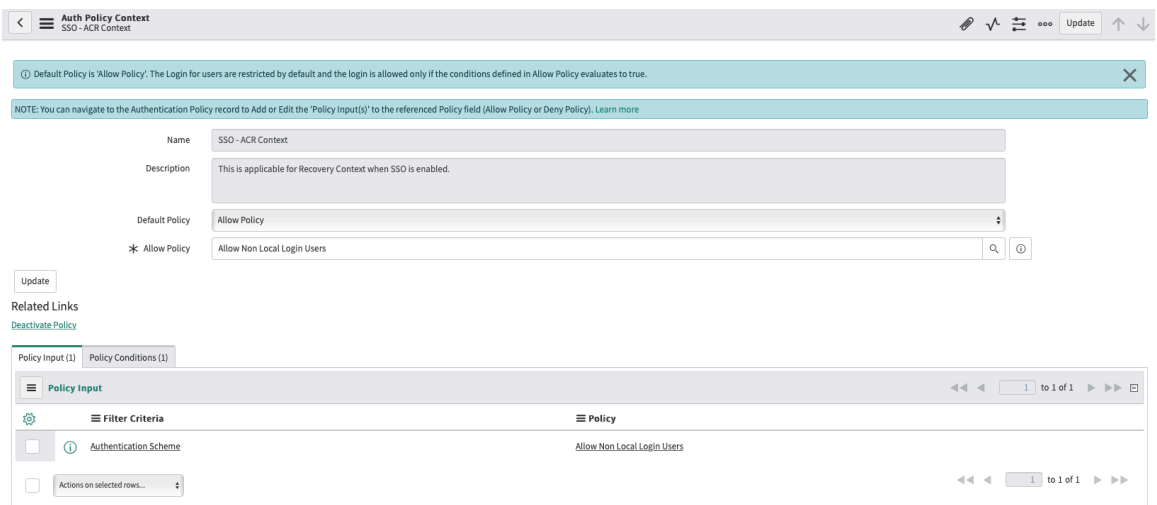
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et conditions de la politique sélectionnées dans le champ Autoriser la **politique** ou Refuser la **politique** . Ces onglets servent de référence, mais ne peuvent pas être utilisés pour modifier les entrées ou les conditions de la politique. Pour modifier les paramètres de votre politique, accédez à la politique à l'aide de l'icône **Afficher l'aperçu de cet enregistrement** en regard du champ **Autoriser la politique** ou **Refuser la politique** .

Remarque :
Les conditions de politique peuvent être créées à partir d'ici, mais comme bonne pratique, il est recommandé d'ajouter de nouvelles conditions de politique à partir de la page de politique.



Contexte de validation de la session

Utilisez le contexte de validation de session comme couche supplémentaire de protection contre le détournement de session ou de cookie.

Vous pouvez utiliser le contexte de validation de session avec le cadre de travail des Authentification adaptative politiques. Le cadre de travail utilise des politiques d'authentification pour évaluer les demandes d'authentification, puis refuse ou autorise l'accès en fonction des entrées et des conditions de la politique.

La politique de contexte de validation de session peut être utilisée conjointement avec la politique de post-authentification, où un administrateur peut appliquer des restrictions IP à certains ou à tous les utilisateurs pendant la session connectée.

La fonctionnalité Contexte de validation de session évalue les adresses IP en fonction des conditions que vous définissez et autorise l'accès à l'instance au sein d'une session. Les résultats du contexte de validation de la session sont les suivants :

- Refuser la politique : sélectionner la politique de refus d'accès comme politique par défaut permet aux utilisateurs de poursuivre la session par défaut. La session n'est interrompue que lorsque l'une des conditions de politique définies dans la politique de refus d'accès est évaluée comme vraie.
- Autoriser la politique : sélectionner la politique d'accès comme politique par défaut met fin immédiatement à la session utilisateur, sauf si l'une des conditions de politique définies dans la politique d'autorisation d'accès est évaluée comme vraie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le contexte de validation de session pour une politique d'authentification est défini sur **Autoriser la politique** par défaut.
- Le contexte de validation de session est implémenté via la politique d'autorisation. Il n'est pas recommandé de définir le contexte sur refuser la politique.

Le contexte de validation de session fonctionne selon le mécanisme suivant :

- Capture l'adresse IP de l'utilisateur lors de la création de session à partir de la demande de l'utilisateur et la stocke dans la session et la base de données.
- Rejette une demande lorsque son adresse IP diffère de celle de la session ou en dehors des plages IP valides définies par le client que vous avez définies.

Remarque :

Le contexte de validation de la session est le suivant :

- Disponible uniquement pour les utilisateurs authentifiés.
- Ne s'applique pas aux sessions d'utilisateurs invités ou aux applications mobiles natives.
- Facultative et basée sur l'exigence qu'elle puisse être configurée.
- Exécuté uniquement pour les demandes post-connexion.

Avantages de la validation de session

Le contexte de validation de session présente les avantages suivants :

- Restreint l'accès lorsque ServiceNow® les pirates de l'air copient les cookies de session d'un utilisateur d'un appareil à un autre pour emprunter l'identité de la session.
- Restreint l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.
- Configure les différentes règles et plages d'adresses IP par groupe d'utilisateurs ou par rôle pour les connexions des utilisateurs.

Enregistrement de contexte de validation de session

Les politiques dans le contexte de validation de session exécutent des demandes post-connexion.

Utilisez les champs de l'enregistrement de contexte de la politique de validation de session pour définir la façon dont votre instance utilise votre politique.

Formulaire de contexte de validation de session

Champ	Description
Nom	Nom du contexte de la politique. Ce champ est statique et ne peut pas être modifié.
Description	Description du contexte.
Politique par défaut	Définit le comportement par défaut de ce contexte lors de l'évaluation de la politique. Sélectionnez l'une des options suivantes. **Autoriser la politique**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de contexte de validation de session (suite)

Champ	Description
	Refuse l'accès à tous les utilisateurs par défaut et n'autorise l'accès que lorsque les conditions du champ **Politique d'autorisation** sont évaluées comme vraies. **Refuser la politique** Permet l'accès à tous les utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions du champ **Politique de refus** sont évaluées comme vraies.
Autoriser la politique	Politique utilisée pour ce contexte. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Autoriser la politique**.
Refuser la politique	Politique utilisée pour ce contexte. Ce champ s'affiche uniquement lorsque le champ **Politique par défaut** est défini sur **Refuser la politique**.

Vous pouvez choisir la **politique de validation** de session en tant que politique d'autorisation ou refuser la politique en fonction de l'entrée et des conditions de la politique.

Remarque :

Vous ne pouvez utiliser que les critères de filtre d'adresse IP, de rôle et de groupe pour la politique de validation de session.

Entrées et conditions de la politique

Les onglets **Entrée de politique** et **Conditions de politique** affichent les entrées et conditions de la politique sélectionnées dans le champ Autoriser la **politique** ou Refuser la **politique** . Ces onglets servent de référence ; mais ils ne peuvent pas être utilisés pour modifier les entrées ou les conditions de politique. Pour modifier votre politique, accédez à la politique à l'aide de l'icône de référence (ⓘ) en regard du champ **Autoriser la politique** ou **Refuser la politique** .

Activer le contexte de validation de session

Utilisez le contexte de validation de session pour restreindre l'accès lorsque ServiceNow® les pirates de l'air copient les cookies de session d'un utilisateur d'un appareil à un autre pour emprunter l'identité de la session ou restreignent l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.

Avant de commencer
Rôle requis : administrateur

Pour utiliser la validation de session, vous devez effectuer les étapes suivantes :

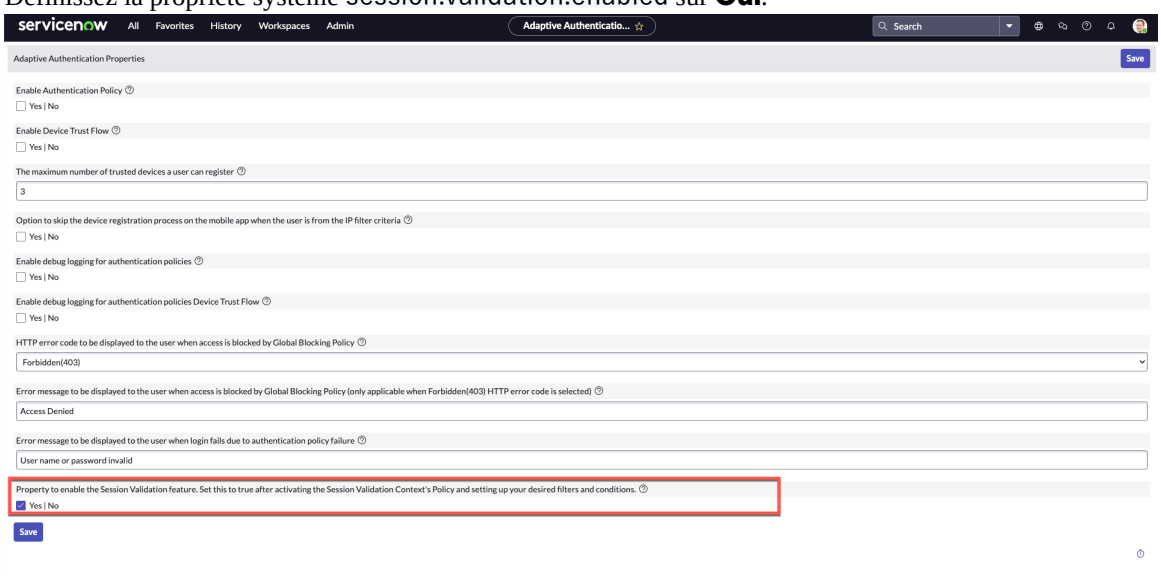
Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.
2. Sélectionnez la **politique de validation** de session sur la page Politiques (sys_authentication_policy_list.do).
3. Spécifiez les **entrées et les** conditions de **la politique**.
4. Définissez les conditions sur **vrai** ou **faux** pour les filtres que vous avez ajoutés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Cochez la case **Actif** pour activer la politique une fois que vous avez configuré la validation de session La politique est configurée avec les entrées et conditions de la politique.
6. Cochez la case **Forcer l'AuthnRequest** pour le fournisseur d'identité par défaut dans la table sso_properties si la SSO est configurée pour l'instance.
7. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.
8. Définissez la propriété système session.validation.enabled sur **Oui**.



Résultats

La fonction de validation de session est activée. Vous pouvez configurer les entrées et les conditions de la politique pour utiliser la fonctionnalité. Pour en savoir plus, consultez Didacticiel : Configuration de la validation de session.

Didacticiel : Configuration de la validation de session

Configurez la validation de session dans le cadre de travail d'authentification adaptative pour fournir une couche supplémentaire de protection contre le détournement de session ou de cookie.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : **Adaptive Authentication** (com.snc.adaptive_authentication)

Pour configurer la validation de session, vous devez effectuer les étapes suivantes :

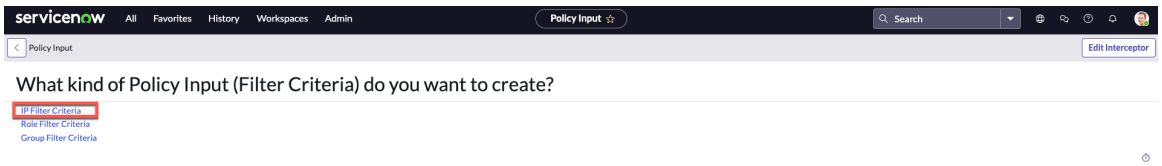
Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.
2. Sélectionnez la **politique de validation** de session sur la page Politiques (sys_authentication_policy_list.do).
3. Sélectionnez **Entrées de politique**.
   a. Sélectionnez **Nouveau** ou **Modifier**.
   b. Choisissez le type d'entrée de politique (critères de filtrage) que vous souhaitez créer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les options disponibles sont l'adresse IP, le rôle et les critères de filtre de groupe. Choisissons **Critères de filtre**



IP.

c. Remplissez le formulaire avec les détails du filtre et fournissez la **plage IP**.



Pour en savoir plus sur la création d'un filtre IP, reportez-vous à la section Créer des critères de filtre IP.

d. Sélectionnez **Soumettre**.

4. Sélectionnez **Conditions de politique** sur la page Politique de validation de session.

a. Sélectionnez **Nouveau**.

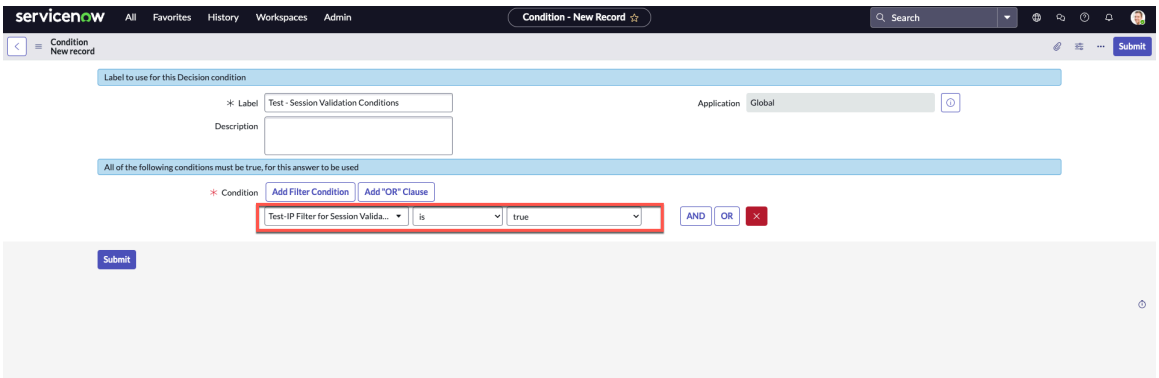
b. Remplissez le formulaire et définissez la condition pour l'entrée de politique.

Traduction automatique

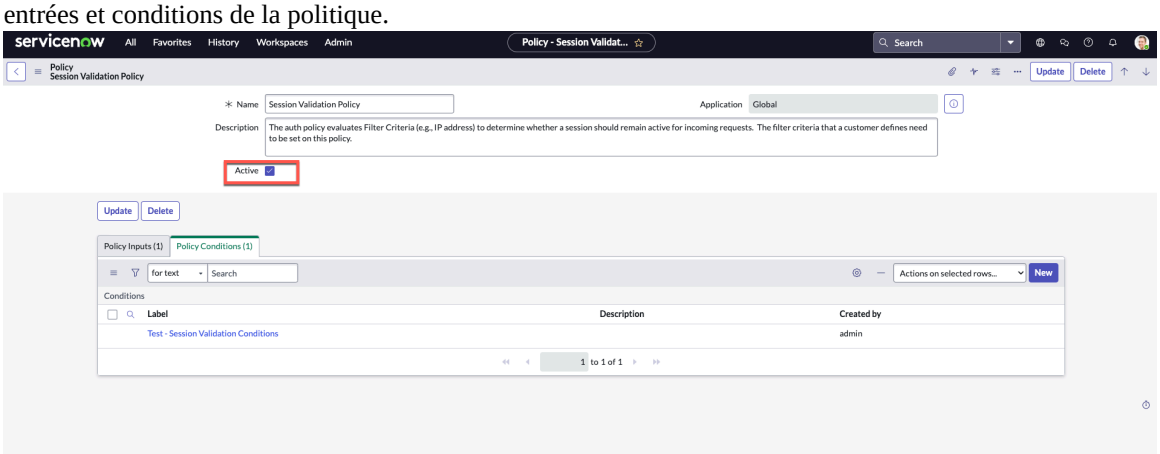
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

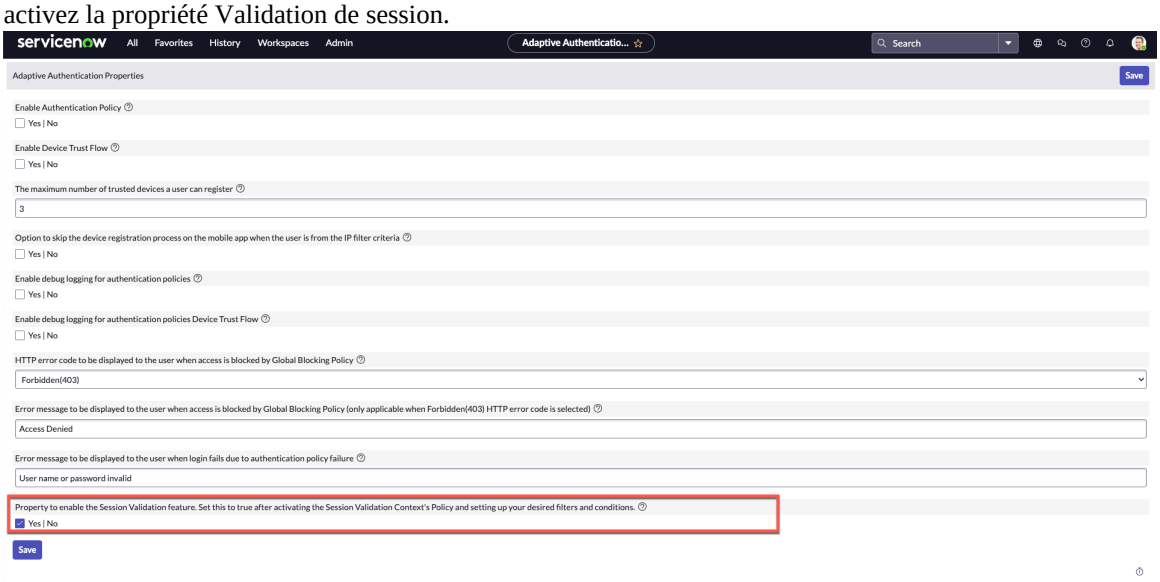
Vous pouvez définir les conditions sur vrai ou faux en fonction de la configuration de l'entrée de politique. Dans cet exemple, elle est définie sur true. Dans ce cas, la définition de la condition sur vrai permet uniquement à l'utilisateur avec l'adresse IP configurée de se connecter.



5. Cochez la case Actif pour activer la politique une fois la politique de validation de session configurée avec les entrées et conditions de la politique.



6. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés** et activez la propriété Validation de session.



7. Accédez à la **Tout** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de validation de la session**.

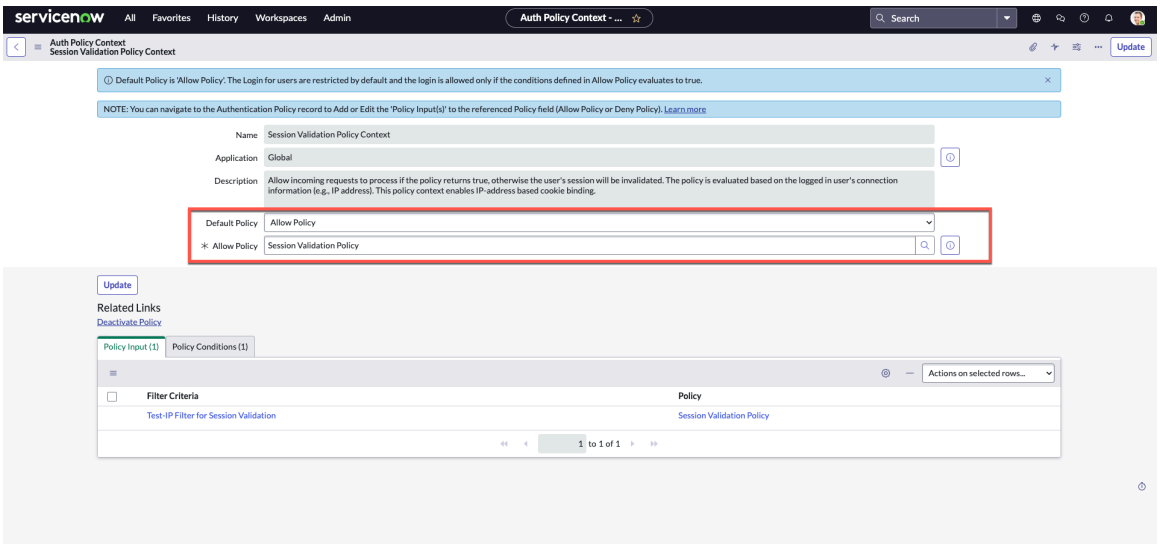
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Définissez la politique par défaut sur **Autoriser la politique** ou **Refuser la politique** pour définir le contexte de validation de session en fonction de l'entrée et des conditions de la politique.

Remarque :
Par défaut :

- Le contexte de validation de la session est défini sur **Autoriser la politique**.
- La politique d'autorisation est sélectionnée en tant que **politique de validation de session**.



Résultats
La configuration évalue la session de connexion en fonction des éléments suivants :

- Restreint l'accès à l'instance ServiceNow® lorsque les pirates de l'air copient les cookies de session d'un utilisateur d'un appareil à un autre pour emprunter l'identité d'une session.
- Restreint l'accès à la session de l'utilisateur s'il utilise un réseau non sécurisé.

Politiques d'authentification

Les politiques d'authentification évaluent les demandes d'authentification en fonction des conditions de politique spécifiées et autorisent ou refusent l'accès en fonction du résultat de l'évaluation des conditions de politique. Par exemple, l'accès n'est autorisé que si toutes les conditions de politique spécifiées dans la **politique d'accès** sont définies sur vrai.

Utilisez les politiques d'authentification intégrées ou créez une politique d'authentification en fonction de vos exigences de sécurité. Vous pouvez trouver les politiques sur votre instance en accédant à **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.

Remarque :
À tout moment, la politique d'autorisation d'accès ou la politique de refus d'accès peuvent être exécutées, mais pas les deux.

Politique	Description
Politique d'autorisation d'accès	Refuse par défaut toutes les demandes d'authentification. N'autorise que les demandes

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politique	Description
	d'authentification qui correspondent aux conditions de politique spécifiées.
Autoriser la politique de pré-authentification	Autoriser la politique de pré-authentification d'accès.
Autoriser les utilisateurs à connexion non locale	Choisissez cette politique pour autoriser les utilisateurs de connexion non locaux. Utilisé dans le contexte des flux de récupération SSO.
Refuser la politique d'accès	Autorise les demandes d'authentification par défaut. Refuse uniquement les demandes d'authentification qui correspondent aux conditions de politique spécifiées.
Politique de blocage globale	Refuse les demandes d'accès des utilisateurs et des API avant authentification. Cette politique peut être utilisée comme alternative au contrôle d'accès à l'adresse IP.
Politique de validation de session	La politique d'authentification évalue les critères de filtre (par exemple, l'adresse IP) pour déterminer si une session doit rester active pour les demandes entrantes. Vous devez définir les critères de filtrage sur cette politique.
Politique de refus de la connexion locale	Choisissez cette stratégie pour bloquer toutes les connexions locales. Utilisé dans le contexte des flux de récupération SSO.
Politique MFA descendante	Choisissez la **politique MFA descendante** comme politique par défaut dans les situations où les utilisateurs n'ont pas besoin d'authentification MFA. Lorsque les conditions de politique définies dans la politique MFA ascendante sont évaluées comme vraies, les utilisateurs ne sont pas tenus de se connecter à l'aide de la MFA.
Politique MFA ascendante	Choisissez la **politique MFA ascendante** comme politique par défaut pour exiger l'authentification MFA lorsque les conditions de politique définies dans la politique MFA ascendante sont évaluées comme vraies.

Traduction automatique

Configurer une politique d'authentification

Configurez une politique d'authentification pour définir les entrées et les conditions à utiliser pour accorder l'accès à une instance ou appliquer l'authentification multifacteur.

Avant de commencer

Rôle requis : administrateur

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.

   Remarque :
   Pour voir des exemples de politiques terminées, vous pouvez examiner ces politiques sur votre instance :

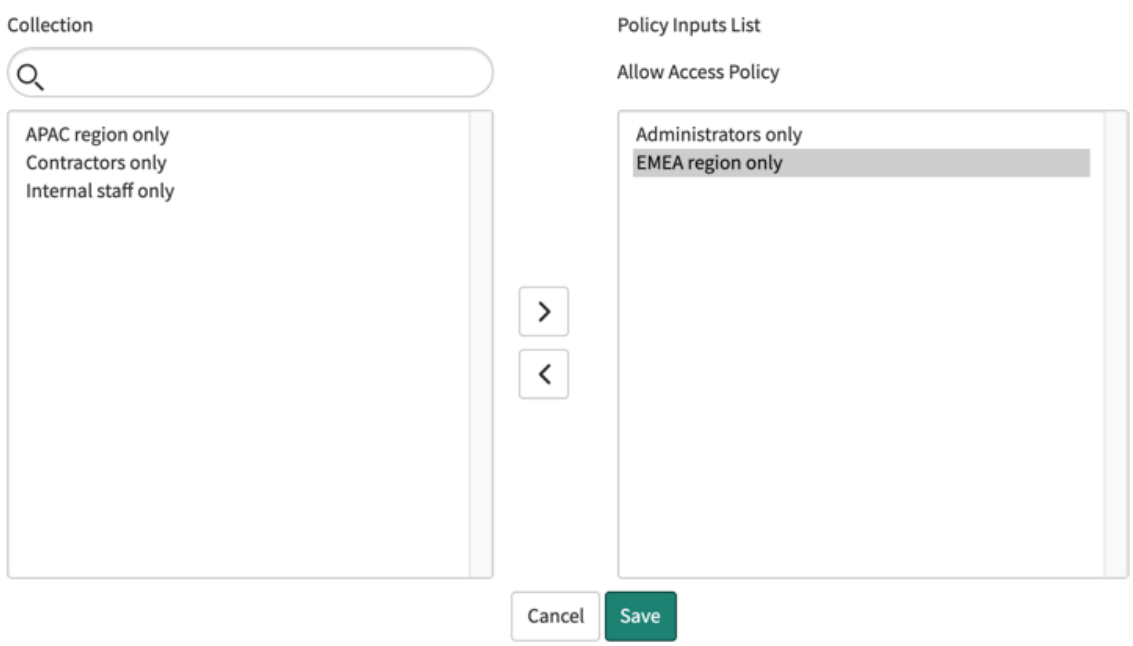
   - POLITIQUE DE DÉMONSTRATION : autoriser la connexion locale pour les administrateurs à partir de la plage d'adresses IP de confiance uniquement
   - POLITIQUE DE DÉMONSTRATION : autoriser la connexion locale pour les administrateurs uniquement
   - POLITIQUE DE DÉMONSTRATION : restreindre l'authentification basée sur le nom d'utilisateur et le mot de passe pour des utilisateurs spécifiques

2. Cliquez sur le bouton **Nouveau** pour créer un enregistrement de politique.
3. Renseignez les champs du formulaire **Politique** .

Formulaire de police

Champ	Description
Nom	Nom de votre politique.
Application	Application incluse dans le périmètre de la politique. Ce champ est renseigné automatiquement avec l'application actuelle.
Description	Description de la politique
Actif	Indique si la politique est active.

4. Dans l'onglet **Entrées de politique** , cliquez sur **Modifier**.
5. Sélectionnez un ou plusieurs critères de filtre dans la liste **Collection** et **déplacez-les vers la liste Entrées de politique** de la liste **Politique d'autorisation d'accès** .



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour plus d'informations sur la création de vos propres critères de filtre à utiliser dans cette section, reportez-vous à la section Critère de filtre.

6. Dans l'onglet **Conditions de politique** , cliquez sur **Nouveau**.
7. Renseignez les champs suivants du formulaire :

Formulaire Condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtrage) qui est utilisée pour évaluer les demandes d'authentification. Par exemple, vous pouvez créer des conditions qui n'autorisent que les prestataires d'une liste d'adresses IP fiables.

8. **Facultatif :** Répétez l'étape 7 pour créer des conditions de politique supplémentaires.

Remarque :
Si vous créez plusieurs conditions de politique, le résultat final de la politique d'accès dépend de la sortie logique OU de toutes les conditions de politique. Cela signifie que la police sera évaluée comme vraie si l'une de vos conditions de police est remplie.

9. Cliquez sur **Enregistrer**.

Ajouter une politique d'authentification à un contexte de politique d'authentification

Ajoutez une politique d'authentification à l'un des contextes de politique d'authentification. Le contexte d'authentification utilise les entrées et conditions de la politique pour déterminer si les usages bénéficient d'un accès à l'instance ou si la MFA est appliquée pour vos utilisateurs.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Contextes de politique d'authentification**, puis sélectionnez l'une des entrées en fonction de vos besoins.

Contexte de pré-authentification

Utilisez le contexte de préautorisation pour évaluer votre politique avant que l'utilisateur ne voie l'écran de connexion. L'accès est accordé ou refusé aux utilisateurs en fonction de cette évaluation.

Contexte de post-authentification

Utilisez le contexte de post-autorisation pour évaluer votre politique une fois que l'utilisateur a entré ses informations d'identification de connexion. L'accès est accordé ou refusé aux utilisateurs en fonction de cette évaluation. Étant donné que cette évaluation a lieu une fois

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que l’instance a identifié l’utilisateur, les politiques de ce contexte peuvent effectuer leur évaluation en fonction des données utilisateur, telles que leur rôle ou leur groupe.

Contexte MFA

Utilisez le contexte MFA pour déterminer si un utilisateur doit utiliser l’authentification multifacteur lors de la connexion.

Contexte de validation de la session

Utilisez le contexte de validation de session pour évaluer l’adresse IP qui est définie en fonction des conditions définies comme un filtre et qui autorise l’accès à l’instance au sein d’une session.

2. Dans le champ **Politique par défaut** , sélectionnez une valeur.
   La valeur de ce champ détermine la façon dont le contexte utilise le résultat des conditions de votre politique.

   Les options disponibles dans ce champ dépendent du contexte sélectionné. Pour plus de détails sur ces contextes, reportez-vous à la section Contextes de politique d’authentification.

3. Affectez une politique au contexte.
   Le nom du champ dépend du contexte que vous avez sélectionné.

   Contexte de pré-authentification et de post-authentification

   Ces contextes disposent d’un champ **Refuser la politique** ou **Autoriser la politique** , en fonction de la sélection dans le champ **Politique par défaut** .

   Contexte MFA

   Ce contexte comporte un champ **Politique MFA ascendante** ou **Politique MFA descendante** , en fonction de la sélection dans le champ Politique par **défaut** .

   Contexte de validation de session

   Ce contexte comporte un champ **Autoriser la politique** ou **Refuser la politique** , en fonction de la sélection dans le champ Politique par **défaut** .

4. Cliquez sur **Mettre à jour**.
   Après avoir mis à jour l’enregistrement, vous pouvez consulter les entrées et les conditions de votre politique dans les onglets **Entrée de politique** et **Conditions de politique** .

Événements d'authentification adaptative

Vous pouvez utiliser la table des événements d’authentification adaptative pour connaître les événements.

Voici quelques-uns des journaux qui peuvent être suivis dans la table des événements d’authentification adaptative :

- `glide.adaptive.auth.log.success.event` : pour connaître les événements de `réussite` pour les connexions post-authentification et API.
- `glide.adaptive.auth.log.mfa.relax.event` : pour connaître les `événements mfa_relaxation` pour le contexte MFA.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Pour le contexte de pré-authentification, les politiques d'accès API REST de type « pre_auth » : par défaut, les événements d'échec sont consignés. Les événements de réussite ne peuvent pas être consignés.
- Pour le contexte de post-authentification, les politiques d'accès API REST de type autre que « pre_auth » : par défaut, les événements d'échec sont consignés. Pour que les événements de réussite soient consignés, vous devez activer la propriété glide.adaptive.auth.log.success.event .
- Pour MFA : par défaut, les événements d'application de la MFA sont consignés.
- Pour que les événements MFA Relaxation soient consignés, vous devez activer la propriété glide.adaptive.auth.log.mfa.relax.event . L'assouplissement MFA consignerait le même événement que l'application MFA, mais avec le champ de résultat renseigné avec Faux.

Configurer les propriétés d'Authentification adaptative

Après avoir activé l'authentification adaptative, configurez les propriétés d'authentification adaptative en fonction de vos exigences de sécurité.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.
2. Configurez ces propriétés :

Propriétés d'Authentification adaptative

Propriété	Description	Valeur
Activer la politique d'authentification (glide.authenticate.auth.policy.enabled)	Option permettant d'activer la politique d'authentification.	Oui | Non
Activer la journalisation du débogage pour les politiques d'authentification (glide.authenticate.policy.debug)	Option permettant d'activer la journalisation de débogage pour les politiques d'authentification.	Oui | Non
Code d'erreur HTTP à afficher l'utilisateur lorsque l'accès est bloqué par la politique de blocage globale (glide.authenticate.global.blocking_policy.error_code)	Code d'erreur HTTP qui s'affiche pendant la connexion lorsque la politique de blocage globale bloque la connexion d'un utilisateur.	Sélectionner à partir de : ○ Interdit(403) ○ Introuvable(404)
Message d'erreur à afficher à l'utilisateur lorsque l'accès est bloqué par la politique de blocage globale (applicable uniquement si le code d'erreur HTTP 403 Forbidden est sélectionné) (glide.authenticate.global.blocking_policy.error_message)	Message d'erreur qui s'affiche lorsque la politique de blocage globale bloque l'accès.	Champ de texte
Activer le flux de confiance de l'appareil (glide.authenticate.preauth.allow.trusted.device)	Option permettant d'activer le flux d'appareils de confiance.	Oui | Non
Nombre maximal d'appareils de confiance qu'un utilisateur peut enregistrer (glide.trusted.device.max.count)	Il s'agit du nombre maximal d'appareils de confiance qu'un utilisateur peut enregistrer.	Champ de texte

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description	Valeur
Ignorer l'inscription de l'appareil pour le flux de confiance de l'appareil si l'utilisateur provient du réseau approuvé (glide.authenticate.preauth.skip.user.registration)	Option permettant d'ignorer l'inscription si l'utilisateur tente de s'inscrire à partir du réseau approuvé	Oui | Non
Propriété permettant d'activer la fonctionnalité de validation de session. Définissez-la sur vrai après avoir activé la politique du contexte de validation de session et configuré les filtres et conditions souhaités (session.validation.enabled)	Option permettant d'activer la fonctionnalité de validation de session. Définissez-la sur vrai après avoir activé la politique du contexte de validation de session et configuré les filtres et conditions souhaités.	Oui | Non

Didacticiel : Configurer Authentification adaptative

Utilisez ces exemples d'étapes pour configurer Adaptive Authentication sur une instance.

Pour utiliser ce didacticiel, vous devez disposer d'une instance sur laquelle l'authentification adaptative est activée. Pour obtenir des détails sur ce processus, consultez Activer Authentification adaptative.

Cet exemple vous guide dans la création d'une nouvelle stratégie et son application à une instance. Dans ce didacticiel, vous allez :

Créer un enregistrement de critères de filtre

Créez un enregistrement de critères de filtre de groupe à utiliser comme entrée pour votre politique. Cet enregistrement permet à votre politique de déterminer l'accès en fonction du groupe d'un utilisateur. Au cours de ces étapes, vous définissez le ou les groupes que la politique utilise pour déterminer l'accès.

Créer une politique

Créez une politique qui détermine si un utilisateur peut accéder à l'instance. Cette politique utilise l'enregistrement de critères de filtre de groupe que vous créez comme entrée. Au cours de ces étapes, vous définissez également les conditions de politique qui définissent la manière dont la politique utilise l'entrée de politique pour déterminer l'accès des utilisateurs.

Configurer un contexte de politique

Configurez le **contexte de la politique de post-authentification** pour utiliser votre nouvelle politique. Lors de la configuration, votre instance refuse l'accès aux utilisateurs du groupe défini dans l'enregistrement de critères de filtrage.

Créer un enregistrement de critères de filtre

Découvrez comment créer un enregistrement de critères à utiliser comme entrée de politique pour votre politique d'authentification adaptative.

Avant de commencer

Rôle requis : administrateur

Pour refuser l'accès à votre instance en fonction des groupes d'utilisateurs, vous devez créer un enregistrement de critères de filtre de groupe. Cet enregistrement définit un groupe d'utilisateurs ou un ensemble de groupes d'utilisateurs auxquels votre politique peut accorder ou refuser l'accès. Dans cet exemple, vous allez créer un enregistrement de critères de filtre de groupe pour un seul groupe d'utilisateurs.

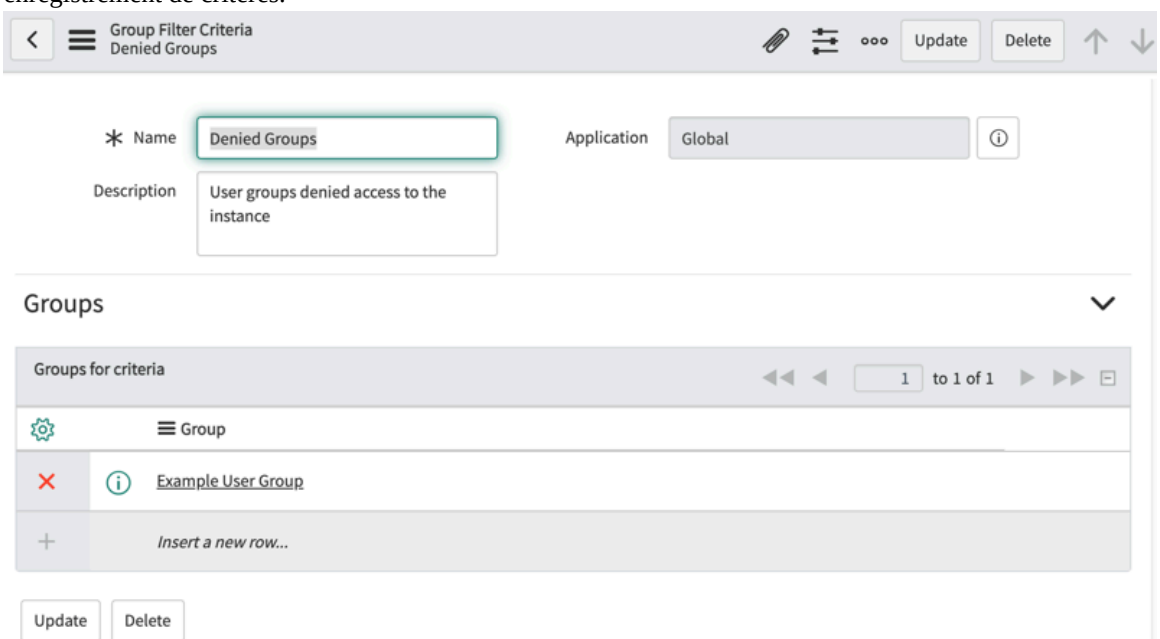
Pour en savoir plus sur les groupes d'utilisateurs et leur utilisation dans votre instance, reportez-vous à la section Exploring user administration .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Critère de filtre** > **Critères de groupe**.
2. Cliquez sur **Nouveau** et créez un enregistrement.
3. Dans le champ **Nom** , donnez un nom à votre enregistrement.
   Par exemple, Groupes refusés.
4. Dans le champ **Description** , saisissez une description brève.
   Par exemple, des groupes d'utilisateurs ont refusé l'accès à l'instance.
5. Dans la liste **Groupe pour les critères**, double-cliquez sur **Insérer une nouvelle ligne...**
6. Entrez le nom d'un groupe d'utilisateurs ou cliquez sur l'icône de référence ( ) pour sélectionner un groupe dans une liste.
   Si vous souhaitez créer un nouveau groupe d'utilisateurs pour vos critères de filtrage, cliquez sur l'icône de référence (icône), puis sur le bouton **Nouveau** . Pour plus d'informations sur la création de groupes d'utilisateurs, consultez Créer un groupe d'utilisateurs .
7. Une fois que vous avez ajouté votre groupe d'utilisateurs, cliquez sur **Envoyer** pour enregistrer votre enregistrement de critères.



Créer une politique

Découvrez comment créer une politique de refus d'accès aux groupes d'utilisateurs définis dans les critères de filtrage de votre groupe.

Avant de commencer

Rôle requis : administrateur

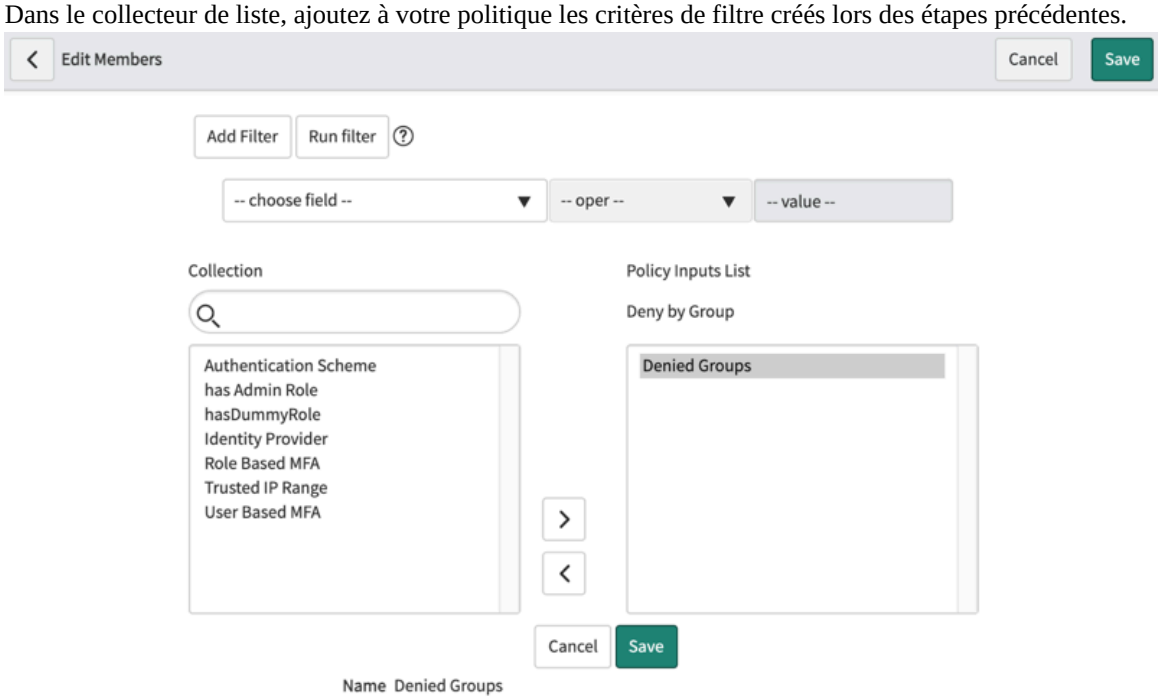
Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Toutes les politiques**.
2. Dans la liste **Stratégies** , cliquez sur **Nouveau**.
3. Dans le champ **Nom** , donnez un nom à votre enregistrement.
   Par exemple, Refuser par groupe.

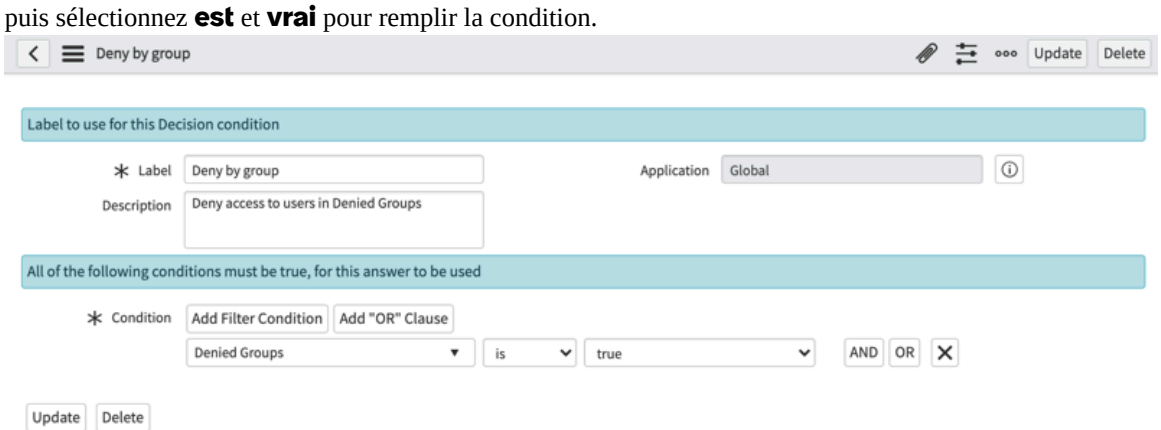
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Dans le champ **Description** , saisissez une description brève.
   Par exemple, des groupes d'utilisateurs ont refusé l'accès à l'instance.
5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer**.
   Après enregistrement, les listes **Entrées de politique** et **Conditions de politique** s'affichent sur le formulaire.
6. Dans la liste **Entrées de la politique** , cliquez sur **Modifier**.
7. Dans le collecteur de liste, ajoutez à votre politique les critères de filtre créés lors des étapes précédentes.



8. Cliquez sur **Enregistrer**.
   L'instance enregistre l'entrée de politique et affiche à nouveau l'enregistrement de politique.
9. Dans la liste **Conditions de politique** , cliquez sur **Nouveau**.
10. Dans le champ **Étiquette** , créez une étiquette pour cette condition, par exemple Refuser par groupe.
11. Dans le champ **Description** , saisissez une description brève.
    Par exemple, Refuser l'accès aux utilisateurs des groupes refusés.
12. Dans le champ **Condition** , sélectionnez les critères de filtre que vous avez créés lors des étapes précédentes, puis sélectionnez **est** et **vrai** pour remplir la condition.



13. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer un contexte de politique

Configurez le contexte de la politique de post-authentification pour utiliser votre nouvelle politique. Lors de la configuration, votre instance refuse l'accès aux utilisateurs du groupe défini dans l'enregistrement de critères de filtrage.

Avant de commencer
Rôle requis : administrateur

Procédure

1. **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de post-authentification**.
   Vous devez utiliser le **contexte de post-authentification** , car la stratégie utilisée dans ce didacticiel doit évaluer le groupe auquel appartient un utilisateur. Ces informations ne sont disponibles qu'une fois les informations d'identification saisies.
2. Dans le champ **Politique par défaut** , sélectionnez Refuser la politique.
   Cette sélection accorde l'accès aux utilisateurs par défaut et refuse l'accès uniquement lorsque les conditions de la politique sont évaluées comme vraies.
3. Dans le champ **Refuser la politique** , sélectionnez la politique que vous avez créée aux étapes précédentes.
4. Cliquez sur **Mettre à jour** pour enregistrer l'enregistrement du contexte de la politique.

Authentification adaptative pour les applications mobiles de confiance

Accédez à vos ServiceNow réseaux non approuvés à l'aide du Application Now Mobilefichier .

Authentification adaptative pour les applications mobiles de confiance

L'application Authentification adaptative pour les applications mobiles de confiance permet aux utilisateurs d'accéder à l'instance à l'aide ServiceNow du Application Now Mobile. L'instance est protégée derrière une limite de réseau IP approuvée.

Voici quelques-uns des scénarios dans lesquels vous devez accéder à l'instance lorsque vous êtes en dehors de votre réseau.

En tant qu'employé, vous devez accéder au Application Now Mobile Centre de services aux employés (portail) depuis l'extérieur du réseau. Le filtre Application mobile de confiance vous permet d'identifier la demande entrante provenant d'une demande de confiance Application Now Mobile liée à un compte utilisateur.

En tant qu'administrateur, vous pouvez configurer la politique. La politique permet aux utilisateurs d'enregistrer leurs équipements mobiles et d'accéder à l'instance sur un réseau approuvé.

En tant qu'utilisateur, vous pouvez enregistrer votre équipement mobile en scannant le code QR affiché sur l'instance. Après l'inscription, vous pouvez vous connecter à votre instance à partir de , Application Now Mobileà l'aide de vos informations d'identification.

Remarque :
Pour enregistrer l'appareil mobile, vous devez être sur un réseau de confiance. Après l'inscription, vous pouvez également vous connecter à l'instance à partir d'autres réseaux.

Fonctionnalités

En tant qu'administrateur, vous pouvez utiliser les fonctionnalités suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Configurez les politiques à l'aide des critères de filtre d'applications approuvées.
- Créez des conditions de politique avec un nouveau critère de filtre pour les applications mobiles approuvées.
- Prend en charge toutes les méthodes de connexion sur l'application mobile de confiance pour les utilisateurs (connexion locale, SAML, OIDC et MFA).
- Révoquer un appareil de confiance
- Ajoutez des événements de sécurité pour toutes les actions d'inscription ou de révocation des appareils. Les événements peuvent être utilisés pour notifier l'utilisateur.
- Prendre en charge les événements de sécurité pour les échecs de signature, les échecs de validation des cookies, les jetons non valides, les en-têtes ou les paramètres de requête non valides.
- Contrôlez le nombre maximal d'appareils enregistrés.
- Empêchez une nouvelle inscription d'appareil, sauf si l'utilisateur supprime un appareil déjà couplé.
- Capturez la dernière fois qu'un appareil a été utilisé.

Activer l'application mobile de confiance

Activez l'authentification adaptative avec l'application mobile de confiance en utilisant la politique d'authentification et les conditions de filtre.

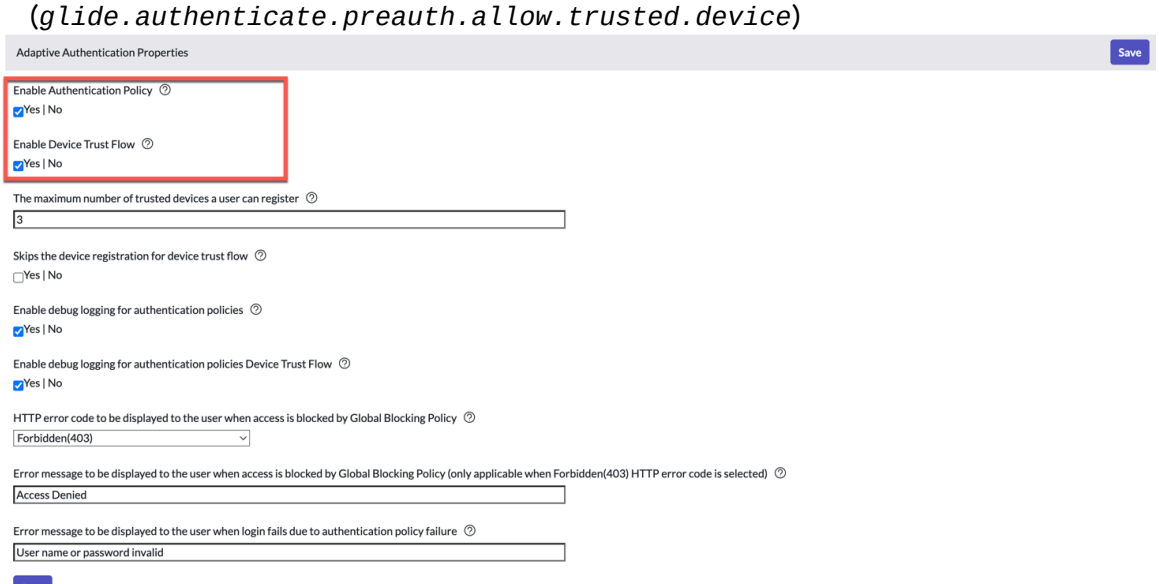
Avant de commencer

Assurez-vous que le module d'extension Authentification adaptative (`com.snc.adaptive_authentication`) est installé.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.
2. Sur la page des propriétés d'Authentification adaptative, activez les propriétés suivantes :
   - Activer la politique d'authentification (`glide.authenticate.auth.policy.enabled`)
   - Activer le flux de l'appareil de confiance (`glide.authenticate.preauth.allow.trusted.device`)



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

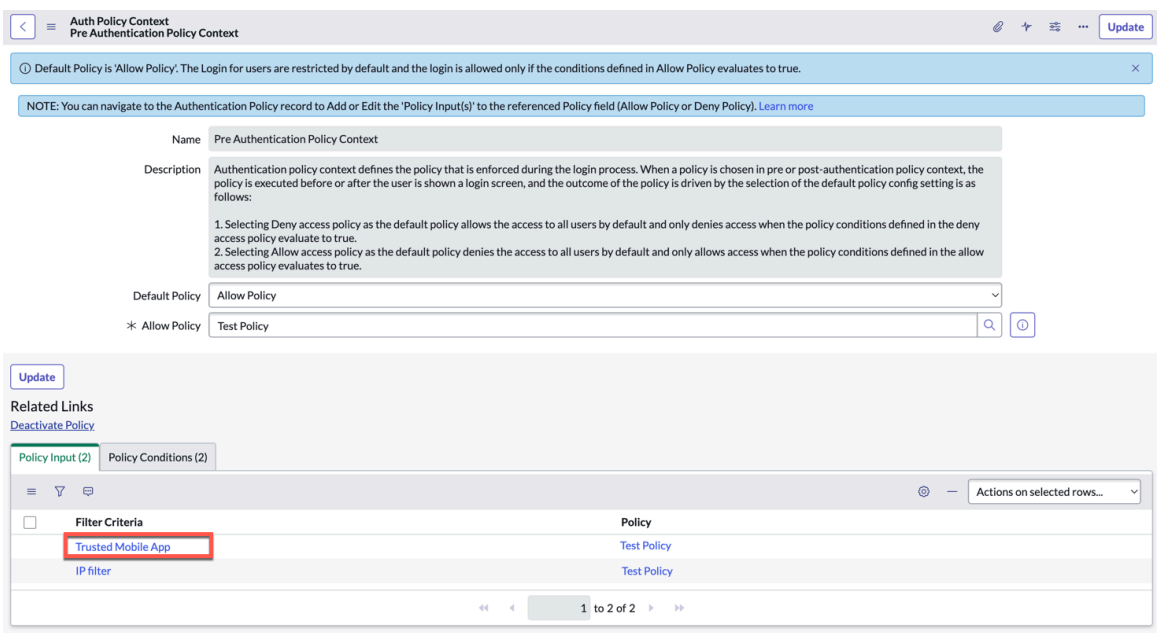
Remarque :
Pour désactiver la propriété de flux de confiance de l'appareil, vous devez supprimer les conditions avec un filtre mobile approuvé. Dans le cas contraire, un message d'erreur s'affiche pour supprimer les conditions.

3. Accédez à la **Tout** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte de pré-authentification**.
4. Définissez les conditions dans le contexte de pré-authentification.
   Pour en savoir plus, Contexte de pré-authentification.

Remarque :
Par défaut, la condition de politique est **Refuser la politique**. Vous pouvez passer à **la politique d'autorisation**. Ces politiques sont aux antipodes l'une de l'autre.

- Avec la **politique d'autorisation**, l'accès est refusé par défaut à tous les utilisateurs, et elle n'autorise l'accès que lorsque les conditions de la politique d'autorisation d'accès sont vraies.
- Avec la **politique de refus,** tous les utilisateurs sont autorisés à accéder par défaut et l'accès n'est refusé que lorsque les conditions de la politique de refus d'accès sont vraies.

Dans l'entrée de politique, l'entrée **de politique Application mobile de confiance** est une entrée de politique pour l'application mobile de confiance.



5. Dans les Conditions de la politique, créez la condition en cliquant sur **Nouveau**.
6. Renseignez les champs du formulaire.

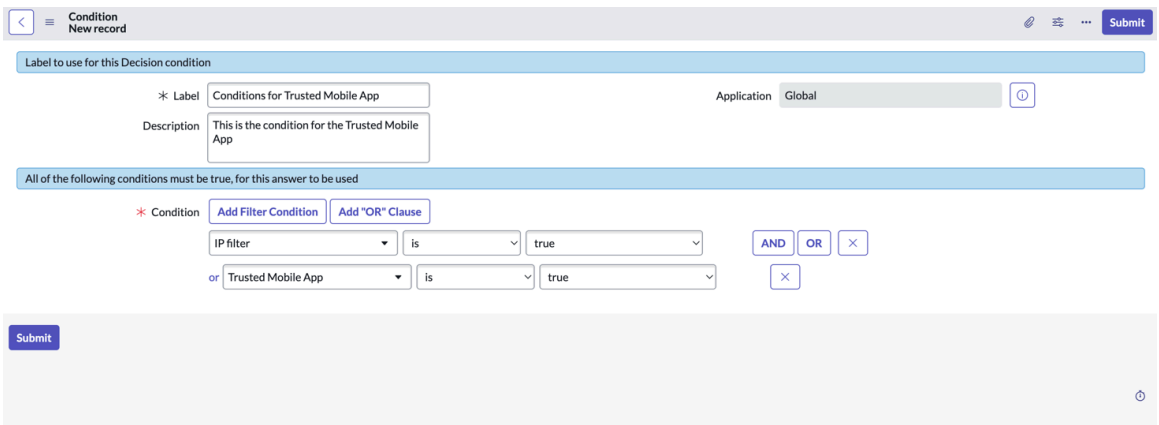
Formulaire Condition de filtre

Champ	Description
Étiquette	Nom de la condition
Description	Description de la condition

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Le périmètre de l'application pour cet enregistrement.
Condition	Conditions basées sur ET et OU. Étant donné que la politique d'authentification est définie sur **Politique d'autorisation**, la condition pour Application mobile de confiance est définie sur vrai dans l'exemple illustré sur l'image.



7. Cliquez sur **Envoyer**.

Résultats

L'entrée de politique et les conditions de filtre sont créées pour la fonctionnalité Appareil de confiance. Les utilisateurs peuvent continuer à utiliser la fonctionnalité Appareil de confiance pour accéder à l'instance à partir de réseaux non approuvés à l'aide ServiceNow de .Application Now Mobile Pour plus d'informations, consultez Enregistrer un appareil de confiance.

Enregistrer un appareil de confiance

Enregistrez un appareil de confiance pour accéder à l'instance ServiceNow en dehors du réseau.

Avant de commencer

Vous devez être dans le réseau approuvé pour effectuer l'enregistrement de l'appareil approuvé.

Rôle requis : aucun

Procédure

1. Accédez à l'une des options de menu suivantes :

- Dans le , accédez Now Platformà **Tout** > **Libre-service** > **Mon profil**.

> **Remarque :**
> Vous pouvez également accéder à votre profil en cliquant sur votre nom d'utilisateur dans l'en-tête de l'instance.

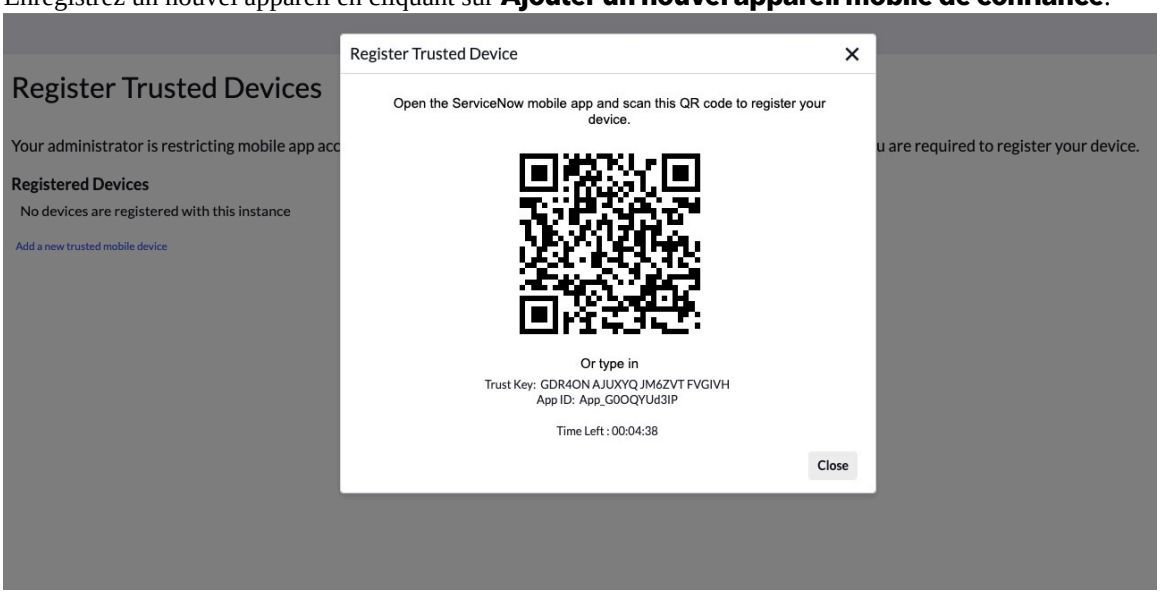
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- Sur le Now Support, cliquez sur le profil et sélectionnez **Appareil de confiance**.

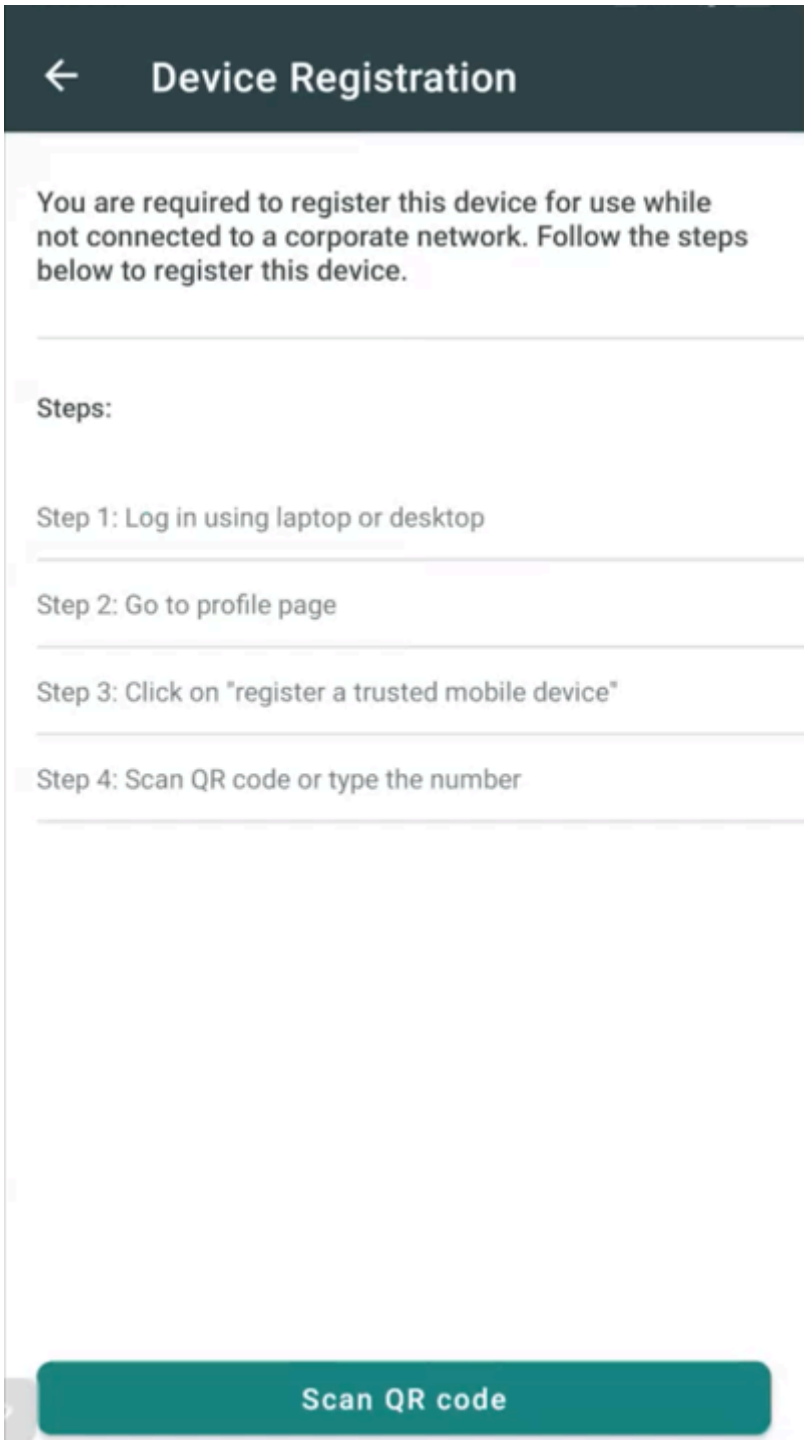
2. Dans votre profil d'utilisateur, cliquez sur **Enregistrer un appareil mobile de confiance** dans la section Liens connexes.
   La page Enregistrer les appareils de confiance s'affiche.
3. Enregistrez un nouvel appareil en cliquant sur **Ajouter un nouvel appareil mobile de confiance**.



4. Sur l'écran d'enregistrement de l'appareil de votre ServiceNow application mobile, appuyez sur le bouton **Scanner le code QR** et scannez le code QR qui s'affiche sur votre ordinateur portable ou de bureau.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



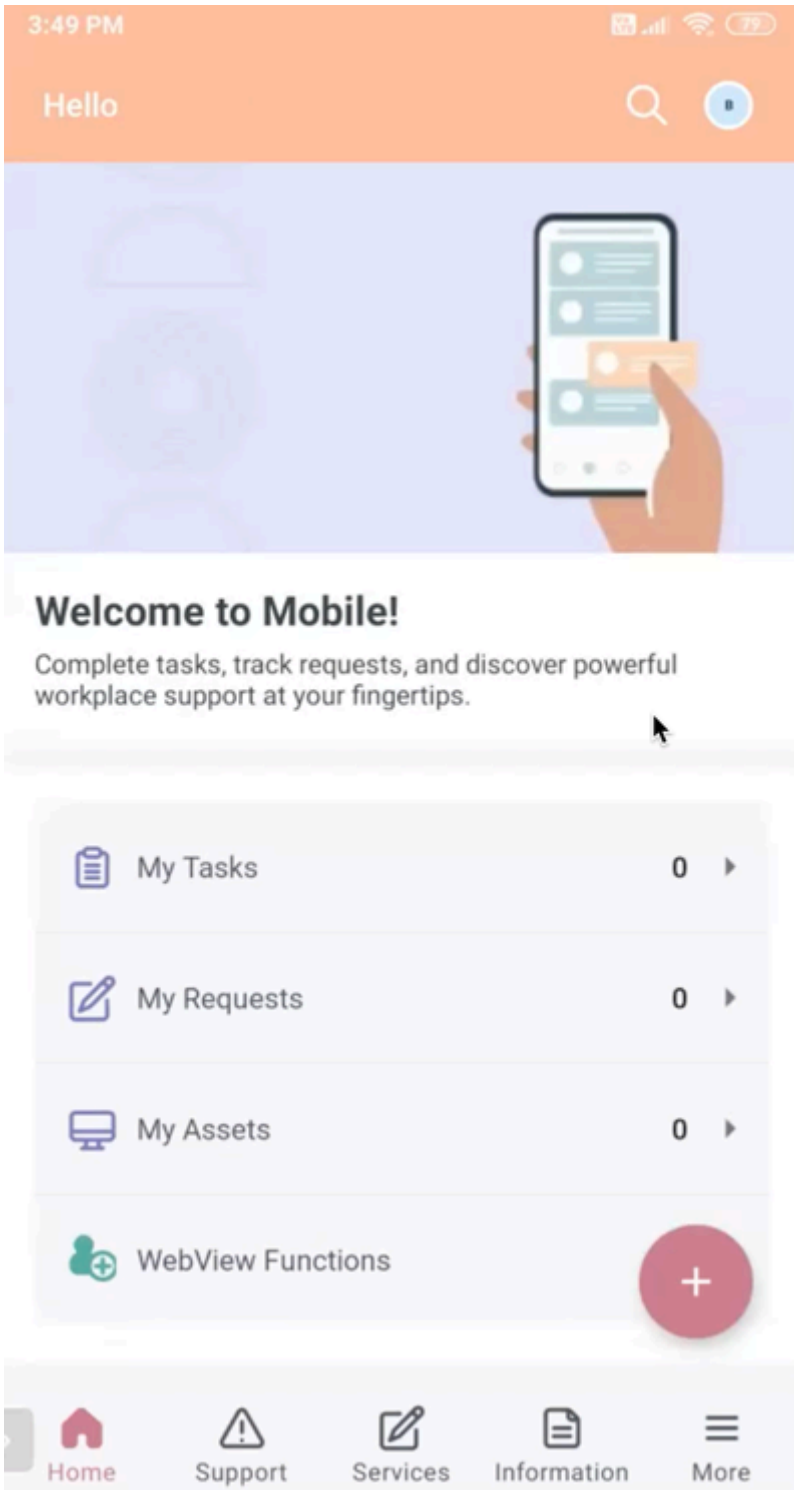
Le processus d’inscription se terminera et vous serez invité à accéder à votre page de connexion pour terminer votre authentification.

5. Spécifiez vos informations d’identification et connectez-vous au Application Now Mobile.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’écran d’accueil mobile s’affiche.



Résultats

Sur la page Enregistrer des appareils de confiance sur votre ordinateur portable ou de bureau, l’appareil enregistré s’affiche. Vous pouvez utiliser si vous souhaitez supprimer l’appareil enregistré de la page.

Que faire ensuite

Accédez à la **Tout** > **Authentification Adaptative** > **Appareil de confiance** > **Inscription du périphérique** pour afficher tous les détails de l’appareil enregistré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Gérer votre appareil de confiance

Gérez votre appareil de confiance à partir de la page d'enregistrement des appareils de confiance.

Avant de commencer

Rôle requis : aucun

Procédure

1. Accédez à l'une des options de menu suivantes :
   - Dans le , accédez Now Platformà **Tout** > **Libre-service** > **Mon profil**.

     Remarque :
     Vous pouvez également accéder à votre profil en cliquant sur votre nom d'utilisateur dans l'en-tête de l'instance.

   - Sur le Now Support, cliquez sur le profil et sélectionnez **Appareil de confiance**.
2. Dans votre profil d'utilisateur, cliquez sur **Enregistrer un appareil de confiance** dans la section Liens connexes.
   La page Enregistrer les appareils de confiance s'affiche.
3. Sur la page Enregistrer des appareils de confiance, supprimez l'appareil en cliquant sur .

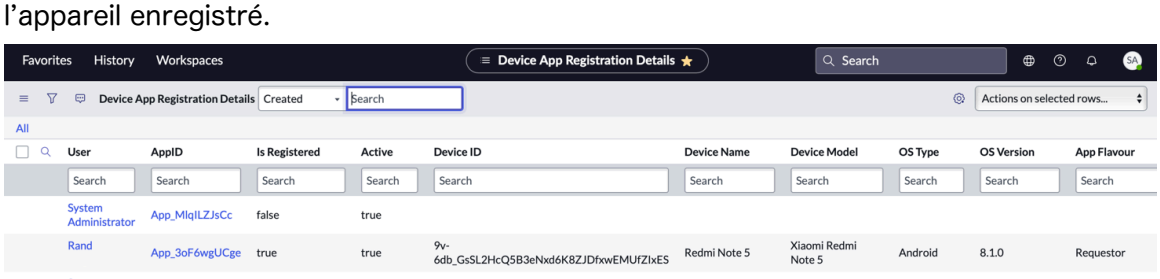
   Remarque :
   L'équipement mobile supprimé doit être enregistré à nouveau pour accéder à l'instance.

Détails d'enregistrement des appareils enregistrés

Affichez les détails des appareils enregistrés auprès de votre ServiceNow instance.

Pour afficher tous les détails de l'appareil enregistré avec l'instance, accédez à **Tout** > **Authentification Adaptative** > **Appareil de confiance** > **Inscription du périphérique**.

Utilisez le filtre pour identifier l'appareil. Cliquez sur le champ **AppID** pour en savoir plus sur l'appareil enregistré.



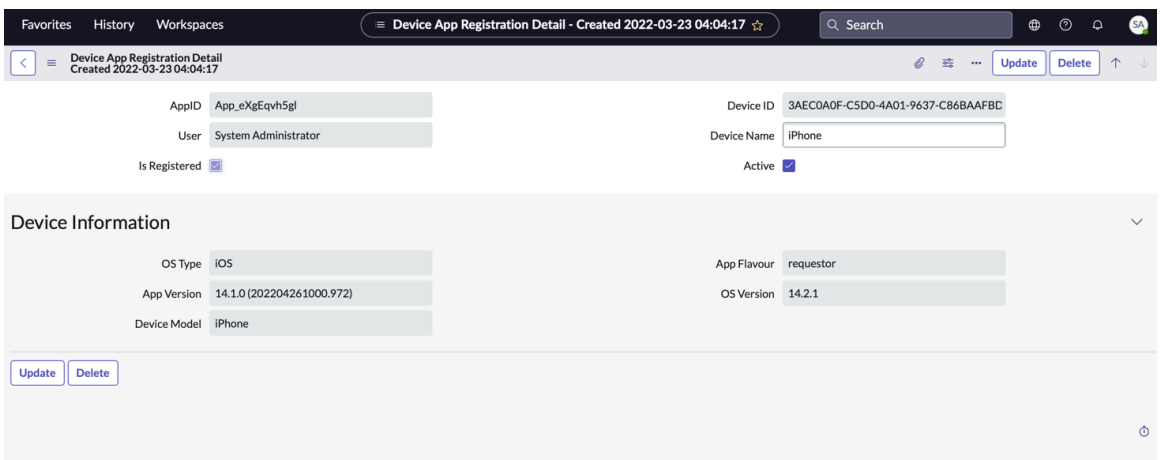
Les détails suivants s'affichent pour l'appareil :

- ID application
- ID d'équipement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilisateur
- Nom de l'équipement
- Informations sur l’appareil telles que :
  - Type de SE
  - Saveur de l'application
  - Version de l'application
  - Version de SE
  - Modèle d'équipement



Dépannage de l’application mobile de confiance

Passez en revue ces scénarios de dépannage pour résoudre les problèmes liés à l’application mobile de confiance.

Les sections suivantes décrivent certains scénarios de dépannage et les méthodes de dépannage.

Décalage horaire entre instance et mobile (décalage d’horloge)

En cas de décalage d’horloge, vous pouvez ajuster ou réinitialiser l’horloge de votre appareil mobile pour utiliser l’appareil de confiance.

Expiration du code QR dans les cinq minutes

Le code QR pour la fonctionnalité Appareil de confiance expire au bout de cinq minutes. Dans ce cas, vous pouvez cliquer pour obtenir un nouveau code QR.

Remarque :
L’expiration du code QR peut être prolongée. Pour prolonger l’expiration du code, contactez votre administrateur.

La propriété système a changé

Si la propriété système a changé, vérifiez l’inscription en fonction de la propriété système pour les informations d’identification valides qui peuvent être utilisées pour la connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nombre maximal d'appareils enregistrés

Si le nombre maximal d'inscriptions d'appareils est atteint, supprimez l'appareil existant ou contactez votre administrateur pour modifier le nombre maximal d'appareils.

Authentification API

Configurations d'authentification pour l'API.

L'authentification basée sur une API dans valide l'identité d'un utilisateur qui accède à ServiceNow®une instance, puis autorise l'utilisateur à utiliser les fonctionnalités qui correspondent au rôle ou à la fonction de l'utilisateur lorsqu'il effectue un appel d'API à l'instance ServiceNow® .

Voici les types d'authentification API dans ServiceNow®:

- Authentification basée sur certificat
- OAuth
- Authentification basée sur un jeton

Authentification basée sur certificat

L'authentification basée sur certificat vous permet d'authentifier mutuellement les demandes d'API entrantes à l'aide des certificats d'une autorité de certification (CA) approuvée.

Authentification basée sur certificat pour les services Web entrants

Authentifiez les demandes entrantes aux ServiceNow API SOAP et REST. Pour configurer l'authentification réciproque des services Web entrants, reportez-vous à la section Configurer l'authentification basée sur certificat.

OAuth

L'authentification basée sur OAuth valide l'identité du client qui tente d'établir une confiance dans le système à l'aide d'un protocole d'authentification.

OAuth 2.0 - Open Authorization est le protocole standard de l'industrie pour l'autorisation, qui utilise la simplicité des développeurs clients tout en fournissant des flux d'autorisation spécifiques pour les applications Web, les applications de bureau et les équipements mobiles.

Entrant

Créez un point de terminaison pour les clients externes qui veulent accéder à votre instance. Cela crée un enregistrement d'application cliente OAuth et génère un ID client et un secret client indiquant que le client a besoin pour accéder aux ressources restreintes sur l'instance. Pour plus d'informations, reportez-vous à la section OAuth entrant.

Authentification basée sur un jeton

Authentification basée sur les jetons pour la configuration des API REST entrantes à l'aide d'une clé API ou HMAC.

Prend en charge les jetons d'API pour les points de terminaison de l'API REST afin que l'authentification ServiceNow® utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'authentification basée sur un jeton pour la configuration des API REST entrantes peut être effectuée sur l'instance ServiceNow® avec la clé API ou le jeton HMAC.

Clé API et authentification HMAC pour les API REST entrantes

Prend en charge les jetons d'API pour les points de terminaison d'API REST afin que le nom d'utilisateur et le ServiceNow® mot de passe ne soient pas visibles dans l'URL Webhook.

Activez l'authentification basée sur la clé API pour authentifier en toute sécurité l'URL du webhook entrant.

Pour utiliser la clé API et l'authentification HMAC, vous devez installer le (module d'extension : com.glide.tokenbased_auth) dans l'instance ServiceNow® .

⚠ Avertissement :
Utilisez la demande **POST** lorsque vous soumettez des informations sensibles au serveur.

L'installation de la clé API et de l'authentification HMAC dépend des modules d'extension suivants :

- Module d'extension REST API Auth Scope (com.glide.rest.auth.scope)
- Module d'extension REST API Access Policy (com.glide.rest.policy)
- Périmètre d'authentification (com.glide.auth.scope)

Avantages

L'authentification par clé API et HMAC pour les API REST entrantes permet :

- Possibilité de spécifier une clé API ou un jeton HMAC pour l'authentification REST API.
- Possibilité d'associer un compte utilisateur à la clé API ou au jeton HMAC.
- Possibilité de spécifier un jeton comme paramètre de requête ou en-tête dans l'appel d'API REST.
- Possibilité d'associer le périmètre d'authentification à des configurations de clé API ou de jeton HMAC afin que les clés API puissent uniquement être utilisées pour appeler les API associées à des périmètres particuliers.
- Possibilité d'associer une configuration de clé API ou de jeton HMAC à un profil d'authentification utilisable dans les politiques d'accès API.

Activer la clé API et l'authentification HMAC

Vous pouvez activer la clé API du module d'extension et l'authentification HMAC (com.glide.tokenbased_auth) dans votre ServiceNow® instance.

Avant de commencer
Rôle requis : admin.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher la clé API et le module d'extension d'authentification HMAC (com.glide.tokenbased_auth).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

> **Remarque :**
> Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Configurer la clé API : authentification basée sur les jetons

Configurez une clé API pour prendre en charge l'authentification des points de terminaison REST API.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : clé API et authentification HMAC (com.glide.tokenbased_auth)

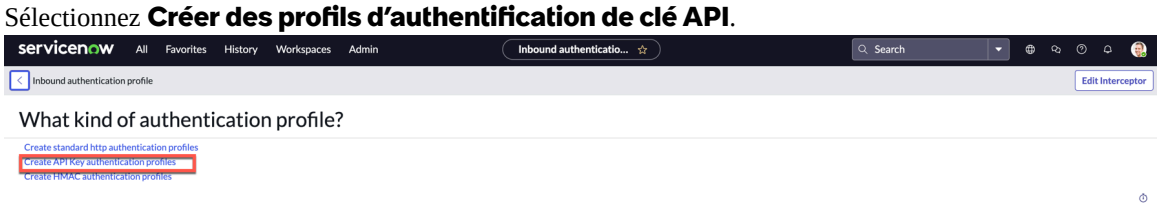
Procédure

1. Créez un profil d'authentification entrant.

   a. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Profils d'authentification entrants**.

   b. Sélectionnez **Nouveau**.
   Le système affiche le message Quel type de profil d'authentification ?

   c. Sélectionnez **Créer des profils d'authentification de clé API**.



   d. Renseignez les champs du formulaire.

Profils d'authentification de clé API

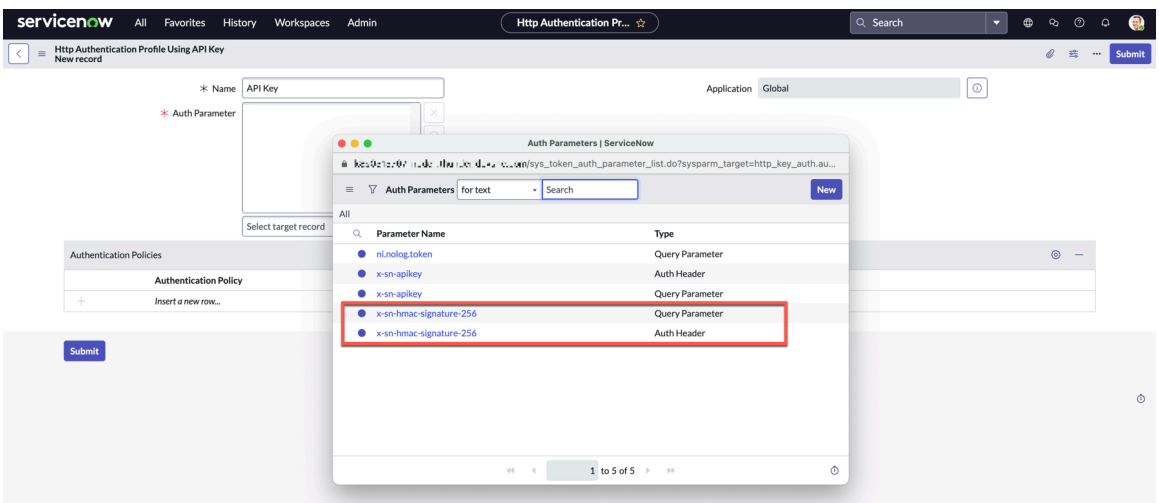
Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Application	Périmètre de la politique d'authentification.
Paramètre d'authentification	Sélectionnez le paramètre d'authentification pour la demande d'authentification. Vous pouvez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	sélectionner les options par défaut ou créer un nouveau paramètre d'authentification : ▪ x-sn-apikey : en-tête d'authentification ▪ x-sn-apikey : en-tête du paramètre de requête

Remarque :
L'option sélectionnée doit être définie dans l'appel REST dans le cadre de l'en-tête d'authentification ou du paramètre de requête.



e. Envoyez le formulaire.

2. Créez une clé API REST.

a. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Clé API REST**.

b. Sélectionnez **Nouveau**.

c. Renseignez les champs du formulaire :

Clé API

Champ	Description
Nom	Nom permettant d'identifier la clé API REST
Description	Description de la clé API REST.
Actif	État de la clé API REST.
Utilisateur	Utilisateur associé à la clé API REST. Utilisez l'icône de recherche pour sélectionner l'utilisateur.
Périmètre d'authentification	Option permettant d'ajouter un périmètre d'authentification pour gérer l'autorité de la clé API REST.
Jeton	Clé API REST générée par le Now Platformfichier . Copiez la clé à utiliser dans le

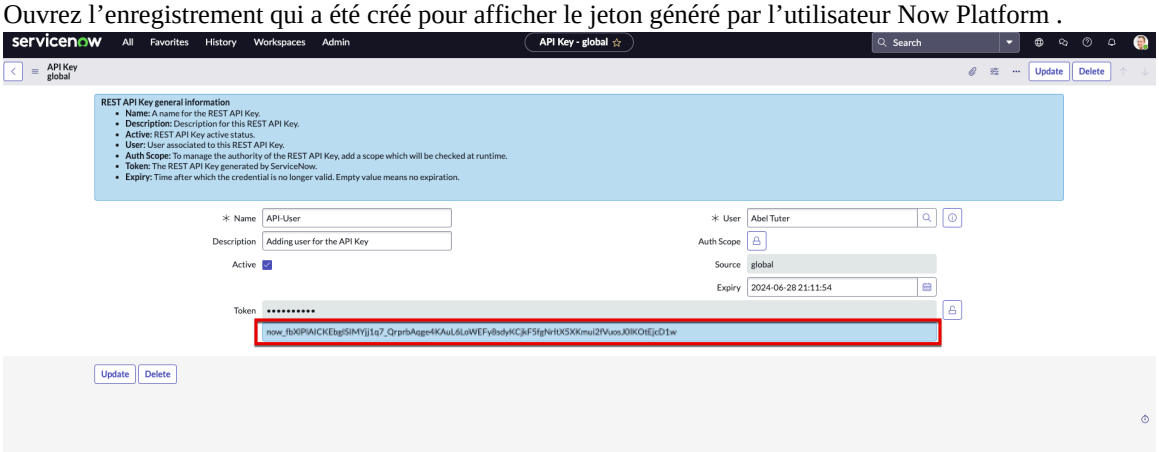
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	cadre de l'appel d'API REST dans le paramètre En-tête ou Requête.
Expiration	Heure après laquelle les informations d'identification ne sont plus valides. Une valeur vide signifie qu'il n'y a pas d'expiration. **Remarque :** Pour plus d'informations sur l'expiration du jeton, reportez-vous à la section Nettoyage de l'expiration du jeton .

d. Envoyez le formulaire.

e. Ouvrez l'enregistrement qui a été créé pour afficher le jeton généré par l'utilisateur Now Platform .



3. Créez une politique d'accès REST API.

a. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès REST API**.

b. Sélectionnez **Nouveau**.

c. Renseignez les champs du formulaire.

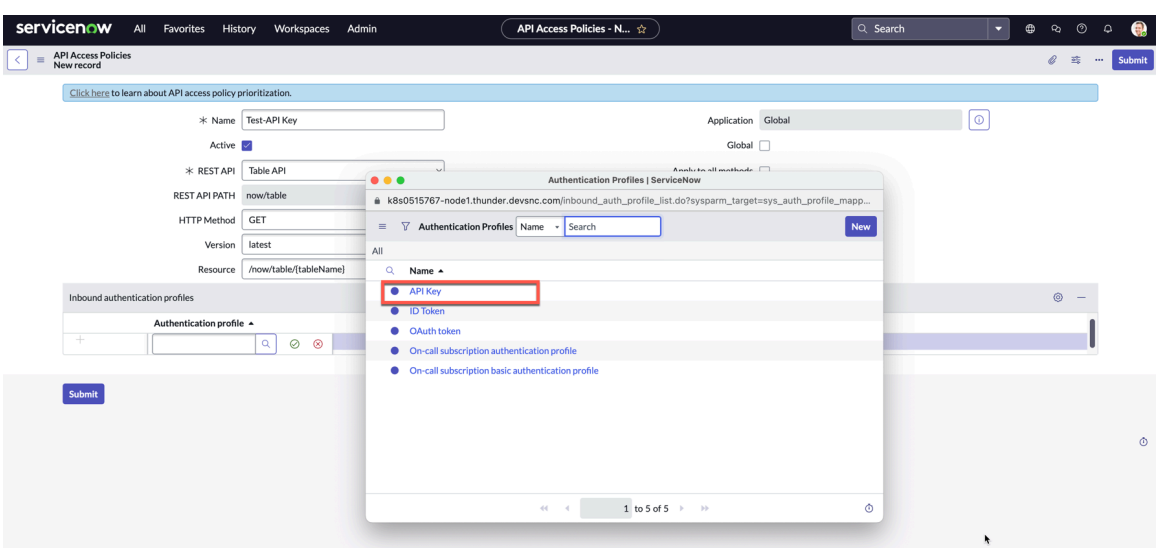
Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d'accès à l'API.
Actif	Option permettant d'activer la politique d'accès API.
API REST	L'API REST à laquelle la politique d'accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d'accès de l'API de REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **now/attachment**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fonction de message REST	Méthode utilisée pour interagir avec l'API. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d'authentification pour toutes les versions d'une REST API, vous devez créer des politiques individuelles pour chaque version.
Ressource	Ressource enfant de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **/now/attachment**
Application	Périmètre de l'application.
Global	Activez ce champ pour appliquer la politique d'authentification à toutes les méthodes, versions et ressources de l'API. **Remarque :** L'authentification basée sur le jeton n'est pas autorisée dans la politique API REST globale.
Appliquer à toutes les méthodes	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les méthodes, versions et ressources de l'API.
Appliquer à toutes les ressources	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les versions.
Appliquer à toutes les versions	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les ressources.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Ajoutez le profil d'authentification API qui a été créé.

e. Envoyez le formulaire.

Vous pouvez envoyer l'appel d'API REST avec le x-sn-apikey (jeton) qui a été généré par lors Now Platform de la création de la clé API dans le paramètre En-tête ou Requête en fonction de la configuration de l'authentification.

> **⚠ Avertissement :**
> Utilisez la demande **POST** lorsque vous soumettez des informations sensibles au serveur.

Configurer HMAC : authentification basée sur les jetons

Configurez HMAC pour prendre en charge l'authentification pour les points de terminaison d'API REST.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : clé API et authentification HMAC (com.glide.tokenbased_auth)

Procédure

1. Créez une configuration HMAC.

a. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Configuration HMAC**.

b. Sélectionnez **Nouveau**.

> **ⓘ Remarque :**
> Vous pouvez également utiliser **l'encodage HMAC SHA256 Base64 par défaut** qui est créé lors de l'installation du module d'extension.

c. Renseignez les champs du formulaire :

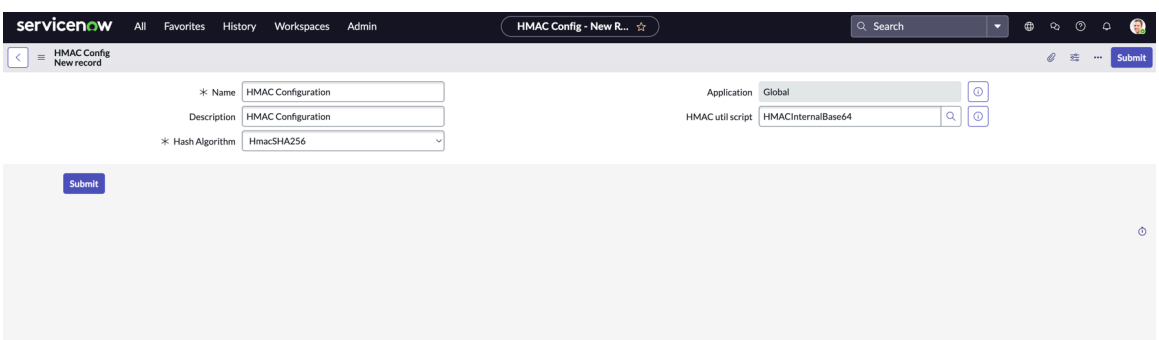
Configuration HMAC

Champ	Description
Nom	Nom de la configuration HMAC.
Application	Périmètre de la configuration.
Description	Description détaillée de la configuration.
Algorithme de hachage	Choisissez l'algorithme de hachage. Options disponibles : ▪ HmacSHA256 ▪ HmacSHA384 ▪ HmacSHA512
Script d'utilitaire HMAC	Script utilitaire pour HMAC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si vous validez l'authentification HMAC à l'aide du corps de la demande, de l'horodatage et du secret sans ID de clé, procédez comme suit : ▪ Créer une inclusion de script personnalisée en tant que script d'utilitaire HMAC ▪ Utilisez cet utilitaire de script include pour interpréter l'horodatage transmis et le corps de la demande. Il existe un ID de clé pour chaque secret partagé créé dans l'instance ServiceNow® . Vous devez configurer l'ID de clé en ID de clé par défaut dans le profil d'authentification HMAC.



d. Envoyez l'enregistrement.

2. Créez un profil d'authentification entrant.

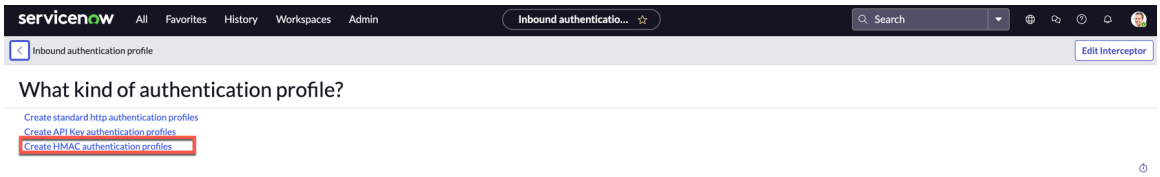
a. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Profils d'authentification entrants**.

b. Sélectionnez **Nouveau**.
Le système affiche le message Quel type de profil d'authentification ?

c. Sélectionnez **Créer des profils d'authentification HMAC**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

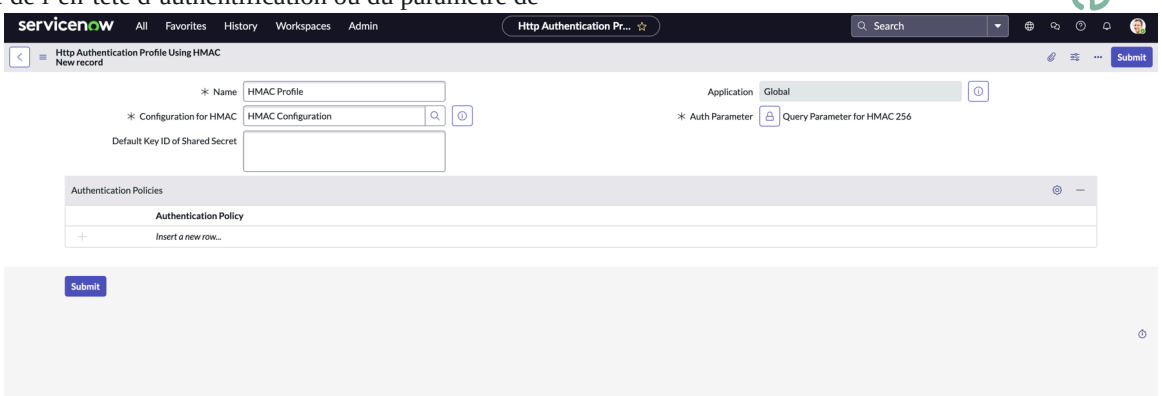


d. Renseignez les champs du formulaire.

Profils d'authentification HMAC

Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Application	Périmètre de la politique d'authentification.
Configuration pour HMAC	Sélectionnez la configuration HMAC qui a été créée.
Paramètre d'authentification	Sélectionnez le paramètre d'authentification pour la demande d'authentification. Vous pouvez sélectionner les options par défaut ou créer un nouveau paramètre d'authentification : ▪ x-sn-hmac-signature-256 : en-tête d'authentification ▪ x-sn-hmac-signature-256 : paramètre de requête
ID de clé par défaut du secret partagé	Informations de jeton qui peuvent être mises à jour dans ce champ pour l'utilisation de HMAC.

Remarque :
L'option sélectionnée doit être définie dans l'appel REST dans le cadre de l'en-tête d'authentification ou du paramètre de requête.



e. Envoyez le formulaire.

3. Créez un secret HMAC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Secret HMAC de l'API REST**.

b. Sélectionnez **Nouveau**.

c. Renseignez les champs du formulaire :

Secret HMAC de l'API REST

Champ	Description
Nom	Nom permettant d'identifier le secret HMAC de l'API REST.
Description	Description du secret HMAC de l'API REST.
Actif	État du secret HMAC de l'API REST.
Utilisateur	Utilisateur associé au secret HMAC de l'API REST. Utilisez l'icône de recherche pour sélectionner l'utilisateur.
ID clé	ID de clé qui doit être envoyé dans le cadre de l'appel REST. L'ID de clé est généré après l'envoi du formulaire.
Secret partagé	Secrets partagés de l'utilisateur. Par exemple, le mot de passe.
Source	Source de l'enregistrement.
Expiration	Heure après laquelle les informations d'identification ne sont plus valides. Une valeur vide signifie qu'il n'y a pas d'expiration. **Remarque :** Pour plus d'informations sur l'expiration du jeton, reportez-vous à la section Nettoyage de l'expiration du jeton .

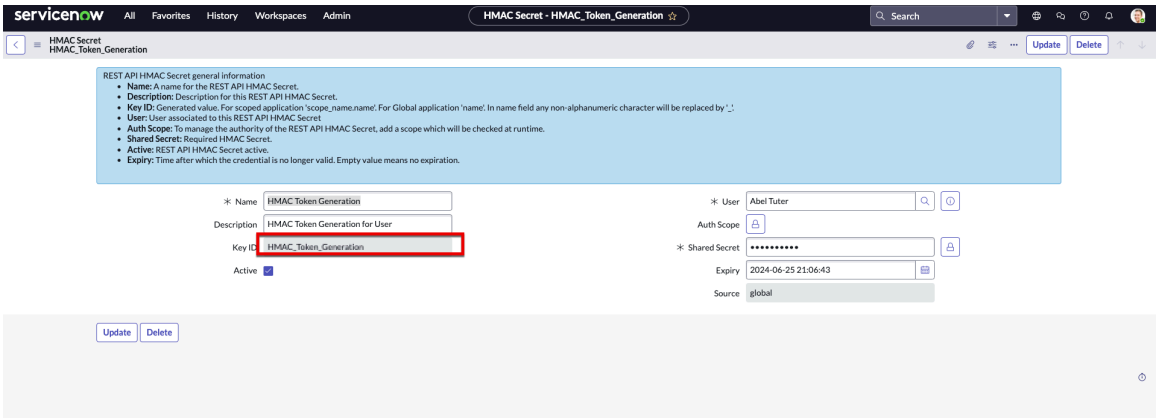
d. Envoyez le formulaire.

e. Ouvrez l'enregistrement qui a été créé.

Recherchez l'ID de clé généré par l'utilisateur Now Platform

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
Vous pouvez ajouter l'ID de clé qui a été généré pendant l'ID de clé dans le profil d'authentification qui a été créé pour HMAC si vous ne souhaitez pas spécifier le paramètre d'authentification ou de requête pour l'appel d'API.

4. Créez une politique d'accès à l'API REST.

a. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès REST API**.

b. Sélectionnez **Nouveau**.

c. Renseignez les champs du formulaire.

Politiques d'accès API

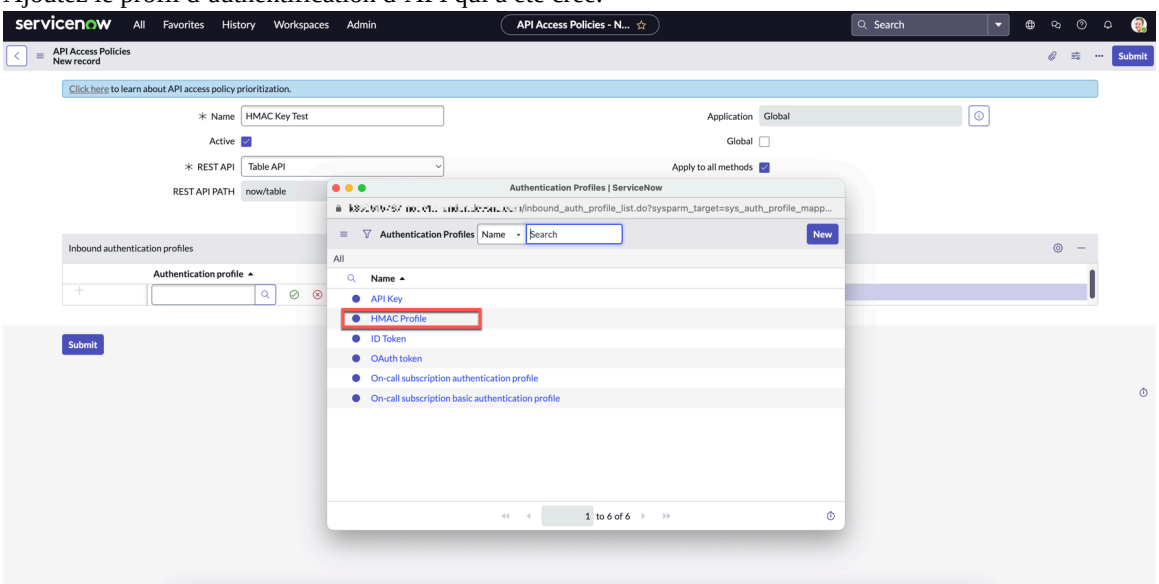
Champ	Description
Nom	Nom unique de la politique d'accès à l'API.
Actif	Option permettant d'activer la politique d'accès API.
API REST	L'API REST à laquelle la politique d'accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d'accès de l'API de REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **now/attachment**.
Fonction de message REST	Méthode utilisée pour interagir avec l'API. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d'authentification pour toutes les versions d'une REST API, vous devez créer des politiques individuelles pour chaque version.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Ressource	Ressource enfant de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **/now/attachment**
Application	Périmètre de l'application.
Global	Activez ce champ pour appliquer la politique d'authentification à toutes les méthodes, versions et ressources de l'API. **Remarque :** L'authentification basée sur le jeton n'est pas autorisée dans la politique API REST globale.
Appliquer à toutes les méthodes	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les méthodes, versions et ressources de l'API.
Appliquer à toutes les ressources	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les versions.
Appliquer à toutes les versions	Activez ce champ pour appliquer la politique d'authentification de l'API à toutes les ressources.

d. Ajoutez le profil d'authentification d'API qui a été créé.



e. Envoyez le formulaire.
Vous pouvez envoyer l'appel d'API REST :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Avec la x-sn-hmac-signature-256 qui a été générée lors ServiceNow® de la création de la clé API dans le paramètre En-tête ou Requête en fonction de la configuration pour authentification.
- Avec un script préalable à la demande avec secret partagé spécifié dans le cadre de la demande.

⚠ Avertissement :
Utilisez la demande **POST** lorsque vous soumettez des informations sensibles au serveur.

Nettoyage de l'expiration du jeton

Détails sur le nettoyage de l'expiration du jeton à l'aide de différentes propriétés système.

Une fois la clé API ou le secret HMAC expiré, les détails sont conservés pendant 7 jours. Une tâche planifiée : nettoyer les informations d'identification pour l'authentification du jeton expiré supprime ensuite les clés API ou les secrets HMAC expirés. Vous pouvez configurer ce comportement et contrôler la suppression à l'aide des propriétés suivantes :

- **com.snc.platform.security.token.auth.cleanup** : utilisez cette propriété si vous souhaitez supprimer les clés API et les jetons HMAC expirés. Par défaut , vrai.
- **com.snc.platfrom.security.token.auth.days.expired.api_key.is.kept** : définissez la valeur en fonction de vos besoins pour déterminer le nombre de jours pendant lesquels vous souhaitez conserver le jeton d'API expiré dans le système. Par défaut 7.
- **com.snc.platfrom.security.token.auth.days.expired.hmac_key.is.kept** : définissez la valeur en fonction de vos besoins pour déterminer le nombre de jours pendant lesquels vous souhaitez conserver le jeton HMAC expiré dans le système. Par défaut 7.

Pour accéder à la propriété d'expiration du jeton, saisissez sys.trigger.list dans la barre de navigation, puis recherchez les propriétés suivantes. Modifiez l'expiration en fonction de vos besoins.

Politique d'accès API

La politique d'accès des API définit les autorisations et la durée d'accès à une API.

La politique d'accès des API vous permet de restreindre l'accès aux API entrantes ServiceNow® en fonction du type d'authentification et des critères de filtrage spécifiés dans la politique d'accès.

Voici les trois niveaux de prise en charge de la politique d'authentification pour les sessions non interactives :

- **API REST** : l'administrateur peut définir une politique d'authentification d'API globale ou une politique d'authentification spécifique à l'API.
- **API SOAP** : l'administrateur peut définir une politique d'authentification d'API globale ou une politique d'authentification spécifique à l'API.
- **Processeur système/d'exportation** : l'administrateur peut définir cinq profils d'authentification du système de base, qui peuvent être utilisés pour appliquer le profil d'authentification à la politique d'authentification de l'API du processeur ou à la politique d'authentification spécifique du processeur.

ℹ Remarque :
Si vous ajoutez une politique d'authentification globale, cette politique s'applique à toutes les API REST, API SOAP ou processeurs système/d'exportation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Voici les modules d'extension installés automatiquement pour les stratégies d'API et le périmètre d'authentification :

- com.glide.rest.policy
- com.glide.soap.policy
- com.glide.processor.policy
- com.glide.rest.auth.scope

Vous pouvez configurer la politique de blocage globale par défaut ou créer une politique d'accès API personnalisée en fonction de vos besoins de sécurité. Et appliquez des critères de filtre contenant des conditions de filtre ou des requêtes qui sont utilisées comme entrées de politique pour une politique d'authentification.

Les politiques d'accès API suivantes sont prises en charge dans ServiceNow®:

- Politiques d'accès REST API
- Politiques d'accès de l'API SOAP

Pour plus d'informations sur les politiques relatives aux processeurs d'exportation, reportez-vous à la section Politique d'accès pour les processeurs système/d'exportation.

Politiques d'accès REST API

Les politiques d'accès des API REST vous permettent de restreindre l'accès aux API REST entrantes en fonction du type d'authentification et des critères de filtre spécifiés dans la politique d'accès.

Une API REST, également connue sous le nom d'API RESTful, est un type d'interface de programmation d'application (API) qui adhère aux directives du style architectural REST. Les API REST offrent un haut degré de flexibilité, ce qui les rend répandues sur le Web.

Les critères de filtre contiennent des conditions ou des requêtes de filtre qui sont utilisées comme entrées de politique pour une politique d'authentification.

Vous pouvez configurer la politique de blocage globale par défaut ou créer une politique d'accès API personnalisée en fonction de vos besoins de sécurité. Par exemple, vous pouvez créer une politique d'accès API personnalisée qui autorise uniquement le type d'authentification OAuth 2.0 à partir d'une plage spécifiée d'adresses IP. Les demandes d'authentification d'autres types d'authentification et les demandes d'accès à partir d'adresses IP autres que les adresses IP spécifiées sont refusées.

Activer la politique d'accès REST API

Vous pouvez activer le module d'extension REST API Access Policy (com.glide.rest.policy) si vous disposez du rôle administrateur. L'application inclut des données de démonstration et installe les applications et modules d'extension ServiceNow® Store connexes s'ils ne sont pas déjà installés.

Avant de commencer

Rôle requis : admin.

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec la politique d'accès API REST :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Modules d’extension : com.gilde.auth.profile, com.snc.adaptive_authentication, com.snc.platform.security.oauth
- Tables : sys_api_access_policy, sys_auth_profile_mapping, auth_policy_mapping, inbound_auth_profile, std_http_auth.

Pour plus d'informations, consultez Authentification adaptative.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d’extension REST API Access Policy (com.glide.rest.policy).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée.

Créer un profil d’authentification

Créez un profil d’authentification et ajoutez une ou plusieurs politiques d’authentification au profil. Vous pouvez également configurer les profils **d’authentification de jeton d’ID** et de **jeton OAuth** qui sont disponibles par défaut.

Avant de commencer
Rôle requis : administrateur

Remarque :
Vous pouvez appliquer des politiques d’authentification, une plage IP, basées sur les rôles, basées sur l’utilisateur, etc., avec l’authentification réciproque et l’authentification personnalisée.

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Profils d’authentification entrants**.
2. Sélectionnez **Nouveau**.
   Le système affiche le message. Quel type de profil d'authentification ?
3. Sélectionnez **Créer des profils d’authentification http standard**.
4. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Profil d'authentification standard

Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Description	Description de la politique d'authentification.
Actif	Option permettant d'activer la politique d'authentification.
Application	Périmètre de la politique d'authentification.
Type	Type de l'authentification disponible. Vous pouvez sélectionner **l'authentification de base**, le **jeton d'ID**, **l'authentification basée sur certificat** ou **OAuth**.
Entité OAuth	Profil de l'entité OAuth. Ce champ s'affiche uniquement lorsque **Jeton d'ID** ou **OAuth** est sélectionné dans **Type**.

5. Double-cliquez sur **Insérer une nouvelle ligne**.
6. Sélectionnez une politique d'authentification dans la liste et sélectionnez l'icône .

Remarque :
Ne sélectionnez pas Autoriser la politique d'accès ou Refuser la politique d'accès. Ces politiques ne sont destinées qu'aux connexions des utilisateurs.

Vous pouvez ajouter une ou plusieurs politiques d'authentification pour un profil d'authentification.

Remarque :

Authentifier l'en-tête [WWW-Authenticate].

Lorsque la politique d'accès REST API est active, nous renvoyons le profil d'authentification mappé le plus récemment dans l'en-tête d'authentification. Si vous souhaitez que le serveur renvoie tous les schémas d'authentification, utilisez la propriété `glide.security.response.authenticate.header.auth_profile.first_scheme_only` et définissez-la sur **false**. La réponse est renvoyée avec plusieurs en-têtes. Par exemple :

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Créer une politique d'accès REST API

Créez une politique d'accès API et mappez un profil d'authentification pour restreindre le type d'authentification d'une REST API. Par exemple, vous pouvez créer une politique d'accès API qui autorise uniquement l'authentification par jeton d'ID pour une REST API.

Avant de commencer

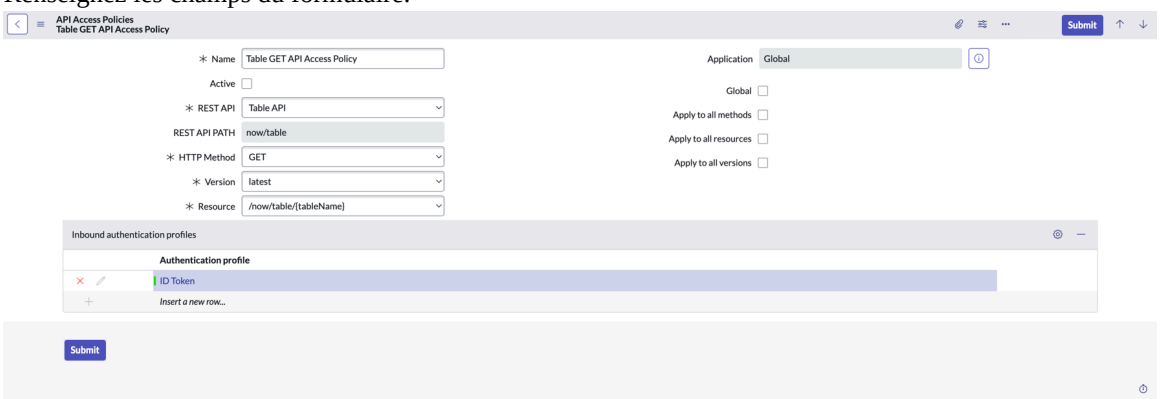
- Rôle requis : administrateur
- Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, consultez Créer un profil d'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès REST API**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.



Politiques d'accès API

Champ	Description
Nom	Nom unique de la politique d'accès à l'API.
Actif	Option permettant d'activer la politique d'accès API.
API REST	L'API REST à laquelle la politique d'accès est appliquée. Par exemple, **API de pièce jointe**.
CHEMIN REST API	Chemin d'accès de l'API de REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **now/attachment**.
Fonction de message REST	Méthode utilisée pour interagir avec l'API. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée.
Version	Version de l'API. Par exemple, **v1**. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. **Remarque :** Si vous souhaitez créer une politique d'authentification pour toutes les versions d'une REST API, vous devez créer des politiques individuelles pour chaque version.
Ressource	Ressource enfant de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, **/now/attachment**
Application	Périmètre de l'application.
Global	Activez cette option pour appliquer la politique d'authentification à toutes les méthodes, versions et ressources de l'API.

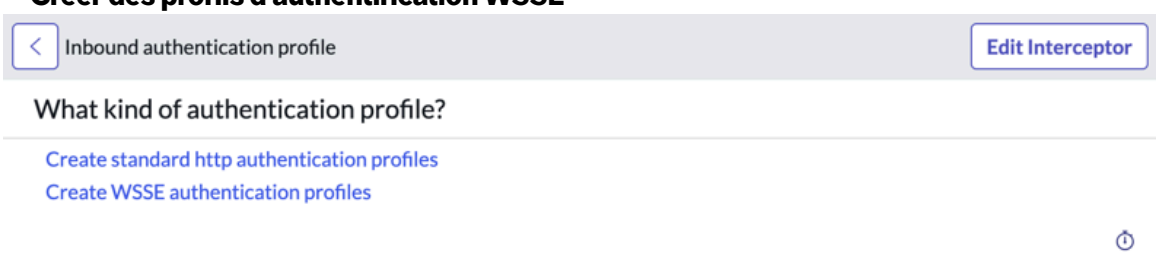
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Appliquer à toutes les méthodes	Activez cette option pour appliquer la politique d'authentification de l'API à toutes les méthodes, versions et ressources de l'API.
Appliquer à toutes les ressources	Activez cette option pour appliquer la politique d'authentification de l'API à toutes les versions.
Appliquer à toutes les versions	Activez cette option pour appliquer la politique d'authentification de l'API à toutes les ressources.

Remarque :
Pour en savoir plus sur la priorisation des stratégies d'accès API, reportez-vous à la section Priorisation de la politique d'accès API.

4. Double-cliquez sur **Insérer une nouvelle ligne**.
5. Sélectionnez un profil d'authentification entrant dans la liste et cliquez sur l'icône .
   Par exemple, vous pouvez ajouter **l'authentification de base**, le **jeton d'ID, l'authentificationbasée sur certificat**, **l'authentification OAuth** ou **WSSE**.
   a. Pour ajouter un ou plusieurs profils d'authentification entrants, cliquez sur **Nouveau** pour créer un profil.
   b. **Choisir quels types de profils d'authentification ?**
      - **Créer des profils d'authentification http standard**
      - **Créer des profils d'authentification WSSE**



   c. Après avoir créé le profil d'authentification, enregistrez l'enregistrement.
6. Cliquez sur **Envoyer** pour soumettre la politique d'accès à l'API REST.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Priorisation de la politique d'accès API

Découvrez la logique de hiérarchisation des politiques si plusieurs politiques d'accès API sont configurées pour votre ServiceNow® instance.

Les politiques d'accès API sont classées par ordre de priorité en fonction du type de politique REST API définie sur votre ServiceNow® instance.

L'approche consiste à définir différents poids pour chaque partie de l'API, tels que la méthode, la ressource et la version.

La politique d'API est priorisée pour les éléments non globaux d'abord, puis globaux. En d'autres termes, une politique d'accès non globale remplacera toujours une politique d'accès API globale.

Les logiques de hiérarchisation sont les suivantes :

Ordre de priorité

Champs	Priorité	Logique de hiérarchisation
Méthode, ressource et version	1	Si les 3 champs correspondent à la politique, celle-ci prend la 1re priorité.
Méthode+ ressource	2	Si les 2 champs correspondent à la politique, celle-ci prend la 1ère priorité.
Ressource + version	3	Si les 2 champs ainsi que le champ **Appliquer à toutes les méthodes** correspondent à la politique, celle-ci prend la 3e priorité.
Ressource	4	Si le champ et le champ **Appliquer à toutes les méthodes correspondent à** la politique, celle-ci prend la 4e priorité.
Méthode + version	5	Si les 2 champs ainsi que le champ **Appliquer à toutes les ressources correspondent à** la politique, celle-ci prend la 5e priorité.
Méthode	6	Si le champ et le champ **Appliquer à toutes les ressources correspondent à** la politique, celle-ci prend la 5e priorité.
Version	7	Si le champ et les champs **Appliquer à toutes les méthodes** et **Appliquer à toutes les versions** correspondent à la politique, celle-ci prend la 7e priorité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ordre de priorité (suite)

Champs	Priorité	Logique de hiérarchisation
Global et appliquer à toutes les méthodes	8	Si les champs **Global** est vrai et **Appliquer à toutes les méthodes** est faux , alors cette politique prend la 8e priorité.
Global et appliquer à toutes les méthodes	9	Si les champs **Global** est vrai et **Appliquer à toutes les méthodes** est vrai , alors cette politique prend la 9e priorité.

Périmètre d'authentification REST API

Prise en charge du périmètre d'authentification pour l'API REST.

Avant Xanadu la publication, chaque jeton d'accès ou jeton OIDC est lié au périmètre useraccount qui a un accès complet aux API REST de l'utilisateur. À partir de Xanadu la version, pour fournir un accès uniquement aux API REST particulières, les champs d'application des jetons OAuth sont introduits.

Lorsqu'une entité OAuth est liée à un périmètre d'authentification, jeton émis ou géré par cette entité OAuth et ne peut être utilisé que pour accéder aux API REST (une entité OAuth peut être liée à plusieurs périmètres d'authentification). Pour la nouvelle entité OAuth, le périmètre d'authentification par défaut est vide. Vous devez lier manuellement le périmètre d'authentification à l'entité OAuth.

Remarque :

- Une fois le périmètre d'authentification de l'API REST activé et ajouté au périmètre d'authentification de l'API REST, tous les jetons OAuth existants ne peuvent plus accéder à cette API, sauf si l'administrateur ajoute ce champ d'application d'authentification à l'entité OAuth correspondante
- L'administrateur est responsable de s'assurer que le oauth_entity dispose du bon périmètre d'authentification après avoir lié le périmètre d'authentification à l'API REST.
- Les jetons d'accès OAuth émis par ServiceNow prennent en charge le périmètre d'authentification.
- Jeton OIDC qui n'est pas émis par ServiceNow est validé par ServiceNow.
- Le jeton OIDC a sa portée à partir d'IdP lorsque vous avez besoin d'un jeton d'ID. Ici, le périmètre d'authentification est pour ServiceNow au lieu de tiers (IdP).

Configurations du périmètre de l'API REST

Pour configurer le périmètre de l'API REST, procédez comme suit :

- Créer un périmètre d'authentification
- Lier le périmètre d'authentification avec l'API REST
- Lier le périmètre d'authentification à l'entité OAuth
- Exécutez un flux OAuth pour obtenir le jeton d'accès OAuth
- Utiliser le jeton d'accès OAuth pour effectuer l'appel d'API

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Activer le périmètre d'authentification de REST API

Vous pouvez activer le module d'extension Champ d'application d'authentification de l'API REST (com.glide.rest.auth.scope) pour lier l'entité OAuth aux champs d'application d'authentification.

Avant de commencer
Installez les modules d'extension suivants :

- OAuth 2.0
- Fournisseur d'API REST
- Périmètre d'authentification
- Périmètre de REST API

Remarque :
Le *REST API Scope* module d'extension est ajouté dans le cadre de la Tokyo version.

Rôle requis : administrateur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtre et la barre de recherche pour rechercher le module d'extension REST API *auth Scope (com.glide.rest.auth.scope*).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Propriétés et tables du périmètre d'authentification de l'API REST

Le module d'extension REST API Auth Scope (com.glide.rest.auth.scope) inclut les propriétés système, tables et scripts suivants.

Propriétés du périmètre d'authentification de l'API REST

Le champ d'application d'authentification de l'API REST ajoute les propriétés système suivantes.

Propriétés

Nom	Description
com.glide.rest.api.auth.scope.check.enable	Cette propriété permet de désactiver la vérification du périmètre d'authentification au niveau de la plateforme.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés (suite)

Nom	Description
	Si la valeur est définie sur faux, la vérification du périmètre d'authentification est ignorée pendant l'exécution, qu'elle soit liée ou non à l'API RETS. Par défaut, cette propriété est définie sur true. Cette propriété est utilisée lorsque vous souhaitez revenir au comportement de la version précédente.
`com.glide.oauth.token.scope.useraccount`	Cette propriété n'est utilisée que lorsque `useraccount` le périmètre d'authentification est supprimé et est rajouté manuellement par l'utilisateur final. Dans ce cas, l'ID système du `useraccount` est modifié. Il est nécessaire de mettre à jour cette propriété vers le nouveau sys_id. Pendant l'exécution, l'ID système du périmètre d'authentification est utilisé à la place du nom du périmètre d'authentification.

Tables du périmètre d'authentification de l'API REST

Périmètre d'authentification de l'API REST les tables suivantes.

Tables

Nom	Description
Périmètre d'authentification (sys_auth_scope)	Cette table définit le périmètre d'authentification qui peut être lié à l'API REST et à l'entité OAuth. Le nom du périmètre d'authentification doit être unique et global.
Périmètre d'authentification de l'API REST (sys_api_access_scope)	Cette table relie l'API REST au périmètre d'authentification.

Configurer le périmètre d'authentification de l'API REST

Liez l'entité OAuth à un périmètre d'authentification pour gérer le jeton afin d'accéder aux API REST liées au périmètre d'authentification.

Avant de commencer
Installez les modules d'extension suivants :

- OAuth 2.0
- Fournisseur d'API REST

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Périmètre d’authentification
- Périmètre d'authentification REST API

Remarque :
Le *REST API Auth Scope* module d’extension est ajouté dans le cadre de la Tokyo version.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Périmètres d'authentification API** > **Périmètre d'authentification REST API**.
   La page Périmètres d’authentification de l’API REST s’affiche.
2. Pour configurer un nouveau périmètre d’authentification de l’API REST, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Périmètre d'authentification REST API

Nom	Nom unique qui identifie le périmètre d’authentification de l’API REST.
Actif	Cochez la case pour rendre la configuration active.
Application	Champ d'application de l'application en lecture seule.
API REST	L’API REST à laquelle le périmètre d’authentification est appliqué. Par exemple, l’API Table.
Périmètre d'authentification	Sélectionnez le périmètre d’authentification dans l’icône de recherche.
CHEMIN REST API	Chemin d’accès de l’API de REST. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée. Par exemple, now/table.
Fonction de message REST	Méthode utilisée pour interagir avec l’API. Sélectionnez la méthode dans la liste déroulante. Vous pouvez désactiver manuellement le **périmètre d’authentification Appliquer à toutes les méthodes HTTP dans ce** champ API du formulaire pour sélectionner la méthode.
Version de REST API	Version de l'API. Par exemple, v1. Ce champ est renseigné automatiquement en fonction de l’API REST sélectionnée. Vous pouvez désactiver manuellement le **périmètre d’authentification Appliquer à toutes les versions dans ce** champ API du formulaire pour sélectionner la version.

Traduction automatique

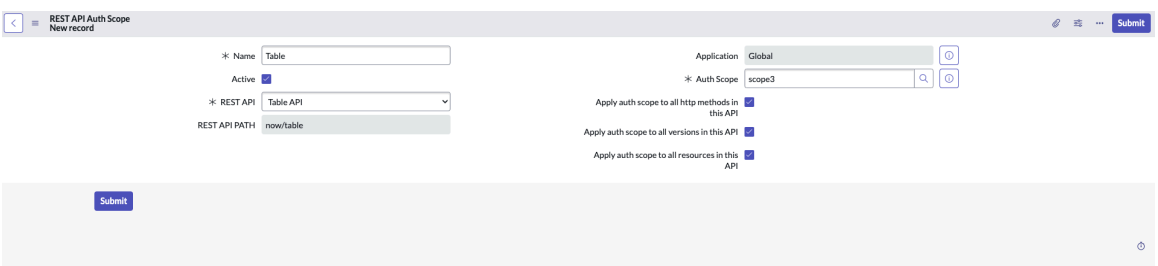
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ressource	Ressource enfant de l'API REST. Ce champ est renseigné automatiquement en fonction de l'API REST sélectionnée. Par exemple, /now/table. Vous pouvez désactiver manuellement le **champ d'application d'authentification Appliquer à toutes les ressources dans ce champ API** du formulaire pour sélectionner les ressources.
Appliquer le périmètre d'authentification à toutes les méthodes HTTP dans cette API.	Lorsque cette option est activée, elle applique le périmètre d'authentification à toutes les méthodes HTTP de l'API.
Appliquer le périmètre d'authentification à toutes les versions dans cette API.	Si la fonctionnalité est activée, applique le périmètre d'authentification à toutes les versions de l'API.
Appliquer le périmètre d'authentification à toutes les ressources dans cette API.	Lorsque cette option est activée, elle applique le périmètre d'authentification à toutes les ressources de l'API

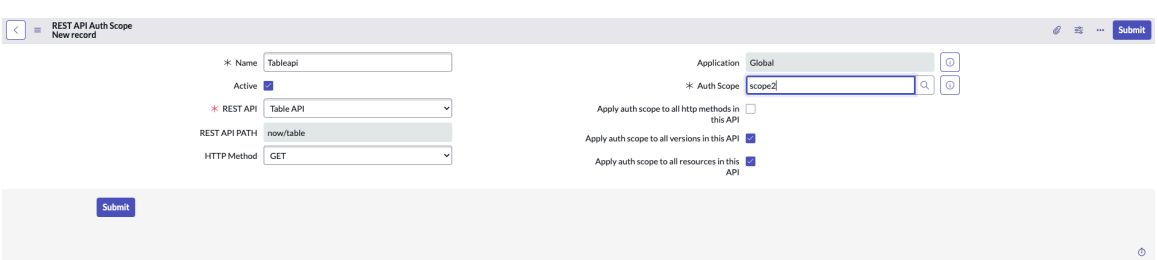
4. Cliquez sur **Envoyer**.
   En fonction de l'API REST et du périmètre d'authentification sélectionnés, les API récupèrent les informations qui sont propres au périmètre.

Example: Envisagez de créer trois périmètres d'authentification de l'API REST pour l'API de table

Le premier périmètre d'authentification est mappé à **l'API Table** avec toutes les méthodes, versions et ressources http activées.



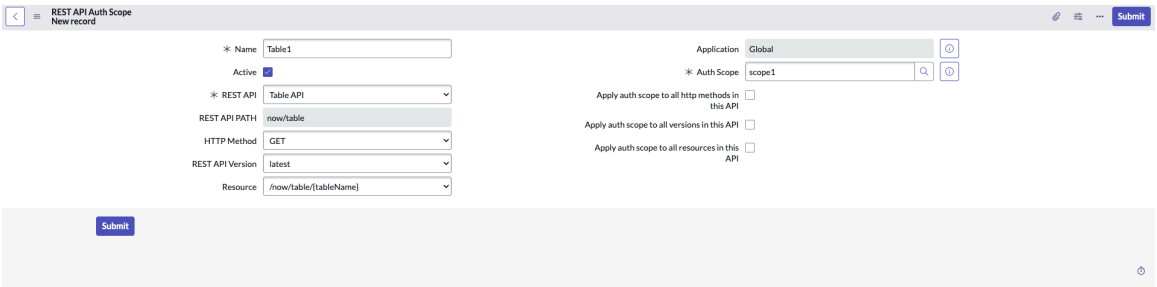
Le deuxième périmètre d'authentification est mappé à **l'API Table** avec toutes les versions et ressources activées. Mais, vous choisissez la méthode HTTP, dans cet exemple, la méthode **GET** .



Le troisième périmètre d'authentification est mappé à **l'API Table** sans que les méthodes, versions et ressources http soient activées. Cependant, vous choisissez manuellement la méthode HTTP, la version et la ressource. Dans cet exemple, la méthode HTTP est **GET**, la version de l'API REST est **la dernière** et la ressource est `/now/table/{tableName}`.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Si tous ces champs d'application d'authentification sont créés, vous pouvez utiliser la méthode **GET** avec les trois champs d'application, mais pour les méthodes **POST,PUT,DELETE** ou **PATCH** , seul **scope3** peut être utilisé.

Dépannage du périmètre de l'API REST

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de la configuration ou de l'exécution du périmètre de l'API REST.

Dépannage

Problème	Action
L'API REST est liée au périmètre d'authentification, cependant en cours d'exécution, il n'y a pas de vérification du périmètre d'authentification, même à l'aide de l'authentification par jeton de support.	• Assurez-vous que l'enregistrement sys_api_access_policy est actif. L'exécution ignore les enregistrements inactifs. • Vérifiez si la propriété *com.glide.rest.api.auth.scope.check.enable* est définie sur faux. • Vérifiez si le jeton OAuth a un périmètre d'authentification useraccount .
L'API REST est liée à *auth_scope1*, mais le jeton d'accès qui a *auth_scope2* est également en mesure d'y accéder.	• Vérifiez si cet enregistrement est actif. • Vérifiez ce REST, vérifiez s'il existe d'autres enregistrements, qui ont les mêmes API mais des méthodes d'application différentes, des versions ou des ressources.
L'API REST est liée au périmètre d'authentification, mais en cours d'exécution, il n'y a pas de vérification du périmètre d'authentification pour *basicAuth* et *mutualAuth*.	Cela est attendu car le périmètre d'authentification de l'API REST ne s'applique qu'au jeton d'accès OAuth ou au jeton OIDC. Il n'applique pas l'authentification basée sur BasicAuth, les cookies de session et les certificats.
L'appel d'API REST renvoie 403 lors de l'utilisation du jeton d'accès OAuth.	Vérifiez le message d'erreur « Périmètre d'accès API requis manquant ». Si cette API REST est trouvée, la vérification du périmètre d'authentification échoue
Le compte d'utilisateur prédéfini est supprimé et ne doit pas être restauré à coup sûr.	Exportez useraccount au format XML à partir de l'autre instance et importez-le ou créez un useraccount et modifiez la propriété *glide.oauth.token.scope.useraccount*

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage (suite)

Problème	Action
	système dans l'enregistrement de sys_id nouvellement créé.

Forum Aux Questions

Voici quelques-unes des questions fréquemment posées lors de l'utilisation du périmètre d'authentification de l'API REST :

Un jeton OAuth peut-il être lié à plusieurs étendues d'authentification ?

Oui, un oauth_entity peut être lié à plusieurs étendues d'authentification, chaque jeton OAuth émis par cette oauth_entity a les mêmes étendues d'authentification.

Différents jetons OAuth avec des périmètres d'authentification différents peuvent-ils accéder à la même API REST ?

Oui, pour la même API REST, différents périmètres d'authentification peuvent y accéder. Tant qu'un périmètre d'authentification est mis en correspondance, le champ d'application d'authentification renvoie les résultats.

Le jeton d'accès OAuth avec le périmètre d'authentification useraccount **peut-il accéder à n'importe quelle API REST ?**

Oui, le compte utilisateur dispose d'un accès complet au périmètre d'authentification.

Le jeton d'accès OAuth : le champ d'application OAuth peut-il être modifié dynamiquement ?

Oui, l'authentification incluse dans le champ d'application n'est pas codée en dur avec le jeton d'accès de la table oauth_credential . Au lieu de cela, le champ d'application d'authentification est obtenu à partir d'oauth_entity liés pendant l'exécution.

Le jeton OAuth peut-il conserver les mêmes étendues d'authentification après l'actualisation ?

Oui, le périmètre d'authentification ne changera pas après l'actualisation du jeton, sauf si oauth_admin modifiez le périmètre d'authentification lié à oauth_entity.

L'enregistrement de périmètre d'authentification useraccount **prédéfini est supprimé. Un nouveau périmètre d'authentification avec le nom** useraccount **peut être créé ?**

La création d'un nouveau périmètre d'authentification avec le même compte utilisateur ne fonctionne pas. Dans l'exécution, il utilise le sys_id au lieu du nom pour vérifier le périmètre d'authentification et modifier la propriété `glide.oauth.token.scope.useraccount` système en l'enregistrement de sys_id nouvellement créé.

Si l'administrateur modifie l'authentification incluse dans le périmètre liée à oauth_entity**, tous les jetons d'accès OAuth existants émis par cette entité OAuth sont-ils également modifiés ?**

Oui, le champ d'application d'authentification n'est pas directement lié au jeton d'accès OAuth, il est obtenu à partir de oauth_entity pendant l'exécution.

Différents jetons d'accès OAuth émis par le même oauth_entity **peuvent-ils avoir des étendues d'authentification différentes ?**

Non, tous les accès au jeton sont émis par la même oauth_entity et ont toujours les mêmes étendues d'authentification.

Un utilisateur peut-il définir différents champs d'application d'authentification pour un point de terminaison particulier ?

Non, il existe une vérification de contrainte unique pour un point de terminaison d'API REST particulier. Toutefois, pour le même point de terminaison de REST API, il peut avoir plusieurs champs d'application d'authentification correspondants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La vérification du périmètre d'authentification est-elle également utilisée pour BasicAuth ?

Non, la vérification du périmètre d'authentification porte uniquement sur le jeton d'accès OAuth et le jeton OIDC, elle n'est pas demandée *`basicAuth`* et *`mutualAuth`*

Politiques d'accès de l'API SOAP

Les politiques d'accès de l'API SOAP vous permettent de restreindre l'accès aux API SOAP entrantes en fonction du type d'authentification et des critères de filtre spécifiés dans la politique d'accès.

Les politiques d'accès de l'API SOAP vous permettent d'appliquer le profil d'authentification entrant et les politiques d'accès des API aux API SOAP entrantes et aux API SOAP scriptées.

Vous pouvez tirer parti ServiceNow des politiques d'accès d'API telles que les restrictions basées sur la plage IP et les rôles pour autoriser ou interdire les appels d'API SOAP entrants en fonction de l'authentification.

En tant qu'administrateur, vous pouvez effectuer les actions suivantes pour appliquer les politiques.

- Activez les modules d'extension de la politique d'accès de l'API SOAP et du profil d'authentification. Pour plus d'informations, consultez Activer la politique d'accès de l'API SOAP.
- Créez des politiques d'accès de l'API SOAP et associez-les à un profil d'authentification. Pour plus d'informations, consultez Créer une politique d'accès à l'API SOAP et Créer un profil d'authentification.

  Remarque :
  Les politiques sont applicables à l'API de table SOAP ou à l'API SOAP scriptée. Outre le profil d'authentification `http` et `WSSE` standard.

- Créez des politiques d'authentification telles que la plage IP, les restrictions basées sur les rôles et associez-les au profil d'authentification. Pour plus d'informations, consultez Créer une politique d'authentification API.

Activer la politique d'accès de l'API SOAP

Pour la politique d'accès de l'API SOAP, installez le module d'extension Politique d'accès de l'API SOAP (`com.glide.soap.policy`).

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
L'élément suivant est installé avec le module d'extension SOAP API Access Policy : Processor Access Policy (`com.glide.processor.policy`)

Module d'extension dépendant : Profil d'authentification (`com.glide.auth.profile`)

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Recherchez le module d'extension SOAP API Access Policy (`com.glide.soap.policy`) à l'aide des critères de filtre et de la barre de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Créer un profil d'authentification

Créez un profil d'authentification et ajoutez une ou plusieurs politiques d'authentification au profil. Vous pouvez également configurer les profils **d'authentification de jeton d'ID** et de **jeton OAuth** qui sont disponibles par défaut.

Avant de commencer
Rôle requis : administrateur

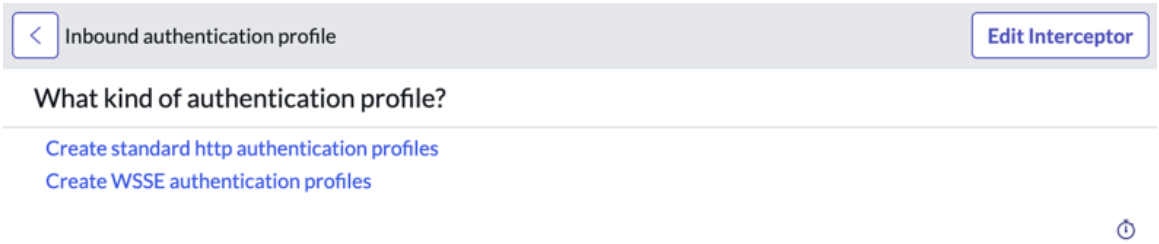
Remarque :
Vous pouvez appliquer des politiques d'authentification, une plage IP, basées sur les rôles, basées sur l'utilisateur, etc., avec l'authentification réciproque et l'authentification personnalisée.

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Profils d'authentification entrants**.
2. Sélectionnez **Nouveau**.
   Le système affiche le message. Quel type de profil d'authentification ?
3. **Choisir quels types de profils d'authentification ?**
   - **Créer des profils d'authentification http standard**
   - **Créer des profils d'authentification WSSE**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Renseignez les champs du formulaire.

Formulaire Profil d'authentification standard

Champ	Description
Nom	Nom permettant d'identifier la politique d'authentification.
Description	Description de la politique d'authentification.
Actif	Option permettant d'activer la politique d'authentification.
Application	Périmètre de la politique d'authentification.
Type	Type de l'authentification disponible. Vous pouvez sélectionner **l'authentification de base**, **le jeton d'ID**, **l'authentification basée sur certificat**, **OAuth** ou **WSSE** (dans le cas d'un profil d'authentification WSSE).
Entité OAuth	Profil de l'entité OAuth. Ce champ s'affiche uniquement lorsque **Jeton d'ID** ou **OAuth** est sélectionné dans **Type**.

5. Double-cliquez sur **Insérer une nouvelle ligne**.

6. Sélectionnez une politique d'authentification dans la liste et sélectionnez l'icône .

Remarque :
Ne sélectionnez pas **Autoriser la politique d'accès** ou **Refuser la politique d'accès**. Ces politiques ne sont destinées qu'aux connexions des utilisateurs.

Vous pouvez ajouter une ou plusieurs politiques d'authentification pour un profil d'authentification.

En cas de changement du profil d'authentification, l'en-tête d'autorisation renvoie une valeur spécifique aux changements apportés à ce moment-

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

là. Pour avoir la possibilité d'obtenir tous les schémas d'authentification renvoyés dans l'en-tête « WWW-Authenticate », vous devez activer glide.security.response.authenticate.header.auth_profile.first_scheme_only sur **false**. La réponse est renvoyée avec plusieurs en-têtes. Par exemple :

```
< WWW-Authenticate: BEARER realm="Service-now"
< WWW-Authenticate: BASIC realm="Service-now"
```

Créer une politique d'accès à l'API SOAP

Créez une politique d'accès API et mappez un profil d'authentification pour restreindre le type d'authentification d'une API SOAP. Par exemple, vous pouvez créer une politique d'accès API qui autorise uniquement l'authentification par jeton d'ID pour une API SOAP.

Avant de commencer

- Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, consultez Créer un profil d'authentification.
- Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Politiques d'accès de l'API SOAP**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Politiques d'accès API

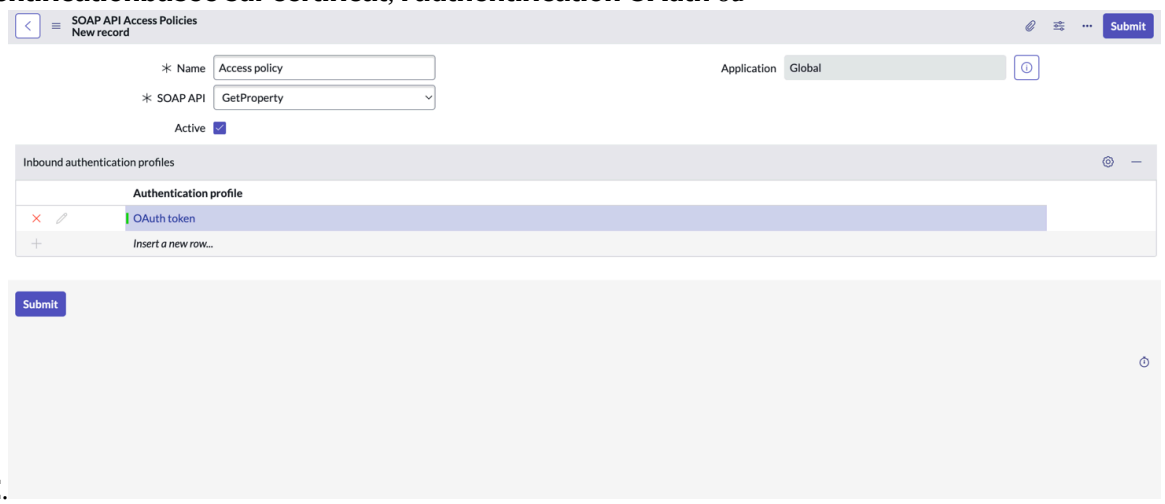
Champ	Description
Nom	Nom unique de la politique d'accès à l'API.
API SOAP	API SOAP à laquelle la politique d'accès est appliquée. Par exemple, **l'API GetProperty**.
Application	Périmètre de l'application.
Actif	Option permettant d'activer la politique d'accès API.

4. Dans la section Authentification entrante, double-cliquez sur **Insérer une nouvelle ligne**.
5. Sélectionnez un profil d'authentification entrant dans la liste et cliquez sur l'icône .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

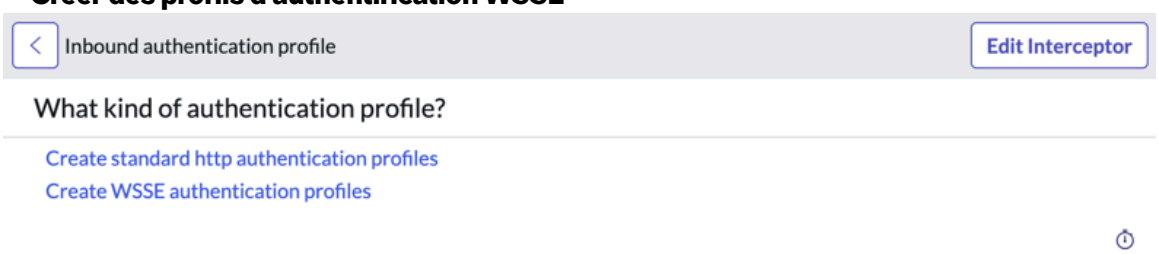
Par exemple, vous pouvez ajouter **l'authentification de base**, le **jeton d'ID, l'authentificationbasée sur certificat**, **l'authentification OAuth** ou **WSSE**.



a. Pour ajouter un ou plusieurs profils d'authentification entrants, cliquez sur **Nouveau** pour créer un profil.

b. Choisir quels types de profils d'authentification ?

- **Créer des profils d'authentification http standard**
- **Créer des profils d'authentification WSSE**



c. Pour créer un profil d'authentification WSSE, renseignez les champs du formulaire.

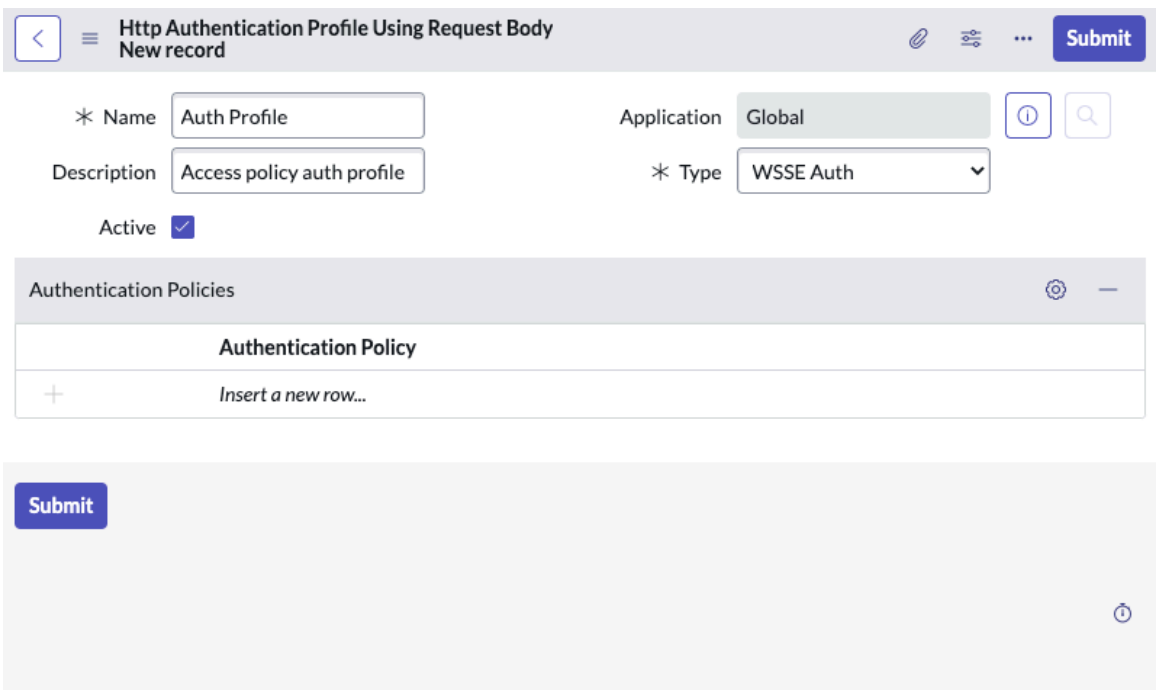
Profil d'authentification WSSE

Champ	Description
Nom	Nom unique de la politique d'accès à l'API.
Description	Description du profil d'authentification.
Application	Périmètre de l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Actif	Option permettant d'activer la politique d'accès API.
Type	Authentification WSSE en tant que profil d'authentification WSSE (Web Security).



d. Après avoir créé le profil d'authentification, enregistrez l'enregistrement.

6. Cliquez sur **Envoyer** pour soumettre la politique d'accès de l'API SOAP.

Créer une politique d'accès API globale pour protéger les API SOAP

Créez une politique d'accès API globale unique pour protéger toutes les API SOAP.

Avant de commencer

- Rôle requis : administrateur
- Installer le module **d'extension Processor Access policy** (com.glide.processor.policy)
- Assurez-vous qu'un profil d'authentification est créé. Pour plus d'informations, consultez Créer un profil d'authentification.

Les étapes suivantes décrivent comment créer une politique d'accès globale unique pour protéger toutes les API SOAP.

Remarque :
Les politiques définies au niveau de chaque API SOAP remplacent la politique d'accès global au niveau **SOAPProcessor** .

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Politiques d'accès aux processus**.

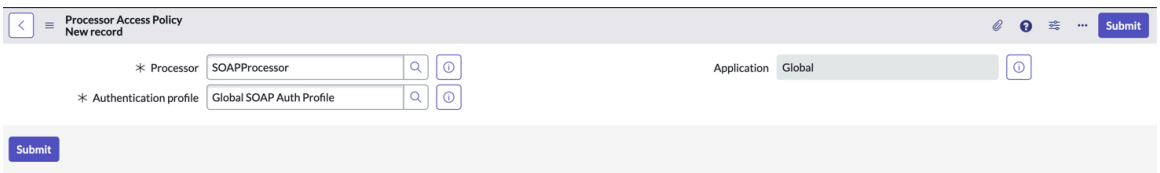
2. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire de la politique d'accès au processus

Champ	Description
Processeur	Nom permettant d'identifier la politique d'authentification. Par exemple, sélectionnez **SOAPProcessor** (Profil d'authentification).
Application	Périmètre de la politique d'authentification. Par défaut : global
Profil d'authentification	Type du profil d'authentification. Sélectionnez **Profil d'authentification SOAP global**.



3. Sélectionnez **Soumettre**.

Critères de filtre pour les API

Les critères de filtre contiennent des conditions ou des requêtes de filtre qui sont utilisées comme entrées de politique pour une politique d'authentification. Les entrées de politique sont utilisées pour regrouper un ou plusieurs critères de filtre et définir les conditions de politique d'une politique d'authentification. Par exemple, un critère de filtre IP définit une adresse IP au format CIDR (Classless Inter-Domain Routing) ou une plage d'adresses IP.

Vous pouvez créer des critères de filtre basés sur l'adresse IP de l'utilisateur, son rôle et le groupe d'utilisateurs auquel il appartient.

Remarque :
Vous pouvez également utiliser les critères de filtre créés à partir du module **Authentification adaptative** . Pour plus d'informations, consultez Authentification adaptative.

Vous pouvez créer des critères de filtre pour les API à l'aide du même processus que les critères de filtre pour l'authentification adaptative. Pour obtenir des détails, consultez Critère de filtre.

Information associée

Créer des critères de filtre IP

Créer un critère de filtre de rôle

Créer un critère de filtre de groupe

Politiques d'authentification API

Les politiques d'authentification évaluent les demandes d'authentification en fonction des conditions de politique spécifiées et autorisent ou refusent l'accès en fonction des critères de correspondance.

Vous pouvez utiliser la stratégie de blocage globale intégrée ou créer une politique d'authentification en fonction de vos exigences de sécurité. La politique de blocage globale refuse les demandes d'authentification des utilisateurs et des API en fonction des critères de filtrage spécifiés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
N’utilisez pas et ne modifiez pas la politique d’autorisation d’accès et la politique de refus d’accès. Ces politiques ne sont destinées qu’aux connexions des utilisateurs.

Créer une politique d’authentification API

Les politiques d’authentification vous permettent d’appliquer des restrictions d’accès sur les API en fonction des critères de filtre spécifiés.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Politique d'authentification API**.
2. Cliquez sur **Nouveau**.
3. Renseignez ces champs du formulaire.

Formulaire de police

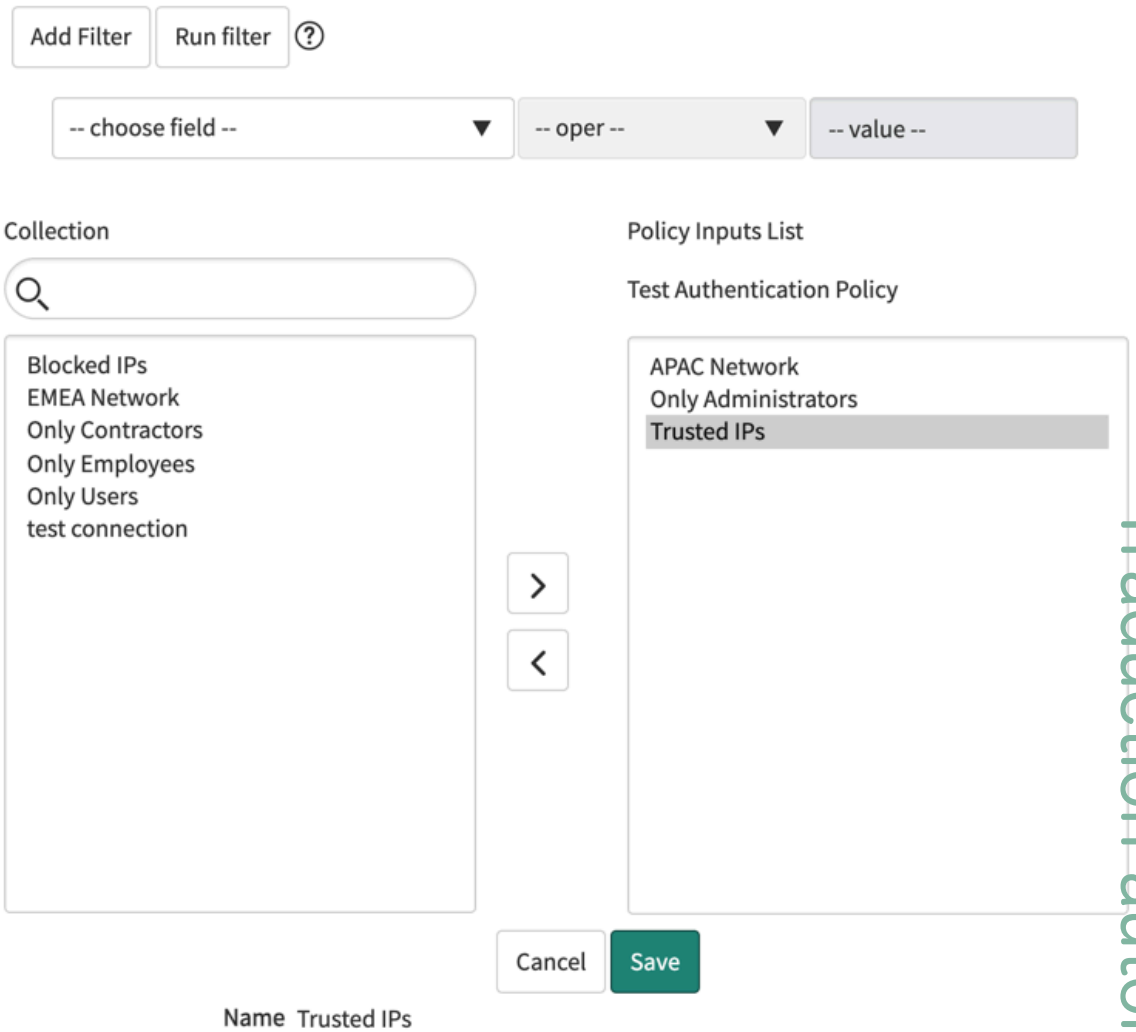
Champ	Description
Nom	Nom permettant d’identifier la politique.
Description	Brève description de la politique.
Application	Périmètre de l'application.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.
5. Dans l’onglet Entrées de politique, sélectionnez **Modifier** pour ajouter les critères de filtre existants.
   Vous pouvez également créer une nouvelle entrée de politique. Pour plus d’informations, consultez Créer des entrées de politique .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Déplacez un ou plusieurs critères de filtre de la liste Collections vers la liste Entrées de



politique.

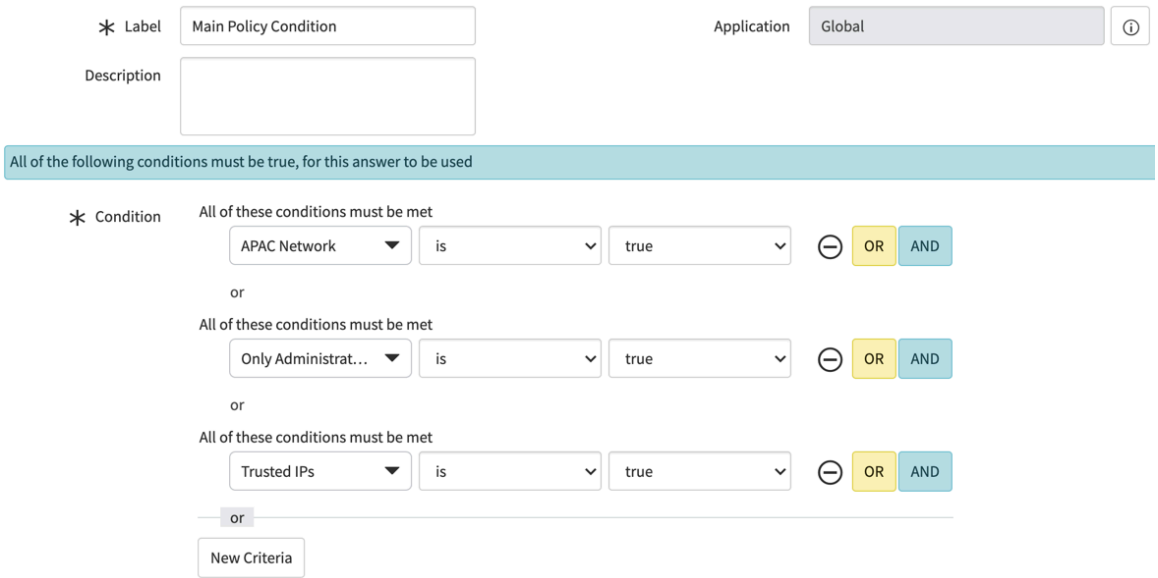
7. Sélectionnez **Enregistrer**.
8. Dans l’onglet Conditions de politique, sélectionnez **Nouveau**.
9. Renseignez ces champs du formulaire.

Formulaire Condition

Champ	Description
Étiquette	Nom de la condition de politique.
Description	Brève description de la condition de politique.
Application	Périmètre de l'application.
Condition	Une ou plusieurs conditions combinées avec le filtre **OU** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



10. Sélectionnez **Soumettre**.

Configurer une politique de blocage globale pour les API

La politique de blocage globale refuse les demandes d'authentification des utilisateurs et des API en fonction des conditions de politique spécifiées. Cette politique peut être utilisée comme alternative au contrôle d'accès à l'adresse IP.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès API** > **Politique de blocage globale**.
2. Dans l'onglet **Entrées de politique** , cliquez sur **Modifier**.
3. Sélectionnez un ou plusieurs critères de filtre dans la liste **Collection** et déplacez-les vers la liste **Politique de blocage globale** .
   Vous pouvez également ajouter des filtres supplémentaires.
4. Dans l'onglet **Conditions de politique** , cliquez sur **Nouveau**.
5. Renseignez les champs suivants du formulaire :

Formulaire de condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtrage) qui est utilisée pour évaluer les demandes d'authentification. Par exemple, vous pouvez créer des conditions qui n'autorisent que les prestataires d'une liste d'adresses IP fiables.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Politique d'accès pour les processeurs système/d'exportation

Possibilité pour les processeurs système/d'exportation d'exploiter la politique d'accès au processeur pour sécuriser tous les points de terminaison d'exportation.

Capacité à sécuriser tous les points de terminaison d'exportation et à appliquer le profil d'authentification entrant et les politiques d'accès du processeur au niveau global ou de l'instance.

Remarque :

- Les processeurs non publics, y compris les processeurs d'exportation tels que CSV, PDF, etc., sont pris en charge pour les politiques d'accès.
- Les processeurs de script sont également pris en charge pour les politiques d'accès.

Exemples de cas d'utilisation

- L'administrateur peut bloquer le processeur RSS s'il n'a pas l'intention de l'utiliser, en tirant parti de la politique d'accès API.
- L'administrateur peut créer un profil d'authentification avec l'authentification de base et associer une politique d'authentification qui renvoie toujours la valeur faux.

  Par exemple, créez des critères IP avec une plage comprise entre `0.0.0.0` et `255.255.255.255` (ajoutez également un espace d'adressage ipv6), puis ajoutez une condition de politique avec l'opérateur false. De cette façon, les conditions de politique seront toujours évaluées comme fausses et la politique d'accès API bloquera l'accès, quelle que soit l'origine de la demande.
- Autoriser l'accès au processeur uniquement à partir d'un réseau de confiance.

Activer la politique d'accès au processeur

Pour Processor, installez le module d'extension Processor Access policy (`com.glide.processor.policy`).

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Les éléments suivants sont installés avec la politique d'accès au processeur :

- Propriété système : com.glide.auth.profile.supported.processor.list
- Module de navigation : politiques d'accès au processeur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d'extension Processor Access Policy (`com.glide.processor.policy`).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Que faire ensuite

.

Configurez le profil d'authentification pour les processeurs, pour plus d'informations, reportez-vous à la section Configurer le profil d'authentification pour le processeur.

Configurer le profil d'authentification pour le processeur

Appliquez le profil d'authentification pour les processeurs d'exportation.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : Processor Access Policy (com.glide.processor.policy)

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Politiques d'accès aux processus**.
2. Pour ajouter un profil d'authentification au processeur, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire de la politique d'accès au processus

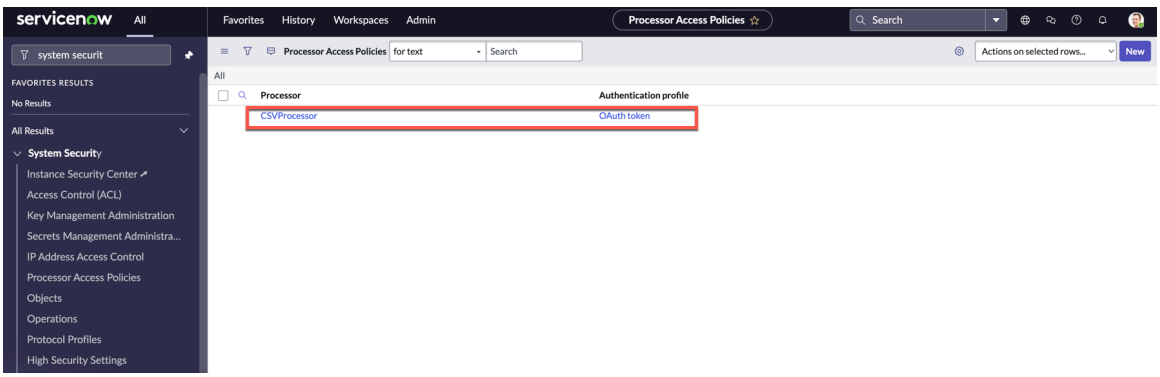
Champ	Description
Processeur	Nom permettant d'identifier la politique d'authentification. **Remarque :** Les processeurs publics ne sont pas pris en charge. Si un processeur non pris en charge est sélectionné, une erreur s'affiche lors de la soumission du processeur.
Application	Périmètre de la politique d'authentification. Par défaut : global
Profil d'authentification	Type du profil d'authentification. Vous pouvez sélectionner **Jeton d'ID** ou **Jeton OAuth**.

4. Cliquez sur **Envoyer**.
   Le profil d'authentification est appliqué au processeur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, le profil d'authentification OAuth est configuré pour le processeur CSV. Dans ce cas, vous devez utiliser le jeton d'accès OAuth pour exporter à l'aide de CSV comme option d'exportation.



Authentification basée sur certificat

L'authentification basée sur certificat vous permet d'authentifier mutuellement les connexions des utilisateurs ou les demandes d'API entrantes à l'aide des certificats d'une autorité de certification (CA) approuvée.

Remarque :
L'authentification basée sur certificat n'est pas prise en charge sur l'instance On-Prem et Edge Encryption.

Authentification basée sur certificat pour les connexions à l'interface utilisateur

Permettez aux utilisateurs finaux d'utiliser des cartes PIV (Personal Identity Filification) ou CAC (Common Access Card) pour se connecter Now PlatformPortail de services ou au lieu d'utiliser un nom d'utilisateur et un mot de passe. Pour configurer l'authentification réciproque pour les connexions à l'interface utilisateur, reportez-vous à la section Configurer l'authentification basée sur certificat.

Une fois l'authentification basée sur certificat configurée, les utilisateurs finaux peuvent finaliser leur configuration et se connecter. Consultez Se connecter à l'aide de l'authentification basée sur certificat.

Authentification basée sur certificat pour les services Web entrants

Authentifiez les demandes entrantes aux ServiceNow API SOAP et REST. Pour configurer l'authentification réciproque des services Web entrants, reportez-vous à la section Configurer l'authentification basée sur certificat.

Configurer l'authentification basée sur certificat

Configurez l'authentification réciproque pour les connexions basées sur l'interface utilisateur ou les services Web entrants.

Avant de commencer

Rôle requis : administrateur

Vérifiez que votre instance utilise un équilibreur de charge ADCv2. Pour plus d'informations, consultez l'article de labase de connaissances Migration ADCv2 . Si votre instance n'utilise pas l'équilibreur de charge ADCv2, contactez Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Configurez l’authentification basée sur certificat pour :

- Autorisez les utilisateurs finaux à se connecter en toute sécurité au ou Portail de services à l’aide de Now Platform cartes PIV ou CAC. Une fois l’authentification basée sur certificat activée, vous pouvez enregistrer vous-même le certificat PEM ou un administrateur peut mapper le certificat pour vous. Consultez Se connecter à l’aide de l’authentification basée sur certificat.
- Activez l’authentification réciproque pour les services Web entrants. Une fois l’authentification basée sur certificat configurée, le système utilise les certificats fournis pour s’authentifier mutuellement les demandes d’accès aux ServiceNow API REST et SOAP.

Activer l’authentification basée sur certificat

Vous pouvez activer le module d’extension d’authentification basée sur certificat (com.glide.auth.mutual) si Now Platform vous disposez du rôle administrateur.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Les tables suivantes sont installées avec l’authentification basée sur certificat :

- sys_user_certificate
- sys_ca_certificate
- sys_ca_certificate_api_track

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d’extension Certificate Based Authentication (com.glide.auth.mutual).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée.

Enregistrer le certificat de l’autorité de certification

Enregistrez les certificats racines ou intermédiaires pour qu'ils soient disponibles à l'authentification.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Authentification basée sur certificat** > **Chaîne de certificats CA**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs suivants du formulaire :

Formulaire de certificat d'authentification de l'autorité de certification mutuelle

Champ	Description
Nom	Nom permettant d'identifier le certificat.
Notification d'échéance	Option permettant d'avertir les utilisateurs lorsqu'un certificat est sur le point d'expirer.
Notification à l'expiration	Liste des utilisateurs à notifier lorsque le certificat expire.
Avertissement avant l'expiration (en jours)	Nombre de jours pendant lesquels une notification est envoyée aux utilisateurs avant l'expiration d'un certificat.
Actif	Option permettant d'activer le certificat client.
Format	PEM
Type	Type de certificat. Les options incluent : ○ **Certificat CA** : certificat de l'autorité de certification racine. Peut également inclure des certificats intermédiaires dans la chaîne. Les certificats CA sont automatiquement synchronisés avec l'équilibreur de charge. Utilisez cette option lorsque cela est possible pour éviter de manquer un certificat requis dans la chaîne. ○ **Certificat intermédiaire** : un certificat intermédiaire dans la chaîne de certificats. Ce certificat reste sur l'instance uniquement et n'est pas synchronisé avec l'équilibreur de charge. N'utilisez cette option que si vous avez besoin d'ajouter un certificat intermédiaire à une chaîne existante.
Description brève	Brève description du certificat client de l'utilisateur.

Remarque :
Lors du chargement du certificat, les champs en lecture seule **Valide à partir de**, **Expire,Expire dans jours**, **Émetteur** et **Objet**, **Chaîne de certificats** et **Certificat PEM** sont extraits et renseignés automatiquement.

4. Cliquez sur **Envoyer**.
5. **Facultatif :** Cliquez sur **Valider les magasins/certificats pour valider** le certificat.

Mapper le certificat PEM à l'utilisateur

Mappez les certificats PEM aux utilisateurs pour leur permettre de se connecter à l'aide de cartes PIV ou CAC ou pour authentifier les demandes entrantes. Vous pouvez mapper plusieurs certificats PEM à un utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Rôle requis : administrateur
- Assurez-vous de disposer du certificat PEM (Privacy Enhanced Mail) de l'utilisateur.

Remarque :
Une fois le certificat PEM mappé à la configuration utilisateur, « vérifier le certificat » échouera. Cela est dû au fait que le certificat PEM n'est pas stocké.

Procédure

1. Accédez à la **Tout** > **Authentification basée sur certificat** > **Utilisateur vers Mappage de certificat** et cliquez sur **Nouveau**.
2. Renseignez les champs suivants du formulaire :

Formulaire Certificat client utilisateur

Champ	Description
Nom	Nom du certificat client de l'utilisateur.
Notification d'échéance	Option permettant d'avertir les utilisateurs lorsqu'un certificat est sur le point d'expirer.
Avertissement avant l'expiration (en jours)	Nombre de jours pendant lesquels une notification est envoyée aux utilisateurs avant l'expiration d'un certificat.
Notification à l'expiration	Liste des utilisateurs à notifier lorsque le certificat expire.
Actif	Option permettant d'activer le certificat client.
Utilisateur	Utilisateur mappé au certificat client. Le système reçoit le certificat client à partir de la demande entrante ou de l'enregistrement du certificat, puis utilise l'utilisateur désigné dans ce champ pour lancer une session afin d'exécuter la demande.
Description brève	Brève description du certificat client de l'utilisateur.
Format	Le format PEM (Privacy Enhanced Mail) est un certificat DER (Distinguished Encoding Rules) codé en base 64.
Type	Cert. client Ce champ est en lecture seule.

Remarque :
Lors du chargement du certificat, les champs en lecture seule **Valide à partir de**, **Expire,Expire in days**, **Émetteur** et **Objet** sont extraits et renseignés automatiquement.

3. Cliquez sur l'icône Pièces jointes et chargez le certificat.
4. Cliquez sur **Envoyer**.
   Le certificat est validé et mappé à l'utilisateur spécifié si le certificat provient d'une autorité de certification (CA) approuvée.

Configurer les propriétés d'authentification basée sur certificat

Utilisez les propriétés système pour activer ou désactiver les fonctionnalités d'authentification basée sur certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification basée sur certificat** > **Propriétés**.
2. Renseignez les champs suivants du formulaire :

Formulaire Propriétés de l'authentification basée sur certificat

Propriété	Description
Activer l'authentification basée sur certificat	Option permettant d'activer l'authentification basée sur certificat pour les connexions à l'interface utilisateur et les services Web entrants. Valeur par défaut : true
Afficher l'option « Se connecter avec PIV/CAC » sur l'écran de connexion	Affiche l'option **Se connecter avec la carte PIV/CAC** sur l'écran de connexion. Permet aux utilisateurs de se connecter à l'aide de l'authentification basée sur certificat à l'aide de l'interface utilisateur. Valeur par défaut : false
Activer la redirection automatique pour la connexion basée sur certificat	Détermine s'il faut exiger que l'utilisateur clique sur **Se connecter avec la carte PIV/CAC** après avoir sélectionné un certificat enregistré et saisi son code PIN. Activez cette option pour connecter automatiquement l'utilisateur une fois qu'il a sélectionné un certificat client enregistré et saisi son code PIN. Désactivez cette option pour exiger que l'utilisateur clique sur **Se connecter avec la carte PIV/CAC** après avoir sélectionné un certificat client enregistré et entré son code PIN. Valeur par défaut : false

Se connecter à l'aide de l'authentification basée sur certificat

Après avoir configuré l'authentification basée sur certificat, votre administrateur peut enregistrer le certificat client et vous connecter à l'aide de votre carte PIV (Personal Identity Verification) ou CAC (Common Access Card).

Enregistrer le certificat client pour votre carte PIV ou CAC

Avant de vous connecter à Now Platform à l'aide de votre carte PIV ou CAC, vous devez enregistrer le certificat client de votre carte PIV ou CAC. Si vous ne parvenez pas à enregistrer le certificat client, contactez votre administrateur. Votre administrateur peut également enregistrer le certificat client de votre carte PIV ou CAC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Assurez-vous que l'authentification basée sur certificat est activée.
- Assurez-vous qu'un lecteur de carte est connecté à votre ordinateur et que votre carte PIV ou CAC est insérée.
- Rôle requis : aucun

Pourquoi et quand exécuter cette tâche

Si vous avez besoin d'un administrateur pour enregistrer votre certificat client, reportez-vous à la section Mapper le certificat PEM à l'utilisateur.

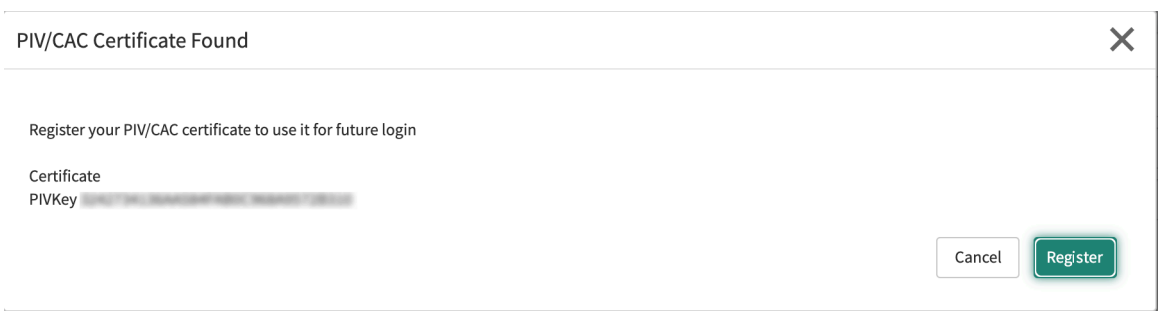
Procédure

1. Connectez-vous à Now Platform à l'aide de votre nom d'utilisateur et de votre mot de passe.
2. Cliquez sur votre nom dans le **menu utilisateur** et sélectionnez **Profil**.



3. Dans les **liens connexes**, cliquez sur **Enregistrer le certificat client**.

   Si un certificat valide est disponible, le message suivant s'affiche :



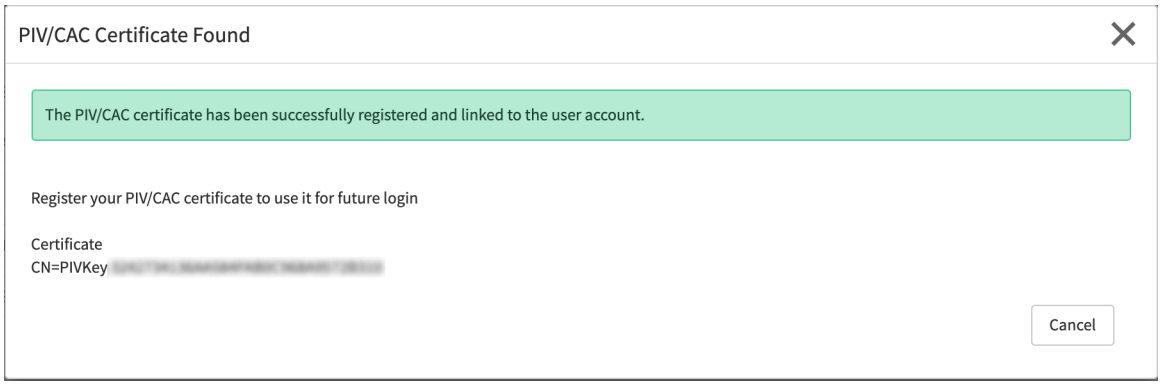
4. Cliquez sur **Inscrire**.

   Une fois l'inscription réussie, le message suivant s'affiche :

   Le certificat PIV/CAC a été correctement enregistré et lié au compte utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La prochaine fois que vous vous connecterez à votre Now Platform, vous pourrez vous connecter à l'aide de votre carte PIV ou CAC. Pour plus d'informations, consultez Se connecter à l'aide de Now Platform la carte PIV ou CAC.

Se connecter à l'aide de Now Platform la carte PIV ou CAC

Vous pouvez vous connecter avec votre carte PIV ou CAC au lieu du nom d'utilisateur et du mot de passe lorsque l'authentification basée sur certificat est activée sur Now Platform.

Avant de commencer

- Rôle requis : aucun
- Assurez-vous que l'authentification basée sur certificat est activée.
- Assurez-vous qu'un lecteur de carte PIV ou CAC est connecté à votre ordinateur.
- Assurez-vous qu'un certificat client de votre carte PIV ou CAC est mappé à vous. Pour plus d'informations, consultez Enregistrer le certificat de l'autorité de certification.

Procédure

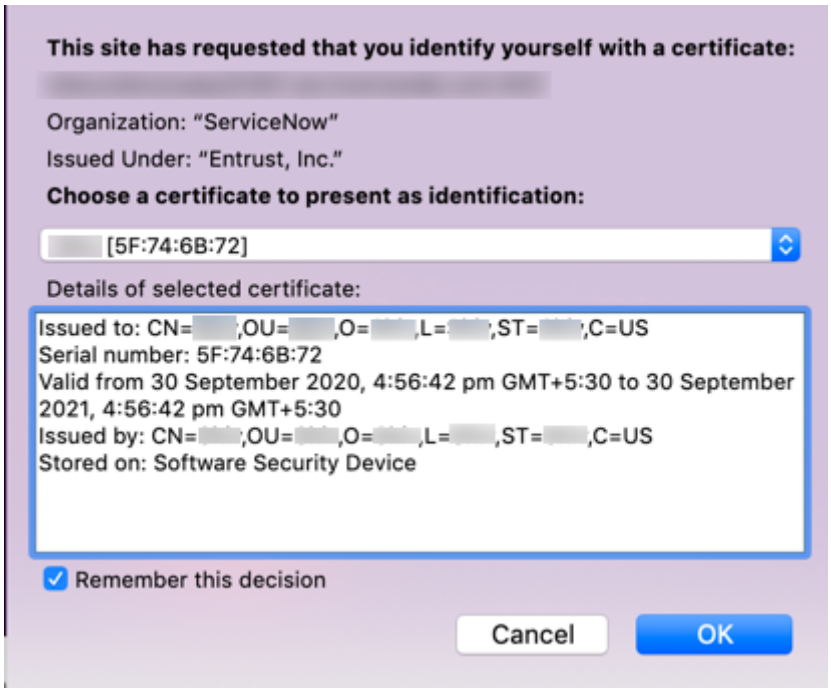
1. Insérez votre carte PIV ou CAC dans le lecteur de carte.
2. Accédez à votre instance dans un navigateur.
   Le navigateur vous demande de saisir un code PIN pour votre carte PIV ou CAC.
3. Saisissez le code PIN de votre carte PIV ou CAC dans l'invite du navigateur.

   Remarque :
   En cas d'oubli de votre code PIN, contactez votre administrateur.

4. Si vous entrez le code PIN correct, le navigateur vous invite à sélectionner un certificat.

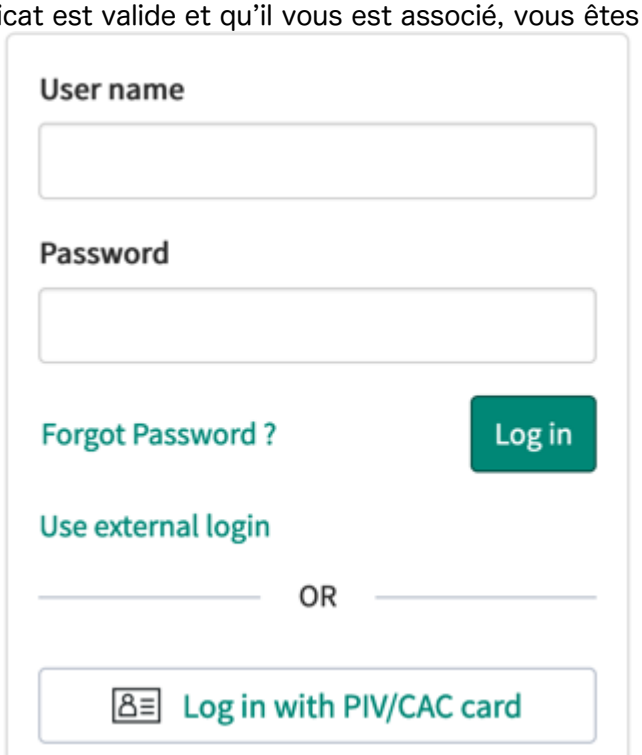
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez un certificat à partir de l'invite du navigateur.

   Si le certificat est valide et qu'il vous est associé, vous êtes redirigé vers la page de connexion.



6. Cliquez sur le bouton **Se connecter avec la carte PIV/CAC** .

   Pour vous déconnecter de Now Platform, vous devez supprimer le PIV ou le CAC du lecteur de carte, puis fermer le navigateur.

Gérer vos certificats clients

Affichez et supprimez les certificats clients associés à votre compte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Assurez-vous que l'authentification basée sur certificat est activée.
- Rôle requis : aucun

Procédure

1. Connectez-vous à l'aide Now Platform de votre nom d'utilisateur et de votre mot de passe.
2. Cliquez sur votre nom dans le **menu utilisateur** et sélectionnez **Profil**.



3. Dans les **liens connexes**, cliquez sur **Gérer vos certificats clients**.
   La table Certificats clients utilisateur [sys_user_certificate] s'ouvre et affiche les certificats associés à votre compte.
4. Affichez ou supprimez les certificats associés à votre compte.

Association d'URL personnalisées à votre instance

Vous pouvez rendre votre instance accessible à partir d'une URL personnalisée ou portant la marque de l'entreprise ServiceNow .

Vue d'ensemble des URL personnalisées

Vous pouvez utiliser une URL personnalisée pour permettre ServiceNow à l'instance d'être accessible à partir d'une ou de plusieurs URL personnalisées ou portant la marque de l'entreprise.

Les URL personnalisées peuvent être associées à un portail spécifique. Par exemple, l'administrateur peut définir http://support.acme.com pour le portail CSM et http://hr.acme.com pour le portail RH. Dans une telle situation, il est nécessaire de rediriger les utilisateurs vers différents IdP pour authentification sur la base de l'URL personnalisée à laquelle les utilisateurs accèdent.

Important :

- Ne créez pas d'URL personnalisée avec plus de 100 domaines par instance.
- Vous devez d'abord supprimer l'enregistrement d'URL personnalisée de l'instance ServiceNow , puis supprimer toutes les entrées du serveur de noms de domaine (DNS) du serveur DNS.
- Toute suppression d'une entrée DNS du serveur DNS avant la suppression d'un enregistrement d'URL personnalisée de l'instance ServiceNow entraînerait le blocage de la suppression des autres enregistrements d'URL personnalisées correspondants de ServiceNow.

À partir de Tokyo, vous pouvez autoriser les utilisateurs à rediriger automatiquement vers les IdP spécifiés définis dans l'enregistrement d'URL personnalisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les URL personnalisées ne sont pas disponibles pour les clients sur site ou les instances de développeur. En outre, l'URL doit être accessible au public.

Seul le propriétaire du domaine de niveau supérieur (TLD) ou de tout sous-domaine peut configurer l'URL personnalisée pour un sous-domaine DNS. Par exemple, votre instance peut avoir l'URL désignée suivante et des URL personnalisées supplémentaires :

Exemple d'URL personnalisée

Exemples d'URL	Utilisation
https://acme.service-now.com	Le nom de domaine initial pour Acme fourni avec l'instance ServiceNow .
https://support.acme.com	URL personnalisée qui s'associe à votre ServiceNow instance. Cette URL est appelée alias (CNAME) du nom de domaine initial.
https://US-support.acme.com	URL personnalisée secondaire qui s'associe à un portail de services sur votre instance. Votre instance peut prendre en charge plusieurs URL personnalisées vers le même portail de services.

Considérations relatives aux URL personnalisées en dehors de votre instance

Avant de pouvoir associer une URL personnalisée, vous devez posséder (ou acheter) une URL par l'intermédiaire d'un fournisseur de domaine. Certaines configurations spécifiques sont également nécessaires avant de pouvoir créer et associer une URL personnalisée sur votre instance.

Configurations d'URL personnalisées

Éléments de configuration	Description
Définir le CNAME avec le fournisseur	L'enregistrement CNAME doit être défini comme l'URL de l'instance ServiceNow .
Déterminer votre statut VIP dédié	Le statut de VIP.

Remarque :
Lors de la suppression ou de la mise à jour d'enregistrements CNAME qui pointent vers votre instance, vous devez suivre cette séquence pour éviter de faire pendre des enregistrements dans l'instance. Tout d'abord, supprimez les enregistrements CNAME de votre instance, puis supprimez ou mettez à jour le paramètre CNAME de votre fournisseur DNS.

Activer les URL personnalisées

Activez la configuration des URL personnalisées sur votre ServiceNow instance. Vous pouvez activer le module d'extension URL personnalisée (com.snc.customurl) si vous disposez du rôle administrateur.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Modules d'extension**.
2. Recherchez et cliquez sur le module d'extension **URL personnalisée** .

> **Remarque :**
> Ne sélectionnez pas le module **d'extension URL personnalisée - interne** , qui est un composant interne pour les API d'URL personnalisées scriptées.

3. Dans l'enregistrement URL personnalisée, cliquez sur le lien connexe **Activer/Réparer** .
4. Dans la fenêtre Activation du module d'extension, cliquez sur **Activer**.
   Lorsque la fenêtre d'activation du module d'extension s'ouvre à nouveau avec un message indiquant que le module d'extension est activé, cliquez sur **Fermer et recharger le formulaire** pour rester sur ce formulaire.
5. Dans la liste connexe Fichiers du module d'extension, recherchez la propriété suivante et modifiez la valeur du paramètre :

Option	Description
glide.customurl.enabled	Pour activer les URL personnalisées, définissez la valeur sur **Vrai**. Par défaut, cette propriété est définie sur **Faux**, ce qui signifie que vous ne pouvez pas associer d'URL personnalisée. **Remarque :** Pour désactiver cette fonctionnalité, redéfinissez cette propriété sur **Faux**.

6. Cliquez sur **Mettre à jour**.

Définir une URL personnalisée comme URL d'instance

Ajoutez une URL personnalisée à votre configuration d'instance à utiliser à la place de votre ServiceNow URL.

Avant de commencer

Rôle requis : administrateur

Vous devez activer le module d'extension URL personnalisée et avoir acheté ou enregistré une URL avant d'ajouter l'URL personnalisée à votre instance.

Procédure

1. Accédez à la **Tout** > **URL personnalisée** > **URL personnalisées**.
2. Vous devez soit :
   - Cliquez sur **Nouveau** pour associer un nouveau nom de domaine à votre instance.
   - Sélectionnez une URL personnalisée déjà configurée pour être définie en tant qu'URL de votre instance.
3. Renseignez les champs appropriés :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'URL personnalisés

Champ	Description
Nom du domaine	Nom de domaine complet (FQDN) de l'URL personnalisée. Le nom de domaine complet (FQDN) est une redirection CNAME créée dans l'enregistrement du serveur de noms pour le domaine personnalisé. **Remarque :** Par exemple, dans le serveur de noms pour acme.com, vous pouvez créer une entrée : `support.acme.com 300 IN CNAME acme.servicenow.com`
Est une URL d'instance	Case à cocher permettant d'activer cette URL personnalisée pour toutes les URL sortantes. Une seule URL personnalisée active peut être l'URL de l'instance. Pour activer ce paramètre pour une URL personnalisée, cliquez sur **Définir comme URL d'instance** sur l'enregistrement URL. Toutes les URL personnalisées précédentes sont alors supprimées.
Statut	État de l'enregistrement d'URL personnalisée. Si l'état est **Actif**, l'URL personnalisée est mise en service et prête à l'emploi.
Portail de services	Portail de services que vous souhaitez utiliser lorsque vous redirigez les utilisateurs vers votre instance à l'aide de l'URL personnalisée.
Fournisseur d'identité	Le fournisseur d'identité pour l'URL personnalisée vous permet d'autoriser les utilisateurs à rediriger automatiquement vers les IdP spécifiés définis dans l'enregistrement d'URL personnalisée.

Une URL personnalisée doit s'activer dans les six heures sur votre instance.

Remarque :

- Vous devez d'abord supprimer l'enregistrement d'URL personnalisée de l'instance ServiceNow , puis supprimer toutes les entrées du serveur de noms de domaine (DNS) du serveur DNS.
- Toute suppression d'une entrée DNS du serveur DNS avant la suppression d'un enregistrement d'URL personnalisée de l'instance ServiceNow entraînerait le blocage de la suppression des autres enregistrements d'URL personnalisées correspondants de ServiceNow.

URL personnalisée avec fournisseur d'identité

Définissez votre URL personnalisée auprès du fournisseur d'identité pour permettre à l'utilisateur de se connecter avec son fournisseur d'identité.

Traduction automatique

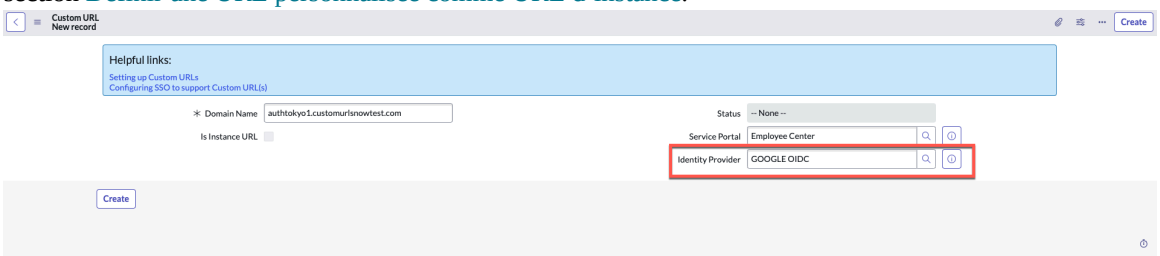
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur

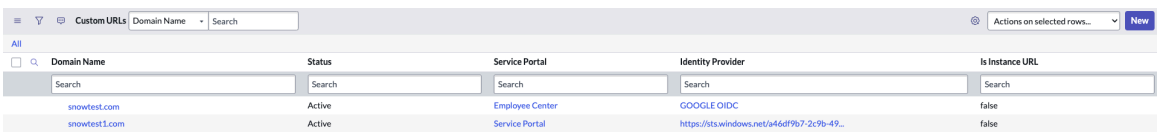
Procédure

1. Accédez à la **Tout** > **URL personnalisée** > **URL personnalisées**.
2. Cliquez sur **Nouveau**.
3. Fournissez les détails de l'IdP dans le champ **Fournisseur d'identité** .
   Pour en savoir plus sur les autres champs, reportez-vous à la section Définir une URL personnalisée comme URL d'instance.



4. Cliquez sur **Créer**.

   L'enregistrement est créé et affiché sur la page URL personnalisée.



   Lors de l'accès à l'URL personnalisée, l'utilisateur est redirigé vers le fournisseur d'identité configuré. Dans ce cas, en accédant au snowtest.com, l'utilisateur est dirigé vers Centre des **employés**, puis redirigé vers le fournisseur d'identité Google .

   Remarque :

   - Si le Portail de services champ est vide et que le champ Fournisseur d'identité est défini, lorsque l'utilisateur accède à l'URL personnalisée, il est directement dirigé vers le fournisseur d'identité configuré.
   - Si le champ et le fournisseur d'identité Portail de services sont définis, lorsque l'utilisateur accède à l'URL personnalisée avec le Portail de services qui est défini, l'utilisateur est dirigé vers le fournisseur d'identité configuré.
   - Si le champ et le Portail de services fournisseur d'identité sont définis, lorsque l'utilisateur accède à l'URL personnalisée avec un autre portail qui n'est pas défini, il est dirigé vers le fournisseur d'identité de redirection automatique s'il est configuré sur l'instance.

5. Utilisez les informations d'identification pour vous connecter à l'application.

URL personnalisée Informations sur l'emploi du centre de données

Chaque URL personnalisée associée à votre instance a une tâche de centre de données ServiceNow correspondante qui s'exécute et affiche les informations d'URL pertinentes pour votre instance, comme décrit dans la table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ du poste	Description
ID de tâche	ID unique de la tâche qui vérifie le domaine de l'URL personnalisée.
Dernière exécution à	Date et heure de la dernière exécution de la tâche.
Charge utile	Liste de domaines ou d'URL personnalisées qui ont été envoyés au centre de données pour la mise en service CERT.
Nombre d'interrogations	Nombre de sondages effectués pour cette tâche dans les résultats.
Résultat	Vérifie et valide chaque domaine ou URL personnalisée envoyée dans une charge utile.
Statut	Statut de la tâche du centre de données.

Générer des métadonnées SP pour les installations d'URL personnalisées SAML/SSO

Une installation SAML ou SSO a besoin des métadonnées SP générées pour l'IdP avant que l'instance d'URL personnalisée ne les génère.

Avant de commencer

Rôle requis : administrateur

L'IdP a besoin des métadonnées du portail de services pour que l'instance puisse s'authentifier et transmettre les demandes.

Remarque :
L'ajout de l'URL du service consommateur d'assertion (URL de connexion SP) peut être différent pour chaque IdP (Azure, ADFS ou Okta).

Procédure

1. Choisissez votre module d'extension SSO installé :

Option	Description
Authentification unique (SSO) de plusieurs fournisseurs	Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**. Choisissez un IdP et cliquez sur le bouton **Générer les métadonnées** . L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres des propriétés système.
SAML 2 SSO	Accédez à la **Authentification unique SAML 2** > **Métadonnées**. L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres des propriétés système.

2. Copiez les métadonnées du portail de services dans la zone de texte.

Par exemple :

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="https://yourinstance.service-now.com">
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
 <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
 <AssertionConsumerService isDefault="true" index="0"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://yourinstance.service-now.com/navpage.do" />
 <AssertionConsumerService index="1"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Fournissez les métadonnées du fournisseur de services d'instance à l'IdP.
   Par exemple, SSOCircle permet à un utilisateur de fournir les métadonnées SP en ligne.
4. **Facultatif :** Pour configurer des URL personnalisées dans Azure :
   a. Accédez à **Inscriptions de l'application**.
   b. Sélectionnez **Toutes les applications** dans le menu.
   c. Sélectionnez **l'application ServiceNow**.
   d. Cliquez sur Paramètres pour configurer l'URL.
5. **Facultatif :** Pour configurer des URL personnalisées dans Okta :
   a. Créez deux ServiceNow applications Okta UD.
   b. Une application Okta pour l'URL d'instance « service-now.com ».
   c. Une application Okta pour l'URL personnalisée.

   Remarque :
   - Désactivez la **désactivation forcée de l'authentification** dans la configuration Okta pour que le **test de la connexion** s'exécute correctement.
   - Si vous testez l'enregistrement du fournisseur d'identité associé à l'URL de base, assurez-vous de vous connecter à l'instance avec l'URL de base.
   - Si vous testez le fournisseur d'identité associé à l'URL personnalisée, assurez-vous de vous connecter à l'instance avec l'URL personnalisée.
6. **Facultatif :** Pour utiliser l'authentification OAuth, configurez l'URL de redirection comme toutes les URL personnalisées enregistrées dans la configuration du point de terminaison de l'application OAuth pour les applications clientes externes.
   L'URL de redirection est synonyme de l'URL de rappel vers laquelle le serveur d'autorisation redirige.
7. **Facultatif :** Pour utiliser le service Google reCAPTCHA, configurez une paire de clés API.

Erreurs et correctifs d'URL personnalisées

Une liste des erreurs courantes et des correctifs associés pour l'installation et la configuration d'une URL personnalisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de l'installation

Message d'erreur	Corriger
Impossible de créer une URL personnalisée. Réessayez ultérieurement.	Il se peut qu'un problème indépendant de votre volonté interfère avec la création de l'URL personnalisée. Exécutez à un autre moment avant de contacter l'assistance. **Remarque :** La création d'une URL personnalisée prend généralement 30 minutes. Si cela prend plus de temps, contactez https://support.servicenow.com/now?draw=case.
Impossible de soumettre votre nouvelle demande URL personnalisée, car une autre demande URL personnalisé pour votre instance est toujours en cours.	Vérifiez l'état de vos tâches URL personnalisées avant d'envoyer une nouvelle demande.
Vous devez effacer les propriétés suivantes pour pouvoir définir l'URL de l'instance : proxy Glide, servlet Glide.	
La mise en service de <custom_domain> est toujours en cours. Ce processus peut prendre jusqu'à X heures. Votre administrateur d'instance recevra une notification une fois ce processus terminé.	Une fois que la mise en service d'une URL personnalisée sur une instance a commencé, vous devez attendre que le processus se termine avant que l'état ne change.
<custom_domain> est maintenant définie comme la nouvelle URL d'instance. <base.service-now.com> est toujours en service, mais toutes les nouvelles URL, par exemple dans les notifications, utiliseront <custom_domain>.	Une seule URL peut être désignée comme URL d'instance. Les autres URL associées à votre instance peuvent être actives, mais seule l'URL de l'instance peut utiliser des notifications.
L'URL personnalisée <custom_domain> est définie pour être immédiatement supprimée de la configuration d'instance et revenir à <base.service-now.com>. <custom_domain> continue une association à cette instance tant que l'enregistrement CNAME dans votre DNS est défini.	Ce message confirme que vous avez l'intention de modifier votre URL personnalisée. En acceptant cette confirmation, vous initiez le changement de l'URL en votre instance. Toute URL figurant sur votre liste de noms de domaine, en tant qu'URL personnalisée, peut être active, sauf si vous la supprimez de l'enregistrement CNAME de votre fournisseur.
Vous ne pouvez pas modifier glide.servlet.uri. Cette propriété est définie par URL personnalisée.	
Vous ne pouvez pas modifier glide.proxy.host. Cette propriété est définie par URL personnalisée.	
L'enregistrement CNAME pour <custom_domain> ne pointe pas vers <base.service-now.com>.	La configuration côté fournisseur d'URL n'est pas correcte. Vérifiez votre configuration sur l'enregistrement CNAME.
Enregistrement CNAME manquant pour <custom_domain>.	L'enregistrement CNAME doit être configuré à partir de votre fournisseur d'URL pour pouvoir définir l'URL personnalisée pour votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sorties d'installation

Les sorties d'installation sont des personnalisations qui quittent Java pour appeler un script avant de revenir à Java.

Remarque :
Les fonctionnalités décrites ici nécessitent le rôle **admin.**

Sorties d'installation disponibles

Accédez à la **Définition du système** > **Sorties d'installation**. Certains noms de sortie d'installation (Login, Logout, ValidatePassword, ExternalAuthentication) sont réservés et ne peuvent pas être modifiés. Les autres sorties d'installation peuvent être remplacées par un script personnalisé qui remplace le script dans la sortie d'installation par défaut.

Les sorties d'installation suivantes sont disponibles dans le système de base :

Sortie de l'installation	Description
Connexion	Prend une paire de nom d'utilisateur et de mot de passe et s'authentifie avec l'objet utilisateur
Déconnecter	Dirige l'utilisateur vers la page d'accueil lorsqu'il se déconnecte. peut être remplacé par LogoutRedirect
Redirection de déconnexion	Dirige l'utilisateur vers une URL spécifiée lors de la déconnexion
Authentification externe	Authentifie à l'aide d'un en-tête, d'un paramètre ou d'un cookie ; peut être remplacé par DigestSingleSignOn et PGPSingleSignOn
Synthèse d'authentification unique	Authentifie à l'aide d'un en-tête, d'un paramètre ou d'un cookie et déchiffre le chiffrement Digest
PGPSingleSignOn	Authentifie à l'aide d'un en-tête, d'un paramètre ou d'un cookie et déchiffre le chiffrement PGP
ValidatePassword (en anglais seulement)	Actif par défaut, à partir de la Helsinki mise en production ; permet aux clients de définir leur propre validation de mot de passe ; peut être remplacé par ValidatePasswordStronger
ValiderMotDePassePlus Fort	Exige que les mots de passe comportent au moins 8 caractères dont un chiffre, une lettre majuscule et une lettre minuscule
GetIntegrationSessionTimeout	Implémente le comportement d'expiration de session d'intégration par défaut.

Traduction automatique

Modifications de connexion

La modification suivante de la sortie d'installation de **connexion** définit la valeur de délai d'expiration de session de chaque utilisateur au moment de la connexion de l'utilisateur. Dans cet exemple particulier, si le nom d'utilisateur est *admin*, la session est définie pour expirer au bout de 30 secondes.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

      process : function() {
```

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
        // the request is passed in as a global
        var userName = request.getParameter("user_name");
        var userPassword = request.getParameter("user_password");

        var authed = GlideUser.authenticate(userName, userPassword);
        if (authed) {
          // ************************************************************
          // customization - if the userName == admin, set the session
          // timeout to be 30 seconds. You can implement your own
          // session timeout algorithm here by checking to see if a user
          // belongs to a certain group or has a certain role.
          // Values of setMaxInactiveInterval exceeding 1440 minutes are
          // treated as one day (1440 minutes).

         if (userName == "admin") {
            request.getSession().setMaxInactiveInterval(30);
          }
          // ************************************************************
          return GlideUser.getUser(userName);
        }

        this.loginFailed();

        return "login.failed";
      },

      loginFailed : function() {
        var message = GlideSysMessage.format("login_invalid");
        var gSession = GlideSession.get();
        gSession.addErrorMessage(message);

        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", "", userName, "");
      }

}
```

Le délai d'expiration de la session peut également être défini en fonction de l'adresse IP.

```
gs.include("PrototypeServer");

var Login = Class.create();
Login.prototype = {
 initialize : function() {
 },

      process : function() {
        // the request is passed in as a global
        var userName = request.getParameter("user_name");
        var userPassword = request.getParameter("user_password");

        var authed = GlideUser.authenticate(userName, userPassword);
        if (authed) {

        // ************************************************************
        // customization - if the user is logging in from a particular IP
        // range starting with XXX.XXX you can implement your own
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
        // session timeout algorithm here by checking the login IP
        //
        // Values of setMaxInactiveInterval exceeding 1440 minutes are
        // treated as one day (1440 minutes).

        var clientIP = gs.getSession().getClientIP().toString();

        // if client IP starts with specified range
        if (clientIP.indexOf('XXX.XXX') == 0) {
          // set to 10 hours
          request.getSession().setMaxInactiveInterval(60 * 60 * 10);
        }
        // ************************************************************

          return GlideUser.getUser(userName);
        }

        this.loginFailed();

        return "login.failed";
      },

      loginFailed : function() {
        var message = GlideSysMessage.format("login_invalid");
        var gSession = GlideSession.get();
        gSession.addErrorMessage(message);

        var userName = request.getParameter("user_name");
        EventManager.queue("login.failed", "", userName, "");
      }

}
```

Information associée

Appliquer des mots de passe forts

Authentification basée sur la plage IP

Une façon de sécuriser une application Web consiste à restreindre l'accès en fonction de l'adresse IP.

Vous pouvez bloquer l'accès à une adresse spécifique ou à une plage d'adresses que vous soupçonnez d'appartenir à des personnes malveillantes. L'instance vous permet de contrôler l'accès par adresse IP.

Remarque :
Utilisez la politique de contexte de pré-authentification d'Authentification adaptative (AA) pour appliquer des authentifications basées sur IP et des restrictions pour des options supplémentaires. Pour plus d'informations, consultez Authentification adaptative.

Remarques et limitations :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le système ne vous laissera pas vous verrouiller, donc si vous essayez d'ajouter une règle de sorte que votre adresse actuelle serait verrouillée, le système vous avertit et refuse votre insertion.
- Si vous êtes à l'intérieur d'un intranet d'entreprise, soyez très prudent lors de la configuration de vos règles en matière de propriété intellectuelle. L'adresse IP que vous voyez sur votre propre ordinateur (comme 10.10.10.25) n'a généralement aucun rapport avec l'adresse IP que vous apparaîtrez réellement sur Internet. Votre entreprise proxys et/ou NAT proxysent probablement votre adresse dans un ensemble prévisible d'adresses sortantes que vous devrez probablement interroger votre équipe réseau.
- Un utilisateur dont l'accès est restreint en fonction d'une règle d'accès reçoit une erreur 403 sur son navigateur.
- Les utilisateurs restreints n'utilisent pas de transactions, de sémaphores ou ne comptent pas dans le décompte des ressources serveur.
- Cette fonctionnalité ne remplace ni ne remplace vos règles de contrôle d'accès existantes si, par exemple, vous utilisez un VPN pour accéder à notre centre de données. Il s'agit d'une vérification supplémentaire qui doit être effectuée en plus des contrôles d'accès que nous avons éventuellement mis en place sur votre PIX.
- Les règles d'autorisation ont toujours priorité sur les règles de refus. Donc, si une adresse est à la fois autorisée (par une règle) et refusée (par une deuxième règle), elle est, en fait, autorisée.
- Les astérisques et les blocs CIDR ne sont actuellement pas pris en charge.
- En ce qui concerne les adresses proxy transférées, les règles d'autorisation sont appliquées à chaque adresse de la chaîne, puis les règles de refus sont appliquées à chaque adresse de la chaîne si aucune des règles d'autorisation ne correspond.
- L'authentification basée sur la plage IP peut effectuer le transfert des ensembles de mises à jour. Si le contrôle d'accès à l'adresse IP est activé sur l'instance source, ajoutez les adresses IP de tous les nœuds d'application prenant en charge votre instance en tant qu'exceptions.

Remarque :
Pour trouver les informations relatives à l'adresse IP de votre instance, connectez-vous à ServiceNow - Support NOW et recherchez l'élément de catalogue de services **Mes informations IP** .

Remarque :
Pour en savoir plus sur les propriétés and `glide.ip.authenticate.strict` qui restreignent l'accès `com.snc.ipauthenticator` des instances à des plages IP spécifiques, consultez les rubriques suivantes dans Paramètres de renforcement de la sécurité de l'instance :

- Restreindre l'accès aux plages IP spécifiques
- Restriction IP stricte

Contrôle d'accès à l'adresse IP

Appliquez un contrôle d'accès IP au trafic sortant, au trafic entrant ou au trafic bidirectionnel. Le système ne bloque une adresse IP que si une règle de refus associée existe et qu'aucune règle d'autorisation correspondante n'existe. Par défaut, il n'existe aucune restriction d'accès à votre instance.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Utilisez la politique de contexte de pré-authentification d'Authentification adaptative (AA) pour appliquer des authentifications basées sur IP et des restrictions pour des options supplémentaires. Pour plus d'informations, consultez Authentification adaptative.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Contrôle d'accès à l'adresse IP** pour afficher la liste de vos contrôles d'accès IP.
   Vous devrez peut-être activer le module d'extension Authentification basée sur la plage IP [com.snc.ipauthenticator].
2. Renseignez le formulaire.

Remarque :
Pour trouver les informations relatives à l'adresse IP de votre instance, connectez-vous à ServiceNow - Support NOW et recherchez l'élément de catalogue de services **Mes informations IP** .

Champ	Description
Type	Type de règle de contrôle d'accès à inclure. ○ *Autoriser* : toute adresse IP de cette plage peut interagir avec cette instance. ○ *Refuser* : toute adresse IP de cette plage ne peut pas interagir avec cette instance à moins qu'elle ne soit répertoriée dans une règle d'autorisation. En outre, lors de l'ajout de règles de refus, vous ne pouvez pas refuser votre propre adresse IP publique ou votre instance ne met pas à jour une règle de refus. **Remarque :** Pour prendre en charge la maintenance, les mises à niveau et Service et assistance client, certaines ServiceNow adresses IP internes ne peuvent pas être bloquées par des règles de refus.
Direction	Direction de la règle de contrôle d'accès IP. ○ **Entrantes** : autorise ou refuse les transactions entrantes. Il s'agit de transactions initiées en dehors de votre instance. ○ **Sortant** : autorise ou refuse les transactions sortantes. Il s'agit de transactions initiées à partir de votre instance. ○ **Bidirectionnel** : autorise ou refuse les transactions entrantes et sortantes.
Actif	Lorsque cette option est sélectionnée, le formulaire est actif.
Description	Description du contrôle d'accès.
Début de plage	Plage de départ d'adresses IP à autoriser ou refuser. **Remarque :** Ces règles affectent également le transfert des ensembles de mises à jour. Pour vous assurer que le contrôle d'accès à l'adresse IP n'entraîne pas l'échec des ensembles de mises à jour, ajoutez l'instance cible en tant qu'exception.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Fin de plage	Plage de fin d'adresses IP à autoriser ou refuser. **Remarque :** Pour limiter l'accès à des adresses VPN spécifiques uniquement, entrez une plage de refus comprise entre **0.0.0.0** et **255.255.255.255** dans le champ **de refus** , et ne saisissez que les plages VPN autorisées spécifiques.

3. Cliquez sur **Envoyer**.

Rechercher les adresses IP refusées

Recherchez les adresses IP refusées dans les fichiers journaux du nœud de l'instance.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Les entrées de journal pour l'adresse IP bloquée apparaissent comme suit : `2015-10-21 18:37:43 (175) http-30 AVERTISSEMENT *** AVERTISSEMENT *** Sécurité restreinte : accès restreint (xx.xx.xxx.xxx non autorisé).`

Remarque :
Les adresses IP refusées sont des fichiers journaux de nœud de l'instance visible, qui ne sont pas visibles à partir des journaux système.

Procédure

1. Accédez à la **Tout** > **Journaux Système** > **Utilités** > **Navigateur de fichier journal de nœud.**.
2. Parcourez les journaux par critères, tels que la période et le message.
3. Vous pouvez également télécharger des fichiers journaux lorsque vous savez quel journal vous recherchez, en accédant à **Journaux Système** > **Utilités** > **Téléchargement du fichier journal de nœud**.

Intégration LDAP

Une intégration LDAP permet à votre instance d'utiliser votre serveur LDAP existant comme source principale de données utilisateur.

Les administrateurs s'intègrent à un répertoire LDAP (Lightweight Directory Access Protocol) pour rationaliser le processus de connexion de l'utilisateur et automatiser les tâches administratives telles que la création d'utilisateurs et leur affectation de rôles. Une intégration LDAP permet au système d'utiliser votre serveur LDAP existant comme source principale de données utilisateur. En règle générale, une intégration LDAP fait également partie d'une implémentation d'authentification unique.

L'intégration utilise les informations d'identification du compte de service LDAP pour récupérer le nom unique (ND) de l'utilisateur sur le serveur LDAP. En fonction de la valeur DN de l'utilisateur, l'intégration se relie ensuite à LDAP avec le ND et le mot de passe de l'utilisateur. Le mot de passe saisi par l'utilisateur est entièrement contenu dans la session HTTPS. L'intégration ne stocke jamais les mots de passe LDAP.

L'intégration utilise une connexion en lecture seule qui n'écrit jamais dans l'annuaire LDAP. L'intégration se contente de demander des informations, puis met à jour sa base de données interne en conséquence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour en savoir plus sur la configuration de l'intégration, reportez-vous à la section Configuration de l'intégration LDAP.

Remarque :
Si votre instance utilise une intégration LDAP et que les paramètres Active Directory exigent que les utilisateurs réinitialisent leur mot de passe lors de la connexion, vos utilisateurs ne seront pas en mesure de se connecter à l'instance. L'instance ne peut pas modifier le mot de passe Active Directory d'un utilisateur.

Fonctionnalités de l'intégration LDAP

Les fonctionnalités d'intégration LDAP sont les suivantes.

Actualisation LDAP planifiée

Une analyse planifiée de votre serveur LDAP est généralement exécutée une fois par nuit. Il interroge tous les attributs des enregistrements d'utilisateurs applicables et les compare avec le compte sur nos serveurs. S'il y a une différence, nous modifions notre enregistrement d'utilisateur avec l'attribut modifié. La charge placée sur le serveur LDAP pendant l'actualisation dépend du nombre d'enregistrements interrogés et du nombre d'attributs comparés. Nous vous recommandons de programmer l'actualisation en dehors des heures de pointe. Une opération d'actualisation importante peut affecter d'autres opérations planifiées, telles que l'exécution de rapports, et doit être planifiée de manière à minimiser les conflits.

Écouteur LDAP

L'écouteur LDAP est notre version d'une requête persistante (ou recherche persistante). Nous émettons une requête permanente pour les modifications apportées à votre serveur LDAP et sommes constamment à l'écoute d'une réponse. En supposant que votre serveur prenne en charge une recherche persistante, toutes les modifications apportées à l'un de vos comptes LDAP applicables sont renvoyées à l'écouteur LDAP et envoyées à votre instance dans un délai d'environ 10 secondes. Il s'agit d'un outil extrêmement utile, qui nous permet d'avoir une copie presque en temps réel des détails du compte de vos utilisateurs, sans avoir à attendre la prochaine actualisation programmée.

Connexion LDAP sur demande

Une fois qu'une intégration LDAP est établie, l'instance peut autoriser de nouveaux utilisateurs à se connecter au système même s'ils n'ont pas encore de compte sur l'instance. Lorsqu'un nouvel utilisateur tente de se connecter à l'instance, l'intégration vérifie si cet utilisateur dispose d'un compte dans l'instance. Si l'intégration ne trouve pas de compte d'utilisateur existant, elle interroge automatiquement le serveur LDAP pour le nom d'utilisateur qui a été saisi. Si un compte LDAP correspondant est trouvé, l'intégration tente de s'authentifier avec le mot de passe entré par l'utilisateur. Si le mot de passe est valide, l'instance crée un compte pour l'utilisateur, remplit le compte avec toutes les informations LDAP applicables et connecte l'utilisateur à l'instance.

La connexion à la demande utilise la carte de transformation d'importation d'utilisateur LDAP. Pour en savoir plus sur les exigences relatives aux cartes de transformation, reportez-vous à Cartes de transformation LDAP.

Remplissage des données LDAP

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
La fonctionnalité décrite dans cette intégration n'est pas disponible par défaut. Cette intégration implique une personnalisation post-déploiement effectuée par un administrateur expérimenté ou par des consultants en ServiceNow services professionnels.

Une intégration aux serveurs LDAP vous permet de remplir rapidement et facilement la base de données de l'instance avec des enregistrements utilisateur provenant de la base de données LDAP existante. Pour éviter les incohérences de données, vous pouvez créer, ignorer ou ignorer les enregistrements LDAP entrants.

Vous pouvez également limiter les données importées par l'intégration en spécifiant des attributs LDAP, ce qui permet d'importer uniquement les données que vous souhaitez exposer à une instance. En règle générale, les attributs LDAP que vous spécifiez font partie de la carte de transformation d'intégration. Si vous ne spécifiez aucun attribut LDAP, l'intégration importe tous les attributs d'objet disponibles à partir du serveur LDAP. L'instance stocke les données LDAP importées dans des tables de jeu d'importation temporaires, donc plus vous importez d'attributs et plus le temps d'importation est long. Pour plus d'informations, consultez Spécifier les attributs LDAP.

Authentification LDAP

Utilisez l'authentification LDAP pour accéder à l'application à l'aide d'informations d'identification LDAP.

Lorsqu'un utilisateur saisit ses informations d'identification réseau sur la page de connexion :

1. L'instance transmet les informations d'identification à un serveur LDAP pour trouver l'instance.
2. Avec les RDN, il valide la chaîne DN de l'utilisateur. Il valide uniquement si au moins une des configurations LDAP OU avec `table=sys_user` a un RDN configuré.
3. Le serveur LDAP répond par un message autorisé ou non autorisé que le système utilise pour déterminer si l'accès doit être accordé.

En s'authentifiant auprès de votre serveur LDAP, les utilisateurs accèdent à la plateforme avec les mêmes informations d'identification que celles qu'ils utilisent pour d'autres ressources internes sur votre domaine réseau. En outre, vous pouvez réutiliser les politiques de mot de passe et de sécurité existantes qui sont déjà en place. Par exemple, le serveur LDAP peut déjà avoir des stratégies de verrouillage de compte et d'expiration de mot de passe.

Lorsque vous activez LDAP, le système met à jour les enregistrements utilisateur avec ces champs.

Mises à jour de l'enregistrement de l'utilisateur LDAP

Champ	Description
Source	Identifie si LDAP est utilisé ou non pour valider un utilisateur. Si la source commence par LDAP, l'utilisateur est validé via LDAP. Si la source ne commence pas par ldap, le mot de passe sur l'enregistrement utilisateur est utilisé pour valider l'utilisateur lors de la connexion.
Serveur LDAP	Identifie quel serveur LDAP authentifie l'utilisateur lorsqu'il existe plusieurs serveurs LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le système ne prend pas en charge l'authentification par mot de passe LDAP via un serveur MID. Une instance doit pouvoir se connecter directement à un serveur LDAP pour prendre en charge l'authentification par mot de passe.

Présentation de l'intégration LDAP

Une intégration LDAP permet à votre instance d'utiliser votre serveur LDAP existant comme source principale de données utilisateur.

Conditions préalables de l'intégration LDAP

- Le serveur des services de répertoire doit être conforme à la norme LDAP v3
- L'accès au réseau entrant via le pare-feu doit être autorisé (au serveur LDAP)
- Adresse IP externe ou nom du serveur LDAP
- Informations d'identification de l'utilisateur avec accès en lecture seule
- Pour LDAPS, un certificat PKI

Minutage de l'intégration LDAP

Les intégrations LDAP sont généralement effectuées avant la mise en service de l'instance, mais elles peuvent être intégrées à tout moment.

Intégrité des données du serveur LDAP

Certains utilisateurs craignent qu'un tiers (l'instance en l'occurrence) apporte des modifications (écriture) à votre serveur LDAP. Dans une intégration LDAP, votre instance n'écrit pas dans le répertoire LDAP interne. L'instance recherche des informations et met à jour sa base de données en conséquence.

Aucune modification n'est apportée au serveur LDAP interne par l'instance. Le compte de service est en lecture seule.

La plupart des changements (y compris les ajouts) apportés à votre serveur LDAP sont disponibles pour l'instance en quelques secondes, en fonction du nombre de composants de l'intégration LDAP complète en place.

Pour maintenir les enregistrements LDAP synchronisés, planifiez une analyse périodique du serveur LDAP pour détecter les changements.

L'instance ne synchronise pas les enregistrements du département. Les utilisateurs et les appartenances aux groupes sont tenus à jour par le mécanisme d'écoute LDAP et une navigation LDAP complète quotidienne, mais l'instance ne supprime aucune de ces entrées une fois qu'elles ont disparu de LDAP.

Si une entrée devait être supprimée, tout l'historique serait également supprimé, et toute référence à celle-ci serait effacée ou supprimée. Les éléments de configuration (CI), les accords SLA, les licences de logiciel, les bons de commande et les entrées de Catalogue de services ont tous une référence au département, et si le département est supprimé, ces références sont effacées. Il existe de nombreuses références aux utilisateurs, et donc la suppression d'un utilisateur entraînerait la perte de tout historique de ce qu'il a fait. Actuellement, la décision de supprimer ou de ne pas supprimer est prise par nos clients.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécurité

La connexion se fait à partir d'une seule machine à l'aide d'une adresse IP fixe via un port spécifique de votre pare-feu. L'authentification se fait avec un compte LDAP en lecture seule de votre choix. Vous pouvez utiliser LDAP standard, ou charger le côté public d'un certificat SSL installé sur votre répertoire, auquel cas nous pouvons utiliser LDAPS. Pour ajouter une couche de sécurité supplémentaire, nous offrons également l'option d'un tunnel VPN IPSEC point à point. Adressez-vous à votre chargé de clientèle pour en savoir plus et connaître les tarifs.

Connexions LDAP sécurisées

Connexion	Description
Serveur MID	Pour protéger votre serveur LDAP du trafic réseau externe, installez un serveur MID sur le réseau local et configurez le système pour qu'il communique avec le serveur MID via un canal sécurisé.
LDAPS (en anglais seulement)	Pour établir une connexion LDAPS chiffrée, chargez le côté public du certificat SSL de votre serveur LDAP. L'intégration utilise le certificat pour chiffrer toutes les communications entre le serveur LDAP et l'instance.
VPN	Pour sécuriser le serveur LDAP avec un tunnel VPN IPSEC point à point chiffré, contactez votre chargé de clientèle pour plus de détails et pour connaître les tarifs.

Un autre aspect de sécurité à prendre en compte est le partage de données dans une intégration LDAP. Pour limiter les données exposées à votre instance, spécifiez des attributs dans votre carte de transformation. Pour plus d'informations, consultez Cartes de transformation LDAP.

Importation de données LDAP dans l'instance

Il est recommandé de définir des attributs pour importer uniquement les données requises. Les attributs définis sont mappés dans la base de données des utilisateurs de l'instance.

Nous ne pouvons pas répondre à la question de savoir quels attributs spécifiques sont nécessaires, car cela est déterminé par la portée du projet et les exigences de l'entreprise.

Types de serveurs LDAP pris en charge

L'instance s'est intégrée avec succès à Microsoft Active Directory, Novell, Domino (Lotus Notes) et Open LDAP. Nous utilisons JNDI pour l'interface avec le serveur LDAP. Tant que votre serveur LDAP est conforme à la norme LDAP v3, l'intégration est réussie.

Authentification unique LDAP

Outre la fonctionnalité de remplissage de données fournie avec l'importation LDAP, vous pouvez utiliser la fonctionnalité d'authentification externe prise en charge par l'application pour éviter que vos utilisateurs n'aient à se connecter à chaque fois.

Plusieurs domaines LDAP

Pour gérer plusieurs domaines, il est recommandé de créer un enregistrement de serveur LDAP distinct pour chaque domaine. Chaque enregistrement de serveur LDAP doit pointer vers un contrôleur de domaine pour ce domaine. Cela signifie que le réseau local doit autoriser les connexions à chacun des contrôleurs de domaine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Après l'extension à plusieurs domaines réseau, il est essentiel d'identifier les attributs LDAP uniques pour les noms d'utilisateur d'application et d'importer les valeurs de fusion. objectSid est un attribut de coalescence unique commun pour Active Directory. Les noms d'utilisateur uniques peuvent varier en fonction de la conception des données LDAP. Les attributs communs sont `e-mail` ou `userPrincipalName`.

Gestion des limites de requête

Par défaut, Active Directory 2000/2003 dispose d'une limite de requête LDAP (maxPageSize) de 1 000 objets pour empêcher les charges excessives et les attaques par déni de service. Nous avons deux méthodes pour faire face à cette limite.

La méthode par défaut consiste à diviser la requête pour renvoyer moins de 1 000 objets à la fois. Par exemple, interrogez uniquement les objets commençant par la lettre « a », puis les objets « b ». La méthode la plus efficace pour les grands environnements consiste à activer la pagination. La pagination est prise en charge par défaut sur tous les serveurs Microsoft Active Directory. Il divise automatiquement les résultats en plusieurs ensembles de résultats, de sorte que nous n'avons pas à diviser la requête en plusieurs demandes.

Type de requête LDAP

Si un mot de passe LDAP est fourni, une liaison simple est effectuée. Si aucun mot de passe LDAP n'est fourni, « aucun » n'est utilisé, auquel cas le serveur LDAP doit autoriser la connexion anonyme.

Authentification LDAP

Nous utilisons les informations d'identification du compte de service fournies pour LDAP afin de récupérer le DN de l'utilisateur à partir du serveur LDAP. En fonction de la valeur DN de l'utilisateur, nous rétablissons la liaison avec LDAP en fonction du DN de l'utilisateur et du mot de passe fourni.

Stockage des mots de passe

Le mot de passe saisi par l'utilisateur est entièrement contenu dans sa session HTTPS. Nous ne stockons ce mot de passe nulle part.

Configuration d'une authentification LDAP

Les champs suivants de l'enregistrement utilisateur appartiennent à LDAP :

- **Source** : le champ Source identifie si un utilisateur est validé ou non à l'aide de LDAP. Si le champ source commence par « ldap », l'utilisateur est validé via LDAP. Si le champ Source ne commence pas par « ldap », le mot de passe sur l'enregistrement utilisateur est utilisé pour valider l'utilisateur lors de la connexion.
- **Serveur LDAP** : l'instance prend en charge plusieurs serveurs LDAP, de sorte que le champ Serveur LDAP détermine quel serveur doit être utilisé pour authentifier l'utilisateur.

Exigences relatives à l'intégration LDAP

Passez en revue les exigences relatives à l'intégration LDAP, qui incluent un certificat PKI et un serveur de services d'annuaire conforme à LDAP.

L'intégration LDAP nécessite :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Un serveur de services d'annuaire conforme à la norme LDAP v3
  - Permet l'accès au réseau entrant via le pare-feu (vers le serveur LDAP)
  - (Facultatif) Accepte les logins anonymes
  - (Facultatif) Prend en charge la pagination des requêtes LDAP volumineuses
- Adresse IP externe ou nom de domaine complet du serveur LDAP. Vous pouvez également utiliser un MID Server.
- Un compte LDAP en lecture seule de votre choix
- Pour plusieurs domaines, l'accès réseau pour chaque contrôleur de domaine
- Pour LDAPS, un certificat PKI
- Pour l'écouteur LDAP, un serveur Microsoft Active Directory qui prend en charge les requêtes persistantes (ADNotify)

Serveurs LDAP pris en charge

En utilisant *JNDI* pour s'interfacer avec le serveur LDAP, l'instance s'est intégrée avec succès aux serveurs suivants :

- Microsoft Active Directory
- Novell (en anglais seulement)
- Domino (Lotus Notes)
- Ouvrir LDAP

Limites de requêtes LDAP

Par défaut, Active Directory 2000/2003 dispose d'une limite de requête LDAP (maxPageSize) de 1 000 objets pour empêcher les charges excessives et les attaques par déni de service. Le système dispose de deux méthodes pour faire face à cette limite.

- La méthode par défaut consiste à diviser la requête pour renvoyer moins de 1 000 objets à la fois. Par exemple, interrogez uniquement les objets commençant par la lettre a, puis les objets b.
- La méthode la plus efficace pour les environnements volumineux consiste à activer la pagination, qui est prise en charge par défaut sur tous les serveurs Microsoft Active Directory. La pagination divise automatiquement les résultats en plusieurs ensembles de résultats afin que l'intégration n'ait pas à fractionner la requête en plusieurs demandes.

Configuration de l'intégration LDAP

Les administrateurs peuvent activer l'intégration LDAP pour autoriser la connexion des utilisateurs à partir de l'annuaire LDAP de leur entreprise.

LDAP utilise généralement l'un de ces types de canaux de communication.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Canaux de communication LDAP

Connexion	Description	Prise en charge de l'importation LDAP ?	Prise en charge de l'authentification LDAP ?
Connexion au MID Server	Communique par défaut via HTTP sur le port 80. Ce canal de communication ne nécessite pas de certificat. La connexion entre le serveur MID et l'instance se fait via HTTPS (port 443). Vous pouvez utiliser le serveur MID pour importer des données via LDAP, mais vous ne pouvez pas utiliser le serveur MID pour l'authentification LDAP. Poursuivez la définition du serveur LDAP.	Oui	Non
Intégration LDAP standard	Communique par défaut via TCP sur le port 389. Ce canal de communication ne nécessite pas de certificat. Poursuivez la définition du serveur LDAP.	Oui	Oui
Intégration LDAP chiffrée par SSL (LDAPS)	Communique par défaut via TCP sur le port 636, ce canal de communication nécessite un certificat. Procédez à Installer le certificat SSL LDAP X.509 pour obtenir et télécharger le certificat.	Oui	Oui
Connexion VPN	Communication via un tunnel IPSEC. Achetez ou créez un tunnel IPSEC sur votre réseau local. Poursuivez la définition du serveur LDAP.	Oui	Oui

Si vous utilisez un serveur MID, le serveur MID se connecte à l'instance et le serveur MID se connecte également au serveur LDAP. Dans les deux cas, c'est le MID Server qui initie la connexion :

1. Tout d'abord, le MID Server se connecte au serveur LDAP via LDAP sur le port 389.
2. Ensuite, le MID Server initie une connexion chiffrée HTTPS à l'instance sur le port 443 pour transmettre les données à l'instance.

Pour plus d'informations sur les VPN, les MID Servers et LDAP, consultez Vous n'avez pas besoin d'un VPN Partie II sur la communauté.

Installer le certificat SSL LDAP X.509

Vous pouvez installer un certificat X.509 pour votre intégration LDAP.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Achetez ou générez un certificat SSL sur votre serveur LDAP.
2. Accédez à la **LDAP** > **Certificat** et cliquez sur **Nouveau**.
3. Remplissez les champs du formulaire :

Champ	Description
Nom	Nom du certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Notification d'échéance	Sélectionnez cette option pour envoyer une notification aux utilisateurs sélectionnés dans le champ **Notifier à l'expiration** . Cette option est activée par défaut.
Notification à l'expiration	Sélectionnez les utilisateurs pour relancer la notification concernant l'expiration du certificat. Si aucun utilisateur n'est sélectionné, l'utilisateur connecté est ajouté par défaut, ainsi que les deux derniers utilisateurs connectés ayant le rôle administrateur.
Avertissement avant l'expiration (en jours)	Nombre de jours avant l'expiration du délai d'envoi de la notification par l'instance. Saisissez une valeur d'au moins 20. Les instances mises à niveau vers Istanbul et les versions ultérieures ont cette valeur définie sur 20, sauf si une valeur supérieure est spécifiée.
Actif	Case à cocher indiquant que ce certificat est actif.
Format	Le format du certificat.
Type	Le conteneur de certificats. L'instance reconnaît les certificats des magasins de confiance, du magasin de clés Java et des magasins de clés PKCS#12.
Début de validité	L'instance ajoute automatiquement la date de début de validité du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Date d'expiration	L'instance ajoute automatiquement la date d'expiration du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Échéance en jours	Nombre calculé de jours jusqu'à l'expiration.
Description brève	Description du certificat.
Émetteur	L'instance ajoute automatiquement l'émetteur du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Objet	L'instance ajoute automatiquement l'objet du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Certificat PEM	Saisissez la valeur du certificat X509.

Remarque :
À l'heure actuelle, l'intégration ne signe pas le certificat dans les communications entre l'instance et l'IdP.

4. Cliquez sur **Enregistrer**.

Que faire ensuite
Cliquez sur **Valider les magasins/certificats** pour tester le magasin de confiance et le certificat.

Définir un serveur LDAP

Créez un enregistrement de serveur LDAP dans l'instance.

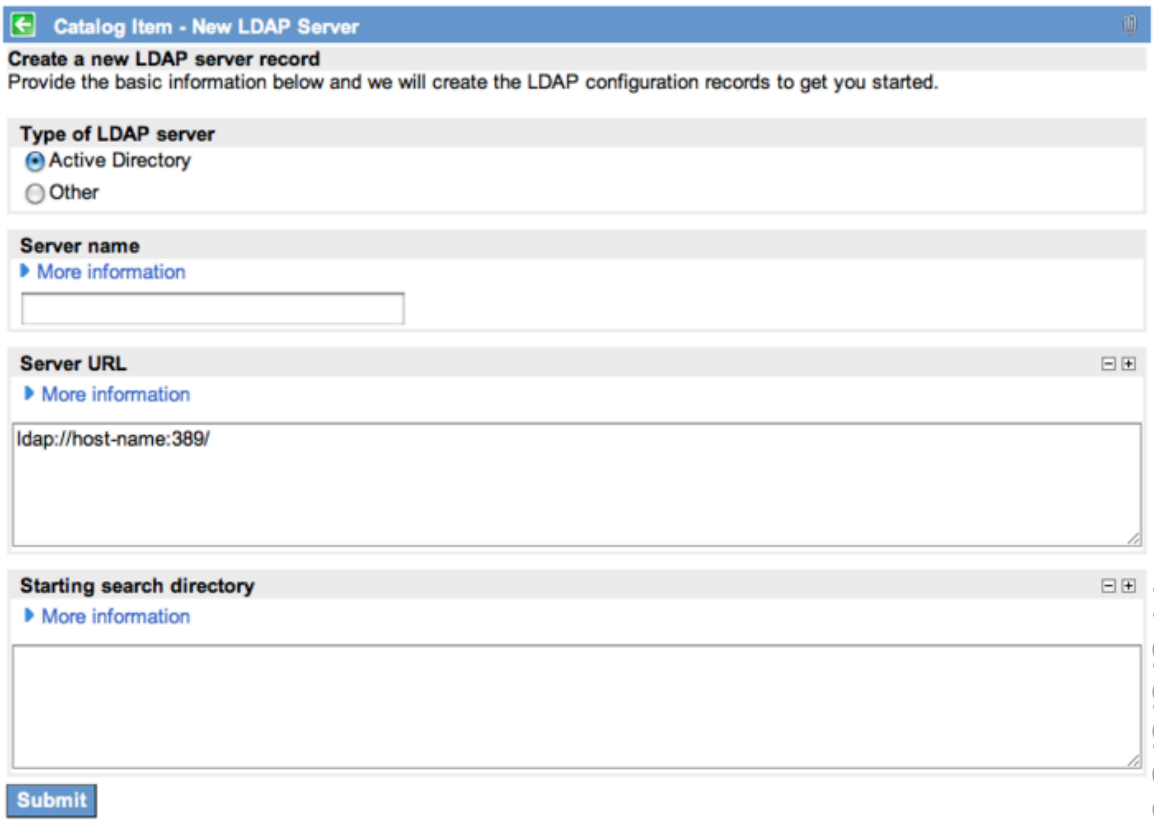
Avant de commencer
Rôle requis : admin.

Procédure

1. Accédez à la **Tout** > **Système LDAP** > **Créer un serveur**.
2. Renseignez les champs de formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Dans le champ **URL du serveur** , les URL valides de tous les serveurs apparaissent séparées par un espace. Les serveurs sont d'abord triés par statut opérationnel, les serveurs étant listés **en** premier, puis classés par la valeur **d'ordre** que vous spécifiez. Le premier serveur répertorié est le serveur LDAP principal. Les autres sont des serveurs redondants.

Remarque :
Il y a un léger délai entre le changement de l'état de fonctionnement réel et l'affichage.

Vous pouvez également ajouter un serveur LDAP redondant en accédant à un enregistrement de serveur LDAP existant et en insérant une ligne dans la liste incorporée des URL des serveurs LDAP.

3. Cliquez sur **Envoyer**.

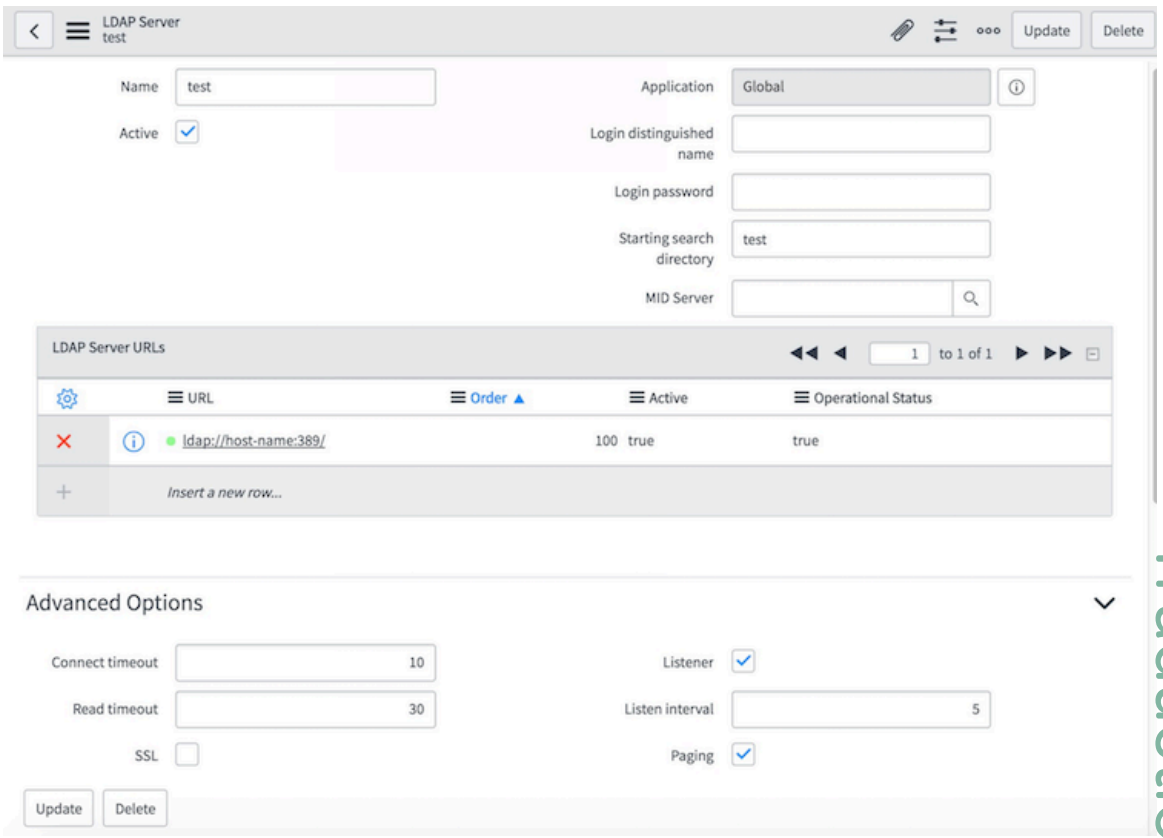
Remarque :
Vous pouvez également modifier un enregistrement de serveur LDAP existant en accédant à **Système LDAP** > **Serveurs LDAP** et d'apporter les changements nécessaires.

4. Apportez des modifications aux champs si nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire du serveur LDAP



Champ	Description
Nom	Entrez le nom du serveur.
Actif	Cochez cette case si le serveur est actif.
URL des serveurs LDAP	Entrez les URL du serveur LDAP principal et du serveur LDAP de sauvegarde. Les serveurs sont d'abord triés par statut opérationnel, les serveurs étant listés en premier, puis classés par la valeur d'ordre que vous spécifiez. Le premier serveur répertorié est le serveur LDAP principal. Les autres sont des serveurs redondants.
URL serveur	Entrez l'URL du serveur. Configurez le formulaire pour ajouter ce champ si nécessaire. Il s'agit d'un champ calculé en lecture seule qui affiche la liste des serveurs LDAP que vous pouvez également voir dans le champ **URL du serveur LDAP** , séparée par un espace et triée par statut opérationnel et valeurs d'ordre des URL.
Nom de connexion distinct	Entrez le nom unique (ND) de l'utilisateur authentifiant la connexion LDAP. Pour accéder à un serveur d'annuaire LDAP, le nom d'utilisateur doit être au format de nom unique complet : servicenow@service-now.com
Mot de passe de connexion	Entrez le mot de passe du serveur.
Répertoire de recherche de départ	Entrez le nom distinct relatif (RDN) du répertoire de recherche par défaut. Toutes les requêtes adressées à ce serveur LDAP commencent à partir de ce RDN.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Serveur MID	Sélectionnez le serveur MID que vous voulez utiliser pour vous connecter au serveur LDAP. L'utilisation d'un serveur MID pour établir une connexion LDAP vous évite d'avoir à exposer le serveur LDAP au trafic réseau externe. Il élimine également la nécessité d'établir un tunnel VPN entre votre serveur LDAP et ServiceNow les centres de données. **Remarque :** ◦ L'utilisateur du Serveur MID doit disposer du rôle user_admin pour pouvoir lire les enregistrements de configuration du serveur LDAP. ◦ Les éléments suivants ne sont pas disponibles avec le MID Server : ▪ Authentification LDAP ▪ Connexion SSL
Délai de Connexion	Si un serveur MID est configuré, la connexion expire au bout de 10 secondes, quel que soit ce paramètre. Ce paramètre est codé en dur et ne peut pas être modifié.
Délai d'expiration de lecture	Spécifiez le nombre de secondes dont dispose l'intégration pour lire les données LDAP. L'intégration arrête la lecture des données LDAP une fois que la connexion a dépassé le délai de lecture. Si vous activez une connexion SSL, vous pouvez également définir une valeur de délai de lecture avec la`com.glide.ssl.read.timeout`propriété système. Si vous saisissez des valeurs de délai d'expiration pour ce champ et pour la propriété système, la valeur de délai d'expiration la plus faible est prioritaire.
SSL	Activez cette case à cocher pour exiger du serveur LDAP qu'il établisse une connexion chiffrée SSL. Si vous avez sélectionné un serveur MID, ce champ n'est pas disponible. Si vous utilisez une intégration LDAPS et que le port SSL par défaut est 636, aucune autre configuration n'est nécessaire ; SSL est automatiquement activé. Si l'intégration LDAPS utilise un autre port SSL, définissez les autres propriétés de connexion SSL. **Remarque :** Assurez-vous qu'un administrateur réseau configure le pare-feu local pour permettre au serveur d'applications d'accéder au serveur LDAP. Si le serveur LDAP est situé dans un réseau interne, le pare-feu transfère (ou NAT) l'adresse IP du serveur d'applications via le pare-feu sur le port approprié.
Écouteur	Cochez cette case pour permettre à l'intégration d'interroger Microsoft périodiquement les serveurs Active Directory ou les serveurs LDAP qui prennent en charge le contrôle des demandes de recherche persistante. En outre, si vous avez sélectionné un serveur MID, la fonctionnalité d'écouteur est disponible pour ce serveur MID. Consultez Activer un écouteur LDAP et définir les propriétés système pour plus d'informations.
Intervalle d'écoute (valeur	Spécifiez la valeur du délai d'expiration de l'écouteur en nombre de minutes pendant lesquelles l'intégration écoute les données LDAP à chaque connexion. L'intégration arrête l'écoute des données LDAP lorsque la connexion dépasse l'intervalle d'écoute.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
du délai d'expiration)	
Pagination	Cochez cette case pour que le serveur LDAP divise les données d'attribut LDAP en plusieurs jeux de résultats plutôt que d'envoyer plusieurs requêtes.

Remarque :
Si vous fournissez un mot de passe LDAP, l'intégration effectue une opération de liaison simple. Si vous ne fournissez pas de mot de passe LDAP, le serveur LDAP doit autoriser la connexion anonyme ou l'intégration ne peut pas se lier au serveur LDAP.

Résultats

Lorsqu'un enregistrement de serveur LDAP est défini sur actif, le système teste automatiquement chaque connexion pour le valider.
Les validations comprennent :

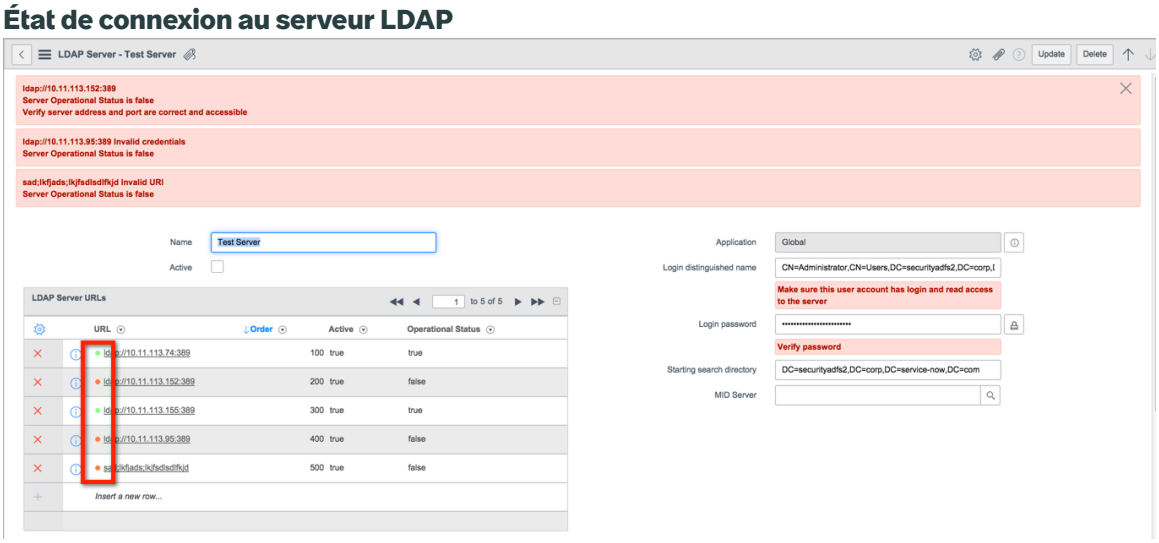
- Le serveur LDAP est accessible à l'URL et au port fournis.
- L'URL du serveur LDAP est correctement formatée
- Les informations d'identification de connexion sont valides

À partir de la version Fuji, le système affiche des points colorés à côté de chaque URL de serveur :

Icônes de connexion au serveur LDAP

Couleur	Description
Vert	Le serveur s'il est actif et opérationnel
Gris	Le serveur n'est ni actif ni opérationnel.
Rouge	Le serveur est actif mais pas opérationnel.

État de connexion au serveur LDAP



Activer un écouteur LDAP et définir les propriétés système

L'activation d'un écouteur est facultative. Si cette option est activée, un écouteur informe le système de traiter les enregistrements LDAP peu de temps après qu'il y a une mise à jour sur le serveur LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Un *écouteur* est un processus dédié qui recherche périodiquement des modifications sur le serveur LDAP.

L'écouteur peut être déployé sur un serveur Microsoft Active Directory qui prend en charge les requêtes persistantes (ADNotify) ou sur un serveur LDAP qui prend en charge le contrôle des demandes de recherche persistante (avec OID 2.16.840.1.113730.3.4.3).

Si le serveur LDAP prend en charge une recherche persistante, l'écouteur LDAP reconnaît toutes les modifications apportées par utilisateur ou groupe à l'un des comptes LDAP applicables et les transfère à votre instance dans un délai d'environ 10 secondes. Cela permet à l'instance d'avoir une copie en temps quasi réel des détails du compte de vos utilisateurs sans avoir à attendre la prochaine actualisation planifiée. L'écouteur LDAP peut uniquement synchroniser les objets mappés aux tables Utilisateur [sys_users] et Groupe [sys_user_group].

Remarque :
Si un utilisateur est ajouté via l'écouteur, mais qu'il ne répond pas aux exigences définies par le filtre d'OU, l'instance ignore l'enregistrement sur le serveur LDAP. S'il répond aux critères, l'utilisateur est ajouté à l'instance.

Pour activer un écouteur :

Procédure
1. Accédez à la **Tout** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à configurer.
3. Sélectionnez la case à cocher **Listener** .
4. Cliquez sur **Mettre à jour**.

Remarque :

Le système importe uniquement les enregistrements utilisateur qui correspondent au filtre LDAP OU. Les enregistrements d'utilisateurs entrants qui ne répondent pas aux exigences de filtre sont marqués comme non valides et ignorés par l'importation. Les administrateurs peuvent activer la connexion LDAP détaillée pour déterminer si les enregistrements entrants ne correspondent pas au filtre LDAP OU.

5. **Facultatif :** Accédez à la table Propriétés système [sys_properties] et définissez les propriétés système de l'écouteur LDAP.

Propriétés de l'écouteur LDAP

Propriété	Description
glide.ldap.listener.use_background_transaction	Si la valeur est « vrai », l'écouteur LDAP démarre en tant que transaction d'arrière-plan. En exécutant l'écouteur LDAP en tant que transaction d'arr plan, la règle de quota de la transaction de démarrage/arrêt de l'écouteur LDAP peut annuler la transaction une fois que la durée maximale est attei 5 minutes par défaut. Ce comportement empêche un écouteur LDAP d'att indéfiniment.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : Cette propriété s'applique uniquement aux connexions LDAP qui n'utilisent pas de Serveur MID. Permet `glide.ldap.listener.mid.use_background_transac` de contrôler le comportement des connexions LDAP qui passent par serveur MID. ○ Type : true | false ○ Valeur par défaut : faux ○ Emplacement : l'ajouter à la table Propriétés système [sys_properties]
glide.ldap.listener.mid.use_background_transaction	Si la valeur est « vrai », l'écouteur LDAP démarre en tant que transaction d'arrière-plan. En exécutant l'écouteur LDAP en tant que transaction en a plan, la règle de quota de démarrage/arrêt de la transaction MID de l'écou LDAP peut annuler la transaction une fois que la durée maximale est attei 5 minutes par défaut. Ce comportement empêche un écouteur LDAP d'att indéfiniment. **Remarque :** Cette propriété s'applique uniquement aux connexions LDAP qui utilisent un serveur MID. Permet `glide.ldap.listener.use_background_transaction` contrôler le comportement des connexions LDAP qui ne passent pas un serveur MID. ○ Type : true | false ○ Valeur par défaut : faux ○ Emplacement : l'ajouter à la table Propriétés système [sys_properties]
glide.ldap.listener.mid.one_listener	Si la valeur est vrai, un seul message de file d'attente ECC est créé pour démarrer ou arrêter l'écouteur LDAP via un serveur MID. Si la valeur est sur false, plusieurs messages de file d'attente ECC peuvent être créés, ce entraîne la création de plusieurs threads pour démarrer ou arrêter l'écouteu LDAP. ○ Type : true | false ○ Valeur par défaut : true ○ Emplacement : l'ajouter à la table Propriétés système [sys_properties]

Production automatique

Spécifier les attributs LDAP

Spécifiez les attributs inclus dans les requêtes du serveur LDAP à l'aide du champ **Attributs** du serveur LDAP. Cela peut améliorer les performances ainsi que la sécurité.

Avant de commencer
Rôle requis : administrateur

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

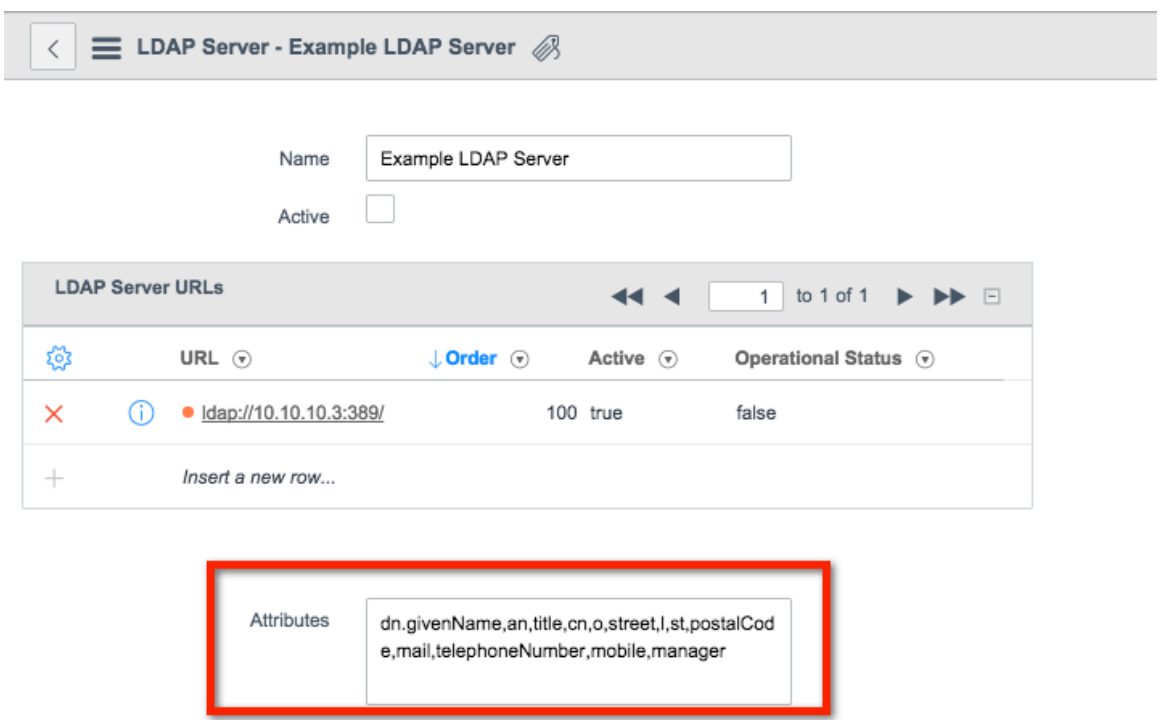
Par défaut, le système charge tous les attributs pour chaque objet qu'il est autorisé à lire à partir de votre serveur LDAP. À l'aide du champ **Attributs** , vous pouvez spécifier et ainsi limiter les attributs renvoyés par la requête LDAP. L'utilisation de cette approche pour les importations LDAP importantes peut considérablement améliorer la vitesse de ces importations.

Procédure

Définissez explicitement les attributs dans la mesure du possible.

S'il existe des informations que vous ne souhaitez pas exposer à l'instance, excluez l'attribut. Si vous ne spécifiez pas les attributs du serveur LDAP, les transactions utilisateur risquent de se bloquer pendant de longues périodes lorsque de nouveaux attributs sont ajoutés à un objet de serveur LDAP, car le système est occupé par le chargement des données à partir des nouveaux attributs.

Remarque :
Pour utiliser les scripts de recherche de gestionnaire décrits dans Sélectionner ou créer une carte de transformation pour les données LDAP, spécifiez **le gestionnaire** et le **dn** (nom unique) dans le champ **Attributs** . Aucun des deux attributs n'est requis pour faire partie d'une carte de transformation.



Tester une connexion LDAP

L'instance teste automatiquement la connexion chaque fois qu'un utilisateur ouvre le formulaire du serveur LDAP. Vous pouvez également tester manuellement la connexion au serveur LDAP à partir du formulaire du serveur LDAP.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Par défaut, des messages d'erreur s'affichent sur le formulaire du serveur LDAP en cas de problème de connexion au serveur LDAP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les employés peuvent également vérifier la connectivité entre l'instance et le serveur LDAP. Contactez le support technique pour obtenir de l'aide lors de la vérification de la connectivité LDAP.

Pour tester manuellement une connexion :

Procédure

1. Accédez à la **Tout** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à tester.
3. Sous **Liens connexes**, cliquez sur **Test de la connexion**.
4. Sous **Liens connexes**, cliquez sur **Parcourir** pour vérifier que la structure de répertoire LDAP appropriée est visible par le système.
5. **Facultatif :** Si la connexion a réussi, cliquez sur **Parcourir** pour afficher la structure des répertoires LDAP source visible par l'instance.

Remarque :
Les champs **Filtre** et **RDN** à gauche de la fenêtre Parcourir sont ignorés lorsque vous utilisez le champ de recherche à droite.

Résultats
L'instance modifie l'état opérationnel des serveurs LDAP en fonction du résultat du test de connexion.

- Si votre instance établit une connexion à un serveur dont la valeur **d'état opérationnel** est **inactif**, la valeur **d'état opérationnel** passe automatiquement à **haut**. Cette fonctionnalité est prise en charge pour les tests de connexion automatiques et manuels.
- S'il n'est pas possible d'établir une connexion à un serveur dont la valeur État **opérationnel** est **En hausse**, la valeur État **opérationnel** passe automatiquement en **Inactif**. Cette fonctionnalité est prise en charge uniquement pour les tests de connexion automatiques, et non pour les tests manuels.

Définir des unités organisationnelles LDAP

Une définition d'unité organisationnelle (OU) spécifie les répertoires sources LDAP disponibles pour l'intégration.

Avant de commencer
Rôle requis : admin.

Pourquoi et quand exécuter cette tâche
Les définitions d'unités organisationnelles peuvent contenir des emplacements, des personnes ou des groupes d'utilisateurs. Chaque définition de serveur LDAP contient deux exemples de définitions d'unités organisationnelles : l'une pour l'importation de groupes dans le système et l'autre pour les utilisateurs.

Procédure

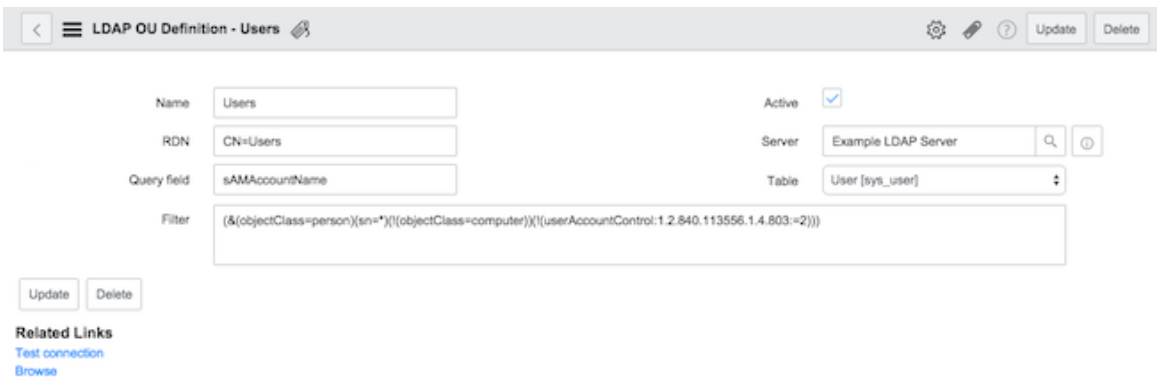
1. Accédez à la **Tout** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à configurer.
3. Dans la liste connexe **Définitions d'UO LDAP** , sélectionnez l'exemple de définition d'UO **Groupes** ou **Utilisateurs** .
4. Remplissez le formulaire Définition d'UO LDAP (voir table).
5. Cliquez sur **Mettre à jour**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le système teste automatiquement la connexion au serveur LDAP.

6. Sous **Liens connexes**, cliquez sur **Parcourir** pour afficher les enregistrements du répertoire LDAP renvoyés par la définition d'OU.



Formulaire de définition d'unité organisationnelle

Champ	Description
Nom	Spécifiez le nom que l'intégration utilise lorsqu'elle fait référence à cette unité organisationnelle. Le nom que vous entrez ici devient une cible LDAP dans l'enregistrement de source de données.
Nom distinct relatif à traiter	Spécifiez le nom distinct relatif du sous-répertoire dans lequel vous souhaitez effectuer la recherche. Ce RDN est combiné avec le répertoire de démarrage de recherche de la définition du serveur LDAP afin d'identifier le sous-répertoire contenant des informations pour cette unité organisationnelle. Par exemple, l'exemple de définition d'OU utilise la valeur RDN de `CN=Users` pour rechercher le répertoire LDAP `CN=Users,DC=service-now,DC=com` et tout répertoire en dessous de ce point. Ce champ doit correspondre à un sous-répertoire de votre système LDAP.
Champ d'interrogation	Spécifiez le nom de l'attribut dans le serveur LDAP pour interroger les enregistrements. Le champ de requête doit être unique dans les instances de domaine unique et multiple. Pour de meilleurs résultats, utilisez des adresses e-mail ou d'autres informations d'identification qui identifient de façon unique l'utilisateur dans une instance à domaines multiples. Active Directory utilise l'attribut **sAMAccountName** . D'autres serveurs LDAP ont tendance à utiliser l'attribut **cn** . **Remarque :** Le **champ Requête** doit être mappé au champ **ID d'utilisateur** dans la table Utilisateur [sys_user]. Par exemple, si un utilisateur Active Directory se connecte en tant que `joe.example`, il doit avoir un enregistrement utilisateur avec la valeur **d'ID d'utilisateurjoe.example** et un enregistrement LDAP avec la valeur **sAMAccountNamejoe.example**.
Actif	Cochez cette case pour activer la définition d'OU et permettre aux administrateurs de tester l'importation de données. Toutefois, l'intégration ne peut apporter des données dans le système qu'à partir de définitions d'unités organisationnelles actives.
Table	Spécifiez la table qui reçoit les données mappées de votre serveur LDAP. Pour les utilisateurs, sélectionnez **Utilisateur (sys_user)** et pour les groupes, sélectionnez **Groupe (sys_group).**
Filtre	Entrez une chaîne de filtre LDAP pour sélectionner des enregistrements spécifiques à importer à partir de l'OU. Plus la requête de filtre LDAP est spécifique, plus la requête est efficace.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par exemple, la définition LDAP OU des utilisateurs utilise le filtre suivant pour sélectionner les enregistrements qui sont classifiés comme une personne, qui ont une valeur d'attribut **sn** , qui ne sont pas des ordinateurs et qui ne sont pas marqués comme inactifs : `(&(objectClass=person)(sn=*)( !( objectClass=ordinateur)) ( ! ( userAccountControl :1.2.840.113556.1.4.803 :=2)))` Vous pouvez trouver une description de la syntaxe des filtres LDAP en recherchant sur Internet la RFC des filtres LDAP.

Example: Exemples de définitions d'unités organisationnelles

Supposons que vous disposiez d'un serveur LDAP avec la structure de répertoires suivante :

dc=mon-domaine,dc=com

- ou=Groupes
  - cn=Développement
  - cn=RH
  - cn=Ventes
- ou=Utilisateurs
  - ou=Développement
  - ou=RH
  - ou=Ventes

Supposons en outre que vous souhaitiez exclure le groupe RH et les utilisateurs RH de l'application. Effectuez les actions suivantes :

1. Créez un enregistrement de serveur LDAP avec un répertoire de recherche de départ de dc=mon-domaine,dc=com.
2. Créez un enregistrement de définition d'OU pour ou=Groupes avec un filtre pour exclure cn=HR.
3. Créez un enregistrement de définition d'OU pour ou=Utilisateurs avec un filtre permettant d'exclure ou=HR.

Si vous ne spécifiez pas d'attributs ou de filtres supplémentaires avec une définition d'OU, la requête LDAP renvoie la sous-arborescence complète du répertoire de départ et du RDN.

Dans ces exemples, une définition d'OU avec la valeur RDN ou=Groups et sans filtre aurait renvoyé tous les groupes. De même, une définition d'OU avec la valeur RDN ou=Users et sans filtre aurait renvoyé tous les utilisateurs et les unités organisationnelles enfants.

Créer une source de données pour LDAP

Chaque définition d'unité organisationnelle (UO) LDAP possède sa propre liste connexe de sources de données.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Remarque :
Le serveur LDAP et **la définition d'UO LDAP** doivent être actifs pour que l'action de chargement de test fonctionne correctement. Lorsque le chargement de test est activé pour la première fois, le système échantillonne jusqu'à 20 enregistrements pour déterminer la longueur des champs de jeu d'importation. Si les enregistrements échantillonnés ne contiennent pas de valeurs pour le champ **ID d'utilisateur** , le système définit la longueur de champ pour toutes les importations ultérieures à la longueur par défaut de 40. L'importation tronque toutes les données importées qui dépassent la longueur du champ de la table de l'ensemble d'importations. De plus, le champ **ID d'utilisateur** est tronqué à un maximum de 40 caractères. Sachez que les 20 enregistrements chargés ne peuvent pas être transformés et qu'ils ne sont effectués qu'à des fins de test. Si les enregistrements de test contiennent des valeurs pour le champ **ID d'utilisateur** , la longueur du champ est définie en fonction de la longueur de champ de l'ID d'utilisateur le plus long dans les enregistrements de test.

Pour créer une source de données :

Procédure

1. Accédez à la **Tout** > **Système LDAP** > **Serveurs LDAP**.
2. Sélectionnez le serveur LDAP à configurer.
3. Dans la liste **connexe Définitions LDAP OU** , sélectionnez un élément, tel que **Groupes** ou **Utilisateurs**.
4. Dans la liste connexe **Sources de données** , cliquez sur **Nouveau**.
5. Remplissez le formulaire Source de données (voir table).
6. Cliquez sur **Envoyer**.
7. Sous **Liens connexes**, cliquez sur Tester le **chargement de 20 enregistrements** pour vérifier si la source de données peut apporter des données LDAP dans la table d'importation.

Formulaire Sources de données

Champ	Description
Nom	Spécifiez le nom que l'intégration utilise lorsqu'elle fait référence à cette source de données.
Nom de la table des jeux d'importation	Entrez le nom de la table intermédiaire dans laquelle le système place temporairement les enregistrements LDAP importés et les attributs. Examinez cette table pour afficher les enregistrements LDAP importés. Vous pouvez utiliser le même nom de table de jeu d'importation pour toutes les sources de données LDAP.
Type	Sélectionnez **LDAP** pour indiquer que les données importées sont des données LDAP. Une fois le type **LDAP** sélectionné, le formulaire affiche le champ **cible LDAP** .
Cible LDAP	Sélectionnez la définition LDAP OU associée à cette source de données.

Mise en service automatique des utilisateurs LDAP

Vous provisionnez automatiquement les utilisateurs qui se trouvent dans le serveur LDAP, mais qui ne se trouvent pas encore dans votre instance.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Dans la table Propriétés système [sys_properties], créez les propriétés suivantes :

Propriétés LDAP

Propriété LDAP	Description
glide.ldap.authentication	Active l'authentification LDAP en utilisant LDAP pour authentifier les utilisateurs. Définissez cette propriété sur **vrai** (la valeur par défaut).
glide.ldap.user.autoprovision	Permet à LDAP de créer automatiquement des utilisateurs dans la table Utilisateur [sys_user] lorsque l'utilisateur existe dans LDAP, mais qu'il ne se trouve pas encore dans l'instance. Définissez cette propriété sur **vrai** (la valeur par défaut).

Ces deux propriétés doivent être définies sur **vrai** pour que la mise en service automatique fonctionne.

Intégration LDAP via Serveur MID

Les administrateurs peuvent s'intégrer à l'aide d'une source de données LDAP sur un serveur MID (Management, Instrumentation, and Discovery).

Le serveur MID permet la communication et le mouvement de données entre les applications, sources de Now Platform données et services externes. Pour plus d'informations sur l'installation d'un serveur MID, consultez Installation d'un serveur MID .

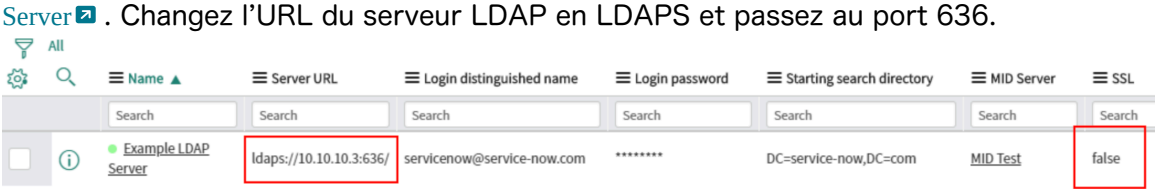
L'utilisation d'un serveur MID pour établir une connexion LDAP vous évite d'avoir à exposer le serveur LDAP au trafic réseau externe. Il élimine le besoin d'établir un tunnel VPN entre votre serveur LDAP et les centres de données. L'utilisateur du Serveur MID doit avoir le rôle user_admin pour pouvoir lire les enregistrements de configuration du serveur LDAP.

Remarque :
Le serveur MID n'autorise pas l'utilisation de l'action d'interface utilisateur `<instance>/sys_ui_action.do ?sys_id=1b4f7ef30a0001060058e223c9a5744c` pour actualiser les enregistrements d'utilisateurs et de groupes de LDAP.

Par défaut, une connexion au serveur MID communique par HTTP sur le port 80. Ce canal de communication ne nécessite pas de certificat. La connexion entre le serveur MID et l'instance se fait via HTTPS (port 443). L'instance se connecte directement au serveur LDAP à l'aide de LDAP ou LDAPS. Cette connexion peut se faire via Internet ou via un tunnel VPN.

Remarque :
LDAP ne peut pas communiquer via le MID Server avec authentification par mot de passe.

Pour une communication sécurisée via SSL, vous devez ajouter un certificat SSL pour le MID Server . Changez l'URL du serveur LDAP en LDAPS et passez au port 636.



Remarque :
Si vous créez un serveur LDAP, le marqueur SSL du serveur MID est défini sur false par défaut. Vous pouvez ignorer ce comportement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour définir les propriétés de connexion d'un serveur LDAP spécifique, reportez-vous à la section Définir un serveur LDAP.

Configurer la surveillance des connexions LDAP

Modifiez ou désactivez la surveillance et les notifications de connexion LDAP.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
L'instance envoie automatiquement un e-mail aux utilisateurs configurés dans le groupe d'administrateurs LDAP lorsqu'une connexion au serveur LDAP échoue. Elle utilise la notification par e-mail d'échec de connexion , qui est lancée par la tâche planifiée **Test de connexion LDAP**. Cette notification par e-mail est activée par défaut.

Remarque :
L'instance n'envoie pas de notification par e-mail à moins qu'il n'y ait au moins un membre dans le groupe d'administrateurs LDAP. Assurez-vous de renseigner ce groupe avec les utilisateurs que vous souhaitez voir recevoir l'e-mail.

Par défaut, la tâche planifiée teste la connexion toutes les 15 minutes. Pour modifier cet intervalle ou désactiver la surveillance :

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Travaux planifiés**.
2. **Ouvrez le test de connexion LDAP**.
3. Effectuez l'une des actions suivantes :
   - Modifiez l'intervalle dans le champ **Intervalle de répétition** .
   - Désactivez la surveillance en décochant la case **Actif** .

Importer des données binaires via un serveur MID

En tant qu'administrateur, vous pouvez importer des données d'objet BLOB (Binary Large Object) avec une intégration LDAP via le serveur MID.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Procédure

1. Ajoutez le nom de la colonne LDAP à partir de laquelle vous souhaitez importer des données binaires à la `glide.ldap.binary_attributes` des propriétés système.
2. Ajoutez une propriété de serveur MID avec le nom `glide.ldap.binary_attributes` et la même valeur que celle que vous avez définie pour la propriété système.

Dépannage de l'intégration LDAP via un serveur MID

Vous pouvez rencontrer des problèmes dans les domaines suivants lors de l'intégration de LDAP via Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez résoudre ces problèmes en affichant les sorties trouvées dans la file d'attente ECC (canal de communication externe) (**Découverte** > **Résultats et artefacts** > **File d'attente ECC**).

Problèmes liés au test de la connexion

Lors de la définition d'unités organisationnelles dans le serveur, la liste connexe **Test de la connexion** est utilisée pour vérifier la connexion LDAP. Lorsque vous cliquez sur ce lien, la file d'attente ECC doit afficher un message de sortie unique avec le nom de rubrique **LDAPConnectionTesterProbe**. Une fois le test terminé sur le serveur MID, la file d'attente ECC doit afficher un message d'entrée portant le même nom de rubrique. Si la colonne **Nom** du message d'entrée **affiche vrai**, le test a réussi. Explorez l'enregistrement pour afficher la charge utile et vous assurer qu'il ne contient pas de messages d'erreur.

Test de la connexion

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:24:17	mid.server.local_mid	LDAPConnectionTesterProbe	true	04a952038f21010036bf21ca47e79a30	input	processed	2013-07-29 13:24:19
2013-07-29 13:24:04	mid.server.local_mid	LDAPConnectionTesterProbe		04a952038f21010036bf21ca47e79a30	output	processed	2013-07-29 13:24:17

Parcourir les problèmes

Lors de la définition d'unités organisationnelles dans le serveur, une liste connexe **Parcourir** permet d'afficher les enregistrements du répertoire LDAP renvoyés par la définition d'unité organisationnelle. Lorsque vous cliquez sur ce lien, la file d'attente ECC doit afficher un message de sortie unique avec le nom de rubrique **LDAPBrowseProbe**. Une fois que les données ont été renvoyées par le serveur MID, la file d'attente ECC doit afficher un message d'entrée portant le même nom de rubrique. Si la colonne **Nom** du message d'entrée **affiche vrai**, le test a réussi. Explorez l'enregistrement pour afficher la charge utile et vous assurer qu'il ne contient pas de messages d'erreur.

Charger les problèmes d'importation

Lors du chargement des données (par exemple, à l'aide de la fonctionnalité Tester le chargement de 20 enregistrements), la file d'attente ECC doit afficher un seul message de sortie avec un nom de rubrique **LDAPProbe**.

Une fois que les données ont été renvoyées par le MID Server, la file d'attente ECC doit afficher un autre message d'entrée appelé **LDAPProbeCompleted**. La colonne **Nom** de ce message d'entrée affiche le nombre total d'enregistrements renvoyés.

Un message d'entrée supplémentaire, également appelé **LDAPProbe**, s'affiche. La colonne **Nom** de ce message d'entrée affiche le numéro d'enregistrement le plus élevé du lot. Si le nombre total d'enregistrements retournés est de 258 et que la taille du lot est de 200 (valeur par défaut), deux messages entrants LDAPProbe (200, 258) messages entrants sont reçus, et un message entrant LDAPProbeCompleted (258) est reçu.

Explorez l'enregistrement pour afficher la charge utile et vous assurer qu'il ne contient pas de messages d'erreur.

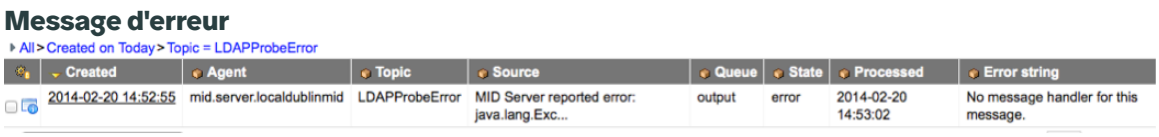
Chargement de l'importation

Created	Agent	Topic	Name	Source	Queue	State	Processed
2013-07-29 13:09:48	mid.server.local_mid	LDAPProbeCompleted	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:48	LDAPProbeResult	LDAPProbe	11	ed0a0d7a8f32010036bf21ca47e79a56	input	processed	2013-07-29 13:09:51
2013-07-29 13:09:36	mid.server.local_mid	LDAPProbe		ed0a0d7a8f32010036bf21ca47e79a56	output	processed	2013-07-29 13:09:46

Gardez également un œil sur un message de sortie appelé **LDAPProbeError**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Cliquez sur le lien dans la colonne **Nom** pour afficher les détails de l'erreur.

Pagination LDAP

La pagination LDAP ne fonctionne pas si la taille de pagination sur le serveur LDAP est inférieure à 1 000. Définissez la propriété `glide.ldap.max_results` du serveur MID sur une valeur inférieure ou égale à la taille de pagination du serveur LDAP.

LDAP échoue dans l'importation des données binaires

Pour importer des données binaires via LDAP, telles qu'une photo d'utilisateur, vous devez inclure l'attribut binaire dans la propriété `glide.ldap.binary_attributes`Serveur MID . Pour l'exemple de photo d'utilisateur, l'attribut peut être `jpegphoto`.

Importer et mapper des données

Les mappages d'importation LDAP font correspondre les champs de votre base de données LDAP aux champs de votre instance.

Remarque :
Le mappage LDAP ayant un effet sur les performances, il est recommandé de le planifier pendant les heures creuses ou de traiter quelques enregistrements à la fois pour maintenir la disponibilité du système.

Définissez une carte de transformation qui importe uniquement les attributs nécessaires ou requis. Selon la version de l'instance que vous utilisez, la méthode de spécification des relations de mappage LDAP varie.

Le moyen le plus simple de savoir si vous exécutez ou non une version qui utilise l'application LDAP système pour l'intégration LDAP consiste à trouver l'application dans le navigateur d'application.

L'option **Exécuter les règles métier** n'est appliquée qu'à la table cible. Seules les cartes de transformation associées à la table cible exécutent les règles métier associées à différentes tables. Si vous mettez à jour un groupe d'utilisateurs et que des règles métier sont en cours d'exécution sur une table de groupe d'utilisateurs, des rôles doivent être définis pour le groupe.

Options de mappage d'importation LDAP

Application LDAP du système ?	Carte
Oui	Utilisez une *carte de transformation* pour spécifier votre mappage.
Non	Utilisez une *carte d'importation LDAP héritée* pour spécifier votre mappage ou la transformation LDAP par défaut incluse dans les instances de base de référence. N'oubliez pas d'ajuster le champ **Fusion** pour qu'il corresponde aux champs corrects.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Importations planifiées

Une importation planifiée permet aux administrateurs d'importer des données LDAP selon un calendrier régulier. Par défaut, l'intégration LDAP inclut deux exemples d'importations planifiées :

- Exemple d'importation d'utilisateur LDAP
- Exemple d'importation de groupe LDAP

Aucun des exemples n'est actif par défaut. Modifiez ces importations planifiées pour répondre aux besoins professionnels de votre entreprise.

Cartes de transformation LDAP

La carte de transformation déplace les données de la table de jeux d'importation vers la table cible (utilisateur ou groupe).

L'intégration LDAP utilise des ensembles d'importation et des cartes de transformation standard. Vous pouvez également créer des cartes de transformation LDAP personnalisées.

Important :
Que vous sélectionniez ou créiez des cartes de transformation LDAP personnalisées, il doit y avoir une carte de transformation active pour un ensemble de tables source et cible. L'activation de plusieurs cartes de transformation pour les mêmes tables source et cible peut produire des entrées en double dans la table cible, à moins que vous ne fusionniez avec les champs correspondants.

Cartes de transformation LDAP par défaut

Par défaut, le système fournit deux cartes de transformation pour les données LDAP.

Cartes de transformation LDAP par défaut

Carte de transformation	Table source	Table cible	Description
Importation d'utilisateur LDAP	[ldap_import]	[sys_user]	Carte de transformation par défaut pour la création d'enregistrements utilisateur à partir d'informations d'identification LDAP dans le cadre de la connexion LDAP à la demande. Contient des mappages pour un serveur LDAP Active Directory.
Importation de groupe LDAP	[ldap_group_import]	[sys_user_group]	Carte de transformation par défaut pour la création d'enregistrements de groupe à partir d'unités organisationnelles LDAP. Contient des mappages pour un serveur LDAP Active Directory.

Remarque :
Par défaut, le système ne dispose pas d'une carte de transformation pour les enregistrements du département LDAP.

Exigences relatives aux cartes de transformation LDAP personnalisées

Si vous choisissez de créer une carte de transformation personnalisée, celle-ci doit répondre aux exigences de mappage suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exigences relatives aux cartes de transformation LDAP personnalisées

Table source	Champ source	Table cible	Champ cible	Fusion	Description
ldap_import	u_source	sys_user	source	faux	Le champ **u_source** identifie le DN LDAP de l'utilisateur ou du groupe importé. Le système utilise ce champ pour déterminer qu'un utilisateur a besoin d'une authentification LDAP, pour trouver le responsable d'un utilisateur et pour placer les utilisateurs dans des groupes.
ldap_import	Sélectionnez l'un des champs suivants : • u_samaccountname • u_dn • u_cn	sys_user	user_name	VRAI	Si LDAP s'intègre à Active Directory, sélectionnez **u_samaccountname** comme champ source. Si d'autres répertoires LDAP sont utilisés, sélectionnez **u_dn** ou **u_cn** comme champ source.

Différences entre les cartes de transformation LDAP et les cartes d'importation héritées

Lors de la spécification de relations de mappage LDAP à l'aide de cartes de transformation, il existe une différence majeure dans la façon dont les champs de référence sont définis pour le gestionnaire et le département.

Lors de l'utilisation d'une *carte de transformation*, il est nécessaire d'utiliser un *script de transformation* pour créer des références. Cela est dû au fait que la valeur associée à un attribut LDAP comme « gestionnaire » est le nom unique (DN) du gestionnaire.

En l'absence d'une logique supplémentaire, le résultat est la création d'un enregistrement utilisateur avec un nom de gestionnaire qui est le nom unique de cet utilisateur dans LDAP. L'intégration inclut un script de transformation pour faciliter la création de ces références. La carte de transformation par défaut « Importation de l'utilisateur LDAP » inclut des scripts de transformation pour ces références.

Relations de mappage existantes

Lors de la mise à jour des cartes d'importation héritées vers des cartes de transformation, vous pouvez conserver les relations de mappage LDAP qui existaient avant l'ajout de l'application LDAP système. Le serveur LDAP dispose d'un champ **Carte** qui fait référence à la carte d'importation héritée.

Remarque :
Par défaut, ce champ est masqué, vous devez donc configurer le formulaire pour l'afficher.

Si vous souhaitez effectuer une transition vers l'utilisation d'une carte de transformation, effacez la référence à la carte d'importation héritée.

Paramètres de carte d'importation LDAP

Vérifiez et utilisez des attributs pour limiter les champs importés par l'intégration à partir de la source LDAP. En outre, il est important de mapper

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

le champ user_name à l'attribut LDAP qui contient l'ID de connexion de l'utilisateur. Pour Active Directory, il s'agit généralement de l'attribut sAMAccountName. Si vous souhaitez importer et fusionner sur un attribut binaire (tel que objectSID ou objectGUID), vous devez créer un script de transformation personnalisé.

Remarque :
Toute valeur mappée au champ user_name doit être unique.

Si vous ne spécifiez pas de carte de transformation (telle que LDAP User Import), l'intégration utilise les mappages par défaut suivants :

Mappage par défaut de l'importation LDAP

Champ ou variable d'utilisateur	Attribut LDAP
user_name	sAMAccountName
E-mail	Courrier
Téléphone	numéro de téléphone
home_phone	Téléphone d'accueil
mobile_phone	mobile
first_name	Nom donné
last_name	Sn
Titre	Titre
département	département
responsable	responsable
middle_name	paraphe
u_memberof	groupes
u_member	membres
u_manager	responsable

Transformation des données LDAP

Si un attribut LDAP contient des données simples, la carte de transformation lie un attribut LDAP importé à un champ approprié dans la table cible (Utilisateur ou Groupe). Par exemple, les données témoins de l'attribut sAMAccountName sont mappées au champ **ID d'utilisateur** de la table Utilisateur.

Si les données LDAP importées sont mappées à un champ de référence, l'instance recherche un enregistrement correspondant existant. Si aucun enregistrement correspondant n'existe, l'instance crée un nouvel enregistrement pour le champ de référence, sauf indication contraire du mappage de champ.

Par exemple, supposons que l'attribut LDAP l est mappé au champ **de référence Emplacement** de la table Utilisateur. Chaque fois que l'importation apporte une valeur d'attribut qui ne correspond pas à une valeur d'enregistrement d'emplacement existante, la carte de transformation crée un nouvel enregistrement d'emplacement. Le nouvel enregistrement d'emplacement a la même valeur que l'attribut importé, et l'enregistrement d'utilisateur importé dispose désormais d'un lien vers le nouvel enregistrement d'emplacement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Toutefois, il arrive que l'attribut LDAP renvoie un nom unique (DN), qui est essentiellement une référence à un autre enregistrement dans l'annuaire LDAP. Par exemple, l'attribut gestionnaire contient généralement le nom unique du gestionnaire de l'entrée actuelle de l'annuaire LDAP. Un DN importé utilise généralement une longue chaîne de texte telle que : cn=Beth Anglin,ou=Users,dc=my-domain,dc=com.

⚠ Avertissement :
Assurez-vous que vos champs cibles sont suffisamment longs pour contenir un DN. De nombreux champs de texte utilisent la longueur par défaut de 40, qui peut ne pas être assez longue pour certaines valeurs DN. Le ServiceNow système tronque toute valeur qui dépasse la longueur du champ.

En général, les administrateurs ne souhaitent pas que le système crée de nouveaux utilisateurs à partir de la valeur DN, car le nouvel utilisateur n'est pas associé à un utilisateur existant. Au lieu de cela, les administrateurs souhaitent que l'importation localise l'enregistrement utilisateur existant du gestionnaire et l'associe à l'utilisateur nouvellement importé. L'include de script LDAPUtils contient les fonctions setManager et processManagers qui peuvent analyser un DN et rechercher un utilisateur existant. Pour de meilleurs résultats, utilisez ces fonctions pour créer une carte de transformation personnalisée.

Par exemple, le script de carte de transformation d'importation de l'utilisateur LDAP appelle la fonction setManager :

```
//
// The manager coming in from LDAP is the DN value for the manager.
// The line of code below will locate the manager that matches the
// DN value and set it into the target record.  If you are not
// interested in getting the manager from LDAP then remove or
// comment out the line below
ldapUtils. setManager (source , target ) ;
```

Dans certains cas, l'intégration importe l'enregistrement d'un utilisateur avant l'enregistrement de l'utilisateur du gestionnaire associé. Pour gérer de tels cas, vous pouvez appeler la fonction processManagers une fois la transformation terminée. Par exemple, la carte de transformation **d'importation d'utilisateur LDAP** utilise un script de transformation onComplete pour appeler la fonction processManagers .

```
// It is possible that the manager for a user did not exist in the database when // the
 user was processed and therefore we could not locate and set the manager field. // The
 processManagers call below will find all those records for which a manager could  // not be
 found and attempt to locate the manager again. This happens at the end of the  // import and
 therefore all users should have been created and we should be able to  // locate the manager
 at this point
ldapUtils. processManagers ( ) ;
```

Supprimez ou commentez les appels de fonction setManager et processManagers si votre intégration LDAP n'utilise pas l'attribut manager.

Scripting LDAP

Créez des cartes de transformation, des scripts et des règles métier personnalisés pour spécifier les exigences lors de l'importation de données.

Les cartes de transformation personnalisées doivent inclure les scripts de transformation onStart et onAfter .

Le script onStart doit appeler l'include de script LDAPUtils et commencer la journalisation. Par exemple, la carte de transformation **Importation de l'utilisateur LDAP** possède un script onStart qui utilise le code suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
gs.include ( "LDAPUtils" ) ; var ldapUtils  = new LDAPUtils ( ) ;
ldapUtils. setLog (log ) ;
```

Le script `onAfter` doit appeler la fonction `addMembers` . Par exemple :

```
ldapUtils.addMembers (source , target ) ;
```

Définir les utilisateurs Active Directory désactivés comme inactifs

Utilisez le script suivant pour désactiver automatiquement les utilisateurs lorsque l'utilisateur AD associé est désactivé.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Vous pouvez identifier les utilisateurs Active Directory désactivés en vérifiant la valeur de l'attribut `userAccountControl` . Cette règle s'exécute chaque fois que la valeur `userAccountControl` change et désactive les comptes d'utilisateurs si le **contrôle de compte d'utilisateur** signifie un compte AD désactivé.

Utilisez le script suivant pour désactiver automatiquement les utilisateurs lorsque l'utilisateur AD associé est désactivé.

Procédure

1. Configurez le formulaire Utilisateur et créez un nouveau champ entier appelé **Contrôle de compte d'utilisateur**.
2. Ajoutez un mappage pour userAccountControl (externe) au nouveau champ.
3. Créez une règle métier avec les propriétés suivantes :

Désactiver la règle métier des utilisateurs AD

Champ de règle métier	Valeur
Nom	Désactiver les utilisateurs AD
Table	Utilisateur [sys_user]
Quand	Avant
Condition	current.u_user_account_control.changes()

Le champ Script doit contenir les éléments suivants :

```
var disabledFlag = 2;
//perform a bitwise comparison on userAccountControl to see if the 2 bit flag is enabled
if (current.u_user_account_control & disabledFlag) {
  gs.log('Disabling user: ' + current.user_name + 'userAccountControl=' +
 current.u_user_account_control);
  current.active='false';
  current.locked_out='true';
}
```

Affecter des valeurs de champ LDAP

Vous pouvez utiliser un script pour affecter une valeur à n'importe quel champ pour lequel il existe un mappage de champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par exemple, pour affecter une valeur au champ sys_user.company, créez une carte de champ pour le champ entreprise et ajoutez un script de transformation de :

```
company = "Don's Sporting Goods";
```

Exclure certains utilisateurs LDAP

Si vous ne pouvez pas filtrer complètement la liste des utilisateurs LDAP à l'aide des propriétés du filtre LDAP, vous pouvez exclure des utilisateurs à l'aide d'un script de mappage.

Une fois que vous avez exécuté la logique pour identifier un utilisateur qui ne doit pas être importé, définissez le champ user_name sur une chaîne vide et cet utilisateur ne sera pas importé.

```
user_name='';
```

Une façon d'identifier les utilisateurs à filtrer consiste à rechercher une chaîne dans l'attribut `distinguishedName` . Par exemple, ce script exclut les comptes qui ne se trouvent pas dans une UO Utilisateurs. Vous pouvez utiliser ce script si vous avez trop d'UO d'utilisateurs pour les inclure dans l'UO cible Option LDAP.

```
//vdn is a variable mapped to distinguishedName
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
if (vdn.indexOf('OU=Users')<0) {
  user_name='';
  gs.log('LDAP Import Skipping User: ' + vdn);
}
```

Une méthode de filtrage plus complexe consiste à utiliser des expressions régulières.

```
//vcn is a variable mapped to cn
//vdn is a variable mapped to distinguishedName
//c is the regular expression string
gs.include("LDAPUtils");
var vdn = source.getElement(this.distinguishedName);
var vcn = source.getElement(this.cn);
var c = /^[a-z][a-z][a-z][0-9][0-9][0-9]$/;
var nvcn = vcn.toLowerCase();
//test to see if the cn is in the form of 3 letters followed by 3 numbers, only import these
if (c.test(nvcn)) {
 user_name = nvcn;
} else {
 gs.log("LDAP import rejected username: " + vcn + " for DN: " + vdn);
 user_name = "";
}
```

Définir l'action de choix pour les importations de champs de référence

La carte de transformation LDAP détermine la façon dont les champs de la table Jeu d'importation sont mappés aux champs de tables existantes telles que Incident ou Utilisateur.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Si la carte de transformation LDAP met à jour un champ dans la table de jeux d'importation, l'intégration crée automatiquement un nouvel enregistrement chaque fois qu'un nouvel enregistrement existe dans les données LDAP. Si la carte de transformation LDAP met à jour un champ de référence stockant les données d'une autre table, l'administrateur peut choisir de créer, d'ignorer ou de rejeter de nouveaux enregistrements LDAP. Par exemple, si l'intégration reçoit un nouvel enregistrement de département qui ne correspond à aucun département existant, vous pouvez mettre à jour tous les autres champs d'enregistrement LDAP sans créer de nouvel enregistrement de département dans l'instance. La carte de transformation vous permet de définir les options de création d'enregistrement pour chaque champ de référence.

Procédure

1. Accédez à la **Tout** > **Système LDAP** > **Cartes de transformation**.
2. Dans la liste connexe Cartes de champs, sélectionnez l'une des actions suivantes dans le champ **Action de choix** :
   - **Créer** : crée un nouvel enregistrement de champ de référence si aucun enregistrement correspondant n'existe.
   - **Ignorer** : ignore les nouveaux enregistrements dans le champ de référence et termine le traitement de tous les autres champs dans la carte de transformation.
   - **Rejeter** : arrête la transformation pour l'ensemble de l'enregistrement.

Remarque :
La carte de champs affiche uniquement le champ **d'action Choix** pour les champs de référence.

Vérifier le mappage LDAP

Après avoir créé une carte de transformation LDAP, actualisez les données LDAP pour vérifier que la carte de transformation fonctionne comme prévu.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Système LDAP** > **Charges planifiées**.
2. Cliquez sur votre tâche d'importation LDAP.
3. Cliquez sur **Exécuter maintenant**.

Dépannage de l'intégration LDAP

Si vous intégrez votre serveur LDAP et que vous avez des questions, ces éléments peuvent vous aider à résoudre le problème.

Vérifications préliminaires

- Si LDAP n'est pas disponible, les utilisateurs ne peuvent pas se connecter à l'instance. Une bonne pratique consiste à avoir des comptes locaux pour les administrateurs afin qu'en cas d'arrêt du LDAP, les administrateurs puissent toujours accéder à l'instance.
- Vérifiez le compte de service pour vous assurer qu'il n'est pas expiré ou verrouillé.
- Vérifiez le format du nom d'utilisateur. Au lieu d'utiliser uniquement le nom d'utilisateur, essayez d'utiliser le domaine avec le nom d'utilisateur, ou username@domain.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vérifiez que vous avez modifié l'entrée de system_id dans l'enregistrement ldap_server_config . Si vous modifiez le system_id de manière involontaire avec un ensemble de mises à jour, system_id pointe vers le mauvais nœud pour l'instance cible et ne fonctionne pas.

Codes d'erreur

Le fichier journal LDAP répertorie les codes d'erreur standard du secteur pour LDAP et Active Directory (AD). Le fichier journal LDAP est contenu dans le fichier wrapper. Les codes d'erreur LDAP sont des nombres à deux chiffres, tandis que les codes d'erreur Active Directory sont des nombres à trois chiffres. Pour obtenir la liste des codes d'erreur les plus courants, consultez Codes d'erreur LDAP.

Intégration dans plusieurs domaines

Vous pouvez intégrer plusieurs domaines au sein d'une même forêt ou dans des domaines totalement non approuvés. Nous vous recommandons de créer un enregistrement de serveur LDAP distinct pour chaque domaine. Chaque enregistrement de serveur LDAP doit pointer vers un contrôleur de domaine pour ce domaine donné. Cela signifie que vous devrez autoriser les connexions à chacun des contrôleurs de domaine. Plusieurs forêts AD via LDAP avec un seul compte LDAP ne sont pas prises en charge.

Lorsque vous étendez à plus d'un domaine, il est essentiel d'identifier des attributs LDAP uniques pour les noms d'utilisateur d'application et d'importer des valeurs de fusion. objectSid est un attribut de coalescence unique commun pour Active Directory. Les noms d'utilisateur uniques varient en fonction de la conception de vos données LDAP. Les attributs uniques courants sont e-mail ou userPrincipalName.

Enregistrements entrants

Reportez-vous à la rubrique Cartes de transformation LDAP pour définir comment l'intégration traite les enregistrements LDAP entrants pour lesquels il manque des valeurs correspondantes dans les champs de référence.

Erreurs d'authentification courantes

- L'utilisateur ne peut pas se connecter (DN non valide)
- CN non valide
- Connexion non valide

Tests automatiques de connexion LDAP

Vous pouvez tester manuellement les connexions aux serveurs LDAP ou autoriser ServiceNow le test automatique des connexions.

Le système teste automatiquement la connexion :

- Chaque fois qu'un utilisateur ouvre le formulaire du serveur LDAP.
- Via la tâche planifiée de test de connexion LDAP, qui s'exécute toutes les 15 minutes par défaut.

  Vous pouvez modifier la fréquence d'exécution de cette tâche planifiée. Si cette tâche planifiée n'est pas en mesure d'établir une connexion, une nouvelle tâche planifiée ponctuelle retente le test de connexion après cinq minutes ou la moitié de la valeur **de l'intervalle de répétition** de la tâche planifiée, selon ce qui se produit en premier.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Des messages d'erreur s'affichent sur le formulaire en cas de problème de connexion au serveur LDAP. Les connexions de test sont également prises en charge pour les serveurs derrière un MID Server.

Afficher la surveillance LDAP

Vous pouvez afficher des informations actuelles sur les serveurs et les écouteurs LDAP à l'aide du moniteur LDAP.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les états disponibles sont les suivants :

- Actif
- Inactif
- Erreur
- Actif (arrêt...)
- Erreur (arrêt...)

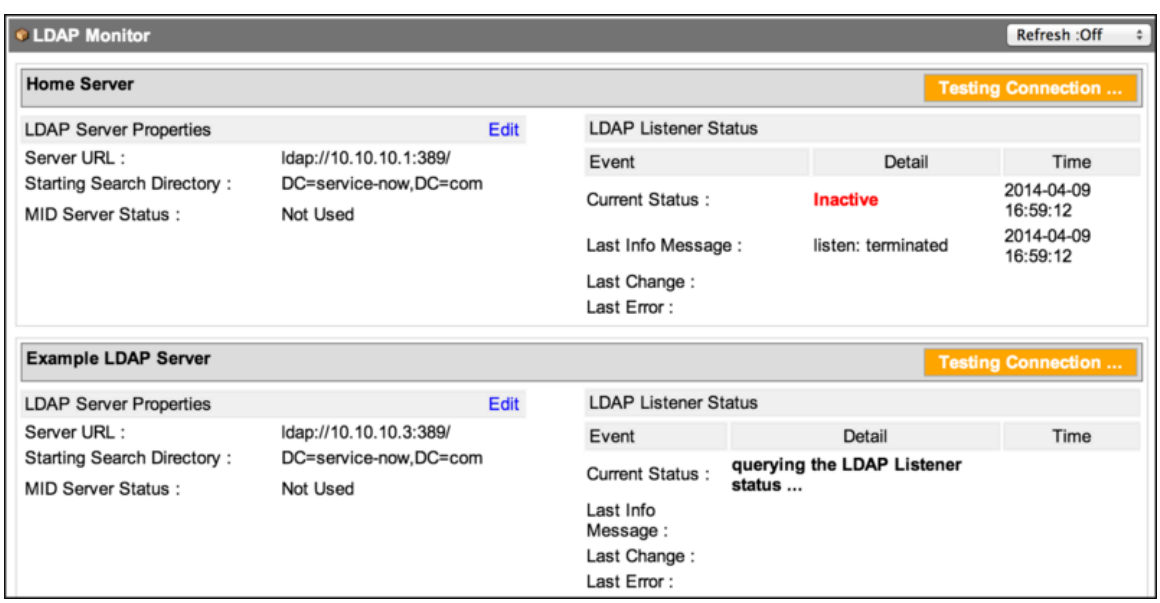
En plus de son état actuel, le moniteur affiche également :

- Dernier message détecté par l'écouteur, tel que l'attente de changements LDAP, une erreur de connexion, etc.
- Le dernier changement d'utilisateur LDAP, tel qu'un nouvel utilisateur, un utilisateur mis à jour, etc.
- La dernière erreur qui s'est produite.

Pour afficher le moniteur LDAP :

Procédure

Accédez à la **Tout** > **LDAP** > **Système LDAP** > **Surveillance LDAP**.



Consultez le tableau pour obtenir une description des propriétés et des champs à l'écran.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Surveillance LDAP

Champ	Description
Actualiser	Vous pouvez configurer le taux d'actualisation en cliquant sur le champ **Actualiser** dans la barre d'en-tête du moniteur du serveur LDAP et en sélectionnant le nombre de secondes entre chaque actualisation de données. Vous pouvez également sélectionner **Aucun** pour supprimer l'actualisation.
État de connexion	L'indicateur de connexion au serveur se trouve sur le côté droit, au-dessus des champs État de l'écouteur LDAP. Lorsque le serveur est connecté, la case est verte et affiche *Connecté*. Lorsque le serveur n'est pas connecté, la case est rouge et indique *Non connecté*. Lorsque la connexion au serveur est en cours de test, la zone est jaune et affiche *Test de la connexion*.
Propriétés du serveur LDAP	
Modifier	Lorsque vous surveillez les serveurs LDAP, vous pouvez apporter des modifications aux propriétés en cliquant sur **Modifier** dans l'écran Moniteur du serveur LDAP.
URL serveur	Combinaison du nom du serveur et du port de serveur sur lequel le serveur LDAP est à l'écoute. Souvent, le port est défini sur l'une des valeurs suivantes : • 389 : port par défaut pour la connexion à LDAP en texte clair • 636 : port standard pour la connexion à LDAP via une connexion SSL Exemple de valeur : ldap://10.10.10.3:389/ Votre serveur LDAP peut avoir plusieurs adresses URL. Cela n'établit PAS plusieurs structures de répertoires à partir desquelles vous pouvez importer des données, ce qui se fait en créant une autre entrée de serveur LDAP, mais prévoit une redondance lorsque vous avez plusieurs serveurs LDAP pour éviter un point de défaillance unique. Les adresses URL LDAP sont séparées par un espace, et le système essaie automatiquement chaque adresse de serveur à tour de rôle jusqu'à ce qu'une connexion valide puisse être établie.
Répertoire de recherche de départ	Répertoire de départ ou NDR (Nom Distinct Relatif) dans lequel le système commence à rechercher des utilisateurs ou des groupes. Exemple de valeur : DC=service-now,DC=com Aucune donnée AU-DESSUS de ce point n'est disponible pour l'importation. L'instance a une visibilité sur le répertoire spécifié et les répertoires EN DESSOUS dans la hiérarchie LDAP.
État du serveur MID	L'état actuel de la connexion du Serveur MID.
État de l'écouteur LDAP	
État actuel	Cela indique si l'écouteur est actif.
Dernier message d'informations	Il affiche le dernier message que le serveur LDAP a reçu concernant les changements d'utilisateurs et de groupes, ainsi que l'heure à laquelle le message a été reçu.
Dernier changement	Affiche la dernière modification apportée au serveur LDAP et l'heure à laquelle elle a été apportée.
Dernière erreur	Il affiche la dernière erreur qui s'est produite sur le serveur LDAP et l'heure à laquelle elle s'est produite.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Codes d’erreur LDAP

Le fichier journal LDAP répertorie les codes d’erreur standard du secteur pour LDAP et Active Directory (AD).

Codes d’erreur standard

Erreurs LDAP standard

Code d’erreur/ de données	Texte	Description
0	LDAP_SUCCESS	Indique que l’opération client demandée s’est terminée avec succès.
2	LDAP_PROTOCOL_ERROR	Indique que le serveur a reçu une demande non valide ou mal formée du client.
3	LDAP_TIMELIMIT_EXCEEDED	Indique que la limite de temps de l’opération spécifiée par le client ou le serveur a été dépassée. Lors des opérations de recherche, les résultats incomplets sont renvoyés.
4	LDAP_SIZELIMIT_EXCEEDED	Indique que dans une opération de recherche, la limite de taille spécifiée par le client ou le serveur a été dépassée. Les résultats incomplets sont renvoyés.
5	LDAP_COMPARE_FALSE	N’indique pas une condition d’erreur. Indique que les résultats d’une opération de comparaison sont faux.
6	LDAP_COMPARE_TRUE	N’indique pas une condition d’erreur. Indique que les résultats d’une opération de comparaison sont vrais.
7	LDAP_AUTH_METHOD_NOT_SUPPORTED	Indique que lors d’une opération de liaison, le client a demandé une méthode d’authentification non prise en charge par le serveur LDAP.
8	LDAP_STRONG_AUTH_REQUIRED	Indique l’un des éléments suivants : Dans les demandes de liaison, le serveur LDAP accepte uniquement l’authentification forte. Dans une demande client, le client a demandé une opération, telle que la suppression, qui nécessite une authentification forte. Dans un avis de déconnexion non sollicité, le serveur LDAP découvre que la sécurité protégeant la communication entre le client et le serveur a échoué de manière inattendue ou a été compromise.
9		Réservé.
10	LDAP_REFERRAL	N’indique pas une condition d’erreur. Dans LDAPv3, indique que le serveur ne détient

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
		pas l'entrée cible de la requête, mais que les serveurs dans le champ de référence le peuvent.
11	LDAP_ADMINLIMIT_EXCEEDED	Indique qu'une limite du serveur LDAP définie par une autorité administrative a été dépassée.
12	LDAP_UNAVAILABLE_CRITICAL_EXTENSION	Indique que le serveur LDAP n'a pas été en mesure de satisfaire une demande car une ou plusieurs extensions critiques n'étaient pas disponibles. Soit le serveur ne prend pas en charge le contrôle, soit le contrôle n'est pas approprié pour le type d'opération.
13	LDAP_CONFIDENTIALITY_REQUIRED	Indique que la session n'est pas protégée par un protocole TLS (Transport Layer Security), qui assure la confidentialité de la session.
14	LDAP_SASL_BIND_IN_PROGRESS	N'indique pas une condition d'erreur, mais indique que le serveur est prêt pour l'étape suivante du processus. Le client doit envoyer au serveur le même mécanisme SASL pour poursuivre le processus.
15		Pas utilisé(e).
16	LDAP_NO_SUCH_ATTRIBUTE	Indique que l'attribut spécifié dans l'opération de modification ou de comparaison n'existe pas dans l'entrée.
17	LDAP_UNDEFINED_TYPE	Indique que l'attribut spécifié dans l'opération de modification ou d'ajout n'existe pas dans le schéma du serveur LDAP.
18	LDAP_INAPPROPRIATE_MATCHING	Indique que la règle de correspondance spécifiée dans le filtre de recherche ne correspond pas à une règle définie pour la syntaxe de l'attribut.
19	LDAP_CONSTRAINT_VIOLATION	Indique que la valeur d'attribut spécifiée dans une opération DN de modification, d'ajout ou de modification enfreint les contraintes placées sur l'attribut. Il peut s'agir d'une contrainte de taille ou de contenu (chaîne uniquement, aucun binaire).
20	LDAP_TYPE_OR_VALUE_EXISTS	Indique que la valeur d'attribut spécifiée dans une opération de modification ou

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
		d'ajout existe déjà en tant que valeur pour cet attribut.
21	LDAP_INVALID_SYNTAX	Indique que la valeur d'attribut spécifiée dans une opération d'ajout, de comparaison ou de modification est une syntaxe non reconnue ou non valide pour l'attribut.
22-31		Pas utilisé(e).
32	LDAP_NO_SUCH_OBJECT	Indique que l'objet cible est introuvable. Ce code n'est pas renvoyé lors des opérations suivantes : Opérations de recherche qui trouvent la base de recherche, mais ne trouvent aucune entrée correspondant au filtre de recherche. Lier les opérations.
33	LDAP_ALIAS_PROBLEM	Indique qu'une erreur s'est produite lorsqu'un alias a été déréférencé.
34	LDAP_INVALID_DN_SYNTAX	Indique que la syntaxe du DN est incorrecte. (Si la syntaxe DN est correcte, mais que les règles de structure du serveur LDAP ne permettent pas l'opération, le serveur renvoie le code 53 : LDAP_UNWILLING_TO_PERFORM.)
Ratio	LDAP_IS_LEAF	Indique que l'opération spécifiée ne peut pas être effectuée sur une entrée terminale. (Ce code n'est pas actuellement dans les spécifications LDAP, mais est réservé à cette constante.)
36	LDAP_ALIAS_DEREF_PROBLEM	Indique que lors d'une opération de recherche, soit le client n'a pas les droits d'accès pour lire le nom de l'objet aliassé, soit le déréférencement n'est pas autorisé.
37-47		Pas utilisé(e).
48	LDAP_INAPPROPRIATE_AUTH	Indique que lors d'une opération de liaison, le client tente d'utiliser une méthode d'authentification qu'il ne peut pas utiliser correctement. Par exemple, l'une des situations suivantes est à l'origine de cette erreur : Le client retourne des informations d'identification simples lorsque des informations d'identification solides sont requises... OU... Le client retourne un DN et un mot de passe pour une liaison simple lorsque l'entrée n'a pas de mot de passe défini.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
49	LDAP_INVALID_CREDENTIALS	Indique que l'une des situations suivantes s'est produite au cours d'une opération de liaison : le client a transmis un DN ou un mot de passe incorrect, ou le mot de passe est incorrect car il a expiré, la détection d'intrusion a verrouillé le compte ou une autre raison similaire. Consultez le code de données pour plus d'informations.
49 / 52e	AD_INVALID INFORMATIONS D'IDENTIFICATION	Indique une erreur Active Directory (AD) AcceptSecurityContext, qui est renvoyée lorsque le nom d'utilisateur est valide mais que la combinaison du mot de passe et des informations d'identification de l'utilisateur n'est pas valide. Il s'agit de l'équivalent AD du code d'erreur LDAP 49.
49 / 525	L'UTILISATEUR EST INTROUVABLE.	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est renvoyée lorsque le nom d'utilisateur n'est pas valide.
49 / 530	NOT_PERMITTED_TO_LOGON_AT_THIS_TIME	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec de connexion causé par le fait que l'utilisateur n'est pas autorisé à se connecter pour l'instant. Renvoie uniquement lorsqu'un nom d'utilisateur et des informations d'identification de mot de passe valides sont présentés.
49 / 531	RESTRICTED_TO_SPECIFIC_MACHINES	Indique une erreur de données Active Directory (AD) AcceptSecurityContext, c'est-à-dire un échec d'ouverture de session dû au fait que l'utilisateur n'est pas autorisé à se connecter à partir de cet ordinateur. Renvoie uniquement lorsqu'un nom d'utilisateur et des informations d'identification de mot de passe valides sont présentés.
49 / 532	PASSWORD_EXPIRED	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec de connexion. Le mot de passe de compte spécifié a expiré. Renvoie uniquement lorsqu'un nom d'utilisateur et un mot de passe valides lui sont présentés.
49 / 533	ACCOUNT_DISABLED	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec de connexion. Le compte est actuellement désactivé. Renvoie

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
		uniquement lorsqu'un nom d'utilisateur et un mot de passe valides lui sont présentés.
49 / 568	ERROR_TOO_MANY_CONTEXT_IDS	Indique que lors d'une tentative de connexion, le contexte de sécurité de l'utilisateur a accumulé trop d'ID de sécurité. Il s'agit d'un problème lié à l'objet/compte utilisateur LDAP spécifique qui doit être examiné par l'administrateur LDAP.
49 / 701	ACCOUNT_EXPIRED	Indique une erreur de données Active Directory (AD) AcceptSecurityContext qui est un échec de connexion. Le compte de l'utilisateur a expiré. Renvoie uniquement lorsqu'un nom d'utilisateur et un mot de passe valides lui sont présentés.
49 / 773	L'UTILISATEUR DOIT RÉINITIALISER LE MOT DE PASSE	Indique une erreur de données Active Directory (AD) AcceptSecurityContext. Le mot de passe de l'utilisateur doit être changé avant la première connexion. Renvoie uniquement lorsqu'un nom d'utilisateur et un mot de passe valides lui sont présentés.
50	LDAP_INSUFFICIENT_ACCESS	Indique que l'appelant ne dispose pas des droits suffisants pour effectuer l'opération demandée.
51	LDAP_BUSY	Indique que le serveur LDAP est trop occupé pour traiter la demande client pour l'instant, mais que si le client attend et soumet à nouveau la demande, le serveur peut être en mesure de la traiter à ce moment-là.
52	LDAP_UNAVAILABLE	Indique que le serveur LDAP ne peut pas traiter la demande de liaison du client, généralement parce qu'il est en cours d'arrêt.
52e	AD_INVALID INFORMATIONS D'IDENTIFICATION	Indique une erreur Active Directory (AD) AcceptSecurityContext, qui est renvoyée lorsque le nom d'utilisateur est valide mais que la combinaison du mot de passe et des informations d'identification de l'utilisateur n'est pas valide. Il s'agit de l'équivalent AD du code d'erreur LDAP 49 : LDAP_INVALID_CREDENTIALS.
53	LDAP_UNWILLING_TO_PERFORM	Indique que le serveur LDAP ne peut pas traiter la demande en raison de restrictions

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
		définies par le serveur. Cette erreur est renvoyée pour les raisons suivantes : La demande d'ajout d'entrée enfreint les règles de structure du serveur... OU... La demande de modification d'attribut spécifie les attributs que les utilisateurs ne peuvent pas modifier... OU... Des restrictions de mot de passe empêchent l'action... OU... Des restrictions de connexion empêchent l'action.
54	LDAP_LOOP_DETECT	Indique que le client a découvert un alias ou une boucle de référence et qu'il n'est donc pas en mesure de terminer cette demande.
55-63		Pas utilisé(e).
64	LDAP_NAMING_VIOLATION	Indique que l'opération d'ajout ou de modification DN enfreint les règles de structure du schéma. Par exemple, la requête place l'entrée subordonnée à un alias. La demande place l'entrée subordonnée à un conteneur interdit par les règles d'imbrication. Le RDN pour l'entrée utilise un type d'attribut interdit.
65	LDAP_OBJECT_CLASS_VIOLATION	Indique que l'opération Ajouter, modifier ou modifier DN enfreint les règles de classe d'objet pour l'entrée. Par exemple, les types de demandes suivants renvoient cette erreur : L'opération d'ajout ou de modification tente d'ajouter une entrée sans valeur pour un attribut requis. L'opération d'ajout ou de modification tente d'ajouter une entrée avec une valeur pour un attribut que la définition de classe ne contient pas. L'opération de modification tente de supprimer un attribut requis sans supprimer la classe auxiliaire qui définit l'attribut comme requis.
66	LDAP_NOT_ALLOWED_ON_NONLEAF	Indique que l'opération demandée n'est autorisée que sur les entrées terminales. Par exemple, les types de demandes suivants renvoient cette erreur : Le client demande une opération de suppression sur une entrée parente. Le client demande une opération de modification DN sur une entrée parente.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs LDAP standard (suite)

Code d'erreur/ de données	Texte	Description
67	LDAP_NOT_ALLOWED_ON_RDN	Indique que l'opération de modification a tenté de supprimer une valeur d'attribut qui forme le nom distinct relatif de l'entrée.
68	LDAP_ALREADY_EXISTS	Indique que l'opération d'ajout a tenté d'ajouter une entrée qui existe déjà, ou que l'opération de modification a tenté de renommer une entrée au nom d'une entrée qui existe déjà.
69	LDAP_NO_OBJECT_CLASS_MODS	Indique que l'opération de modification a tenté de modifier les règles de structure d'une classe d'objets.
70	LDAP_RESULTS_TOO_LARGE	Réservé au CLDAP.
71	LDAP_AFFECTS_MULTIPLE_DSAS	Indique que l'opération modifier DN déplace l'entrée d'un serveur LDAP vers un autre et nécessite plusieurs serveurs LDAP.
72-79		Pas utilisé(e).
80	LDAP_OTHER	Indique une condition d'erreur inconnue. Il s'agit de la valeur par défaut pour les codes d'erreur NDS qui ne sont pas mappés à d'autres codes d'erreur LDAP.
775	USER_ACCOUNT_LOCKED	Indique que les utilisateurs ne peuvent pas se connecter parce que le compte d'utilisateur est verrouillé.

Codes d'erreur personnalisés

Codes d'erreur LDAP personnalisés

Code d'erreur/de données	Texte
10 000	LDAP_ERROR_GENEREL
10001	LDAP_ERROR_MAL_FORMED_URL
10002	LDAP_ERROR_UNAUTHENTICATED_BIND
10300	LDAP_ERROR_COMMUNICATION_EXCEPTION
10301	LDAP_ERROR_SOCKET_TIMEOUT
10302	LDAP_ERROR_CONNECTION_REFUSED
10303	LDAP_ERROR_CONNECTION_RESET
10304	LDAP_ERROR_NO_ROUTE
10305	LDAP_ERROR_UNKNOW_HOST

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Codes d'erreur LDAP personnalisés (suite)

Code d'erreur/de données	Texte
10400	LDAP_ERROR_SSL_EXCEPTION
10401	LDAP_ERROR_SSL_EMPTY_CERT_STORE
10402	LDAP_ERROR_SSL_CERT_NOT_FOUND
10403	LDAP_ERROR_SSL_CERT_EXPIRED
10500	LDAP_ERROR_INVALID_SEARCH_FILTER_EXCEPTION

Envoyer un mot de passe à usage unique lorsque le serveur LDAP est en panne

Une propriété LDAP est disponible pour envoyer un mot de passe à usage unique à un utilisateur si l'utilisateur ne peut pas se connecter parce que le serveur LDAP est en panne. Vous pouvez également configurer une autre propriété pour contrôler la durée de validité du mot de passe.

Avant de commencer

Rôle requis : administrateur

Pour recevoir un mot de passe à usage unique, les notifications doivent être activées sur le profil d'utilisateur de l'utilisateur. La notification est un e-mail uniquement. Les messages SMS ne sont pas pris en charge.

Pourquoi et quand exécuter cette tâche

Les deux propriétés sont activées par défaut. La valeur par défaut de la propriété qui contrôle la validité du mot de passe est de 10 minutes.

Procédure

1. Ouvrez la liste des propriétés système en saisissant `sys_properties.list` dans le filtre du navigateur d'applications.
2. Trouvez la `glide.ldap.onetime.password.enabled` propriété.
3. Définissez la propriété sur `true`.
4. Pour modifier la durée de validité du mot de passe pour un utilisateur, définissez la propriété suivante sur un nombre entier de minutes : `glide.authenticate.onetime.password.validity`.

Synchronisation des enregistrements LDAP

Les administrateurs peuvent synchroniser les enregistrements LDAP inactifs, désactivés ou supprimés avec leurs enregistrements LDAP.

La synchronisation des enregistrements LDAP est le processus qui consiste à détecter les enregistrements inactifs sur le serveur LDAP et à mettre à jour les enregistrements LDAP correspondants. La détection des enregistrements LDAP inactifs implique de définir des indicateurs de données cohérents pour chaque objet utilisateur, d'importer des données LDAP et d'évaluer les indicateurs de données.

Un indicateur de données peut être :

- Champ de date
- Appartenance à une UO spécifique (identifier en analysant l'attribut*dn*), à l'aide de l'attribut `useraccountcontrol`
- Une combinaison de ces indicateurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les données importées arrivent dans l'instance par le biais de tables de jeu d'importation où les données peuvent être évaluées et traitées.

Le processus d'importation peut être utilisé Actualiser les filtres LDAPsur plusieurs tâches d'importation pour diviser différents types d'enregistrements utilisateur et séparer les enregistrements pour un traitement séparé.

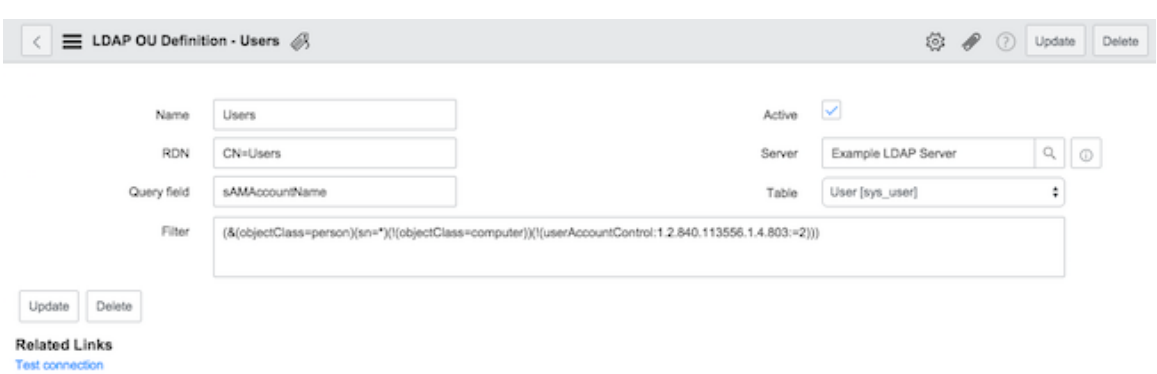
Actualiser les filtres LDAP

Les filtres du processus d'actualisation LDAP peuvent être utilisés pour spécifier un traitement qui ignore les insertions d'utilisateurs désactivés.

Vous pouvez desserrer le filtre LDAP OU pour importer toutes les données dans votre table de jeu d'importation (y compris les utilisateurs inactifs), puis spécifier un traitement qui ignore les insertions d'utilisateurs désactivés. L'exemple de définition d'unité organisationnelle « Utilisateurs » fourni par l'instance dans son exemple LDAP prêt à l'emploi contient un filtre.

Ce filtre est important car il définit les enregistrements utilisateur qui sont importés dans la table de jeu d'importation à évaluer. Bien qu'il réduise la charge de données, l'une des limites de ce filtre est qu'il filtre les utilisateurs inactifs, de sorte que les enregistrements d'utilisateurs inactifs ne sont pas importés dans les tables temporaires du jeu d'importation. Étant donné que les enregistrements utilisateur inactifs ne sont pas visibles, il n'est pas possible d'évaluer les indicateurs d'enregistrement.

Filtre LDAP OU



Pour utiliser le filtrage dans le processus d'actualisation LDAP principal, modifiez le filtre afin d'intégrer tous les enregistrements utilisateur. Le résultat est que tous les enregistrements seront chargés dans la table temporaire de jeu d'importation où ils pourront être évalués et transformés.

Remarque :
Il y a une précaution ici : comme le filtrage rassemble tous les enregistrements, vous pouvez vous retrouver avec un grand nombre d'anciens comptes LDAP inactifs qui ne doivent pas être insérés dans l'instance. Un enregistrement utilisateur ne doit jamais être créé pour un utilisateur désactivé.

Extraction LDAP

Un processus d'extraction LDAP peut être mis en œuvre pour détecter les utilisateurs désactivés.

Un extrait de votre source LDAP peut être filtré pour les utilisateurs désactivés à l'aide d'un marqueur actif qui peut être défini sur « faux » pour chaque enregistrement de l'importation. Spécifiez ('target.active=false') et copiez-la dans le champ **Script** directement sur l'enregistrement de carte de transformation de table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avantages

Les avantages de cette méthode sont les suivants :

- Écriture de scripts simple
- Les enregistrements d'utilisateurs existants ne sont pas impliqués dans le traitement
- Les utilisateurs inactifs ne sont pas chargés dans une table d'importation temporaire
- Aucun impact sur les performances

Inconvénients

Les inconvénients de cette méthode sont les suivants :

- Un processus supplémentaire est créé
- L'ensemble d'extraits doit être placé à un emplacement où votre source de données peut y accéder

Méthode alternative

Actualiser les filtres LDAP Utilisez plusieurs tâches d'importation pour diviser différents types d'enregistrements d'utilisateurs, en séparant les enregistrements pour un traitement séparé.

Comptes d'utilisateurs LDAP inactifs

Détectez qu'un compte d'utilisateur existant et actuel est inactif ou a été désactivé ou supprimé d'un LDAP Active Directory (AD).

Un problème courant lié à l'intégration LDAP est la façon de détecter les utilisateurs désactivés ou supprimés dans un Active Directory (AD), puis de les désactiver dans l'instance. Dans un LDAP Active Directory, un filtre est généralement défini pour exclure les utilisateurs inactifs lors de l'actualisation, afin que l'instance ne prenne pas en compte les utilisateurs désactivés ou supprimés dans AD. Le problème est de savoir comment détecter qu'un utilisateur actuel existant est inactif ou a été supprimé d'AD.

Pour plus d'informations sur la localisation des comptes inactifs, consultez Rechercher des comptes LDAP inactifs à l'aide du champ userAccountControl .

Remarque :
L'approche recommandée consiste à *désactiver* les enregistrements utilisateur et tous les autres types d'enregistrements, et non à les supprimer. Chaque enregistrement est lié à d'autres enregistrements. La suppression d'un enregistrement détruit toutes les relations avec ces autres enregistrements. La désactivation des enregistrements maintient ces relations en place.

Rechercher les comptes LDAP inactifs à l'aide du champ userAccountControl

Identifiez quand un utilisateur Active Directory (AD) est supprimé (ou rendu inactif).

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

L'une des méthodes consiste à suivre l'état actif des utilisateurs AD et à créer une règle métier pour mettre à jour les comptes correspondants lorsqu'un compte AD est inactif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Créez un champ de chaîne sur la table Utilisateur [sys_user] pour suivre la valeur du champ **userAccountControl** AD.
   Par exemple : `u_ad_user_account`.
2. Créez un script de transformation LDAP pour définir la valeur du champ.

   Example

   ```
   target.u_ad_user_account = source.userAccountControl
   ```

3. Mettez à jour le filtre LDAP pour afficher les comptes AD désactivés.

   Example
   Voici un exemple de filtre.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer))(!
   (userAccountControl:1.2.840.113556.1.4.803:=2)))
   ```

   Voici un exemple de filtre de remplacement que vous pouvez utiliser.

   ```
   (&(objectClass=person)(sn=*)(!(objectClass=computer)))
   ```

4. Créez une règle métier onChange pour attribuer la valeur false au champ Actif chaque fois que le champ u_ad_user_account contient la valeur 514.
   « 514 » indique un compte inactif.

Exemples de scripts LDAP

Les exemples de script suivants supposent que vous utilisez un Active Directory (AD) pour votre serveur LDAP.

Script de valeurs d'attributs userAccountControl

Cet exemple teste la source des valeurs de l'attribut userAccountControl associées à un utilisateur désactivé (514 ou 546).

```
//Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
if(source.u_useraccountcontrol == '514' || source.u_useraccountcontrol == '546'){
  target.active=false;
  target.locked_out=true;
}
```

Voici un exemple utilisant une vérification au niveau du bit :

```
if(source.u_useraccountcontrol & 2){
  active = false;
}
```

Script de l'attribut userAccountControl

Cet exemple examine l'attribut userAccountControl, mais ne teste pas de valeurs spécifiques. Il offre également la possibilité de réactiver les comptes utilisateur LDAP.

```
/*
* Deactivate LDAP-disabled users during transform based on 'userAccountControl' attribute
* Convert the userAccountControl attribute back to a hex value
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
*/
var ctrl = parseInt(source.u_useraccountcontrol, 10);
ctrl = ctrl.toString(16);

/*
* The only digit we care about is the final one
* A final hex digit value of '2' in 'ctrl' means disabled
*/
if(ctrl.substr(-1) == "2"){

  //Deactivate and lock the user account
  target.active = false;
  target.locked_out = true;

  //Ignore any insert of a disabled record
  if(action == 'insert'){
    ignore = true;
  }
}
/* Optional: Uncomment else block to reactivate and unlock the user account
else {
  target.active = true;
  target.locked_out = ctrl.substr(-2, 1) == "1";
}
*/
```

Script de carte de transformation onBefore

Voici un exemple de script de carte de transformation onBefore. Le script identifie les enregistrements désactivés et les enregistrements en cours d'insertion. Si une insertion d'un utilisateur désactivé se produit, l'opération de transformation ignore l'enregistrement.

```
//Ignore any insert of a disabled record as defined by the 'userAccountControl' attribute
var uc = source.u_useraccountcontrol;
if((uc == '514' || uc == '546') && action == 'insert'){
  ignore = true;
}
```

Script de membre DN

Cet exemple de script introduit de la flexibilité en ne s'appuyant pas sur les valeurs 546 et 514 userAccountControl, mais en vérifiant si l'utilisateur est membre d'un nom unique (ND) particulier. Vous pouvez utiliser ce script dans le champ **Script** de l'enregistrement « Carte de transformation de table » ou dans un script de carte de transformation onBefore.

```
//Deactivate LDAP-disabled users during transform based on OU membership in 'dn'
if(source.u_dn.indexOf('OU=Disabled Accounts') > -1){
  target.active = false;
  target.locked_out = true;
}
```

Mode d'application Active Directory (ADAM)

Active Directory Application Mode (ADAM) est un service d'annuaire conforme au protocole LDAP (Lightweight Directory Access Protocol).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Un niveau de compréhension de base avec Microsoft Windows Server et Active Directory est nécessaire pour comprendre cette rubrique. Vous devez également disposer des autorisations d'administrateur sur le serveur que vous configurez pour ADAM.

Il s'agit d'exemples de procédures. En raison des variations d'installation et d'environnement, nous ne pouvons pas offrir d'assistance directe. Nous vous recommandons de travailler avec un Microsoft consultant.

ADAM dispose d'une installation simple et s'exécute en tant que service sur Windows les systèmes d'exploitation. Il peut être entièrement personnalisé et distribué en tant que composant d'application ou utilisé en tant qu'annuaire LDAP autonome. ADAM utilise les mêmes technologies que celles que l'on trouve sur les contrôleurs de domaine Active Directory (y compris les fonctionnalités de réplication et de délégation) et dispose de ses propres fonctionnalités d'administration et de personnalisation. Il peut être exécuté en tant que Windows service. ADAM peut être installé sur Windows les systèmes d'exploitation XP, 2000, 2003 et 2008. ADAM est inclus dans Server Windows 2003 R2 et Windows Server 2008. Un téléchargement est disponible à http://www.microsoft.com/downloads http://www.microsoft.com/downloads pour les systèmes d'exploitation antérieurs.

Sécurité

Certaines politiques de sécurité d'entreprise interdisent aux fournisseurs et partenaires externes de se connecter directement à un contrôleur de domaine Active Directory (AD). S'il est interdit d'exposer certains objets ou attributs AD à un fournisseur ou un partenaire externe, l'accès aux objets et attributs peut être bloqué à l'aide des entrées de contrôle d'accès AD Security (ACE ou ACL). En fonction des exigences de sécurité, cette méthode peut introduire de la complexité dans l'intégration. Il est recommandé de consolider plusieurs domaines et forêts. Si toutes les importations et authentifications LDAP doivent être acheminées via une source unique, ADAM peut être utilisé comme source consolidée. Avec la sortie de Windows 2008, cette fonctionnalité a été renommée en Light-Weight-Directory Service, LDS. L'installation et la configuration sont similaires à celles de Windows Server 2003 R2.

Connaissances recommandées

Pour effectuer cette tâche, vous devez comprendre AD, les classes d'objets et les attributs. Pour réussir votre intégration, vous devez connaître la structure d'objet AD actuelle, connaître les délégations Active Directory et disposer d'une stratégie sur la façon d'utiliser ADAM et à quelles fins. Si vous n'êtes pas familier avec AD ou ADAM, contactez votre administrateur AD pour configurer un nouvel environnement ADAM.

Fiducies

Si *des objets userProxy* sont utilisés, l'ordinateur hébergeant ADAM doit être membre du domaine qui dispose des comptes AD ou membre d'un domaine de confiance.

Connectivité interne

Si des objets *userProxy* sont utilisés, l'ordinateur ADAM doit être en mesure de se connecter aux contrôleurs de domaine connexes pour effectuer une authentification proxy.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration d'une instance avec ADAM

La première installation copie les fichiers ADAM sur votre ordinateur, enregistre les composants requis et crée les raccourcis d'application.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Par défaut, tous les fichiers d'application sont installés dans %systemroot%\ADAM.

- Windows Server 2003 R2 - ADAM peut être installé à l'aide de la commande **Panneau de configuration > Ajout et suppression de programmes > gestionnaire de composants en option**.
- Windows Server 2000 et Windows XP - Téléchargé http://www.microsoft.com/downloads depuis Microsoft.

Créez le service de première instance qui fonctionne comme le premier service d'annuaire hébergé par ADAM. Effectuez l'une des actions suivantes :

Procédure

- Exécutez `adaminstall.exe` à partir du dossier ADAM.
- Utiliser le raccourci **Créer une instance ADAM** à partir du **Menu Démarrer > programmes > ADAM** dossier.

1. Sélectionnez l'option **Installation d'une instance unique** .

> **Remarque :**
> Vous pouvez utiliser cette option pour installer un réplica d'instance sur un deuxième serveur afin de fournir un système tolérant aux pannes.

2. Renseignez les champs.

ADAM Instance

Champ	Description
Nom d'instance	utilisé principalement pour identifier le nom et le nom d'affichage du Windows service
Ports	définit les numéros de port à utiliser pour les écouteurs LDAP et LDAPS. Le port LDAP par défaut est 389, LDAPS est 636. Si ces ports sont utilisés sur le serveur, l'assistant d'installation sélectionne de nouveaux ports. Collaborez avec votre administrateur réseau pour déterminer les meilleurs ports à utiliser
Partition de répertoire d'application	Crée une partition de répertoire d'application. Non nécessaire à cette étape. Nous vous recommandons de créer la nouvelle partition maintenant. Une bonne pratique consiste à utiliser le même nom unique que votre forêt ou votre domaine, mais à remplacer le domaine de plus haut niveau par adam au lieu de com ou local. Par exemple, si votre partition de forêt est `dc=myCompany,dc=com`, vous pouvez créer la partition ADAM en tant que `dc=myCompany,dc=adam`
Emplacements de fichiers	sélectionne le ou les emplacements pour les données de partition ADAM.
Sélection du compte de service	Sélectionne un compte de service sous lequel l'instance est exécutée. Pour les services autonomes, vous pouvez utiliser le compte de service réseau par défaut. Si vous

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	prévoyez d'utiliser des réplicas, vous devez utiliser un compte qui a accès à toutes les instances ADAM.
Administrateurs ADAM	la délégation sur l'annuaire ADAM qui exploite l'authentification intégrée de Windows. C'est ainsi que l'accès initial est accordé pour l'administration. Une fois les droits accordés au compte initial, cet utilisateur ou groupe délègue les droits à d'autres utilisateurs Windows ou utilisateurs ADAM. Vous pouvez sélectionner la valeur par défaut pour accorder uniquement l'accès administrateur à l'utilisateur actuel ou accorder l'accès à un autre utilisateur ou groupe en fonction de vos besoins.
Importer des fichiers LDIF	fichiers à importer. MS-UserProxy est le fichier le plus important à importer, mais il vaut la peine d'ajouter tous les fichiers disponibles car il y a peu de surcharge dans le schéma et vous n'aurez pas à vous soucier de l'étendre plus tard si vos besoins augmentent. Confirmez les détails et l'assistant termine la configuration.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Configurer la console ADAM

Configurez la console ADAM. Même s'il existe de nombreuses similitudes entre ADAM et Active Directory, l'administration peut être très différente puisqu'il n'y a pas de console de gestion **Utilisateurs et Ordinateurs** .

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La majeure partie de l'administration générale est effectuée à l'aide de la console ADAM ADSI MMC disponible dans le menu Démarrer **d'ADAM** . La première fois que vous exécutez la console ADAM ADSI, vous devez vous connecter à la partition que vous avez créée.

Procédure

1. Cliquez avec le bouton droit de la souris sur l'élément **ADAM ADSI Edit** dans le cadre de gauche.
2. Donnez un nom à la nouvelle connexion et mettez à jour le nom du serveur et les champs de port avec les informations utilisées lors de la création de l'instance.
3. Sélectionnez un **nom ou** un **contexte de dénomination** unique et spécifiez le nom unique de la partition d'application que vous avez créée précédemment.
   Vous pouvez vous connecter aux partitions `Configuration et Schema` pour obtenir des options de configuration avancées.
   Vous devriez maintenant être en mesure de voir à l'intérieur de la partition et des conteneurs par défaut pour LostAndFound, les quotas NTDS et les rôles. Le conteneur Rôles n'a pas encore été configuré.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Créer des conteneurs et des unités organisationnelles pour ADAM

Regroupez logiquement les objets stockés dans ADAM en conteneurs et unités organisationnelles (OU) comme ils le seraient dans Active Directory.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Cliquez avec le bouton droit sur la partition racine et accédez à **Nouveau** > **Objet** > **Unité organisationnelle**.

   Remarque :
   Vous pouvez également consulter la liste des autres objets disponibles. Cette liste varie en fonction des extensions de schéma installées lors de l'importation des fichiers LDF.

2. Lorsque vous êtes invité à entrer une valeur, entrez le nom de l'UO, par exemple `Utilisateurs`.
   L'écran affiche un bouton **Plus d'attributs** .
3. Utilisez le bouton pour attribuer des valeurs à des attributs supplémentaires.
   Pour les unités organisationnelles et les conteneurs, aucune valeur supplémentaire n'est nécessaire.
   Après la création des unités organisationnelles, les nouvelles unités organisationnelles sont répertoriées comme enfants de l'objet racine.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Délégation avec ADAM

Une fois la structure OU créée, définissez les délégations d'autorisations pour sécuriser correctement les objets pour les utilisateurs limités.

Comme pour Active Directory, il existe deux façons générales d'accorder des autorisations :

- Ajoutez des utilisateurs à un groupe auquel les autorisations appropriées sont déjà affectées.
- Définissez de nouvelles autorisations sur les objets ADAM.

Pour cette tâche, nous abordons les autorisations au niveau de l'objet. Reportez-vous à la section Administration des groupes pour plus d'informations sur les appartenances aux groupes.

Étant donné que nous n'avons pas de console Utilisateurs et ordinateurs pour ADAM, toutes les autorisations au niveau de l'objet sont définies à l'aide de `l'utilitaire` Active Directory DSACLS.exe. Ce fichier se trouve dans le répertoire du programme ADAM. Lors de l'exécution d'utilitaires ADAM, il est préférable de lancer l'invite de commande des outils ADAM. Cela permet de s'assurer que les versions des outils sont correctes. DSALCS permet d'afficher et de définir des droits d'accès aux objets.

Exemple : « `dsacls \\localhost :50010\dc=myCompany,dc=adam` » affiche les permissions affectées à la racine de la partition *`dc=myCompany,dc=adam`* en cours d'exécution sur le localhost, le port 50010. DSACLS est un outil complexe utilisé pour créer une délégation complexe. Exécutez *`« DSACLS / ? » pour les`* notes d'utilisation.

Information associée

Créer des conteneurs et des unités organisationnelles pour ADAM

Utiliser ADAMSync pour renseigner ADAM

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remplissage des objets ADAM

Les objets ADAM comprennent les objets utilisateur, l'objet UserProxy et les objets de groupe.

Objets utilisateur

Les utilisateurs peuvent être créés à l'aide de la console ADAM ADSI Edit comme nous l'avons fait pour la création d'OU. Les utilisateurs peuvent également être administrés à l'aide des outils de ligne de commande AD, ce qui dépasse le cadre de ce document. Le seul attribut obligatoire pour les nouveaux objets utilisateur est le *cn*, qui est un nom court ou le nom complet de l'utilisateur. Il existe également un large éventail d'attributs facultatifs similaires aux attributs d'utilisateur Active Directory. Vous pouvez accéder à la liste complète des attributs en sélectionnant des propriétés dans l'objet utilisateur.

Objets UserProxy

Pour ServiceNow l'intégration LDAP, nous vous recommandons d'utiliser des objets *UserProxy* dans ADAM qui créent un compte proxy lié au compte d'utilisateur AD associé. ADAM peut ainsi authentifier les informations d'identification de connexion à l'aide des noms d'utilisateur et mots de passe AD du domaine sans ServiceNow se connecter directement au contrôleur de domaine. *Les objets UserProxy* sont très similaires aux objets AD et ADAM User, sauf qu'ils ne stockent pas les mots de passe et qu'ils ont un attribut *objectSID* qui contient le SID de l'objet AD User lié. Voici comment fonctionne le proxy. *Les objets UserProxy* sont créés à l'aide de la console *ADSIEdit* ou des outils en ligne de commande, mais cela peut être fastidieux. Il est recommandé d'utiliser un processus automatisé tel que défini ci-dessous.

Objets de groupe

Les groupes sont créés à l'aide de la console ADSIEdit et des outils de ligne de commande AD. Les concepts des groupes sont similaires à ceux d'AD et sont utilisés pour intégrer des groupes et des membres à ServiceNow. La plus grande différence réside dans le fait que les groupes ADAM peuvent contenir des membres provenant d'ADAM ou de domaines AD de confiance.

Automatisation de la création d'objets ADAM

Si vous souhaitez synchroniser des comptes Active Directory avec ADAM, nous vous recommandons d'utiliser Microsoft *ADAMSync* outil. Il s'agit de l'utilisation la plus courante d'ADAM pour ServiceNow l'intégration LDAP.

À propos de la délégation des autorisations

ADAM contient des groupes intégrés avec des autorisations par défaut. Ces groupes se trouvent dans le conteneur *cn=roles,dc=myCompany,dc=adam*. Ceux-ci sont similaires aux groupes de niveau de domaine et ont des droits sur les objets dans la partition courante. À l'instar d'AD Forests, vous pouvez également définir un niveau d'autorisation supérieur à l'aide des groupes par défaut dans *cn=roles,cn=configuration,dc=myCompany,dc=adam*. Vous devez vous connecter à la partition de configuration dans *ADSIEdit*. Le groupe Administrateurs inclut par défaut le compte spécifié lors de la configuration. Ce membre n'est pas toujours visible, car il est hérité par le biais des groupes de configuration. Les administrateurs ont le contrôle total de tous les objets de partition. Le groupe Lecteurs ne contient aucun membre par défaut et dispose d'un accès en lecture à tous les objets de la partition. Le groupe Utilisateurs est un groupe dynamique, tout comme dans Active Directory. D'un point de vue transitif, il inclut tous les utilisateurs ADAM créés dans la partition.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Test et dépannage de la configuration d'ADAM

L'outil principal utilisé pour les tests est LDP. Cela vous permet de tester entièrement l'authentification utilisateur.

La majeure partie de la gestion des objets peut être effectuée à l'aide de la console ADAM ADSI Edit qui permettra d'accéder à l'ensemble de la collection d'objets et d'attributs. Le plus haut niveau de contrôle et de dépannage des services ADAM consiste à utiliser le Windows service créé lors de la configuration de l'instance. Le nom du service varie et dépend du nom de l'instance créée. Ce service doit être en cours d'exécution pour que le service ADAM s'exécute. Si vous rencontrez des problèmes de connexion, vous devez examiner les configurations réseau pour vous assurer que vous disposez de l'accès réseau approprié pour vous connecter au serveur et au port ADAM. Pour chaque instance ADAM installée, un journal des événements Windows est créé. Il s'agit également d'un excellent outil pour dépanner les services ADAM.

Le Windows journal des événements de sécurité est également utile lors du dépannage des authentifications `userProxy` . Toutes les tentatives d'ouverture de session `userProxy` sont enregistrées dans le journal de sécurité et font référence à l'adresse de l'appareil client distant, au nom unique de l'utilisateur qui tente de se connecter et au code de résultat ou d'état.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Sauvegarde et restauration avec ADAM

Toutes les données ADAM peuvent être sauvegardées à l'aide de méthodes de sauvegarde de système de fichiers standard.

Redondance

ADAM dispose d'utilitaires de réplication intégrés basés sur la même technologie qu'AD. Un réplica complet en lecture et en écriture d'une partition ADAM peut exister sur le même ordinateur ou sur un ordinateur différent. Vous pouvez utiliser ce réplica de différentes façons pour fournir une intégration LDAP tolérante aux pannes avec l'instance. Une option consiste à exposer les deux partitions à l'instance via le pare-feu et à définir les deux serveurs dans le champ serveur des propriétés LDAP.

Information associée

Mode d'application Active Directory (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Utiliser LDAPS avec ADAM

La configuration par défaut de l'authentification d'objet `userProxy` consiste à appliquer des communications LDAPS (LDAP sécurisées). LDAPS exige des certificats SSL pour sécuriser le trafic réseau.

Pour supprimer cette condition, effectuez la modification suivante à l'aide de la console `ADSIEdit` connectée à la partition de configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
Object: CN=Directory Service, CN=Windows NT, CN=Services, CN=Configuration
Attribute: msDS-Other-Setings
Value: change RequiresSecureProxyBind from 1 (enforced) to 0 (disabled)
```

Redémarrez le service ADAM pour utiliser le nouveau paramètre.

Pour prendre en charge les liaisons sécurisées et chiffrer les informations d'utilisateur et de mot de passe transmises, un certificat SSL doit être installé sur le serveur et tout client LDAP. Étant donné que les utilisations du service ADAM sont limitées et contrôlées, il est possible d'utiliser un certificat auto-signé qui répondrait aux besoins sans encourir de coûts de certificat ni construire d'infrastructure d'autorité de certification (CA). Si vous disposez déjà d'une autorité de certification, vous pouvez émettre un certificat. Sinon, créez un certificat auto-signé.

Création d'un certificat autosigné

Pour utiliser l'utilitaire `selfssl` , Internet Information Services (IIS) doit être installé. Ce service peut être supprimé une fois que vous avez généré le certificat. Vous pouvez obtenir l'utilitaire selfssl.exe à partir du kit de ressources IIS. Si IIS est déjà installé, créez un nouveau site web afin que les sites existants ne soient pas impactés lors de la génération de certificats. Selfssl doit joindre temporairement le nouveau certificat auto-émis à un site web valide.

Selfssl est un outil en ligne de commande et possède les paramètres communs suivants.

Descriptions des paramètres Selfssl

Paramètre	Description
/T	Ajoute le certificat aux « Certificats approuvés » sur l'ordinateur local
/N :cn	Définissez le nom commun du certificat. Celui-ci doit correspondre au nom de domaine complet du serveur exécutant le service Web utilisant le certificat
/K	Définit la force de la taille de clé en bits
/V	Nombre de jours de validité du certificat
/S	ID du site Web auquel joindre le certificat
/P	Port IP du service Web

L'attribut de nom commun doit correspondre au nom ou à l'adresse externe que l'instance utilisera pour se connecter à votre ordinateur ADAM. Vous aurez besoin d'obtenir l'ID du site du site Web IIS, sauf si vous utilisez le site Web par défaut qui est 1 et n'a pas besoin d'être défini dans la commande selfssl. Voici un exemple de commande permettant de générer un certificat pour myCompany :

```
selfssl /N:CN=myCompany.externaldomain.com /K:1024 /V:3650 /S:12345 /P:50001 /T
```

Cette déclaration crée un certificat qui est valide pendant 10 ans. Définissez la valeur sur n'importe quelle durée, mais n'oubliez pas que le nouveau certificat doit être généré et soumis à l'instance avant l'expiration de l'ancien. Nous vous recommandons de noter la date d'expiration sur le certificat.

Une fois le certificat généré, vous pouvez le supprimer du site Web ou supprimer l'ensemble du site Web si vous avez créé un site temporaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Affecter le certificat à ADAM

Installez un certificat SSL sur le serveur et tout client LDAP pour prendre en charge les liaisons sécurisées et chiffrer les informations d'utilisateur et de mot de passe transmises.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Étant donné que les utilisations du service ADAM sont limitées et contrôlées, il est possible d'utiliser un certificat auto-signé pour répondre à vos besoins sans encourir de coûts de certificat ni construire d'infrastructure d'autorité de certification (CA).

Procédure

1. Ouvrez la console MMC Certificats et créez deux connexions de console, l'une pour les certificats d'ordinateurs locaux et l'autre pour les certificats de services informatiques locaux sur le nouveau service ADAM.
   Le nouveau certificat se trouve sous Certificats (ordinateur local)\Personnel\Certificats.
2. Copiez le certificat dans le conteneur du service ADAM Certificats – Service (Nom de service ADAM)\ADAM_ADAM Nom de service\Certificats racine approuvés\Certificats et copiez le certificat dans Certificats – Service (Nom de service ADAM)\ADAM_ADAM Nom de service \Personnel\Certificats.
3. Ouvrez l'onglet Détails sur le certificat que vous avez copié, notez l'horodatage de début de validité et affectez un accès en lecture au fichier de clé de certificat.
   Accédez à C :\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA \MachineKeys et identifiez le certificat avec l'horodatage correspondant. Affectez des droits de lecture et d'exécution au compte de service exécutant ADAM. Par défaut, il s'agit **du service réseau**.
4. Redémarrez le service ADAM pour activer le nouveau certificat.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Exporter le certificat de clé publique

Les clients LDAPS, y compris l'instance, ont besoin du certificat de clé publique afin d'établir une connexion sécurisée à ADAM.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
À partir des consoles de certificat de serveur que vous avez utilisées ci-dessus, exportez une clé publique à utiliser par les clients.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Sélectionnez le certificat, cliquez avec le bouton droit de la souris, puis sélectionnez **toutes les tâches/exportation**.
   N'exportez pas la clé privée. Sélectionnez le format X.509 binaire codé DER par défaut et spécifiez le nom du fichier d'exportation.
2. Installez le certificat public sur les clients LDAP qui se connectent au serveur à l'aide de LDAPS.
   Lorsque vous y êtes invité, ajoutez le certificat au magasin des `autorités de certification racine approuvées` .

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Compte d'accès en mode d'application Active Directory (ADAM)

Le système requiert qu'un compte utilisateur lise les informations d'objet du mode d'application Active Directory (ADAM) importées dans l'instance d'application.

Créez le compte à l'aide de l'une des méthodes suivantes :

- Créez un compte utilisateur ADAM local, affectez-lui un mot de passe et affectez-lui des autorisations.
- Affecter une autorisation à un Windows compte de domaine sur la partition ADAM.
- Utilisez un compte `userProxy` .

Lors de l'utilisation d'ADAM en tant que source LDAP, vous devez spécifier le nom unique complet (FQDN) du compte ADAM dans le champ **Nom distinctif de connexion** du serveur LDAP de l'instance.

Information associée

Mode d'application Active Directory (ADAM)

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Tester les connexions LDAPS

Testez les connexions LDAPS. Il existe deux connexions à la console, l'une pour les certificats d'ordinateurs locaux et l'autre pour les certificats de services informatiques locaux sur le nouveau service ADAM.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Exécutez `LDP.exe` à partir du dossier d'installation ADAM c :\windows\adam.
   Vérifiez que la version ADAM est sélectionnée, car il ne s'agit pas du client LDP standard Windows .
2. Ouvrez une nouvelle connexion à l'aide du menu **Connexion/Connexion** .
   Le nom du serveur doit correspondre au CN affecté au certificat.
3. Saisissez le **port LDAPS** et cochez la case **SSL** .
   Les résultats d'une connexion réussie sont des informations générales sur le serveur et aucune erreur.
4. Lier (se connecter) au service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour répliquer des connexions client LDAP classiques, sélectionnez l'option Liaison simple. Dans le champ utilisateur, saisissez un nom unique d'utilisateur ADAM ou `de userProxy` valide ainsi que le mot de passe associé.
Si vous voyez un message de retour indiquant « Authentifié en tant que... » alors vous vous êtes connecté avec succès à l'aide de LDAPS.

Information associée

http://www.microsoft.com/downloads/en/details.aspx?familyid=9688f8b9-1034-4ef6-a3e5-2a2a57b5c8e4&displaylang=en%7C

Utiliser ADAMSync pour renseigner ADAM

Les administrateurs utilisent MS ADAMSync pour remplir les répertoires LDAP qui utilisent MS ADAM.

Remarque :

Ce document suppose que vous avez au moins un niveau de compréhension de base avec Microsoft Windows Server, Active Directory et ADAM et que vous disposez déjà d'une instance fonctionnelle Mode d'application Active Directory (ADAM) avec une partition.

Il s'agit d'exemples de procédures. En raison de la complexité et du fait qu'il s'exécute dans votre environnement, nous ne pouvons pas offrir d'assistance directe. Nous vous recommandons de travailler avec un consultant si Microsoft vous rencontrez des Microsoft problèmes.

Une fois qu'ADAM a été installé et que la première partition a été créée, vous pouvez la remplir avec des objets.

Les options suivantes sont disponibles :

- Création manuelle d'objets à l'aide d'une interface graphique ou de scripts. Cette option est inefficace et lente.
- Intégrez Active Directory à l'aide du serveur d'informations d'intégration Microsoft . En fin de compte, cette option offre le plus de flexibilité et de fonctionnalités, mais nécessite certaines configurations avancées. Il existe une version gratuite de MIIS compatible avec Active Directory, ADAM etMicrosoft les listes d'adresses globales d'Exchange. À moins que vous n'ayez déjà de l'expérience avec MIIS, nous vous conseillons de ne pas essayer d'implémenter un nouvel environnement pour l'intégration LDAP uniquement.
- Utilisez ADAMSync, un outil de synchronisation fourni Microsoft avec ADAM. C'est l'option qui est expliquée ici.

Définir les comptes utilisateur ADAM

Définissez des comptes d'utilisateurs dans ADAM. Un compte d'utilisateur est utilisé pour l'instance à laquelle se connecter et l'autre compte d'utilisateur est pour ADAMSync.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Ces comptes peuvent être des objets utilisateur ADAM locaux, des objets UserProxy ou un compte Windows d'un domaine de confiance.

Le `ADAM User` compte nécessite un accès en lecture seule à la structure de répertoires que vous importez dans votre instance. La meilleure façon d'y parvenir est d'ajouter le compte à l'attribut membre dans le groupe Lecteurs qui se trouve dans cn=roles,dc=myCompany,dc=adam.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les nouveaux comptes utilisateur ADAM sont désactivés par défaut. Vous devrez activer les nouveaux comptes et définir un mot de passe.

Procédure

1. Activez les utilisateurs en remplaçant l'attribut msDS-UserAccountDisabled par FALSE.
2. Cliquez avec le bouton droit de la souris sur l'objet utilisateur et réinitialisez le mot de passe.
3. Testez les nouveaux comptes à l'aide de LDP comme défini dans Mode d'application Active Directory (ADAM) pour vous assurer qu'ils peuvent se connecter.
   Utiliser le **LDAP** > **Vue/arborescence** , en laissant le DN de base vide pour vous assurer que vous pouvez afficher les objets dans le répertoire à l'aide des nouveaux comptes. La configuration, le schéma et la partition de domaine doivent être visibles dans le volet gauche. Traversez la partition de domaine. Si vous utilisez un nouveau compte ADAM local, il affichera « Aucun enfant », ce qui signifie que vous n'avez pas d'accès en lecture aux objets. Vérifiez les appartenances aux groupes de configuration et relancez le test.

   ADAMSync utilise le compte pour gérer les *`ADAMSync User`* objets de la partition ADAM. Ce compte nécessite des droits de niveau administrateur car il créera, mettra à jour et supprimera les objets ADAM.

   ADAMSync utilise le *`ADAMSync AD`* compte pour lire les objets AD qui seront synchronisés avec ADAM.

Configurer ADAMSync

ADAMSync est inclus dans Windows Server 2003 R2. Téléchargez et installez ADAMSync si vous utilisez un autre système d'exploitation.

Extension du schéma

Le schéma ADAM doit être étendu pour prendre en charge ADAMSync.

1. Exécutez la commande suivante à partir de c :\windows\adam pour importer les extensions de schéma ADAMSync. Vous devrez peut-être modifier le server :port et ajouter des informations d'identification si l'utilisateur actuel n'y a pas accès. Pour plus d'informations, consultez le fichier AdamSyncMetadata.ldf.

   ```
   ldifde -i -f MS-AdamSyncMetadata.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
    #configurationNamingContext
   ```

2. Faites de même avec MS-AdamSchemaW2k3.ldf pour prendre en charge les attributs Windows 2003.

   ```
   ldifde -i -u -f MS-AdamSchemaW2K3.LDF -s localhost:50000 -j . -c "cn=Configuration,dc=X"
    #configurationNamingContext
   ```

Changements de schéma recommandés

Voici quelques changements de schéma supplémentaires que nous recommandons.

1. Ouvrez une nouvelle console MMC et ajoutez le composant logiciel enfichable Schéma ADAM.
2. Connectez-vous à l'instance ADAM.
3. Développez le dossier Classes et localisez la classe userProxy, ouvrez **Propriétés**.
4. Vérifiez les attributs facultatifs suivants dans l'onglet Attributs et ajoutez-en qui n'existent pas déjà.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- company
- département
- givenNane
- Courrier
- physicalDeliveryOfficeName
- sAMAccountName
- Sn
- numéro de téléphone
- Titre
- userAccountControl
- userPrincipalName

5. Redémarrez le service ADAM pour activer les nouveaux paramètres.

Installer le fichier de configuration ADAM

Installez le fichier de configuration ADAM via la ligne de commande Windows.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Installez le fichier de configuration.

```
C:\WINDOWS\adam>adamsync /install localhost:50000 MS-AdamSyncConf-SNC.XML
```

2. Exécutez le fichier de synchronisation pour vous connecter à la console.

```
C:\WINDOWS\adam>adamsync /sync localhost:50000
"ou=users,dc=service-now,dc=adam" /log -
```

3. Révisez les résultats à l'aide de la console ADSIEdit.
   Vous devriez voir les nouveaux objets et attributs qui ont été créés par ADAMSync.
4. Exécutez ldap pour tester l'authentification UserProxy.
   Automatisation du processus de synchronisation

   Configurez le processus de synchronisation comme une Windows tâche planifiée. Vous devez soit fournir les informations d'identification dans le fichier de configuration, soit la ligne de commande, soit exécuter la tâche planifiée avec un compte disposant d'un accès.

   Remarques spéciales

   - Vous pouvez créer plusieurs fichiers de configuration et travaux planifiés pour synchroniser ADAM à partir de plusieurs sources.

     Cet exemple importe l'attribut sAMAccountName qui peut être utilisé comme ouverture de session de l'application. Si vous synchronisez la source, vous devez vous assurer que vous disposez d'une valeur d'attribut unique pouvant être utilisée pour les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

informations d'identification de connexion. sAMAccountName est garanti comme unique au sein d'un domaine, mais pas sur plusieurs domaines.

- Si vous utilisez Microsoft Exchange, nous vous recommandons d'exclure les objets cn=SystemMailbox* dans le cadre de la configuration objet-filtre.

Exemples de fichiers de configuration ADAM

Toutes les configurations d'ADAMSync sont stockées dans des fichiers XML.

Fichier de configuration par défaut avec commentaires

Un fichier de configuration par défaut appelé MS-AdamSyncConf.xml est inclus avec l'installation d'ADAMSync. Faites une copie de ce fichier afin d'avoir un exemple de base auquel vous référer à l'avenir. Cet exemple est le fichier de configuration par défaut auquel des commentaires ont été ajoutés.

```
<?xml version="1.0"?>
<doc>
 <configuration>
<!-- Sync File Description -->
<description>MyCompany ADAMSync Configuration</description>
  <security-mode>object</security-mode>;
<!-- source-ad-name = fqdn of the domain controller -->;
  <source-ad-name>;fully.qualified.domain.name.of.domain.controller</source-ad-name>;
<!-- source-ad-partition = root AD domain partition -->;
  <source-ad-partition>;dc=myCompany,dc=com</source-ad-partition>;
<!-- source-ad-account = use this to specify an account to connect to AD -->;
<!-- if not used, the current user will be used  -->;
  <source-ad-account>;</source-ad-account>;
  <account-domain>;</account-domain>;
<!-- target-dn = target ADAM OU -->;
  <target-dn>;ou=servicenow users,dc=myCompany,dc=adam</target-dn>;
  <query>;
<!-- base-dn = should be the root AD partition if you want all users -->;
   <base-dn>;dc=myCompany,dc=com</base-dn>;
<!-- object-filter = standard ldap query format, this will grab all users -->;
<!-- need to review results to see if you should modify this filter -->;
   <object-filter>;(objectCategory=person)</object-filter>;
   <attributes>;
<!-- include=userproxy requires objectSID to link back to the AD account -->;
    <include>;objectSID</include>;
    <include>;givenName</include>;
    <include>;sn</include>;
    <include>;description</include>;
    <include>;title</include>;
    <include>;company</include>;
    <include>;department</include>;
    <include>;mail</include>;
    <include>;physicalDeliveryOfficeName</include>;
    <include>;telephoneNumber</include>;
    <include>;sAMAccountName</include>;
   </attributes>;
  </query>;
<!-- map for user-to-userproxy object types -->;
  <user-proxy>;
    <source-object-class>;user</source-object-class>;
    <target-object-class>;userProxy</target-object-class>;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 </user-proxy>;
 <schedule>;
  <aging>;
   <frequency>;0</frequency>;
   <num-objects>;0</num-objects>;
  </aging>;
  <schtasks-cmd>;</schtasks-cmd>;
 </schedule>;
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```

Filtre LDAP Fichier de configuration

Vous pouvez fournir n'importe quel niveau de filtrage dans la valeur object-filter du fichier de configuration. Utilisez la syntaxe de requête LDAP standard avec les caractères d'échappement XML suivants à la place des opérateurs standard.

- ET = « & » remplacer par &
- OR = « | » (ligne verticale) remplacer par |
- NOT = « ! » remplacer par !

Fichier de configuration de référence

Voici un fichier de configuration réel qui peut être référencé à titre d'exemple.

```
<?xml version="1.0"?>;
<doc>;
 <configuration>;
<description>;SNCTest ADAMSync Configuration</description>;
 <security-mode>;object</security-mode>;
 <source-ad-name>;domaincontroller.service-now.com</source-ad-name>;
 <source-ad-partition>;dc=service-now,dc=com</source-ad-partition>;
 <source-ad-account>;</source-ad-account>;
 <account-domain>;</account-domain>;
 <target-dn>;ou=servicenow users,dc=service-now,dc=adam</target-dn>;
 <query>;
  <base-dn>;dc=service-now,dc=com</base-dn>;
  <object-filter>;(objectCategory=person)</object-filter>;
  <attributes>;
   <include>;objectSID</include>;
   <include>;givenName</include>;
   <include>;sn</include>;
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
  <include>;description</include>;
  <include>;title</include>;
  <include>;company</include>;
  <include>;department</include>;
  <include>;mail</include>;
  <include>;physicalDeliveryOfficeName</include>;
  <include>;telephoneNumber</include>;
  <include>;userAccountControl</include>;
 </attributes>;
</query>;
<user-proxy>;
 <source-object-class>;user</source-object-class>;
 <target-object-class>;userProxy</target-object-class>;
</user-proxy>;
<schedule>;
 <aging>;
  <frequency>;0</frequency>;
  <num-objects>;0</num-objects>;
 </aging>;
 <schtasks-cmd>;</schtasks-cmd>;
</schedule>;
</configuration>;
<synchronizer-state>;
 <dirsync-cookie>;</dirsync-cookie>;
 <status>;</status>;
 <authoritative-adam-instance>;</authoritative-adam-instance>;
 <configuration-file-guid>;</configuration-file-guid>;
 <last-sync-attempt-time>;</last-sync-attempt-time>;
 <last-sync-success-time>;</last-sync-success-time>;
 <last-sync-error-time>;</last-sync-error-time>;
 <last-sync-error-string>;</last-sync-error-string>;
 <consecutive-sync-failures>;</consecutive-sync-failures>;
 <user-credentials>;</user-credentials>;
 <runs-since-last-object-update>;</runs-since-last-object-update>;
 <runs-since-last-full-sync>;</runs-since-last-full-sync>;
</synchronizer-state>;
</doc>;
```

Configurer Microsoft Active Directory pour une communication LDAPS sécurisée

Utilisez des paires de certificats pour activer les communications LDAPS Microsoft Active Directory (AD).

Remarque :
Ces procédures ont été conçues et testées à l'aide de Windows 2003 R2 Standard Edition et fonctionnent avec toutes les versions de Windows 2003.

La communication LDAP sécurisée (LDAPS) est similaire à la communication SSL (HTTPS) en ce sens que les deux chiffrent les données entre les serveurs et les clients. Pour ce faire, le serveur et les clients partagent des informations communes à l'aide de paires de certificats. Le serveur détient le certificat de clé privée et les clients détiennent le certificat de clé publique. Ces certificats sont requis pour activer les communications LDAPS Microsoft Active Directory (AD).

Pour configurer LDAPS pour Active Directory, vous devez :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Assurez-vous que le domaine Active Directory est configuré et que l'instance peut se connecter au serveur Active Directory via le pare-feu.
- Vérifiez qu'une autorité de certification (CA) peut émettre un certificat pour le contrôleur de domaine (contrôleur de domaine). Si vous ne disposez pas encore d'une infrastructure CA, deux options s'offrent à vous.
  - Configurer une autorité de certification autonome pour émettre le certificat
  - Demander un certificat tiers
- Si vous disposez déjà d'une autorité de certification, vous pouvez générer un certificat à partir d'une autorité de certification interne.

Tous les certificats ont une date d'expiration définie qui peut être consultée dans les propriétés du certificat. Si le certificat expire, tout le trafic LDAPS échoue et vos utilisateurs ne peuvent plus se connecter à l'instance. Pour résoudre ce problème, un nouveau certificat doit être émis et installé sur votre instance.

L'expiration par défaut des certificats Microsoft CA est d'un an. Les certificats CA externes sont généralement achetés par incréments d'un an. Notez la date d'expiration de votre certificat ou utilisez la fonction de notification d'expiration de l'application (située dans **Système LDAP** > **Certificats**). Assurez-vous d'avoir un nouveau certificat prêt avant l'expiration de l'ancien. Cela vous donne le temps d'installer et de tester le nouveau certificat avant l'expiration de l'ancien.

Configurer une autorité de certification autonome pour Active Directory

La première étape pour configurer Microsoft Active Directory pour l'accès SSL consiste à configurer une autorité de certification (CA) autonome.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Ne vous inquiétez pas de l'utilisation supplémentaire des ressources, car les deux services requis (IIS et CA) peuvent être désactivés après l'émission du ou des certificats.

Procédure

1. Installez Internet Information Server (IIS).
2. Installez les services de l'autorité de certification en mode autonome.
3. Vérifiez que l'application Web Services de certificats est installée et active.

Que faire ensuite
À l'aide de la console Gestionnaire IIS, développez l'ordinateur local et sélectionnez *Sites Web*. L'état du **site Web par défaut** doit être *En cours d'exécution*. Vous devriez également voir une application *CertSrv* répertoriée sous le **site Web par défaut**. Si le site n'est pas en cours d'exécution ou si l'application est manquante, vous devez résoudre le problème avant de poursuivre.

Générer un certificat à partir d'une autorité de certification interne

Lorsque vous configurez Microsoft Active Directory pour l'accès SSL, vous devez générer un certificat interne et demander le certificat externe.

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Ces étapes s'appliquent aux services Microsoft CA. Si vous disposez d'une autre plate-forme d'autorité de certification interne, adressez-vous à votre administrateur d'autorité de certification local pour obtenir de l'aide.

Procédure

1. À partir du contrôleur de domaine (DC) pour lequel vous souhaitez créer un certificat, accédez à `http://localhost/certsrv` ou spécifiez le nom du serveur CA s'il se trouve sur un serveur distant.
2. Sur la page d'accueil, cliquez sur **Demander un certificat** et sélectionnez *Demande de certificat avancée*.
3. Sur la page Demande de certificat avancée, sélectionnez **Créer** et soumettre une demande à cette autorité de certification.
4. Complétez la demande de certificat avancé comme suit :

Champs de demande de certificat avancé

Champ	Entrée
Nom	Le nom de domaine complet (FQDN) du contrôleur de domaine qui demande le certificat.
Courriel	L'adresse e-mail de la personne responsable du certificat.
Société	Nom de votre société.
Paramètres des options clés	
Créer un nouvel ensemble de clés	Sélectionnez-le.
Demande de signature de certificat	Fournisseur de chiffrement Microsoft RSA SChannel.
Utilisation de la clé	Échanger.
Taille de la clé	1024 est recommandé. L'instance prend en charge jusqu'en 2048.
Nom du conteneur de clés automatique	Sélectionnez-le.
Stocker le certificat dans le magasin de certificats de l'ordinateur local	Sélectionnez-le.

5. Cliquez sur **Envoyer**.
   Vous êtes redirigé vers une page qui fournit votre **ID de demande**, notez cet ID.
6. Pour traiter la demande en attente, procédez comme suit :
   a. Ouvrez la console de gestion de l'autorité de certification.
   b. Développez le nœud du serveur et sélectionnez **Demandes en attente**.
   c. Localisez l'ID de la demande que vous venez d'envoyer, cliquez avec le bouton droit de la souris et sélectionnez *Toutes les tâches/Problème pour approuver la demande et émettre le certificat*.
7. Pour récupérer le certificat émis, procédez comme suit :
   a. À partir du collecteur de données à partir duquel vous avez effectué la demande, accédez à `http://localhost/certsrv` ou spécifiez le nom du serveur CA s'il se trouve sur un serveur distant.
   b. Sélectionnez `Afficher l'état d'une demande de certificat en attente`.
   c. Sélectionnez le lien vers le nouveau certificat.
   d. Sélectionnez le lien pour **installer ce certificat**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Vous devez demander un certificat tiers. Les certificats des autorités de certification externes peuvent être achetés pour aussi peu que 30 $ par an. Pour connaître les procédures détaillées de demande d'un certificat auprès d'une autorité de certification externe, consultez l'article Microsoft 321051 . Une fois qu'il est reçu, installé et testé, suivez la procédure d'exportation.

Tester la connectivité LDAPS localement

Testez la connectivité LDAPS après l'installation des certificats internes et tiers lorsque vous configurez Microsoft Active Directory pour l'accès SSL.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Assurez-vous que les outils de support Windows sont installés sur le contrôleur de domaine (DC).
   Le programme d'installation des outils de support (suptools.msi) se trouve dans le répertoire `\Support \Tools` de votre CD du serveur Windows.
2. Accédez à la **Début** > **Tous les programmes** > **Outils d'assistance Windows** > **Ligne de commande**.
   Sur la ligne de commande, entrez `ldp pour démarrer l'outil` .
3. Dans la fenêtre *LDP* , sélectionnez **Connexion** > **Connexion** et indiquez le nom de domaine complet local et le numéro de port (636).
   Sélectionnez également le *SSL*.
   En cas de réussite, une fenêtre affiche et répertorie les informations relatives à la connexion SSL Active Directory. Si la connexion échoue, essayez de redémarrer votre système et répétez cette procédure.

Exporter le certificat de clé publique pour approuver le certificat LDAP

Exportez le certificat de clé publique et importez-le dans l'application lorsque vous configurez Microsoft Active Directory pour l'accès SSL.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Si votre autorité de certification n'est pas un fournisseur tiers de confiance, vous devez exporter le certificat pour l'autorité de certification émettrice afin que nous puissions lui faire confiance et, par association, approuver le certificat du serveur LDAP. Pour les utilisateurs de MS Certificate Services, vous pouvez afficher le chemin d'accès au certificat en affichant le certificat dans la console utilisée pour l'exportation ; sélectionnez l'onglet **Chemin d'accès au certificat** . Vous devez exporter tous les certificats de la chaîne. Vous pouvez trouver le certificat CA dans le même dossier que le certificat LDAP en recherchant son nom dans le chemin d'accès au certificat. Soumettez tous les certificats pour importation dans votre instance.

Procédure

1. À partir d'une console MMC actuelle ou nouvelle, ajoutez le composant logiciel enfichable Certificat (ordinateur local).
2. Ouvrez le dossier `Personnel/Certificats` .
3. Localisez le nouveau certificat.
   La colonne Émis à affiche le nom de domaine complet (FQDN) du contrôleur de domaine.
4. Cliquez avec le bouton droit de la souris sur le certificat et sélectionnez *Toutes les tâches/Exporter*.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Exportez au format DER ou Base-64.
   Nommez le fichier en utilisant le format `MyCompany.cer`. Il s'agit du certificat de clé publique dont vous avez besoin pour communiquer en toute sécurité avec votre contrôleur de domaine.
6. Testez LDAPS localement avant d'envoyer le certificat à l'instance.

Que faire ensuite

Une fois cette procédure terminée, importez le certificat de clé publique dans l'application.
Reportez-vous à la section Installer le certificat SSL LDAP X.509 pour télécharger le certificat dans l'application.

Utilisation du catalogue global LDAP

Un contrôleur de domaine peut se voir attribuer le rôle de catalogue global (GC). Le rôle Global Catalog (GC) est un répertoire conforme à LDAP qui consiste en une représentation partielle de chaque objet de chaque domaine d'une forêt.

Les administrateurs configurent Active Directory pour héberger les informations d'annuaire LDAP (Lightweight Directory Access Protocol) à l'aide de l'une des méthodes d'hébergement suivantes.

- La méthode courante d'hébergement des informations de répertoire LDAP consiste à utiliser le LDAP ou LDAPS (LDAP sécurisé) par défaut sur les ports 389 ou 636. Ces ports LDAP standard existent toujours sur un contrôleur de domaine (DC) et sont rarement modifiés. L'accès à cette partition de répertoire permet d'accéder à tous les objets du domaine hébergé sur le contrôleur de domaine. Il n'existe aucun moyen d'accéder aux objets d'autres domaines à l'aide de cette méthode.
- Un contrôleur de domaine peut également se voir attribuer le rôle de catalogue global (GC). Le rôle Global Catalog (GC) est un répertoire conforme aux normes LDAP qui consiste en une représentation partielle de chaque objet de chaque domaine de la forêt. Ce répertoire LDAP est accessible sur le port 3268, avec LDAPS sur le port 3269. Les exigences en matière de certificats des ports LDAPS et LDAP par défaut sont les mêmes.

Catalogue global Dépendances LDAP

- Le rôle Catalogue global doit être activé pour le contrôleur de domaine auquel votre instance se connecte.
- Les règles de pare-feu doivent autoriser le trafic entrant vers le contrôleur de domaine sur le port 3268 (LDAP) ou 3269 (LDAPS).

Remarques spéciales

- Tous les attributs ne sont pas répliqués sur la partition GC. Les attributs communs tels que le prénom, le nom, l'adresse e-mail, le numéro de téléphone, la description et l'adresse sont inclus. Des attributs supplémentaires peuvent être ajoutés au GC, mais doivent être limités afin de minimiser l'impact sur le trafic de réplication forestière.
- Les intégrations LDAP standard utilisent généralement sAMAccountName comme ID d'utilisateur de l'instance et comme clé de fusion dans la carte d'importation LDAP, car il est garanti qu'il s'agit d'une clé unique au sein d'un domaine. Cet attribut n'est plus unique lors de l'affichage d'une forêt entière de domaines. Un nouvel attribut unique doit être identifié, en tant qu'ID utilisateur et clé de fusion. Ceux-ci n'ont pas besoin d'être les mêmes attributs et peuvent varier en fonction de la conception de votre forêt. Consultez votre administrateur Active Directory. En règle générale, userPrinicpalName est un attribut unique dans tous les domaines, mais ce n'est peut-être pas un nom convivial pour se connecter, mais il peut être utilisé pour l'identificateur unique lors des importations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’adresse e-mail est un attribut couramment utilisé pour l’ID utilisateur. Ces décisions ont un impact sur les propriétés LDAP et le mappage LDAP.

- La valeur utilisée pour la clé de fusion sur la carte d’importation LDAP doit être unique et exister sur chaque objet importé. S’il n’est pas unique ou n’existe pas, les enregistrements incorrects sont mis à jour avec les changements.
- Si vous disposez déjà d’une intégration LDAP et que vous souhaitez la remplacer par un GC, changez la clé de coalescence d’importation. Les nouvelles valeurs de clé doivent être importées avant de pouvoir modifier la clé de fusion.
- Si vous apportez des modifications à votre intégration LDAP qui interrompent votre intégration, votre première étape doit être d’annuler ces changements. Après cela, contactez-nous Service et assistance client avec des informations complètes sur ce que vous tentez.

Modification mineure du schéma OpenLDAP

Dans les systèmes OpenLDAP 2.3 qui utilisent le back-bdb (backend Berkley), les administrateurs apportent une modification mineure à leur schéma pour faciliter l’intégration.

Avertissement :
La personnalisation décrite ici a été développée pour une utilisation dans des instances spécifiques, et n'est pas prise en charge par Now Support. Cette méthode est fournie telle quelle et doit être testée rigoureusement avant d'être implémentée. Publiez toutes les questions et commentaires concernant cette personnalisation dans notre forum communautaire.

Dans OpenLDAP 2.3, back-bdb n’a qu’une prise en charge limitée de l’indexation (ordonnancement) des inégalités. Il est implémenté uniquement pour les syntaxes generalizedTime et ChangeSequenceNumber. Il ne peut pas être pris en charge sur une syntaxe qui prend en charge les sous-chaînes. Les filtres de recherche contenant des inégalités sont traités à l’aide de l’index de présence.

Nous vous recommandons de créer un attribut personnalisé à cet effet, au lieu de modifier ce qui est déjà indexé ou présent dans le schéma (par exemple, `servnowid`).

Modifier le schéma OpenLDAP

Modifiez le schéma OpenLDAP. Ces étapes détaillent une modification de schéma d’OpenLDAP 2.3 fournie par l’un de nos clients qui l’a aidé à s’intégrer à son instance.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Avertissement :
La personnalisation décrite ici a été développée pour une utilisation dans des instances spécifiques, et n'est pas prise en charge par Now Support. Cette méthode est fournie telle quelle et doit être testée rigoureusement avant d'être implémentée. Publiez toutes les questions et commentaires concernant cette personnalisation dans notre forum communautaire.

Pour modifier le schéma OpenLDAP en vue de son intégration à l’instance :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Créez un attribut personnalisé.

   Example

   ```
   attribute ( 1.3.6.1.4.1.3403000.2.1.8

      NAME 'servnowid'
   ORDERING caseIgnoreOrderingMatch
   EQUALITY caseIgnoreMatch
   SYNTAX '1.3.6.1.4.1.1466.115.121.1.15' )
   ```

2. Inclure l'attribut dans l'OID objectclass sélectionné.

   Example

   ```
   objectclass ( 1.3.6.1.4.1.3403000.2.2.1
      NAME 'BcfUserIdentifiers' SUP top AUXILIARY
   MAY ( uniqid $ unixid $ servnowid ) )
   ```

   Dans OpenLDAP 2.3, vous pouvez modifier dynamiquement les configurations du serveur, mais vous ne pouvez étendre que le schéma. Vous ne pouvez pas modifier ou supprimer le schéma existant. Au lieu de créer une autre classe d'objet pour cet attribut dans la configuration dynamique, utilisez le fichier de configuration statique, slapd.conf.

3. Dans slapd.conf, incluez l'indexation pour le nouvel attribut dans la section bdb de votre backend de base de données principal.

   Example

   ```
   database bdb (configs here) ....

   index servnowid pres

   (other indexes here) .....
   ```

4. En tant que root, exécutez slapindex pour indexer cet attribut afin de le rendre disponible dans les filtres de recherche.
   Assurez-vous que le démon OpenLDAP n'est pas en cours d'exécution ou qu'il est en mode lecture seule avant de démarrer le slapindex.

Enregistrer les suppressions LDAP

Par défaut, l'instance ne supprime aucune entrée une fois qu'elle a disparu de LDAP.

La suppression d'une entrée, également appelée *enregistrement*, supprime également tout l'historique et les références à l'entrée supprimée.

Par exemple, les éléments de configuration (CI), les accords SLA, les licences logicielles, les bons de commande et les entrées de Service Catalog font tous référence au département. Si un département est supprimé, l'intégration efface toutes les références au département. En outre, la suppression d'un utilisateur entraîne la perte de tout historique de ce qu'il a fait.

Décidez s'il faut conserver ou Delete all records from a table en fonction des besoins de votre organisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sessions simultanées limites

Vous pouvez limiter le nombre de sessions interactives simultanées pour un utilisateur ou un rôle sur une instance dans tous les nœuds.

Explorer



Découvrez les fonctionnalités et la valeur commerciale des sessions simultanées limitées.

Activer



Découvrez comment activer les sessions simultanées limitées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définir



Définissez la limite de sessions simultanées pour un utilisateur ou un rôle.

Désactiver



Découvrez comment désactiver la limite de sessions simultanées.

Traduction automatique

Exploration de la limite de sessions simultanées

Vous pouvez limiter le nombre de sessions interactives simultanées pour un utilisateur ou un rôle sur une instance dans tous les nœuds.

Les sessions interactives simultanées font référence au nombre de sessions qu'un utilisateur peut avoir actives par ServiceNow instance. Une session d'instance active se produit à chaque nouvelle connexion à une instance spécifique ServiceNow . Par défaut, il n'y a aucune limite au nombre de sessions d'instance actives qu'un utilisateur peut avoir.

Avec la version Jakarta, vous pouvez limiter le nombre de sessions simultanées actives par utilisateur. Lorsque l'utilisateur se connecte après avoir atteint le nombre maximal de sessions actives, la session active la plus ancienne se termine et une nouvelle session interactive devient active. Si un utilisateur tente d'accéder à une session fermée via un navigateur, il est redirigé vers la page de connexion.

Remarque :
Le module d'extension **Limite de sessions simultanées** doit être actif pour activer une limite de sessions maximale. Les limites sont définies via la propriété glide.authenticate.max.concurrent.interactive.sessions. Une valeur limite maximale s'applique à tout utilisateur ou rôle dont la propriété limite est active. Un utilisateur ou un rôle connecté à l'utilisateur doit avoir la valeur limit_concurrent_sessions définie sur vrai pour la limite de sessions à initier. Pour la version Jakarta, cette fonctionnalité ne prend pas en charge les sessions créées via l'application mobile native ou des mécanismes non interactifs.

Un cas d'utilisation typique si une session simultanée maximale de 1 est définie :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

1. L'utilisateur accède à l'instance initiale ServiceNow via Chrome.
2. Une fois que l'utilisateur est connecté, ServiceNow la session 1 (S1) est créée pour l'utilisateur.
3. L'utilisateur décide d'initier un autre accès à l'instance ServiceNow via Firefox.
4. Une fois que l'utilisateur est connecté, ServiceNow la session 2 (S2) est créée pour l'utilisateur.
5. Étant donné que l'utilisateur a une limite de session simultanée maximale de 1, la session S1 est invalidée lorsque S2 est créé.
6. Lorsque l'utilisateur revient via Chrome pour accéder à l'instance S1 ServiceNow , il est redirigé vers la page de connexion, car S1 n'est pas valide.

Les limites de sessions simultanées fonctionnent avec tous les mécanismes d'authentification ServiceNow : SAML, LDAP et authentification de base de données locale. Il fonctionne également avec l'authentification multifacteur et tous les mécanismes d'authentification interactifs ServiceNow . La source de la session est visible via la table **sys_user_session** , sous la colonne **Type**. Les valeurs peuvent être :

- Navigateur Web
- Navigateur mobile
- ServiceNow Application mobile
- Non interactif (SOAP, WSDL, OAuth)

Activation et configuration du module d'extension Limite de sessions simultanées

Vous pouvez activer le module d'extension Limite de sessions simultanées (com.glide.limit.concurrent.sessions) si vous disposez du rôle administrateur.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Modules d'extension**.
2. Recherchez et cliquez sur le module d'extension Limit Concurrent Sessions.
3. Dans le formulaire Module d'extension système, examinez les détails du module d'extension, puis cliquez sur le lien connexe **Activer/Mettre à niveau** .
4. Cliquer sur **Activer**.
5. Pour activer cette fonctionnalité et définir une limite maximale de sessions simultanées, accédez à l'onglet **Fichiers du module d'extension** , recherchez les propriétés suivantes et modifiez les valeurs des paramètres.

Option	Description
glide.authenticate.limit.concurrent.interactive-.sessions	Vous pouvez activer la possibilité de limiter les sessions simultanées en définissant la valeur sur **Vrai**. Par défaut, cette propriété est définie sur **False**, ce

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	qui signifie qu'il n'y a aucune limite au nombre de sessions interactives qu'un utilisateur peut activer. **Remarque :** Pour désactiver cette fonctionnalité, redéfinissez cette propriété sur **Faux**.
glide.authenticate.max.concurrent.interactive-.sessions	Vous pouvez définir le nombre maximal de sessions interactives actives simultanées qu'un utilisateur peut avoir sur l'instance dans tous les nœuds.

6. **Facultatif :** Vous pouvez également modifier les propriétés suivantes, si nécessaire.

Option	Description
glide.authenticate.session.types.to.limit.concurrency	Cette propriété limite les types de sessions. Par défaut, seules les sessions du navigateur Web ont une limite. Les types de sessions sont les suivants : ○ Navigateur Web (1) ○ Navigateur mobile (2) ○ ServiceNow Application mobile (3) ○ Non interactif (10) Vous pouvez configurer et définir la valeur sur « 1 » pour le navigateur Web, « 2 » pour le navigateur mobile ou « 1,2 » pour les deux. **Remarque :** Seules les sessions de navigateur Web et mobile peuvent avoir une limite. Il n'y a aucune limite pour les sessions provenant de l'application ServiceNow mobile ou les sessions non interactives.
glide.authenticate.limit.concurrent.sessions-.across.all.nodes	Cette propriété limite la limite de sessions simultanées par nœud au lieu de les restreindre à tous les nœuds d'une ServiceNow instance. Par défaut, la valeur est définie sur vrai, ce qui limite les sessions utilisateur sur tous les nœuds. Si la propriété est définie sur false, seules les sessions sur ce nœud et non celles sur les autres nœuds sont soumises à la limite.

7. Cliquez sur **Mettre à jour** pour que les paramètres prennent effet.

Que faire ensuite

Définition d'une limite de sessions simultanées par utilisateur ou rôle.

Information associée

Liste des modules d'extension (Xanadu)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition d'une limite de sessions simultanées par utilisateur ou rôle

Vous pouvez définir une limite de sessions simultanées pour un utilisateur spécifique ou pour un rôle particulier.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs** ou **Administration utilisateurs** > **Rôles**.
2. Sélectionnez un utilisateur ou un rôle pour lequel vous souhaitez définir une limite de sessions simultanées, cochez la case **Limiter les sessions simultanées** , puis cliquez sur **Mettre à jour**.
   L'utilisateur ou le rôle limite le nombre de sessions simultanées pouvant être ouvertes à la fois.

Désactivation d'une limite de sessions simultanées par utilisateur ou rôle

Vous pouvez désactiver une limite de sessions simultanées pour un utilisateur spécifique ou pour un rôle particulier.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs** ou **Administration utilisateurs** > **Rôles**.
2. Sélectionnez un utilisateur ou un rôle pour lequel vous souhaitez désactiver une limite de sessions simultanées, décochez la case **Limiter les sessions simultanées** , puis cliquez sur **Mettre à jour**.
   L'utilisateur ou le rôle n'est pas soumis à une limite du nombre de sessions simultanées pouvant être ouvertes à la fois.

Authentification locale

Utilisez ServiceNow® l'authentification locale pour sécuriser la connexion des utilisateurs sur un équipement local.

L'authentification locale est une méthode de vérification de l'identité d'un utilisateur sur un appareil local. Elle utilise des caractéristiques ou des informations d'identification uniques possédées par l'utilisateur pour valider la connexion de l'utilisateur.

Utilisez ServiceNow®les fonctionnalités d'authentification locale de pour accéder en toute sécurité à l'instance ServiceNow® sur vos appareils locaux.

Sécurité de connexion et d'authentification

Configurez les options de sécurité de connexion pour contrôler l'accès à votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer votre sécurité de connexion



Découvrez comment configurer la sécurité de connexion.

Définir des scénarios de connexion



Définissez les scénarios de connexion.

Réinitialisation du mot de passe



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus sur la réinitialisation du mot de passe de connexion.

Explorer la sécurité de connexion et d'authentification

Configurez les options de sécurité de connexion pour contrôler l'accès à votre instance.

Options de sécurité

Vous pouvez contrôler plusieurs aspects de la sécurité de connexion et d'authentification de l'utilisateur :

Fonctionnalité	Description	Rubriques connexes
Contrôles de connexion et de déconnexion	Contrôlez plusieurs dimensions du processus de connexion et de déconnexion pour les utilisateurs, telles que la spécification d'une page de destination que l'utilisateur voit lors de la connexion et contrôlez la façon dont les utilisateurs se déconnectent.	• Définition des scénarios de connexion • Configuration de l'invite de confirmation de déconnexion • Sorties d'installation • Spécifier le verrouillage pour les échecs de tentatives de connexion
Sécurité de l'authentification	Contrôlez le processus de réinitialisation du mot de passe et les fonctionnalités telles que l'option Se souvenir de moi. Vous pouvez également utiliser des contrôles basés sur l'adresse IP pour accéder à l'instance et implémenter un nonce à utiliser avec l'authentification Single-Sign-on Digest.	• Configuration de votre politique de mot de passe • Réinitialisation du mot de passe • Mémoriser mon nom • Authentification basée sur la plage IP • Implémentation d'une valeur de circonstance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Définition des scénarios de connexion

Vous pouvez diriger tous les utilisateurs vers la même page après la connexion.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Lorsque les utilisateurs se connectent directement à une instance, par exemple en accédant à http://{instance_name}.service-now.com/, le système effectue les opérations suivantes :

1. Accède à la valeur de la propriété `glide.entry.page.script`. La valeur par défaut de la propriété est dérivée d'un include de script nommé *CMSEntryPage*.
2. Dirige l'utilisateur vers la page de connexion de l'instance si la page d'entrée nécessite une connexion.
3. Applique les règles de connexion, le cas échéant, à l'utilisateur.

Pour forcer le système à rediriger tous les utilisateurs vers la même page après la connexion :

Procédure

1. Accédez à la **Tout** > **Gestion du contenu** > **Configuration** > **Page de configuration**.
2. Sélectionnez une valeur pour le champ *Page de connexion* ou créez une nouvelle page comme vous le souhaitez.

   Si cette page n'est pas la page par défaut du site, elle redirige toujours ici. S'il s'agit d'une page par défaut du site, des règles de connexion s'appliquent. Si cette valeur est nulle, le système utilise navpage.do comme page d'entrée. N'entrez pas de page de connexion ici ; Dans le cas contraire, les utilisateurs doivent se connecter deux fois.

   Se connecter à une instance pour accéder à un enregistrement :

   Lorsque les utilisateurs se connectent à une instance pour accéder à un enregistrement à l'aide de son identificateur unique global (sys_id), tel que http://{instance}.service-now.com/incident.do?sys_id={sys_id}, le système effectue les opérations suivantes :

   a. Dirige l'utilisateur vers une page de connexion s'il n'est pas déjà connecté.

   b. Dirige l'utilisateur vers l'enregistrement approprié s'il est autorisé à y accéder. Si l'utilisateur ne dispose pas des droits d'accès à l'enregistrement, un message de refus d'accès s'affiche.

   Connexion au Service Portal ou à un site CMS :

   Lorsque les utilisateurs se connectent au Service Portal ou à un site CMS, tel que http://<instance>.service-now.com/site-name/page.do, le système effectue les opérations suivantes :

   - S'il y a une valeur dans le champ *Page de connexion* du formulaire Portail de services ou du site CMS, il dirige l'utilisateur vers cette page de connexion et applique les règles de connexion, le cas échéant, à l'utilisateur.
   - Si aucune page de connexion n'est spécifiée, elle dirige l'utilisateur vers la valeur du champ *Page d'accueil* du formulaire Portail de services ou du site CMS.

   Se connecter à Service Portal ou à un site CMS pour accéder à un enregistrement :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque les utilisateurs se connectent au Service Portal ou à un site CMS pour accéder à un enregistrement, par exemple http://{instance}.service-now.com/ess/incident_detail.do?sysparm_document_key=incident,{sys_id}, le système suit la même procédure et finalement dirige l'utilisateur vers l'enregistrement. Si l'utilisateur ne dispose pas des droits d'accès à l'enregistrement, un message de refus d'accès s'affiche.

Les connexions et le portail en libre-service employé

Le système conserve la trace de la première page de démarrage à laquelle un utilisateur essaie d'accéder, même s'il souhaite se connecter au portail libre-service Employés.

Examinez les scénarios suivants.

Exemple 1 :

1. Un utilisateur n'est pas connecté et tente ensuite d'accéder à un enregistrement à l'aide d'un ID système spécifique dans l'URL.
2. Le système redirige l'utilisateur vers la page de connexion.
3. Plutôt que de se connecter, l'utilisateur tente d'accéder à un autre site, tel que le portail libre-service employés (/ess).
4. Le système redirige à nouveau l'utilisateur vers la page de connexion.
5. L'utilisateur se connecte et est redirigé vers l'enregistrement auquel il essayait d'accéder en premier plutôt que vers le portail en libre-service employé.

Exemple 2 :

1. Un utilisateur n'est pas connecté, puis tente d'accéder à un enregistrement à l'aide d'un ID système spécifique dans l'URL via le portail libre-service employés (/ess).
2. Le système redirige l'utilisateur vers la page de connexion.
3. Plutôt que de se connecter, l'utilisateur tente d'accéder à un autre enregistrement via le portail libre-service Employés.
4. Le système redirige à nouveau l'utilisateur vers la page de connexion.
5. L'utilisateur se connecte et est redirigé vers le premier enregistrement plutôt que vers le second.

Spécifier une page de destination de connexion

Par défaut, les utilisateurs voient leur page d'accueil lors de la connexion. Vous pouvez spécifier une page de destination de connexion différente à l'aide d'une propriété système ou du système de gestion de contenu.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Pour spécifier une page de destination de connexion pour tous les utilisateurs, modifiez la valeur de la propriété sur la table sys_properties.

Procédure

1. Saisissez sys_properties.list dans le filtre de navigation.
2. Localisez la propriété **système glide.login.home** .
3. Dans le champ **Valeur** , saisissez le nom de la page que tous les utilisateurs voient lorsqu'ils se connectent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez <nom de la page>.do ; vous pouvez omettre la partie http ://"instance".service-now.com/ de l'URL. Pour déterminer le nom de la page ou l'URL d'une page dans le système, vous pouvez pointer vers un lien. Certaines pages possibles sont welcome.do et incident.do.

Pour spécifier une page de destination de tableau de bord, définissez la propriété sur $dashboards.do ?dashboard=<SYS_ID>. Remplacez <SYS_ID> par la sys_id du tableau de bord.

Pour diriger les utilisateurs vers Service Portal, définissez la propriété sur /sp

Remarque :
Cette propriété s'applique à l'ensemble du système, donc sa définition affecte tous les utilisateurs. Pour définir une connexion spécifiquement destinée aux utilisateurs n'ayant aucun rôle, vous pouvez appliquer ces mêmes étapes et utiliser la propriété **glide.entry.loggedin.page_ess** .

Vous pouvez également spécifier une page de destination de connexion avec le système de gestion de contenu.

Spécifier le verrouillage pour les échecs de tentatives de connexion

Le système fournit des actions de script inactives qui vous permettent de spécifier le nombre d'échecs de tentatives de connexion avant qu'un compte utilisateur ne soit verrouillé et de réinitialiser le nombre après une connexion réussie.

Avant de commencer
Rôle requis : administrateur

Procédure

Accédez à la **Tout** > **Politique système** > **Actions des scripts** pour afficher ou activer les scripts.

Remarque :
À partir de la Kingston mise en production, après un zBoot, les actions des scripts **Vérification du verrouillage de l'utilisateur SNC avec déverrouillage automatique** et **Effacement de l'utilisateur SNC** sont activées.

Pour en savoir plus sur les propriétés qui affectent les échecs de tentative de connexion, consultez Gestion des échecs de tentatives de connexion (renforcement de la sécurité de l'instance) dans les paramètres de renforcement de la sécurité de l'instance.

Action des scripts	Description
Vérification du verrouillage de l'utilisateur SNC avec déverrouillage automatique	• Utilise la valeur de la propriété `glide.user.max_unlock_attempts` pour définir la limite des échecs de tentative de connexion. • Déverrouille le compte d'utilisateur après la période spécifiée pour la propriété `glide.user.unlock_timeout_in_mins` . Si aucune valeur n'est spécifiée, le système déverrouille le compte utilisateur après la période par défaut de 15 minutes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Action des scripts	Description
Vérification du verrouillage de l'utilisateur SNC	Suit le nombre d'échecs de tentatives de connexion et verrouille le compte utilisateur après un nombre spécifié d'échecs de tentatives de connexion (par défaut : 5).
Effacement de l'utilisateur SNC	Met à jour l'enregistrement utilisateur après une connexion réussie : réinitialise le nombre d'échecs de tentatives de connexion et met à jour la date de la dernière connexion.

Que faire ensuite

Chaque fois qu'un utilisateur tente de se connecter, l'action est enregistrée dans un journal des événements. Vous pouvez afficher un journal des tentatives de connexion infructueuses.

1. Accédez à la **Politique système** > **Journaux des événements**.
2. Filtre **pour login.failed** dans le champ **Nom** . Vous pouvez afficher le nom de connexion, la date et l'adresse IP de la tentative de connexion.

Rendre les pages de l'interface utilisateur publiques ou privées

Vous pouvez rendre les pages publiques si vous souhaitez que vos utilisateurs voient les pages sans se connecter.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La plupart des pages ne sont consultables que par les utilisateurs connectés. Un nombre limité de pages sont publiques afin que les utilisateurs n'aient pas à se connecter pour les consulter, comme la page d'accueil, la page d'accueil et les pages de connexion et de déconnexion.

Avertissement :
Plusieurs pages publiques du système de base sont nécessaires pour la fonctionnalité de nombreuses fonctionnalités. Ne désactivez pas les pages publiques du système de base.

Procédure

1. Dans le filtre du navigateur d'application, saisissez `sys_public.list`.
2. Cliquez sur **Nouveau**.
3. Dans la table sys_public, créez un enregistrement avec les valeurs suivantes.

Champ	Description
Page	Le nom de la page. Par exemple : $sp
Actif	Lorsque cette option est sélectionnée, la page est publiquement accessible. Désélectionnez l'option Actif lorsque vous souhaitez que la page soit privée.

4. Cliquez sur **Enregistrer**.
   Si actif est défini sur vrai, la page devient publique et toute personne visitant `<instance_name>/sp` ou `<instance_name>/$sp.do` peut y accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exigences de complexité des mots de passe

Les mots de passe de votre ServiceNow® instance doivent répondre aux exigences de complexité.

Explorer	Activer
	
Découvrez les fonctionnalités et la valeur commerciale des exigences de complexité des mots de passe.	Découvrez comment activer les exigences de complexité des mots de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer



Configurez les exigences de complexité du mot de passe.

Référence : caractères de mot de passe non pris en charge



Renseignez-vous sur les caractères de mot de passe non pris en charge.

Traduction automatique

Explorer les exigences de complexité des mots de passe

Les mots de passe de votre ServiceNow® instance doivent répondre aux exigences de complexité.

Le paramètre de politique Exigences de complexité des mots de passe détermine si les mots de passe doivent respecter une série de directives relatives aux mots de passe forts.

Les exigences de complexité des mots de passe s'appliquent lorsqu'un mot de passe est modifié ou créé.

Les exigences en matière de complexité des mots de passe sont respectées et fonctionnent sur la base des éléments suivants :

- Si la *glide.apply.password_policy.on_login* propriété est activée, la vérification de la politique de mot de passe est appliquée à l'utilisateur pendant la connexion. Pendant la connexion, l'utilisateur doit respecter la politique de mot de passe et changer le mot de passe de l'instance.
- Les exigences de la politique de mot de passe sont basées sur le plan multilingue de base (BMP) qui contient des caractères pour toutes les langues modernes. ServiceNow Les instances sont livrées avec des BMP d'environ 10 000 caractères.
- Il est possible de définir des mots de passe dans les BMP autorisées pour votre instance. Les mots de passe qui n'adhèrent pas à ces PGO ne sont pas autorisés.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si nécessaire, vous pouvez exiger que les mots de passe soient changés régulièrement, au moins tous les 90 jours.

Conditions obligatoires et caractères interdits

Pour activer un environnement réseau sécurisé, il est nécessaire que les utilisateurs utilisent des mots de passe forts qui incluent une combinaison de lettres, de chiffres et de symboles. Ces combinaisons permettent d'empêcher les utilisateurs non autorisés qui utilisent généralement des méthodes manuelles ou automatisées de deviner des mots de passe faibles.

Le mot de passe de votre instance doit répondre aux exigences suivantes :

- 8 caractères minimum.
- 100 caractères maximum.
- Contient des caractères en minuscules et en majuscules
- Contient des caractères spéciaux.
- Contient des chiffres.

Vous pouvez interdire une liste de mots de passe malveillants courants, tels que les suivants :

- Des séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$%^ », « aaaaa », etc.
- Nom de l'employé ou noms d'utilisateur.
- Noms de marques ou de produits pertinents.
- Emplacements, tels que le siège social de la société, la ville, le pays, et ainsi de suite.
- Termes internes ou abréviations spécifiques à l'entreprise.
- Des émojis.

Remarque :
Les caractères spécifiques à l'utilisateur, à la marque ou à la société qui ne peuvent pas être utilisés dans le mot de passe peuvent être configurés dans la page Politique de mot de passe ou Exclure le mot de passe.

Activer les politiques de mot de passe sur votre instance

Implémentez des contrôles de politique de mot de passe lors de la connexion. Forcer les utilisateurs à changer leur mot de passe si le mot de passe ne répond pas aux critères de politique de mot de passe.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Le module d'extension Password Policy (com.glide.password_policy) est activé par défaut. La politique entre en vigueur lorsqu'un utilisateur modifie ou réinitialise le mot de passe.
Le champ **Force du mot de passe prédéfinie** est automatiquement défini sur **Fort par défaut**.
Si vous souhaitez ajouter de nouveaux critères, vous pouvez procéder comme suit.

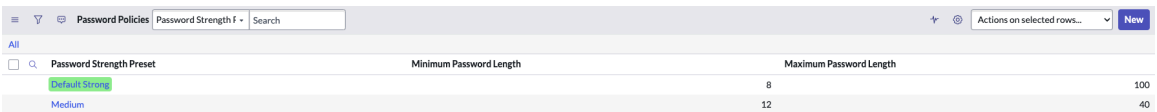
Si vous avez personnalisé votre instance via la sortie d'installation ou votre propriété de banque `pwd_cred_store` d'identifiants `ValidatePasswordStronger` Réinitialisation

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

du mot de passe, consultez les propriétés de la politique de mot de passe pour savoir comment implémenter une politique de mot de passe pour votre instance.

Remarque :
La politique de mot de passe active est mise en surbrillance pour l'instance, comme indiqué.



Pour modifier la politique de mot de passe, accédez à **Tout** > **Réinitialisation du mot de passe** > **Banques d'informations d'identification**, sélectionnez les informations d'identification et remplacez le champ **Politique de mot de passe** par l'entrée de politique requise.

Procédure

1. Accédez à la **Tout** > **Politique de mot de passe** > **Politiques de mot de passe**.
2. Cliquez sur **Nouveau**.
   Le formulaire Politique de mot de passe s'affiche.
3. Spécifiez le **nom** de votre politique de mot de passe.
4. Dans la section Critères de politique de mot de passe, sélectionnez l'un des paramètres prédéfinis suivants dans le champ Paramètre prédéfini de **niveau de sécurité du mot de passe** .

   Remarque :
   La politique de mot de passe est appliquée en fonction du paramètre prédéfini sélectionné.

5. Renseignez les champs restants du formulaire.

Formulaire Politique de mot de passe

Champ	Description
Longueur minimale du mot de passe	Longueur minimale du mot de passe. Cette option s'affiche pour tous les préréglages à l'exception **de Avancé**. Définissez ce champ sur un minimum de 8 à 10 caractères.
Longueur maximale du mot de passe	Longueur maximale du mot de passe. Cette option s'affiche pour tous les paramètres prédéfinis à l'exception **de l'option Avancé**. Définissez ce champ sur un maximum de 100 caractères.
Caractère(s) majuscule(s) minimum	Nombre minimum de caractères majuscules dans le mot de passe, de 0 à 10.
Caractère(s) minuscule(s) minimum	Nombre minimum de caractères minuscules dans le mot de passe, de 0 à 10.
Caractère(s) numérique(s) minimum	Nombre minimum de caractères dans le mot de passe, de 0 à 10.
Caractère(s) spécial(ux) minimum	Nombre minimum de caractères spéciaux dans le mot de passe, de 0 à 10.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Caractères spéciaux inclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, si vous saisissez `$,!`, les utilisateurs peuvent uniquement utiliser « $ » et « ! » comme caractères spéciaux dans le mot de passe. Aucun autre caractère spécial ne peut être utilisé. Un mot de passe avec d'autres caractères spéciaux n'est pas autorisé.
Caractères spéciaux exclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, si vous saisissez `@$!`, les caractères spéciaux que les utilisateurs ne peuvent pas utiliser dans leurs mots de passe sont « @ », « $ » et « ! ». **Remarque :** Cette option est disponible si la *glide.password_policy.use_excluded_special_ch* propriété est activée.
Interdire les données utilisateur	Option permettant d'interdire les données utilisateur liées à l'authentification.
Seuil de longueur de séquence	La longueur de la séquence de votre mot de passe.
Seuil de longueur de répétition	La longueur de répétition de votre mot de passe. **Remarque :** ◦ Le seuil de longueur de séquence et le seuil de longueur de répétition peuvent tous deux comporter un maximum de huit caractères. Ces champs vous permettent de restreindre les combinaisons faibles de mots de passe ayant des séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$%^ », « aaaaa », etc. ◦ Si la **force prédéfinie du mot de passe** est définie sur **Fort par défaut**, la longueur du seuil de longueur de séquence et du seuil de longueur de répétition est définie sur quatre caractères.
Testez votre mot de passe	Spécifiez votre mot de passe réel dans ce champ.

6. Cliquez sur **Tester votre mot de passe**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Une fois que la validité du mot de passe a été testée, cliquez sur **Envoyer** pour soumettre le mot de passe.

Remarque :
Testez toujours votre mot de passe avant de soumettre.

Propriétés de la politique de mot de passe

Les propriétés de la politique de mot de passe vous permettent d'administrer les politiques de mot de passe, d'exclure la liste des mots de passe et d'appliquer une politique de mot de passe pendant la connexion.

Accédez à la **Politique de mot de passe** > **Propriétés** pour afficher et modifier les propriétés de la politique de mot de passe.

Propriété	Description
glide.enable.password_policy	Active une politique de mot de passe pour votre instance. La politique entre en vigueur lorsqu'un utilisateur modifie ou réinitialise un mot de passe. Cette propriété est automatiquement définie sur **true**. **Remarque :** • Si votre instance est personnalisée, via la sortie d'installation ou votre `ValidatePasswordStronger` banque d'informations d'identification Réinitialisation du mot de passe [pwd_cred_store], vous devez créer cette propriété et l'ajouter à vos propriétés système. • Avant la Orlando publication, si votre instance était personnalisée avec la `ValidatePasswordStronger` sortie d'installation, vous deviez créer la propriété Politique de mot de passe pour que la politique de mot de passe fonctionne. • À partir de la Orlando version, il n'y a pas de personnalisation de la sortie de l'installation. Les propriétés de la politique de mot de passe fonctionnent par défaut. Ces propriétés peuvent être désactivées manuellement.
glide.enable.blacklist_password	L'utilisation de mots de passe spécifiques est interdite. L'administrateur peut insérer des mots de passe dans la table Mot de passe exclu. Cette propriété est automatiquement définie sur **true**.
glide.apply.password_policy.on_login	Oblige les utilisateurs à changer les mots de passe lors de leur prochaine connexion si les mots de passe existants ne sont pas conformes à la politique de mot de passe actuelle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Cette propriété est automatiquement définie sur **faux**. Définir la valeur sur **vrai** applique une politique de mot de passe pendant la connexion. **Remarque :** L'activation de cette propriété peut forcer un nombre important d'utilisateurs qui ne sont pas en conformité avec la nouvelle politique de mot de passe à changer leur mot de passe.
glide.password_policy.user_excluded_special_char	Permet aux utilisateurs d'utiliser l'option caractère spécial exclu sur le formulaire de politique de mot de passe.
glide.validate.sys_user.password.field	Active la validation du mot de passe de l'utilisateur par rapport à la politique de mot de passe lorsqu'un administrateur modifie le formulaire sys_user ou la vue de liste.
glide.password.policy.generate.password.field.disabled	Désactive le champ **Mot de passe** dans la fenêtre contextuelle Définir le mot de passe du formulaire sys_user.
glide.user.show.password.field	Active le champ **Mot de passe** sur le formulaire sys_user.
glide.password_policy.debug	Active la journalisation du débogage pour la politique de mot de passe.

Configuration de votre politique de mot de passe

Les critères de politique de mot de passe vous permettent de sécuriser votre mot de passe et de respecter les exigences minimales de complexité de mot de passe.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Le module d'extension Politique de mot de passe [com.glide.password_policy] est activé par défaut. Elle entre en vigueur lorsqu'un utilisateur modifie ou réinitialise le mot de passe. Si vous avez personnalisé votre instance, via la sortie d'installation ValidatePasswordStronger ou votre banque d'informations d'identification Réinitialisation du mot de passe [pwd_cred_store], consultez les propriétés de la politique de mot de passe.

Procédure

1. Accédez à la **Tout** > **Politique de mot de passe** > **Politiques de mot de passe**.

   Remarque : Le paramètre prédéfini **Strong par défaut** est activé comme critère d'acceptation du mot de passe par défaut. Si vous souhaitez ajouter un nouveau critère, vous pouvez procéder comme suit.

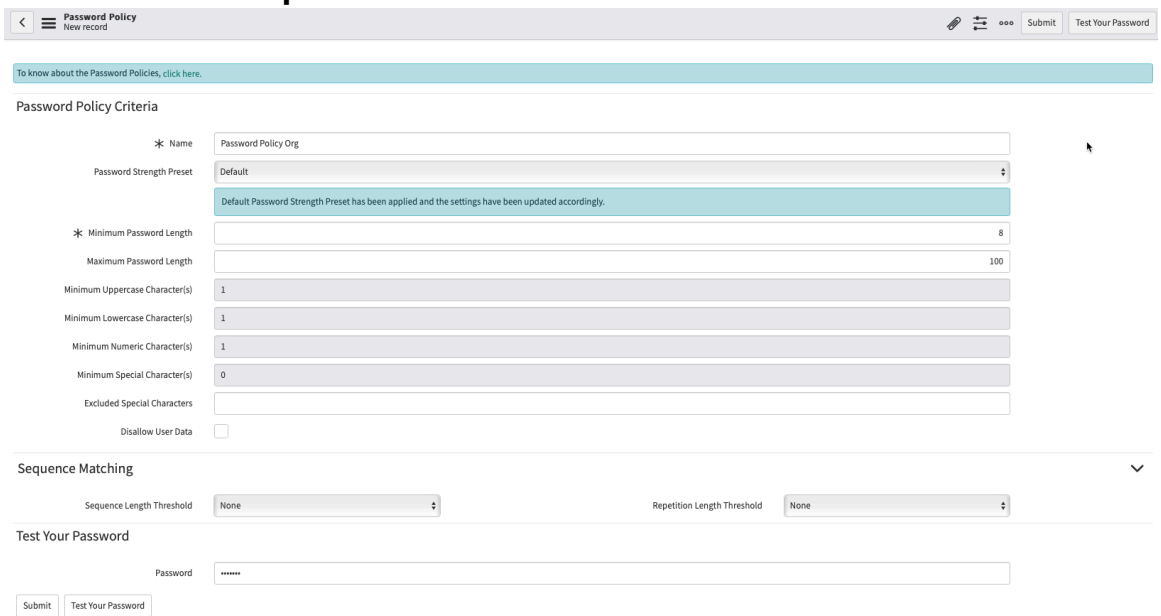
2. Cliquez sur **Nouveau**.

   La page Nouvel enregistrement de politique de mot de passe comporte les sections suivantes que vous devez spécifier pour définir votre mot de passe :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Critères de politique du mot de passe**
- **Correspondance de la séquence**
- **Tester votre mot de passe**



3. Spécifiez le **nom** de votre politique de mot de passe.
4. Dans la section **Critères de politique de mot de passe** , sélectionnez le paramètre prédéfini à partir du **Paramètre prédéfini de niveau de sécurité du mot de passe**. Les paramètres prédéfinis disponibles sont les suivants :

Force du mot de passe prédéfinie et sa description

Force du mot de passe prédéfinie	Description
Par défaut	Si **vous sélectionnez Par défaut** , les caractères de mot de passe requis sont remplis automatiquement, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum
Moyen	Si vous sélectionnez **Moyen** , les caractères de mot de passe requis sont remplis automatiquement en fonction des caractères, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum ○ Un caractère spécial minimum
Élevé	Si **vous sélectionnez Élevé** , les caractères de mot de passe sont remplis automatiquement, comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Force du mot de passe prédéfinie	Description
	○ Un caractère majuscule minimum ○ Deux caractères minuscules minimum ○ Un caractère numérique minimum ○ Trois caractères spéciaux minimum
Fort par défaut	Si vous sélectionnez **Fort par défaut** , les caractères de mot de passe requis sont remplis automatiquement en fonction des caractères, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum ○ Un caractère spécial minimum
Personnalisé	Si **vous sélectionnez Personnalisé** , les caractères de mot de passe requis sont remplis automatiquement en fonction des caractères, comme suit : ○ Un caractère majuscule minimum ○ Un caractère minuscule minimum ○ Un caractère numérique minimum ○ Un caractère spécial minimum Vous pouvez également personnaliser le **script de politique de mot de passe** qui s'affiche.
Avancés	La sélection de **Avancé** affiche le **script de règle de mot de passe** et le **script de force du mot de passe**. En fonction de vos besoins, vous pouvez personnaliser ces scripts.

Remarque :
La politique de mot de passe est appliquée en fonction du paramètre prédéfini sélectionné.

5. Spécifiez les champs décrits dans la table :

Formulaire Politique de mot de passe

Champ	Description
Longueur minimale du mot de passe	Longueur minimale du mot de passe. Cette option s'affiche pour tous les paramètres prédéfinis à l'exception **de l'option Avancé**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : **La longueur minimale du mot de passe** est un champ obligatoire et il est recommandé de le définir sur un minimum de 8 à 10 caractères.
Longueur maximale du mot de passe	Longueur maximale du mot de passe. Cette option s'affiche pour tous les paramètres prédéfinis à l'exception **de l'option Avancé**. **Remarque :** **Longueur maximale du mot de passe** est un champ facultatif et il est recommandé de le définir sur un maximum de 100 caractères.
Caractère(s) majuscule(s) minimum	Nombre minimum de caractères majuscules dans le mot de passe, de 0 à 10.
Caractère(s) minuscule(s) minimum	Nombre minimum de caractères minuscules dans le mot de passe, de 0 à 10.
Caractère(s) numérique(s) minimum	Nombre minimum de caractères dans le mot de passe, de 0 à 10.
Caractère(s) spécial(ux) minimum	Nombre minimum de caractères spéciaux dans le mot de passe, de 0 à 10.
Caractères spéciaux inclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, si vous saisissez « $, ! », les utilisateurs peuvent uniquement utiliser « $ » et « ! » comme caractères spéciaux dans le mot de passe. Aucun autre caractère spécial ne peut être utilisé et un mot de passe avec d'autres caractères spéciaux n'est pas autorisé.
Caractères spéciaux exclus	Autorisez un ensemble restreint de caractères spéciaux sans aucun délimiteur. Par exemple, lorsque « @$! » est saisi, les caractères spéciaux que ne peuvent pas inclure les utilisateurs dans leurs mots de passe sont « @ », « $ » et « ! ». **Remarque :** Cette option est disponible si la propriété glide.password_policy.use_excluded_special_char est activée.
Interdire les données utilisateur	Cela est activé pour interdire les données utilisateur.

6. Dans la section Correspondance de la séquence, spécifiez le **seuil de longueur de séquence** et le **seuil de longueur de répétition**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le seuil de longueur de séquence et le seuil de longueur de répétition peuvent tous deux comporter un maximum de huit caractères. Ces champs vous permettent de restreindre les combinaisons faibles de mots de passe ayant des séquences prévisibles et répétitives telles que « 123456 », « qwerty », « !@#$%^ », « aaaaa », etc.
- Pour **Fort par défaut**, la longueur du seuil de longueur de séquence et du seuil de longueur de répétition est sélectionnée sous la forme de quatre caractères.

7. Dans la section **Tester votre mot de passe** , spécifiez votre mot de passe.
8. Cliquez sur **Tester votre mot de passe**.
9. Une fois le mot de passe valide, cliquez sur **Envoyer** pour soumettre le mot de passe.

Remarque :
Testez toujours votre mot de passe avant de soumettre.

Configurer le mot de passe pour un utilisateur

Définissez le mot de passe de vos utilisateurs pour l'instance en fonction de la politique de mot de passe configurée.

Avant de commencer
Utilisateurs créés pour définir le mot de passe pour leur première connexion. Pour plus d'informations, consultez Créer un utilisateur .

Pour renseigner le champ **Mot de passe** directement sur le formulaire utilisateur, activez **l'option Activer pour afficher le champ Mot de passe sur le formulaire sys_user** (glide.user.show.password.field). Pour en savoir plus sur les propriétés, reportez-vous à la section Propriétés de la politique de mot de passe.

Rôle requis : administrateur

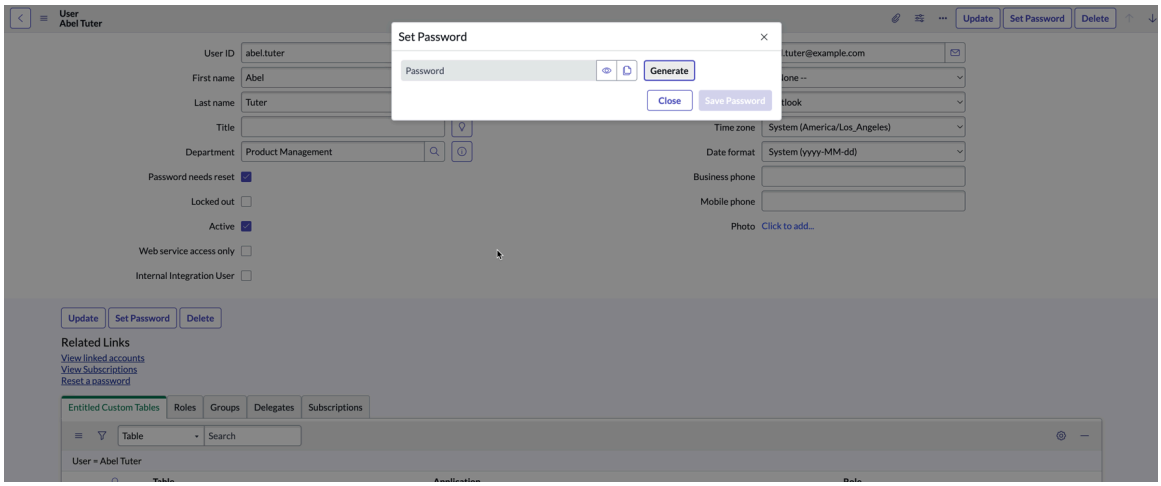
Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs**.
2. Sélectionnez un utilisateur dans la liste de la page Utilisateurs.
3. Pour définir le mot de passe en fonction de la politique de mot de passe, cliquez sur **Définir le mot de passe**.

   La fenêtre contextuelle Définir le mot de passe s'affiche.

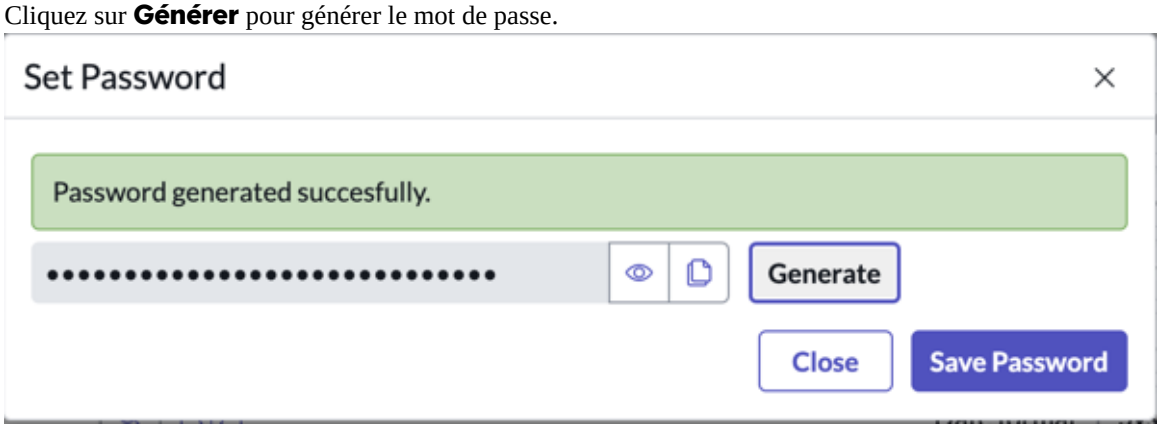
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

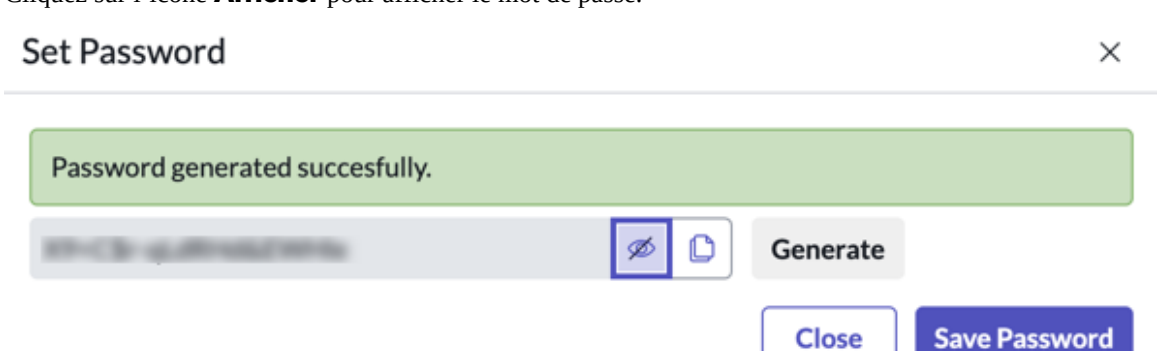


4. Dans Définir le mot de passe, procédez comme suit.

a. Cliquez sur **Générer** pour générer le mot de passe.



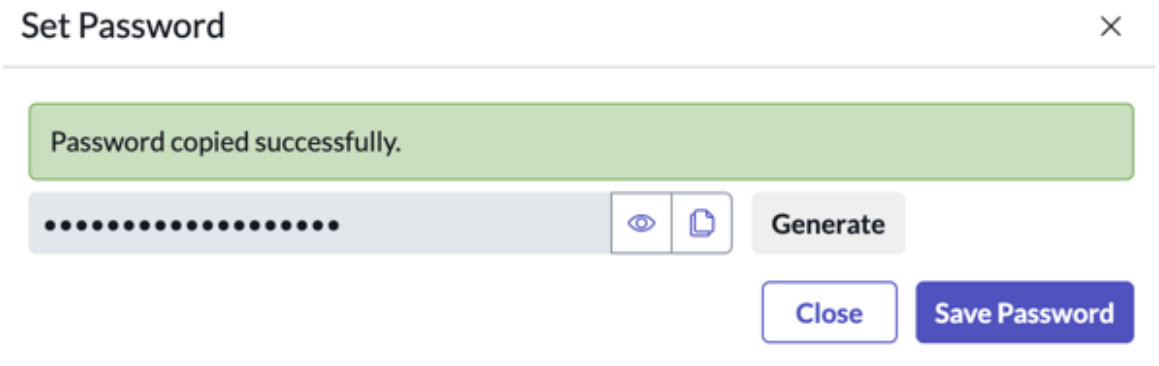
b. Cliquez sur l'icône **Afficher** pour afficher le mot de passe.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Cliquez sur l'icône **Copier** pour copier le mot de passe et le partager avec l'utilisateur.



5. Cliquez sur **Enregistrer le mot de passe**.

   Le mot de passe est défini pour l'utilisateur. De plus, la case Le mot de passe doit reposer est automatiquement activée.

   Lors de la première connexion, l'utilisateur doit utiliser le même mot de passe pour se connecter et changer le mot de passe lors de la connexion, conformément à la politique de mot de passe configurée par les administrateurs.

Exclure les mots de passe via des politiques de mot de passe sur votre instance

Ajoutez des mots de passe à la table Mot de passe exclu pour interdire l'utilisation de mots de passe spécifiques par les utilisateurs sur votre instance.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Vous pouvez interdire autant de mots de passe que nécessaire. En voici quelques exemples :

- Séquences prévisibles et répétitives, telles que « 123456 », « qwerty », « !@#$%^ », « aaaaa », etc.
- Nom de l'employé ou noms d'utilisateur.
- Noms de marques ou de produits pertinents.
- Emplacements, tels que le siège social d'une société, la ville, le pays, etc.
- Termes internes ou abréviations spécifiques à l'entreprise.
- Des émojis.

Procédure

1. Accédez à la **Tout** > **Politique de mot de passe** > **Mots de passe exclus**.
2. Pour ajouter un mot de passe à votre liste d'exclusion, cliquez sur **Nouveau** et saisissez le mot de passe.
3. Accédez à la **Politique de mot de passe** > **Gestion de la liste d'exclusion** pour régir le mot de passe de vos utilisateurs et empêcher les utilisateurs d'utiliser un mot de passe incorrect pour l'instance.

   La **gestion de la liste d'exclusion** contient environ 5000 mots de passe couramment utilisés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Caractères de mot de passe non pris en charge

Certains caractères de mot de passe ne sont pas pris en charge. Les utilisateurs ne peuvent pas utiliser ces caractères en raison des exigences de complexité du ServiceNow mot de passe.

Pour activer un environnement réseau sécurisé, il est nécessaire que les utilisateurs utilisent des mots de passe forts qui incluent une combinaison de lettres, de chiffres et de symboles. Ces combinaisons permettent d'empêcher les utilisateurs non autorisés qui utilisent généralement des méthodes manuelles ou automatisées de deviner des mots de passe faibles.

- Les exigences de la politique de mot de passe sont basées sur le plan multilingue de base (BMP) qui contient des caractères pour toutes les langues modernes. ServiceNow est livrée avec des BMP d'environ 10 000 caractères.
- Vous pouvez définir des caractères de mot de passe dans ces BMP autorisés, mais les caractères de mot de passe qui n'adhèrent pas à ces BMP ne sont pas autorisés.

Remarque :
Les caractères spécifiques à l'utilisateur ou à la société qui ne peuvent pas être utilisés dans le mot de passe peuvent être configurés dans la liste Exclure le mot de passe.

Pour plus d'informations sur les propriétés de la politique de mot de passe, consultez Propriétés de la politique de mot de passe.

Réinitialisation du mot de passe

Le processus en libre-service Réinitialisation du mot de passe par défaut permet à un utilisateur de réinitialiser le mot de passe sans l'aide d'agents du centre de services.

Example: Flux de réinitialisation du mot de passe en libre-service par défaut

1. Si un utilisateur a oublié le mot de passe, il peut cliquer sur le lien **Mot de passe oublié ? sur** l'écran de connexion.
2. L'application Réinitialisation du mot de passe démarre. Sur la page **Identité** , l'utilisateur s'identifie en saisissant un **nom d'utilisateur**.
3. Sur la page **Vérifier** , l'utilisateur prouve qu'il est bien la personne associée au nom d'utilisateur. Dans cet exemple, l'utilisateur saisit l'adresse e-mail associée au profil d'utilisateur. L'administrateur peut configurer une méthode de vérification différente ou exiger des vérifications supplémentaires, par exemple, une question personnelle à laquelle seul l'utilisateur peut répondre.
4. La page **Réinitialiser** indique à l'utilisateur de vérifier ses e-mails pour obtenir des instructions.
5. L'utilisateur ouvre l'e-mail et clique sur le lien **ici** pour réinitialiser le mot de passe. Le lien est valide pour une période que vous spécifiez (utilisez la propriété**password_reset.request.expiry**).
6. La page **Réinitialiser le mot de passe** guide l'utilisateur dans la réinitialisation du mot de passe.

Le processus en libre-service Réinitialisation du mot de passe (`com.glideapp.password_reset`) par défaut définit les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- L'URI qui spécifie où les utilisateurs sont redirigés lorsqu'ils cliquent sur **Mot de passe oublié ?**. Par défaut, cette valeur est **/$pwd_reset.do ?sysparm_url=ss_default**, qui est la même valeur que celle utilisée dans la `glide.security.password_reset.uri` propriété. Dans les versions précédentes, cette valeur était définie sur **/reset_password.do**.
- L'option **Activer l'URL de réinitialisation du mot de passe** , qui précise que l'utilisateur doit recevoir un e-mail contenant un lien pour réinitialiser son mot de passe après avoir cliqué sur **Mot de passe oublié ?**.
- Le flux de vérification Données personnelles - Saisir l'adresse e-mail qui spécifie le flux de réinitialisation du mot de passe en trois étapes.

Consultez Configurer votre processus de réinitialisation du mot de passe pour obtenir des instructions sur l'accès à ce formulaire et la configuration des champs.

Remarque :

- Cette fonctionnalité fonctionne pour les utilisateurs authentifiés localement qui saisissent le nom d'utilisateur et le mot de passe spécifiés dans leur enregistrement utilisateur. Les utilisateurs qui se connectent à l'instance via une solution SSO ou une intégration LDAP ne peuvent pas réinitialiser les mots de passe à l'aide de l'exemple de processus en libre-service Réinitialisation du mot de passe .
- L'utilisateur final doit activer et configurer les préférences de notification. Reportez-vous à la section Notifications basées sur l'abonnement . Les administrateurs peuventx modifier l'e-mail qui est envoyé à l'utilisateur final.

Modifier le texte de l'e-mail de Réinitialisation du mot de passe notification

Les utilisateurs du processus en libre-service Réinitialisation du mot de passe reçoivent une notification par e-mail lorsqu'ils demandent la réinitialisation du mot de passe. Vous pouvez modifier le texte de l'e-mail et d'autres aspects de la notification.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Ce processus n'est pertinent que si les utilisateurs sont des notifications basées sur un abonnement .

Procédure

1. Accédez à la **Tout** > **Notification système** > **Notifications**.
2. Sélectionnez la notification **par URL de réinitialisation du mot de passe** .
3. Modifiez le texte de l'e-mail dans la section **Ce qu'il contiendra** .
   Pour plus d'informations sur la configuration d'autres aspects de la notification, consultez Créer une notification par e-mail .

Configuration des Réinitialisation du mot de passe propriétés

Vous pouvez spécifier des propriétés qui configurent l'expérience pour les Réinitialisation du mot de passe utilisateurs finaux.

Avant de commencer

Rôle requis : password_reset_admin

Pourquoi et quand exécuter cette tâche

Bien qu'il n'existe aucune limite de plage pour les valeurs que vous pouvez entrer pour les propriétés, envisagez d'utiliser uniquement des valeurs entières positives à partir de 1.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque vous déterminez la limite de la plage supérieure d'une propriété, tenez compte de la tâche que l'utilisateur effectue.

Par exemple, vous ne voudriez pas autoriser 100 tentatives aux utilisateurs pour vérifier leur identité. Une valeur plus courante est 3 tentatives. De même, vous ne voudrez peut-être pas forcer les utilisateurs qui terminent le processus d'inscription à passer du temps à sélectionner et à répondre à 30 questions de sécurité. Le nombre de questions de sécurité le plus couramment utilisé se situe entre 5 et 7.

Procédure

1. Accédez à la **Tout** > **Réinitialisation du mot de passe** > **Propriétés**.
   Pour plus d'informations sur les Réinitialisation du mot de passe propriétés, voir Réinitialisation du mot de passe Propriétés globales .
2. Mettez à jour les paramètres selon vos besoins, puis cliquez sur **Enregistrer**.

Mémoriser mon nom

Lorsque la case **à cocher Se souvenir de moi** est cochée lors de la connexion, un cookie est stocké sur l'ordinateur de l'utilisateur. Ce cookie authentifie automatiquement l'utilisateur lors de visites ultérieures.

Si l'utilisateur se déconnecte, le cookie est détruit. La valeur par défaut de la case à cocher **Se souvenir de moi** est contrôlée par une propriété, et l'apparition ou non de la case à cocher sur la page de connexion est contrôlée par une propriété différente.

Deux propriétés, `glide.ui.user_cookie.life_span_in_days` et `glide.ui.user_cookie.max_life_span_in_days` contrôler la valeur d'expiration du cookie générée par le système glide_user. Lorsqu'un utilisateur accède à une instance avec l'option « Se souvenir de moi » activée, l'accès réinitialise la période d'expiration du cookie jusqu'à ce que la limite de durée de vie maximale (glide.ui.user_cookie.max_life_span_in_days) soit atteinte.

Remarque :
Pour en savoir plus sur ces propriétés, consultez les rubriques suivantes dans Paramètres de renforcement de la sécurité de l'instance :

- Délai absolu de la session
- Délai d'expiration de la fenêtre de session

Modifier la valeur par défaut de la case à cocher Se souvenir de moi

Vous pouvez modifier la valeur par défaut de la case à cocher **Se souvenir de moi** .

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Propriétés de l'interface utilisateur**.
2. Localisez la `Default value of "Remember me" checkbox on login page` propriété (`glide.ui.remember.me.default`).
3. Pour définir la valeur par défaut de la case à cocher **Se souvenir de moi** sur **Non**, décochez la case de propriété.
4. Pour restaurer la valeur par défaut de la case à cocher **Se souvenir de moi** sur **Oui**, cochez la case de propriété.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Supprimer la case à cocher Se souvenir de moi

Vous pouvez supprimer la case à cocher **Se souvenir de moi** afin que les utilisateurs n'aient pas accès à cette fonctionnalité.

Avant de commencer
Rôle requis : security_admin

Remarque :
Pour en savoir plus sur cette propriété, reportez-vous Supprimer Se souvenir de moi à la section Paramètres de sécurisation renforcée de la sécurité de l'instance.

Procédure

1. Élevez votre rôle à security_admin.
2. Accédez à la **Propriétés système** > **Propriétés de l'interface utilisateur**.
3. Localisez la *`Remove "Remember me" checkbox from login page`* propriété (*`glide.ui.forgetme`*).
4. Cochez la case de la propriété.
   Ce paramètre supprime la case à cocher **Se souvenir de moi** , invalide les cookies existants et désactive entièrement la fonctionnalité Se souvenir de moi.
5. Pour restaurer la case à cocher **Se souvenir de moi** sur la page de connexion, décochez la case de propriété.

Configuration de l'invite de confirmation de déconnexion

Vous pouvez activer une invite de confirmation de déconnexion pour empêcher les utilisateurs de se déconnecter par inadvertance.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Remarque :
La procédure suivante ne fonctionne que dans les versions d'interface utilisateur antérieures à Interface utilisateur principale, qui est la plus récente et la plus couramment utilisée.

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Système**.
2. Localisez la propriété **Inviter l'utilisateur à confirmer une demande de déconnexion** et cochez la case.
3. Lorsque l'utilisateur clique sur le bouton **Déconnexion** , une boîte de dialogue de confirmation s'affiche.

Implémentation d'une valeur de circonstance

Vous pouvez implémenter un nonce à utiliser avec l'authentification Synthèse d'authentification unique.

Pour utiliser un nonce avec les méthodes de jeton non chiffré ou de jeton chiffré de l'authentification unique, ces étapes s'appliquent avec seulement quelques modifications mineures.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
La valeur de circonstance n'est utilisée que pour les demandes de connexion, et non pour tout autre type de demande. Si le système reçoit une valeur de valeur de circonstance après la connexion, la valeur de circonstance n'est pas consommée.

Avantages

L'utilisation d'un caractère de circonstance empêche un utilisateur malveillant d'effectuer une attaque par relecture afin de se connecter à votre système.

Flux de processus de valeur de circonstance

Lorsqu'un client a implémenté le jeton digéré Single Sign-on et souhaite ajouter la sécurité d'une nonce, il suit un certain flux de processus.

1. Un utilisateur se connecte au portail du client.
2. Le client génère les paramètres SSO requis et ajoute une valeur de circonstance aléatoire à la fin. Par exemple, si le client transmet la réponse d'authentification via la chaîne de requête, elle peut ressembler à ceci :

```
SM_USER=itil&DE_USER=V1QuWMmxSfBgfRS099X0cAjKo5Q=&NONCE=1407743018
```

L'instance reçoit cette demande et récupère les variables d'authentification. Avant d'essayer de vérifier l'intégrité de la réponse d'authentification, l'instance vérifie le nonce par rapport à une table interne (u_authentication_nonce) pour vérifier qu'il n'existe pas encore. Si la valeur de circonstance n'existe pas dans cette table, elle est ajoutée à la table et le processus d'authentification peut se poursuivre. Toutefois, si cette valeur de valeur de circonstance existe déjà dans la table, la tentative d'authentification est annulée et un code d'erreur de `failed_missing_requirement` est renvoyé, ce qui ramène généralement l'utilisateur à la page de connexion.

Implémenter un nonce

Ajoutez un nonce de chiffrement à l'en-tête d'authentification pour vous assurer qu'il ne peut être utilisé qu'une seule fois.

- Créez une propriété système appelée *`glide.authenticate.header.nonce_key`* et définissez sa valeur sur le nom de variable que vous utilisez pour le nonce, tel que NONCE ou NCE.
- Créez une table appelée `u_authentication_nonce`. Ajoutez un champ appelé `u_nonce` à la table.
- Accéder à **Propriétés système** > **Sorties d'installation** et créez un élément appelé DigestSingleSignOnNonce qui remplace ExternalAuthentication (*`glide.authenticate.external_property`*).
- Ajoutez le code suivant à la portion de script de DigestSingleSignOnNonce nouvellement créé.

```
gs.include("PrototypeServer");

var DigestSingleSignOnNonce = Class.create();
DigestSingleSignOnNonce.prototype = {

 process : function() {

 var headerKey = GlideProperties.get("glide.authenticate.header.key", "SM_USER");
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 var headerDigestKey = GlideProperties.get("glide.authenticate.header.encrypted_key",
"DIGEST");
 var headerNonceKey = GlideProperties.get("glide.authenticate.header.nonce_key", "NCE");
 var fieldName = GlideProperties.get("glide.authenticate.header.value", "user_name");
 var fkey = GlideProperties.get("glide.authenticate.secret_key");

 // Look in the Headers
 var data = request.getHeader(headerKey);
 var encdata = request.getHeader(headerDigestKey);
 var nonce = request.getHeader(headerNonceKey);

 // If not, then check the URL Parameters
 if (data == null || encdata == null || nonce == null) {
  data = request.getParameter(headerKey);
  encdata = request.getParameter(headerDigestKey);
  nonce = request.getParameter(headerNonceKey);
 }

 // then maybe its a cookie
 if (data == null || encdata == null || nonce == null) {
  var cookies = request.getCookies();
  data = GlideCookieMan.getCookieValue(cookies, headerKey);
  encdata = GlideCookieMan.getCookieValue(cookies, headerDigestKey);
  nonce = GlideCookieMan.getCookieValue(cookies, headerNonceKey);
 }

 // if found run encryption
 if (data != null && encdata != null && nonce != null) {
  try {

   // Replace all spaces with plus(+)'s, converted in url
   encdata = encdata.replaceAll(' ', '+');

   // ----- Encrypt the username|nonce
   var key = this.getDigest( data + "|" + nonce, fkey);

   // Check for match of received encoded data
   // and your encoding of user name
   if (encdata == key) {
    var ugr = new GlideRecord("sys_user");
    ugr.initialize();
    if (!ugr.isValidField(fieldName)) {
     GlideLog.warn("External authorization is set to use field: '"+ fieldName + "' which doesn't
exist");
     return "failed_missing_requirement";
    }
    ugr.addQuery(fieldName, data);
    ugr.query();
    if (!ugr.next()) {
     var userLoad = GlideUser.getUser(data);
     if (userLoad == null)
      return "failed_authentication";

     ugr.initialize();
     ugr.addQuery(fieldName, data);
     ugr.query();
     if (!ugr.next())
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
      return "failed_authentication";

    }

    if (this.processNonce(nonce)){
     var userName = ugr.getValue("user_name");
     return userName;
    }
    else return "failed_missing_requirement";
    }
   else {

    return "failed_authentication";
   }
  } catch(e) {
   gs.log(e);
   return "failed_authentication";
  }
  // Encoded data didn't match recieved Encoded data
 } else {

  return "failed_missing_requirement";
 }
},

getDigest : function( data, fkey ) {
 try {
  // default to something JDK 1.4 has
  var MAC_ALG = "HmacSHA1";
  return SncAuthentication.encode(data, fkey, MAC_ALG);

 } catch (e) {
  gs.log(e.toString());
  throw 'failed_missing_requirement';
 }
} ,

processNonce : function( sentNonce ) {
 var ngr = new GlideRecord("u_authentication_nonce");

 ngr.addQuery("u_nonce", sentNonce);
 ngr.query();
 if (ngr.next()) {
  gs.log("This SSO entry has already been processed! (Nonce: " + sentNonce + ")");
  return false;
 }
 var ngrNew = new GlideRecord("u_authentication_nonce");
 ngrNew.initialize();
 ngrNew.u_nonce = sentNonce;
 ngrNew.insert();
 gs.log("Inserted new nonce: " + sentNonce);
 return true;
}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
};
```

- Une fois que vous avez enregistré votre nouvelle sortie d'installation, accédez à la sortie d'installation de DigestSingleSignOn et assurez-vous qu'elle est définie sur Active = false.

Votre instance doit maintenant être configurée pour implémenter un nonce.

Authentification multifacteur (MFA)

Découvrez comment activer et configurer l'authentification multifacteur.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de la MFA.

Activer



Découvrez comment activer l'authentification multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utiliser



Configurez et utilisez l’authentification multifacteur.

MFA avec authentification unique (SSO)



Découvrez comment configurer l’authentification multifacteur avec authentification unique (SSO).

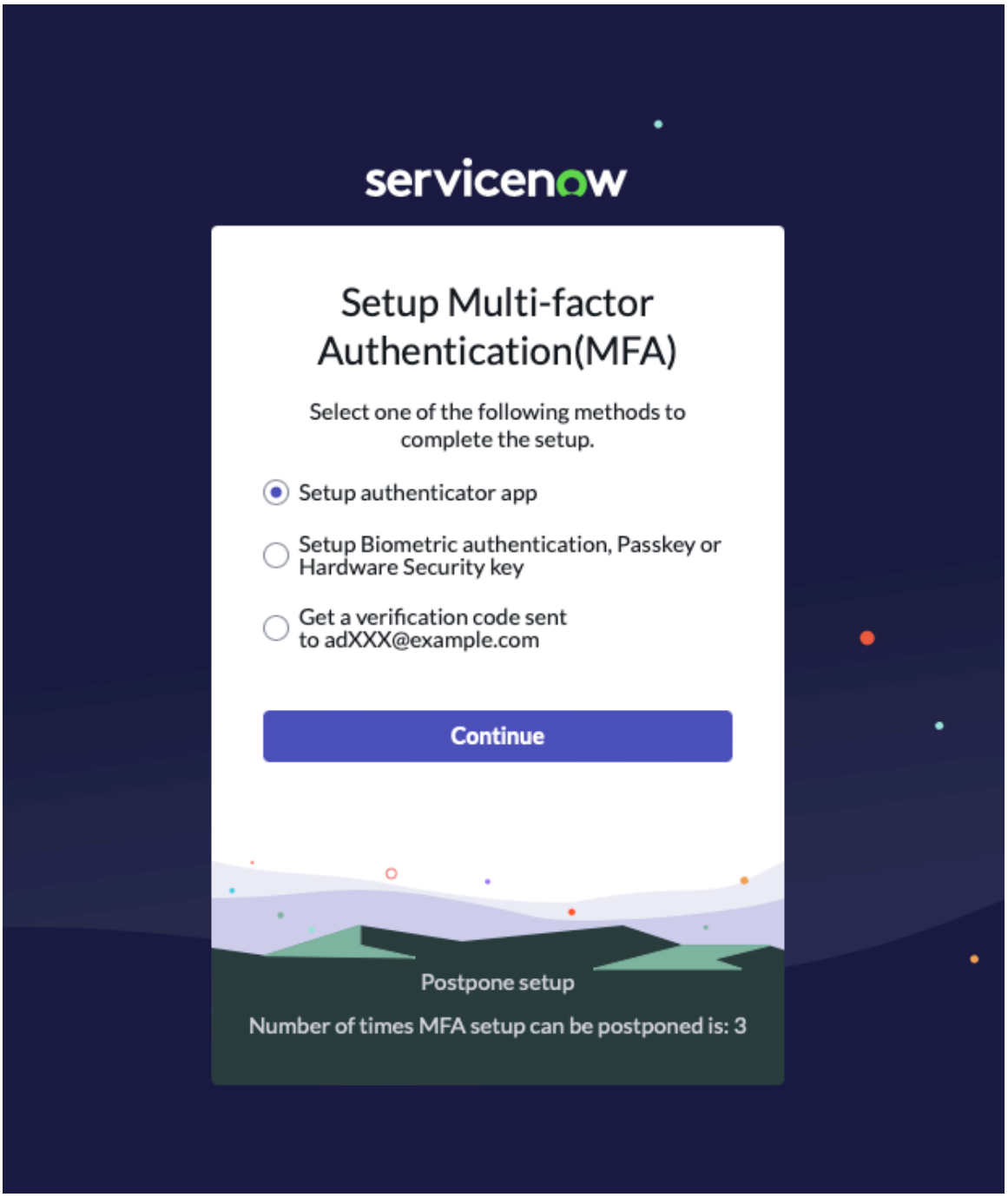
Explorer l’authentification multifacteur

L’authentification multifacteur (MFA) est une méthode d’authentification qui oblige les utilisateurs à fournir des informations autres que leurs informations d’identification de base.

ServiceNow fournit des options MFA telles que la configuration d’une application d’authentification, d’une clé biométrique, d’une clé d’accès ou d’une clé de sécurité matérielle, d’un SMS et d’un e-mail pour l’authentification. Vous pouvez utiliser l’authentificateur FIDO2, les clés d’accès, les authentificateurs biométriques et les clés de sécurité matérielles comme facteur d’authentification multifacteur (MFA) sans nécessiter la configuration d’une application d’authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Si l'utilisateur a terminé la configuration à l'aide d'un facteur, il peut toujours accéder à sa page de profil et terminer la configuration des facteurs restants.

Activer la MFA

Activez le module d'extension **Intégration - Authentification multifacteur** (com.snc.integration.multifactor.authentication) pour commencer à utiliser la MFA sur une instance. La MFA est activée par défaut sur ServiceNow.

Critère multifacteur

Utilisez des critères multifacteur pour déterminer quels utilisateurs et rôles doivent utiliser la vérification multifacteur en deux étapes. Vous pouvez utiliser l'un de ces critères ou une combinaison de ceux-ci en fonction des besoins de votre entreprise.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Critère multifacteur basé sur l'utilisateur

Utilisez des critères multifacteur basés sur l'utilisateur pour sélectionner les utilisateurs individuels qui doivent se connecter à l'aide de la MFA. Les administrateurs mettent à jour le champ **Activer l'authentification multifacteur** sur un enregistrement utilisateur pour activer ou désactiver les exigences MFA d'un utilisateur. Pour obtenir des détails sur ce processus, consultez Configurer les critères multifacteur basés sur l'utilisateur.

Critère multifacteur basé sur le rôle

Utilisez des critères multifacteur basés sur les rôles pour exiger une connexion MFA pour tous les utilisateurs affectés à un rôle spécifique. L'enregistrement **d'authentification multifacteur basée sur les rôles** de la table **Critères multifacteur** [multi_factor_criteria] contient la liste des rôles qui nécessitent une connexion MFA. Pour plus d'informations sur la gestion de cette liste, reportez-vous à la section Configurer les critères multifacteur basés sur les rôles.

Critères multifacteur basés sur une politique d'authentification adaptative

Utilisez l'authentification adaptative pour déterminer quand votre instance a besoin d'une authentification MFA. L'authentification adaptative utilise des politiques d'authentification pour évaluer des critères tels que l'adresse IP d'un utilisateur ou les groupes d'utilisateurs. Pour en savoir plus sur la fonctionnalité d'authentification adaptative, reportez-vous à la section Authentification adaptative.

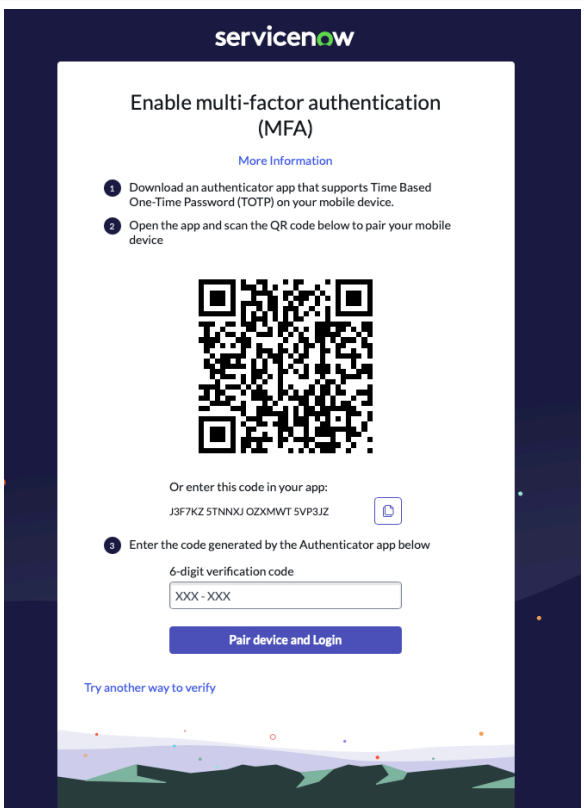
Méthodes d'authentification multifacteur

Les utilisateurs peuvent utiliser les options suivantes en plus de leur nom d'utilisateur et de leur mot de passe pour répondre aux exigences d'authentification multifacteur. Les utilisateurs peuvent configurer indépendamment des facteurs MFA tels que des applications d'authentification, des scanners biométriques, des clés matérielles et des SMS.

Applications d'authentification

Une application d'authentification est un logiciel tiers qui génère des codes d'accès temporaires. Les utilisateurs peuvent utiliser ces codes secrets pour se connecter à une instance qui nécessite l'authentification multifacteur (MFA). Pour plus d'informations sur ces applications, reportez-vous à la section Applications d'authentification.

Suivez les instructions à l'écran pour configurer l'application d'authentification.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scanners biométriques

Les authentificateurs biométriques utilisent les empreintes digitales ou la reconnaissance faciale pour identifier les utilisateurs. Vos utilisateurs peuvent utiliser ces authentificateurs sur leurs appareils dans le cadre du processus de connexion multifacteur. Pour plus d'informations sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.



Clés matérielles

Les clés matérielles sont des éléments physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour plus d'informations sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.



Traduction automatique

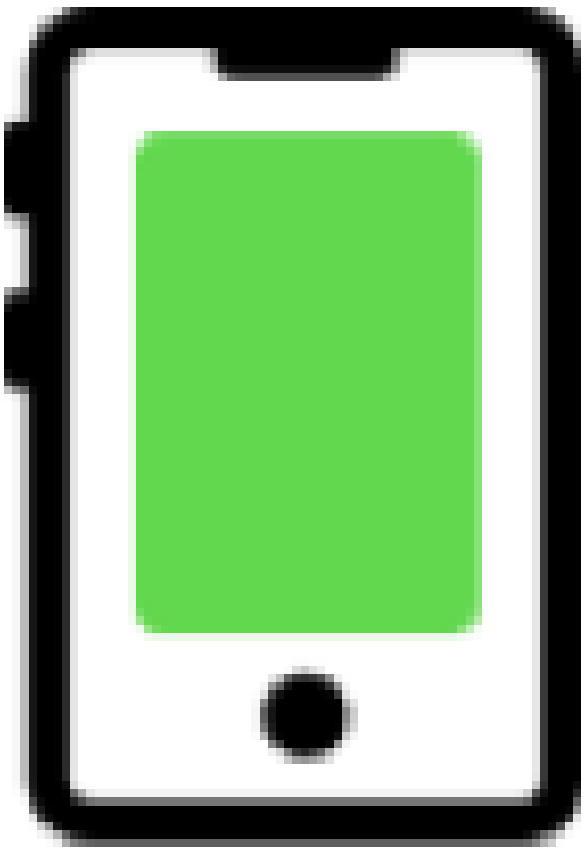
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

SMS

L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de se connecter à l’instance à l’aide d’un OTP basé sur un SMS.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un OTP SMS est envoyé au numéro de téléphone portable associé à l’enregistrement sys_user. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.

Pour plus d'informations, consultez Authentification multifacteur par SMS.



E-mail

L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de se connecter à l’instance à l’aide d’un OTP basé sur un e-mail.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un OTP e-mail est envoyé à l’adresse e-mail de l’utilisateur. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu’il a envoyé à l’adresse e-mail et vérifier leur identité.

Pour plus d'informations, consultez Authentification multifacteur par e-mail.



Propriétés de l'authentification multifacteur

Utilisez les propriétés d’authentification multifacteur pour activer, désactiver et configurer l’authentification MFA sur votre instance. Pour en savoir plus sur ces propriétés, reportez-vous à la section Propriétés système d’authentification multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration de l'authentification multifacteur, des méthodes prises en charge et du workflow

La MFA, également connue sous le nom de vérification en deux étapes, est une exigence de sécurité selon laquelle les utilisateurs doivent saisir plus d'un ensemble d'informations d'identification pour accéder à une instance.

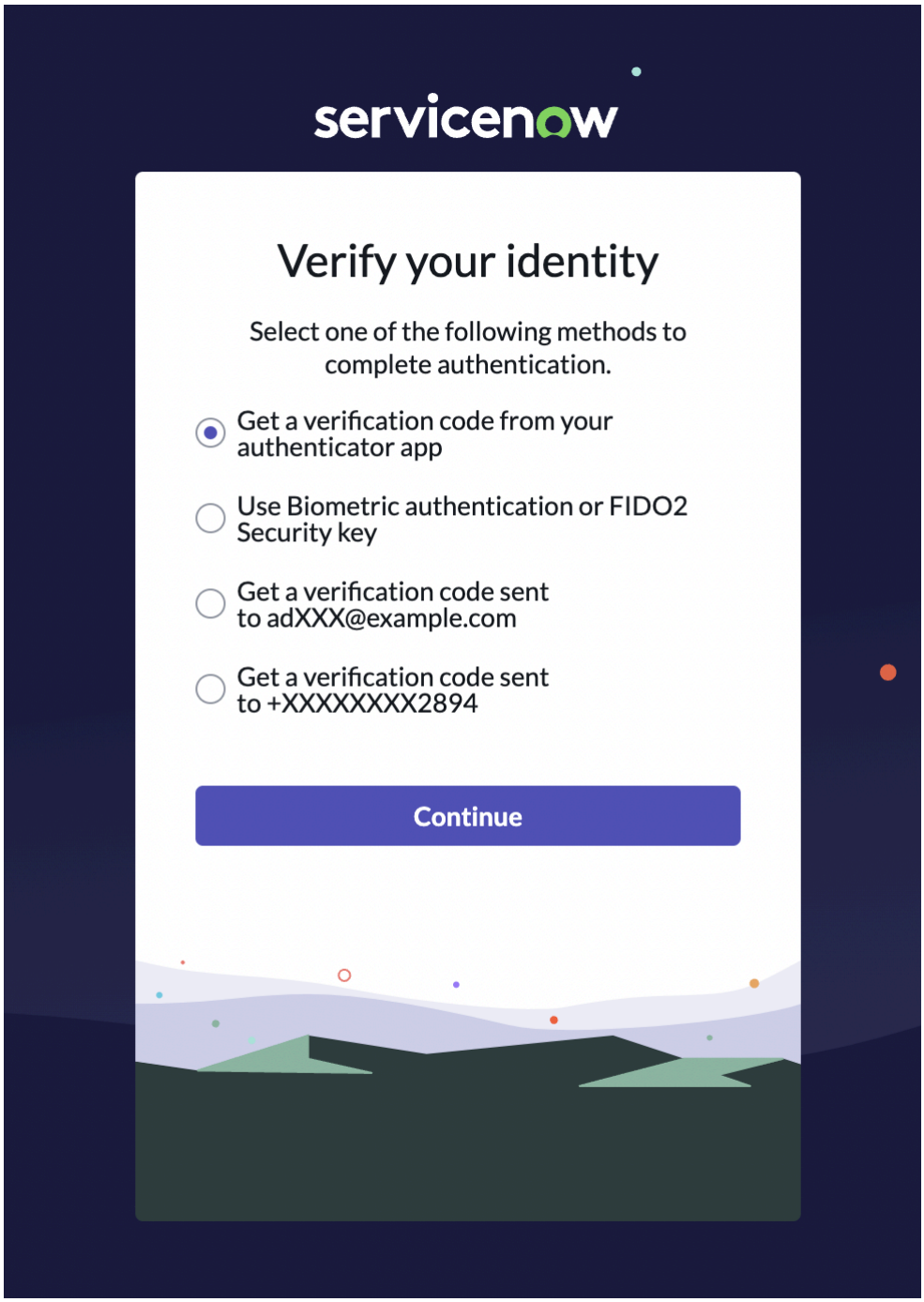
Le niveau d'authentification de base d'une instance est l'authentification de base de données locale où un utilisateur entre son nom d'utilisateur et son mot de passe. La MFA permet aux administrateurs et aux utilisateurs d'exiger un deuxième niveau d'authentification.

Le deuxième niveau d'authentification peut être basé sur les éléments suivants :

- Code d'accès d'une application d'authentification
- Une clé matérielle
- Un authentificateur biométrique, tel qu'un lecteur d'empreintes digitales ou la reconnaissance faciale.
- un SMS ou un e-mail

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

En tant qu'administrateur, vous pouvez configurer MFA pour des utilisateurs individuels ou pour tous les utilisateurs disposant d'un rôle spécifique. Vous pouvez également permettre à vos utilisateurs d'opter et d'utiliser la MFA.

Activation

Le *`Integration - Multifactor Authentication`* module d'extension (com.snc.integration.multifactor.authentication) est installé par défaut sur votre instance, mais il doit être activé par un administrateur à l'aide d'une propriété système. Pour plus de détails, voir Propriétés système d'authentification multifacteur.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Après avoir cloné une instance, vous devez réactiver la MFA sur l'instance clonée. Pour plus d'informations, consultez ces articles de la base de connaissances KB0657100 , KB0860689 , KB0825390 , KB0779908 , KB0717367 , KB0727991 .

Méthodes d'authentification prises en charge

Vous pouvez utiliser la MFA avec les méthodes d'authentification suivantes :

- Authentification de base de données locale (authentification native ServiceNow)
- Intégration LDAP
- SSO SAML
- SSO OIDC

Workflow de configuration de l'authentification multifacteur

L'administrateur active l'authentification multifacteur

Le module **d'extension Intégration - Authentification multifacteur** (com.snc.integration.multifactor.authentication) est activé par défaut sur votre instance. Pour commencer à utiliser la MFA, les administrateurs doivent activer la MFA à l'aide d'une propriété système. Une fois activé, les administrateurs sélectionnent les utilisateurs ou les rôles qui nécessitent des connexions MFA.

Pour plus d'informations sur la configuration de l'administrateur pour MFA, reportez-vous à la section Authentification multifacteur (MFA).

Les utilisateurs se connectent à l'aide d'une application d'authentification

Les utilisateurs sont invités à utiliser les options MFA pour se connecter. Les utilisateurs peuvent choisir l'une des options pour terminer la MFA et si un utilisateur a terminé la configuration à l'aide d'un facteur, il peut toujours accéder à sa page de profil et terminer la configuration des facteurs restants s'il le souhaite.

Authentification Web

Activez *`Integration - Web Authentication`* (com.snc.integration.webauthn) pour autoriser l'authentification par clé matérielle ou par lecteur biométrique sur votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les clés matérielles sont des éléments physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour plus d'informations sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.



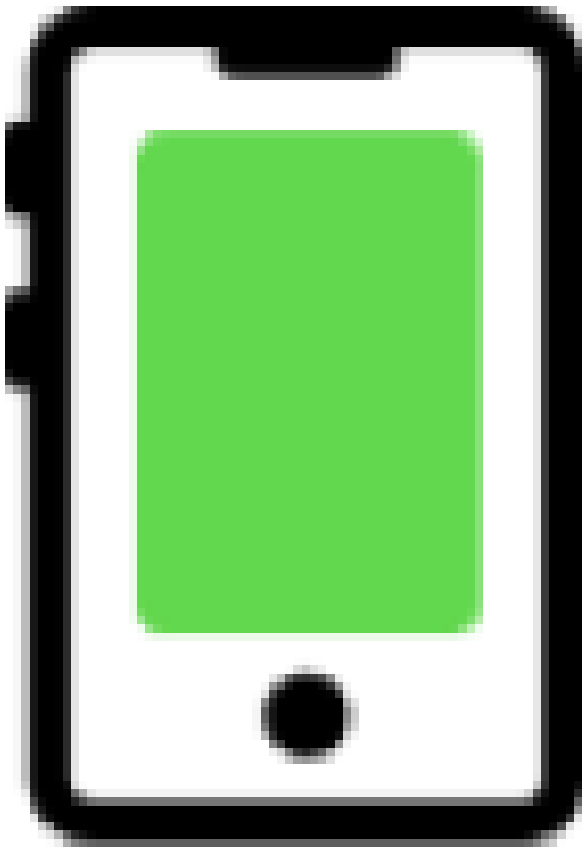
Les authentificateurs biométriques utilisent les empreintes digitales ou la reconnaissance faciale pour identifier les utilisateurs. Vos utilisateurs peuvent utiliser ces authentificateurs sur leurs appareils dans le cadre du processus de connexion multifacteur. Pour plus d'informations sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Traduction automatique

SMS ou e-mail (mot de passe à usage unique)

Pour permettre aux utilisateurs de se connecter à une instance et de profiter d'une ServiceNow expérience plus fluide lors de leurs déplacements, la MFA est prise en charge par SMS et par e-mail.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de se connecter à l’instance à l’aide d’un OTP basé sur un SMS.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par SMS est envoyé au numéro de téléphone mobile associé à l'enregistrement sys_user. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.

Pour plus d'informations, consultez Authentification multifacteur par SMS.



L’administrateur peut configurer ServiceNow l’instance pour exiger des utilisateurs qui tentent de se connecter à l’instance à l’aide d’un OTP basé sur un e-mail.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par e-mail est envoyé à l'adresse e-mail associée à l'utilisateur. L’utilisateur peut saisir le code de vérification à six chiffres qu’il a envoyé à l’adresse e-mail et vérifier son identité.

Pour plus d'informations, consultez Authentification multifacteur par e-mail.

Propriétés système d’authentification multifacteur

Utilisez les propriétés système pour activer et personnaliser l’authentification multifacteur afin de répondre à vos exigences de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de l'authentification multifacteur

Propriété	Description
Activer l'authentification multifacteur (*glide.authenticate.multifactor*)	Option qui permet aux utilisateurs et aux administrateurs d'utiliser cette fonctionnalité. Cette option est activée par défaut. Pour en savoir plus sur cette propriété, reportez-vous Activer l'authentification multifacteur (MFA) à la section Paramètres de sécurisation renforcée de la sécurité de l'instance.
Nombre de fois qu'un utilisateur peut contourner l'authentification multifacteur (*glide.authenticate.multifactor.setup.bypass.count*)	Nombre de fois qu'un utilisateur peut choisir d'ignorer la configuration de la MFA. Vos utilisateurs peuvent toujours se connecter à l'instance même s'ils n'ont pas leur appareil mobile avec eux. Si vous désactivez cette fonctionnalité, puis que vous la réactivez, le compteur est réinitialisé. La valeur par défaut est 3.
Durée, en minutes, pendant laquelle le code à usage unique envoyé à l'adresse e-mail de l'utilisateur est valide (*glide.multifactor.onetime.code.validity*)	Nombre de minutes pendant lesquelles le code de réinitialisation est valide. Consultez Connectez-vous avec l'authentification multifacteur. La valeur par défaut est 5. **Remarque :** Cette propriété est destinée au temps de validation du mot de passe à usage unique de l'e-mail.
Temps supplémentaire, en secondes, pendant lequel le code est valide pour tenir compte du décalage d'horloge. La valeur maximale est de 60 secondes. (*glide.authenticate.multifactor.clock_skew*)	Nombre de secondes supplémentaires pendant lesquelles le code de réinitialisation est valide. Le maximum est de 60. La valeur par défaut est 10. L'instance valide le code saisi par l'utilisateur par rapport au code unique généré par l'application qui est généré à l'heure actuelle. Vous pouvez décaler la fenêtre temporelle avec cette propriété et autoriser la génération d'un ou plusieurs codes au cours d'une fenêtre temporelle pour qu'ils soient considérés comme valides. La valeur de la propriété est utilisée dans le calcul suivant : heure actuelle - X/2 et heure actuelle + X/2, où X est la valeur de cette propriété. Si vous utilisez la valeur de 10, par exemple, l'instance considère que tous les codes générés par l'application dans la plage horaire [l'heure actuelle - 5 secondes] et [l'heureactuelle + 5 secondes] sont valides. Utilisez cette propriété pour éviter les problèmes de connexion lorsque l'utilisateur n'est pas en mesure d'entrer le code correct dans le temps imparti par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de l'authentification multifacteur (suite)

Propriété	Description
Activez la fonctionnalité Mémoriser le navigateur pour l'authentification multifacteur. (*glide.authenticate.multifactor.remember.browser.enable*)	Configurez votre instance pour inviter un utilisateur à utiliser MFA lorsqu'il se connecte à partir d'un nouvel appareil ou d'un nouveau navigateur. La valeur par défaut est oui.
Validité de l'empreinte digitale du navigateur en heures. (*glide.authenticate.multifactor.browser.fingerprint.validity*)	Une fois que MFA s'est souvenu du navigateur, l'utilisateur n'est pas confronté à la MFA dans le même navigateur pendant cette durée. La valeur par défaut est de 8 heures.
Nombre maximal de navigateurs dont un utilisateur peut se souvenir. (*glide.authenticate.multifactor.remembered.browser.max.count*)	Nombre de navigateurs dont MFA se souvient pour cet utilisateur.
Valeur par défaut de la case à cocher Mémoriser le navigateur dans la page multifacteur de validation. (*glide.authenticate.multifactor.remember.browser.default*)	Valeur par défaut de la case à cocher remember-browser dans la page multifacteur de validation.
Activez la MFA basée sur l'authentification Web (FIDO2). (*glide.webauthn.enabled*)	Option permettant d'activer les méthodes d'authentification sans mot de passe telles que la clé matérielle et l'authentification biométrique.
Activer l'OTP d'e-mail pour l'authentification multifacteur (*glide.authenticate.multifactor.email.otp.enable*	Option permettant d'activer l'OTP basé sur l'e-mail en tant que facteur pour MFA.
Activez l'interface utilisateur de configuration de l'authentification multifacteur (MFA) améliorée pour permettre aux utilisateurs de configurer le facteur indépendamment. *glide.auth.mfa.ui.v2.enabled*	Option permettant d'activer le facteur MFA de manière indépendante pour les utilisateurs sans configurer d'application d'authentification.

Critères d'authentification multifacteur

Utilisez des critères multifacteur pour déterminer quels utilisateurs et rôles doivent utiliser la vérification multifacteur en deux étapes.

Vous pouvez utiliser l'un de ces critères ou une combinaison de ceux-ci en fonction des besoins de votre entreprise.

Remarque :
Il est recommandé d'utiliser la MFA basée sur une politique d'authentification adaptative.

Critères d'authentification multifacteur

Critères	Description
Critère multifacteur basé sur l'utilisateur	Utilisez des critères multifacteur basés sur l'utilisateur pour sélectionner les utilisateurs individuels qui doivent se connecter à l'aide de la MFA. Les administrateurs mettent à jour le champ **Activer l'authentification multifacteur** sur un enregistrement utilisateur pour activer ou désactiver

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Critères d'authentification multifacteur (suite)

Critères	Description
	les exigences MFA d'un utilisateur. Pour obtenir des détails sur ce processus, consultez Configurer les critères multifacteur basés sur l'utilisateur.
Critère multifacteur basé sur le rôle	Utilisez des critères multifacteur basés sur les rôles pour exiger une connexion MFA pour tous les utilisateurs affectés à un rôle spécifique. L'enregistrement **d'authentification multifacteur basée sur les rôles** de la table **Critères multifacteur** [multi_factor_criteria] contient la liste des rôles qui nécessitent une connexion MFA. Pour plus d'informations sur la gestion de cette liste, reportez-vous à la section Configurer les critères multifacteur basés sur les rôles.
Critères multifacteur basés sur une politique d'authentification adaptative	Utilisez l'authentification adaptative pour déterminer quand votre instance a besoin d'une authentification MFA. L'authentification adaptative utilise des politiques d'authentification pour évaluer des critères tels que l'adresse IP d'un utilisateur ou les groupes d'utilisateurs. Pour en savoir plus sur la fonctionnalité d'authentification adaptative, reportez-vous à la section Authentification adaptative.

Configurer les critères multifacteur basés sur l'utilisateur

Utilisez des critères multifacteur basés sur l'utilisateur pour activer la MFA pour un utilisateur.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Administration utilisateurs** > **Utilisateurs**.
2. Configurez la liste pour afficher la colonne **Activer l'authentification multifacteur** .
3. Modifiez les valeurs de la colonne **Activer l'authentification multifacteur** pour les utilisateurs sélectionnés sur **vrai**.

   Lorsque l'utilisateur se connecte avec son nom d'utilisateur et son mot de passe, il est invité à configurer l'authentification multifacteur.

Configurer les critères multifacteur basés sur les rôles

Utilisez des critères multifacteur basés sur les rôles pour appliquer l'authentification multifacteur à tous les utilisateurs affectés à des rôles spécifiques.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Authentification multifacteur** > **Critère multifacteur**.
2. Dans la liste **Critères multifacteur** , ouvrez l'enregistrement **d'authentification multifacteur basée sur les rôles** .
3. Utilisez la liste **Rôles multifacteur** pour ajouter ou supprimer des rôles.

Option	Description
Ajouter un rôle	Double-cliquez sur **Insérer une nouvelle ligne...** et entrez ou sélectionnez un nom de rôle. Cliquez sur **l'icône Enregistrer** (icône) pour enregistrer l'entrée.
Supprimer un rôle	Cliquez sur l'icône de suppression ( ) pour supprimer un rôle de la liste.

4. Cliquez sur **Mettre à jour**.

Résultats

Votre instance applique l'authentification multifacteur à tous les utilisateurs qui sont membres des rôles répertoriés dans la liste **Rôles multifacteur** .

Important :
L'enregistrement doit être actif pour appliquer l'authentification multifacteur basée sur les rôles.

Configurer des critères multifacteur basés sur une politique d'authentification adaptative

Utilisez des politiques adaptatives pour déterminer quels utilisateurs doivent utiliser la vérification multifacteur (MFA) en deux étapes.

Avant de commencer

Rôle requis : administrateur

Remarque :

- Si la politique par défaut est Politique **de MFA ascendante**, les utilisateurs s'affichent avec l'authentification multifacteur si la politique configurée dans la **politique de MFA ascendante** est évaluée comme vrai. La politique a priorité sur la configuration basée sur l'utilisateur ou le rôle.
- MFA avec connexion SSO n'est disponible que si la propriété glide.authenticate.mfa.with.multisso.enabled est définie sur vrai.
- Vous pouvez accéder à l'enregistrement Politique d'authentification pour ajouter ou modifier les « entrées de politique » au champ de politique référencé (**Politique de MFA ascendante** ou **Politique de MFA descendante**).

Procédure

1. Accédez à la **Tout** > **Authentification Adaptative** > **Contextes de politique d'authentification** > **Contexte MFA**.
   L'enregistrement de contexte de politique de contexte MFA s'ouvre.
2. Sélectionnez la politique par défaut dans le champ **Politique par défaut** .
   Cette sélection détermine la façon dont votre instance utilise les conditions de politique pour déterminer si elle doit exiger la MFA.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

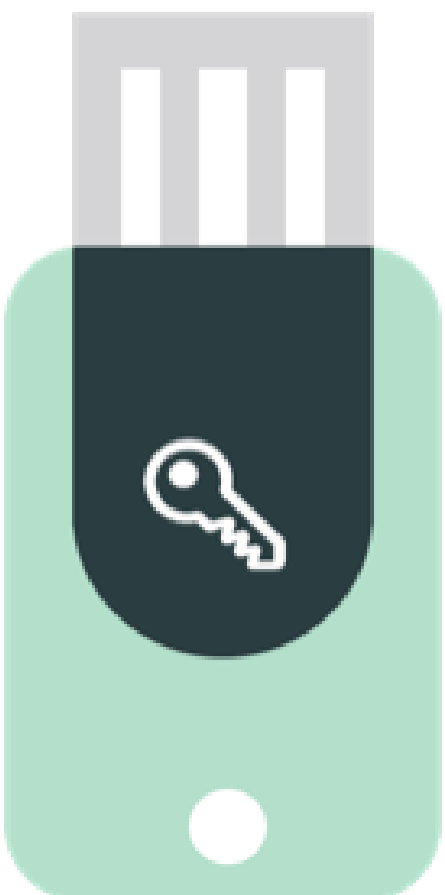
Politiques par défaut

Politique par défaut	Définition
Politique MFA ascendante	Sélectionnez cette option pour appliquer la MFA lorsque les conditions de politique définies dans la **politique de MFA donnent la** valeur vrai.
Politique MFA descendante	Sélectionnez cette option pour contourner la MFA lorsque les conditions de politique définies dans la **politique MFA descendante** sont évaluées comme vraies.

3. Dans le champ **Politique MFA ascendante** , sélectionnez une politique à utiliser dans ce contexte.
4. Cliquez sur **Mettre à jour**.
   Après avoir enregistré l'enregistrement, les listes **Entrée de politique** et **Conditions de politique** sont mises à jour pour afficher les entrées et conditions de politique associées à la politique sélectionnée dans le champ **Politique MFA ascendante** .

Authentification Web : MFA

Utilisez **l'intégration : authentification Web (com.snc.integration.webauthn)** pour autoriser l'authentification par clé matérielle ou par lecteur biométrique sur votre instance.



Les clés matérielles sont des éléments physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour plus d'informations sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les authentificateurs biométriques utilisent les empreintes digitales ou la reconnaissance faciale pour identifier les utilisateurs. Vos utilisateurs peuvent utiliser ces authentificateurs sur leurs appareils dans le cadre du processus de connexion multifacteur. Pour plus d'informations sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Configurer l'authentification multifacteur (MFA) avec la biométrie

Les administrateurs peuvent utiliser la liste Informations d'identification publiques de l'utilisateur pour afficher et gérer les informations d'identification créées par l'utilisateur.

Lorsqu'un utilisateur inscrit une application d'authentification, une authentification biométrique ou une clé matérielle, votre instance crée un enregistrement dans la table **Informations d'identification publiques de l'utilisateur**[sys_user_public_credential]. Utilisez cette table pour voir quels utilisateurs ont enregistré un authentificateur, ainsi que quels types, et quand ils ont été enregistrés et utilisés. Vous pouvez également marquer ces enregistrements comme inactifs pour empêcher les informations d'identification d'empêcher les utilisateurs d'utiliser ces informations d'identification.

Formulaire Informations d'identification publiques de l'utilisateur

Champ	Description
Pseudonyme des informations d'identification	Pseudonyme des informations d'identification. Ce pseudo est choisi par l'utilisateur lors de l'enregistrement d'un authentificateur.
Utilisateur	Utilisateur associé aux informations d'identification
Actif	Indique si les informations d'identification sont actives. Les administrateurs peuvent définir un enregistrement sur inactif pour empêcher un utilisateur de s'authentifier avec ces informations d'identification.
Authentificateur	Type d'authentificateur enregistré par l'utilisateur.
Heure d'inscription	Date et heure auxquelles l'utilisateur a créé ces informations d'identification
Heure de la dernière utilisation	Date et heure auxquelles l'utilisateur s'est connecté pour la dernière fois avec ces informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types d'authentificateur restreints

Si vous avez restreint une méthode d'authentification, comme les authentificateurs biométriques, les utilisateurs ne pourront pas créer d'informations d'identification de ce type. Toutefois, toutes les informations d'identification créées avant que vous n'ayez effectué cette restriction continueront de fonctionner. Vous pouvez désactiver les enregistrements de la table **Informations d'identification publiques de l'utilisateur** pour empêcher l'utilisation de ces informations d'identification une fois créées.

Options de configuration de l'authentificateur

Utilisez la page Configuration de l'authentificateur pour gérer les options d'authentificateur sur votre instance.

Accédez à la **Authentification multifacteur** > **Authentification Web** > **Configuration de l'authentificateur** pour afficher et modifier les options de configuration par défaut.

Formulaire Configuration de l'authentificateur

Champ	Description
Type d'authentificateur autorisé	Type d'authentificateurs autorisés à être enregistrés. Sélectionner à partir de : • **Les** authentificateurs de plateforme sont attachés ou intégrés à un appareil. Les lecteurs d'empreintes digitales ou la reconnaissance faciale disponibles sur les appareils mobiles (tels que Apple FaceID ou TouchID) entrent dans cette catégorie. • Les authentificateurs **itinérants** peuvent être supprimés d'un ordinateur ou d'un autre appareil client et utilisés ailleurs. Les clés matérielles entrent dans cette catégorie.
Type d'attestation	Définir la valeur sur direct ou indirect requiert l'importation des métadonnées d'authentificateur pour attester la provenance d'un authentificateur pendant l'enregistrement. • Aucun • Direct • Indirect
Auto-attestation de plateforme	Indique si l'auto-attestation est activée pour les authentificateurs de plateforme.
Auto-attestation entre plateformes	Indique si l'auto-attestation est activée pour les authentificateurs itinérants.
Vérification de l'utilisateur	Sélectionnez **Préféré** ou **Obligatoire**. Si nécessaire, le flux d'authentification Web invite les utilisateurs à effectuer une vérification à l'aide d'un code PIN ou biométrique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Configuration de l'authentificateur (suite)

Champ	Description
Vérifier la présence de l'utilisateur	Indique si le flux d'authentification Web nécessite la vérification de présence de l'utilisateur.
Clé de résident	Sélectionnez **Préféré** ou **Obligatoire**. Si nécessaire, l'authentificateur conserve les informations d'identification de clé publique dans le stockage de l'authentificateur.
Délai d'expiration (en ms)	Limite de temps maximale pour terminer l'enregistrement et l'authentification Web. Le temps est exprimé en millisecondes.

Authentification multifacteur par SMS

Authentification multifacteur (MFA) avec SMS comme facteur d'authentification.

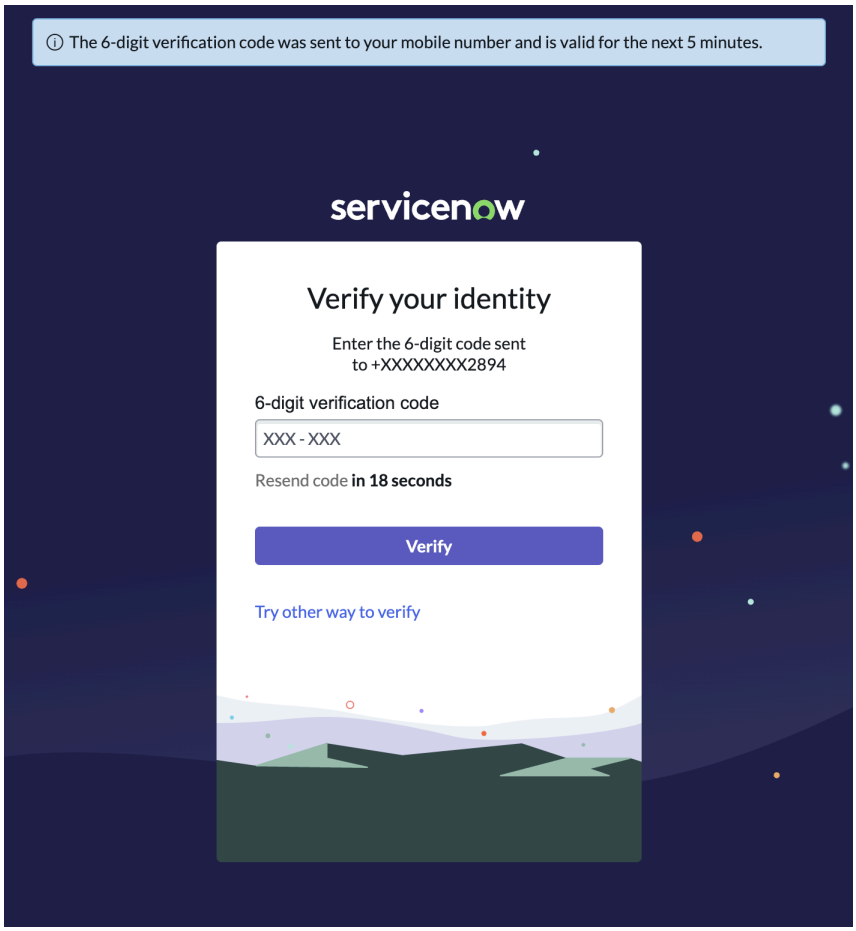
L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de se connecter à l'instance à l'aide d'un OTP basé sur un SMS.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par SMS est envoyé au numéro de téléphone mobile associé à l'enregistrement sys_user. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.

Vous pouvez également configurer l'authentification multifacteur avec SMS à l'aide du formulaire prêt à l'emploi Twilio . Pour plus d'informations, consultez Fournisseurs d'authentification multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



De plus, l'authentification multifacteur avec SMS peut être contrôlée en fonction de l'entrée et des conditions de la politique à l'aide de critères de filtrage. Les types de critères de filtre sont les suivants :

- Critère de filtre d'adresses IP
- Critère de filtre de rôle
- Critères de filtre de groupe

Activer le module d'extension MFA avec SMS

Pour MFA avec SMS, installez le module d'extension Multi-factor authentication with SMS (com.snc.authentication.sms_mfa).

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les éléments suivants sont installés avec l'authentification multifacteur par SMS :

- Authentification adaptative (com.snc.adaptive_authentication
- Notification - Pilote Twilio Direct (com.snc.notify.twilio_direct)

Module d'extension dépendant : Integration - Multifactor Authentication (com.snc.integration.multifactor.authentication)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez charger les données de démonstration lors de l'installation du module d'extension si vous configurez un fournisseur personnalisé pour la génération du SMS.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d'extension Multi-factor authentication with SMS (com.snc.authentication.sms_mfa).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Configurer SMS en tant que facteur MFA

Configurez l'entrée et la condition de politique pour afficher le mot de passe à usage unique du SMS en tant que politique de facteur MFA pour l'authentification.

Avant de commencer

Module d'extension requis : authentification multifacteur par SMS (com.snc.authentication.sms_mfa).

Rôle requis : administrateur

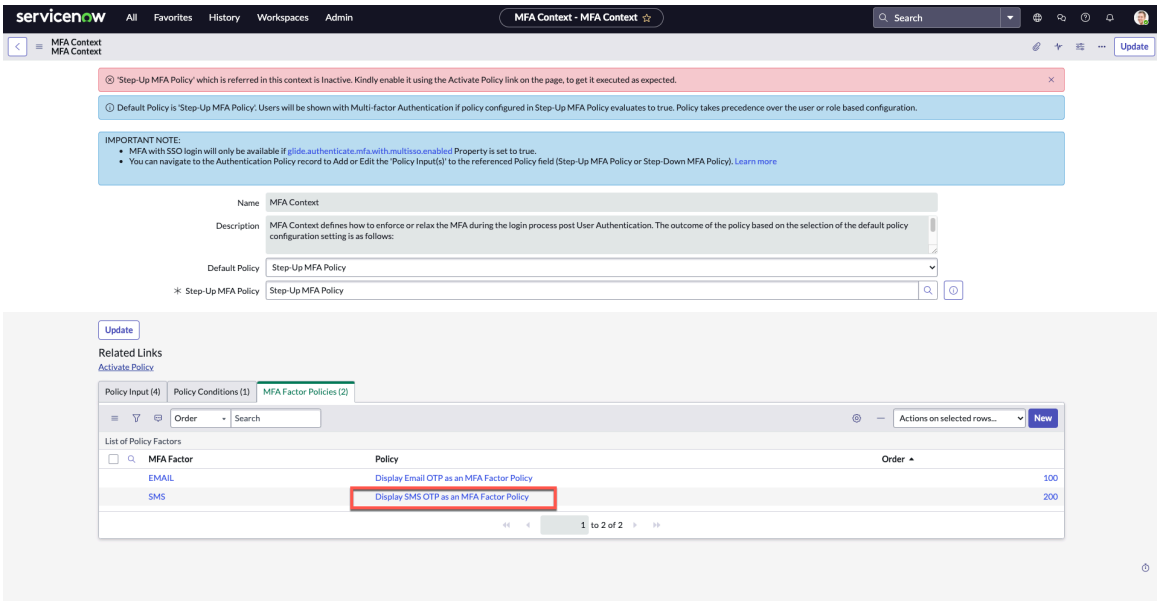
Remarque :
La politique de contexte MFA doit être évaluée comme vraie pour appliquer la politique de facteur SMS.

Procédure

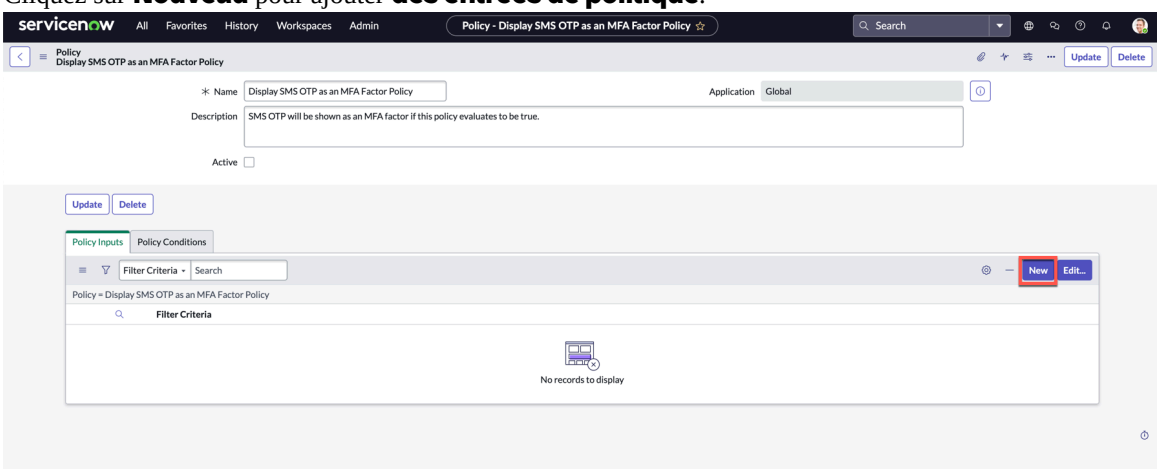
1. Accédez à la **Tout** > **Authentification multifacteur** > **Contexte MFA**.
2. Cliquez sur l'onglet **Politiques de facteur MFA** .
3. Sélectionnez **Afficher le mot de passe à usage unique SMS en tant que politique de facteur MFA**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Nouveau** pour ajouter **des entrées de politique**.

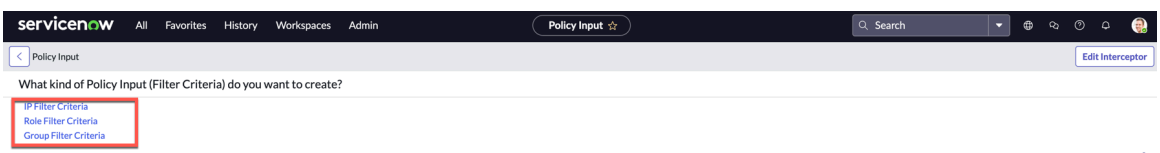


5. Sélectionnez les critères de filtre que vous souhaitez créer.

Les types de critères de filtre sont les suivants :

- Critère de filtre d'adresses IP
- Critère de filtre de rôle
- Critères de filtre de groupe

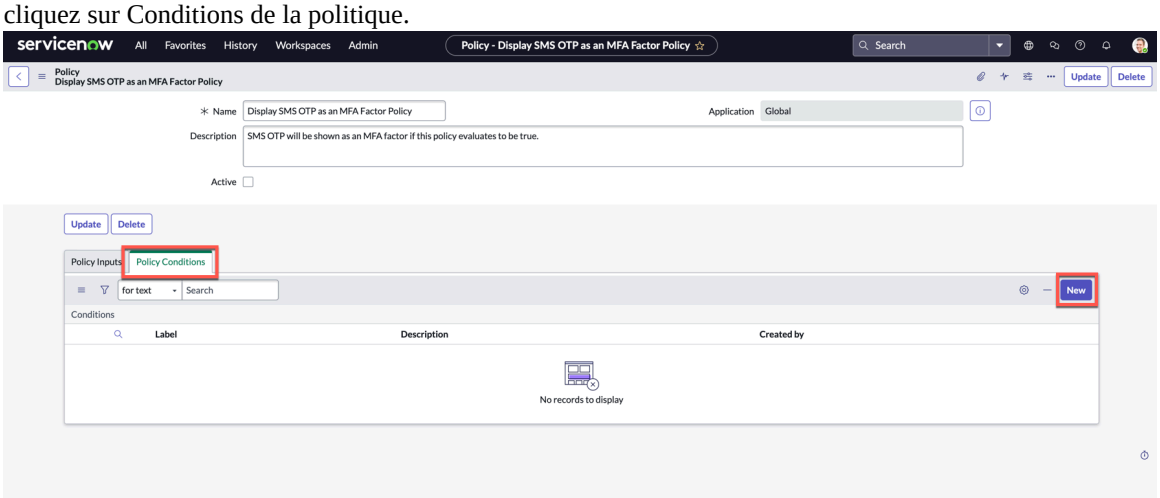
Par exemple, Critères de filtre de rôle.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Critères de filtre de rôle**, renseignez les champs des critères de filtre de rôle et envoyez l'enregistrement.
   La nouvelle politique est créée. Pour plus d'informations, consultez Critères de filtre de rôle.
7. Sur la page Politique - Afficher le mot de passe à usage unique du SMS en tant que politique de facteur MFA, cliquez sur Conditions de la politique.



8. Cliquez sur **Nouveau** pour ajouter des **conditions de politique**.
9. Renseignez les champs du formulaire.

Formulaire Condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtrage) qui est utilisée pour évaluer les demandes d'authentification. Sélectionnez la politique de critères de filtre basée sur les rôles qui a été créée pour la condition.

10. Cliquez sur **Envoyer**.
11. **Facultatif :** Répétez l'étape 8 pour créer des conditions de politique supplémentaires.

Remarque :
Si vous créez plusieurs conditions de politique, le résultat final de la politique d'accès dépend de la sortie logique OU de toutes les conditions de politique. Cela signifie que la police est évaluée comme vraie si l'une de vos conditions de police est remplie.

En fonction de la politique de filtre de rôle (utilisateurs) et des conditions spécifiées pour le rôle de correspondance, le SMS comme facteur MFA est affiché comme option d'authentification pour les utilisateurs.

Fournisseurs d'authentification multifacteur

Utilisez les fournisseurs de MFA pour configurer l'authentification par SMS et par e-mail afin de garantir que chaque utilisateur peut se connecter en toute sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sur le Now Platform, vous pouvez configurer les fournisseurs MFA avec le mécanisme d'authentification multifacteur tel que la messagerie et les SMS.

Vous pouvez utiliser la configuration de fournisseur suivante disponible pour MFA dans :Now Platform

- Configuration du fournisseur de messagerie
- Configuration du fournisseur Twilio
- Configuration du fournisseur Infobip.

Remarque :
La configuration des fournisseurs Twilio et Infobip est remplie automatiquement en activant l'option Charger les données de démonstration lors de l'installation des modules d'extension Authentification multifacteur avec SMS (com.snc.authentication.sms_mfa) et Notification - Pilote Twilio Direct (com.snc.notify.twilio_direct).

Vous pouvez également créer votre propre configuration de fournisseur pour activer l'authentification multifacteur par SMS et par e-mail.

Remarque :
La configuration du fournisseur Infobip est fournie dans le cadre des données de démonstration, vous pouvez modifier les champs en fonction de vos besoins pour configurer votre propre fournisseur.

Configurer le fournisseur MFA

Configurez les SMS et les e-mails avec le fournisseur pour vous assurer que chaque utilisateur peut se connecter en toute sécurité.

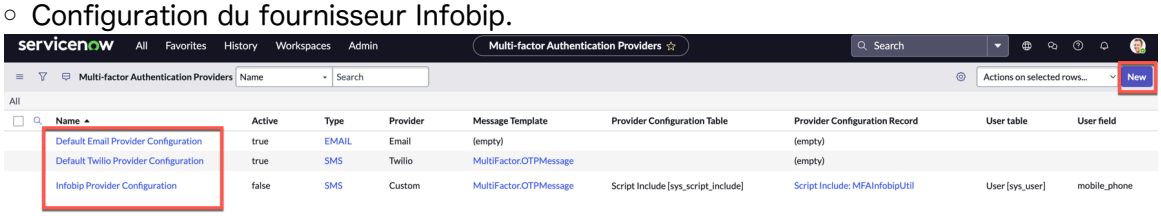
Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification multifacteur** > **Fournisseurs**.

   La configuration du fournisseur suivante est disponible pour MFA dans :Now Platform

   - Configuration du fournisseur de messagerie
   - Configuration du fournisseur Twilio
   - Configuration du fournisseur Infobip.



2. Pour créer un nouveau fournisseur, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Condition

Champ	Description
Nom	Nom de l'enregistrement.
Type	Description de l’enregistrement.
Fournisseur	Choisissez **Twilio** ou **Personnalisé**. **Remarque :** Pour configurer Twilio, consultez Configurer Notification with Twilio . Lorsque vous choisissez **Personnalisé**, vous devez spécifier les champs suivants : ○ Table de configuration du fournisseur ○ Enregistrement de configuration du fournisseur ○ Script ○ Table des utilisateurs ○ Champ d'utilisateur
Modèle de message	Modèle de message pour l’enregistrement.
Actif	Option permettant d’activer la configuration du fournisseur.

4. Cliquez sur **Envoyer**.

   En fonction du modèle de message et des configurations du fournisseur, le SMS ou l’e-mail est envoyé aux utilisateurs en tant que facteur d’authentification pendant le processus de connexion.

Configuration personnalisée du fournisseur Vonage (tutoriel)

Configurez un SMS avec le fournisseur Vonage pour vous assurer que chaque utilisateur peut se connecter en toute sécurité.

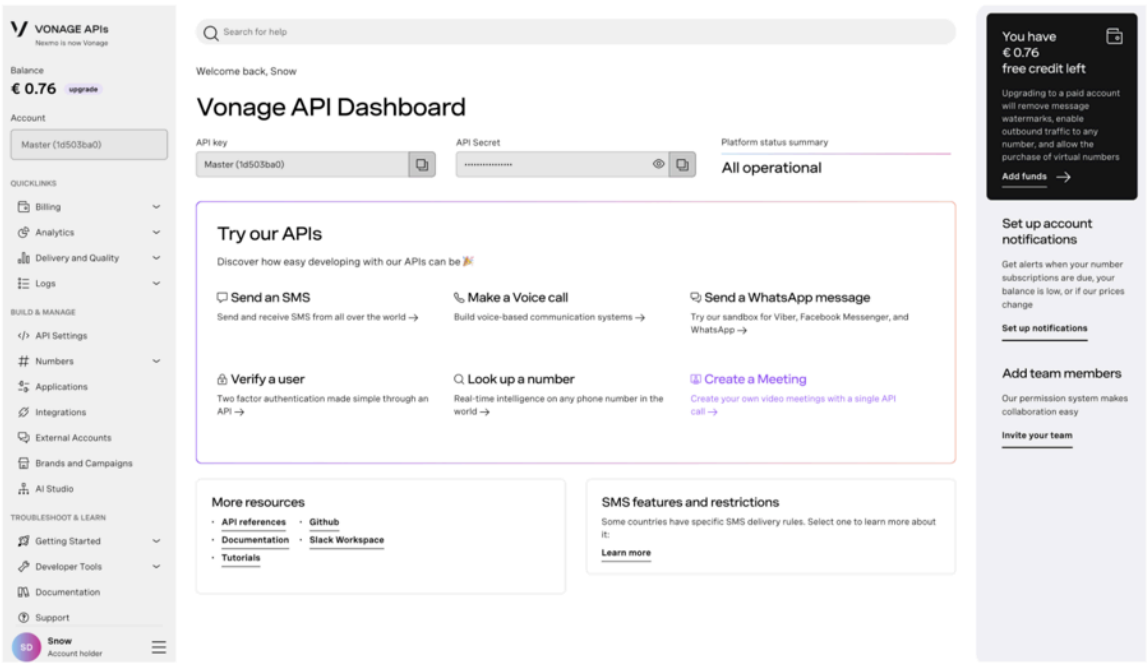
Avant de commencer
Rôle requis : administrateur

Traduction automatique

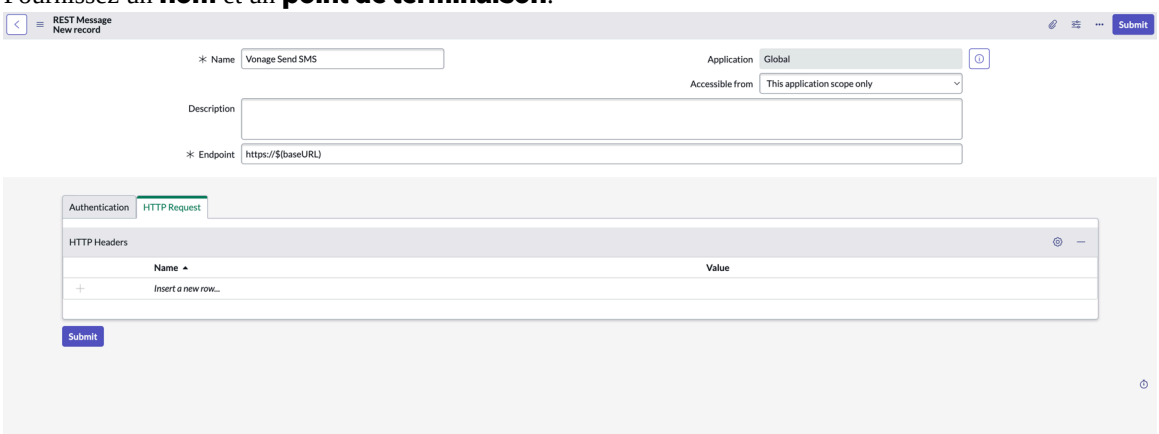
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Sortant** > **Message REST** et effectuez la configuration des messages REST en fonction des informations issues du tableau de bord de l'API Vonage.



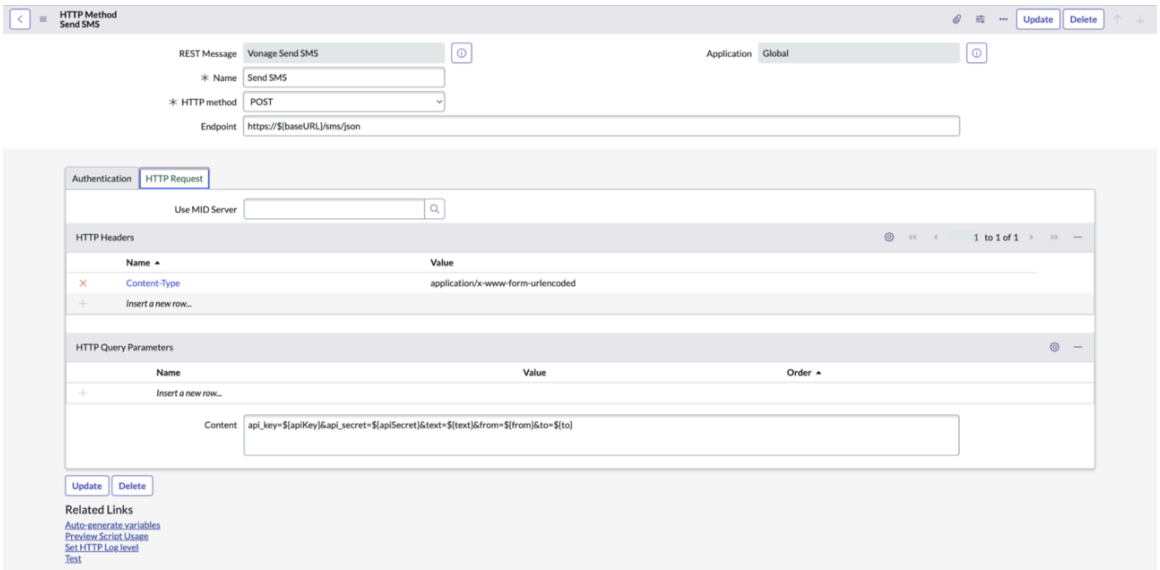
2. Cliquez sur **Nouveau** pour créer un **nouveau message REST**.
3. Fournissez un **nom** et un **point de terminaison**.



4. Cliquez sur **Envoyer**.
5. Ouvrez l'enregistrement créé, dans la liste connexe **Méthodes HTTP**, cliquez sur **Nouveau** et sélectionnez la méthode HTTP en tant que **POST.**
6. Renseignez les champs suivants :
   - Point de terminaison : `https://${baseURL}/sms/json`
   - Contenu :`api_key=${apiKey}&api_secret=${apiSecret}&text=${text}&from=${from}&to=${to}`
   - Type de contenu : `application/x-www-form-urlencoded`

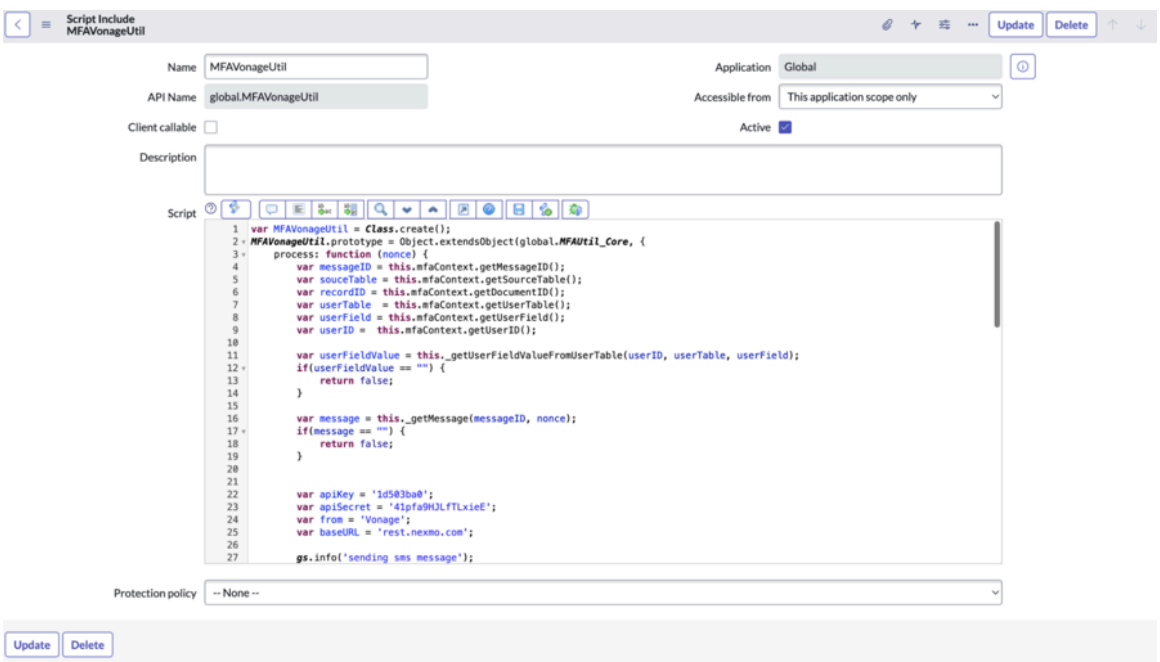
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Mettez à jour l'enregistrement.
8. Cliquez sur **Générer automatiquement des variables** à partir de la section **Liens connexes** .
9. Importez le SI partagé dans le dossier et copiez l'apiKey et le secret à partir du tableau de bord de l'API Vonage.

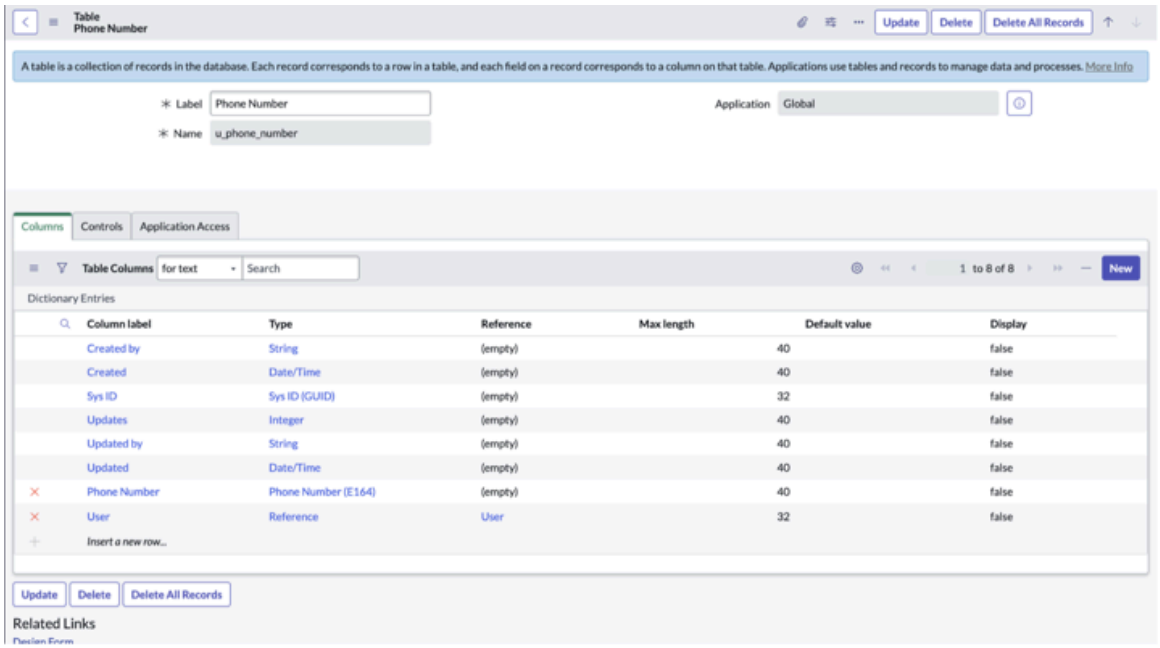
> **Remarque :**
>
> L'apiKey et le secret se trouvent dans les paramètres de votre compte Vonage dans le tableau de bord Vonage.



10. Créez une table Numéros de téléphone personnalisée avec deux colonnes, par exemple :
    - **Étiquette de colonne** : **Utilisateur, Type** : Référence, **Référence : Utilisateur** (sys_user).
    - **Étiquette de colonne** : Numéro de téléphone, **Type** : Numéro de téléphone (E164).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Créez un fournisseur personnalisé dans la table Fournisseur multifacteur.



Pour en savoir plus sur la configuration du fournisseur, reportez-vous à la section Configurer le fournisseur MFA.

Authentification multifacteur par e-mail

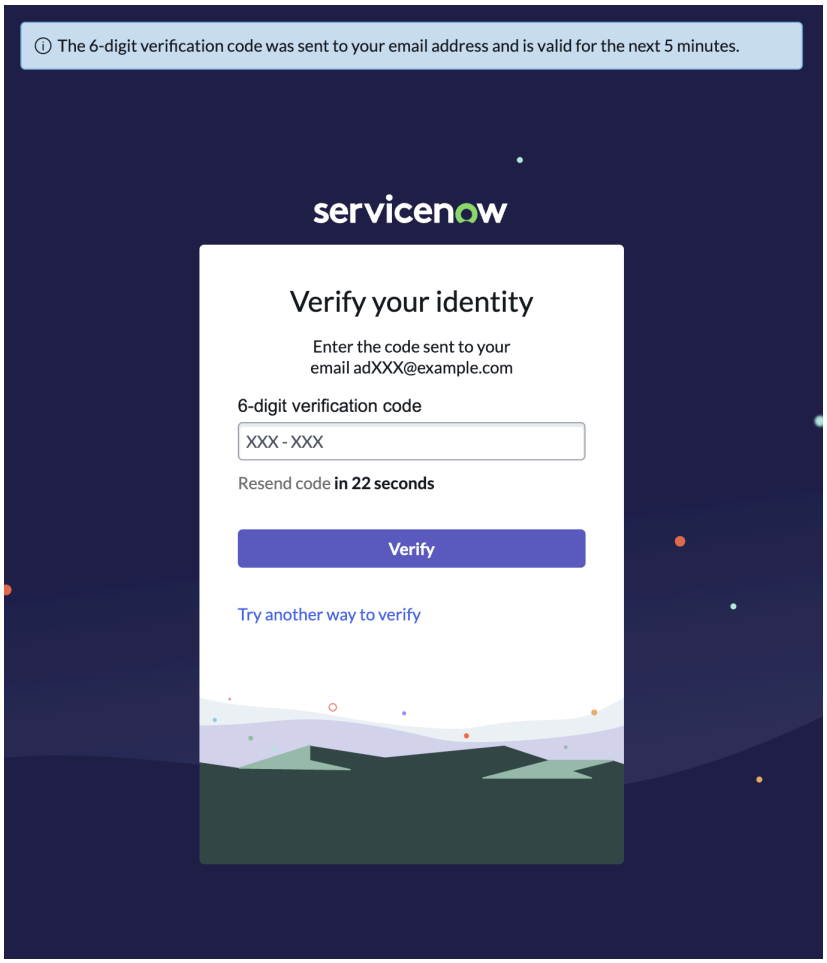
Authentification multifacteur (MFA) avec l'e-mail comme facteur d'authentification.

L'administrateur peut configurer ServiceNow l'instance pour exiger des utilisateurs qui tentent de se connecter à l'instance à l'aide d'un OTP basé sur un e-mail.

Remarque :
MFA avec e-mail est activé par défaut avec le module d'extension Intégration - Authentification multifacteur (com.snc.integration.multifactor.authentication). Vous devez configurer les entrées et les conditions de la politique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Lorsque les utilisateurs tentent de se connecter à ServiceNow, un OTP e-mail est envoyé à l'adresse e-mail associée. L'utilisateur peut saisir le code de vérification à six chiffres qu'il a envoyé à l'adresse e-mail et vérifier son identité.

Configurer l'e-mail en tant que facteur MFA

Configurez l'entrée et la condition de politique pour afficher l'OTP d'e-mail en tant que politique de facteur MFA pour l'authentification.

Avant de commencer
Rôle requis : administrateur

Procédure

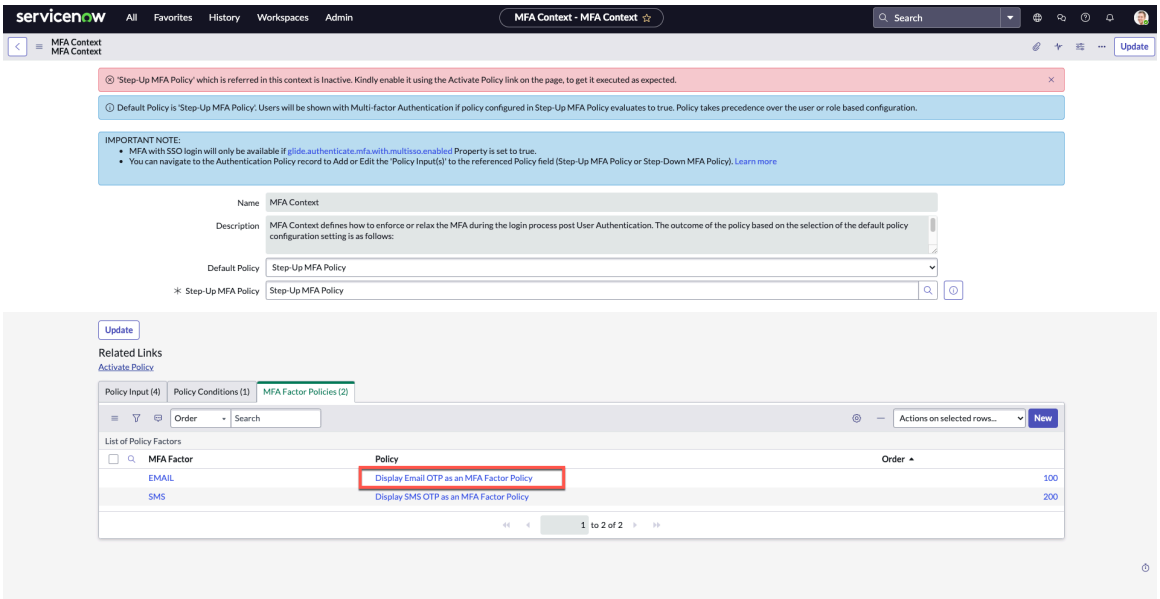
1. Accédez à la **Tout** > **Authentification multifacteur** > **Contexte MFA**.
2. Cliquez sur **l'onglet Politiques de facteur MFA** .

> **Remarque :**
> **L'option EMAIL** en tant que **facteur MFA avec une politique** est disponible par défaut. Vous pouvez modifier la politique et spécifier les entrées et les conditions de la politique.

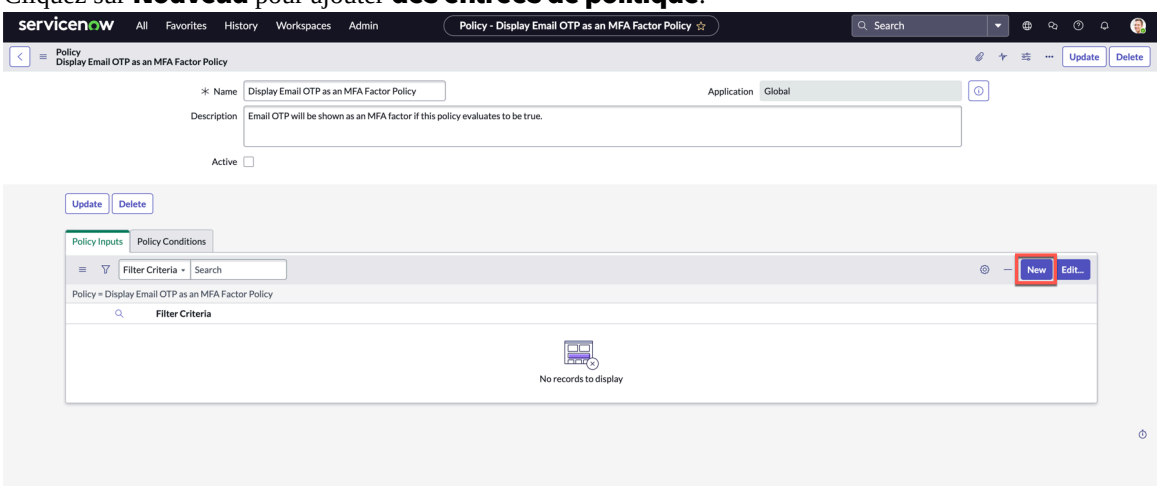
3. Sélectionnez **l'OTP Afficher l'e-mail comme politique de facteur MFA**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Cliquez sur **Nouveau** pour ajouter **des entrées de politique**.



5. Sélectionnez les critères de filtre que vous souhaitez créer.

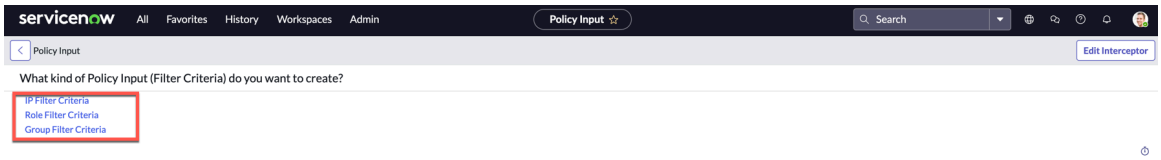
   Les types de critères de filtre sont les suivants :

   - Critère de filtre d'adresses IP
   - Critère de filtre de rôle
   - Critères de filtre de groupe

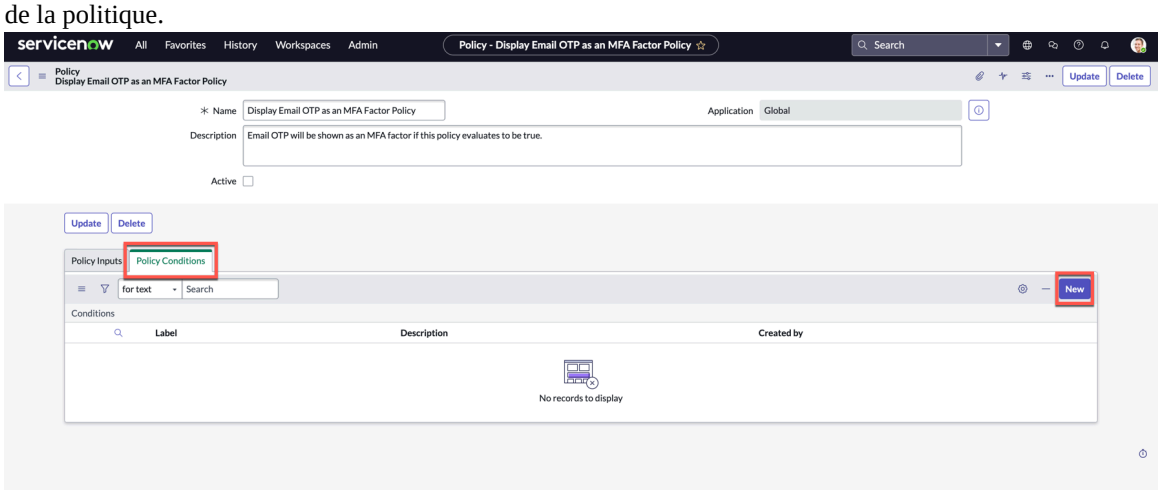
   Par exemple, Critères de filtre de rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Critères de filtre de rôle**, renseignez les champs des critères de filtre de rôle et envoyez l'enregistrement. La nouvelle politique est créée. Pour plus d'informations, consultez Critères de filtre de rôle.
7. Sur la page Politique - Afficher l'OTP d'e-mail en tant que politique de facteur MFA, cliquez sur Conditions de la politique.



8. Cliquez sur **Nouveau** pour ajouter des **conditions de politique**.
9. Renseignez les champs suivants du formulaire :

Formulaire Condition

Champ	Description
Étiquette	Nom permettant d'identifier la condition.
Description	Description de la condition.
Condition	Combinaison logique de plusieurs entrées de politique (critères de filtrage) qui est utilisée pour évaluer les demandes d'authentification. Sélectionnez la politique de critères de filtre basée sur les rôles qui a été créée pour la condition.

10. Cliquez sur **Envoyer**.
11. **Facultatif :** Répétez l'étape 8 pour créer des conditions de politique supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Si vous créez plusieurs conditions de politique, le résultat final de la politique d'accès dépend de la sortie logique OU de toutes les conditions de politique. Cela signifie que la police sera évaluée comme vraie si l'une de vos conditions de police est remplie.

En fonction de la politique de filtre de rôle (utilisateurs) et des conditions spécifiées pour le rôle, le facteur MFA des e-mails est affiché comme une option d'authentification pour les utilisateurs.

Réinitialiser l'authentification multifacteur (MFA) pour les utilisateurs

Les administrateurs peuvent réinitialiser la MFA pour les utilisateurs qui ont supprimé l'application, qui ont perdu l'accès à l'appareil ou qui n'ont pas d'alternative MFA associée à leur appareil.

Avant de commencer
Rôle requis : administrateur

La procédure suivante décrit comment un ServiceNow® administrateur peut réinitialiser la validation MFA pour débloquer les utilisateurs et leur permettre d'enregistrer à nouveau MFA.

Procédure

1. Accédez à la **Tout** > **Authentification multifacteur** > **Configuration multifacteur pour l'utilisateur**.
2. Dans la table utilisateur, recherchez l'utilisateur que vous souhaitez débloquer.
3. Définissez la validation sur **faux**.
4. Accédez à la **Tout** > **Authentification multifacteur** > **Facteurs des utilisateurs récents**.
5. Recherchez le même utilisateur.
6. Définissez le facteur Est récent sur **faux** pour le type de MFA que vous souhaitez réinitialiser pour l'utilisateur.
   Changer la valeur en **faux** débloque l'utilisateur et lui permet d'enregistrer à nouveau MFA.
   Lorsque l'utilisateur débloqué saisit les informations d'identification et se connecte, la page **Activer l'authentification multifacteur (MFA)** s'affiche. L'utilisateur peut suivre les étapes indiquées sur la page pour réenregistrer MFA.

Rubrique de référence : Authentification multifacteur

Rubrique de référence associée à la configuration de l'authentification multifacteur.

Authentifications multifacteurs des utilisateurs

Pour accéder aux détails de l'authentification multifacteur de l'utilisateur, accédez à **Tout** > **Authentification multifacteur** > **Configuration multifacteur pour l'utilisateur**.

Authentifications multifacteurs des utilisateurs

Champ	Description
Utilisateur	Nom d'utilisateur de l'utilisateur
Contournements restants	Nombre total de contournements restant pour l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentifications multifacteurs des utilisateurs (suite)

Champ	Description
Secret multifacteur	Les détails du secret multifacteur.
Validés	Le multifacteur est-il validé. Changer la valeur en **faux** invalide la configuration de l'application d'authentification existante.

Remarque :
Les facteurs MFA récemment utilisés par les utilisateurs sont disponibles dans le module Facteurs utilisés récemment par l'utilisateur. Accédez à la **Tout** > **Authentification multifacteur** > **Facteurs des utilisateurs récents**. Pour plus d'informations, consultez Facteurs de l'utilisateur utilisés récemment.

Empreintes digitales du navigateur multifacteur

Pour accéder aux détails sur les empreintes digitales du navigateur de l'utilisateur, accédez à **Tout** > **Authentification multifacteur** > **Empreintes digitales du navigateur multifacteur**.

Empreintes digitales du navigateur multifacteur

Champ	Description
Utilisateur	Nom d'utilisateur de l'utilisateur
Navigateur	Le navigateur utilisé par l'utilisateur.
Empreinte digitale du navigateur	Les détails de l'empreinte digitale du navigateur.
Cookie d'empreinte digitale du navigateur	Les détails du cookie d'empreinte digitale du navigateur.
Expiration du cookie d'empreinte digitale du navigateur	Les détails d'expiration du cookie d'empreinte digitale du navigateur.

Facteurs de l'utilisateur utilisés récemment

Pour accéder aux détails sur les facteurs récemment utilisés par l'utilisateur, accédez à **Tout** > **Authentification multifacteur** > **Facteurs des utilisateurs récents**.

Configurations multifacteurs pour les utilisateurs

Champ	Description
Utilisateur	Nom d'utilisateur de l'utilisateur
Type multifacteur	Le type multifacteur que l'utilisateur a utilisé pour se connecter.
Est un facteur récent	Les récents détails multifacteurs de l'utilisateur.

Utilisation de l'authentification multifacteur (MFA)

Découvrez comment utiliser les outils d'authentification multifacteur pour accéder en toute sécurité à votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Se connecter avec l'authentification MFA

ServiceNow requiert des applications d'authentification qui prennent en charge les mots de passe à usage unique et durée définie (TOTP). ServiceNow teste l'authentification MFA avec les applications d'authentification suivantes :

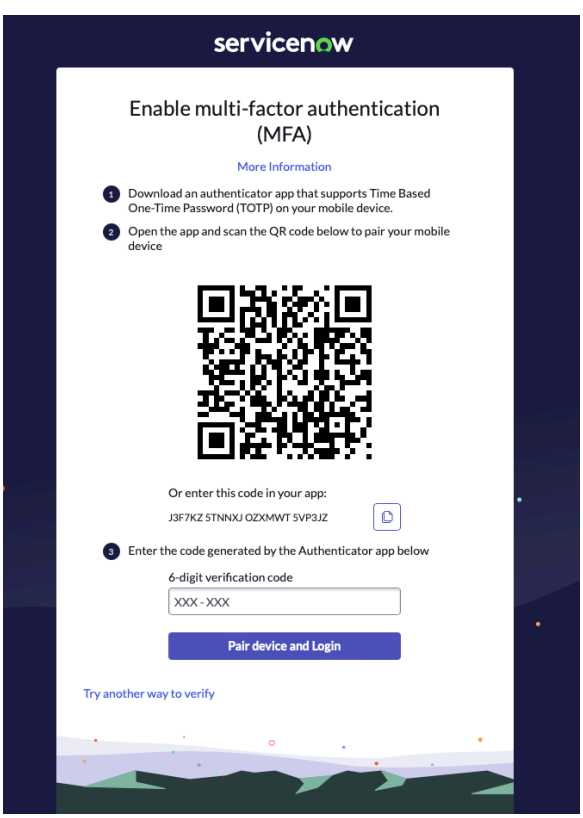
- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy
- FreeOTP
- Duo
- Okta Verify

Remarque :

- d'autres applications d'authentification non répertoriées peuvent également être compatibles, mais ne sont pas testées par ServiceNow.
- Pour plus d'informations sur le changement de comportement spécifique au navigateur, consultez cet article de la base de connaissances

---

Validation avec l'application d'authentification



Si votre administrateur a activé l'authentification multifacteur (MFA) sur votre instance, vous êtes invité à effectuer une seconde authentification après avoir saisi votre nom d'utilisateur et votre mot de passe. Pour obtenir plus de détails sur le processus de connexion avec l'authentification MFA, consultez Connectez-vous avec l'authentification multifacteur.

Si vous n'avez pas configuré un second formulaire d'authentification, une page de configuration s'affiche après la connexion pour vous guider dans le processus de configuration d'une application d'authentification. Pour en savoir plus sur cette configuration, consultez Configurer l'authentification multifacteur pour la première fois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Saisissez le code affiché sur votre application d'authentification pour vous connecter.

Enregistrer un appareil d'authentification

Une fois que vous avez configuré une application d'authentification, vous pouvez enregistrer d'autres méthodes d'authentification.



Authentificateurs biométriques

Vous pouvez utiliser des authentificateurs biométriques comme les empreintes digitales ou la reconnaissance faciale comme seconde authentification MFA. Si votre administrateur autorise cette option, vous pouvez configurer des authentificateurs biométriques en suivant les étapes de la rubrique Enregistrer un authentificateur biométrique.

Authentificateurs de clé matérielle

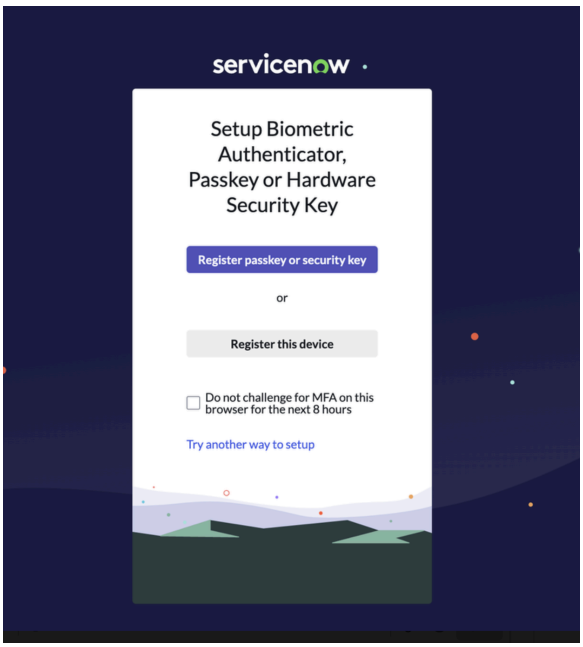
Les clés matérielles sont des appareils de sécurité physique que vous pouvez utiliser pour l'authentification. Vous pouvez enregistrer un appareil matériel à utiliser avec votre instance en suivant les étapes de la rubrique Enregistrer une clé de sécurité matérielle.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Validation avec biométrie ou clé matérielle



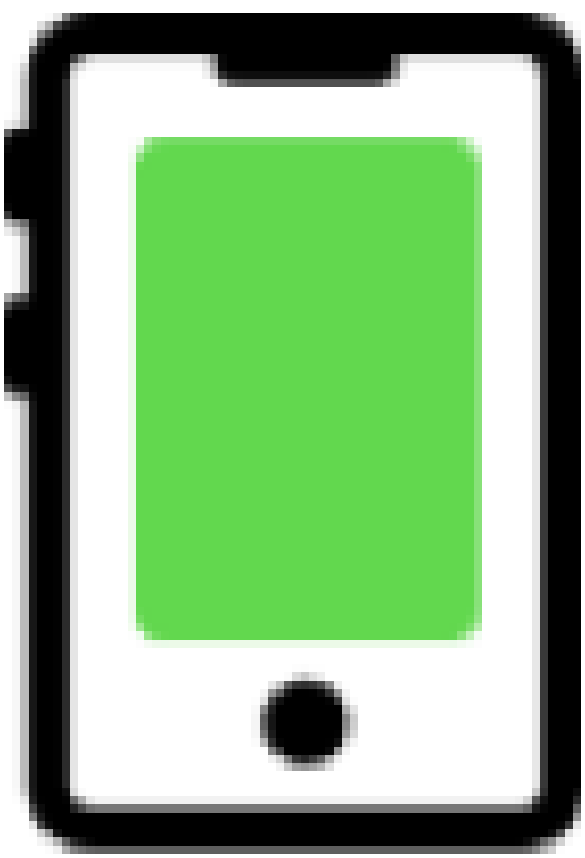
Utilisez la biométrie ou une clé de sécurité pour vous connecter.

Enregistrer un numéro de téléphone pour le mot de passe à usage unique

SMS

L'administrateur configure l'instance ServiceNow pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique basé sur un SMS.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par SMS est envoyé au numéro de téléphone mobile associé à l'enregistrement sys_user. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.

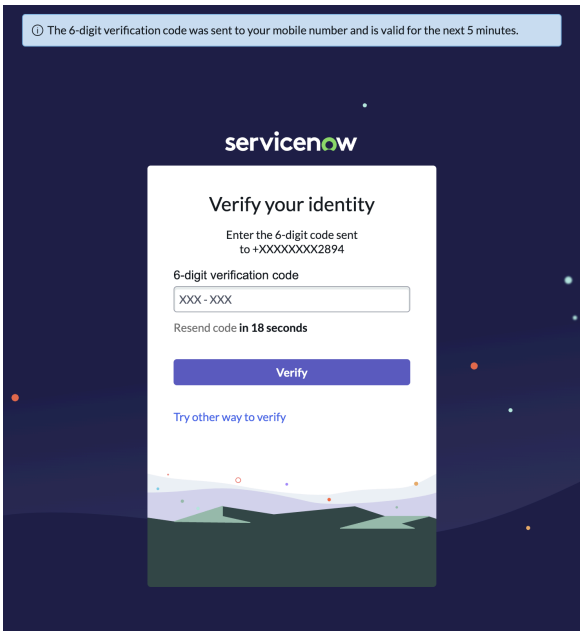


Validation par SMS

Saisissez le code à 6 chiffres envoyé au numéro de téléphone mobile pour vous connecter. Le code

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



envoyé est valide pendant les 5 minutes qui suivent sa réception. Vous pouvez utiliser Renvoyer le code pour que le code vous soit de nouveau envoyé.

Enregistrer une adresse e-mail pour le mot de passe à usage unique

Adresse e-mail

L'administrateur configure l'instance ServiceNow pour exiger des utilisateurs qui tentent de s'y connecter d'utiliser un mot de passe à usage unique basé sur une adresse e-mail.

Lorsque les utilisateurs tentent de se connecter à ServiceNow, un mot de passe à usage unique par e-mail est envoyé à l'adresse e-mail associée à l'utilisateur. Les utilisateurs peuvent saisir le code de vérification à six chiffres qu'ils ont reçu sur leur équipement mobile et confirmer leur identité.

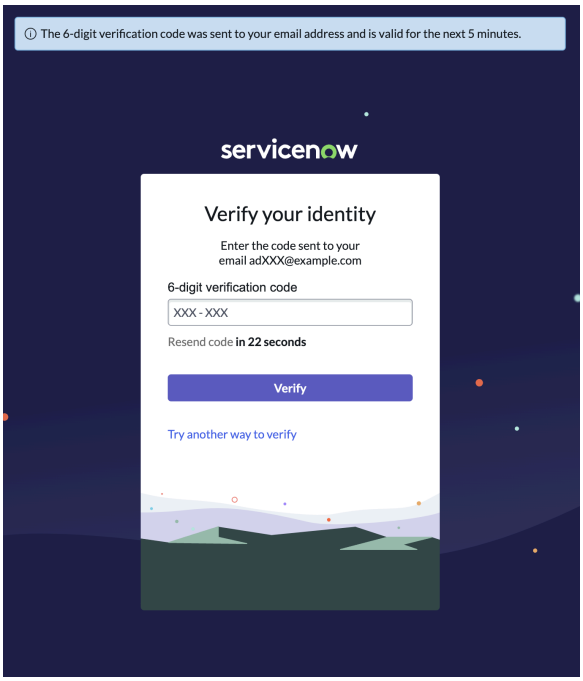


Validation par e-mail

Saisissez le code à 6 chiffres envoyé à l'adresse e-mail pour vous connecter. Le code envoyé est valide pendant les 5 minutes qui suivent sa réception. Vous pouvez utiliser Renvoyer le code pour que le code vous soit de nouveau envoyé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Configurer l'authentification multifacteur pour la première fois

Si votre administrateur a activé l'authentification multifacteur sur votre profil, mais que vous n'avez pas encore configuré l'application, vous pouvez le faire lors de la connexion.

Avant de commencer

Rôle requis : aucun

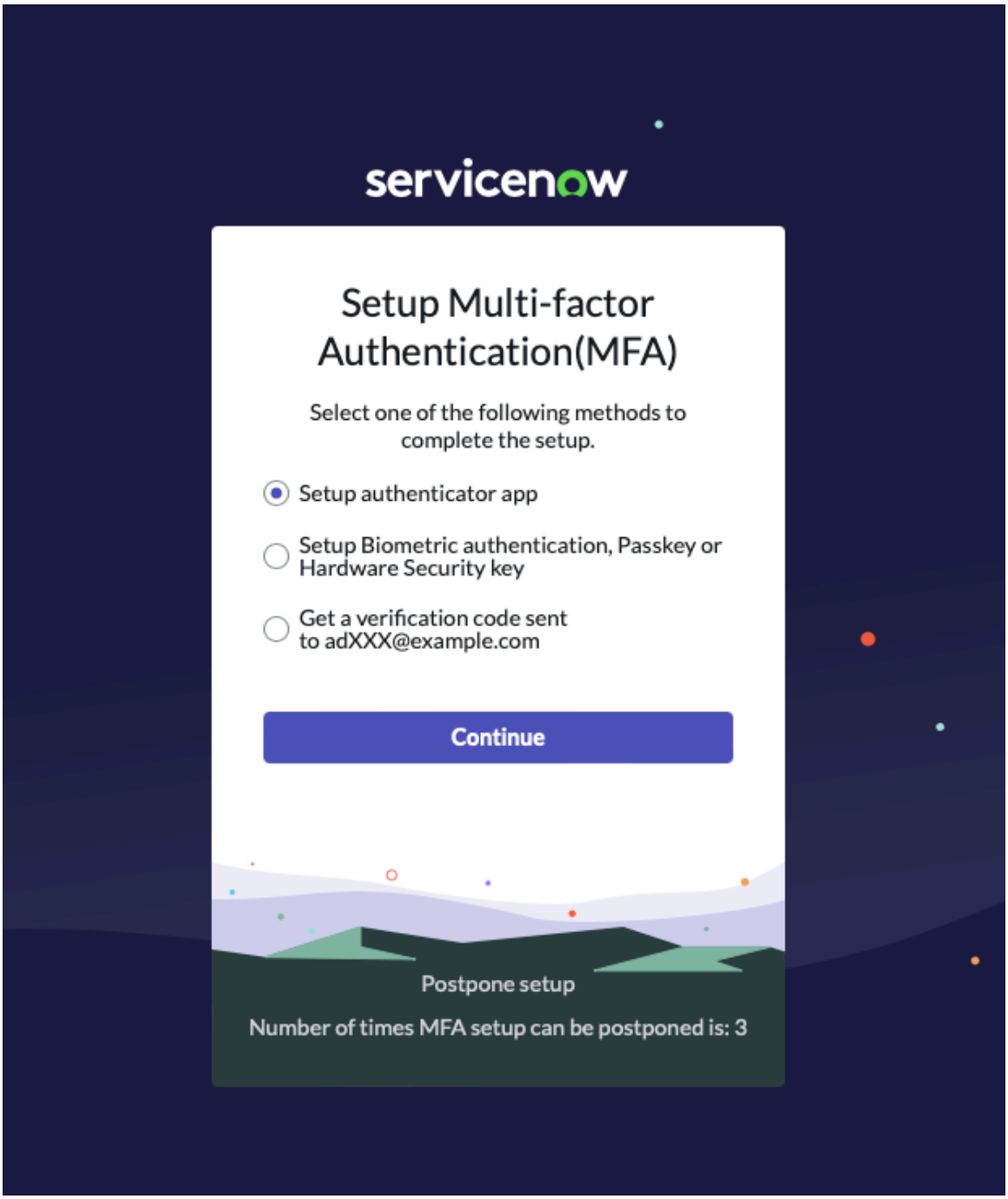
Procédure

1. Connectez-vous à votre instance à l'aide de votre nom d'utilisateur et de votre mot de passe.

   L'écran de configuration de l'authentification multifacteur intercepte votre connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

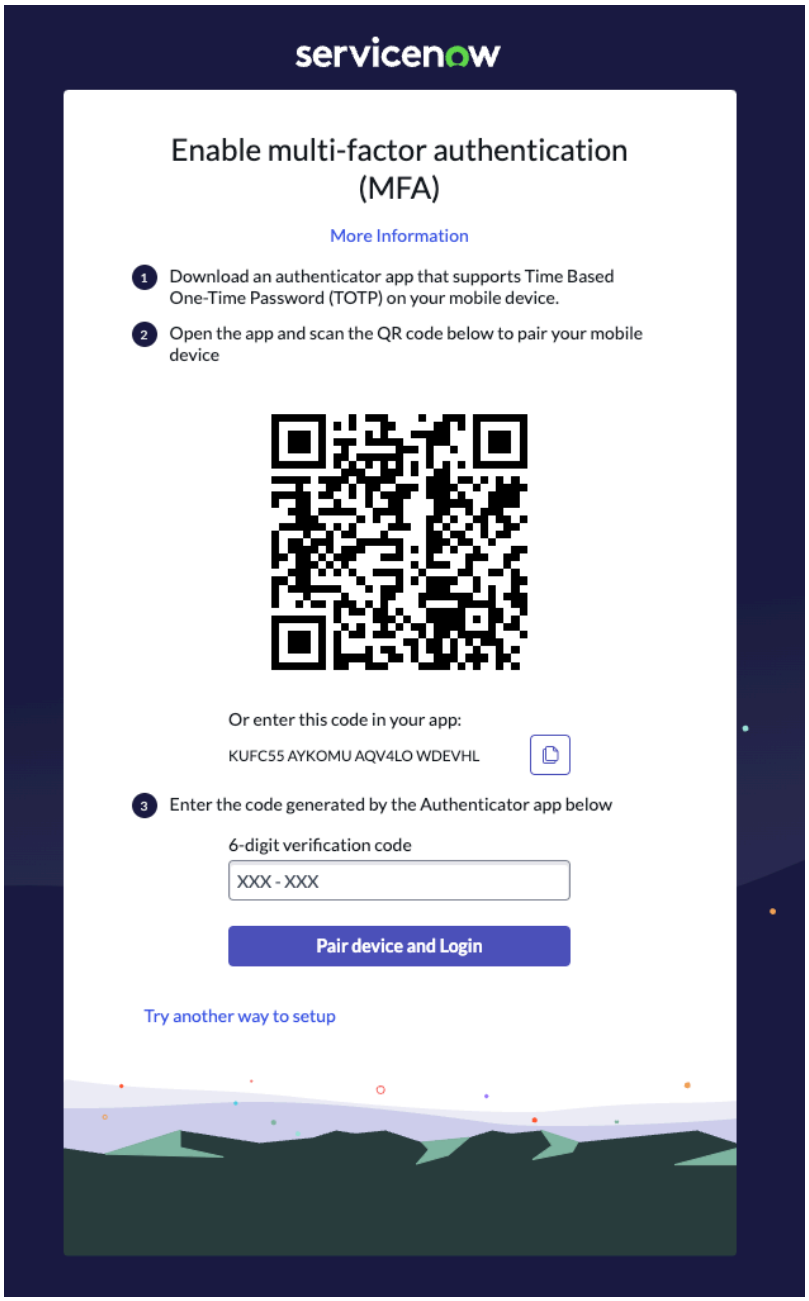
Remarque :
Si vous souhaitez ignorer la configuration de l'authentification maintenant, cliquez sur **Configuration du contournement**. Vous pouvez contourner l'authentification multifacteur pour un nombre limité de fois si votre administrateur l'autorise. Enfin, vous devez configurer l'authentification multifacteur.

2. Sélectionnez l'une des méthodes suivantes pour terminer la configuration MFA.

a. Configurer une application d'authentificateur

Suivez les instructions à l'écran pour coupler l'appareil et vous connecter.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

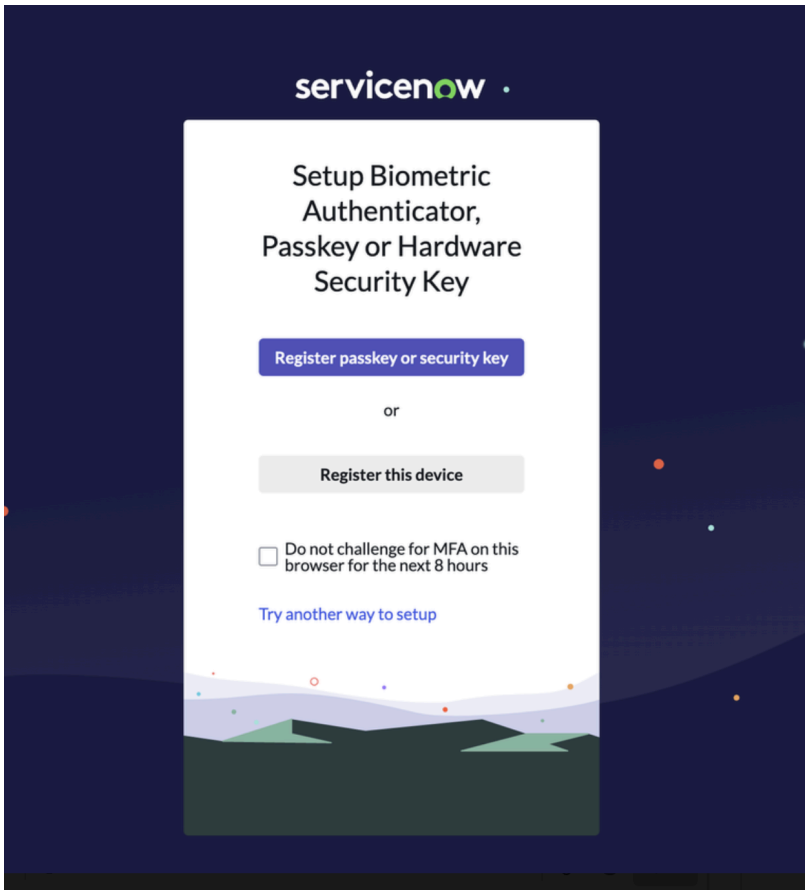


b. Configurer l'authentification biométrique, la clé d'accès ou la clé de sécurité du matériel

Sélectionnez l'une des options pour terminer la configuration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

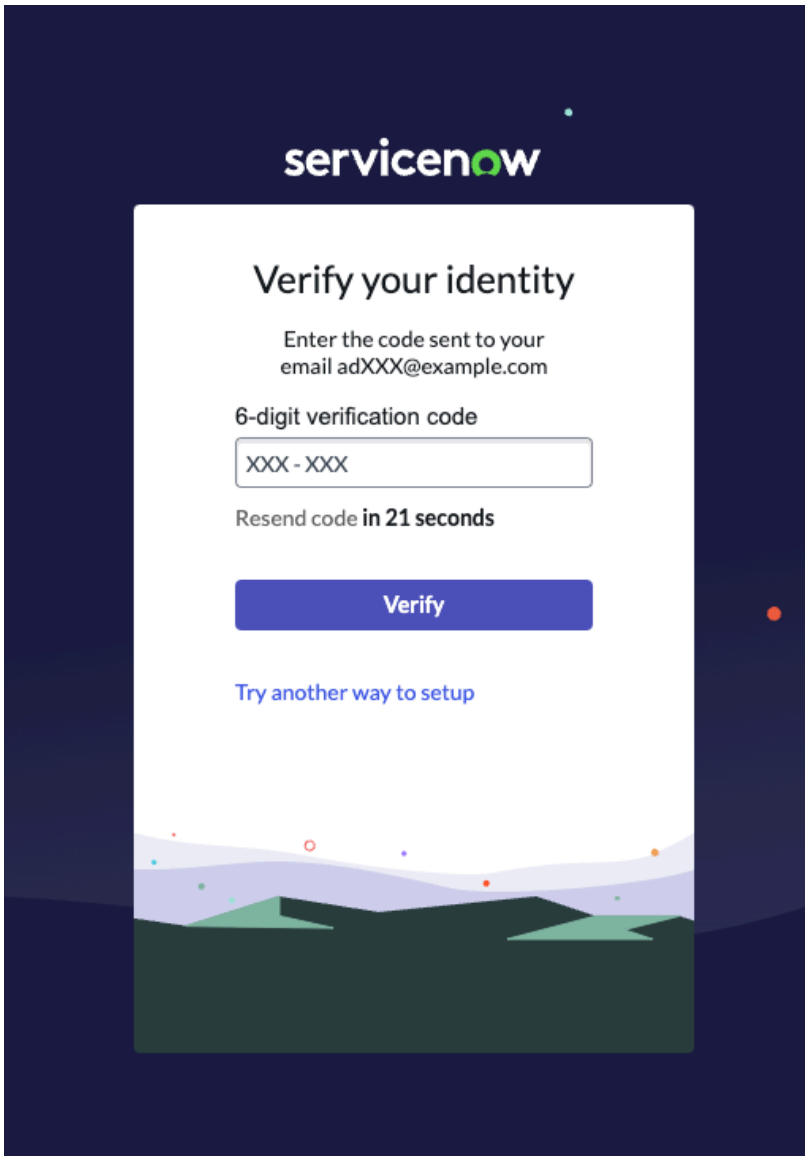


c. Recevez un code de vérification envoyé à votre adresse e-mail

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Entrez le code de vérification qui a été envoyé à votre adresse e-mail.



Une fois l'une ou l'autre des configurations terminée, vous êtes connecté à l'instance.

Configurer l'authentification multifacteur sur votre profil d'utilisateur

Activez l'authentification multifacteur pour votre compte dans les paramètres de votre profil d'utilisateur.

Avant de commencer
Rôle requis : aucun

L'authentification multifacteur doit être activée sur votre instance.

Remarque :
Votre administrateur peut exiger que vous utilisiez l'authentification multifacteur. Dans ce cas, vous y êtes automatiquement invité lorsque vous vous connectez. Consultez Configurer l'authentification multifacteur pour la première fois. Suivez la procédure ci-dessous si votre administrateur vous autorise à accepter l'authentification multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

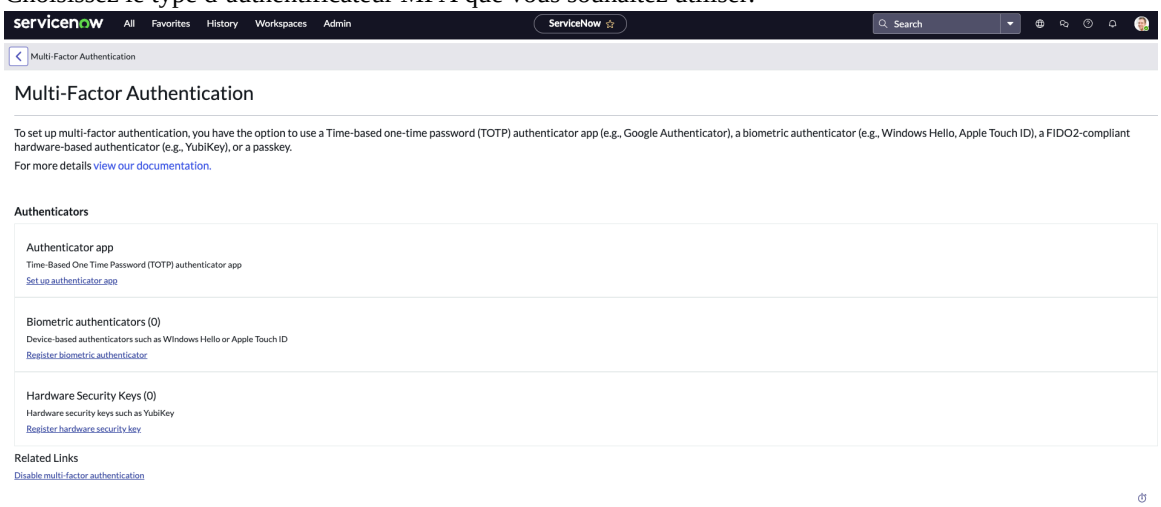
Procédure

1. Accédez à la **Tout** > **Libre-service** > **Mon profil**.

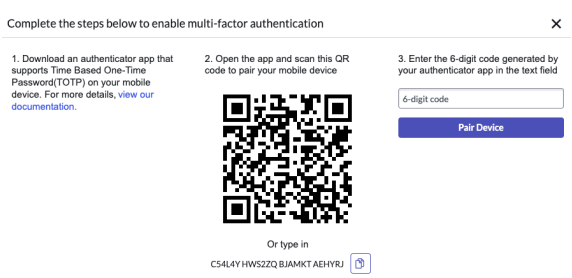
   > **Remarque :**
   > Vous pouvez également accéder à votre profil en cliquant sur votre nom d'utilisateur dans l'en-tête de l'instance.

2. Dans votre profil d'utilisateur, cliquez sur **Authentification multifacteur** dans la section **Liens connexes** .

3. Choisissez le type d'authentificateur MFA que vous souhaitez utiliser.

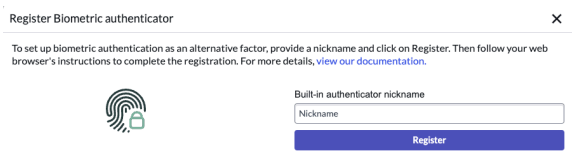
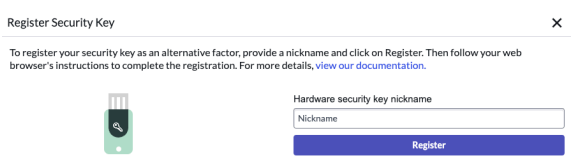


Authentificateurs MFA

Authentificateurs MFA	Description
Application d'authentification	Application d'authentification basée sur un mot de passe unique et durée définie (TOTP) Sélectionnez **Configurer une application d'authentification** et suivez les instructions à l'écran pour vous inscrire à une application d'authentification comme deuxième facteur d'authentification. 
Authentificateurs biométriques	Authentificateurs basés sur l'appareil tels que Windows Hello ou Apple Touch ID Sélectionnez **Enregistrer l'authentification biométrique** et suivez les instructions à l'écran pour vous inscrire à une application

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Authentificateurs MFA	Description
	d’authentification comme deuxième facteur d’authentification. 
Clés de sécurité matérielles	Clés de sécurité matérielles telles que YubiKey Sélectionnez **Enregistrer les clés de sécurité matérielles** et suivez les instructions à l’écran pour vous inscrire à une application d’authentification comme deuxième facteur d’authentification. 

Résultats

L’authentification multifacteur est activée pour votre compte utilisateur. Vous serez invité à utiliser l’authentification multifacteur la prochaine fois que vous vous connecterez.

Remarque :
Vous ne pouvez pas désactiver l’authentification multifacteur sur votre compte une fois que vous l’avez activée. Si vous devez désactiver l’authentification multifacteur, contactez votre administrateur.

Connectez-vous avec l’authentification multifacteur

Connectez-vous avec l’authentification multifacteur lorsqu’elle est activée par votre administrateur sur votre instance.

Avant de commencer

Vous devez avoir activé l’authentification multifacteur pour votre profil. Vous pouvez l’activer vous-même sur votre profil d’utilisateur ou votre administrateur peut l’activer pour vous.

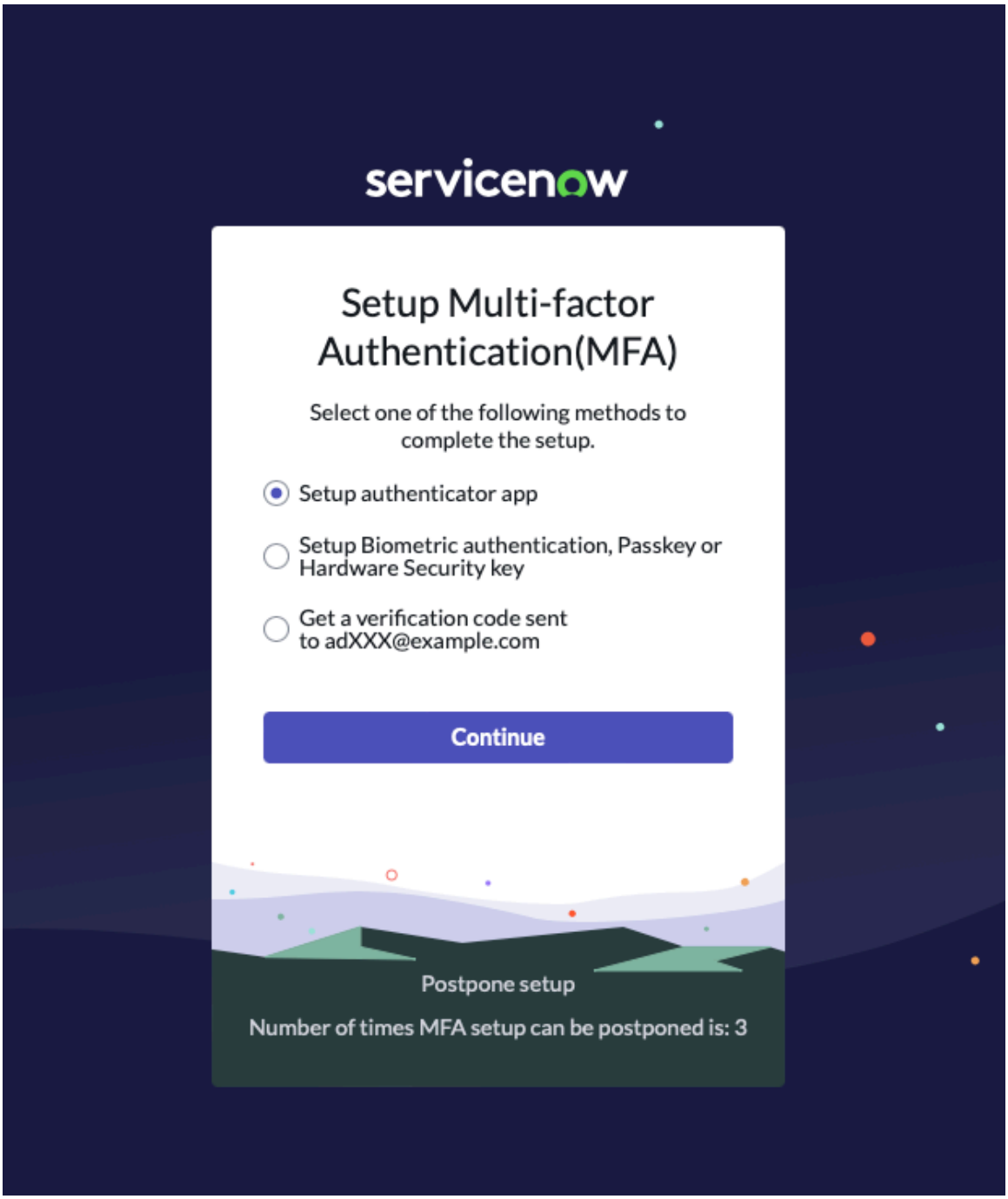
Rôle requis : aucun

Procédure

1. Accédez à l’URL de votre instance pour ouvrir l’écran de connexion.
2. Entrez votre nom d'utilisateur et votre mot de passe.
3. Cliquez sur **Se connecter**.
   L’écran d’authentification multifacteur s’affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Sélectionnez l’une des méthodes pour terminer la configuration MFA.
   Pour plus d’informations sur chaque configuration, reportez-vous à la section Configurer l’authentification multifacteur pour la première fois.

   Si vous souhaitez reporter la configuration, sélectionnez **Reporter la configuration**. La durée maximale de report de la configuration s’affiche à l’écran et cette valeur est configurée par votre administrateur.

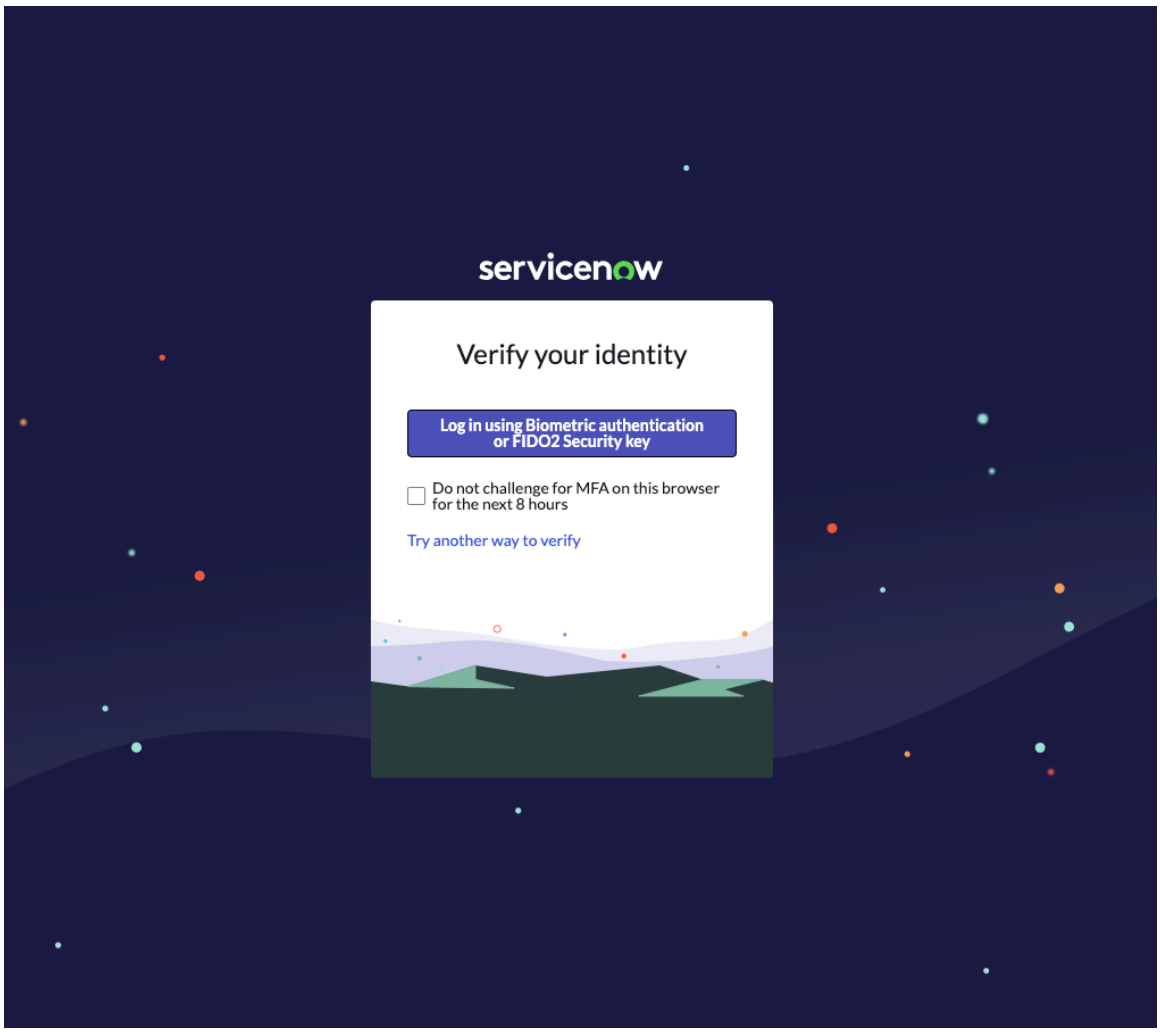
Résultats

Si vous avez déjà configuré l’authentification multifacteur, le facteur récemment utilisé s’affiche lorsque vous connectez votre instance après avoir entré votre nom d’utilisateur et votre mot de passe.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example: Facteur MFA récemment utilisé

Si le facteur utilisé récemment était la connexion biométrique, lors de la connexion à l'aide de votre nom d'utilisateur et de votre mot de passe, vous vous affichez directement avec l'écran de configuration de l'authentification multifacteur biométrique.



Applications d'authentification

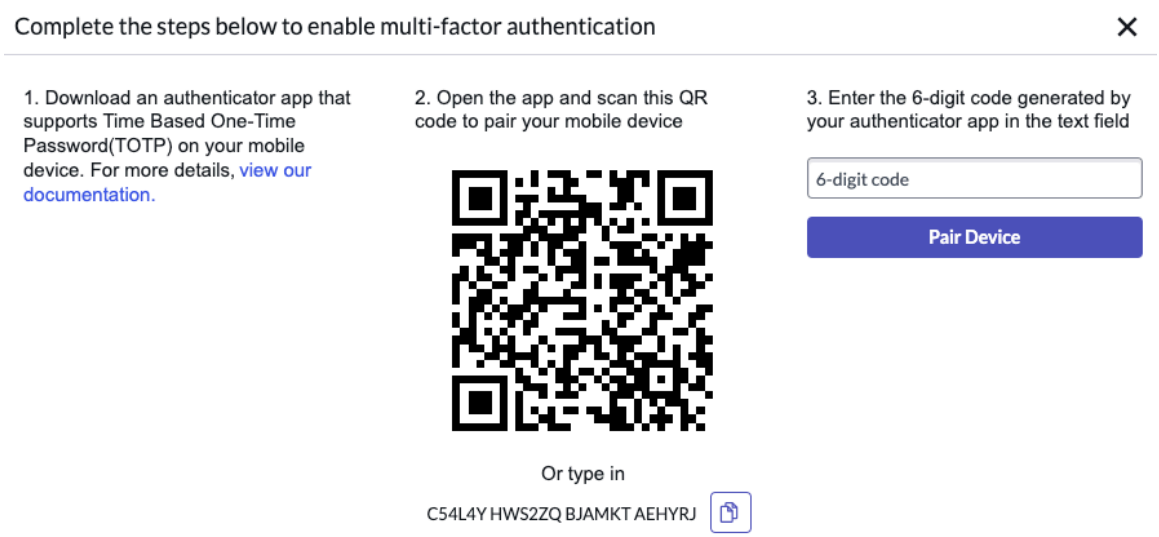
Utilisez des applications d'authentification tierces pour générer des codes d'accès MFA temporaires.

Une application d'authentification est un logiciel tiers qui génère des codes d'accès temporaires. Vous pouvez utiliser ces codes secrets avec votre mot de passe pour vous connecter à une instance qui nécessite l'authentification multifacteur (MFA).

Si votre administrateur a activé l'authentification multifacteur sur votre instance, vous êtes invité à saisir un code secret après la saisie de votre utilisateur et de votre mot de passe pendant la connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



ServiceNow nécessite des applications d'authentification qui prennent en charge les mots de passe uniques basés sur le temps (TOTP).

ServiceNow Teste l'authentification multifacteur avec les authentificateurs suivants :

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy
- FreeOTP
- Duo
- Okta Verify

Remarque :
d'autres applications d'authentification non répertoriées peuvent également être compatibles, mais ne sont pas testées par ServiceNow.

Changer l'application d'authentification

Générez un nouveau code pour changer l'application d'authentification sur votre appareil.

Avant de commencer

Vous devez avoir activé l'authentification multifacteur pour votre profil. Vous pouvez l'activer vous-même sur votre profil d'utilisateur ou votre administrateur peut l'activer pour vous.
Rôle requis : aucun

Procédure

1. Accédez à la **Tout** > **Libre-service** > **Mon profil**.

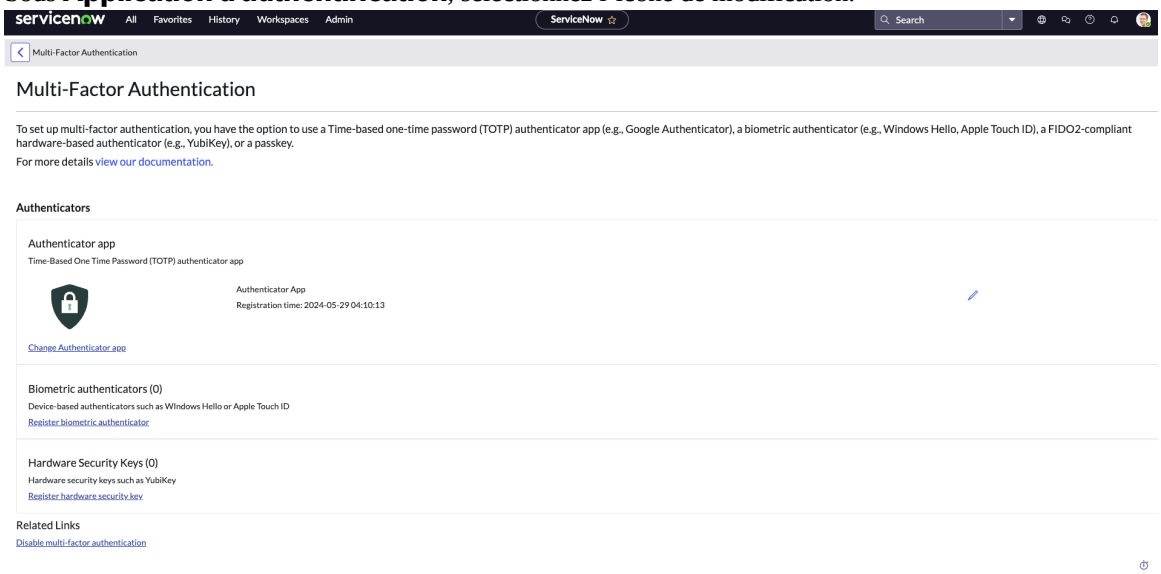
Remarque :
Vous pouvez également accéder à votre profil en cliquant sur votre nom d'utilisateur dans l'en-tête de l'instance.

2. Dans votre profil d'utilisateur, cliquez sur **Authentification multi-facteurs** dans la section **Liens connexes** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sous **Application d'authentification**, sélectionnez l'icône de modification.



4. Dans la fenêtre Modifier le code de l'authentificateur, cliquez sur **Modifier**.
5. Suivez les instructions à l'écran pour enregistrer l'application d'authentification auprès de l'appareil.

Authentification Web

Vos utilisateurs peuvent utiliser des clés matérielles ou les lecteurs biométriques de leur appareil (FIDO2) pour s'authentifier auprès d'une instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Clés matérielles



Les clés matérielles sont des éléments physiques que vous pouvez utiliser pour vous authentifier. Les clés matérielles sont insérées dans un port de votre appareil pour fournir une authentification. Pour plus d'informations sur l'enregistrement des clés matérielles, reportez-vous à la section Enregistrer une clé de sécurité matérielle.

Biométrie

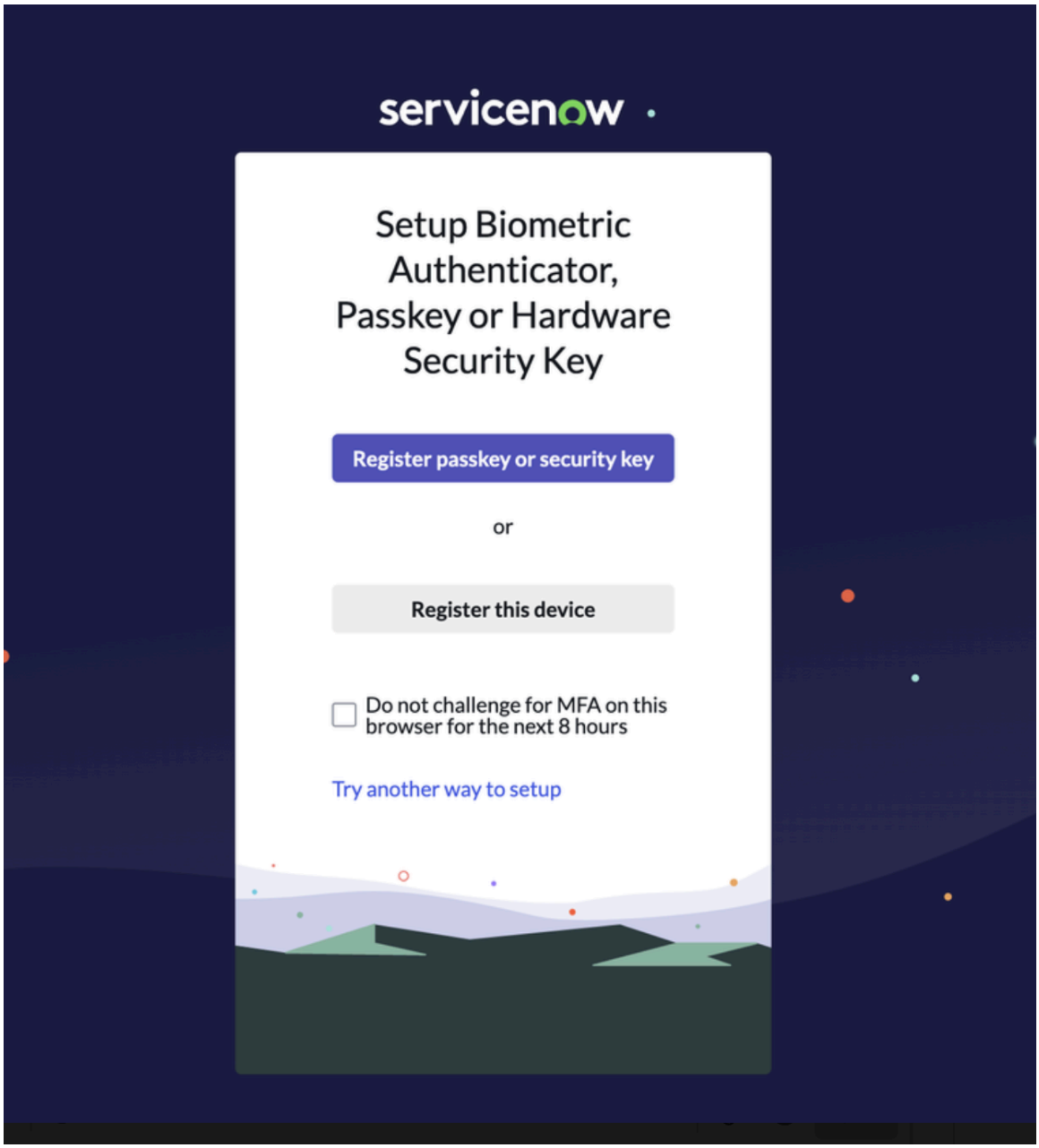


Les authentificateurs biométriques utilisent les empreintes digitales ou la reconnaissance faciale pour identifier les utilisateurs. Vos utilisateurs peuvent utiliser ces authentificateurs sur leurs appareils dans le cadre du processus de connexion multifacteur. Pour plus d'informations sur l'enregistrement des authentificateurs biométriques, reportez-vous à la section Enregistrer un authentificateur biométrique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Choisissez le deuxième facteur que vous souhaitez authentifier et authentifiez à votre instance.



Pour configurer le module d'extension d'authentification Web, reportez-vous à la section .

Enregistrer un authentificateur biométrique

Enregistrez un authentificateur biométrique à utiliser dans le cadre de votre connexion d'authentification multifacteur.

Avant de commencer
Rôle requis : aucun

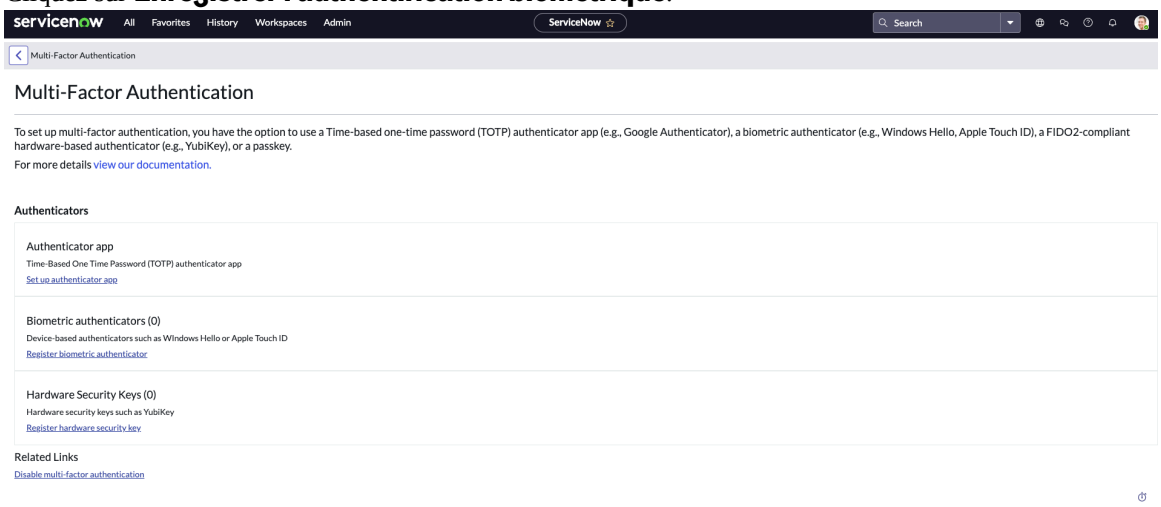
Procédure

1. Accédez à la **Tout** > **Libre-service** > **Mon profil**.
2. Sous **Liens connexes**, cliquez sur **Authentification multifacteur**.
   La page d'authentification multifacteur s'ouvre.

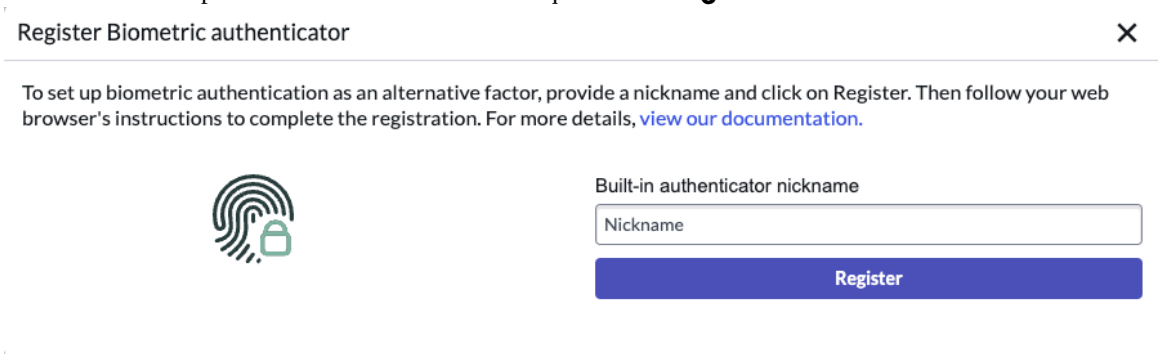
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Enregistrer l'authentification biométrique**.

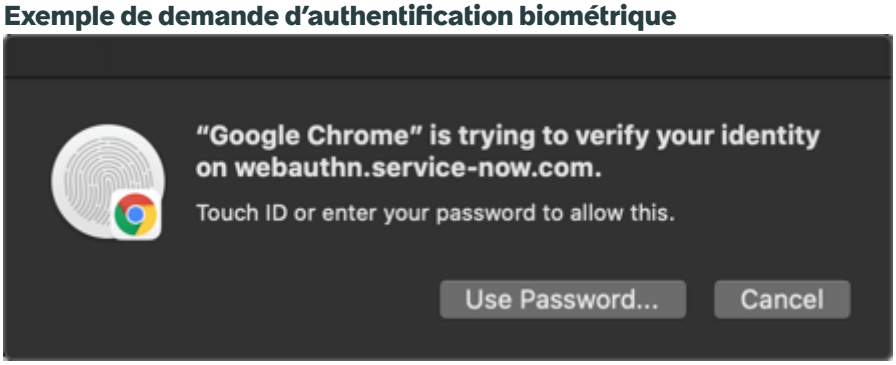


4. Entrez un surnom pour votre authentificateur et cliquez sur **Enregistrer**.



5. Lorsque vous y êtes invité, suivez les instructions à l'écran pour vous authentifier avec votre authentificateur biométrique.
   Ce message varie en fonction de votre authentificateur spécifique.

Exemple de demande d'authentification biométrique



Une fois l'authentification réussie, une fenêtre de confirmation s'affiche. Cliquez sur X pour fermer la confirmation.

Résultats

Votre authentificateur biométrique est enregistré. Vous pouvez voir l'authentificateur biométrique répertorié sur la page Authentification multifacteur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Enregistrer une clé de sécurité matérielle

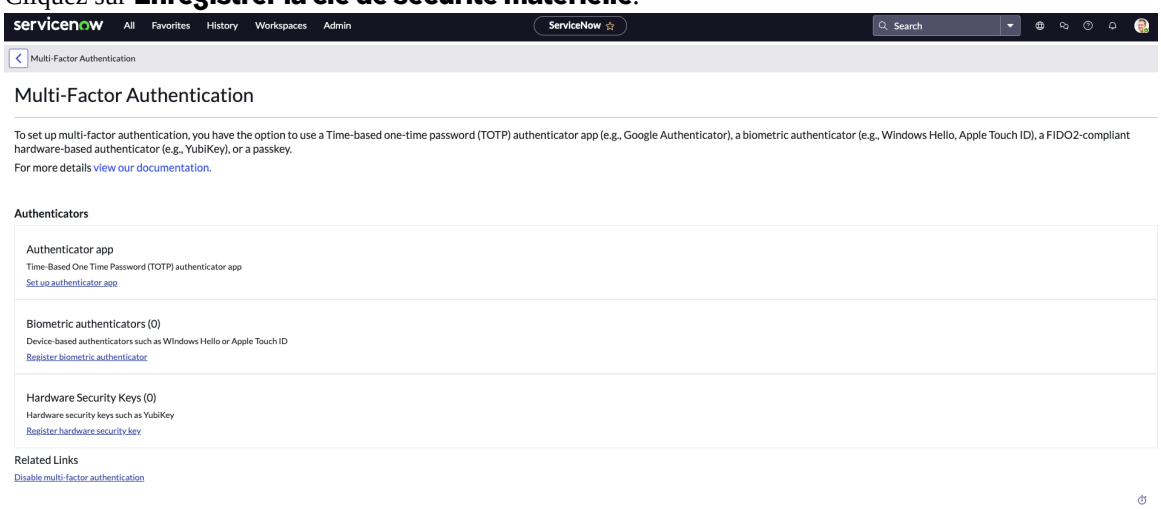
Enregistrez une clé matérielle à utiliser dans le cadre de votre connexion à l'authentification multifacteur.

Avant de commencer

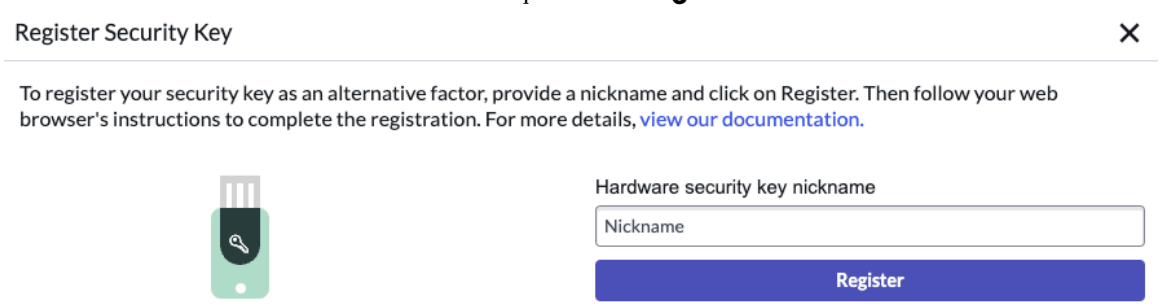
Rôle requis : aucun

Procédure

1. Accédez à la **Tout** > **Libre-service** > **Mon profil**.
2. Sous **Liens connexes**, cliquez sur **Authentification multifacteur**.
   La page Authentification multifacteur s'ouvre.
3. Cliquez sur **Enregistrer la clé de sécurité matérielle**.



4. Attribuez un surnom à votre clé matérielle et cliquez sur **Enregistrer**.



5. Lorsque vous y êtes invité, insérez votre clé de sécurité matérielle et activez-la.
   Une fois l'authentification réussie, une fenêtre de confirmation s'affiche. Cliquez sur X pour fermer la confirmation.

Résultats

Votre clé matérielle est enregistrée. Vous pouvez voir la clé matérielle répertoriée dans la page Authentification multifacteur.

Authentification multifacteur avec authentification unique

Configurez l'authentification multifacteur (MFA) avec un fournisseur SSO (Single Sign-On) pour votre ServiceNow instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étant donné que de nombreux utilisateurs de votre organisation se connectent à votre réseau d'entreprise et accèdent à votre ServiceNow instance, il est plus nécessaire de disposer d'une authentification sécurisée.

La MFA associée à la SSO offre une sécurité renforcée pour votre instance. Cette option offre la flexibilité nécessaire pour activer conditionnellement la MFA pour les utilisateurs.

Remarque :

- ServiceNow La MFA est appliquée une fois que l'utilisateur a été redirigé après une authentification réussie auprès du fournisseur d'identité.
- La MFA n'était pas appliquée avec SSO avant la version San Diego.

Par exemple, si vous souhaitez fournir à vos utilisateurs externes un protocole de sécurité supplémentaire, vous pouvez appliquer la MFA uniquement à ces utilisateurs. De cette façon, vous pouvez ajouter des capacités d'authentification supplémentaires et contrôler votre accès utilisateur.

Pour les connexions basées sur l'authentification unique telles que SAML, OpenID Connect et Digest, vous pouvez appliquer la MFA pour l'authentification.

La MFA avec SSO peut être configurée sur demande en fonction de vos besoins. À l'aide de schémas d'authentification et de fournisseurs d'identité, vous pouvez appliquer la MFA à des utilisateurs spécifiques avec un mécanisme de connexion spécifique.

Vous pouvez appliquer la MFA dans les conditions suivantes :

- Schéma d'authentification
- Fournisseur d'identité

MFA avec SSO est proposé dans le cadre du module d'extension Adaptive Authentication (com.snc.adaptive_authentication). Pour en savoir plus sur la configuration de l'authentification adaptative, reportez-vous à la section Authentification adaptative.

Configurer MFA avec SSO

Appliquez la MFA avec SSO pour vos utilisateurs à l'intérieur ou à l'extérieur de votre organisation.

Avant de commencer

La MFA avec fonctionnalité SSO est proposée dans le cadre du module d'extension Authentification adaptative (com.snc.adaptive_authentication). Vous devez activer la propriété d'authentification adaptative pour utiliser la MFA avec la fonctionnalité SSO. Pour en savoir plus sur la configuration de l'authentification adaptative, reportez-vous à la section Authentification adaptative.

Remarque :

MFA avec connexion SSO est disponible si la `glide.authenticate.mfa.with.multisso.enabled` propriété est définie sur **vrai**.

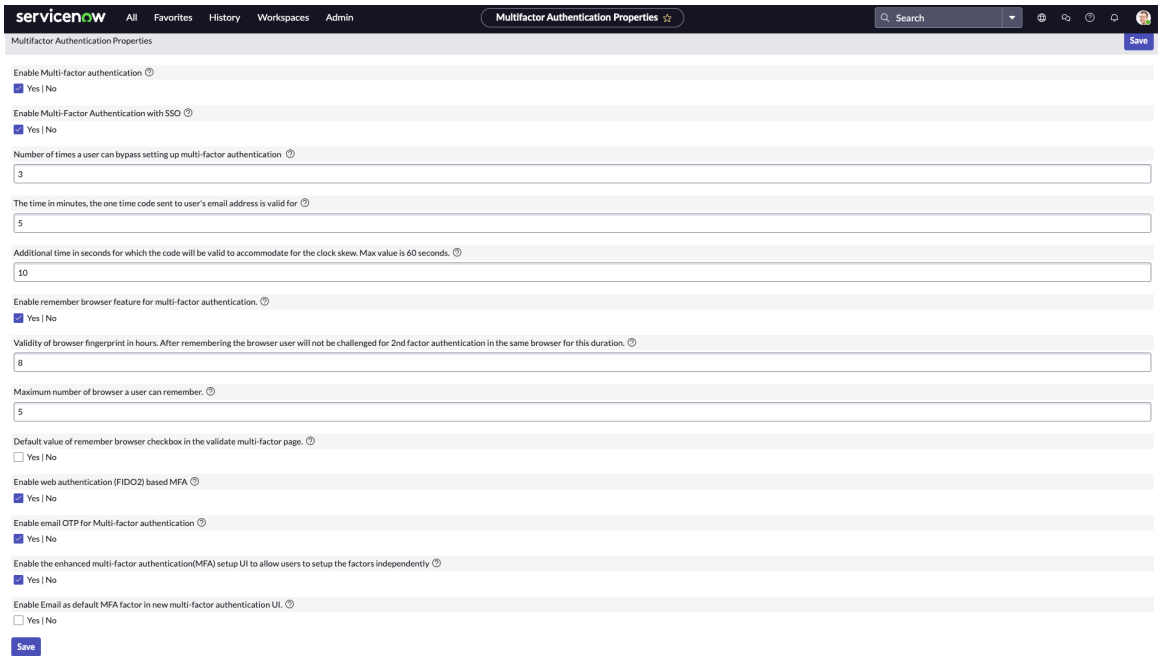
Rôle requis : administrateur

Procédure

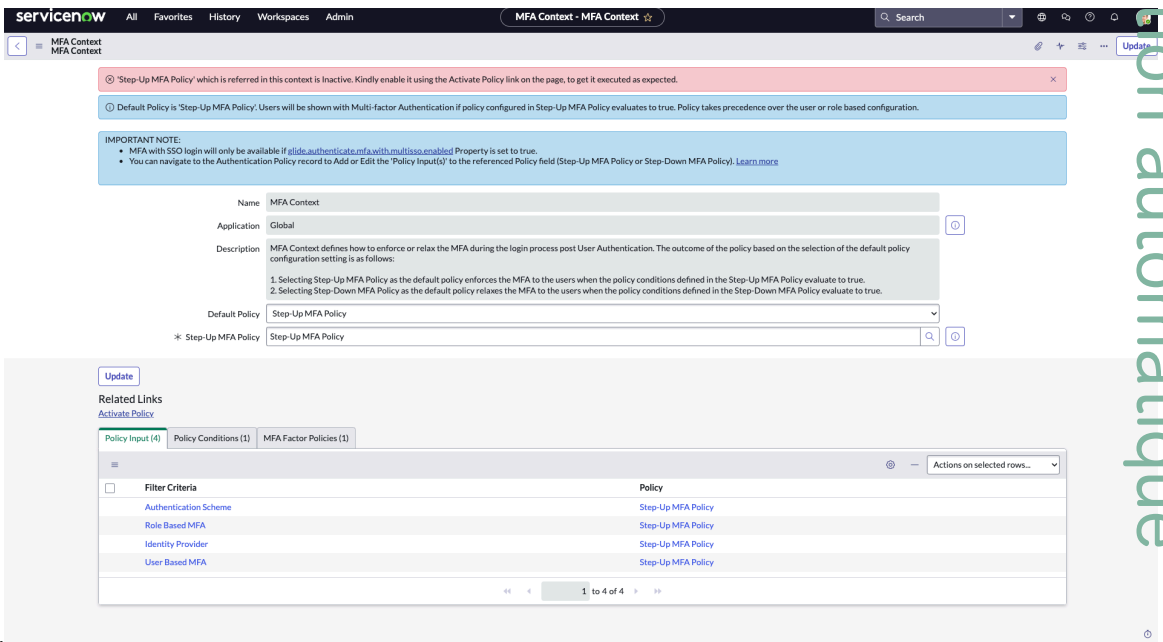
1. Accédez à la **Tout** > **Authentification multifacteur** > **Propriétés**.
2. Cochez les cases **Activer l'authentification multifacteur** et **Activer l'authentification multifacteur avec SSO** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur **Enregistrer**.
4. Accédez à la **Authentification multifacteur** > **Contexte MFA**.
   Le formulaire Contexte MFA



s'affiche.

> **Remarque :**
> Par défaut, il **s'agit d'une politique MFA ascendante**. Les utilisateurs s'affichent avec l'authentification multifacteur si une condition configurée dans la **politique de configuration MFA donne** la valeur **vrai**. La politique a priorité sur la configuration basée sur l'utilisateur ou le rôle.

5. **Facultatif :** Pour modifier une politique, revenez à l'enregistrement de la politique d'authentification, modifiez les conditions et revenez en arrière.
   Lorsque vous accédez à l'enregistrement Politique d'authentification, vous pouvez ajouter ou modifier les « Entrées de politique » aux champs de politique référencés, **Politique de MFA ascendante** ou **Politique de MFA descendante**.
6. Pour définir une nouvelle condition de police, cliquez sur **Conditions de police**.

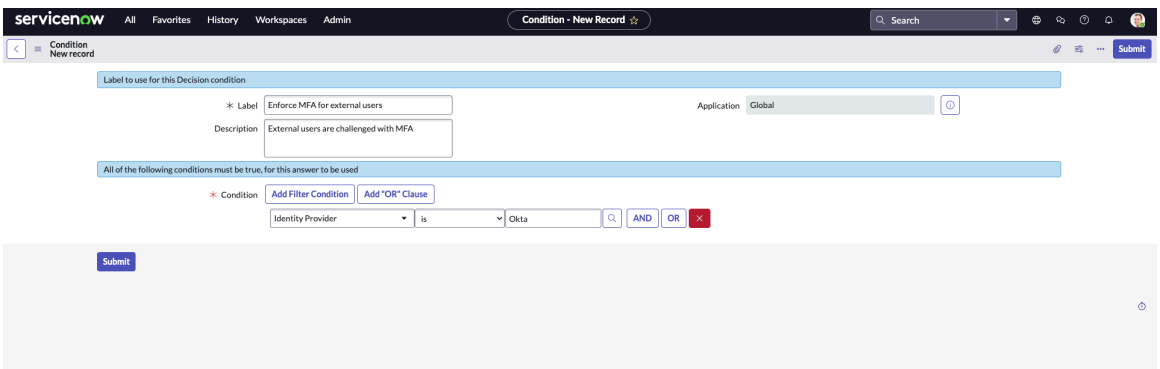
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Cliquez sur **Nouveau**.
8. Renseignez les champs du formulaire.

Formulaire de conditions

Champs	Description
Étiquette	Nom unique de la condition que vous souhaitez créer pour l'étiquette.
Description	Description de la condition de politique.
Conditions	Type de condition que vous souhaitez appliquer à la police. Vous pouvez ajouter des conditions de filtre et des clauses « OU ». **Remarque :** L'ajout de diverses conditions et clauses de filtre vous permet de contester la MFA pour des utilisateurs spécifiques.



Example

Pour configurer vos conditions, considérez l'exemple suivant. Supposons que vous souhaitez le schéma d'authentification avec le fournisseur d'identité comme condition pour les utilisateurs externes. Vous pouvez définir les conditions comme suit :

a. Sélectionnez **Schéma d'authentification** et définissez les critères sur **Authentification unique** ou **Nom d'utilisateur et mot de passe**.

   Sur la base de cette sélection, l'utilisateur reçoit une connexion basée sur l'authentification unique ou un formulaire de connexion pour spécifier le nom d'utilisateur et le mot de passe.

b. Sélectionnez **Fournisseur d'identité** et spécifiez le fournisseur en tant qu'enregistrement IdP pour lequel vous souhaitez activer la MFA. Par exemple, **Okta**.

Sur la base de cette sélection, si l'utilisateur se connecte avec SSO, il n'est pas confronté à la MFA. En revanche, si l'utilisateur se connecte à l'aide Oktade , l'utilisateur est confronté à des difficultés avec l'authentification multifacteur.

9. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Authentification adaptative

Authentification multifacteur avec authentification unique

Authentification unique (SSO) de plusieurs fournisseurs

L'authentification unique externe permet aux organisations d'utiliser plusieurs fournisseurs d'identité SSO (IdP) pour gérer l'authentification et conserver l'authentification de base de données locale (de base).

L'intégration prend en charge n'importe quelle combinaison de méthodes d'authentification locales et externes sur une seule instance :

- SAML 2.0
- Authentification Digest
- Connexion OpenID

Vous devez effectuer plusieurs étapes pour configurer l'authentification unique (SSO) de plusieurs fournisseurs, notamment la configuration des propriétés, la création de fournisseurs d'identité (IdP) et la configuration des utilisateurs pour utiliser l'authentification unique (SSO).

Par exemple, une entreprise dispersée à l'échelle mondiale peut avoir besoin d'un fournisseur SSO pour ses employés, d'un autre pour ses fournisseurs et d'une authentification de base de données locale pour ses administrateurs. Une entreprise peut également implémenter des solutions d'authentification par jeton SAML 2.0 et Digest sur la même instance.

Activer le module d'extension SSO de plusieurs fournisseurs

Cette intégration nécessite le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).

Avant de commencer

Rôle requis : admin.

Le module d'extension com.snc.integration.sso.multi.installer peut également être utilisé pour OIDC, SAML et Digest.

Rôle requis : administrateur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module d'extension Intégration - Programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Propriétés, tables et scripts SSO de plusieurs fournisseurs

Le module d'extension Intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs inclut les propriétés système, les tables et les scripts suivants.

Propriétés

La SSO de plusieurs fournisseurs ajoute les propriétés système suivantes.

Propriétés SSO de plusieurs fournisseurs

Nom	Description
glide.authenticate.multisso.debug	Active (vrai) ou désactive (faux) la journalisation de débogage pour l'intégration SSO de plusieurs fournisseurs. • Type : true | false • Valeur par défaut : faux
glide.authenticate.multisso.enabled	Active (vrai) ou désactive (faux) l'authentification unique (SSO) de plusieurs fournisseurs. • Type : true | false • Valeur par défaut : faux **Remarque :** Définir cette propriété sur faux ne désactive pas la SSO de plusieurs fournisseurs si la récupération de compte (ACR) est également activée sur l'instance. Pour vous connecter avec un nom d'utilisateur et un mot de passe, ACR doit également être désactivé à l'aide de la *glide.sso.acr.enabled* propriété. Pour obtenir des détails sur cette propriété, consultez Propriétés de récupération de compte.
glide.authenticate.multissov2_feature.enabled	Cette propriété détermine si la version MultiSSOv2 est activée dans l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tables

L'authentification unique de plusieurs fournisseurs ajoute les tables suivantes.

Tables SSO de plusieurs fournisseurs

Nom	Description
Propriétés SSO [sso_properties]	Stocke les données pour chaque IdP, schéma, données SSO communes, etc.
Propriétés SAML 2 Update 1 [saml2_update1_properties]	Stocke les données des configurations SAML 2.0 Update 1 telles que les certificats SAML.
Propriétés de synthèse [digest_properties]	Stocke les données pour les configurations d'authentification par jeton de synthèse.
Fédération SSO [sso_federation]	Stocke les données de chaque fédération SSO.
Fournisseur d'identité OIDC [oidc_identity_provider]	Stocke les données des fournisseurs d'identité basés sur Open ID Connect.

Scripts

L'authentification unique (SSO) de plusieurs fournisseurs ajoute les scripts suivants.

Scripts SSO de plusieurs fournisseurs

Nom	Description
SSO à fournisseurs multiples	Permet à un client d'avoir un type de SSO défini pour la société.
MultiSSOLogin	Permet à chaque domaine d'avoir son propre script de connexion.
MultiSSOLogout	Permet à chaque domaine d'avoir son propre script de déconnexion.
MultiSSO_OIDC_custom	Permet à un utilisateur de définir un script Single Sign-on personnalisé pour la connexion OIDC.
MultiSSO_OIDC_logout_custom	Permet à un utilisateur de définir un script de déconnexion personnalisé pour la connexion OIDC.
MultiSSO_Abstract_Core	Fournit une classe de base pour toutes les classes SSO de fournisseurs multiples.
MultiSSO_ClientHelper	Fournit des fonctions d'utilitaire d'appel de client pour l'authentification unique (SSO) de plusieurs fournisseurs.
MultiSSO_DigestedToken	Fournit une logique système de base pour l'authentification par jeton digéré.
MultiSSO_SAML2_Update1	Fournit une logique pour traiter l'authentification SAML 2.0 Update 1 pour une authentification unique mutualisée.

Configurations SSO de plusieurs fournisseurs

Vous devez effectuer plusieurs étapes pour configurer l'authentification unique (SSO) de plusieurs fournisseurs, notamment la configuration des propriétés, la création de fournisseurs d'identité (IdP) et la configuration des utilisateurs pour utiliser l'authentification unique (SSO).

Consultez les rubriques suivantes pour en savoir plus sur chacune des configurations.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Flux d’authentification IdP SSO de plusieurs fournisseurs (SAML)
- Configurer les propriétés SSO de plusieurs fournisseurs
- Créer un fournisseur d’identité externe
- Configurer les utilisateurs pour la SSO de plusieurs fournisseurs

Configurer les propriétés SSO de plusieurs fournisseurs

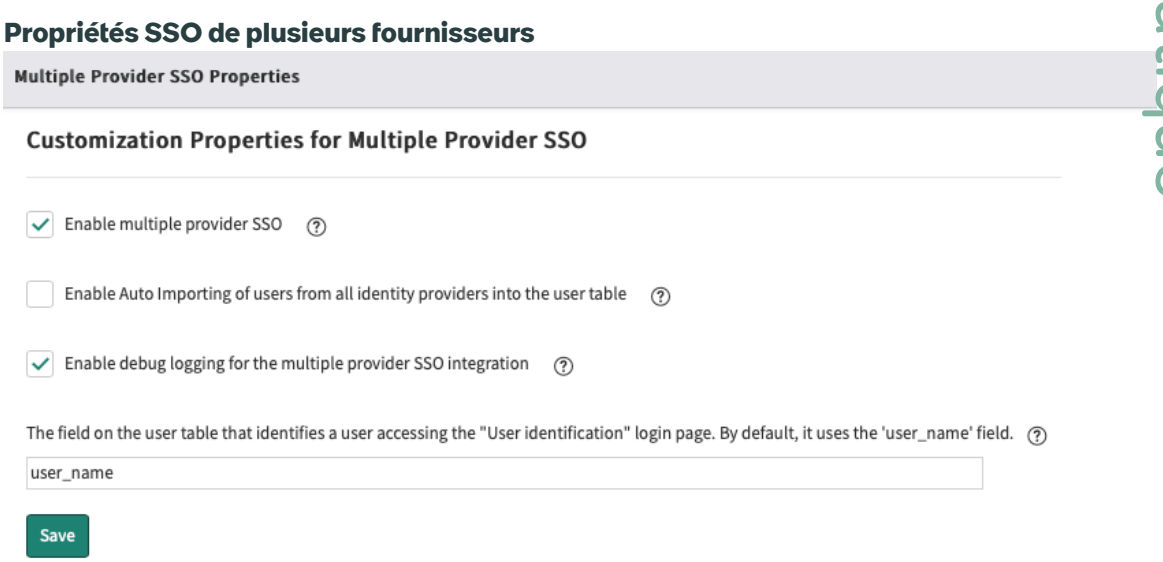
Configurez les propriétés SSO et ajoutez une propriété à la table Propriétés système pour configurer une liste d’inclusion d’IdP.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Administration** > **Propriétés**.
2. Cochez la case **Activer l’authentification unique de plusieurs fournisseurs** .
   Cette sélection ajoute le lien Utiliser une connexion externe à la page de connexion.
3. Pour mettre à jour la table utilisateur avec les utilisateurs dans l’IdP, sélectionnez l’option **Activer l’importation automatique** .
4. Pour que les messages de débogage s’affichent au bas du cadre de contenu, cochez la case **Activer la journalisation du débogage pour l’intégration SSO de plusieurs fournisseurs** .
   Si elle est activée, la fonctionnalité de journalisation de débogage ralentit les performances et utilise de l’espace disque pour générer des journaux.
5. Dans la propriété **Champ de la table utilisateur qui identifie un utilisateur accédant à la page de connexion d’identification de l’utilisateur**, saisissez le champ de la table Utilisateur qui contient la valeur que l’IdP utilise pour identifier l’utilisateur. La valeur par défaut est **user_name**.

   La valeur par défaut est **user_name**.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Enregistrer**.
7. Demandez à vos utilisateurs de cliquer sur le lien **Utiliser une connexion externe** lorsqu'ils se connectent à l'instance.

Information associée

Attribution d'utilisateurs SAML

Créer un fournisseur d'identité externe

Une fois que vous avez configuré les propriétés SSO de plusieurs fournisseurs, vous pouvez mettre à jour ou créer un nouveau fournisseur d'identité SAML 2.0 ou de jeton de synthèse.

Avant de commencer

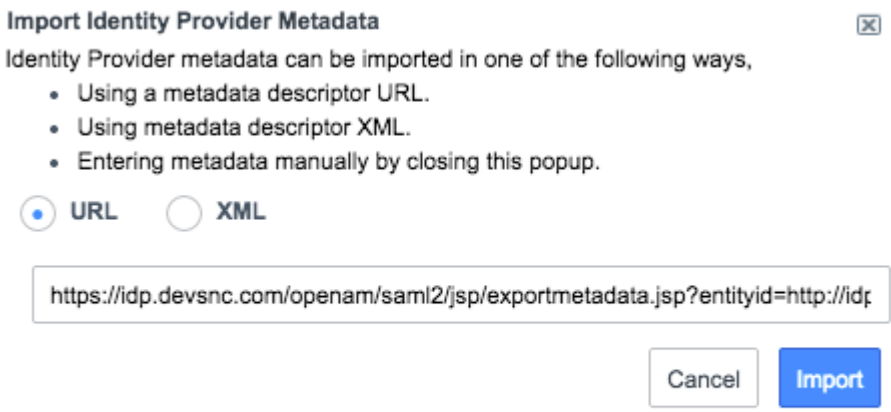
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Pour modifier un enregistrement de fournisseur d'identité, cliquez sur l'enregistrement.
   - Pour les configurations de jetons de synthèse, mettez à jour manuellement les propriétés.
   - Pour les configurations de la mise à jour 1 de SAML2, mettez à jour automatiquement les métadonnées du fournisseur d'identité avec le lien connexe **Importer les métadonnées du fournisseur d'identité** ou mettez à jour les propriétés manuellement.
   - Pour les configurations OpenID Connect, mettez à jour manuellement les propriétés.
3. Pour créer un fournisseur d'identité, cliquez sur **Nouveau**.
   - Pour les configurations des jetons de synthèse : cliquez sur **SSO de synthèse** et entrez les propriétés de synthèse pour l'authentification unique de plusieurs fournisseurs.
   - Pour les configurations SAML2 : cliquez sur **MultiSSOV2_SAML2_custom** et importez les métadonnées du fournisseur d'identité à partir d'une URL, au format XML, ou saisissez manuellement les informations du fournisseur d'identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



- Pour OpenID Connect : cliquez sur **OpenID Connect** et saisissez l'ID client, le secret client et l'URL de configuration connue.

4. Pour faire de l'IdP l'IdP de basculement utilisé lorsque l'IdP par défaut n'est pas disponible, cochez la case **Par défaut** .

   Si SAML 2 Update 1 est actif et que vous effectuez une mise à niveau vers la version Fuji, l'IdP SAML 2 Update 1 est sélectionné comme basculement par défaut. Aucun IdP de basculement par défaut n'est sélectionné pour les nouvelles instances ou si vous effectuez une mise à niveau à partir d'une version sur laquelle SAML 2 Update 1 n'est pas actif.

   Remarque :
   Le processus d'importation des métadonnées crée automatiquement un enregistrement de certificat pour le fournisseur d'identité. Accédez au module **Certificat x509** pour voir le certificat.

   Remarque :
   Les certificats pour l'authentification unique doivent toujours être au format PEM pour fonctionner avec les certificats SAML.

5. Si la signature électronique est active, configurez le formulaire du fournisseur d'identité et ajoutez **l'URL de consommateur d'assertion pour le champ d'authentification de signature électronique** . Dans la plupart des cas, cette URL est : https://YOURINSTANCE.service-now.com/consumer.do. Toutefois, si vous utilisez une méthode personnalisée de gestion de l'authentification SAML pour les signatures électroniques, vous pouvez configurer votre propre URL de consommateur. Si vous utilisez uniquement SAML 2.0 Update 1 et que vous n'utilisez pas l'authentification unique de plusieurs fournisseurs, configurez l'URL de consommateur d'assertion avec les propriétés SAML de signature électronique.

Générer les métadonnées du fournisseur de service d'instance (SP) pour le SAML

Dans le cadre de votre configuration SSO, vous pouvez générer les métadonnées du SP d'instance à fournir à l'IdP.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
L'IdP a besoin des métadonnées du SP d'instance pour s'authentifier et transmettre les demandes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Choisissez votre module d'extension SSO installé :

Option	Description
Authentification unique (SSO) de plusieurs fournisseurs	Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**. Choisissez un IdP et cliquez sur le bouton **Générer les métadonnées** . L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres des propriétés système.
SAML 2 SSO	Accédez à la **Authentification unique SAML 2** > **Métadonnées**. L'intégration génère automatiquement les métadonnées SP de l'instance à partir des paramètres des propriétés système.

2. Copiez les métadonnées du portail de services dans la zone de texte.

   Par exemple :

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
 entityID="https://yourinstance.service-now.com">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
 Location="https://yourinstance.service-now.com/navpage.do" />

 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFor
mat>
  <AssertionConsumerService isDefault="true" index="0"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/navpage.do" />
  <AssertionConsumerService index="1"
 Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="https://yourinstance.service-now.com/consumer.do"/>
 </SPSSODescriptor>
</EntityDescriptor>
```

3. Fournissez les métadonnées du fournisseur de services d'instance à l'IdP.
   Par exemple, SSOCircle permet à un utilisateur de fournir les métadonnées SP en ligne.

Configurer les utilisateurs pour la SSO de plusieurs fournisseurs

Les administrateurs peuvent configurer la SSO de plusieurs fournisseurs pour des utilisateurs individuels ou pour tous les utilisateurs appartenant à une société. Vous ne pouvez pas configurer la SSO de plusieurs fournisseurs pour les groupes.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Cliquez avec le bouton droit sur un enregistrement de fournisseur d'identité, puis sélectionnez **Copier sys_id**.
3. Copiez les données dans votre presse-papiers.
4. Accédez à un enregistrement d'utilisateur ou de société.
5. Configurez le formulaire et ajoutez le champ **Source SSO** .
6. Dans le champ **Source SSO** , entrez l'une des valeurs suivantes :
   - **Utilisateurs SAML** : entrez **SSO :** suivi de l'sys_id de l'enregistrement du fournisseur d'identité.
   - **Utilisateurs de la fédération SSO: entrez la fédération :** suivi de la sys_id de l'enregistrement de la fédération.
7. Cliquez sur **Mettre à jour**.

Test des connexions IdP

Le test de la connexion à un fournisseur d'identités valide les paramètres avant d'activer l'authentification externe.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La version Jakarta prend en charge le test de la connexion dans une fenêtre contextuelle. Si votre IdP ne fonctionne pas correctement avec cette option, vous pouvez désactiver ce paramètre par défaut.
La tâche d'actualisation des métadonnées IdP à fournisseurs multiples récupère et met à jour le certificat pour l'IdP lors de la création, de la mise à jour ou du test de la connexion.

Remarque :
Pour certains tickets IdP, en cas d'échec de la connexion de test, ils doivent créer glide.authenticate.multisso.test.connection.mandatory avec la valeur false et vous pouvez activer l'IdP sans la connexion de test.

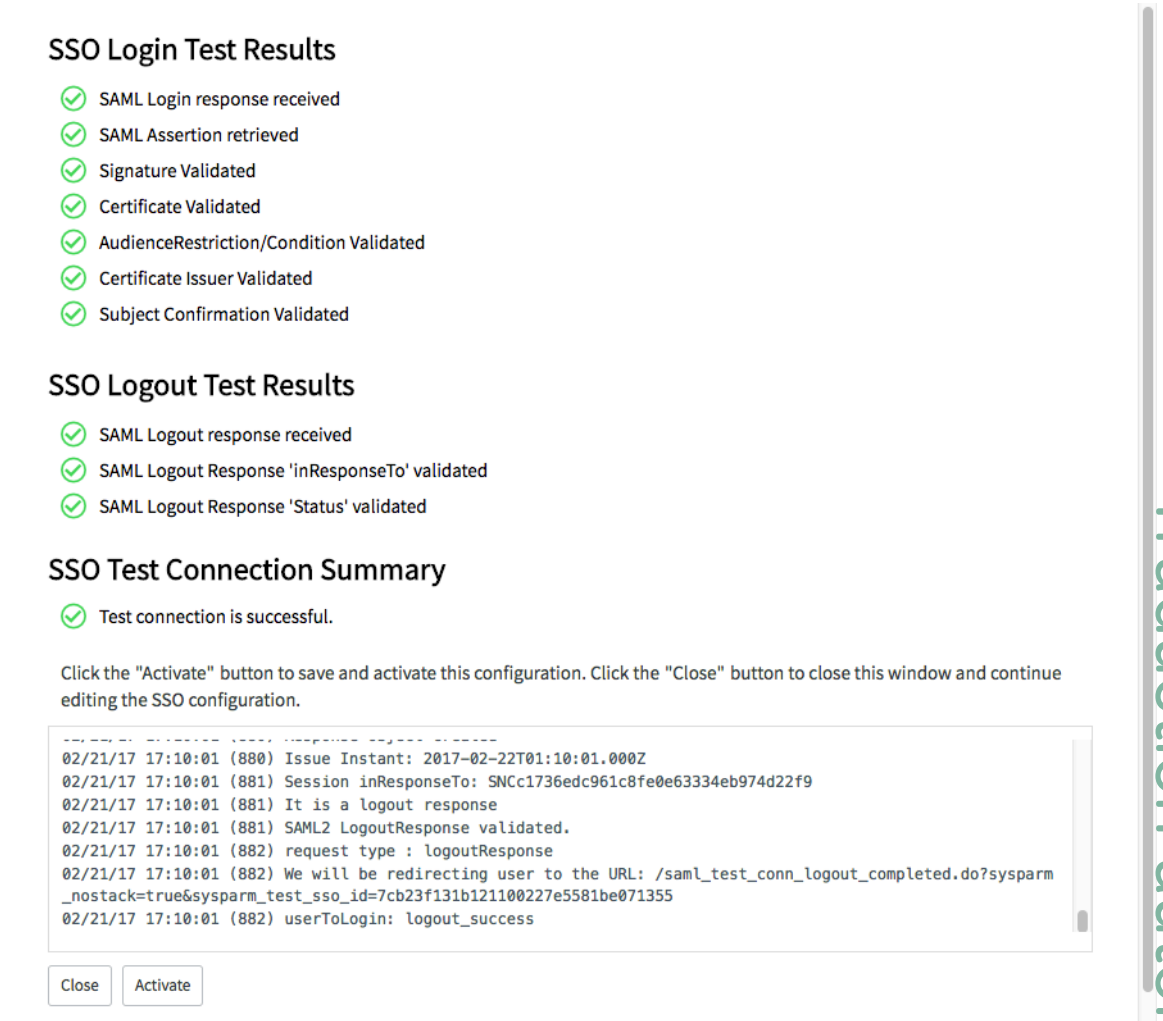
Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Sélectionnez un IdP défini ou cliquez sur **Nouveau** pour définir un nouvel IdP.
3. **Facultatif :** Configurez un fournisseur d'identité si vous configurez un nouvel IdP.
4. Cliquez sur **Test de la connexion**, entrez les informations d'identification de connexion pour l'IdP afin de vérifier la connexion.
   Vous ne pouvez pas activer l'IdP tant que vous n'avez pas réussi à tester la connexion. Si le test échoue, vous pouvez mettre à jour pour enregistrer vos informations de configuration, mais vous ne pouvez pas activer cette configuration.
5. Vérifiez les résultats à l'aide de la section **Résultats/résumé des tests SSO** ou de la section **Test des journaux SSO** pour afficher les messages du journal.
   En cas d'erreurs, reportez-vous à la section Erreurs et correctifs de l'authentification unique (SAML 2.0)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Cliquez sur **Annuler** lorsque le test est terminé.



Erreurs de connexion IdP courantes

Le tableau suivant décrit certaines des erreurs de connexion IdP courantes et leurs solutions.

Dépannage des connexions de test IdP

Messages d'erreur	Solution
Échec de la validation du champ Utilisateur. Champ d'utilisateur non valide « < nom de champ > » n'est pas un champ de sys_user table.	Vérifiez que le contenu du champ Table d'utilisateur que vous avez sélectionné correspond au jeton NameID SAML.
L'émetteur de l'assertion n'est pas valide.	Vérifiez que **l'URL du fournisseur d'identité** contient une URL valide pour votre fournisseur d'identité. Chaque URL IdP doit être unique.
Échec de la validation de AudienceRestriction.	Vérifiez que **l'URI de l'audience** contient une URL valide pour votre instance.
Impossible de se déconnecter de la session d'IdP.	Vérifiez que l'URL **SingleLogoutRequest** contient une URL valide vers le service de déconnexion de votre fournisseur d'identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage des connexions de test IdP (suite)

Messages d'erreur	Solution
La signature n'a pas été validée par rapport à la clé d'informations d'identification.	Vérifiez qu'un certificat valide est installé sur l'IdP.

Résoudre les problèmes de script avec SAML

Résolvez les problèmes de script avec SAML. Vous pouvez rencontrer des problèmes de script si le SAML est déjà actif au moment de l'activation de l'authentification unique multiple et si vous avez déjà personnalisé les sorties d'installation.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Sauvegardez les SAML2SingleSignon_update1 de sortie d'installation et les SAML2_update1 d'include de script modifiés.
2. Rétablissez la sortie d'installation et l'include de script à la version disponible avec le système de base de référence.
3. Activez ou mettez à niveau le module **d'extension Intégration - Programme d'installation de l'authentification unique de plusieurs fournisseurs** .
   Le système met à niveau SAML et tous les fichiers nécessaires vers SAML 2 Update 1.
4. Ouvrez la page des propriétés de l'authentification unique à plusieurs fournisseurs et cochez la case **Activer l'authentification unique de plusieurs fournisseurs** pour l'activer.
5. Placer les changements de sortie de l'installation SAML2SingleSignon_update1 dans le **MultiSSO_SAML2_Update1 d'inclusion de script de base de référence et les changements d'inclusion de script de SAML2_update1** dans l'include de script de SAML2_update1 de base de référence.

Se connecter à l'aide de l'authentification unique (SSO) de plusieurs fournisseurs

La méthode recommandée et la plus efficace pour que les utilisateurs se connectent à l'aide de la SSO de plusieurs fournisseurs consiste à utiliser une URL spécifiquement configurée.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Une fois la SSO de plusieurs fournisseurs configurée, vous pouvez envoyer une URL à vos utilisateurs avec l'IdP correct dans la chaîne de paramètres. Par exemple :

```
/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Une fois qu'un utilisateur s'est connecté avec succès à la page IdP, un cookie contenant le sys_id IdP est ajouté au navigateur. La prochaine fois que l'utilisateur tentera de se connecter, le système redirigera l'utilisateur vers le serveur IdP, qui se connectera automatiquement à l'instance.

Si un paramètre d'URL n'est pas défini ou si le cache du navigateur a été effacé, les utilisateurs peuvent également effectuer les opérations suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Cliquez sur le lien **Utiliser une connexion externe** sur la page de connexion.

   La page de connexion externe s'affiche. Les utilisateurs peuvent cliquer sur **Utiliser la connexion locale** pour revenir à la page de connexion standard.

2. Saisissez la valeur du champ spécifié dans la table utilisateur que vous avez configurée dans les propriétés SSO de plusieurs fournisseurs.

   L'utilisateur est redirigé vers le serveur IdP, où il se connecte.

Résultats

Une fois que les utilisateurs se sont connectés à un fournisseur d'identité, ils sont automatiquement redirigés vers cet fournisseur d'identités chaque fois qu'ils tentent d'accéder à l'instance. Pour qu'un utilisateur accède à un autre IdP, envoyez-lui une URL avec les nouvelles informations IdP dans le paramètre. Le nouvel IdP remplace l'ancien IdP dans le cookie si l'utilisateur se connecte avec succès. Si l'utilisateur ne parvient pas à se connecter, les anciennes informations IdP sont conservées dans le cookie.

Permettre aux utilisateurs de choisir le fournisseur d'identité pour la connexion

La prise en charge de la fédération SSO permet aux utilisateurs de choisir l'IdP auquel se connecter.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Les fédérations SSO regroupent les métadonnées de plusieurs IdP et fournisseurs de service, y compris votre instance. Les fédérations publient ensuite les métadonnées sous la forme d'un fichier XML, qui comprend des informations telles que les noms d'IdP et les certificats d'IdP. Les administrateurs peuvent ensuite demander à l'instance de lire le fichier XML et remplir automatiquement la table Propriétés SSO avec toutes les informations IdP nécessaires.

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fédération**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs comme il convient (voir la table).
4. Cliquez sur **Envoyer**.
5. Après avoir configuré une fédération, activez la tâche planifiée d'actualisation des métadonnées SSO, puis configurez les utilisateurs auxquels vous souhaitez donner accès aux IdP de fédération. Utilisez les sys_ID de l'enregistrement de fédération que vous venez de créer.

   Utilisez les sys_ID de l'enregistrement de fédération que vous venez de créer.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L’instance remplit la table des propriétés SSO avec les informations IdP. Lorsque les utilisateurs configurés pour utiliser la fédération se connectent, ils sont redirigés vers l’URL du service de détection que vous avez configurée. Ensuite, ils sélectionnent l’IdP et fournissent les informations d’identification nécessaires. Vous pouvez également envoyer aux utilisateurs une URL avec l’IdP dans le paramètre.

Permettre aux utilisateurs de choisir le fournisseur d’identité pour la connexion

Champ	Description
Nom	Entrez un nom descriptif pour la fédération.
Actif	Cochez cette case pour permettre à l’instance d’extraire le fichier XML de la fédération.
Type	Sélectionnez le type d’authentification pris en charge par cette fédération.
Découverte Service URL	Saisissez l’URL du service de découverte pour cette fédération. Il s’agit du site où les utilisateurs sont invités à sélectionner un IdP et à se connecter.
URL des métadonnées	Entrez l’URL du fichier XML qui contient les métadonnées de fédération.
Certificat x509	Sélectionnez le certificat de fédération.
Domaine	Sélectionnez le domaine auquel les données appartiendront.

Remarque :
L’IdP de gestion des identités fédérées InCommon est préconfiguré.

Utiliser Portail de services avec la SSO de plusieurs fournisseurs pour rediriger une URL

Portail de services utilise une combinaison de propriétés système et d’includes de script pour déterminer comment le système gère les redirections d’URL pour les utilisateurs qui se connectent au portail.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Si vous utilisez la propriété système pour effectuer automatiquement une redirection vers votre fournisseur d’identité principal (IdP), alors Portail de services vous êtes automatiquement redirigé vers cet IdP. Si vous avez plusieurs IdP, Portail de services affiche un lien sur la page de connexion pour **utiliser une connexion externe**.

Procédure

1. Configurer la page de connexion de Portail de services
2. Rediriger vers Portail de services après la connexion

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Récupération de compte (ACR)

Les administrateurs peuvent configurer la récupération de compte (ACR) pour effectuer des activités de récupération telles que le traitement d'une erreur de configuration SSO ou de certificats expirés.

Remarque :
L'activation d'ACR désactive les connexions interactives locales (basées sur le nom d'utilisateur ou le mot de passe) lorsque la SSO est activée vers vos instances.

ACR fournit les fonctionnalités suivantes :

- Contournez votre connexion Single Sign-On (SSO) pour résoudre les problèmes de configuration SSO en tant qu'administrateur.
- Connectez-vous à l'aide de l'authentification unique (SSO) pour effectuer des tâches avec un compte administrateur configuré en tant que récupération de compte.
- Les flux ACR permettent aux administrateurs d'utiliser des options en libre-service pour traiter la récupération de compte lorsque la récupération est nécessaire (par exemple, configuration SSO incorrecte, certificats expirés).
- Réduisez les accès non autorisés à l'instance et fournissez une base solide pour l'utilisation d'ACR en dehors des cas d'utilisation SSO.

Nouvelle instance

Pour qu'une nouvelle instance utilise ACR, procédez comme suit :

- Activez le module d'extension Mutli-SSO (`com.snc.integration.sso.multi.installer`)
- Activer ACR (`glide.sso.acr.enabled`) : cette option est activée par défaut dans le cas d'une nouvelle instance.
- Avant d'activer la propriété SSO (`glide.authenticate.multisso.enabled`), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.

  Remarque :
  Définir cette propriété sur faux ne désactive pas la SSO de plusieurs fournisseurs si la récupération de compte (ACR) est également activée sur l'instance. Pour vous connecter avec un nom d'utilisateur et un mot de passe, ACR doit également être désactivé à l'aide de la *`glide.sso.acr.enabled`* propriété. Pour obtenir des détails sur cette propriété, consultez Propriétés de récupération de compte.

- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer MFA avant de s'inscrire en tant qu'utilisateur ACR.

Instance mise à niveau

Pour qu'une instance mise à niveau utilise ACR, procédez comme suit :

- Activez le module d'extension Mutli-SSO (`com.snc.integration.sso.multi.installer`)
- Activer ACR (`glide.sso.acr.enabled`)

  Remarque :
  En cas de mise à niveau de l'instance, l'administrateur doit activer ACR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Avant d'activer la propriété SSO (glide.authenticate.multisso.enabled), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.
- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer MFA avant de s'inscrire en tant qu'utilisateur ACR.

Configurer les utilisateurs de récupération de compte

Pour utiliser la récupération de compte, vous devez enregistrer au moins un compte administrateur en tant qu'utilisateur de récupération de compte. L'authentification unique ne peut pas être activée sur votre instance tant qu'au moins un compte n'est pas configuré. Pour obtenir des détails sur ce processus, consultez Configurer un utilisateur de récupération de compte à partir de la page Propriétés de récupération de compte.

Remarque :
Si vous mettez à niveau une instance qui utilise déjà l'authentification unique vers une version ultérieure Rome , l'authentification unique continuera de fonctionner sans qu'un utilisateur de récupération ne soit configuré.

Configuration de la récupération du compte

La fonctionnalité de récupération de compte est incluse dans les **modules d'extension Intégration - Programme d'installation de l'authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer).** La fonctionnalité est activée par défaut. Vous pouvez modifier ce paramètre et d'autres paramètres de récupération de compte à l'aide des propriétés système. Pour en savoir plus sur ces propriétés, reportez-vous à la section Propriétés de récupération de compte.

Contexte de politique de récupération de compte

Une fois que vous avez enregistré un utilisateur de récupération de compte et activé l'authentification unique (SSO), votre instance restreint toutes les connexions locales. Cette restriction est définie dans le contexte **SSO - ACR contexte** de politique d'authentification. Pour plus d'informations sur le contexte, reportez-vous à Contexte de récupération de compte.

Pour en savoir plus sur le fonctionnement des politiques d'authentification et des contextes de politique sur votre instance, reportez-vous à la section Authentification adaptative.

Configurer un utilisateur de récupération de compte

Configurez un utilisateur de récupération de compte pour effectuer des activités de récupération de compte sur votre instance.

Un utilisateur de récupération de compte est un compte d'utilisateur que les administrateurs peuvent utiliser pour effectuer des tâches de récupération de compte, telles que le traitement d'une erreur de configuration SSO ou le traitement des certificats expirés.

Remarque :
Si vous utilisez la récupération de compte sur votre instance, vous devez configurer un utilisateur de récupération de compte. Cette étape est nécessaire avant d'activer l'authentification unique de plusieurs fournisseurs sur une instance.

Configurer un utilisateur de récupération de compte à partir de la page Propriétés de récupération de compte

Configurez une récupération de compte à partir de la page des propriétés de récupération de compte.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Pour qu'une nouvelle instance configure ACR, procédez comme suit :

- Activez le module d'extension Mutli-SSO (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled) : cette option est activée par défaut dans le cas d'une nouvelle instance.
- Avant d'activer la propriété SSO (glide.authenticate.multisso.enabled), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.
- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer MFA avant de s'inscrire en tant qu'utilisateur ACR.

Pour qu'une instance mise à niveau utilise ACR, procédez comme suit :

- Activez le module d'extension Mutli-SSO (com.snc.integration.sso.multi.installer)
- Activer ACR (glide.sso.acr.enabled)

  Remarque :
  En cas de mise à niveau de l'instance, l'administrateur doit activer ACR.

- Avant d'activer la propriété SSO (glide.authenticate.multisso.enabled), l'administrateur doit s'inscrire en tant qu'utilisateur ACR.

  Remarque :
  Définir cette propriété sur faux ne désactive pas la SSO de plusieurs fournisseurs si la récupération de compte (ACR) est également activée sur l'instance. Pour vous connecter avec un nom d'utilisateur et un mot de passe, ACR doit également être désactivé à l'aide de la *glide.sso.acr.enabled* propriété. Pour obtenir des détails sur cette propriété, consultez Propriétés de récupération de compte.

- L'administrateur doit définir un mot de passe pour la connexion locale et enregistrer MFA avant de s'inscrire en tant qu'utilisateur ACR.

Procédure

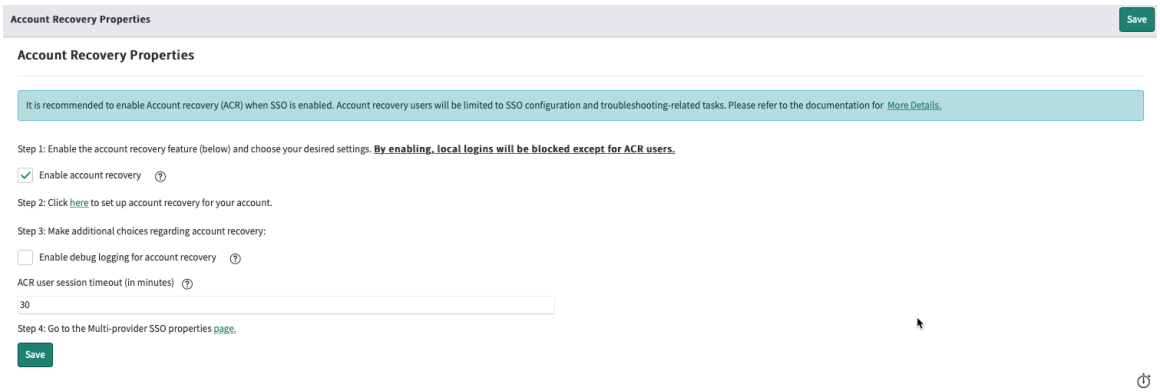
1. Accédez à la **Tout** > **Récupération de compte** > **Propriétés**.
2. Cliquez sur **Activer la récupération de compte**.

   Remarque :
   Vous devez activer la récupération de compte lorsque la SSO est activée. Les utilisateurs de la récupération de compte seront limités à la configuration SSO et aux tâches liées au dépannage.

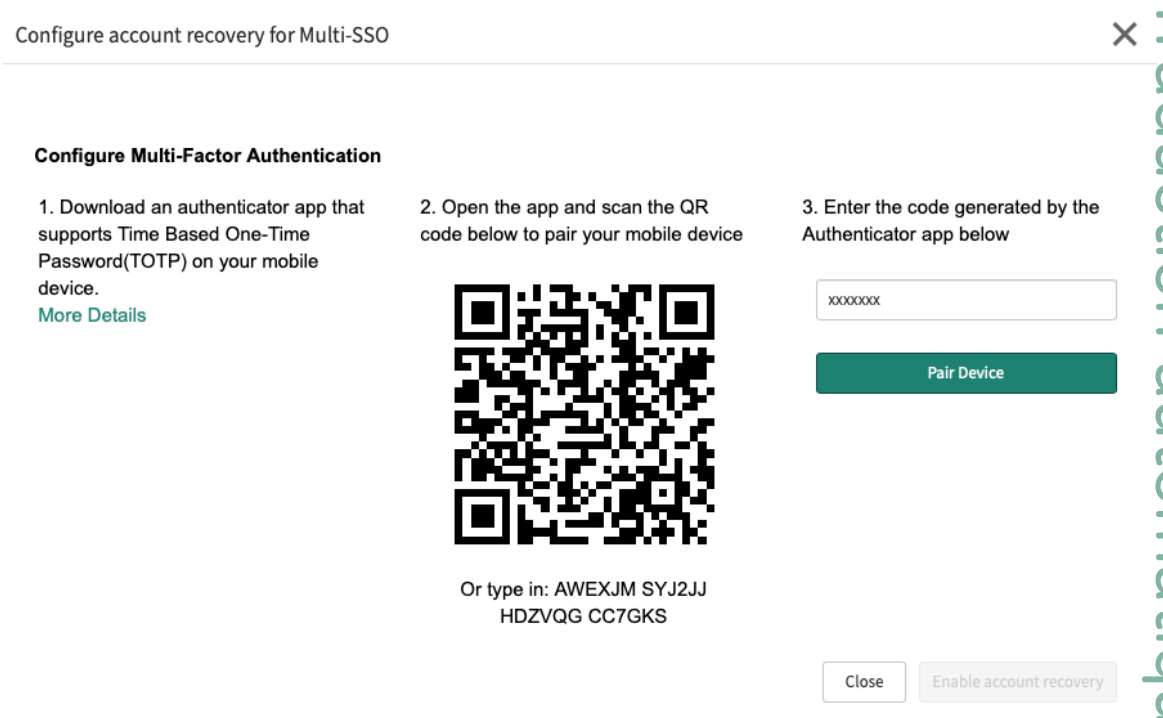
3. Cliquez sur le texte **ici** à l'étape 2.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. En suivant les instructions à l'écran dans le modal **Configurer la récupération de compte pour l'authentification unique (SSO) à fournisseurs multiples** .



Une fois les étapes à l'écran terminées, **l'option Activer la récupération de compte** est activée.

5. Cliquez sur **Activer la récupération de compte**.

Résultats

Vous avez configuré votre compte d'utilisateur en tant qu'utilisateur de récupération de compte. Vous pouvez vérifier ce compte et afficher tous les autres utilisateurs de récupération de compte configurés en accédant à **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Utilisateurs**.

Configurer un utilisateur de récupération de compte à partir d'un profil d'utilisateur administrateur

Configurez un administrateur en tant qu'utilisateur de récupération de compte à partir du profil d'utilisateur administrateur.

Traduction automatique

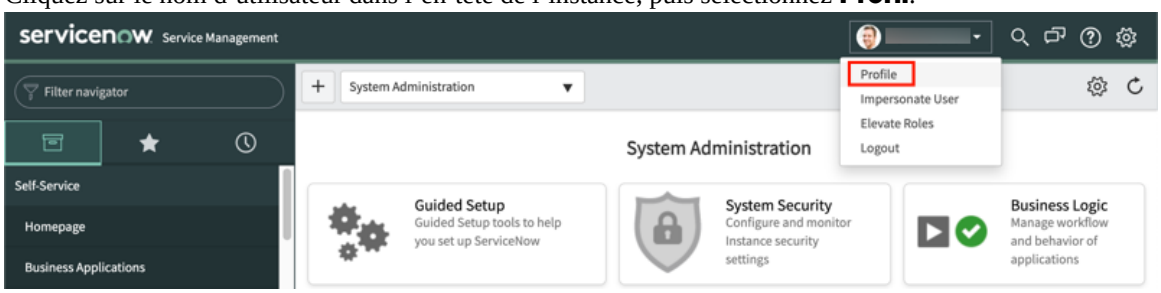
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

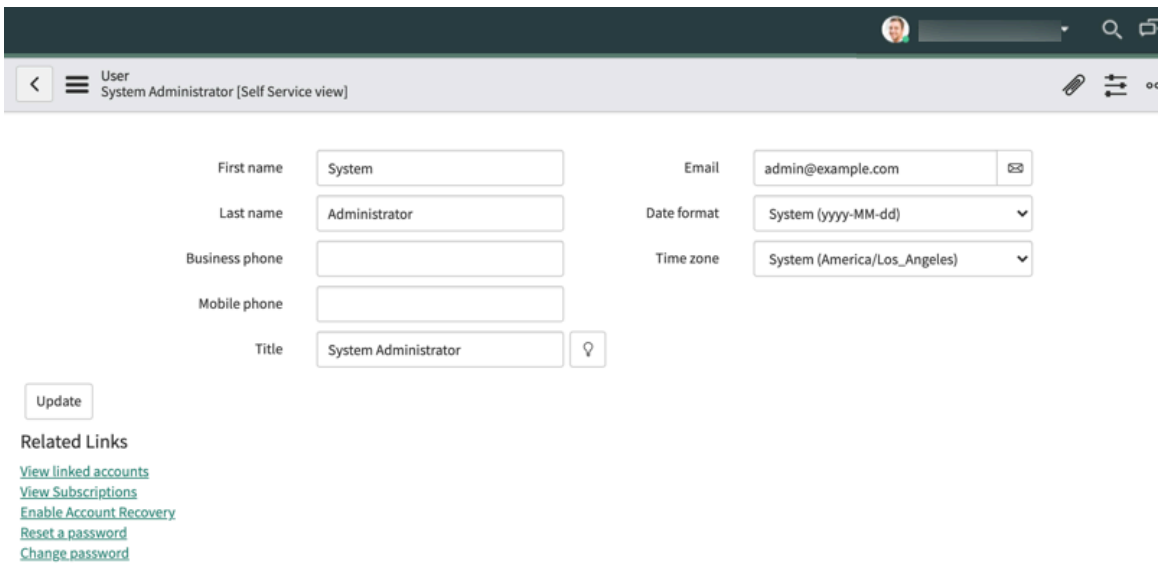
Rôle requis : administrateur

Procédure

1. Connectez-vous à votre instance à l'aide d'un compte administrateur.
2. Cliquez sur le nom d'utilisateur dans l'en-tête de l'instance, puis sélectionnez **Profil**.



3. Dans le formulaire **Utilisateur** , cliquez sur **Activer la récupération de compte** dans la section **Liens connexes** .



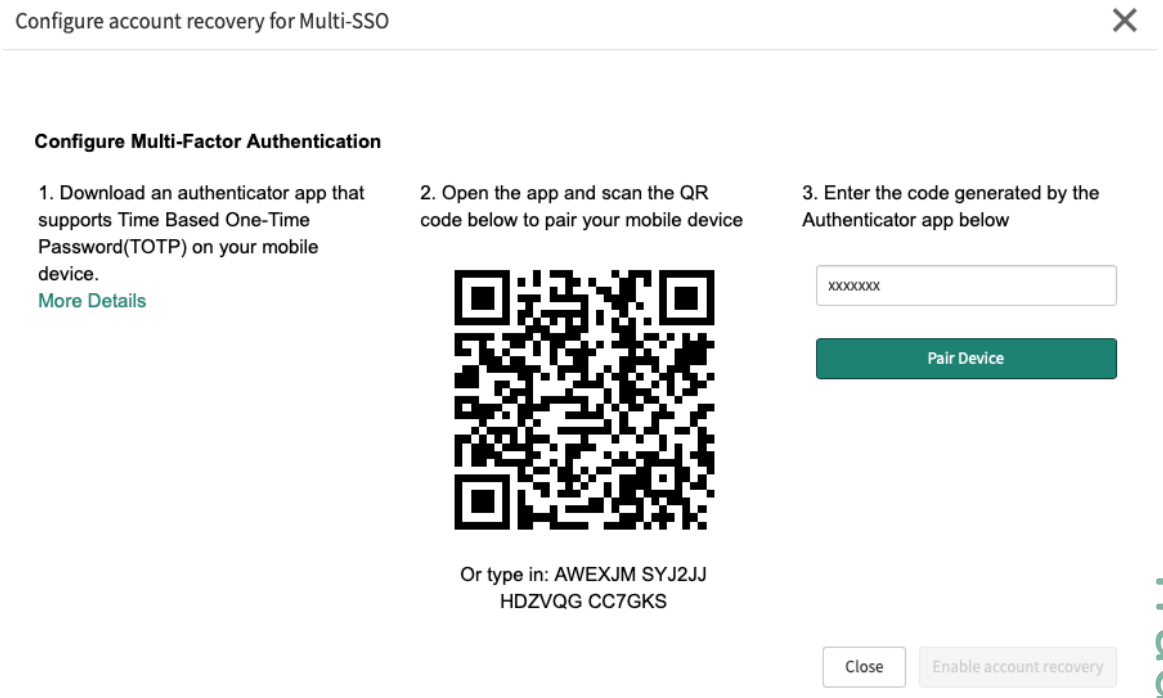
Remarque :

Si la récupération de compte est déjà activée pour l'utilisateur sélectionné, **l'option Activer la récupération de compte** n'apparaît pas dans les liens connexes. Il y aura une option **Désactiver la récupération de compte** à la place.

4. En suivant les instructions à l'écran dans le modal **Configurer la récupération de compte pour l'authentification unique (SSO) à fournisseurs multiples** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Une fois les étapes à l'écran terminées, **l'option Activer la récupération de compte** est activée.

5. Cliquez sur **Activer la récupération de compte**.

Résultats

Vous avez configuré votre compte d'utilisateur en tant qu'utilisateur de récupération de compte. Vous pouvez vérifier ce compte et afficher tous les autres utilisateurs de récupération de compte configurés en accédant à **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Utilisateurs**.

Propriétés de récupération de compte

Utilisez les propriétés système pour configurer la récupération de compte (ACR) sur votre instance.

Accédez aux propriétés de récupération de compte sur votre instance en naviguant vers **Authentification unique (SSO) de plusieurs fournisseurs** > **Récupération de compte** > **Propriétés**.

Propriétés système de récupération de compte

Propriété	Description
Activer la fonctionnalité de récupération de compte [glide.sso.acr.enabled]	Si la fonctionnalité de récupération de compte est activée sur votre instance. Cette propriété est activée par défaut.
Activer la journalisation du débogage pour la récupération de compte [glide.sso.acr.debug.log.enabled]	Indique si votre instance inclut des informations de récupération de compte dans la journalisation du débogage. Cette propriété est désactivée par défaut.
Délai d'expiration de la session utilisateur ACR (en minutes) [glide.sso.acr.ui.session.timeout]	Minutes d'inactivité avant que votre instance ne mette fin à une session utilisateur de récupération de compte. Cette propriété a une valeur par défaut de 30.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Signature électronique pour l'authentification unique (SSO) de plusieurs fournisseurs

La signature électronique avec l'authentification unique de plusieurs fournisseurs vous permet d'utiliser les propriétés de signature électronique au lieu des propriétés SAML ou OIDC pour l'authentification.

Pour la vérification par authentification unique (SSO) pendant l'authentification et pour exiger des utilisateurs qu'ils fournissent des informations d'identification avant d'envoyer leur signature électronique, vous pouvez configurer l'authentification pour demander les informations d'identification de l'utilisateur avant d'envoyer une signature.

Vous pouvez installer le module d'extension Approbations avec signature électronique (com.glide.e_signature_approvals) pour disposer de la configuration de signature électronique pour les connexions SSO.

Remarque :
Vous devez installer Code Signing Signatures (com.glide.code_signing.signatures) pour installer le module d'extension E-signature.

Activer l'approbation avec le module d'extension Signature électronique

Le module d'extension Approbation avec signature électronique (com.glide.e_signature_approvals) permet aux utilisateurs d'approuver les demandes en saisissant à nouveau leurs informations d'identification de connexion.

Avant de commencer
Rôle requis : administrateur

Remarque :
Vous devez installer Code Signing Signatures (com.glide.code_signing.signatures) pour installer le module d'extension E-signature.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée.

Utiliser la SSO de plusieurs fournisseurs pour configurer une approbation SSO pour une authentification SAML 2.0

Une approbation SSO avec signature électronique nécessite une configuration sur l'IdP SAML et l'instance ServiceNow .

Avant de commencer
Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

L'IdP SAML doit prendre en charge et respecter l'attribut forceAuthn dans les demandes d'assertion SAML. La signature électronique ne fonctionne pas sans ce paramètre IdP. Configurez une approbation avec signature électronique à l'aide des informations d'identification d'une authentification SAML 2.0.

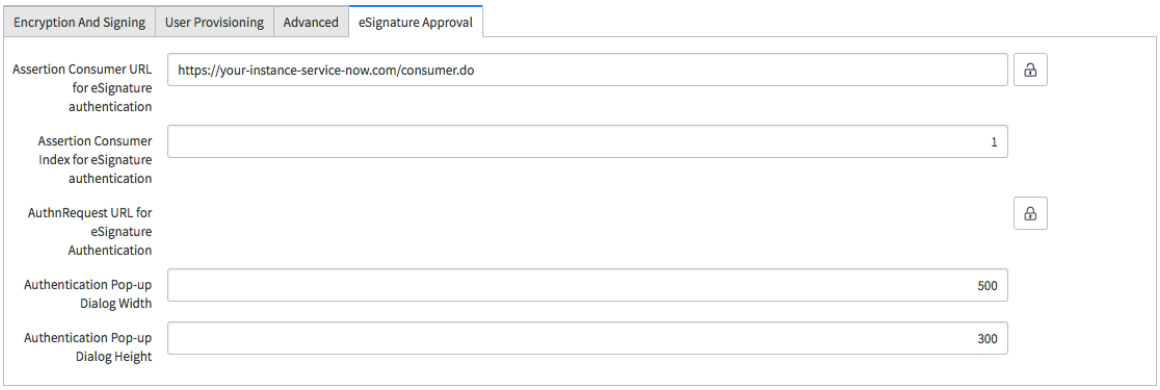
Procédure

1. Activez ou mettez à niveau vers SAML 2.0 avec le module d'extension Activate Multi-Provider SSO.
2. Activez le module d'extension Approbation avec signature électronique.
3. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité** et vérifiez que l'onglet Avancé de votre configuration d'IdP SAML 2.0 affiche l'attribut **Forcer l'AuthnRequest** coché.
   Votre IdP SAML 2.0 doit prendre en charge l'attribut **Forcer l'AuthnRequest** , sinon la signature électronique n'est pas prise en charge.
4. Dans l'onglet Approbation de signature électronique, entrez les propriétés SAML de signature électronique suivantes.

Option	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Cette propriété est définie par défaut sur l'URL appropriée. Pour configurer cette propriété, sélectionnez l'icône de verrou pour rendre ce champ modifiable. Après les modifications, sélectionnez l'icône pour verrouiller le champ.
Index de consommateur d'assertion pour l'authentification de signature électronique	Si votre fournisseur de service dispose de plusieurs URL définies pour AssertionConsumerURL, vous pouvez définir l'index à utiliser pour les signatures électroniques, en commençant par l'index 1 ou plus.
URL AuthnRequest pour l'authentification de signature électronique	Vous pouvez entrer l'URL qui pointe sur l'URL AuthnRequest IdP SAML 2.0 pour l'authentification de signature électronique. Si l'URL est identique à l'URL du consommateur d'assertion, vous pouvez laisser ce paramètre vide.
Largeur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir des informations d'identification. Ce paramètre contrôle la largeur de cette boîte de dialogue. La valeur par défaut est 500.
Hauteur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir des informations d'identification. Ce paramètre contrôle la hauteur de cette boîte de dialogue. La valeur par défaut est 300.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez le bouton **Générer les métadonnées** sous les onglets pour régénérer les métadonnées du fournisseur de service.
6. Copiez les métadonnées du fournisseur de service et mettez-les à jour sur l'IdP SAML.

Utiliser la SSO de plusieurs fournisseurs pour configurer une approbation SSO pour une authentification OIDC

Une approbation SSO avec signature électronique nécessite une configuration sur l'IdP SAML et l'instance ServiceNow .

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

L'IdP SAML doit prendre en charge et respecter l'attribut forceAuthn dans les demandes d'assertion SAML. La signature électronique ne fonctionne pas sans ce paramètre IdP. Configurez une approbation avec signature électronique à l'aide des informations d'identification d'une authentification SAML 2.0.

Procédure

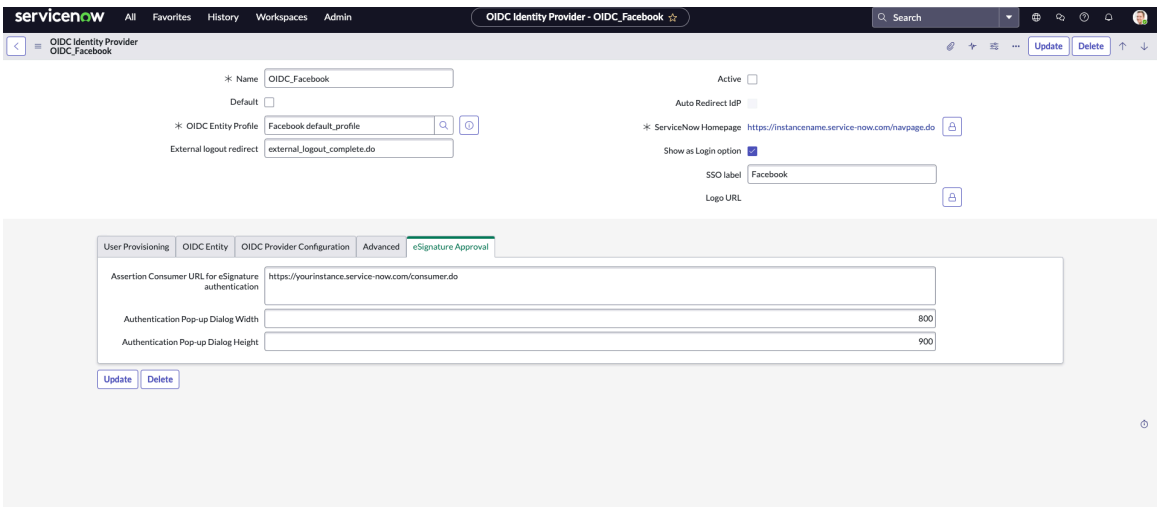
1. Activez le module d'extension Approbation avec signature électronique.
2. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité** et vérifiez les configurations de votre fournisseur OIDC
3. Dans l'onglet Approbation de signature électronique, entrez les propriétés SAML de signature électronique suivantes.

Option	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Cette propriété est définie par défaut sur l'URL appropriée. Pour configurer cette propriété, sélectionnez l'icône de verrou pour rendre ce champ modifiable. Après les modifications, sélectionnez l'icône pour verrouiller le champ.
Largeur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir des informations d'identification. Ce paramètre contrôle la largeur de cette boîte de dialogue. La valeur par défaut est 800.
Hauteur de la boîte de dialogue contextuelle d'authentification	Lorsqu'un utilisateur approuve une demande à l'aide d'une signature électronique, une boîte de dialogue s'ouvre et l'utilisateur peut saisir des informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
	d’identification. Ce paramètre contrôle la hauteur de cette boîte de dialogue. La valeur par défaut est 900.



4. Sélectionnez **Soumettre** si vous configurez la signature électronique lors de la configuration initiale d’OIDC ou **Mettre à jour** si vous souhaitez mettre à jour les détails dans la signature électronique.

OpenID Connect (OIDC) en tant que fournisseur d’identité (IdP) Single Sign-On (SSO)

OpenID Connect (OIDC) est une couche d’identité construite sur le protocole OAuth, qui offre une expérience d’authentification unique (SSO) moderne et intuitive à vous et à vos utilisateurs finaux. OIDC améliore également l’expérience de connexion pour les applications mobiles en permettant aux utilisateurs de se connecter aux applications à ServiceNow l’aide de leur fournisseur d’identité sociale. Par exemple, les administrateurs peuvent configurer l’authentification unique avec un fournisseur d’identité tiers qui prend en charge OpenID Connect. Les utilisateurs ont ensuite la possibilité de se connecter à votre application personnalisée ServiceNow à l’aide de leurs informations d’identification de fournisseur d’identité.

Vous pouvez choisir d’utiliser des fournisseurs d’identité sociale comme Google pour vos utilisateurs B2C (Business-to-Customer) et des fournisseurs d’identité d’entreprise comme Okta Microsoft Azure AD , pour vos utilisateurs business-to-business.

Créer une configuration OpenID Connect (OIDC) pour Single Sign-On (SSO)

Créez ou mettez à jour une configuration OpenID Connect (OIDC) à l’aide du module d’extension SSO de plusieurs fournisseurs.

Configuration d’OpenID Connect (OIDC) pour Single Sign-On (SSO)

Avant de commencer

- Enregistrez une application OIDC auprès de votre fournisseur d’identité (IdP) et notez l’ID client, le secret client et l’URL de configuration connue.
- Activer le module d’extension SSO de plusieurs fournisseurs
- Configurer les propriétés SSO de plusieurs fournisseurs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez le module d'extension Approbation avec signature électronique pour activer la signature électronique pour l'IdP OIDC.
- Rôle requis : administrateur

Si vous disposez d'un ID client, d'un secret client et d'une URL de configuration connue du fournisseur d'identité, vous pouvez importer directement la configuration OIDC pour SSO.

Remarque :
L'option de connexion avec l'IdP OIDC n'est pas prise en charge si le module d'extension Séparation de domaine est installé.

Si vous ne disposez pas des informations requises sur le fournisseur d'identité, vous pouvez configurer manuellement OIDC pour SSO. Une fois la configuration terminée, les utilisateurs peuvent se connecter aux applications à ServiceNow l'aide de fournisseurs d'identité sociale tiers tels que Google Okta.

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Choisissez une des options suivantes.
   - Pour mettre à jour une configuration existante, cliquez sur un enregistrement de fournisseur d'identité OIDC.
   - Pour créer une configuration, cliquez sur **Nouveau** et sélectionnez **OpenID Connect**.
3. Pour une nouvelle configuration, entrez les informations de configuration OIDC dans l'une des méthodes suivantes.

Option	Description
Importer la configuration connue OpenID Connect	Si vous disposez de l'URL de configuration connue ainsi que des informations d'identification du client qui vous sont associées, vous pouvez importer directement une configuration OIDC. **Remarque :** Si vous importez la configuration OIDC connue, tous les champs connexes sont renseignés automatiquement.
Configurer manuellement le formulaire Fournisseur d'identité OIDC	Si vous n'avez pas d'entité OIDC OAuth existante, fermez la fenêtre contextuelle Importer la configuration connue d'OpenID Connect et remplissez manuellement les champs du formulaire Fournisseur d'identité OIDC.

Importer les champs de configuration connus OpenID Connect

Propriété	Description
Nom	Nom unique de la configuration du fournisseur d'identité OIDC.
ID client	ID client de l'application enregistré dans le fournisseur d'identité OIDC tiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Secret client	Secret client de l'application enregistrée dans le fournisseur d'identité OIDC tiers.
URL de configuration bien connue	URL contenant des métadonnées sur le fournisseur d'identité OIDC tiers.

Tous les champs obligatoires doivent être remplis sur le formulaire Fournisseur d'identité OIDC.

Avant de remplir manuellement le formulaire Fournisseur d'identité OIDC, assurez-vous que vous disposez déjà d'un profil d'entité OAuth pour l'IdP OIDC.

Si vous n'avez pas de profil d'entité OAuth, vous pouvez le créer à l'aide des modèles de fournisseur OIDC externe par défaut, tels qu'Okta, Azure et d'autres.

Le type d'attribution du profil d'entité OAuth doit être avec un code d'autorisation. Pour plus d'informations, consultez Configurer un fournisseur OIDC OAuth sur Now Platform.

Remarque :
Vous pouvez utiliser les modèles des fournisseurs d'identité tiers, Auth0, Azure AD, Google et Okta sont disponibles dans les données de démonstration du module d'extension Programme d'installation de l'authentification unique de plusieurs fournisseurs.

Champs du fournisseur d'identité OIDC

Propriété	Description
Nom	Nom de l'enregistrement de fournisseur d'identité OIDC.
Actif	Option permettant d'activer la configuration d'IdP OIDC. **Remarque :** Cette option ne peut être définie sur Actif qu'après une connexion de test réussie.
Par défaut	Option permettant de définir la configuration IdP OIDC par défaut lorsqu'il existe plusieurs configurations OIDC.
Rediriger automatiquement l'IdP	Option permettant d'activer la redirection automatique des utilisateurs vers la page de connexion du fournisseur d'identité. Ce champ s'affiche lorsque l'option **Définir comme IdP de redirection automatique** est définie dans la section Liens connexes. **Remarque :** Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie est automatiquement mis à jour avec le nouvel IdP de redirection automatique. La `glide.authenticate.sso.update.idp.cookie` propriété système contrôle cette fonctionnalité.
Profil de l'entité OIDC	Profil de l'entité OAuth pour la configuration OIDC.
ServiceNow Page d'accueil	URL de la page de connexion utilisée pour l'authentification. Ce champ est automatiquement défini sur l'URL de votre instance. Le format de l'URL est le suivant : https://yourinstance.service-now.com/navpage.do

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Redirection de déconnexion externe	URL vers laquelle l'intégration redirige les utilisateurs après leur déconnexion. En règle générale, il s'agit du portail, qui est utilisé pour SSO. Ce champ est automatiquement défini sur external_logout_complete.do Par exemple, https://yourinstance.service-now.com/external_logout_complete.do
Afficher comme option de connexion	Option permettant d'afficher l'IdP OIDC comme option de connexion sur la page de connexion. L'option de connexion apparaît comme le bouton **de connexion avec le fournisseur d'identité** .
Étiquette SSO	Étiquette de l'IdP OIDC affichée sur la page de connexion. Ce champ s'affiche uniquement lorsque **l'option Afficher en tant que connexion** est activée.
URL du logo	URL accessible au public contenant le logo du fournisseur d'IdP OIDC. Ce champ s'affiche uniquement lorsque **l'option Afficher en tant que connexion** est activée.

4. **Facultatif :** Activez l'attribution automatique d'utilisateurs dans l'onglet Allocations d'utilisateurs>onglet Attribution d'utilisateurs.

(Optional) Vous pouvez choisir d'activer l'attribution automatique de l'utilisateur lors de la connexion de l'utilisateur. Lorsque l'attribution automatique d'utilisateurs est activée, un enregistrement utilisateur est automatiquement créé dans l'instance ServiceNow si cet enregistrement utilisateur n'existe pas.

Champs d'attribution d'utilisateurs

Propriété	Description
Attribuer automatiquement les utilisateurs	Option permettant d'activer l'attribution automatique des utilisateurs. Cette propriété crée un utilisateur dans la table Utilisateur de l'instance (sys_user) lorsque l'utilisateur quitte l'IdP, mais n'existe pas dans la table Utilisateur.
Mise en service à l'aide de	Source de données à utiliser pour transformer un jeton d'ID, un point de terminaison d'informations utilisateur ou les deux jetons d'ID et des informations utilisateur en un utilisateur ServiceNow. Utilisez la liste de recherche pour sélectionner le modèle de source de données prédéfini, puis ouvrez l'enregistrement pour configurer le mappage de la table de transformations.
Mettre en service la source de données	Source de données de jeton d'ID utilisée pour la mise en service de l'utilisateur.
Source d'informations de l'utilisateur	Source de données du point de terminaison d'informations utilisateur utilisée pour la mise en service de l'utilisateur. Ce champ s'affiche lorsque des informations utilisateur ou un jeton d'ID et des informations utilisateur sont sélectionnés pour le champ **Mettre en service à l'aide de** .
Mettre à jour l'utilisateur lors de la prochaine connexion	Option permettant d'activer la mise à jour de l'utilisateur lors de la prochaine connexion.
Mettre à jour la durée de l'intervalle d'utilisateur (en secondes)	Intervalle de temps minimum, en secondes, pour mettre à jour un enregistrement utilisateur entre deux connexions. Ce champ est automatiquement défini sur 3 600 secondes. Par exemple, une fois qu'un utilisateur est connecté, l'enregistrement utilisateur est mis à jour après 3 600 secondes jusqu'à la prochaine connexion. Ce champ n'est disponible que lorsque le champ **Mettre à jour l'utilisateur lors de la prochaine connexion** est activé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Rôles d'utilisateur appliqués aux utilisateurs attribués	Liste des rôles appliqués aux utilisateurs nouvellement attribués.

5. Onglet Entité OIDC
   Vous pouvez afficher et modifier la configuration du client OIDC et le flux de connexion OIDC à l'aide de l'enregistrement d'entité.
6. Onglet Configuration du fournisseur OIDC
   Vous pouvez afficher et modifier l'URL de configuration bien connue de la validation de la demande de jeton d'IdP ou d'ID OIDC.
7. **Facultatif :** Onglet Avancé

   (Optional) Scripts exécutés pendant l'authentification unique et la déconnexion.

   Champs avancés

Propriété	Description
Script d'authentification unique	Script qui s'exécute pendant l'authentification unique. Ce champ est automatiquement défini sur `MultiSSO_OIDC_custom`.
Script de déconnexion	Script qui s'exécute une fois que l'utilisateur s'est déconnecté. Ce champ est automatiquement défini sur `MultiSSO_OIDC_logout_custom`.

8. **Facultatif :** Dans l'onglet Approbation de signature électronique, configurez la signature électronique pour l'Idp OIDC.

   Remarque :
   L'onglet Approbation de signature électronique s'affiche uniquement lorsque vous installez le module **d'extension Approbation avec signature électronique** (com.glide.e_signature_approvals).

   Champs d'approbation de signature électronique

Propriété	Description
URL de consommateur d'assertion pour l'authentification de signature électronique	Si vous utilisez une méthode personnalisée de gestion de l'authentification OIDC pour les signatures électroniques, vous pouvez configurer votre propre URL de consommateur. Par exemple, si vous utilisez l'authentification unique (SSO) de plusieurs fournisseurs, vous n'avez pas besoin d'utiliser cette propriété. Ce format de l'URL est `https://yourinstance.service-now.com/consumer.do`
Largeur de la boîte de dialogue contextuelle d'authentification	Largeur de la boîte de dialogue contextuelle d'authentification. Ce champ est automatiquement défini sur `800`.

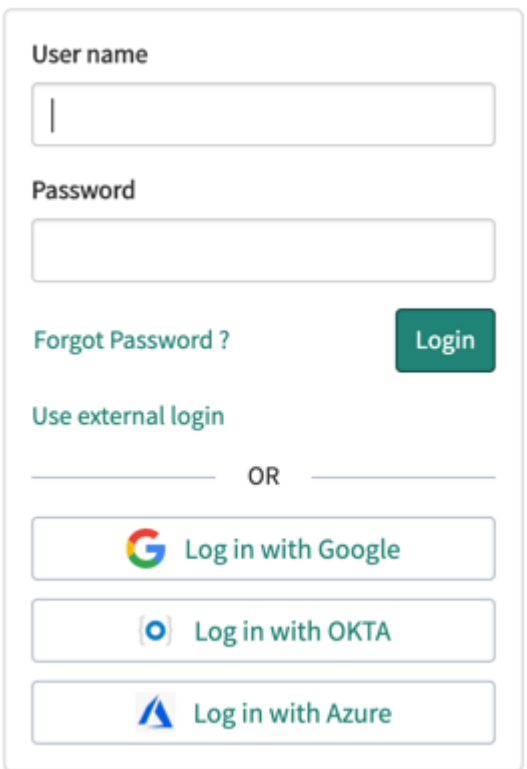
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Hauteur de la boîte de dialogue contextuelle d'authentification	Hauteur de la boîte de dialogue contextuelle d'authentification. Ce champ est automatiquement défini sur 900.

9. **Facultatif :** Accédez à la page de connexion de l'instance pour vérifier que IdP s'affiche comme option de connexion.
   Le format de l'URL doit être le suivant : `https://yourinstance/login_with_sso.do?glide_sso_id=sysId_IdP`

   Remarque :
   Si vous avez activé **l'option Sélectionné comme option de connexion**, vous pouvez accéder à l'URL de connexion de l'instance.



Utiliser l'authentification unique (SSO) basée sur Facebook

Connectez-vous à votre ServiceNow instance à l'aide de vos Facebook informations d'identification sur l'authentification unique basée sur Facebook.

Avant de commencer
L'authentification unique basée sur Facebook est fournie avec votre ServiceNow instance.

Vous pouvez définir les configurations du fournisseur d'identité (IdP) sur l'IdP **OIDC_Facebook** en tant que **vos fournisseurs d'identité**. Pour en savoir plus sur les configurations Idp, reportez-vous à la rubrique Configurer une authentification unique (SSO) basée sur Facebook.

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Sélectionnez **OIDC_Facebook**.
3. Sur la page OIDC_Facebook, spécifiez les champs suivants :

Remarque :

- La plupart des champs sont renseignés automatiquement lors de l'utilisation de l'IdP par défaut.
- Les détails de la page d'accueil ServiceNow doivent être fournis.
- Les détails relatifs à l'utilisateur, tels que l'ID client et le secret client d'origine Facebook , doivent être fournis dans l'IdP.

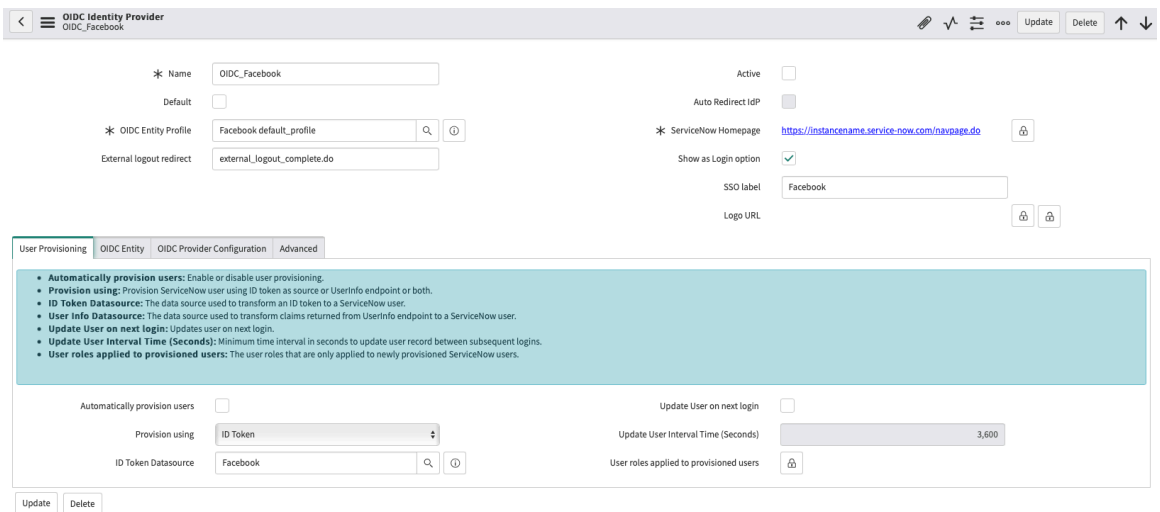
Détails du fournisseur d'identité OIDC_Facebook

Champ	Description
Nom	Nom de l'enregistrement IdP OIDC. Saisissez OIDC_Facebook.
Par défaut	Option permettant de définir la configuration d'IdP OIDC par défaut.
Profil de l'entité OIDC	Profil de l'entité OAuth pour la configuration OIDC. C'est là qu'intervient Facebook default_profile.
Redirection de déconnexion externe	URL vers laquelle l'intégration redirige les utilisateurs après leur déconnexion. En règle générale, cette URL est le portail utilisé pour SSO. Ce champ est automatiquement défini sur **external_logout_complete.do**. Par exemple, https://<votreinstance>.service-now.com/external_logout_complete.do.
Actif	Option permettant d'activer la configuration d'IdP OIDC. **Remarque :** Cette option ne peut être définie sur Actif qu'après une connexion de test réussie.
Rediriger automatiquement l'IdP	Option permettant d'activer la redirection automatique des utilisateurs vers la page de connexion du fournisseur d'identité.
ServiceNow Page d'accueil	L'URL de la page de connexion qui est utilisée pour l'authentification. Ce champ est automatiquement défini sur l'URL de votre instance. Le format de l'URL est https://<votreinstance>.service-now.com/navpage.do
Afficher comme option de connexion	Option permettant d'afficher l'IdP OIDC comme option de connexion sur la page de connexion. Dans

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	ce cas, l'option de connexion apparaît sous la forme du bouton **Se connecter avec Facebook** .
Étiquette SSO	Étiquette de l'IdP OIDC affichée sur la page de connexion. Ce champ s'affiche uniquement lorsque **l'option Afficher comme connexion** est activée.
URL du logo	URL accessible au public contenant le logo du fournisseur d'IdP OIDC. Ce champ s'affiche uniquement lorsque **l'option Afficher comme connexion** est activée.



4. **Facultatif :** Ouvrez l'onglet **Attribution d'utilisateurs** et renseignez les champs.

Remarque :
Vous devez configurer les informations liées à OIDC telles que l'ID client et le secret client de vos utilisateurs à partir de Facebook.

Onglet d'attribution d'utilisateurs

Champ	Description
Attribuer automatiquement les utilisateurs	Option permettant d'activer l'attribution automatique des utilisateurs. Cette propriété crée un utilisateur dans la table Utilisateur de l'instance [sys_user] lorsque l'utilisateur existe dans l'IdP, mais n'existe pas dans la table Utilisateur. **Remarque :** Vous pouvez choisir d'activer l'attribution automatique de l'utilisateur lors de la connexion de l'utilisateur. Lorsque l'attribution automatique d'utilisateurs est activée, un enregistrement utilisateur est automatiquement créé dans l'instance ServiceNow si cet enregistrement utilisateur n'existe pas.
Mise en service à l'aide de	La source de données à utiliser pour la transformation en ServiceNow utilisateur. Les choix sont les suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ **Un jeton d'ID** ○ **Point de terminaison d'informations utilisateur** ○ **Jeton d'ID et informations utilisateur** Utilisez la liste de recherche pour sélectionner le modèle de source de données prédéfini, puis ouvrez l'enregistrement pour configurer le mappage de la table de transformations.
Mettre en service la source de données	La source de données du jeton d'ID utilisée pour la mise en service de l'utilisateur.
Source d'informations de l'utilisateur	Source de données du point de terminaison d'informations utilisateur utilisée pour la mise en service de l'utilisateur. Ce champ **s'affiche uniquement lorsque Informations sur l'utilisateur** ou **Jeton d'ID et Informations sur l'utilisateur** sont sélectionnés dans le champ **Mettre en service à l'aide** de.
Mettre à jour l'utilisateur lors de la prochaine connexion	Option permettant d'activer les mises à jour de l'utilisateur lors de la prochaine connexion.
Mettre à jour la durée de l'intervalle d'utilisateur (en secondes)	Intervalle de temps minimum (en secondes) pour mettre à jour un enregistrement utilisateur entre deux connexions. Ce champ est automatiquement défini sur 3600 secondes. Par exemple, une fois qu'un utilisateur est connecté, l'enregistrement utilisateur est mis à jour après 3 600 secondes jusqu'à la prochaine connexion. Ce champ n'est disponible que lorsque le champ **Mettre à jour l'utilisateur lors de la prochaine connexion** est activé.
Rôles d'utilisateur appliqués aux utilisateurs attribués	Liste des rôles appliqués aux utilisateurs nouvellement attribués.

5. Dans l'onglet **Entité OIDC** , affichez et modifiez la configuration du client OIDC et le flux de connexion OIDC à l'aide de l'enregistrement d'entité.
   Pour plus d'informations sur la configuration basée sur OIDC, consultez Configurer un fournisseur OIDC OAuth pour accepter un jeton tiers
6. Dans l'onglet **Configuration du fournisseur OIDC** , affichez et modifiez l'URL de configuration bien connue de l'IdP OIDC.
7. **Facultatif :** Ouvrez l'onglet **Avancé** et renseignez les champs.

Onglet Avancé

Propriété	Description
Script d'authentification unique	Le script qui s'exécute pendant l'authentification unique.
Script de déconnexion	Script qui s'exécute une fois que l'utilisateur s'est déconnecté.

Remarque :
Les scripts sont exécutés pendant l'authentification unique et la déconnexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

8. Pour activer et tester la configuration, cliquez sur **Actif**.
9. Pour mettre à jour l'enregistrement, cliquez sur **Mettre à jour**.
   L'option de connexion basée sur Facebook est affichée sur le formulaire de connexion.
10. Lorsque vous vous connectez au formulaire de connexion, procédez comme suit :
    a. Sélectionnez l'option Facebook .
    b. Pour vous connecter à l'instance, spécifiez vos Facebook informations d'identificationServiceNow.

Configurer une authentification unique (SSO) basée sur Facebook

Configurez une authentification unique basée sur Facebook pour votre ServiceNow instance.

Avant de commencer

Disposer d'un ID client valide configuré en tant qu'IdP à partir de Facebook.

Activez les propriétés suivantes :

- Activez l'authentification unique (SSO) de plusieurs fournisseurs.
- Activez la journalisation du débogage pour les intégrations SSO de plusieurs fournisseurs.

Rôle requis : administrateur

Procédure

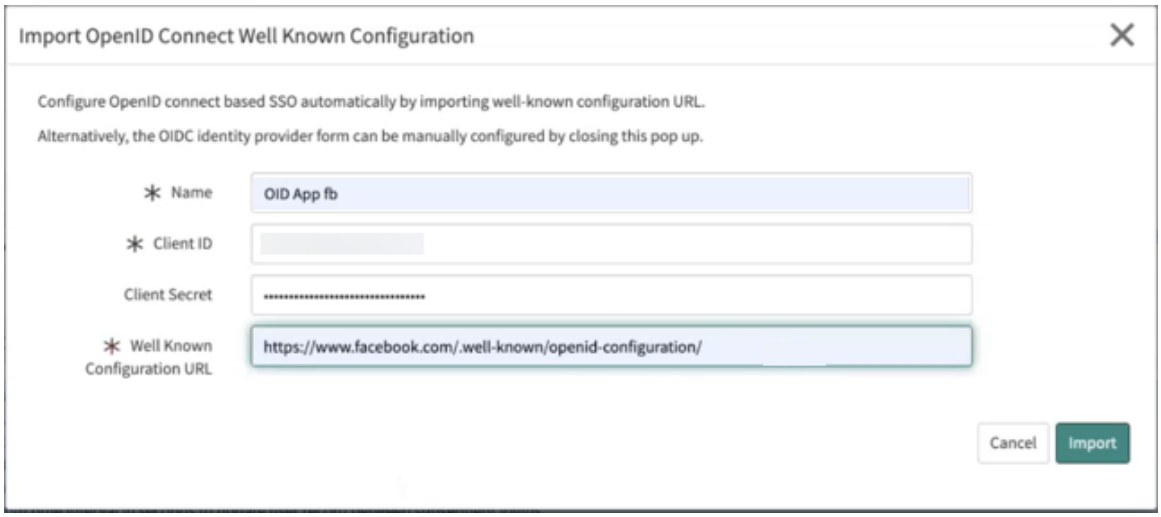
1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Pour créer un fournisseur d'identité Facebook , cliquez sur **Nouveau**.
3. Cliquez sur **OpenID Connect**.
4. Renseignez les champs du formulaire.

Importer le formulaire de configuration connue OpenID Connect

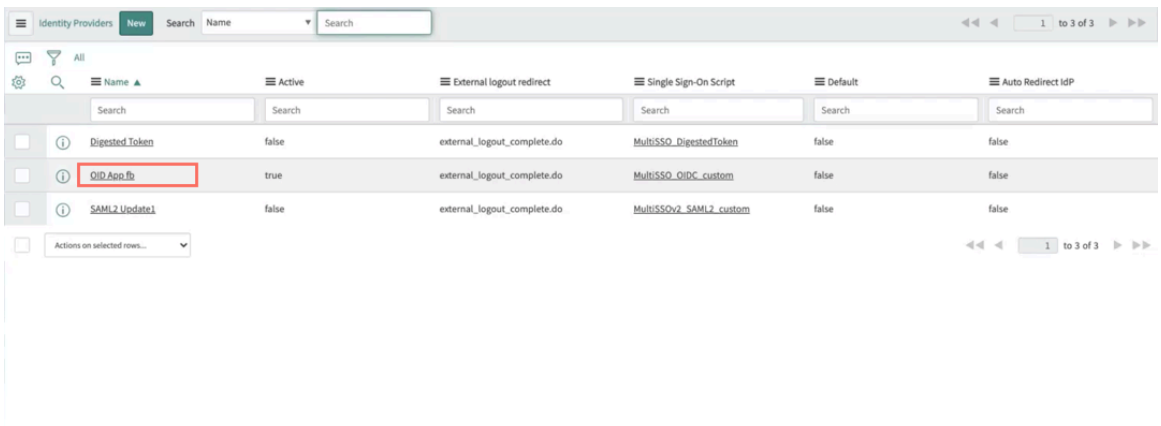
Champs	Description
Nom	Nom unique de la configuration du fournisseur d'identité OIDC.
ID client	ID client de l'application enregistré dans le fournisseur d'identité OIDC tiers.
Secret client	Le secret client de l'application enregistré dans le fournisseur d'identité OIDC tiers.
URL de configuration reconnue	URL qui contient les métadonnées sur le fournisseur d'identité OIDC tiers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Importer**.
   L'IdP basé sur Facebook est créé.

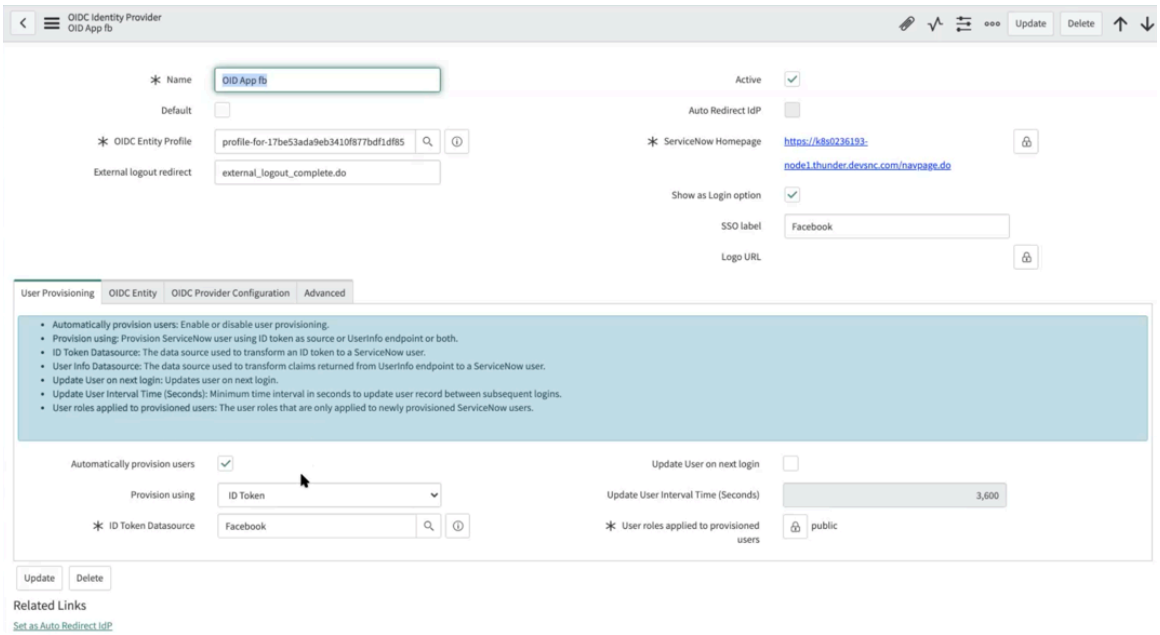


6. Sélectionnez l'IdP Facebook .
7. Dans l'idP Facebook , procédez comme suit :
   a. Validez tous les champs tels que **Nom**, **Profil de l'entité OIDC**, **Redirection de déconnexion externe** et **Page d'accueil ServiceNow**.
   b. Fournissez votre **étiquette SSO**.
8. Dans l'onglet **Allocations d'utilisateurs** , spécifiez les champs dont vous avez besoin pour configurer les utilisateurs pour des licences et rôles d'utilisateur spécifiques.

   Seuls les champs obligatoires sont obligatoires. Vous pouvez spécifier les champs restants en fonction de vos besoins.

Traduction automatique

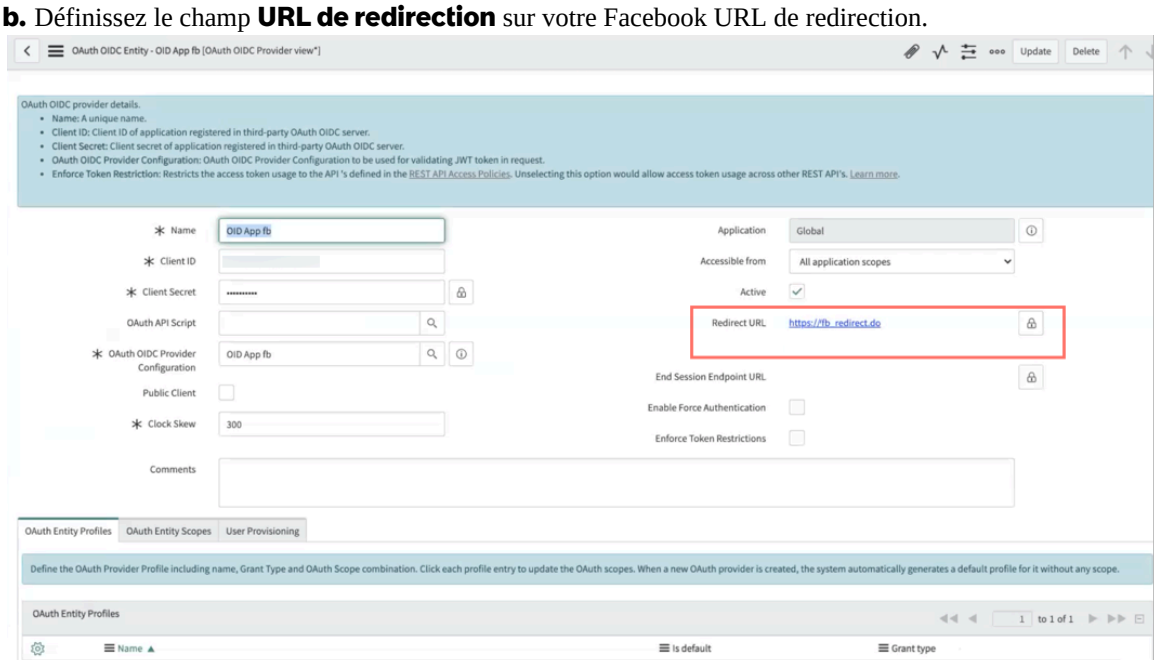
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



9. Dans l'onglet **Entité OIDC** , procédez comme suit :

   a. Cliquez sur l'entité.

   b. Définissez le champ **URL de redirection** sur votre Facebook URL de redirection.



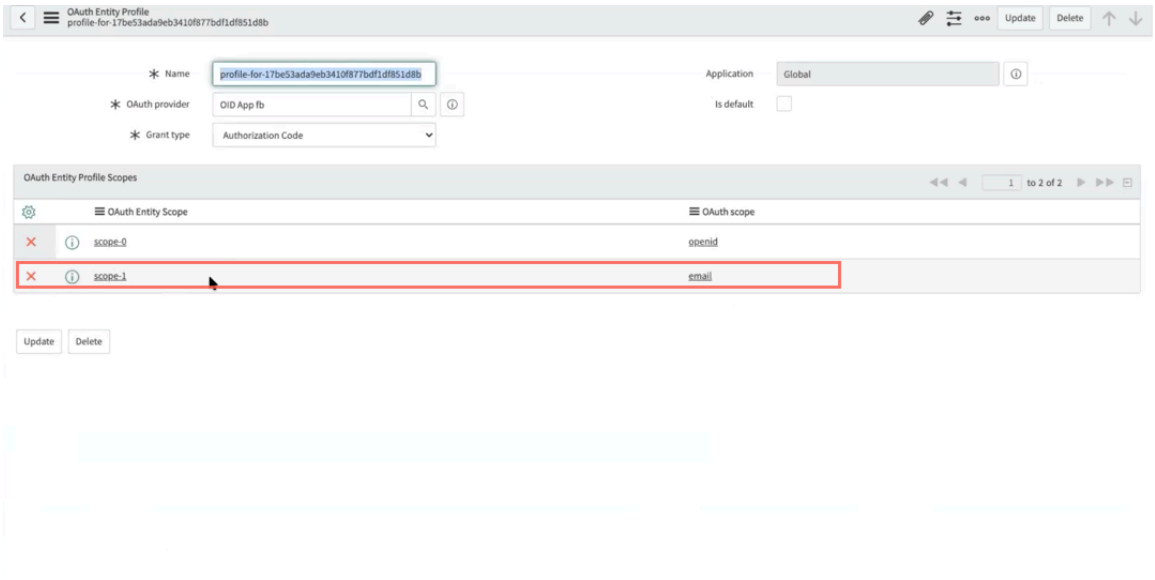
10. Dans l'onglet **Profils des entités OAuth** , procédez comme suit :

    a. Dans les détails du profil, cliquez sur un profil.

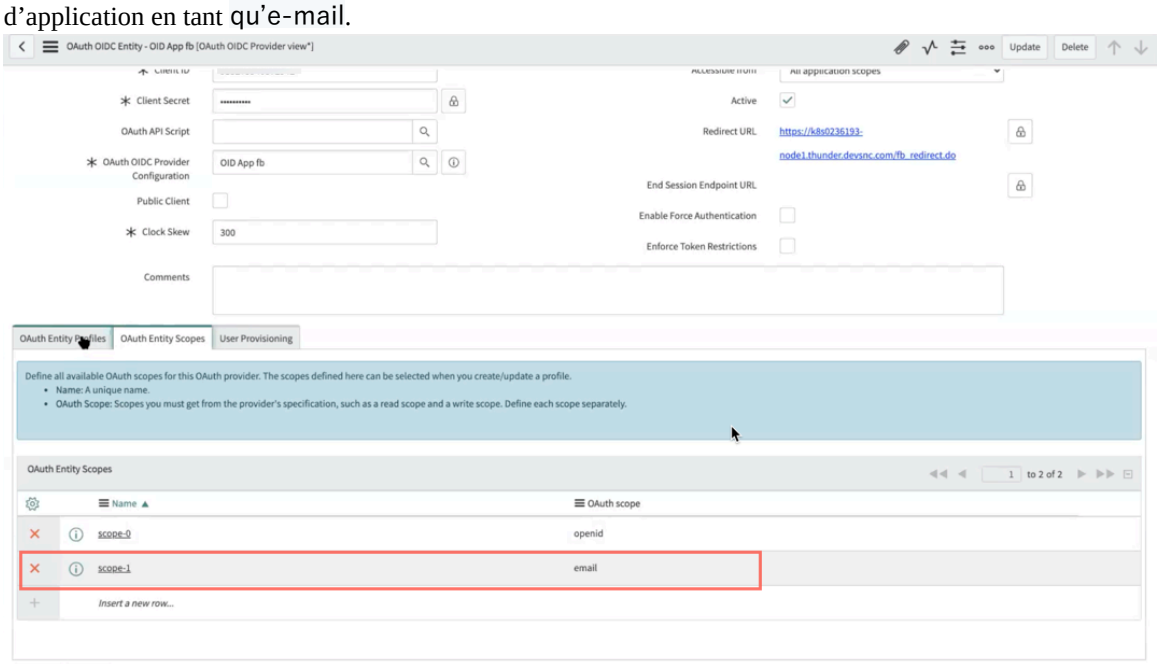
    b. Sélectionnez un périmètre et vérifiez les détails.
    Par exemple, sélectionnez **scope-1**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



11. Dans l'onglet **Périmètres de l'entité OAuth** , cliquez sur le lien **scope-1** et ajoutez le champ d'application en tant qu'e-mail.



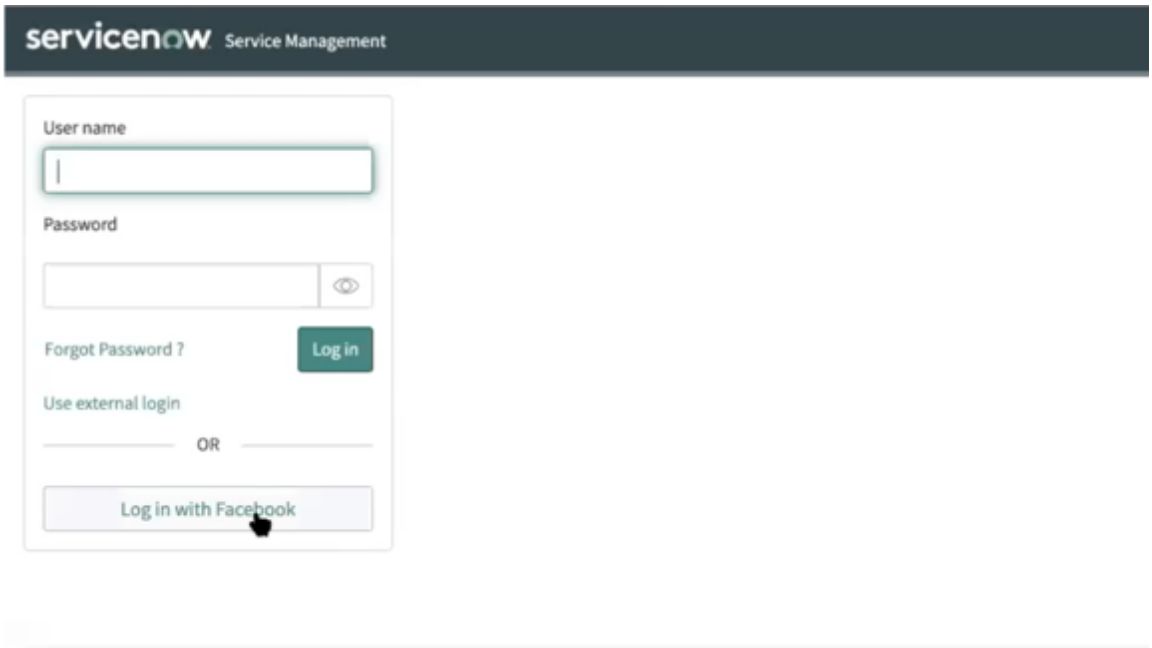
12. Pour enregistrer la configuration, cliquez avec le bouton droit sur l'en-tête, puis cliquez sur **Enregistrer**.
13. Pour définir la configuration comme active, sélectionnez **Actif**.

Résultats

Les utilisateurs s'affichent avec l'option Facebook SSO sur le formulaire de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



SAML

Le langage SAML (Security Assertion Markup Language) est une norme basée sur XML pour l'échange de données d'authentification et d'autorisation entre des domaines de sécurité.

SAML échange des informations de sécurité entre un fournisseur d'identité (un producteur d'assertions) et un fournisseur de service (un consommateur d'assertions). SAML est un produit du comité technique des services de sécurité d'OASIS. Lorsqu'il est mis en œuvre correctement, SAML est l'une des méthodes d'authentification unique (SSO) les plus sécurisées du marché.

L'intégration SAML 2.0 active la SSO en échangeant des jetons XML avec un fournisseur d'identité (IdP) externe. L'IdP authentifie l'utilisateur et transmet un jeton NameID au système. Si le système trouve un utilisateur avec un jeton NameID correspondant (par exemple, l'adresse e-mail), l'instance connecte cet utilisateur.

Si vous utilisez le module d'extension SAML 2.0 pour l'authentification SSO, vous devez définir la propriété glide.ui.rotate_sessions sur false. Sinon, cela interfère avec le partage d'informations de session qui a lieu entre l'instance et le fournisseur d'identité. Les utilisateurs disposant du privilège élevé security_admin peuvent accéder à cette propriété.

Remarque :
Nous recommandons aux clients utilisant une intégration SAML 2.0 existante d'effectuer une mise à niveau vers le module d'extension SSO de plusieurs fournisseurs.

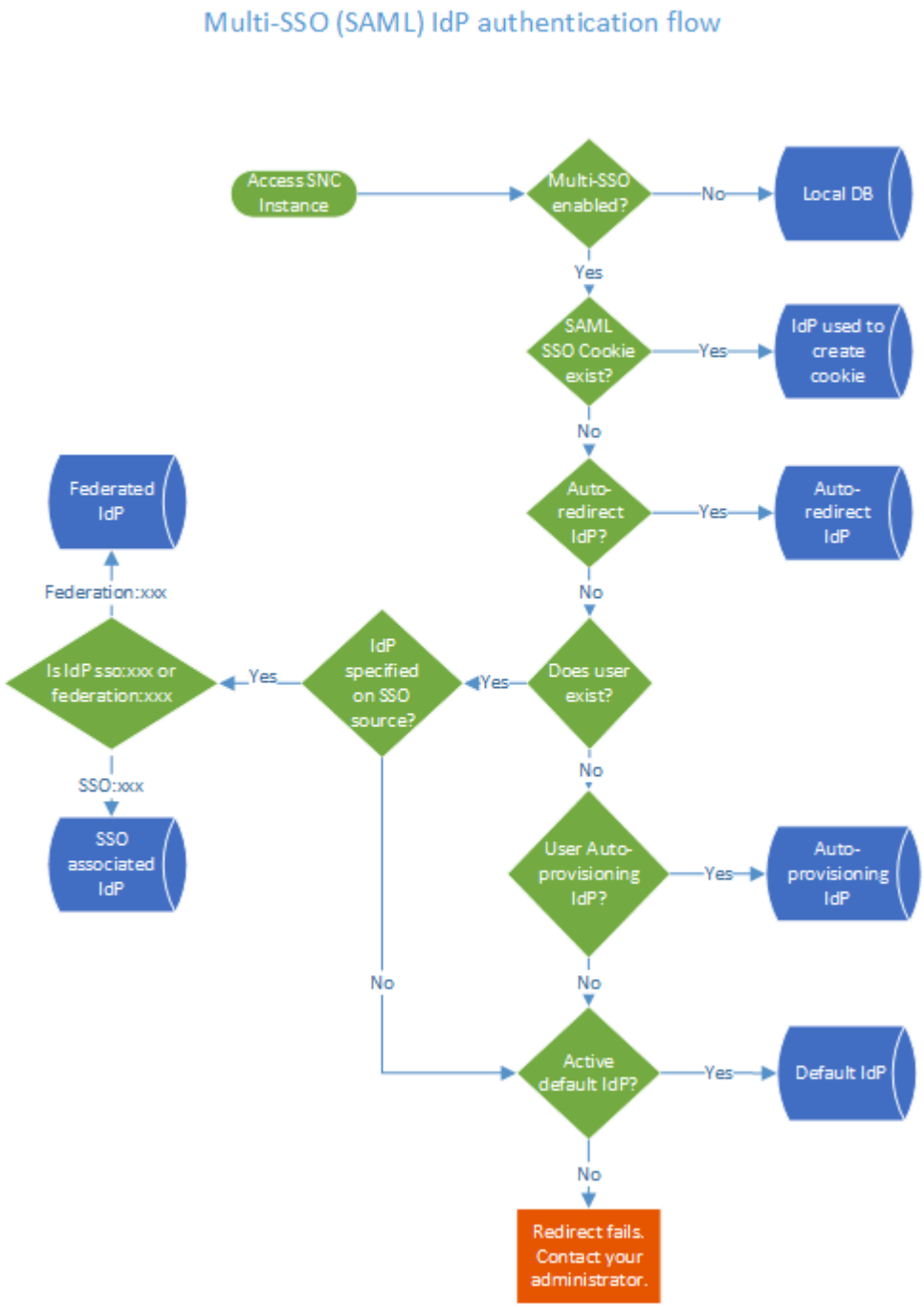
Flux d'authentification IdP SSO de plusieurs fournisseurs (SAML)

Décrit les différentes entités qui peuvent authentifier un utilisateur via l'authentification unique (SSO) SAML.

Vous pouvez suivre le flux d'authentification pour comprendre quand une entité authentifie un utilisateur à l'aide de l'authentification unique (SSO) à plusieurs fournisseurs.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Local DB

Si l'authentification unique (SSO) à fournisseurs multiples n'est pas activé, l'authentification dirige vers une base de données locale.

SAML SSO Cookie IdP

Si un cookie SAML SSO existe, l'IdP spécifié avec ce cookie authentifie l'utilisateur.

IdP de redirection automatique

Si l'IdP de redirection automatique est activé, cet IdP authentifie l'utilisateur.

IdP fédéré

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion d'autorisation externe (login_locate_sso.do) et que l'utilisateur existe dans la table des utilisateurs avec l'IdP défini dans le champ **Source SSO** en tant que fédération : xxx, l'IdP fédéré authentifie l'utilisateur.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

IdP associé

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion d'autorisation externe (login_locate_sso.do) et que l'utilisateur existe dans la table utilisateur avec l'IdP défini dans le champ **Source SSO** en tant que sso : xxx, l'IdP associé authentifie l'utilisateur.

IdP de mise en service automatique

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion d'autorisation externe (login_locate_sso.do) et que l'utilisateur n'existe pas dans la table utilisateur, mais que la mise en service automatique est activée, l'IdP de mise en service automatique authentifie l'utilisateur.

Remarque :
Si plusieurs IdP de mise en service automatique sont activés, l'utilisateur peut choisir l'IdP de mise en service automatique qu'il peut utiliser.

IdP par défaut

Si le navigateur de l'utilisateur est redirigé vers l'écran de connexion d'autorisation externe (login_locate_sso.do) et que l'utilisateur :

- N'existe pas dans la table utilisateur, la mise en service automatique n'est pas activée et un IdP par défaut actif
- Existe dans la table utilisateur, un IdP n'est pas spécifié sur l'utilisateur source SSO ou l'enregistrement de société, et il existe un IdP par défaut actif

puis l'IdP par défaut authentifie l'utilisateur.

Propriétés système du fournisseur d'identité (IdP)

Un IdP propose généralement un document XML contenant ses métadonnées d'authentification et de déconnexion.

Par exemple, SSOCircle publie ses métadonnées en ligne.

Parcourez les métadonnées IdP pour trouver ces entrées :

- Élément SingleSignOnService avec un attribut Binding qui contient une valeur de HTTP-Redirect. L'attribut Location répertorie l'URL requise par l'intégration pour le service AuthnRequest.
- Élément SingleLogoutService avec un attribut Binding qui contient une valeur de HTTP-Redirect. L'attribut Location répertorie l'URL requise par l'intégration pour le service SingleLogoutRequest.

Remarque :
L'intégration SAML 2.0 prend uniquement en charge la liaison aux services IdP par redirection HTTP.

Par exemple :

```
<SingleSignOnServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location
="https://idp.ssocircle.com:443/sso/SSORedirect/metaAlias/ssocircle"/>
```

```
<SingleLogoutServiceBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"Location
="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"ResponseLocation="https://
idp.ssocircle.com:443/sso/IDPSloRedirect/metaAlias/ssocircle"/>
```

Définissez l'URL de l'émetteur d'IdP

Fournissez l'URL aux IdP qui émettront le jeton de sécurité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
L'intégration vérifie que chaque réponse SAML contient la même URL répertoriée dans cette propriété système que l'URL répertoriée dans l'élément *Émetteur* . Par exemple :

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
     ...
  </saml:Assertion></samlp:Response>
```

Procédure
1. Accédez à la **Tout** > **Authentification unique SAML 2** > **Propriétés**.
2. Dans la propriété *URL du fournisseur d'identité qui émettra le jeton de sécurité SAML2 avec les informations de l'utilisateur*, entrez l'URL de votre fournisseur d'identité.

   Chaque URL IdP doit être unique. Par défaut, l'intégration contient l'URL de SSOCircle. Pour plus d'informations, consultez http://idp.ssocircle.com .

Définir l'URL du service AuthnRequest
À l'aide des métadonnées d'IdP, définissez les URL du service de demande pour l'IdP de l'intégration.

Avant de commencer
Rôle requis : administrateur

Procédure
1. Dans la propriété *L'URL de base pour le service AuthnRequest du fournisseur d'identité. L'AuthnRequest sera publiée sur cette URL en tant que paramètre* SAMLRequest, entrez l'URL de la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService .
2. Cochez la case à côté de *Signer l'AuthnRequest* pour activer le service d'authentification unique du fournisseur d'identité afin de recevoir une AuthnRequest signée.
3. Dans la propriété *Lorsque l'authentification unique SAML 2.0 échoue parce que la session n'est pas authentifiée ou s'il s'agit de la première connexion, redirigez vers cette URL. Il s'agit de l'URL de base où la SAML 2.0 AuthnRequest initiale est envoyée à l'aide du paramètre* SAMLRequest, entrez l'URL de la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService .

   Par défaut, l'intégration contient l'URL du service SSOCircle.

Définir l'URL du service SingleLogoutRequest
Définissez les URL du service de demande pour l'IdP de l'intégration à l'aide des métadonnées d'IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Dans l'URL *de base du service SingleLogoutRequest du fournisseur d'identité. La LogoutRequest sera publiée sur cette URL car la propriété du paramètre* SAMLRequest, entrez l'URL obtenue à partir de l'élément SingleLogoutService .
   La LogoutRequest est publiée sur cette URL en tant que paramètre SAMLRequest. Par défaut, l'intégration contient l'URL du service SSOCircle.
2. Dans *l'URL pour rediriger les utilisateurs après la déconnexion, généralement vers le portail qui a activé la propriété SSO (par exemple, http://portal.companya.com/logout)*, entrez l'URL à laquelle vous souhaitez rediriger les utilisateurs une fois qu'ils se sont déconnectés.

   Si votre IdP utilise l'authentification basée sur des formulaires, entrez l'URL du formulaire de connexion de votre IdP. Si votre fournisseur d'identités utilise une méthode d'authentification non basée sur les formulaires, telle que Kerberos, vous devez définir l'URL sur une page de déconnexion statique. De cette façon, les utilisateurs qui se déconnectent ne sont pas immédiatement redirigés vers l'IdP et se connectent à nouveau. Par défaut, l'intégration contient l'URL de la page d'interface utilisateur statique external_logout_complete.do.

(Facultatif) Activer les demandes de déconnexion signées

Certains IdP exigent que le fournisseur de service signe les demandes de déconnexion avec un certificat.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Si votre IdP nécessite des demandes de déconnexion signées, utilisez les metdata d'IdP pour définir les propriétés système suivantes.

Procédure

1. Dans l'onglet **Avancé** , à partir de la propriété *Sign LogoutRequest. Définissez cette propriété sur vrai si le service SingleLogoutRequest du fournisseur d'identité nécessite une LogoutRequest* signée, sélectionnez **Oui** pour spécifier que votre IdP nécessite une demande de déconnexion signée ou sélectionnez **Non** pour utiliser des demandes de déconnexion non signées.
2. Si vous avez sélectionné **Oui** pour *signer LogoutRequest*, dans *le protocole de liaison du service SingleLogoutRequest du fournisseur d'identité. (La valeur peut être « urn :oasis :names :tc :SAML :2.0 :bindings :HTTP-Redirect » ou « urn :oasis :names :tc :SAML :2.0 :bindings :HTTP-POST ».)* , entrez l'une des valeurs prises en charge répertoriées dans Attribut de liaison à partir de l'élément SingleLogoutService .

   Par défaut, l'intégration utilise une liaison de redirection HTTP.
3. Cliquez sur **Mettre à jour**.
4. Installez un magasin de clés de fournisseur de service (SP).

Propriétés système du fournisseur de services (SP)

Ces propriétés système définissent la façon dont l'instance interagit avec l'IdP en tant que fournisseur de service.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Suivez le processus séquentiel pour définir IdP en tant que fournisseur de service.

Définir l'URL d'instance pour le SAML

Définissez les URL spécifiques à l'instance afin que l'IdP puisse authentifier les utilisateurs.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Dans la propriété *URL de l'instance ServiceNow (généralement cette instance)*, saisissez l'URL (y compris la page de connexion) de l'instance pour laquelle l'IdP s'authentifie.
   Par exemple : https://yourinstance.service-now.com/navpage.do
2. Dans la propriété *L'identification d'entité ou l'émetteur*, saisissez l'URL de base (hors page de connexion) de l'instance pour laquelle l'IdP s'authentifie.
   Par exemple : https://yourinstance.service-now.com/

Définir l'URL de l'audience pour le SAML

Activez votre instance pour vérifier qu'elle est le destinataire prévu d'une réponse SAML à l'aide de la propriété Audience.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
L'intégration vérifie que chaque réponse SAML contient la même URL répertoriée dans cette propriété système que l'URL répertoriée dans l'élément *Audience* . Par exemple :

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do">
...
<saml:Conditions NotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
...
</samlp:Response>
```

Procédure

1. Accédez à la **Tout** > **Authentification unique SAML 2** > **Propriétés**.
2. Dans la propriété *L'URI d'audience qui accepte les jetons SAML2. (Normalement, il s'agit de votre URI d'instance. Par exemple : https://<nom d'instance>.service-now.com.)*, entrez l'URL de votre instance.
   Par exemple, https://demoi2.service-now.com. Cette URL doit correspondre à la valeur de l'élément *Audience* dans la réponse SAML.
3. Cliquez sur **Mettre à jour**.

Configurer une politique NameID pour le SAML

Configurez une stratégie NameID pour SAML. SAML 2.0 exige que l'IdP échange un jeton NameID avec le fournisseur de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Pour l'intégration SAML 2.0, le jeton NameID doit correspondre à un champ particulier de la table Utilisateur. L'intégration utilise la valeur du jeton NameID pour déterminer l'utilisateur authentifié par l'IdP.

Procédure

1. Parcourez les métadonnées IdP pour trouver l'élément `NameIDFormat` qui contient une valeur de `emailAddress`.
   La valeur de cet élément est le format par défaut utilisé par l'intégration.
2. Passez en revue d'autres éléments `NameIDFormat` pour déterminer s'il existe des formats qui correspondent à d'autres champs de la table Utilisateur.

Déterminer quel champ de table d'utilisateur correspond au jeton NameID

Les fournisseurs d'identité spécifient le format du jeton `NameID` .

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
La configuration de SAML 2.0 nécessite la sélection d'un champ dans la table Utilisateur qui correspond au format du jeton `NameID` . En règle générale, les IdP offrent la possibilité d'utiliser une adresse e-mail comme jeton `NameID` . Étant donné que la table Utilisateur contient un champ d'e-mail, ce champ est un choix logique pour une utilisation en tant que jeton `NameID` . Pour utiliser un autre champ de la table Utilisateur comme jeton `NameID` , vérifiez d'abord que l'IdP propose un format `NameID` qui correspond à la valeur d'un champ de table Utilisateur. Cela peut nécessiter l'ajout du champ à la table Utilisateur.

Procédure

1. Comparez les formats disponibles dans l'élément `NameIDFormat` de l'IdP aux champs de la table Utilisateur.
2. Sélectionnez un format `NameID` lorsqu'il y a une valeur correspondante dans la table Utilisateur.
3. Dans le *champ Table Utilisateur à mettre en correspondance avec l'élément NameID de l'objet dans le champ SAMLResponse* , saisissez le nom du champ Table Utilisateur pour rechercher les valeurs correspondantes dans le jeton `NameID` .

   Par défaut, l'intégration utilise le champ e-mail.

Définir la politique NameID d'IdP

Spécifiez le format que l'IdP utilise pour le jeton `NameID` .

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Ce format est répertorié dans le cadre des métadonnées de l'IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans la propriété *La politique NameID à utiliser pour renvoyer le NameID de l'objet dans SAMLResponse. Votre fournisseur d'identité SAML devra prendre cela en charge en déclarant la politique dans ses métadonnées. La valeur NameID est utilisée pour établir une correspondance avec le champ spécifié dans la table Utilisateur. Pour rechercher l'utilisateur,* saisissez la valeur de l'élément NameIDFormat que l'intégration utilise.

   Par défaut, l'intégration utilise le `NameIDFormat` SSOCircle pour les adresses e-mail.

2. Cliquez sur **Enregistrer**.

Valeurs du champ Table d'utilisateur pour SAML

Assurez-vous que le champ Table d'utilisateur de l'intégration contient les valeurs correspondantes appropriées.

Par exemple, si l'intégration utilise le champ e-mail comme jeton `NameID` , assurez-vous que l'instance répertorie la même adresse e-mail que l'IdP. L'intégration ne parvient pas à authentifier les utilisateurs qui n'ont pas de valeur correspondante pour le jeton `NameID` .

(Facultatif) Activer la fourniture d'une classe de contexte d'authentification pour SAML

Vous pouvez activer l'instance pour envoyer une demande de classe de contexte d'authentification à l'IdP contenant le format de demande d'authentification préféré de votre instance.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Si vous activez la création d'un message AuthContextClass, vous devez également spécifier un format de référence de classe de contexte d'authentification.

Remarque :
Certains IdP n'autorisent pas le fournisseur de service à définir la classe de contexte d'authentification. La désactivation de ce paramètre permet à l'IdP de choisir la classe de contexte d'authentification.

Procédure

1. À partir de la propriété *Créer une demande AuthnContextClass Dans l'instruction AuthnRequest*, sélectionnez **Oui** pour spécifier une classe de contexte particulière telle que Transport protégé par mot de passe, ou sélectionnez **Non** pour que l'IdP sélectionne la classe de contexte la plus appropriée.
2. Si vous avez sélectionné **Oui** pour *créer une demande AuthnContextClass dans l'instruction AuthnRequest*, alors dans *la méthode AuthnContextClassRef que nous demanderons dans notre SAML 2.0 AuthnRequest à la propriété Fournisseur d'identité* , entrez l'URN de la classe de contexte que vous souhaitez utiliser pour l'authentification (voir table).

Options d'URN AuthnContextClass

Type d'authentification	URN de classe de contexte d'authentification
Authentification basée sur les formulaires	`urn :oasis :names :tc :SAML :2.0 :ac :classes :PasswordProtectedTransport`
Authentification basée sur Kerberos	`urn :federation :authentication :windows`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Par défaut, l'intégration utilise une méthode d'authentification de transport protégée par mot de passe.

3. Cliquez sur **Mettre à jour**.

(Facultatif) Définir les propriétés du magasin de clés pour la signature des demandes de déconnexion pour le SAML

Définissez les propriétés du keystore pour permettre à l'intégration de signer les demandes de déconnexion à l'aide de votre serveur signé et de certificats d'autorité de certification signés.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Dans la propriété *L'alias de saisie de clé stocké dans le magasin de clés SAML 2.0 SP utilisé pour signer les demandes SAML 2*, entrez le nom de l'alias que vous avez créé pour le magasin de clés SAML 2.0.
   Par défaut, l'intégration recherche l'alias *saml2sp*.
2. Dans la propriété *Mot de passe de saisie de clé stocké dans le magasin de clés SAML 2.0 SP utilisé pour signer les demandes SAML 2*, saisissez le mot de passe de votre magasin de clés SAML 2.0.
   Par défaut, le mot de passe est le même que le nom d'alias par défaut.
3. Cliquez sur **Mettre à jour**.
4. Régénérez les métadonnées de votre portail de services.
   Pour plus d'informations, consultez Métadonnées SP.

Créer un magasin de clés de fournisseur de service pour SAML

Créez un magasin de clés Java contenant les éléments suivants pour que votre instance signe les demandes de déconnexion.

Avant de commencer
Rôle requis : admin

Pourquoi et quand exécuter cette tâche

- Certificat de serveur signé pour l'instance
- Certificat de l'autorité de certification signé
- Paire de clés publique et privée

Vous pouvez créer votre propre certificat signé auprès d'une autorité de certification privée ou en acheter un auprès d'une autorité de certification publique.

Les étapes suivantes illustrent comment générer un nouveau fichier de magasin de clés Java Keytool, créer une demande de signature de certificat (CSR) et importer des certificats. Tous les certificats racines ou intermédiaires doivent être importés avant d'importer le certificat primaire pour votre domaine. Tapez ces commandes dans une interface de ligne de commande.

Remarque :
Ces instructions ne sont pas spécifiques à la plateforme et nécessitent des connaissances techniques en matière de certificats de sécurité. Le support technique ne peut pas vous aider à créer les certificats.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Générez un magasin de clés Java et une paire de clés.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Générez une CSR pour un magasin de clés Java existant.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Importez un certificat d'autorité de certification (CA) racine ou intermédiaire dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

4. Importez un certificat primaire dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

Installer un magasin de clés de fournisseur de service pour signer les demandes SAML

Procédez comme suit pour supprimer l'exemple de magasin de clés existant et installer votre propre magasin de clés de fournisseur de service contenant votre paire de clés publique et privée.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Créez un magasin de clés de fournisseur de service.
2. Accédez à la **Authentification unique SAML 2** > **Certificat** ou **Multi-fournisseur** > **Administrateur** > **Certificat x509**.
3. Cliquez sur **SAML 2.0 Keystore_Key2048_SHA256**.
4. Cliquez sur le lien **Gérer les pièces jointes** .
5. Cochez la case Supprimer en regard de *saml2sp_key2048withsha256.jks*.
6. Cliquez sur **Supprimer**.
7. Cliquez sur **Choisir des fichiers** et sélectionnez le magasin de clés contenant vos certificats signés.
8. Cliquez sur **Joindre**.
9. Fermez la fenêtre contextuelle Pièces jointes.

> **Remarque :**
> Il est recommandé de fournir un nom différent pour le certificat qui vient d'être joint.

10. Dans *Mot de passe du magasin de clés*, saisissez le mot de passe pour accéder à l'alias SAML 2.
11. Cliquez sur **Mettre à jour**.

(Facultatif) Propriétés SAML avancées

Les paramètres avancés suivants vous permettent d'augmenter davantage la sécurité et de déboguer l'intégration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres avancés

Accédez à la **Tout** > **Authentification unique SAML 2** > **Propriétés**.

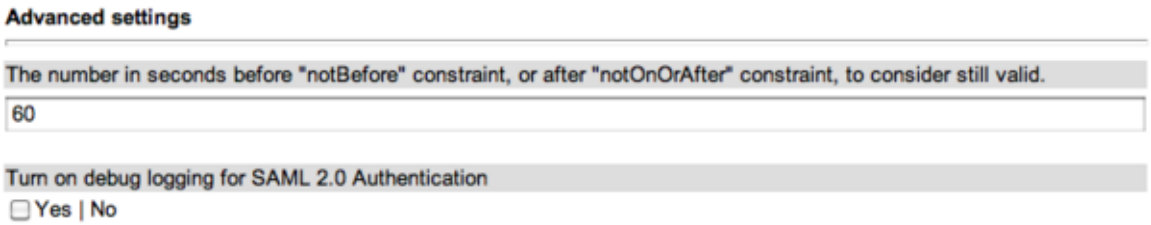


Table des propriétés système avancées

Propriété	Description
Nombre de secondes pendant lesquelles considérer toujours valable la contrainte « notBefore » ou après la contrainte « notOnOrAfter »	Entrez le nombre de secondes à ajouter aux contraintes *NotBefore* et *NotOnOrAfter* pour tenir compte des différences de temps entre l'horloge IdP et l'horloge SP. Ces contraintes empêchent les attaques par rejeu en refusant les demandes qui ne sont pas effectuées dans le délai spécifié. Si l'horloge IdP et l'horloge SP sont significativement différentes, la latence du réseau peut entraîner le refus de l'autorisation de la demande SAML. Cette propriété ajoute une période de grâce au cours de laquelle les demandes et les réponses SAML sont toujours considérées comme valides.
Activez la journalisation du débogage pour l'authentification SAML 2.0	Sélectionnez **Oui** pour activer des informations de journalisation supplémentaires pour les événements SAML 2.0.

Installer le certificat du fournisseur d'identité

Vous pouvez coller un certificat PEM dans un formulaire de certificat X.509 afin que le fournisseur identifié puisse vérifier les communications avec le fournisseur de service.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Le certificat de l'IdP se trouve dans les métadonnées de l'IdP. Le développeur IdP détermine où résident les métadonnées du certificat lors de la création de l'IdP local.

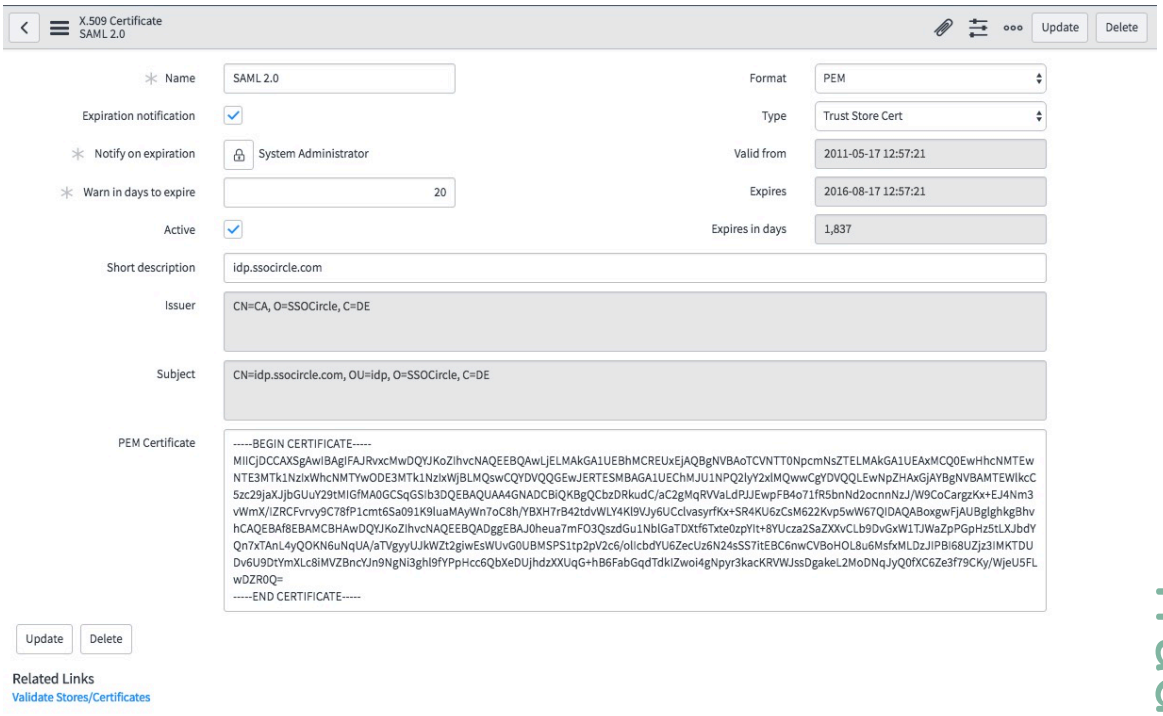
Remarque :
Les certificats pour l'authentification unique doivent toujours être au format PEM pour fonctionner avec les certificats SAML.

Procédure

1. Accédez à la **Tout** > **Authentification unique SAML** > **Certificat**.
2. Renseignez les champs de formulaire (consultez la table).
3. Cliquez sur **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :
À l’heure actuelle, l’intégration ne signe pas le certificat dans les communications entre l’instance et l’IdP.

Champ	Description
Nom	Nom du certificat. Ne modifiez pas l’entrée *Nom* . Le nom du certificat X.509 doit être *SAML 2.0* pour que l’intégration l’utilise. Cette condition n’est vraie que si vous n’utilisez Authentification unique (SSO) de plusieurspas .
Notification d'échéance	Sélectionnez cette option pour envoyer une notification aux utilisateurs sélectionnés dans le champ **Notifier à l’expiration** . Cette option est activée par défaut.
Notification à l'expiration	Sélectionnez les utilisateurs pour relancer la notification concernant l’expiration du certificat. Si aucun utilisateur n’est sélectionné, l’utilisateur connecté est ajouté par défaut, ainsi que les deux derniers utilisateurs connectés ayant le rôle administrateur.
Avertissement avant l'expiration (en jours)	Nombre de jours avant l’expiration du délai d’envoi de la notification par l’instance. Saisissez une valeur d’au moins 20. Les instances mises à niveau vers Istanbul et les versions ultérieures ont cette valeur définie sur 20, sauf si une valeur supérieure est spécifiée.
Actif	Case à cocher indiquant que ce certificat est actif.
Format	Le format du certificat. SAML utilise le format PEM.
Type	Le conteneur de certificats. L’instance reconnaît les certificats des magasins de confiance, du magasin de clés Java et des magasins de clés PKCS#12.
Début de validité	L’instance ajoute automatiquement la date de début de validité du certificat à ce champ. Joignez le certificat à l’enregistrement de certificat X.509 pour remplir ce champ.
Date d'expiration	L’instance ajoute automatiquement la date d’expiration du certificat à ce champ. Joignez le certificat à l’enregistrement de certificat X.509 pour remplir ce champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Échéance en jours	Nombre calculé de jours jusqu'à l'expiration.
Description brève	Description du certificat.
Problème	L'instance ajoute automatiquement l'émetteur du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Objet	L'instance ajoute automatiquement l'objet du certificat à ce champ. Joignez le certificat à l'enregistrement de certificat X.509 pour remplir ce champ.
Certificat PEM	Saisissez la valeur du certificat X509.

Que faire ensuite

Cliquez sur **Valider les magasins/certificats** pour tester le magasin de confiance et le certificat.

Remplacement d'un certificat manquant pour SAML

Si le module **Certificat** affiche une page vide, cela signifie que l'enregistrement du certificat SAML 2.0 a été supprimé. Vous pouvez remplacer le certificat manquant en créant manuellement un enregistrement de certificat.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Certificats**.
2. Créez un nouvel enregistrement appelé `SAML 2.0`.

> **Important :**
> Vous DEVEZ utiliser ce nom. Cette condition n'est vraie que si vous n'utilisez Authentification unique (SSO) de plusieurspas .

3. Cliquer sur **Authentification unique SAML 2** > **Certificat**.
4. Dans le champ *Certificat PEM* , entrez la valeur de l'élément `ds :X509Certificate` à partir des métadonnées de votre IdP.
5. Cliquez sur **Enregistrer**.

Tester l'intégration SAML

Testez l'intégration SAML une fois que vous avez terminé toutes les autres tâches de configuration.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Connectez-vous à l'instance en tant qu'utilisateur disposant du rôle administrateur.
2. Accédez à la **Authentification unique SAML 2** > **Propriétés**.
3. Dans la propriété *Activer l'authentification externe*, sélectionnez **Oui**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

L'activation de l'authentification externe nécessite que tous les utilisateurs utilisent l'authentification unique SAML 2.0. Si quelqu'un tente d'accéder à l'application dans un état non authentifié, l'instance envoie automatiquement une demande d'authentification à l'IdP (IdP) et redirige l'utilisateur vers la page Authentification IdP SAML.

4. Cliquez sur **Enregistrer**.
5. Déconnectez-vous de l'instance.
6. Accédez à l'URL de l'instance.
   Si l'intégration fonctionne correctement, l'IdP doit demander les informations d'identification de l'utilisateur.

Information associée

Erreurs et correctifs de l'authentification unique (SAML 2.0)

Erreurs et correctifs de l'authentification unique (SAML 2.0)

Une liste des erreurs courantes et des correctifs associés pour l'installation et la configuration de l'authentification unique (SAML 2.0).

Erreurs lors de la configuration de l'authentification unique (SSO) à fournisseurs multiples (SAML 2.0)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
NotAfter : <Thu Jun 05 22:57:44 PDT 2014>.	Vérifiez que le certificat x509 IDP est présent, valide et actif.	N/A	Le certificat actuel ou l'assertion SAML a expiré.	• Synchronisez l'horloge SNC avec l'horloge du serveur IdP SAML. • Mettez à jour l'enregistrement du certificat SAML 2.0.
• Impossible de localiser le certificat SAML 2.0. • Impossible de trouver une signature numérique stockée dans l'instance ServiceNow.	Vérifiez que le certificat x509 IDP est présent, valide et actif	La chaîne formatée PEM doit être saisie dans le champ Certificat PEM.	Le certificat SAML n'existe pas. Il est peut-être inactif.	Assurez-vous que le certificat au format PEM correct est téléchargé dans l'instance.
Les certificats ne correspondent pas.	Vérifiez que le certificat	N/A	Le certificat disponible dans SNC ne correspond pas au certificat dans	Vérifiez que la chaîne formatée PEM dans l'enregistrement de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de la configuration de l'authentification unique (SSO) à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
Attente : <certStr>, réelle : <inboundCert>.	x509 IDP est présent, valide et actif.		l'assertion. Les causes sont les suivantes : • Le certificat est mis à jour sur l'IdP, mais pas dans l'instance ServiceNow. • Le certificat n'est pas dans le bon format.	certificat SAML 2.0 correspond au certificat X509 dans SAMLResponse pour l'IdP de l'utilisateur.
Échec de la vérification de la validité du certificat.	Vérifiez que le certificat x509 IDP est présent, valide et actif	N/A	Le certificat actuel a peut-être expiré.	Mettez à jour l'enregistrement du certificat SAML 2.0.
Échec de la validation du profil de signature.	Vérifiez que le certificat x509 IDP est présent, valide et actif.	N/A	L'assertion peut être signée avec un certificat différent.	Vérifiez si l'IdP possède le même certificat que l'instance SNC.
InResponseTo dans l'incompatibilité de SubjectConfirmationData. Attendre : <inResponseTo>, réel : <inResponseTo>.	Échec de la validation de la confirmation d'objet.	N/A	Cette erreur s'affiche si l'une des situations suivantes se produit : • L'IdP renvoie une réponse SAML pour une autre requête SAMLRequest • Un utilisateur met en signet l'URL avec SAMLRequest au lieu de l'URL d'instance uniquement • Si une valeur Null est attendue, la réponse peut être envoyée à un autre nœud lorsque	L'administrateur IdP doit confirmer que la réponse SAML attendue est renvoyée. Il peut s'agir d'un problème d'équilibreur de charge ou d'infrastructure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de la configuration de l'authentification unique (SSO) à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
			l'instance dispose de plusieurs nœuds.	
Valeur d'index de session introuvable : <message>...	SessionIndex non valide.	N/A	Le SessionIndex est requis dans l'instance SNC. L'IdP le renvoie dans la réponse SAML pour s'authentifier avec succès.	L'administrateur IdP doit confirmer que le SessionIndex est défini dans SAMLResponse.
Aucune confirmation d'objet valide trouvée.	Échec de la validation de la confirmation d'objet.	N/A	Les conditions peuvent être manquantes en raison d'une erreur dans l'IdP. Le StatusCode dans la réponse contiendrait Responder au lieu de Réussite attendue.	Passez en revue la SAMLResponse pour déterminer si les conditions sont incluses dans la SAMLResponse. Les données valides de confirmation de l'objet peuvent être expirées ou non pour la bonne audience.
Incohérence de l'audience d'assertion. Attendu : <propAudience>, réel : <audienceUri>. ou Échec de la validation de AudienceRestriction. Aucune audience correspondante trouvée.	Vérifiez que le champ 'URI de l'audience' est défini correctement.	L'URI du public qui accepte le jeton SAML2. (Normalement, il s'agit de votre URI d'instance. Par exemple : https://demo.service-now.com.)	L'URI d'audience configuré pour l'instance SNC doit correspondre à la valeur dans IdP.	Recherchez <saml2 :Audience> dans SAMLResponse dans les journaux et vérifiez que la valeur correspond à celle de l'instance.
L'émetteur de l'assertion n'est pas valide. Attente : <valeur sur l'instance> réelle : <valeur renvoyée par l'IdP>	L'émetteur de l'assertion n'est pas valide.	L'URL du fournisseur d'identité qui émet le jeton de sécurité SAML2 avec les	L'ID de l'entité IdP (émetteur) ne correspond pas à la valeur définie dans l'instance SNC.	• Vérifiez si l'IdP ou le SP n'est pas configuré correctement. • Vérifiez que la propriété SAML (l'URL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs lors de la configuration de l'authentification unique (SSO) à fournisseurs multiples (SAML 2.0) (suite)

Erreur dans les journaux d'instance	Message de test de la connexion	Propriété SAML	Diagnostic	Corriger
		informations de l'utilisateur.		du fournisseur d'identité qui émet le jeton de sécurité SAML2 avec les informations de l'utilisateur) est définie correctement.
L'objet est valide dans le futur. Maintenant : <now>, NotBefore : <notBefore> ou L'objet a expiré. Maintenant : <now>, NotOnOrAfter : <notOnOrAfter>	Échec de la confirmation de validation de l'objet.	Nombre de secondes avant la contrainte notBefore ou après la contrainte notOnOrAfter à considérer toujours valide.	L'horloge IdP n'est pas synchronisée avec l'horloge du fournisseur de services.	Mettez à jour la propriété SAML glide.authenticate.sso.saml2.clockskew sur une valeur plus élevée. La valeur par défaut est de 180 secondes. Certains cas nécessitent un réglage de 300 ou plus. Vous devrez peut-être également vérifier l'heure sur votre serveur IdP.
L'assertion est valide dans le futur, maintenant : <now>, notBefore : <notBefore> ou L'assertion a expiré, maintenant : <now>, notOnOrAfter : <notOnOrAfter>	L'assertion n'est pas valide.	Nombre de secondes avant la contrainte notBefore ou après la contrainte notOnOrAfter à considérer toujours valide.	L'horloge IdP n'est pas synchronisée avec l'horloge du fournisseur de services	Mettez à jour la propriété SAML sur une valeur plus grande. La valeur par défaut est de 60 secondes. Certains cas nécessitent un réglage de 300 ou plus. Vous devrez peut-être également vérifier l'heure sur votre serveur IdP.

Erreurs de connexion et d'IdP courantes

Erreur ou symptôme	Diagnostic	Corriger
Les demandes de connexion génèrent une boucle infinie entre le système et l'IdP lorsque la haute sécurité est active.	• En règle générale, le point de terminaison de l'URL est une page d'erreur ou une page de déconnexion. • Le logout_redirect.do peut créer cette boucle	Définissez (ou créez) le glide.authenticate.failed_redirect de propriété système pour rediriger les demandes ayant échoué à l'authentification vers cette URL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Erreurs de connexion et d'IdP courantes (suite)

Erreur ou symptôme	Diagnostic	Corriger
	lorsque vous définissez *glide.security.url.whitelist* sans ajouter le nom d'hôte IdP à la valeur de propriété. **Remarque :** Pour en savoir plus sur cette propriété, reportez-vous Liste d'autorisation d'URL pour les redirections de déconnexion à la section Paramètres de sécurisation renforcée de la sécurité de l'instance.	
Le jeton utilisé pour authentifier l'utilisateur ou la demande est signé avec l'algorithme de signature http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 qui n'est pas l'algorithme de signature attendu http://www.w3.org/2000/09/xmldsig#rsa-sha1.	Consultez l'onglet Contexte de l'alerte pour connaître les détails de l'événement.	Accédez à l'onglet Avancé de la boîte de dialogue de configuration de l'approbation de la partie de confiance et vérifiez que l'algorithme est défini sur SHA-1 et non sur SHA-256.
Le message d'erreur urn :oasis :names :tc :SAML :2.0 :status :Requester s'affiche dans la table journal système (syslog).	Lorsque votre IdP (par exemple, ADFS) répond avec un état oasis :names :tc :SAML :2.0 :status :Requester, cela signifie que l'IdP a rejeté la connexion en raison d'un problème avec la demande qui lui a été envoyée. Malheureusement, dans la plupart des cas, la réponse SAML reçue de l'IdP ne fournit pas plus de détails sur l'erreur.	Examinez la demande SAML envoyée à l'IDP et collaborez avec l'administrateur IdP pour mettre à jour les paramètres SAML de votre instance afin d'éviter l'erreur. Vous devrez peut-être contacter votre fournisseur IDP pour connaître la raison de l'échec de la connexion.

Rediriger les connexions Single Sign-On (SSO)

Lorsque SSO est activé, vous pouvez rediriger les utilisateurs vers des pages spécifiques ou les inciter à se connecter localement.

Par exemple, si un utilisateur tente d'accéder à https://customerX.service-now.com, un portail d'entreprise interne peut s'afficher à la place de la page de connexion par défaut. Ainsi, lorsqu'un utilisateur se déconnecte d'une application, le navigateur peut le rediriger vers une page interne spécifique. Vous pouvez définir des propriétés de redirection au sein de l'instance pour vous assurer que les utilisateurs voient une page de connexion SSO plutôt que la page de connexion par défaut.

Remarque :
Les propriétés suivantes ne forcent pas l'authentification unique. La page login.do est toujours accessible et les utilisateurs peuvent se connecter au système s'ils disposent d'un mot de passe local.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés de la redirection

Lorsqu'un utilisateur se déconnecte, ou en cas d'échec de tentative de connexion à l'aide de SSO, vous pouvez définir l'endroit suivant vers lequel l'utilisateur est redirigé (page du portail principal ou article de la base de connaissances contenant les informations de connexion SSO). Utilisez les propriétés suivantes pour spécifier les URL. Si l'une de ces propriétés n'existe pas dans votre instance, vous pouvez la créer.

glide.authenticate.failed_requirement_redirect

URL vers laquelle rediriger les utilisateurs lorsqu'ils tentent d'accéder à une page privée (par exemple, pour afficher un incident) et ne fournissent pas d'informations d'identification SSO. La propriété est généralement définie sur le portail de connexion d'un client (par exemple, `http://portal.companya.com/`).

glide.authenticate.failed_redirect

URL permettant de rediriger des utilisateurs après un échec de tentative SSO. Vous pouvez rediriger vers un article de la base de connaissances publique qui décrit l'erreur et contient des liens utiles (par exemple, `http://portal.companya.com/error`).

glide.authenticate.external.logout_redirect

URL vers laquelle rediriger les utilisateurs après la déconnexion, généralement vers le portail qui a activé la connexion avec authentification unique (par exemple, `http://portal.companya.com/logout`).

glide.authentication.external.disable_local_login

Lorsque la valeur est définie sur vrai, elle requiert des informations d'identification SSO pour la page de connexion principale. La valeur par défaut est false. Cette propriété doit être utilisée conjointement avec la *`glide.authenticate.failed_requirement_redirect`* propriété.

Le tableau suivant montre la relation entre les valeurs de retour de sortie d'installation, les propriétés et le comportement attendu.

Connexion forcée à l'aide de l'authentification unique (SSO) uniquement

Valeur de retour	Propriété	Comportement
failed_missing_requirement	*`glide.authenticate.failed_requirement_redirect`*	Lorsque cette valeur est r indique que les informatio SSO requises ne sont pas session. La connexion éch est redirigée vers l'URL s propriété. Il s'agit généra fournisseur SSO où la co et où les informations d'i collectées.
failed_authentication	*`glide.authenticate.failed_redirect`*	Lorsque cette valeur est r indique que les informatio SSO fournies ont échoué que l'utilisateur n'existe p verrouillé. La connexion est redirigée vers l'URL s propriété. Il s'agit généra fournisseur SSO où la co et où les informations d'i collectées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Connexion forcée à l'aide de l'authentification unique (SSO) uniquement (suite)

Valeur de retour	Propriété	Comportement
`<user_id>`	N/A	Connexion autorisée pour par <`user_id`>. Cette v au nom de champ défini d `glide.authenticat` SSO (« nom de champ de en correspondance avec l

Restriction de la connexion locale

Par mesure de sécurité, vous ne devez pas vous contenter de vous fier aux propriétés de redirection pour interdire la connexion locale. Si un utilisateur ne doit jamais se connecter localement et qu'il sera toujours authentifié par votre système d'authentification unique interne, un mot de passe aléatoire doit être attribué à chaque utilisateur importé dans l'instance. Le mot de passe aléatoire est le plus facile à définir au moment de l'importation de l'utilisateur. Si les données utilisateur sont importées dans votre système par le biais d'un jeu d'importation, vous pouvez créer un script de transformation onBefore à l'aide du code .

```
var r  = new Packages. java. util. Random ( ) ;

 var str1  = Packages. java. lang. Long. toString (Packages. java. lang.
 Math. abs (r. nextLong ( ) ) , 36 ) ; var str2  = Packages. java. lang.
 Long. toString (Packages. java. lang. Math. abs (r. nextLong ( ) ) , 36
 ) ;

 var newPass  = str1  + str2 ;

target. user_password = newPass ;

 //password now set to a random string like this:
 //qvm81zdrn7cwwylpvw94eebk
```

Cloner une instance avec une intégration SAML

Clonez une instance avec une intégration SAML. Avant de cloner une instance qui utilise SAML 2.0, conservez les paramètres liés à l'authentification unique SAML sur l'instance cible, sinon vous risquez de rendre l'instance cible inaccessible.

Avant de commencer

Rôle requis : administrateur

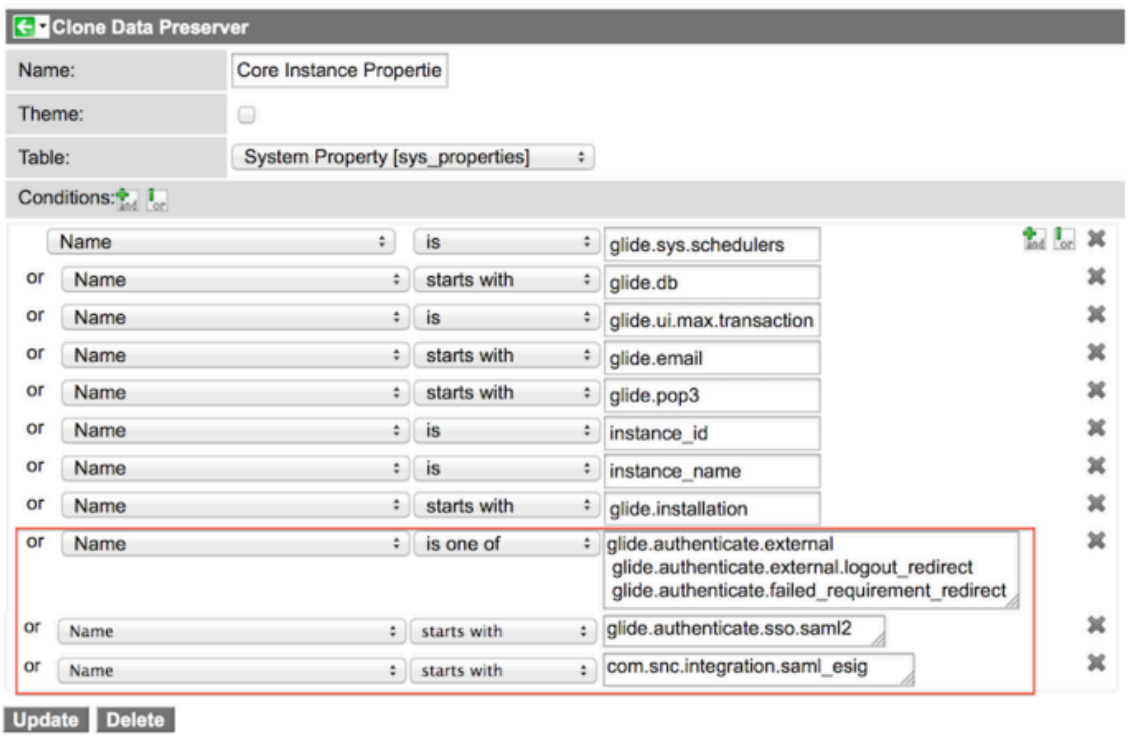
Procédure

1. Sur l'instance source, accédez à **Clone système** > **Conserver les données** > **Propriétés de l'instance principale**.
2. Assurez-vous que les propriétés liées à l'authentification unique SAML suivantes sont préservées à l'aide de conditions.
   - glide.authenticate
   - glide.security
   - glide.entry
   - glide.script

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- glide.session
- glide.saml2
- com.glide.communications
- com.snc.integration.saml_esig



Remarque :
Lorsque vous créez le clone, incluez les pièces jointes afin que les certificats soient transférés vers l'instance cible. Assurez-vous également que la case **Thème** est décochée afin que ces propriétés soient préservées, que vous conserviez ou non le thème d'instance.

3. Sur l'instance source, accédez à **Clone système** > **Conserver les données** pour conserver les certificats SAML sur les sys_certificate et les utilisateurs SAML sur les sys_user liés à SAML/SSO/Multi SSO.

   Si vous en avez besoin, exportez-les en XML, puis importez-les manuellement sur la cible.

Avertissement :
N'essayez pas de cloner la configuration SAML/SSO/Multi SSO d'un système à un autre. La plupart des transferts des paramètres SAML/SSO ou Multi SSO ne fonctionnent PAS, car ils doivent être configurés sur le fournisseur d'identité. Si vous remplacez une configuration de travail, l'instance cible ne pourra pas s'authentifier et votre instance cible deviendra inaccessible. De plus, ne modifiez pas la sys_id de votre enregistrement de fournisseur Multi SSO ; Cela forcera vos utilisateurs à vider leurs cookies. Pour plus d'informations sur les précautions à prendre en matière de clonage, consultez Liste de vérification avant de cloner une instance .

4. Excluez les tables Multi SSO sso_properties, digest_properties et saml2_update1_properties.
5. Créez manuellement les enregistrements SAML/SSO/Multi SSO sur chaque instance indépendamment, et configurez également les enregistrements sur votre fournisseur d'identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Assurez-vous de créer manuellement un compte administrateur LOCAL sur sys_user enregistrement (et non dans LDAP ou SAML) sur l'instance cible et avec un sys_id qui n'existe pas dans l'instance source.
7. Cliquez sur **Mettre à jour**.

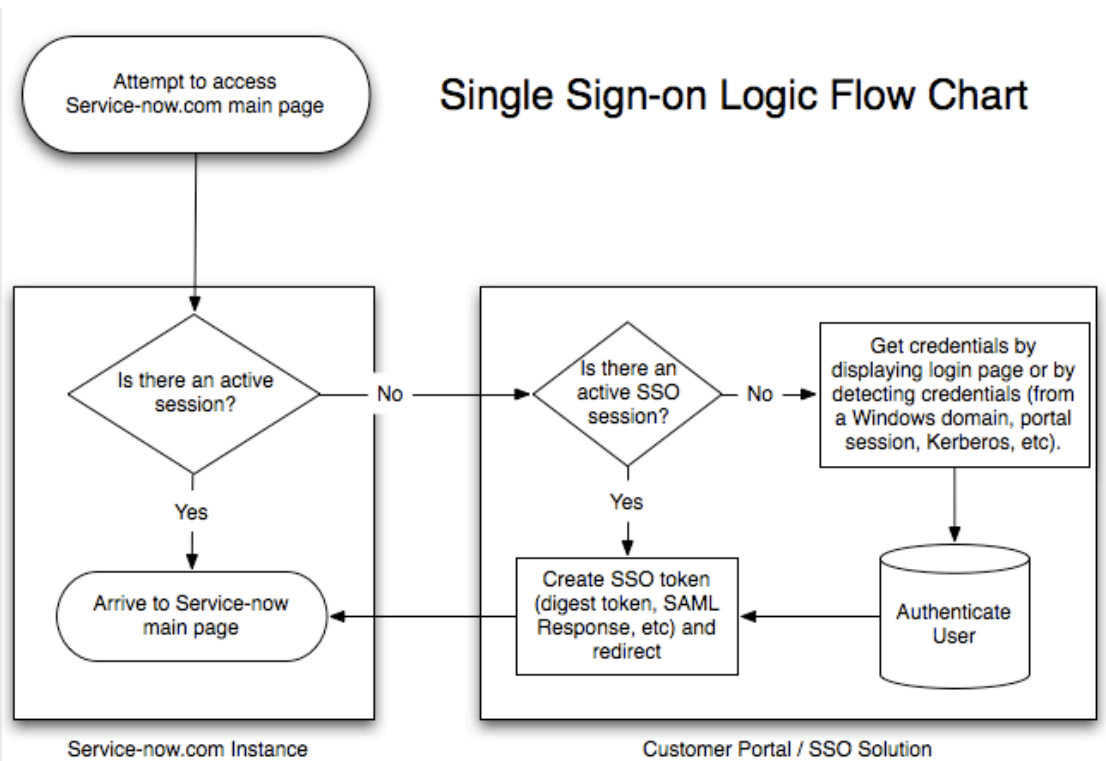
Concepts SAML 2.0

Familiarisez-vous avec ces concepts SAML.

Flux de processus SAML classique (diagramme)

Un flux logique SSO classique implique la recherche d'une session active, la vérification des informations d'identification de l'utilisateur et la création du jeton nécessaire.

Norme SSO



Flux de processus de connexion (AuthnRequest)

SAML 2.0 spécifie un profil SSO de navigateur Web qui implique l'échange d'informations entre un fournisseur d'identité (IdP), un fournisseur de service (SP) et un principal (utilisateur) sur un navigateur Web.

Le fournisseur d'identité peut être n'importe quel service SSO offrant des services d'authentification SAML (par exemple, SSOCircle). Le fournisseur de service est toujours une instance. Le flux de messages commence par une demande de ressource sécurisée auprès du fournisseur de service.

Demander la ressource cible au niveau du portail de services

Le principal demande une ressource cible au fournisseur de service :

https://instance.service-now.com/

L'instance vérifie la demande pour voir si les paramètres URL SAMLRequest et RelayState sont présents. S'ils existent, l'utilisateur a déjà validé avec l'IdP et peut ignorer les étapes 2 à 6.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Émettre une AuthnRequest au fournisseur d'identité

L'instance construit une demande AuthnRequest à envoyer à l'IdP à l'aide de la valeur SAMLRequest . L'instance construit et envoie également une valeur de paramètre d'URL RelayState .

Le jeton RelayState est une référence opaque aux informations d'état conservées chez le fournisseur de service. La valeur du paramètre SAMLRequest est la valeur déflatée et codée base64 de l'élément <samlp :AuthnRequest> :

```
<samlp:AuthnRequest    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"    ID="identifier_1"
   Version="2.0"    IssueInstant="2004-12-05T09:21:59Z"
 AssertionConsumerServiceIndex="0"><saml:Issuer>https://
sp.example.com/SAML2</saml:Issuer><samlp:NameIDPolicy      AllowCreate="true"
 Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/></samlp:AuthnRequest>
```

L'intégration encode ensuite l'élément <samlp :AuthnRequest> et l'envoie en tant que paramètre d'URL SAMLRequest .

Le service SSO traite l'élément <samlp :AuthnRequest> par décodage d'URL, décodage base64 et gonflage de la demande, dans cet ordre. Il procède ensuite à un contrôle de sécurité. Si l'utilisateur ne présente pas de contexte de sécurité valide, l'IdP l'identifie en l'invitant à entrer des informations d'identification de connexion. Si l'utilisateur est déjà connecté, l'IdP répond simplement avec les paramètres d'URL SAMLResponse<tt> et <tt>RelayState (voir étape 3).

Répondre avec une réponse SAML et RelayState

Après avoir collecté les identifiants de connexion requis, le service SSO valide la demande et répond avec un document contenant un formulaire XHTML :

```
<formmethod="post"action="https://instance.service-now.com/navpage.do" ...><input
 type="hidden" name="SAMLResponse" value="response ..." /><input type="hidden"
 name="RelayState" value="token ..." />
   ...
   <input type="submit" value="Submit" /></form>
```

La valeur du paramètre RelayState provient de cette étape. La valeur du paramètre SAMLResponse est le codage base64 de l'élément <samlp :Response> suivant :

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="s2cdc74f37f923e26fe1aeec42b70a93d24230334f"
InResponseTo="90AA6073F01567BFB0DF194F596314E2"
 Version="2.0"  IssueInstant="2010-04-29T23:21:51Z"
Destination="https://dloomac.service-now.com/navpage.do"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://
idp.ssocircle.com</saml:Issuer><samlp:Status
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><samlp:StatusCode
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode></samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="s23e536bfc51b8487d4d3299dec162d9c2e338823b"
IssueInstant="2010-04-29T23:21:51Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#">

...
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    </Signature><saml:Subject><saml:NameID
 Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
         NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml:NameID><saml:Su
bjectConfirmation
 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:SubjectConfirmationData
           InResponseTo="90AA6073F01567BFB0DF194F596314E2"
           NotOnOrAfter="2010-04-29T23:31:51Z"
 Recipient="https://dloomac.service-now.com/navpage.do" /
></saml:SubjectConfirmation></saml:Subject><saml:Conditions
 NotBefore="2010-04-29T23:11:51Z"
 NotOnOrAfter="2010-04-29T23:31:51Z"><saml:AudienceRestriction><saml:Audience>http
s://
dloomac.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
<saml:AuthnStatement AuthnInstant="2010-04-29T23:21:51Z"
 SessionIndex="s2dbf89ab99001e0e8cdaed67266d9d4b21b968a04"><saml:AuthnContext><sa
ml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo
rt</saml:AuthnContextClassRef></saml:AuthnContext></saml:AuthnStatement></saml:Asse
rtion></samlp:Response>
```

Valider la SAMLResponse

La valeur `SAMLResponse` est décodée et gonflée en base64 pour révéler le document XML à l'étape 3. Le script de connexion extrait la valeur XML de l'élément `Subject/NameID` et l'utilise pour rechercher un utilisateur existant dans la table Utilisateur.

Le script de connexion extrait également l'ID de session de l'élément `AuthnStatement/@SessionIndex` et le stocke pour la `LogoutRequest`.

Flux de processus de déconnexion (LogoutRequest)

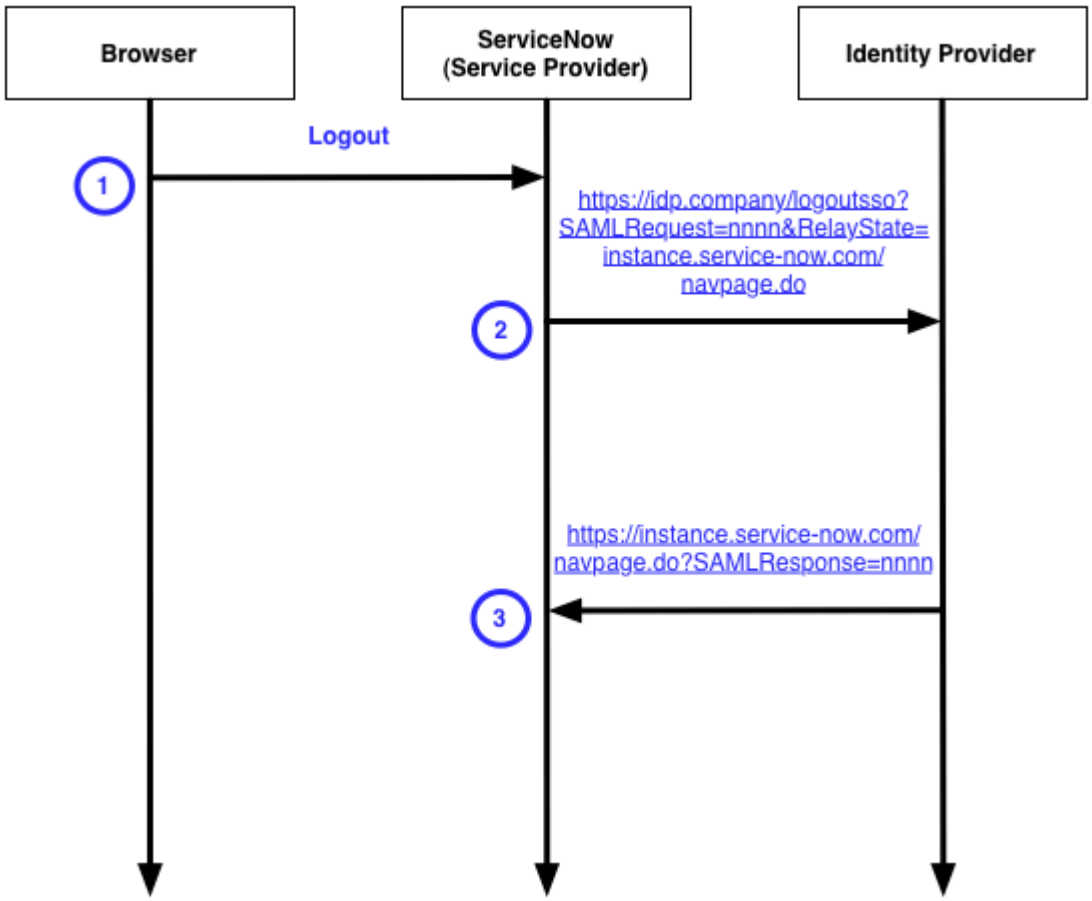
Pendant la déconnexion, l'instance émet l'appel de service SAML 2.0 *LogoutRequest* à l'IdP.

Ce service déconnecte l'utilisateur, puis le redirige vers l'URL de déconnexion spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Déconnexion SAML 2



L'utilisateur clique sur le bouton de déconnexion

L'utilisateur clique sur le bouton **Déconnexion** et l'instance exécute le script de déconnexion.

LogoutRequest émise

Le script de déconnexion crée une `LogoutRequest` SAML 2.0 et la publie sur le service SAML 2.0 SingleLogoutRequest préconfiguré sur l'IdP. L'IdP déflate la demande, puis la code base64. Voici un exemple de `LogoutRequest` :

```
<saml2p:LogoutRequestxmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
 ID="21B78E9C6C8ECF16F01E4A0F15AB2D46"  IssueInstant="2010-04-28T21:36:11.230Z"
 Version="2.0"><saml2:Issuer
 xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://dloomac.service-now.com
 </saml2:Issuer><saml2:NameID xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
        NameQualifier="http://idp.ssocircle.com"
 SPNameQualifier="https://
dloomac.service-now.com/navpage.do">david.loo@service-now.com</saml2:NameID><saml2
p:SessionIndex>s211b2f811485b2a1d2cc4db2b271933c286771104
 </saml2p:SessionIndex></saml2p:LogoutRequest>
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

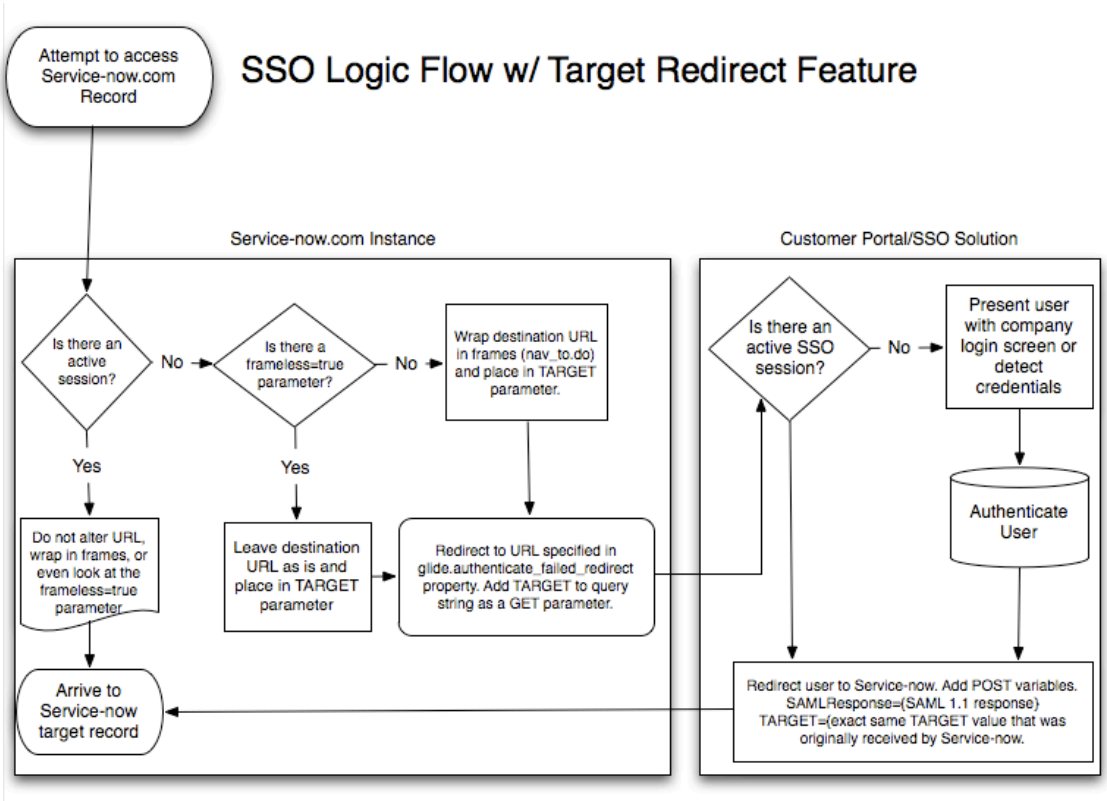
L'utilisateur se déconnecte

L'utilisateur se déconnecte de l'IdP. L'IdP redirige vers l'instance, qui à son tour redirige vers l'IdP puisque l'utilisateur n'est pas connecté.

Informations sur l'URL d'un fournisseur SSO

Lors d'un défi de connexion résultant d'un lien URL vers l'instance qui nécessite une session SSO, il peut être nécessaire de fournir l'URL de référence au fournisseur SSO afin qu'après authentification, l'URL puisse être renvoyée à l'instance et liée à la ressource appropriée.

Redirection de cible SSO



Les valeurs de retour de sortie d'installation ont été améliorées pour transmettre une URL à la place ou en plus de l'URL définie par les propriétés. En règle générale, vous devez renvoyer un nom d'utilisateur ou une valeur de chaîne prédéfinie pour contrôler, autoriser ou défier la session SSO. Les exemples suivants montrent le comportement étendu de la transmission d'une URL.

```
return
 "failed_missing_requirement:%26amp;TARGET=https://
instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345";
```

L'exemple ci-dessus transmet la https://instance.service-now.com/nav_to.do?uri=incident.do?sys_id=12345 d'URL au fournisseur SSO sous la forme d'un paramètre d'URL nommé TARGET.

Remarque :
Nous supposons que le fournisseur SSO utilise ces informations dans le paramètre TARGET pour rediriger vers l'instance lorsque les informations d'identification de l'utilisateur ont été collectées et que l'authentification a été réussie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Un deux-points : délimite les deux valeurs de retour et un & codé (%26amp ;) concatène l'URL définie dans la propriété *glide.authenticate.failed_missing_requirement* et le paramètre TARGET.

Configuration SAML 2.0 à l'aide de la SSO de plusieurs fournisseurs

Vous pouvez créer ou mettre à jour une configuration SSO SAML 2.0 à partir de la fonctionnalité SSO de plusieurs fournisseurs.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Remarque :

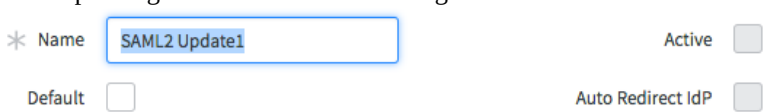
Nouveauté de la Jakarta version, vous devez valider votre configuration à l'aide de la fonctionnalité de test de la connexion avant de pouvoir activer votre configuration IdP. Vous pouvez toujours utiliser la fonctionnalité de mise à jour pour enregistrer vos données de configuration, mais il ne s'agit pas d'une configuration active sans une connexion de test réussie.

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Effectuez l'une des actions suivantes.
   - Pour mettre à jour une configuration, cliquez sur un enregistrement de configuration SSO.
   - Pour créer une configuration, cliquez sur **Nouveau** > **SAML**.
3. Entrez les informations IdP par l'une des méthodes suivantes.

Option	Description
Utilisation d'une URL de descripteur de méta-données	Cochez la case URL et entrez l'URL de l'IdP que vous utilisez.
Utilisation d'un fichier XML de descripteur de métadonnées	Cochez la case XML et collez les données XML générées à partir de l'IdP que vous utilisez.
Saisie manuelle des métadonnées	Fermez la fenêtre contextuelle et saisissez manuellement les données dans les champs de propriété.

Tous les champs obligatoires doivent être renseignés sur le formulaire du fournisseur d'identité.



Champs d'authentification unique de plusieurs fournisseurs

Propriété	Obligatoire	Description
Nom	Oui	Saisissez le nom de l'IdP. Cet IdP est l'ID système de redirection automatique.
Actif	Oui	Actif doit être défini sur vrai pour que l'IdP soit utilisé pour l'authentification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Obligatoire	Description
		Remarque : L'option permettant de définir cette propriété n'est disponible qu'après une connexion de test réussie.
Par défaut	Non	L'IdP de redirection automatique, anciennement connu sous le nom d'IdP principal, redirige automatiquement les utilisateurs pour accéder à l'URL de l'instance de base. Cette propriété définit cette configuration IdP comme configuration par défaut.
Rediriger automatiquement l'IdP	Non	Définit cette configuration IdP comme IdP de redirection automatique. **Remarque :** Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie est mis à jour avec le nouvel IdP de redirection automatique. La `glide.authenticate.sso.update.idp.cookie` propriété système, activée automatiquement, contrôle cette fonctionnalité.
URL du fournisseur d'identité	Oui	Entrez l'URL de votre fournisseur d'identité. Chaque URL IdP doit être unique.
Service AuthnRequest du fournisseur d'identité	Oui	Entrez l'URL de la liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService.
Service SingleLogoutRequest du fournisseur d'ident	Non	Entrez l'URL obtenue à partir de l'élément SingleLogoutService.
ServiceNow Page d'accueil	Oui	Entrez l'URL, y compris la page de connexion, de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/navpage.do
ID d'entité/Émetteur	Oui	Entrez l'URL de base, à l'exclusion de la page de connexion. de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
URI de l'audience	Oui	Entrez l'URL de base, à l'exclusion de la page de connexion. de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
Politique NameID	Oui	Saisissez la valeur de l'élément NameIDFormat que l'intégration utilise.
Redirection de déconnexion externe	Non	Saisissez l'URL vers laquelle l'intégration redirige les utilisateurs après leur déconnexion.
Échec de la redirection du besoin	Non	Entrez l'URL de redirection des demandes d'authentification ayant échoué. Par défaut, il s'agit du point de terminaison d'URL d'une page d'erreur ou d'une page de déconnexion configurée dans l'IdP. Vous pouvez renseigner cette valeur dans le champ glide.authenticate.failed_requirement_redirect.
Type de client	Non	Choisissez le type de client en fonction du type de votre client. Options :**Iframe intégré**.

Traduction automatique

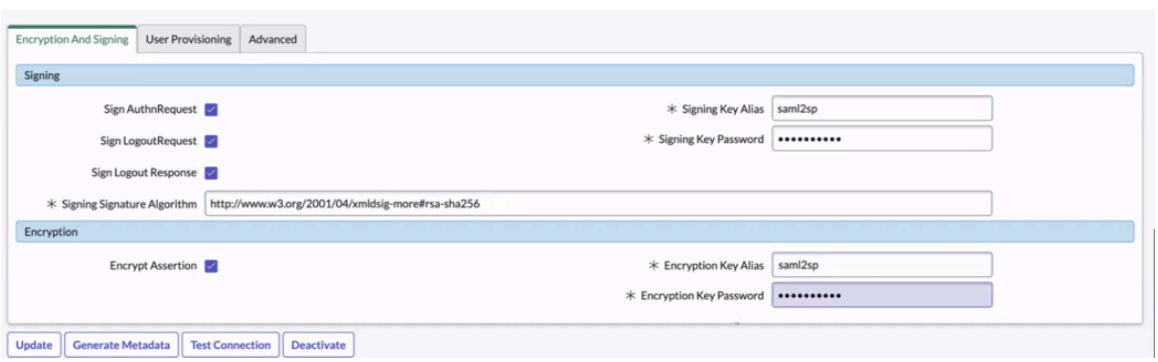
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Obligatoire	Description
		Remarque : Si le champ de type client est requis pour votre configuration, vous pouvez modifier le formulaire et ajouter le champ. Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

4. **Facultatif :** Onglet Chiffrement et signature

Remarque :

- Il est recommandé d'utiliser vos propres certificats pour le chiffrement et la signature.
- Le **mode approuvé FIPS** nécessite différents certificats pour le **chiffrement** et la **signature**
- Lors de l'utilisation des certificats, veillez à mettre à jour les propriétés système suivantes avec l'sys_id des certificats (certificats x.509) :
  - **Signature** (glide.authenticate.sso.saml2.keystore)
  - **Chiffrement** (glide.authenticate.sso.saml2.encryption.keystore)
- Assurez-vous de mettre à jour l'alias de clé et le mot de passe de clé des magasins de clés **de signature** et de **chiffrement** dans l'enregistrement du fournisseur d'identité et de générer les métadonnées (sélectionner **Générer les métadonnées**).
- Chargez les certificats de signature et de chiffrement présents dans les métadonnées générées (XML) vers le fournisseur d'identité.



Champs de chiffrement et de signature

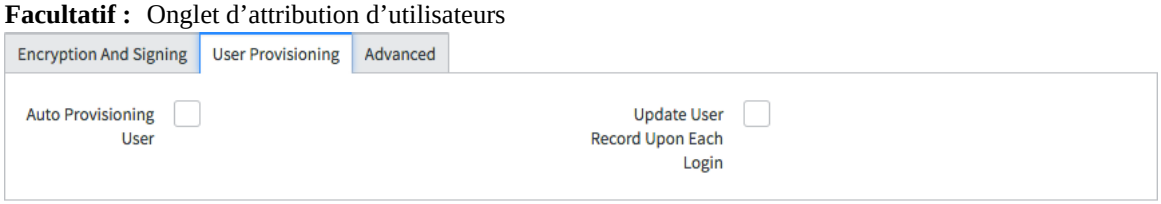
Propriété	Description
Signature avec l'alias de clé	Saisissez l'alias de signature de l'entrée de clé stockée dans le magasin de clés SAML 2.0 SP.
Signature avec le mot de passe de clé	Saisissez le mot de passe de signature de l'entrée de clé stocké dans le magasin de clés SAML 2.0 SP.
Alias de clé de chiffrement	Entrez l'alias de chiffrement de l'entrée de clé stockée dans le magasin de clés SAML 2.0 SP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
Mot de passe de clé de chiffrement	Saisissez le mot de passe de chiffrement de l'entrée de clé stockée dans le magasin de clés SAML 2.0 SP.
Chiffrer l'assertion	Cochez la case pour chiffrer l'assertion dans la réponse SAML. Les métadonnées générées pour l'IDP incorporent le certificat x509, que l'IDP utilise pour chiffrer l'assertion dans la réponse SAML qu'il génère.
Algorithme de signature pour la signature	Entrez l'URL qui pointe sur le consommateur AuthnRequest du fournisseur d'identité SAML 2.0 pour l'authentification de signature électronique.
Signer l'AuthnRequest	Cochez la case pour permettre au service d'authentification unique IdP de recevoir une demande AuthnRequest signée.
Signer la LogoutRequest	Cochez la case pour permettre au service d'authentification unique IdP de recevoir une LogoutRequest signée.
Signer la réponse de déconnexion	Cochez la case pour permettre au service d'authentification unique IdP de recevoir une réponse de déconnexion signée.

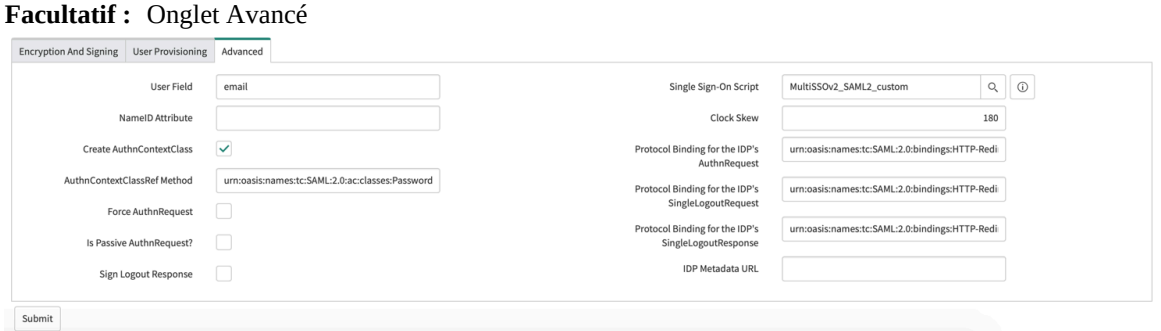
5. **Facultatif :** Onglet d'attribution d'utilisateurs



Champs d'attribution d'utilisateurs

Propriété	Description
Mise en service automatique de l'utilisateur	Activez l'attribution automatique d'utilisateurs, crée les utilisateurs lorsque l'utilisateur n'existe pas dans la table des utilisateurs de l'instance en fonction des informations fournies par l'IdP.
Mettre à jour l'enregistrement utilisateur à chaque connexion	Met à jour les informations utilisateur dans la table Utilisateur de l'instance avec les informations dans l'IdP chaque fois que l'utilisateur se connecte à l'aide de SAML.

6. **Facultatif :** Onglet Avancé



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs avancés

Propriété	Description
Champ d'utilisateur	Saisissez le champ de la table Utilisateur qui contient la valeur requise par l'IdP pour identifier l'utilisateur. Il s'agit d'un ID unique dans le cadre de la réponse. Par exemple, nom d'utilisateur, ID d'employé, etc. Dans la table utilisateur système, cet ID unique correspond aux détails de l'utilisateur.
Attribut NameID	Laissez ce champ vide à moins que vous ne configuriez une nouvelle stratégie NameID. Si vous configurez une nouvelle politique, le système requiert la table Utilisateur qu'il doit utiliser pour identifier l'utilisateur qui se connecte. Le système fait correspondre le jeton NameID au nom de ce champ de table d'utilisateur ici.
Créer une AuthnContextClass	Cochez la case pour spécifier une classe de contexte particulière, telle que Transport protégé par mot de passe. Si la case est décochée, l'IdP sélectionne la classe de contexte la plus appropriée.
Méthode AuthnContextClassRef	Entrez l'URL du mécanisme de connexion que l'IdP doit utiliser pour authentifier les utilisateurs.
Forcer l'AuthnRequest	Cochez la case pour forcer l'exécution des AuthnRequests.
Est une AuthnRequest passive	Cochez la case si l'AuthnRequest est passive.
Script d'authentification unique	Sélectionnez le script d'authentification unique. La valeur par défaut est *MultiSSOV2_SAML2_custom*.
Signer la réponse de déconnexion	Saisissez les détails de la réponse de déconnexion dans ce champ.
Décalage d'horloge	Entrez le nombre de secondes entre les deux attributs qui composent la réponse SAMLResponse nonce. La valeur par défaut est 60. Une réponse SAML valide doit se situer entre les valeurs de date/heure *notBefore* et *notOnOrAfter* . Consultez Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData et Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience pour un exemple de message SAMLResponse.
Protocole de liaison du service SingleLogoutReuqest de l'IDP	Entrez l'une des valeurs prises en charge répertoriées dans l'attribut Binding à partir de l'élément SingleLogoutService.
URL des métadonnées à partir de laquelle les propriétés IDP sont importées	Les propriétés IdP sont importées à partir de cette URL. Si défini, il active l'importation automatique du certificat SAML à partir de l'IdP si le certificat précédent a expiré. **Remarque :** Si vous effectuez une mise à niveau de la mise à jour 1 de SAML2 vers la SSO de plusieurs fournisseurs ou si vous configurez manuellement votre connexion SSO, l'URL des métadonnées IdP ne s'affiche pas automatiquement.
Demande	ID unique dans le cadre de la demande, l'ID peut être le nom d'utilisateur, l'ID d'employé, etc.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

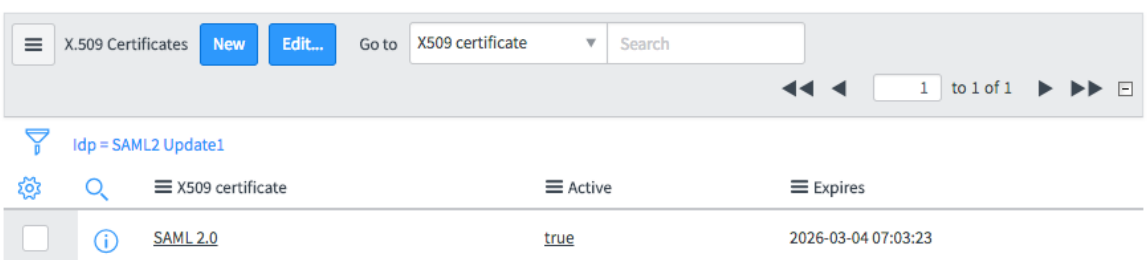
Propriété	Description
	Remarque : La redirection et la liaison postérieure sont prises en charge pour la demande. L'option permettant de définir ce champ n'apparaît qu'après une connexion de test réussie. Pour plus d'informations, reportez-vous à la section Test des connexions IdP.
Réponse	ID unique Dans le cadre de la réponse, l'ID peut être le nom d'utilisateur, l'ID d'employé, etc. **Remarque :** La redirection et la liaison postérieure sont prises en charge pour la réponse. L'option permettant de définir ce champ n'apparaît qu'après une connexion de test réussie. Pour plus d'informations, reportez-vous à la section Test des connexions IdP.

Certificats X.509 pour SAML

Stockez et activez les certificats IdP nécessaires pour votre configuration SAML.

Les certificats X.509 sont les certificats IdP qu'une configuration SAML utilise. Après avoir installé un certificat, vous pouvez ajouter autant de certificats que nécessaire. Lorsqu'il existe plusieurs certificats, le système utilise le premier certificat actif trouvé. Si vous définissez l'URL pour **l'URL des métadonnées à partir de laquelle les propriétés IDP sont importées**, le système interroge automatiquement l'IdP pour obtenir un certificat valide actuel lorsque votre certificat n'est plus valide. Il ajoute ce certificat à votre instance et l'utilise pour votre configuration SAML active.

Remarque :
L'interrogation a lieu si l'IdP est accessible en dehors de votre réseau.



Visite guidée SAML

Utilisez la visite guidée SAML pour configurer le SAML pour l'authentification unique.

La visite guidée SAML vous aide à former et à configurer l'authentification unique (SSO) pour votre ServiceNow® instance. Les administrateurs peuvent sélectionner la visite guidée pour connaître rapidement les actions requises lors de la configuration de la SSO pour les instances.

Avant d'utiliser la visite guidée, vous devez configurer une application SAML dans votre fournisseur d'identité préféré, comme Okta, Microsoft Azure, ADFS, etc. Pour en savoir plus sur la configuration d'une application SAML, consultez la documentation suivante :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Okta: Pour Okta, vous devez effectuer les opérations suivantes :
  - Ajouter une application SAML Okta
  - Configurer SAML 2.0 pour ServiceNow®
- Microsoft Azure : Intégration de Single Sign-on (SSO) avec ServiceNow®
- Ping: Configuration de l'authentification SSO SAML avec ServiceNow®
- ADFS : Intégration avec SAML 2.0

Pour utiliser la visite guidée SAML, activez le module d'extension Intégration - Programme d'installation de l'authentification unique de plusieurs fournisseurs. Pour plus d'informations, reportez-vous à la section Activer le module d'extension SSO de plusieurs fournisseurs.

Pour utiliser la visite guidée SAML, procédez comme suit :

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseur d'identité**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez **SAML.**
4. Cliquez sur l'icône **Aide** .
5. Cliquez sur **Suivre une visite guidée**.

La visite guidée SAML utilise une série d'étapes qui s'étendent sur plusieurs pages pour terminer la configuration, en suivant les étapes et les instructions fournies dans le cadre de la visite guidée et terminer la visite. Pour en savoir plus sur la configuration SAML, reportez-vous à la section Configuration SAML 2.0 à l'aide de la SSO de plusieurs fournisseurs.

Intégration de SAML 2.0 avec d'autres fonctionnalités

Vous pouvez intégrer votre solution SAML 2.0 à d'autres fonctionnalités telles que la signature électronique, les liens profonds et ADFS.

Ajouter la prise en charge des liens profonds pour SAML

Le lien profond permet aux instances de prendre en charge des liens d'e-mail directs vers un enregistrement particulier dans le système.

Lorsque l'intégration SAML 2.0 est activée, les URL de liens profonds doivent passer un contrôle d'authentification avant que l'IdP ne redirige l'utilisateur vers l'URL demandée à l'origine. Prenons l'exemple d'un e-mail qui contient l'URL suivante : `https://<nom d'instance>.service-now.com/nav_to.do?uri=incident.do?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`

L'instance envoie une demande d'authentification à l'IdP et utilise le paramètre `URL RelayState` pour conserver la ressource demandée à l'origine (dans ce cas, `uri=incident.do ?sys_id=46c88ac1a9fe1981014de1c831fbcf6d`). Une fois que l'IdP a authentifié l'utilisateur, l'instance lit la valeur du paramètre URL RelayState et redirige l'utilisateur vers la ressource demandée (si elle existe dans l'instance).

Pour ajouter la prise en charge du lien profond, vérifiez que le fournisseur d'identité prend en charge le paramètre `URL RelayState` .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Intégration ADFS avec SAML 2.0

Le ServiceNow module d'extension SSO de plusieurs fournisseurs prend en charge une intégration SAML 2. Single Sign-On (SSO) avec Microsoft ADFS.

Pour plus d'informations sur l'installation et la configuration d'ADFS, consultez Vue d'ensemble des services de fédération Active Directory . Le module d'extension SSO de plusieurs fournisseurs a été configuré et testé avec une intégration SAML 2.0 SSO avec ADFS 2.0, 3.0, Azure AD.ributes ne prend pas en charge la réponse SAML dans

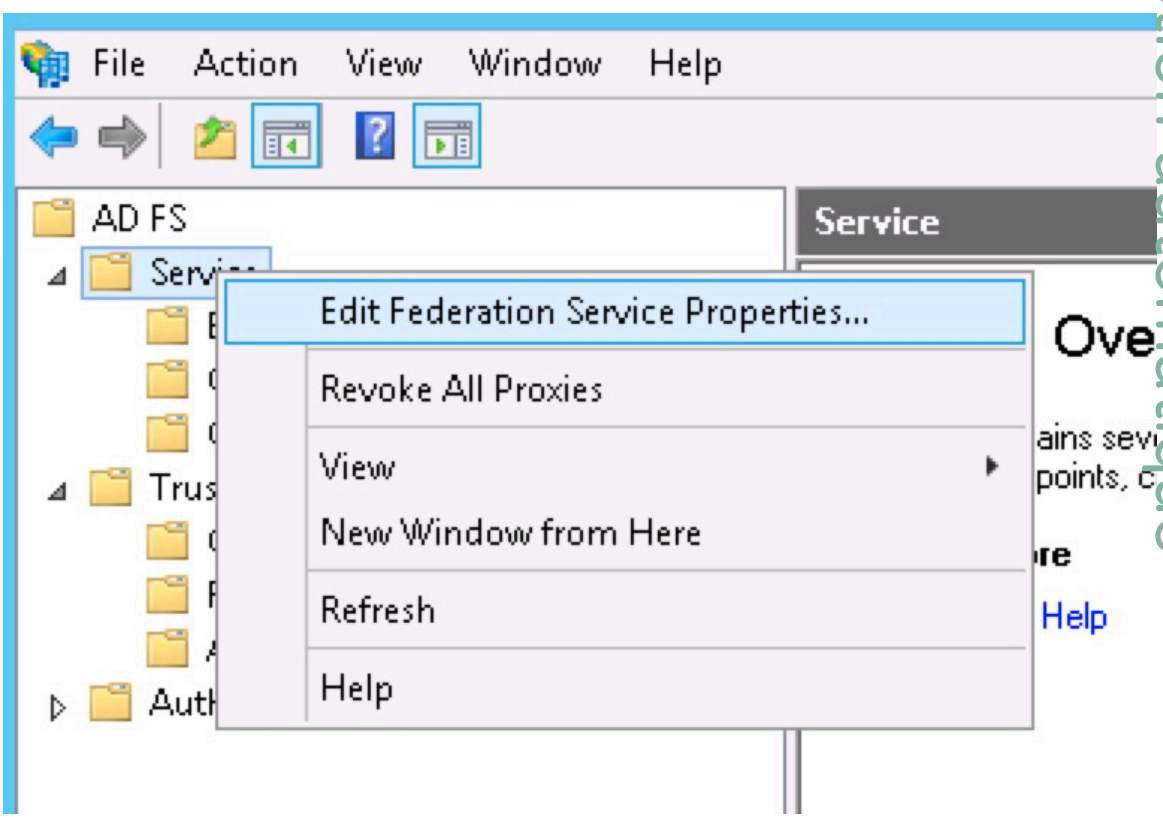
Configurer ADFS pour SAML

Configurez ADFS pour SAML. Cette procédure utilise ADFS 2.0 et affiche samportal.example.com comme site Web ADFS. Remplacez-la par l'adresse de votre site Web ADFS.

Avant de commencer
Rôle requis : administrateur

Procédure

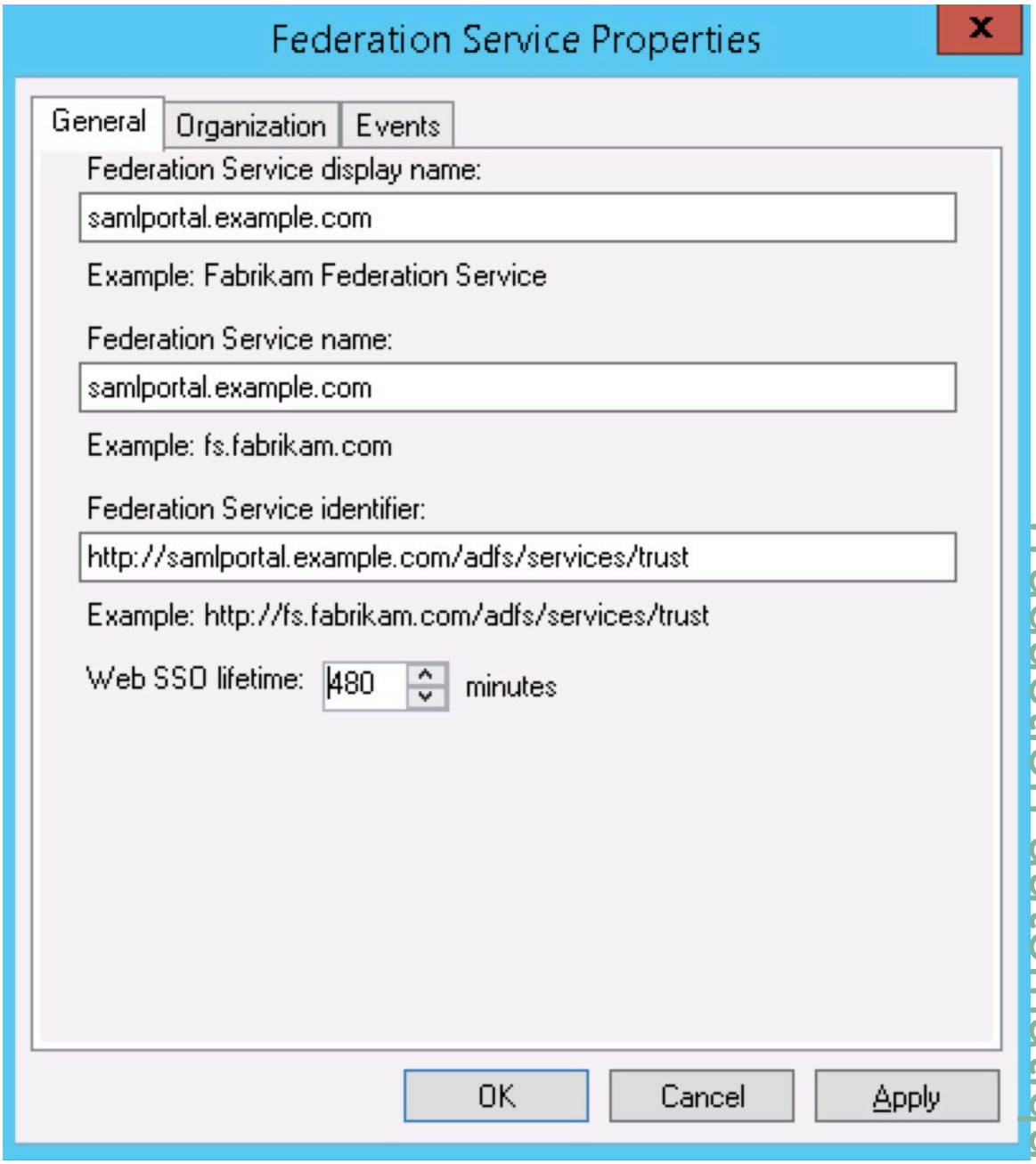
1. Connectez-vous au serveur ADFS 3.0 et ouvrez la console de gestion.
2. Cliquez avec le bouton droit sur **Service** et sélectionnez **Modifier les propriétés de service de fédération**.



3. Vérifiez que les paramètres généraux correspondent à vos entrées DNS et à vos noms de certificat.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

4. Accédez aux certificats et exportez le certificat de signature de jeton.

   a. Cliquez avec le bouton droit sur le certificat et sélectionnez **Afficher le certificat**.

   b. Sélectionnez l'onglet **Détails**.

   c. Cliquez sur **Copier dans le fichier**.
   L'assistant d'exportation du certificat s'ouvre.

   d. Sélectionnez **Suivant**.

   e. Assurez-vous que l'option **Non, ne pas exporter la clé privée** est sélectionnée, puis cliquez sur **Suivant**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

f. Sélectionnez **X.509 (.cer) binaire codé DER**, puis cliquez sur **Suivant**.

g. Sélectionnez l'emplacement où vous souhaitez enregistrer le fichier, donnez-lui un nom, puis cliquez sur **Suivant**.

h. Sélectionnez **Finish** (Terminer).
L'instance exige que ce certificat soit au format PEM. Vous pouvez convertir ce certificat à l'aide d'outils clients ou d'outils en ligne tels que SSL Shopper.

5. Utilisez le certificat DER/binaire que vous venez de créer et exportez-le au format PEM standard.

Configurer l'instance pour ADFS

Configurez votre instance et les paramètres SAML 2.0 pour qu'ils fonctionnent avec ADFS.

Avant de commencer
Effectuez ces étapes uniquement une fois que vous avez configuré ADFS pour SAML. Pour plus d'informations sur ce processus, consultez Configurer ADFS pour SAML.

Rôle requis : administrateur

Procédure

1. S'ils ne sont pas déjà actifs, Activer le module d'extension SSO de plusieurs fournisseurs.
2. Configurez SAML, mais lorsque vous installez le certificat IdP, joignez le certificat PEM que vous avez créé lors de l'installation Configurer ADFS pour SAMLdu certificat IdP.
3. Cliquez sur **Enregistrer**.
4. Vérifiez que les champs **Problème** et **Objet** ont des valeurs et qu'il n'y a pas d'erreurs.
Si une erreur se produit, ouvrez le certificat au format PEM enregistré dans le Bloc-notes et copiez-collez le certificat dans le champ Certificat PEM.
5. Vérifiez que la sortie de l'installation SAML2SingleSignon_update1 est active.
6. Poursuivez la configuration SAML 2.0.

Remarque :
Lorsqu'un certificat est mis à jour sur le serveur ADFS, vous devez également charger un certificat mis à jour dans l'instance.

Configurer une partie de confiance ADFS

Prenez les métadonnées de l'instance et importez-les dans votre serveur ADFS. Toutefois, la configuration manuelle de la partie de confiance semble plus facile à mettre en œuvre.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité** > **Mise à jour 1 SAML2** > **Chiffrement et signature** et vérifiez que la propriété SAML Sign AuthnRequest (`glide.authenticate.sso.saml2.require_signed_authnrequest`) n'est pas active.
Ne conservez cette propriété active que si votre administrateur ADFS peut vérifier que vous exigez des demandes signées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

2. Copiez les métadonnées que vous avez générées via le lien des métadonnées SAML 2 et enregistrez-les dans un fichier.
3. Connectez-vous au serveur ADFS et ouvrez la console de gestion.
4. Sélectionnez **les approbations de la partie de confiance**.
5. Sélectionnez **Ajouter une approbation de partie de confiance** dans le coin supérieur droit de la fenêtre.

   L'assistant d'ajout s'affiche.
6. Cliquez sur **Démarrer** pour commencer.
7. Utilisez l'option **Importer un fichier** pour importer le fichier de métadonnées.
8. Donnez-lui un nom d'affichage tel que ServiceNow et entrez les notes de votre choix.
9. Sélectionnez **le profil ADFS 3.0**.
10. Ne sélectionnez pas de certificat de chiffrement de jeton.
    Il utilisera le certificat défini sur le service qui a déjà été exporté. La définition d'un certificat empêche une communication correcte avec l'instance.
11. N'activez aucun paramètre sur **l'URL de configuration**.
12. Entrez le site de l'instance auquel vous vous êtes connecté comme identificateur d'approbation de la partie de confiance.
    Dans ce cas, utilisez https://company.service-now.com et cliquez sur **Ajouter**.
13. Autorisez tous les utilisateurs à accéder à cette partie de confiance.
14. Cliquez sur **Suivant** et décochez **la case Ouvrir les réclamations une fois l'opération terminée** .
15. Fermez cette page.
    La nouvelle approbation de la partie de confiance apparaît dans la fenêtre.
16. Cliquez avec le bouton droit de la souris sur l'approbation de la partie de confiance et sélectionnez **Propriétés**.
17. Accédez à l'onglet **Avancé** et définissez **l'algorithme de hachage sécurisé** sur SHA-256 ou SHA-1.
18. Accédez à l'onglet Points de terminaison et ajoutez un **consommateur d'assertion SAML** avec une liaison **POST** et une URL de https://company.service-now.com/navpage.do.

Configurer les règles de réclamation des parties de confiance ADFS

Modifiez les règles de réclamation pour permettre une communication correcte avec l'instance.

Avant de commencer

Rôle requis : administrateur

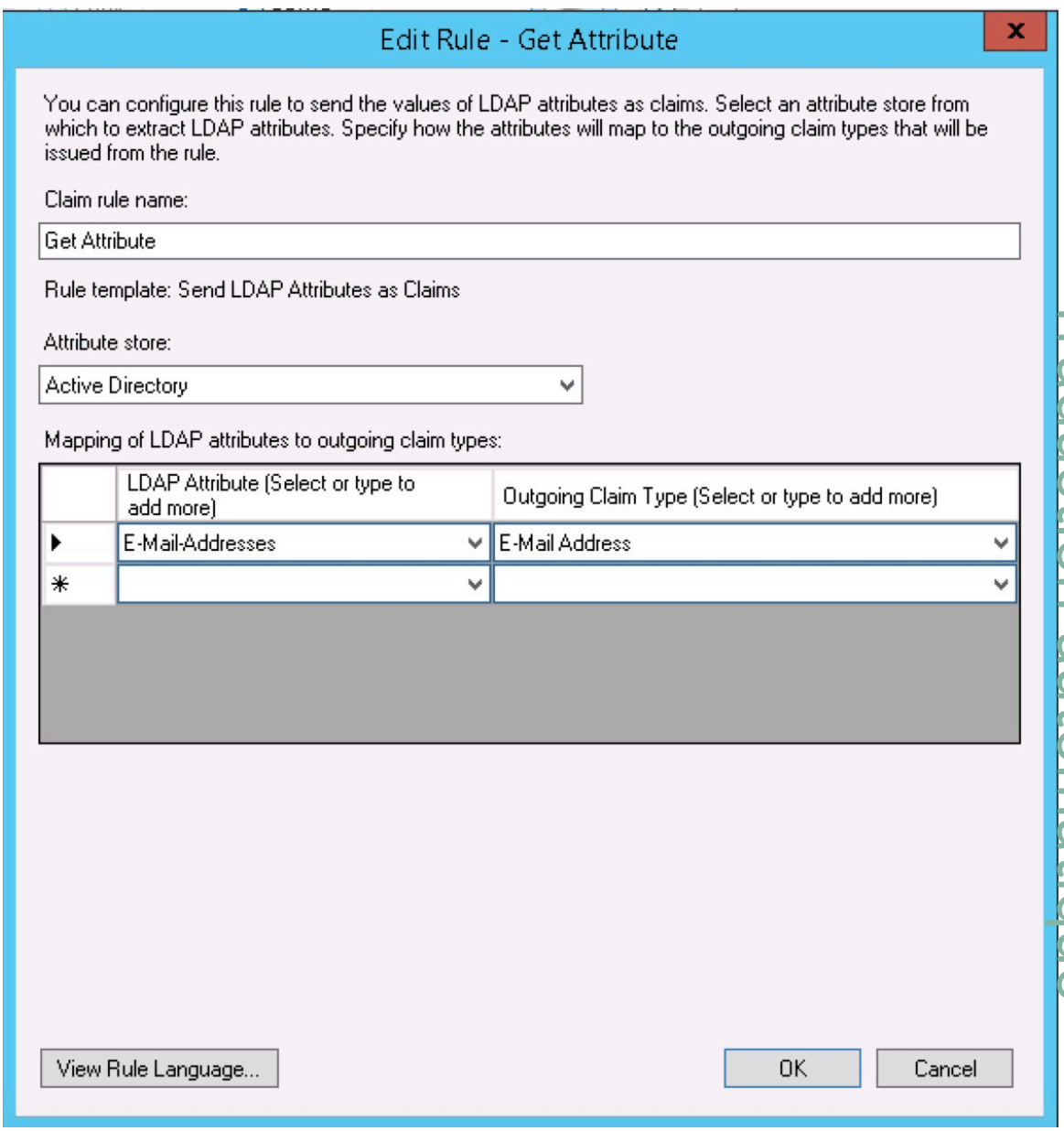
Procédure

1. Connectez-vous au serveur ADFS et ouvrez la console de gestion.
2. Cliquez avec le bouton droit de la souris sur la fiducie de la partie de confiance et sélectionnez **Modifier les règles de réclamation**.
3. Cliquez sur l'onglet **Règles de transformation d'émission** .
4. Sélectionnez **Ajouter des règles**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. Sélectionnez **Envoyer l'attribut LDAP en tant que réclamations** comme modèle de règle de réclamation à utiliser.
6. Donnez à la réclamation un nom tel que Obtenir des attributs LDAP.
7. Définissez le **magasin d'attributs** sur Active Directory, l'attribut **LDAP** sur adresses e-mail et le **type de réclamation sortante** sur adresse e-mail.




```
c:[Type ==
 "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer
 == "AD AUTHORITY"]
=> issue(store = "Active Directory",
types = ("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"),
query = ";mail;{0}", param = c.Value);
```

8. Sélectionnez **Finish** (Terminer).
9. Sélectionnez **Ajouter des règles**.

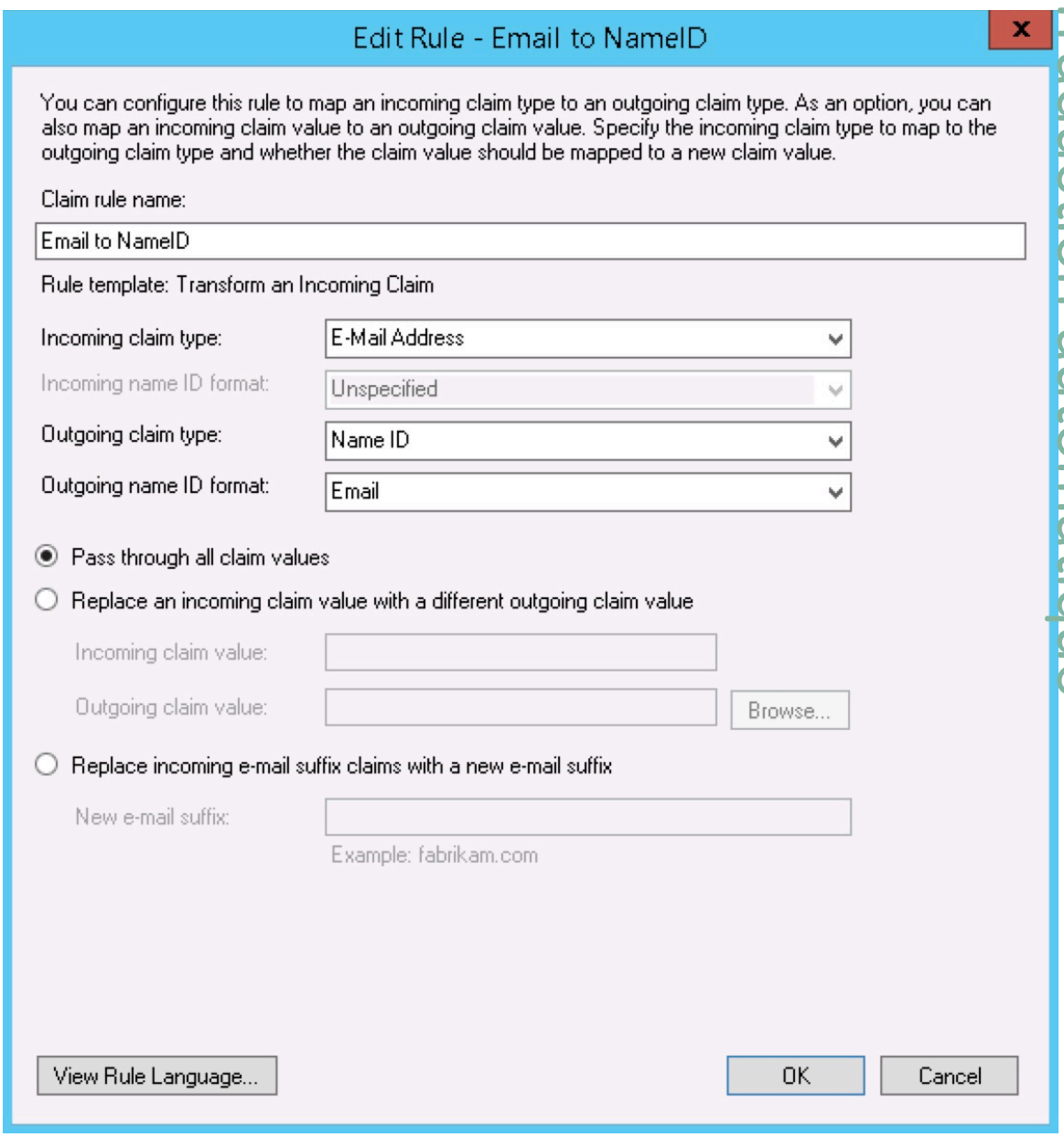
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

10. Sélectionnez **Transformer une réclamation entrante** en tant que modèle de règle de réclamation à utiliser.
11. Donnez un nom à la réclamation, par exemple `Email to Name ID`.
12. Définissez le **type de réclamation entrante** sur le **type de réclamation sortante** dans la règle précédente.
    Par exemple, `Adresse e-mail`.
13. Définissez le **type de réclamation sortante** sur `ID de nom` et le **format d'ID de nom sortant** sur `E-mail`.

    Remarque :
    Ces valeurs doivent correspondre à la politique d'ID de nom que vous définissez lors de la configuration SAML 2.0.

14. Sélectionnez **Transmettre toutes les valeurs de réclamation**.



Cette règle de réclamation doit ressembler au langage suivant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
 => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
 c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"]
= "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress");
```

15. Cliquez sur **Terminer**.

Créer un point de terminaison de déconnexion SAML

Créez un point de terminaison de déconnexion SAML pour permettre une déconnexion unique.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Consultez cet article sur la déconnexion ADFS pour plus d'informations.

Procédure

1. Accéder à **Gestionnaire ADFS** > **Relations de confiance** > **Approbations de partie de confiance** > **Propriétés de**.
2. Sous l'onglet Points de terminaison, cliquez sur **Ajouter SAML.**
3. Configurez les paramètres :
   - **Type de point de terminaison** : déconnexion SAML
   - **Reliure** : POST
   - **URL de confiance** : l'URL de votre serveur ADFS. Par exemple :

     ```
     https://myadfsserver.domain.net/adfs/ls/?wa=wsignout1.0
     ```

   - **URL de réponse** : l'URL de déconnexion de l'application. Par exemple :

     ```
     https://{instancename}.service-now.com/external_logout_complete.do
     ```

Tester la configuration ADFS

Testez votre configuration ADFS pour vérifier qu'elle fonctionne correctement en tant que fournisseur d'identité.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Ouvrez un navigateur Internet Explorer.
2. Accédez à votre portail ADFS.

   Par exemple, https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx. Cette page contient une liste déroulante de toutes les approbations de partie de confiance configurées.

3. Sélectionnez la partie de confiance associée à votre instance.
4. Cliquez sur **Continuer pour vous connecter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous avez correctement configuré l'authentification externe SAML 2.0, vous devez être automatiquement connecté à l'instance.

5. Testez une URL de connexion directe en accédant à https://samportal.example.com/adfs/ls/idpinitiatedsignon.aspx?logintoRP=https://company.service-now.com.

(Solution de contournement) Activer l'authentification initiée par le fournisseur de service

Utilisez cette solution de contournement si l'authentification échoue parce que vous n'avez pas SAML 2.0 Update 1. Ce problème peut se produire si les utilisateurs tentent d'ignorer l'authentification IdP et d'accéder directement à l'instance.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Cette erreur se produit lorsque l'instance ne fournit pas à ADFS la définition et la sémantique nécessaires pour l'attribut SPNameQualifier dans SAMLResponse.

Activez l'authentification initiée par le fournisseur de service en effectuant l'une des actions suivantes :

Procédure

- Effectuez une mise à niveau vers SAML 2.0 Update 1 et effacez l'option pour créer une demande AuthnContextClass.
- Modifiez l'include de script **SAML2** pour commenter les définitions de l'attribut SPNameQualifier lorsque SAML 2.0 est actif (et non SAML 2.0 Update 1).

  Commentez ces lignes dans les fonctions createNameID et createNameIDPolicy :

```
//nid.setSPNameQualifier (serviceURL ) ;

 //nameIdPolicy. setSPNameQualifier (serviceURLStr ) ;
```

Que faire ensuite
Si vous ne souhaitez pas que l'invite de connexion de votre serveur ADFS s'affiche lorsque vous accédez à l'instance, définissez la propriété SAML 2.0 Update 1 suivante sur false : **Créez une demande AuthnContextClass dans l'instruction AuthnRequest** (`glide.authenticate.sso.saml2.createrequestedauthncontext`).

(Solution de contournement) Prise en charge de l'authentification Kerberos

Une solution de contournement est disponible pour l'intégration SAML 2.0 qui modifie le contexte d'authentification de l'authentification basée sur des formulaires en une authentification basée sur Windows.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Actuellement, l'intégration SAML 2 utilise un contexte d'authentification PasswordProtectedTransport ou « authentification basée sur les formulaires ». Dans ce contexte d'authentification, l'IdP doit présenter aux utilisateurs un formulaire d'informations d'identification d'authentification. Avec Kerberos, une session SAML est déjà active via une connexion Windows établie, de sorte que l'utilisateur n'a pas besoin de s'authentifier avec l'IdP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Ouvrez l'enregistrement **IdP SAML2 Update1** .
3. Définissez la **méthode AuthnContextClassRef que nous inclurons dans notre SAML 2.0 AuthnRequest au fournisseur d'identité** sur l'une des valeurs suivantes :

Valeurs de la méthode AuthnContextClassRef
`urn :oasis :names :tc :SAML :2.0 :ac :classes :PasswordProtectedTransport` (par défaut)
`urn :federation :authentication :windows`

4. Cliquez sur **Mettre à jour**.

Intégration d'Azure AD à SAML 2.0

Intégrez ServiceNow Azure Active Directory (Azure AD).

L'intégration ServiceNow à Azure AD vous permet d'effectuer les actions suivantes :

- Contrôler dans Azure AD qui a accès à ServiceNow.
- Permettez aux utilisateurs de se connecter ServiceNow automatiquement avec leurs comptes Azure AD.
- Gérez vos comptes dans le portail Azure.

Demandes préalables

Pour commencer, vous devez effectuer les opérations suivantes :

- Un abonnement Azure AD. Si vous n'avez pas d'abonnement, vous pouvez obtenir un compte gratuit.
- Une ServiceNow authentification unique (SSO) est activée.
- Une ServiceNow instance ou un locataire qui prend en charge les ServiceNow versions San Diego ou ultérieures.
- Un ServiceNow locataire doit avoir activé le module d'extension d'authentification unique de plusieurs fournisseurs.
- Pour la configuration automatique, activez le module d'extension multifournisseur pour ServiceNow.

Ensemble d'actions pour la configuration

Voici l'ensemble des actions à effectuer pour configurer Azure AD :

- Ajoutez ServiceNow à partir de la galerie à Azure AD.
- Configurer l'authentification unique Azure AD
- Créer un utilisateur test Azure AD
- Affecter l'utilisateur test Azure AD
- Configurer ServiceNow

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajouter ServiceNow à partir de la galerie

Ajoutez ServiceNow à partir de la galerie à votre liste d'applications SaaS gérées sur Azure AD.

Avant de commencer

Rôle requis : admin Azure

Procédure

1. Connectez-vous au portail Azure à l'aide d'un compte Microsoft.
2. Sélectionnez le service **Azure Active Directory** dans le volet de gauche.
3. Accédez à la **Applications d'entreprise** > **Toutes les applications**.
4. Pour ajouter une nouvelle application, sélectionnez **Nouvelle** application.
5. Dans la section Ajouter à partir de la galerie, entrez ServiceNow dans la zone de recherche.
6. Sélectionnez ServiceNow dans le panneau des résultats, puis ajoutez l'application.
7. Patientez quelques secondes pendant que l'application est ajoutée à votre locataire.

Configurer l'authentification unique Azure AD

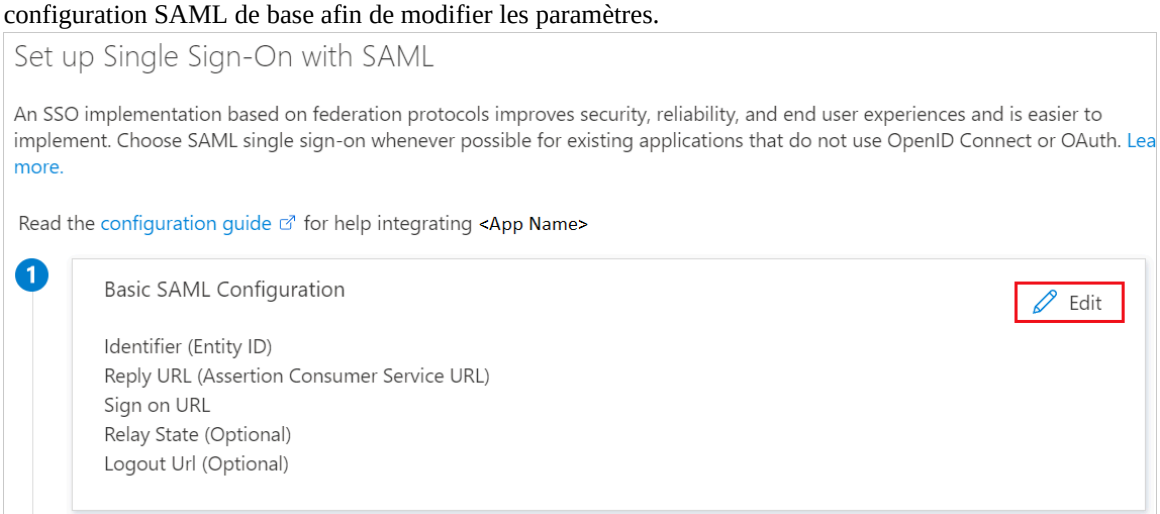
Configurez Azure AD SSO dans le portail Azure.

Avant de commencer

Rôle requis : admin Azure

Procédure

1. Sur le portail Azure, sur la page d'intégration d'application ServiceNow , recherchez la section Gérer.
2. Sélectionnez l'authentification unique.
   Sur la page Sélectionner une méthode d'authentification unique, sélectionnez SAML.
3. Sur la page Configurer l'authentification unique avec SAML, sélectionnez l'icône du stylo pour la configuration SAML de base afin de modifier les paramètres.



4. Dans la section Configuration SAML de base, procédez comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans URL de **connexion**, entrez l'un des modèles d'URL suivants :

```
https://<instancename>.service-now.com/navpage.do
https://<instance-name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id of the sso configuration>
```

Remarque :
Vous devez fournir l'sys_id dans cette URL.

b. Dans Identificateur (ID d'entité), entrez une URL avec le modèle : `https://<nom-instance>.service-now.com`.

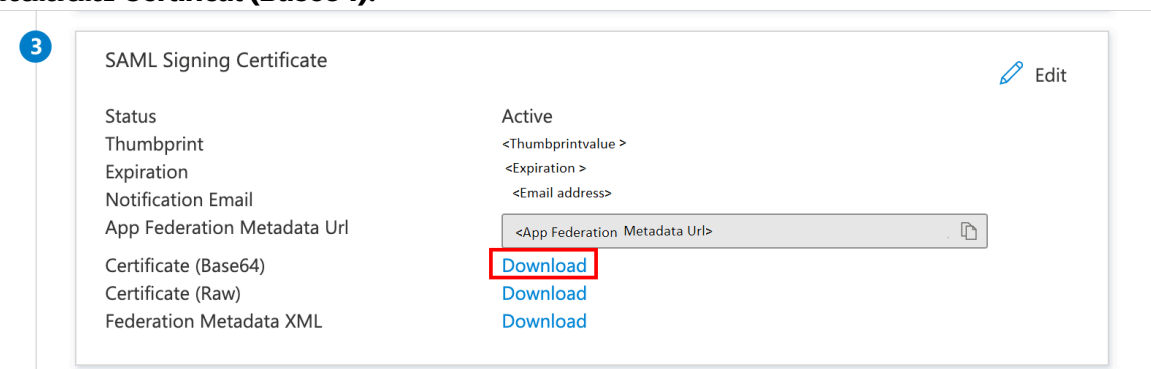
c. Pour **Reply URL (URL de réponse)**, entrez l'un des modèles d'URL suivants :

```
https://<instancename>.service-now.com/navpage.do
https://<instancename>.service-now.com/customer.do
```

d. Dans URL de déconnexion, saisissez une URL avec le modèle suivant : `https://<instancename>.service-now.com/navpage.do`

Remarque :
Vous devez mettre à jour l'URL d'ouverture de session, l'URL de réponse, l'URL de déconnexion et l'identificateur. les valeurs affichées dans ces URL sont à des fins de démonstration.

5. Sur la page Configurer l'authentification unique avec SAML, dans la section Certificat de signature SAML, recherchez **Certificat (Base64).**



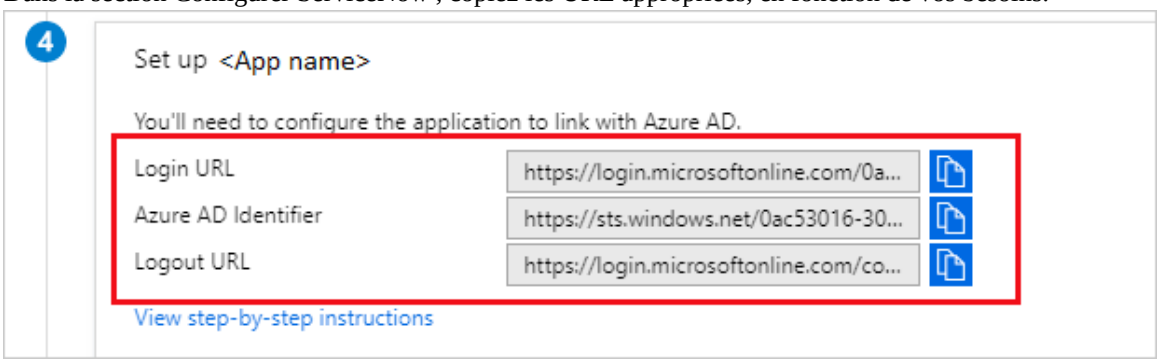
a. Sélectionnez le bouton Copier pour copier **l'URL des métadonnées de fédération d'applications** et collez-la dans le Bloc-notes.
Cette URL est requise pour une configuration ultérieure.

b. Sélectionnez **Télécharger** pour télécharger le certificat (Base64).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

6. Dans la section Configurer ServiceNow , copiez les URL appropriées, en fonction de vos besoins.



Créer un utilisateur test Azure AD

Créer un utilisateur test sur Azure AD.

Avant de commencer
Rôle requis : admin Azure

Procédure

1. Sur le portail Azure, accédez à **Tout** > **Azure Active Directory** > **Utilisateurs** > **Tous les utilisateurs**.
2. Sélectionnez **Nouvel utilisateur**.
3. Dans les propriétés de l'utilisateur, fournissez les informations suivantes :
   - Nom
   - Nom d'utilisateur
   - Mot de passe
4. Cliquez sur **Créer**.

Affecter l'utilisateur test Azure AD

Affectez l'utilisateur test Azure AD créé pour utiliser l'authentification unique Azure en accordant l'accès à ServiceNow.

Avant de commencer
Rôle requis : admin Azure

Procédure

1. Sur le portail Azure, accédez à **Tout** > **Applications d'entreprise** > **Toutes les applications**.
2. Dans la liste des applications, sélectionnez ServiceNow.
3. Sur la page de l'application, dans la section Gérer, sélectionnez **Utilisateurs et groupes**.
4. Sélectionnez **Ajouter un utilisateur**.
5. Dans la fenêtre **Ajouter une affectation** , sélectionnez **Utilisateurs et groupes**.
6. Dans la fenêtre **Utilisateurs et groupes** , sélectionnez l'utilisateur `test` créé dans la liste des utilisateurs.
7. Choisissez le rôle de l'utilisateur affecté dans la liste déroulante **Sélectionner un rôle** si nécessaire.
8. Dans la fenêtre **Ajouter une affectation** , sélectionnez **Affecter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer ServiceNow

Configurez ServiceNow avec les détails Azure AD pour utiliser SSO.

Avant de commencer

Module d'extension : intégration : programme d'installation de l'authentification unique de plusieurs fournisseurs

Activez les propriétés SSO de plusieurs fournisseurs :

- Sélectionnez **Activer l'authentification unique (SSO) de plusieurs fournisseurs**.
- Sélectionnez **Activer l'importation automatique des utilisateurs de tous les fournisseurs d'identité dans la table utilisateur**.
- Sélectionnez **Activer la journalisation du débogage pour l'intégration de l'authentification unique (SSO) de plusieurs fournisseurs**.
- Entrez **l'adresse e-mail**, le champ de la table utilisateur qui .....

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Sur la page Fournisseurs d'identité, sélectionnez **Nouveau**.
3. Dans la fenêtre Fournisseurs d'identité, sélectionnez **SAML.**
4. Sur l'importation des métadonnées du fournisseur d'identité, vous pouvez soit :
   - **URL** : URL des métadonnées de fédération d'applications pour renseigner automatiquement les détails sur la page de configuration du fournisseur d'identité.
   - **Importer** : importez le XML pour importer les détails sur la page de configuration du fournisseur d'identité.
5. Cliquez avec le bouton droit de la souris en haut de l'écran, cliquez sur **Copier sys_id** et utilisez cette valeur dans **l'URL de connexion** dans la section **Configuration SAML de base** .
6. Renseignez les champs du formulaire.

Champs d'authentification unique de plusieurs fournisseurs

Propriété	Obligatoire	Description
Nom	Oui	Nom de l'IdP. Cet IdP est l'ID système de redirection automatique.
Actif	Oui	Actif doit être défini sur vrai pour que l'IdP soit utilisé pour l'authentification. **Remarque :** L'option permettant de définir cette propriété n'est disponible qu'après une connexion de test réussie.
Par défaut	Non	L'IdP de redirection automatique, anciennement connu sous le nom d'IdP principal, redirige automatiquement les utilisateurs pour accéder à l'URL de l'instance de base. Cette propriété définit cette configuration IdP comme configuration par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

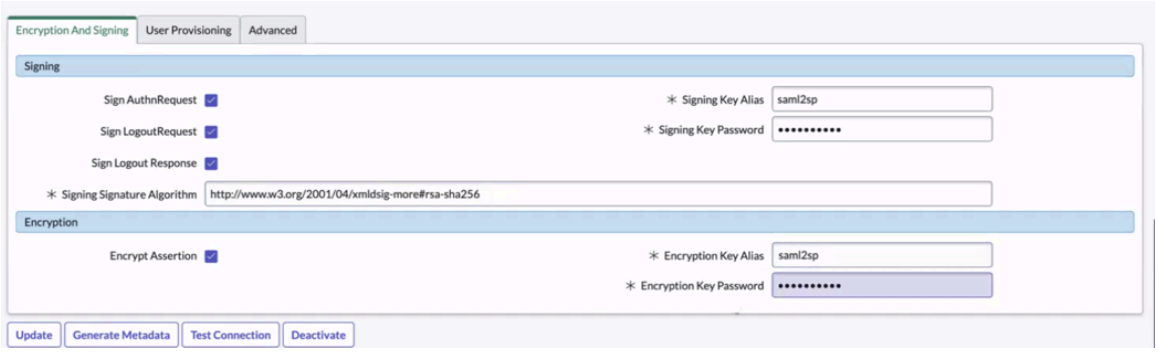
Propriété	Obligatoire	Description
Rediriger automatiquement l'IdP	Non	Configuration IdP que vous pouvez définir comme IdP de redirection automatique. **Remarque :** Si vous activez une nouvelle configuration d'IdP de redirection automatique, le `glide_sso_id` cookie est mis à jour avec le nouvel IdP de redirection automatique. La `glide.authenticate.sso.update.idp.cookie` propriété système, activée automatiquement, contrôle cette fonctionnalité.
URL du fournisseur d'identité	Oui	URL vers votre fournisseur d'identité. Chaque URL IdP doit être unique.
Service AuthnRequest du fournisseur d'identité	Oui	URL de liaison HTTP-Redirect obtenue à partir de l'élément SingleSignOnService.
Service SingleLogoutRequest du fournisseur d'ident	Non	URL obtenue à partir de l'élément SingleLogoutService.
ServiceNow Page d'accueil	Oui	URL de l'instance pour laquelle l'IdP s'authentifie, y compris la page de connexion. Par exemple : https://yourinstance.service-now.com/navpage.do
ID d'entité/Émetteur	Oui	URL de base, à l'exclusion de la page de connexion de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
URI de l'audience	Oui	URL de base, à l'exclusion de la page de connexion de l'instance pour laquelle l'IdP s'authentifie. Par exemple : https://yourinstance.service-now.com/
Politique NameID	Oui	Valeur de l'élément NameIDFormat que l'intégration utilise.
Redirection de déconnexion externe	Non	URL vers laquelle l'intégration redirige les utilisateurs après leur déconnexion.
Échec de la redirection du besoin	Non	URL de redirection des demandes d'authentification ayant échoué. Par défaut, il s'agit du point de terminaison d'URL d'une page d'erreur ou d'une page de déconnexion configurée dans l'IdP. Vous pouvez renseigner cette valeur dans le champ glide.authenticate.failed_requirement_redirect.

7. **Facultatif :** Onglet Chiffrement et signature

Remarque :
Utilisez vos propres certificats pour le chiffrement et la signature.

Traduction automatique

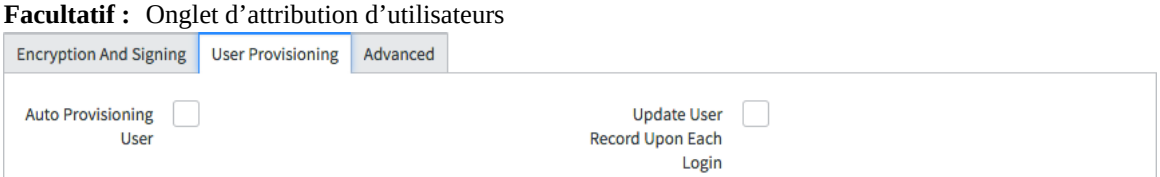
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champs de chiffrement et de signature

Propriété	Description
Alias de la Clé de signature/Clé de chiffrement	Alias de l'entrée de clé stocké dans le magasin de clés SAML 2.0 SP.
Signature avec le mot de passe de clé	Mot de passe de l'entrée de clé stocké dans le magasin de clés SAML 2.0 SP.
Chiffrer l'assertion	Case à cocher pour chiffrer l'assertion dans la réponse SAML. Les métadonnées générées pour l'IDP incorporent le certificat x509, que l'IDP utilise pour chiffrer l'assertion dans la réponse SAML qu'il génère.
Algorithme de signature pour la signature	URL qui pointe vers le consommateur AuthnRequest du fournisseur d'identité SAML 2.0 pour l'authentification de signature électronique.
Signer l'AuthnRequest	Case à cocher permettant au service d'authentification unique IdP de recevoir une demande AuthnRequest signée.
Signer la LogoutRequest	Case à cocher permettant au service d'authentification unique IdP de recevoir une LogoutRequest signée.

8. **Facultatif :** Onglet d'attribution d'utilisateurs



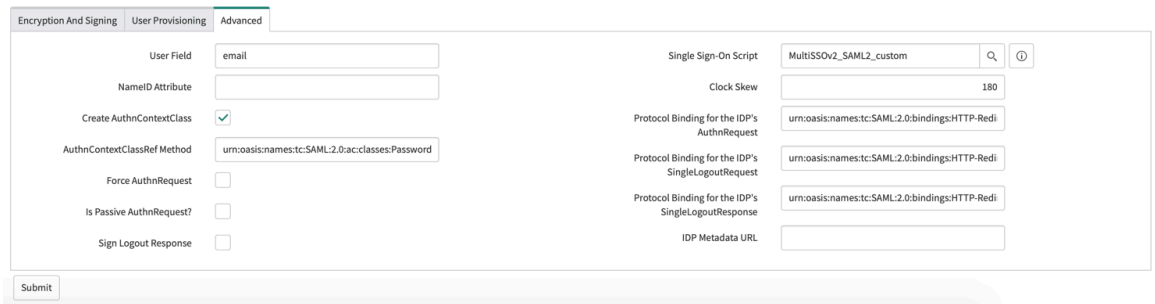
Champs d'attribution d'utilisateurs

Propriété	Description
Mise en service automatique de l'utilisateur	L'attribution automatique d'utilisateurs crée les utilisateurs lorsque l'utilisateur n'existe pas dans la table Utilisateur de l'instance en fonction des informations fournies par l'IdP.
Mettre à jour l'enregistrement utilisateur à chaque connexion	Mettez à jour les informations de l'utilisateur dans la table Utilisateur de l'instance avec les informations dans l'IdP chaque fois que l'utilisateur se connecte à l'aide de SAML.

9. **Facultatif :** Onglet Avancé

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champs avancés

Propriété	Description
Champ d'utilisateur	Champ de la table Utilisateur qui contient la valeur requise par l'IdP pour identifier l'utilisateur. Cet ID unique fait partie de la réponse. Par exemple, un nom d'utilisateur, un ID d'employé, etc. Dans la table utilisateur système, cet ID unique correspond aux détails de l'utilisateur.
Attribut NameID	Champ que vous laissez vide à moins de configurer une nouvelle stratégie NameID. Si vous configurez une nouvelle politique, le système requiert la table Utilisateur qu'il doit utiliser pour identifier l'utilisateur qui se connecte. Le système fait correspondre le jeton NameID au nom du champ de la table Utilisateur.
Créer une AuthnContextClass	Cochez la case pour spécifier une classe de contexte particulière, telle que Transport protégé par mot de passe. Si la case est décochée, l'IdP sélectionne la classe de contexte la plus appropriée.
Méthode AuthnContextClassRef	URN du mécanisme de connexion que vous souhaitez que l'IdP utilise pour authentifier les utilisateurs.
Forcer l'AuthnRequest	Case à cocher pour forcer l'exécution des AuthnRequests.
Est une AuthnRequest passive	Case à cocher si l'AuthnRequest est passive.
Script d'authentification unique	Script d'authentification unique. La valeur par défaut est *MultiSSOV2_SAML2_custom*.
Signer la réponse de déconnexion	Déconnectez-vous des détails de réponse dans ce champ.
Décalage d'horloge	NNombre de secondes entre les deux attributs qui composent la nonce de réponse SAMLResponse. La valeur par défaut est 60. Une réponse SAML valide doit se situer entre les valeurs de date/heure *notBefore* et *notOnOrAfter* . Consultez Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData et Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience pour un exemple de message SAMLResponse.
Protocole de liaison du service SingleLogoutReuqest de l'IDP	L'une des valeurs prises en charge répertoriées dans l'attribut Binding de l'élément SingleLogoutService.
URL des métadonnées à partir de laquelle les propriétés IDP sont importées	Les propriétés IdP sont importées à partir de cette URL. Si défini, il active l'importation automatique du certificat SAML à partir de l'IdP si le certificat précédent a expiré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	Remarque : Si vous effectuez une mise à niveau de la mise à jour 1 de SAML2 vers la SSO de plusieurs fournisseurs ou si vous configurez manuellement votre connexion SSO, l'URL des métadonnées IdP ne s'affiche pas automatiquement.
Demande	ID unique dans le cadre de la demande. Il peut s'agir d'un nom d'utilisateur, d'un ID d'employé, etc. **Remarque :** La redirection et la liaison postérieure sont prises en charge pour la demande. L'option permettant de définir ce champ n'apparaît qu'après une connexion de test réussie. Pour plus d'informations, consultez Test des connexions IdP.
Réponse	ID unique dans le cadre de la réponse. Il peut s'agir d'un nom d'utilisateur, d'un ID d'employé, etc. **Remarque :** La redirection et la liaison postérieure sont prises en charge pour la réponse. L'option permettant de définir ce champ n'apparaît qu'après une connexion de test réussie. Pour plus d'informations, consultez Test des connexions IdP.

10. Sélectionnez **Test** de la connexion dans le coin supérieur droit de la page.
11. Entrez vos informations d'identification.
    Les résultats des tests de déconnexion de l'authentification unique s'affichent.
12. Sélectionnez **Activer** pour activer la configuration.

Liens d'e-mail avec authentification externe

Vous pouvez utiliser des liens d'e-mail lors de l'utilisation de l'authentification externe du jeton digestif, cependant, vous devez établir comment gérer les liens dans les notifications par e-mail.

Les liens par défaut contiennent une URL qui vous dirige vers un emplacement spécifique de l'instance, comme un incident ou une demande de changement, sans intégrer d'informations d'identification SSO. Vous trouverez ci-dessous des exemples permettant de diriger l'utilisateur vers l'emplacement dans l'instance sans se connecter à la page de connexion à l'instance.

- Technique HTTP non chiffrée pour se connecter à l'instance /demo (elle n'accède pas à un enregistrement spécifique) :

```
https://<instance
 name>.service-now.com/?
SM_USER=user_name&DE_USER=lQjIVp7aRJtyPx5+2O/vgU24tbE=
```

- Lien (dans une notification par e-mail) vers un enregistrement spécifique, afin que l'utilisateur accède d'abord au portail de connexion de l'entreprise :

```
https://login.company_portal_page.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2
b01ab4eb094223466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous devez définir la `glide.email.override.url` propriété dans votre instance pour contenir l'URL de la page du portail d'entreprise. Si cette propriété n'existe pas, vous pouvez la créer.

- Le portail d'entreprise doit ensuite prendre cette URL et construire l'URL de redirection vers l'instance en préservant le segment nécessaire pour accéder à l'enregistrement spécifique et en ajoutant les informations d'identification SSO à la fin de l'URL :

```
https://<instance
 name>.service-now.com/nav_to.do?uri=incident.do?sys_id=009f8eda0a0a0b2b01ab4eb0942
23466%26sysparm_stack=incident_list.do%3Fsysparm_query=active=true&SM_USER=user_
name&DE_USER=lQjlVp7aRJtyPx5+2O/vgU24tbE=
```

Ajouter la prise en charge des signatures électroniques pour SAML

Configurez les propriétés suivantes pour Signature électronique avec la mise à jour 1 du langage de balisage d'assertion de sécurité (SAML) 2.0.

Lorsque la signature électronique est active avec l'authentification unique (SSO) multiple, les propriétés SAML ne sont pas utilisées. Le système ajoute des propriétés de signature électronique à la table Propriétés SAML2 Update1 [saml2_update1_properties] :

Propriété	Description	Par défaut
Index de consommateur d'assertion pour l'authentification de signature électronique	Numéro d'index qui identifie le point de terminaison.	1
URL de consommateur d'assertion pour l'authentification de signature électronique	URL qui identifie le consommateur.	`https://yourinstance.service-now.com/consumer.do`
URL AuthnRequest pour l'authentification de signature électronique	URL pour authentification	aucun

Si vous utilisez la signature électronique avec SAML 1.0 ou SAML 2.0 (à l'exception de la mise à jour 1), consultez les instructions de configuration spéciales : Signature électronique pour l'authentification unique (SSO) de plusieurs fournisseurs.

Remarque :
Si vous êtes un client du secteur des sciences de la vie et que vous utilisez la signature électronique, désactivez la règle métier Prévention du verrouillage automatique de l'utilisateur.

Migration d'une intégration SAML 1.1 existante vers SAML 2.0

Pour migrer d'une intégration SAML 1.1 vers une intégration SAML 2.0, contactez le support client.

Mettre à jour votre intégration SAML 2.0 existante

Mettez à jour votre intégration SAML 2.0 existante.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Demandez le module d'extension SAML 2.0 Update 1. Contact Service et assistance client pour demander le module d'extension *SAML 2.0 Single Sign-On - Update 1 : Security enhancements* .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le module d'extension applique les versions mises à jour de la sortie d'installation *SAML2SingleSignon* (script de connexion), de la sortie d'installation *SAML2Logout* (script de déconnexion) et de l'include de script *SAML2* (objet de script).

Fusionnez les personnalisations à partir de scripts de sortie d'installation existants dans de nouveaux scripts. La mise à jour enregistre une copie inactive des scripts de sortie de l'installation d'origine de l'intégration. Vous pouvez utiliser ces copies pour fusionner les personnalisations que vous avez apportées aux scripts de connexion et de déconnexion aux nouvelles versions de ces sorties d'installation.

Fusionner les personnalisations à partir de scripts de sortie d'installation existants dans de nouveaux scripts

Nom du script de sortie de l'installation d'origine	État du script d'origine	Nom du script de sortie de la nouvelle installation	État du nouveau script
SAML2SingleSignon	Inactif	SAML2SingleSignon_update1	Actif
SAML2	Inactif	SAML2_update1	Actif
SAML2Déconnexion	Inactif	SAML2Logout_update1	Actif

Vous pouvez accéder aux scripts de connexion et de déconnexion de l'installation SAML 2.0 à l'aide des chemins suivants :

- **Authentification unique SAML 2** > **Script de connexion**.
- **Authentification unique SAML 2** > **Script de déconnexion**.
- **Définition du système** > **Sorties d'installation**.

Vous pouvez accéder à l'include de script SAML 2.0 mise à jour 1 à l'aide des chemins suivants :

- **Authentification unique SAML 2** > **Objet de script**.
- **Définition du système** > **Includes de script**.

Testez la mise à jour.

Procédure

1. Ajoutez une propriété système appelée `glide.authenticate.sso.saml2.debug` avec la valeur *vrai*.
2. Essayez de vous connecter à SAML 2.0.
3. Examinez le journal système.
   Les erreurs de validation SAML2 commencent par le texte *SAML2ValidationError*.
4. Identifiez et corrigez les erreurs de connexion typiques.
   Pour plus d'informations, consultez Erreurs et correctifs de l'authentification unique (SAML 2.0).

Exemple de réponses SAML 2 après la mise à jour

Les sections suivantes illustrent les nouveaux éléments et attributs requis que le fournisseur d'identité doit fournir dans la réponse SAML.

Exemple de réponse SAML 2 avec élément de l'émetteur

La réponse SAML 2 suivante utilise l'élément *Émetteur* .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
<samlp:Responsexmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 Destination="https://demoi2.service-now.com/navpage.do"
 ID="s28da6774c88ae1eab292bf25fe625db81919d8e1e"
InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
IssueInstant="2012-01-30T20:07:10Z"  Version="2.0"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://idp.ssocircle.com</saml:Issuer>
  ...
  <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="s2f347f973c063836cf70ea38302d94976f9c5b851"
IssueInstant="2012-01-30T20:07:10Z"
Version="2.0"><saml:Issuer>http://idp.ssocircle.com</saml:Issuer>
     ...
  </saml:Assertion></samlp:Response>
```

Exemple de réponse SAML 2 avec les éléments SubjectConfirmation et SubjectConfirmationData

La réponse SAML 2 suivante utilise les éléments *SubjectConfirmation* et *SubjectConfirmationData* avec les attributs *NotOnOrAfter* et *Recipient* .

```
<saml:SubjectConfirmationMethod="urn:oasis:names:tc:SAML:2.0:cm:bearer"><saml:Subject
ConfirmationData InResponseTo="SNC841720c227c81948cfd68cadcad235c6"
 NotOnOrAfter="2012-01-30T20:17:10Z"
 Recipient="https://demoi2.service-now.com/navpage.do"/></saml:SubjectConfirmation>
```

Exemple de réponse SAML 2 avec les éléments AudienceRestrictions et Audience

La réponse SAML 2 suivante utilise les éléments *AudienceRestrictions* et *Audience* avec les attributs *NotBefore* et *NotOnOrAfter* .

```
<saml:ConditionsNotBefore="2012-01-30T19:57:10Z"
 NotOnOrAfter="2012-01-30T20:17:10Z"><saml:AudienceRestriction><saml:Audience>http
s://
demoi2.service-now.com</saml:Audience></saml:AudienceRestriction></saml:Conditions>
```

Attribution d'utilisateurs SAML

Si des utilisateurs existent dans votre IdP, mais ne se trouvent pas dans votre instance, l'attribution d'utilisateurs SAML peut créer automatiquement les utilisateurs dans la table Utilisateur [sys_user] de votre instance.

L'attribution d'utilisateurs SAML est prise en charge pour SAML 2.0 Update 1 lorsque l'authentification unique (SSO) à fournisseurs multiples est activée.

Fonctionnement de l'attribution d'utilisateurs SAML

Lorsque l'attribution d'utilisateurs SAML est activée et que le système rencontre un nouvel utilisateur qui n'est pas dans l'instance, l'instance crée automatiquement un enregistrement dans une table temporaire avec le nom `u_imp_saml_user_<suffixe>`, où `<suffix>` est un identificateur de texte généré automatiquement. Le système crée également une carte de transformation qui spécifie les relations de données entre la table d'importation et la table d'utilisateur. Chaque IdP identifié dans le système possède sa propre carte de transformation. La carte de transformation est créée une fois pour chaque IdP. Les administrateurs peuvent le mettre à jour si nécessaire.

Lorsque l'utilisateur se connecte, il accède à un IdP pour se connecter.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Le système présente une liste de tous les IdP qui sont en mesure d'utiliser l'attribution d'utilisateurs SAML. S'il n'y a qu'un seul IdP qui peut utiliser l'attribution d'utilisateurs SAML, celui-ci est utilisé automatiquement.
- Si aucune des conditions ci-dessus n'est vraie, le système utilise l'IdP de redirection automatique.

Administrer la mise en service d'utilisateurs SAML

Mettez à jour la table Utilisateur avec les utilisateurs de votre IdP en configurant d'abord le mappage de champs, puis en activant l'attribution d'utilisateurs via les paramètres IdP à SSO multiple.

Avant de commencer

Configurez votre mappage IdP pour identifier les champs dans l'IdP qui sont mappés aux champs corrects dans la table Utilisateur.

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Propriétés**.
2. Sélectionnez **Activer l'importation automatique d'utilisateurs à partir de tous les fournisseurs d'identité dans la table des utilisateurs** (`glide.authenticate.multisso.user.autoprovision`) pour activer cette fonctionnalité.
3. Cliquez sur **Enregistrer**.
4. Accédez à la **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
5. Ouvrez l'enregistrement du fournisseur d'identité que vous souhaitez utiliser.
6. Créez un enregistrement dans la table Utilisateur lorsque l'utilisateur n'existe pas déjà en sélectionnant **Utilisateurs mis en service automatiquement**.
   Si vous effectuez une mise à niveau vers cette version, vous devez configurer le formulaire et ajouter ce champ.
7. Activez la mise à jour des enregistrements utilisateur lorsque les utilisateurs se connectent à l'IdP et que les informations sur l'IdP ne sont pas à jour par rapport aux informations de la table Utilisateur en sélectionnant **Mettre à jour l'enregistrement utilisateur à chaque connexion**.
   Si vous effectuez une mise à niveau vers cette version, vous devez configurer le formulaire et ajouter ce champ.
8. Cliquez sur **la carte de transformation de l'attribution d'utilisateurs** pour afficher la carte créée automatiquement par le système.
9. Apportez des modifications à la carte si nécessaire.

Résultats

Lorsque les premiers utilisateurs inconnus tentent de se connecter, le système crée les champs dans la table de jeux d'importation à partir du fichier metadata.xml.

Remarque :
Vous ne pouvez pas mapper les champs à partir de la table IdP tant que le premier utilisateur n'est pas connecté.

Dépannage SAML 2.0

Avant de contacter l'assistance, essayez les solutions de dépannage disponibles dans la base de connaissances sur Hi.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
L'instance ne prend pas en charge les solutions fournies par les sites externes.

Consultez l'article suivant de la base de connaissances : KB0540617 "'Matrice d'erreurs SAML" '.

Autres problèmes courants

Erreur ou symptôme	Solution
Message d'erreur : « n'est pas une fonction ». Ce problème peut se produire dans un environnement à plusieurs nœuds. Si le module d'extension n'est pas activé sur tous les nœuds, une erreur semblable à la suivante s'affiche : org.mozilla.javascript.EcmaError : `[JavaPackage org.opensaml.saml2.core.impl.AuthnRequestBuilder]` n'est pas une fonction.	Cette erreur se produit car le module d'extension n'était pas actif et n'a pas chargé le fichier .jar. Par conséquent, le code semble manquant. Contactez le support technique pour redémarrer les nœuds qui n'ont pas le module d'extension.
SAML n'authentifie pas les utilisateurs accédant aux pages CMS.	Par défaut, les pages CMS sont publiques et ne nécessitent donc pas d'authentification. Si vous souhaitez que le SAML authentifie les pages CMS, modifiez la page publique *view_content.dode active=true* à *active=false*.
Impossible de rediriger un utilisateur vers une page CMS après l'authentification SAML.	Par défaut, l'intégration SSO utilise un paramètre d'URL appelé *URI* pour contrôler où l'utilisateur est dirigé après son authentification auprès de l'IdP. SSO ignore les URL relatives. Par exemple, SSO ne peut pas rediriger les utilisateurs vers une URL relative */ess* . Au lieu de cela, l'utilisateur doit naviguer vers une URL telle que */nav_to.do ?uri=/ess*, qui utilise une syntaxe de liens profonds. Toutefois, cela place le portail ESS à l'intérieur de l'IFrame de contenu de navigation principal. En d'autres termes, le site n'occupe pas la page complète, mais se charge en tant que page dans votre instance. Pour plus d'informations, consultez Sites CMS et Authentification unique. Si vous modifiez la page d'entrée CMS pour la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Autres problèmes courants (suite)

Erreur ou symptôme	Solution
	rendre privée en définissant *view_content.do* sur *active=false*, le comportement du lien profond nécessite alors une personnalisation du script de connexion à *la sortie de l'installation* . Créez un script qui recherche la partie *URI* de l'URL et construit un paramètre d'URL *RelayState* contenant le chemin d'accès de l'URL relative pour rediriger les utilisateurs après s'être authentifiés auprès de l'IdP.
SAML ne redirige pas les utilisateurs vers la page appropriée après authentification.	Déterminez si l'état du relais est transmis à l'IdP, puis renvoyé pendant l'authentification. Vous pouvez le faire avec un navigateur capable d'enregistrer les en-têtes de requête HTTP et les informations POST, comme Chrome avec ses outils de développement intégrés, ou Firefox avec le module complémentaire appelé HTTPfox. Pour Internet Explorer, utilisez une application tierce telle que Fiddler. L'objectif est de voir les requêtes passer du client (navigateur) à l'instance, et du client à l'IdP.

Traduction automatique

Surveiller la file d'attente de l'événement pour les activités de connexion

Chaque intégration d'authentification crée des événements pour les activités de connexion.

Vous pouvez utiliser ces événements pour surveiller les échecs de connexion et déterminer s'il existe des problèmes de sécurité à résoudre.

Surveillance de la file d'attente d'événement pour les échecs de connexion

Nom d'événement	Description	Enregistrement	Paramètre 1	Paramètre 2
`external.authentication.succeeded`	L'authentification externe a réussi et l'utilisateur a accédé à l'URL de l'instance.	ID de session	ID utilisateur de l'utilisateur qui s'est connecté avec succès	L'URL à laquelle l'utilisateur a accédé (qui peut être un lien profond)

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Surveillance de la file d'attente d'événement pour les échecs de connexion (suite)

Nom d'événement	Description	Enregistrement	Paramètre 1	Paramètre 2
external.authentication.failed	Les exigences relatives à l'authentification unique ne sont pas présentes ou sont absentes.		ID de session	Exigences d'authentification manquantes
external.authentication.failed	L'utilisateur n'existe pas dans la table Utilisateur [sys_user]		ID d'utilisateur	La chaîne « L'utilisateur n'existe pas »
external.authentication.failed	L'utilisateur est verrouillé.		ID d'utilisateur	La chaîne « L'utilisateur verrouillé ».

Événements de connexion à la file d'attente de l'événement

L'intégration SAML 2.0 crée des événements pour les activités de connexion.

Vous pouvez utiliser ces événements pour surveiller les échecs de connexion et déterminer s'il existe des problèmes de sécurité à résoudre.

Se connecter aux événements d'activités

Nom d'événement	Description	ID utilisé avec l'événement	Chaîne d'événement
saml2.logout.validation.failed	Échec de la validation de la réponse de déconnexion de l'IdP par rapport à votre demande de déconnexion. L'événement valide l'élément <inResponseTo> par rapport à l'ID de session (attribut ID de l'élément <saml2p :LogoutRequest>). Par exemple, consultez le workflow pour la demande de déconnexion émise.	ID de session	La chaîne « SAML2 LogoutResponse validation failed » (échec de la validation de la réponse de connexion SAML2).
authentification.externe.réussie	Authentification externe réussie.		La chaîne « Authentification réussie »
authentification.externe.réussie	L'authentification externe a réussi et l'utilisateur a accédé à l'URL de l'instance.	ID de session et ID d'utilisateur de l'utilisateur qui s'est connecté avec succès	L'URL à laquelle l'utilisateur a accédé (qui peut être un lien profond)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Se connecter aux événements d'activités (suite)

Nom d'événement	Description	ID utilisé avec l'événement	Chaîne d'événement
external.authentication.failed	Les exigences relatives à l'authentification unique ne sont pas présentes ou sont absentes.	ID de session	Exigences d'authentification manquantes
external.authentication.failed	L'utilisateur n'existe pas dans la table Utilisateur [sys_user].	ID d'utilisateur	La chaîne « L'utilisateur n'existe pas »
external.authentication.failed	L'utilisateur est verrouillé.	ID d'utilisateur	La chaîne « Utilisateur verrouillé »

Authentification entrante et sortante OAuth

L'authentification basée sur OAuth valide l'identité du client qui tente d'établir une confiance dans le système à l'aide d'un protocole d'authentification.

OAuth 2.0 - Open Authorization est le protocole standard de l'industrie pour l'autorisation, qui utilise la simplicité des développeurs clients tout en fournissant des flux d'autorisation spécifiques pour les applications Web, les applications de bureau et les équipements mobiles.

Il s'agit d'une norme conçue pour permettre à un site Web ou à une application d'accéder aux ressources hébergées par d'autres applications Web au nom d'un utilisateur.

Au lieu d'utiliser les informations d'identification de l'utilisateur de la ressource pour accéder aux ressources protégées, le client obtient un jeton d'accès. Les jetons d'accès sont émis aux clients tiers avec l'approbation de l'utilisateur, qui utilise ensuite le jeton d'accès pour accéder aux ressources protégées.

Entrant

Créez un point de terminaison pour les clients externes qui veulent accéder à votre instance. Cela crée un enregistrement d'application cliente OAuth et génère un ID client et un secret client indiquant que le client a besoin pour accéder aux ressources restreintes sur l'instance. Pour plus d'informations, reportez-vous à la section OAuth entrant.

Sortant

Utilisez un fournisseur OAuth tiers qui vous donne l'autorisation d'accéder à votre instance. Spécifiez un profil OAuth et un champ d'application OAuth lorsque vous vous connectez à un autre fournisseur OAuth. Pour plus d'informations, reportez-vous à la section OAuth sortant.

OAuth 2.0

OAuth 2.0 permet aux utilisateurs d'accéder aux ressources de l'instance via des clients externes en obtenant un jeton plutôt qu'en saisissant des informations d'identification de connexion avec chaque demande de ressource.

Vous devez disposer du rôle security_admin pour gérer l'intégration OAuth. Configurez OAuth 2.0 pour les scénarios suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Scénario de client externe OAuth** (entrant) : votre instance fournit un point de terminaison permettant aux clients tiers d'extraire les données de l'instance.
- **Scénario du fournisseur OAuth** (sortant) : votre instance extrait les données d'un fournisseur tiers.

Remarque :
Vous devez authentifier l'utilisateur pour la première fois pour récupérer la publication du jeton, que vous n'avez pas besoin d'authentifier à l'aide d'un compte utilisateur avant l'expiration du jeton.

Les frameworks de sécurité simple et de haute sécurité prennent tous deux en charge OAuth 2.0. Une sécurité élevée est recommandée. Reportez-vous à la section pour plus d'informations sur les versions pour lesquelles la sécurité élevée est déjà active et sur la façon d'activer la sécurité élevée.

Concepts clés de l'implémentation d'OAuth 2.0

Concept	Description
Propriétaire de ressource	Entité capable d'accorder l'accès à une ressource protégée. Un propriétaire de ressource qui est une personne est appelé *un utilisateur final*. Le propriétaire de la ressource est toujours un compte utilisateur.
Client	Application qui, avec l'autorisation du propriétaire de la ressource, effectue des demandes de ressources protégées au nom du propriétaire de la ressource.
Serveur de ressources	Serveur qui héberge les ressources protégées, capable d'accepter et de répondre aux demandes de ressources protégées.
Serveur d'autorisation	Serveur qui émet des jetons d'accès au client après avoir authentifié le propriétaire de la ressource et obtenu l'autorisation.
Demande d'autorisation	Autorisation requise par un client pour accéder à une ressource protégée. La demande d'autorisation est toujours un message HTTP POST qui contient l'ID du client qui agit au nom du propriétaire de la ressource et les informations d'identification qui autorisent la demande.
Octroi d'autorisation	Informations d'identification qui représentent l'autorisation du propriétaire de ressource d'accéder à une ressource. L'autorisation accordée est soit les informations d'identification de connexion de l'utilisateur, soit un jeton d'actualisation.
Jeton d'accès	Chaîne sécurisée qu'un client utilise pour accéder aux ressources protégées. Une instance émet des jetons d'accès aux clients disposant d'une autorisation valide. Chaque jeton d'accès a un périmètre, une durée de vie et d'autres attributs spécifiques. Par défaut, une instance émet des jetons d'accès d'une durée de vie de 30 minutes dans le scénario où l'instance est le fournisseur OAuth. Pour les jetons tiers, 30 jours.
Actualiser le jeton	Informations d'identification qu'un client utilise pour obtenir de nouveaux jetons d'accès sans nécessiter d'autorisation utilisateur supplémentaire. Une instance émet un jeton d'actualisation à un client lorsqu'il est autorisé pour la première fois à disposer d'un jeton d'accès. Par défaut, une instance émet des jetons d'actualisation d'une durée de vie de 100 jours dans le cas où l'instance est le fournisseur OAuth. Pour les jetons tiers, 365 jours.
Certificats auto-signés	Le Now Platform ne prend pas en charge les certificats autosignés. Le client OAuth n'utilise pas le magasin de certificats de confiance et n'autorise pas la connexion aux points de terminaison OAuth qui intègrent un certificat auto-signé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Concept	Description
Agent utilisateur	L'utilisateur qui délègue des droits d'accès à une application cliente, qui est souvent un site web. Les droits d'accès permettent à l'application cliente ou au site web d'accéder aux données dans l'instance à laquelle l'utilisateur a des droits d'accès. L'agent utilisateur est utilisé dans le scénario.

Types d'accords OAuth

Un *type d'attribution* est la façon dont le client obtient le jeton d'accès. Les types de subventions suivants sont pris en charge :

- **Code d'autorisation** : le consommateur obtient d'abord un code d'autorisation, puis l'utilise pour obtenir un jeton d'accès. Vous pouvez spécifier un profil OAuth et spécifier ce type d'accord. Le processus qui utilise le code d'autorisation est également appelé *flux de code d'authentification* ou *flux de code d'autorisation*.
- **Informations d'identification du mot de passe du propriétaire** de la ressource : le consommateur de la ressource possède déjà les informations d'identification de l'utilisateur pour obtenir le jeton d'accès. Ce processus est également appelé *flux de mots de passe*.
- **Informations d'identification du client** : le consommateur de la ressource utilise l'ID client et le secret client qui sont déjà configurés dans le registre d'application.

Stockage des identifiants d'authentification

Le secret client OAuth est stocké en tant que `password2` champ type, qui est chiffré avec KMF. Les mots de passe utilisateur, qui sont utilisés pour vérifier les demandes de points de terminaison entrantes, sont stockés sous forme de valeur de hachage dans la table Utilisateur dans un `password` champ de type (SHA 256). Pour plus d'informations sur ce chiffrement, consultez Chiffrement Password2 avec KMF

Configurer OAuth

Configurez et activez OAuth, activez la propriété système OAuth, créez un point de terminaison d'application OAuth pour que les applications clientes externes accèdent à l'instance et définissez les paramètres OAuth.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Assurez-vous que le module d'extension OAuth est actif et que la propriété d'activation OAuth est définie sur true.
2. Créez un registre d'application OAuth à l'aide de l'une des méthodes suivantes :
   - Créez un point de terminaison pour les clients externes qui veulent accéder à votre instance. Cela crée un enregistrement **d'application cliente OAuth** et génère un ID client et un secret client indiquant que le client a besoin pour accéder aux ressources restreintes sur l'instance.
   - Utilisez un fournisseur OAuth tiers qui vous donne l'autorisation d'accéder à votre instance.

     Spécifiez un profil OAuth et spécifiez un champ d'application OAuth lorsque vous vous connectez à un autre fournisseur OAuth.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Configurez vos applications clientes pour créer un HTTP POST qui demande un jeton OAuth. L'application doit également être en mesure d'analyser la réponse JSON pour utiliser le jeton d'accès renvoyé et le jeton d'actualisation.

Activer OAuth

Par défaut, le module d'extension **OAuth 2.0 (com.snc.platform.security.oauth)** est actif sur les instances nouvelles et mises à niveau. Si le module d'extension n'est pas actif sur votre instance, vous pouvez l'activer.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée.

Définir la propriété OAuth

Pour générer des jetons OAuth 2.0 pour les applications enregistrées, la propriété `com.snc.platform.security.oauth.is.active` doit être active pour l'instance.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Pour utiliser OAuth 2.0, saisissez **sys_properties.list** dans le navigateur de filtre d'espace de travail et cliquez sur **Nouveau**.
2. Remplissez le formulaire avec les paramètres suivants :

   - **Nom** : com.snc.platform.security.oauth.is.active
   - **Type** : vrai | faux
   - **Valeur** : vrai

Changer le paramètre du mot de passe OAuth

Utilisez cette propriété pour vous assurer que seuls les paramètres de corps POST sont acceptés comme entrée pour tous les types d'accord pris en charge.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’envoi d’informations sensibles via les paramètres de requête URI peut entraîner la divulgation d’informations sensibles par les clients, le serveur ou tout hôte entre les demandes. À partir de la version Madrid, cette nouvelle propriété garantit que seuls les paramètres de corps POST sont acceptés comme entrée pour tous les types d’accord pris en charge. Les types de subventions pris en charge sont les suivants :

- Code d’autorisation
- mot de passe
- Informations d’identification du client
- Actualiser le jeton

Propriété du paramètre du mot de passe OAuth

Propriété	Description
glide.oauth.allow.parameters.in.post.body.only	Cette propriété est définie sur vrai pour zBoots uniquement, dans le cadre du module d’extension OAuth 2.0. Si vous avez besoin de ce paramètre pour votre instance, créez et définissez la propriété sur true.

OAuth entrant

OAuth entrant fournit un point de terminaison permettant aux clients tiers d’extraire les données de l’instance.

Vous devez disposer du rôle security_admin pour gérer l’intégration OAuth.

Vous pouvez configurer l’intégration du **scénario de client externe OAuth** (entrant) lorsque vous souhaitez que votre instance fournisse un point de terminaison permettant aux clients tiers d’extraire les données de l’instance.

Remarque :
Vous devez authentifier l’utilisateur pour la première fois pour récupérer la publication du jeton, que vous n’avez pas besoin d’authentifier à l’aide d’un compte utilisateur avant l’expiration du jeton.

Vous pouvez effectuer la configuration OAuth entrante en fonction du type d’attribution suivant :

- **Flux d’octroi de code d’autorisation** : pour un flux d’octroi initié par l’utilisateur, où l’utilisateur peut configurer une URL autorisée pour l’authentification sans avoir à saisir de nom d’utilisateur ou de mot de passe, mais via le jeton d’accès. Pour plus d'informations, consultez Flux d’octroi de code d’autorisation OAuth.
- **Flux d’octroi de mot de passe** : pour un flux d’octroi initié par l’utilisateur, où une interaction de l’utilisateur est requise pour l’authentification. Pour plus d’informations, consultez Configuration du flux d’octroi de mot de passe .

  Remarque :
  Pour le flux de code d’autorisation, l’utilisateur doit terminer l’authentification par connexion locale, SSO ou MFA, puis donner son consentement.

- **Flux d’attribution de porteur JWT** : pour une intégration de système à système, où une intervention de l’utilisateur n’est pas nécessaire. Pour plus d’informations, consultez Configuration du flux d’attribution au porteur JWT .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Flux de jetons d'ID** : pour l'utilisation d'un jeton d'ID émis par des fournisseurs OIDC tiers tels qu'Okta, Azure. Pour plus d'informations, consultez Flux de jetons d'ID pour l'authentification.
- **Subventions implicites OAuth** : pour permettre l'attribution directe du jeton d'accès à l'application cliente via l'agent utilisateur, qui est généralement le navigateur Web ou l'appareil mobile. Pour plus d'informations, consultez Subventions implicites OAuth.
- **Informations d'identification du client** : pour l'utilisation du type d'accord d'informations d'identification du client OAuth pour les intégrations entrantes d'un client OAuth tiers vers la ServiceNow® plateforme. Pour plus d'informations, consultez Informations d'identification du client.

Périmètres OAuth

Vous pouvez étendre la prise en charge du périmètre d'authentification OAuth pour l'API REST. Le champ d'application OAuth ne permet d'accéder qu'aux API REST particulières. Pour plus d'informations, consultez Périmètre d'authentification REST API.

Flux d'octroi de code d'autorisation OAuth

Le flux d'octroi de code d'autorisation permet à un utilisateur d'accéder à une ressource en s'authentifiant directement auprès d'un serveur OAuth qui fait confiance à la ressource, contrairement à l'authentification avec des informations d'identification de nom d'utilisateur/mot de passe.

Cette implémentation du flux de code d'autorisation OAuth permet d'accéder à une ressource via REST. Le cadre de travail du code d'autorisation obtient le jeton d'accès via l'URL autorisée que l'utilisateur configure plutôt que de demander à l'utilisateur de saisir un nom d'utilisateur/mot de passe. Le nom d'utilisateur et le mot de passe ne sont jamais exposés au client qui demande l'accès à la ressource.

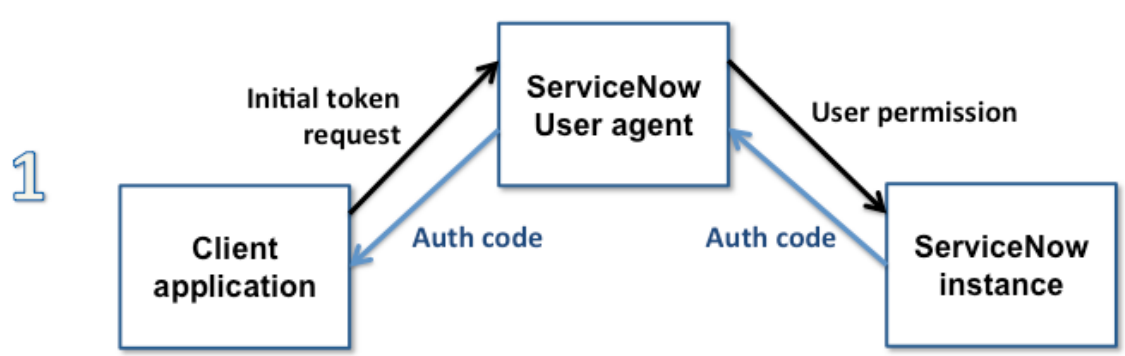
Une ServiceNow instance en tant que serveur d'autorisation

Le serveur OAuth est généralement un serveur d'autorisation tiers. Vous pouvez également spécifier une ServiceNow instance en tant que serveur d'autorisation qui émet les jetons pour le flux de code d'autorisation.

L'utilisateur propriétaire de la ressource restreinte doit autoriser l'accès. L'utilisateur peut également révoquer le jeton d'accès émis à tout moment pour mettre fin à l'accès.

Processus de flux d'octroi de code d'autorisation

Le processus de flux d'attribution du code d'autorisation se compose de ces trois étapes :



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

À la première étape, l'application cliente ou le site web lance un appel d'API REST sous la forme d'une requête GET à l'instance via l'agent utilisateur. En règle générale, l'appel REST est lancé lorsque l'utilisateur final clique sur un bouton ou un lien sur l'application cliente ou le site Web pour demander un jeton d'accès. Dans l'application cliente, l'utilisateur final doit également spécifier l'URL d'autorisation, l'URL du jeton, l'ID client et la clé secrète du client. Pour obtenir des explications sur ces éléments, reportez-vous à la description des champs dans cette rubrique : Utiliser un fournisseur OAuth tiers . Si le client demande un type d'accord, l'utilisateur final doit sélectionner Code **d'autorisation**.

Exemple de demande GET de l'application cliente vers l'instance :

```
https://myinstance.service-now.com/oauth_auth.do?response_type=code&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Remarque :
Le **response_type** doit être **du code** pour utiliser le flux d'attribution de code OAuth standard.

L'utilisateur final doit manuellement autoriser l'accès à la ressource restreinte sur l'instance. Dans l'implémentation ServiceNow , l'utilisateur final doit être connecté à l'instance. L'instance invite l'utilisateur final avec une page d'interface utilisateur comportant des boutons **Autoriser** et **Refuser** .

L'élément auquel l'application cliente demande en fait le jeton est l'enregistrement de registre d'application du fournisseur OAuth que vous avez créé, également connu sous le nom de point de terminaison d'autorisation (voir Utiliser un fournisseur OAuth tiers). Le code d'authentification est envoyé du point de terminaison d'autorisation au client. Il ne va pas directement au client, mais à **l'URL de redirection** que vous spécifiez dans le formulaire de point de terminaison d'autorisation. Cette URL est également connue sous le nom d'URL de rappel. Vous pouvez obtenir cette URL à partir de l'application cliente ou du site Web.

Exemple de réponse de l'instance à l'application cliente, fournissant un code d'autorisation :

```
https/http://{callbackURL}?code={the actual auth code}
```



Maintenant que l'application cliente dispose du code d'autorisation, le client utilise le code pour demander le jeton d'accès. Le code d'autorisation prouve que l'utilisateur a consenti à l'étape 1.

Exemple de demande POST de l'application cliente vers l'instance ServiceNow qui fournit le code d'authentification et demande le jeton d'accès :

```
https://myinstance.service-now.com/oauth_token.do?grant_type=authorization_code&code={the auth
 code}&redirect_uri={the_same_redirect_url}&client_id={the_same_client_identifier}&client_secret={client_secret_value}
```

Le point de terminaison sur l'instance renvoie un jeton d'accès et un jeton d'actualisation. Le jeton d'actualisation peut être utilisé pour demander des jetons d'accès supplémentaires.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez gérer les jetons, y compris révoquer le jeton, dans l'instance. Reportez-vous à la section Gérer les jetons OAuth.



L'application cliente utilise le jeton d'accès pour s'authentifier auprès de l'API REST. Après avoir authentifié l'application cliente, l'API REST renvoie les données demandées dans une charge utile JSON.

Exemple de demande GET pour la charge utile JSON des données de la table Incident [incident] :

```
https://myinstance.service-now.com/api/now/table/incident?access_token={the_token}
```

Remarque :
Le système prend également en charge les concessions implicites OAuth, également connues sous le nom de flux de code d'attribution implicite.

Prise en charge de l'intégration

Le flux de code d'autorisation prend en charge les intégrations suivantes sur l'instance :

- SSO (authentification unique) de plusieurs fournisseurs
- SAML 2.0 Mise à jour 1
- Authentification multifacteur

L'interface mobile est également prise en charge.

Autoriser l'accès à un point de terminaison OAuth à l'aide d'un flux de code d'authentification

Les utilisateurs finaux qui possèdent une ressource protégée sur l'instance ServiceNow doivent autoriser l'accès à la ressource avant que l'instance puisse fournir le jeton d'accès.

Avant de commencer
Rôle requis : aucun. Vous devez déjà être connecté à l'instance qui détient la ressource protégée. Vous pouvez également vous connecter à l'aide de la méthode d'authentification (telle que l'authentification multifacteur ou SAML) déjà configurée par votre ServiceNow administrateur.

Procédure

1. Cliquez sur le lien ou le bouton de l'application cliente dans laquelle vous demandez l'accès à la ressource protégée sur l'instance.
   Cela lance la demande de jeton. Si vous effectuez un appel REST d'une instance à une autre, ce lien est **Obtenir un jeton OAuth** sur le formulaire Message REST.
2. Si vous n'êtes pas connecté, connectez-vous maintenant.
   Si vous n'êtes pas le même utilisateur que l'utilisateur spécifié dans le coin supérieur droit, cliquez sur **Pas vous ?** et connectez-vous.
3. Cliquez sur autorisations de compte pour ouvrir la liste des jetons d'accès que vous avez déjà émis.

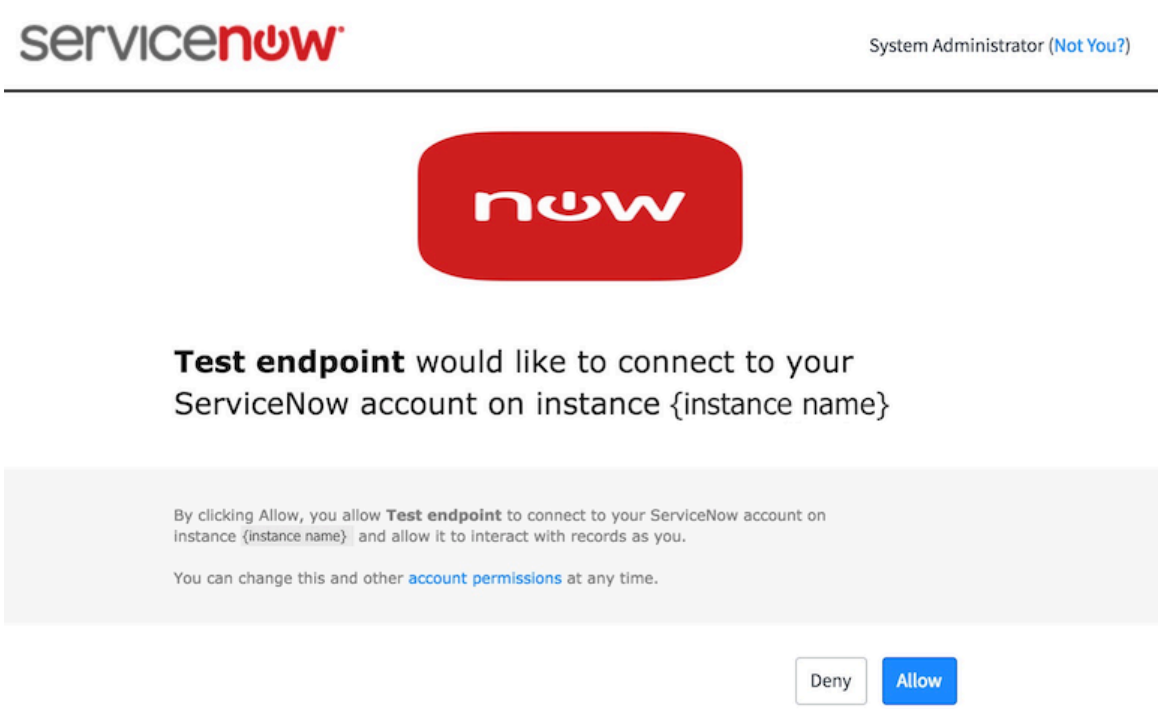
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

C’est la même chose que le **Libre-service** > **Mes connexions** Liste des jetons d’application.

4. Cliquez sur **Autoriser** pour autoriser l’accès et demander à l’instance d’émettre le code d’autorisation (si vous utilisez un flux de code d’authentification) ou le jeton d’accès (si vous utilisez un type d’accord implicite).

   Si vous cliquez sur **Refuser**, l’autorisation n’est pas autorisée, mais vous n’êtes pas déconnecté de l’instance.



Un message de confirmation de l’accès doit s’afficher. Si vous demandez l’accès à partir du formulaire Message REST sur une instance, le message suivant s’affiche en haut du formulaire : Le jeton d’actualisation OAuth est disponible et expirera à {date}.

Code d’autorisation Besoin du paramètre de l’état de flux

La propriété système glide.oauth.state.paramater.required permet d’exiger le paramètre État dans une demande OAuth pour le flux du code d’autorisation.

Paramètre d’état

Rôle requis : aucun.

À partir de la version Madrid, la propriété *`glide.oauth.state.parameter.required`* système ajoute un paramètre d’état pour une demande OAuth. Pour les instances zbooted, la propriété est true. Pour les instances mises à niveau, la propriété n’étant pas présente, le paramètre État n’est donc pas activé. Le paramètre État est une valeur de chaîne et ne doit pas contenir de caractères spéciaux. Le paramètre d’état ne peut pas être vide ou " « .

Validation du paramètre d’état

Créez un point de terminaison pour permettre aux clients d’accéder à l’instance. Lancez un flux de code d’autorisation pour un oauth_auth.do. Par exemple :

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=e9dba45b380d1300e676ccc91cef468f&response_type=code
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous ne spécifiez pas le paramètre d'état dans la demande, vous obtenez une erreur et le code d'autorisation n'est pas retourné.Paramètre d'état manquant dans la demande.

Ajout du paramètre State à la demande :

```
http://myinstance.service-now.com/oauth_auth.do?grant_type=authorization_code&client_id=
e9dba45b380d1300e676ccc91cef468f&response_type=code&state=123
```

L'ajout du paramètre État vous redirige vers l'écran de connexion et le flux de code d'autorisation normal renvoie le code d'autorisation.

Remarque :
L'URL de réponse contient le paramètre d'état transmis dans la demande. Dans l'exemple, le paramètre ajouté est `state=123`.

Si le flux du code d'autorisation commence à partir de oauth_initiator.do :

```
http://myinstance.service-now.com/oauth_initiator.do?oauth_requestor_context=sys_rest_mes
sage&oauth_requestor=eab8341fec0d1300964f214a2c2fcf67&oauth_provider_profile=dfa8f01fe
c0d1300964f214a2c2fcf51&response_type=code
```

Le paramètre State est automatiquement ajouté lorsqu'il est redirigé par oauth_auth.do.

```
http://myinstance.service-now.com/oauth_auth.do?response_type=code&state=-790938844&r
edirect_uri=http://10.11.95.5:16001/oauth_redirect.do&client_id=e9dba45b380d1300e676ccc9
1cef468f
```

Exemple de flux de code d'autorisation : ServiceNow instance en tant que serveur d'autorisation

Vous pouvez utiliser une instance en tant que serveur d'autorisation pour émettre des jetons à un client à l'aide du flux de code d'autorisation.

Avant de commencer
Rôle requis : aucun.

Cet exemple utilise deux instances : l'une en tant que serveur d'autorisation et l'autre en tant que client. Une instance utilise un appel REST pour demander des jetons à une autre instance.

Vous devez le faire Activer OAuth dans les deux cas.

Procédure

1. Sur l'instance du serveur d'autorisation (exécutant la version Istanbul ou ultérieure), accédez à **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Cliquez sur **Créer un point de terminaison d'API OAuth pour les clients externes**.
3. Renseignez les champs de formulaire de l'enregistrement d'application OAuth, comme décrit à la section Créer un point de terminaison pour permettre aux clients d'accéder à l'instance.
   La réalisation de ces étapes configure un serveur d'autorisation. Suivez les étapes suivantes pour configurer le serveur client.
4. Sur l'instance client, accédez à **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
5. **Cliquez sur Se connecter à un fournisseur OAuth tiers**.
6. Renseignez les champs de formulaire de l'enregistrement d'application OAuth, comme décrit à la section .
   Notez les valeurs de champ suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Nom** : nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth.
- **ID client** : ID client de l'enregistrement de registre d'application que vous avez créé pour le serveur d'autorisation.
- **Secret client** : [Lecture seule] ID unique de l'application généré automatiquement. L'instance utilise l'ID client lors de la demande d'un jeton d'accès.
- **Type d'accord par défaut** : sélectionnez **Code d'autorisation**.
- **URL d'autorisation** : URL de l'instance qui est le serveur d'autorisation. N'oubliez pas d'ajouter `oauth_auth.do` à la fin de l'URL.
- **URL du logo** : URL qui contient une image à utiliser comme logo de l'application. Le logo apparaît sur la page d'approbation lorsque l'utilisateur reçoit une demande d'octroi à une application cliente l'accès à une ressource restreinte sur l'instance.
- **URL du jeton** : URL de l'instance qui est le serveur d'autorisation. N'oubliez pas d'ajouter `oauth_token.do` à la fin de l'URL.
- **URL de redirection** : URL de l'instance : l'instance client-serveur. N'oubliez pas d'ajouter `oauth_redirect.do` à la fin de l'URL.

7. Créez un profil pour l'enregistrement avec le type d'accord de **code d'autorisation** .
   Le serveur client est configuré. Vous pouvez maintenant créer un message REST sortant et obtenir un jeton OAuth.

Créer un point de terminaison pour permettre aux clients d'accéder à l'instance

Créez un point de terminaison d'application OAuth pour que les applications clientes externes accèdent à l'instance ServiceNow .

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Créer un point de terminaison d'API OAuth pour les clients externes**, puis remplissez le formulaire.

Champ	Description
Nom	Nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth.
ID client	[Lecture seule] ID unique de l'application généré automatiquement. L'instance utilise l'ID client lors de la demande d'un jeton d'accès.
Secret client	[Obligatoire] Chaîne secrète partagée que l'instance et l'application cliente ou le site web utilisent pour autoriser les communications entre eux. L'instance utilise le secret client lors de la demande d'un jeton d'accès. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets client existants, cliquez sur l'icône de verrouillage.
URL de redirection	URL de rappel vers laquelle le serveur d'autorisation redirige. Entrez les URL complètes des clients demandant l'accès à la ressource, jointes par `/oauth_redirect.do`. Par exemple, `http ://token_consumer :port/oauth_redirect.do`. Saisissez autant d'URL que nécessaire pour tous les consommateurs de jetons possibles. L'instance associe l'URL

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	de la demande entrante à l'une des URL de redirection. Si aucune correspondance n'est établie, l'instance utilise la première URL de redirection.
URL du logo	URL qui contient une image à utiliser comme logo de l'application. Le logo apparaît sur la page d'approbation lorsque l'utilisateur reçoit une demande d'octroi à une application cliente l'accès à une ressource restreinte sur l'instance.
Actif	Cochez la case pour activer le registre d'application.
Durée de vie du jeton d'actualisation	Nombre de secondes pendant lesquelles un jeton d'actualisation est valide. L'instance utilise la valeur de durée de vie lorsqu'elle demande un jeton d'actualisation. Par défaut, les jetons d'actualisation expirent au bout de 100 jours (8640 000 secondes).
Appliquer les restrictions de jeton	Sélectionnez cette option pour autoriser uniquement l'utilisation de jetons avec des API définies pour autoriser le profil d'authentification. Vous pouvez définir l'octroi d'accès à l'aide d'une politique d'accès API. Pour plus d'informations, consultez Créer une politique d'accès REST API. Par défaut : non sélectionné.
Client mobile	Représente l'entité pour l'application mobile ou le Web. Ces informations sont utilisées pour analyser les informations de connexion avec mobile ou web.
Durée de vie du jeton d'accès	Nombre de secondes pendant lesquelles un jeton d'accès est valide. L'instance utilise la valeur de durée de vie lors de la demande d'un jeton d'accès. Par défaut, les jetons d'accès expirent au bout de 30 minutes (1 800 secondes).
Commentaires	Informations supplémentaires à associer à l'application.
Type de client	Choisissez le type de client en fonction du type de votre client. Options : ○ **Iframe incorporé** ○ **Intégration en tant qu'utilisateur** ○ **Intégration en tant que service** Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

3. Cliquez sur **Envoyer**.

Résultats

Le système crée un enregistrement dans la table Registres d'application [oauth_entity] de type client OAuth. Lorsque l'instance émet des jetons et des codes d'autorisation, ceux-ci sont stockés dans la table. Pour plus d'informations, consultez Gérer les jetons OAuth .

Paramètres de réponse de l'API OAuth

L'API OAuth 2.0 génère une réponse JSON contenant les paramètres suivants sous forme de paires nom-valeur.

Paramètres de réponse du jeton d'accès

Paramètre de réponse	Description
périmètre	Quantité d'accès accordé par le jeton d'accès. Le périmètre est toujours **useraccount**, ce qui signifie que le jeton d'accès a les mêmes droits que le compte d'utilisateur qui a autorisé le jeton. Par exemple, si Abel Tuter autorise une application en fournissant des informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de réponse du jeton d'accès (suite)

Paramètre de réponse	Description
	d'identification de connexion, le jeton d'accès qui en résulte accorde au porteur du jeton les mêmes privilèges d'accès qu'Abel Tuter.
token_type	Type de jeton émis par la demande, tel que défini dans la RFC OAuth. Le type de jeton est toujours **Bearer**, ce qui signifie que toute personne en possession du jeton d'accès peut accéder à une ressource protégée sans fournir de clé cryptographique. Consultez RFC6750 pour plus d'informations sur la façon dont OAuth 2.0 utilise les jetons de porteur.
expires_in	Durée de vie du jeton d'accès en secondes.
refresh_token	Valeur de chaîne du jeton d'actualisation.
access_token	Valeur de chaîne du jeton d'accès. Les demandes d'accès effectuées dans le délai d'expiration du jeton d'accès renvoient toujours le jeton d'accès actuel.
format	[Facultatif] Format de sortie de la réponse. Cette valeur est toujours JSON.

Remarque :
Si un fournisseur OAuth envoie le corps de la réponse comme « content-type » au lieu de « Content-Type », le client HTTP OAuth peut ne pas analyser correctement la réponse. Pour corriger ce problème, créez une propriété système à l'aide de ces paramètres.

Champ	Valeur
Nom	glide.oauth.inhouse.httpclient.enabled
Type	true|false
Valeur	faux

Pour plus d'informations sur la création de propriétés système, consultez Ajouter une propriété système

L'exemple suivant illustre la chaîne JSON renvoyée par une demande de jeton d'accès. (Des espaces ont été ajoutés pour améliorer la lisibilité).

```
{"scope":"useraccount","token_type":"Bearer","expires_in":1800,
"refresh_token":"w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FMxHW40H8yOO3Hoe",
"access_token":"F0jh9korTyzd9kaZqZ0SzjKZuS3ut0i4P46Lc52m2JYHiLIcqzFAumpyxshU9mMQ13gJHtxD2fy"}
```

Paramètres de demande de l'API OAuth

Découvrez les paramètres de demande d'API OAuth utilisés par les demandes de jeton d'accès.

Remarque :
Le type de contenu de l'API OAuth doit être `application/x-www-form-urlencoded`. Un type de contenu `d'application/json` entraîne une erreur non spécifiée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de demande de jeton d'accès

Paramètre de demande	Description
grant_type	[Obligatoire] Type d'informations d'identification autorisant la demande de jeton d'accès. Ce paramètre doit avoir l'une des valeurs suivantes : • **mot de passe** : ensemble d'informations d'identification de l'utilisateur pour autoriser la demande de jeton d'accès. Spécifiez les informations d'identification de l'utilisateur dans les paramètres nom d'utilisateur et mot de passe. • **refresh_token** : un jeton d'actualisation existant autorise la demande de jeton d'accès. Spécifiez le jeton d'actualisation dans le paramètre refresh_token.
client_id	[Obligatoire] ID unique généré automatiquement de l'application cliente demandant le jeton d'accès.
client_secret	[Obligatoire] Chaîne secrète partagée que l'instance et l'application OAuth utilisent pour autoriser les communications entre elles.
nom d'utilisateur	Nom du compte d'utilisateur qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jeton d'accès avec un **grant_type** de **mot de passe**.
mot de passe	Mot de passe du compte d'utilisateur qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jeton d'accès avec un **grant_type** de **mot de passe**.
refresh_token	Jeton d'actualisation existant qui autorise la demande de jeton d'accès. Ce paramètre est requis pour les demandes de jetons d'accès avec un **grant_type** de **refresh_token**.

Demandes utilisant les informations d'identification de l'utilisateur

L'instance demande aux clients de fournir des informations d'identification de connexion d'utilisateur lors de la première autorisation du client ou lors de l'autorisation de la création d'un jeton d'actualisation. Ce type de requête renvoie toujours deux jetons :

- Un jeton d'accès
- Un jeton d'actualisation

L'instance vérifie que l'utilisateur est actif, qu'il n'est pas actuellement verrouillé et qu'il dispose d'une session interactive. Si l'une de ces conditions est fausse, l'instance ne produit pas de jeton d'accès. Les demandes d'accès effectuées dans le délai d'expiration du jeton d'accès renvoient toujours le jeton d'accès actuel.

Remarque :
Ce type d'octroi d'autorisation repose sur le cryptage TLS pour protéger les informations d'identification de l'utilisateur lors de la transmission.

L'exemple suivant illustre la demande d'un jeton d'accès avec un ensemble d'informations d'identification de l'utilisateur (des espaces ont été ajoutés pour améliorer la lisibilité).

```
$ curl -d"grant_type=password&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&username=admin&password=admin"
https://instancename.service-now.com/oauth_token.do
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Demandes utilisant un jeton d'actualisation

L'instance peut utiliser un jeton d'actualisation existant pour créer un nouveau jeton d'accès. Ce type de demande renvoie uniquement un jeton d'accès. L'instance confirme que le jeton d'actualisation n'a pas expiré avant de générer un nouveau jeton d'accès. Les demandes d'accès effectuées dans le délai d'expiration du jeton d'actualisation renvoient toujours le jeton d'actualisation actuel. La transmission de jetons d'actualisation est généralement plus sécurisée que la transmission d'informations d'identification d'utilisateur. L'exemple suivant illustre la demande d'un jeton d'accès avec un jeton d'actualisation existant (des espaces ont été ajoutés pour améliorer la lisibilité).

```
$ curl -d"grant_type=refresh_token&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&refresh_token=w599voG89897rGVDmdp12WA681r9E5948c1CJTPi8g4HGc4NWaz62k6k1K0FM
xHW40H8yOO3Hoe"
https://instancename.service-now.com/oauth_token.do
```

Créer un point de terminaison d'API JWT OAuth pour les clients externes (intégration d'ordinateur à ordinateur)

Le jeton de porteur OAuth JWT permet aux applications Web clientes de s'authentifier auprès de votre instance de manière transparente à l'aide du type d'attribution JWT entrant au lieu de demander à l'utilisateur final de se connecter manuellement ou de partager le mot de passe.

Avant de commencer

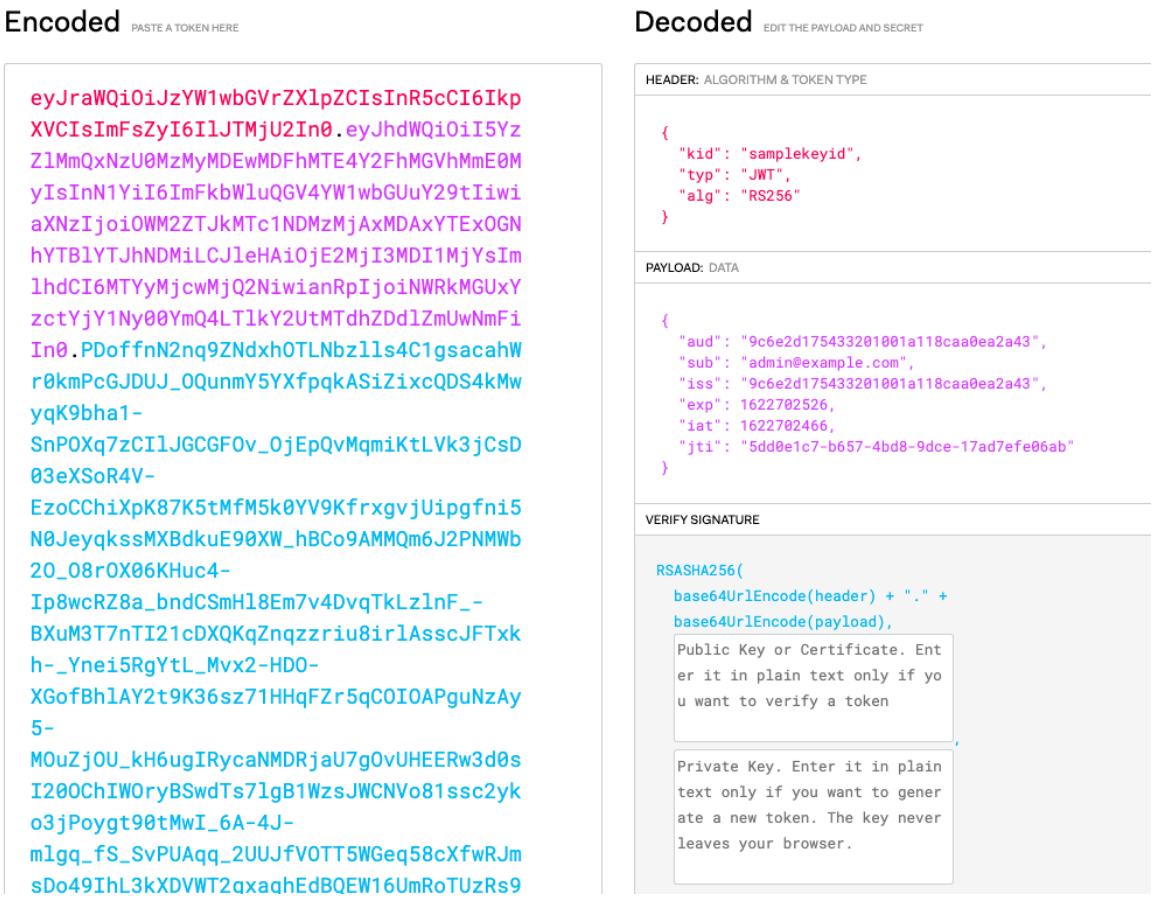
Générez un jeton Web JSON (JWT) avec les réclamations suivantes côté client :

- `aud` : doit correspondre à la valeur de l'ID client.
- `sub` : doit être un identificateur d'utilisateur, tel que l'e-mail de l'utilisateur auquel vous souhaitez associer le jeton.
- `iss` : correspond recommandée à la valeur de l'ID client. Si l'`aud` et l'`iss` ne correspondent pas, ajoutez la valeur `iss` dans la validation de réclamation.
- `exp` : n'importe quelle expiration souhaitée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de jeton Web JSON décodé



Configuration dans ServiceNow

Pourquoi et quand exécuter cette tâche

Étant donné que l'utilisation du type d'attribution JWT n'inclut pas le mot de passe dans la demande, elle permet une plus grande sécurité entre les services Web. Par exemple, vous pouvez développer une application externe et utiliser des jetons pour authentifier les demandes entrantes envoyées à votre ServiceNow instance.

Rôle requis : administrateur

Pour plus d'informations sur les jetons Web JSON, reportez-vous à la section https://jwt.io/ .

Procédure

1. Ajoutez la clé publique de l'application cliente à la table **sys_certificate** .
2. Configurez la configuration dans votre ServiceNow instance pour vérifier le JWT entrant.
   a. Accédez à la **OAuth système** > **Registre d'application**.
   b. Sélectionnez **Créer un point de terminaison d'API JWT OAuth pour les clients externes**.
   c. Remplissez le formulaire avec les informations relatives à votre jeton.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table JWT OAuth

Champ	Description
Nom	Un nom unique qui identifie l'application pour laquelle vous avez besoin d'un accès OAuth JWT.
ID client	ID unique de l'application généré automatiquement. Le système utilise la valeur de ce champ pour récupérer la clé publique ou partagée et valider le JWT. La valeur de ce champ doit correspondre à la valeur des réclamations de l'émetteur et de l'audience dans le JWT.
Secret client	Chaîne secrète partagée que l'instance et l'application cliente ou le site web utilisent pour autoriser les communications entre eux. Laissez ce champ vide pour que l'instance génère automatiquement un secret client. Pour afficher les secrets client existants, sélectionnez l'icône de verrouillage. **Remarque :** Si **Client public** est sélectionné, vous pouvez omettre le **secret client**.
Champ d'utilisateur	Champ dans la table Utilisateur (sys_user) que le système utilise pour correspondre à la valeur de la réclamation objet dans le JWT. Par exemple, si vous ajoutez un jeton dont la valeur de réclamation d'objet est user.name@example.com, vous devez définir le **champ Utilisateur** sur **E-mail**. Ce champ indique au système de rechercher la valeur user.name@example.com dans le champ d'e-mail et d'utiliser l'enregistrement d'utilisateur correspondant dans la demande entrante.
Activer la vérification JTI	Sélectionnez cette option pour exiger un nouveau jeton à chaque échange de jeton. Par défaut : sélectionné.
Application	Champ d'application de l'application en lecture seule. Ce champ est renseigné automatiquement.
Accessible depuis	Politique d'accès entre périmètres. Pour plus d'informations, consultez Paramètres d'accès à l'application .
Durée de vie du jeton d'accès	Durée de validité du jeton. Unité : Secondes
Décalage d'horloge	Décalage horaire autorisé entre les horloges du serveur et du client lors de la validation des réclamations exp et nbf dans JWT. Unité : Secondes Par défaut : 300
Appliquer les restrictions de jeton	Sélectionnez cette option pour autoriser uniquement l'utilisation des jetons avec des API définies pour activer le profil d'authentification. Vous pouvez définir l'octroi d'accès à l'aide d'une politique d'accès API. Pour plus d'informations, consultez Créer une politique d'accès REST API. Par défaut : non sélectionné.
Commentaires	Informations supplémentaires à associer à l'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Client public	Ajoutez ce champ au formulaire si le client JWT est public. Lorsque cette option est sélectionnée, vous n'avez pas besoin d'inclure de **secret client**. Par défaut : non sélectionné.
Type de client	Choisissez le type de client en fonction du type de votre client. Options : ▪ **iframe incorporé** ▪ **Intégration en tant qu'utilisateur** ▪ **Intégration en tant que service** Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

d. Enregistrez le formulaire.

e. Ajoutez des enregistrements à la liste connexe des cartes de vérificateur JWT pour vérifier la signature JWT.

Table des cartes de vérificateur JWT

Champ	Description
Nom	Nom de l'enregistrement de mappage JWT.
Enfant	ID clé de JWT
Clé partagée	Clé partagée pour l'ID de clé spécifié.
Application	Champ d'application de l'application en lecture seule.
Certificat système	Enregistrement de certificat dans la table Certificats X.509 (sys_certificate). Le certificat qui a été chargé à l'étape 1.

f. Ajoutez toutes les réclamations personnalisées associées à votre JWT à la liste connexe Validations des réclamations OAuth JWT.

Vous n'avez pas besoin d'ajouter des enregistrements pour les déclarations obligatoires suivantes :

- Iss
- Aud
- sub
- Exp

Remarque :

- Si l'aud et l'iss ne correspondent pas, ajoutez la valeur iss dans la validation de réclamation.
- Pour les certificats, vous pouvez ajouter plusieurs cartes de vérificateur associées à plusieurs clés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Table de validations de réclamation OAuth JWT

Champ	Description
Mon client externe	Renseigné automatiquement avec l'enregistrement JWT OAuth.
Type de valeur de réclamation	Type de données de la valeur de réclamation.
Nom de la réclamation	Nom de la réclamation que vous souhaitez ajouter.
Valeur de réclamation	Valeur de la réclamation.
Application	Champ d'application de l'application en lecture seule.

3. Envoyez une demande cURL contenant le jeton JWT pour obtenir un jeton d'accès à partir de votre instance.

Example

Voici un exemple de commande cURL demandant un jeton d'accès :

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&client_id=be3aeb583ace210011c15b24a43e25d8
&client_secret=client_password
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HflcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

Si le client JWT est un client public, tel que Mobile SDK, vous pouvez omettre les paramètres client_id et client_secret de la demande. Voici un exemple de commande cURL demandant un jeton d'accès qui omet le client_id et client_secret :

```
$ curl -d"grant_type= urn:ietf:params:oauth:grant-type:jwt-bearer
&assertion=
 eyJraWQiOiJzYW1wbGVrZXlpZCIsInR5cCI6IkpXVCIsImFsZyI6IlJTMjU2In0.eyJhdWQiOiI5YzZl
MmQxNzU0MzMyMDEwMDFhMTE4Y2FhMGVhMmE0MyIsInN1YiI6ImFkbWluQGV4YW1wbG
UuY29tIiwiaXNzIjoiOWM2ZTJkMTc1NDMzMjAxMDAxYTExOGNhYTBlYTJhNDMiLCJleHAiOjE
2MjI3MDI1MjYsImlhdCI6MTYyMjcwMjQ2NiwianRpIjoiNWRkMGUxYzctYjY1Ny00YmQ4LTlkY
2UtMTdhZDdlZmUwNmFiIn0.PDoffnN2nq9ZNdxhOTLNbzlls4C1gsacahWr0kmPcGJDUJ_OQu
nmY5YXfpqkASiZixcQDS4kMwyqK9bha1-SnPOXq7zCIlJGCGFOv_OjEpQvMqmiKtLVk3jCsD03
eXSoR4V-EzoCChiXpK87K5tMfM5k0YV9KfrxgvjUipgfni5N0JeyqkssMXBdkuE90XW_hBCo9AM
MQm6J2PNMWb2O_O8rOX06KHuc4-Ip8wcRZ8a_bndCSmHl8Em7v4DvqTkLzlnF_-BXuM3T7n
TI21cDXQKqZnqzzriu8irlAsscJFTxkh-_Ynei5RgYtL_Mvx2-HDO-XGofBhlAY2t9K36sz71HHqFZr
5qCOIOAPguNzAy5-MOuZjOU_kH6ugIRycaNMDRjaU7gOvUHEERw3d0sI20OChIWOryBSwdT
s7lgB1WzsJWCNVo81ssc2yko3jPoygt90tMwI_6A-4J-mlgq_fS_SvPUAqq_2UUJfVOTT5WGeq58
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
cXfwRJmsDo49IhL3kXDVWT2gxaqhEdBQEW16UmRoTUzRs9A9sOm18y3skmOVtnEOm-MIJM
FQZ754UMzbiH0ZsMmk1ivCGIjex5J0_IDjKElWF5RHGz3YShCoa4JKDZsqYMvIk1SvzyQXjuFqP
dS2vzg2m1eKGUwr3m6uNs_HfIcDystwVdMZ7nLIBG4"
https://instancename.service-now.com/oauth_token.do
```

L'instance renvoie le jeton d'accès dans sa réponse :

```
{
   "access_token":
 "KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxNA",
   "scope": "useraccount",
   "token_type": "Bearer",
   "expires_in": 1799
}
```

Remarque :
Le type d'accord JWT entrant n'inclut pas les jetons d'actualisation.

4. Effectuez un appel d'API REST pour accéder à une ressource à l'aide du jeton d'accès.

Example

Ce qui suit est une commande cURL permettant d'accéder à la table d'incidents à l'aide du jeton.

```
$ curl -H "Authorization: Bearer
 KynMY2H0uwWkRc8g8YLXjnQxWbH5_wbnSiLsnaOoKw61GZkkV0ytZP74uF7hJyjfsWfaaFijq
Qzq2kcABNJxN"
https://instancename.service-now.com/api/now/v1/table/incident
```

Résultats
Le système récupère le jeton d'accès lors de l'appel REST et autorise l'accès à la ressource demandée.

Configurer un fournisseur OIDC OAuth pour accepter un jeton tiers

Vous pouvez configurer un fournisseur OIDC OAuth pour qu'il accepte les jetons d'identité générés par un fournisseur OIDC tiers à l'aide d'appels d'API entrants à l'aide de l'option Single Sign-On (SSO de plusieurs fournisseurs).

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Ils Now Platform prennent en charge OIDC via notre implémentation SSO (Single Sign-On) externe en plus des appels d'API entrants. Pour obtenir un exemple de configuration de fournisseur OIDC, consultez Configuration d'Azure AD. Pour obtenir un exemple de configuration de fournisseur OIDC spécifique à l'authentification unique, consultez Créer une configuration OpenID Connect (OIDC) pour l'authentification unique (SSO).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application**.
   - Sélectionnez **Nouveau**, **Configurer un fournisseur OIDC pour vérifier les jetons d'ID**, puis remplissez le formulaire.
   - Sélectionnez un modèle existant pour un fournisseur OIDC (ADFS, Auth0, Azure AD, Google, Okta), puis remplissez le formulaire.

     Remarque :
     les modèles de fournisseur OIDC sont disponibles après le chargement des données de démonstration avec le module d'extension OAuth 2.0.

Champ	Description
Nom	Nom unique qui identifie l'entité OIDC OAuth.
ID client	ID client de l'application enregistré sur le serveur OAuth OIDC tiers. Cette valeur doit être identique à la valeur de la réclamation `aud` dans le jeton JWT.
Script de l'API OAuth	Script que vous pouvez utiliser pour personnaliser les demandes et les réponses à un fournisseur OAuth externe.
Configuration du fournisseur OIDC OAuth	Les fournisseurs OIDC (ADFS, Auth0, Azure AD, Google, Okta) peuvent être utilisés pour valider le jeton JWT. Sélectionnez l'enregistrement de votre configuration de fournisseur OIDC pour valider que la **réclamation de l'utilisateur** et le **champ d'utilisateur** sont définis de manière appropriée. Assurez-vous également de remplir les champs suivants : ○ **Activer la vérification de la réclamation JTI** : lorsque cette option est activée, la ServiceNow validation du jeton JWT valide également le JTI envoyé par le fournisseur. ○ **URL des métadonnées OIDC** : détails de la configuration bien connue du fournisseur OIDC. **Remarque :** Si la validation n'est pas vérifiée, le `jti` ne peut pas être validé, qu'il soit présent ou non dans le jeton JWT. Le nom de la réclamation dans le jeton doit être `jti`.
Décalage d'horloge	Nombre, en secondes, pendant lequel la contrainte doit être considérée comme valide. La valeur par défaut est 300.
Appliquer les restrictions de jeton	Sélectionnez cette option pour autoriser uniquement l'utilisation des jetons avec des API définies pour activer le profil d'authentification. Vous pouvez définir l'octroi d'accès à l'aide d'une politique d'accès API. Pour plus d'informations, consultez Créer une politique d'accès REST API. Par défaut : non sélectionné.
Actif	Cochez la case pour activer l'application OAuth.
Type de client	Choisissez le type de client en fonction du type de votre client. Options : ○ **Iframe incorporé** ○ **Intégration en tant qu'utilisateur** ○ **Intégration en tant que service**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

2. Sélectionnez **Soumettre**.
   L'enregistrement est enregistré dans la table Registres d'application [oauth_entity].
   Lorsque votre instance émet des jetons et des codes d'autorisation, elle crée un enregistrement dans la table Registres d'application [oauth_entity] avec le type **Fournisseur OIDC externe**. Consultez pour plus d'informations.
3. **Facultatif :** Accédez à la liste connexe de l'enregistrement Profils des entités OAuth pour valider un profil par défaut généré par le système pour le nouveau fournisseur OAuth sans champ d'application.
   Vous pouvez modifier ou ajouter un profil de fournisseur OAuth incluant le nom, le type d'accord et le champ d'application OAuth.
4. **Facultatif :** Accédez à la liste connexe de l'enregistrement Périmètres des entités OAuth pour définir tous les champs d'application OAuth disponibles pour ce fournisseur OAuth.
   Les champs d'application définis peuvent être sélectionnés lors de la création ou de la mise à jour d'un profil. Chaque champ d'application OAuth défini contient un nom et un champ d'application que vous devez obtenir à partir de la spécification du fournisseur, par exemple un champ d'application de lecture ou un champ d'application d'écriture. Chaque champ d'application doit être défini séparément.
5. **Facultatif :** Accédez à la liste connexe de l'enregistrement Attribution d'utilisateurs pour activer l'attribution automatique d'utilisateurs.

Option	Description
Attribuer automatiquement les utilisateurs	Option permettant d'activer l'authentification forcée pour les utilisateurs.
Mettre en service la source de données	La source de données à utiliser pour transformer un jeton OIDC en ServiceNow utilisateur. Utilisez la **liste de recherche** pour sélectionner le modèle de source de données prédéfini, puis ouvrez l'enregistrement pour configurer le mappage de la table transformée. Lors de la configuration du mappage de transformation, les champs sources proviennent du `JWT token`, les champs cibles proviennent de la `sys_user` table.
Rôles d'utilisateur appliqués aux utilisateurs attribués	Les rôles d'utilisateur appliqués aux nouveaux utilisateurs approvisionnés ServiceNow .

Example: Voici un exemple de requête cURL pour invoquer un appel d'API REST

Invoquez un appel d'API REST.

Procédez comme suit :

- Enregistrez l'application dans le fournisseur OpenID Connect.
- Configurez l'entité OIDC OAuth.
- Configurez le fournisseur OIDC :

Fournisseur OIDC

Fournisseur OIDC	Nom du fournisseur OIDC.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

URL des métadonnées OIDC	Spécifiez l'URL des métadonnées OIDC (URL de configuration bien connue). Ces informations sont utilisées pour extraire les clés publiques afin de valider le jeton via le point de terminaison JWKS .
Réclamation de l'utilisateur	La réclamation qui est validée par rapport à la table utilisateur.
Champ d'utilisateur	Réclamation de l'utilisateur qui identifie l'enregistrement de l'utilisateur.
Activer la vérification de la réclamation JTI	Lorsqu'elle est activée, la validation du jeton JWT ServiceNow valide également le JTI envoyé par le fournisseur. **Remarque :** Si la validation n'est pas vérifiée, le jti ne peut pas être validé, qu'il soit présent ou non dans le jeton JWT. Le nom de la réclamation dans le jeton doit être jti. Ces informations sont utilisées pour prévenir les attaques par rejeu.

- Obtenez un jeton JWT.
- Invoquez un appel d'API REST.
  - Jeton d'ID dans l'en-tête d'autorisation pour accéder à l'API de table ou au service Web scripté.

```
curl -X GET --header "Accept:application/json"
 https://<instance_name>.service-now.com/api/now/table/incident/897b04f2dbd4a300a1
35364e9d961952 -k
--header "Authorization: Bearer
 eyJraWQiOiJjNTZtZTlXU0xPVnY3UFMwcTg4Qzl1b0lzNjFQYTdmUG4yZFVFOW9RNUg4Iiwi
YWxnIjoiUlMyNTYifQ.eyJzdWIiOiIwMHVnZDg1OD
VkczI1WXpUSjBoNyIsIm5hbWUiOiJpbXJhbiBhbGkiLCJsb2NhbGUiOiJlbi1VUyIsImVtYWlsIjoi
aW1yb241NDNAZ21haWwuY29tIiwidmVyIjoxLCJpc3MiOiJodHRwczovL2Rldi05MzQ
xMjEub2t0YXByZXZpZXcuY29tIiwiYXVkIjoiMG9hZ2Q4bzk3a2ICT3dwd0IwaDciLCJpYXQiOj
E1Mzc5MzMzMjYsImV4cCI6MTUzNzkzNjkyNiwianRpIjoiSUQueThVdXpWNUg2bm16SzRs
OTI1RFVrQnJoR1o1MmJzVVpGVHRVTEphQjg3ayIsImFtciI6WyJwd2QiXSwiaWRwIjoiMDBvZ
2Q4NTgycEFqZDZTemcwaDciLCJub25jZSI6InNub3ciLCJwcmVmZXJyZWRfdXNlcm5hbW
UiO
iJpbXJvbjU0M0BnbWFpbC5jb20iLCJnaXZlbl9uYW1lIjoiaW1yYW4iLCJmYW1pbHlfbmFtZSI6I
mFsaSIsInpvbmVpbmZvIjoiQW1lcmljYS9Mb3NfQW5nZWxlcyIsInVwZGF0ZWRfYXQiOj
E1Mzc5MzAxOTcsImVtYWlsX3ZlcmlmaWVkIjp0cnVlLCJhdXRoX3RpbWUiOjE1Mzc5Mjk2Nj
F9.OG87SYxWFgHGlhBYby2H79diRm9rlYZTeEkIINRUatwg-p4739htB8xEY-5_t6yU_6k5w1
0pdgtt5M5QFZRPXVbQZNoGtY-Bxn0BjaimcFgoWfhY_0ldnGTkzN2RYyIHvrf9-yhxg347zvcz
mLrgMMa_VwG4rxrtE6rUXaIpIeIK5b-Deq8ADz8UTUTKpF_5RWk4X-oh5xK6BLniFHk4ShO
Zq2v_mjproXwKk5euJKrVrar2lQ4adZCOSTRuTf3ThMO5WDh0sel-82LngXtLzRJJ51IqxAsXns
0kJHLLqLtH1hXNRKfwT1ScQoE_OfWm4t0KryI2j4wSMEanFtLXIw"
```

  - Si l'utilisateur est authentifié, une réponse/json d'application/json valide est renvoyée. Dans le cas contraire, un message d'erreur d'utilisateur non authentifié est renvoyé.

```
User Not Authenticated
{"error":{"message":"User Not Authenticated","detail":"Required to provide Auth
 information"},"status":"failure"}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer le type de client pour les enregistrements OAuth et SSO

Configurez le champ **Type de client** pour les configurations relatives aux enregistrements OAuth et SSO.

Lors de l'établissement de sessions pour différents types de connexion tels que l'interface utilisateur Web (connexion interactive), l'Iframe intégré, intégré ou l'intégration, vous pouvez configurer le type de client pour les enregistrements OIDC (entité OAuth), SAML et Digest utilisés pour différentes connexions.

Les types de clients disponibles sont les suivants :

- **Iframe intégré** : peut être utilisé pour une instance interactive ServiceNow qui réside dans un Iframe sur les sites Web tiers. Par exemple, s'il existe une table sensible (table sys_user - numéro de téléphone de l'utilisateur), en tant qu'administrateur, vous pouvez configurer l'ACL avec l'attribut sec (Iframe intégré) défini sur faux, afin d'éviter que l'utilisateur n'accède aux données (informations de table) sur la session Iframe incorporée dans le tiers.
- **Intégration en tant qu'utilisateur** : peut être utilisé pour le chatbot Agent virtuel installé dans des applications de bureau telles que Slack, Teams...
- **Intégration en tant que service** : peut être utilisé pour l'intégration de machine à machine (communication entre les services).

Remarque :

- [store-future: BEGIN review]Incorporé en tant que type de client est disponible lorsque le module d'extension Embedded client access (com.glide.security.client_access) est installé pour OIDC (OAuth Entity).[End]
- Pour OIDC (OAuth Entity) : tous les choix sont disponibles.
- Pour SAML et Digest : uniquement iframe intégré. Vous devez modifier le formulaire et ajouter le champ **Type de client** à l'enregistrement et sélectionner le type de client **Iframe intégré** .
- Si le **type de client** sélectionné est aucun, il n'y a pas de classification de la session.

Il est recommandé d'utiliser le champ Type de client pour chaque enregistrement créé pour OIDC (entité OAuth), SAML et synthèse. Cela vous permet d'avoir un meilleur contrôle sur chaque méthode de connexion qui a les mêmes configurations mais qui se distingue par le type de client.

Après la configuration du champ, chaque fois qu'un utilisateur se connecte à partir de la configuration correspondante (OAuth ou SSO), une fois l'authentification réussie, la session est considérée comme basée sur le type de client configuré et le délai d'expiration de la session est donc exploité.

Pour la session en cours, les attributs de sécurité correspondants sont inclus ou peuvent être exploités pour empêcher les utilisateurs d'accéder à des informations spécifiques à la table dans le type de client sélectionné. Pour plus d'informations, consultez Attributs de sécurité OOB (prêts à l'emploi).

Délai d'expiration de session pour les types de clients

Voici les propriétés système liées au délai d'expiration de session pour les différents types de clients :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- [store-future: BEGIN review]glide.session_timeout.incorporé[End]
- glide.session_timeout.iframe_embedded
- glide.session_timeout.integration_as_a_user
- glide.session_timeout.integration_as_a_service

Subventions implicites OAuth

ServiceNow Les instances prennent en charge l'octroi implicite d'un jeton d'accès.

Le type d'attribution implicite, également connu sous *`implicit grant code flow`*le nom de , permet de donner le jeton d'accès directement à l'application cliente via l'agent utilisateur, qui est généralement le navigateur Web ou l'équipement mobile. Aucun jeton d'actualisation n'est accordé. L'utilisateur final doit toujours accorder l'accès à la ressource protégée sur l'instance, comme avec le fichier .

Processus de flux d'octroi implicite OAuth

Tout comme pour le processus de flux de code d'autorisation standard, l'application cliente envoie une demande d'utilisation de la ressource restreinte sur l'instance et l'utilisateur final l'approuve. La demande se présente sous la forme d'une URL envoyée à l'instance. L'URL doit inclure les paramètres suivants :

- client_id=<l'ID client nécessaire>. Cette valeur est obligatoire pour identifier la ressource protégée à laquelle l'application cliente veut accéder.
- response_type=jeton. Ceci est obligatoire pour demander le jeton d'accès directement (par opposition à demander un code d'autorisation). La valeur doit être symbolique pour les subventions implicites. Dans l'exemple de flux de code d'autorisation standard, le type de réponse est code.
- redirect_uri=<a URL> : emplacement où le jeton est envoyé.

Le serveur d'autorisation envoie le jeton d'accès, plutôt qu'un code d'autorisation, à l'application cliente via l'agent utilisateur.

Voici un exemple de demande GET pour recevoir la charge utile JSON de données pour la table Incident [incident] :

```
https://myinstance.servicenow.com/oauth_auth.do?response_type=token&redirect_uri={the_redirect_url}&client_id={the_client_identifier}
```

Si l'utilisateur accorde l'accès, le jeton est inclus dans l'URL de redirection (rappel) :

```
https/http://{callbackURL}?access_token={the_token}
```

Gérer les jetons OAuth

Ouvrez les jetons OAuth pour fournir l'accès à des ressources restreintes.

Avant de commencer

Rôle requis : n'importe quel utilisateur ou administrateur

Pourquoi et quand exécuter cette tâche

Les jetons OAuth émis par l'instance et le fournisseur OAuth tiers sont stockés dans oauth_credential table.

Voici quelques-unes des colonnes importantes de ce tableau :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Jeton : valeur du jeton émis par ServiceNow l'instance.
- Type : détermine si le jeton est un jeton d'accès ou un jeton d'actualisation.
- Expire : date/heure d'expiration du jeton d'accès ou d'actualisation.
- Jeton reçu : valeur du jeton émis par un fournisseur OAuth tiers. Cette valeur est chiffrée.

L'expiration et la validité du jeton sont les suivantes :

- Jeton d'accès : par défaut, une instance émet des jetons d'accès d'une durée de vie de 30 minutes dans le scénario où l'instance est le fournisseur OAuth.
- Jeton d'actualisation : par défaut, une instance émet des jetons d'actualisation d'une durée de vie de 100 jours dans le scénario où l'instance est le fournisseur OAuth.

Procédure

1. Accédez à l'une des options de menu suivantes :
   - **Libre-service** > **Mes applications connectées** pour voir les jetons créés par l'instance lorsque vous avez accordé l'accès à une ressource sur l'instance.
   - **OAuth système** > **Gérer les jetons** pour voir tous les jetons. Seuls les administrateurs peuvent accéder à ce module.
2. Cliquez sur le **nom** pour ouvrir le jeton.
3. Cliquez sur **Révoquer l'accès** pour empêcher l'accès à la ressource restreinte.

   Vous pouvez également afficher d'autres informations sur le jeton, notamment le périmètre auquel il permet d'accéder et la date d'expiration.

   Vous pouvez sélectionner l'enregistrement **Nettoyer les informations d'identification OAuth expirées** à partir de la page Calendrier (sys.trigger.list) et configurer les éléments suivants :

   - **com.snc.platform.security.oauth.is.active** : par défaut, la valeur est définie sur 0 (vrai).
   - **com.snc.platform.security.oauth.hours.expired.credential.is.kept :** définissez la valeur en fonction de vos besoins pour déterminer le nombre d'heures pendant lesquelles vous souhaitez conserver les informations d'identification OAuth expirées dans le système.
   - **com.snc.platform.security.oauth.day.old.credential.is.kept** : définissez la valeur en fonction de vos besoins pour déterminer le nombre de jours pendant lesquels vous souhaitez conserver les informations d'identification OATUH expirées dans le système.

Révoquer un jeton OAuth

Pour des raisons de sécurité, vous pouvez vouloir révoquer un accès OAuth ou actualiser le jeton.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La révocation du jeton s'applique à la situation dans laquelle votre instance agit en tant que serveur de ressources OAuth. Vous pouvez révoquer le jeton via une URL ou via .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Accédez à votre instance à l'aide de oauth_revoke_token.do et ajoutez le jeton d'accès ou d'actualisation.

Par exemple : https://[Your_ServiceNow_Instance] :[port]/oauth_revoke_token.do ?token=[jeton d'accès ou d'actualisation] sans les crochets [ ].

Résultats

L'accès à ce point de terminaison ne nécessite pas d'authentification. Le jeton de cette demande est marqué comme expiré.

Informations d'identification du client

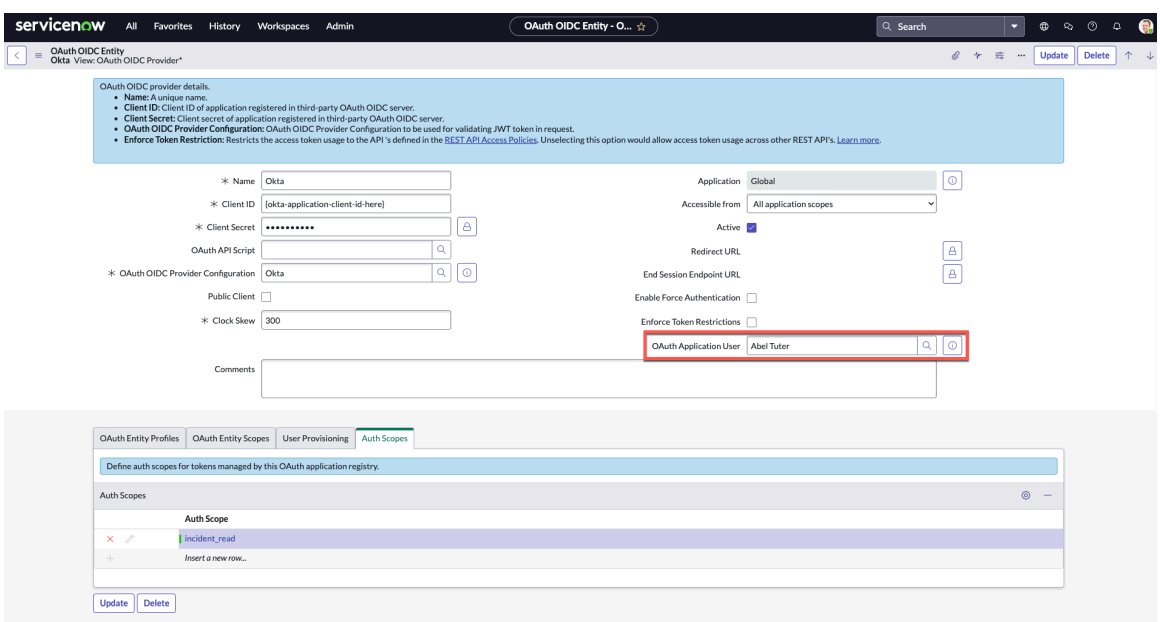
Utilisez le type d'accord d'informations d'identification du client OAuth pour les intégrations entrantes d'un client OAuth tiers vers la ServiceNow® plateforme.

Les administrateurs peuvent utiliser le type d'attribution d'informations d'identification du client (CC) pour permettre l'intégration d'un client OAuth tiers à la ServiceNow plateforme.

Le type d'attribution d'informations d'identification du client entrant est une aptitude qui peut être contrôlée via une propriété système. Par défaut, la propriété système est false.

Pour utiliser le type d'accord d'informations d'identification de client, vous devez procéder comme suit :

- Créez la propriété système glide.oauth.inbound.client.credential.grant_type.enabled .
- Ajoutez le champ **Utilisateur de l'application OAuth** au formulaire Entité OAuth.



Créer la propriété système Informations d'identification du client

Créez la propriété système glide.oauth.inbound.client.credential.grant_type.enabled pour utiliser le type d'attribution Informations d'identification du client pour les intégrations entrantes OAuth.

Avant de commencer

Rôle requis : administrateur

Module d'extension requis : OAuth 2.0.

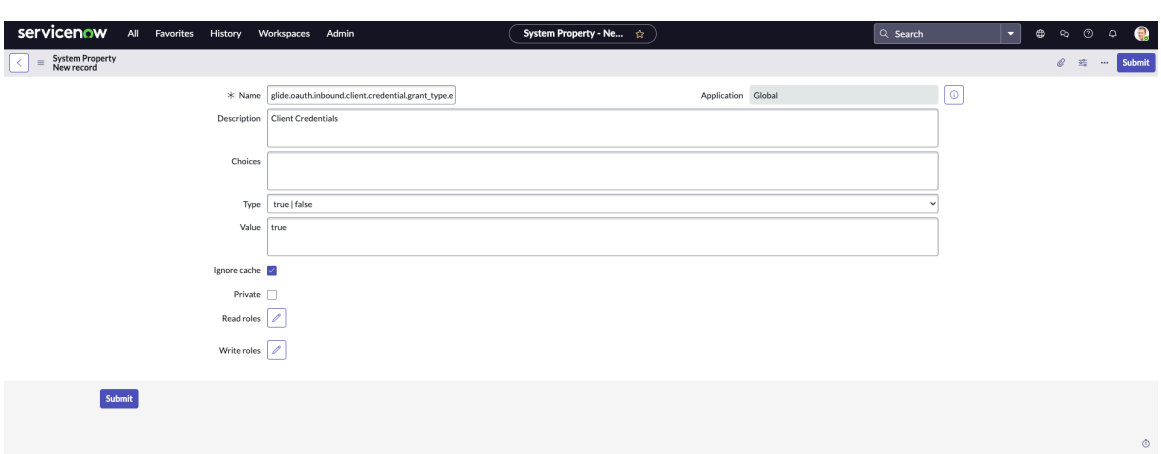
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Dans le filtre de navigation, saisissez `sys_properties.list`.
   La liste exhaustive des propriétés de la table Propriétés système [sys_properties] s'affiche.
2. Sélectionnez **Nouveau**.
3. Renseignez les champs suivants du formulaire.

Champ	Description
Nom	Nom de la propriété que vous créez. Dans ce cas, `glide.oauth.inbound.client.credential.grant_type.enabled`.
Description	Saisissez une phrase brève et descriptive décrivant la fonction de la propriété.
Type	Sélectionnez le type de données approprié dans la liste. Dans ce cas, `vrai| faux`.
Valeur	Définissez la valeur souhaitée pour la propriété. Dans ce cas, `vrai` pour activer le type d'accord d'informations d'identification du client pour les intégrations entrantes OAuth.



Remarque :
D'autres champs du formulaire, tels que Choix, Ignorer le cache, Privé, Rôles de lecture et Rôles d'écriture, peuvent être configurés en fonction de vos besoins.

4. Sélectionnez **Soumettre**.

Remarque :
Si la case **Ignorer le cache** est cochée, le système purge le cache du serveur lorsque le paramètre est modifié.

Vous devez ensuite créer un client OAuth (point de terminaison d'API OAuth pour le client externe) et ajouter le champ Utilisateur de l'application OAuth à l'enregistrement client OAuth.

Ajouter l'utilisateur de l'application OAuth

Ajoutez le champ Utilisateur de l'application OAuth sur le formulaire Entité OAuth pour utiliser le type d'accord Informations d'identification du client pour les intégrations entrantes OAuth.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

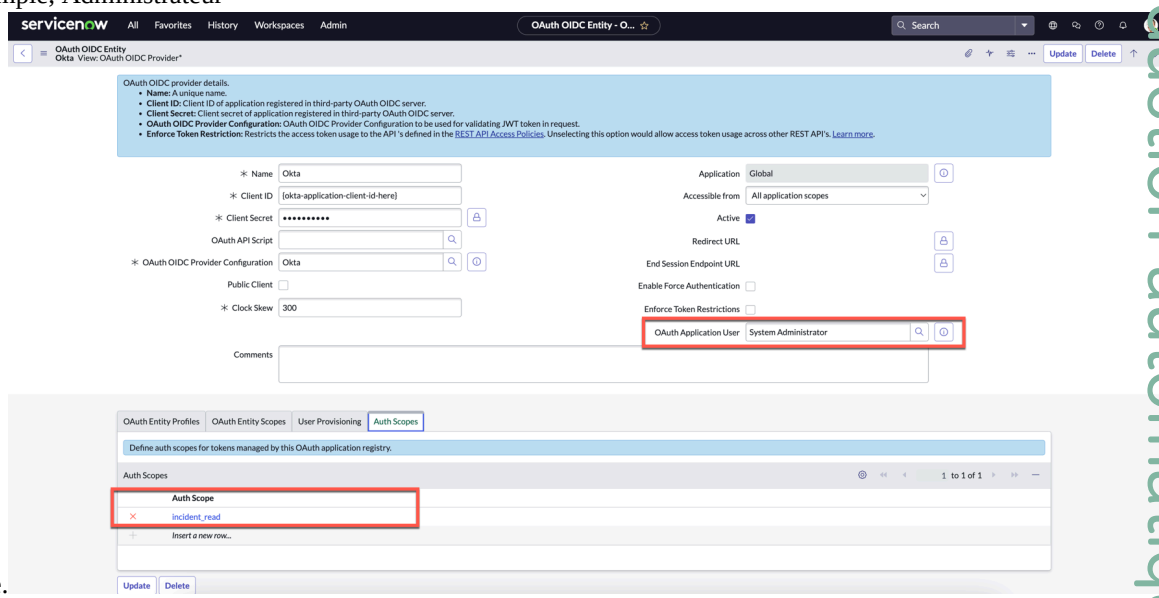
Rôle requis : administrateur

Module d'extension requis : OAuth 2.0.

Vous devez créer un client OAuth. Pour plus d'informations, consultez Créer un point de terminaison pour permettre aux clients d'accéder à l'instance.

Procédure

1. Ouvrez l'enregistrement client OAuth qui a été créé.
2. Sélectionnez l'icône Plus d'options sur l'en-tête de la page.
3. Sélectionner **Configurer** > **Conception de formulaire**.
4. Sur la page Conception de formulaire, ajoutez **un utilisateur de l'application OAuth** à partir de la liste des champs.
5. Enregistrez ou mettez à jour le formulaire.
6. Sélectionnez l'utilisateur de **l'application OAuth**.
   Par exemple, Administrateur système.



> **Remarque :**
> Vous devez utiliser le champ d'application d'authentification de l'API REST avec le type d'attribution d'informations d'identification du client pour contrôler l'accès fourni au client tiers.

7. Enregistrez ou mettez à jour le formulaire.

Toute demande d'autorisation dont le **type** d'accord est Informations **d'identification client**, **ID client** et **Secret** est transmise pour l'utilisateur de l'application OAuth associée dans ServiceNow®.

> **Remarque :**
> Si l'utilisateur de l'application OAuth n'est pas sélectionné sur l'enregistrement client OAuth ou si la propriété Informations d'identification du client est définie sur false, la demande d'autorisation n'est pas transmise.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

OAuth sortant

La sortie OAuth vous permet d'extraire des données d'un fournisseur tiers vers votre instance.

Vous devez disposer du rôle security_admin pour gérer l'intégration OAuth.

Vous pouvez configurer OAuth 2.0 sortant pour les types d'accord suivants :

- **Se connecter à un fournisseur tiers** : utilisez l'ID client et le secret pour l'envoyer au fournisseur OAuth. Pour plus d'informations, consultez Se connecter à un fournisseur OAuth tiers.
- **Support JWT** : un serveur d'autorisation valide un jeton JWT qui permet de partager des informations d'identité et de sécurité entre les domaines de sécurité. Pour plus d'informations, consultez Configurer le fournisseur OAuth avec le type d'attribution JWT Bearer.
- **Support SAML2** : génère l'assertion SAML2, puis échange l'assertion contre les jetons d'accès avec le fournisseur.

> **Remarque :**
> Pour la demande SuccessFactors sortante, utilisez le **support SAML2** comme type d'accord par défaut. Pour en savoir plus sur la configuration du **support SAML2**, reportez-vous à l'exemple de la section Set up the v4.x.x .

- **Code d'autorisation** : Code qui est accordé au client pour obtenir un jeton d'accès, qui est ensuite utilisé pour obtenir l'accès à la ressource. Si vous sélectionnez cette option, vous avez besoin d'une URL d'autorisation (l'URL du serveur d'autorisation).
- **Informations d'identification du mot de passe du propriétaire** de la ressource : nom d'utilisateur et mot de passe de l'utilisateur qui tente d'obtenir l'accès à la ressource.
- **Informations d'identification du client** : l'ID et le secret du client, qui sont tous deux utilisés pour obtenir le jeton d'accès. Cette méthode ne fournit pas de jetons d'actualisation.

Vous pouvez configurer le **scénario du fournisseur OAuth** (sortant) : votre instance extrait les données d'un fournisseur tiers.

> **Remarque :**
> Vous devez authentifier l'utilisateur pour la première fois pour récupérer la publication du jeton, que vous n'avez pas besoin d'authentifier à l'aide d'un compte utilisateur avant l'expiration du jeton.

Se connecter à un fournisseur OAuth tiers

Configurez la manière dont l'ID client et le secret sont envoyés à votre fournisseur OAuth.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Se connecter à un fournisseur OAuth tiers**, puis renseignez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom	Nom unique de la connexion OAuth tierce.
ID client	ID client de l'application enregistrée dans le serveur OAuth tiers.
Secret client	Clé secrète client de l'application enregistrée dans le serveur OAuth tiers.
Script de l'API OAuth	Script utilisé pour personnaliser la demande et la réponse au fournisseur OAuth externe.
URL du logo	URL du logo de l'application OAuth.
Type d'accord par défaut	Type d'accord par défaut utilisé pour établir le jeton. Les choix sont les suivants : ○ **Code d'autorisation** : Code qui est accordé au client pour obtenir un jeton d'accès, qui est ensuite utilisé pour obtenir l'accès à la ressource. Si vous sélectionnez cette option, vous avez besoin d'une URL d'autorisation (l'URL du serveur d'autorisation). ○ **Informations d'identification du mot de passe du propriétaire** de la ressource : nom d'utilisateur et mot de passe de l'utilisateur qui tente d'obtenir l'accès à la ressource. ○ **Informations d'identification du client** : l'ID et le secret du client, qui sont tous deux utilisés pour obtenir le jeton d'accès. Cette méthode ne fournit pas de jetons d'actualisation. ○ **Support JWT** : un serveur d'autorisation valide un jeton JWT qui permet de partager des informations d'identité et de sécurité entre les domaines de sécurité. ○ **Support SAML2** : génère l'assertion SAML2, puis échange l'assertion contre les jetons d'accès avec le fournisseur. **Remarque :** Pour la demande SuccessFactors sortante, utilisez le **support SAML2** comme type d'accord par défaut.
Durée de vie du jeton d'actualisation	Durée de validité du jeton d'actualisation, en secondes. La durée par défaut est de 8 640 000 secondes.
Client public	Permet aux clients publics d'exiger PKCE pour une autorisation. **Remarque :** Vous ne pouvez utiliser que le code d'autorisation `Default Grant type` lorsque PKCE est activé.
Méthode de contestation de code	Méthode de contestation de code utilisée dans le workflow PCKE OAuth. Les choix sont les suivants : ○ S256 [Par défaut] ○ Brut ○ Aucun
Commentaires	Ajoutez des commentaires concernant l'application OAuth.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Application et périmètre contenant cet enregistrement.
Accessible depuis	Rendez cette application accessible à partir de tous les périmètres de l'application ou à partir de ce périmètre uniquement.
Actif	Cochez la case pour rendre l'application active.
URL d'autorisation	Point de terminaison du code d'autorisation OAuth.
URL de jeton	Point de terminaison du jeton du serveur OAuth.
URL de révocation du jeton	Point de terminaison de révocation du jeton du serveur OAuth.
URL de redirection	Point de terminaison de rappel OAuth. Si le champ est vide, l'instance génère automatiquement une entrée.
Activer l'authentification réciproque	Cochez la case pour utiliser l'authentification réciproque pour la demande et la révocation de jeton. Cette fonctionnalité nécessite la spécification d'un profil d'authentification réciproque.
Envoyer les informations d'identification	Le client OAuth renseigne les informations d'identification du client dans la demande : ○ Dans le corps de la demande (codage URL de formulaire) ○ En-tête d'autorisation de base ○ En tant que clé privée JWT
Type de client	Choisissez le type de client en fonction du type de votre client. Options : ○ **Iframe incorporé** ○ **Intégration en tant qu'utilisateur** ○ **Intégration en tant que service** Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

Le système crée un enregistrement dans la table Registres d'application [oauth_entity] de type Fournisseur OAuth.

3. **Facultatif :** Accédez à la liste connexe de l'enregistrement Profils des entités OAuth pour valider un profil par défaut généré par le système pour le nouveau fournisseur OAuth sans champ d'application.
   Vous pouvez modifier ou ajouter un profil de fournisseur OAuth incluant le nom, le type d'accord et le champ d'application OAuth.
4. **Facultatif :** Accédez à la liste connexe de l'enregistrement Périmètres des entités OAuth pour définir tous les champs d'application OAuth disponibles pour ce fournisseur OAuth.
   Vous pouvez sélectionner les champs d'application lorsque vous créez ou mettez à jour un profil. Chaque champ d'application OAuth contient un nom et un champ d'application que vous devez obtenir à partir de la spécification du fournisseur, comme un champ de lecture ou un champ d'écriture. Chaque champ d'application doit être défini séparément.

Support JWT

Les jetons Web JSON (JWT) permettent de configurer les interactions d'API de serveur à serveur entre ServiceNow des fournisseurs d'API externes sans nécessiter d'intervention de l'utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’attribution au porteur de jeton Web JSON (JWT) est une chaîne JSON qui contient des valeurs de réclamation qui sont évaluées et validées par les gestionnaires d’octroi JWT du côté du serveur d’autorisation, avant d’émettre un jeton d’accès.

À l’aide du type d’attribution titulaire JWT, vous pouvez configurer le flux d’attribution titulaire OAuth 2.0 JWT pour le message rest sortant.

Configurer le fournisseur OAuth avec le type d’attribution JWT Bearer

Les jetons Web JSON (JWT) permettent de configurer les interactions d’API de serveur à serveur entre ServiceNow des fournisseurs d’API externes sans nécessiter d’intervention de l’utilisateur. Cette prise en charge permet d’effectuer Hub d'intégration d’autres tâches automatisées à l’aide de JWT pour configurer des intégrations d’API et de services avec différents fournisseurs.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Les tâches suivantes montrent comment ServiceNow il est possible de configurer l’utilisation de JWT pour l’authentification et les autorisations de client OAuth 2.0. ServiceNow est le client OAuth, et vous pouvez configurer un fournisseur OAuth, tel que Box ou Docusign.

Procédure

1. Charger le certificat de magasin de clés Java
   Joignez un certificat JKS à votre instance afin d’activer l’authentification client JWT.
2. Configurer une clé de signature JWT
   Créez une clé de signature JWT à affecter à votre certificat Java KeyStore (JKS).
3. Créer un fournisseur JWT avec une clé de signature JWT
   Ajoutez un fournisseur JWT à votre ServiceNow instance.
4. Se connecter à un fournisseur OAuth tiers
   Créez un fournisseur OAuth tiers avec un porteur JWT comme type d’attribution par défaut dans le registre d’application ServiceNow .
5. Spécifier un profil OAuth
   Ouvrez le profil d’entité OAuth du fournisseur OAuth et affectez un fournisseur JWT.

Charger le certificat de magasin de clés Java

Vous pouvez joindre un certificat Java KeyStore (JKS) à votre instance afin d’activer l’authentification client JWT.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Certificat x509**.
2. Remplissez le formulaire selon vos besoins.

Option	Description
Nom	Nom unique pour votre certificat.
Notification à l'expiration	Désignez la personne à notifier lorsque le certificat expire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Avertissement avant l'expiration (en jours)	Envoyez une notification par e-mail à votre gestionnaire de certificats avant l’expiration de votre certificat.
Actif	Active le certificat pour les demandes de jeton.
Type	Le type de certificat que vous chargez.
Échéance en jours	Nombre de jours avant l’expiration du certificat.
Mot de passe de magasin de clés	Mot de passe associé au certificat.
Description brève	

3. Cliquez sur **Envoyer**.

Configurer une clé de signature JWT

Créer une clé de signature JSON Web Token (JWT) à affecter à votre certificat Java KeyStore (JKS),

Avant de commencer

Rôle requis : administrateur

Remarque :
Si vous souhaitez ajouter **l’empreinte numérique du certificat X.509 SHA-1 int (x5t)** à l’en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ d’empreinte **numérique du certificat X.509 SHA-1 int (x5t).**

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Clés JWT**.
2. Remplissez le formulaire selon vos besoins.

Option	Description
Nom	Un nom unique pour votre configuration de signature de clé JWT.
Magasin de clés de signature	Le magasin de clés désigné lors de la signature de JWT.
ID clé	L’ID de clé (enfant) permet d’identifier la clé utilisée lorsque plusieurs clés sont utilisées pour signer des jetons. **Remarque :** Si vous configurez ce champ, la demande d’ID de clé est incluse dans le JWT. Si vous ne configurez pas ce champ, votre JWT n’aura pas de réclamation d’ID de clé.
Algorithme de signature	L’algorithme à utiliser pour signer avec la clé JWT. RSA 256 est le seul algorithme disponible.
Signature avec le mot de passe de clé	Mot de passe associé à la clé de signature.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Actif	Indiquez que l'alias de clé JWT est activement référencé à partir d'un fournisseur JWT.

3. Cliquez sur **Envoyer**.

Créer un fournisseur JWT avec une clé de signature JWT

Ajoutez un fournisseur JSON Web Token (JWT) à votre ServiceNow instance.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Fournisseur JWT**.
2. Remplissez le formulaire et cliquez sur **Soumettre**.

Option	Description
Nom	Nom unique pour la configuration de votre fournisseur JWT.
Intervalle d'expiration (s)	La durée de vie des jetons, en secondes, générés par le fournisseur JWT.
Configuration de la signature	Configuration ServiceNow de la clé de signature JWT à appliquer.

Générer un jeton Web JSON (JWT)

Créez un jeton Web JSON (JWT) pour représenter en toute sécurité des réclamations entre deux parties sur le Now Platform.

L'API GlideJWT est une API incluse dans le champ d'application et pouvant contenir des scripts qui génère un JWT. Trois arguments sont nécessaires avant de générer le JWT :

- Sys_id du fournisseur JWT
- En-tête sérialisé JSON
- Charge utile sérialisée JSON

Il existe deux scripts d'API JWT, JWTTokenInternal et JWTTokenRestricted, que vous pouvez utiliser lors de la configuration d'un fournisseur JWT. Le script JWTTokenRestricted permet aux administrateurs de configurer qui peut générer un JWT. Le script JWTTokenInternal est en lecture seule et permet uniquement aux utilisateurs connectés de générer un JWT.

Pour générer un JWT :

- Créer une clé JWT avec une clé partagée (HMAC) ou un magasin de clés de signature (RSA)
- Associer un fournisseur JWT à la configuration de signature faisant référence à une clé JWT

Vous pouvez utiliser l'API pour créer votre jeton.

Vous pouvez utiliser des réclamations standard et personnalisées lors de la configuration d'un fournisseur JWT. Vous pouvez transmettre des réclamations d'en-tête dynamique et de charge utile dans le cadre de la signature de l'API generateJWT.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de script pour tester l'API :

```
var jwtAPI = new sn_auth.GlideJWTAPI();
var headerJSON = {  "kid": "a1234"  };
var header = JSON.stringify(headerJSON);

var payloadJSON = { "jti": "testjti", "iss": "testiss", "sub": "testsub" };
var payload = JSON.stringify(payloadJSON);

var jwtProviderSysId = "7a40dde2d5303300964fb7c8f3c14ab5";
var jwt = jwtAPI.generateJWT(jwtProviderSysId, header, payload);

gs.info("JWT:" + jwt);
```

API clientes OAuth

L'API cliente OAuth fournit des méthodes pour demander et révoquer des jetons OAuth.

Le client OAuth fournit les classes suivantes :

- GlideOAuthClient : méthodes de demande et de révocation des jetons d'actualisation et d'accès.
- GlideOAuthClientRequest : méthodes de gestion des demandes client.
- GlideOAuthClientResponse : méthodes de gestion des réponses des clients.
- GlideOAuthToken : méthodes pour récupérer le jeton d'accès et les informations relatives au jeton d'accès.

Vous pouvez également personnaliser l'include de script OAuthUtil pour intercepter les paramètres de requête et analyser les réponses des fournisseurs OAuth externes.

Lorsque vous utilisez des classes OAuth dans un script inclus dans le champ d'application, utilisez l'identificateur d'espace de noms sn_auth.

Paramètres OAuth pour la prise en charge des profils par défaut

La fonctionnalité de profil par défaut nécessite un ensemble de paramètres que vous pouvez utiliser avec l'API `setParameter()` pour spécifier le demandeur OAuth, un contexte pour la demande et le profil du fournisseur.

Dans le scénario du fournisseur OAuth, vous devez définir trois paramètres qui indiquent au fournisseur OAuth quel profil OAuth utiliser par défaut. Lorsque ces trois paramètres sont définis, le jeton d'accès est enregistré dans la base de données de l'instance. Utilisez les paramètres avec `GlideOAuthClientRequest`.

Paramètres OAuth pour la prise en charge des profils par défaut

Paramètre	Description
oauth_requestor	sys_id de l'objet, qui peut être un enregistrement utilisateur ou un compte de messagerie.
oauth_requestor_context	Descripteur qui fournit le contexte pour le demandeur OAuth. Il est recommandé d'utiliser le nom de la table dans laquelle l'objet oauth_requestor est enregistré.
oauth_provider_profile	L'sys_id de l'enregistrement de profil OAuth qui est la valeur par défaut (voir Spécifier un profil OAuth).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous n’avez pas besoin d’utiliser de paramètres pour définir le type d’accord et le champ d’application, car les valeurs sont configurées dans l’enregistrement du profil OAuth. Si vous n’utilisez pas les paramètres, vous pouvez utiliser les méthodes d’API GlideOAuthClientRequest `setScope` et `setGrantType`. Pour plus d’informations, consultez setScope et setGrantType .

Clé privée Prise en charge JWT de l’authentification client OAuth 2.0

Prise en charge JWT Prise en charge de l’authentification client OAuth 2.0.

Clé privée L’authentification client JWT est une méthode d’authentification qui peut être utilisée par les clients pour s’authentifier auprès du serveur d’autorisation lors de l’utilisation du point de terminaison de jeton.

Dans ce mécanisme d’authentification, seuls les clients qui ont enregistré une clé publique et signé un JWT à l’aide de cette clé peuvent s’authentifier.

Le JWT doit contenir des valeurs de réclamation REQUISES et peut contenir des valeurs de réclamation FACULTATIVES. Pour en savoir plus sur les valeurs de réclamation requises pour le JWT pour l’authentification private_key_jwt , reportez-vous à la section Authentification client de la documentation principale d’OpenID Connect .

Remarque :
Le jeton d’authentification doit être envoyé comme la valeur du paramètre client_assertion. La valeur du paramètre **client_assertion_type** doit être urn :ietf :params :oauth :client-assertion-type :jwt-bearer.

Modules d’extension requis pour l’authentification client OAuth 2.0 à l’aide du jeton JWT :

- **OAuth 2.0 (com.snc.platform.security.oauth)** : ce module d’extension est actif sur les instances nouvelles et mises à niveau. Si le module d’extension n’est pas actif sur votre instance, vous pouvez l’activer.
- **Intégration : programme d’installation de l’authentification unique de plusieurs fournisseurs (com.snc.integration.sso.multi.installer)** : pour le cas d’utilisation de l’authentification unique basée sur OIDC.

Vous pouvez utiliser l’authentification client OAuth 2.0 à l’aide de la clé privée JWT pour les actions suivantes :

- Authentification unique basée sur OIDC
- Intégrations OAuth sortantes

Configurer la clé privée JWT pour la SSO basée sur OIDC

Configurez la clé privée JWT pour les intégrations SSO basées sur OIDC.

Avant de commencer
Rôle requis : administrateur

Vous devez effectuer les tâches suivantes avant de choisir la clé privée JWT pour l’authentification unique basée sur OIDC.

- Charger le certificat de magasin de clés Java: joignez un certificat JKS à votre instance afin d’activer l’authentification du client JWT.
- Configurer une clé de signature JWT: créez une clé de signature JWT à affecter à votre certificat Java KeyStore (JKS).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

> **Remarque :**
> Si vous souhaitez ajouter **l'empreinte numérique du certificat X.509 SHA-1 int (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ d'empreinte **numérique du certificat X.509 SHA-1 int (x5t).**

- Créer un fournisseur JWT avec une clé de signature JWT: ajouter un fournisseur JWT à votre ServiceNow instance.

Pour inclure une clé JWT pour le fournisseur d'identité OIDC, vous devez :

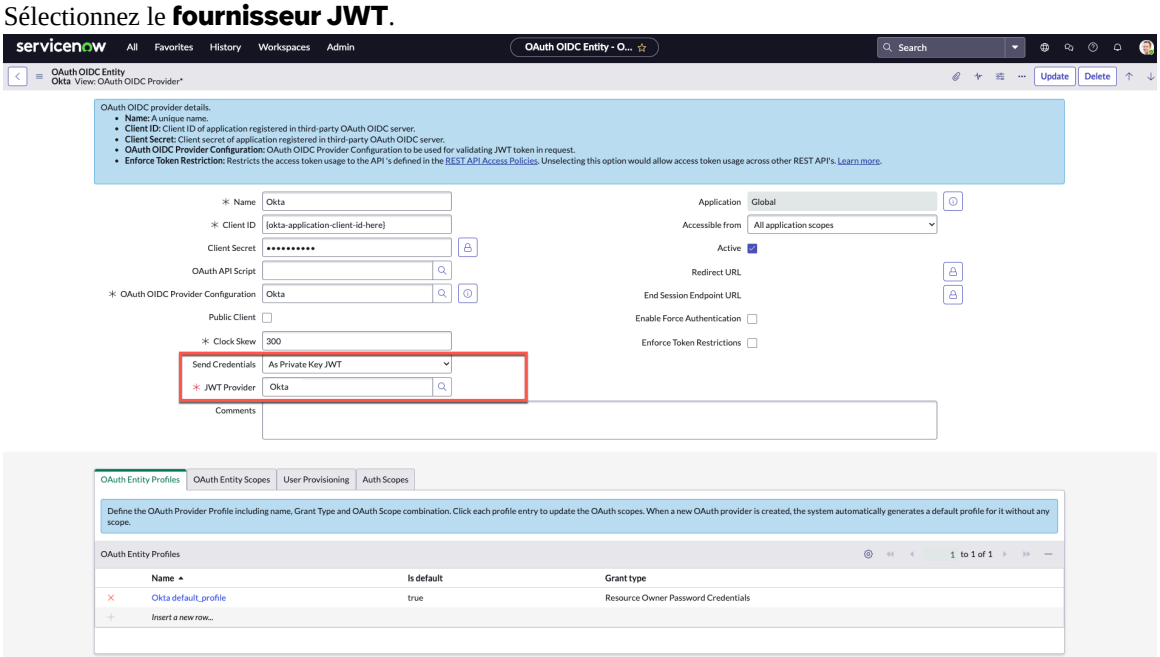
- Installez le module **d'extension Intégration - Programme d'installation de l'authentification unique de plusieurs fournisseurs** (com.snc.integration.sso.multi.installer).
- Activez les propriétés pour **plusieurs propriétés SSO de fournisseur**. Pour plus d'informations, consultez Propriétés, tables et scripts SSO de plusieurs fournisseurs.
- Créer un fournisseur d'identité OIDC. Pour plus d'informations, consultez Créer une configuration OpenID Connect (OIDC) pour Single Sign-On (SSO).

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application**.
2. Sélectionnez le fournisseur d'identité OIDC que vous avez créé.
3. En haut du formulaire, sélectionnez **Configurer** > **Conception de formulaire**.

> **Remarque :**
> Vous devez ajouter **les champs Envoyer les informations d'identification** et **Fournisseur JWT** au formulaire pour utiliser la clé privée JWT pour les demandes d'authentification du fournisseur d'identité basées sur OIDC.

4. Choisir la **clé privée JWT** pour envoyer les informations d'identification.
5. Sélectionnez le **fournisseur JWT**.



Lorsque l'utilisateur s'authentifie, la page d'authentification dispose d'options permettant de se connecter via Okta.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer la clé privée JWT pour OAuth sortant

Configurez la clé privée JWT pour les intégrations OAuth sortantes.

Avant de commencer
Rôle requis : administrateur

Avant de configurer la clé privée JWT pour les intégrations OAuth sortantes, vous devez effectuer les tâches suivantes :

- Charger le certificat de magasin de clés Java: joignez un certificat JKS à votre instance afin d'activer l'authentification du client JWT.
- Configurer une clé de signature JWT: créez une clé de signature JWT à affecter à votre certificat Java KeyStore (JKS).

> **Remarque :**
> Si vous souhaitez ajouter **l'empreinte numérique du certificat X.509 SHA-1 int (x5t)** à l'en-tête dans le cadre de la clé JWT, vous devez configurer le formulaire et ajouter le champ d'empreinte **numérique du certificat X.509 SHA-1 int (x5t).**

- Créer un fournisseur JWT avec une clé de signature JWT: ajouter un fournisseur JWT à votre ServiceNow instance.

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application** , puis cliquez sur **Nouveau**.
2. Sur la page de l'intercepteur, cliquez sur **Se connecter à un fournisseur OAuth tiers**, puis renseignez le formulaire.

> **Remarque :**
> Vous devez ajouter **les champs Envoyer les informations d'identification** et **Fournisseur JWT** au formulaire pour utiliser la clé privée JWT pour les demandes d'authentification OAuth sortantes.

Champ	Description
Nom	Nom unique de la connexion OAuth tierce.
ID client	ID client de l'application enregistré dans le serveur OAuth tiers.
Secret client	Clé secrète client de l'application enregistrée dans le serveur OAuth tiers.
Script de l'API OAuth	Script utilisé pour personnaliser les demandes et les réponses adressées au fournisseur OAuth externe.
URL du logo	URL du logo de l'application OAuth.
Type d'accord par défaut	Choisissez : **Informations d'identification du client** : l'ID et le secret client, qui sont tous deux utilisés pour obtenir le jeton d'accès. Cette méthode ne fournit pas de jetons d'actualisation.
Durée de vie du jeton d'actualisation	Durée de validité du jeton d'actualisation, en secondes. La durée par défaut est de 8 640 000 secondes.
Client public	Permet aux clients publics d'exiger PKCE pour une autorisation.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Vous ne pouvez utiliser que le code d'autorisation `Default Grant type` lorsque PKCE est activé.
Commentaires	Ajoutez des commentaires concernant l'application OAuth.
Application	Application et périmètre contenant cet enregistrement.
Accessible depuis	Rendez cette application accessible à partir de tous les périmètres de l'application ou à partir de ce périmètre uniquement.
Actif	Cochez la case pour rendre l'application active.
URL d'autorisation	Point de terminaison du code d'autorisation OAuth.
URL de jeton	Point de terminaison du jeton du serveur OAuth.
URL de révocation du jeton	Point de terminaison de révocation du jeton du serveur OAuth.
URL de redirection	Point de terminaison de rappel OAuth. Si le champ est vide, l'instance génère automatiquement une entrée.
Activer l'authentification réciproque	Cochez la case pour utiliser l'authentification réciproque pour la demande et la révocation de jeton. Cette fonctionnalité nécessite la spécification d'un profil d'authentification réciproque.
Envoyer les informations d'identification	Choisir : **En tant que clé privée JWT**
Fournisseur JWT	Détails du fournisseur JWT. Vous pouvez utiliser la recherche pour sélectionner le fournisseur JWT.

Le système crée un enregistrement dans la table Registres d'application [oauth_entity] avec le type Fournisseur OAuth qui peut être utilisé pour l'authentification de clé JWT privée.

Créer un message REST sortant

Créez un message REST sortant pour autoriser l'instance en tant que serveur d'autorisation.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Services web du système** > **Sortant** > **Message REST** , puis cliquez sur **Nouveau**.
2. Renseignez les champs de formulaire de l'enregistrement d'application OAuth, comme décrit à la section . Notez les valeurs de champ suivantes :
   - **Point de terminaison** : URL de l'instance qui est le serveur d'autorisation.
   - **Type d'authentification** : **OAuth 2.0**.
   - **Profil OAuth** : profil OAuth que vous avez créé pour le serveur client.
3. Sur l'enregistrement du message REST, cliquez sur **Obtenir le jeton OAuth**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Authentifiez-vous avec l'instance qui fournit le jeton ; la méthode dépend de l'intégration de l'authentification unique.
   Vous pouvez utiliser :
   - Nom d'utilisateur et mot de passe utilisés pour vous authentifier à l'instance.
   - Le nom d'utilisateur et le mot de passe de l'IdP sont activés. Cliquez sur **Utiliser une connexion externe** pour accéder à l'écran de connexion IdP.

     Remarque :
     Pour être automatiquement redirigé vers la page de connexion d'IdP, vous devez définir la propriété système glide.authenticate.external.

   - Votre code, si la MFA est activée.
5. Cliquez sur **Autoriser** ou **Refuser** pour terminer l'autorisation et émettre les jetons.
   Le processus qui suit est décrit à la section Flux d'octroi de code d'autorisation OAuth.

S'inscrire automatiquement dans l'instance ServiceNow

Utilisez l'auto-inscription des utilisateurs externes pour intégrer un grand volume d'utilisateurs externes à votre instance. Cette fonctionnalité améliore la vérification d'identité pour améliorer l'expérience client et prend en charge les flux d'inscription couramment utilisés.

Explorer	Activer
	
Découvrez les fonctionnalités et la valeur commerciale de l'inscription automatique.	Découvrez comment activer l'auto-enregistrement externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer



Configurez l’auto-enregistrement.

Activer



Renseignez-vous sur les propriétés dans Self-register.

Traduction automatique

Explorer l’auto-enregistrement

Utilisez l’auto-inscription des utilisateurs externes pour intégrer un grand volume d’utilisateurs externes à votre instance. Cette fonctionnalité améliore la vérification d’identité pour améliorer l’expérience client et prend en charge les flux d’inscription couramment utilisés.

L’auto-inscription des utilisateurs externes permet à un grand groupe d’utilisateurs de s’inscrire à une ServiceNow application sans l’aide d’un administrateur. Par exemple, une université avec un grand groupe d’étudiants ayant besoin d’un parking sur le campus pourrait s’inscrire à l’application de stationnement du campus. Chaque étudiant se verrait accorder un ensemble limité de privilèges spécifiques au stationnement et suivrait un processus d’inscription automatisé. Ce système pouvait générer un numéro de stationnement, unique à chaque élève, et s’assurer qu’ils disposaient d’une place de stationnement.

Un flux d’auto-inscription se compose d’une application personnalisée ServiceNow , dans ce cas, une application de stationnement de campus. Après avoir configuré une application avec les tables nécessaires, un administrateur configurerait l’inscription, y compris un flux de pré-inscription, un mappage de champs, un mappage de post-inscription, un captcha, un mappage de rôles et un flux de post-inscription.

Activation de l’auto-inscription de l’utilisateur externe

Vous pouvez activer le module d’extension d’auto-inscription de l’utilisateur externe (com.snc.external_user_self_registration) si vous disposez du rôle administrateur.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Trouvez le module d'extension à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

   Un message s'affiche une fois l'installation terminée.

Rôles externes dans l'auto-inscription

Pour éviter de fournir l'accès par inadvertance à des utilisateurs externes, vous pouvez affecter le rôle snc_external à tous les utilisateurs externes.

Les utilisateurs externes qui s'enregistrent automatiquement doivent se voir affecter le rôle snc_external qui dispose du moins de privilèges. Le rôle snc_external indique que l'utilisateur est externe à votre organisation et ne doit pas avoir accès aux ressources à moins d'y être explicitement autorisé par les ACL pour le rôle snc_external ou pour des rôles supplémentaires qui héritent du rôle snc_external.

Par défaut, les utilisateurs dotés du rôle snc_external ne peuvent pas accéder aux éléments suivants :

- Ressources Scripted REST API qui ne sont pas marquées comme étant externes.
- Tables sans le rôle qui hérite du rôle snc_external ou du rôle public.
- Ressources qui ne sont pas de type Enregistrement, telles que les processeurs et les pages de l'interface utilisateur sans le rôle snc_external ou un rôle qui hérite du rôle snc_external.
- Tableaux de bord Platform Analytics.

À partir de la version Paris, vous devez activer une propriété de liste d'exclusion pour appliquer l'affectation explicite de snc_external rôles. Pour plus d'informations sur l'activation de la propriété, voir Empêcher les futures affectations de rôles internes pour les utilisateurs externes .

Configuration d'une configuration d'inscription utilisateur pour les utilisateurs externes

Créez un enregistrement de configuration de l'inscription de l'utilisateur pour amorcer le processus d'intégration des utilisateurs externes aux applications personnalisées

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow . Ce formulaire guide les utilisateurs externes tout au long du processus d'auto-inscription.

Avant de commencer

- Rôle requis : administrateur
- Activation de l'auto-inscription de l'utilisateur externe

Procédure

1. Accédez à la **Tout** > **Enregistrement utilisateur externe automatique** > **Configurations de l'inscription de l'utilisateur** et cliquez sur **Nouveau**.
2. Renseignez les champs du formulaire.

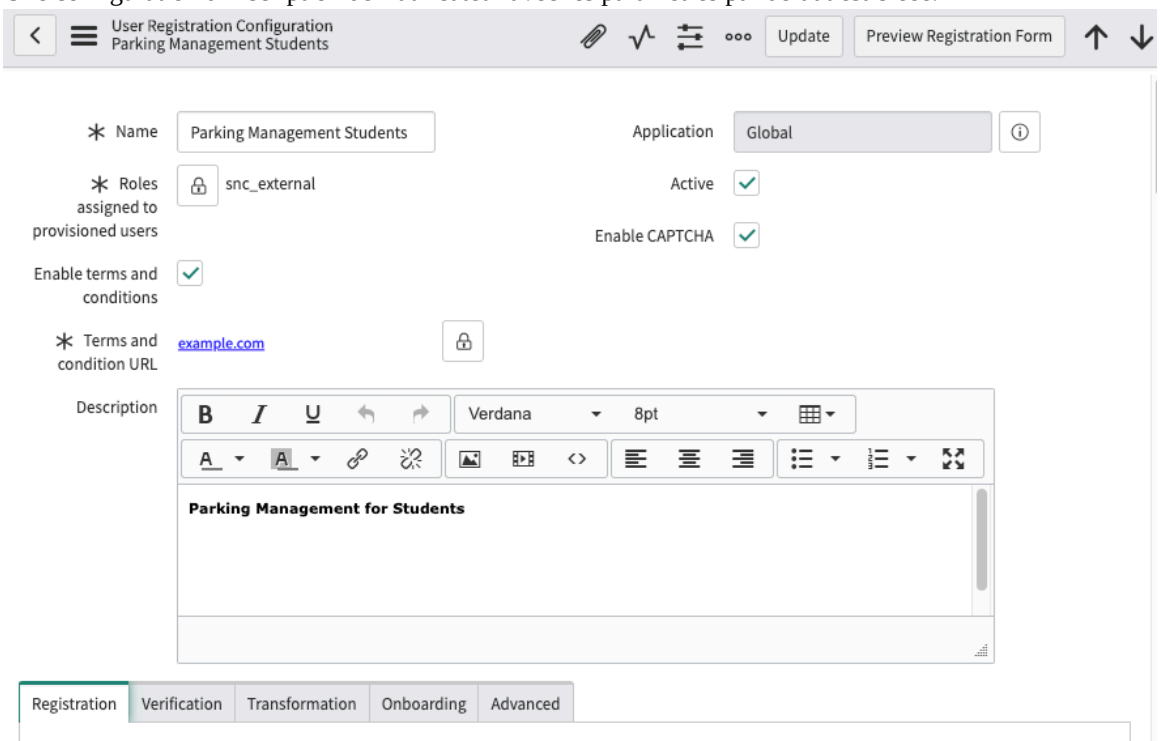
Formulaire de configuration de l'inscription de l'utilisateur

Champ	Description
Nom	Nom du formulaire d'inscription. Par exemple, une inscription de stationnement pour étudiants peut être Étudiants en gestion du stationnement.
Rôles appliqués aux utilisateurs attribués	Rôles affectés aux utilisateurs provisionnés. Les rôles spécifiés doivent étendre ou contenir le rôle `snc_external` . Le rôle spécifié peut également être `snc_external` rôle. Pour les utilisateurs externes, chaque rôle doit disposer d'un `snc_external` pour noter un utilisateur externe. Si vous disposez de rôles préconfigurés, les rôles doivent être accessibles lorsque vous déverrouillez les rôles et recherchez des utilisateurs.
Activer les termes et conditions	Option permettant d'ajouter une URL de termes et conditions à la page d'inscription.
URL des termes et conditions	URL publiquement accessible qui contient les termes et conditions du formulaire d'inscription. Ce champ s'affiche uniquement lorsque **l'option Activer les termes et conditions** est sélectionnée.
Description	Description du formulaire d'inscription. Ce champ s'affiche uniquement lorsque vous enregistrez ou soumettez la configuration. Vous pouvez ajouter plus d'informations sur le formulaire d'inscription dans ce champ. **Remarque :** Vous ne pouvez ajouter une description qu'après avoir enregistré ou mis à jour une configuration d'inscription utilisateur.
Application	Application contenant cet enregistrement. L'application est automatiquement définie sur `Global`.
Actif	Option qui active la configuration de l'inscription de l'utilisateur. Cette option est sélectionnée par défaut.
Activer CAPTCHA	Possibilité d'ajouter un CAPTCHA au formulaire d'inscription. Le fournisseur CAPTCHA par défaut est Google reCAPTCHA. **Remarque :** Pour activer CAPTCHA pour l'enregistrement de l'utilisateur, suivez les étapes de la section Configurer Google reCAPTCHA pour l'auto-inscription de l'utilisateur externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Cliquez sur **Envoyer**.
Une configuration d'inscription de l'utilisateur avec les paramètres par défaut est créée.



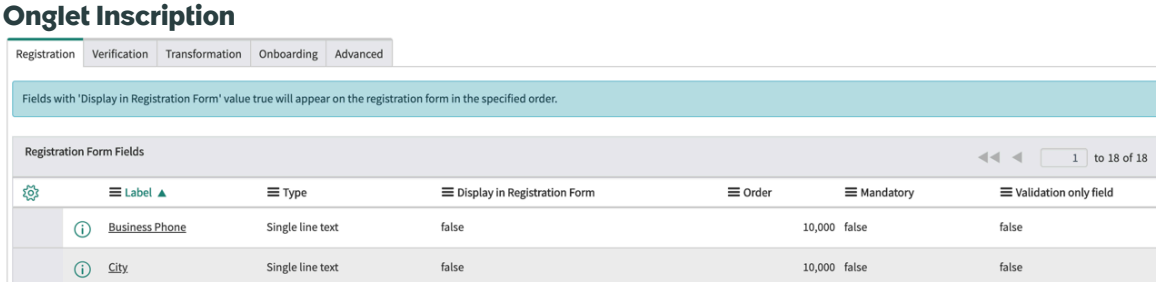
4. Facultatif : Configurez l'onglet **Inscription** pour afficher les champs et leur ordre d'apparition :

Champs de formulaire d'inscription

Colonne	Description
Afficher dans le formulaire d'inscription	Définissez n'importe quel champ que vous souhaitez afficher comme Vrai.
Ordre	Définissez un numéro d'ordre pour afficher les champs sur votre formulaire.
Obligatoire	Définissez n'importe quel champ que vous souhaitez rendre obligatoire sur Vrai.
Champ de validation uniquement	Définissez un champ que vous souhaitez utiliser uniquement pour la validation. Par exemple, le code d'inscription.

Vous pouvez choisir d'afficher les champs de formulaire par défaut ou d'ajouter des champs de formulaire personnalisés au formulaire d'inscription. Pour plus d'informations, consultez Champs de formulaire d'inscription par défaut.

Onglet Inscription



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

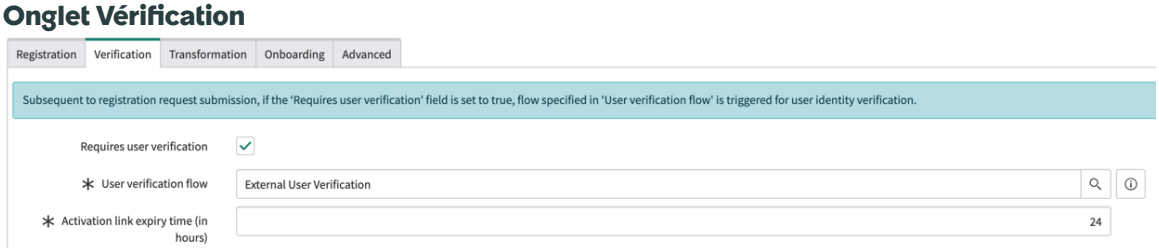
Vous pouvez également ajouter des champs de formulaire d’inscription personnalisés. Pour plus d'informations, consultez Ajouter un champ de formulaire d’inscription personnalisé.

5. **Facultatif :** Configurez l'onglet **Vérification** pour vérifier l'identité des utilisateurs enregistrés. Lorsque le flux de vérification de l’utilisateur se déclenche, un lien d’activation est envoyé à l’adresse e-mail enregistrée de l’utilisateur.

Champs de l’onglet Vérification

Champ	Description
Requiert une vérification de l'utilisateur	Option permettant de déclencher un flux secondaire de vérification de l’utilisateur qui s’exécute après l’inscription de l’utilisateur. Le flux secondaire est destiné à la vérification de l’identité de l’utilisateur.
Flux de vérification de l'utilisateur	Flux secondaire utilisé pour vérifier l’identité de l’utilisateur. Le flux secondaire se déclenche uniquement lorsque vous activez la vérification de l’utilisateur. (Optional) Le flux secondaire **Vérification de l’utilisateur externe** est disponible par défaut. Vous pouvez créer une copie du flux secondaire par défaut dans Studio de workflow et le modifier en fonction de vos besoins. Pour en savoir plus, reportez-vousFlow Designer à . **Remarque :** Pour prévisualiser le flux secondaire de **vérification de l’utilisateur externe** dans un nouvel onglet, utilisez les raccourcis suivants : ○ Macintosh : Commande + clic ○ Windows : Ctrl + clic
Délai d'expiration du lien d'activation (en heures)	Nombre d’heures après l’expiration d’un lien d’activation. La valeur par défaut est 24.

Onglet Vérification

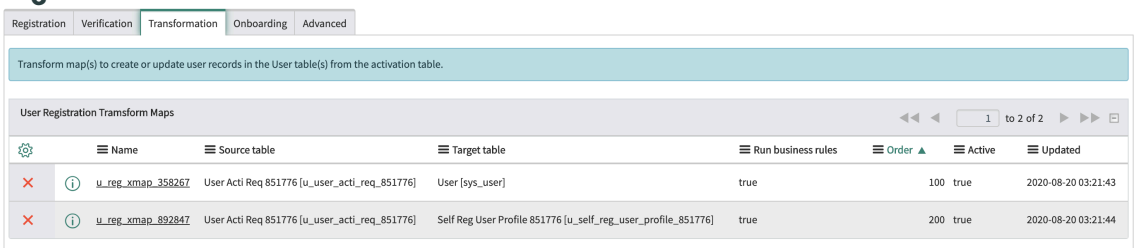


6. **Facultatif :** Configurez l’onglet **Transformation** pour mapper les utilisateurs enregistrés automatiquement et les utilisateurs activés.
Il existe deux cartes de transformation (u_reg_xmap_[numéro]) qui mappent automatiquement les utilisateurs enregistrés à partir de la table Acti Req [numéro] de l’utilisateur à la table [numéro] de l’utilisateur enregistré automatiquement. Vous pouvez créer une copie de ces cartes de transformation par défaut et les modifier en fonction de vos besoins. Pour plus d’informations, reportez-vous à la rubrique Cartes de transformation .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

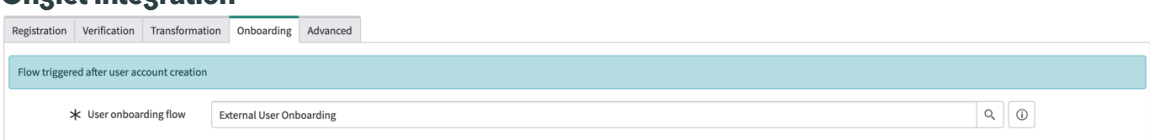
Onglet Transformation



7. Configurez l'onglet **Intégration** pour déclencher des flux secondaires pour les utilisateurs activés en intégration.
   Le flux secondaire **d'intégration d'utilisateur externe** par défaut envoie un e-mail à l'utilisateur contenant un lien pour réinitialiser son mot de passe. Vous pouvez créer une copie du flux secondaire par défaut et le modifier en fonction de vos besoins.

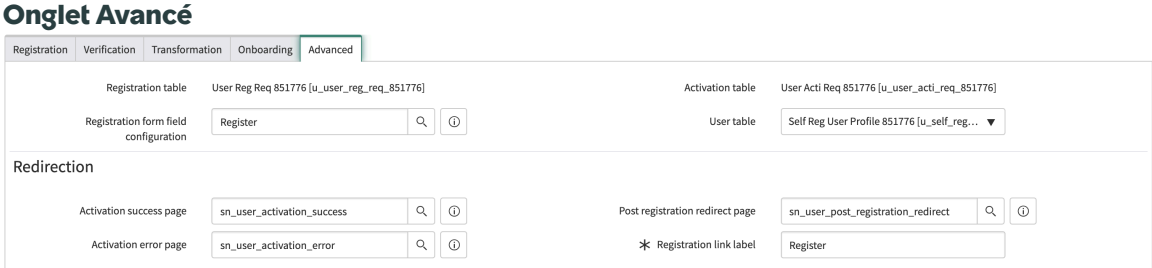
   Remarque :
   Lorsque le flux secondaire **Intégration de l'utilisateur externe** se déclenche, il envoie un e-mail à l'utilisateur contenant un lien pour réinitialiser le mot de passe.

Onglet Intégration



8. **Facultatif :** Configurez l'onglet **Avancé** pour mapper les tables d'utilisateurs et les pages de redirection du formulaire d'inscription.

Onglet Avancé



Onglet Avancé

Champ	Description
Table d'inscription	Nom de la table dans laquelle les informations du formulaire d'inscription sont enregistrées.
Configuration du champ du formulaire d'inscription	Enregistrement associé au formulaire d'inscription dans le créateur d'enregistrement.
Table d'activation	Étiquette et nom de la table utilisée pour l'activation de l'utilisateur. La table d'activation contient les enregistrements des utilisateurs qui ont terminé la vérification.
Table des utilisateurs	Étiquette et nom de la table des profils d'utilisateurs.
Page de réussite d'activation	Page vers laquelle un utilisateur est redirigé après la réussite de l'activation.

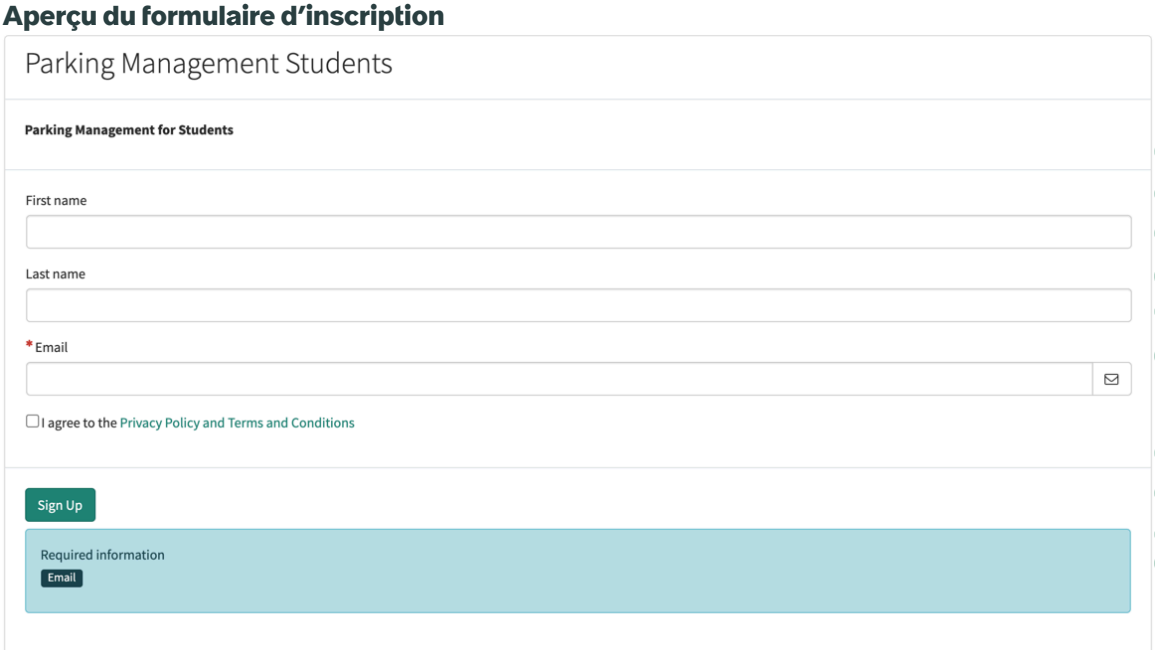
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Page d'erreur d'activation	Page vers laquelle un utilisateur est redirigé lorsque l'activation échoue.
Page de redirection post-inscription	Page vers laquelle l'utilisateur est redirigé après son inscription.
Étiquette de lien d'inscription	Nom du bouton utilisé pour l'inscription à partir du portail de services. La valeur par défaut est Register.

Lorsque vous apportez des modifications ou que toutes les modifications sont terminées dans la configuration de l'inscription de l'utilisateur, vous pouvez utiliser le bouton **Afficher un aperçu du formulaire d'inscription** pour prévisualiser les modifications apportées au formulaire d'inscription.

Aperçu du formulaire d'inscription



Traduction automatique

Configurer Google reCAPTCHA pour l'auto-inscription de l'utilisateur externe

Pour utiliser le Google reCAPTCHA service, vous devez demander une paire de clés API à partir de Google la propriété système connexe, puis la configurer.

Avant de commencer

- Demandez une paire de clés API (une clé de site et un secret) à partir de Google au https://www.google.com/recaptcha .
- Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Procédure

1. Accédez à la **Tout** > **Propriétés système** > **Toutes les propriétés**.
2. Recherchez les propriétés suivantes et définissez les valeurs :

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Valeur
glide.user.registration.google.recaptcha.secret	Le secret autorise la communication entre l'application et le serveur reCAPTCHA. Type : password2
glide.user.registration.google.recaptcha.site_key	Clé de site utilisée pour appeler le service reCAPTCHA sur votre page d'inscription. Type : chaîne
glide.user.registration.captcha.widget	Sys_ID du widget captcha. Type : chaîne

Champs de formulaire d'inscription par défaut

Vous pouvez utiliser les champs de formulaire d'inscription par défaut ou créer des champs de formulaire d'inscription personnalisés.

Champs de formulaire d'inscription

Les champs de formulaire suivants sont ajoutés par défaut dans le formulaire d'inscription.

Étiquette de champ	Type
Tél. professionnel	Texte sur ligne unique
Ville	Texte sur ligne unique
Pays	Zone de sélection
État d'EDU Utilisé pour différencier le personnel, les étudiants et les visiteurs. **Remarque :** Ce champ est utile lorsque le formulaire d'inscription est destiné à un établissement d'enseignement.	Zone de sélection
E-mail	E-mail
Prénom	Texte sur ligne unique
Genre	Texte sur ligne unique
Téléphone du domicile	Texte sur ligne unique
Langue	Zone de sélection
Nom de famille	Texte sur ligne unique
Deuxième prénom	Texte sur ligne unique

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Étiquette de champ	Type
Tél. mobile	Texte sur ligne unique
Nom	Texte sur ligne unique
Préfixe Titre de l'utilisateur. Par exemple, M. , Dr , etc.	Zone de sélection
État / Province	Texte sur ligne unique
Rue	Texte sur ligne unique large
Titre : fonction	Zone de sélection
Code postal	Texte sur ligne unique

Remarque :
Vous ne pouvez pas supprimer les champs de formulaire d'inscription par défaut.

Ajouter un champ de formulaire d'inscription personnalisé

Vous pouvez ajouter des champs personnalisés dans le formulaire d'auto-inscription de l'utilisateur.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Enregistrement utilisateur externe automatique** > **Configurations de l'inscription de l'utilisateur**.
2. Ouvrez l'enregistrement pour la configuration d'inscription d'utilisateur requise.
3. Naviguez jusqu'à la fin de la section Champs du formulaire d'inscription et cliquez sur **Insérer une nouvelle ligne.**
4. Saisissez le nom du champ sous la colonne **Étiquette** et cliquez sur Coche.
   Une nouvelle ligne est ajoutée avec les valeurs par défaut. Vous pouvez configurer le champ de formulaire d'inscription personnalisé en fonction de vos besoins.

Colonnes de champ de formulaire d'inscription

Colonne	Description
Étiquette	Le nom du champ qui apparaît sur le formulaire d'inscription.
Type	Type de l'élément d'interface utilisateur. Les types pris en charge sont les suivants : ○ Texte sur ligne unique ○ E-mail ○ Date ○ Date/Heure ○ Oui/Non ○ Texte sur ligne unique large

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Colonne	Description
	○ Choix multiple ○ Zone de sélection
Afficher dans le formulaire d'inscription	Option permettant d'afficher le champ dans le formulaire d'inscription.
Ordre	Séquence dans laquelle les champs de formulaire apparaissent sur le formulaire d'inscription. Le champ dont la valeur d'ordre est la plus basse apparaît en premier et celui dont la valeur d'ordre est la plus élevée apparaît en dernier. La valeur par défaut est 10 000.
Obligatoire	Possibilité de rendre un champ obligatoire sur le formulaire d'inscription.
Champ de validation uniquement	Option permettant d'utiliser un champ uniquement à des fins de validation. Par exemple, le code d'inscription. Lorsqu'elle est définie sur vrai, ce champ n'est pas enregistré dans la table des utilisateurs (sys_user).

5. Enregistrez ou mettez à jour les changements.

Activer l'auto-inscription de l'utilisateur externe pour Portail de services

Autorisez les utilisateurs externes à s'inscrire à une application ServiceNow via Portail de services.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Portail de services** > **Portails**.
2. Ouvrez un enregistrement de portail.
3. Renseignez le champ Configuration de **l'inscription de l'utilisateur externe** sur le formulaire.

   Sélectionnez une configuration d'inscription utilisateur.
4. Cliquez sur **Mettre à jour**.

Résultats

Le widget de connexion inclut un lien vers le formulaire d'inscription que vous avez configuré au préalable.

Vérifier les demandes d'auto-inscription de l'utilisateur

Une fois qu'un utilisateur s'est inscrit à partir du Portail de services , un enregistrement utilisateur est ajouté au module Demandes d'enregistrement. Vous pouvez afficher la liste des utilisateurs enregistrés avec succès dans le Portail de services fichier .

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Enregistrement utilisateur externe automatique** > **Demandes d'enregistrements**.
   La liste des enregistrements utilisateur s'affiche.
2. (Facultatif) Affichezles enregistrements des utilisateurs individuels et modifiez-les en fonction de vos besoins. Par exemple, vous pouvez modifier l'état d'un formulaire d'enregistrement utilisateur **En attente** en **Traité**.

Authentification basée sur un jeton (connexions de l'utilisateur)

Améliorez le mécanisme de sécurité permettant aux utilisateurs d'accéder à un réseau à l'aide d'une authentification basée sur un jeton.

Authentification temporelle limitée



L'authentification basée sur un jeton est un protocole qui permet aux utilisateurs de vérifier leur identité et de recevoir en retour un jeton d'accès unique.

Il permet d'améliorer le mécanisme de sécurité permettant aux utilisateurs d'accéder à un réseau.

Utilisation de l'authentification du jeton Digest



L'authentification par jeton Digest transmet les informations d'identification de l'utilisateur et un jeton Digest dans un en-tête HTTP non chiffré.

Traduction automatique

Authentification temporelle limitée

Prend en charge l'authentification limitée dans le temps pour votre ServiceNow instance.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l’authentification temporelle limitée.

Activer



Découvrez comment activer l’authentification limitée en temps.

Didacticiel : Authentification temporelle limitée



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

En savoir plus sur les propriétés de l'accès Zero Trust.

Exploration de l'authentification temporelle limitée

Prend en charge l'authentification limitée dans le temps pour votre ServiceNow instance.

Remarque :
L'authentification temporelle limitée est très spécifique à l'instanceServiceNow. Les liens personnalisés pour les utilisateurs ne peuvent être créés que dans .ServiceNow

Les administrateurs peuvent configurer l'authentification basée sur le lien sur l'instance ServiceNow . Le lien configuré peut être partagé avec l'utilisateur par e-mail ou SMS. L'utilisateur peut utiliser ces liens pour se connecter à l'instance.

La connexion à l'instance avec ce schéma d'authentification est contrôlée via les politiques d'authentification adaptative configurées sur l'instance ServiceNow .

L'authentification basée sur le temps vous permet d'effectuer les actions suivantes :

- L'administrateur peut configurer l'authentification basée sur le lien pour l'utiliser dans un délai d'expiration.
- L'équipe d'application peut extraire la valeur de circonstance à utiliser avec le lien pour l'élément de configuration spécifique à l'aide de l'API scriptable exposée. La génération de liens sera prise en charge par l'équipe d'application.
- L'équipe d'application peut générer le lien et l'envoyer à l'utilisateur via un canal existant.
- L'utilisateur disposant du lien peut se connecter à l'instance une seule fois et dans le délai d'expiration spécifié dans le cadre de la configuration.
- Les administrateurs peuvent configurer les rôles avec peu de privilèges pour le schéma d'authentification.
- Les administrateurs peuvent appliquer la MFA pour le schéma d'authentification comme deuxième facteur pour l'authentification avec la liaison TLA.

Activer l'authentification limitée en temps

L'authentification limitée dans le temps s'active via le module d'extension Intégration - programme d'installation de l'authentification unique de plusieurs fournisseurs.

Avant de commencer
Rôle requis : administrateur

Remarque :
L'authentification temporelle limitée est très spécifique à l'instanceServiceNow. Les liens personnalisés pour les utilisateurs ne peuvent être créés que dans .ServiceNow

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtrage et la barre de recherche pour rechercher le module *d'extension* Time Limited Authentication (com.snc.authenticate.time_limited_authentication).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

> **Remarque :**
> Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Authentification temporelle limitée par SMS - Twilio Tutoriel

Configurez une authentification temporelle limitée à l'aide de facteurs MFA tels que SMS à l'aide de Twilio.

Avant de commencer

Rôle requis : administrateur

Modules d'extension requis :

- *com.snc.authenticate.time_limited_authentication* (authentification temporelle limitée)
- *com.snc.authentication.sms_mfa* (authentification multifacteur par SMS)

> **Remarque :**
> L'authentification temporelle limitée (TLA) est très spécifique à l'instanceServiceNow. Les liens personnalisés pour les utilisateurs ne peuvent être créés que dans .ServiceNow

Les instructions du didacticiel fournies permettent à l'administrateur de fournir une connexion basée sur un lien avec SMS comme deuxième facteur (MFA) pour les utilisateurs ayant un rôle spécifique.

Une fois la configuration réussie, le système génère un lien, puis le partage avec l'utilisateur via le canal de notification (e-mail/SMS). En cliquant sur le lien, l'utilisateur est invité à spécifier le facteur OTP envoyé à E-mail ou SMS en fonction du rôle d'utilisateur (configuration).

> **Remarque :**
> - TLA doit toujours être suivi par MFA et MFA doit être activé par l'administrateur à l'aide de l'authentification adaptative pour la connexion TLA. Pour en savoir plus sur la configuration de l'authentification MFA avec Adaptive Authentication, reportez-vous à la section Contexte MFA (Multi-Factor Authentication).
> - TLA doit être utilisé pour les utilisateurs qui ont des privilèges limités.

Procédure

1. Création d'une Twilio configuration.
   a. Créez un Twilio compte test. Pour plus d'informations, consultez Twilio .
   b. Accédez à la **Tout** > **Notification** > **Administration** > **Configuration Twilio Direct**.
   c. Fournissez le **SID de compte** et le **jeton d'authentification** (créé à partir de Twilio) et enregistrez l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Vous pouvez créer votre propre configuration de fournisseur et l'utiliser pour TLA. Dans cet exemple, il s'agit de Twilio. Pour en savoir plus sur la création d'une configuration de fournisseur MFA, reportez-vous à la section Configurer le fournisseur MFA.

2. Configuration et activation de l'enregistrement d'authentification limitée en temps (TLA).

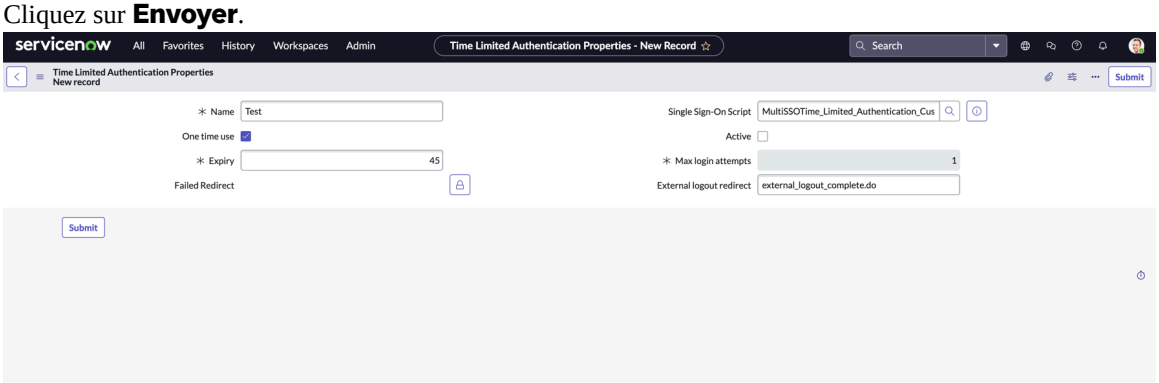
a. Accédez à la **Tout** > **Enregistrements de configuration de l'authentification temporelle limitée** et cliquez sur **Nouveau**.

b. Renseignez les champs du formulaire.

Propriétés d'authentification temporelle limitée

Champ	Description
Nom	Nom de l'enregistrement.
Utilisation ponctuelle	Activez cette option pour utiliser le lien TLA une seule fois.
Expiration	Spécifiez les secondes avant l'expiration du lien. La valeur par défaut est de 45 minutes.
Échec de la redirection	Entrez l'URL pour rediriger les utilisateurs après un échec d'authentification.
Script d'authentification unique	Détails du script SSO que vous souhaitez utiliser.
Actif	Option permettant d'activer la configuration.
Nombre maximal de tentatives de connexion	Spécifiez le nombre de tentatives autorisées avec le lien TLA généré pour la connexion. Décochez la case **Utilisation unique** pour indiquer le nombre maximal de tentatives.
Redirection de déconnexion externe	Entrez l'URL pour rediriger les utilisateurs après la déconnexion.

c. Cliquez sur **Envoyer**.



d. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Administration** > **Propriétés** et activez la propriété **Activer l'authentification unique de plusieurs fournisseurs** et **cliquez sur Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

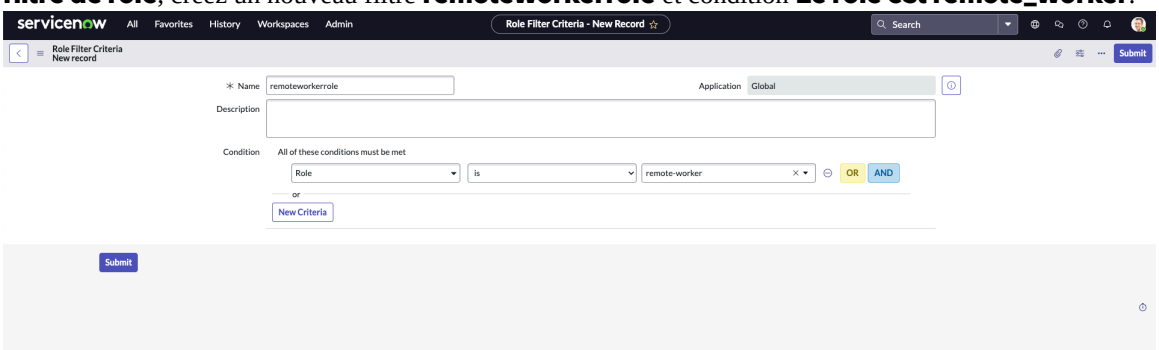
3. Autoriser TLA uniquement à un profil d'utilisateur spécifique en utilisant la politique de contexte post-authentification.

   a. Accédez à **Rôles** et créez un rôle. Par exemple : remote_worker.

   b. Créez un utilisateur avec un ID d'e-mail et un numéro de téléphone portable valides. Pour savoir comment créer un utilisateur, consultez Créer un utilisateur .

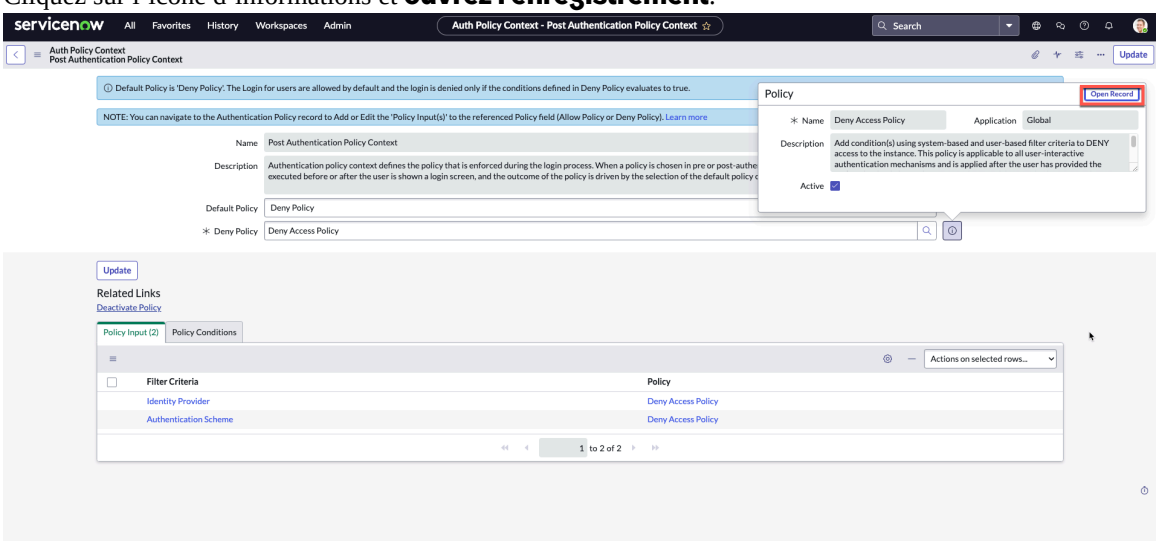
   c. Affectez le rôle à l'utilisateur. Pour savoir comment attribuer le rôle à l'utilisateur, consultez Affecter un rôle à un utilisateur .

   d. Pour créer un critère de filtre de rôle, accédez à **Tout** > **Authentification Adaptative** > **Critère de filtre de rôle**, créez un nouveau filtre **remoteworkerrole** et condition **Le rôle est remote_worker**.



   e. Pour ajouter une condition de politique basée sur le contexte de politique de refus basé sur les critères IdP et de filtre de rôle, accédez à **Tout** > **Authentification Adaptative** > **Contexte de post-authentification**.

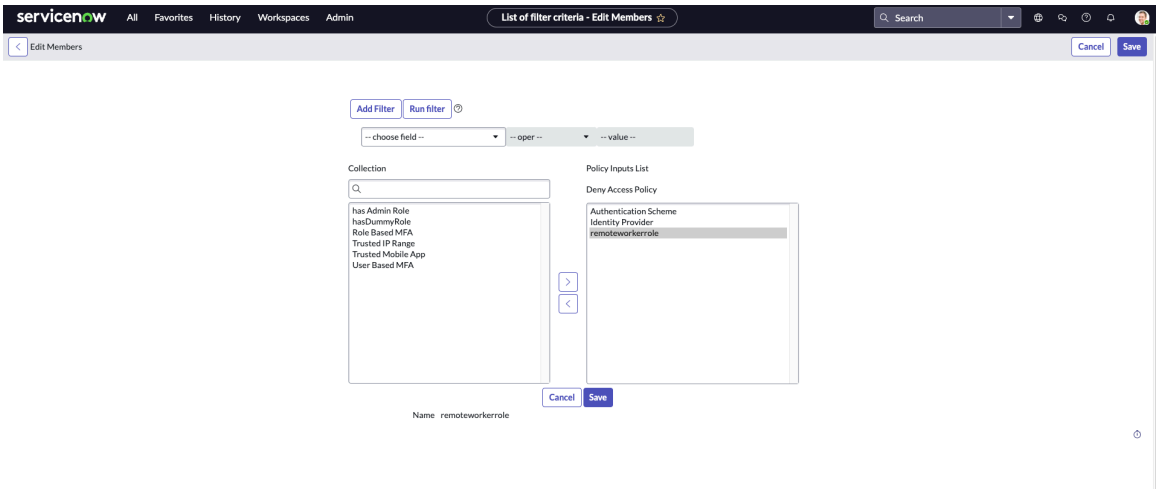
   f. Cliquez sur l'icône d'informations et **ouvrez l'enregistrement**.



   g. Dans l'entrée Politique, cliquez sur **Modifier** et ajoutez le rôle (remoteworkerrole) et **cliquez sur Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

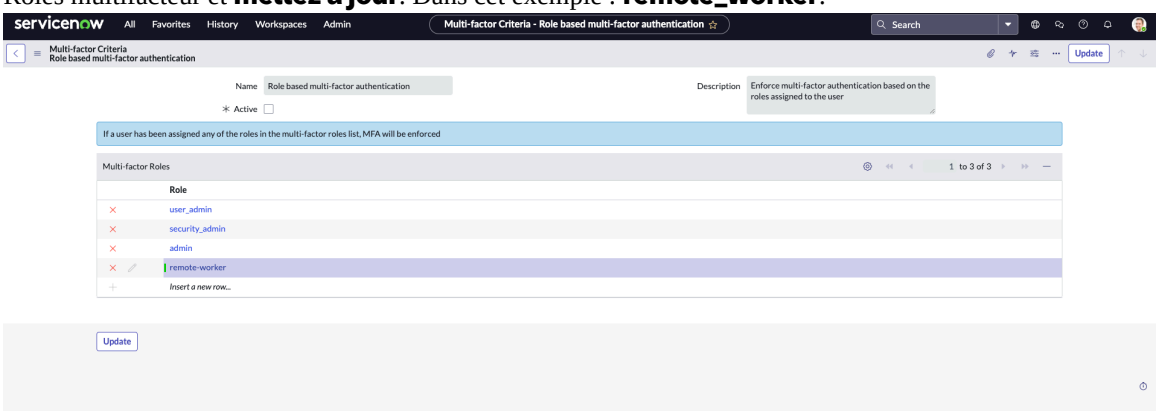


h. Dans la Condition de politique, ajoutez la condition de l'entrée de politique et **soumettez** l'enregistrement.

4. Configuration de la politique d'authentification ascendante : contexte MFA.

a. Accédez à la **Tout** > **Critère multifacteur**.

b. Sélectionnez **l'authentification multifacteur basée sur les rôles** et ajoutez le rôle dans la section Rôles multifacteur et **mettez à jour**. Dans cet exemple : **remote_worker**.



c. Accédez à la **Tout** > **Authentification Adaptative** > **Contexte MFA**.

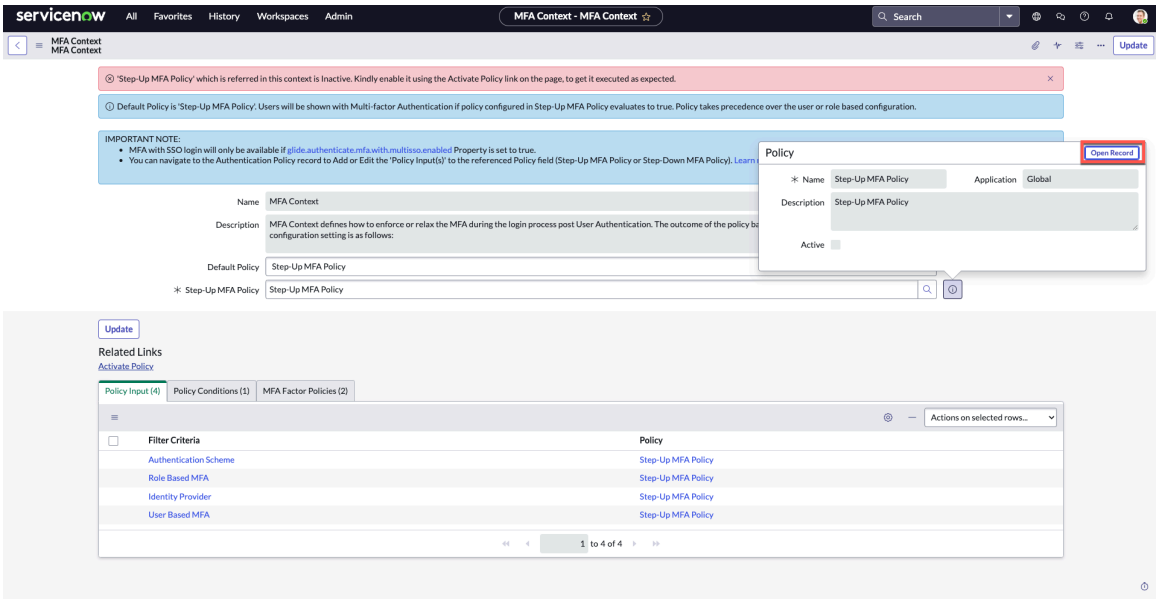
d. Assurez-vous des points suivants :

- Le champ Politique par défaut est **Politique MFA ascendante**
- La politique MFA ascendante est **une politique MFA ascendante**

e. Cliquez sur l'icône Informations et **ouvrez l'enregistrement**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



f. Dans le formulaire Politique de MFA ascendante, dans les entrées de politique, cliquez sur **Modifier**.

g. Ajoutez **l'authentification multifacteur basée sur les rôles** à la liste et **enregistrez**. Dans cet exemple, **remoteworkerrole**.

h. Dans la condition de politique, cliquez sur **Appliquer la MFA si les paramètres MFA basés sur le rôle ou l'utilisateur sont vrais**.

i. Sur la page Appliquer la MFA si les paramètres MFA basés sur le rôle ou l'utilisateur sont vrais, assurez-vous que **MFA basé sur les rôles** est **défini sur vrai**.

5. L'application de la MFA pour utiliser SMS comme politique de facteur MFA.

a. Accédez à la **Tout** > **Authentification Adaptative** > **Contexte MFA**.

b. Sur la page Contexte MFA, cliquez sur **Politiques de facteur MFA** , puis sur Politique **Afficher le mot de passe à usage unique du SMS en tant que politique de facteur MFA**.

c. Cliquez sur **Modifier** et ajoutez **remoteworkerrole** dans les **entrées de politique**.

d. Cliquez sur **Conditions de politique** et créez une condition de politique.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Cliquez sur **Envoyer**.

Le lien TLA généré et partagé avec les utilisateurs affectés avec **remoteworkerrole** en tant que rôle sera promu pour utiliser le code SMS comme deuxième facteur de connexion à l'instance.

6. l'activation des autres propriétés requises.

a. Accédez à la **Tout** > **Authentification multifacteur** > **Propriétés**.

b. Cochez les cases suivantes.

- **Activer l'authentification multifacteur**
- **Activer l'authentification multifacteur avec SSO**

c. Enregistrez l'enregistrement.

d. Accédez à la **Tout** > **Authentification Adaptative** > **Politiques d'authentification** > **Propriétés**.

e. Cochez la case **Activer la politique d'authentification** .

f. Enregistrez l'enregistrement.

7. Génération d'un lien TLA – Exemple.

a. Accédez à la **Tout** > **Définition du système** > **Scripts – Arrière-plan**.

b. Utilisez l'API suivante en fournissant le sysid et l'ID de configuration de l'utilisateur.
`var tla=new global. TimeLimitedAuthentication() ; gs.info(tla.generateNonce(« user_sysid », « config1_sys_id »,"IAR2 »)) ;`

Remarque :
La source (IAR2) n'est pas un paramètre obligatoire.

c. Le paramètre de requête est renvoyé comme indiqué :
`nonce=VCeinfboDt0M&glide_sso_id=b3277f1b44351110f8779b5a2d9909f3&user=3b0277d344351110f8779b5`

d. Créez une URL dans le format ci-dessous :
`https://<instance-url> /login_with_sso.do ?uri=<url codée>&`
`nonce=2ollQSxdgkjs&glide_sso_id=0c15bf09c3711110c5ec4e483c40dd7a&user=62826bf03710200044e0bfc8`

8. Cliquez sur l'URL, l'écran MFA suivant s'affiche pour la connexion.

Authentification du jeton Digest

L'authentification par jeton Digest transmet les informations d'identification de l'utilisateur et un jeton Digest dans un en-tête HTTP non chiffré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l'authentification par jeton Digest.

Configurer



Découvrez comment configurer l'authentification par jeton Digest.

Traduction automatique

Exploration de l'authentification par jeton Digest

L'instance lit la valeur de l'en-tête HTTP et compare sa valeur de hachage calculée du jeton de synthèse. Si la valeur de hachage calculée correspond à la valeur du jeton de synthèse, l'instance recherche une valeur correspondante dans la table Utilisateur. S'il existe une valeur correspondante dans la table Utilisateur, l'instance considère l'utilisateur comme pré-authentifié et le connecte.

L'authentification par jeton Digest est plus sécurisée que les simples en-têtes HTTP non chiffrés, car toute modification accidentelle ou intentionnelle de l'en-tête HTTP non chiffré produit une valeur de hachage différente. Si la valeur de hachage ne correspond pas, l'instance refuse à l'utilisateur l'accès à l'instance demandée. Cela empêche les utilisateurs de tenter de se connecter avec les informations d'identification d'un autre utilisateur.

Pour en savoir plus sur l'expiration du lien de synthèse, consultez cet article de la base de connaissances .

Remarque :
Utilisez l'authentification limitée dans le temps (TLA) pour configurer les liens d'expiration basés sur le temps. Pour en savoir plus, reportez-vous à la section Authentification temporelle limitée.

Exigences d'intégration

Une intégration d'authentification par jeton Digest nécessite :

- Un serveur web
- SiteMinder ou une autre application d'authentification unique pour pré-authentifier l'utilisateur sur le réseau local

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Page Web ou portail qui transmet les informations d'identification de l'utilisateur à l'instance cible dans l'un des formats suivants
  - En-tête HTTP
  - Paramètre d'URL
  - Cookie
- Page Web ou portail qui crée et transmet un jeton de synthèse à l'instance cible à l'aide de l'une de ces techniques de codage
  - SHA1
  - MD5
  - SHA 256 (recommandé)

Configuration des propriétés de synthèse pour l'authentification unique (SSO) de plusieurs fournisseurs

Après l'activation d'un script d'installation de synthèse, configurez les propriétés pour l'authentification unique (SSO) de plusieurs fournisseurs.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Si vous n'utilisez pas l'authentification unique de plusieurs fournisseurs, configurez les propriétés d'authentification unique standard.

Procédure

1. Accédez à la **Tout** > **Authentification unique (SSO) de plusieurs fournisseurs** > **Fournisseurs d'identité**.
2. Renseignez les champs du formulaire Propriétés de synthèse.

Option	Description
Nom	Saisissez le nom du jeton de synthèse.
Utilisateur	Saisissez le champ sys_user qui contient les données correspondantes pour l'en-tête entrant.
Nom d'en-tête HTTP Digest	Entrez l'en-tête HTTP que vous avez généré. Par exemple, DE_USER.
Nom d'en-tête HTTP	Entrez l'en-tête HTTP que vous avez généré pour votre jeton synthétisé créé. Par exemple, SM_USER.
Phrase de sécurité secrète	Entrez la clé secrète à utiliser pour coder les clés de synthèse. Par exemple, 32 caractères ou plus.
Échec de l'authentification unique (SSO) : champ de redirection	Entrez l'URL pour rediriger les utilisateurs après un échec d'authentification.
Redirection de déconnexion externe	Entrez l'URL pour rediriger les utilisateurs après une déconnexion.
Script d'authentification unique	Sélectionnez **MultiSSO_DigestedToken**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Type de client	Choisissez le type de client en fonction du type de votre client. Options :**Iframe intégré**. **Remarque :** Si le champ de type client est requis pour votre configuration, vous pouvez modifier le formulaire et ajouter le champ. Pour en savoir plus, reportez-vous à la section Configurer le type de client pour les enregistrements OAuth et SSO.

3. Cliquez sur **Mettre à jour**.
4. Définissez votre jeton digéré par défaut sur vrai.
   Lorsque vous définissez la valeur par défaut sur vrai, cela remplace l'enregistrement de jeton de synthèse par défaut du système associé à SSO. Une fois que le premier enregistrement IdP associé à l'authentification unique (SSO) de plusieurs fournisseurs est activé, seuls les enregistrements associés à l'authentification unique (SSO) de plusieurs fournisseurs sont utilisés.

   Les enregistrements de jetons de synthèse qui existent dans la table des propriétés de synthèse peuvent être appelés individuellement en ajoutant la Sys_ID de l'IdP. Par exemple, un enregistrement de jeton de synthèse dans l'URL d'authentification suivante : https://<instance_name>.service-now.com/login_with_sso.do?glide_sso_id=<sys_id_of_Digest_token_record>&SM_USER=<user_name>&DE_USER=<digested_token>

Exemples d'implémentations de jetons de synthèse

Voici plusieurs exemples de création d'un jeton de synthèse.

Exemples d'implémentations d'authentification de synthèse

Synthèse créée avec	Valeur de clé secrète	Méthode de hachage	Exemple
Java	32 caractères et plus	SHA256	Exemple d'algorithme Java Digest pour le chiffrement
C	Valeur du paramètre sharedKey	Valeur du paramètre strEncryptionMethod (SHA256 ou MD5)	Exemple C

Exemple d'algorithme de synthèse Java pour le chiffrement

Cet algorithme Java illustre la création d'un jeton de synthèse à partir d'un en-tête HTTP.

Cet exemple suppose que :

- Le serveur Web prend en charge Java
- La méthode de calcul du hachage est SHA1
- La valeur de la clé secrète est abc123
- Le nom de l'en-tête HTTP non chiffré est user_name

Modifiez le code Java pour utiliser un autre mécanisme de calcul de hachage (tel que MD5), modifiez la valeur de la clé secrète ou le nom de l'en-tête HTTP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
public class DigestTest
{
   private static final String MAC_ALG = "HmacSHA256";
     fKey  = {32 or more characters};
   public byte[] getDigest(String acct) {
      try {
         byte[] bkey = fKey.getBytes();
         byte[] data = acct.getBytes();
         Mac mac = null;
         try {
            mac = Mac.getInstance(MAC_ALG);
            mac.init(new SecretKeySpec(bkey, MAC_ALG));
         } catch (Exception e) {
            e.printStackTrace();
         }
         byte[] sig = mac.doFinal(data);
         String signature = new String(sig);
         System.out.println("value:" + acct);
         System.out.println("digested value:  " + signature);
         return sig;
      } catch (IllegalStateException e) {
         e.printStackTrace();
      }
      return null;
   }
   public static void main(String[] args) {
      BASE64Encoder encoder = new BASE64Encoder();
      DigestTest test = new DigestTest();
      String userName = "user_name";
      System.out.println("base 64 digest username: " +
 encoder.encode(test.getDigest(userName)));
   }
}
```

Exemple C

Cette classe C illustre la création d'un jeton de synthèse à partir de trois paramètres d'entrée.

- strEncryptionMethod – répertorie la méthode de calcul de hachage (SHA1, SHA256 ou MD5)
- Message : répertorie la valeur à convertir en jeton de synthèse.
- sharedKey – répertorie la clé secrète

Remarque :
Utilisez un algorithme de hachage sécurisé plus fort comme SHA256 pour la génération de jetons de synthèse.

Cet exemple suppose que :

- Le serveur Web prend en charge C
- Un autre code appelle cette classe et transmet les paramètres attendus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple de code

```
private stringdigestData(string strEncryptionMethod , string message , string sharedKey ) {
        UnicodeEncoding myUnicodeEncoding  = new UnicodeEncoding ( ) ;

        byte [ ] messageBytes  = System. Text. Encoding. ASCII. GetBytes (message ) ;
        byte [ ] sharedKeyBytes  = System. Text. Encoding. ASCII. GetBytes (sharedKey ) ;
        byte [ ] hashedMessage ;

        string b64SHA1Message ;

         if (this. DEBUG ) {
           TextBoxMessage. Text = message ;
           TextBoxSecret. Text = sharedKey ; }

         switch ( (strEncryptionMethod ) )

         { case "SHA1" :

              HMACSHA1 hmacsha1  = new HMACSHA1 ( ) ;
              hmacsha1. Key = sharedKeyBytes ;
              hashedMessage  = hmacsha1. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

           case "MD5" :

              HMACMD5 hmacmd5  = new HMACMD5 (sharedKeyBytes ) ;
              hashedMessage  = hmacmd5. ComputeHash (messageBytes ) ;
              b64SHA1Message  = Convert. ToBase64String (hashedMessage ) ; if (this.
DEBUG ) TextBoxDigest. Text = Convert. ToString (hashedMessage ) ; break ;

           default :

              b64SHA1Message  = "Unknown Encryption Method" ; break ;

         }


        TextBoxBase64. Text = b64SHA1Message ; return b64SHA1Message ;

      }
```

Traduction automatique

Sécurité des services Web

Appliquez la sécurité à l’aide de l’authentification de base, de l’authentification réciproque ou de la sécurité WS.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorez la sécurité Web



Découvrez les fonctionnalités et les valeurs commerciales de la sécurité des services web.

Configurer l’authentification réciproque



Utilisez l’authentification réciproque pour établir la confiance en échangeant des certificats SSL (Secure Sockets Layer).

Traduction automatique

Exploration de la sécurité des services Web

Appliquez la sécurité à l’aide de l’authentification de base, de l’authentification réciproque ou de la sécurité WS.

Authentification de base

Pour appliquer l’authentification de base à chaque demande d’un document WSDL ou d’une publication de messages SOAP, vous pouvez définir la propriété *glide.basicauth.required* sur true. Dans ce cas, chaque requête WSDL ou SOAP devra contenir l’en-tête « Autorisation » tel que spécifié dans le protocole d’authentification de base . Étant donné que la demande n’est pas interactive, l’en-tête **d’autorisation** est toujours requis au cours d’une demande.

Fournir des informations d’authentification de base, qu’elles soient requises ou non, présente l’avantage supplémentaire que les données créées ou mises à jour à la suite de l’appel de service Web sont effectuées pour le compte de l’utilisateur fourni dans les informations d’identification d’authentification de base. Par exemple, lors de la création d’un enregistrement d’incident, les champs journal affichent l’ID d’utilisateur de l’utilisateur authentifié de base, au lieu de l’utilisateur **invité** par défaut.

Pour que l’en-tête d’autorisation ignore les règles de capitalisation, utilisez la *glide.security.script.include.name.case.insensitive.list* propriété. Vous pouvez modifier cette propriété dans la table Propriétés système [sys_properties] et ajouter les includes de script nécessaires au traitement de l’authentification. Par défaut, cette propriété comporte les valeurs suivantes :

- BasicAuth
- Authentification personnalisée

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajoutez d'autres includes de script si nécessaire.

Pour fournir une authentification de base lors de l'utilisation de Perl et des bibliothèques SOAP ::Lite, vous pouvez implémenter la fonction suivante :

```
sub SOAP :: Transport :: HTTP :: Client :: get_basic_credentials { return 'user_name' =>
 'password' ; }
```

- Lors de l'utilisation de C# .NET par rapport à 2005 ou une version antérieure, vous pouvez tirer parti de l'objet Informations d'identification, par exemple :

```
System.Net . ICredentials cred  = new System.Net . NetworkCredential ( "user_name",
 "password" ) ;

service . ServiceNow proxy  = new service . ServiceNow ( ) ;
service . get getService  = newservice . get ( ) ;
service . getResponse getServiceResponse  = new service . getResponse ( ) ;

 try {
  proxy . Credentials = cred ;
  getService . sys_id = "bf522c350a0a140701972dbf876f1610" ;
  getServiceResponse  = proxy . get (getService ) ; catch (Exception ex ) { }
```

- Lors de l'utilisation de C# .NET VS 2008, vous pouvez tirer parti de l'objet ClientCredentials, par exemple :

```
Demo_Incident. ServiceNowSoapClient client  = new Test08WebService . Demo_Incident .
 ServiceNowSoapClient ( ) ;
client . ClientCredentials . UserName . UserName = "admin" ;
client . ClientCredentials . UserName . Password = "admin" ;
```

Ensuite, dans votre fichier app.config, recherchez ce qui suit et remplacez `None` par `Basic` :

```
<transport clientCredentialType= "None" proxyCredentialType= "None" realm= "" />
```

- Lors de l'utilisation de VB .NET, l'utilisation de l'objet Informations d'identification ressemblerait à ce qui suit :

```
Sub Main()
       Dim cred  As New System.Net.NetworkCredential( "user_name",  "password")

       Dim proxy  As New VB_Democm.incident.ServiceNow
       Dim getIncident  As New VB_Democm.incident. get Dim getResponse  As New
 VB_Democm.incident.getResponse

      proxy.Credentials = cred

      getIncident.sys_id =  "[your sysID here]"

      getResponse = proxy. get(getIncident)

   End Sub
```

La réponse qui en résulte, lorsque l'authentification de base est activée et qu'aucune information d'identification n'est fournie, ressemble à ceci :

```
<html> <head > <title >Apache Tomcat/5.0.28 - Error report </ title > <style > <!--H1
 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;}
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 H2
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;}
 H3
{font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;}
   BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;}
 B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;}    P
{font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}   A
{color : black;}   A.name {color : black;}   HR {color : #525D76;}--> </
style > </ head > <body > <h1 >HTTP Status 401 -\ </ h1 > <HR size = "1" noshade =
"noshade" > <p >< b >type </ b > Status report </ p > <p >< b >message </ b > <u >< /
u >< / p > <p >< b >description </ b > <u >This request requires HTTP authentication ().
</ u >< / p > <HR size = "1" noshade = "noshade" > <h3 >Apache Tomcat/5.0.28 </ h3 >
</ body > </ html >
```

Configuration de l'authentification réciproque

L'authentification réciproque établit la confiance par l'échange de certificats SSL (Secure Sockets Layer).

Lors de l'établissement de liaison SSL, le serveur présente son certificat au client. Par la suite, en fonction de la configuration du serveur, il peut demander un certificat au client. Le serveur et le client effectuent des procédures de validation des certificats pour garantir l'authenticité et l'intégrité des certificats présentés.

Une fois la validation réussie, les accusés de réception sont échangés avant l'établissement de la connexion HTTPS.

Les administrateurs effectuent le travail préliminaire de configuration du magasin de clés client et de génération des certificats avant que les demandes de certification ne soient satisfaites.

⚠ Avertissement :
Cette fonctionnalité active uniquement l'authentification réciproque sur les connexions HTTPS sortantes.

Création du magasin de clés

L'instance prend actuellement en charge le chargement d'un fichier Java Key Store, qui contient une clé privée et une paire de certificats publics. Le certificat public inclut une chaîne complète, y compris le certificat racine.

Pour configurer votre magasin de clés client :

- Vous avez besoin d'un certificat signé par une autorité de certification (CA) de confiance.
- Votre fournisseur de point de terminaison d'API peut vous aider à générer le magasin de clés.

Si vous devez générer le magasin de clés, le processus implique plusieurs étapes à l'aide de commandes de l'interface de ligne de commande pour générer un nouveau fichier du magasin de clés, créer une demande de signature de certificat (CSR) et importer des certificats signés. Avant d'importer le certificat principal de votre domaine, vous devez d'abord importer les certificats racines ou intermédiaires. Voici une instruction étape par étape :

1. Générez un magasin de clés Java et une paire de clés.

```
keytool -genkey -alias mydomain -keyalg RSA -keystore my.keystore
```

2. Générez une CSR pour un magasin de clés Java existant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
keytool -certreq -alias mydomain -keystore my.keystore -file mydomain.csr
```

3. Envoyez la CSR à votre autorité de signature de l'autorité de certification pour qu'elle signe et renvoie les fichiers de certificat, qui comprennent les certificats intermédiaires et racine ainsi que le certificat signé.
4. Importez un certificat d'autorité de certification (CA) racine ou intermédiaire dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias root -file Thawte.crt -keystore my.keystore
```

Remarque :
Vous pouvez regrouper tous les certificats dans un seul fichier et les importer. C'est une option préférable. Si vous faites de cette façon, vous pouvez sauter 5

```
keytool -import -alias mydomain -file merged.crt -keystore my.keystore
```

5. Importez un certificat primaire dans un magasin de clés Java existant.

```
keytool -import -trustcacerts -alias mydomain -file mydomain.crt -keystore my.keystore
```

Configuration du magasin de clés

Maintenant que le magasin de clés a été créé, il peut être téléchargé dans la table Certificats. Sur le **Définition du système** > **Certificats** , cliquez sur **Nouveau** et définissez les champs suivants :

- **Entrez un nom** de certificat.
- Stockez le magasin de clés en tant **qu'actif**.
- **Définir le type = Magasin de clés Java**.
- Fournissez un **mot de passe de magasin de clés**. Il s'agit du mot de passe utilisé pour créer le magasin de clés.

Cliquez sur **Envoyer** pour créer l'entrée du magasin de clés Java.

Magasin de clés

X.509 Certificate | = Required field — Update — Delete

Attachments: my.keystore [view]

Name:	Key store	Type:	Java Key Store
Active:	☑	Key store password:	••••••••••••••••••••••
Short description:	key store used for mutual authentication		

Spécification d'un certificat de serveur de confiance

Lors d'une connexion SSL sortante, qui est un appel de service Web HTTPS, il est possible de spécifier un certificat fourni par le fournisseur de service qui assure la validité du fournisseur de service pendant la connexion SSL. Par exemple, un navigateur qui tente de se connecter à un service sécurisé et qui s'identifie par un certificat.

En téléchargeant le certificat du serveur approuvé, ServiceNow il s'assure que le service auquel il se connecte est valide et sécurisé.

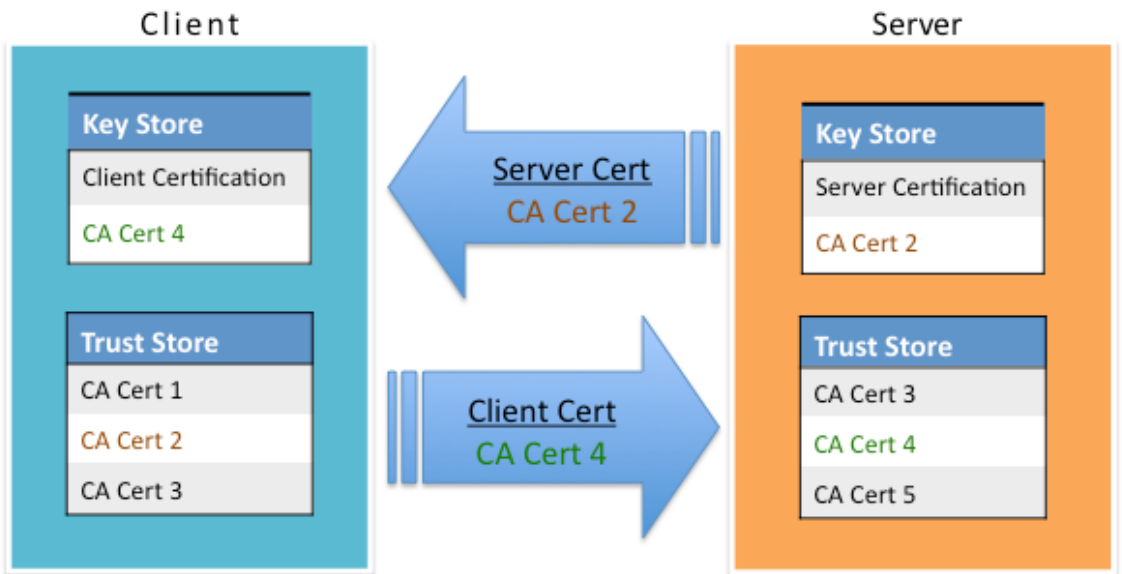
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créez une nouvelle entrée de certificat avec le type de « Certificat de magasin de confiance » et joignez un certificat au format DER, ou copiez-collez son format PEM dans le champ **Certificat PEM** .

Profil du protocole

Échange de certificats



- Lorsqu'un client demande le certificat du serveur pour l'authentification, une demande de signature de certificat (CSR) est générée.
- Pour répondre à une CSR, le serveur génère deux clés cryptographiques uniques : une clé publique, qui est utilisée pour chiffrer les messages vers le serveur et une clé privée, qui est utilisée pour déchiffrer les messages. Les deux clés sont conservées dans le magasin de clés.
- Les clés sont utilisées pour déchiffrer les messages sécurisés du client afin qu'ils puissent être lus par le serveur. Toute connexion sortante au format HTTPS vérifie la certification en vérifiant le magasin de clés, en offrant sa certification publique, et utilise les certificats du magasin de clés de confiance pour vérifier la confiance mutuelle.
- Pour compléter le lien sécurisé entre le client et le serveur, le serveur associe le certificat à la clé privée correspondante. Étant donné que seul le serveur a accès à la clé privée, il peut déchiffrer les données du client.

Voici un exemple de commande qui enregistre MYHTTPS avec l'usine de sockets `com.glide.certificates.DBKeyStoreSocketFactory` sur le port 443. L'usine de magasins de clés de base de données est utilisée pendant le processus d'échange SSL pour offrir un certificat client pour l'authentification mutuelle.

```
glide.httpclient.protocol.myhttps.class = "com.glide.certificates.DBKeyStoreSocketFactory"
glide.httpclient.protocol.myhttps.port = "443"
```

La configuration ci-dessus affecte toute URL de `myhttps://host.domain.com/target` sortante pour utiliser l'instanciateur de sockets personnalisé et échanger des certificats pendant SSL.

Remarque :
Le remplacement de l'usine de sockets de protocole HTTPS par défaut affecte chaque connexion HTTPS sortante. Ce n'est généralement pas souhaitable.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le serveur répond par l’envoi d’un certificat. S’agit-il d’un certificat accepté par le client ? Si c’est le cas, un message est envoyé au serveur qui accepte le certificat et un canal sécurisé est lancé. Si le certificat n’est pas accepté, cela peut signifier que l’autorité racine est nécessaire pour la certification.

Règles de la liste de contrôle d’accès

Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Explorer	Configurer
	
En savoir plus sur ACL.	Configurez l’ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Référence



Obtenir des détails sur le gestionnaire de sécurité contextuelle.

Avancés



En savoir plus sur l’ACL avancé.

Traduction automatique

Exploration des listes de contrôle d’accès

Explorez les listes de contrôle d’accès (ACL).

Toutes les règles de la liste de contrôle d’accès spécifient :

- *Le type de décision*, *le type de règle* et *l’opération* qui définissent l’ACL
- *Objet* sécurisé
- *Conditions* d’accès à l’objet

Composants de l’ACL

Le type de décision définit si les utilisateurs sont autorisés à accéder à l’objet si les conditions sont remplies ou refuse l’accès à l’objet si les conditions ne sont pas remplies.

Type de décision	Description
Refuser à moins que	Restreignez l’accès aux ressources en refusant explicitement l’accès sauf si les conditions sont remplies. Consultez #unique_1393_Connect_42_section_qnd_snl_zbc pour plus d'informations.
Autoriser si	Autoriser l’accès à la ressource si les conditions sont réussies.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'objet est la cible dont l'accès doit être contrôlé. Chaque objet se compose d'un type et d'un nom qui identifient de manière unique une table, un champ ou un enregistrement particulier. Avec le champ *S'applique à*, les utilisateurs disposent d'un contrôle granulaire sur les enregistrements spécifiques auxquels cette ACL s'appliquera.

Par exemple, toutes ces entrées spécifient un objet :

Type	Nom	Objet sécurisé
enregistrement	[incident]. [--Aucun--]	La table Incident.
enregistrement	[incident]. [actif]	Champ Actif de la table Incident.
enregistrement	[incident] S'applique à : priorité = P1	Uniquement les incidents de priorité 1 dans la table d'incidents.
REST_Endpoint	user_role_inheritance	Enregistrement de l'API REST scriptée user_role_inheritance.

Chaque *opération* décrit une *action* valide que le système peut effectuer sur l'objet spécifié. Certains objets, tels que les enregistrements, prennent en charge plusieurs opérations, tandis que d'autres, tels qu'un REST_Endpoint, ne prennent en charge qu'une seule opération.

Par exemple, toutes ces entrées spécifient une opération :

Type	Nom	Opération	Opération sécurisée
enregistrement	[incident]. [-- Aucun --]	créer	Création d'enregistrements dans la table Incident.
enregistrement	[incident]. [actif]	write	Mise à jour du champ Actif dans la table Incident.
REST_Endpoint	user_role_inheritance	execute	Exécution de l'API REST basée sur un script user_role_inheritance.

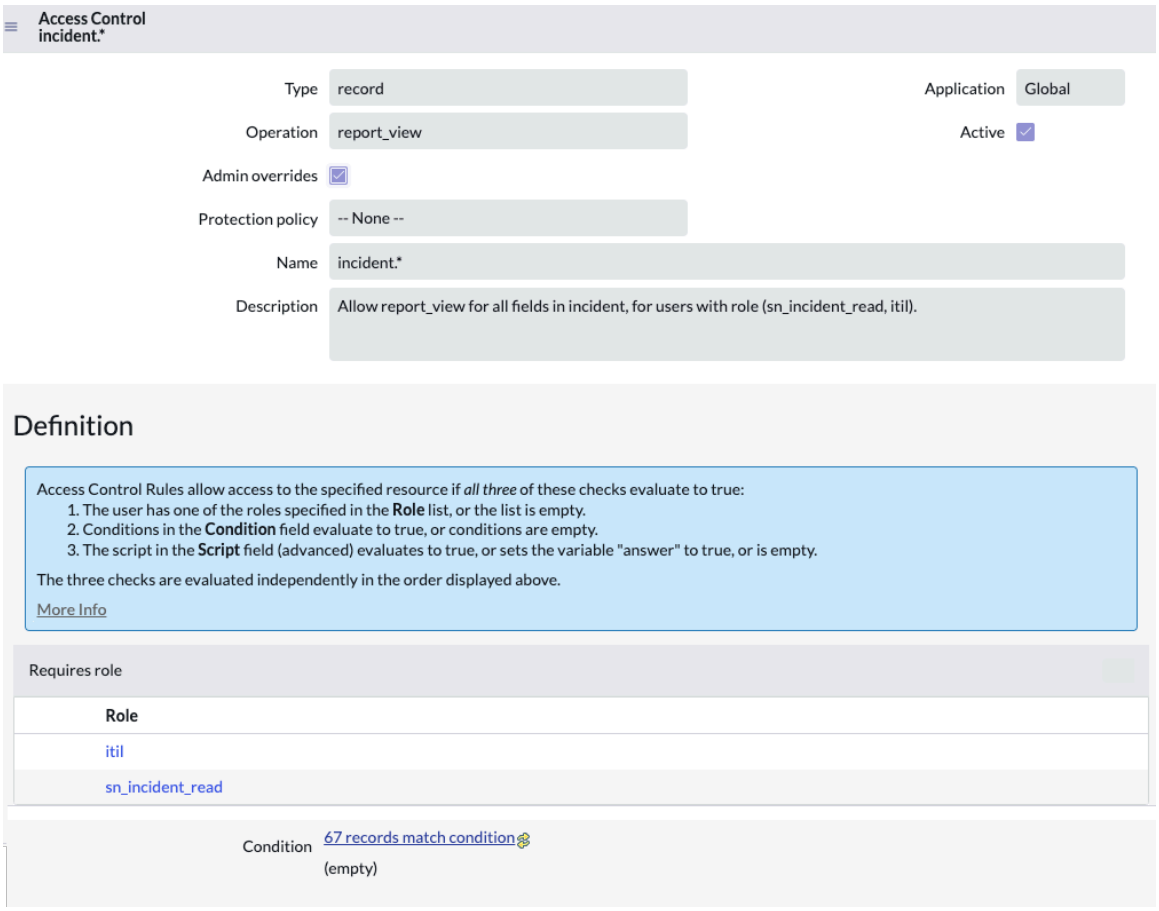
Les *conditions* spécifient quand quelqu'un peut accéder à l'objet et à l'opération nommés. Les administrateurs de sécurité peuvent spécifier les exigences de condition en ajoutant :

- Un ou plusieurs rôles d'utilisateur à la liste **Requiert un rôle** .
- Un ou plusieurs attributs de sécurité doivent être évalués pour être vrais.
- Une ou plusieurs conditions de données.
- Script qui évalue sur vrai ou faux ou qui définit la variable `de réponse` sur vrai ou faux.

Pour accéder à un objet et à une opération, un utilisateur doit satisfaire à toutes les conditions répertoriées dans un contrôle d'accès. Par exemple, ce contrôle d'accès restreint l'accès à la vue des opérations sur la table d'incident.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pour mettre à jour un enregistrement dans la table d'incidents, un utilisateur doit avoir les rôles répertoriés et l'enregistrement doit remplir la condition.

Type de condition	Besoin	Description
Demande un rôle	**Exige role** :itil	Autorisez uniquement les utilisateurs disposant du rôle itil à mettre à jour les incidents.
Attributs de sécurité	UserIsAuthenticated	Seuls les utilisateurs authentifiés peuvent mettre à jour les incidents.
Condition de données	[État de l'incident] [n'est pas] [Fermé]	Autoriser uniquement les mises à jour des enregistrements d'incidents actifs.

Comportement de refus par défaut

Par défaut, le moteur ACL refuse complètement l'accès si une ACL est vide ou non valide. Les ACL vides sont définies comme des ACL sans un ou plusieurs de ces composants :

- Rôle défini
- Attribut de sécurité
- Condition de données
- Script

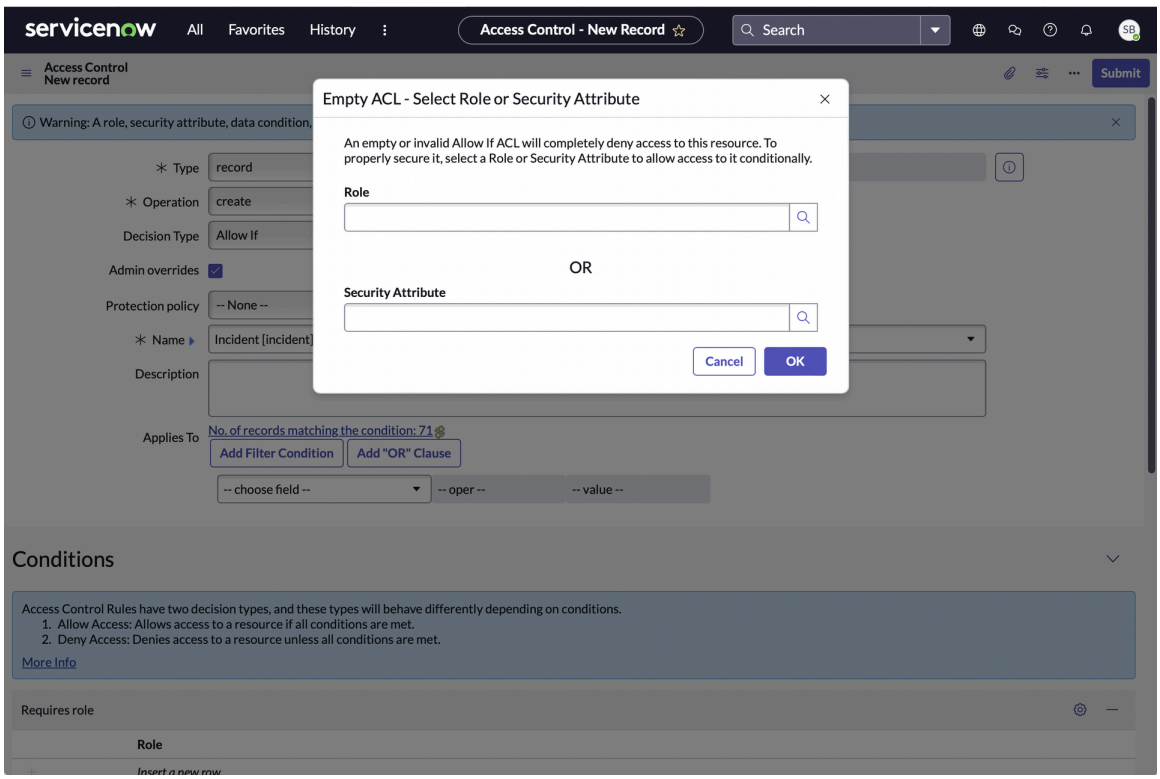
Les ACL non valides sont définies comme :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- ACL avec des rôles qui n'existent pas (par exemple, n'ont pas de ligne dans la base de données)
- ACL avec des attributs de sécurité qui n'existent pas (par exemple, n'ont pas de ligne dans la base de données)
- ACL avec un script qui contient « answer=true » ou « true »

Si le système détecte que l'utilisateur crée une ACL, il l'invite à sélectionner un rôle ou un attribut de sécurité existant.



Processus d'évaluation ACL

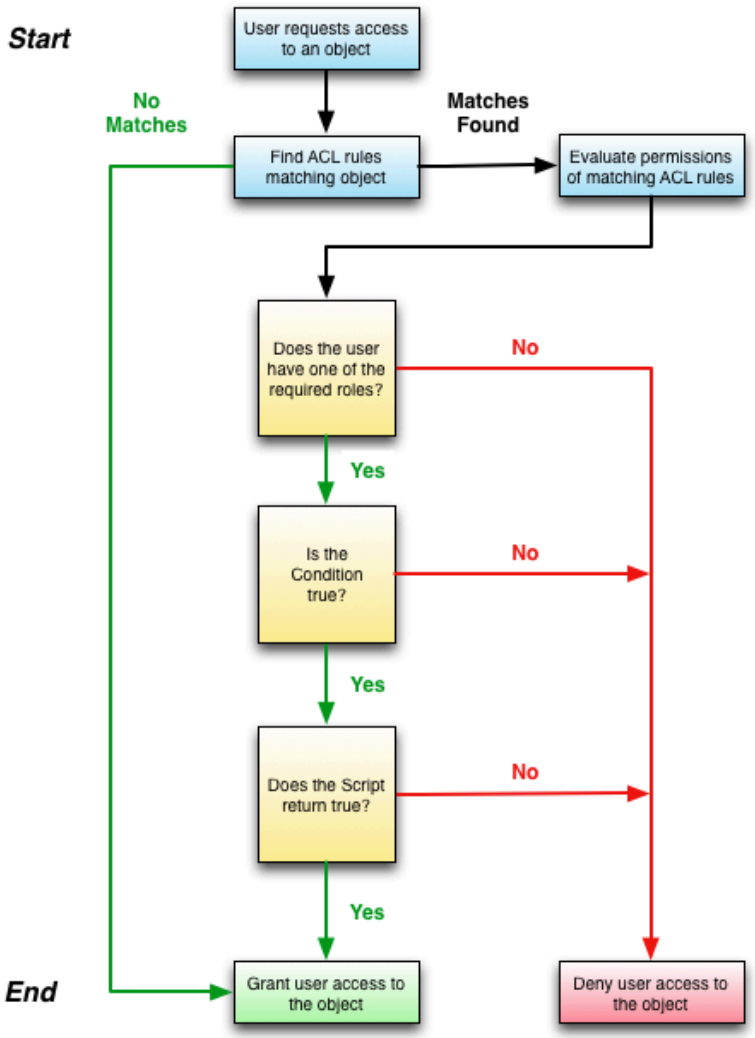
Une règle ACL n'accorde à un utilisateur l'accès à un objet que si l'utilisateur remplit toutes les conditions requises par la règle ACL correspondante.

- La condition doit être évaluée *comme vraie*.
- Le script doit avoir la valeur *vrai* ou renvoyer une variable de réponse avec la valeur *vrai*.
- L'utilisateur doit avoir l'un des rôles de la liste des rôles requis. Si la liste est vide, cette condition est *évaluée comme vrai*.
- [Règles ACL d'enregistrement uniquement] Les règles ACL correspondantes au niveau de la table et au niveau du champ doivent toutes les deux être évaluées sur *vrai*.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conditions d'évaluation ACL



Chaque fois qu'une session demande des données, le système recherche des règles de contrôle d'accès qui correspondent à l'objet et à l'opération demandés. S'il existe une règle de contrôle d'accès correspondante, le système évalue si l'utilisateur remplit les conditions requises pour accéder à l'objet et à l'opération. Si une règle de contrôle d'accès spécifie plusieurs conditions, l'utilisateur doit remplir toutes les conditions pour accéder à l'objet et à l'opération. L'échec d'une vérification de condition empêche l'utilisateur d'accéder à l'objet et à l'opération correspondants.

Si un utilisateur ne répond pas aux conditions de la première règle de correspondance, le système évalue les conditions de la règle de contrôle d'accès correspondante suivante, telles que spécifiées par l'ordre de traitement du contrôle d'accès. Si l'utilisateur ne remplit pas les conditions d'une règle de contrôle d'accès correspondante, le système refuse l'accès à l'objet et à l'opération demandés.

Remarque :
S'il n'y a pas de règles de contrôle d'accès correspondantes pour l'objet et l'opération demandés, le système accorde l'accès à l'utilisateur. Dans la pratique, il est rare que le système ne trouve aucune règle correspondante, car le système dispose d'un ensemble de règles de contrôle d'accès par défaut qui protègent toutes les opérations d'enregistrement.

Les conséquences du refus d'accès à un objet dépendent de la règle ACL que l'utilisateur a défaillante. Par exemple, l'échec d'une règle ACL d'opération de lecture empêche

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

l'utilisateur de voir l'objet. Selon l'objet sécurisé, la règle ACL masque un champ dans un formulaire, masque des lignes d'une liste ou empêche un utilisateur d'accéder à une page de l'interface utilisateur. La table suivante contient une liste complète des résultats de l'échec d'une règle ACL pour une opération et un type d'objet donnés.

Vérifications ACL avant et après requête

Votre instance vérifie les règles ACL avant et après qu'un utilisateur effectue une requête. Étant donné que différentes informations sont disponibles avant et après une requête, les résultats peuvent être différents.

Vérification de l'ACL avant requête

Avant d'exécuter une requête de base de données, l'instance vérifie les règles ACL de chaque champ de la table interrogée afin de déterminer les champs auxquels un utilisateur peut accéder. Cette vérification examine uniquement les rôles de l'utilisateur et vérifie si ces rôles autorisent l'accès aux champs. Étant donné que cette vérification s'exécute avant la requête, l'ACL n'a pas accès aux enregistrements de la table et ne peut donc pas prendre en compte ces données. Les scripts et les conditions qui reposent sur la connaissance du contenu d'un enregistrement ne sont pas évalués.

Si l'utilisateur ne dispose pas d'un accès en lecture à ce stade, la valeur du champ ne lui est pas présentée.

Vérification de l'ACL après requête

Après la requête, votre instance vérifie chaque enregistrement renvoyé par la requête. Au cours de cette vérification, il existe un contexte pour l'ACL, de sorte que les parties rôle, condition et script de l'ACL sont évaluées. Si l'utilisateur ne dispose pas d'un accès en lecture à ce stade, la valeur du champ ne lui est pas présentée, mais l'utilisateur voit l'étiquette du champ si ses rôles autorisent l'accès au champ.

Opération	Résultats de l'échec d'une règle ACL sur un objet
execute	L'utilisateur ne peut pas exécuter de scripts sur un enregistrement ou une page d'interface utilisateur.
créer	L'utilisateur ne peut pas voir la **nouvelle** action d'interface utilisateur dans les formulaires. L'utilisateur ne peut pas non plus insérer d'enregistrements dans une table à l'aide de protocoles API tels que les services Web. Une ACL **de création** avec une condition exigeant qu'un champ contienne une valeur spécifique est toujours évaluée comme faux. Les champs des nouveaux enregistrements sont considérés comme vides jusqu'à ce que l'enregistrement soit enregistré.
lu	L'utilisateur ne peut pas voir l'objet dans les formulaires ou les listes. L'utilisateur ne peut pas non plus récupérer d'enregistrements à l'aide de protocoles API tels que les services Web.
write	L'utilisateur voit un champ en lecture seule dans les formulaires et les listes, et il ne peut pas mettre à jour des enregistrements à l'aide de protocoles API tels que les services Web.
supprimer	L'utilisateur ne peut pas voir l'action d'interface utilisateur **Supprimer** des formulaires. L'utilisateur ne peut pas non plus supprimer les enregistrements d'une table à l'aide de protocoles API tels que les services Web.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opération	Résultats de l'échec d'une règle ACL sur un objet
edit_task_relations	L'utilisateur ne peut pas définir de relations entre les tables de tâches.
edit_ci_relations	L'utilisateur ne peut pas définir de relations entre les tables d'éléments de configuration [cmdb_ci].
save_as_template	Utilisé pour contrôler les champs qui doivent être enregistrés lors de la création d'un modèle.
add_to_list	L'utilisateur ne peut pas afficher ou personnaliser des colonnes spécifiques dans la mécanique de liste.
list_edit	L'utilisateur ne peut pas mettre à jour les enregistrements (lignes) d'une liste.
report_on	L'utilisateur ne peut pas créer de rapport sur la table ACL. Pour plus d'informations, consultez Restreindre la création de rapports avec une règle ACL .
report_view	L'utilisateur ne peut pas afficher le contenu d'un rapport dans la table ACL ou dans le champ ACL. Pour plus d'informations, consultez Reporting .
personalize_choices	L'utilisateur ne peut pas cliquer avec le bouton droit sur un champ de liste et sélectionner **Configurer les choix**.

ACL correspondant aux exigences pour les objets

Type d'objet	Règles ACL de correspondance requises pour accéder à l'objet	Règles ACL génériques existantes
Includes de script pouvant être appelés par le client Processeurs	Les utilisateurs doivent remplir les conditions de deux règles ACL : 1. Toutes les règles ACL génériques pour l'objet (le cas échéant, une règle ACL existe pour l'opération). 2. La première règle ACL qui correspond au nom de l'objet (si une règle ACL existe pour l'opération).	Par défaut, il n'existe pas de règle générique (*) pour ces types d'objets. Si vous créez une règle ACL générique pour l'un de ces objets, la règle ACL s'applique à tous les objets de ce type.
Pages de l'interface utilisateur Enregistrement	Les utilisateurs doivent remplir les conditions de deux règles ACL : 1. La première règle ACL qui correspond au champ de l'enregistrement (si une règle ACL existe pour l'opération). 2. La première règle ACL qui correspond à la table de l'enregistrement (si une règle ACL existe pour l'opération).	Par défaut, il existe des règles de table génériques (*) pour les opérations de création, de lecture, d'écriture et de suppression et des règles de champ génériques (*.*) pour les opérations personalize_choices, create et save_as_template. Lorsque vous créez une table, créez des règles ACL pour la table, à moins que vous ne souhaitiez utiliser les règles ACL génériques fournies.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
La propriété Comportement par défaut du gestionnaire de sécurité (`glide.sm.default_mode`) détermine si les utilisateurs peuvent accéder aux objets qui ne correspondent qu'aux règles ACL de table à caractère générique. Lorsque cette propriété est définie sur *Refuser l'accès*, seuls les administrateurs peuvent accéder aux objets qui correspondent aux règles ACL de la table à caractère générique.

Remarque :
La règle ACL du champ générique (*.*) pour l'opération de création réutilise les mêmes conditions que l'opération d'écriture. Cela signifie que les conditions de création sont les mêmes que les conditions d'écriture, sauf si vous définissez une règle ACL d'opération de création explicite.

Plusieurs règles ACL au même point dans l'ordre de traitement

Si deux règles ou plus correspondent au même point de l'ordre de traitement, l'utilisateur doit passer l'une des conditions de règles ACL pour accéder à l'objet. Par exemple, si vous créez deux règles ACL de champ pour `incident.number`, un utilisateur qui transmet une règle a accès au champ Numéro, qu'il ait ou non échoué à une autre règle ACL de champ au même point de l'ordre de traitement.

Rôle requis

Les utilisateurs administrateurs normaux peuvent afficher et déboguer les règles de contrôle d'accès. Toutefois, pour créer ou mettre à jour des règles de contrôle d'accès existantes, les administrateurs doivent élever les privilèges au rôle security_admin. Consultez les Élever à un rôle privilégié pour obtenir les instructions.

Règles ACL dans les applications incluses dans le périmètre

Vous pouvez créer des règles ACL pour les objets dans le même champ d'application que la règle ACL. Vous pouvez également créer des règles ACL pour les tables comportant au moins un champ qui se trouve dans le même champ d'application que la règle ACL.

Pour les tables qui sont dans un champ d'application différent de l'enregistrement de règle ACL, les types de règles sont limités.

- Vous pouvez créer une règle ACL pour n'importe quelle table, page d'interface utilisateur ou autre objet dans le même champ d'application que la règle ACL.
- Vous pouvez créer une ACL pour un champ qui est dans le même périmètre que la règle ACL.
  - Si la table est dans le même périmètre, vous pouvez utiliser un script pour évaluer les conditions.
  - Si la table se trouve dans un périmètre différent, vous ne pouvez pas utiliser de script pour évaluer les conditions.
- Vous ne pouvez pas créer ni modifier les règles ACL pour les objets qui se trouvent dans un périmètre différent de celui de l'application que vous avez sélectionnée dans le sélecteur d'application, y compris ajouter un rôle à un ACL d'un périmètre différent.
- Vous pouvez créer des règles de table génériques (*) uniquement dans le champ d'application global.
- Vous pouvez créer des règles de champ génériques (*) uniquement pour les tables dans le même champ d'application que la règle ACL.

Types de règles ACL

Créez des règles ACL sur différents composants du système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Règles ACL d'enregistrement

Les règles ACL d'enregistrement comprennent des noms de tables et de champs.

- Le nom de table correspond à la table que vous souhaitez sécuriser. Si d'autres tables s'étendent à partir de cette table, alors la table est considérée comme une table parente. Les règles ACL pour les tables parentes s'appliquent à toute table qui étend la table parente.
- Le nom du champ est le champ que vous souhaitez sécuriser. Certains champs font partie de plusieurs tables en raison de l'extension de table. Les règles ACL pour les champs d'une table parente s'appliquent à toute table qui étend la table parente.

Les règles ACL peuvent sécuriser les opérations d'enregistrement suivantes :

Opération	Description
créer	Permet aux utilisateurs d'insérer de nouveaux enregistrements (lignes) dans une table.
lu	Permet aux utilisateurs d'afficher les enregistrements d'une table.
write	Permet aux utilisateurs de mettre à jour les enregistrements d'une table.
supprimer	Permet aux utilisateurs de supprimer des enregistrements d'une table ou de supprimer une table.
edit_task_relations	Permet aux utilisateurs d'étendre la table Tâche [task].
edit_ci_relations	Permet aux utilisateurs d'étendre la table Élément de configuration [cmdb_ci].
save_as_template	Permet aux utilisateurs d'enregistrer un enregistrement en tant que modèle.
add_to_list	Empêche les utilisateurs d'afficher ou de personnaliser des colonnes spécifiques dans la mécanique de liste. **Remarque :** Les conditions et les scripts ne sont pas pris en charge.
list_edit	Permet aux utilisateurs de mettre à jour les enregistrements (lignes) d'une liste.
report_on	Permet aux utilisateurs de générer des rapports sur les tables.
report_view	Permet aux utilisateurs de générer des rapports sur les ACL de champ.
personalize_choices	Permet aux utilisateurs de configurer la table ou le champ.
query_exact	Permet aux utilisateurs de soumettre des requêtes de correspondance (« est », « n'est pas », « est vide », etc.).
query_range	Permet aux utilisateurs de soumettre des requêtes de plage (« commence par », « se termine par », « contient », etc.) et le tri n'est pas restreint.

Les règles ACL d'enregistrement sont traitées dans l'ordre suivant :

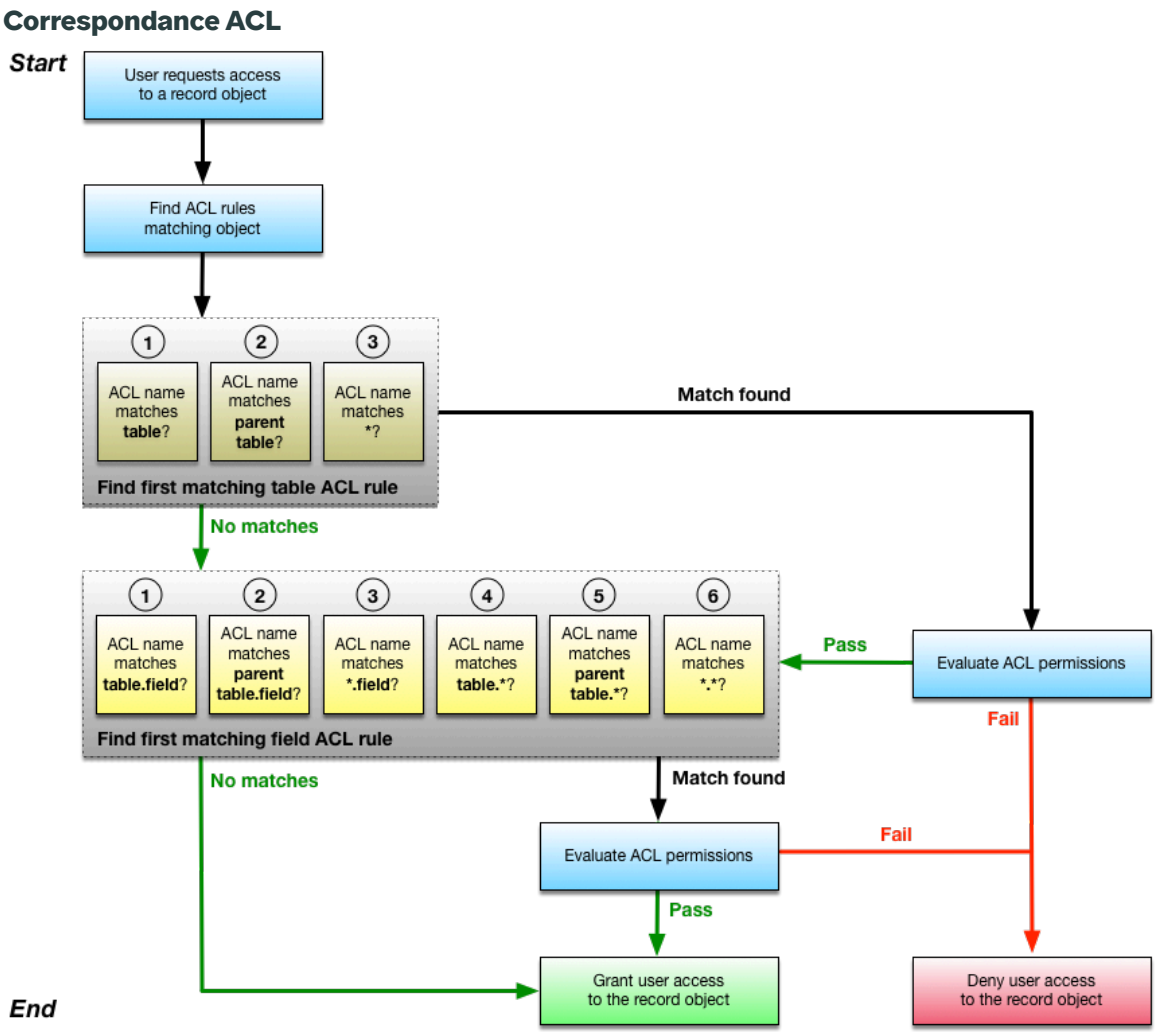
- Faites correspondre l'objet aux règles ACL de table.
- Faites correspondre l'objet aux règles ACL de champ.

Cet ordre de traitement garantit que les utilisateurs ont accès à des objets plus spécifiques avant d'accéder à des objets plus généraux. Un utilisateur doit transmettre les règles ACL de table et de champ pour accéder à un objet d'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si un utilisateur échoue à une règle ACL de table, l'accès à tous les champs de la table lui est refusé, même s'il transmet une règle ACL de champ.
- Si un utilisateur transmet une règle ACL de table, mais qu'il échoue à une règle ACL de champ, il ne peut pas accéder au champ décrit par la règle ACL de champ.



Règles ACL de processeur

Les règles ACL de processeur spécifient le processeur que vous voulez sécuriser. Pour obtenir la liste des processeurs disponibles, accédez à **Définition du système** > **Processeurs**.

Par défaut, une règle ACL pour EmailClientProcessor est incluse afin de restreindre le client de messagerie aux utilisateurs disposant du rôle itil.

Les règles ACL de processeur respectent la règle STAR (*) si elles ne peuvent pas trouver d'ACL plus spécifique pour ces ressources.

Règles ACL de table

L'utilisateur doit d'abord transmettre la règle ACL de table. Étant donné que le système de base inclut des règles ACL de table STAR (*) qui correspondent à toutes les tables, l'utilisateur doit toujours transmettre au moins une règle ACL de table. Le système de base fournit des règles ACL de table supplémentaires pour contrôler l'accès à des tables spécifiques.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les règles ACL de table sont traitées dans l'ordre suivant :

1. Correspond au nom de la table. Par exemple, incident.
2. Correspond au nom de la table parente. Par exemple, tâche.
3. Correspond à n'importe quel nom de table (*). Par exemple*.

Si un utilisateur échoue à toutes les règles ACL de table, il ne peut accéder à aucun champ de la table. Si un utilisateur transmet une règle ACL de table, le système évalue ensuite les règles ACL de champ.

Règles ACL de champs

Lorsqu'un utilisateur transmet une règle ACL de table, les règles ACL de champ sont traitées dans l'ordre suivant :

1. Faites correspondre le nom de la table et du champ. Par exemple, incident.number.
2. Faites correspondre la table parente et le nom du champ. Par exemple, task.number.
3. Correspond à n'importe quel nom de table (*) et de champ. Par exemple, *.number.
4. Faites correspondre la table et n'importe quel champ (*). Par exemple, incident.*.
5. Faites correspondre la table parente et n'importe quel champ (*). Par exemple, task.*.
6. Mettez en correspondance n'importe quelle table (*) et n'importe quel champ (*). Par exemple*.*.

Un utilisateur doit transmettre la règle ACL de table pour avoir accès aux champs de la table. Par exemple, l'utilisateur doit d'abord transmettre la règle ACL de table pour la table d'incidents afin d'accéder au champ **Numéro** de la table d'incidents.

La première évaluation réussie de l'ACL de champ arrête le traitement des règles ACL au niveau du champ. Lorsqu'un utilisateur transmet une règle ACL de champ, le système arrête de rechercher d'autres règles ACL de champ correspondantes. Par exemple, si un utilisateur transmet la règle ACL de champ pour incident.number, le système arrête de rechercher d'autres règles ACL qui sécurisent le champ **Numéro** dans la table d'incident.

L'accès aux informations de requête des données déduites est restreint pour les champs protégés, empêchant ainsi le retour d'informations prédictives.

Règles ACL de la page d'interface utilisateur

Les règles ACL de page d'interface utilisateur spécifient la page d'interface utilisateur à sécuriser. Pour obtenir la liste des pages de l'interface utilisateur disponibles, accédez à **Interface utilisateur du système** > **Pages de l'interface utilisateur**. Lors de la définition d'une règle ACL pour une page d'interface utilisateur, utilisez le nom de page dans le champ d'application complet. Par exemple, **x_myapp_mypage**.

Remarque :
Vous pouvez utiliser le caractère ÉTOILE (*) dans le champ **Nom** sur les ACL **de type ui_page** pour correspondre à n'importe quelle page de l'interface utilisateur.

Les règles ACL de page d'interface utilisateur respectent la règle STAR (*) si elles ne peuvent pas trouver une ACL plus spécifique pour ces ressources. Par exemple, si vous avez une page d'interface utilisateur nommée `mysecretpage` , mais que vous ne définissez pas d'ACL pour cette page d'interface utilisateur, la règle STAR (*) du processeur de page d'interface utilisateur est utilisée pour la vérification d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les règles ACL peuvent sécuriser l'opération de page d'interface utilisateur suivante :

Opération	Description
lu	Permet aux utilisateurs d'afficher la page de l'interface utilisateur.

Règles ACL du script include pouvant être appelé par le client

Les règles ACL de script include spécifient l'include de script pouvant être appelé par le client à sécuriser. Pour obtenir la liste des includes de script disponibles, accédez à **Définition du système** > **Includes de script**. Vous pouvez personnaliser la liste pour afficher la colonne *Client pouvant être appelé* .

Le système de base n'inclut aucune règle ACL pour les includes de script pouvant être appelés par le client.

Les règles ACL d'include de script pouvant être appelées par le client respectent la règle STAR (*) s'ils ne peuvent pas trouver d'ACL plus spécifique pour ces ressources.

Contrôle ACL des champs de fonction

Lors de l'évaluation de l'accès à un champ de fonction, en plus de vérifier l'accès au champ de fonction lui-même, le système vérifie également l'accès aux champs de contribution de la fonction. Les champs de contribution sont ceux utilisés comme arguments dans une définition de fonction donnée.

Pour plus d'informations sur les champs de fonction, reportez-vous à la rubrique Champ de fonction .

À partir Rome des années précédentes, le système vérifie simplement l'accès au champ de fonction lui-même (comme pour n'importe quel autre champ). Si les ACL de ce champ autorisent l'accès, l'utilisateur reçoit la valeur résultante, qu'il ait ou non accès aux champs de contribution.

À partir Xanadu des versions ultérieures, le système nécessite également l'accès à tous les champs de contribution afin de permettre l'accès au champ de fonction. Si une ou plusieurs ACL de champ de contribution refusent l'accès, le champ de fonction refuse également l'accès.

Les seules opérations affectées par la nouvelle exigence sont read et report_view. Report_view a ses propres exigences supplémentaires.

Opération	Description
Opération de lecture	Un utilisateur a un accès en lecture à un champ de fonction uniquement si deux des conditions suivantes sont remplies : • L'utilisateur dispose d'un accès en lecture au champ de fonction. • L'utilisateur a un accès en lecture à tous les champs de contribution utilisés dans la fonction.
report_view opération	Un utilisateur a report_view accès à un champ de fonction uniquement si toutes les conditions suivantes sont remplies : • L'utilisateur a report_view accès au champ de fonction. • L'utilisateur a report_view accès à chacun des champs de contribution.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Opération	Description
	• Il existe une ACL de lecture de rôle uniquement, sans conditions et sans script, et l'utilisateur dispose de ce rôle. • L'utilisateur dispose d'un accès en lecture aux champs de contribution avec un rôle uniquement, de sorte que seuls les ACL sans condition ni script peuvent l'autoriser.

Exemples

Donné:

- Tableau : salaire
- Colonnes : base, bonus, total (tous sont des entiers dans cet exemple)
- Champ de fonction : La colonne Total est marquée comme un champ de fonction, avec la définition de fonction glidefunction :add(base, bonus).
- Champs de contribution : base et bonus, car ils sont utilisés dans la définition de la fonction
- Rôles : salary_admin, bonus_admin

Exemple 1 : Tous les champs autorisent l'accès

ACL	Résultat
Total, base, bonus : lire et report_view pour le rôle salary_admin, sans conditions ni scripts	Un utilisateur disposant du rôle salary_admin se voit accorder l'accès en lecture et report_view au total, car il possède le rôle requis.

Exemple 2 : le champ Contribution refuse l'accès en lecture

ACL	Résultat
• Total, base : lecture et report_view pour les salary_admin de rôle, sans conditions ni scripts • Bonus : report_view pour le rôle salary_admin, sans conditions ni scripts • Bonus : Lecture pour le rôle bonus_admin, sans conditions ni scripts	Un utilisateur ayant le rôle salary_admin se voit refuser l'accès en lecture et report_view au total, car le bonus refuse l'accès en lecture à son rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple 3 : l'ACL du champ Contribution comporte un script

ACL	Résultat
• Total, base : lecture et report_view pour les salary_admin de rôle, sans conditions ni scripts • Bonus : report_view pour le rôle bonus_admin, sans conditions ni scripts • Bonus : lisez pour le rôle salary_admin, avec un script (notez que ce qu'il y a dans le script n'a pas d'importance, seulement qu'il soit là)	Un utilisateur ayant le rôle salary_admin se voit accorder un accès en lecture à Total, car il possède le rôle requis pour tous les champs. Mais l'accès est refusé report_view même utilisateur avec le salary_admin, car l'ACL de lecture avec le script refuse l'accès par défaut dans ce cas, même s'il dispose du rôle requis.

Démarrage rapide de la sécurité - Module d'extension des règles ACL

Le module d'extension de niveau de contrôle d'accès de démarrage rapide de la sécurité (règles ACL) est installé automatiquement sur toutes les nouvelles instances. Utilisez ce module d'extension pour sécuriser rapidement plusieurs tables système et accélérer le processus de lancement de production pour votre organisation.

Ce module d'extension n'est pas conçu pour les instances existantes, car il peut altérer l'accès de sécurité aux tables déjà utilisées dans un environnement de production. Si un administrateur souhaite fortement installer ce module d'extension sur une instance existante, il doit d'abord le tester minutieusement dans une instance de test. Cela permet de vérifier la compatibilité avec l'implémentation actuelle de l'organisation.

Si un administrateur est intéressé par les nouvelles règles ACL fournies par ce module d'extension, il peut en créer une ou plusieurs manuellement dans une instance existante, en utilisant la liste des ACL comme guide.

Les ACL suivantes sont incluses dans ce module d'extension. Sélectionnez l'icône dans une ligne d'en-tête pour trier cette colonne par ordre croissant ou décroissant. La touche Opération est la suivante :

- R = lecture
- W = écriture
- D=supprimer
- C=créer

Nom	Opération	Description
cmdb_ci	WCD (en anglais seulement)	Rôle actif ou ITIL requis pour écrire/créer/supprimer des enregistrements d'éléments de configuration
cmn_department	Naine blanche	user_admin rôle requis pour écrire/supprimer des enregistrements de département
cmn_location	TOILETTE	user_admin rôle requis pour écrire/créer des enregistrements d'emplacement

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
core_company	Naine blanche	user_admin rôle requis pour écrire/supprimer des enregistrements de société
kb_knowledge	créer	rôle de la base de connaissances requis pour créer des enregistrements de la base de connaissances
ldap_ou_config	RWCD (en anglais seulement)	user_admin rôle requis pour lire/écrire/créer/supprimer des enregistrements de définition LDAP OU
ldap_server_config	RWCD (en anglais seulement)	user_admin rôle requis pour lire/écrire/créer/supprimer des enregistrements de serveur LDAP
process_guide	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements du guide de processus
process_step	WCD (en anglais seulement)	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements d'étapes du processus
sc_category	créer	catalog_admin rôle requis pour créer des enregistrements de catégorie de Catalogue de services
sc_category	supprimer	catalog_admin rôle requis pour supprimer des enregistrements de catégorie de Catalogue de services
sc_category	write	catalog_admin rôle requis pour écrire dans les enregistrements de catégorie de Catalogue de services
sc_cat_item	write	catalog_admin rôle requis pour écrire dans des enregistrements d'éléments de catalogue
sc_cat_item	supprimer	catalog_admin rôle requis pour supprimer des enregistrements d'éléments de catalogue
sc_cat_item	créer	catalog_admin rôle requis pour créer des enregistrements d'éléments de catalogue
sysevent_email_action	lu	tous les utilisateurs peuvent lire les enregistrements de notification par e-mail (à des fins d'abonnement)
sysevent_register	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements du registre des événements
sysevent_script_action	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements d'action des scripts
syslog	RWCD (en anglais seulement)	administrateur tenu de lire/écrire/créer/supprimer des enregistrements d'entrée de journal
règle système	RWCD (en anglais seulement)	administrateur tenu de lire/écrire/créer/supprimer des enregistrements de règles (notifications par e-mail, actions d'e-mail entrant, règles d'approbation, etc.)
règle système	lu	tous les utilisateurs peuvent lire les enregistrements de notification par e-mail pour (notifications basées sur un abonnement)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
sys_app_application	WCD (en anglais seulement)	administrateur tenu d'écrire/créer/supprimer des enregistrements d'applications
sys_app_category	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de catégorie d'application
sys_app_module	WCD (en anglais seulement)	administrateur tenu d'écrire/créer/supprimer des enregistrements de module
sys_audit	RWCD (en anglais seulement)	administrateur tenu de lire/écrire/créer/supprimer des enregistrements d'audit
sys_dictionary	RWC	personalize_dictionary rôle requis pour lire/écrire/créer des enregistrements de dictionnaire
sys_dictionary.*	lu	personalize_dictionary rôle peut lire les champs du dictionnaire
sys_documentation	supprimer	Le rôle « personalize_dictionary » est requis pour supprimer des enregistrements d'étiquette de champ.
sys_documentation	créer	Le rôle « personalize_dictionary » est requis pour créer des enregistrements d'étiquette de champ.
sys_documentation	write	Le Rôle « personalize_dictionary » est requis pour écrire dans des enregistrements d'étiquette de champ.
sys_gauge	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de jauge
sys_gauge_count	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de nombre de jauges
sys_group_has_role	lu	Rôle itil requis pour afficher les enregistrements de rôles de groupe
sys_home	WCD (en anglais seulement)	itil_admin rôle requis pour écrire/créer/supprimer des enregistrements de section de page d'accueil
sys_installation_exit	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de sortie d'installation
sys_job	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de tâches système
sys_nav_link	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de lien de navigation
sys_perspective	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de liste de menu

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
sys_portal	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements du portail
sys_portal_page	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de la page d'accueil
sys_portal_preferences	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements de préférences du portail
sys_processor	TOILETTE	Le rôle administrateur est requis pour écrire/créer des enregistrements de processeur
sys_properties	TOILETTE	Le rôle administrateur est requis pour écrire/créer des enregistrements de propriétés système.
sys_properties_category	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de catégorie de propriété
sys_report	supprimer	Rôles pouvant supprimer des enregistrements de rapports (ne restreint pas la suppression via l'interface utilisateur de rapport)
sys_report	write	Rôles pouvant écrire dans des enregistrements de rapports (ne restreint pas la modification via l'interface utilisateur de rapport)
sys_report	lu	Les utilisateurs peuvent lire leurs propres enregistrements de rapports, ceux de leur groupe et les enregistrements GLOBAUX (n'affecte pas l'affichage via l'interface utilisateur du rapport)
sys_report	lu	rôles qui peuvent lire les enregistrements de rapports (ne restreint pas l'affichage via l'interface utilisateur du rapport)
sys_reportroles	lu	le rôle administrateur est requis pour lire les enregistrements des rôles de rapport
sys_script	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de règle métier
sys_script_ajax	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de script AJAX
sys_script_client	WCD (en anglais seulement)	le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements de script client
sys_script_include	WCD (en anglais seulement)	Le rôle administrateur est requis pour écrire/créer/supprimer des enregistrements d'include de script
sys_security_acl	write	Rôle administrateur requis pour écrire dans les enregistrements de contrôle d'accès
sys_security_acl_role	créer	Le rôle administrateur est requis pour créer des enregistrements de rôles d'accès
sys_security_acl_role	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements des rôles d'accès

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
sys_security_acl_role	write	le rôle administrateur est requis pour écrire dans les enregistrements des rôles d'accès
sys_security_operation	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements des opérations de sécurité
sys_security_operation	créer	Le rôle administrateur est requis pour créer des enregistrements d'opérations de sécurité.
sys_security_operation	write	Rôle administrateur requis pour écrire dans les enregistrements d'opérations de sécurité
sys_security_operation	query_range	
sys_security_operation		
sys_security_type	write	Le rôle administrateur est requis pour écrire dans les enregistrements de type de sécurité
sys_security_type	créer	Le rôle administrateur est requis pour créer des enregistrements de type de sécurité
sys_security_type	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements de type de sécurité
sys_status	créer	Le rôle administrateur est requis pour créer des enregistrements de l'état du système
sys_status	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements de l'état du système
sys_status	write	Le rôle administrateur est requis pour écrire dans les enregistrements d'état du système
sys_template	write	template_editor rôle requis pour écrire dans des enregistrements de modèles
sys_template	créer	emplate_editor rôle requis pour créer des enregistrements de modèles
sys_template	supprimer	template_editor rôle requis pour supprimer des enregistrements de modèles
sys_template	lu	template_editor rôle requis pour lire les enregistrements de rôles de modèle
sys_ui_action	créer	Le rôle administrateur est requis pour créer des enregistrements d'action d'interface utilisateur
sys_ui_action	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements d'action d'interface utilisateur
sys_ui_action	write	Le rôle administrateur est requis pour écrire dans les enregistrements d'action d'interface utilisateur
sys_ui_action_view	write	Rôle administrateur requis pour écrire dans les enregistrements d'action de vue de l'interface utilisateur
sys_ui_action_view	créer	Rôle administrateur requis pour créer des enregistrements d'action de vue de l'interface utilisateur
sys_ui_action_view	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements d'action de vue de l'interface utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Nom	Opération	Description
sys_ui_policy	créer	rôle administrateur requis pour créer des enregistrements de politique d'interface utilisateur
sys_ui_policy	supprimer	le rôle administrateur est requis pour supprimer des enregistrements de politique d'interface utilisateur
sys_ui_policy	write	le rôle administrateur est requis pour écrire dans les enregistrements de politique d'interface utilisateur
sys_ui_policy_action	créer	Le rôle administrateur est requis pour créer des enregistrements d'action de politique d'interface utilisateur
sys_ui_policy_action	supprimer	Le rôle administrateur est requis pour supprimer les enregistrements d'action de politique d'interface utilisateur
sys_ui_policy_action	write	le rôle administrateur est requis pour écrire dans les enregistrements d'action de politique d'interface utilisateur
sys_ui_script	write	le rôle administrateur est requis pour écrire dans les enregistrements de script d'interface utilisateur
sys_ui_script	supprimer	le rôle administrateur est requis pour supprimer des enregistrements de script d'interface utilisateur
sys_ui_script	créer	Le rôle administrateur est requis pour créer des enregistrements de script d'interface utilisateur
sys_user	write	Les utilisateurs sans rôle ne peuvent pas mettre à jour un enregistrement d'utilisateur autre que le leur
sys_user_grmember	supprimer	user_admin rôle requis pour supprimer les enregistrements des membres du groupe
sys_user_grmember	write	user_admin rôle requis pour écrire dans les enregistrements de membres du groupe
sys_user_group	créer	Seuls ITIL et une version supérieure peuvent créer des enregistrements de groupe
sys_user_group	write	Seuls ITIL et les versions supérieures peuvent écrire dans les enregistrements de groupe
sys_user_has_role	lu	Rôle itil requis pour afficher les enregistrements de rôle d'utilisateur
sys_user_role	créer	Rôle administrateur requis pour créer des enregistrements de rôles
sys_user_role	supprimer	Le rôle administrateur est requis pour supprimer des enregistrements de rôle
sys_user_role	write	Rôle administrateur requis pour écrire dans les enregistrements de rôles
sys_user_role_contains	lu	Rôle itil requis pour afficher les enregistrements de rôles contenus
sys_user_role_contains	write	le rôle administrateur est requis pour écrire dans les enregistrements de rôles contenus
sys_user_token	RWCD (en anglais seulement)	le rôle administrateur est requis pour lire/écrire/créer/supprimer des enregistrements à jeton d'utilisateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Démarrage rapide de la sécurité (règles ACL) (renforcement de la sécurité de l'instance) dans les paramètres de renforcement de la sécurité de l'instance.

Configuration d'une règle ACL

Configurez une règle ACL personnalisée pour sécuriser l'accès à de nouveaux objets ou pour modifier le comportement de sécurité par défaut.

Avant de commencer
Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche
Pour créer des règles ACL, vous devez élever les privilèges au rôle security_admin.

Pour les tables qui sont dans un champ d'application différent de l'enregistrement de règle ACL, les types de règles sont limités. Pour que les tables principales du champ d'application dérivent le champ d'application et exécutent des ACL incluses dans le champ d'application, définissez la `glide.enforce_security_scope.<scope_name>` propriété sur **true**. Cela garantit que les ACL du champ d'application global ne correspondent pas lorsque des ACL spécifiques au champ d'application sont créées dans la table pertinente. Par exemple, lors de la sécurisation des données dans des tables d'applications partagées dans le périmètre global, telles que les tables sys_attachment ou question_answer.

Procédure

1. Rôles de privilège élevés au rôle security_admin.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès (ACL)**.
3. **Conseil :**
   Lors de la création d'une ACL, il est utile d'examiner le Refuser à moins qu'ACLfichier .

   Cliquez sur **Nouveau**.
4. Renseignez le formulaire.

Champs de contrôle d'accès

Champ	Description
Type	Sélectionnez le type d'objet sécurisé par cette règle ACL. Le type d'objet détermine la façon dont l'objet est nommé et les opérations disponibles. Ce champ passe en lecture seule une fois la règle ACL créée. Si vous souhaitez modifier le type, vous devez supprimer l'ACL et en créer une nouvelle avec le type approprié.
Opération	Sélectionnez l'opération sécurisée par cette règle ACL. Chaque type d'objet possède sa propre liste d'opérations. Une règle ACL ne peut sécuriser qu'une seule opération. Pour sécuriser plusieurs opérations, créez une règle ACL distincte pour chacune d'elles.
Remplacement administrateur	Cochez cette case pour que les utilisateurs dotés du rôle administrateur passent automatiquement la vérification des autorisations pour cette règle ACL. Les utilisateurs administrateurs transmettent, quelles que soient les restrictions de script ou de rôle qui s'appliquent. Toutefois, le rôle **personne** , que seul ServiceNow le personnel peut affecter, a priorité sur l'option de remplacement administrateur. Si le rôle **personne** est affecté à une ACL, les utilisateurs administrateurs ne peuvent pas accéder à

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la ressource, même lorsque l'option **Remplacements administrateur** est sélectionnée. Reportez-vous à la section Rôles système de base . Décochez cette case si les administrateurs doivent satisfaire aux autorisations définies dans cette règle ACL pour accéder à l'objet sécurisé. Étant donné que les administrateurs réussissent toujours les vérifications de rôle (voir la description du champ **Requiert un rôle**), utilisez le créateur de conditions ou le champ **Script** pour créer une vérification des autorisations que les administrateurs doivent passer.
Actif	Cochez cette case pour appliquer cette règle ACL.
Avancés	Cochez cette case pour afficher le champ **de script** . **Important :** S'il y a un script dans le champ **Script** . Ce script s'exécute même si le champ n'est pas affiché sur le formulaire.
Nom	Saisissez le nom de l'objet sécurisé, soit le nom de l'enregistrement, soit les noms de table et de champ. Plus le nom est spécifique, plus la règle ACL est spécifique. Vous pouvez utiliser le caractère générique astérisque (*) à la place d'un nom d'enregistrement, de table ou de champ pour sélectionner tous les objets qui correspondent à un type d'enregistrement, toutes les tables ou tous les champs. Vous ne pouvez pas combiner un caractère générique et une recherche de texte. Par exemple, inc* n'est pas un nom de règle ACL valide, mais incident.* et *.number sont des noms de règles ACL valides. **Remarque :** Cliquez sur le triangle bleu pour entrer manuellement le nom de l'enregistrement ou les noms de table et de champ de l'objet sécurisé. Utilisez cette option pour sécuriser un objet qui n'apparaît pas dans la liste déroulante.
Description	Entrez une description de l'objet ou des autorisations que cette règle ACL sécurise.
Demande un rôle	Utilisez cette liste pour spécifier les rôles qu'un utilisateur doit avoir pour accéder à l'objet. Si vous répertoriez plusieurs rôles, un utilisateur disposant de l'un des rôles répertoriés peut accéder à l'objet. La liste *Requiert un rôle* apparaît sous la forme d'une liste connexe. **Remarque :** Les utilisateurs disposant du rôle administrateur réussissent toujours cette vérification d'autorisation, car le rôle administrateur accorde automatiquement aux utilisateurs tous les autres rôles.
Condition	Utilisez ce créateur de conditions pour sélectionner les champs et les valeurs qui doivent être vrais pour que les utilisateurs puissent accéder à l'objet.
Script	Saisissez un script personnalisé décrivant les autorisations requises pour accéder à l'objet. Le script peut utiliser les valeurs des variables globales *actuelles* et *précédentes* dans les règles métier ainsi que dans les propriétés système. Le script doit générer une réponse vrai ou faux de l'une des deux façons suivantes : ○ Renvoyer un jeu de variables de *réponse* sur une valeur vrai ou faux ○ Évaluer à vrai ou faux Dans les deux cas, les utilisateurs n'ont accès à l'objet que lorsque le script est défini sur vrai et que l'utilisateur remplit toutes les conditions de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la règle ACL. Les conditions et le script doivent être définis sur vrai pour qu'un utilisateur puisse accéder à l'objet. **Remarque :** Si l'élément évalué se trouve dans une liste connexe, **current** pointe vers l'élément sur lequel se trouve la liste associée, et non vers l'élément actuel auquel l'ACL est destinée. Toutefois, si l'élément dont vous évaluez l'ACL ne se trouve pas dans une liste connexe, **actuel** pointe vers l'élément réel.

5. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis sélectionnez **Enregistrer**.

Refuser à moins qu'ACL

En savoir plus sur les ACL de refus.

Les ACL « refuser-sauf » sont évaluées à l'aide d'une approche « refuser-sauf si ». L'ACL définit les utilisateurs qui ne seront PAS refusés. En d'autres termes, l'accès sera refusé à l'utilisateur **sauf si** les conditions requises par le rôle, la condition et le script sont remplies.

Important :
Les ACL Refuser à moins que la liste de contrôle d'accès ait la priorité sur les ACL Autoriser si dans l'évaluation des ACL, car elle sera évaluée en premier.

Une ACL refus à moins produit 2 résultats

Résultat de l'évaluation	Résultat
Succès	Les rôles, les conditions de données, les attributs de sécurité et les exigences de script définis sont remplis. L'ACL procède à une évaluation plus approfondie **Important :** Les ACL d'autorisation If doivent toujours accorder l'accès pour que le sujet puisse accéder à la ressource.
Échec	L'ACL refuser-sauf si elle est marquée comme défaillante et l'accès sera refusé.

Voici un exemple expliqué d'ACL de refus à moins que :

- ACL a les rôles sn_hr_core.manager et itil
- La condition a actif = vrai
- script a une réponse = gs.isLoggedIn() ;

L'accès est refusé à l'utilisateur sauf si les 3 conditions requises de cette ACL sont satisfaites. Pour que cette ACL de refus à moins que cette ACL ne soit réussie, un utilisateur doit avoir le rôle sn_hr_core.manager ou itil , accéder à un enregistrement qui a le champ actif = true et être connecté. L'ACL Refus sauf si l'une des trois conditions n'est pas remplie.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ACL de requête

Les ACL de requête vous permettent de définir un contrôle d'accès plus granulaire en définissant explicitement qui peut interroger les données.

Qu'est-ce qu'une ACL de requête ?

L'opération des ACL de requête est définie sur `query_range` ou `query_match`. Les ACL de requête permettent un contrôle plus spécifique des requêtes utilisateur, en restreignant ou en activant l'accès en fonction de leur configuration. Les ACL de requête sont des outils puissants contre les attaques par requête aveugle, où un attaquant interroge aveuglément les données pour extraire des informations des résultats, même s'il ne peut pas voir les valeurs.

Quand utiliser une ACL de requête

Lorsqu'une colonne contient des valeurs sensibles et autorise un accès partiel/conditionnel aux données, une ACL de requête doit être envisagée et implémentée si nécessaire en fonction de la sensibilité des données. En cas d'accès partiel/conditionnel aux lignes et à leurs colonnes dans les tables, en particulier lorsque cet accès n'est pas renforcé par des filtres de données, des ACL de requête doivent être implémentées si nécessaire en fonction de la sensibilité des données.

Remarque :
Prenez en compte les ACL de requête lorsque certains utilisateurs ont accès à certaines lignes ou colonnes et pas à d'autres.

Example: Contrôle de requête de paie

Je peux voir une ligne dans le tableau des salaires avec mon salaire, mais il n'y a aucune raison pour que je puisse émettre des requêtes de plage pour interroger les utilisateurs avec un salaire contenu dans 2 limites. Une ACL `query_range` sur le salaire m'empêcherait d'émettre cette requête.

Example: Contrôle de requête RH

Je peux voir tous les hr_profiles, mais je ne peux voir le SSN que pour moi-même. Je n'ai aucune tâche à interroger le SSN, et les ACL de requête doivent m'empêcher d'exécuter des requêtes sur le SSN d'autres profils RH pour essayer d'extraire des mappages SSN.

Comportement de l'ACL de requête

Les ACL de requête utilisent des opérations `query_match` et `query_range` pour un comportement d'interrogation de table sécurisé et granulaire. Leurs comportements sont décrits ci-dessous :

`query_match`

`query_match` est composé de : EQUALS, NOT_EQUALS, IN, NOT_IN, SAMEAS, NSAMEAS, ANYTHING, ISEMPTYSTRING, ISEMPTY, ISNOTEMPTY, ISNULL, ISNOTNULL. `query_match` est fait des « opérateurs sûrs », dans le sens où ils sont conçus pour récupérer des enregistrements spécifiques et ne peuvent pas être exploités pour en renvoyer d'autres.

Résultat de l'évaluation	Résultat
Succès	L'utilisateur peut soumettre des requêtes de correspondance

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Résultat de l'évaluation	Résultat
Échec	L'utilisateur ne sera pas en mesure de soumettre des requêtes de correspondance : • ÉGALE • NOT_EQUALS • DANS • NOT_IN • IDENTIQUES • NSAMEAS (en anglais seulement) • RIEN • CHAÎNE ISEMPTYSTRING • EST VIDE • ISNOTEMPTY • ISNULL (en anglais seulement) • ISNOTNULL (en anglais seulement)

`query_range`

`query_range` est composé de tous les autres (STARTS_WITH, CONTAINS, >=, <=, etc.) qui sont plus dangereux car ils permettent aux utilisateurs de demander plus d'enregistrements en ajustant les valeurs de limite.

Résultat de l'évaluation	Résultat
Succès	L'utilisateur peut soumettre des requêtes de plage et le tri n'est pas restreint
Échec	L'utilisateur ne sera pas en mesure de soumettre des requêtes de plage avec (STARTS_WITH, CONTAINS, >=, <=, etc. Le tri par colonne est restreint

Important :

Les ACL de requête (query_match et query_range) sont par défaut une ACL star.star qui délègue l'accès en lecture. Cela signifie que, lorsque les ACL sont appliquées aux requêtes, si aucune ACL de requête n'a été créée, l'accès en lecture à la colonne est évalué ; si les ACL de requête sont définies, elles remplacent le comportement par défaut.

Sécuriser les enregistrements dans une liste incorporée

Pour appliquer la sécurité aux enregistrements des listes incorporées, limitez la modification et la suppression des enregistrements des listes incorporées à des rôles spécifiques.

Avant de commencer

Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Contrôle d'accès (ACL)**.
2. Ouvrez l'enregistrement **Écriture** ou **Suppression** de la table appropriée.
3. Dans la section Exige un rôle du formulaire, ajoutez les rôles qui ont l'autorisation d'écriture ou de suppression pour cette table.
4. Enregistrez les changements.
   Lorsque les enregistrements de la table associée apparaissent dans une liste incorporée, les options de modification et de suppression ne sont disponibles que pour les utilisateurs ayant les rôles spécifiés.

Gestionnaire de sécurité contextuelle

Le Gestionnaire de sécurité contextuelle protège vos données en contrôlant les autorisations de lecture, d'écriture, de création et de suppression.

Avantages clés

Le gestionnaire de sécurité contextuelle connaît la hiérarchie des tables système, ce qui vous permet de créer des règles de sécurité spécifiques pour un champ en fonction de l'endroit où il est affiché dans la hiérarchie. Les avantages du gestionnaire de sécurité contextuelle incluent :

- **Sécurité contextuelle** : sécurisez un enregistrement en fonction de son contenu.
- **Sécurité hiérarchique** : appliquez des règles de sécurité à n'importe quel niveau de la hiérarchie des objets.

Sécurisation des champs et des tables

Avec l'ancien Simple Security Manager, vous pouviez sécuriser les champs et les tables en ajoutant des rôles à l'entrée de dictionnaire appropriée. Avec le Gestionnaire de sécurité contextuelle, ces rôles de dictionnaire ne sont plus testés. Au lieu de cela, le système recherche des règles ACL sur les champs et les tables.

⚠ Avertissement :
Après avoir installé le gestionnaire de sécurité contextuelle, vous devez sécuriser les champs et les tables via les règles ACL. Même si vous configurez la mise en page du formulaire de dictionnaire et que vous ajoutez des rôles à une entrée de dictionnaire, aucun changement dans les droits ne se produit.

Sécurité contextuelle et rôles

Vous pouvez accorder des rôles aux utilisateurs ou aux groupes. Toutefois, après l'installation du gestionnaire de sécurité contextuelle, le champ **Rôles** de l'enregistrement utilisateur n'est plus vérifié et n'apparaît plus sur vos formulaires d'utilisateur et de groupe. Au lieu de cela, vous devez ajouter des rôles à la liste connexe Rôles plutôt qu'à l'enregistrement d'utilisateur ou de groupe.

Les applications et les modules contiennent des listes des rôles requis pour les afficher. Par exemple, le rôle administrateur est requis pour afficher l'application Définition du système. Les droits de sécurité pour les applications et les modules sont toujours définis à l'aide de tableaux de rôles.

Les éléments de catalogue et les variables de catalogue contiennent des listes des rôles requis pour les afficher. Les droits de sécurité pour les éléments de catalogue et les variables de catalogue sont toujours définis via ces tableaux de rôles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sous le Gestionnaire de sécurité contextuelle, un groupe hérite toujours automatiquement de tout rôle qui lui est accordé lorsque le marqueur d'héritage du rôle est défini sur *vrai*.

Activation du gestionnaire de sécurité contextuelle

Le gestionnaire de sécurité contextuelle est actif dans le système de base. S'il y a beaucoup d'entrées en double dans la table Rôles d'utilisateur, vous devrez peut-être effectuer une mise à niveau vers Sécurité contextuelle : Gestion des rôles V2 pour éliminer les rôles en double. Les modules d'extension incluent :

Sécurité contextuelle : Gestion des rôles [com.glide.role_management]

Fournit une fonctionnalité de sécurité contextuelle. Ce module d'extension est installé automatiquement.

Sécurité contextuelle : Gestion des rôles V2 [com.glide.role_management.inh_count]

Empêche les entrées en double causées par les rôles hérités dans la table Rôles d'utilisateur [sys_user_has_role]. Ce module d'extension est automatiquement installé sur les nouvelles instances et peut être activé pour les mises à niveau. Le module d'extension Sécurité contextuelle : Améliorations de la gestion des rôles est une version précédente de ce module d'extension. Le module d'extension Role Management Enhancements n'inclut pas le script RoleManagementVerify(). Ce script renvoie une liste des changements qu'une mise à niveau effectuera, ce qui vous permet de surveiller les changements apportés par le module d'extension.

Remarque :
Après avoir activé Gestion des rôles V2, vous devez définir la propriété système glide.role_management.v2.audit_roles pour permettre à la table Rôles d'audit de créer des enregistrements d'audit liés aux rôles d'utilisateur. Pour en savoir plus sur la définition de cette propriété et sur la table Rôles d'audit, voir :

- Activer l'audit des rôles avec Sécurité contextuelle : Gestion des rôles V2.
- Module d'extension Sécurité contextuelle : Gestion des rôles dans les paramètres de sécurisation renforcée de la sécurité de l'instance.
- Rôles d'utilisateur d'audit

Empêcher les entrées en double avec Sécurité contextuelle : Gestion des rôles V2

Les rôles hérités d'autres rôles sont ajoutés en tant qu'entrées individuelles dans la table Rôles d'utilisateur [sys_user_has_role], ce qui peut entraîner des entrées en double pour un rôle. Sécurité contextuelle : Gestion des rôles V2 élimine ces entrées en double et empêche les doublons futurs.

Éliminez les entrées en double grâce au nombre d'héritages

Sécurité contextuelle : Gestion des rôles V2 utilise la colonne Nombre d'héritages (inh_count) pour suivre le nombre de fois qu'un rôle est hérité d'un autre rôle ou groupe. Dans la table Rôles d'utilisateur [sys_user_has_role], un utilisateur ne peut hériter d'un rôle spécifique qu'une seule fois, ce qui élimine les doublons. La colonne Nombre d'héritages (inh_count) est en lecture seule et calcule le nombre de fois que l'utilisateur hérite d'un rôle.

Changements apportés à l'activation

Sécurité contextuelle : Gestion des rôles V2 est automatiquement installé sur les nouvelles instances et peut être activé pour les mises à niveau. Lorsqu'il est activé, Sécurité contextuelle : Gestion des rôles V2 remplace à la fois Sécurité contextuelle et Sécurité contextuelle : améliorations de la gestion des rôles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Lorsque Sécurité contextuelle : Gestion des rôles V2 est activé, les colonnes suivantes sont déconseillées, mais restent dans la table Rôles d'utilisateur pour des raisons de rétrocompatibilité :

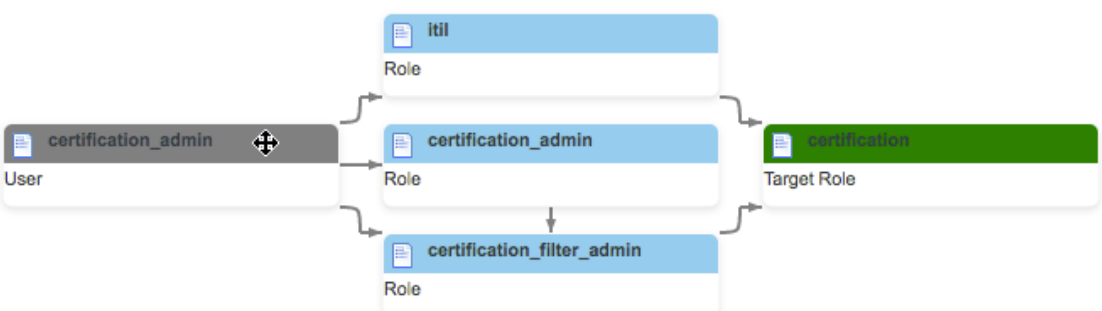
- granted_by (utilisé uniquement par la délégation de rôle)
- included_in_role
- included_in_role_instance

Avertissement :
Si ces colonnes sont utilisées dans des scripts personnalisés sur votre instance, n'effectuez pas de mise à niveau vers Gestion des rôles V2.

Visualiser l'héritage de rôle via la carte d'héritage de rôle

La carte d'héritage de rôles affiche une représentation visuelle des rôles hérités. Vous pouvez utiliser cette carte pour comprendre les rôles représentés dans la colonne Nombre d'héritages (inh_count). Pour afficher la carte d'héritage de rôles, configurez la table Rôles d'utilisateur [sys_user_has_role] pour afficher la colonne Carte d'héritage de rôles.

Carte d'héritage de rôle



Mise à niveau vers Sécurité contextuelle : Gestion des rôles V2

Sécurité contextuelle : Gestion des rôles V2 est automatiquement installé sur les nouvelles instances. Vous pouvez effectuer une mise à niveau de Sécurité contextuelle : Gestion des rôles vers Sécurité contextuelle : Gestion des rôles V2 pour éliminer les doublons de rôles dans la table Rôles d'utilisateur et empêcher de futurs doublons.

Avant de commencer

Rôle requis : admin, security_admin
Vous devez avoir le rôle admin et Élever à un rôle privilégié pour obtenir le rôle security_admin effectif.

Remarque :
Avant d'effectuer la mise à niveau vers Sécurité contextuelle : Rôle : Gestion V2, vous devez activer la table Rôles d'audit pour créer des enregistrements d'audit liés aux rôles d'utilisateur. Pour en savoir plus sur la définition de la propriété système requise, reportez-vous à la section Activer l'audit des rôles avec Sécurité contextuelle : Gestion des rôles V2.

Pourquoi et quand exécuter cette tâche

Cette procédure décrit comment mettre à niveau votre rôle de sécurité contextuelle et comment activer les modules d'extension connexes décrits dans le tableau suivant.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Modules d'extension pour Sécurité contextuelle : Gestion des rôles V2

Module d'extension	Description
Sécurité contextuelle : Gestion des rôles V2 [com.glide.role_management.inh_count]	Empêche les entrées en double dans la table Rôles d'utilisateur [sys_user_has_role]. Le rôle security_admin ou un utilisateur avec des privilèges élevés est requis pour activer le module d'extension, ou contactez Service et assistance client.
Sécurité contextuelle : API REST V2 de Gestion des rôles [com.glide.role_management.inh_count.rest_api]	Active la fonctionnalité d'API pour la gestion des rôles.

Avant d'effectuer une mise à niveau de Sécurité contextuelle : Gestion des rôles vers Sécurité contextuelle : Gestion des rôles V2, testez les résultats d'une mise à niveau en exécutant le script. Le script renvoie une liste des changements qu'une mise à niveau effectuera. Si les changements sont acceptables, installez le module d'extension Sécurité contextuelle : Gestion des rôles V2. Si les modifications ne sont pas acceptables, n'installez pas le module d'extension Sécurité contextuelle : Gestion des rôles V2. Vous pouvez également effectuer la mise à niveau, puis apporter manuellement les modifications nécessaires.

Procédure

1. Testez l'impact d'une mise à niveau avant la mise à niveau en exécutant le script suivant.

   a. Accédez à la **Définition du système** > **Scripts - Arrière-plan**.

   b. Exécuter le script suivant dans le périmètre global.

   ```
   new RoleManagementVerify().verifyInheritedRoles();
   ```

   Pour les tables sys_user_has_role volumineuses, l'exécution peut prendre jusqu'à plusieurs heures. Ne modifiez pas et n'ajoutez pas de rôles d'utilisateur pendant cette période.
   Exemple de résultat basé sur des données de test :

   ```
   *** Script: 2016-12-01 19:58:54 Starting checking of inherited roles for all users...
   *** Script: User: itam, inherited roles to be ADDED: financial_mgmt_user
   *** Script: User: bernard.laboy, inherited roles to be DELETED:
    api_analytics_read,pa_viewer,rest_api_explorer,a123
   *** Script: User: bernard.laboy, inherited roles to be ADDED: dependency_views
   *** Script: Number of inherited-role records in sys_user_has role, current: 260, after
    re-calculation: 258
   *** Script: Number of users with discrepancies for inherited roles: 2
   *** Script: 2016-12-01 19:58:55 Finished checking of inherited roles for all users!
   ```

   c. Évaluez les résultats du script pour déterminer si les changements proposés sont acceptables.

2. Activez le module d'extension Sécurité contextuelle : Gestion des rôles V2.

> **Important :**
> Le rôle security_admin ou un utilisateur avec des privilèges élevés est requis pour activer le module d'extension, ou contactez Service et assistance client.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Accédez à la **Définition du système** > **Modules d'extension**.

b. Recherchez et cliquez sur le nom du module d'extension.

c. Dans le formulaire Module d'extension système, examinez les détails du module d'extension, puis cliquez sur le lien connexe **Activer/Mettre à niveau** .

d. Cliquer sur **Activer**.

Résultats

Après l'activation de Gestion des rôles V2, les modifications décrites dans le résultat du script sont mises en œuvre. La colonne Nombre d'héritages (inh_count) de la table Rôles d'utilisateur est en lecture seule et reflète automatiquement le nombre de fois que l'utilisateur hérite d'un rôle.

Activer l'audit des rôles avec Sécurité contextuelle : Gestion des rôles V2

Définissez une propriété système pour activer la table Rôles d'audit afin de créer des enregistrements d'audit liés aux rôles d'utilisateur.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Lorsqu'elle est activée, la table Rôles d'audit [sys_audit_role] gère les changements apportés aux enregistrements utilisateur. Pour plus d'informations sur les audits de rôles, consultez Rôles d'utilisateurs d'audit . Si le module d'extension Sécurité contextuelle : Gestion des rôles V2 [com.glide.role_management.inh_count] est installé, vous devez définir une propriété système sur **vrai** pour activer l'audit des rôles.

Procédure

1. Accédez à la table Propriétés système [sys_properties].
2. Ajoutez la `glide.role_management.v2.audit_roles` propriété système et définissez-la sur **true**.

   Si le module d'extension Sécurité contextuelle : Gestion des rôles V2 [com.glide.role_management.inh_count] est installé, la définition de cette propriété sur **vrai** permet à la table Rôles d'audit [sys_audit_role] de créer des enregistrements lorsque les rôles d'utilisateur changent.

Vérifier deux fois la soumission du formulaire

Lorsque le système détermine qu'un champ particulier (tel que task.number) ne doit pas être écrit par l'utilisateur actuel, le système affiche ce champ en mode lecture seule, raison pour laquelle le champ nombre n'est pas accessible en écriture sur la plupart des incidents.

Si vous configurez le système pour qu'il vérifie l'écriture des valeurs de tous les champs entrants, le système applique le même ensemble de règles de sécurité à la partie entrante d'une transaction. Lorsque vous soumettez un incident, par exemple, le système vérifie deux fois si le champ numérique est accessible par écriture avant de publier des modifications.

Si vous indiquez au système de ne pas revérifier les transactions entrantes, le système vous permet d'écrire dans un champ en lecture seule s'il s'agit de la transaction renvoyée par le client. Dans de nombreux déploiements, il s'agit en fait d'un comportement souhaitable si, par exemple, vous utilisez des scripts clients pour définir des champs en lecture seule en réponse aux sélections de l'utilisateur dans d'autres champs accessibles en écriture.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété de refus par défaut

La propriété de refus par défaut (glide.sm.default_mode) contrôle le comportement par défaut du gestionnaire de sécurité lorsque les seules règles ACL correspondantes sont les règles ACL de table à caractère générique.

Un ensemble de règles ACL de table à caractère générique pour les opérations basées sur les enregistrements les plus courantes est disponible : lecture, écriture, création et suppression. Un nombre important d'ACL fournissant un accès basé sur les rôles aux tables système sont également disponibles. Par exemple, il existe des ACL qui sys_script'accordent l'accès au rôle business_rule_admin, car ce rôle est documenté comme étant capable de gérer les règles métier.

Utilisez la propriété glide.sm.default_mode pour refuser ou autoriser ces opérations sur toutes les tables :

- **Refuser l'accès** : les règles ACL de table à caractère générique restreignent les opérations de lecture, d'écriture, de création et de suppression sur toutes les tables, sauf si l'utilisateur dispose du rôle administrateur ou répond aux exigences d'une autre règle ACL de table. Les autres opérations, telles que report_on et personalize_choices, ne sont pas affectées par ce paramètre.
- **Autoriser l'accès** : les règles ACL de table à caractère générique autorisent les opérations de lecture, d'écriture, de création et de suppression sur toutes les tables, sauf s'il existe des règles ACL de table spécifiques en place pour restreindre ces opérations.

Vous ne pouvez pas réinitialiser glide.sm.default_mode sur **Autoriser l'accès** une fois qu'il a été défini sur **Refuser l'accès**.

Remarque :
Par défaut, les règles ACL de table à caractère générique sont les seules règles ACL qui vérifient la valeur de la propriété glide.sm.default_mode . Si vous souhaitez contrôler d'autres opérations avec ce paramètre, créez vos propres règles ACL pour vérifier la valeur de cette propriété.

Pour en savoir plus sur cette propriété, reportez-vous Refus par défaut à la section Paramètres de sécurisation renforcée de la sécurité de l'instance.

Configuration ACL avancée

En plus de créer de nouveaux ACL ou de modifier les listes de contrôle d'accès existantes, vous pouvez configurer d'autres aspects de la fonctionnalité des ACL.

Refuser les règles ACL

Refuser à moins que

Règles ACL de requête

Tâche	Description
Appliquer les conditions de script ACL aux champs de référence	Activez une propriété pour permettre aux conditions de script de s'appliquer aux champs de référence si vous souhaitez contrôler l'accès aux données qu'un champ de référence affiche dans un formulaire ou dans une liste. L'activation de cette option peut avoir un impact sur les performances de votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Tâche	Description
Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client)	Appliquez des ACL aux appels d'API `GlideAjax` afin que le système interroge uniquement les données auxquelles l'utilisateur actuellement connecté a le droit d'accéder.
Évaluer le remplacement administrateur au niveau de l'accès	Forcez l'évaluation de l'ACL pour les remplacements administrateur au niveau de l'accès. Par défaut, les utilisateurs disposant du rôle administrateur réussissent automatiquement la vérification des autorisations pour cette règle ACL lorsque l'option Remplacements administrateur est sélectionnée dans le formulaire Règles ACL.
Utiliser les outils de débogage et de dépannage d'ACL	Utilisez des outils tels que l'observateur d'ACL, le débogage au niveau des champs et accédez aux messages de sortie des règles ACL pour vous aider à dépanner et à déboguer les ACL.

Fournir l'accès à une table aux utilisateurs externes

Pour permettre aux utilisateurs ayant seulement le rôle snc_external d'accéder à la vue de liste d'une table, vous devez créer une série d'ACL.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Élevez-vous à un rôle privilégié.
2. Créez une règle ACL avec les paramètres suivants :
   - **Type** : ui_page
   - **Opération** : lecture
   - **Nom** : {table_name}_list
   - **Rôle requis** : snc_external
3. Sur les ACL de **lecture** par défaut pour la table, ajoutez **snc_external** dans la liste des Rôles requis. Créez l'ACL s'il n'existe pas encore.
4. Utilisez les paramètres suivants pour créer un autre ACL :
   - **Type** : ui_page
   - **Opération** : lecture
   - **Nom** : {table_name}
   - **Rôle requis** : snc_external
5. Utilisez les paramètres suivants pour créer un autre ACL afin de fournir à l'utilisateur l'accès en écriture à un champ dans la table :
   - **Type** : enregistrement
   - **Opération** : créer
   - **Nom** : {table_name} {column_name}
   - **Rôle requis** : snc_external

   Répétez cette étape pour chaque champ auquel vous souhaitez donner l'accès en écriture à l'utilisateur. Utilisez un astérisque * à la place du nom de la colonne pour donner accès à tous les champs à la fois.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Appliquer les conditions de script ACL aux champs de référence

Utilisez la propriété système pour activer les `glide.sys_reference_row_check` conditions de script pour les champs de référence.

Le comportement par défaut vise à améliorer les performances de l'instance. Si vous souhaitez activer les conditions de script pour les champs de référence, ajoutez la propriété système suivante.

Remarque :
Pour plus d'informations sur la création de propriétés système, reportez-vous à la section Add a system property .

Propriété système

Propriété	Description
glide.sys_reference_row_check	Contrôle si les conditions de script des règles de contrôle d'accès s'appliquent aux champs de référence d'une table. • Type : true | false • Valeur par défaut : **faux** • Emplacement : ajouter une propriété système à la table Propriétés système [sys_properties]

Remarque :
Si la propriété système n'est `glide.sys_reference_row_check` pas présente ou a été définie sur faux, les conditions de script pour les règles de contrôle d'accès ne sont pas appliquées. Cela signifie qu'une ACL contenant des conditions scriptées réussira sa vérification tant que les autres critères ACL sont remplis (tels que les exigences de rôle).

Appliquer des ACL à AJAXGlideRecord (enregistrement Glide côté client)

Utilisez une propriété système pour effectuer la validation des règles de liste de contrôle d'accès (ACL) lorsque l'accès aux enregistrements côté serveur (par exemple, les tables) se fait grâce à des API GlideAjax à l'intérieur d'un script client.

Si vous choisissez d'appliquer des listes de contrôle d'accès (ACL) aux appels d'API `GlideAjax` , vous ne pouvez interroger que les données auxquelles l'utilisateur actuellement connecté a le droit d'accéder. Par exemple, si l'utilisateur est connecté en tant qu'utilisateur ESS et qu'il n'a pas le droit de lire la table `cmn_location` , tout appel d'API `GlideAjax` effectué par l'utilisateur échoue.

Si vous exécutez le système sans qu'une ACL vérifie les appels `GlideAjax` , l'API peut renvoyer des informations auxquelles l'utilisateur actuellement connecté ne pourrait pas accéder via l'interface utilisateur.

Remarque :
Définir cette propriété dans **Propriétés système** > **Sécurité**.

Avertissement :
Les `sys_class_name`, `sys_id` et `sys_domain` sont ignorés pour les vérifications d'ACL.

Pour en savoir plus sur cette propriété, reportez-vous Activation de la vérification de l'ACL de AJAXGlideRecord à la section Paramètres de sécurisation renforcée de la sécurité de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluer le remplacement administrateur au niveau de l'accès

Si vous souhaitez forcer l'évaluation de l'ACL pour les remplacements administrateur au niveau de l'accès, vous pouvez ajouter une propriété système.

Avant de commencer

Rôle requis : security_admin

Pourquoi et quand exécuter cette tâche

Les ACL sont évaluées de façon cumulative. S'il existe un certain nombre d'ACL sur un champ donné et que l'option **Remplacements administrateur** est **définie sur faux** (non sélectionnée) sur l'un d'eux, les remplacements administrateur effectifs pour toutes les ACL sont considérés comme **faux**. Les administrateurs ne peuvent donc même pas transmettre l'ACL dans laquelle le remplacement doit être effectué.

Procédure

Ajoutez la propriété suivante à la table des propriétés système :

Propriété	Description
glide.security.admin.override.accessterm	Évalue la condition de remplacement administrateur au niveau des conditions d'accès. • Type : true | false • Valeur par défaut : **true** pour les nouvelles instances, **false** pour les mises à niveau • Emplacement : Ajouter à la table Propriétés *[sys_properties]* système **Remarque :** Si la propriété n'est pas définie sur l'instance, la valeur est évaluée comme false.

Outils de débogage ACL

Des messages de sortie de règle ACL de débogage et d'accès au niveau du champ sont disponibles pour vous aider à dépanner et à déboguer les ACL. L'observateur de configuration des ACL vous permet de savoir quelles ACL connexes existent lorsque vous en modifiez une.

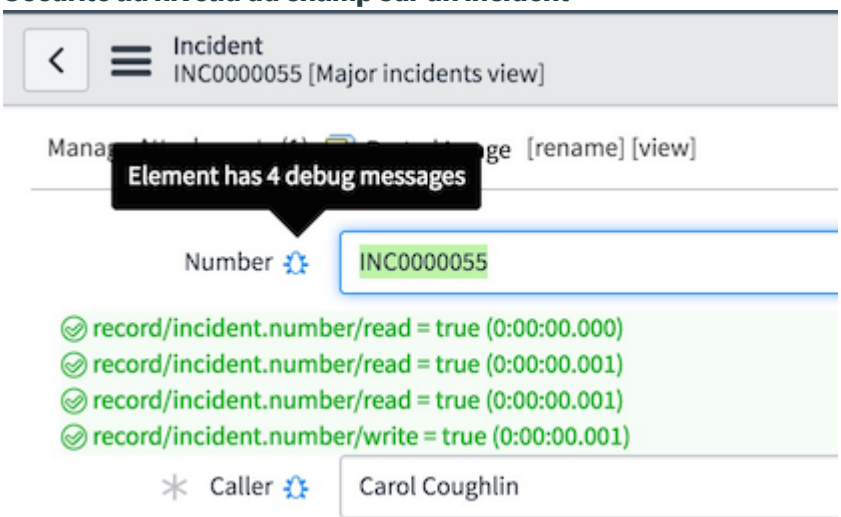
Débogage au niveau des champs

Lorsque le débogage est activé, une petite icône de bogue ( ) apparaît à côté de chaque champ avec une règle ACL. Cliquez sur l'icône pour afficher la liste des règles ACL qui s'appliquent au champ et aux résultats de l'évaluation. Activez le débogage en accédant à **Sécurité de système** > **Débogage** > **Déboguer les règles de sécurité**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Sécurité au niveau du champ sur un incident



Après avoir activé le débogage d'ACL, vous pouvez emprunter l'identité d'un autre utilisateur pour voir quelles règles ACL l'utilisateur réussit et échoue. Lorsque vous empruntez l'identité d'un utilisateur, vous ne pouvez voir que ce que cet utilisateur est autorisé à voir. Par exemple, vous ne pouvez pas afficher un enregistrement qu'une ACL empêche l'utilisateur de voir. Pour faciliter le débogage, l'accès en lecture seule à certaines tables liées aux ACL est activé par défaut, même en cas d'emprunt d'identité d'un utilisateur qui n'a pas d'accès en lecture aux tables. Pour modifier cette fonctionnalité, définissez la propriété suivante sur **false**.

Pour activer le débogage de règle ACL, accédez à **Sécurité de système** > **Déboguer les règles de sécurité**.

Propriété système	Description	Paramètre par défaut
glide.security.access_acl_as_impersonator	Permet d'accorder un accès en lecture aux tables suivantes lors de l'emprunt d'identité d'un utilisateur : sys_security_acl, sys_security_operation, sys_security_type et sys_user_role. Par conséquent, l'utilisateur empruntant l'identité peut lire des données que l'utilisateur dont l'identité est empruntée ne peut pas lire.	VRAI **Remarque :** Lorsque la propriété est définie sur false, l'utilisateur dont l'identité est empruntée peut être empêché de lire les données liées à ACL. Dans ce cas, une deuxième session connectée en tant qu'administrateur ou security_admin peut être nécessaire pour déboguer les ACL.

Messages de sortie de la règle ACL

Le débogage ACL affiche les messages de sortie de règle ACL au bas de chaque liste et formulaire. Le message de sortie affiche les éléments suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Élément de message	Description
HEURE	Durée totale utilisée pour traiter cette règle ACL.
CHEMIN D'ACCÈS	Informations qui identifient de façon unique chaque règle ACL au format suivant : <Type de règle ACL>/<Nom de la règle ACL>/<Opération>.
CONTEXTE	Objet évalué par la règle ACL.
RC	Code de retour de la règle ACL. Une valeur vraie transmet la règle ACL. Une valeur fausse fait échouer la règle ACL.
RÈGLE	Bref résumé des processeurs et des scripts, suivi des résultats ACL pour chaque évaluation ACL au niveau de la table et du champ. La plupart des évaluations ACL indiquent un résultat global de réussite ou d'échec, suivi d'une ventilation des résultats pour chaque type de critère ACL : • iAccessHandler : une vérification interne du système à l'aide du code source masqué sur la plateforme. Il s'agit d'un contrôle de sécurité du système que vous ne pouvez pas modifier. IAccessHandler peut accorder ou refuser l'accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées. Vous ne pouvez en aucun cas modifier les contrôles IAccessHandler. Par exemple, une implémentation IAccessHandler est utilisée pour les contrôles d'accès sur les ressources d'application et cela ne peut pas être modifié. Cette option est disponible à partir de la Istanbul version. • Rôles : vérification que l'utilisateur dispose du rôle approprié. • Condition : vérification que l'utilisateur a réussi la condition spécifiée dans la règle ACL (le cas échéant). • Script : vérification que l'utilisateur a réussi le script spécifié dans la règle ACL (le cas échéant).

Les icônes qui s'affichent montrent comment l'ACL a été évaluée :

Icône	Description
Une coche verte ()	Indique que la table ou le champ a satisfait aux critères.
Icône x rouge (icône )	Indique que la table ou le champ n'a pas réussi.
Icône cercle gris vide ()	Indique que l'évaluation ACL n'a pas eu besoin d'être effectuée.
Une coche bleue, un x ou un cercle vide	Indique que l'ACL a été extraite d'un résultat mis en cache d'une vérification d'ACL précédente. Les icônes signifient la même chose que ce qui précède.

Vous pouvez effectuer ces actions sur la sortie de débogage ACL :

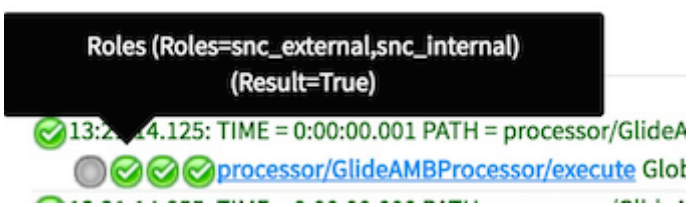
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Activez ou décochez les cases suivantes en haut de la sortie de débogage :
  - **Règles de sécurité** : affichez ou masquez les résultats des contrôles ACL.
  - **Autres** : affichez ou masquez d'autres avertissements ou messages.
- Cliquez sur le nom de l'ACL en regard de l'un des messages de sortie pour ouvrir cet enregistrement ACL.



- Placez le curseur sur l'une des icônes des quatre vérifications d'ACL pour afficher plus d'informations.



Référence de dépannage ACL

Une liste des erreurs courantes de règle ACL et leurs solutions.

Activez le débogage pour aider à résoudre un problème.

Dépannage

Erreur ou symptôme	Solution
Vous ne pouvez pas accéder aux enregistrements à partir d'une table personnalisée.	Créez une règle ACL de table pour la table personnalisée accordant aux utilisateurs l'accès à la table. En l'absence d'une règle ACL de table explicite, les utilisateurs doivent transmettre les autorisations de la règle ACL de caractère générique de table (*) qui, par défaut, limite l'accès aux seuls administrateurs. Activez le débogage et déterminez quelles règles ACL sont évaluées pour la table personnalisée.
Vous créez une règle ACL personnalisée qui ne fonctionne pas correctement.	Les problèmes les plus probables sont qu'une autre règle a priorité sur votre règle personnalisée dans l'ordre de traitement ou que l'utilisateur ne répond pas à toutes les exigences d'autorisation pour le type d'objet. Activez le débogage et vérifiez que la règle ACL est en cours d'évaluation.
La règle ACL de votre champ ne fonctionne pas correctement.	Il existe probablement une règle ACL de table que l'utilisateur n'a pas respectée. Activez le débogage et déterminez quelles règles ACL sont évaluées pour le champ. Vérifiez qu'il n'y a pas de règle ACL de table en conflit ou de règle ACL de champ en double.
Votre règle ACL de table ne fonctionne pas correctement.	Il existe soit une règle ACL plus haut dans l'ordre de traitement, soit une règle ACL de table en double qui interfère avec la règle ACL de table. Activez le débogage et déterminez quelles règles ACL sont évaluées pour la table.
Vous pouvez voir un champ dans une	Il est possible que les conditions ou le script de la règle ACL soient déclenchés dans la liste, mais pas dans le formulaire. Activez le débogage et déterminez

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage (suite)

Erreur ou symptôme	Solution
liste, mais pas dans un formulaire.	quand les règles ACL sont évaluées comme vrai. Mettez à jour les conditions ou le script pour qu'ils aient le même comportement sur la liste et le formulaire.
Vous recevez un message d'erreur lorsque vous essayez d'exécuter un include de script de processeur ou de client pouvant être appelé.	Il existe une règle ACL pour l'include de script du processeur ou du client pouvant être appelé que l'utilisateur n'a pas respectée. Si l'utilisateur doit avoir accès à l'objet, activez le débogage et déterminez quelles règles ACL sont évaluées pour le processeur ou le script include. Mettez à jour la règle ACL ou les rôles d'utilisateur selon les besoins pour accéder à l'objet.

Observateur de configuration ACL

L'observateur de configuration des ACL vous permet de savoir quelles ACL associées existent dans une table lorsque vous insérez, mettez à jour ou supprimez une ACL sur la même table.

L'observateur de configuration ACL est une fenêtre d'intercepteur qui s'affiche chaque fois que vous apportez des modifications importantes dans la table Contrôle d'accès [sys_security_acl]. Il affiche une fenêtre récapitulative des règles de sécurité dans laquelle vous pouvez afficher les ACL associées à celle que vous modifiez. Vous ne pouvez pas modifier les ACL à partir de la fenêtre des règles de sécurité. Pour apporter des modifications, fermez la fenêtre d'observateur et accédez à ces ACL.

L'observateur de configuration ACL n'apparaît pas dans les situations suivantes :

- Si vous enregistrez ou mettez à jour un enregistrement ACL sans réellement apporter de modifications.
- Si vous effectuez des mises à jour mineures (pas une insertion ou une suppression), telles que la mise à jour des scripts, des conditions et de l'option admin-overrides.
- Si l'enregistrement ACL n'est pas actif.

Fenêtre Règles de sécurité ACL

L'observateur de configuration affiche le plan d'exécution de l'ACL. Le plan d'exécution est affiché dans la fenêtre contextuelle des règles de sécurité. Vous pouvez afficher ce type d'informations :

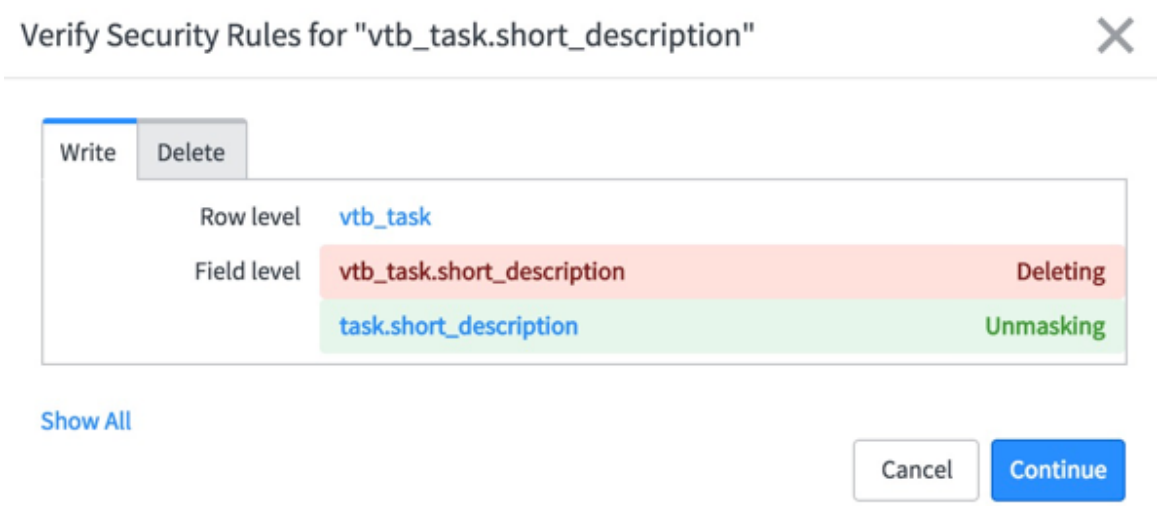
Éléments de fenêtre de configuration ACL

Élément	Description
surbrillance rouge	ACL supprimée ou désactivée.
Surlignage bleu	ACL modifiée.
surbrillance verte	ACL qui est ajoutée ou qui devient active.
Masqué	ACL qui était en vigueur jusqu'à ce que vous fassiez un changement.
Démasqué	ACL qui vient d'être rendue effective lorsque vous avez effectué un changement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exemple d'observateur de configuration



Afficher le plan d'exécution de l'ACL

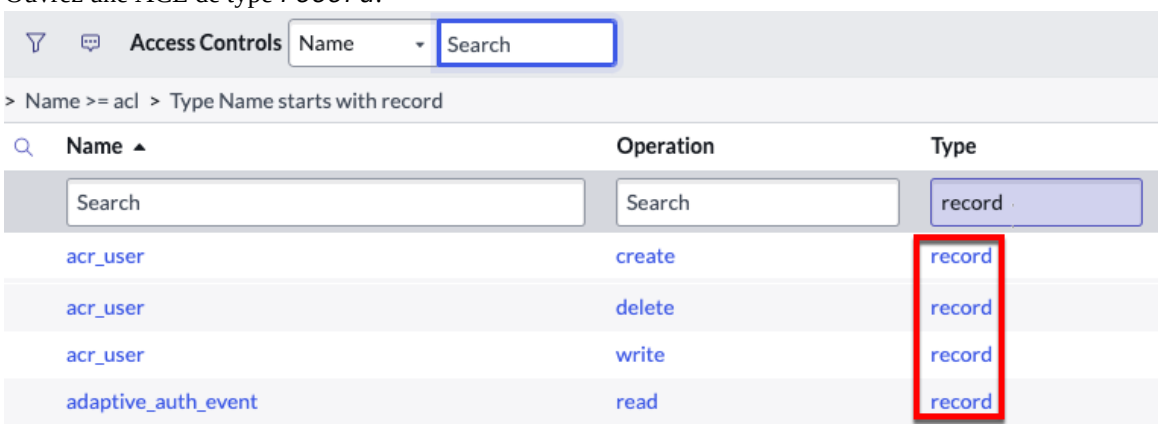
Les administrateurs peuvent voir comment les ACL sont liées les unes aux autres en affichant un plan d'exécution pour n'importe quelle ACL de l'instance.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Élever à un rôle privilégié.
2. Accédez à la **Sécurité de système** > **Contrôle d'accès (ACL)**.
3. Ouvrez une ACL de type `record`.

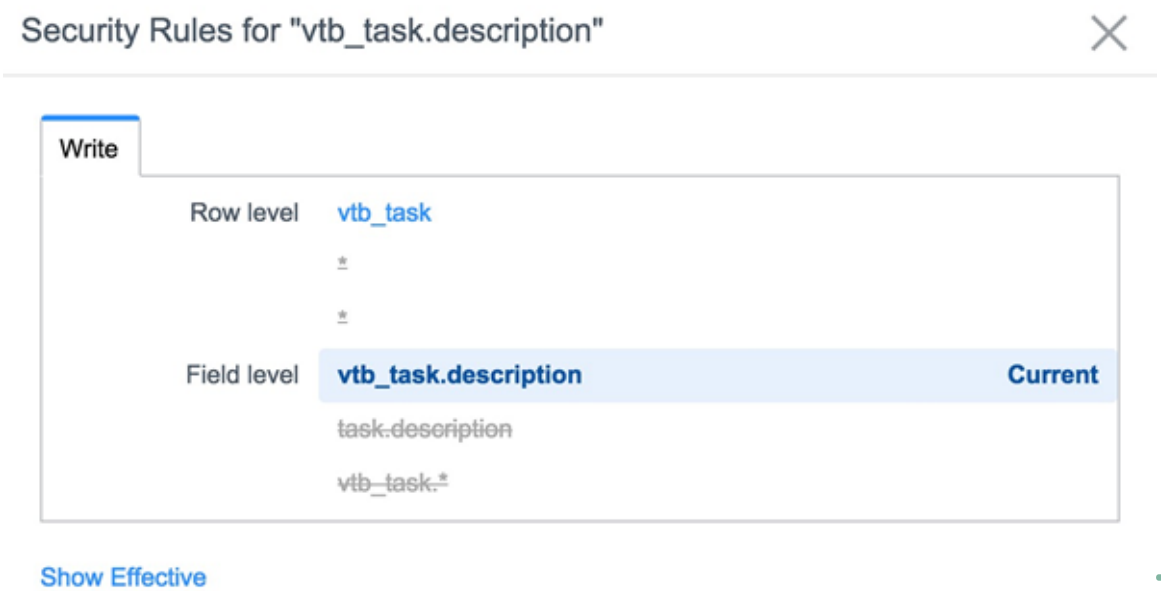


4. Cliquez sur **Afficher le plan d'exécution ACL** dans la section Liens connexes.

   La fenêtre des règles de sécurité s'affiche pour l'ACL. L'exemple affiche le plan d'exécution pour « vtb_task ».

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Fenêtre du plan d'exécution ACL

Élément de l'interface utilisateur	Description
Titre	Nom de l'ACL.
Nom d'onglet	Si l'ACL est créer, lire, écrire ou supprimer.
Niveau de ligne	ACL au niveau des lignes qui s'exécutent sur cette table.
Niveau de champ	ACL au niveau du champ qui s'exécutent uniquement sur ce champ (ou colonne de la table).

5. Cliquez sur **Afficher tout** pour afficher toutes les ACL associées, y compris les ACL remplacées et les ACL génériques qui s'appliquent à tous les enregistrements.
   Les ACL remplacées traversent le nom par une ligne et le nom est barré par les ACL génériques.
6. Affichez uniquement les ACL immédiates associées à celle que vous visualisez et masquez les ACL sur les tables à partir desquelles la table ACL est étendue et les ACL génériques génériques (*) en cliquant sur **Afficher effectif**.

Utiliser l'observateur de configuration ACL

Utilisez l'observateur de configuration ACL après votre élévation à security_admin rôle.

Avant de commencer

Rôle requis : security_admin
Élever à un rôle privilégié

Procédure

1. Ouvrez une ACL de type enregistrement.
2. Effectuez une action sur l'ACL, telle que la modifier ou sélectionner une option dans le menu contextuel comme **Insérer**.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

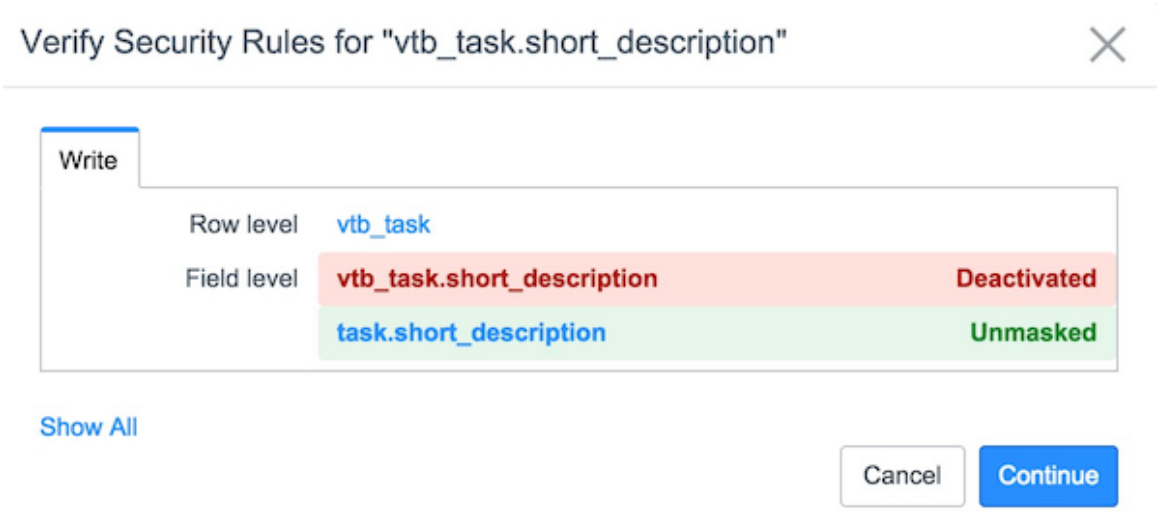
3. Si vous avez modifié des valeurs dans le formulaire de contrôle d'accès, cliquez avec le bouton droit sur l'en-tête et sélectionnez **Enregistrer** ou cliquez sur **Mettre à jour** ou **Supprimer**.

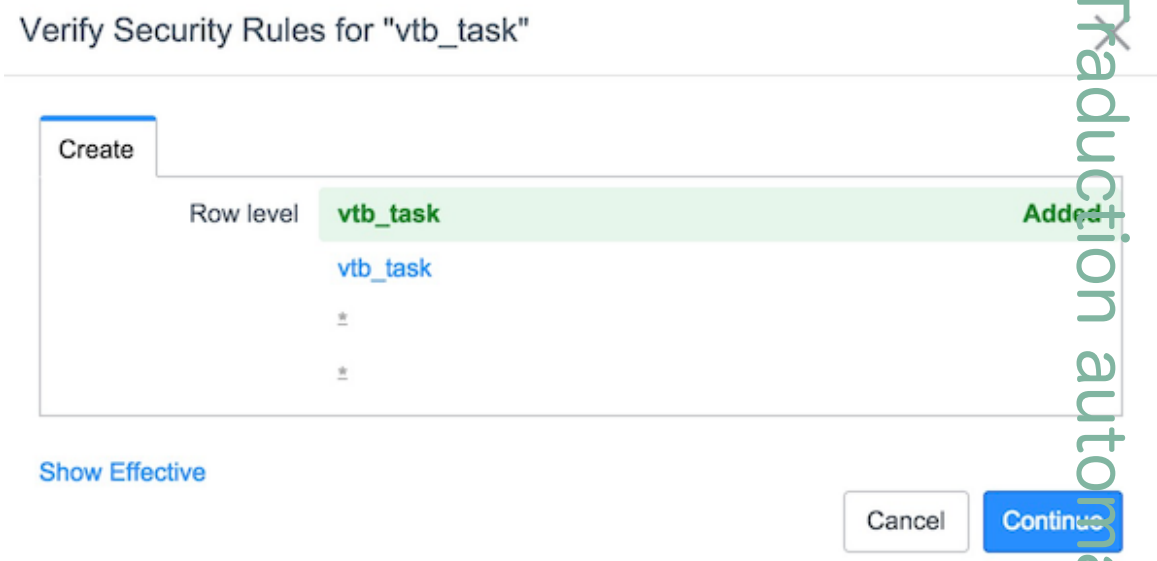
   La fenêtre Règles de sécurité s'affiche. Le système n'a pas encore effectué l'action de base de données sur l'ACL, les changements ne sont donc pas encore enregistrés.

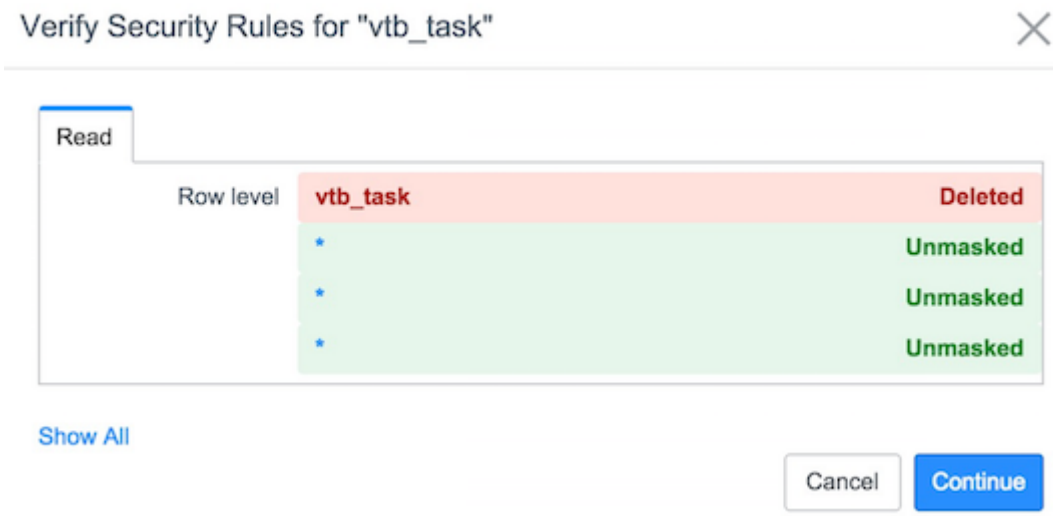
   Il s'agit d'exemples de règles de sécurité sur la table Tâche privée [vtb_task] de l'application Visual Task Board. Reportez-vous Observateur de configuration ACL à la section pour obtenir une description des éléments de cette fenêtre.

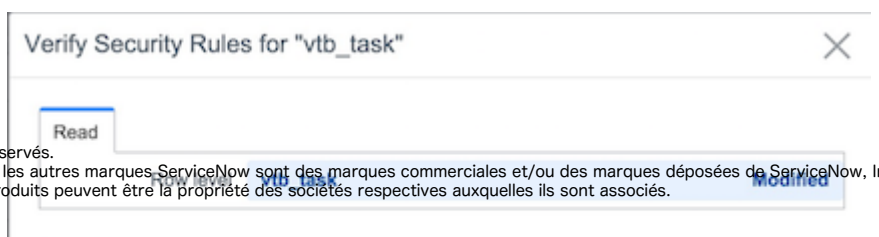
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.









Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays.
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

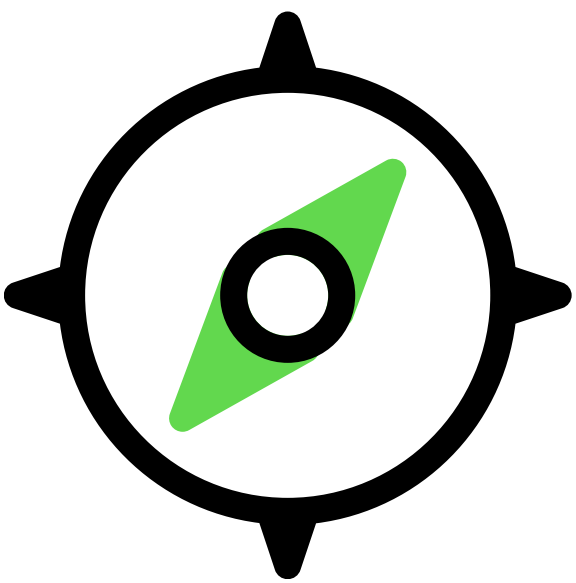
4. Tout comme pour le plan d’exécution, vous pouvez cliquer sur **Afficher tout** pour afficher toutes les ACL associées, y compris celles qui sont remplacées et les ACL génériques qui s’appliquent à tous les enregistrements, ou cliquer sur **Afficher** effectif pour afficher uniquement les ACL immédiates associées à celle que vous consultez.
5. Passez votre souris sur l’un des ACL pour afficher une description.

Attributs de sécurité

Les attributs de sécurité offrent une alternative flexible aux listes de contrôle d’accès.

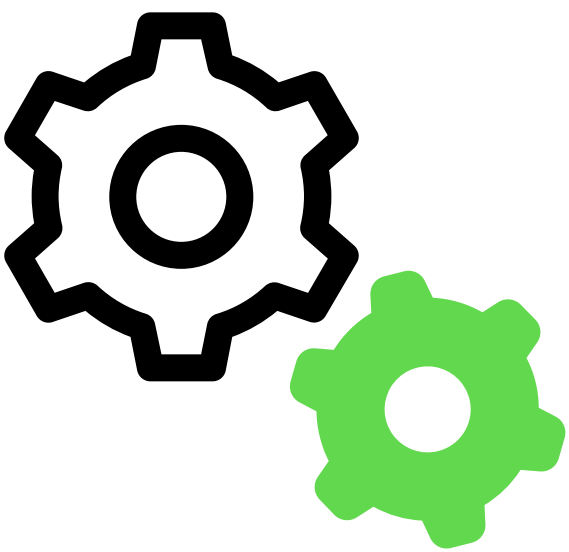
Premiers pas

Explorer les attributs de sécurité



Apprendre les notions fondamentales des attributs de sécurité

Créer des attributs de sécurité

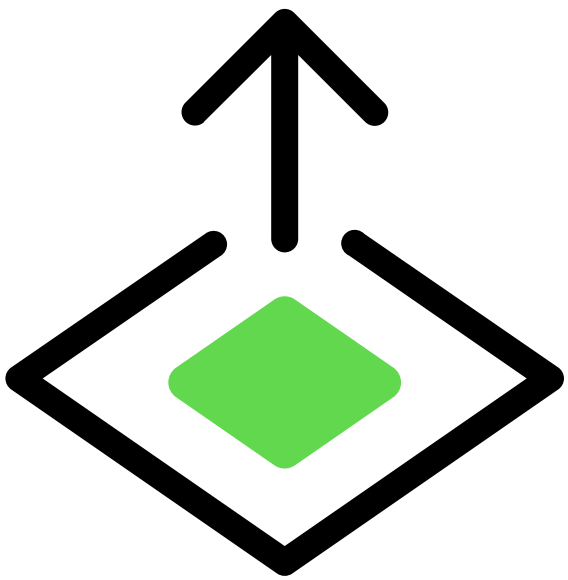


Créer des attributs de sécurité

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attributs de sécurité OOB (prêts à l’emploi)



Expliquer les attributs de sécurité OOB

Connexion des attributs de sécurité



Examiner la journalisation de l’attribut de sécurité

Notions fondamentales des attributs de sécurité

Un attribut de sécurité est un élément d’information hautement configurable sur un sujet ou son environnement. Lorsqu’il est utilisé dans les contrôles d’accès, il permet une configuration fine de la sécurité de manière non complexe.

Vue d'ensemble

Les attributs de sécurité offrent une méthode alternative de contrôle d’accès via des définitions de rôles à la configuration ACL (listes de contrôle d’accès) actuellement en vigueur. Les attributs de sécurité offrent plusieurs avantages aux configurations basées sur ACL :

Meilleure sécurité

L’amélioration de l’obfuscation de l’évaluation des autorisations garantit la sécurité de votre organisation.

Lisible par l’homme

Les attributs de sécurité sont conçus pour simplifier la création et la facilité d’utilisation des autorisations de sécurité.

Sécurité flexible

Créez des définitions de profil à partir de la configuration prête à l’emploi en combinaison avec des profils définis par le client.

Journalisation et audit

Les attributs de sécurité offrent un audit et une journalisation détaillés pour donner plus d’informations sur les mesures et la théorie de la sécurité.

Créer des attributs de sécurité

Créez de nouveaux attributs de sécurité à l’aide d’un guide étape par étape.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Sécurité de système** > **Attributs de sécurité**.
2. Dans la liste Attributs de sécurité, sélectionnez **Nouveau**.
3. Renseignez les champs du formulaire Attributs de sécurité.

Champs d'attributs de sécurité

Champ	Description
Étiquette	Étiquette de l'attribut de sécurité.
Nom	Nom de l'attribut de sécurité.
Type	Type d'attribut de sécurité. ○ Composé **Remarque :** Pour plus d'informations sur les attributs de sécurité composés, voir Attributs de sécurité composés ○ entier ○ liste ○ chaîne ○ booléen(vrai|faux)
Est dynamique	Si la valeur de l'attribut de sécurité doit être réévaluée pour chaque
Description	Description de l'attribut de sécurité générée par l'utilisateur
Application	Champ statique, périmètre de l'application.
Table de recherche	Référencez une table externe pour évaluation.
Colonne de table de recherche	Référencez une colonne de table pour évaluation.
Script	Dériver une valeur à partir d'un script.

Attributs de sécurité OOB (prêts à l'emploi)

Rôles d'attributs de sécurité généralisés couramment utilisés, prêts à l'emploi.

Vue d'ensemble

Les attributs de sécurité prêts à l'emploi sont un moyen facile de commencer à utiliser et à apprendre les options des attributs de sécurité avec une série de rôles d'attributs de sécurité préconfigurés. Les rôles d'attribut de sécurité OOB sont des rôles de contrôle d'accès couramment utilisés.

Pour créer votre propre attribut de sécurité ou étendre les options d'attributs de sécurité OOB, consultez Attributs de sécurité composés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attributs de sécurité OOB

Attribut	Description
Groupe	L'utilisateur est membre d'un groupe spécifié
Explicite de groupe	L'utilisateur est un membre explicite d'un groupe spécifique
HasAdminRole	L'utilisateur a le profil administrateur
Emprunt d'identité	Un utilisateur est victime d'un empreint d'identité
Session interactive	Session interactive en cours
Connecté	L'utilisateur est connecté et authentifié
Critères de réseau	Critères réseau supplémentaires
Rôle	L'utilisateur a un rôle spécifique
Rôle explicite	L'utilisateur a un rôle spécifique explicitement défini

Attributs de sécurité pour la session du client

Les attributs de sécurité suivants sont ajoutés pour la session client (module d'extension : com.glide.client_session_security_attributes) :

- [store-future: BEGIN review]**IsEmbeddedSession** : l'attribut est utilisé dans ServiceNow les composants Web intégrés.

  Remarque :
  IsEmbeddedSession est ajouté en tant qu'attribut de sécurité uniquement lorsque le module d'extension Embedded Client Access (com.glide.security.client_access) est installé.

  [End]

- **IsIframeEmbeddedSession** : l'attribut est utilisé dans l'iframe incorporé dans les portails tiers. Par exemple, Engagement Messenger, Client Web de l'Agent virtuel, Session incorporée, etc.
- **IsIntegrationAsAServiceSession** : l'attribut est utilisé dans les applications de messagerie comme Agent virtuel dans Teams, Agent virtuel dans Slack, Virtual Agent dans whatapp.
- **IsIntegrationAsAUserSession** : l'attribut est utilisé dans l'utilisateur du compte d'intégration ou l'utilisateur de service web.
- **Est une session Web ServiceNow** : l'attribut est utilisé dans une session interactive mobile.
- **Est une session d'application mobile** : l'attribut est utilisé si la propriété **mobile_client** est vraie dans l'enregistrement **de oauth_entity** .

Comportement non explicite et explicite expliqué

Les attributs de sécurité répondent à des besoins d'autorisation nuancés avec une évaluation explicite par rapport à une évaluation non explicite (héritée) des autorisations de rôle.

[qa: BEGIN review]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example: Séparer l'accès à un profil IT de l'accès au fichier de rôle RH
Nous allons définir un attribut de sécurité qui permet à l'administrateur de voir les fichiers liés aux RH, mais ne permet pas à l'administrateur d'y accéder. Supposons que le rôle administrateur n'est pas défini dans le cadre du groupe RH, mais qu'il est _____. Le **rôle** voit _____[End]

Attributs de sécurité composés

Les attributs de sécurité composés vous permettent de créer des profils d'attributs de sécurité cohérents et réutilisables pour répondre aux besoins de votre entreprise

Vue d'ensemble

Les attributs de sécurité composés sont définis à partir d'un ou de plusieurs attributs de sécurité préexistants afin de créer une combinaison de référence unique d'attributs de sécurité pour l'évaluation des autorisations.

[qa: BEGIN review]

Comportement de l'attribut de sécurité composé
[End]

Créer des attributs de sécurité composés

Créez un attribut de sécurité composé pour faciliter sa réutilisation.

Avant de commencer
Rôle requis : security_admin

Procédure

1. Accédez à la **Sécurité de système** > **Attributs de sécurité**.
2. Dans la liste Attributs de sécurité, sélectionnez **Nouveau**.
3. Sélectionnez `Composé` dans le champ **Type** .
4. Renseignez les champs du formulaire Attributs de sécurité.

Champs d'attributs de sécurité

Champ	Description
Étiquette	Étiquette de l'attribut de sécurité.
Nom	Nom de l'attribut de sécurité.
Description	Description de l'attribut de sécurité générée par l'utilisateur
Condition	Conditions spécifiques d'attribut de sécurité utilisées pour définir l'évaluation des attributs de sécurité.
Nouveau critère	Ajouter un ensemble supplémentaire de conditions **Ou** pour l'évaluation.

Champ d'application de l'attribut de sécurité

Les attributs de sécurité prennent en charge les options de définition du champ d'application.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Attribut de sécurité Définition du champ d'application

Le comportement dans le champ d'application des attributs de sécurité est cohérent avec les comportements de définition du champ d'application de la plateforme. Les attributs de sécurité créés dans un champ d'application ne sont disponibles que dans les contrôles d'accès du même champ d'application.

Attributs de sécurité locaux et existants

Les attributs de sécurité existants et locaux permettent aux clients de réutiliser les ensembles de conditions d'attributs de sécurité.

Attributs locaux et existants

Le créateur de conditions d'attribut de sécurité ACL permet aux clients de spécifier si un attribut de sécurité est existant ou local.

Remarque :
Les conditions des attributs de sécurité sont définies par défaut sur local.

Un attribut de sécurité défini localement n'est enregistré que dans l'ACL unique dans laquelle il est créé.

L'option existante permet aux utilisateurs de référencer des conditions d'attributs de sécurité existantes au générateur de conditions.

Rôles et restrictions de requête de champ

Les attributs **Rôles de requête de champ** et Restrictions de requête de **champ**vous permettent de mieux contrôler les informations disponibles pour les utilisateurs dans les tables.

Vue d'ensemble

Les attributs **Rôles de requête de champ** et **Restrictions de requête de champ** permettent un contrôle plus précis sur les actions que les utilisateurs peuvent effectuer sur les tables.

Rôles de requête de champ

Empêche l'interrogation des champs sensibles en fonction du rôle de l'utilisateur.

Restrictions de requête de champ

Limitez l'accès à l'enregistrement si l'accès au champ applicable est refusé.

Configurer un rôle de requête de champ

Découvrez comment activer et configurer un attribut de rôle de requête de champ.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Tables**.
2. Sélectionnez une **table**.
3. Sélectionnez une **étiquette de colonne** pour afficher son entrée de **dictionnaire** .
4. Sélectionnez l'onglet **Attributs**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Conseil :**
   Si vous ne disposez pas du champ **Rôles de requête de champ** , sélectionnez **Nouveau** pour en créer un

   Sélectionnez l'attribut **Rôles de requête de champ** .
6. Entrez les rôles requis pour afficher cette colonne de table dans la **Valeur**
7. **Sélectionner Mettre à jour**

Résultats
La colonne de table ne peut être interrogée que par les rôles définis dans l'attribut **Rôles de requête de champ** . Si un utilisateur sans les rôles définis interroge la colonne de la table, l'accès à l'opération lui est refusé.

Configurer les restrictions de requête de champ

Découvrez comment configurer une restriction de requête de champ

Avant de commencer
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Tables**.
2. Sélectionnez une **table**.
3. Sélectionnez une **étiquette de colonne** pour afficher son entrée de **dictionnaire** .
4. Sélectionnez l'onglet **Attributs**.
5. **Conseil :**
   Si vous ne disposez pas du champ **Restreindre l'accès à l'enregistrement de la requête de champ** , sélectionnez **Nouveau** pour en créer un

   Sélectionnez l'attribut **Requête de champ Restreindre l'accès aux enregistrements** .
6. Saisissez `vrai` dans le champ **Valeur** pour limiter l'accès à l'enregistrement aux seuls utilisateurs qui peuvent afficher le champ, sinon saisissez `Faux`.
7. **Sélectionner Mettre à jour**

Résultats
La colonne de table limite les résultats de toutes les requêtes. Les utilisateurs restreints seront informés du nombre de résultats renvoyés par une requête, mais aucune autre information.

Filtration des données

Utilisez la filtration des données pour contrôler l'accès aux tables et aux enregistrements en fonction des attributs d'objet lors de l'exécution de requêtes de lecture.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorez la filtration des données



En savoir plus sur le filtrage des données.

Créer des règles de filtration de données



Créez vos propres règles de filtration des données en fonction de vos besoins.

Données de débogage



Découvrez comment déboguer vos résultats de filtration de données.

Traduction automatique

Exploration de la filtration des données

Utilisez la filtration des données pour contrôler l'accès aux tables et aux enregistrements en fonction des attributs d'objet lors de l'exécution de requêtes de lecture.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La filtration des données est une forme distincte de contrôle d'accès conçue pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance. La filtration des données refuse l'accès aux tables et aux enregistrements qui ne correspondent pas aux attributs de sujet définis par un administrateur. La filtration des données est conçue pour faciliter l'audit, le reporting et le dépannage.

Il s'agit d'une fonctionnalité facultative que les administrateurs peuvent activer sur leur instance.

Fonctionnalités de filtration des données

Filtres de données

Utilisez des filtres de données pour accorder l'accès en fonction des informations contenues dans un enregistrement. Les filtres de données utilisent les données d'un champ de tables pour déterminer si un enregistrement est disponible pour vos utilisateurs.

Générateur de conditions basé sur l'attribut de sujet

Utilisez les attributs de sujet pour évaluer le rôle d'utilisateur, le groupe, les critères de sujet ou l'adresse de réseau IP.

La filtration des données utilise un modèle basé sur le refus

La filtration des données utilise un modèle basé sur le refus pour contrôler l'accès aux enregistrements. Avec le filtrage des données, votre instance refuse l'accès aux enregistrements sauf si un enregistrement répond aux critères définis par le filtrage des données.

Mise en application de la filtration des données

Les règles de filtration de données s'exécutent après la requête de base de données pour les opérations de LECTURE et sont évaluées avant les ACL. Un enregistrement refusé par une règle de filtrage de données ne sera pas poursuivi et évalué par les règles ACL.

- L'application des règles de filtration des données est cohérente avec celle des ACL en lecture.
- Le filtrage des données, comme les ACL, fonctionne en conjonction avec les comportements existants *`Report_view access control list`* . Pour plus d'informations sur la configuration de ces contrôles de rapport, consultez Report_view contrôle d'accès .

Débogage de session

La filtration des données prend en charge le débogage de session. Utilisez le débogage de session pour voir quels enregistrements de filtration de données s'appliquent à une requête donnée. Les administrateurs peuvent utiliser ces informations pour résoudre les problèmes d'accès des utilisateurs aux enregistrements.

Composants de la filtration des données

La filtration des données fonctionne à l'aide des types d'enregistrement suivants :

Enregistrements de filtration des données

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créez un enregistrement de filtration de données [sys_df_data_filtration] pour accorder l'accès aux tables sur votre instance. L'enregistrement de filtration des données contient les conditions **d'attribut** de **filtre de données** et d'objet décrites ci-dessus pour limiter la portée de la règle et les utilisateurs affectés.

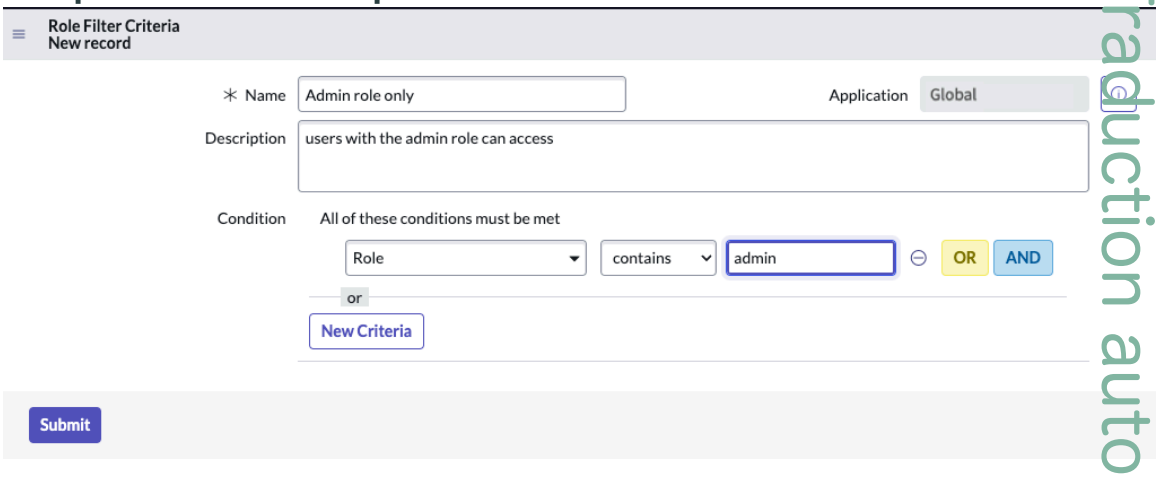
Enregistrements de critères de sujet

Les enregistrements de critères de sujet [sys_df_subject_criteria] représentent des attributs d'utilisateur spécifiques que vous pouvez utiliser pour déterminer s'il convient d'accorder l'accès avec une règle de filtrage des données. Ces attributs peuvent être les groupes, les rôles ou l'adresse IP d'un utilisateur. Pour créer un critère de sujet, vous devez créer l'enregistrement de critères de sujet, ainsi que des enregistrements d'entrée de critères et de conditions de critères. Pour obtenir des détails sur ce processus, consultez Création de critères de sujet.

Après avoir créé un enregistrement de critères de sujet, vous pouvez les appliquer à une règle. Cela se fait dans l'onglet **Condition d'objet** de votre règle de filtration des données.

Exemples d'enregistrements d'entrées de critères

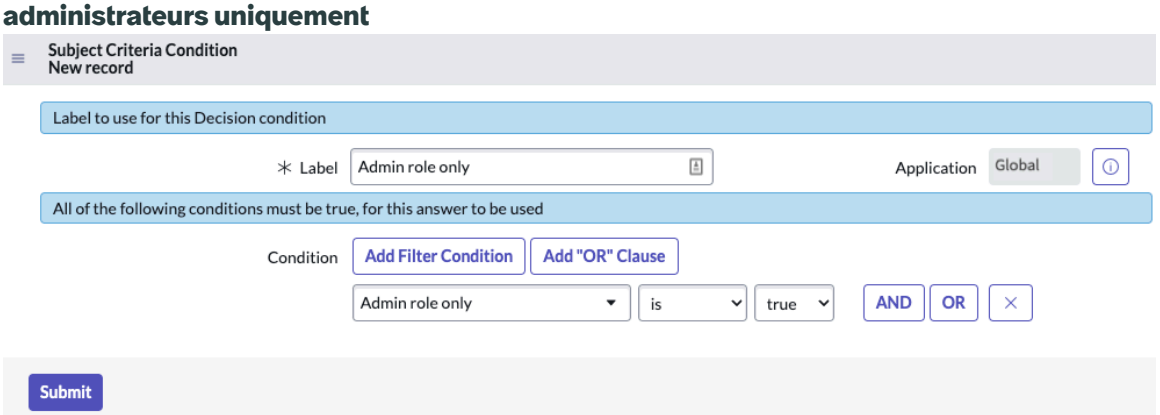
Exemple d'entrée de critères pour tous les rôles contenant admin



Les entrées de critères [sys_df_subject_filter_criteria_m2m] sont des enregistrements qui contiennent des critères à comparer avec l'utilisateur. Il peut s'agir d'une liste de groupes ou de rôles d'utilisateurs, d'une plage d'adresses IP ou d'un sous-réseau d'adresses IP. Ces enregistrements sont utilisés avec les enregistrements de conditions de critères de sujet pour évaluer leur rapport aux groupes, rôles ou adresse IP d'un utilisateur afin de déterminer l'accès à une table ou à ses enregistrements.

Enregistrements de conditions de critères de sujet

Exemple de condition de critères utilisant l'entrée Critères administrateurs uniquement



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Utilisez les enregistrements de condition de critères de sujet [sys_df_subject_criteria_condition] pour définir comment comparer les attributs d'utilisateur avec les rôles, les groupes ou les adresses IP définis dans vos entrées de critères. Vous pouvez utiliser plusieurs entrées de critères dans une seule condition de critères de sujet pour affiner davantage l'accès à vos enregistrements.

Activation de la filtration des données

Découvrez comment activer la filtration de données sur votre instance.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Accédez à la **Tout** > **Définition du système** > **Modules d'extension**.
2. Utilisez le champ de recherche pour trouver le module d'extension Data Filtration (com.glide.data_filtration).
3. Cliquez sur **Installer**, puis cliquez sur **Activer** dans la boîte de dialogue Activer le module d'extension.

Création de règles de filtrage des données

Découvrez comment créer des règles de filtrage des données pour accorder à vos utilisateurs l'accès aux enregistrements sont des tables.

Avant de commencer

Rôle requis : security_admin

Remarque :
Pour créer ou modifier des règles de filtrage de données, vous devez vous élever au rôle de privilégié. Pour plus d'informations sur ce processus, reportez-vous à la section Élever à un rôle privilégié.

Procédure

1. Accédez à la **Tout** > **Filtration des données** > **Enregistrements de filtration des données**.
2. Cliquez sur **Nouveau** dans la liste **Filtration des données** .
   Un nouveau formulaire de filtrage des données s'affiche.
3. Renseignez les champs du formulaire, selon vos besoins.

Formulaire de filtration des données

Champ	Description
Table	Table à laquelle s'applique cette règle de filtrage des données.
Actif	Définit la règle de filtration des données comme active. **Remarque :** Conservez les règles de filtration des données inactives jusqu'à ce que vous soyez prêt à effectuer le test pour éviter de bloquer involontairement l'accès des enregistrements aux utilisateurs.
Description	Description de la règle de filtration des données.
En cascade	Sélectionnez cette option pour définir la règle de filtration des données à appliquer aux tables étendues.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Par exemple, vous sélectionnez la table Tâche [task] et activez la cascade. Dans ce cas, la règle de filtrage des données s'applique également à toutes les tables étendues à partir de la tâche, telles que Incident[incident] et Demande de changement[change_request]. Pour plus d'informations sur l'extension de table, consultez Table extension and classes **Remarque :** Ce champ est activé par défaut.

4. Sélectionnez **Enregistrer** dans le menu Formulaire.
   Une fois que vous avez enregistré votre règle de filtrage des données, cette règle s'applique automatiquement à tous les enregistrements de la table sélectionnée. Vous pouvez restreindre le champ d'application de cette règle à des enregistrements spécifiques de la table à l'aide des conditions des onglets **Filtre de données** et **Condition de sujet** .

Ajouter un filtre de données pour votre règle de filtrage des données

Vous pouvez éventuellement utiliser un filtre de données pour restreindre la portée de votre règle de filtration de données afin qu'elle ne s'applique qu'à des enregistrements spécifiques d'une table.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Dans votre enregistrement de filtrage des données, ouvrez l'onglet **Filtre de données** .
2. Utilisez le générateur de conditions pour filtrer les valeurs de champ des enregistrements de table.
   Le filtre de données utilise le même générateur de conditions que celui utilisé dans d'autres parties de la plateforme. Pour plus d'informations sur l'utilisation de cette interface, consultez Créateur de conditions .

   Important :
   L'onglet **Filtre de données** apparaît vide jusqu'à ce que vous sélectionniez une table dans le champ **Table** .

3. Utilisez le bouton **Aperçu** pour afficher un décompte du nombre d'enregistrements correspondant à votre filtre de données.
4. Sélectionnez le nombre d'enregistrements pour ouvrir une liste des enregistrements correspondants.

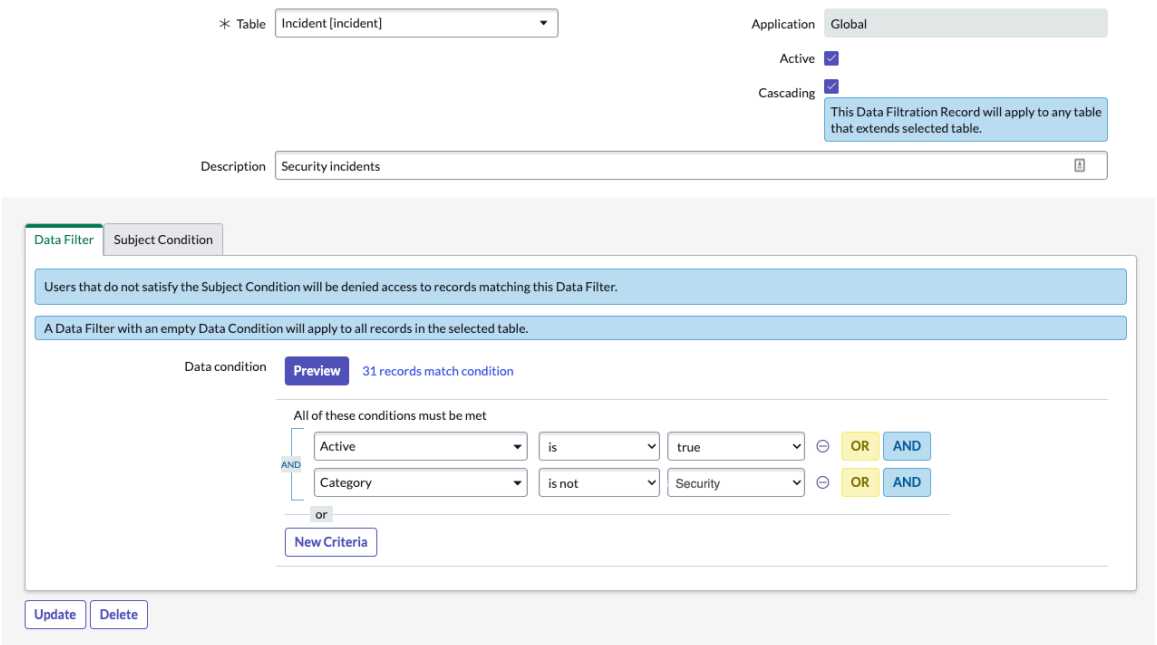


5. Sélectionnez **Enregistrer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Example:
Cet exemple montre une règle de filtration des données pour la table Incident[incident]. Le filtre de données est défini pour sélectionner tous les enregistrements actifs qui ne sont pas dans la catégorie **de sécurité** . Lorsque cette règle est active, les utilisateurs peuvent voir ces enregistrements. Reportez-vous à la section ci-dessous pour en savoir plus sur l'utilisation de critères autres que le contenu de l'enregistrement.



Important :

L'opération not dans vos conditions peut renvoyer des résultats inattendus, selon le type de base de données utilisé par votre instance. Prenons l'exemple de la condition suivante :

Pour cette condition, le résultat attendu serait que l'ensemble des résultats soit constitué de tous les enregistrements pour lesquels l'entreprise n'est pas ServiceNow et de tous les enregistrements qui n'ont pas de valeur dans le champ **Entreprise** . Les instances utilisant des bases de données autres que MySQL et Maria ne renvoient pas d'enregistrements de valeurs avec un champ **entreprise** vide. Lors de l'utilisation de requêtes **not** pour ces instances, incluez des conditions pour vous assurer que les valeurs vides sont renvoyées.

Ajouter des attributs de sujet à votre règle de filtrage des données

Vous pouvez également utiliser des attributs de sujet pour affiner la portée de votre règle de filtrage de données en fonction d'attributs tels que l'adresse réseau IP, les groupes et rôles d'utilisateurs ou les critères de sujet.

Avant de commencer
Rôle requis : administrateur

Procédure

1. Dans votre enregistrement de filtrage des données, ouvrez l'onglet **Critères de sujet** .
2. Utilisez le créateur de conditions pour filtrer les enregistrements de table en fonction d'un ou plusieurs des critères suivants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Options de critères de sujet

Option	Description
Critères réseau	Permet l'accès aux enregistrements en fonction d'un réseau, d'une plage d'adresses IP ou d'un sous-réseau IP.
Critères de sujet	Permet l'accès aux enregistrements en fonction de critères de sujet. Sélectionnez un enregistrement de critères de sujet pour appliquer ses conditions à votre règle de filtration de données. Pour plus d'informations sur la création d'enregistrements de critères de sujet, reportez-vous à la section Création de critères de sujet.
Groupe de sujets	Autorisez l'accès si l'utilisateur est membre d'un groupe spécifique. Sélectionnez un groupe dans la table **Groupes**[sys_user_group].
Rôle du sujet	Autorisez l'accès si l'utilisateur est membre d'un groupe spécifique. Sélectionnez un groupe dans la table **Rôles**[sys_user_role].

Important :
Les conditions de critères de sujet prennent uniquement en charge l'opérateur **is** .

3. Après avoir ajouté vos critères de sujet, cliquez sur **Enregistrer**.

Création de critères de sujet

Créez des enregistrements de critères de sujet à utiliser dans les règles de filtrage des données.

Avant de commencer

Rôle requis : security_admin

Important :
Pour créer ou modifier des règles de filtrage de données, vous devez élever à un rôle privilégié. Pour plus d'informations sur ce processus, reportez-vous à la section Élever à un rôle privilégié.

Procédure

1. Accédez à la **Tout** > **Filtration des données** > **Critères de sujet**.
2. Dans la liste **Critères de sujet** , cliquez sur le bouton **Nouveau** .
   Un nouveau formulaire de critères d'objet s'affiche.
3. Renseignez les champs du formulaire, selon vos besoins.

Champs de critères de sujet

Champ	Description
Nom	Nom des critères de sujet.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Application incluse dans le périmètre pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuelle.
Description	Description des critères de sujet.

4. Cliquez avec le bouton droit sur l'en-tête du formulaire, puis cliquez sur **Enregistrer** dans le menu contextuel.
   Une fois enregistrés, les champs **Entrées de critères** et **Conditions de critères** s'affichent.

Créer une entrée de critère de sujet

Créez une entrée de critères d'objet pour définir les critères sur lesquels vos règles de filtration des données filtrent.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Dans votre enregistrement de critères de sujet, ouvrez l'onglet **Entrées de critères** .
2. Dans la liste **Entrées de critères** , cliquez sur **Nouveau**.
3. Sélectionnez l'entrée de politique pour les critères que vous souhaitez créer.

Entrées de la politique

Entrée de politique	Description
Critère de filtre d'adresses IP	Créer une entrée de politique basée sur l'adresse IP
Critère de filtre de rôle	Créer une entrée de politique basée sur le rôle d'utilisation
Critères de filtre de groupe	Créer une entrée de politique basée sur un groupe d'utilisateurs

   Un formulaire **Critères de filtre d'adresse IP**, **Critères de filtre de rôle** ou **Critères de filtre de groupe** s'affiche, en fonction de votre sélection à cette étape.
4. Dans le formulaire des critères de filtre, renseignez les champs selon vos besoins.

Champs de critères de filtres

Champ	Description
Nom	Nom des critères de filtre
Application	Application incluse dans le périmètre pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuelle.
Description	Description du critère de filtre

5. Sous les champs de formulaire se trouvent des onglets utilisés pour définir les adresses IP, les groupes ou les rôles pour les entrées de critères de filtrage.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Filtrer les champs de critères pour des types d'entrées spécifiques

Type d'entrée de politique	Description	Création
Critère de filtre d'adresses IP	Critères de filtre IP de l'utilisateur pour créer une plage ou un sous-réseau d'adresses IP. Vos critères de sujet peuvent ensuite être comparés à l'adresse IP de l'utilisateur par rapport à cette plage ou à ce sous-réseau.	Utilisez la **plage IP** ou le **sous-réseau (CIDR)** pour définir des adresses IP pour votre entrée. **Plage IP** Dans la liste **Plages IP** , double-cliquez sur **Insérer une nouvelle ligne** et entrez une adresse IP de départ dans l'adresse **IP de démarrage**. Ensuite, appuyez sur la touche de tabulation et entrez une adresse IP de fin dans le champ **Adresse IP de fin** . Enfin, appuyez sur Entrée pour enregistrer l'entrée de liste. **Sous-réseau (CIDR)** Dans la liste **Sous-réseaux** , double-cliquez sur **Insérer une nouvelle ligne** et entrez une adresse IP de réseau dans le champ **adresse IP de réseau** . Ensuite, appuyez sur la touche de tabulation et entrez un masque réseau dans le champ **Masque réseau** . Enfin, appuyez sur Entrée pour enregistrer l'entrée de liste. **Remarque :** Les travaux planifiés déclenchés par un planificateur ne sont pas destinés à filtrer leurs données à l'aide d'un critère de réseau, car ils n'ont pas le contexte de l'adresse IP du client demandeur. Un type de filtration plus approprié peut être la condition de sujet Rôle/Groupe.
Critère de filtre de rôle	Utilisez des critères de filtre de rôles pour créer une sélection de rôles. Vos critères de sujet peuvent ensuite être comparés aux rôles affectés à l'utilisateur par rapport à cette sélection.	Utilisez le générateur de conditions dans le **champ Condition** pour sélectionner des rôles pour votre entrée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type d'entrée de politique	Description	Création
Critères de filtre de groupe	Utilisez les critères de filtre de groupe pour créer une sélection de groupes d'utilisateurs. Vos critères de sujet peuvent ensuite être comparés aux groupes affectés par l'utilisateur par rapport à cette sélection.	Dans le tableau **Groupe pour les critères** , double-cliquez sur **Insérer une nouvelle ligne** et sélectionnez un groupe d'utilisateurs. Appuyez sur Entrée ou cliquez sur l'icône en forme de coche verte pour enregistrer le groupe. Cliquez sur le texte **Insérer une nouvelle ligne** sous la première entrée pour créer des entrées supplémentaires.

6. Après avoir défini votre entrée, cliquez sur **Soumettre**.

Remarque :
En plus de créer des entrées de critères pour vos critères de sujet, vous pouvez également ajouter des entrées existantes. Cliquez sur **Modifier** dans l'onglet **Entrées de critères** , puis sélectionnez parmi n'importe quelle entrée existante.

Créer une condition de critères de sujet

Créez une condition pour comparer les informations d'un utilisateur avec l'entrée existante des critères de sujet.

Avant de commencer
Rôle requis : security_admin

Les conditions de critères comparent les attributs de l'utilisateur aux entrées de critères existantes pour déterminer s'il faut autoriser l'accès aux enregistrements. Pour créer une condition de critères, vous devez avoir créé des critères d'objet. Pour plus d'informations sur ce processus, Créer une entrée de critère de sujetreportez-vous à la section .

Procédure

1. Dans votre enregistrement de critères de sujet, ouvrez l'onglet **Conditions de critères** .
2. Dans la liste **Conditions de critères** , cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire **Condition de critères de sujet** .

Formulaire de condition de critères de sujet

Champ	Description
Étiquette	Une étiquette descriptive pour votre condition
Application	Application incluse dans le périmètre pour les critères de sujet. Ce champ est en lecture seule et se remplit automatiquement avec l'application incluse dans le périmètre actuelle.

4. Créez une condition pour votre condition de critères de sujet à l'aide du Créateur de conditions en sélectionnant parmi les options de condition suivantes.
   Ces options de condition incluent toutes les entrées de critères de sujet que vous avez créées.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

5. **Facultatif :** Créez d'autres conditions en cliquant sur les boutons **Ajouter une condition de filtre** ou **Ajouter une clause « OU ».**

> **Remarque :**
> À moins que vos conditions ne soient séparées par une clause **or** , toutes les conditions doivent être évaluées sur vrai pour que la condition de critères de sujet soit évaluée sur vrai.

6. Cliquez sur **Soumettre** pour enregistrer la condition de critères de sujet.

Que faire ensuite

Utilisez des critères de sujet dans vos règles de filtrage des données pour limiter l'accès aux tables et aux enregistrements. Pour en savoir plus sur l'utilisation des critères de sujet dans les règles de filtrage des données, reportez-vous à la section Création de critères de sujet.

Débogage de filtration de données

Utilisez le journal de session pour voir comment la filtration des données affecte vos enregistrements et déboguer les problèmes d'accès des utilisateurs.

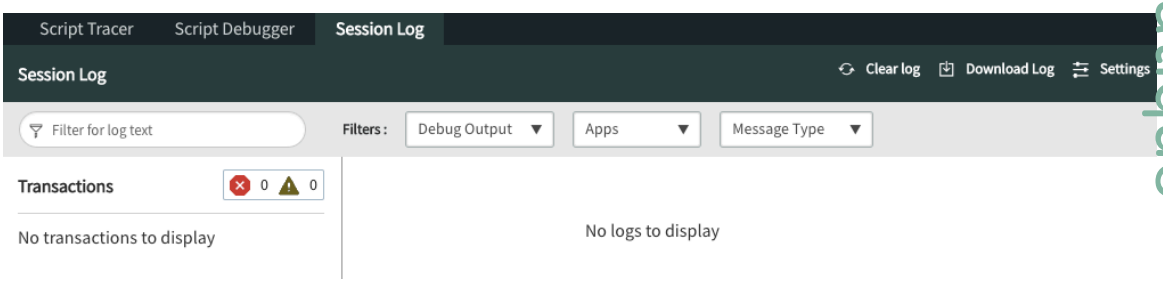
Avant de commencer

Rôle requis : administrateur

Les informations de sortie s'affichent dans les journaux de session lorsque les utilisateurs accèdent aux enregistrements. Vous pouvez utiliser ces informations de connexion avec l'emprunt d'identité pour savoir pourquoi les utilisateurs voient ou ne voient pas les enregistrements. Vous pouvez ensuite utiliser ces informations pour ajuster vos règles de filtrage des données et vous assurer que les utilisateurs ne voient que ce que vous souhaitez.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Débogage** > **Déboguer toute la sécurité**.
   Le **débogueur de script** s'ouvre dans un nouvel onglet ou une nouvelle fenêtre de navigateur.



2. Dans la fenêtre **Script Debugger** , sélectionnez l'onglet **Journal de session** .
3. Dans un autre onglet ou une autre fenêtre de navigateur, empruntez l'identité d'un utilisateur pour résoudre les problèmes d'accès de cet utilisateur.

> **Remarque :**
> L'emprunt d'identité permet à un administrateur de voir une instance avec les paramètres et l'accès d'un autre utilisateur. Pour en savoir plus sur l'emprunt d'identité, consultez Emprunter l'identité d'un utilisateur .

4. Lorsque vous empruntez l'identité d'un utilisateur, accédez à une liste ou à un enregistrement dans lequel vous observez un comportement inattendu.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Il peut s'agir d'un enregistrement que l'utilisateur voit, mais qu'il ne doit pas voir, ou d'une liste d'enregistrements qui n'apparaissent pas comme prévu pour un utilisateur.
Après avoir accédé aux enregistrements avec l'utilisateur dont l'identité a été empruntée, vous devriez commencer à voir la sortie dans le débogueur de session.

5. Recherchez des informations sur la filtration des données dans le débogueur de session.



Cet exemple montre deux messages du journal dans lesquels un filtre de données refusait l'accès aux enregistrements. Les entrées du journal apparaissent en rouge et incluent la raison pour laquelle le filtre de données a refusé l'accès, ainsi que la sys_id du filtre de données. Vous pouvez cliquer sur cette sys_id pour ouvrir l'enregistrement de filtrage des données.



Cet exemple montre un message de journal dans lequel un filtre de données a autorisé l'accès à un enregistrement. Ces entrées de journal apparaissent sous forme de texte vert. Comme pour le premier message, vous pouvez cliquer sur ce sys_id pour ouvrir l'enregistrement de filtrage des données.

6. Utilisez ces informations pour ajuster vos règles de filtrage des données.
Répétez ces étapes pour affiner vos règles et donner aux utilisateurs l'accès dont ils ont besoin.

Rôles de sécurité

Les rôles de sécurité offrent une sécurité supplémentaire : chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse distinguer les utilisateurs internes des utilisateurs externes.

Explorer les rôles explicites



Explorez les privilèges élevés



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découvrez les fonctionnalités clés et la valeur commerciale des rôles explicites.

Découvrez comment le rôle Privilège élevé permet d'activer les privilèges basés sur la session.

Explicit Roles

Vous pouvez donner l'accès à votre instance à la fois aux utilisateurs internes et aux utilisateurs externes. Cependant, vous ne souhaitez peut-être pas donner le même niveau d'accès à ces deux types d'utilisateurs. Pour fournir une sécurité accrue, chaque utilisateur doit avoir au moins un rôle afin que l'instance puisse faire la distinction entre les utilisateurs internes et externes.

Pour la version Paris, aucun utilisateur ne peut avoir les deux rôles explicites (snc_internal et snc_external). Les groupes et le rôle de confinement ne peuvent pas inclure les deux rôles, car cela aurait pour conséquence qu'un membre du groupe ou un utilisateur qui est affecté à un tel groupe ou un tel rôle recevrait automatiquement les deux rôles. Now Platform abandonne toute opération qui créerait un tel scénario.

Les utilisateurs externes doivent au minimum obtenir le rôle snc_external. Le rôle snc_external indique que l'utilisateur est externe à votre organisation. Il ne doit pas avoir accès aux ressources à moins d'y être explicitement autorisé par les ACL pour le rôle snc_external ou pour des rôles supplémentaires qui héritent du rôle snc_external. Par défaut, les utilisateurs dotés du rôle snc_external ne peuvent pas accéder aux éléments suivants :

- Ressources Scripted REST API qui ne sont pas marquées comme étant externes.
- Tables sans le rôle qui hérite du rôle snc_external ou du rôle public.
- Ressources de type autre qu'un enregistrement, telles que les processeurs et les pages de l'interface utilisateur sans accorder l'accès au rôle snc_external ou à un rôle qui hérite du rôle snc_external.
- Tableaux de bord Platform Analytics.

Ne marquez pas le rôle snc_internal comme élevé. Sinon, les utilisateurs internes ne pourront pas accéder à l'instance.

Module d'extension Explicit Roles

Lorsque le module d'extension Explicit Roles est activé :

- Tous les Les utilisateurs doivent avoir le rôle snc_internal pour accéder aux ressources internes ou le rôle snc_external pour accéder aux ressources externes. Les utilisateurs sans rôle explicite ne peuvent accéder qu'aux ressources publiques.
- Tous les utilisateurs existants se voient affecter automatiquement le rôle snc_internal. Ce rôle ne modifie pas les niveaux d'accès existants ni le comportement du système. Au lieu de cela, il fournit une catégorie pour différencier les utilisateurs internes des utilisateurs externes. Tous les utilisateurs internes maintiennent le même niveau d'accès qu'avant l'activation du module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Conseil :
Pour éviter de modifier les fonctionnalités existantes pour les utilisateurs, l'activation du module d'extension Explicit Roles affecte le rôle d'utilisateur snc_internal à tous les utilisateurs existants dans l'instance. Cela inclut tous les utilisateurs externes ajoutés avant que le module d'extension Explicit Roles ait été activé. Après avoir activé le module d'extension Explicit Roles, effectuez les actions suivantes pour tous les utilisateurs externes ajoutés avant l'activation du module d'extension Explicit Roles :

- Supprimez le rôle snc_internal.
- Ajoutez le rôle snc_external.

Cela garantit que les utilisateurs externes ajoutés avant l'activation du module d'extension Explicit Roles n'ont pas accès aux ressources internes qui ne doivent être disponibles que pour les utilisateurs internes.

- Les utilisateurs nouvellement créés se voient affecter automatiquement le rôle snc_internal lorsqu'ils tentent pour la première fois de se connecter à l'instance, à moins que le rôle snc_external ne leur ait été explicitement affecté. Vous pouvez ajouter le rôle snc_external à un nouvel utilisateur avant qu'il ne se connecte pour la première fois à l'instance pour lui fournir des droits d'utilisateur externe.

  Important :

  Activez ce module d'extension pendant une fenêtre de maintenance ou lorsque peu d'utilisateurs sont connectés. Les utilisateurs actuellement connectés lorsque le module d'extension est activé ne se verront pas attribuer dynamiquement le rôle snc_internal. Les utilisateurs doivent plutôt se déconnecter et se reconnecter pour se voir affecter le rôle snc_internal. Une fois le module d'extension activé, vous pouvez ajouter ou supprimer les rôles snc_internal et snc_external à tout moment pour changer les droits des utilisateurs.

  Une fois que le module d'extension est activé, chaque fois qu'un utilisateur se connecte, il reçoit le rôle snc_internal si le compte n'a pas déjà ce rôle ou celui de snc_external. Cela inclut les utilisateurs connectés via l'emprunt d'identité.

- Tous les ACL existants qui n'ont pas de rôle requis se voient affecter automatiquement le rôle snc_internal. Étant donné que le rôle snc_internal est affecté aux ACL comme aux utilisateurs existants, les niveaux d'accès existants ne changent pas.
- Les ACL nouvellement créés qui n'ont pas de rôle requis se voient affecter automatiquement le rôle snc_internal. Cette affectation de rôle ne s'applique pas à un ACL nouvellement créé avec un rôle affecté.
- Pour tous les enregistrements de processeur [sys_processor] existants ou les enregistrements de processeur [sys_processor] nouvellement créés avec **Type = script**, le rôle snc_internal est automatiquement ajouté au champ **Rôles** si celui-ci est vide.
- Pour restreindre l'accès aux pages de l'interface utilisateur aux utilisateurs internes, le module d'extension affecte automatiquement le rôle snc_internal à l'ACL ***** avec un **type** de **ui_page**.
- Pour restreindre l'accès aux processeurs aux utilisateurs internes, le module d'extension affecte automatiquement le rôle snc_internal à l'ACL ***** avec un **type** de **processeur**.
- Les utilisateurs externes doivent au minimum obtenir le rôle snc_external pour accéder à l'instance. Ce rôle doit être accordé manuellement aux utilisateurs externes. L'accès aux enregistrements est accordé par l'intermédiaire des ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ne déplacez pas les ensembles de mises à jour système entre les instances avec et sans le module d'extension Explicit Roles activé. Pour plus d'informations, consultez Ensembles de mises à jour système .

Remarque :
Ce module d'extension nécessite également le module d'extension Contextual Security Manager.

Comportement glide.security.explicit_roles.do_not_fix

À partir de la Xanadu version, le glide.security.explicit_roles.do_not_fix a été ajusté avec des modifications apportées à snc_internal. Le rôle snc_internal est maintenant le même à la fois en mémoire et en sys_user_has_role. Le nouveau comportement de glide.security.explicit_roles.do_not_fix est le suivant :

Nouveau comportement glide.security.explicit_roles.do_not_fix

Valeur	Résultat
Faux	Ajouter snc_internal rôle à la fois dans la mémoire et dans la sys_user_has_role
Vrai	N’ajoutez pas snc_internal rôle dans la mémoire ou sys_user_has_role

Pour exclure snc_internal rôle pour certains utilisateurs, utilisez la propriété glide.security.explicit_roles.ignore.snc_internal.exclude_role_list .

Conseil :
Pour revenir au comportement glide.security.explicit_roles.do_not_fix précédent, utilisez la propriété glide.security.explicit_roles.do_not_fix_in_memory .

Fournir l'accès aux tables aux utilisateurs externes

Vous pouvez donner accès à une table à des utilisateurs externes en ajoutant un rôle à la table qui hérite du rôle snc_external. Pour plus d'informations, consultez Provide external users access to a table .

La méthode hasRoles()

La méthode hasRoles() est toujours disponible, mais elle est déconseillée dans la version Geneva. Utilisez plutôt la méthode hasRole(nom de rôle).

Si vous utilisez la méthode hasRoles(), notez les changements suivants :

- Cette méthode exclut automatiquement le rôle snc_internal par défaut lorsqu'elle vérifie les rôles. Cela signifie que si un utilisateur possède uniquement le rôle snc_internal, la méthode hasRoles() renvoie toujours la valeur **faux**.
- Si l'utilisateur possède le rôle snc_external, la méthode renvoie la valeur **faux** car l'instance considère que les utilisateurs externes n'ont pas de rôle.

Exclusion mutuelle : snc_external contre snc_internal

Now Platform empêche les utilisateurs d'avoir le rôle snc_external et le rôle snc_internal à la fois. L'application Now Platform applique cette exclusion mutuelle partout dans le système et saisit des messages d'erreur dans les journaux pour chaque conflit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les ACL peuvent avoir les deux rôles si les ressources ACL doivent être accessibles à tous les utilisateurs.

Exemple : ajout de rôles explicites à un utilisateur (collision directe) :

1. Affectez à l'utilisateur Abel Tuter le rôle snc_internal.
2. Affectez à l'utilisateur Abel Tuter le rôle snc_external.

Résultat : l'ajout du rôle snc_external échoue car Abel Tuter a déjà le rôle snc_internal.

Exemple : ajout de deux rôles explicites à un groupe (collision directe) :

1. Considérez un groupe appelé groupe de tests qui n'a actuellement aucun rôle explicite affecté au groupe.
2. Ajoutez Abel Tuter au groupe de tests.
3. Ajoutez le rôle snc_external au groupe de tests.

Résultat : l'ajout du rôle snc_external échoue car Abel Tuter a déjà le rôle snc_internal et ne peut pas avoir les deux rôles.

Exemple : ajout d'un rôle explicite à un groupe dans lequel un membre du groupe a déjà le rôle explicite en conflit (collision indirecte) :

1. Affectez à l'utilisateur Abel Tuter le rôle snc_internal.
2. Considérez un groupe appelé groupe de tests qui n'a actuellement aucun rôle explicite affecté au groupe.
3. Ajoutez Abel Tuter au groupe de tests.
4. Ajoutez le rôle snc_external au groupe de tests.

Résultat : l'ajout du rôle snc_external au groupe échoue, car Abel Tuter hérite du rôle snc_external en appartenant au groupe. Les deux rôles explicites seront affectés au même utilisateur, ce qui n'est pas autorisé.

Pour d'autres exemples, consultez la table suivante :

Rôle	Tentative d'action	Résultat
Collision directe		
L'utilisateur a le rôle snc_internal.	Ajoutez le rôle snc_external.	L'action est abandonnée.
L'utilisateur a le rôle snc_external.	Ajoutez le rôle snc_internal.	L'action est abandonnée.
L'utilisateur n'a pas de rôle explicite.	Ajoutez les rôles snc_external et snc_internal.	Le rôle est ajouté.
L'utilisateur a les deux rôles explicites (collision existante).	Ajoutez l'utilisateur à un groupe sans rôles.	L'action est abandonnée.
Un rôle qui n'est associé à aucun	Ajoutez le rôle snc_external.	L'action est abandonnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle	Tentative d'action	Résultat
utilisateur a le rôle snc_internal.		
Un rôle qui n'est associé à aucun utilisateur contient le rôle snc_internal.	Ajoutez le rôle snc_internal.	L'action est abandonnée.
Un rôle contient les deux rôles explicites (collision existante).	Ajoutez le rôle à un utilisateur, un rôle ou un groupe.	L'action est abandonnée.
Un groupe sans membre a le rôle snc_internal.	Ajoutez le rôle snc_external.	L'action est abandonnée.
Un groupe sans membre a le rôle snc_external.	Ajoutez le rôle snc_internal.	L'action est abandonnée.
Un groupe sans membre n'a aucun rôle.	Ajoutez les rôles snc_external et snc_internal.	Le rôle est ajouté.
Collision indirecte		
Confinement de rôle avec collision	1. Accordez un rôle appelé Rôle de test à un utilisateur avec le rôle snc_internal. 2. Ajoutez le rôle snc_external au rôle de test.	L'action est abandonnée.
Confinement de rôle sans collision	1. Accordez un rôle appelé Rôle de test à un utilisateur sans rôle. 2. Ajoutez le rôle snc_external au rôle de test.	Le rôle est ajouté à la fois à l'utilisateur et au rôle de test.
Confinement de groupe avec collision	1. Ajoutez un utilisateur qui a le rôle snc_internal à un groupe appelé Groupe de tests 2 (enfant du groupe de tests 1). 2. Ajoutez le rôle snc_external au groupe de tests 2. 3. Ajoutez le rôle snc_external à un groupe parent appelé Groupe de tests 1 (parent du groupe de tests 2).	L'action est abandonnée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôle	Tentative d'action	Résultat
Confinement de groupe sans collision	1. Ajoutez un utilisateur sans rôle à un groupe appelé Groupe de tests 2 (enfant du groupe de tests 1). 2. Ajoutez le rôle snc_external ou snc_internal au groupe de tests 1 (parent du groupe de tests 2).	Le rôle est ajouté au groupe parent, au groupe enfant et à l'utilisateur.
Confinement de groupe et confinement de rôle avec collision	Ajoutez contains_external au groupe de tests 1, le parent du groupe de tests 2.	Le groupe de tests 1 et le groupe de tests 2 obtiennent tous les deux contains_external, mais n'obtiennent pas explicitement le rôle snc_external.
	Ajoutez le rôle snc_internal au groupe de tests 2, l'enfant du groupe de tests 1.	L'action est abandonnée.
Changement de groupe parent plus confinement de groupe	1. Supprimez le groupe de tests 1 en tant que parent du groupe de tests 2. 2. Ajoutez le rôle snc_internal au groupe de tests 1. 3. Ajoutez le rôle snc_external au groupe de tests 2. 4. Dans le groupe de tests 2, définissez le groupe de tests 1 en tant que groupe parent et enregistrez.	L'action est abandonnée. Répétez pour les groupes déjà imbriqués, avec la même attente.

La cause d'une action abandonnée s'affiche dans le message d'erreur et doit être traitée avant la réussite d'une autre tentative.

Pour les tickets directs, tels que l'ajout d'un rôle explicite à un utilisateur individuel, vérifiez quel rôle explicite l'utilisateur doit avoir. Si l'utilisateur a un rôle explicite erroné, il doit d'abord être supprimé, puis le rôle explicite correct doit être ajouté.

Pour les incidents indirects, tels que l'ajout d'un rôle explicite à un groupe (afin qu'un membre du groupe ait les deux rôles explicites), évaluez si cet utilisateur doit être dans le groupe. Déterminez également si le groupe doit recevoir le rôle explicite, y compris tout héritage par la hiérarchie de groupe et la confinement des rôles.

Notez que Now Platform rapporte uniquement la première collision potentielle rencontrée. Si des tentatives répétées continuent d'échouer après la correction, avec une nouvelle cause première à chaque fois, réévaluez l'interdépendance utilisateur/groupe/rôle pertinente de façon plus étendue. Vous devrez peut-être repenser la façon dont les groupes et les conteneurs de rôles sont structurés.

Demander des rôles explicites

Activez Explicit Roles en demandant le module d’extension Explicit Roles (com.glide.explicit_roles) via Service Now Support Catalog.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

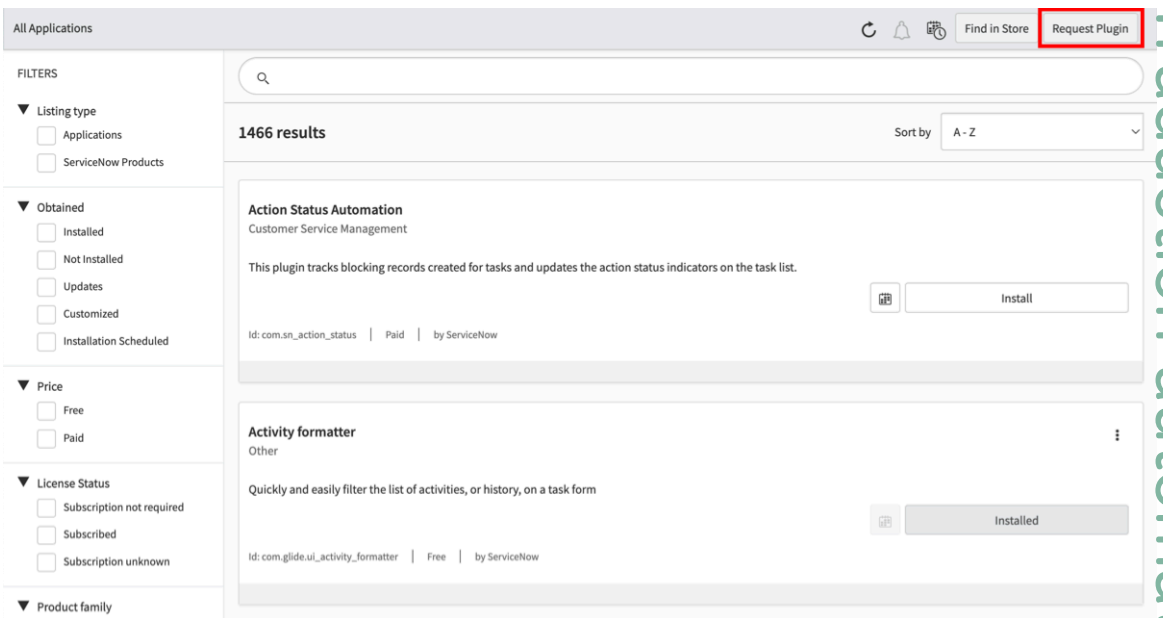
Avant de commencer

Rôle requis : administrateur

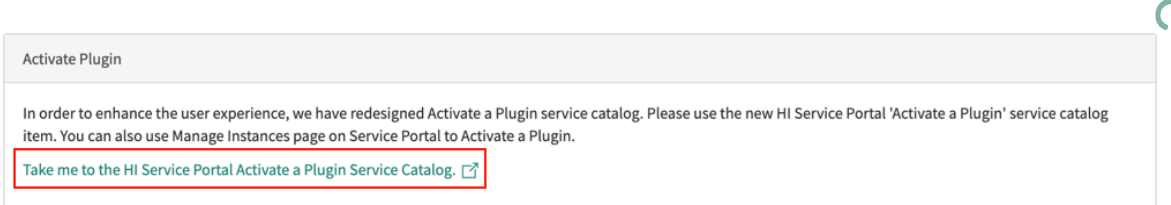
Important :
Activez ce module d'extension pendant une fenêtre de maintenance ou lorsque peu d'utilisateurs sont connectés. Les utilisateurs actuellement connectés lorsque le module d'extension est activé ne se verront pas attribuer dynamiquement le rôle snc_internal. Les utilisateurs doivent plutôt se déconnecter et se reconnecter pour se voir affecter le rôle snc_internal. Une fois le module d'extension activé, vous pouvez ajouter ou supprimer les rôles snc_internal et snc_external à tout moment pour changer les droits des utilisateurs.

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

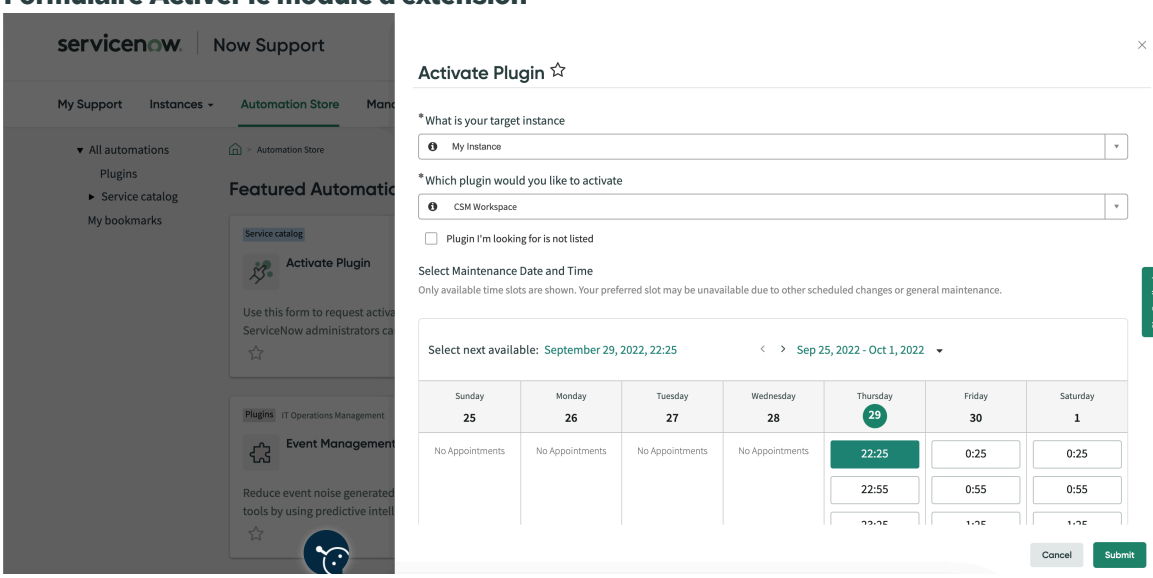
Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

7. Sélectionnez **Envoyer**.
   Pour plus de détails sur la demande d'un module d'extension, consultez l'article Requesting a Plugin from the Service Catalog [KB0751715] de la Now Support Base de connaissances.

Rôles à privilèges élevés

Les rôles de privilège élevé vous obligent à accepter manuellement la responsabilité d'utiliser le rôle avant de pouvoir accéder aux fonctionnalités du rôle.

Par défaut, vous ne disposez pas de rôles de privilège élevé lors de la connexion. Vous devez vous élever manuellement au privilège du rôle. Un rôle de privilège élevé ne dure que le temps de votre session utilisateur. L'expiration de la session ou la déconnexion supprime le rôle.

Vous pouvez désigner n'importe quel rôle comme rôle de privilège élevé, puis affecter ce rôle à un ou plusieurs utilisateurs. Effectuez cette action lorsque vous souhaitez empêcher les utilisateurs d'accéder aux droits conférés par le rôle immédiatement après la connexion. Vous pouvez désigner le rôle de privilège sur le formulaire Rôle. Consultez Créer un rôle pour obtenir des instructions.

Pour utiliser un rôle élevé, vous devez remplir les conditions suivantes :

- Le rôle élevé doit vous être affecté.
- Vous devez vous élever manuellement à un rôle élevé spécifique pour obtenir ses privilèges, même si vous êtes déjà élevé à un deuxième rôle élevé qui contient le premier rôle élevé.

  Par exemple, si le rôle A élevé contient un rôle B élevé, même si vous vous élevez au rôle A, vous devez quand même l'élever au rôle B pour obtenir ses privilèges.

Le rôle administrateur

Pour accorder le rôle administrateur à un utilisateur, l'utilisateur qui l'accorde doit également avoir le rôle administrateur. Par exemple, un utilisateur ayant uniquement le rôle user_admin ne peut pas accorder le rôle administrateur à d'autres utilisateurs.

- Les utilisateurs non administrateurs ne peuvent pas ajouter d'utilisateur à un groupe qui contient le rôle administrateur.
- Pour accorder le rôle security_admin à un utilisateur, celui-ci doit également avoir le rôle administrateur et s'élever au rôle security_admin avant d'accorder le rôle security_admin à d'autres utilisateurs. Un utilisateur ayant uniquement le rôle administrateur ne peut pas accorder le rôle security_admin à d'autres utilisateurs.
- Un utilisateur sans le rôle security_admin ne peut pas ajouter d'utilisateur à un groupe qui contient le rôle security_admin.

⚠ Avertissement :
L'utilisation de privilèges élevés sur le rôle administrateur n'est pas prise en charge et peut provoquer un comportement inattendu. Pour exiger des administrateurs qu'ils élèvent manuellement, reportez-vous à la section Forcer les administrateurs à élever manuellement.

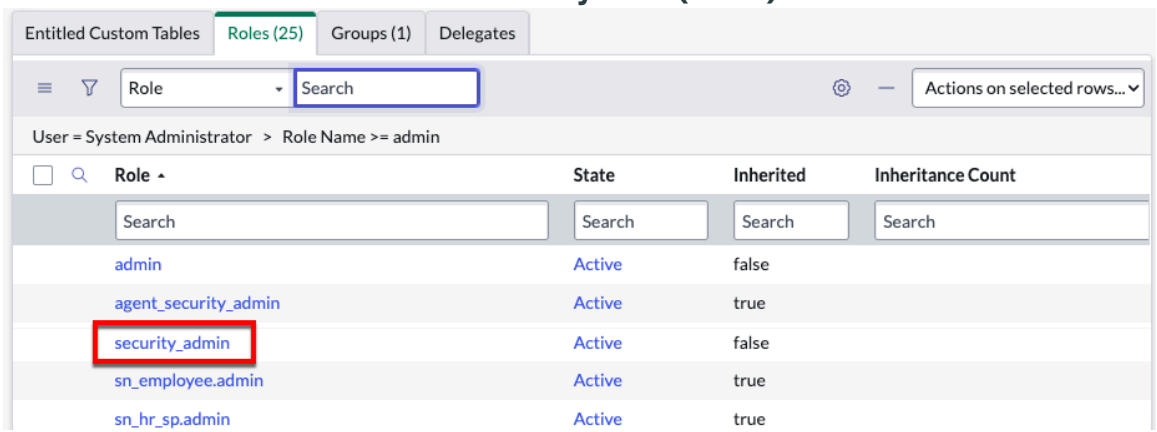
Le rôle security_admin

Dans le système de base, le rôle security_admin est le seul rôle qui dispose de privilèges élevés. Ce rôle est automatiquement affecté à l'utilisateur qui est l'administrateur système par défaut (administrateur). Il permet d'accéder aux ACL et aux paramètres de sécurité élevée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles affectés à l'utilisateur Administrateur système (admin)



Remarque :
Pour voir ce rôle, vous devez d'abord vous élever au rôle security_admin. Si vous êtes connecté en tant qu'utilisateur administrateur système (admin) uniquement, vous ne pouvez pas voir l'enregistrement security_admin dans la liste des rôles.

Security_admin rôle

Le rôle security_admin est un rôle de privilège élevé fourni avec les paramètres de sécurité élevée qui permet aux utilisateurs de créer et de modifier les contrôles d'accès et de modifier les paramètres de sécurité élevée.

Dans le système de base, seul l'utilisateur administrateur système par défaut (admin) dispose du rôle security_admin. Étant donné que cela nécessite des privilèges élevés, l'utilisateur administrateur ne dispose pas de ce rôle lors de la connexion. Après avoir élevé les privilèges, l'utilisateur administrateur dispose du rôle security_admin pour la durée de la session utilisateur. Consultez Élever à un rôle privilégié pour plus d'informations.

Pour maintenir une sécurité élevée, le rôle security_admin nécessite d'élever les privilèges. Limitez les utilisateurs et les groupes auxquels vous affectez ce rôle.

Élever à un rôle privilégié

L'administrateur système de base peut s'élever à un rôle privilégié pour avoir accès aux fonctionnalités des paramètres de sécurité élevée.

Avant de commencer

Rôle requis : administrateur

Remarque :
Si vous accordez à d'autres utilisateurs le rôle administrateur, ils ne peuvent pas accéder à un rôle privilégié. Seul l'administrateur système de base peut effectuer une élévation

Procédure

1. Dans la bannière, cliquez sur votre image ou cliquez sur vos initiales si aucune image n'a été téléchargée.
2. Sélectionnez **Élever les rôles**.
   Une boîte de dialogue contenant les rôles disponibles pour l'élévation s'affiche.
3. Sélectionnez les rôles élevés à affecter, puis cliquez sur **OK**.
   Ce rôle accorde à l'utilisateur des privilèges élevés sur toutes les ressources contrôlées par le rôle pour le reste de la session. Lorsque l'utilisateur se déconnecte, les privilèges élevés prennent fin avec la session, mais peuvent être rétablis à la prochaine connexion.
4. Mettez fin à l'élévation du rôle en revenant à la boîte de dialogue de l'étape 2 et en désélectionnant le rôle.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forcer les administrateurs à élever manuellement

Une propriété est disponible pour forcer tous les utilisateurs ayant le rôle administrateur à sélectionner manuellement le rôle auquel ils souhaitent s'élever.

Avant de commencer

Rôle requis : security_admin

Procédure

1. Connectez-vous en tant qu'administrateur.
2. Élevez votre rôle à security_admin.
3. Accédez à **sys_properties.list**.
4. Recherchez et sélectionnez la `glide.security.strict_elevate_privilege` propriété.
5. Définissez le champ Valeur sur **vrai** et cliquez sur **Soumettre**.

Résultats

Lorsque l'utilisateur se connecte, une fenêtre de dialogue lui est présentée pour sélectionner le rôle auquel il peut s'élever.

Connexions et informations d'identification

Les informations d'identification et de connexion sont nécessaires pour accéder à un ordinateur ou à un appareil réseau pour Découverte, Mappage des services et Gestion cloud, ou pour travailler avec Orchestration. Lorsque vous ajoutez du contenu à Share ou AppStore, vous pouvez configurer des connexions et des informations d'identification pertinentes pour votre environnement sans modifier le contenu généré.

Explorer



En savoir plus sur les informations d'identification.

Configurer



Configurez les informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Référence



Obtenir des détails sur les informations d’identification.

Dépannage



Découvrez comment résoudre les problèmes liés aux connexions et aux informations d’identification.

Traduction automatique

Explorer les informations d’identification, les connexions et les alias

Toutes les intégrations d’applications dans le Now Platform utilisent des connexions, des informations d’identification et des alias pour permettre aux applications d’accéder aux ressources.

Avant de pouvoir exécuter une intégration d’application dans le Now Platform, vous devez créer et configurer les informations de connexion, les informations d’identification correspondantes et ajouter un alias. Pour comprendre comment ServiceNow définit ces termes :

Connexion

Une *connexion* est une intégration à un système, tel qu’une adresse IP ou un point de terminaison avec des protocoles. Elle contient des détails spécifiques, tels que les détails de la base de données, lors de l’intégration à une base de données.

Informations d'identification

Les *informations d’identification* sont les données d’authentification nécessaires pour établir la connexion, telles qu’un ID et un mot de passe.

Alias

Un *alias* est une convention de dénomination, ou balise, liée à un ensemble de connexions ou d’informations d’identification sur votre instance. Un alias contient les informations de connexion et d’identification nécessaires pour effectuer une intégration d’application. Plutôt

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

que d’entrer ces informations à chaque fois que vous intégrez, vous pouvez utiliser un alias. Par exemple, vous pouvez désigner un alias pour abriter vos informations d’identification d’assurance qualité, de développement et de production pour la même intégration d’application. L’alias résout l’intégration d’application pour chaque environnement.

On Now Platform distingue différents types d’alias :

Alias d'informations d'identification

Cet alias s’associe uniquement aux données d’identification et se résout pendant l’exécution.

Alias de connexion et d'informations d'identification

Cet alias s’associe aux informations de connexion et aux données d’identification requises pour terminer l’intégration, et se résout pendant l’exécution.

Dans les alias de connexion et d’informations d’identification, vous pouvez également créer des alias supplémentaires appelés *alias enfants*. Les alias enfants vous permettent de créer plusieurs connexions au sein de la même intégration d’application. Lorsque vous créez un alias enfant, l’alias sous lequel vous l’avez créé devient un *alias parent*. Alors que les alias enfants héritent des propriétés de leur alias parent, ils contiennent leurs propres informations de connexion et d’informations d’identification.

Avantages de l’utilisation des connexions, des informations d’identification et des alias

- Emplacement central pour stocker et gérer les informations d’identification d’un service externe
- Définir une seule fois et réutiliser pour plusieurs fonctionnalités de la plateforme
- Minimiser la configuration des autres fonctionnalités de la plateforme
- Autoriser les non-administrateurs à utiliser des connexions et des informations d’identification prédéfinies
- Sécurité accrue

Fonctionnalités utilisant des connexions, des informations d’identification et des alias

Les fonctionnalités suivantes utilisent des connexions, des informations d’identification et des alias :

- Concepteur de flux
- Centre d'intégration
- Gestion cloud
- Découverte
- Orchestration
- Mappage des services

Vous pouvez configurer des alias sur le Now Platform de l’une des deux manières suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Utilisation du Connexions et informations d'identification module. Consultez Créer un alias de connexion et d'informations d'identification.
- Dans le tableau de bord Connexions de Hub d'intégration. Voir Ajouter une connexion .

Remarque :
Hub d'intégration nécessite un abonnement distinct. Pour plus d'informations, consultez Demande Hub d'intégration .

Synchronisation des informations d'identification sur les serveurs MID

Chaque *MID Server*de votre réseau synchronisé avec l'instance conserve une copie de chaque identifiant que vous créez. Le Serveur MID (Management, Instrumentation, and Discovery) est une application Java qui permet la communication et le mouvement de données entre une instance ServiceNow et des applications, sources de données et services externes. Cette synchronisation accélère la lecture des informations d'identification lorsque les applications aiment Découverte ou Mappage des services ont besoin d'accéder à plusieurs périphériques sur le réseau. Les serveurs MID se synchronisent lorsqu'ils trouvent une `credentials_reload` tâche dans la file d'attente ECC. La tâche de rechargement demande au serveur MID d'effectuer un appel SOAP à l'instance pour obtenir la liste complète des informations d'identification dans la table Informations d'identification [discovery_credentials], y compris toutes les valeurs de champ. Pour en savoir plus, reportez-vous à la section Serveur MID .

La réponse SOAP que votre instance envoie à chaque Serveur MID inclut également des champs personnalisés que vous avez ajoutés à n'importe quel formulaire d'informations d'identification que vous avez personnalisé. Si vous avez ajouté des champs de référence, les données de la table référencée sont également envoyées dans le cadre de la réponse SOAP. Cela peut entraîner des problèmes de performances lorsque la synchronisation des informations d'identification se produit avec plusieurs MID Server. Pour contrôler cela, ajoutez manuellement ces propriétés à la table Propriétés système [sys_properties] :

Remarque :
Pour modifier les valeurs de ces propriétés, ajoutez-les à la table Propriétés système [sys_properties]. Si vous ne les ajoutez pas, le système utilise la valeur par défaut.

Propriété	Description
com.snc.credentials_user_fields	Inclut tous les champs personnalisés dans la synchronisation des informations d'identification. Définissez cette propriété sur faux si vous ne voulez pas inclure les champs que vous avez ajoutés aux formulaires d'informations d'identification. • **Type** : vrai | faux • **Valeur par défaut** : true
com.snc.credentials_recursion_depth	Définit le nombre de tables à parcourir lorsque le mécanisme de synchronisation des informations d'identification collecte les champs des tables de référence. Réduisez ce nombre si vous rencontrez des problèmes de performances et si vous avez personnalisé des formulaires d'informations d'identification qui incluent des champs de référence vers des tables qui ont également des champs de référence.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriété	Description
	• **Type** : nombre entier • **Valeur par défaut** : 3

Protections du champ d'application pour les informations d'identification et les connexions

Vous pouvez classer certains types d'enregistrements Connexion et informations d'identification comme appartenant à un champ d'application et leur étendre des protections de champ d'application. Ces politiques de champ d'application protègent les enregistrements que vous créez dans une table et empêchent les interactions avec des enregistrements privés à un autre champ d'application.

Un champ **Application** est disponible dans les tables Connexion [sys_connection] et Informations d'identification de découverte [discovery_credentials] pour associer ces types d'enregistrements à des champs d'application spécifiques. Il n'est pas visible sur les formulaires d'interface utilisateur dans Xanadu, mais vous pouvez facilement l'y ajouter. Pour en savoir plus sur ces types d'enregistrement et sur l'ajout du champ à leurs formulaires d'interface utilisateur, consultez :

- Mise en route des connexions
- Introduction aux informations d'identification
- Alias d'informations d'identification pour Détection
- Configurer la mise en page du formulaire

Restreindre l'utilisation d'un enregistrement Connexion et informations d'identification à un champ d'application spécifique est primordial pour gérer les applications qui nécessitent une sécurité appliquée. Ces applications comprennent Prestation de services RH ou Opérations de sécurité Les enregistrements de connexion et d'informations d'identification créés dans les applications administrées dans le périmètre ne sont pas visibles par les utilisateurs administrateurs. L'association d'un enregistrement de connexion et d'informations d'identification à un périmètre d'application spécifique offre les protections suivantes :

- Applique les règles de liste de contrôle d'accès (ACL) aux périmètres restreints. Pour en savoir plus sur les ACL incluses dans le champ d'application, consultez Règles de liste de contrôle d'accès.

  Remarque :
  Certaines applications utilisant l'administration du périmètre et la sécurité renforcée peuvent nécessiter une configuration supplémentaire. Pour en savoir plus, reportez-vous à la section Gérer les rôles RH

- Protège les enregistrements lorsqu'ils sont interrogés à l'aide d'un script. Si vous effectuez une requête à partir du périmètre global et que l'enregistrement Connexion et informations d'identification se trouve dans un périmètre protégé, il n'apparaît pas dans la requête, sauf s'il est autorisé à y accéder.

Vous pouvez personnaliser et accorder l'accès aux enregistrements restreints par requête à l'aide de l'accès restreint pour l'appelant. Pour en savoir plus, reportez-vous à la section Paramètres des privilèges d'accès restreint pour l'appelant . Les restrictions de définition du champ d'application s'appliquent également à toutes les tables enfants des tables Connexion [sys_connection] et Informations d'identification de découverte [discovery_credentials]. Les champs vides et autres champs d'application ne sont pas restreints.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Les protections de champ d'application ne sont activées que pour des champs d'application sécurisés spécifiques afin d'éviter toute confusion lors de la configuration de nouveaux enregistrements. Si quelqu'un établit une connexion dans le périmètre de l'application incluse dans le périmètre, il n'y a pas de restriction automatique du périmètre.

Séparation de domaine et Informations d'identification et connexions

L'application Séparation de domaine est prise en charge dans Informations d'identification et connexions. Séparation de domaine vous permet de séparer les données, les processus et les tâches administratives en groupes logiques appelés domaines. Vous pouvez contrôler plusieurs aspects de cette séparation, notamment les utilisateurs qui peuvent voir les données et y accéder.

Niveau de prise en charge : Standard

- Inclut la prise en charge de niveau **Basique**.
- Logique métier : le fournisseur de service (SP) crée ou modifie des processus par client. Les cas d'utilisation reflètent l'utilisation appropriée de l'application par plusieurs clients SP dans une seule instance.
- Le propriétaire de l'instance doit configurer la logique métier et les paramètres de données du produit minimum viable (MVP) par locataire comme prévu pour l'application spécifique.

Exemple de cas d'utilisation : un administrateur doit être en mesure de donner les commentaires appropriés lorsqu'un enregistrement se ferme pour un locataire, mais pas pour un autre.

Pour en savoir plus sur les niveaux de prise en charge, consultez la rubrique Prise en charge de Séparation de domaine par les applications.

Vue d'ensemble

Les informations d'identification sont liées à diverses ServiceNow fonctionnalités qui accèdent aux systèmes en dehors de l'instance. Les informations d'identification suivent la séparation de domaine liée à la fonctionnalité qui utilise les informations d'identification.

Les connexions sont des informations spécifiques au protocole qui font référence à un hôte cible en dehors de l'instance. Une connexion peut spécifier le domaine d'exécution d'une activité.

Fonctionnement de Séparation de domaine dans Informations d'identification et connexions

Les informations d'identification accèdent à des ressources en dehors de l'instance et sont utilisées par Discovery , Orchestration , Mappage des services , et Cloud Provisioning and Governance Applications. Ces informations d'identification ne sont pas liées à un domaine spécifique, elles peuvent être liées à une application, puis suivre la séparation de domaine que l'application utilise. Les informations d'identification peuvent également être affectées à un MID Server , puis suivre Séparation de domaine spécifiée par la Serveur MID configuration.

Les connexions accèdent à un hôte cible à l'aide d'une connexion *JMS*, *JDBC* ou *HTTP(s)*. Vous pouvez spécifier un domaine global ou spécifique auquel appartient la connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Séparation de domaine pour les fournisseurs de services

Modèles de configuration de connexion et d'informations d'identification

Permettez aux utilisateurs ayant les rôles administrateur et flow_designer de configurer des intégrations de spoke avec des systèmes tiers à l'aide d'un formulaire unique personnalisable.

Par exemple, vous pouvez configurer une intégration OAuth, qui enregistre un fournisseur OAuth, génère un jeton et crée des enregistrements de connexion et d'informations d'identification. Un concepteur d'action ou un développeur peut utiliser un modèle de configuration pour configurer le spoke en un seul endroit, et le système crée les enregistrements associés.

Avantages

Les modèles de configuration permettent :

- Permettre aux administrateurs ou aux concepteurs de flux de configurer des intégrations complexes à l'aide d'un formulaire unique.
- Les développeurs doivent définir des valeurs statiques dans une intégration, simplifiant ainsi le processus de configuration pour les administrateurs et les concepteurs de flux.

Types d'informations d'identification pris en charge

Vous pouvez créer des modèles de configuration pour les intégrations avec les types d'informations d'identification suivants :

- Authentification de base
- Clé API
- Type d'attribution titulaire OAuth JWT
- Type d'accord du code d'autorisation OAuth
- Authentification personnalisée

Composants de modèle de configuration

Modèle de données par défaut

Définit les informations statiques qui s'appliquent à chaque intégration. Par exemple, vous pouvez définir l'API et l'URL du jeton si la valeur s'applique à chaque intégration.

Modèle de données dynamiques

Définit les informations que l'utilisateur doit renseigner pour configurer l'intégration. Par exemple, vous pouvez ajouter des paires de valeurs clés de nom d'utilisateur et de mot de passe pour collecter des valeurs définies par l'utilisateur.

Script de post-traitement

Crée les enregistrements supplémentaires requis par l'intégration. Par exemple, si votre spoke inclut des tables personnalisées, vous pouvez créer des enregistrements dans ces tables en fonction de l'entrée de l'utilisateur dans le modèle de configuration. Ce script s'exécute une fois que les enregistrements de connexion et d'informations d'identification sont créés.

Script de pré-édition

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pré-remplit les champs personnalisés de la section **Informations supplémentaires** lorsque vous modifiez une connexion existante. Le pré-remplissage des champs personnalisés vous permet d'afficher la valeur actuelle associée au champ personnalisé.

Données de démonstration

La table Modèles de connexion et d'informations d'identification [sys_alias_templates] comprend des exemples de modèles pour montrer comment configurer des modèles pour les types d'authentification courants. Utilisez ces exemples comme guide lorsque vous créez le vôtre.

Configurer un modèle pour le type d'attribution titulaire OAuth JWT

Cet exemple de modèle de configuration configure les enregistrements d'informations d'identification et de connexion à l'aide du type d'attribution JWT Bearer pour authentifier les demandes adressées à Docusign.

Modèle de données par défaut

Chaque élément de niveau supérieur du modèle de données par défaut crée un enregistrement associé. Le modèle comprend les sections suivantes :

- `Informations d'identification` : crée un enregistrement dans la table Informations d'identification.
- `Connexion` : crée un enregistrement dans la table Connexions [sys_connection] et tous les enregistrements de connexion associés.
- `Supplémentaire` : crée éventuellement des enregistrements dans une table personnalisée. Le script de post-traitement indique au système ce qu'il peut faire de ces enregistrements.

L'exemple suivant crée les enregistrements requis pour l'authentification du type d'attribution OAuth JWT Bearer.

```
{
 "credential": {
  "oauth_entity": {
   "oauth_entity_profile": [
    {
     "grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
     "name": "Docusign Profile",
     "default": true,
     "oauth_entity_profile_scope": [
      "users:read.email"
     ]
    }
   ],
   "code_challenge_method": "S256",
   "type": "consumer",
   "oauth_entity_scope": [
    {
     "oauth_entity_scope": "users:read.email",
     "name": "email"
    }
   ],
   "client_id": "<provider-client-id>",
   "use_mutual_auth": false,
   "revoke_token_url": "https://<provider-domain-name>.com/oauth2/revoke",
   "default_grant_type": "urn:ietf:params:oauth:grant-type:jwt-bearer",
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
    "public_client": false,
    "oauth_api_script": "3e3a3a11c333210016194ffe5bba8f70",
    "name": "Docusign Spoke OAuth",
    "client_secret": "<provider-client-secret>",
    "auth_url": "https://<provider-domain-name>.com/oauth2/auth",
    "token_url": "https://<provider-domain-name>.com/oauth2/token",
    "redirect_url": "https://<instance-name>.service-now.com/oauth_redirect.do"
   },
   "jwt_provider": {
    "jwt_keystore_aliases": {
     "kid": "<provider-key-id>",
     "name": "Docusign Spoke JWT Key",
     "signing_keystore": "<signing-keystore-sys-id>",
     "signing_algorithm": "rsa_256",
     "signing_key_password": "password"
    },
    "jwt_claim_validation" : [ {
     "name" : "iss",
     "is_standard" : true,
     "data_type" : "string",
     "value":"<docusign-iss-claim>"
    }, {
     "name" : "sub",
     "is_standard" : true,
     "data_type" : "string",
     "value":"<docusign-sub-claim>"
    }, {
     "name" : "aud",
     "is_standard" : true,
     "data_type" : "string",
     "value":"<docusign-aud-claim>"
    }, {
     "name" : "scope",
     "is_standard" : false,
     "data_type" : "string",
     "value" : "signature impersonation"
    } ],
    "name": "Docusign Spoke JWT Provider",
    "jwt_api_script": "9ef6af86ff10330001d3cd6bd53bf144"
   },
   "name": "Docusign Spoke Credential",
   "table": "oauth_2_0_credentials"
  },
  "connection": {
   "use_mid": false,
   "connection_url": "https://<provider-domain-name>.com",
   "name": "Docusign Spoke Connection",
   "table": "http_connection"
  },
"additional":{
   "docusign_account_name": "<docusign-account-name>",
   "docusign_account_email": "<docusign-account-email>"
}
}
```


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Schéma de données dynamique

Le schéma de données dynamiques définit ce que voit l'utilisateur lorsqu'il crée un alias de connexion et d'informations d'identification et collecte ses entrées. Utilisez la syntaxe de remontée pas à pas pour mapper l'entrée de l'utilisateur aux champs créés dans le modèle de données par défaut. Par exemple, `connection_fields` mappe l'entrée de l'utilisateur au champ `connection_url` dans l'objet de `connexion` créé par le modèle de données par défaut.

```
{
 "connection_fields": [
   {
    "name": "connection.connection_url",
    "label": "Connection URL",
    "type": "text",
    "defaultValue": "https://demo.docusign.net",
    "hint": "Connection URL for Docusign"
   }],
"additional_fields":[
   {
    "name": "additional.docusign_account_id",
    "label": "Docusign Account Number",
    "type": "text",
    "hint": "Docusign Account Number"
   },
   {
    "name": "additional.docusign_account_name",
    "label": "Docusign Account Name",
    "type": "text",
    "hint": "Name to identify the Docusign account"
   },
   {
    "name": "additional.docusign_account_email",
    "label": "Docusign Account Email",
    "type": "text",
    "hint": "Docusign Account Email"
   }
 ],
 "credential_fields": [
   {
    "name": "credential.oauth_entity.client_id",
    "label": "OAuth Client ID",
    "type": "text",
    "hint": "Client ID for Docusign"
   },
   {
    "name": "credential.oauth_entity.redirect_url",
    "label": "OAuth Redirect URL",
    "type": "text",
    "defaultValue": "https://<instance-name>.service-now.com/oauth_redirect.do",
    "hint": "Callback URL for Docusign"
   },
{
    "name": "credential.jwt_provider.jwt_claim_validation[0].value",
    "label": "Issuer (iss) Claim value",
    "type": "text",
    "hint": "The integrator key (also known as client ID) of the application"
   },
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
{
    "name": "credential.jwt_provider.jwt_claim_validation[1].value",
    "label": "Subject (sub) Claim value",
    "type": "text",
    "hint": "The user ID of the user to be impersonated"
  },
{
    "name": "credential.jwt_provider.jwt_claim_validation[2].value",
    "label": "Audience (aud) Claim value",
    "type": "text",
    "defaultValue": "account-d.docusign.com",
    "hint": "The URI of the authentication service instance to be used e.g.
account.docusign.com"
  },
  {
    "name": "credential.jwt_provider.jwt_keystore_aliases.kid",
    "label": "Key ID (kid)",
    "type": "text",
    "hint": "Indicates which key was used to secure the JWS"
  },
  {
    "name": "credential.jwt_provider.jwt_keystore_aliases.signing_keystore",
    "label": "Key Store",
    "type": "file"
  }
 ]
}
```

Script de post-traitement

Le script de post-traitement suivant mappe l'entrée de l'utilisateur aux champs de la table sn_docusign_spoke_accounts.

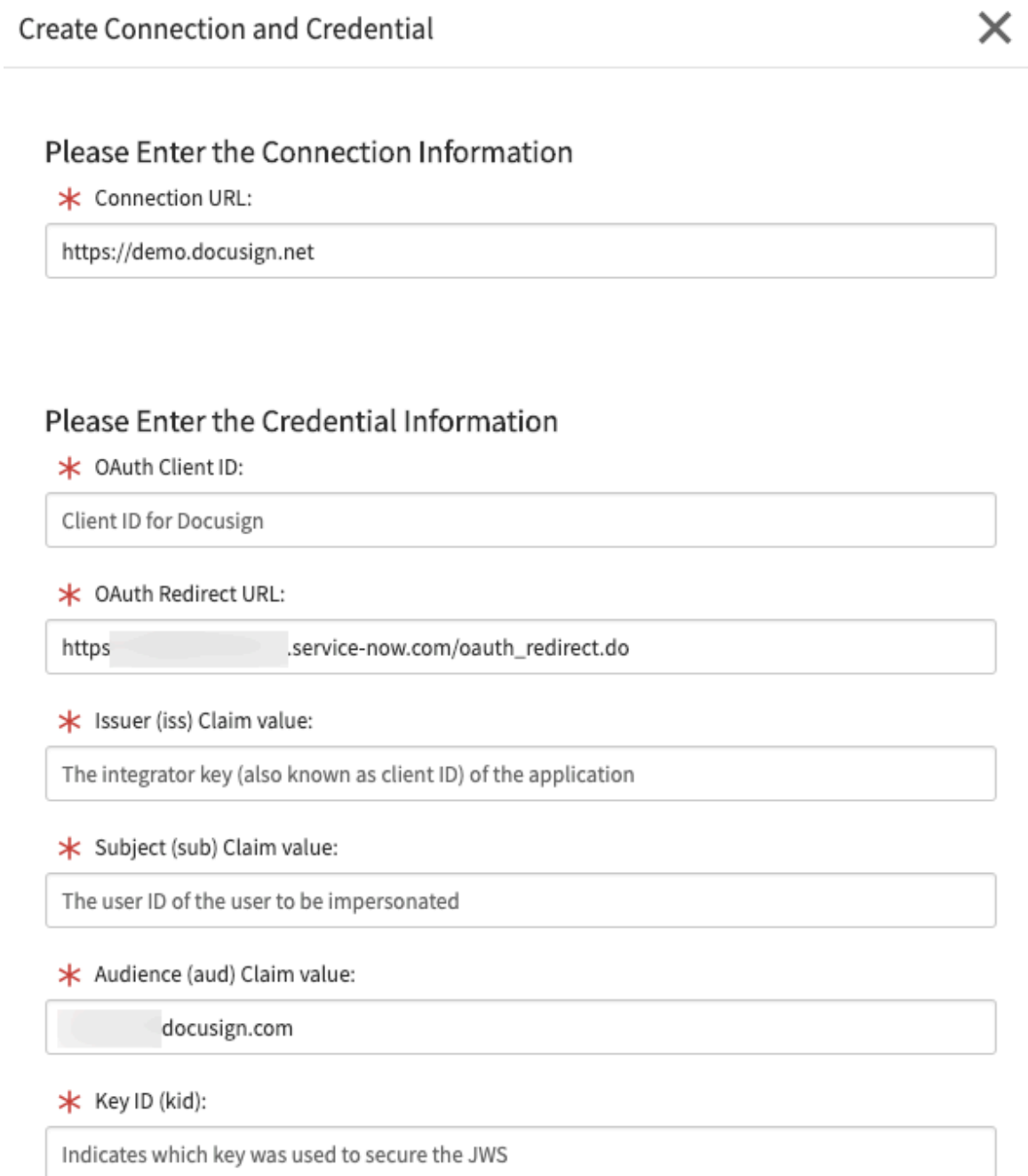
```
(function execute(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData) {
 var jsonDynamicDataP = JSON.parse(jsonDynamicData);
 var accountGR = new GlideRecord("sn_docusign_spoke_accounts");
   accountGR.setValue("account_name",
 jsonDynamicDataP["additional.docusign_account_name"]);
   accountGR.setValue("alias", aliasId);
   accountGR.setValue("email", jsonDynamicDataP["additional.docusign_account_email"]);
   accountGR.setValue("id", jsonDynamicDataP["additional.docusign_account_id"]);
   accountGR.insert();
})(aliasId, connectionSysId, jsonDefaultData, jsonDynamicData);
```

Formulaire de configuration de la connexion et des informations d'identification Docusign qui en résulte

Lorsque l'utilisateur accède à l'alias de connexion et d'informations d'identification Docusign associé et sélectionne **Créer une nouvelle connexion et de nouvelles informations d'identification**, la boîte de dialogue suivante s'affiche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Traduction automatique

Créer un modèle de configuration

Créez un modèle qui définit les entrées requises pour configurer un spoke. Définissez des paires clé-valeur statiques pour créer des enregistrements et définir des valeurs qui s'appliquent à chaque intégration. Définissez des paires clé-valeur dynamiques pour recueillir l'entrée de l'utilisateur et définir des valeurs de champ qui peuvent varier. À l'aide de ce modèle, les administrateurs et les concepteurs de flux peuvent configurer le spoke à partir d'un formulaire unique.

Avant de commencer

Rôle requis : administrateur

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Centre d'intégration** > **Connexions et informations d'identification** > **Modèles de configuration**.
2. Sélectionnez **Nouveau**.
3. Sélectionnez le type de modèle de configuration que vous souhaitez créer.
4. Dans le champ **Nom** , ajoutez un nom pour identifier le modèle.
5. Dans le champ **Modèle de données par défaut** , apportez les modifications nécessaires.

   Ce champ définit des informations statiques qui s'appliquent à chaque intégration. Par exemple, vous pouvez définir l'API et l'URL du jeton si la valeur s'applique à chaque intégration.

   Ces objets dans le modèle de données par défaut sont requis :

   - `informations d'identification` : crée un enregistrement d'informations d'identification avec les champs requis.
   - `connexion` : crée un enregistrement de connexion avec les champs requis. Accédez aux attributs de connexion à l'aide de l'objet enfant `extended_attributes` . Par exemple :

```
"connection": {
        "extended_attributes": {
           "api_version": "v1"

        },
     "connection_url": "https://<provider-domain-name>.com",
     "name": "Spoke Connection",
     "table": "http_connection"
  }
```

   Vous pouvez utiliser l'objet `supplémentaire` pour configurer les données d'une table personnalisée et utiliser le script de post-traitement pour insérer les données dans la table.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Dans le modèle de données par défaut pour le type d'attribution du code d'autorisation OAuth, les valeurs des clés `oauth_entity_profile_scope` et `oauth_entity_scope` doivent correspondre. Dans l'exemple suivant, les deux clés ont la valeur `d'e-mail de lecture de l'utilisateur` .

```
"oauth_entity_profile": [
      {
        "grant_type": "authorization_code",
        "name": "<provider-name> Profile",
        "default": true,
        "oauth_entity_profile_scope": [
          "Read user's email"
        ]
      }
    ],
    "code_challenge_method": "S256",
    "type": "consumer",
    "oauth_entity_scope": [
      {
        "oauth_entity_scope": "Read user's email",
        "name": "email"
      }
    ],
```

6. Dans le champ **Schéma de données dynamique** , apportez les modifications nécessaires.

   Ce champ Définit les informations que l'utilisateur doit renseigner pour configurer l'intégration. Par exemple, vous pouvez ajouter des paires de valeurs clés de nom d'utilisateur et de mot de passe pour collecter des valeurs définies par l'utilisateur.

   Les champs du schéma de données dynamiques incluent les propriétés suivantes :

   - `nom` : champ auquel l'entrée de l'utilisateur est mappée. Par exemple, pour mapper l'entrée de l'utilisateur au champ URL de connexion dans l'enregistrement de connexion, saisissez `connection.connection_url`.
   - `étiquette` : l'étiquette du champ que l'utilisateur voit lorsqu'il remplit le modèle.
   - `type` : type de champ. Assurez-vous que ce type de données correspond au type de données du champ auquel vous mappez la valeur.
   - `defaultValue` : facultatif. Valeur par défaut du champ. Si aucune valeur par défaut n'est fournie, l'astuce s'affiche.
   - `Astuce` : Facultatif. Texte de conseil à afficher en l'absence de valeur par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Lors de la configuration d'un modèle pour l'authentification de type d'attribution titulaire OAuth JWT, vous souhaiterez peut-être une entrée utilisateur pour une seule paire clé-valeur dans le tableau `jwt_claim_validation` . Vous pouvez faire référence à une paire clé-valeur unique dans le schéma de données dynamiques en vous référant à son index dans le tableau. Par exemple, votre modèle de données par défaut peut inclure cet extrait.

```
"jwt_claim_validation" : [ {
      "name" : "iss",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-iss-claim>"
    }, {
      "name" : "sub",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-sub-claim>"
    }, {
      "name" : "aud",
      "is_standard" : true,
      "data_type" : "string",
      "value":"<docusign-aud-claim>"
    }, {
      "name" : "scope",
      "is_standard" : false,
      "data_type" : "string",
      "value" : "signature impersonation"
    } ],
```

Reportez-vous à la paire clé-valeur `iss` à l'aide de l'index de base zéro de l'élément : `credential.jwt_provider.jwt_claim_validation[0].value`.

7. **Facultatif :** Dans le champ **Script de post-traitement** , ajoutez un script qui c Crée les enregistrements supplémentaires requis par l'intégration. Par exemple, si votre spoke inclut des tables personnalisées, vous pouvez créer des enregistrements dans ces tables en fonction de l'entrée de l'utilisateur dans le modèle de configuration. Ce script s'exécute une fois que les enregistrements de connexion et d'informations d'identification sont créés.
   Le script de post-traitement a accès à ces objets globaux.

Objet global	Description
aliasId	Sys_id de l'enregistrement d'alias à partir de la table Alias de connexion et d'informations d'identification [sys_alias].
connectionSysId	Sys_id de l'enregistrement de connexion créé par le modèle.
jsonDefaultData (en anglais seulement)	Contenu JSON issu du champ **Modèle de données par défaut** au format chaîne.
données dynamiques jsonDynamicData	Contenu JSON issu du champ **Modèle de données dynamiques** au format chaîne.

8. Dans le champ **Script de pré-modification** , ajoutez un script pour pré-remplir les champs supplémentaires lorsque vous modifiez une connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce script renvoie un tableau d'objets. Chaque objet dispose d'une paire nom-valeur pour renseigner les champs supplémentaires. Par exemple, si la connexion nécessite des champs qui se trouvent dans une table personnalisée, vous pouvez mapper ces champs à la table personnalisée.

Le **script de pré-édition** a accès aux objets globaux suivants :

Objet global	Description
aliasId	Sys_id de l'enregistrement d'alias à partir de la table Alias de connexion et d'informations d'identification [sys_alias].
connectionSysId	Sys_id de l'enregistrement de connexion créé par le modèle.
jsonDefaultData (en anglais seulement)	Contenu JSON issu du champ **Modèle de données par défaut** au format chaîne.
données dynamiques jsonDynamicData	Contenu JSON issu du champ **Modèle de données dynamiques** au format chaîne.

Chaque objet du script possède les propriétés suivantes :

- `nom` : Nom du champ personnalisé pour spécifier la valeur dans la connexion.
- `Valeur` : valeur que vous souhaitez mapper pour renseigner le champ personnalisé. Vous pouvez mapper le champ à l'aide d'une fonction ou d'une variable ou en le codant en dur.

Les types de données suivants sont pris en charge pour les champs :

Types de données pris en charge pour les champs

Type	Description
Texte	Valeur de chaîne.
Booléen	Zone de sélection. La sélection indique une valeur vraie et la désélection indique une valeur fausse.
Numéro	Valeur numérique.
Date	Valeur de date au format aaaa-mm-jj. Vous pouvez également utiliser l'objet GlideDate.
Choix	Liste des choix valides définis dans le champ **Schéma de données dynamique**.
Référence	GlideRecord valide.

Groupe de cases d'option	Groupes contenant un ensemble différent de champs. Ces groupes sont disponibles en tant que choix dans une liste déroulante lorsque vous modifiez une connexion. Les champs de chaque groupe s'affichent lorsque vous sélectionnez le groupe requis dans la liste déroulante.
	
	Par exemple, considérez la structure suivante du groupe de cases d'option définie dans le champ **Schéma de données dynamiques** :
	
	`{`
	`"name": "radio_groups",`
	`"label": "Radio Groups",`
	`"type": "radio",`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Type	Description

	<pre>"groups": [{
	"name": "radio_group1",
	"label": "Radio Group 1",
	"fields": [{
	"name": "radio_field1",
	"label": "Radio Field 1",
	"type": "text",
	"defaultValue": "efgh",
	"mandatory": true
	}]
	}, {
	"name": "radio_group2",
	"label": "Radio Group 2",
	"fields": [{
	"name": "radio_field2",
	"label": "Radio Field 2",
	"type": "text",
	"defaultValue": "abcd",
	"mandatory": true
	}],
	"default_group": true
	}</pre>
	Pour cet exemple, vous pouvez utiliser l'extrait de code suivant pour comprendre comment les groupes de cases d'option sont utilisés dans le script à l'aide de la remontée pas à pas :
	<pre>{
	name: "radio_field.first_radio_group.radio_field1",
	value: "radio field 1"
	}, {
	name:
	"radio_field.second_radio_group.radio_field2",
	value: "radio field 2"
	}, {
	name: “radio_groups”,
	value: gr.getValue(‘radio_groups’)
	}</pre>
	Pour plus d'informations sur l'utilisation de la remontée pas à pas, voir Remontée pas à pas .

Conseil :
Si les valeurs pré-remplies n'apparaissent pas dans les champs lors de la modification d'une connexion, accédez à **Diagnostics du système** > **Débogage de session** > **Journal des débogages** pour diagnostiquer le problème.

9. Ajoutez le modèle à un alias de connexion et d'informations d'identification.

a. Accédez à la **Centre d'intégration** > **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.

b. Ouvrez l'enregistrement d'alias pour le spoke.

c. Dans le champ **Modèle de configuration** , cliquez sur l'icône de recherche.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d. Sélectionnez le modèle que vous avez créé dans la liste.

e. Cliquez sur **Mettre à jour**.

Résultats

Lorsque l'utilisateur accède à l'alias de connexion et d'informations d'identification associé et sélectionne **Créer une nouvelle connexion et de nouvelles informations d'identification**, une boîte de dialogue s'affiche pour recueillir ses informations. Si vous avez créé un modèle pour le type d'accord du code d'autorisation OAuth, vous pouvez également récupérer un jeton OAuth à partir de cette boîte de dialogue.

Que faire ensuite

Testez le modèle en accédant à l'alias de connexion et d'informations d'identification associé et en sélectionnant **Créer une nouvelle connexion et de nouvelles informations d'identification**. Vérifiez que la boîte de dialogue collecte les données attendues et crée les enregistrements requis dans le système.

Mise en route des connexions

Utilisez la table connexions pour configurer une connexion Basic, JMS, JDBC ou HTTP(s) à un hôte cible.

Table de connexion

La table Connexion (sys_connection) est la table de base pour toutes les tables de connexion. Vous pouvez configurer des connexions pour les protocoles suivants :

- Connexion de base pour PowerShell et SSH
- JDBC
- JMS
- HTTP(S)

La table de connexion fait référence à la table d'alias de connexion, qui couple l'alias de connexion aux informations de connexion. Chaque connexion enregistre les informations suivantes :

Propriétés de la connexion de base

Champ	Description
Nom	Nom de la connexion. Ce champ doit être unique dans la table.
Informations d'identification	Spécifiez les informations d'identification à utiliser avec cette connexion. Ceci est facultatif.
Alias de connexion	L'alias de connexion résout votre connexion et vos informations d'identification au moment de l'exécution. Une seule connexion est active par alias de connexion à la fois.
Actif	Cochez cette case pour activer la connexion actuelle.
Domaine	Domaine auquel appartient la connexion.

Les informations d'identification sont uniques parmi les connexions actives, si elles ne sont pas vides.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise à niveau des informations de connexion

- Les tables Connexion JDBC [jdbc_connection] et Connexion JMS [orch_jms_ds] sont des tables de connexion Orchestration existantes qui s'étendent désormais à partir de la table Connexion [sys_connection]. À l'origine, les tables s'étendaient à partir de sys_metadata. Les données associées au sys_metadata sont supprimées.
- Les tables passent du module d'extension d'exécution Orchestration [com.snc.runbook_automation.runtime] au module d'extension Informations d'identification et connexions.
- Le processus de mise à niveau obtient les informations de connexion JDBC et JMS, crée les alias de connexion correspondants et affecte l'alias à sa connexion correspondante.
- Le nom du champ JDBC change :
  - Le serveur JDBC est renommé en hôte
  - Le port de base de données est renommé en port
  - Les données du serveur JDBC et de la base de données migrent vers l'hôte et le port pendant la mise à niveau

Créer une connexion de base pour PowerShell et SSH

Configurez les informations de connexion à utiliser avec une activité ou une action personnalisée qui utilise le protocole PowerShell ou Secure Shell (SSH).

Avant de commencer

Rôle requis : admin ou connection_admin

Procédure

1. Accédez à la **Tout** > **Informations d'identification et connexions** > **Connexions**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez **Connexion de base pour PowerShell et SSH.**
4. Renseignez le formulaire.

Champ	Description
Nom	Nom unique de l'enregistrement de connexion.
Informations d'identification	Sélectionnez l'enregistrement des informations d'identification utilisé pour autoriser la connexion.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Hôte	Nom de domaine complet de l'hôte cible sur lequel le système exécute l'activité ou l'action. Par exemple, host.domain.com.
Actif	Sélectionnez cette option pour rendre cette connexion active.
Domaine	Détermine le domaine dans lequel l'activité s'exécute. Concepteur de flux ne prend pas en charge Séparation de domaine et ignore ce champ.
Remplacer le port par défaut	Port cible utilisé par la connexion. Si vous laissez ce champ vide, le système utilise la valeur de port par défaut.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utiliser Serveur MID	Sélectionnez cette option pour vous connecter à l'hôte cible via un Serveur MID. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID. **Remarque :** PowerShell nécessite un fichier Serveur MID.
Sélection de MID	Option permettant de sélectionner le serveur MID ou la grappe MID spécifique. ○ **Sélectionner automatiquement un serveur MID** : sélectionne automatiquement le serveur MID. ○ **Serveur MID spécifique** : utilise le serveur MID que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée. **Remarque :** Assurez-vous que l'enregistrement de Hub d'intégration connexion est référencé et non un enregistrement de Orchestration connexion.
Aptitudes	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Les options requises déterminent celle qui Serveur MID est sélectionnée lors de l'exécution. Pour en savoir plus sur la façon dont un est sélectionné pendant l'exécution, reportez-vous à la section Sélection d'un Serveur MID serveur MID. Ce champ n'est visible que lorsque **l'option Sélectionner automatiquement le serveur MID** est sélectionnée dans la liste Sélection MID.
Application MID	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .
Serveur MID	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un Serveur MID spécifique** est sélectionné dans la liste Sélection de MID.
Grappe MID	La grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée et **qu'une grappe MID spécifique** est sélectionnée dans la liste Sélection MID.

5. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Créer une connexion HTTP(s)

La connexion HTTP(s) fournit les informations que les actions ou les activités HTTP(s) personnalisées utilisent pour se connecter.

Avant de commencer

Rôle requis : connection_admin

Procédure

1. Accédez à la **Tout** > **Informations d'identification et connexions** > **Connexions**, cliquez sur **Nouveau**, puis sélectionnez **Connexion HTTP(s).**
2. Ajoutez les informations de connexion suivantes et cliquez sur **Soumettre** :

Champ	Description
Nom	Nom unique de cette connexion HTTP(s).
Informations d'identification	Sélectionnez l'enregistrement des informations d'identification utilisé pour autoriser la connexion.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Générateur d'URL	Entrez manuellement l'URL de connexion ou utilisez le système pour créer l'URL en fonction des entrées. Cette option n'est pas cochée par défaut. Si cette option est cochée, l'URL de connexion est calculée à partir des champs suivants : ○ Authentification réciproque : case à cocher si l'authentification réciproque est utilisée. ○ Protocole : si l'authentification réciproque n'est pas utilisée, entrez protocole. La valeur par défaut est HTTPs. ○ Profil de protocole : si l'authentification réciproque est utilisée, entrez le profil de protocole à partir de sys_protocol_profile. ○ Hôte ○ Port ○ Chemin de base : chemin d'accès de la chaîne de connexion. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est construite : Protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est construite : profil de protocole + :// + host :port +URL
URL de connexion	Si l'option Générateur d'URL n'est pas cochée, saisissez l'URL de connexion dans ce champ. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est construite : Protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est construite : profil de protocole + :// + host :port +URL
Actif	Cochez la case pour activer cette connexion.
Domaine	Déterminez le domaine dans lequel l'action ou l'activité s'exécute.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Utiliser un serveur MID	Cochez cette case pour utiliser un Serveur MID pour cette action ou cette activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID.
Sélection de MID	Option permettant de sélectionner le serveur MID ou la grappe MID spécifique. ○ **Sélectionner automatiquement un serveur MID** : sélectionne automatiquement le serveur MID. ○ **Serveur MID spécifique** : utilise le serveur MID que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée. **Remarque :** Assurez-vous que l'enregistrement de Hub d'intégration connexion est référencé et non un enregistrement de Orchestration connexion.
Aptitudes	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Les options requises déterminent celle qui Serveur MID est sélectionnée lors de l'exécution. Pour en savoir plus sur la façon dont un est sélectionné pendant l'exécution, reportez-vous à la section Sélection d'un Serveur MID serveur MID. Ce champ n'est visible que lorsque **l'option Sélectionner automatiquement le serveur MID** est sélectionnée dans la liste Sélection MID.
Application MID	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .
Serveur MID	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un Serveur MID spécifique** est sélectionné dans la liste Sélection de MID.
Grappe MID	La grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée et **qu'une grappe MID spécifique** est sélectionnée dans la liste Sélection MID.
Délai de connexion	Nombre de millisecondes pendant lesquelles le système attend une connexion de l'hôte réussie. Si aucune connexion réussie n'a lieu pendant cette durée, la demande de connexion expire. Laissez ce champ vide pour utiliser la valeur de délai de connexion par défaut du système.

3. Cliquez sur **Envoyer**.
   Vous êtes prêt à créer une action ou une activité HTTP(s) personnalisée.

Créer une connexion JDBC

La connexion JDBC fournit les informations que les actions ou activités JDBC personnalisées utilisent pour se connecter à diverses bases de données cibles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Vous devez disposer d'un fichier JAR approprié, qu'il soit fourni avec l'instance ou d'un fichier JAR personnalisé.

Remarque :

L'instance ServiceNow fournit des fichiers mysql-connector-java-5.1.21.jar, sql-server-jdbc-4.0.jar et ojdbc6.jar dans le cadre de la version actuelle, qui prend en charge les bases de données MySQL, SQLServer et Oracle. D'autres bases de données, telles que Sybase ou DB2 Universal, doivent utiliser un fichier JAR personnalisé qui doit être téléchargé sur l'instance avant de définir la connexion JDBC.

Rôle requis : connection_admin

Pourquoi et quand exécuter cette tâche

Les informations d'identification JDBC sont récupérées séparément par le modèle de concepteur d'activité et prennent en charge le stockage des informations d'identification externe, tel que CyberArk.

Procédure

1. Accédez à la **Tout** > **Informations d'identification et connexions** > **Connexions**, cliquez sur **Nouveau** et sélectionnez **Connexion JDBC**.
2. Remplissez le formulaire à l'aide des champs de la table.
   La sélection de base de données dans le champ **Format** détermine les champs qui sont disponibles.

Champs de connexion JDBC

Champ	Format de base de données	Description
Nom	Tout	Nom unique de cette connexion JDBC. Par exemple, vous pouvez entrer **JDBC MySQLProd**.
Informations d'identification	Tout	Ajouter des informations d'identification pour le fournisseur JDBC.
Alias de connexion	Tout	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Délai d'expiration de requête	Tout	Durée maximale écoulée pendant laquelle la requête JDBC est autorisée à s'exécuter sans réponse.
Délai de connexion	Tout	Nombre de secondes pendant lesquelles le système attend une connexion JDBC réussie. Si aucune connexion réussie n'a lieu pendant cette durée, la demande de connexion expire. Laissez ce champ vide pour utiliser la valeur de délai de connexion par défaut du système.
Actif	Tout	Cochez la case pour en faire une connexion active.
Domaine	Tout	Domaine de cette table. Par défaut, la table Connexion JDBC [jdbc_connection] s'exécute dans le domaine **global** .
Format	Tout	Type de base de données pour cette connexion. Les choix par défaut sont les suivants : ○ **MySQL** ○ **Oracle**

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Format de base de données	Description
		○ **SQL Server** ○ **Aucun** Vous pouvez ajouter **Sybase** ou **DB2 Universal** à la liste de choix en chargeant le fichier JAR du pilote JDBC approprié dans l'instance. Orchestration reconnaît automatiquement ces pilotes lorsqu'ils sont chargés dans le système et les ajoute à cette liste.
Hôte	Oracle, MySQL, SQL Server	Nom d'hôte ou adresse IP du serveur de base de données.
SID Oracle	Oracle	L'identificateur de site de base de données Oracle. La valeur par défaut est **orcl**.
Port Oracle	Oracle	Port utilisé par la base de données Oracle. La valeur par défaut est **1521**.
Nom de base de données	MySQL, SQL Server	Nom de la base de données.
Port	MySQL, SQL Server	Port utilisé par la base de données sélectionnée.
Nom d'instance	SQL Server	Nom d'instance pour le SQL Server sélectionné
URL de connexion	Tout	URL que le Serveur MID utilise pour se connecter à la base de données spécifiée. L'URL est créée automatiquement lorsque vous enregistrez le formulaire et est en lecture seule pour les bases de données par défaut. **Remarque :** Si le format sélectionné n'est pas l'une des bases de données par défaut, vous devez créer l'URL de connexion manuellement afin que le serveur MID sache comment créer la connexion.
Pilote JDBC	Aucun, DB2 universel, Sybase	Pilote JDBC à utiliser pour cette connexion lorsqu'il ne s'agit pas d'une base de données par défaut. **Remarque :** Si vous ajoutez une base de données Sybase ou DB2 Universal, vous devez saisir le nom du pilote dans ce champ et charger le fichier JAR du pilote dans l'instance.
Utiliser un MID Server	Tout	Cochez cette case pour utiliser un MID Server pour cette action ou cette activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID.
Sélection de MID	Tout	Option permettant de sélectionner le serveur MID ou la grappe MID spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Format de base de données	Description
		○ **Sélectionner automatiquement un serveur MID** : sélectionne automatiquement le serveur MID. ○ **Serveur MID spécifique** : utilise le serveur MID que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée. **Remarque :** Assurez-vous que l'enregistrement de Hub d'intégration connexion est référencé et non un enregistrement de Orchestration connexion.
Aptitudes	Tout	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Les options requises déterminent celle qui Serveur MID est sélectionnée lors de l'exécution. Pour en savoir plus sur la façon dont un est sélectionné pendant l'exécution, reportez-vous à la section Sélection d'un Serveur MID serveur MID. Ce champ n'est visible que lorsque **l'option Sélectionner automatiquement le serveur MID** est sélectionnée dans la liste Sélection MID.
Application MID	Tout	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .
Serveur MID	Tout	Spécifique Serveur MID sur lequel l'étape s'exécute. Ce champ n'est visible que **lorsqu'un Serveur MID spécifique** est sélectionné dans la liste Sélection de MID.
Grappe MID	Tout	La grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée et **qu'une grappe MID spécifique** est sélectionnée dans la liste Sélection MID.

3. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Information associée

Informations d’identification JDBC

Créer une connexion JMS

Configurez votre système pour utiliser JMS (Java Messaging Service) avec une activité ou une action JMS personnalisée.

Avant de commencer

Rôle requis : connection_admin

Pourquoi et quand exécuter cette tâche

Le serveur MID doit disposer des instanciateurs de connexions JMS appropriés pour votre organisation. Configurez ces valeurs dans la `mid.property.jms.command.allowed_factory_names` propriété, qui se trouve dans **Serveur MID** > **Propriétés**. Les valeurs par défaut de cette propriété peuvent être remplacées par n’importe quelle valeur ou par une liste de valeurs séparées par des virgules annoncées par le fournisseur JMS tiers.

Procédure

1. Accédez à la **Informations d'identification et connexions** > **Connexions**.
2. Cliquez sur **Nouveau**, sélectionnez **Connexion JMS**, remplissez le formulaire, puis cliquez sur **Soumettre**.

Option	Description
Nom	Nom unique de cette fabrique de connexions.
Informations d'identification	Ajouter des informations d’identification pour le fournisseur JMS.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Instanciateur de contexte initial	Nom de la classe JNDI utilisée pour créer l’InitialContext. **Remarque :** Par exemple, pour vous connecter à ActiveMQ V5.10 (fournisseur JMS), la valeur est org.apache.activemq.jndi.ActiveMQInitialContextFactory.
URL du fournisseur	Emplacement de l’installation du fournisseur JMS en cours d’exécution. **Remarque :** Par exemple, pour vous connecter à ActiveMQ V5.1 : tcp://ipAddressOrHostName:61616.
Actif	Cochez la case pour en faire une connexion active.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Option	Description
Domaine	Déterminez le domaine dans lequel l'action ou l'activité s'exécute.
Utiliser un MID Server	Cochez cette case pour utiliser un Serveur MID pour cette action ou cette activité. Si cette option est sélectionnée, définissez les champs dans la section Configuration avancée de Serveur MID.
Sélection de MID	Option permettant de sélectionner le serveur MID ou la grappe MID spécifique. ○ **Sélectionner automatiquement un serveur MID** : sélectionne automatiquement le serveur MID. ○ **Serveur MID spécifique** : utilise le serveur MID que vous sélectionnez. ○ **Grappe MID spécifique** : utilise la grappe MID que vous sélectionnez. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée.
Grappe MID	La grappe MID spécifique que vous souhaitez utiliser. Ce champ est disponible lorsque **l'option Utiliser un serveur MID** est cochée et **qu'une grappe MID spécifique** est sélectionnée dans la liste Sélection MID.
Aptitudes	Options que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action ou l'activité à partir d'un Serveur MID qui prend en charge les options sélectionnées. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .
Application MID	Application que Serveur MID doit prendre en charge pour être éligible à la sélection. Le système exécute l'action à partir d'un Serveur MID qui prend en charge l'application sélectionnée. S'affiche uniquement si l'option **Utiliser un MID Server** est sélectionnée. Pour en savoir plus sur la façon dont un Serveur MID est sélectionné pendant l'exécution, consultez MID Server selection .

3. Accédez à la **Connexions et informations d'identification** > **Informations d'identification**.
4. Cliquez sur **Nouveau**, sélectionnez **Informations d'identification JMS**, puis indiquez le nom d'utilisateur et le mot de passe que le MID doit utiliser pour communiquer avec le fournisseur JMS.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour plus d'informations, consultez Informations d’identification JMS.

5. Cliquez sur **Envoyer**.
   Vous êtes prêt à créer une action ou une activité JMS personnalisée.

Créer des attributs de connexion pour le Centre d’intégration

Définissez des variables spécifiques à la connexion que vous pouvez utiliser dans les étapes d'intégration Hub d'intégration.

Avant de commencer

Rôle requis :

- Le rôle administrateur est requis pour créer des attributs de connexion.
- Le rôle connection_admin ou administrateur est requis pour affecter des valeurs d’attribut.
- Le rôle action_designer ou administrateur est requis pour utiliser des attributs dans une action personnalisée.

Les attributs de connexion ne sont utilisés que par les étapes d’intégration, qui nécessitent un abonnement à Hub d'intégration. Pour plus d’informations sur l’activation Hub d'intégration, voir Demander un Hub d'intégration module d'extension .

Pourquoi et quand exécuter cette tâche

Lorsque vous utilisez une étape d'intégration, vous devez établir une connexion avec un système externe. Utilisez un alias de connexion et d'informations d'identification au lieu de définir l'inline de la connexion. Un alias vous permet de mettre à jour les détails de la connexion une seule fois, sans avoir à reconfigurer chaque action. Toute étape d'action qui utilise un alias hérite des attributs qui lui sont associés. Studio de workflow affiche les attributs en tant que pastilles de données que vous pouvez faire glisser dans votre étape d'action. Par exemple, vous pouvez créer un attribut de taille de page qui devient un paramètre de requête d'étape REST.

Pour plus d’informations sur la création d’actions personnalisées Studio de workflow , consultez Studio de workflow .

Procédure

1. Accédez à la **Tout** > **Informations d'identification et connexions** > **Alias de connexion et d'informations d'identification**.
2. Créez ou sélectionnez un enregistrement d’alias.
3. Dans la liste connexe des attributs de connexion, cliquez sur **Nouveau**.
4. Définissez l’étiquette d’attribut et le type de champ.
   Pour obtenir la liste des types de champs, reportez-vous à la rubrique Types de champs .
5. Cliquez sur le lien connexe Vue avancée pour définir les préférences avancées du dictionnaire pour l’attribut. Par exemple, pour créer un attribut avec une valeur calculée dynamiquement. Consultez Dictionary entry form .
6. Cliquez sur **Envoyer**.
7. Définissez les valeurs d’attribut dans l’enregistrement de connexion.

   a. Accédez à la **Informations d'identification et connexions** > **Connexions**.

   b. Créez ou sélectionnez un enregistrement de connexion avec le même type de connexion que l’alias.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Dans **Alias de connexion**, sélectionnez l’alias avec des attributs de connexion.

d. Enregistrez l'enregistrement.
L’onglet Attributs est renseigné avec les attributs de connexion définis dans l’enregistrement d’alias.

e. Définissez des valeurs pour les attributs.
Si la **prise en charge de plusieurs connexions actives** est activée pour l’alias, vous pouvez associer plus d’un enregistrement de connexion à un alias et définir des valeurs d’attribut dans chaque enregistrement de connexion. S’il existe plusieurs enregistrements de connexion avec des valeurs d’attribut pour le même alias, la connexion utilisée lorsque le flux s'exécute détermine les valeurs d'attribut. Par exemple, vous activez une action qui utilise un alias avec deux points de terminaison de connexion actifs : production et test. L'attribut se résout à la valeur définie par la connexion utilisée lors de l'exécution.

8. Ajouter l’alias à une étape d’intégration dans Studio de workflow.

a. Naviguez et Studio de workflow créez ou sélectionnez une action.

b. Ajoutez une étape d’intégration à l’action.

c. Sous Détails de la connexion, ajoutez l’alias pour lequel vous avez créé des attributs.

Les attributs de connexion associés à l’alias s’affichent sous forme de pastilles de données dans le volet Données.

Remarque :
Le système ne suit pas les changements apportés aux étiquettes d’attributs de connexion et aux types de données après que vous avez associé l’alias à une étape. Pour actualiser l’étiquette d’attribut de connexion ou le type de données, supprimez l’alias de l’étape et ajoutez-le à nouveau.

Introduction aux informations d'identification

Le serveur MID utilise les informations d’identification que vous créez dans la table Informations d’identification [discovery_credentials] pour accéder aux ressources de Découverte, d’orchestration, de Mappage des services et de Gestion cloud.

Comment les MID Server utilisent-ils les informations d’identification ?

Par défaut, les serveurs MID Windows utilisent les informations d’identification de connexion du service du serveur MID sur l’ordinateur hôte pour détecter Windows les périphériques du réseau. Vous devez configurer les informations d’identification du service Windows MID Server afin qu’elles disposent au moins des privilèges d’administrateur local. Pour Linux les machines et UNIX les périphériques réseau, le Serveur MID utilise les informations d’identification SSH et SNMP configurées dans l’instance dans **Découverte** > **Informations d'identification**.

Les serveurs MID utilisés Orchestration doivent avoir accès aux informations d’identification nécessaires pour exécuter des commandes sur les ordinateurs du réseau, comme spécifié par les activités du workflow . Orchestration peut utiliser les mêmes informations d’identification SSH et SNMP que Découverte, mais dispose de deux informations d’identification supplémentaires conçues pour des activités de workflow spécifiques : Windows (pour les activités PowerShell) et VMware.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Chiffrement et déchiffrement

La plateforme stocke les informations d'identification dans un champ chiffré de la table Informations d'identification [discovery_credentials]. Une fois entrés, ils ne peuvent plus être visualisés.

Lorsque le MID Server demande des informations d'identification, il Now Platform les déchiffre à l'aide du processus suivant :

1. Les informations d'identification sont déchiffrées sur l'instance avec la clé fixe password2.
2. Les informations d'identification sont chiffrées à nouveau sur l'instance avec la clé publique du MID Server.
3. Les informations d'identification sont chiffrées sur l'équilibreur de charge avec SSL.
4. Les informations d'identification sont déchiffrées sur le serveur MID avec SSL.
5. Les informations d'identification sont déchiffrées sur le serveur MID à l'aide de la clé privée du serveur MID.

Remarque :
La plateforme ne dispose pas de clés de chiffrement distinctes pour les instances mutualisées.

Ordre des informations d'identification

Une valeur d'ordre peut être affectée aux informations d'identification dans le formulaire Informations d'identification, ce qui oblige l'application à essayer toutes les informations d'identification à sa disposition dans un certain ordre. Si vous ne spécifiez pas de valeur d'ordre, l'application teste les informations d'identification dans la table Informations d'identification [discovery_credential] de manière aléatoire, jusqu'à ce qu'elle en trouve une qui fonctionne. Par exemple, lorsque :

- Orchestration tente d'exécuter une commande sur un serveur SSH, tel qu'un ordinateur Linux ou UNIX.
- Discovery tente d'interroger un périphérique SNMP, tel qu'une imprimante, un routeur ou un onduleur.

Après avoir identifié les informations d'identification d'un appareil et Orchestration, Découverte créez une relation entre les informations d'identification et l'appareil à l'aide de la table Relation d'informations d'identification [dscy_credentials_affinity]. Toutes les détections ultérieures ou activités d'Orchestration tentent de faire correspondre les informations d'identification de cette table avec un appareil pour lequel il existe une affinité. Si les informations d'identification d'un périphérique changent, Découverte et Orchestration réessayez toutes les informations d'identification disponibles jusqu'à ce qu'elles créent une nouvelle relation.

Remarque :
Si Orchestration et Découverte sont installés et que l'alias d'informations d'identification est activé, plusieurs affinités peuvent exister. Dans ce cas, la plateforme recherche les informations d'identification pour chaque relation et insère les informations d'identification de la relation avec l'ordre le plus bas dans la sonde.

La commande d'informations d'identification est utile dans les situations suivantes :

- La table Informations d'identification contient de nombreuses informations d'identification, certaines étant utilisées plus fréquemment que d'autres. Par exemple, la table contient 150 informations d'identification SSH, dont cinq sont utilisées pour se connecter à 90 % des appareils. Il est recommandé de configurer ces cinq informations d'identification avec des numéros de commande basse, qui les placent en haut de la liste

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'exécution. Découverte et Orchestration fonctionnent plus rapidement lorsqu'ils essaient d'abord ces informations d'identification courantes. Après la première connexion réussie, le sait Now Platform quelles informations d'identification utiliser la prochaine fois pour chaque appareil.

- Il Now Platform dispose d'une sécurité de connexion agressive. Par exemple, configurez les informations d'identification de base de données avec une valeur d'ordre inférieur si les serveurs de base de données Solaris du réseau ne fournissent que trois échecs de tentatives de connexion avant de verrouiller le MID Server.

Alias d'informations d'identification

Les alias d'informations d'identification sont disponibles pour Détection et Orchestration.

Les alias pour Discovery permettent à un administrateur d'effectuer les opérations suivantes :

- Utilisez un comportement de filtrage des informations d'identification avec des niveaux de conformité configurables.
- Affectez plusieurs alias d'informations d'identification à un calendrier de détection.
- Empêchez la création de relations d'informations d'identification qui utilisent des informations d'identification inappropriées ou sensibles. Pour en savoir plus, consultez la rubrique Affinités d'identifiants.

Les alias pour Orchestration permettent aux créateurs de workflows :

- Affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration
- Affecter des informations d'identification individuelles à n'importe quelle action dans Concepteur de flux
- Affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
- Affectez des informations d'identification différentes à chaque occurrence de la même action dans le flux Designer.

Banques d'identifiants externes

Si vous ne souhaitez pas que les informations d'identification soient stockées dans votre instance, vous pouvez utiliser des référentiels d'informations d'identification externes. Les banques d'informations d'identification externes enregistrent les informations d'identification dans un site externe auquel votre instance peut accéder. CyberArk est la seule banque d'identifiants externes prise en charge. Toutefois, d'autres magasins externes peuvent être configurés à l'aide de l'API ServiceNow.

Créer un alias de connexion et d'informations d'identification

Définissez un alias pour étiqueter un enregistrement d'informations d'identification ou de connexion.

Avant de commencer

Rôle requis :

- Le rôle administrateur est requis pour créer un alias.
- Les rôles credential_admin et connection_admin disposent d'un accès en lecture à l'enregistrement d'alias.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

L'alias Connexion et informations d'identification définit un alias qui étiquette un enregistrement d'informations d'identification ou de connexion. L'alias contient ces champs.

Procédure

1. Accédez à la **Tout** > **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Complétez les champs du formulaire.

Alias de connexion et d'informations d'identification

Champ	Description
Nom	Nom de l'alias. Un alias ne peut contenir que des caractères alphanumériques, numériques et de soulignement. Lors d'une mise à niveau, la balise dans l'enregistrement d'informations d'identification migre vers un alias de connexion et d'informations d'identification. Si la balise d'informations d'identification contient des caractères spéciaux autres que des lettres, des chiffres et des traits de soulignement, elle conserve le nom de la balise après la mise à niveau. Vous pouvez toujours utiliser cet alias migré, mais vous ne pouvez pas mettre à jour l'alias tant que vous n'avez pas modifié le nom pour respecter les restrictions de dénomination.
ID	Identificateur unique de l'alias de connexion et d'informations d'identification, basé sur le format `scope_name.alias_name`. ○ Si le périmètre est Global, l'ID est le nom de l'alias. Par exemple, si vous créez un alias Workday dans le champ d'application global, l'ID est défini sur `Workday`. ○ Si vous créez un alias Workday dans le périmètre de l'application RH, l'ID est défini sur `x_hr_app.workday`.
Type	Sélectionnez **Informations d'identification** ou **Connexion et informations d'identification**. La valeur par défaut est Connexion et informations d'identification.
Application	Périmètre de l'application par rapport auquel l'alias de connexion et d'informations d'identification est affecté. Le champ d'application de la session en cours que vous avez sélectionné pour la dernière fois dans le sélecteur d'application s'affiche. ○ Par exemple, **Global** s'affiche s'il s'agit du champ d'application actuel de cette session. ○ Vous pouvez modifier le périmètre dans le sélecteur d'application avant de créer un alias. Pour en savoir plus sur les périmètres de l'application et comment les sélectionner, consultez : ▪ Périmètre de l'application ▪ Select an application from the application picker
Type de connexion	Nom du type de connexion, soit De base, HTTP, JDBC, JMS ou Kafka. La valeur par défaut est HTTP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Prendre en charge plusieurs connexions actives	Désignateur qui indique si l'alias prend en charge plusieurs connexions actives. Ajoutez des connexions à l'aide de la table Connexions et associez-les à l'alias à l'aide de la liste connexe Connexions.
Politique des nouveaux essais par défaut	Politique des nouveaux essais pour l'alias. Pour plus d'informations, consultez la politique des nouveaux essais .
Modèle de configuration	Modèle de configuration à utiliser pour créer un enregistrement de connexion et d'informations d'identification.

4. Cliquez sur **Enregistrer**.
   La liste connexe Connexions et attributs de connexion s'affiche.

Liste connexe	Description
Connexions	Enregistrements de connexion connexes associés à cet alias. Après avoir créé l'alias, vous pouvez définir des enregistrements de connexion et les associer à l'alias. Si **l'option Prendre en charge plusieurs connexions actives** est sélectionnée, vous pouvez associer plus d'une connexion à un alias.
Attributs de connexion	Attributs de la connexion. Définissez des données spécifiques à une connexion et utilisez-les dans une étape d'intégration Hub d'intégration . Pour plus d'informations, consultez Créer des attributs de connexion pour le Centre d'intégration.
Alias enfants	Alias enfants associés à l'alias parent. Après avoir créé un alias de connexion et d'informations d'identification, vous pouvez créer un *alias enfant* pour configurer plusieurs connexions pour la même intégration d'application.

Liste connexe	Description
Connexions	Enregistrements de connexion connexes associés à cet alias. Après avoir créé l'alias, vous pouvez définir des enregistrements de connexion et les associer à l'alias. Si **l'option Prendre en charge plusieurs connexions actives** est sélectionnée, vous pouvez associer plus d'une connexion à un alias.
Attributs de connexion	Attributs de la connexion. Définissez des données spécifiques à une connexion et utilisez-les dans une étape d'intégration Hub d'intégration . Pour plus d'informations, consultez Créer des attributs de connexion pour le Centre d'intégration.

5. **Facultatif :** Si vous souhaitez créer des informations d'identification et une connexion associées à votre alias d'informations d'identification, sous `Related Links`, cliquez sur **Créer une nouvelle connexion et de nouvelles informations d'identification**.
   Les enregistrements de connexion et d'informations d'identification qui en résultent sont basés sur un modèle de configuration prédéfini. Voir les modèles de configuration de connexion et d'informations d'identification.
6. **Facultatif :** Si vous souhaitez créer un alias enfant pour votre alias de connexion et d'informations d'identification, sous la liste connexe **Alias enfants** , sélectionnez **Nouveau**.

   a. Donnez un nom à l'alias enfant et sélectionnez **Soumettre**.
      L'alias enfant hérite des propriétés de l'alias parent. Vous pouvez ensuite configurer un alias enfant pour qu'il contienne son propre ensemble d'informations de connexion et d'informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Que faire ensuite

Créez un ou plusieurs enregistrements de connexion à associer à l'alias ou aux alias enfant. Pour en savoir plus sur la création de connexions, reportez-vous à la section Mise en route des connexions. Ajoutez des attributs de connexion à l'alias pour rendre les métadonnées de connexion disponibles aux flux dans Studio de workflow.

Configurer l'intégration OAuth via Serveur MID

Créez un enregistrement de connexion permettant l'envoi d'une demande de jeton OAuth à un serveur tiers via un Serveur MID.

Avant de commencer

Confirmez que vous êtes abonné au programme d'installation du pack standard ServiceNow Centre d'intégration. Pour plus d'informations, consultez https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Rôle requis : admin

Procédure

Configurez la connexion avec un modèle de configuration.

a. Accédez à la **Tout** > **Centre d'intégration** > **Modèles de configuration**.

b. Sélectionnez **Nouveau**.

c. Sélectionnez le **type d'accord de connexion HTTP avec les informations d'identification du client OAuth**.

d. Mettez à jour le formulaire selon vos besoins.
Par exemple, vous pouvez fournir le champ d'application dans les champs `oauth_entity_profile_scope` et `oauth_entity_scope` de la section Modèle de données par défaut. Pour apprendre à créer un modèle de configuration, reportez-vous à la section Créer un modèle de configuration.

e. Sélectionnez **Soumettre**.
Vous avez créé le modèle de configuration.

f. Accédez à la **Tout** > **Centre d'intégration** > **Alias de connexion et d'informations d'identification**.

g. Mettez à jour le formulaire.

Alias de connexion et d'informations d'identification

Champ	Description
Nom	Nom de l'alias. Un alias ne peut contenir que des caractères alphanumériques, numériques et de soulignement. Lors d'une mise à niveau, la balise dans l'enregistrement d'informations d'identification migre vers un alias de connexion et d'informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'identification. Si la balise d'informations d'identification contient des caractères spéciaux autres que des lettres, des chiffres et des traits de soulignement, elle conserve le nom de la balise après la mise à niveau. Vous pouvez toujours utiliser cet alias migré, mais vous ne pouvez pas mettre à jour l'alias tant que vous n'avez pas modifié le nom pour respecter les restrictions de dénomination.
Application	Identificateur unique de l'alias de connexion et d'informations d'identification, basé sur le format `scope_name.alias_name`. ○ Si le périmètre est Global, l'ID est le nom de l'alias. Par exemple, si vous créez un alias Workday dans le champ d'application global, l'ID est défini sur `Workday`. ○ Si vous créez un alias Workday dans le périmètre de l'application RH, l'ID est défini sur `x_hr_app.workday`.
Alias parent	Option permettant de sélectionner l'alias sous lequel vous créez cet alias de connexion et d'informations d'identification. L'alias de connexion et d'informations d'identification que vous créez est un alias enfant. Un alias enfant est répertorié sous l'onglet **Alias enfants** de la page parente Alias de connexion et d'informations d'identification. 
Type	Option permettant d'indiquer le type d'alias que vous créez. Choisissez parmi les options suivantes. ○ Informations d'identification : alias qui contient un enregistrement d'informations d'identification. ○ Connexion et informations d'identification : alias qui contient à la fois l'enregistrement de connexion et d'informations d'identification. Cette option est sélectionnée par défaut. Confirmez que Connexion et informations d'identification sont sélectionnées.
Prendre en charge plusieurs connexions actives	Désignateur qui indique si l'alias prend en charge plusieurs connexions actives. Ajoutez des connexions à l'aide de la table Connexions et associez-les à l'alias à l'aide de la liste connexe Connexions.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Politique des nouveaux essais par défaut	Politique des nouveaux essais pour l'alias. Pour plus d'informations, consultez la politique des nouveaux essais .
Modèle de configuration	Option permettant de sélectionner le modèle de configuration sur lequel vous créez l'alias de connexion et d'informations d'identification. Sélectionnez le modèle de type **d'attribution de connexion HTTP avec les informations d'identification du client OAuth** que vous avez créé.

h. Sélectionnez **Soumettre**.
Vous avez créé l'enregistrement d'alias de connexion et d'informations d'identification.

i. Accédez à la **Tout** > **Centre d'intégration** > **Tableau de bord des connexions**.

j. Dans le champ Rechercher toutes les connexions, saisissez le nom de l'enregistrement d'alias de connexion et d'informations d'identification que vous avez créé.

k. Sur l'enregistrement de l'alias de connexion et d'informations d'identification, sélectionnez **Afficher les détails**.

l. Sélectionnez **Configurer**.

m. Remplissez le formulaire.

Enregistrement de connexion

Champ	Description
Nom de la connexion	Nom de l'enregistrement de connexion. Vous ne pouvez pas mettre à jour le nom.
URL de connexion	Option permettant de fournir l'URL qui se connecte au serveur tiers.
Utiliser MID	Option permettant de spécifier que vous souhaitez envoyer des demandes de jetons OAuth via un serveur MID. **Important :** Confirmez que l'option est sélectionnée.
Sélection de MID	Option permettant de spécifier si vous souhaitez utiliser un Serveur MID spécifique, activer la sélection automatique de Serveur MID ou utiliser une grappe MID. Choisissez une des options suivantes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ Sélectionner automatiquement Serveur MID ○ Serveur MID spécifique ○ Grappe MID spécifique
Serveur MID	Option permettant de sélectionner un serveur MID. **Remarque :** Cette option s'affiche si vous sélectionnez **Serveur MID spécifique** dans le champ Sélection de MID.
Grappe MID	Option permettant de sélectionner une grappe MID. **Remarque :** Cette option s'affiche si vous sélectionnez **Grappe MID spécifique** dans le champ Sélection MID.
ID client OAuth	Option permettant de spécifier l'ID client.
Secret client OAuth	Option permettant de spécifier le secret client.
Se connecter au serveur d'authentification via Serveur MID	Option permettant de spécifier que la connexion entre l'instance ServiceNow et le serveur d'authentification s'effectue via le MID Server. **Important :** Confirmez que l'option est sélectionnée.
URL du jeton OAuth	Option permettant de spécifier l'URL du jeton OAuth utilisée pour demander des jetons OAuth.

n. Sélectionnez **Configurer et obtenir un jeton OAuth**.
L'enregistrement de connexion et d'informations d'identification est créé.

Alias d'informations d'identification pour Détection

Alias d'informations d'identification permettant Découverte à un administrateur d'utiliser des informations d'identification spécifiques sur les calendriers Discovery. Vous pouvez configurer des comportements pour vos alias qui déterminent le niveau de rigueur avec lequel le système applique leur utilisation.

Sans alias d'informations d'identification, les calendriers de découverte peuvent accéder à toutes les informations d'identification qui sont définies dans l'instance. Ce comportement peut ne pas être souhaitable dans certaines circonstances, en particulier pour les informations d'identification avec des privilèges élevés. Les alias d'informations d'identification permettent un meilleur contrôle sur les informations d'identification qu'un calendrier Discovery est autorisé à utiliser et empêchent l'exposition inutile des informations d'identification avec des privilèges élevés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fonctionnement des alias d'informations d'identification

Une règle métier appelée *Insérer des alias de détection et d'informations d'identification* (précédemment nommée Insérer des *alias de découverte*) s'exécute lorsqu'un enregistrement est inséré dans la file d'attente ECC. La règle métier joint les alias d'informations d'identification définis dans le calendrier Discovery à la sonde, afin que le MID Server puisse effectuer un filtrage des informations d'identification. La première tâche du MID Server consiste à créer la liste des informations d'identification à rechercher. Il filtre les informations d'identification par affinité , puis par balises, s'il en existe. Les affinités vont en haut de la liste, et les balises correspondantes vont en bas de la liste. Le MID Server parcourt la liste jusqu'à ce qu'il trouve des informations d'identification qui fonctionnent. Le Serveur MID crée ensuite une affinité pour ces informations d'identification.

Remarque :
Les informations d'identification doivent correspondre à toutes les balises d'informations d'identification.

Si la règle métier détermine qu'il existe une affinité pour l'appareil, elle identifie le *credential_id* approprié à utiliser. Il s'agit du *sys_id* de l'enregistrement dans la table Informations d'identification [discovery_credentials]. Lorsque la plateforme rencontre une relation avec une valeur d'alias d'informations d'identification, définie comme *credential_alias* dans la règle métier, la règle métier détermine si les informations d'identification référencées par la relation ont l'alias spécifié ou non. Si tel est le cas, la règle métier sélectionne le *credential_id* de l'alias et transmet cette valeur au serveur MID. Si les informations d'identification n'ont pas l'alias d'informations d'identification spécifié, toutes les autres affinités existantes pour le système cible sont vérifiées.

Créer un alias d'informations d'identification Découverte

Créez l'alias, puis ajoutez-le aux informations d'identification dans l'enregistrement d'informations d'identification. Vous pouvez ajouter des informations d'identification à plusieurs alias et ajouter plusieurs informations d'identification à un seul alias.

Avant de commencer
Rôle requis : admin, credential_admin (accès en lecture seule), connection_admin (accès en lecture seule)

Pourquoi et quand exécuter cette tâche
Un calendrier Discovery utilise uniquement les informations d'identification contenues dans les alias définis pour ce calendrier.

Remarque :
Si un alias d'informations d'identification est défini pour un calendrier, il ignorera toute relation d'informations d'identification précédemment existante entre les informations d'identification et la cible détectée dans un calendrier configuré pour utiliser cet alias d'informations d'identification.

Procédure

1. Créez un alias.

a. Accédez à la **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification**.

b. Cliquez sur **Nouveau**.

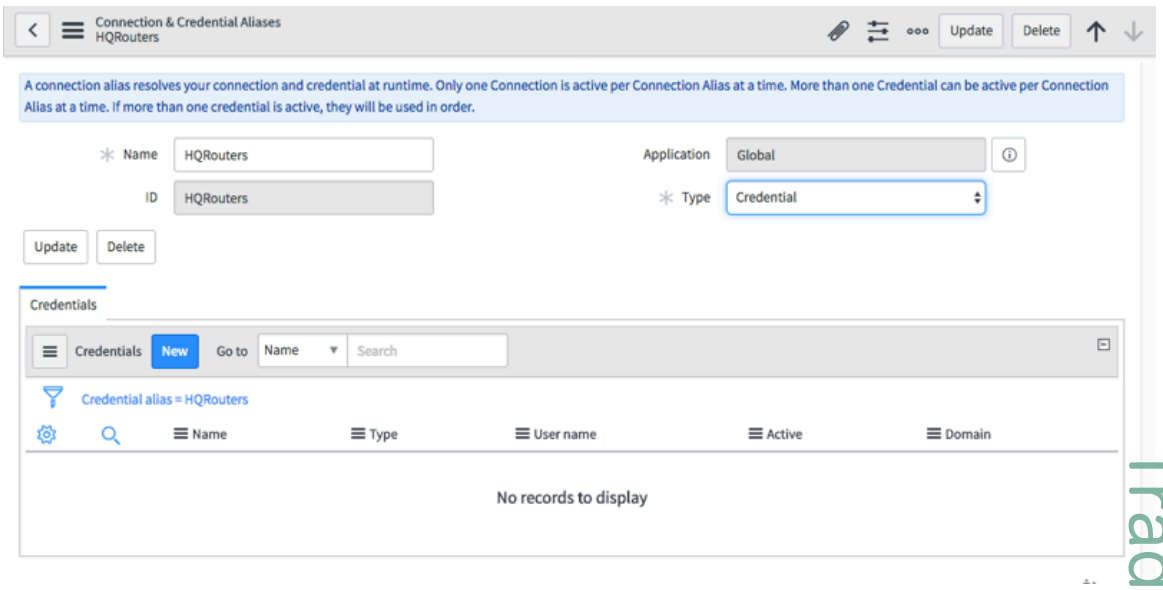
c. Entrez un nom unique pour l'alias et sélectionnez **Informations d'identification** pour le **type d'alias**.

d. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La liste **connexe Informations d'identification** s'affiche. Vous pouvez ajouter de nouvelles informations d'identification pour cet alias dans cette liste, mais pas les informations d'identification existantes.

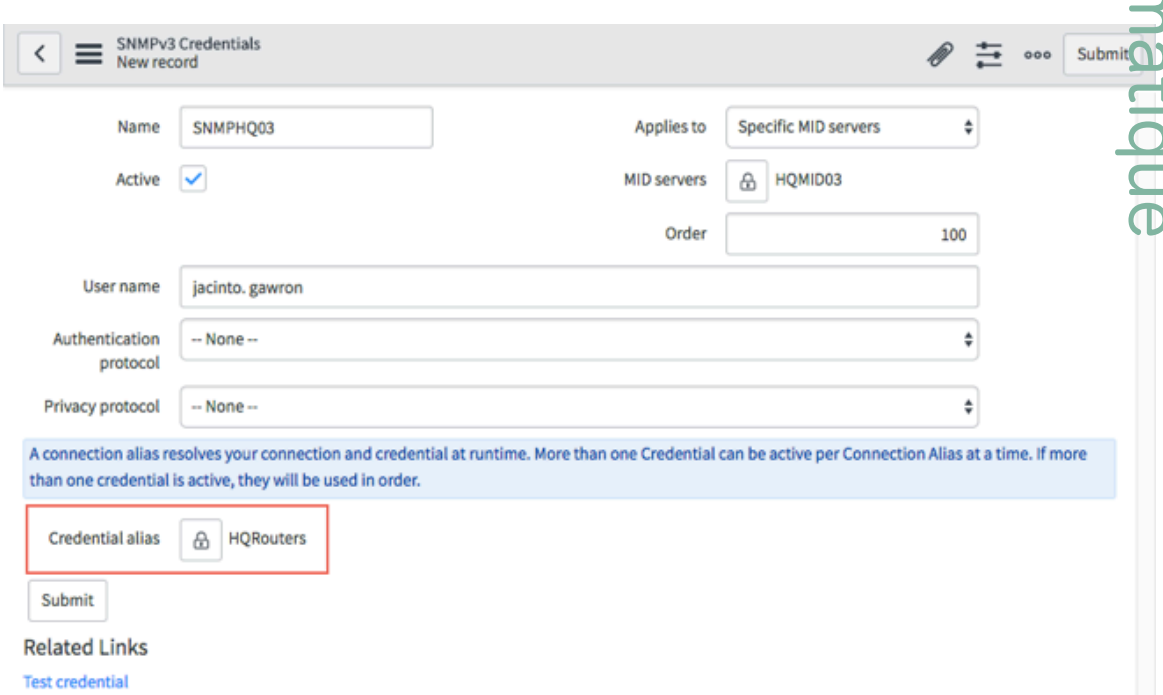


2. Configurez des informations d'identification pour le nouvel alias.

a. Accédez à la **Connexions et informations d'identification** > **Informations d'identification**.

b. Sélectionnez des informations d'identification existantes dans la liste ou cliquez sur **Nouveau** pour créer des informations d'identification.

c. Dans l'enregistrement Informations d'identification, déverrouillez le champ **Alias d'informations d'identification** et sélectionnez l'alias que vous avez créé.

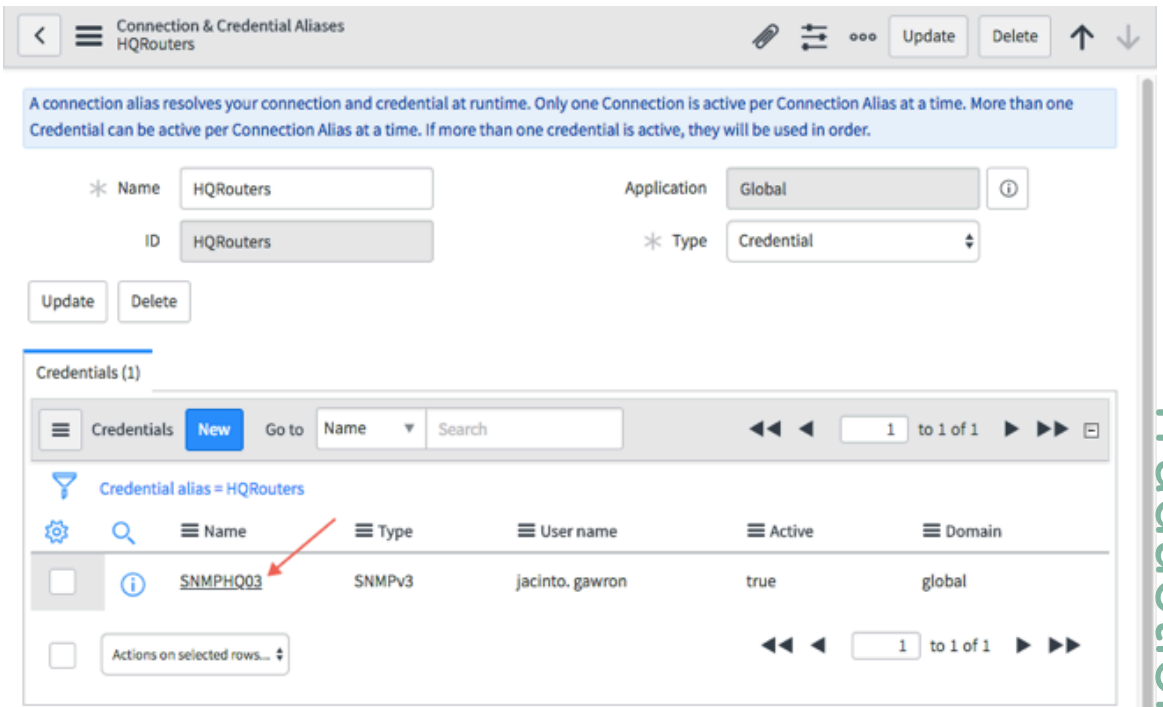


d. Enregistrez ou soumettez l'enregistrement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Retourner à **Connexions et informations d'identification** > **Alias de connexion et d'informations d'identification** et ouvrez votre nouvel alias.
   Les informations d'identification que vous avez jointes à l'alias apparaissent maintenant dans la liste connexe.



4. Pour créer des informations d'identification supplémentaires pour cet alias, cliquez sur **Nouveau** dans la liste connexe et sélectionnez un type d'informations d'identification.
   Le nom de l'alias est pré-rempli dans le champ **Alias d'informations d'identification** de l'enregistrement d'informations d'identification.
5. Renseignez les champs dans le formulaire et envoyez l'enregistrement.

Alias d'informations d'identification pour les activités Orchestration

L'alias d'informations d'identification donne à l'administrateur davantage de contrôle sur les informations d'identification utilisées dans les activités d'Orchestration.

Cela est utile lorsqu'une activité nécessite des informations d'identification spécifiques pour effectuer une tâche. Vous pouvez utiliser une balise d'informations d'identification pour attribuer des informations d'identification individuelles à n'importe quelle activité dans un workflow Orchestration ou attribuer des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.

L'alias d'informations d'identification interagit avec l'affinité des informations d'identification pour déterminer quelles informations d'identification doivent être utilisées pour une activité Orchestration.

Fonctionnement de l'alias d'informations d'identification

Une règle métier appelée *Insérer une relation de détection* (renommée Insérer une relation d'informations d'identification dans la version Geneva) s'exécute lorsqu'un enregistrement est inséré dans la file d'attente ECC. Cette règle détermine s'il existe une relation d'informations d'identification pour l'équipement et identifie le *credential_id* approprié (le *sys_id* de l'enregistrement dans la table Informations d'identification [discovery_credentials])

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

à utiliser. Lorsque la plateforme rencontre une relation avec une valeur d'alias d'informations d'identification définie (*credential_alias* dans la règle métier), la règle métier détermine si les informations d'identification référencées par la relation ont l'alias spécifié. Si tel est le cas, la règle métier sélectionne le *credential_id* de l'alias d'informations d'identification et transmet cette valeur au serveur MID. Si les informations d'identification n'ont pas l'alias d'informations d'identification spécifié, toutes les autres affinités qui existent pour le système cible seront vérifiées. Si aucune relation ne fait référence à des informations d'identification correctement balisées, le MID Server parcourt la table Informations d'identification *[discovery_credentials]* et sélectionne les informations d'identification avec la balise appropriée. Le Serveur MID crée alors une nouvelle affinité pour ces informations d'identification.

Créer et tester vos informations d'identification

Créez et testez les informations d'identification dont Découverte, Mappage des services, Gestion cloud et Orchestration ont besoin pour accéder au matériel et aux logiciels de votre réseau.

Avant de commencer

Rôle requis : administrateur

Passez en revue votre politique et vos options de sécurité avec l'équipe de sécurité de votre organisation.

Pourquoi et quand exécuter cette tâche

Cette tâche contient des procédures générales pour la création d'informations d'identification. Consultez la documentation relative à votre type d'informations d'identification pour plus d'informations sur les champs et les exigences spécifiques.

Types d'informations d'identification pris en charge

Informations d'identification applicatives	Informations d'identification d'authentification de base	Informations d'identification du serveur Chef
Informations d'identification CIM	Informations d'identification dans le cloud	Informations d'identification Infoblox
Informations d'identification JDBC	Informations d'identification JMS	Informations d'identification OAuth 2.0
Informations d'identification SAP	Informations d'identification SNMP	Informations d'identification SSH
Informations d'identification VMware	Informations d'identification Windows	Informations d'identification du référentiel d'images de conteneur

Remarque :
Pour améliorer la sécurité, limitez le périmètre des informations d'identification à un calendrier ou à un serveur MID spécifique afin d'éviter les informations d'identification inutiles.

Procédure

1. Accédez à l'un de ces modules :
   - **Découverte** > **Informations d'identification**
   - **Mappage des services** > **Informations d'identification**
   - **Orchestration** > **Informations d'identification**
2. Cliquez sur **Nouveau**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

3. Sur la page Informations d'identification, cliquez sur un lien pour le type d'informations d'identification et remplissez le formulaire.

   Consultez la documentation du type d'informations d'identification que vous avez sélectionné pour en savoir plus.

   Vous pouvez d'abord soumettre un enregistrement d'informations d'identification avant de le tester ultérieurement, ou tester les informations d'identification immédiatement avant de les enregistrer.

   Le test des informations d'identification est pris en charge pour ces types d'informations d'identification :

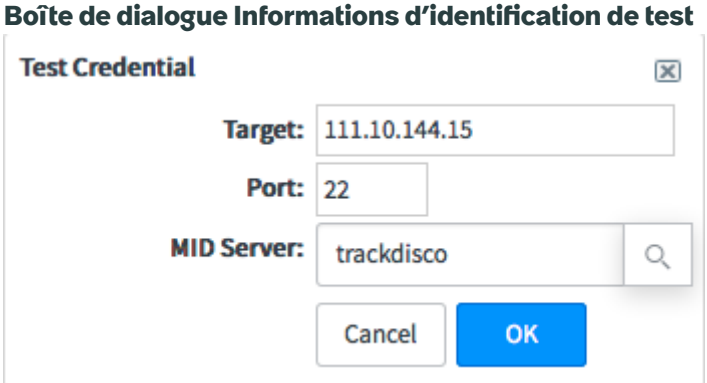
   - Clés privées SSH
   - Windows
   - SNMP v3
   - VMware
   - JDBC
   - JMS

4. Sous **Liens connexes**, cliquez sur Tester les **informations d'identification**.

   Remarque :
   Les informations d'identification sont chiffrées à tout moment pendant le test.

5. Renseignez les champs de la boîte de dialogue Tester les informations d'identification.

Boîte de dialogue Informations d'identification de test



Champs de test d'informations d'identification

Champ	Description	Type d'informations d'identification
Cible	Hôte cible sur lequel ces informations d'identification sont exécutées. Cette valeur doit être une adresse IP pour tous les types d'informations d'identification, à l'exception de VMware, qui peut être l'URL de l'hôte. Vous ne pouvez pas cibler de MID Server.	Tout

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description	Type d'informations d'identification
	Remarque : Pour JMS, il s'agit de l'URL du fournisseur. Les informations contenues dans cette URL indiquent à JNDI comment trouver et accéder au fournisseur JMS. Un exemple de valeur pour la connexion à ActiveMQ V5.1 est `tcp://ipAddressOrHostName:61616`.	
Port	Port sur la cible à utiliser pour ce test. Le système pré-remplit ce champ avec le port par défaut pour le type d'informations d'identification sélectionné.	Tout
Serveur MID	Serveur MID à utiliser pour ce test. Vous devez utiliser un Serveur MID Windows pour tester les informations d'identification Windows. Seuls les MID Servers **En service** et **Validés** sont disponibles.	Tout
Type de base de données	Type de base de données sur laquelle tester ces informations d'identification.	JDBC
Adresse de la carte	Nom de la base de données sur laquelle tester ces informations d'identification.	JDBC
Instanciateur de contexte initial	Nom de la classe JNDI utilisée pour créer l'InitialContext. À l'aide de cette **fabrique de contexte initiale**, divers objets JMS, tels que JMS Connection, sont créés. Par exemple, pour vous connecter à ActiveMQ V5.10 (fournisseur JMS), la valeur de ce champ serait `org.apache.activemq.jndi.ActiveMQInitialContextFactory`	JMS

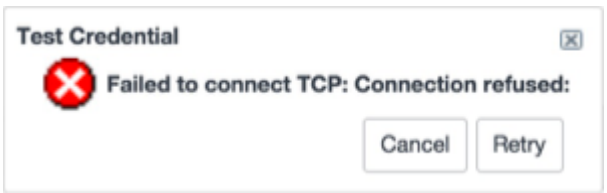
6. Cliquez sur **OK** pour commencer le test.
   Un indicateur s'affiche, indiquant que le système tente de contacter la cible à l'aide des informations d'identification que vous avez fournies. Lorsque l'instance se connecte à la cible, un message de réussite s'affiche. Si l'instance rencontre un problème avec les entrées de test que vous avez fournies, elle affiche le message d'erreur approprié. Vous trouverez ci-dessous quelques-uns des messages d'erreur courants.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

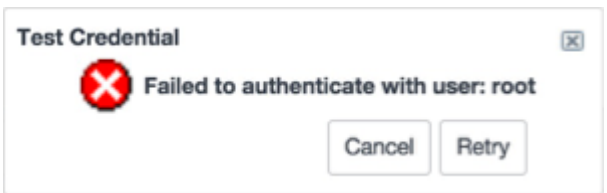
- Numéro de cible ou de port incorrect :

  Échec de la connexion TCP

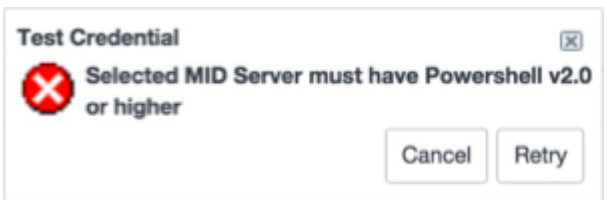
- Nom d'utilisateur ou mot de passe incorrect :

  Échec de l'authentification

- Informations d'identification incorrectes de Serveur MID pour Windows :

  Erreur du serveur MID

7. Cliquez sur **Réessayer** pour ouvrir la boîte de dialogue Tester les informations d'identification et corriger l'erreur d'entrée.
8. Une fois votre test d'informations d'identification réussi, cliquez sur **Envoyer** pour enregistrer l'enregistrement.

> **Important :**
> Le test des informations d'identification ne garantit pas que les informations d'identification disposent des privilèges nécessaires pour les tâches de workflow Découverte ou Orchestration prévues.

Informations d'identification de la tour Ansible

Les informations d'identification Ansible Tower sont requises pour accéder à votre compte de gestion des configurations Ansible. Utilisez ces informations d'identification pour gérer les ressources Ansible via l'application Gestion dans le cloud .

Pour intégrer Cloud Provisioning and Governance avec le compte de gestion des configurations Ansible, vous devez configurer le nom d'utilisateur et le mot de passe du compte administrateur dans Ansible.

Champs de formulaire pour les informations d'identification de la tour Ansible

Champ	Description
Nom	Fournissez un nom descriptif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire pour les informations d'identification de la tour Ansible (suite)

Champ	Description
Nom d'utilisateur/ mot de passe	Entrez les informations d'identification d'authentification pour l'utilisateur de la tour Ansible avec les droits d'administrateur.

Remarque :
Vous n'avez pas besoin de configurer les autres champs.

Informations d'identification de clé API

Une clé API est un code unique transmis à une API pour identifier l'application ou l'utilisateur appelant.

Informations d'identification de clé API

Champs de formulaire Informations d'identification de clé API

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Clé API	Saisissez la clé API.
Alias d'informations d'identification	Autorisez les créateurs de flux et de workflow à affecter des informations d'identification individuelles à n'importe quelle activité d'un flux ou d'un workflow ou à attribuer des informations d'identification différentes à chaque occurrence du même type d'activité dans un flux ou un workflow.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification applicatives

Certaines applications nécessitent des informations d'identification en plus des informations d'identification requises par l'ordinateur hôte. Les informations d'identification requises pour accéder à ces applications sont appelées informations d'identification applicatives.

Les informations d'identification classiques contiennent un nom d'utilisateur et un mot de passe pour se connecter à un appareil ou à une application. Bien que la plupart des applications n'aient besoin que d'un seul identifiant pour se connecter, les hôtes et les applications disposent parfois d'informations d'identification distinctes pour plus de

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

sécurité. Par exemple, ABAP SAP Central Services (ASCS) nécessite des informations d'identification applicatives en plus des informations d'identification de l'hôte SSH ou Windows pour le serveur qui héberge ASCS.

Remarque :
ServiceNow désignent les appareils et les applications dont les éléments de configuration (CI) contiennent un service d'application.

Comme pour les informations d'identification de l'hôte, vous attribuez des informations d'identification applicatives à Serveurs MID.

Vous créez des informations d'identification applicatives par type de CI, par exemple, le type de CI pour ASCS est SAP ASCS Application [cmdb_ci_appl_sap_ascs]. Le modèle préconfiguré pour la détection des CI appartenant à ce type de CI contient des commandes qui nécessitent qu'un Serveur MID utilise les informations d'identification applicatives pour ce type de CI. S'il existe plusieurs informations d'identification configurées pour ce type de CI, le Serveur MID essaie d'utiliser ces informations d'identification dans l'ordre que vous définissez jusqu'à ce qu'il trouve les informations d'identification qui correspondent.

Vérifiez les informations sur les besoins Découverte dans la documentation ServiceNow afin de déterminer si vous devez configurer des informations d'identification applicatives pour des CI d'application spécifiques. Il n'est pas nécessaire de configurer les informations d'identification applicatives si Découverte les prérequis ne le mentionnent pas.

Champs du formulaire Informations d'identification applicatives

Champ	Description
Nom	Nom des informations d'identification. Utilisez un nom descriptif comme « Base de données Oracle » ou « Base de données Oracle London » (pour une base de données Oracle). N'utilisez pas d'espaces ou de caractères spéciaux pour le nom des informations d'identification.
Actifs	Cochez la case pour utiliser les informations d'identification.
Nom d'utilisateur	Entrez le nom d'utilisateur réel des informations d'identification applicatives.
Mot de passe	Entrez le mot de passe réel des informations d'identification applicatives. N'utilisez pas d'espaces ou de caractères spéciaux pour le nom des informations d'identification.
Type de CI	Sélectionnez un type de CI auquel le CI appartient.
Alias d'informations d'identification	Créez un alias pour affecter des informations d'identification spécifiques à des calendriers de détection spécifiques. Lorsque vous affectez un alias, vous devez identifier le nom de table du type de CI dont les informations d'identification applicatives sont utilisées par l'application. Les applications peuvent utiliser des informations d'identification applicatives d'un type de CI différent du leur. Pour une application spécifique, consultez la liste de la table appropriée : • SAP ABAP Central Services (ASCS) : cmdb_ci_appl_sap_ascs • IBM Security Access Manager appliance : cmdb_ci_app_server_webseal • Instance SAP Central : cmdb_ci_appl_sap_ascs • SAP Central Services (SCS) : cmdb_ci_appl_sap_ascs • Evaluated Receipt Settlement (ERS) SAP : cmdb_ci_appl_sap_ascs • Grappe Java SAP : cmdb_ci_appl_sap_ascs

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs du formulaire Informations d'identification applicatives (suite)

Champ	Description
	• Instance de boîte de dialogue SAP NetWeaver : cmdb_ci_appl_sap_ascs • Messagerie Microsoft Exchange (pour Microsoft Exchange) : cmdb_ci_exchange_mailbox • Base de données SQL Microsoft : cmdb_ci_db_mssql_instance • Serveur MySQL : cmdb_ci_db_mysql_instance • File d'attente avancée Oracle : cmdb_ci_db_ora_instance • Oracle Database : cmdb_ci_db_ora_instance • Oracle E-Business Suite : cmdb_ci_db_ora_instance • Module Oracle WebLogic : cmdb_ci_app_server_weblogic • TIBCO Enterprise Message Service (EMS) : cmdb_ci_appl_tibco_message
S'applique à	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification d'authentification de base

Le type d'informations d'identification d'authentification de base gère l'accès au stockage des informations d'identification d'authentification de base.

Ces champs sont disponibles dans le formulaire Informations d'identification pour l'authentification de base.

Formulaire des informations d'identification pour l'authentification de base

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l'appeler **authentification de base**.
Noms d'utilisateur	Entrez le nom d'utilisateur.
Mot de passe	Entrez le mot de passe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire des informations d'identification pour l'authentification de base (suite)

Champ	Valeur d'entrée
ID de certification	Saisissez la clé unique configurée pour ces informations d'identification dans le système de stockage d'informations d'identification externe CyberArk . L'ID d'informations d'identification peut être utilisé comme remplacement sécurisé lorsque plusieurs coffres-forts sont en cours d'utilisation. Par défaut, la syntaxe du champ **ID d'informations d'identification** est la suivante : `<safe name>:<Credential ID>`. Si le nom de sauvegarde est omis, il doit y avoir un nom de confiance défini dans le fichier de config.xml . Pour remplacer le caractère de séparation par deux-points par défaut par un autre caractère, remplacez la valeur par le paramètre facultatif `ext.cred.safe_name` . Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Stockage externe** est cochée.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Actuellement, le seul système de stockage externe pris en charge est CyberArk.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification du serveur Chef

Les informations d'identification du serveur Chef permettent d'accéder aux intégrations de Chef avec l'instance.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type serveur Chef. Ces informations proviennent des paramètres que vous avez configurés lors de l'installation du serveur Chef .

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom de l'administrateur	Fournissez le nom de l'administrateur que vous avez créé lors de l'installation du serveur Chef.
Clé d'administrateur	Saisissez la clé privée RSA générée par le serveur Chef lors de la création de l'administrateur.
Nom de validateur	Entrez le validateur.
Clé de validateur	Saisissez la clé privée RSA générée par le serveur Chef lors de la création d'une organisation.
Nom du certificat	Saisissez le nom de la certification.
Clé du certificat	Saisissez la clé de certification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification CIM

Le type d'informations d'identification CIM gère l'accès à un serveur CIM (également appelé CIMOM pour « Common Information Model Object Manager ») afin d'obtenir des informations sur les serveurs ESX VMware. Ce type d'informations d'identification est disponible pour la découverte.

Ces champs sont disponibles dans le formulaire Informations d'identification de CIM.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations d'identification n'est disponible que lorsque le module d'extension Stockage externe des informations d'identification est activé. **Remarque :** À l'heure actuelle, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : La sélection **d'un MID Server spécifique** n'affecte pas la sélection d'un MID Server. Il est utilisé uniquement pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Des MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Configurer les périphériques de stockage NetApp pour les informations d'identification CIM

Les périphériques de stockage NetApp nécessitent une configuration supplémentaire pour Découverte pouvoir les explorer.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Installez l'agent SMI-S sur l'hôte de l'appareil de stockage.

   Reportez-vous au Guide d'installation et de configuration de Data ONTAP SMI-S Agent 5.2 pour connaître les instructions et les conditions requises.

   Remarque :

   ServiceNow ne gère pas la documentation sur ce site. Ce document peut être modifié sans préavis.

2. Créez un compte utilisateur et un mot de passe pour l'agent SMI-S.
3. Créez un enregistrement d'informations d'identification pour les informations d'identification de l'agent SMI-S.
   Définissez le type d'informations d'identification sur **CIM**.

Informations d'identification dans le cloud

Les types d'informations d'identification dans le cloud gèrent l'accès aux applications basées sur le cloud, y compris Amazon Web Services et le cloud Microsoft Azure.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Rôles AWS Identity and Access Management (IAM)

Si un serveur MID est installé sur Amazon EC2 dans un cloud AWS et que ce serveur MID est configuré pour détecter les ressources dans le cloud, vous pouvez utiliser les informations d'identification de sécurité fournies par les rôles AWS Identity and Access Management (IAM) plutôt que les informations d'identification gérées sur votre instance. Ces informations d'identification AWS accordent des autorisations dans le cloud via un *profil d'instance*, en fonction des rôles. Ces informations d'identification sont temporaires et tournent automatiquement à un intervalle configurable. Lorsqu'un rôle IAM est défini sur le MID Server. Pour plus d'informations, consultez Configurer le serveur MID pour les rôles AWS IAM .

La détection ignore les informations d'identification stockées sur l'instance en faveur des informations d'identification accordées par le rôle dans le profil d'instance. Pour plus d'informations sur les profils d'instance AWS, consultez Rôles IAM pour Amazon EC2 .

Informations d'identification AWS

Champs du formulaire Informations d'identification AWS

Champ	Valeur d'entrée
Nom	Nom unique et descriptif pour les informations d'identification AWS.
Actifs	Option pour utiliser les informations d'identification.
ID de clé d'accès	L'**ID de clé d'accès** que vous avez généré sur AWS Management Console, tel que : APIAIOSFODNN7EXAMPLE.
Clé d'accès secrète	**Clé d'accès secrète** que vous avez générée sur AWS Management Console, par exemple : wPalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY.

Champs de formulaire d'informations d'identification du principal du service Azure

Champ	Valeur
Nom	Entrez le nom du principal du service à enregistrer avec l'instance.
ID de locataire et	Collez la valeur **ID de répertoire** Azure à partir du portail Azure dans le champ Gestion dans le cloud **ID de locataire**.
ID client	Collez la valeur **ID d'application** Azure de l'application que vous avez enregistrée dans Azure dans le champ Gestion dans le cloud **ID client**.
Méthode d'authentification	Sélectionnez **Secret client**. **Remarque :** **Assertion du client** n'est pas pris en charge.
Clé secrète	Collez la clé secrète qui a été générée lors de la création du principal du service Azure. Ce champ s'affiche lorsque la **Méthode d'authentification** est **Secret client**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification de l'accord d'entreprise Azure

Les informations d'identification de l'Accord entreprise Azure sont nécessaires pour la fonctionnalité de facturation fournie par l'application Gestion cloud.

Champs de formulaire des informations d'identification de l'accord d'entreprise Azure

Champ	Description
Nom	Saisissez un nom descriptif.
Numéro d'inscription	Entrez le numéro d'inscription à partir d'Azure.
Clé d'accès	Collez la clé d'accès fournie par Azure.

Informations d'identification de Gestion cloud

Ce type d'informations d'identification est disponible pour Orchestration.

Champs de formulaire Informations d'identification de Gestion cloud

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l'appeler **Cloud Atlanta**.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Type	Spécifiez **AWS**.
Nom d'utilisateur	Entrez le nom d'utilisateur CIM à créer dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur.
Mot de passe	Entrez le mot de passe CIM.
Phrase de sécurité SSH	Saisissez une phrase mémorable pour la génération de clés. Par exemple, vous pouvez saisir **Vendredi est un bon jour**.
Clé privée SSH	Saisissez la clé privée SSH.
Protocole d'authentification	Sélectionnez le protocole d'authentification **MD5**ou **SHA** utilisé pour générer la **clé d'authentification**.
Clé d'authentification	Entrez une clé d'authentification générée par SSH.
Protocole de confidentialité	Entrez l'un des protocoles de confidentialité suivants qui décrit le chiffrement de la **clé de confidentialité** : • **3DES** pour Triple Data Encryption Standard (DES) • **AES128 pour AES** (Advanced Encryption Standard) avec chiffrement 128 bits • **AES192** pour AES avec cryptage 192 bits • **AES256** pour AES avec cryptage 256 bits • **DES** pour le chiffrement DES hérité
Saisissez une clé de confidentialité supplémentaire.	

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire Informations d'identification de Gestion cloud (suite)

Champ	Valeur d'entrée
Alias d'informations d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Actuellement, le seul système de stockage externe pris en charge est CyberArk.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
Classification	Entrez la classification d'application pour la découverte de CI.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification du nœud Cloud Management (CMP)

Les informations d'identification de nœud de Gestion cloud (CMP) associent les informations d'identification pour un serveur virtuel que Gestion cloud met en service. L'application Gestion cloud crée automatiquement ces informations d'identification.

Remarque :
Vous devrez peut-être désactiver ces informations d'identification si vous ne souhaitez plus les utiliser, modifier l'ordre de priorité ou sélectionner un serveur MID autorisé à y accéder. Sinon, vous n'avez pas besoin de créer ou de modifier manuellement ce type d'informations d'identification.

Champs de formulaire Informations d'identification du nœud CMP

Champ	Description
Nom	Nom généré automatiquement en fonction du centre de données où se trouve l'ordinateur virtuel.
Actif	Si les informations d'identification sont actives.
Concerne	Choisissez si ces informations d'identification sont disponibles pour un MID Server spécifique ou pour tous les serveurs MID.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de formulaire Informations d'identification du nœud CMP (suite)

Champ	Description
	nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Nom d'utilisateur et mot de passe	Nom d'utilisateur et mot de passe du serveur virtuel.
Phrase de sécurité SSH et clé privée SSH	La clé privée et la phrase de sécurité qui protège la clé si le serveur virtuel l'exige.
Protocole d'authentification et clé d'authentification	La clé privée et la phrase de sécurité qui protège la clé si le serveur virtuel l'exige.
Protocole de confidentialité et clé de confidentialité	Protocole de chiffrement utilisé avec le serveur virtuel et entrez la clé de confidentialité.
Alias d'informations d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.

Informations d'identification de la paire de clés SSH de Cloud Management (CMP)

Les paires de clés SSH Gestion cloud (CMP) stockent les clés que l'application Gestion cloud génère automatiquement lorsque les utilisateurs mettent en service des ressources de pile.

Remarque :
Vous devrez peut-être désactiver ces informations d'identification si vous ne souhaitez plus qu'elles soient utilisées. Sinon, vous n'avez pas besoin de créer ou de modifier manuellement ce type d'informations d'identification.

Champs de formulaire d'informations d'identification de la paire de clés SSH CMP

Champ	Description
Nom	Nom généré automatiquement.
Actif	Si les informations d'identification sont actives.
Clé publique SSH	La clé publique.
Clé privée SSH	Une clé privée sécurisée qui peut être utilisée à la place d'un mot de passe pour les connexions SSH.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification Infoblox

Les informations d'identification Infoblox sont nécessaires pour configurer des pools d'IP (IPAM) dans l'application Gestion cloud.

Ces champs sont disponibles sur le formulaire Informations d'identification pour les informations d'identification de type Infoblox.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Concerne	Choisissez si ces informations d'identification sont disponibles pour un MID Server spécifique ou pour tous les serveurs MID.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement. Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Version wAPI	Entrez la version de wAPI que vous utilisez.
Nom d'utilisateur et mot de passe	Entrez le nom d'utilisateur et le mot de passe InfoBlox.

Informations d'identification JDBC

Le type d'informations d'identification JDBC gère l'accès à une connexion JDBC (Java Database Connectivity). Ce type d'informations d'identification est disponible pour Détection et Orchestration.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type JDBC.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations d'identification n'est disponible que lorsque le module d'extension Stockage externe des informations d'identification est activé. **Remarque :** À l'heure actuelle, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **d'un MID Server spécifique** n'affecte pas la sélection d'un MID Server. Il est utilisé uniquement pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Des MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Informations d’identification JMS

Le type d’informations d’identification JMS gère l’accès à un service de messagerie Java (JMS). Ce type d’informations d’identification est disponible pour Détection et Orchestration.

Ces champs sont disponibles dans le formulaire Informations d’identification de JMS.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations d’identification n’est disponible que lorsque le module d’extension Stockage externe des informations d’identification est activé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : À l'heure actuelle, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **d'un MID Server spécifique** n'affecte pas la sélection d'un MID Server. Il est utilisé uniquement pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Des MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Informations d'identification OAuth 2.0

Les informations d'identification OAuth 2.0 permettent à ServiceNow d'obtenir l'accès aux comptes d'utilisateurs sur un service HTTP.

Ces champs sont disponibles dans le formulaire Informations d'identification pour OAuth 2.0.

Formulaire des informations d'identification OAuth 2.0

Champ	Valeur d'entrée
Nom	Entrez un nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l'appeler **informations d'identification OAuth2**.
Actif	Spécifiez si ces informations d'identification sont actives.
Profil de l'entité OAuth	Un profil OAuth est une combinaison d'un type d'accord et d'au moins un périmètre.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

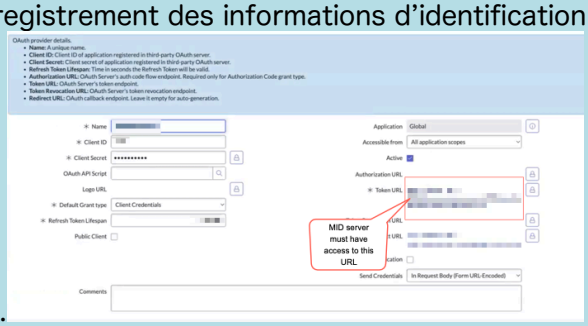
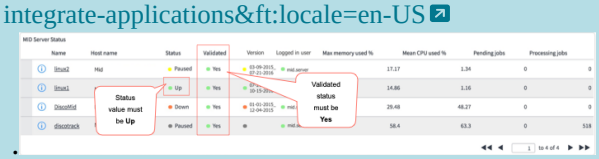
Formulaire des informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
Se connecter au serveur d'authentification via Serveur MID	Connecte votre ServiceNow instance à un serveur OAuth sur site qui réside derrière un pare-feu via un Serveur MID. Il peut également connecter votre ServiceNow instance à un serveur OAuth basé sur le cloud via un MID Server. Lorsque cette option est activée, la demande de jeton OAuth est envoyée via le Serveur MID. **Important :** • L'option s'affiche lorsque la valeur du champ Type **d'accord** dans le profil de l'entité OAuth est définie sur **Informations d'identification du client**. Pour savoir comment définir un profil d'entité OAuth pour un fournisseur OAuth tiers, reportez-vous à la section Se connecter à un fournisseur OAuth tiers. • Si vous activez la case à cocher **Se connecter au serveur d'authentification via Serveur MID** , vous devez identifier le serveur requis Serveur MID ou Serveurs MID à partir de la liste **S'applique à** .
Concerne	Spécifiez si l'enregistrement des informations d'identification s'applique à tous les serveurs MID ou à un serveur MID spécifique. Si spécifique, ajoutez les serveurs MID si nécessaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire des informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
	Important : Assurez-vous d'être conscient de ces considérations si vous avez coché la case **Se connecter au serveur d'authentification via le serveur MID** . • Assurez-vous que tous les éléments Serveurs MID sélectionnés dans S'applique à peuvent communiquer avec le serveur d'authentification. Cela est nécessaire pour exécuter la demande de jeton par rapport à **l'URL de jeton** mentionnée dans l'enregistrement du fournisseur OAuth (qui est lié au profil d'entité OAuth spécifié dans l'enregistrement des informations d'identification OAuth 2.0).  • Assurez-vous qu'il y en a au moins un Serveur MID (dans la sélection dans **S'applique**Serveurs MID à) avec ces configurations : ◦ La valeur du champ **État** est **En hausse**. ◦ La valeur du champ **Validé** est **Oui**. ◦ L'aptitude du Serveur MID est définie sur **REST** ou **ALL.** Pour en savoir plus sur la configuration du serveur MID, reportez-vous à la section https://www.webstg.servicenow.com/docs/access?context=configure-capabilities&version=xanadu&pubname=xanadu-integrate-applications&ft:locale=en-US  . Pour en savoir plus sur ces états, reportez-vous MID Server dashboard à .
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire des informations d'identification OAuth 2.0 (suite)

Champ	Valeur d'entrée
Alias d'informations d'identification	Spécifiez l'alias d'informations d'identification que vous souhaitez lier aux informations d'identification OAuth 2.0.
Type d'intégration	Indique le type d'intégration des informations d'identification. Invoquez une API d'un tiers avec une demande OAuth qui génère un jeton OAuth spécifique au système ou à l'utilisateur. Les types d'intégration sont les suivants : • **Système** : extrayez les informations de jeton en fonction du profil du demandeur. • **Personnel** : extrait les informations de jeton spécifiques à l'utilisateur. Utilisateur qui lance la session. Si cette **personne** est sélectionnée sur la page Profil du demandeur OAuth, un marqueur supplémentaire appelé **Personnel** s'affiche. **Remarque :** • Les informations relatives à un utilisateur ne sont accessibles qu'avec des jetons OAuth spécifiques à l'utilisateur dont le type d'intégration est **Personnel**. • Pour utiliser le jeton lié à l'utilisateur de la session, vous devez sélectionner **l'option Exécuter en tant que** déposée dans les propriétés du flux en tant **qu'utilisateur qui lance la session**.

Informations d'identification SAP

Le type d'informations d'identification SAP gère l'accès aux systèmes SAP JCo. Ce type d'informations d'identification est disponible pour Détection et Orchestration.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type SAP.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations d'identification n'est disponible que lorsque le module d'extension Stockage externe des informations d'identification est activé. **Remarque :** À l'heure actuelle, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **d'un MID Server spécifique** n'affecte pas la sélection d'un MID Server. Il est utilisé uniquement pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Des MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification SNMP

Découverte explore de nombreux types de périphériques (commutateurs, routeurs, imprimantes, etc.) à l'aide du protocole SNMP. Les informations d'identification pour SNMP n'incluent pas de nom d'utilisateur, seulement un mot de passe, appelé *chaîne de communauté*.

La chaîne de communauté en lecture seule par défaut pour de nombreux équipements SNMP est publique et Découverte l'essaiera automatiquement. Entrez les informations d'identification SNMP appropriées s'ils sont différents de la chaîne de communauté *publique* .

La détection de SNMP utilise toutes les chaînes de communauté configurées. Ce comportement ne s'applique pas à la détection de SNMPv3.

La requête SNMP de l'activité Orchestration par défaut renvoie l'identificateur d'objet (OID) d'un appareil et nécessite des informations d'identification SNMP.

Informations d'identification de la communauté SNMP

Le type d'informations d'identification Communauté SNMP gère l'accès à la détection de nombreux types de périphériques (commutateurs, routeurs, imprimantes, etc.) à l'aide du protocole SNMP. Ce type d'informations d'identification est disponible pour Découverte, Mappage des services, et Orchestration.

Les informations d'identification pour SNMP n'incluent pas de nom d'utilisateur, juste un mot de passe (la chaîne de communauté). La chaîne de communauté en lecture seule par défaut pour de nombreux équipements SNMP est publique, et le système l'essaie automatiquement. Entrez les informations d'identification SNMP appropriées s'ils sont différents de la chaîne de communauté publique.

Ces champs sont disponibles dans le formulaire Informations d'identification de la communauté SNMP.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations d'identification n'est disponible que lorsque le module d'extension Stockage externe des informations d'identification est activé. **Remarque :** À l'heure actuelle, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **d'un MID Server spécifique** n'affecte pas la sélection d'un MID Server. Il est utilisé uniquement pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Des MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Informations d'identification SNMPv3

Les informations d'identification SNMPv3 acceptent un protocole de confidentialité et une clé de confidentialité supplémentaire et sont disponibles pour Discovery et Orchestration. Pour le stockage externe dans CyberArk, vous pouvez sélectionner une clé de compte de confidentialité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ces champs sont disponibles dans le formulaire Informations d'identification pour SNMPv3.

Champs d'informations d'identification SNMPv3

Champ	Valeur d'entrée
Nom	Nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez l'appeler **SNMP Community Atlanta**.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
S'applique à	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les MID Servers qui doivent utiliser ces informations d'identifications dans le champ **MID servers**.
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Nom d'utilisateur	Entrez le nom d'utilisateur SNMP. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur.
Protocole d'authentification	Sélectionnez le type d'authentification à utiliser pour ces informations d'identification. Les choix possibles sont les suivants : • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512
Clé d'authentification	Entrez la clé d'authentification à utiliser pour ces informations d'identification.
Protocole de confidentialité	Sélectionnez le protocole de chiffrement pour ces informations d'identification. Les choix possibles sont les suivants : • 3DES • AES128

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'informations d'identification SNMPv3 (suite)

Champ	Valeur d'entrée
	• AES192 • AES256 • DES
Clé de confidentialité	Entrez la clé associée au protocole de confidentialité sélectionné.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un fournisseur d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
ID d'informations d'identification de confidentialité	Entrez la clé de compte de confidentialité configurée pour les informations d'identification SNMPv3 dans CyberArk. Si vous utilisez un protocole de confidentialité dans CyberArk, ce champ doit avoir la même valeur que le champ **Nom** du compte de confidentialité SNMPv3 CyberArk. Ce champ n'est visible que pour SNMPv3 lorsque vous sélectionnez **CyberArk** dans le champ **Type de banque d'identifiants**. Si vous n'utilisez pas de clé de confidentialité pour CyberArk, laissez ce champ vide.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque le stockage externe est activé, le champ **ID d'informations d'identification** s'affiche. Le stockage des informations d'identification externe n'est disponible que lorsque le module d'extension Stockage des informations d'identification externe est activé et que la vue **Stockage externe** est sélectionnée.
Type de banque d'identifiants	Sélectionnez le fournisseur de stockage externe. Sélectionnez **CyberArk** uniquement si vous utilisez une clé de confidentialité SNMPv3 CyberArk. Le champ **ID d'informations d'identification de confidentialité** apparaît pour autoriser l'entrée de la clé.
Contexte d'utilisation	Cochez cette case pour ajouter une valeur de contexte pour ces informations d'identification. Ce champ est visible dans la vue **Discovery**. Les contextes ne sont pas actuellement pris en charge pour le stockage des informations d'identification externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs d'informations d'identification SNMPv3 (suite)

Champ	Valeur d'entrée
	Remarque : Un contexte est une collection d'informations de gestion accessibles par des informations d'identification SNMPv3 qui fait référence à un OID spécifique. Les contextes sont parfois référencés pour collecter des informations sur l'appareil qui ne peuvent pas être consultées par les informations d'identification normales. Un contexte peut être fourni par le fabricant ou être configuré séparément. Pour plus d'informations, voir Nom de contexte et ID de contexte. Si vous avez plusieurs informations d'identification SNMPv3 avec le même nom d'utilisateur et les mêmes clés d'utilisateur, mais que certains de vos appareils ont besoin d'un contexte et d'autres pas, vous devrez créer des enregistrements distincts pour chaque appareil.
Nom de contexte	Entrez la valeur du nom de contexte pour ces informations d'identification. Cette valeur ne doit être utilisée que si vous avez des appareils qui la nécessitent pour un accès complet. Ce champ n'est visible que lorsque la case **Contexte d'utilisation** est cochée.

Informations d'identification SSH

Découverte, Orchestration et Hub d'intégration explorer UNIX et Linux périphériques en utilisant les informations d'identification SSH pour exécuter des commandes sur Secure Shell (SSH). Les commandes SSH doivent s'exécuter avec les privilèges racines, soit avec les informations d'identification racine, soit via Sudo. Les informations d'identification de clé privée SSH fournissent une sécurité supplémentaire.

Octroi des privilèges racines

Avant d'octroyer des privilèges racines, examinez votre politique et vos options de sécurité avec l'équipe de sécurité de votre organisation.

Utilisez l'une ou l'autre de ces approches pour permettre aux utilisateurs d'exécuter des commandes SSH avec des privilèges racines :

- Donnez d'autres informations d'identification pour Découverte, Orchestration ou Hub d'intégration, mais octroyez à l'utilisateur ayant ces informations d'identification le droit d'exécuter certaines commandes avec des privilèges racine, à l'aide de Sudo. Il s'agit d'un moyen sécurisé d'octroyer des privilèges limités. Découverte, Orchestration ou Hub d'intégration utilisent Sudo sur n'importe quelle sonde dont le paramètre `must_sudo` est défini sur **true** (sa valeur par défaut est **false**). Toutefois, chaque système doit être configuré pour permettre à Sudo de fonctionner. Pour ce faire, modifiez le fichier **/etc/sudoers** à l'aide de la commande **visudo**.
- Donnez les informations d'identification **racine**. Il s'agit bien entendu des informations d'identification les plus puissantes, mais elles ne sont pas toujours souhaitables pour des raisons de sécurité. Si Découverte, Orchestration ou Hub d'intégration ont les informations d'identification racine pour n'importe quel système UNIX ou Linux, aucune autre configuration n'est nécessaire.

Commandes privilégiées

La plateforme fournit des commandes privilégiées par défaut que le MID Server doit utiliser et la possibilité d'ajouter des commandes supplémentaires au système. Pour plus

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d'informations sur l'utilisation de sudo et d'autres commandes privilégiées, consultez Commandes privilégiées du serveur MID .

Type d'informations d'identification de clé privée SSH

Remarque :
Les informations d'identification de clé privée SSH doivent être utilisées dans la plupart des cas, car elles offrent une meilleure sécurité que les informations d'identification de mot de passe SSH.

Champ	Valeur d'entrée
Nom	Nom unique et descriptif pour ces informations d'identification. Par exemple, vous pouvez les appeler **SSH Atlanta**.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez un nom d'utilisateur UNIX ou Linux. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur.
Mot de passe	Entrez le mot de passe UNIX ou Linux. Pour les informations d'identification de type **Clé privée SSH** , entrez le mot de passe Sudo si le nom d'utilisateur en nécessite un.
Phrase de sécurité SSH	Saisissez une phrase de sécurité SSH. Ce champ est disponible uniquement pour les informations d'identification de **Clé privée SSH** .

Clé privée SSH	Saisissez une clé sécurisée, RSA, DSA, ECDSA ou ED25519 privée.
	
	La clé privée doit être saisie au bon format pour être correctement chiffrée. La clé privée doit commencer par la chaîne -----BEGIN.
	
	Voici un exemple de clé privée RSA correctement formatée :
	`-----BEGIN RSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END RSA PRIVATE KEY-----`
	
	Voici un exemple de clé DSA :
	`-----BEGIN DSA PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END DSA PRIVATE KEY-----`
	
	Un exemple de clé ECDSA :
	`-----BEGIN EC PRIVATE KEY-----`
	`MIIEogIBAAKCAQEAsEK65scPssPSobpDFMpR+Btv3MS4Q7NP8ERaStRZsh3`
	`IWz+x...`
	`...7hrxV2dbSug60FahyupGWBGtPnXm5PaE2X5WPLuUj94ue48i1Fs`
	`-----END EC PRIVATE KEY-----`
	
	Et un exemple de clé privée ED25519 :
	`-----BEGIN OPENSSH PRIVATE KEY-----`
	`b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMw`
	`AAAAtzc2gtZW`

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur d'entrée
	QyNTUxOQAAACAIYIqhcdwx8VQzZ5XaIC5ltQpjRr3IIIq/aE66mufmiwAAAKDQUtxZ0FLc WQAAAAtzc2gtZWQyNTUxOQAAACAIYIqhcdwx8VQzZ5XaIC5ltQpjRr3IIIq/aE66mufmiw AAAECuvsTkFUPdpTh0kw23i8TYx19qsFOZ3TRgowkkHBh6wSViWqFx3DHxVDNnIdogLmW1 CmNGveUiWr9oTrqa5+aLAAAAGmFiaGluYXYuc3V0YXJATVJFTUE3OTAzMkI3AQID -----END OPENSSH PRIVATE KEY----- **Remarque :** Pour une clé privée ED25519, seul le format de clé OpenSSH, qui est généré à l'aide de l'utilitaire SSH-keygen OpenSSH est pris en charge. Le Now Platform prend en charge les clés privées au format PEM généré par l'utilitaire OpenSSH ssh-keygen. Pour convertir les clés PPK qui ont été générées par PuTTY : • Ouvrez votre clé privée dans PuTTYGen. • Exportez-le au format OpenSSH à partir du menu **Conversions** > **Exporter la clé OpenSSH**. • Enregistrez la nouvelle clé OpenSSH.
Certificat SSH	Saisissez un certificat OpenSSH basé sur RSA ou ED25519. Lors de la saisie du certificat, une clé privée est utilisée pour l'authentification basée sur certificat. Cette authentification est prise en charge à partir d'OpenSSH 7.8.
Alias d'informations d'identification	• Autorisez les concepteurs de flux à utiliser des alias pour gérer les connexions et les informations d'identification. L'utilisation d'un alias élimine la nécessité de configurer plusieurs informations d'identification et profils d'informations de connexion lors de l'utilisation d'environnements multiples. Si les informations de connexion ou d'identification changent, vous n'avez pas besoin de mettre à jour les actions qui utilisent la connexion. Pour plus d'informations, consultez Connexions et informations d'identification. • Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Actuellement, le seul système de stockage externe pris en charge est CyberArk.
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Valeur d'entrée
S'applique à	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les MID Servers qui doivent utiliser ces informations d'identifications dans le champ **MID servers**.
Ordre	Ordre (séquence) dans lequel la plateforme essaie ces informations d'identification lorsqu'elle tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des numéros élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), Discovery ou Orchestration essaie les informations d'identification aléatoirement.

Type d'informations d'identification SSH

Ces champs sont disponibles dans le formulaire Informations d'identification SSH.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	• Autorisez les concepteurs de flux à utiliser des alias pour gérer les connexions et les informations d'identification. L'utilisation d'un alias élimine la nécessité de configurer plusieurs informations d'identification et profils d'informations de connexion lors de l'utilisation d'environnements multiples. Si les informations de connexion ou d'identification changent, vous n'avez pas besoin de mettre à jour les actions qui utilisent la connexion. Pour plus d'informations, consultez Connexions et informations d'identification. • Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations d'identification n'est disponible que lorsque le module d'extension Stockage externe des informations d'identification est activé. **Remarque :** À l'heure actuelle, le seul système de stockage externe pris en charge est CyberArk.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Commandes qui nécessitent des privilèges racine pour Discovery, Orchestration et Hub d'intégration

Dans ces exemples, le nom d'utilisateur est **Disco**. Remplacez le nom d'utilisateur et assurez-vous que les chemins d'accès des commandes correspondent aux chemins d'accès du système.

Remarque :
Les commandes Sudo ne fonctionnent pas avec les informations d'identification de clé privée, car il n'y a pas de mot de passe à fournir à la commande Sudo. Une solution consiste à ajouter l'option *NOPASSWD* à la configuration Sudo. Par exemple, vous pouvez entrer : `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

Commandes UNIX et Linux nécessitant des privilèges racine

Commande	Objectif
HP-UX	
adb	Collecte la vitesse et la mémoire du processeur. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/adb • **Utilisée par** : Discovery

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif
Toutes les versions Linux et UNIX	
chage	Modifie le nombre de jours entre les changements de mot de passe et la date du dernier changement de mot de passe. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/chage • **Utilisée par** : Orchestration et Hub d'intégration
chpasswd	Modifie les mots de passe utilisateur. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/chpasswd • **Utilisée par** : Orchestration et Hub d'intégration
Toutes les versions Linux	
dmidecode	Collecte différentes informations sur le matériel, y compris le numéro de série incorporé dans la carte mère. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/dmidecode • **Utilisée par** : Discovery
fdisk	Collecte les informations sur les disques et la taille sur le système. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/fdisk -l • **Utilisée par** : Discovery
multipath	Collecte les mappages d'appareils pour le MPIO. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/multipath -ll • **Utilisée par** : Discovery
Linux et Solaris	
dmsetup	Examine un volume de faible niveau. • **Exemple de ligne de /etc/sudoers** : ◦ Disco ALL=(root) /usr/bin/dmsetup table * ◦ Disco ALL=(root) /usr/bin/dmsetup ls • **Utilisée par** : Discovery
Toutes les versions UNIX	
lsof	Détermine la relation entre les processus et les connexions en cours au système.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif
	• **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /sbin/lsof • **Utilisée par** : Discovery
oratab	Accorde un accès en lecture au fichier oratab pour localiser la page d'accueil et le profil Oracle. • **Exemple de ligne /etc/sudoers** : N. A. • **Utilisée par** : Discovery
Solaris	
iscsiadm	Obtient des IQN iSCSI • **Exemple de ligne /etc/sudoers** : ${sudo:iscsiadm list target -S} • **Utilisée par** : Discovery
fcinfo	Obtient des WWPN pour les ports. • **Exemple de ligne /etc/sudoers** : ${sudo:fcinfo remote-port -sl -p $port} • **Utilisée par** : Discovery
prtvtoc	Communique des informations sur les partitions de disque. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/prtvtoc • **Utilisée par** : Discovery
pfiles	Utilisé pour collecter des informations sur les connexions TCP. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/pfiles • **Utilisée par** : Discovery
PGREP (en anglais seulement)	Utilisé pour répertorier les ID de processus d'une région particulière sur laquelle exécuter les fichiers p. • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/pgrep • **Utilisée par** : Discovery
/usr/bin/ps	Répertorie le processus d'exécution. Vous pouvez ajouter le rôle proc_owner au lieu de l'exécuter avec l'accès racine.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Commandes UNIX et Linux nécessitant des privilèges racine (suite)

Commande	Objectif
	• **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/bin/ps • **Utilisée par** : Discovery
/usr/ucb/ps	Répertorie le processus d'exécution. Vous pouvez ajouter le rôle proc_owner au lieu de l'exécuter avec l'accès racine. L'utilisation de la commande `/usr/ucb/ps` est déconseillée à partir de Solaris 11. Étant donné que Découverte, Orchestration et Hub d'intégration nécessitent l'utilisation de cette commande pour toutes les versions Solaris, vous devez installer l'utilitaire ucb manuellement sur les systèmes Solaris 11. Pour obtenir des instructions, consultez KB0564262 . • **Exemple de ligne /etc/sudoers** : Disco ALL=(root) /usr/ucb/ps • **Utilisée par** : Discovery

Pour obtenir la liste des commandes privilégiées dont vous avez besoin pour Découverte et Mappage des services, consultez Service Mapping commands requiring a privileged user la liste des commandes qui nécessitent des droits élevés pour détecter et mapper les hôtes Unix de votre organisation.

Besoins relatifs à l'accès pour les informations d'identification non racine

Si vous ne fournissez pas d'informations d'identification Découverte avec accès racine, vous devez fournir les informations d'identification avec les besoins relatifs à l'accès suivantes.

Application	Fichier ou répertoire	Accès requis
Apache	httpd.conf	Lecture
HBase	hbase-site.xml	Lecture
JBoss	jboss-service.xml	Lecture
	Répertoire de base JBoss	Lecture
	web.xml	Lecture
MySQL	my.cnf	Lecture
NGINX	nginx.conf	Lecture
Oracle	oratab	Lecture
	Fichiers pfiles (s) associés	Lecture
Oracle Listener	lsnrctl	Exécuter
	listener.ora	Lecture
Tomcat	catalina.jar	Lecture
	server.xml	Lecture
	web.xml	Lecture

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Application	Fichier ou répertoire	Accès requis
Unix	/etc/*release	Lecture
	/etc/bashrc	Lecture
	/etc/profile	Lecture
	/proc/cpuinfo	Lecture
	/proc/vmware/sched/ncpus	Lecture
	/var/log/dmesg	Lecture
	Répertoire APD	Lecture
WebSphere	cell.xml	Lecture
	server.xml	Lecture
	serverindex.xml	Lecture

Informations d'identification VMware

Le type d’informations d’identification VMware gère l’accès aux informations d’identification vCenter.

Les applications qui accèdent aux ressources dans le cloud VMware ont besoin d'accéder aux informations d'identification VMware. Par exemple, le type d’informations d’identification VMware permet à Détection d’explorer vCenter de VMware en cours d’exécution sur un ordinateur Windows pour détecter les ordinateurs ESX, les ordinateurs virtuels et les pools de ressources. L’API VMware Découverte et Automation (API vCenter) fournit désormais le numéro de série unique au niveau mondial pour les CI d’ordinateur. Les informations d’identification CIM ne sont pas nécessaires pour activer l’accès à chaque hôte VMware.

Remarque :
Les informations d’identification Windows ne sont pas nécessaires pour vCenter Découverte, lorsque des informations d’identification VMWare valides sont utilisées.

Important :
N’utilisez pas les informations d’identification de type **VMware** pour les activités d’Orchestration qui exécutent le travail sur les ordinateurs virtuels individuels clonés par vCenter (par exemple, le redémarrage d’un ordinateur virtuel Linux). Pour ces activités, le **type** d’informations d’identification dépend du système d’exploitation de l’ordinateur virtuel (**SSH** ou **Windows**).

Formulaire Informations d'identification VMware

Champ	Description
Nom	Entrez un nom unique et descriptif pour les informations d'identification VMware.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
Nom d'utilisateur	Saisissez le nom d’utilisateur que vous utilisez pour votre compte VMware. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Les informations d'identification VMware doivent avoir un rôle en lecture seule dans vCenter.
Mot de passe	Entrez le mot de passe du compte VMware.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Informations d'identification VMware (suite)

Champ	Description
Concerne	Sélectionnez un ou plusieurs Serveurs MID fichiers dans la liste des fichiers .Serveurs MID Les informations d'identification Serveurs MID configurées dans cet enregistrement sont disponibles dans cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.

Informations d'identification Windows

Les informations d'identification Windows permettent d'accéder aux ordinateurs Windows. Ce type d'informations d'identification est disponible pour Détection et Orchestration.

Exigences en matière d'informations d'identification

Découverte et Orchestration ont les exigences suivantes en matière Windows d'informations d'identification :

- Installer un serveur MID sur un Windows hôte en tant que service.
- Ajoutez Windows des informations d'identification à l'un de ces emplacements :
  - Une entrée dans la table Informations d'identification [windows_credentials]
  - Un compte de service Serveur MID à exécuter en tant qu'utilisateur ou compte de domaine Windows spécifique.

Accorder les autorisations appropriées

Pour fournir des autorisations suffisantes, Windows les informations d'identification doivent être l'une des suivantes :

- un utilisateur de domaine avec un accès administrateur local sur les hôtes Windows cibles ;
- Un compte local dont les privilèges d'administrateur et le contrôle d'accès utilisateur (UAC) sont désactivés sur le même hôte cible.
- Un utilisateur qui répond aux exigences en matière de Windows sondes et d'autorisations (Découverte uniquement).
- Un utilisateur qui répond aux exigences de l'activité Orchestration à exécuter (Orchestration uniquement).

Remarque :
Aucun privilège d'ouverture de session n'est nécessaire. Le compte n'a PAS besoin d'être interactif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La sécurité autour de l'octroi d'un accès privilégié peut être améliorée en utilisant des profils JEA pour exécuter Découverte. Pour plus d'informations, consultez Microsoft Just Enough Administration (JEA) pour Discovery .

Ordinateurs de groupe de travail

Pour exécuter des commandes Powershell afin de détecter un ordinateur de groupe de travail, configurez les informations d'identification du serveur MID pour l'un de ces utilisateurs :

- Compte administrateur intégré sur l'ordinateur du groupe de travail.
- Utilisateur du domaine sur l'ordinateur du groupe de travail.

Configuration multi-domaines

Pour activer le fonctionnement des informations d'identification Windows dans plusieurs domaines, assurez-vous d'utiliser les formats de nom et la configuration de Serveur MID corrects.

Découverte et Orchestration prennent en charge Windows les informations d'identification de domaine dans les formats **Nom principal de l'utilisateur** et **Nom d'utilisateur de connexion de niveau inférieur** . Par exemple, **Domaine\UserName** ou **UserName@example.domain.com**. Vous pouvez fournir les Windows informations d'identification du groupe de travail au format suivant : GROUPE DE TRAVAIL\UserName.

Remarque :
Vous pouvez également fournir un compte local à l'aide du nom d'utilisateur . \.

Ces actions supplémentaires sont nécessaires pour permettre aux informations d'identification de fonctionner dans plusieurs Windows domaines.

Condition	Actions supplémentaires requises
Hôte de Serveur MID sur le même domaine que la Windows cible.	Aucun
Hôte de Serveur MID sur un domaine différent de la Windows cible.	Assurez-vous que PowerShell 3.0 (ou version ultérieure jusqu'à 5.1) est installé sur l'hôte du Serveur MID.
Hôte de Serveur MID sur un domaine différent de la cible Microsoft SQL Server.	Reportez-vous à la section Découverte du serveur MSSQL .

Type d'informations d'identification Windows

Ces champs sont disponibles dans le formulaire Informations d'identification pour Windows :

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Nom d'utilisateur	Entrez le nom d'utilisateur ou créez-le dans la table Informations d'identification. Évitez les espaces blancs dans les noms d'utilisateur. Un avertissement apparaît si la plateforme détecte des espaces blancs dans le nom d'utilisateur. Pour CIM Discovery, l'utilisateur doit avoir le rôle administrateur.
Mot de passe	Entrez le mot de passe.
ID d'informations d'identification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Le champ **ID d'informations d'identification** a une limite de 40 caractères. Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Alias d'identification	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration. Pour utiliser les informations d'identification afin de détecter les CI qui n'appartiennent pas à ce type de CI à l'aide des modèles de mappage de service et de détection, entrez le nom de table du type de CI auquel le CI appartient, par exemple cmdb_ci_apache_web_server.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations d'identification n'est disponible que lorsque le module d'extension Stockage externe des informations d'identification est activé. **Remarque :** À l'heure actuelle, le seul système de stockage externe pris en charge est CyberArk .
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez qui Serveurs MID doit utiliser ces informations d'identification dans le champ **MID Servers** .
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**. **Remarque :** La sélection **d'un MID Server spécifique** n'affecte pas la sélection d'un MID Server. Il est utilisé uniquement pour décider quels serveurs MID doivent avoir une visibilité sur les informations d'identification. **Des MID Servers spécifiques** ne sont pas pris en charge dans les activités Orchestration.
Ordre	Ordre (séquence) dans lequel Découverte teste ces informations d'identification lorsqu'il tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des nombres élevés ou lorsque

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), l'instance essaie les informations d'identification aléatoirement.
Compte de service Serveur MID Windows	Lorsqu'il est actif, les informations d'identification définies représentent le compte de services Serveur MID.

Configurer les informations d'identification Windows pour le Serveur MID

Configurez le serveur MID pour qu'il utilise soit les informations d'identification de son propre service Windows, soit les informations d'identification de la table Informations d'identification [discovery_credentials].

Avant de commencer

Rôle requis : administrateur

Procédure

1. Configurez le serveur MID pour utiliser les informations d'identification du compte de service du serveur MID.
   a. Définissez les informations d'identification du service Configurer Windows MID Server sur un utilisateur qui remplit les conditions d'autorisation.
   b. Vérifiez que le nom d'utilisateur répond aux exigences de format de nom.
   c. Renseignez les champs du formulaire comme il convient.
   d. Vérifiez que les informations d'identification répondent aux exigences du domaine.
2. Configurez le Serveur MID à l'aide des informations d'identification de la table Informations d'identification [discovery_credentials].
   a. Ajoutez des informations d'identification individuelles Windows à la table Informations d'identification [windows_credentials].
      - Vérifiez que chaque information d'identification répond aux exigences d'autorisation.
      - Vérifiez que chaque nom d'utilisateur répond aux exigences de format de nom.
      - Vérifiez que chaque information d'identification répond aux exigences du Windows domaine.
   b. **Facultatif :** Configurez le serveur MID pour utiliser Powershell en définissant le paramètre mid.use_powershell**sur vrai**.
   Reportez-vous à la section Configuration des MID Servers .
   c. Cochez la case Compte de service Windows MID Server pour créer des informations d'identification qui représentent le compte de service Windows MID Server à exécuter en tant qu'utilisateur ou compte de domaine Windows spécifique.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Informations d'identification du référentiel d'images de conteneur

Les informations d'identification du référentiel d'images du conteneur gèrent l'accès aux référentiels privés pour l'analyse des images du conteneur. Ce type d'informations d'identification est disponible pour Découverte.

Ces champs sont disponibles dans le formulaire Informations d'identification pour les informations d'identification de type référentiel d'images d'identification.

Formulaire Informations d'identification du référentiel d'images du conteneur

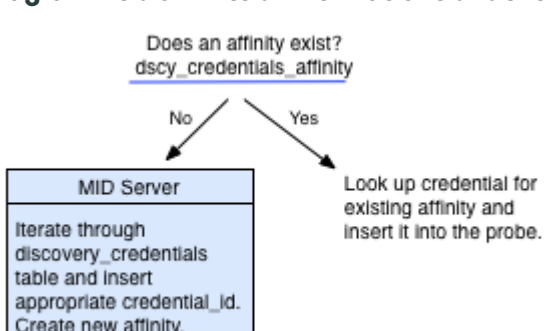
Champ	Description
Nom	Nom des informations d'identification affecté par l'utilisateur.
Nom d'utilisateur	Nom d'utilisateur avec des autorisations de lecture pour le référentiel.
Mot de passe	Mot de passe avec autorisations en lecture pour le référentiel.
Référentiel	Nom de domaine complet du référentiel. Par exemple : `docker.io/snow_images`.

Relation d'informations d'identification pour Détection et Orchestration

L'affinité d'informations d'identification est une association entre un ensemble d'informations d'identification et un appareil de votre réseau.

Lorsqu'une Découverte équipe d'Orchestration tente d'accéder à un périphérique pour la première fois, elle teste toutes les informations d'identification disponibles jusqu'à ce qu'elle trouve les informations d'identification correctes. Après avoir identifié les informations d'identification d'un appareil et Orchestration, Découverte créez une relation entre les informations d'identification et l'appareil à l'aide de la table Relation d'informations d'identification [`dscy_credentials_affinity`]. Toutes les détections ultérieures ou activités d'Orchestration tentent de faire correspondre les informations d'identification de cette table avec un appareil pour lequel il existe une affinité. Si les informations d'identification d'un périphérique changent, Découverte et Orchestration réessayez toutes les informations d'identification disponibles jusqu'à ce qu'elles créent une nouvelle relation.

Diagramme d'affinité d'informations d'identification



Remarque :
Si Orchestration et Découverte sont installés et que l'alias d'informations d'identification est activé, plusieurs affinités peuvent exister. Dans ce cas, la plateforme recherche les informations d'identification pour chaque relation et insère les informations d'identification de la relation avec l'ordre le plus bas dans la sonde.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage des informations d'identification

Examinez la section <credentials_debug> de la charge utile de la file d'attente ECC pour résoudre les problèmes liés aux informations d'identification.

Certaines sondes prennent en charge le débogage des informations d'identification. Le débogage d'informations d'identification insère une section de <credentials_debug> dans la charge utile que le Serveur MID renvoie à la file d'attente ECC de l'instance. Vous pouvez consulter la section <credentials_debug> pour afficher des informations détaillées sur la recherche d'informations d'identification.

La section <credentials_debug> apparaît dans la charge utile si :

- Les informations d'identification échouent pour la sonde WMIRunner, la sonde PowerShell, la sonde JMS ou SSHCommand.
- Vous définissez le *credentials_debug* paramètre sur **vrai** pour les sondes WMIRunner, PowerShell ou SSHCommand. Si vous définissez le paramètre sur true, la section <credentials_debug> s'affiche même si la recherche d'informations d'identification réussit.

La section <credentials_debug> affiche les éléments suivants :

- Informations sur la recherche d'informations d'identification, telles que les types d'informations d'identification, les balises et les relations.
- Adresse IP ciblée.
- Informations sur chaque identifiant (dans l'ordre) utilisé par le Serveur MID, notamment le type, la classification, la balise, le nom, l'ID système et l'ID d'informations d'identification externe le cas échéant.

Exemple de charge utile affichant des informations d'identification non valides

Payload XML


```
<?xml version="1.0" encoding="UTF-8"?><results probe_time="6891" result_code="0"><result
id="6f10ed420a0a0b7e49052d83a32b586f" name="sh ${file:esx.sh}" order="1" topic="SSHCommand"><results
error="SSHCommand: Adding target to blacklist.  No valid credential found for types [SSH Password,SSH
Private Key]" probe_time="6860" result_code="42"><result error="SSHCommand: Adding target to blacklist.
No valid credential found for types [SSH Password,SSH Private Key]"><debug_info>{"debug_info":
[{"10.11.129.81":{"credentials_attempted":[{"credential_type":"SSH
Password","credential_name":"badCredential1","credential_order":"100","credential_success":false,"credenti
al_id":"6b43751d1362a200efffb6004244b0c3"},{"credential_type":"SSH
Password","credential_name":"badCredential2","credential_order":"200","credential_success":false,"credenti
al_id":"1553b11d1362a200efffb6004244b01b"},{"credential_type":"SSH
Password","credential_name":"badCredential3","credential_order":"300","credential_success":false,"credenti
al_id":"7d63f11d1362a200efffb6004244b0b0"}],"adding_key_to_target_blacklist":true,"connection_parameters":
{"credential_types":["SSH Password","SSH Private Key"],"target":"10.11.129.81"}}}]}</debug_info></result>
<parameters><parameter name="discover" value="CIs"/><parameter name="agent"
value="mid.server.demonightlyIstanbul_MID"/><parameter name="glide.xmlhelper.trim.enable" value="true"/>
<parameter name="use_class" value="discovery_classy_unix"/><parameter name="source" value="10.11.129.81"/>
<parameter name="priority" value="0"/><parameter name="use_snc_ssh" value="true"/><parameter name="probe"
value="10e0eebd0a0a0b4f61f46a5027df7fb6"/><parameter name="port_probe"
value="97ff2abd0a0a070300b7f37daa11a241"/><parameter name="port" value="22"/><parameter name="cidata"
value="&lt;CIData&gt;&lt;data&gt;&lt;fld name=&quot;ip_address&quot;&gt;10.11.129.81&lt;/fld&gt;&lt;/data&
gt;&lt;/CIData&gt;"/><parameter name="used_by_discovery" value="true"/><parameter name="name" value="sh
${file:esx.sh}"/><parameter name="topic" value="SSHCommand"/><parameter name="esx.sh" value="#!/bin
/sh&#13;&#10;# This command is rarely installed, so a Bourne shell script is used to squelch the exit
status and sensor warning when not found.&#13;&#10;# tcsh doesn't squelch exist status codes within
backticked statements&#13;&#10;echo `vmware -v 2&gt;&amp;1`"/><parameter name="ecc_queue" value=""/>
</parameters></results></result><result id="e5e075a2a9fe1561018f2a9636d5ec39" name="uname -a" order="1"
topic="SSHCommand"><results error="SSHCommand: Target is blacklisted.  No valid credential found for
```


Les détails apparaissent pour le paramètre PowerShell :

- Si les informations d'identification du Serveur MID local ont été utilisées après l'échec de toutes les informations d'identification Windows.
- Si les informations d'identification ont été ignorées parce que vous essayez de détecter le même ordinateur que celui sur lequel se trouve le serveur MID.
- Si le paramètre mid.powershell.use_credentials est défini sur true.

Les détails apparaissent pour le SSHCommand :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Si la recherche d'informations d'identification a été ignorée, car l'adresse IP cible est exclue.
- Si l'adresse IP cible a été ajoutée à la liste d'exclusion.

Remarque :
Le serveur MID enregistre les adresses IP pour les recherches d'informations d'identification ayant échoué dans une liste d'exclusion de la mémoire cache. Cette liste d'exclusion spécifie les périphériques auxquels le MID Server doit cesser d'essayer d'accéder. Les adresses IP sont ajoutées à la liste d'exclusion après l'échec de chaque identifiant. Les adresses IP sont effacées du cache de la liste d'exclusion au bout de cinq minutes, si le MID Server est redémarré ou si les enregistrements d'informations d'identification de l'instance sont mis à jour.

Stockage externe des informations d'identification

Une instance peut stocker les informations d'identification utilisées par DécouverteOrchestration et Mappage des services dans un référentiel d'informations d'identification externe plutôt que directement dans un enregistrement d'informations d'identification ServiceNow .

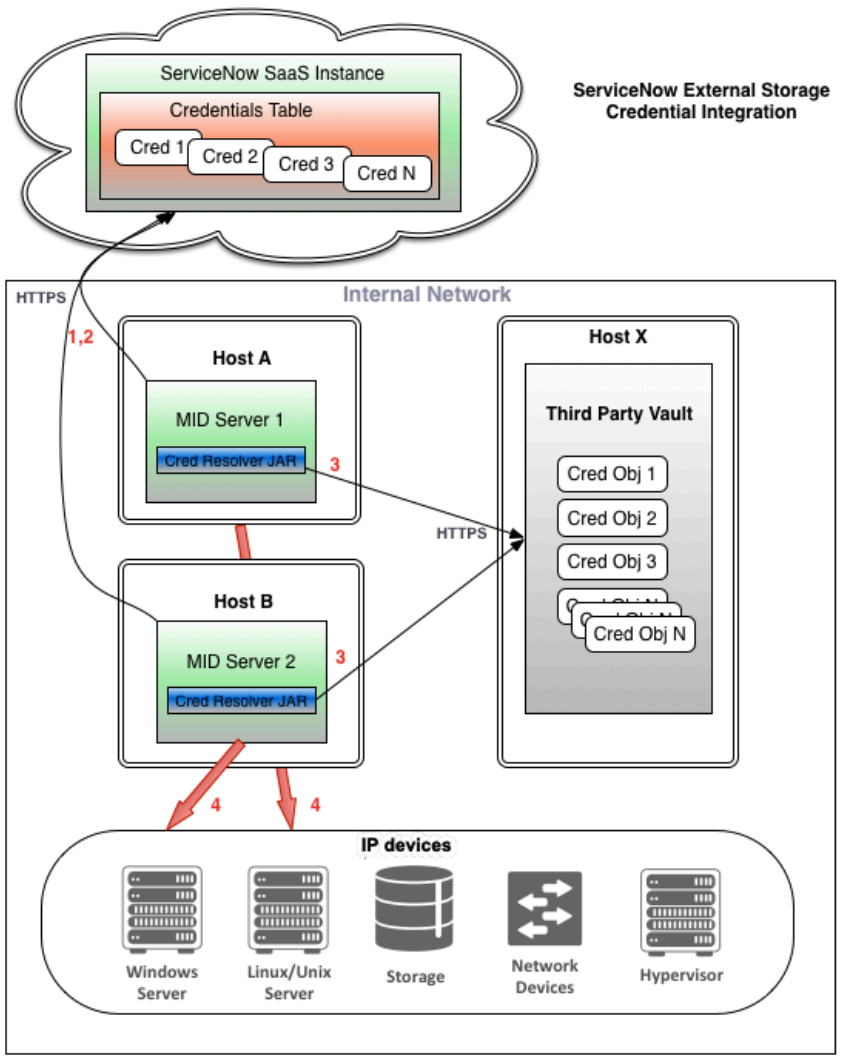
L'instance conserve un identificateur unique pour chaque information d'identification, le type d'information d'identification (par exemple, SSH, SNMP ou Windows) et toutes les relations d'informations d'identification. Le MID Server obtient l'identificateur d'informations d'identification à partir de l'instance, puis utilise un fichier JAR fourni par le client pour résoudre l'identificateur du référentiel en informations d'identification utilisables. Actuellement, la ServiceNow® plateforme prend en charge l'utilisation du coffre-fort CyberArk ou de BeyondTrust pour le stockage des informations d'identification externes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture de stockage des informations d'identification externe

Architecture de stockage des informations d'identification externe



Flux de processus des informations d'identification

Le MID Server récupère les informations d'identification d'un magasin externe à l'aide du processus suivant :

1. Serveur MID télécharge les objets d'informations d'identification à partir de la ServiceNow table Informations d'identification [discovery_credentials] qui contiennent l'ID d'informations d'identification correspondant à partir du coffre-fort cible.
2. Au fur et à mesure que chaque sonde ou modèle s'exécute à partir de Découverte ou Orchestration de tâches, le MID Server demande les informations d'identification en transmettant des informations telles que l'ID d'informations d'identification, l'adresse IP cible et le type d'informations d'identification au fichier JAR Java du programme de résolution des informations d'identification. Les détails sur l'objet d'informations d'identification à récupérer du coffre-fort sont déterminés par le programme de résolution des informations d'identification.

   De nombreux outils de résolution d'informations d'identification tels que CyberArk appellent une application fournie par le fournisseur de coffres-forts tiers fonctionnant sur le même ordinateur que le MID Server. Cette application peut souvent être configurée

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

pour mettre en cache les informations d'identification et sait mettre à jour le cache lorsqu'un identifiant change dans le coffre-fort, ce qui est très important pour éviter des appels réseau inutiles au coffre-fort chaque fois que le serveur MID demande des informations d'identification. Le résolveur des informations d'identification (à l'aide de l'application facultative du fournisseur, le cas échéant) appelle le coffre-fort pour obtenir le nom d'utilisateur, le mot de passe, etc. réels.

Pour les outils de résolution d'informations d'identification fournis prêts à l'emploi (uniquement CyberArk aujourd'hui), le MID Server ne met en cache les informations d'identification que pendant plusieurs secondes maximum en utilisant le chiffrement dans la mémoire de processus du MID Server. Cela signifie que le MID Server peut effectuer plusieurs demandes au programme de résolution des informations d'identification pour les mêmes informations d'identification, même lors de la détection d'un seul appareil. Contactez des fournisseurs tiers pour en savoir plus sur les implémentations de mise en cache pour d'autres outils de résolution d'informations d'identification.

3. Le Serveur MID exécute la sonde avec les informations d'identification appropriées.

Remarque :
L'affinité d'accréditation s'applique toujours. Le mécanisme reste le même, car la seule vraie différence du point de vue du MID Server est que les véritables détails d'identification (nom d'utilisateur et mot de passe) proviennent du coffre-fort tiers.

Journalisation de stockage des informations d'identification externe

Le MID Server publie des messages de journal sur le stockage des identifiants externes.

Si le référentiel rencontre une erreur lors d'une tentative de résolution d'une demande d'informations d'identification, le MID Server publie des messages de journal avec le préfixe Problem with client's CredentialResolver:

Composants installés avec Stockage externe des informations d'identification

Règle métier

La règle métier Stockage des informations d'identification externe effectue les tâches suivantes lorsqu'un administrateur modifie la propriété Activer le stockage des informations d'identification externe :

- Elle remplace la vue de la liste et du formulaire d'enregistrement Informations d'identification par la vue Stockage externe. Cette vue permet aux utilisateurs d'afficher la colonne **ID d'informations d'identification** dans la liste.
- Elle indique au MID Server d'actualiser son cache d'informations d'identification en vue de changer la façon dont les informations d'identification sont obtenues.

Propriété

Une propriété appelée Activer le stockage des informations d'identification externe [com.snc.use_external_credentials] active ou désactive le module d'extension Stockage des informations d'identification externe une fois qu'il est activé. La propriété est située à **Définition de découverte** > **Propriétés** et **Orchestration** > **Propriétés de Serveur MID**et est activé lorsque vous activez le module d'extension.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Si vous désactivez le stockage des informations d'identification externe avec la propriété système, le système définit automatiquement toutes les informations d'identification externe comme inactives dans l'instance. Si vous réactivez la fonctionnalité avec cette propriété, le système ne réinitialise pas les enregistrements d'informations d'identification externes en mode actif. Vous devez réactiver manuellement chaque enregistrement d'informations d'identification.

Demander un stockage d'informations d'identification externe pour Discovery et Orchestration

Le module d'extension External Credential Storage est disponible sur demande.

Avant de commencer

Rôle requis : admin

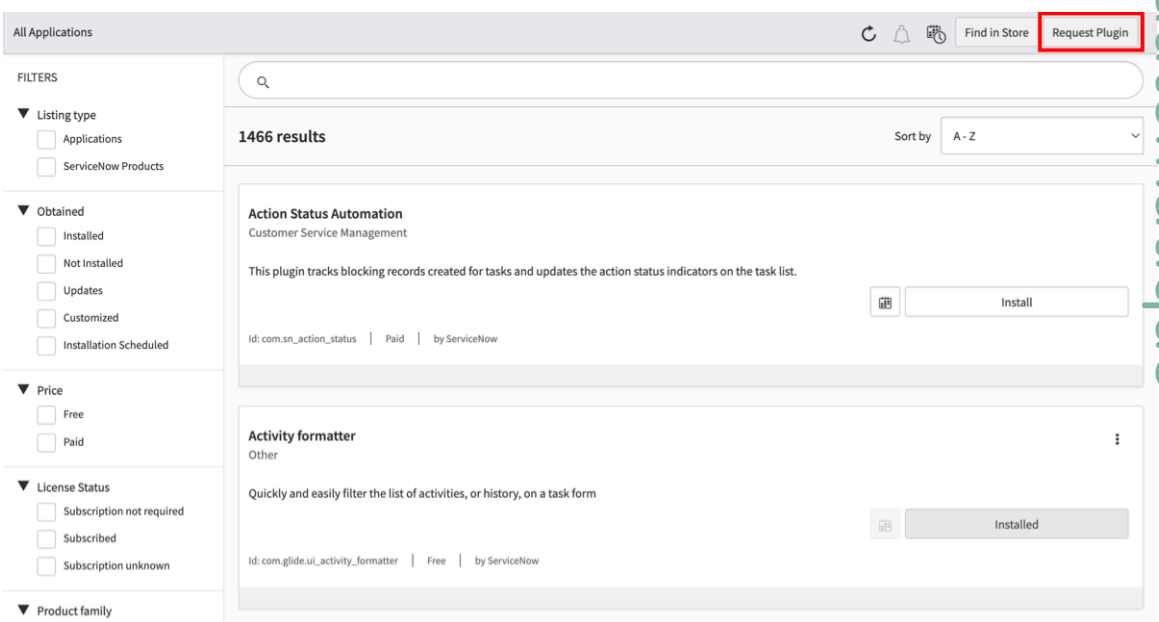
Pourquoi et quand exécuter cette tâche

Il existe deux façons de demander un module d'extension :

- Accéder directement au Catalogue de services de Now Support en sélectionnant **Tout** > **Catalogue de services** > **Activer le module d'extension** sur Now Support.
- Accéder au Catalogue de services de Now Support via la page Toutes les applications de votre instance en suivant ces étapes.

Procédure

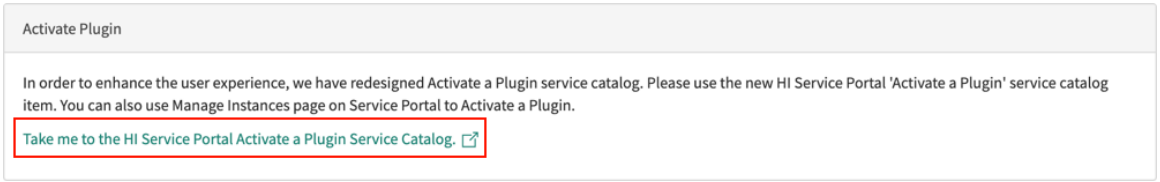
1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

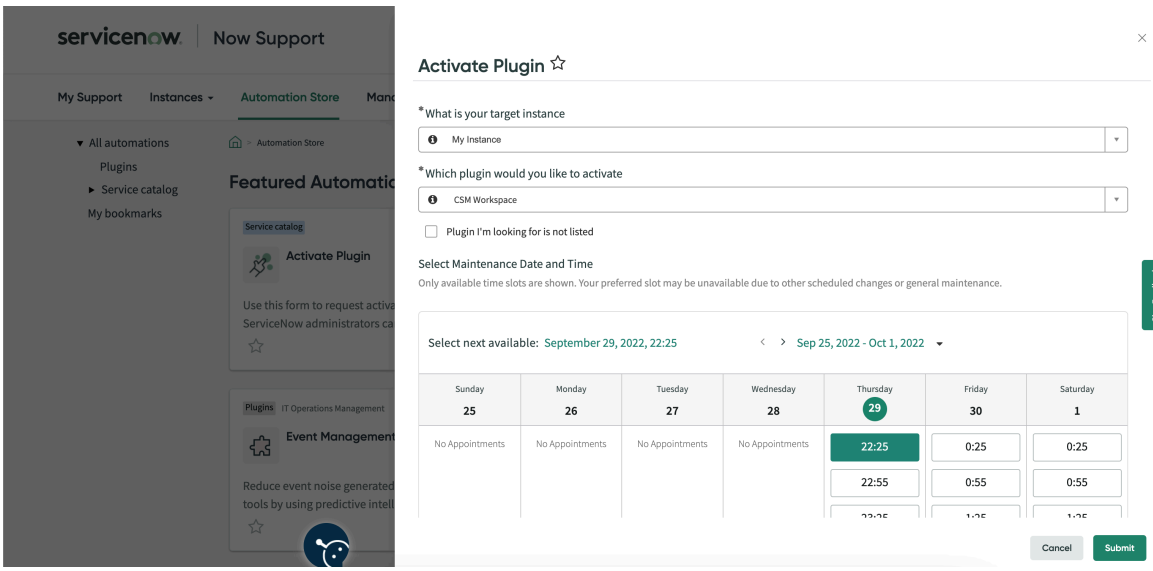
Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Activer le module d'extension



7. Sélectionnez **Envoyer**.
Pour plus de détails sur la demande d'un module d'extension, consultez l'article Requesting a Plugin from the Service Catalog [KB0751715] de la Now Support Base de connaissances.

Configuration de stockage des informations d'identification externe

Configurez votre instance pour obtenir des informations d'identification à partir d'un référentiel distant.

Ces procédures supposent que vous disposez déjà d'un référentiel externe configuré avec les informations d'identification que vous souhaitez protéger. L'identificateur d'informations d'identification configuré dans l'instance ServiceNow doit être mappé aux informations d'identification réelles dans le référentiel via le fichier JAR.

Remarque :
ServiceNow prend en charge deux coffres-forts externes à la fois : un résolveur d'informations d'identification CyberArk par défaut et un résolveur d'informations d'identification externes personnalisé. La création d'un résolveur d'informations d'identification CyberArk personnalisé utilise toujours le deuxième coffre-fort externe personnalisé, et aucun coffre-fort externe personnalisé supplémentaire ne peut être utilisé.

Pour configurer le stockage des informations d'identification externe, effectuez les tâches suivantes dans l'ordre.

Créer un fichier JAR pour résoudre les informations d'identification

Créez un fichier JAR pour résoudre les identificateurs d'informations d'identification envoyés par le serveur MID en informations d'identification réelles à partir du référentiel.

Avant de commencer
Rôle requis : agent_admin ou admin

Assurez-vous d'inclure tous les éléments d'informations d'identification attendus par l'instance, tels que la clé privée.

Pour créer un fichier JAR afin de résoudre les informations d'identification :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

Utilisez les modèles fournis sur Github ServiceNow ou l'exemple de fichier Java.

> **⚠ ATTENTION :**
> Ces exemples ne sont fournis qu'à titre de modèle. N'utilisez **PAS** ce code en production sans le modifier pour votre environnement.

a. Téléchargez les fichiers JAR open source avec les ServiceNow instructions du github :

- Outil de résolution d'informations d'identification externes HashiCorp
- Résolution d'informations d'identification externes CyberArk

b. Utilisez l'exemple de fichier Java suivant comme modèle et modifiez-le en fonction de votre environnement :

Example

```
package com.snc.discovery;

import java.util.*;
import java.io.*;

/**
 * Basic implementation of a CredentialResolver that uses a properties file.
 */

public class CredentialResolver {

 private static String ENV_VAR = "CREDENTIAL_RESOLVER_FILE";
 private static String DEFAULT_PROP_FILE_PATH = "C:\\dummycredentials.properties";

 // These are the permissible names of arguments passed INTO the resolve()
 // method.

 // the string identifier as configured on the ServiceNow instance...
 public static final String ARG_ID = "id";

 // a dotted-form string IPv4 address (like "10.22.231.12") of the target
 // system...
 public static final String ARG_IP = "ip";

 // the string type (ssh, snmp, etc.) of credential as configured on the
 // instance...
 public static final String ARG_TYPE = "type";

 // the string MID server making the request, as configured on the
 // instance...
 public static final String ARG_MID = "mid";

 // These are the permissible names of values returned FROM the resolve()
 // method.

 // the string user name for the credential, if needed...
 public static final String VAL_USER = "user";
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
// the string password for the credential, if needed...
public static final String VAL_PSWD = "pswd";

// the string pass phrase for the credential if needed:
public static final String VAL_PASSPHRASE = "passphrase";

// the string private key for the credential, if needed...
public static final String VAL_PKEY = "pkey";

// the string authentication protocol for the credential, if needed...
public static final String VAL_AUTHPROTO = "authprotocol";

// the string authentication key for the credential, if needed...
public static final String VAL_AUTHKEY = "authkey";

// the string privacy protocol for the credential, if needed...
public static final String VAL_PRIVPROTO = "privprotocol";

// the string privacy key for the credential, if needed...
public static final String VAL_PRIVKEY = "privkey";


private Properties fProps;

public CredentialResolver() {
}

private void loadProps() {
 if(fProps == null)
  fProps = new Properties();

 try {
  String propFilePath = System.getenv(ENV_VAR);
  if(propFilePath == null) {
   System.err.println("Environment var "+ENV_VAR+" not found. Using default file:
"+DEFAULT_PROP_FILE_PATH);
   propFilePath = DEFAULT_PROP_FILE_PATH;
  }

  File propFile = new File(propFilePath);
  if(!propFile.exists() || !propFile.canRead()) {
   System.err.println("Can't open "+propFile.getAbsolutePath());
  }
  else {
   InputStream propsIn = new FileInputStream(propFile);
   fProps.load(propsIn);
  }

 //fProps.load(CredentialResolver.class.getClassLoader().getResourceAsStream("dummycred
entials.properties"));
 } catch (IOException e) {
  System.err.println("Problem loading credentials file:");
  e.printStackTrace();
 }
}

 /**
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
 * Resolve a credential.
 */
public Map resolve(Map args) {
 loadProps();
 String id = (String) args.get(ARG_ID);
 String type = (String) args.get(ARG_TYPE);
 String keyPrefix = id+"."+type+".";

 if(id.equalsIgnoreCase("misbehave"))
  throw new RuntimeException("I've been a baaaaaaaaad CredentialResolver!");

 // the resolved credential is returned in a HashMap...
 Map result = new HashMap();
 result.put(VAL_USER, fProps.get(keyPrefix + VAL_USER));
 result.put(VAL_PSWD, fProps.get(keyPrefix + VAL_PSWD));
 result.put(VAL_PKEY, fProps.get(keyPrefix + VAL_PKEY));
 result.put(VAL_PASSPHRASE, fProps.get(keyPrefix + VAL_PASSPHRASE));
 result.put(VAL_AUTHPROTO, fProps.get(keyPrefix + VAL_AUTHPROTO));
 result.put(VAL_AUTHKEY, fProps.get(keyPrefix + VAL_AUTHKEY));
 result.put(VAL_PRIVPROTO, fProps.get(keyPrefix + VAL_PRIVPROTO));
 result.put(VAL_PRIVKEY, fProps.get(keyPrefix + VAL_PRIVKEY));

 System.err.println("Error while resolving credential id/type["+id+"/"+type+"]");

 return result;
}


/**
 * Return the API version supported by this class.
 */
public String getVersion() {
 return "1.0";
}

public static void main(String[] args) {
 CredentialResolver obj = new CredentialResolver();
 obj.loadProps();

 System.err.println("I spy the following credentials: ");
 for(Object key: obj.fProps.keySet()) {
  System.err.println(key+": "+obj.fProps.get(key));
 }

 }
}
```

Importer un fichier JAR pour résoudre les informations d'identification

Importez un fichier JAR créé pour résoudre les identificateurs d'informations d'identification envoyés par le serveur MID en informations d'identification réelles à partir du référentiel.

Avant de commencer
Rôle requis : agent_admin ou admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Une fois le fichier JAR créé, importez-le dans l'instance où il devient accessible au serveur MID.

Procédure

1. Après avoir créé le fichier JAR et les fichiers de propriétés, copiez le fichier de propriétés sur le serveur MID.
2. Accédez à la **Serveur MID** > **Fichiers JAR**.
3. Cliquez sur **Nouveau**.
4. Renseignez les champs suivants :

Champ	Description
Nom	Un nom unique et descriptif permettant d'identifier le fichier dans l'instance.
Version	Numéro de version du fichier, le cas échéant.
Source	Emplacement du fichier JAR à des fins de référence. Les informations sources ne sont pas utilisées par le système.
Description	Brève description du fichier JAR et de sa fonction dans l'instance.

5. Cliquez sur l'icône du trombone dans la bannière et joignez le fichier JAR à l'enregistrement.

Example

Joindre un fichier JAR

6. Cliquez sur **Envoyer**.
7. Redémarrez le service MID Server.
   La plate-forme met le fichier JAR à la disposition de n'importe quel MID Server configuré pour communiquer avec l'instance.

Configurer l'identificateur d'informations d'identification

Configurez l'identificateur d'informations d'identification dans l'instance.

Avant de commencer

Rôle requis : administrateur

Vérifiez les points suivants :

- Le module d'extension External Credential Storage doit être actif.
- La propriété Activer la découverte de stockage d'informations d'identification externe est activée.

Procédure

1. Accédez à la **Tout** > **Découverte** > **Informations d'identification** ou **Orchestration** > **Informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Sélectionnez un type d'informations d'identification.
4. Cochez la case **Banque d'identifiants externe** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Les champs **Nom d'utilisateur** et **Mot de passe** disparaissent, et le champ **ID d'informations d'identification** et le menu **Coffre-fort de stockage des informations d'identification** apparaissent.

5. Dans le menu **Chambre forte de stockage des informations d'identification** , sélectionnez Aucun, le coffre-fort CyberArk ou une chambre forte de stockage d'informations d'identification externe personnalisée.

> **Remarque :**
>
> Si CyberArk Vault est sélectionné, le menu **Clé de recherche** s'affiche avec quatre choix de clés de recherche : ID d'informations d'identification, Adresse IP, FQDN, Tous les éléments ci-dessus. La sélection de Toutes les options ci-dessus peut dégrader les performances, car elle nécessite d'accéder au coffre-fort plusieurs fois.

a. Pour utiliser un coffre de stockage d'informations d'identification externe personnalisé, accédez à Configurations du coffre-fort [vault_configuration.list] dans l'instance.

b. Créez un enregistrement à l'aide d'un nom associé à un fichier JAR importé pour un programme de résolution d'informations d'identification personnalisé.

Consultez les procédures Créer un fichier JAR pour résoudre les informations d'identification et Importer un fichier JAR pour résoudre les informations d'identification pour plus d'informations sur la création d'un coffre-fort de stockage des informations d'identification externe personnalisé.

6. Renseignez le formulaire Informations d'identification à l'aide des champs de la table suivante.

Champ	Description
Nom	Entrez un nom unique et descriptif pour ces informations d'identification.
Actif	Activez ou désactivez ces informations d'identification pour les utiliser.
ID de certification	Entrez la clé unique configurée pour les informations d'identification externes dans le fichier JAR téléchargé sur le MID Server pour un système d'informations d'identification externe. Il s'agit de l'ID passé à la classe Java dans la carte des paramètres : `public static final String ARG_ID = "id";` Le serveur MID utilise cet identificateur pour résoudre les informations d'identification réelles sur le référentiel. **Remarque :** Ce champ n'est visible que lorsque la case **Banque d'identifiants externes** est cochée.
Balises	Autorisez les créateurs de workflows à affecter des informations d'identification individuelles à n'importe quelle activité d'un workflow Orchestration ou affectez des informations d'identification différentes à chaque occurrence du même type d'activité dans un workflow Orchestration.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque vous sélectionnez cette option, les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification**. Le stockage externe des informations

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	d'identification n'est disponible que lorsque le module d'extension Stockage externe des informations d'identification est activé.
Chambre forte de stockage des informations d'identification	Choisissez le coffre-fort de stockage des informations d'identification externe dans la liste des coffres disponibles. Le menu est composé d'enregistrements provenant des configurations de coffre-fort [vault_configuration.list]. De nouveaux enregistrements peuvent être ajoutés et utiliser des noms associés à des fichiers JAR de résolution d'informations d'identification personnalisés. Consultez les procédures Créer un fichier JAR pour résoudre les informations d'identification et Importer un fichier JAR pour résoudre les informations d'identification pour plus d'informations sur la création d'un coffre-fort de stockage des informations d'identification externe personnalisé.
Concerne	Choisissez si appliquer ces informations d'identification à **Tous les serveurs MID** de votre réseau, ou à un ou plusieurs **MID servers spécifiques**. Spécifiez les MID Servers qui doivent utiliser ces informations d'identifications dans le champ **MID servers**.
MID Servers	Sélectionnez un ou plusieurs MID Servers dans la liste des MID Servers disponibles. Les informations d'identification configurées dans cet enregistrement sont disponibles pour les MID Servers de cette liste. Ce champ est disponible uniquement lorsque vous sélectionnez **MID servers spécifiques** depuis le champ **S'applique à**.
Ordre	Entrez l'ordre (la séquence) dans lequel la plateforme teste ces informations d'identification lorsqu'elle tente de se connecter aux appareils. Plus le nombre est petit, plus les informations d'identification apparaissent en haut dans la liste. Établissez un ordre pour les informations d'identification lorsque vous utilisez des informations d'identification avec des numéros élevés ou lorsque la sécurité verrouille les utilisateurs après trois tentatives de connexion échouées. Si toutes les informations d'identification ont le même numéro d'ordre (ou n'en ont pas), Discovery ou Orchestration essaie les informations d'identification aléatoirement.

7. Cliquez sur **Envoyer**.

Configurer l'identificateur d'informations d'identification pour AWS

Configurez votre instance pour obtenir des informations d'identification à partir d'un référentiel distant.

Avant de commencer

Rôle requis : cloud_admin

Vérifiez que ces modules d'extension sont actifs et que le Serveur MID a été installé :

- Discovery (com.snc.discovery)
- Cloud Provisioning and Governance [com.snc.cloud.mgmt]
- Stockage des informations d'identification externe [com.snc.discovery.external_credentials]

Pourquoi et quand exécuter cette tâche

Ces procédures supposent que vous disposez déjà d'un référentiel externe configuré avec les informations d'identification que vous souhaitez protéger. L'identificateur d'informations d'identification configuré dans l'instance ServiceNow doit être mappé aux informations d'identification réelles dans le référentiel via le fichier JAR.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Découverte** > **Informations d'identification**.
2. Sélectionnez un identifiant pris en charge par votre fournisseur de stockage des informations d’identification externe.
3. Remplissez le formulaire en utilisant les champs de la table.

Champ	Description
Nom	Nom unique et descriptif pour ces informations d’identification. Par exemple, Amazon Web Services.
Concerne	Sélectionnez les MID Server qui peuvent utiliser ces informations d’identification. Les choix sont **Tous les serveurs MID ouMID Servers spécifiques**. Si vous sélectionnez cette dernière option, le champ **Serveurs MID** s’affiche.
Actif	Case à cocher permettant d’activer ou de désactiver les informations d’identification.
Compte AWS	Saisissez votre ID de compte AWS si vos informations d’identification AWS se trouvent sur un fournisseur de stockage externe.
Serveurs MID	Sélectionnez un ou plusieurs MID Server qui peuvent utiliser ces informations d’identification.
ID de certification	Saisissez le nom sous lequel ces informations d’identification sont stockées dans le fournisseur de stockage des informations d’identification externe.
ID d'informations d'identification de confidentialité	Saisissez le nom d’une clé de confidentialité SNMPv3 de CyberArk. Ce champ n'est visible que pour SNMPv3 lorsque vous sélectionnez **CyberArk** dans le champ **Type de banque d'identifiants**. Si vous n'utilisez pas de clé de confidentialité pour CyberArk, laissez ce champ vide.
Alias d'informations d'identification	Sélectionnez un alias pour cet identifiant qui contient des comportements spécifiques. Consultez Alias d’informations d’identification pour Détection pour plus d'informations.
Banque d'identifiants externes	Cochez cette case pour utiliser un système de stockage des informations d'identification externe. Lorsque le stockage externe est activé, le champ **ID d'informations d'identification** s'affiche. Si cette case à cocher n’est pas visible, cliquez sur l’icône de menu dans la barre d’en-tête et sélectionnez **Vue** > **Stockage externe** dans le menu contextuel.
Type de banque d'identifiants	Sélectionnez **CyberArk** uniquement si vous utilisez une clé de confidentialité SNMPv3 CyberArk. Le champ **ID d'informations d'identification de confidentialité** apparaît pour autoriser l'entrée de la clé.

4. Cliquez sur **Envoyer**.

CyberArk Intégration de stockage des informations d’identification

L’intégration Serveur MIDCyberArk au coffre-fort permet ServiceNow® Orchestrationà , ServiceNow® Découverteet ServiceNow® Mappage des services de s’exécuter sans stocker d’informations d’identification sur l’instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Introduction à CyberArk

CyberArk Le produit Application Identity Management (AIM) utilise la solution de sécurité des comptes privilégiés pour éliminer la nécessité de stocker les mots de passe d'application intégrés dans les applications, les scripts ou les fichiers de configuration, et permet de stocker, de journaliser et de gérer ces mots de passe hautement sensibles de manière centralisée dans le CyberArk coffre-fort. Cette approche permet aux organisations de se conformer aux exigences internes et réglementaires en matière de remplacement périodique des mots de passe et de surveiller les activités associées à tous les types d'identités privilégiées, que ce soit sur site ou dans le cloud.

L'instance conserve un identificateur unique pour chaque identifiant, le type d'identifiant (par exemple, SSH, SNMP ou Windows) et toutes les relations d'informations d'identification. Le Serveur MID obtient l'identificateur d'informations d'identification, le type d'informations d'identification et l'adresse IP à partir de l'instance, puis utilise le CyberArk coffre-fort pour résoudre ces éléments en informations d'identification utilisables. Le résolveur d'informations d'identification peut également rechercher le nom d'hôte, le nom de domaine complet et utiliser la recherche DNS inversée pour obtenir le nom de domaine complet.

L'intégration CyberArk nécessite le ServiceNow® module d'extension External Credential Storage, qui est disponible dans **Définitions système** > **Modules d'extension**. CyberArk Le Serveur MID client AIM/API doivent être installés sur le même ordinateur. Les fournisseurs d'informations d'identification CyberArk Application Access Manager (AAM) version 12.0.1 et ultérieure sont pris en charge.

Installé avec CyberArk

- **Règle métier** : la règle métier Stockage externe des informations d'identification exécute les tâches suivantes lorsqu'un administrateur apporte des modifications à la propriété de stockage des informations d'identification externe :
  - Elle remplace la vue de la liste et du formulaire d'enregistrement Informations d'identification par la vue Stockage externe. Cette vue permet aux utilisateurs d'afficher la colonne ID d'informations d'identification dans la liste.
  - Indique à l'd'actualiser Serveur MID son cache d'informations d'identification non externes en prévision d'un changement dans la manière dont les informations d'identification sont obtenues.
- **Propriété système** : une propriété appelée Activer le stockage des informations d'identification externe [com.snc.use_external_credentials] active ou désactive le module d'extension Stockage des informations d'identification externe une fois qu'il est activé. Cette propriété est située à**Définition de découverte** > **Propriétés**et**Orchestration** > **Propriétés de Serveur MID**et est activé lorsque vous activez le module d'extension.

> **Remarque :**
> Si vous désactivez le stockage des informations d'identification externes avec la propriété système, le système définit automatiquement toutes les informations d'identification externes comme inactives dans l'instance. Si vous réactivez la fonctionnalité avec cette propriété, le système ne réinitialise pas les enregistrements d'informations d'identification externes en mode actif. Vous devez réactiver chaque enregistrement d'informations d'identification manuellement.

Types d'informations d'identification pris en charge

L'intégration CyberArk prend en charge ces ServiceNow types d'informations d'identification :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- GCP
- Azure
- CIM
- JMS
- Forum SNMP
- SNMPv3
- Authentification de base
- Paire de clés SSH
- Clé privée SSH (avec clé, mot de passe et mot de passe)
- VMware
- Windows
- Informations d'identification applicatives

Remarque :
Pour utiliser CyberArk l'intégration avec le type d'informations d'identification GCP, vous devez modifier le fichier JAR de stockage des informations d'identification externes. Pour en savoir plus, consultez ServiceNow GCP Credential Resolver à l'aide de CyberArk .

Now Platform Les entités qui utilisent ces protocoles réseau prennent également en charge l'utilisation d'informations d'identification stockées dans un CyberArk coffre-fort.

Informations d'identification prises en charge par le protocole réseau

Protocole réseau	ServiceNow® Studio de workflow soutien	Orchestration soutien
SOAP	Étape SOAP	Créer une activité de service Web SOAP avec des remplacements d'authentification de base
REST	Étape REST	Créer une activité de service Web REST avec des remplacements d'authentification de base
JDBC	Étape JDBC	Activité JDBC
SSH	Étape SSH	Activité SSH
PowerShell	Étape PowerShell	Activité PowerShell
SFTP	Étape SFTP	Activité SFTP
JMS		Activité JMS

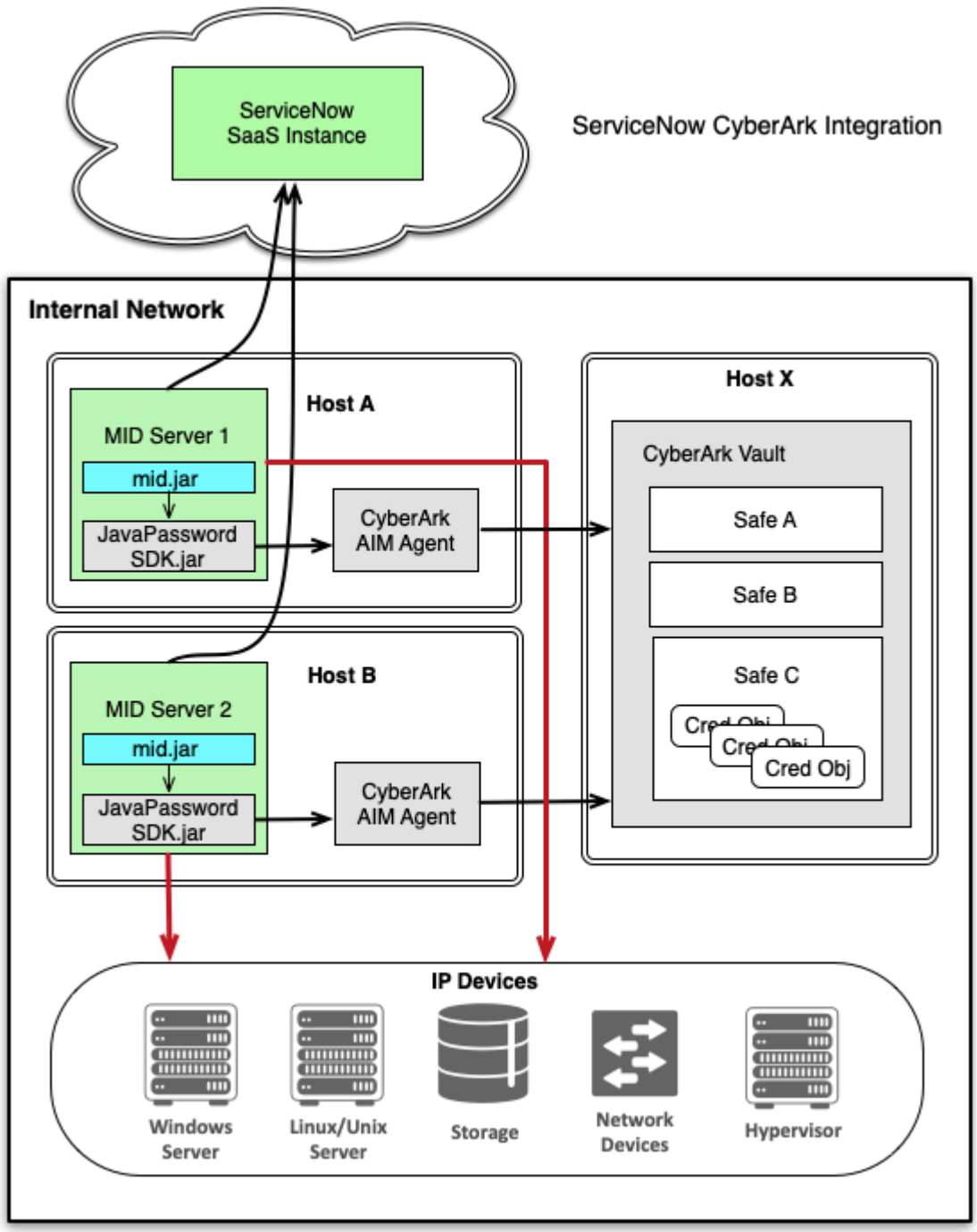
Important :
Vous ne pouvez pas gérer les informations d'identification stockées sur un CyberArk coffre-fort et un système de stockage d'informations d'identification externe personnalisé utilisant le même Serveur MID. CyberArk Le Serveur MID client AIM/API doivent être installés sur le même ordinateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture CyberArk

CyberArk Architecture de stockage



Remarque :
CyberArk utilise le fichier `de mid.jar` système de base pour résoudre les informations d'identification.

Serveur MID Gestion des Windows comptes

La recherche d'informations d'identification tente initialement de faire correspondre l'ID d'informations d'identification spécifié à une valeur existante dans le champ **Nom** du

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

CyberArk coffre-fort. Si une correspondance est trouvée, les informations d'identification sont renvoyées. Si aucune correspondance n'est trouvée, la recherche d'informations d'identification tente de trouver une correspondance à l'aide de l'adresse IP. Si la recherche d'adresse IP correspond à plusieurs informations d'identification, telles que Windows et Tomcat sur le même serveur, la recherche échoue. Pour éviter ce problème, définissez le `ext.cred.type_specifier` paramètre dans le Serveur MID fichier config.xml **sur true** pour forcer CyberArk le renvoi des informations d'identification qui correspondent à la fois au type d'informations d'identification et à l'adresse IP. Par exemple, si une adresse IP est partagée par les deux Windows et Tomcat, un type d'informations d'identification de renvoie uniquement les Windows informations d'identificationWindows.

Mettre à niveau la CyberArk bibliothèque

Vous pouvez mettre à niveau la CyberArk bibliothèque si un paramètre de configuration sécurisé est nécessaire.

Vérifiez le paramètre de configuration suivant dans le **config.xml** : < parameter name="mid.secure_config.provider » value="com.service_now.mid.services.config.CyberArkSecuredConfigProvider »/>

Pour effectuer la mise à niveau, procédez comme suit si un fournisseur de paramètres de configuration sécurisé est configuré.

1. Renommez la CyberArk version du client en JavaPasswordSDK_MajorVersion_minorVersion_patchNum.jar.
2. Créez une entrée jar dans la table ecc_agent à laquelle le jar de renommage peut être joint. Cette nouvelle entrée est téléchargée dans le Serveur MIDfichier . Cette étape génère deux fichiers jar (Passworsdk.jar et JavaPasswordSDK _12_X_X.jar).
3. Supprimez l'ancienne entrée de ecc_agent de l'instance. Cette étape supprime Passworsdk.jar du Serveur MID, et la _12_X_X.jar JavaPasswordSDK reste dans le système.

Configuration de l'intégration CyberArk

Ces procédures comprennent à la fois des tâches de configuration CyberArk et ServiceNow, y compris des références à la documentation CyberArk appropriée.

L'identifiant d'informations d'identification configuré dans l'instance ServiceNow doit être mappé au nom des informations d'identification dans le coffre-fort CyberArk. Lors de la recherche d'informations d'identification, le serveur MID trouve les informations d'identification en faisant correspondre l'identificateur d'informations d'identification à un nom dans le coffre-fort, qui doit être unique. Si l'identificateur d'informations d'identification est vide, le Serveur MID trouve les informations d'identification par adresse IP. Pour identifier les informations d'identification par adresse IP, le système examine le type d'information d'identification pour s'assurer qu'il n'existe qu'une seule information d'identification de ce type à cette adresse. Par exemple, lorsqu'un serveur Windows et vCenter s'exécutent tous deux sur la même adresse IP. Pour prendre en charge des exigences strictes en matière d'informations d'identification dans un environnement SSH, un paramètre de configuration de MID Server vous permet d'exiger que le type d'informations d'identification demandé corresponde au type renvoyé par CyberArk.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Le champ **ID d'informations d'identification** est le seul champ nécessaire pour mapper vos informations d'identification à CyberArk, dans tous les cas, à l'exception de SNMPv3. Le champ **ID d'informations d'identification de confidentialité est facultatif et n'est** requis que lors de l'utilisation d'informations d'identification SNMPv3 et de l'utilisation d'un protocole de confidentialité pour les informations d'identification. Reportez-vous à la rubrique Configurer l'identificateur d'informations d'identification CyberArk pour en savoir plus.

Pour configurer votre instance afin d'obtenir des informations d'identification à partir d'un coffre-fort CyberArk, effectuez ces tâches dans l'ordre dans lequel elles apparaissent ci-dessous.

Configurez le coffre-fort CyberArk et installez l'API AIM

Configurez le coffre-fort CyberArk pour autoriser l'accès au MID Server et installez l'API CyberArk AIM sur l'ordinateur du MID Server.

Avant de commencer

Rôle requis : administrateur

Avant de commencer cette procédure, assurez-vous que le module d'extension External Credential Storage est activé. Les fournisseurs d'informations d'identification CyberArk Application Access Manager (AAM) version 12.0.1 et ultérieure sont pris en charge.

Procédure

1. Configurez le coffre-fort CyberArk avec l'ID d'application et les détails d'authentification que tous les MID Server demandant des informations d'identification utiliseront.
   Pour en savoir plus, consultez le Guide de mise en œuvre de CyberArk Credential Provider et ASCP.

   a. Assurez-vous que CyberArk est configuré pour permettre au MID Server d'accéder au coffre-fort en créant un App-ID dans CyberArk appelé `ServiceNow_MID_Server`.

   b. Assurez-vous que toutes les informations d'identification dont le MID Server a besoin ont accès à l'App-ID `ServiceNow_MID_Server` .

   Remarque :
   Vous pouvez remplacer **l'ID** d'application ServiceNow_MID_Server par défaut dans le fichier de config.xml du Serveur MID à l'aide du paramètre ext.cred.app_id . Si vous modifiez la valeur de ce paramètre, assurez-vous de configurer une valeur correspondante dans le coffre-fort.

2. Installez le fournisseur d'informations d'identification CyberArk, y compris l'API AIM, sur chaque machine qui héberge un service MID Server utilisé pour accéder à la banque d'informations d'identification.
3. Provisionnez des comptes CyberArk et définissez des autorisations pour accéder aux applications.
   Pour plus d'informations, consultez le Guide de mise en œuvre de la sécurité des comptes privilégiés de CyberArk.

   a. Dans CyberArk Password Safe, créez les comptes privilégiés requis par Discovery, Orchestration ou Service Mapping pour accéder aux différents appareils et assurez-vous que ces comptes sont membres des coffres-forts dans lesquels les informations d'identification nécessaires sont stockées.

   b. Ajoutez le fournisseur d'informations d'identification et les utilisateurs de l'application en tant que membres des coffres-forts où les mots de passe des applications sont stockés.

Importer le fichier JAR CyberArk

Importez le fichier CyberArk JavaPasswordSDK.jar dans l'instance pour le rendre accessible au MID Server.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

Rôle requis : agent_admin ou admin

Avant de commencer cette procédure, assurez-vous que CyberArk est configuré pour permettre au MID Server d'accéder aux informations d'identification. Assurez-vous que l'API AIM de CyberArk est installée sur chaque serveur hébergeant un MID Server utilisé pour accéder au coffre-fort.

Pourquoi et quand exécuter cette tâche

Utilisez ce processus même si le fichier JavaPasswordSDK.jar existe déjà sur le serveur MID.

Procédure

1. Accédez à la **Tout** > **Serveur MID** > **Fichiers JAR**.
2. Cliquez sur **Nouveau**.
3. Remplissez le formulaire à l'aide des champs de la table.

Champs de formulaire du fichier JAR

Champ	Description
Nom	Nom unique et descriptif permettant d'identifier le fichier dans l'instance.
Version	Numéro de version facultatif du fichier, le cas échéant.
Source	Fournisseur du fichier JAR. Les informations sources ne sont pas utilisées par le système.
Description	Brève description facultative du fichier JAR et de sa fonction dans l'instance.

4. Joignez le fichier JAR à cet enregistrement.
   Le fichier de JavaPasswordSDK.jar AIM est fourni avec les fichiers d'installation du SDK AIM et se trouve généralement sur le serveur MID dans le répertoire d'installation d'AIM à l'adresse <install_dir>/CyberArk/ApplicationPasswordSdk.
5. Cliquez sur **Envoyer**.
6. Redémarrez le service MID Server.
   La plate-forme met le fichier JAR à la disposition de n'importe quel MID Server configuré pour communiquer avec l'instance.

Configurer MID Server pour CyberArk

Configurez le fichier config.xml pour accorder au MID Server l'accès au coffre-fort CyberArk.

Avant de commencer

Rôle requis : administrateur

Avant de commencer cette procédure, importez le fichier JavaPasswordSDK.jar dans l'instance.

Procédure

Configurer manuellement le Serveur MID Ajouter un fichier de paramètres du Serveur MID avec ces paramètres.

Cette configuration ne peut pas être effectuée à partir de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètres de configuration requis

Paramètre	Valeur	Description
ext.cred.safe_folder	Nomdudossier	Dossier à utiliser pour toutes les recherches d'informations d'identification. Par exemple, **root**.
ext.cred.use_cyberark	VRAI	Paramètre booléen indiquant que ce MID Server est intégré à CyberArk.

Paramètres de configuration facultatifs

Paramètre	Valeur	Description
ext.cred.safe_timeout	5 (seconde)	Délai d'expiration de chaque recherche d'informations d'identification dans le coffre-fort, spécifié en secondes.
ext.cred.safe_name	Nom de coffre-fort	Nom sûr par défaut utilisé pour toutes les recherches d'informations d'identification. Si les paramètres se trouvent dans plusieurs coffres-forts, l'ID d'informations d'identification peut être spécifié au format *<safeName>:<CredentialID>*. Lorsqu'il est configuré de cette manière, le champ **NameOfSafe** est ignoré. Si tous les identifiants d'identification externes ont leur ID d'informations d'identification spécifié au format, laissez de côté le champ **NameOfSafe** . **Remarque :** Par défaut, le caractère de séparation dans ce format est un deux-points. Pour affecter n'importe quel caractère que vous voulez comme séparateur, ajoutez cette ligne au fichier CredMap.properties : safe.cred.split.string=<string>.
ext.cred.app_id	ServiceNow_MID_Server	Spécifie l'ID d'application utilisé pour accorder l'autorisation au MID Server d'accéder au coffre-fort CyberArk. La valeur par défaut, **ServiceNow_MID_Server**, doit être définie dans le coffre-fort CyberArk. Vous pouvez utiliser ce paramètre pour remplacer la valeur par défaut et spécifier votre propre ID d'application. Si vous modifiez l'App-ID dans ce paramètre, assurez-vous de configurer CyberArk pour qu'il corresponde.
ext.cred.type_specifier	VRAI	Force une recherche d'adresse IP à renvoyer des informations d'identification qui correspondent à la fois à l'ID de la plateforme CyberArk et à l'adresse IP. Par exemple, si une adresse IP est partagée à la fois par Windows et Tomcat, les informations d'identification avec un ID de plateforme commençant **par Win** renvoient uniquement les informations d'identification Windows. Lorsque ce paramètre est défini sur true, CyberArk recherche les ID de plateforme qui commencent par :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Paramètre	Valeur	Description
		• Win : Windows • Unix : SSH • VMWare : VMware
ext.cred.check_ssh_type	faux	Lorsque la valeur est définie sur vrai, elle exige que le type d'informations d'identification SSH renvoyées par CyberArk corresponde au type d'informations d'identification demandées. Par exemple, si un nom d'utilisateur/mot de passe SSH normal est demandé et que seules les clés SSH sont disponibles, la recherche d'informations d'identification échoue.

Configurer CyberArk pour les informations d'identification SNMPv2

Si votre système utilise SNMPv2, vous pouvez créer un fichier spécial pour mapper l'attribut d'un identifiant à la chaîne de communauté.

Avant de commencer

Rôle requis : administrateur

Avant de commencer cette procédure, configurez le MID Server pour qu'il ait accès au coffre-fort CyberArk.

Pourquoi et quand exécuter cette tâche

Remarque :
Si la chaîne de communauté apparaît dans le champ du mot de passe des informations d'identification CyberArk, il n'est pas nécessaire d'effectuer cette procédure.

SNMPv2 n'est pas pris en charge nativement dans CyberArk. Si votre organisation a créé des informations d'identification SNMPv2 personnalisées dans lesquelles la chaîne de communauté n'apparaît pas dans le champ de mot de passe des informations d'identification, utilisez cette procédure pour mapper l'attribut des informations d'identification à la chaîne de communauté.

Procédure

1. Dans un éditeur de texte, créez un fichier appelé CredMap.properties, contenant ce code : `SNMPv2.Communauté=attribute_name`
2. Enregistrez le fichier dans le répertoire `/agent` de votre installation de MID Server.
   Lors de la recherche d'informations d'identification, le serveur MID tente de trouver cet attribut pour les informations d'identification. Si l'attribut est introuvable, le serveur MID effectue alors une recherche dans le champ de mot de passe. Si le champ Mot de passe est vide, la recherche d'informations d'identification échoue.

Configurer l'identificateur d'informations d'identification CyberArk

Créez la clé unique que CyberArk peut utiliser pour identifier des informations d'identification spécifiques dans le référentiel externe.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer cette procédure, assurez-vous que le module d'extension External Credential Storage est activé et que la propriété système com.snc.use_external_credentials est définie sur true.

Procédure

1. Accédez à la **Tout** > **Découverte** > **Informations d'identification** ou **Orchestration** > **Informations d'identification**.
2. Cliquez sur **Nouveau**.
3. Dans la liste des types d'informations d'identification, sélectionnez un type qui prend en charge le stockage externe CyberArk.
4. Remplissez le formulaire à l'aide des champs de votre type d'informations d'identification.
5. Cochez la case **Banque d'identifiants externe** .
   Les champs **Nom d'utilisateur** et **Mot de passe** sont remplacés par le champ **ID d'informations d'identification** .

   Remarque :
   Si la case à cocher n'est pas visible, cliquez sur l'icône de menu dans la barre d'en-tête et sélectionnez **Vue** > **Stockage externe**.

6. Dans le champ **ID d'informations d'identification** , entrez une expression à l'aide de l'un des formats suivants :
   - Si toutes vos informations d'identification se trouvent dans le même coffre-fort, configurez ce nom de sécurité dans le fichier de config.xml du Serveur MID à l'aide du paramètre ext.cred.safe_name , puis spécifiez l'ID d'informations d'identification par nom uniquement, comme **<ID d'informations d'identification>**.
   - Pour nommer les informations d'identification d'une plateforme donnée qui réside dans un coffre-fort spécifique, définissez l'ID d'informations d'identification **comme <safe> :<credential ID> :<ID de plateforme**>.
   - Si vos informations d'identification se trouvent dans plusieurs coffres-forts, spécifiez l'ID d'informations d'identification au format suivant : **<safe> :<credential ID**>.
   - Si vous souhaitez que CyberArk recherche les informations d'identification par adresse IP, à l'aide d'un autre coffre-fort, spécifiez l'ID d'informations d'identification au format suivant : **<safe> :**.
   - Si vous souhaitez que CyberArk recherche les informations d'identification d'un autre identifiant de plateforme dans le même coffre-fort, utilisez le format suivant : **::<ID de plateforme**>
   - Si vous souhaitez que CyberArk recherche les informations d'identification dans un coffre-fort configuré à partir de l'adresse IP plutôt que de l'identifiant d'identification, laissez ce champ vide. Il s'agit de la meilleure pratique pour la gestion des installations dans lesquelles chaque serveur dispose d'informations d'identification uniques.
     Sans ce type de recherche, vous devez créer un enregistrement d'ID d'informations d'identification dans votre instance pour chaque serveur de votre environnement.

   Remarque :
   L'identifiant doit correspondre à la valeur du champ **Nom** du compte CyberArk. Le champ **ID d'informations d'identification** est limité à 180 caractères.

7. Si vous stockez des informations d'identification SNMPv3 dans CyberArk et que vous utilisez le protocole de confidentialité et la clé de confidentialité, configurez l'ID comme suit :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

a. Dans le champ **Type de banque d'informations d'identification** , sélectionnez **CyberArk**. Le champ **ID d'informations d'identification de confidentialité** s'affiche.

b. Saisissez le **nom** du compte de confidentialité CyberArk SNMPv3 dans le champ **ID d'informations d'identification de confidentialité** .

8. Cliquez sur **Envoyer**.

Configurer les informations d'identification AWS sur un coffre-fort CyberArk

Configurez votre coffre-fort CyberArk avec les informations d'identification AWS à récupérer pour une utilisation par votre instance.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

Stockez les informations d'identification en tant que clé SSH dans le coffre-fort CyberArk. Lorsque vous configurez l'accès au coffre-fort sur votre instance, le nom que vous donnez à la clé SSH doit également être utilisé comme ID d'informations d'identification.

Procédure

1. Dans CyberArk, accédez à **Comptes** > **Ajouter une clé SSH**.
2. Saisissez les informations suivantes :

Informations d'identification CyberArk

Champ	Valeur
Type d'équipement	Sélectionnez **Cloud Service**.
Nom de la plateforme	Sélectionnez **Amazon Web Services - AWS - Clés d'accès**.
ID de clé d'accès AWS	Saisissez la clé d'accès AWS, telle que fournie par AWS.
Nom d'utilisateur AWS IAM	Entrez à nouveau la clé d'accès AWS, telle que fournie par AWS.
Mot de passe	Saisissez la clé d'accès secrète AWS, telle que fournie par AWS.
Nom	Entrez un nom pour cette clé.

3. Choisissez **Save (Enregistrer)**.

Que faire ensuite

Si vous ne l'avez pas déjà fait, créez un identifiant d'informations d'identification sur votre instance pour configurer l'accès au coffre-fort CyberArk. Pour plus d'informations, consultez Configurer l'accès au stockage d'informations d'identification externe pour AWS.

Configurer les informations d'identification Azure sur un coffre-fort CyberArk

Configurez votre coffre-fort CyberArk avec les informations d'identification Azure à récupérer pour une utilisation par votre instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche
Pour stocker des informations d'identification Azure, créez d'abord un modèle d'informations d'identification Azure dans le coffre-fort CyberArk. Ce processus ne doit être effectué qu'une seule fois pour le coffre-fort.

Procédure

1. Connectez-vous à CyberArk en mode Administration.
2. Accédez à l'onglet **Administration** .
3. Dans **Configuration système**, modifiez **Platform Management**.
4. Accédez au **modèle de fournisseur dans le cloud** et dupliquez-le.
5. Modifiez le modèle pour les informations d'identification Azure.
6. Ajoutez les deux propriétés suivantes :
   - *Name*au fur et *Display Name* à mesure *UsernameClient ID*
   - *Name*au fur et *DisplayName* à mesure *AddressTenant ID*
7. Appliquez les modifications.
8. Accédez à la section **Compte** et sélectionnez **Ajouter un compte**.
9. Sélectionnez **Sûr**.
10. Définissez le **type d'appareil** sur **Service dans le cloud**.
11. Sélectionnez le modèle Azure qui a été modifié précédemment.
12. Remplissez les informations pour les champs **ID client**, **ID de locataire** et **Mot de passe** .
13. Sélectionnez **Enregistrer**.

Authentification OAuth 2.0 via Serveur MID l'utilisation d'un stockage d'informations d'identification externe

Stockez les informations d'identification OAuth 2.0 (ID client et secret client) dans le CyberArk coffre-fort au lieu de l'instance ServiceNow . Le obtient Serveur MID les informations d'identification du CyberArk coffre-fort, lorsque cela est nécessaire pour obtenir le jeton OAuth. Le jeton est stocké dans le serveur MID et actualisé automatiquement à son expiration.

Le CyberArk produit Application Identity Management (AIM) utilise la solution Privileged Account Security pour éliminer la nécessité de stocker les mots de passe d'application intégrés dans les applications, les scripts ou les fichiers de configuration, et permet de stocker, de journaliser et de gérer ces mots de passe hautement sensibles de manière centralisée dans le CyberArk coffre-fort. Vous pouvez configurer le CyberArk coffre-fort pour stocker les informations d'identification OAuth 2.0 plutôt que directement dans un enregistrement d'informations d'identification ServiceNow . Pour en savoir plus sur CyberArk, consultez CyberArk Intégration de stockage des informations d'identification.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Architecture de l'authentification OAuth 2.0 de la Serveur MID requête

L'architecture se compose de deux parties : ServiceNow l'instance et l'environnement dans lequel le client Application Identity Manager (AIM) et le serveur MID sont configurés. Le cloud ou l'environnement client sont des exemples d'environnement.

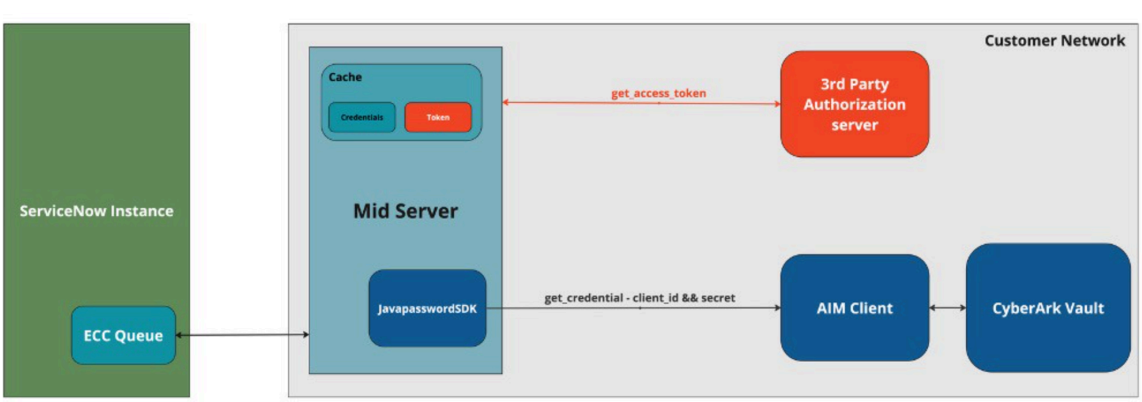
Le Serveur MID client Application Identity Manager (AIM) et celui-ci doivent être configurés sur le même environnement et Application Identity Manager (AIM) doit être configuré pour interagir avec le CyberArk coffre-fort externe. Le CyberArk coffre-fort externe peut être hébergé dans le même environnement que celui de MID Server et Application Identity Manager (AIM) ou dans un environnement différent.

L'instance ServiceNow conserve les identificateurs d'informations d'identification qui correspondent à des informations d'identification OAuth 2.0 spécifiques stockées dans le CyberArk coffre-fort. Avant d'envoyer une demande de jeton OAuth, le MID Server obtient l'identificateur d'informations d'identification auprès de l'instance, puis utilise un fichier JAR fourni par le client pour envoyer l'identificateur au client AIM. Le client AIM envoie la demande au CyberArk coffre-fort. Le CyberArk coffre-fort renvoie les informations d'identification OAuth 2.0 au MID Server via le client AIM. Après avoir reçu les informations d'identification OAuth 2.0, le MID Server envoie la demande de jeton OAuth au serveur d'autorisation tiers. La demande de jeton comprend des informations telles que le client et le secret client qui CyberArk stockent, le périmètre OAuth et l'URL du jeton que l'instance stocke. Une fois que le serveur d'autorisation a émis le jeton OAuth, le MID Server le stocke dans sa mémoire cache.

Remarque :
Cette fonctionnalité prend en charge le type d'accord d'informations d'identification du client.

L'image montre le processus d'authentification des requêtes du MID Server.

Remarque :
Il est supposé que le serveur d'autorisation tiers et le CyberArk coffre-fort sont hébergés sur le réseau du client.



Configurer un fichier JAR et des identificateurs d'informations d'identification

Configurez un fichier JAR et des identificateurs d'informations d'identification afin que le fichier JAR résolve les identificateurs d'informations d'identification en informations d'identification CyberArk réelles provenant du coffre externe. Le processus permet au MID Server d'obtenir et d'inclure les informations d'identification OAuth 2.0 dans la demande de jeton OAuth.

Avant de commencer
Rôle requis : agent_admin ou admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le CyberArk coffre-fort externe stocke les informations d'identification sensibles et l'instance ServiceNow stocke les identificateurs d'informations d'identification qui correspondent aux noms d'informations d'identification spécifiques que le coffre-fort stocke. Le fichier JAR permet de mapper un identificateur d'informations d'identification à un nom d'informations d'identification spécifique dans le coffre-fort externe. Le mappage permet au d'acquérir et d'inclure les informations d'identification Serveur MID requises dans la demande de jeton OAuth. Vous devez configurer les identificateurs d'informations d'identification et le fichier JAR respectivement dans l'instance ServiceNow et dans le serveur MID.

Procédure

1. Importer le fichier JAR CyberArk.
2. Configurer une connexion pour envoyer une demande OAuth via le Serveur MID coffre-fort externe à l'aide.

Configurer CyberArk

Configurez le CyberArk coffre-fort pour stocker les informations d'identification OAuth 2.0 et répondre aux demandes d'informations d'identification OAuth 2.0 à partir du Serveur MID.

Avant de commencer

Confirmez que vous êtes abonné au programme d'installation du pack standard ServiceNow Centre d'intégration. Pour plus d'informations, consultez https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Rôle requis : agent_admin ou admin

Procédure

1. Configurez le coffre-fort CyberArk et installez l'API AIM.
2. Importer le fichier JAR CyberArk.
3. Configurer les informations d'identification OAuth 2.0 sur CyberArk.
4. Configurer une connexion pour envoyer une demande OAuth via le Serveur MID coffre-fort externe à l'aide.

Configurer les informations d'identification OAuth 2.0 sur CyberArk

Configurez votre coffre-fort CyberArk avec les informations d'identification OAuth 2.0 demandées par l'instance ServiceNow .

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Pour stocker les informations d'identification OAuth 2.0, créez d'abord un modèle d'informations d'identification OAuth 2.0 dans le coffre-fort CyberArk. Ce processus ne doit être effectué qu'une seule fois pour le coffre-fort.

Procédure

1. Procédez comme suit si vous configurez les informations d'identification OAuth 2.0 pour la première fois.
   a. Connectez-vous à CyberArk en mode Administration.
   b. Accédez à l'onglet **Administration** .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

c. Sélectionnez **Gestion de la plateforme**.
La page Gestion des plates-formes affiche les plates-formes sous l'onglet Cibles.

d. Développez un type de plateforme.

e. Sélectionnez l'icône de paramètres ( qui correspond à un modèle de plateforme et sélectionnez **Dupliquer**.

f. Dans la fenêtre Dupliquer la plateforme, entrez un nom pour le modèle et sélectionnez **Créer**.

Remarque :
Notez le type de système sous lequel vous avez créé un modèle en double. Par exemple, Service dans le cloud est un type de système.

g. Sélectionnez l'icône des paramètres ( qui correspond au modèle de plateforme dupliqué que vous avez créé, puis sélectionnez **Modifier**.

h. Ajoutez la propriété.
Nom en tant que nom d'utilisateur et nom d'affichage en tant qu'ID client.

i. Renommez les autres propriétés.

Conseil :
Choisissez des noms de propriété pertinents pour OAuth 2.0.

j. Sélectionnez **Appliquer**.
Les mises à jour sont appliquées.

k. Sélectionnez **OK**.

l. Sur le panneau de gauche, accédez à Comptes.

m. Sélectionnez **Ajouter un compte**.

n. Sous l'en-tête Type de système, sélectionnez le type de système sous lequel vous avez créé le modèle de plateforme.
Le type de système affiche les modèles de plateforme.

o. Sous l'en-tête Sélectionner la plateforme, sélectionnez le modèle de plateforme que vous avez créé.

p. Sélectionnez Sûr.
Enregistrez la valeur Safe pour une utilisation ultérieure.

q. Renseignez les informations relatives à l'ID client, au mot de passe (indiquez le secret client comme valeur) et à d'autres champs si nécessaire.

r. Sélectionnez **Ajouter**.
Le compte est ajouté.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

s. Sur la page Vue du compte, ouvrez un compte.

t. Sélectionnez l'onglet **Détails**.

u. Copiez la valeur stockée dans la section Nom de compte et enregistrez-la pour une utilisation ultérieure.
La valeur que vous avez copiée et stockée est utilisée comme identificateur d'informations d'identification dans l'instance ServiceNow.

2. Procédez comme suit si vous ne configurez pas les informations d'identification OAuth 2.0 pour la première fois.

a. Connectez-vous à CyberArk en mode Administration.

b. Accédez à la section **Compte** et sélectionnez **Ajouter un compte**.

c. Sélectionnez le type de système dans **Type de système** sous lequel le modèle de stockage OAuth 2.0 existe.

d. Sélectionnez le modèle de plateforme requis que vous avez créé, puis sélectionnez **Sûr**.
Enregistrez la valeur Safe pour une utilisation ultérieure.

e. Renseignez les informations relatives à l'ID client, au mot de passe (indiquez le secret client comme valeur) et à d'autres champs si nécessaire.

f. Sélectionnez **Ajouter**.
Le compte est ajouté.

g. Sur la page Vue du compte, ouvrez un compte.

h. Sélectionnez l'onglet **Détails**.

i. Copiez la valeur stockée dans la section Nom de compte et enregistrez-la pour une utilisation ultérieure.
La valeur que vous avez copiée et stockée est utilisée comme identificateur d'informations d'identification dans l'instance ServiceNow .

Configurer une connexion pour envoyer une demande OAuth via le Serveur MID coffre-fort externe à l'aide

Configurez une connexion pour envoyer des demandes de jetons OAuth 2.0 à un serveur d'authentification tiers via le Serveur MID. Le Serveur MID ajoute les informations d'identification OAuth 2.0 (ID client et secret client) du coffre externe, du CyberArk périmètre OAuth et de l'URL de jeton de l'instance à la demande et les envoie au serveur d'authentification tiers.

Avant de commencer

Vérifiez les éléments suivants.

- Confirmez que vous êtes abonné au programme d'installation du pack standard ServiceNow Centre d'intégration. Pour plus d'informations, consultez https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/legal/snc-addendum-integrationhub.pdf .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Vous avez créé un fichier JAR qui permet au serveur MID de résoudre les informations d'identification avec le CyberArk coffre-fort externe. Consultez Créer un fichier JAR pour résoudre les informations d'identification.
- Vous avez importé le fichier JAR dans Serveur MID.
- Le MID Server est configuré pour CyberArk. Consultez Configurer MID Server pour CyberArk.
- OAuth 2.0 sont configurés sur le stockage externe CyberArk. Consultez Configurer les informations d'identification OAuth 2.0 sur CyberArk.

Rôle requis : aucun

Pourquoi et quand exécuter cette tâche

Vous pouvez configurer la connexion et les informations d'identification à l'aide d'un modèle de configuration ou manuellement. Un modèle de configuration définit les composants du formulaire d'enregistrement de connexion et est réutilisable pour d'autres enregistrements de connexion. Manuellement, vous ne pouvez configurer la connexion qu'à cette fin. La rubrique présente les deux approches.

Procédure

1. Configurez la connexion avec un modèle de configuration.

   a. Accédez à la **Tout** > **Centre d'intégration** > **Modèles de configuration**.

   b. Sélectionnez **Nouveau**.

   c. Sélectionnez le **type d'attribution de connexion HTTP avec les informations d'identification du client OAuth (stockage externe).**

   d. Mettez à jour le formulaire selon vos besoins.
   Par exemple, vous pouvez fournir le champ d'application dans les champs `oauth_entity_profile_scope` et `oauth_entity_scope` de la section Modèle de données par défaut. Pour apprendre à créer un modèle de configuration, reportez-vous à la section Créer un modèle de configuration.

   e. Sélectionnez **Soumettre**.
   Vous avez créé le modèle de configuration.

   f. Accédez à la **Tout** > **Centre d'intégration** > **Alias de connexion et d'informations d'identification**.

   g. Mettez à jour le formulaire.

Alias de connexion et d'informations d'identification

Champ	Description
Nom	Nom de l'alias. Un alias ne peut contenir que des caractères alphanumériques, numériques et de soulignement. Lors d'une mise à niveau, la balise dans l'enregistrement d'informations d'identification migre vers un alias

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	de connexion et d'informations d'identification. Si la balise d'informations d'identification contient des caractères spéciaux autres que des lettres, des chiffres et des traits de soulignement, elle conserve le nom de la balise après la mise à niveau. Vous pouvez toujours utiliser cet alias migré, mais vous ne pouvez pas mettre à jour l'alias tant que vous n'avez pas modifié le nom pour respecter les restrictions de dénomination.
Application	Identificateur unique de l'alias de connexion et d'informations d'identification, basé sur le format `scope_name.alias_name`. ▪ Si le périmètre est Global, l'ID est le nom de l'alias. Par exemple, si vous créez un alias Workday dans le champ d'application global, l'ID est défini sur `Workday`. ▪ Si vous créez un alias Workday dans le périmètre de l'application RH, l'ID est défini sur `x_hr_app.workday`.
Alias parent	Option permettant de sélectionner l'alias sous lequel vous créez cet alias de connexion et d'informations d'identification. L'alias de connexion et d'informations d'identification que vous créez est un alias enfant. Un alias enfant est répertorié sous l'onglet **Alias enfants** de la page parente Alias de connexion et d'informations d'identification. 
Type	Option permettant d'indiquer le type d'alias que vous créez. Choisissez parmi les options suivantes. ▪ Informations d'identification : alias qui contient un enregistrement d'informations d'identification. ▪ Connexion et informations d'identification : alias qui contient à la fois l'enregistrement de connexion et d'informations d'identification. Cette option est sélectionnée par défaut. Confirmez que Connexion et informations d'identification sont sélectionnées.
Prendre en charge plusieurs connexions actives	Désignateur qui indique si l'alias prend en charge plusieurs connexions actives. Ajoutez des connexions à l'aide de la table Connexions et

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	associez-les à l'alias à l'aide de la liste connexe Connexions.
Politique des nouveaux essais par défaut	Politique des nouveaux essais pour l'alias. Pour plus d'informations, consultez la politique des nouveaux essais .
Modèle de configuration	Option permettant de sélectionner le modèle de configuration sur lequel vous créez l'alias de connexion et d'informations d'identification. Sélectionnez le modèle de type **d'attribution de connexion HTTP avec les informations d'identification du client OAuth (stockage externe)** que vous avez créé.

h. Sélectionnez **Soumettre**.
Vous avez créé l'enregistrement d'alias de connexion et d'informations d'identification.

i. Accédez à la **Tout** > **Centre d'intégration** > **Tableau de bord des connexions**.

j. Dans le champ Rechercher toutes les connexions, saisissez le nom de l'enregistrement d'alias de connexion et d'informations d'identification que vous avez créé.

k. Sur l'enregistrement de l'alias de connexion et d'informations d'identification, sélectionnez **Afficher les détails**.

l. Sélectionnez **Configurer**.

m. Remplissez le formulaire.

Formulaire Configurer la connexion

Champ	Description
Nom de la connexion	Nom de la connexion. Vous ne pouvez pas mettre à jour le nom.
URL de connexion	URL vers le serveur tiers.
Utiliser MID	Option permettant d'activer Serveur MID. **Important :** Confirmez que l'option est sélectionnée.
Sélection de MID	Option permettant de spécifier la configuration MID pour la connexion. ▪ **Serveur MID spécifique** : option permettant d'indiquer une sélection manuelle d'un Serveur MID spécifique. ▪ **Sélectionner automatiquement Serveur MID** : Option permettant d'indiquer que vous souhaitez que le Serveur MID soit sélectionné automatiquement.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ **Grappe MID spécifique** : option permettant d'indiquer une sélection manuelle d'une grappe MID de serveurs MID. **Important :** Vérifiez que le Serveur MID que vous sélectionnez se trouve sur la même machine que le client AIM de CyberArk qui est configuré pour accéder au coffre-fort CyberArk. Consultez Configurez le coffre-fort CyberArk et installez l'API AIM.
Serveur MID	Option permettant de spécifier manuellement un serveur MID. Cette option s'affiche si vous sélectionnez **Serveur MID spécifique** dans le champ **Sélection de MID** .
Grappe MID	Option permettant de spécifier manuellement une grappe MID. Cette option s'affiche si vous sélectionnez **Grappe MID spécifique** dans le champ **Sélection MID** .
Banque d'identifiants externes	Possibilité d'utiliser le stockage d'informations d'identification externe CyberArk. Lorsque vous sélectionnez l'option, le serveur MID obtient les informations d'identification OAuth 2.0 (ID client et secret client) à partir du stockage d'informations d'identification externe. **Important :** Confirmez que l'option est sélectionnée.
ID de certification	Identificateur du compte CyberArk qui contient les détails de l'ID et du secret du client. Pour connaître la procédure à suivre pour obtenir l'identificateur d'identificateur, reportez-vous à la section Configurer les informations d'identification OAuth 2.0 sur CyberArk. Dans le champ ID d'informations d'identification, entrez une expression à l'aide de l'un de ces formats. ▪ Si toutes vos informations d'identification se trouvent dans le même coffre-fort, configurez ce nom de sécurité dans le fichier de config.xml du Serveur MID à l'aide du paramètre ext.cred.safe_name , puis spécifiez l'ID d'informations d'identification par nom uniquement, comme **<ID d'informations d'identification>**. ▪ Pour nommer les informations d'identification d'une plateforme

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	donnée qui réside dans un coffre-fort spécifique, définissez l'ID d'informations d'identification **comme <safe> :<credential ID> :<ID de plateforme**>. ▪ Si vos informations d'identification se trouvent dans plusieurs coffres-forts, spécifiez l'ID d'informations d'identification au format suivant : **<safe> :<credential ID**>.
URL du jeton OAuth	URL qui spécifie le point de terminaison permettant d'obtenir le jeton d'accès à partir du serveur OAuth.

n. Sélectionnez **Configurer la connexion**.

2. Configurer une connexion manuellement.

a. Accédez à la **Tout** > **OAuth système** > **Registre d'application**.

b. Sélectionnez **Nouveau**.

c. Sélectionnez **Se connecter à un fournisseur OAuth tiers à l'aide d'un coffre externe**.

d. Remplissez le formulaire.

Détails du nouveau registre d'application

Champ	Description
Nom	Nom permettant d'identifier l'enregistrement du registre d'application. Par exemple, saisissez : Demande de jeton OAuth 2.0 via l'application MID.
Application	Option permettant de spécifier les noms des applications qui peuvent accéder à ce registre d'application. Le champ est en lecture seule.
Type d'accord par défaut	Méthode par défaut permettant d'obtenir un jeton d'accès par l'application cliente à partir du serveur OAuth. Le type d'accord par défaut et en lecture seule est Informations d'identification du client.
Accessible depuis	Option permettant de spécifier quelles applications peuvent accéder à ce registre d'application.
URL de jeton	URL qui spécifie le point de terminaison permettant d'obtenir le jeton d'accès à partir du serveur OAuth.
Envoyer les informations d'identification	Option permettant de spécifier la méthode d'envoi d'OAuth 2.0 dans le corps de la demande.
Commentaires	Saisissez les commentaires connexes.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

e. Dans la colonne **Champ d'application OAuth** , créez un ou plusieurs champs d'application OAuth en procédant comme suit.

   i. Dans la colonne Nom, double-cliquez sur le champ et entrez un nom pour le champ d'application OAuth.

   ii. Dans la colonne Champ d'application OAuth, double-cliquez sur le champ et saisissez le champ d'application.

f. Sélectionnez **Soumettre**.
Vous avez créé un profil d'entité OAuth et le registre d'application.

g. Accédez à la **Tout** > **Centre d'intégration** > **Connexions et informations d'identification** > **Informations d'identification**.

h. Sélectionnez **Nouveau**.

i. Sélectionnez **Informations d'identification OAuth 2.0**.

j. Sélectionnez **la vue Stockage externe**.

> **Important :**
> Sélectionnez **la vue de stockage externe** uniquement si la vue est différente de celle d'un formulaire de stockage externe des informations d'identification OAuth 2.0.

k. Remplissez le formulaire.

Informations d'identification OAuth 2.0

Champ	Description
Nom	Nom de l'enregistrement d'informations d'identification.
Concerne	Option permettant de spécifier si l'enregistrement des informations d'identification s'applique à tous les serveurs MID ou à un serveur MID spécifique. Si spécifique, ajoutez les MID Servers. Choisissez l'une des options suivantes. ▪ Tous les serveurs MID : le serveur MID est automatiquement sélectionné dans une collection de serveurs MID. ▪ Serveurs MID spécifiques : option permettant de spécifier un ou plusieurs serveurs MID.
Serveurs MID	Option permettant de spécifier un ou plusieurs MID Servers.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Ce champ s'affiche si vous sélectionnez **Serveurs MID spécifiques** dans le champ S'applique à.
Actif	Option permettant de spécifier si l'enregistrement des informations d'identification est disponible pour utilisation. Par défaut, il est disponible.
Profil de l'entité OAuth	Option permettant de spécifier un profil d'entité OAuth que les informations d'identification utilisent. Sélectionnez le profil d'entité OAuth que vous avez créé ci-dessus. Reportez-vous à la section Configurer un profil d'entité OAuth.
Banque d'identifiants externes	Option permettant de spécifier que les informations d'identification sont stockées dans un stockage externe et non dans l'instance ServiceNow. **Important :** Confirmez que l'option est sélectionnée.
ID de certification	Option permettant de spécifier l'identificateur d'informations d'identification pour le compte CyberArk qui contient l'ID et le secret client. Pour connaître la procédure à suivre pour obtenir l'identificateur d'identificateur, reportez-vous à la section Configurer les informations d'identification OAuth 2.0 sur CyberArk.
Chambre forte de stockage des informations d'identification	Option permettant de spécifier le nom du coffre de stockage des informations d'identification externe. Vérifiez que vous avez sélectionné CyberArk.

l. Sélectionnez **Soumettre**.
Vous avez créé l'enregistrement d'informations d'identification.

m. Créez un alias de connexion et d'informations d'identification.
Pour connaître les étapes à suivre, reportez-vous à la section Créer un alias de connexion et d'informations d'identification.

n. Accédez à la **Tout** > **Centre d'intégration** > **Connexions**.

o. Sélectionnez **Nouveau**.

p. Sélectionnez **Connexion HTTP(s).**

q. Remplissez le formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Formulaire Connexion

Champ	Description
Nom	Nom unique de cette connexion HTTP(s).
Actif	Option permettant de définir la connexion que vous créez active. L'option est sélectionnée par défaut.
Informations d'identification	Sélectionnez l'enregistrement des informations d'identification utilisé pour autoriser la connexion. Sélectionnez les informations d'identification que vous avez créées ci-dessus.
Alias de connexion	Sélectionnez l'enregistrement d'alias à associer à cette connexion. L'utilisation d'un alias vous permet de mettre à jour l'enregistrement de connexion sans avoir à reconfigurer les actions ou les activités qui utilisent l'alias.
Générateur d'URL	Entrez manuellement l'URL de connexion ou utilisez le système pour créer l'URL en fonction des entrées. Cette option n'est pas cochée par défaut. Si cette option est cochée, l'URL de connexion est calculée à partir des champs suivants : ▪ Authentification réciproque : case à cocher si l'authentification réciproque est utilisée. ▪ Protocole : si l'authentification réciproque n'est pas utilisée, entrez protocole. La valeur par défaut est HTTPs. ▪ Profil de protocole : si l'authentification réciproque est utilisée, entrez le profil de protocole à partir de sys_protocol_profile. ▪ Hôte ▪ Port ▪ Chemin de base : chemin d'accès de la chaîne de connexion. **Remarque :** Si l'authentification réciproque est cochée, l'URL de connexion est construite : Protocole + :// + hôte :port +URL. Si l'authentification réciproque n'est pas cochée, l'URL de connexion est construite : profil de protocole + :// + host :port +URL
URL de connexion	Si l'option Générateur d'URL n'est pas cochée, saisissez l'URL de connexion dans ce champ.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	Remarque : Si l’authentification réciproque est cochée, l’URL de connexion est construite : Protocole + :// + hôte :port +URL. Si l’authentification réciproque n’est pas cochée, l’URL de connexion est construite : profil de protocole + :// + host :port +URL
Utiliser un MID Server	Option permettant de spécifier que vous souhaitez envoyer des demandes de jetons OAuth via un serveur MID. **Important :** Confirmez que l’option est sélectionnée.
Délai de connexion	Nombre de millisecondes pendant lesquelles le système attend une connexion de l'hôte réussie. Si aucune connexion réussie n'a lieu pendant cette durée, la demande de connexion expire. Laissez ce champ vide pour utiliser la valeur de délai de connexion par défaut du système.
Sélection de MID	Option permettant de spécifier l’une des options suivantes. ▪ Sélectionner automatiquement Serveur MID : sélectionne parmi les serveurs MID en fonction des critères du serveur MID, qu’ils soient membres ou non d’une grappe. ▪ Serveur MID spécifique : sélectionnez manuellement un Serveur MID. ▪ Grappe MID spécifique : la réaffectation automatique à un autre Serveur MID sélectionne uniquement parmi les membres de la grappe spécifiée. **Important :** Vérifiez que le Serveur MID que vous sélectionnez se trouve sur la même machine que le client AIM de CyberArk qui est configuré pour accéder au coffre-fort CyberArk. Consultez Configurez le coffre-fort CyberArk et installez l’API AIM.
Serveur MID	Sélectionnez manuellement un serveur MID. Cette option s’affiche si vous sélectionnez Serveur MID spécifique dans le champ Sélection de MID.
Grappe MID	Sélectionnez manuellement une grappe MID. Cette option s’affiche si vous sélectionnez Grappe MID spécifique dans le champ Sélection MID.
Application MID	Sélectionnez manuellement une application MID.

Traduction automatique

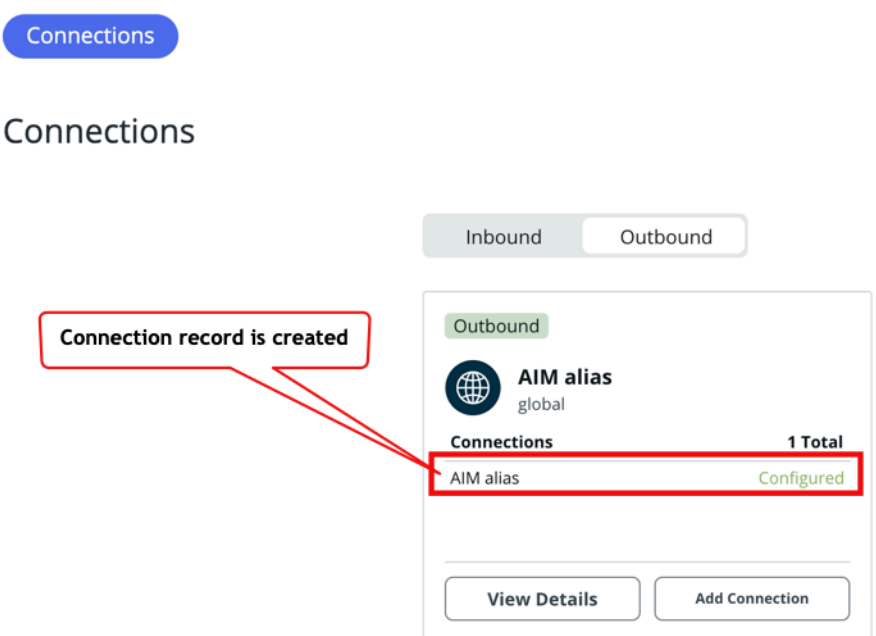
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

r. Sélectionnez **Soumettre**.
Vous avez créé un enregistrement de connexion HTTP(s).

s. Accédez à la **Tout** > **Automatisation des processus** > **Centre d'intégration** > **Tableau de bord des connexions**.

t. Dans le champ Rechercher toutes les connexions, saisissez le nom de l'enregistrement de connexion que vous avez créé.
L'enregistrement d'alias de connexion s'affiche.

L'enregistrement de connexion OAuth 2.0 est créé



Algorithmes d'authentification

Vérifier l'identité de l'expéditeur à l'aide des algorithmes d'authentification

Autorisez les étapes d'intégration pour vous authentifier auprès de services Web qui nécessitent des mécanismes de connexion ou d'informations d'identification complexes ou non standard. Associez des algorithmes d'authentification aux alias d'informations d'identification et de connexion pour réduire ou éliminer la nécessité de configurer manuellement les étapes d'intégration.

Vous pouvez utiliser un algorithme d'authentification pour générer des données d'authentification personnalisées pour vos étapes d'intégration. Les étapes d'intégration peuvent utiliser ces données dynamiques pour créer tous les artefacts personnalisés nécessaires pour s'authentifier auprès du service Web cible. Par exemple, une étape REST peut créer un en-tête d'authentification, des paramètres de requête ou un jeton.

Les algorithmes d'authentification prennent en charge les étapes suivantes :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Étape Obtenir des informations sur la connexion
- Étape REST
- Étape SOAP

Pour plus d'informations, consultez Étapes d'intégration

Types d'algorithmes d'authentification

- **Signature Amazon Version 4** : il s'agit d'un algorithme d'authentification prédéfini pour se connecter aux services Web Amazon.
- **Authentification personnalisée** : il s'agit d'un modèle que les développeurs peuvent utiliser pour créer leurs propres algorithmes d'authentification.

Pour en savoir plus sur la configuration de l'algorithme d'authentification, reportez-vous à la section Configurer un algorithme d'authentification.

Scripts

Les scripts d'authentification d'instance se trouvent sur les scripts d'instance qui font partie de la *sys_script_include* table.

Scripts d'authentification d'instance

Demande d'authentification interne	Script en lecture seule sur l'instance, qui prend en charge la génération de signature AWS V4 ou l'authentification personnalisée envoyée avec la demande sortante.
RequestAuthAWSV4Signataire	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature AWS V4.
RequestAuthTwitterSigner	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature Twitter à l'aide d'OAuth 1.0a.
RequestAuthSampleCustomSigner	Exemple de script étendant RequestAuthInternal pour comprendre comment écrire un signataire personnalisé sur une instance.

Les scripts d'authentification MID se trouvent sur la partie scripts MID de *ecc_agent_script_include* la table.

Scripts d'authentification MID

Demande d'authentification interne	Script en lecture seule sur MID, qui prend en charge la génération de signature AWS V4 ou d'authentification personnalisée envoyée avec la demande sortante.
RequestAuthAWSV4MIDSigner	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature AWS V4.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Scripts d'authentification MID (suite)

RequestAuthTwitterSigner	Script étendant RequestAuthInternal pour implémenter le signataire afin de générer une signature Twitter à l'aide d'OAuth 1.0a.
RequestAuthSampleMidCustomSigner	Exemple de script étendant RequestAuthInternal pour comprendre comment écrire un signataire personnalisé sur MID.

API JavaScript

Voici les API JavaScript pour l'algorithme d'authentification.

- AuthCredential
- Données HttpRequestAuthedData
- Données de demande en ligne
- RequestAuthAPI (API d'authentification de demande)

Configurer un algorithme d'authentification

Configurez un algorithme d'authentification afin de pouvoir signer les demandes HTTP sortantes.

Avant de commencer

Un include de script doit être configuré avant de configurer un algorithme d'authentification.
Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Renseignez les champs du formulaire.
   La sélection de base de données dans le champ **Format** détermine les champs qui sont disponibles.

Formulaire d'authentification

Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante.
Description	Description de l'action de votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Includes de script.
Script d'authentification MID	Script que vous sélectionnez dans la table Includes de script de Serveur MID [vue Détection].

3. Cliquez sur **Envoyer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer un algorithme personnalisé basé sur les Amazon signatures

Générez les données basées sur les signatures nécessaires pour vous authentifier auprès d'un service Web en exécutant le Amazon script.

Avant de commencer

- Base de connaissances JavaScript
- Base de connaissances REST
- Connaissance de l'API de service Web cible
- Base de connaissances sur les connexions, les informations d'identification et les alias
- Rôle requis : développeur

Pourquoi et quand exécuter cette tâche

Utilisez un alias de connexion et d'informations d'identification et Amazon un algorithme basé sur la version de signature 4 pour l'authentification.

Procédure

1. Accédez à la **Tout** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Renseignez les champs du formulaire.
   La sélection de base de données dans le champ **Format** détermine les champs qui sont disponibles.

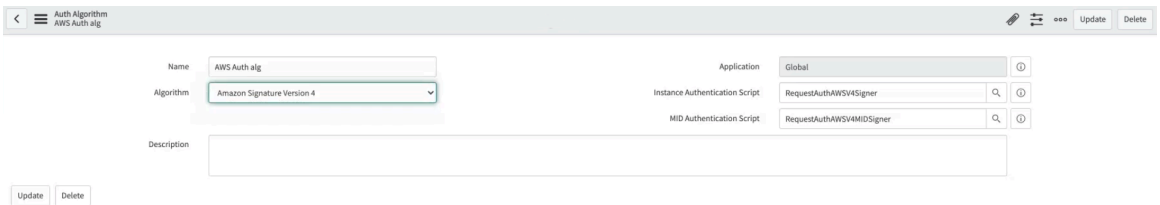
Formulaire d'authentification

Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante. Sélectionnez **Amazon Signature Version 4**.
Description	Description de l'action de votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Includes de script. Dans le cas de l'algorithme **Amazon Signature Version 4** , choisissez **RequestAuthAWSV4Signer**. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ Demande d'authentification interne ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner **Remarque :** Pour en savoir plus sur le script, cliquez sur l'icône d'informations en regard du champ. Les détails du script tels que nom, nom de l'API, application, accessible depuis, script, etc. s'affichent.
Script d'authentification MID	Script que vous sélectionnez dans la table Includes de script de Serveur MID [vue Détection]. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ Demande d'authentification interne

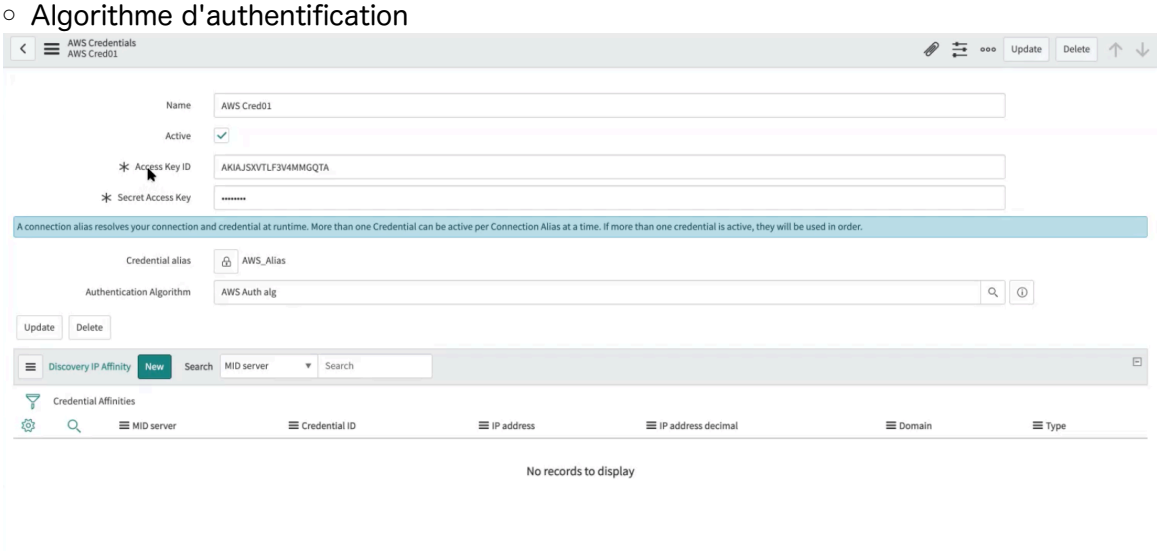
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner



3. Cliquez sur **Mettre à jour**.
4. Accédez à la **Tout** > **Connexions et informations d'identification** > **Informations d'identification**.
5. Cliquez sur **Nouveau**.
6. Créez AWS des informations d'identification avec l'algorithme d'authentification.
   Dans ce cas, **AWS Auth alg**.
7. Spécifiez les éléments suivants :
   - Nom
   - Actif
   - ID de clé d'accès
   - Clé d'accès secrète
   - Alias d'informations d'identification
   - Algorithme d'authentification



8. Cliquez sur **Mettre à jour**.

Résultats
En fonction des scripts et de l'algorithme d'authentification sélectionnés, les informations d'identification configurées (**ID de clé d'accès** et **clé d'accès secrète**) ou les informations d'identification de l'utilisateur (**ID de clé d'accès**, **clé d'accès secrète** et **jeton de session**)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

génèrent une Amazon signature V4 qui est envoyée en tant que demande sortante du ServiceNow fournisseur (dans ce cas AWS).

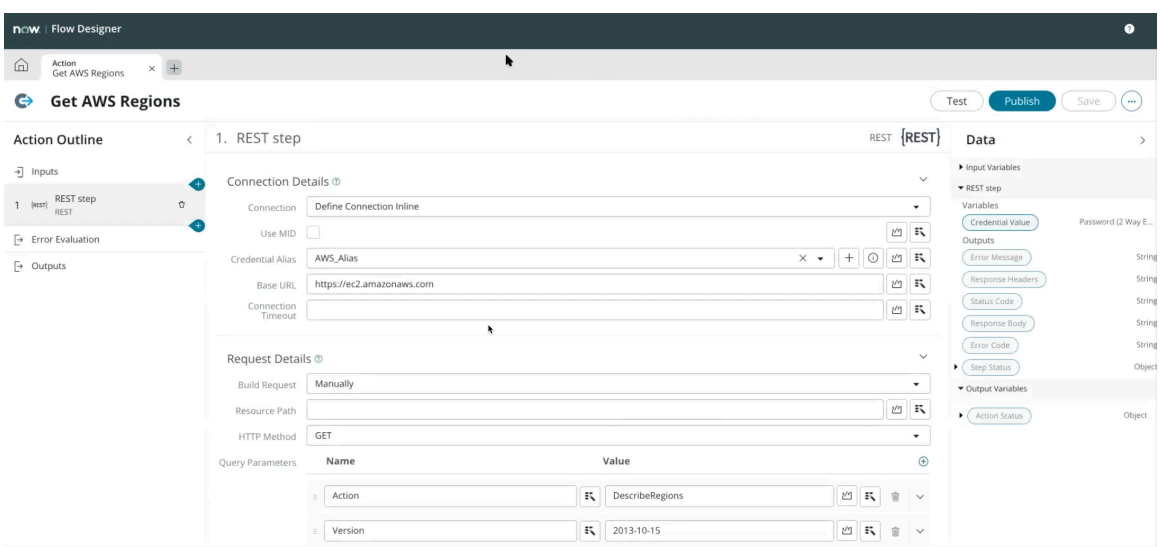
Example: Étape REST avec AWS

Remarque :
Amazon L'authentification basée sur la signature V4 peut également être utilisée à partir de l'arrière-plan de script.

Action : obtenir AWS les régions

Entrez l'étape REST comme AWS suit :

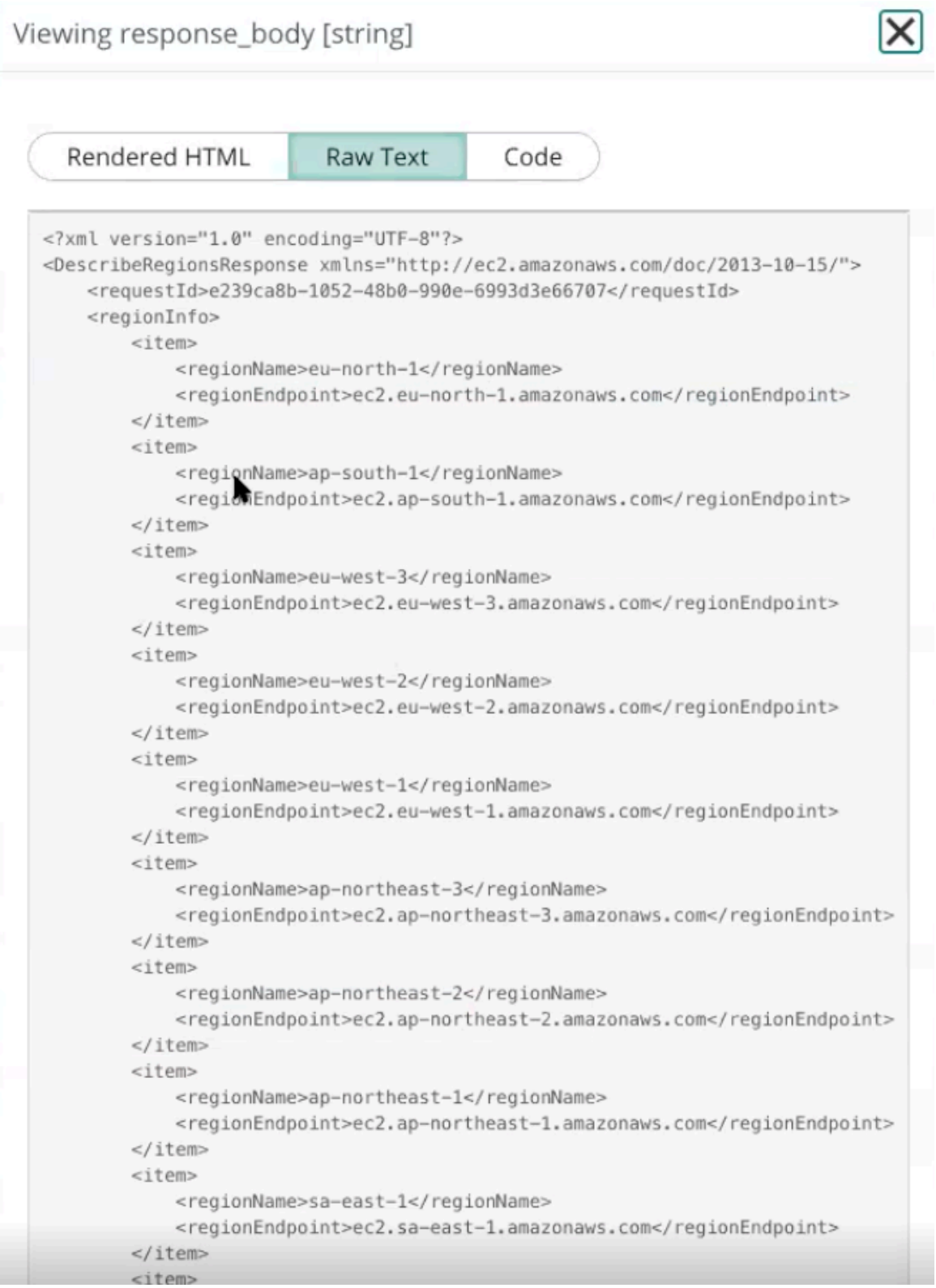
- **Alias des informations d'identification** : alias créé pour AWS.
- **URL de base** : détails de l'URL de base à partir de AWS.
- **Méthode HTTPS** : dans ce cas, il s'agit de la méthode GET.
- **Paramètres de requête** : **action** en tant que **DescribeRegions**.



Vous pouvez tester l'action, les régions associées sont affichées. Le corps de la réponse est le suivant :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Amazon V4 est défini avec un ensemble standard d'algorithmes qui prend en charge le mécanisme d'authentification. Cet algorithme, lorsqu'il est utilisé, ajoute la signature comme en-tête d'autorisation pour l'authentification (demande HTTP) à l'aide de l'étape REST.

Configurer un algorithme d'authentification personnalisé

Générez les données personnalisées nécessaires pour vous authentifier auprès d'un service Web en exécutant le script.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer

- Base de connaissances JavaScript
- Base de connaissances REST
- Connaissance de l'API de service Web cible
- Base de connaissances sur les connexions, les informations d'identification et les alias
- Rôle requis : développeur

Pourquoi et quand exécuter cette tâche

Utilisez un alias de connexion et d'informations d'identification et un algorithme basé sur l'authentification personnalisé pour l'authentification.

Procédure

1. Accédez à la **Tout** > **Informations d'identification et connexions** > **Algorithmes d'authentification**, puis cliquez sur **Nouveau**.
2. Renseignez les champs du formulaire.
   La sélection de base de données dans le champ **Format** détermine les champs qui sont disponibles.

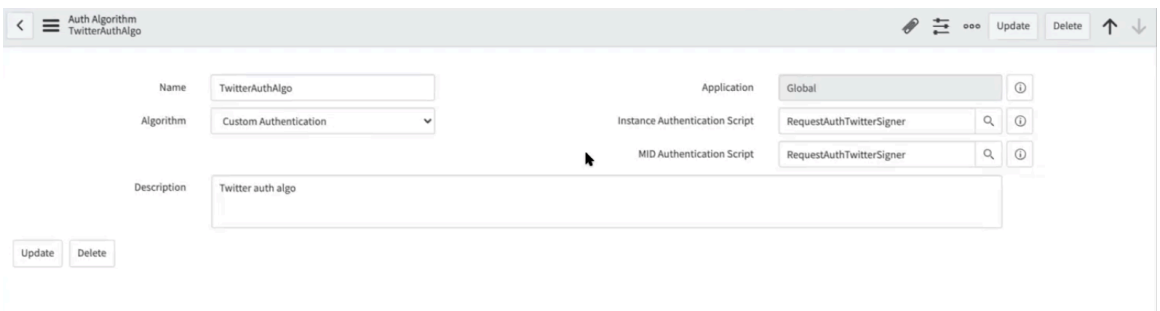
Formulaire d'authentification

Champ	Description
Nom	Nom unique de cet algorithme.
Algorithme	Type de demande sortante. Sélectionnez **Authentification personnalisée**.
Description	Description de l'action de votre algorithme.
Application	Périmètre dans lequel votre application s'exécute.
Script d'authentification d'instance	Script que vous sélectionnez dans la table Includes de script. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ Demande d'authentification interne ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner **Remarque :** ○ Pour en savoir plus sur le script, cliquez sur l'icône d'informations en regard du champ. Les détails du script tels que nom, nom de l'API, application, accessible depuis, script, etc. s'affichent. ○ En cas d'authentification personnalisée avec Twitter, vous pouvez choisir **RequestAuthTwitterSigner**, car il utilise une méthode d'authentification OAuth 1.0a. Cela nécessite des informations telles que **la clé API et le secret** , ainsi que **le jeton d'accès et le secret** qui peuvent être utilisés pour créer des signatures à transmettre dans un en-tête d'autorisation. Pour plus d'informations, consultez la section Authentification dans Twitter .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Script d'authentification MID	Script que vous sélectionnez dans la table Includes de script de Serveur MID [vue Détection]. Les scripts disponibles sont les suivants : ○ RequestAuthAWSV4Signataire ○ Demande d'authentification interne ○ RequestAuthSampleCustomSigner ○ RequestAuthTwitterSigner

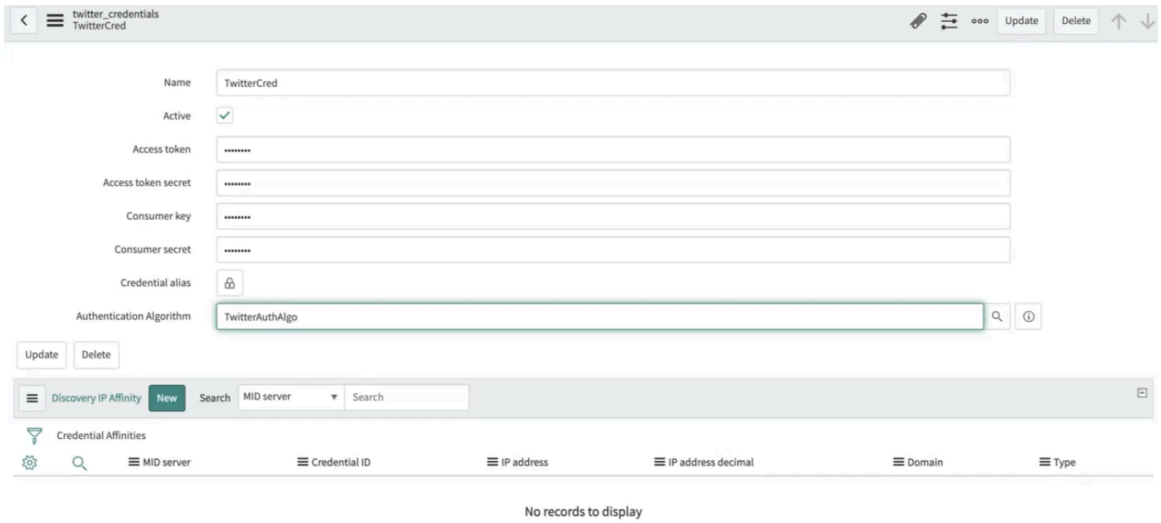


En fonction des scripts et de l'algorithme d'authentification sélectionnés, les informations d'identification configurées sont envoyées en tant que demande sortante du ServiceNow fournisseur.

3. Cliquez sur **Mettre à jour**.
4. Accédez à la **Tout** > **Connexions et informations d'identification** > **Informations d'identification**.
5. Cliquez sur **Nouveau**.
6. Créez Twitter des informations d'identification avec l'algorithme d'authentification.
   Dans ce cas, **TwitterAuthAlgo**.
7. Spécifiez les champs :
   - Nom
   - Actif
   - Jeton d'accès
   - Secret du jeton d'accès
   - Clé du consommateur
   - Secret du consommateur
   - Alias d'informations d'identification
   - Algorithme d'authentification

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



8. Cliquez sur **Mettre à jour**.

Example: Étape REST avec Twitter

En cas de Twitter, vous devez vous assurer que les spokes ou informations d'identification suivants sont disponibles :

- Jeton d'accès
- Secret du jeton d'accès
- Clé du consommateur
- Secret du consommateur
- Algorithme d'authentification

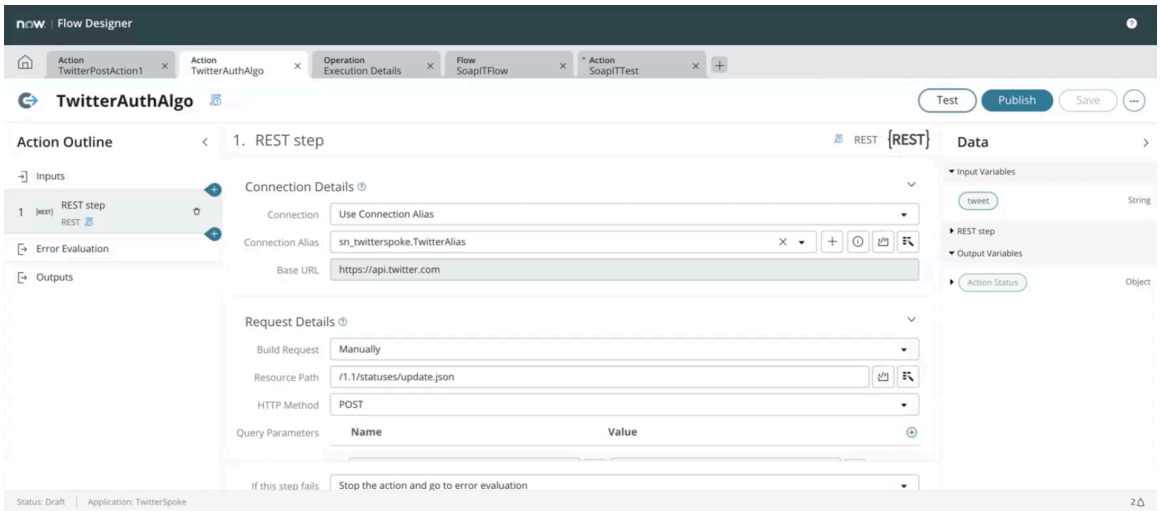
Action : TwitterAuthAlgo.

Entrez l'étape REST comme Twitter suit :

- **Alias des informations d'identification** : alias créé pour Twitter.
- **URL de base** : détails de l'URL de base à partir de Twitter.
- **Méthode HTTPS** : Dans ce cas, il s'agit de la méthode POST. Publier un tweet.
- **Paramètres de requête** : **action** en tant que **tweet**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Vous pouvez tester l'action. Le tweet est publié sur la Twitter page.

Vérifier la relation des services IP pour Discovery et Orchestration

Vous pouvez rechercher dans la table Services IP une liste d'adresses IP associées à un protocole.

Avant de commencer

Rôle requis : administrateur

Pourquoi et quand exécuter cette tâche

La table Services IP mappe un port sur un protocole. Plusieurs mappages sont fournis par défaut pour les combinaisons port-protocole couramment utilisées, tels que le port 80 pour HTTP, le port 22 pour SSH et le port 161 pour SNMP.

Une propriété système appelée `glide.discovery.ip_service_affinity` permet à Découverte de mémoriser le dernier port de l'adresse IP ayant été détecté. Par défaut, cette propriété est définie sur **faux**.

Important :
Vous ne devez pas modifier les services IP à moins que votre organisation n'utilise des ports personnalisés.

Procédure

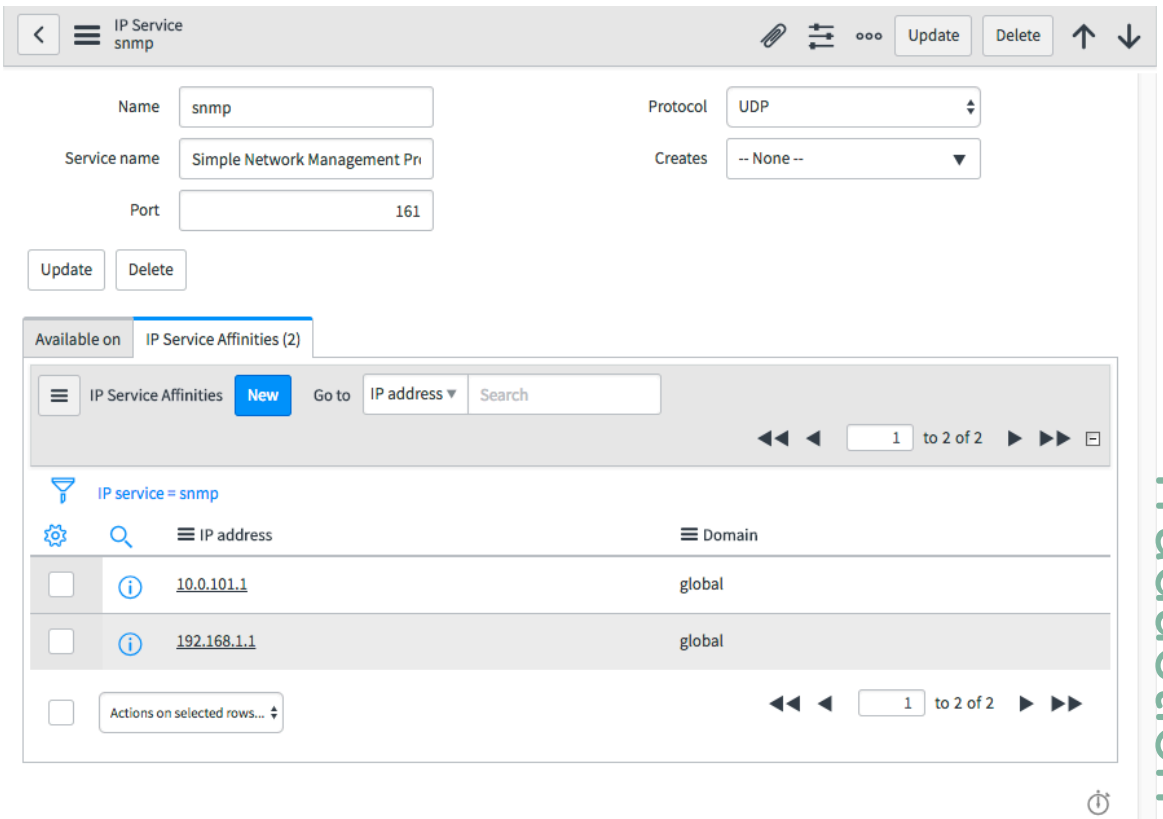
1. Accédez à la **Tout** > **Définition de découverte** > **Services IP**.
2. Filtrez la liste pour rechercher le service IP approprié.
3. Cliquez sur le nom du service pour accéder à la page de ce service IP.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Cliquez sur l'onglet **Relations des services IP** pour obtenir la liste d'adresses IP associées à ce service.

Relations des services IP



Contrôle d'accès ServiceNow®

Le module d'extension SNC Access Control (com.snc.snc_access_control) vous permet de contrôler quels Service et assistance client employés peuvent accéder à votre instance, et quand.

Explorer le contrôle d'accès ServiceNow



Activer le contrôle d'accès ServiceNow



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Découvrez les fonctionnalités du contrôle d'accès ServiceNow® .

Contrôle d'accès actif ServiceNow® .

Configurer le contrôle d'accès ServiceNow



Comprendre comment configurer ServiceNow® le contrôle d'accès.

Journalisation d'audit



Apprenez et examinez la journalisation des audits de contrôle d'accès ServiceNow® .

Traduction automatique

Explorer le ServiceNow® contrôle d'accès

Le module d'extension SNC Access Control (com.snc.snc_access_control) vous permet de contrôler quels Service et assistance client employés peuvent accéder à votre instance, et quand.

Lorsque vous activez le module d'extension pour la première fois, Service et assistance client les employés ne peuvent pas se connecter à l'instance. Tous les employés actuellement connectés Service et assistance client restent connectés. Dans la table Contrôle d'accès SNC, vous créez des enregistrements qui accordent l'accès à des employés SNC spécifiques ou à tous les employés.

Le module d'extension empêche Service et assistance client le personnel d'accéder aux instances sans votre autorisation expresse. Toutefois, d'autres membres du personnel d'exploitation autorisés ServiceNow , en leur capacité à prendre en charge et à gérer le produit et à vérifier l'utilisation, sont tenus d'effectuer des actions administratives sur l'infrastructure sous-jacente. Cette infrastructure comprend des serveurs et des bases de données, entre autres composants d'infrastructure qui composent la solution SaaS. Cette méthode d'accès est entièrement auditable et suivie.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ce module d'extension vous permet de restreindre l'accès à votre instance sans votre autorisation expresse, ce qui peut affecter les niveaux de service de support et le SLA de disponibilité. Le SLA de disponibilité est ensuite mesuré à partir du moment où le personnel de support est autorisé à accéder à votre instance.

Sécurité de connexion

La sécurité des connexions des employés autorisés Service et assistance client aux instances utilise des jetons chiffrés générés par un serveur sécurisé. Seuls les employés correctement authentifiés Service et assistance client ont accès à une instance. Sans le module d'extension SNC Access Control, le serveur de sécurité s'assure que les droits d'accès sont appliqués aux hi.service-now.com. Lorsque le module d'extension est activé, les jetons de connexion chiffrés doivent correspondre aux noms de la liste d'accès fournie par le module d'extension, à l'aide des critères définis dans ces enregistrements. Cette méthode d'authentification vous permet de déterminer précisément quels Service et assistance client employés peuvent accéder à leurs instances, et quand ces employés peuvent le faire.

L'architecture choisie pour ce système comporte plusieurs fonctionnalités conçues pour améliorer la sécurité de vos instances :

Serveur de sécurité

Le serveur de sécurité est un hôte Linux verrouillé auquel seul ServiceNow le personnel de sécurité peut accéder. Ce serveur est le seul système qui a accès à la clé de chiffrement privée critique nécessaire pour produire les jetons de connexion. En utilisant cette compartimentation (une pratique de sécurité standard), la clé privée est protégée, même dans le cas peu probable où un attaquant compromettrait l'instance HI.

Utilisateur synthétique

L'installation sur les instances qui permet aux employés autorisés Service et assistance client de se connecter à leur instance ne nécessite pas qu'un compte soit mis en service sur cette instance. Il n'existe aucun enregistrement utilisateur mis en service ni aucune information d'identification permanente ou persistante. Au lieu de cela, un utilisateur synthétique est créé pour chaque Service et assistance client connexion d'employé. Cet utilisateur n'existe qu'en mémoire et ne fournit aucun privilège permanent. Si le module d'extension Contrôle d'accès SNC est activé, vous pouvez retirer l'autorisation de n'importe quel Service et assistance client employé à tout moment.

Jetons

Les jetons de sécurité sont spécifiques à une instance et à un employé particulier Service et assistance client . De plus, le mécanisme qui génère les jetons ne fonctionne qu'avec les connexions réelles Service et assistance client des employés à HI, et non avec les utilisateurs dont l'identité a été empruntée. Une fois qu'un jeton de sécurité est généré, seul un employé spécifique Service et assistance client peut l'utiliser pour se connecter à une instance.

Limite de temps

Les jetons de sécurité expirent quatre heures après leur génération. Cette expiration limite l'utilité des jetons détournés, qui ne peuvent être utilisés que pendant cette courte période.

Connexion

Les connexions Service et assistance client des employés aux instances sont enregistrées en tant qu'événement de connexion.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Chaque action effectuée par l'employé connecté Service et assistance client est ajoutée au journal des transactions dans la base de données.
- Il est également ajouté au journal d'instance sur le système de fichiers, qui est inaccessible pour la plupart des ServiceNow employés.
- Service et assistance client Les connexions et les actions des employés sont facilement identifiables, car les noms d'utilisateur se terminent tous par @snc (comme frodo.baggins@snc).

Ces actions vous fournissent une journalisation de sécurité facile à utiliser, robuste et fiable pour l'accès des non-employés.

Flux de traitement de sécurité

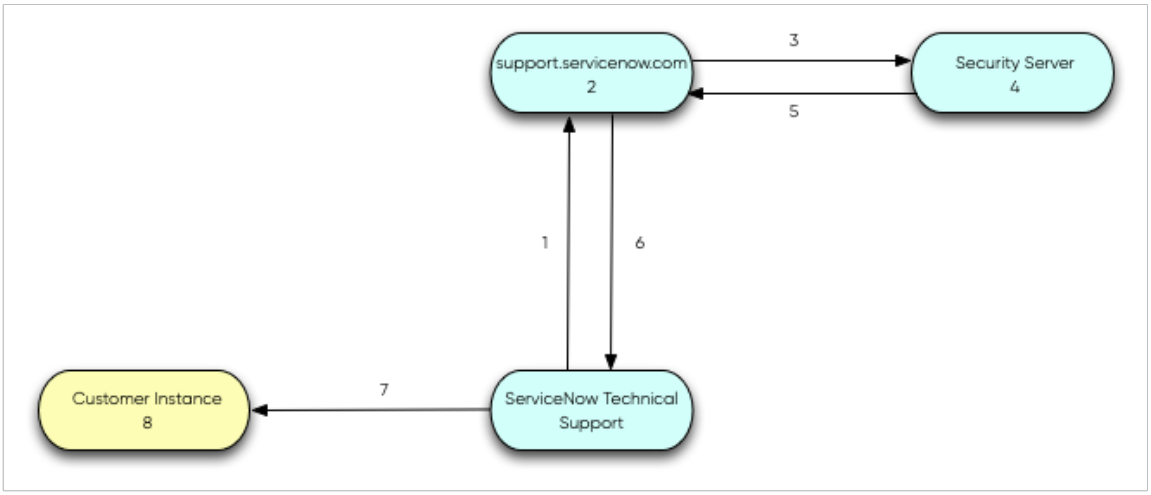
Lorsqu'un Service et assistance client employé veut se connecter à une instance, le flux de traitement de la sécurité est le suivant :

1. Un Service et assistance client technicien demande une connexion pour l'instance via hi.service-now.com.
2. HI vérifie que le technicien dispose du rôle approprié autorisant l'accès aux instances.
3. Si l'utilisateur dispose du rôle approprié, HI envoie la demande d'accès au serveur de sécurité.
4. Le serveur de sécurité vérifie que la demande provient de l'adresse IP HI et évalue la demande (utilisateur, rôle et adresse IP du demandeur). Si la demande est valide, le serveur de sécurité l'approuve et construit un jeton. Ce jeton contient le nom d'utilisateur, les rôles, l'ID de l'instance et l'heure (le début de la durée de vie du jeton de 4 heures). Enfin, le serveur de sécurité crypte le jeton avec la clé de chiffrement privée.
5. Le serveur de sécurité envoie le jeton chiffré à HI.
6. Hi envoie le jeton au navigateur du technicien de support.
7. Le navigateur du technicien de support initie une connexion à l'instance à l'aide du nom d'utilisateur spécial se terminant par @snc.
8. L'instance utilise la clé publique pour déchiffrer le jeton. Pour vérifier le jeton, l'instance le met en correspondance avec le nom d'utilisateur fourni à l'étape précédente, l'ID de l'instance et la fenêtre de temps autorisée. Si le module d'extension SNC Access Control est activé, l'instance vérifie que l'utilisateur est :
   - Énuméré(e/s)
   - Actif
   - Configuré pour accéder à l'instance dans la fenêtre horaire actuelle
9. Si l'utilisateur est authentifié, l'instance crée un *utilisateur synthétique* en mémoire avec les rôles donnés. Cet utilisateur ne persiste pas après l'expiration de la limite de temps, la déconnexion de l'utilisateur ou le redémarrage de l'instance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ServiceNow Flux de processus d'accès de sécurité



Journalisation d'audit

La connexion suivante permet de suivre les connexions et l'activité des Service et assistance client employés :

- Journaux des événements : les journaux des événements affichent toutes les Service et assistance client connexions à une instance.
- Journaux de transactions : les journaux de transactions affichent toute l'activité sur l'instance, y compris toute tentative de suppression de journal.

Remarque :
Pour en savoir plus sur ce module d'extension, consultez Module d'extension du contrôle d'accès SNC Paramètres de renforcement de la sécurité de l'instance.

Activation du contrôle d'accès ServiceNow®

Vous demandez l'activation du module d'extension SNC Access Control (com.snc.snc_access_control).

Avant de commencer

Rôle requis : admin

Pourquoi et quand exécuter cette tâche

Il existe deux façons de demander un module d'extension :

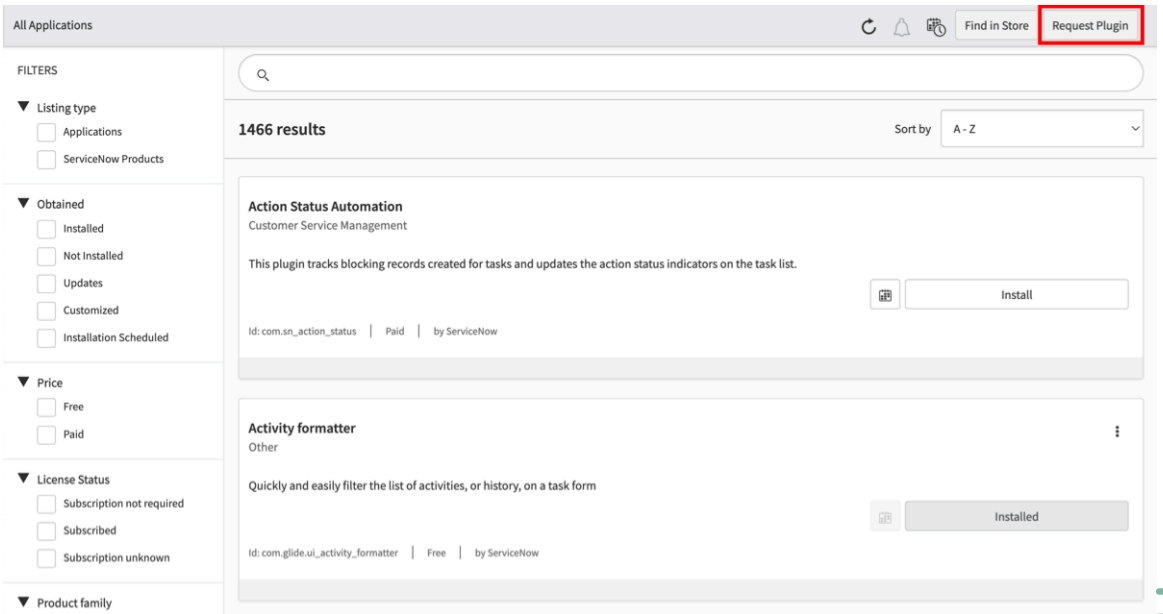
- Accéder directement au Catalogue de services de Now Support en sélectionnant **Tout** > **Catalogue de services** > **Activer le module d'extension** sur Now Support.
- Accéder au Catalogue de services de Now Support via la page Toutes les applications de votre instance en suivant ces étapes.

Procédure

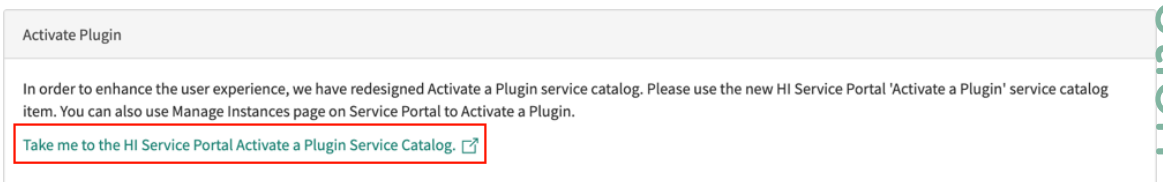
1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Sur la page Toutes les applications, sélectionnez **Demander un module d'extension** pour ouvrir le formulaire **Activer le module d'extension** sur Now Support.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Dans Now Support, sélectionnez le lien pour accéder à Now Support Portail de services Catalogue de services.



4. Sélectionnez votre instance.
5. Sélectionnez **Actions > Activer le module d'extension**.
6. Sur le formulaire **Activer le module d'extension**, fournissez les informations suivantes.

Formulaire Activer le module d'extension

Champ	Description
Quelle est votre instance cible	Instance sur laquelle activer le module d'extension.
Quel module d'extension voulez-vous activer	Nom du module d'extension à activer. **Remarque :** Si le système ne répertorie pas le module d'extension que vous souhaitez ou si vous activez le module d'extension sur une instance OEM ou sur site, cochez la case **Le module d'extension que je recherche n'est pas répertorié** puis saisissez le nom du module d'extension.

Traduction automatique

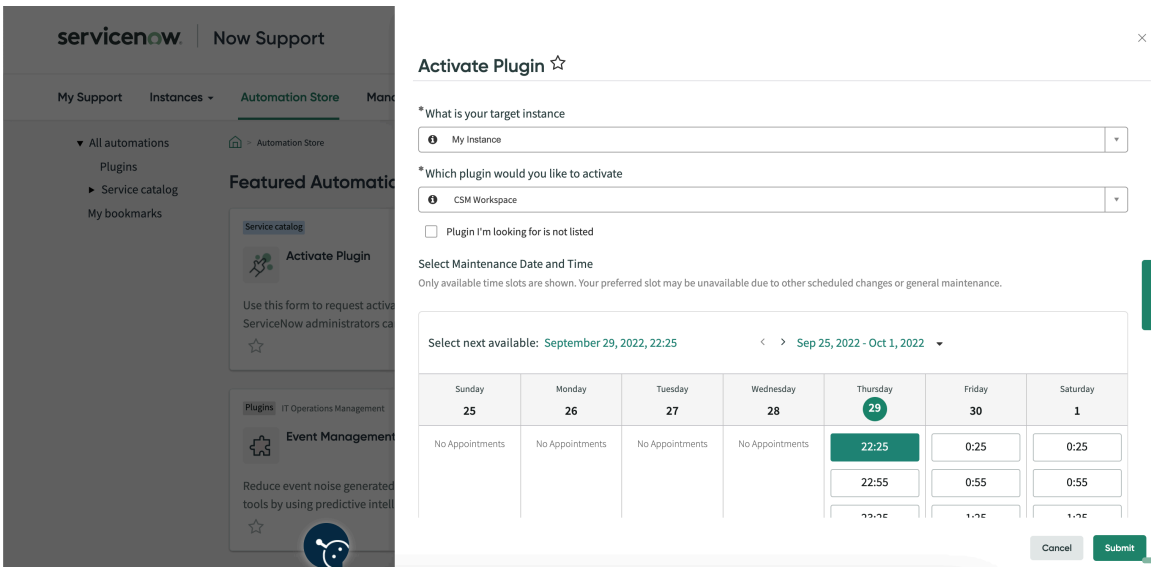
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner la date et l'heure de maintenance	Date et heure d'activation du module d'extension. **Remarque :** Les modules d'extension sont activés deux fois par jour ouvrable (une fois le matin et une fois le soir dans le fuseau horaire du Pacifique). Si le module d'extension doit être activé à un moment précis, indiquez cette demande dans le champ **Motif/commentaires**.

Example

Par exemple, consultez le formulaire suivant pour activer le module d'extension CSM Workspace sur une instance nommée Mon instance.

Formulaire Activer le module d'extension



7. Sélectionnez **Envoyer**.
   Pour plus de détails sur la demande d'un module d'extension, consultez l'article Requesting a Plugin from the Service Catalog [KB0751715] de la Now Support Base de connaissances.

Configuration ServiceNow® du contrôle d'accès

Configurez un enregistrement de contrôle d'accès pour spécifier un ou plusieurs Service et assistance client employés qui ont l'autorisation de se connecter à votre instance.

Avant de commencer

Rôle requis : administrateur

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pourquoi et quand exécuter cette tâche

Remarque :
Le module d'extension SNC Access Control (com.snc.snc_access_control) empêche Service et assistance client le personnel d'accéder aux instances sans votre autorisation expresse. Toutefois, d'autres membres du personnel d'exploitation autorisés ServiceNow , en leur capacité à soutenir et à gérer le produit, sont tenus d'effectuer des actions administratives sur l'infrastructure sous-jacente. Cette infrastructure comprend des serveurs et des bases de données, entre autres composants d'infrastructure qui composent la solution SaaS. Cette méthode d'accès est entièrement auditable et suivie.

Ce module d'extension vous permet de restreindre l'accès à votre instance sans votre autorisation expresse, ce qui peut affecter les niveaux de service de support et le SLA de disponibilité. Le SLA de disponibilité est ensuite mesuré à partir du moment où le personnel de support est autorisé à accéder à votre instance.

Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Contrôle d'accès SNC**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs de formulaire (consultez la table).
4. Cliquez sur **Envoyer**.

Contrôle d'accès SNC

Champs de formulaire	Description
Nom	Nomme chaque Service et assistance client employé qui a l'autorisation de se connecter dans cette instance. ○ Exprimez les noms comme prénom.nom en minuscules, séparés par un point (par exemple, jean.dupont). Chaque nom doit avoir un enregistrement utilisateur correspondant dans *support.servicenow.com*. ○ Si plusieurs employés ont l'autorisation Service et assistance client de se connecter dans cette instance, saisissez plusieurs noms et séparez-les par des virgules. ○ Pour permettre à tous les Service et assistance client employés d'accéder à l'instance en signe de droit de connexion, saisissez un astérisque (*) à la place du nom. ○ Si vous avez l'intention de restreindre l'accès des Service et assistance client employés à l'instance, les valeurs du champ **Nom** ne doivent être marquées d'un astérisque (*) nulle part dans le champ.
Motif	Champ lisible par l'homme qui décrit la raison pour laquelle vous accordez l'autorisation d'accès. Ce champ est facultatif.
Début	Spécifie la date et l'heure de début de la période pendant laquelle les employés spécifiés Service et assistance client ont accès à la connexion. Ce champ est obligatoire.
Fin	Spécifie la date et l'heure de fin de la période pendant laquelle les employés spécifiés Service et assistance client ont accès à la connexion. Ce champ est obligatoire.
Actif	Contrôle si cet enregistrement d'autorisation est actif. La valeur par défaut est Actif.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journalisation d’audit

La connexion suivante suit les connexions et l’activité des ServiceNow employés.

Journaux des événements	Les journaux d’événements affichent toutes les ServiceNow connexions à une instance client.
Journaux de transactions	Les journaux des transactions affichent toute l’activité sur l’instance, y compris tous les efforts de suppression des journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Identité

En savoir plus sur les identités dans l'instance.

Analyseur d'accès



Access Analyzer est un ServiceNow® App Store qui est un outil de diagnostic d'accès qui permet de déterminer qui a accès à une ressource.

Identité globale



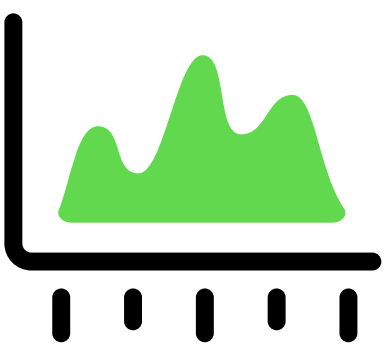
Global Identity est une application ServiceNow® de stockage qui permet de mettre à jour les attributs d'utilisateur d'une instance à l'autre (plusieurs instances).

Identity Center



Identity Center vous permet de surveiller, de gérer et de minimiser les risques et les failles de sécurité liés à l'identité.

Système de gestion des identités entre domaines (SCIM)



Audit d'identité et d'accès



Utilisez l'audit d'identité et d'accès pour comprendre les changements apportés à un utilisateur, un groupe, un rôle et une ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L’API SCIM (System for Cross-domain Identity Management) fournit des points de terminaison pour créer, lire, mettre à jour et supprimer des opérations sur les utilisateurs et les groupes à l’aide du protocole SCIM.

Analyseur d'accès

ServiceNow® L’analyseur d’accès est un outil de diagnostic d’accès qui permet d’afficher les autorisations d’une identité pour une ressource.

Explorer



Découvrez les fonctionnalités et la valeur commerciale d’Access Analyzer.

Utiliser



Comprendre comment utiliser l’analyseur d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluation de l’autorisation



Savoir comment les autorisations sont évaluées

Forum Aux Questions



Obtenez des détails sur les questions fréquemment posées sur l’analyseur d’accès.

Exploration d’Access Analyzer

Analysez les identités sur l’instance ServiceNow .

ServiceNow L’analyseur d’accès est une application qui aide les administrateurs à afficher les autorisations pour l’utilisateur, le rôle ou le groupe sélectionné.

Remarque :

- Access Analyzer est un produit de l’App ServiceNow Store. Visitez le site Web ServiceNow Store pour découvrir toutes les applications disponibles et obtenir des informations sur la procédure à suivre pour soumettre des demandes à la boutique.
- L’analyseur d’accès emprunte l’identité de l’enregistrement d’identité pour récupérer les détails des autorisations et ne lit ni ne stocke aucune donnée personnelle ou sensible de l’identité.
- Les résultats de l’évaluation de l’analyseur d’accès sont les mêmes, quelles que soient les politiques d’accès définies pour les utilisateurs, telles que l’accès zéro confiance (ZTA). Les politiques ne sont évaluées que lors de la connexion réelle de l’utilisateur et ne le sont pas pendant le flux d’analyseur d’accès.
- L’analyseur d’accès a des limites dans l’évaluation précise de l’accès des ressources liées aux ressources de champ d’application gérées et au développeur délégué.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluer l'accès

Évaluer l'accès est une fonctionnalité de l'analyseur d'accès ServiceNow qui aide les administrateurs à afficher les autorisations pour l'utilisateur, le rôle ou le groupe sélectionné.

Il vous permet d'analyser et d'afficher les autorisations des utilisateurs, des groupes, des rôles d'une table, des includes de script pouvant être appelés par un client, des pages de l'interface utilisateur et des points de terminaison REST.

À l'aide d'Access Analyzer, les organisations peuvent améliorer leur posture de sécurité, leur gouvernance des identités et leur gestion des risques, atteindre leurs objectifs de conformité et comprendre qui (identité) a accès à quoi (ressources).

Comparer l'accès

Comparer l'accès est une fonctionnalité de l'analyseur d'accès ServiceNow V2 qui permet aux administrateurs de comparer l'accès des utilisateurs et de déterminer le niveau d'accès approprié pour les utilisateurs de votre ServiceNow instance.

Comparer L'accès peut être effectué entre les utilisateurs pour les enregistrements utilisateur et le contrôle d'accès.

Comparer l'accès vous permet d'effectuer l'analyse suivante :

- Niveau 1 : comparez les enregistrements des utilisateurs pour comprendre les attributs, les rôles et les groupes.
- Niveau 2 : comparez les contrôles d'accès pour exécuter l'analyse de la cause première en identifiant les problèmes d'accès.

Avantages

Voici quelques-uns des avantages de l'utilisation de l'analyseur d'accès :

- Analyser l'accès aux ressources (tables).
- Comparez l'accès de 2 utilisateurs.
- Comparez les rôles et les groupes de 2 utilisateurs.
- Générez un rapport indiquant si une identité a accès à une ressource (table).
- Identifiez qui a accès à des questions d'hygiène de sécurité critiques.
- Aide à empêcher le surprovisionnement des autorisations.
- Obtenez les principaux de privilèges minimum lors de l'implémentation de contrôles d'accès.
- Limitez l'accès à certaines données, notamment les applications, les tables, les lignes ou les colonnes et d'autres ressources.
- Fournissez des options de génération de rapports pour les résultats de l'analyseur.
- Comparez l'accès entre les enregistrements utilisateur et les contrôles d'accès.
- Déterminez le niveau d'accès approprié pour les utilisateurs sur votre ServiceNow instance.

Utilisation de l'analyseur d'accès

Analysez les identités et leur accès sur l'instance ServiceNow® .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôle requis : administrateur

La procédure suivante décrit les étapes d'accès à Access Analyzer et d'utilisation de diverses fonctionnalités dans Access Analyzer.

Remarque :
Access Analyzer est un produit de l'App ServiceNow® Store.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.

   Access Analyzer possède les fonctionnalités suivantes :

   - Évaluer l'accès
   - Comparer les enregistrements de l'utilisateur
   - Comparer les contrôles d'accès

2. Sélectionnez l'onglet correspondant à l'utilisation de l'analyseur d'accès en fonction de vos besoins.

Utilisation de l'évaluation de l'accès

Analysez les identités sur l'instance ServiceNow® .

Avant de commencer
Rôle requis : administrateur

La procédure suivante décrit les étapes d'accès à Évaluer l'accès dans l'analyseur d'accès et d'utilisation de ses différentes fonctionnalités.

Remarque :
Access Analyzer est un ServiceNow Store produit.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez l'onglet **Évaluer l'accès** .
3. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse de l'accès et des autorisations

Champ	Description
Analyser par *	Analyser l'accès d'un utilisateur, d'un rôle ou d'un groupe
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

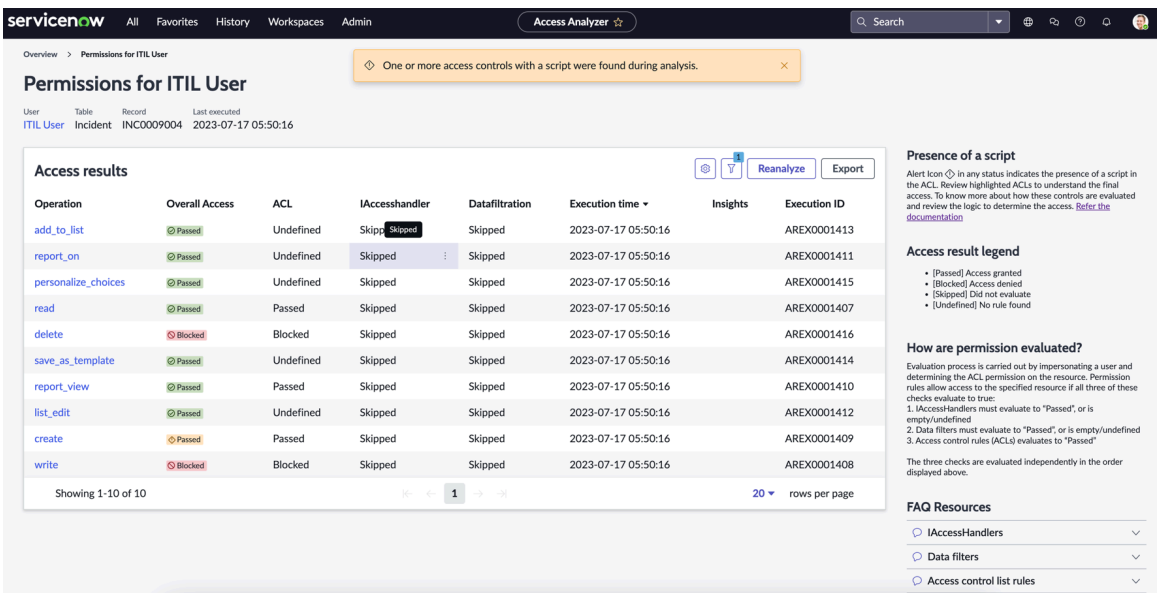
Champ	Description
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste.

4. Spécifiez la description dans le champ **Description** .
5. Sélectionnez **Analyser les autorisations**.

   Les résultats d'accès de l'utilisateur s'affichent. De même, vous pouvez analyser les autorisations d'un groupe ou d'un rôle pour les types de règles suivants :

   - Table (enregistrement)
   - Les scripts clients pouvant être appelés comprennent
   - Points de terminaison REST

   Les résultats des accès s'affichent.



La table Résultats de l'accès comprend les champs suivants :

Résultats des accès

Champs	Description
Opération	Type d'opération que l'utilisateur, le groupe ou le rôle peut effectuer pour la table, l'enregistrement ou le champ sélectionné.
Accès global	Résultat de l'accès global. Les résultats sont les suivants : ○ [Réussi] Accès accordé ○ [Bloqué] Accès refusé ○ [Ignoré] N'a pas évalué ○ [Non défini] Aucune règle trouvée

Traduction automatique

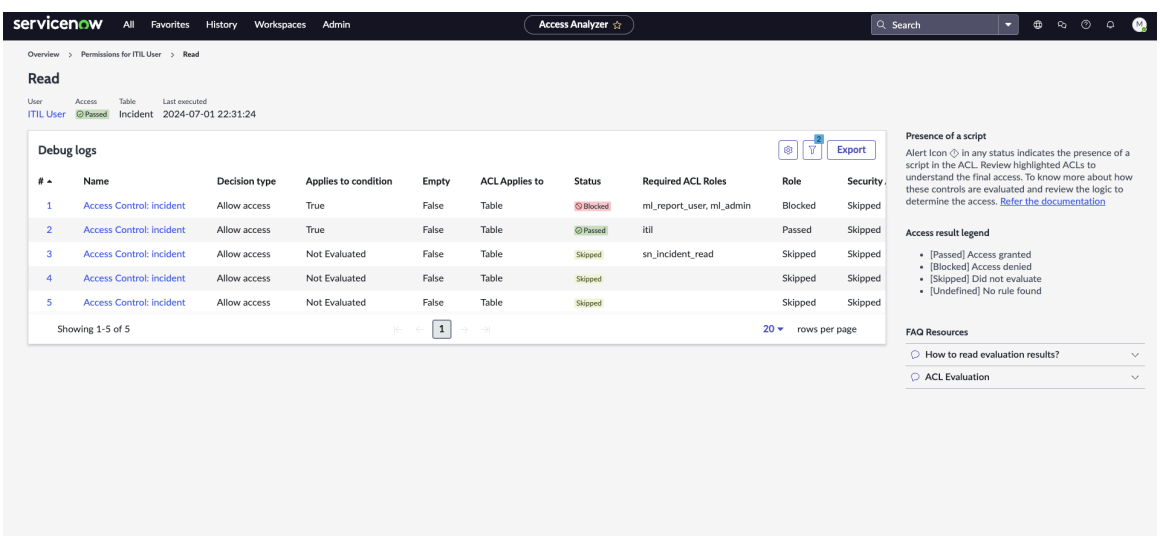
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
ACL	Indique si une ACL est définie pour l'opération sélectionnée.
IAccessHandler	Un contrôle interne du système à l'aide du code source masqué sur la plateforme. IAccessHandler peut accorder ou refuser l'accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées.
Filtrage des données	Un filtre de données est une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance.
Temps d'exécution	Heure à laquelle les résultats d'accès ont été exécutés.
Aperçus	Plus d'informations sur l'opération sélectionnée.
ID d'exécution	ID unique pour chaque exécution de résultat d'accès.

6. Sélectionnez l'opération pour plus d'informations sur l'ACL.
   Par exemple, si vous sélectionnez **lecture**, le contrôle d'accès lié à la lecture s'affiche.

Détails ACL

Champ	Description
Nom	Nom de l'ACL.
Type de décision	Type de décision configuré pour l'ACL. **Autorisez ourefusez l'accès**.
S'applique à la condition	Indique si l'ACL est appliquée à une condition.
ACL s'applique à	Détails sur la ressource à laquelle l'ACL est appliquée.
Statut	État de l'ACL ou du résultat de l'accès.
Rôles ACL requis	Détails du rôle requis pour accéder à la ressource.
Rôle	État du rôle. Réussi, ignoré ou bloqué.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Afficher les autorisations d'un utilisateur

Utilisez l'analyseur d'accès pour afficher les autorisations d'un utilisateur sélectionné.

Avant de commencer
Rôle requis : administrateur

La procédure suivante décrit les exemples d'étapes permettant d'afficher les autorisations d'un utilisateur sélectionné (**utilisateur ITIL**) pour afficher les autorisations de la table **Incident** à l'aide de l'évaluation de l'accès dans l'analyseur d'accès.

Remarque :
Access Analyzer est un produit de l'App ServiceNow® Store.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

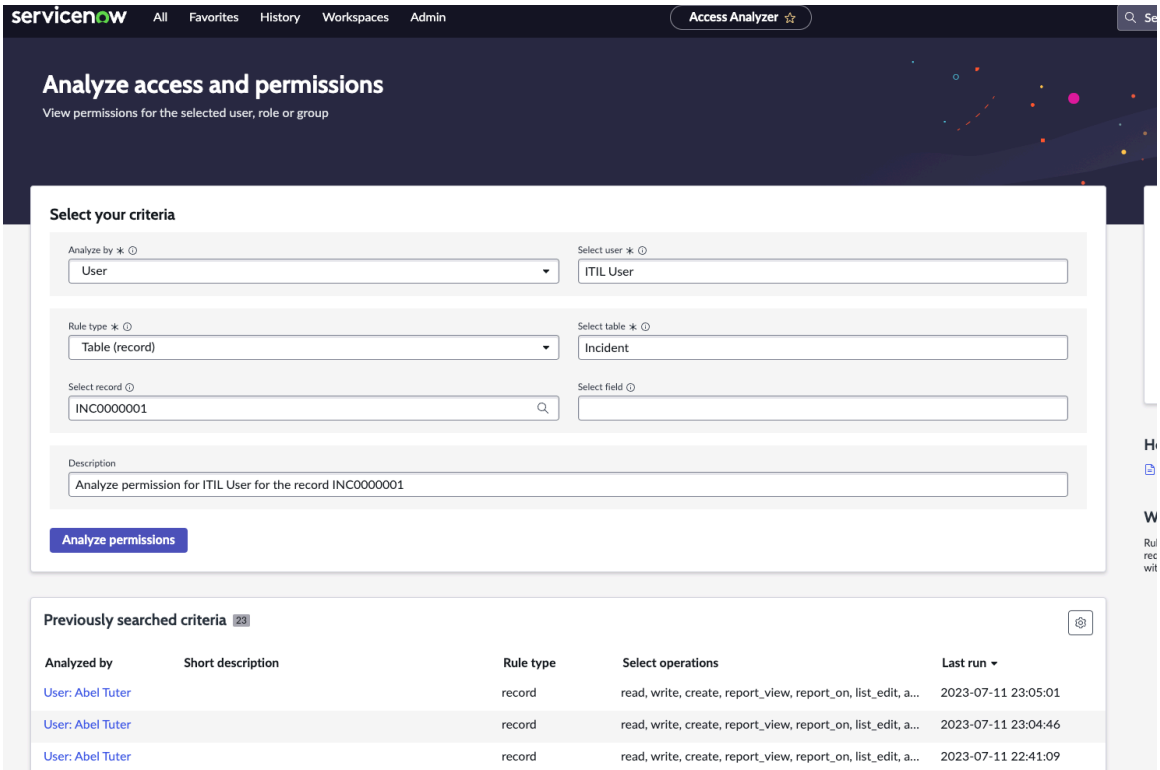
Sélectionnez vos critères d'analyse de l'accès et des autorisations

Champ	Description
Analyser par *	Sélectionner **Utilisateur**.
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **il s'agit de l'utilisateur ITIL**.
Type de règle *	Analysez l'accès pour une **table**, une **page d'interface utilisateur**, un **point de terminaison REST** ou un **include de script de client pouvant être appelé**. Dans l'exemple, Table.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste. Dans cet exemple, **INC0000001**.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ permet d'analyser l'autorisation, même au niveau du champ. Par exemple, Actif, Créé par, etc.

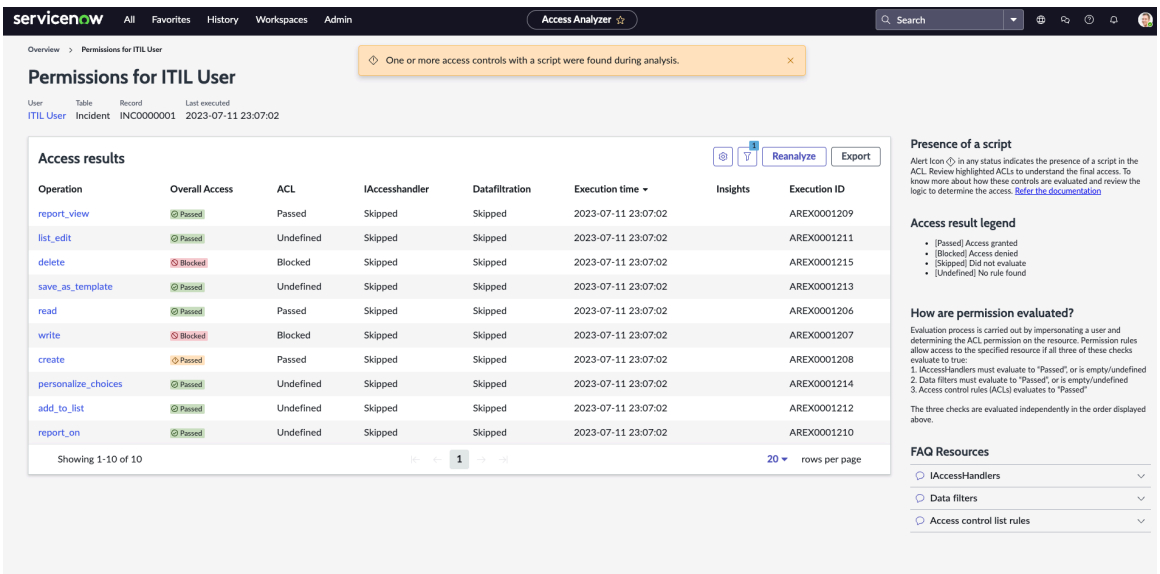
3. Spécifiez la description dans le champ **Description** .
4. Sélectionnez **Analyser les autorisations**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les **résultats de l'accès** pour l'utilisateur **ITIL** s'affichent.



Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), IAccesshandler et Données.

Prenons l'exemple de l'opération de **lecture** . Pour **l'utilisateur ITIL** , l'accès global est réussi, ce qui signifie que l'utilisateur est en mesure de lire l'enregistrement avec les autorisations appropriées (ACL).

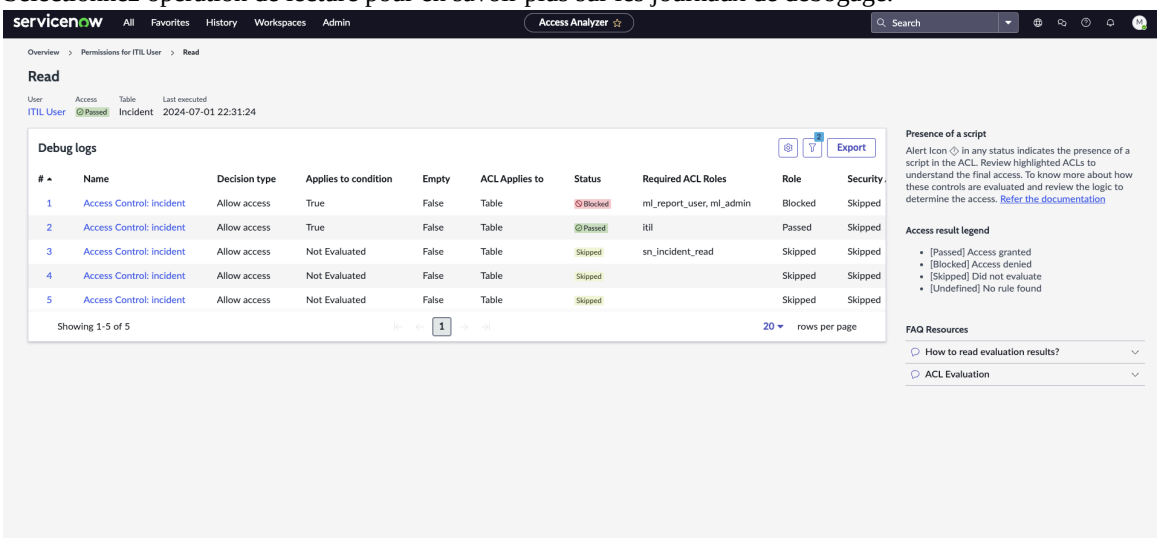
De même, pour l'opération de **création** , l'accès global est transmis avec une icône d'alerte, ce qui signifie qu'il peut y avoir une présence de script pour l'évaluation de l'ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Dans l'exemple, les opérations **d'écriture** et de **suppression** sont bloquées pour l'utilisateur sélectionné et l'utilisateur ne peut pas modifier ou supprimer l'enregistrement sélectionné (INC0000001).

5. Sélectionnez opération de lecture pour en savoir plus sur les journaux de débogage.

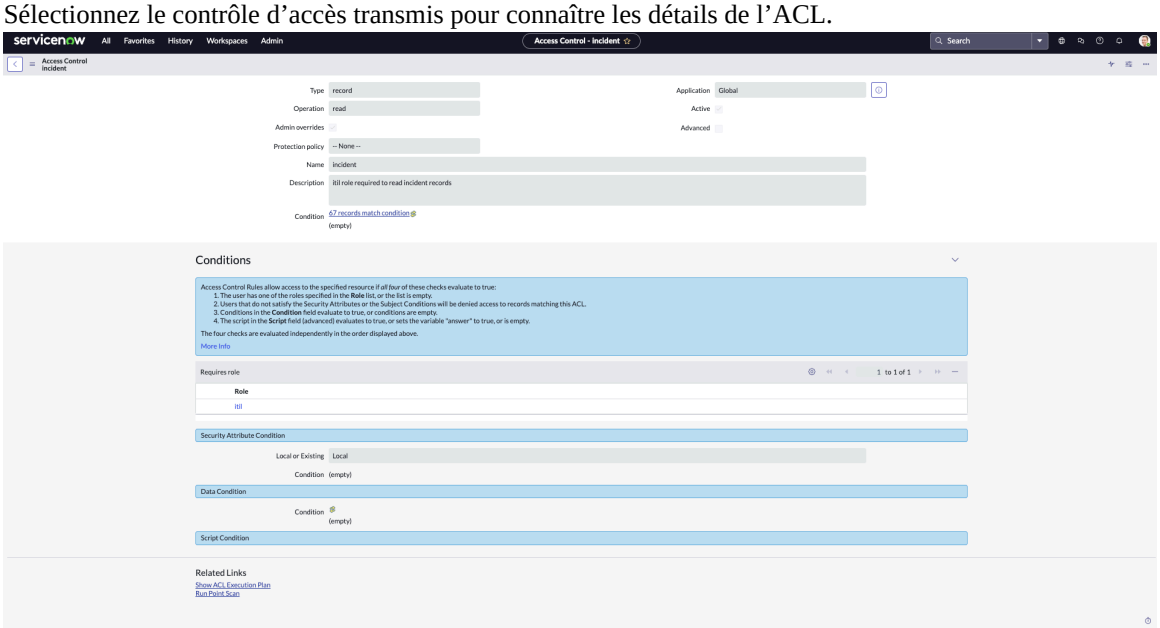


La page Journaux de débogage affiche la règle métier et les ACL associées requises pour effectuer l'opération **de lecture** pour l'enregistrement.

Les journaux de débogage indiquent qu'une règle métier et 4 ACL sont associées pour l'opération de lecture.

Il existe un état **Réussi** pour l'une des ACL, ce qui signifie que pour lire l'enregistrement sélectionné, l'utilisateur dispose de l'ACL requise et peut lire l'enregistrement. Étant donné qu'une des évaluations ACL est **réussie,** les autres évaluations ACL sont **ignorées**.

6. Sélectionnez le contrôle d'accès transmis pour connaître les détails de l'ACL.

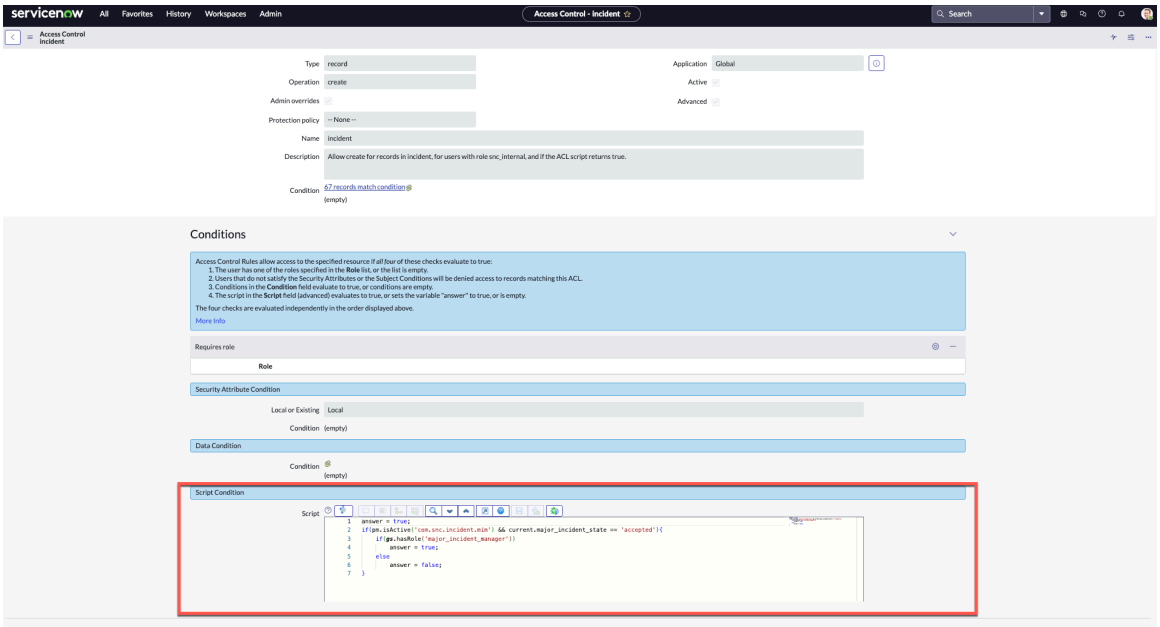


Les détails du contrôle d'accès pour l'ACL sélectionnée s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour une opération sélectionnée avec le **Réussi** et la présence d'un script. La page Contrôle d'accès affiche le script associé à l'enregistrement.



Afficher les autorisations pour un rôle

Utilisez l'analyseur d'accès pour afficher les autorisations d'un rôle sélectionné.

Avant de commencer

Rôle requis : administrateur

La procédure suivante décrit les exemples d'étapes permettant d'afficher les autorisations d'un rôle sélectionné (**user_admin**) pour afficher l'autorisation d'un point de terminaison d'API REST à l'aide de l'évaluation de l'accès dans l'analyseur d'accès.

Remarque :
Access Analyzer est un produit de l'App ServiceNow® Store.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse de l'accès et des autorisations

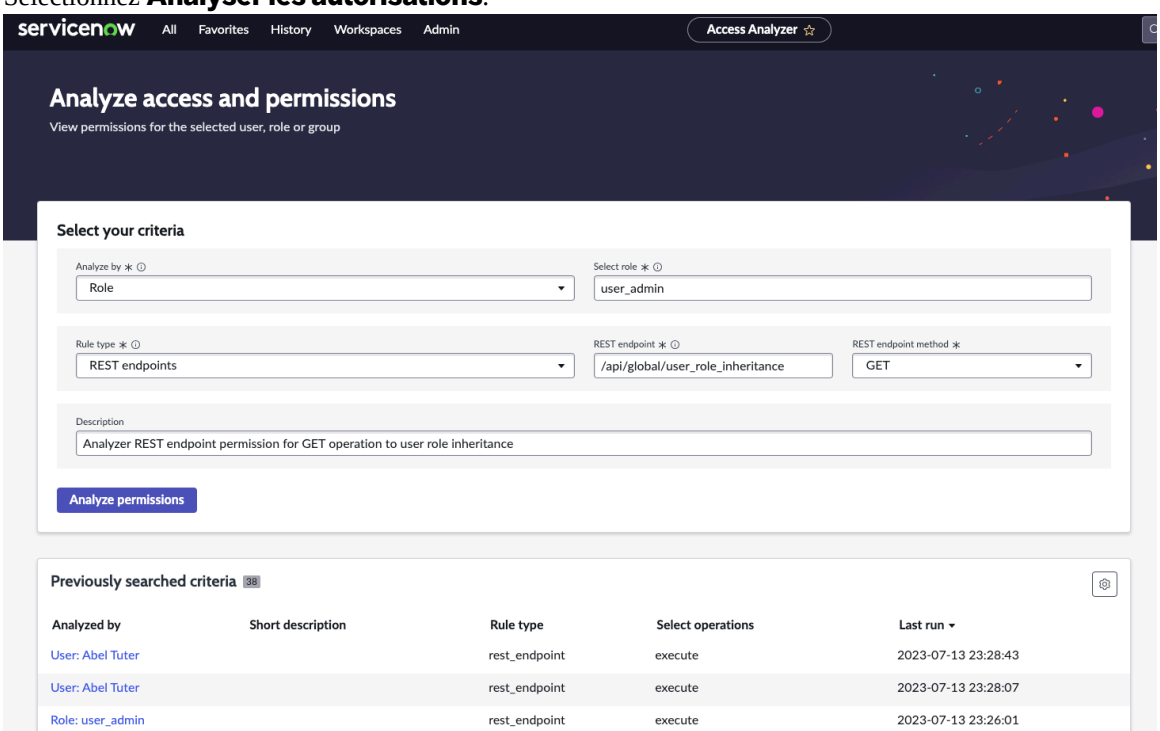
Champ	Description
Analyser par *	Sélectionnez **Rôle**.
Sélectionner un utilisateur *	Spécifiez un rôle à sélectionner dans la liste. Par exemple, **user_admin**.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé. Par exemple, **Point de terminaison REST**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Point de terminaison REST*	Spécifiez un point de terminaison REST. Par exemple, /api/global/user_role_inheritance. **Remarque :** Le point de terminaison REST complet doit être utilisé lors de l'utilisation du champ sélectionné.
Méthode de point de terminaison REST*	Spécifiez une méthode de point de terminaison REST. Par exemple, GET.

3. Spécifiez la description dans le champ **Description** .
4. Sélectionnez **Analyser les autorisations**.



Les **résultats de l'accès** pour le **rôle user_admin** s'affichent.

Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), IAccesshandler et Données.

L'accès global pour le rôle est transmis, ce qui signifie que le rôle (**user_admin**) est en mesure d'accéder au **point de terminaison REST** pour la méthode **GET** sélectionnée.

Afficher les autorisations pour un groupe

Utilisez l'analyseur d'accès pour afficher les autorisations d'un groupe sélectionné.

Avant de commencer
Rôle requis : administrateur

La procédure suivante décrit les exemples d'étapes permettant d'afficher les autorisations d'un groupe sélectionné (**Gestion des incidents**) pour afficher les autorisations d'une page **d'interface utilisateur d'incident** à l'aide de l'évaluation de l'accès dans l'analyseur d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Access Analyzer est un produit de l'App ServiceNow® Store.

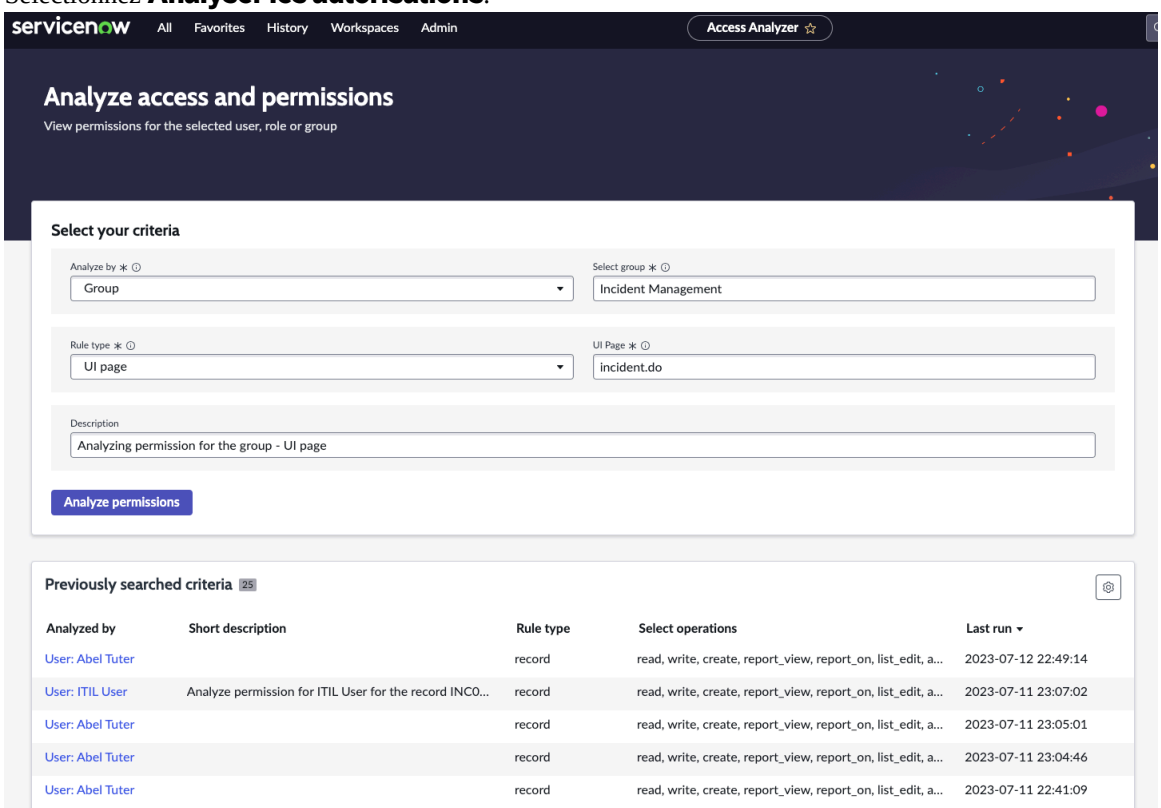
Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse de l'accès et des autorisations

Champ	Description
Analyser par *	Sélectionnez **un groupe**.
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Par exemple, **Gestion des incidents**.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé. Par exemple, **page de l'interface utilisateur**.
Page de l'interface utilisateur *	Spécifiez la page de l'interface utilisateur. Par exemple, **incident.do**.

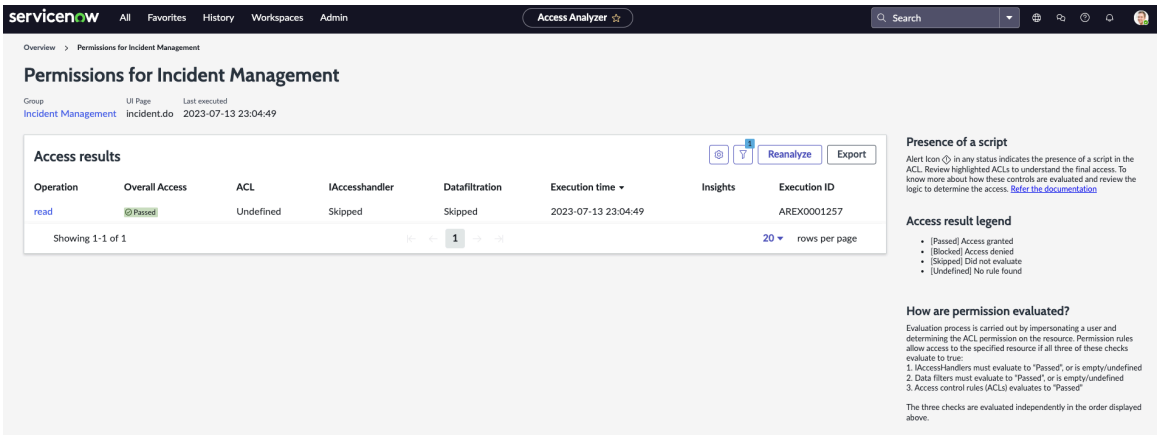
3. Spécifiez la description dans le champ **Description** .
4. Sélectionnez **Analyser les autorisations**.



Les **résultats de l'accès** pour le groupe **Gestion des incidents** s'affichent.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les résultats peuvent être lus en se référant aux filtres Légendes, Liste de contrôle d'accès (ACL), IAccesshandler et Données.

L'accès global du groupe est transmis, ce qui signifie que les utilisateurs du groupe (**Gestion des incidents**) peuvent accéder à l'enregistrement de l'incident.

Exporter les requêtes de l'analyseur d'accès

Exportez les requêtes analysées à l'aide d'Access Analyzer.

Avant de commencer

Rôle requis : administrateur

La procédure suivante décrit les étapes d'accès à Access Analyzer et d'utilisation de diverses fonctionnalités dans Access Analyzer.

Remarque :
Access Analyzer est un produit de l'App ServiceNow® Store.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez vos critères comme suit :

Sélectionnez vos critères d'analyse de l'accès et des autorisations

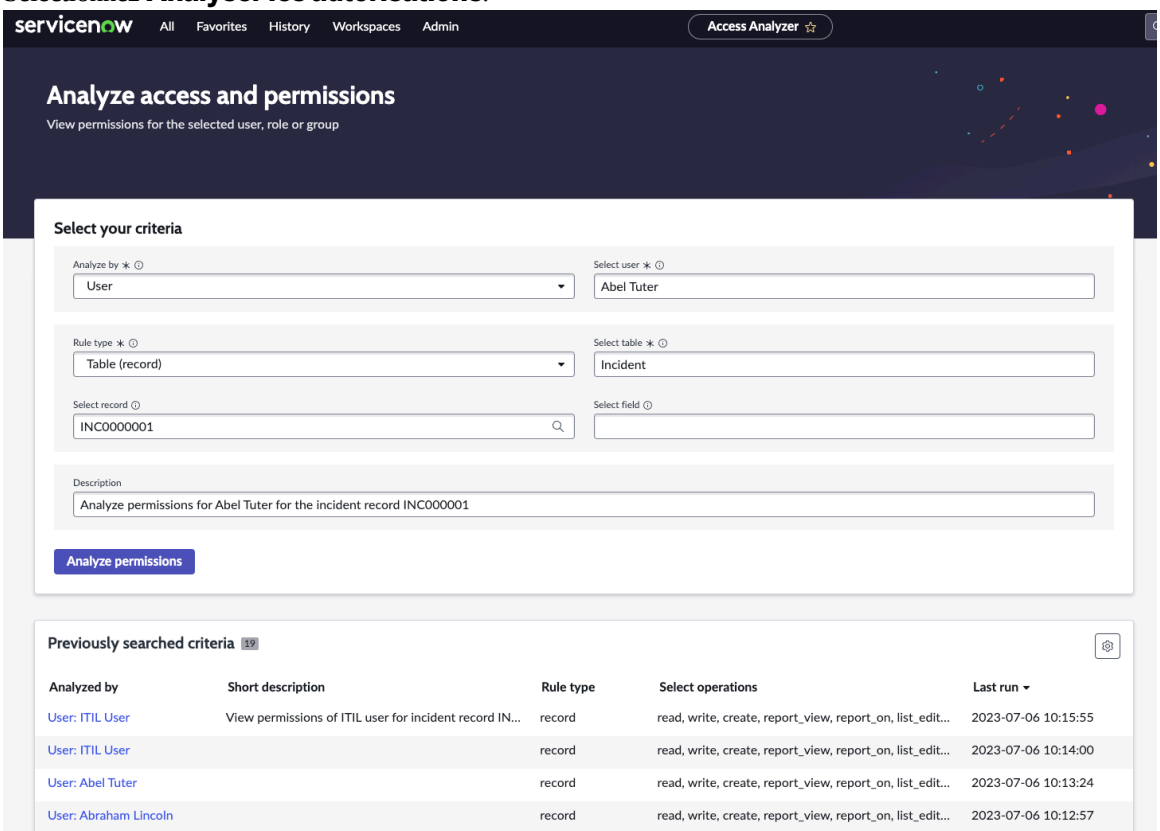
Champ	Description
Analyser par *	Analyser l'accès d'un utilisateur, d'un rôle ou d'un groupe
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste.
Type de règle *	Analysez l'accès pour une table, une page d'interface utilisateur, un point de terminaison REST ou un include de script de client pouvant être appelé.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste.

3. Spécifiez la description dans le champ **Description** .
4. Sélectionnez **Analyser les autorisations**.



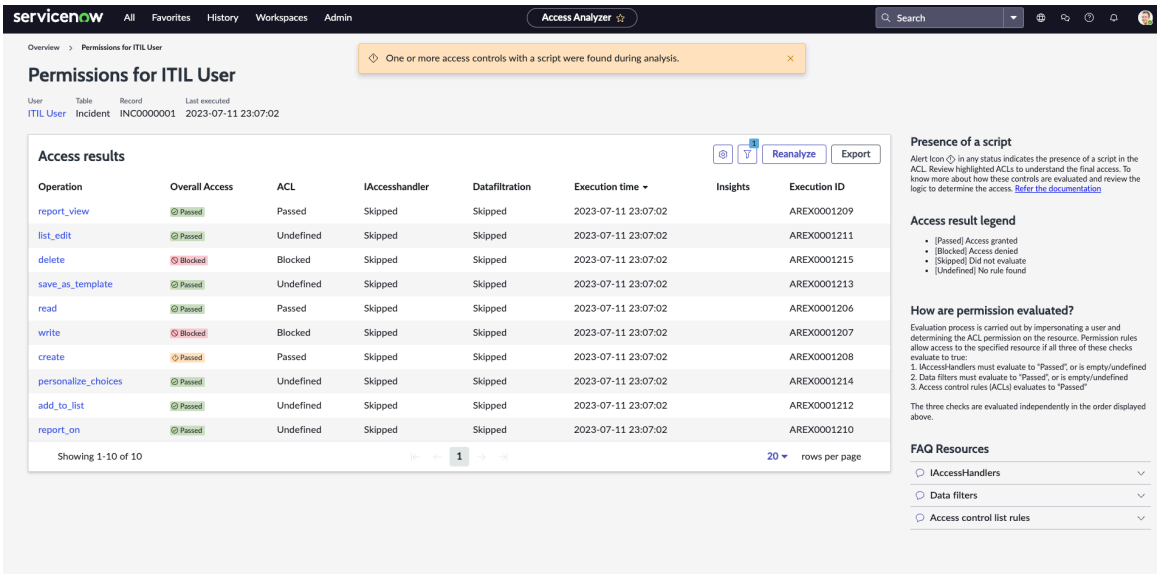
Les résultats d'accès de l'utilisateur s'affichent. De même, vous pouvez analyser les autorisations d'un groupe ou d'un rôle pour les types de règles suivants :

- Table (enregistrement)
- Include de script de client pouvant être appelé
- Points de terminaison REST

Les **résultats d'accès** pour le type de règle sélectionné s'affichent.

Traduction automatique

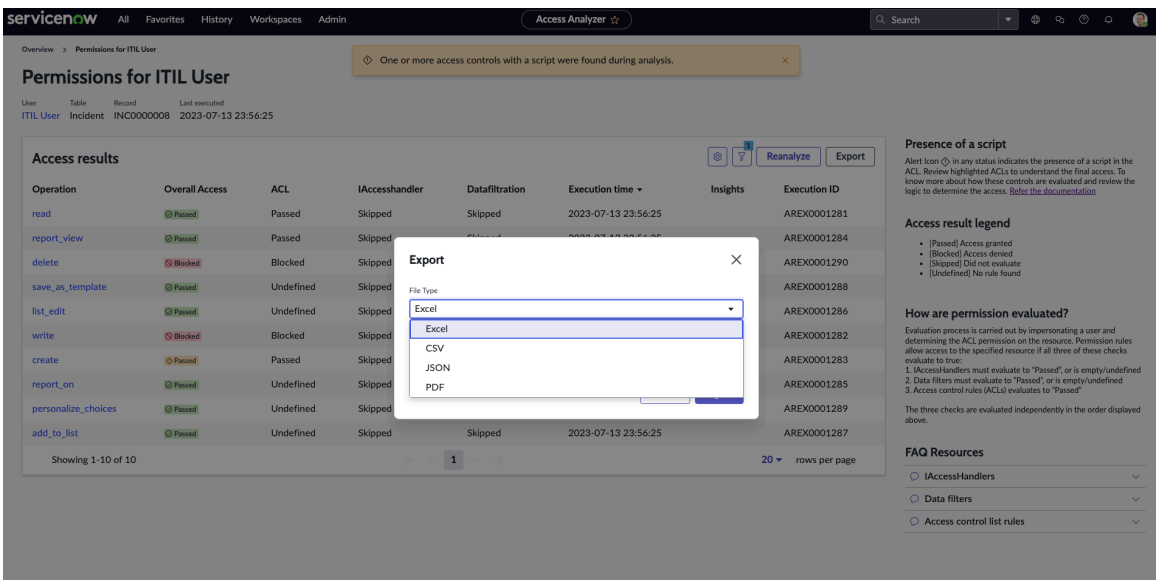
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Cliquez sur **Exporter**.

a. Choisissez le type de fichier.

Les types de fichiers disponibles sont Excel, CSV, JSON, PDF.

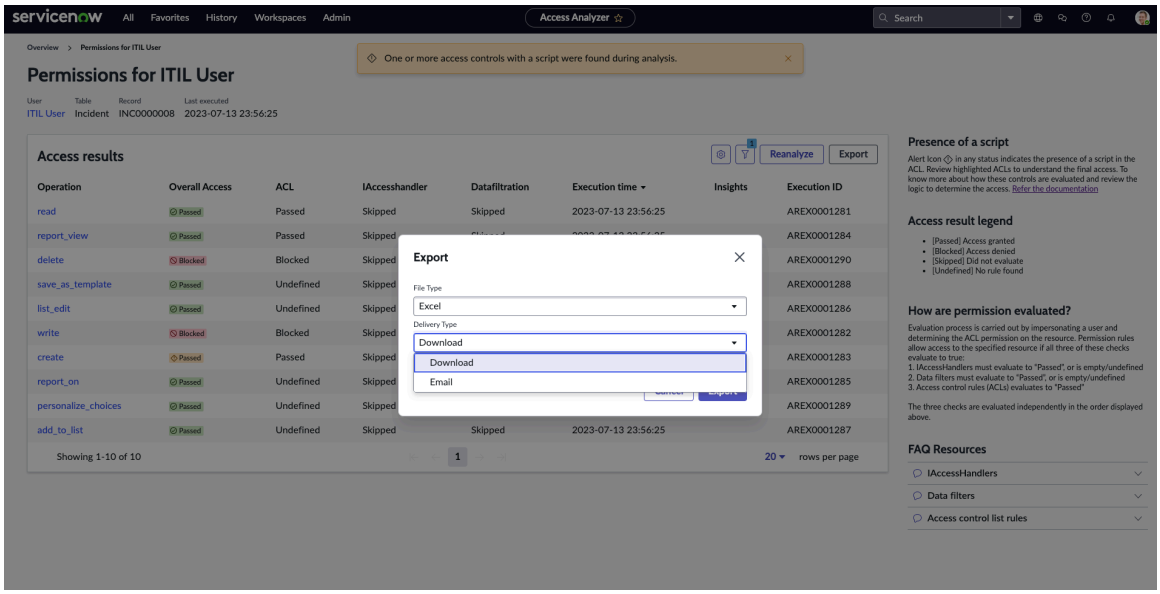


b. Choisissez le type de livraison.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Types de livraison disponibles en téléchargement et par e-mail.



Comparaison des enregistrements de l'utilisateur

Comparez les enregistrements des utilisateurs pour comprendre l’accès entre deux utilisateurs.

Avant de commencer

Rôle requis : administrateur

La procédure suivante décrit les étapes de comparaison des enregistrements utilisateur à l’aide de l’analyseur d’accès.

Remarque :
Access Analyzer est un ServiceNow® Store produit.

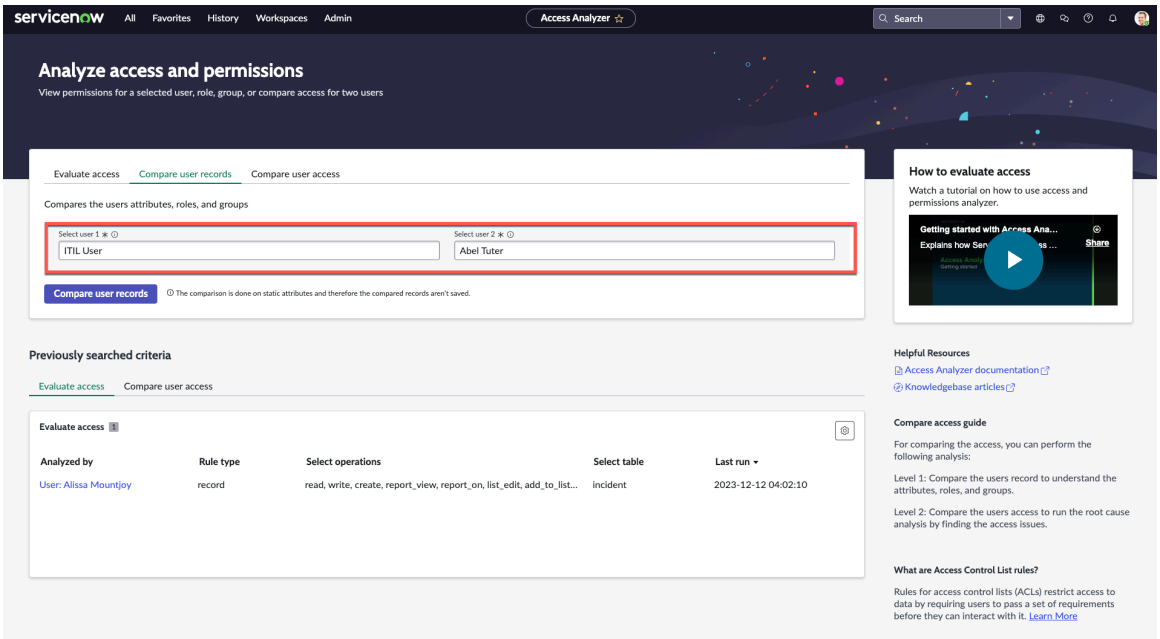
Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d’accueil Analyser l’accès et les autorisations s’affiche.
2. Sélectionnez l’onglet **Comparer les enregistrements utilisateur** .
3. Sélectionnez **l’utilisateur 1** et **l’utilisateur 2** pour comparaison.

   Par exemple, Utilisateur ITIL en tant **qu’utilisateur 1** et Abel Tuter en tant **qu’utilisateur 2**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



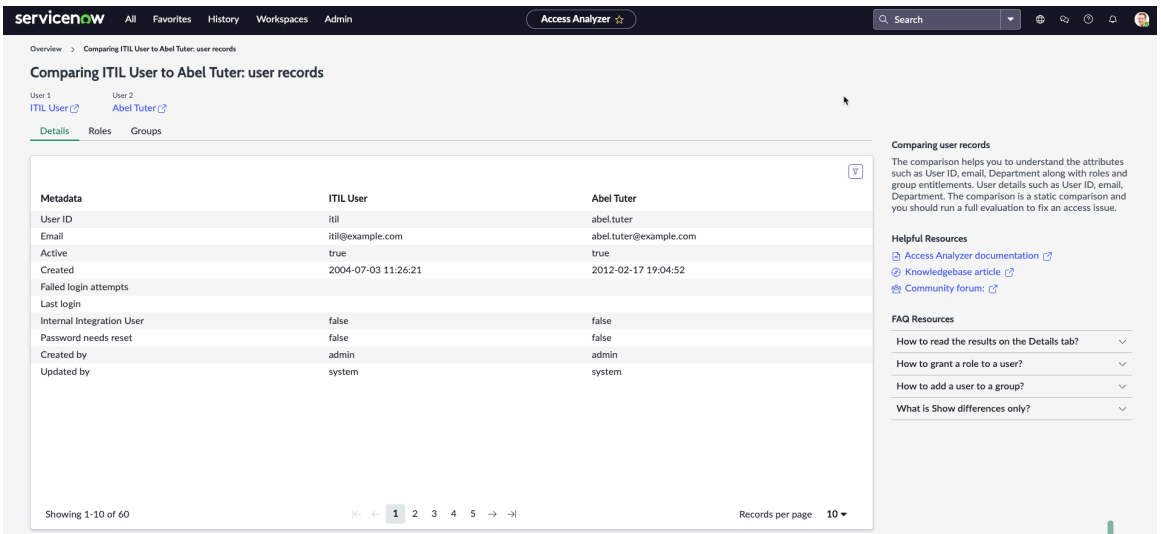
4. Sélectionnez **Comparer les enregistrements de l'utilisateur**.

   Les résultats sont affichés avec les onglets suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Détails** : affichez les métadonnées de



l'utilisateur.

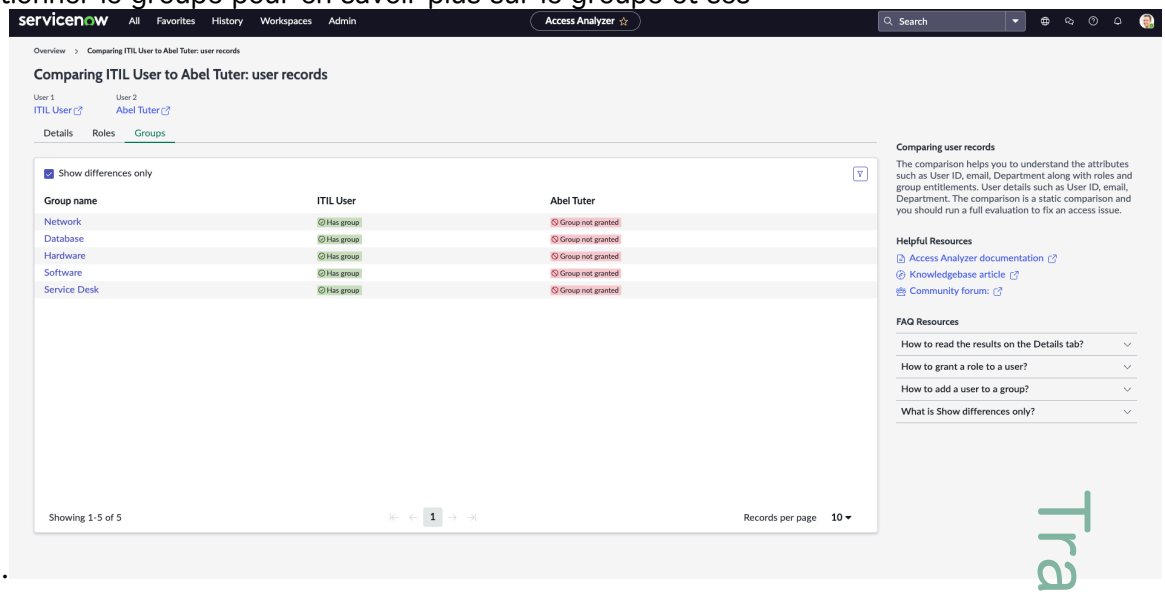
- **Rôles** : affichez les rôles qui sont affectés à l'utilisateur. Vous pouvez sélectionner le rôle pour en savoir plus sur le rôle et ses autorisations.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **Groupes** : affiche les groupes qui sont affectés à l'utilisateur. Vous pouvez sélectionner le groupe pour en savoir plus sur le groupe et ses autorisations.



De même, vous pouvez comparer différents utilisateurs dans l'instance ServiceNow pour comprendre l'accès qui leur est affecté.

Comparaison de l'accès de l'utilisateur

Comparez le contrôle d'accès de l'utilisateur à l'aide de l'analyseur d'accès.

Avant de commencer

Rôle requis : administrateur

La procédure suivante décrit les étapes de comparaison du contrôle d'accès entre les utilisateurs à l'aide de l'analyseur d'accès.

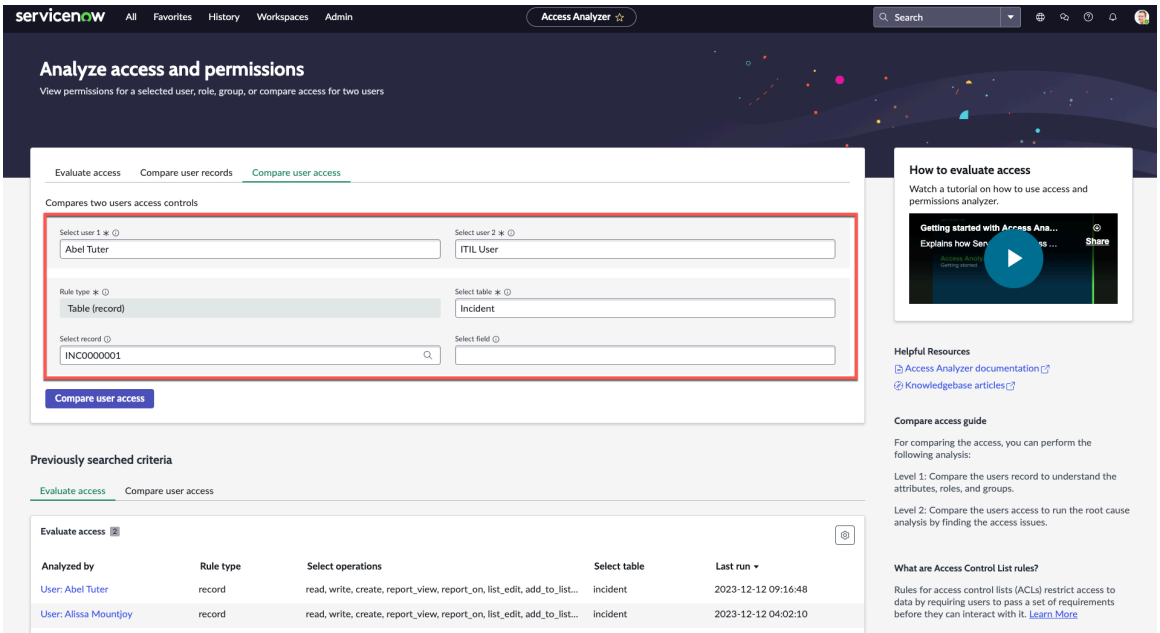
Remarque :
Access Analyzer est un ServiceNow® Store produit.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Analyser les autorisations**.
   La page d'accueil Analyser l'accès et les autorisations s'affiche.
2. Sélectionnez l'onglet **Comparer l'accès utilisateur** .
3. Renseignez les champs suivants :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Comparer l'accès de l'utilisateur

Champ	Description
Sélectionner l’utilisateur 1*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour la comparaison.
Sélectionner l’utilisateur 2*	Spécifiez un nom d’utilisateur à sélectionner dans la liste pour le comparer à l’utilisateur 1.
Type de règle*	Analysez les autorisations d’accès pour une table. **Remarque :** Seules les autorisations d’accès pour une table peuvent être utilisées dans **l’accès utilisateur de comparaison**.
Sélectionner une table*	Spécifiez un nom de table à sélectionner dans la liste.
Sélectionner un enregistrement	Spécifiez un nom d’enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste.

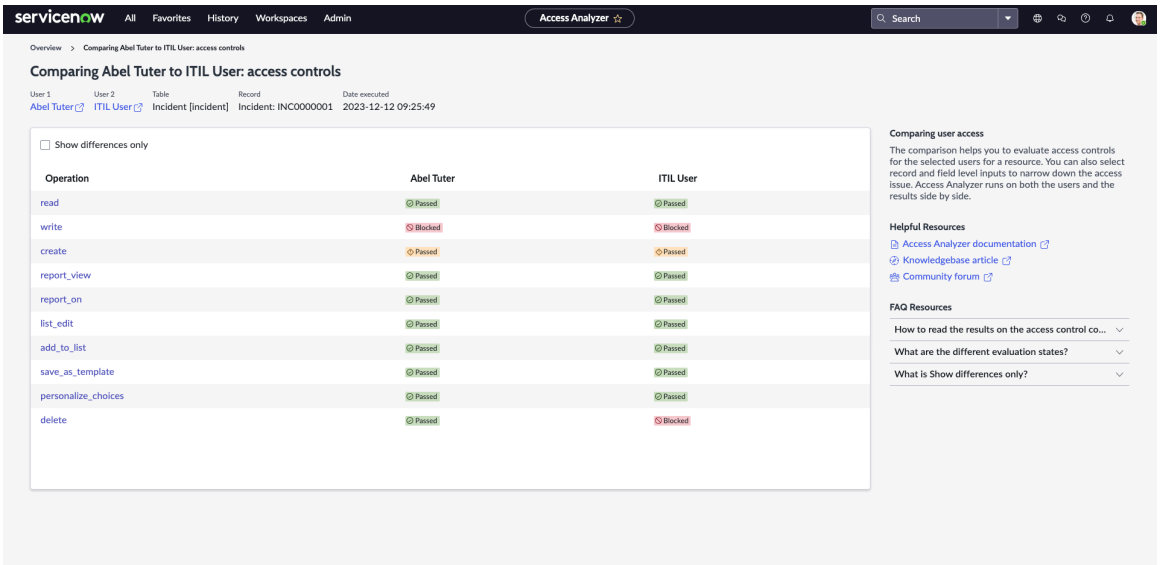
4. Sélectionnez **Comparer l’accès utilisateur**.

   Les résultats de **comparaison de l’accès utilisateur** pour les utilisateurs sélectionnés s’affichent.

   La comparaison des résultats de l’accès de l’utilisateur affiche l’état de l’opération et de l’évaluation de l’accès pour les utilisateurs. Par exemple, Abel Tuter et utilisateur ITIL.

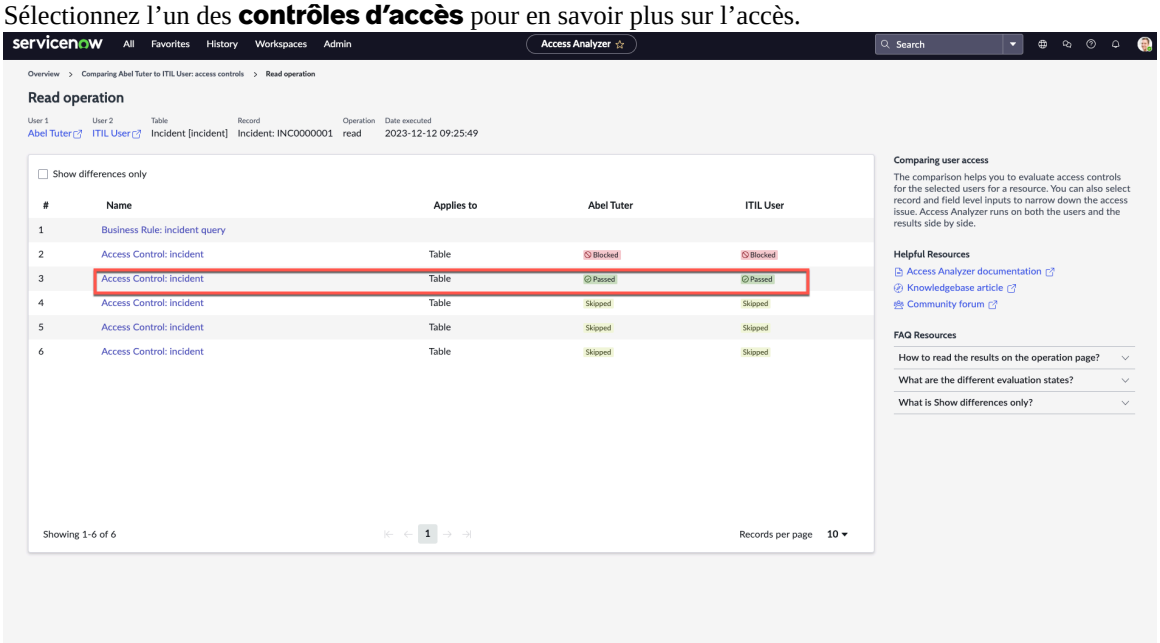
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



5. Sélectionnez l’opération pour en savoir plus sur l’évaluation des autorisations et les rôles auxquels les utilisateurs sont affectés.
Par exemple, **opération de lecture** .

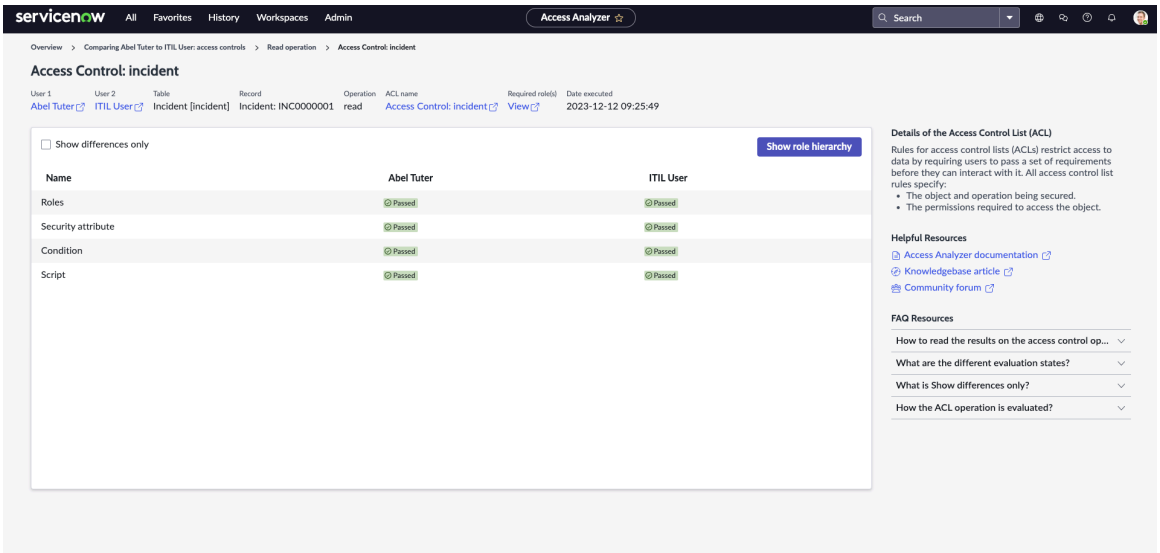
6. Sélectionnez l’un des **contrôles d’accès** pour en savoir plus sur l’accès.



Les détails du contrôle d’accès tels que les rôles, l’attribut de sécurité, la condition et l’état d’évaluation du script s’affichent.

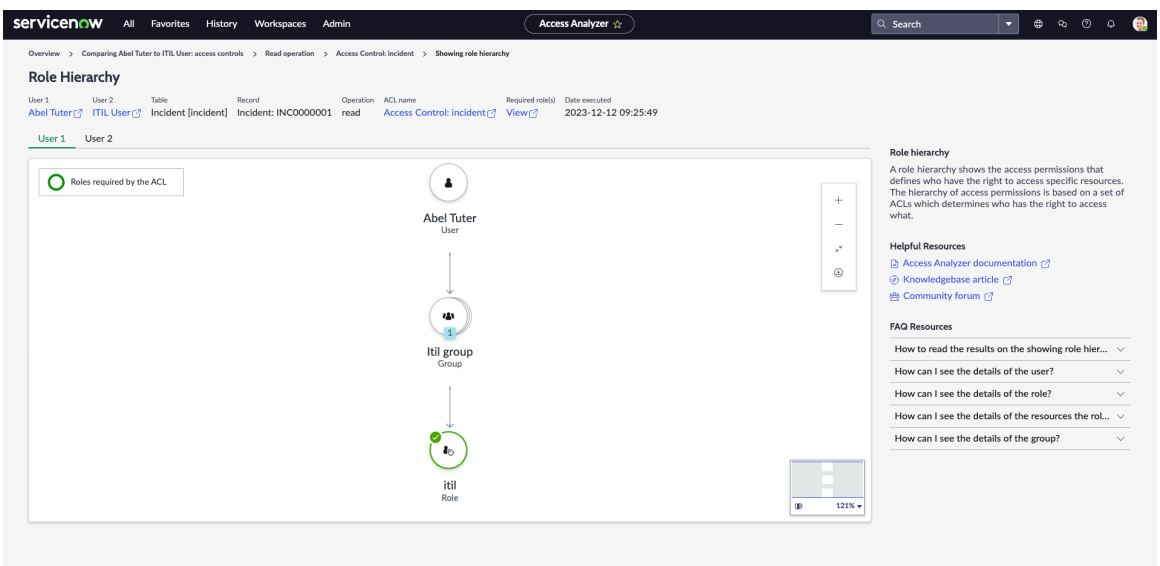
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



7. Sélectionnez **Afficher la hiérarchie des rôles** pour en savoir plus sur les rôles et les groupes affectés à l'utilisateur et comparer les deux utilisateurs.

En fonction de la hiérarchie des rôles, vous pouvez affecter les affectations de rôle et de groupe nécessaires à l'utilisateur pour avoir accès aux ressources (table).

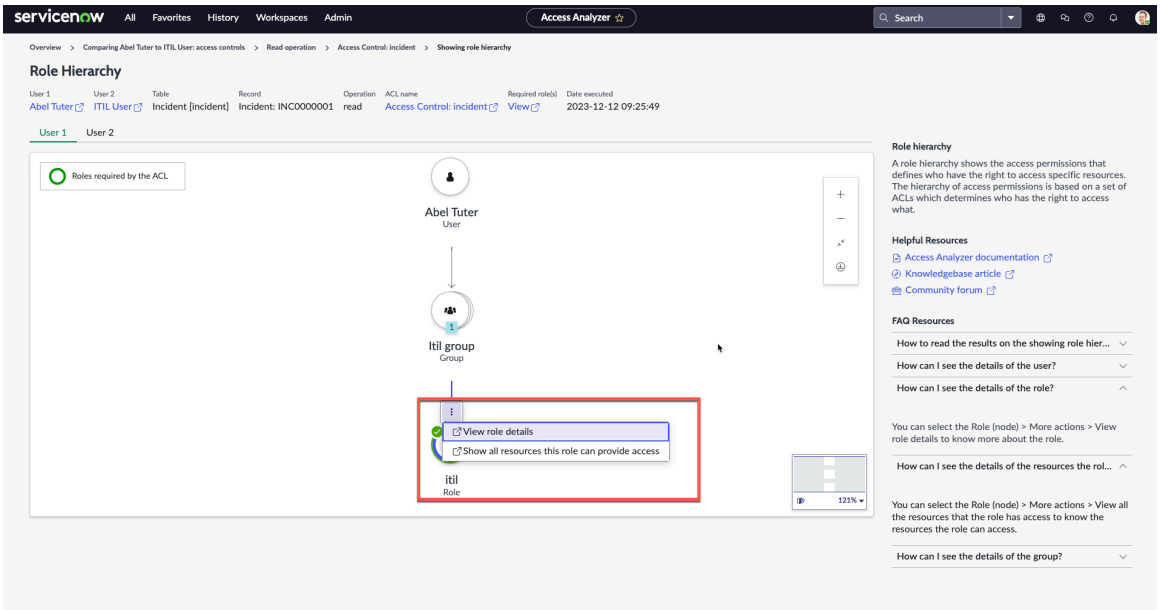


Dans l'exemple, **Abel Tuter** et **l'utilisateur ITIL** ont tous deux un utilisateur ITIL affecté. Le contrôle d'accès a donc été réussi. Vous pouvez déterminer les affectations de rôle et de groupe nécessaires à l'utilisateur en examinant la hiérarchie des rôles.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez sélectionner le nœud pour en savoir plus sur le rôle, les ressources auxquelles le rôle peut accéder ou le groupe.



Affichage des requêtes de l'analyseur d'accès : critères recherchés précédemment

Consultez les critères d'analyseur d'accès recherchés précédemment.

Avant de commencer

Rôle requis : administrateur

Remarque :
Access Analyzer est un ServiceNow® Store produit.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Requêtes d'analyseurs d'accès**.

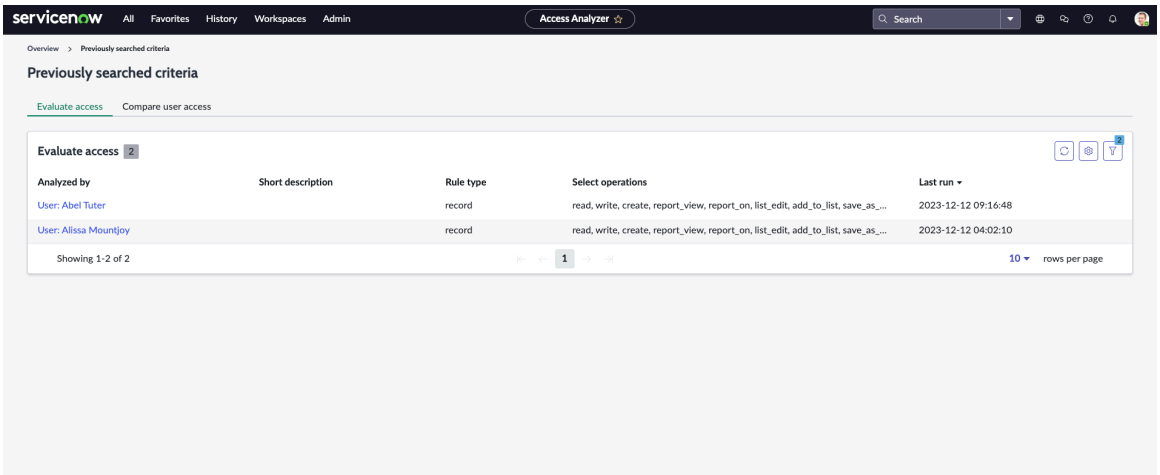
   Les critères recherchés précédemment comportent les sections suivantes :

   - **Évaluer l'accès** : affiche les résultats en fonction des requêtes effectuées via les fonctionnalités **Évaluer l'accès** .
   - **Comparer l'accès de l'utilisateur** : affiche les résultats basés sur les requêtes effectuées via les fonctionnalités **Comparer l'accès de l'utilisateur** .

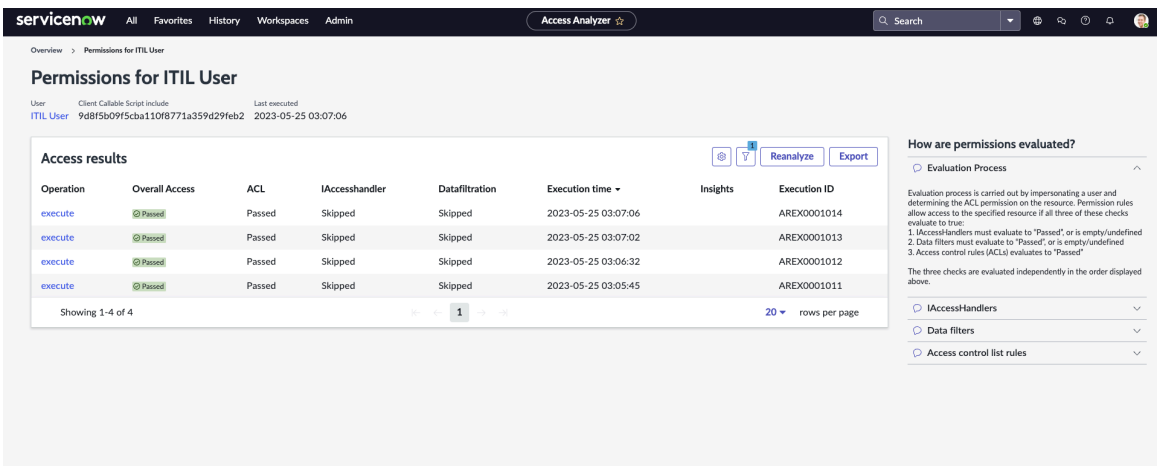
   Remarque :
   Les critères recherchés précédemment ne sont pas stockés lors de l'utilisation de la fonctionnalité de comparaison des enregistrements utilisateur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

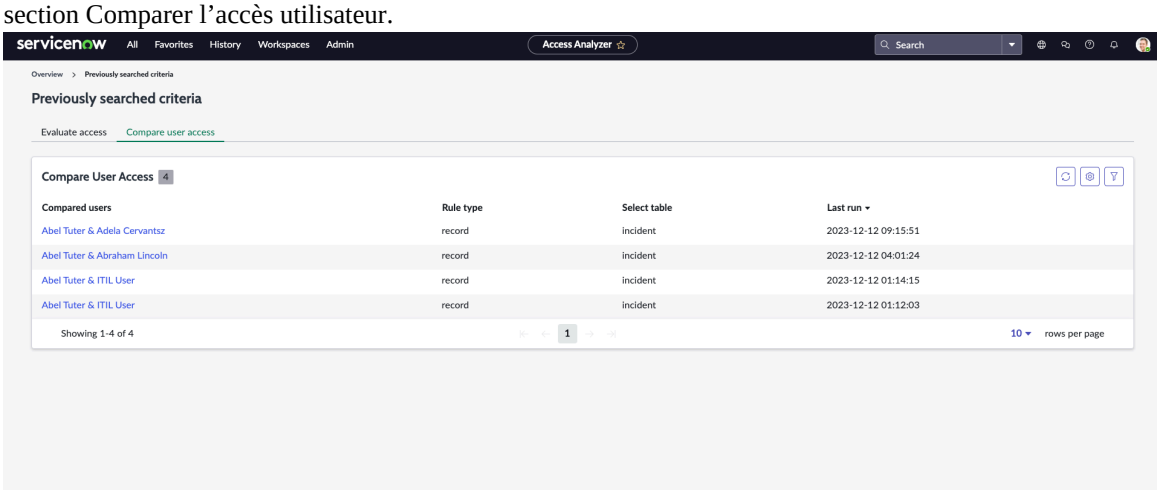


2. Sélectionnez les liens **Analysé par** pour afficher les critères précédemment recherchés dans la section Évaluer l'accès.



Vous pouvez sélectionner **Analyser à nouveau** l'accès pour l'utilisateur. Exportez les détails à l'aide de l'option **Exporter** .

3. Sélectionnez les liens **Utilisateurs comparés** pour afficher les critères précédemment recherchés dans la section Comparer l'accès utilisateur.



Évaluation de l'autorisation

Critères d'évaluation des autorisations lors de l'utilisation de l'analyseur d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Hiérarchie de l'évaluation

L'autorisation pour l'utilisateur, le groupe ou le rôle sélectionné est évaluée dans la hiérarchie suivante :

- Règle métier : une règle métier est un script de serveur configuré pour s'exécuter lorsqu'un enregistrement est affiché, inséré, supprimé ou lorsqu'une table est interrogée.
- Gestionnaire d'accès : une vérification interne du système à l'aide du code source masqué sur la plateforme.
- Filtration des données : le filtre de données est une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance. Le filtre de données ne prend en charge que l'opération de lecture.
- Liste de contrôle d'accès (ACL) : les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Dans une ACL, la hiérarchie suivante est évaluée :
  - Rôle
  - Attribut de sécurité
  - Condition
  - Script

Vous pouvez analyser l'accès et les autorisations de l'utilisateur, du rôle ou du groupe sélectionné à l'aide de l'analyseur d'accès. Les autorisations sont évaluées en fonction des types de règles suivants :

- **Évaluation au niveau** de la table : les ACL d'attributs de rôle et de sécurité sont utilisées pour l'évaluation au niveau de la table.
- **Évaluation au niveau de l'enregistrement ou du champ** : les ACL au niveau de l'enregistrement, de l'attribut de sécurité, de la condition et du script sont utilisées pour l'évaluation au niveau de l'enregistrement ou du champ.
- **Page de l'interface utilisateur** : Prise en charge Opérations prêtes uniquement. Seules les ACL de niveau lecture sont évaluées.
- **Point de terminaison REST** : prise en charge de l'opération d'exécution uniquement. Seules les ACL de niveau d'exécution sont évaluées.

Voici les détails concernant les champs importants dans les résultats de l'accès :

- Présence d'un script
- Légende du résultat d'accès
- Processus d'évaluation
- IAccessHandler
- Filtres de données
- Règles de la liste de contrôle d'accès

Présence d'un script

L'icône d'alerte quel que soit l'état indique la présence d'un script dans l'ACL. Examinez les ACL en surbrillance pour comprendre l'accès final. Pour en savoir plus sur le mode

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

d’évaluation de ces contrôles et examiner la logique de détermination de l’accès, reportez-vous Journaux de débogage d’analyseur d’accèsà .

Légende dans l’analyseur d’accès

Lors de l’analyse de l’accès et des autorisations, des légendes sont affichées dans le cadre du processus d’évaluation. Voici les légendes :

- [Réussi] Accès accordé
- [Bloqué] Accès refusé
- [Ignoré] N'a pas évalué
- [Non défini] Aucune règle trouvée

Processus d’évaluation

Le processus d’évaluation s’effectue en empruntant l’identité d’un utilisateur et en déterminant l’autorisation de liste de contrôle d’accès (ACL) sur la ressource. Les règles d’autorisation permettent d’accéder à la ressource spécifiée si les vérifications suivantes sont évaluées comme vraies :

- L’évaluation des IAccessHandler doit retourner la valeur « Réussi », ou est vide ou non définie
- L’évaluation des filtres de données doit retourner la valeur « Réussi », ou est vide ou non définie
- L’évaluation des règles de contrôle d’accès (ACL) doit retourner la valeur « Réussi »

IAccessHandler

Un contrôle interne du système à l’aide du code source masqué sur la plateforme. IAccessHandler peut accorder ou refuser l’accès à une ressource sans évaluer les ACL. Si IAccessHandler est ignoré, les ACL sont évaluées.

Vous ne pouvez pas modifier les contrôles IAccessHandler. Par exemple, une implémentation IAccessHandler est utilisée pour les contrôles d’accès sur les ressources d’application telles que l’accès en lecture.

Filtre de données

Le filtre de données est une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance.

Règles de la liste de contrôle d'accès

Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Forum aux questions

Questions fréquemment posées lors de l’utilisation de l’analyseur d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Évaluer l’accès

Voici quelques-unes des questions fréquemment posées lors de l’utilisation de la fonctionnalité Évaluer l’accès dans l’analyseur d’accès :

Forum Aux Questions

Questions	Explication
Comment lire les résultats de l’évaluation affichés par l’analyseur d’accès ?	Chaque ligne représente une liste de contrôle d’accès (ACL) individuelle. La séquence (#) dans les résultats indique l’ordre dans lequel les ACL sont évaluées. L’état indique si l’accès global est accordé (réussi) ou refusé (bloqué).
Comment les ACL sont-elles évaluées ?	Au niveau d’une table, les ACL ne sont évalués que pour les rôles et les attributs de sécurité, les conditions et les scripts ne sont pas évalués. Les rôles sont évalués en premier. Si les rôles sont bloqués, les conditions et les scripts sont ignorés. Pour plus d'informations, consultez Configuration d’une règle ACL.
Quelles sont les légendes dans l’analyseur d’accès ?	Lors de l’analyse de l’accès et des autorisations, des légendes sont affichées dans le cadre du processus d’évaluation. Les légendes sont les suivantes : • [Réussi] Accès accordé • [Bloqué] Accès refusé • [Ignoré] N’a pas évalué • [Non défini] Aucune règle trouvée
Que signifie l’icône d’alerte dans les résultats d’accès ?	L’icône d’alerte quel que soit l’état indique la présence d’un script dans l’ACL. Examinez les ACL en surbrillance pour comprendre l’accès final. Pour en savoir plus sur le mode d’évaluation de ces contrôles et examiner la logique de détermination de l’accès, reportez-vous Journaux de débogage d’analyseur d’accèsà .
Qu’est-ce que **IAccesshandler** ?	Un contrôle interne du système à l’aide du code source masqué sur la plateforme. Il s’agit d’un contrôle de sécurité du système que vous ne pouvez pas modifier. **IAccessHandler** peut accorder ou refuser

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forum Aux Questions (suite)

Questions	Explication
	l'accès à une ressource sans évaluer les ACL. Si cet **IAccessHandler** est ignoré, les ACL sont évaluées. Vous ne pouvez en aucun cas modifier les contrôles **IAccessHandler** . Par exemple, une **implémentation IAccessHandler** est utilisée pour les contrôles d'accès sur les ressources d'application telles que l'accès en lecture seule.
Que sont les filtres de données ?	Les filtres de données sont une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance.
Qu'est-ce qu'une règle ACL ?	Les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données.

Affectations de rôles limitées dans le temps trouvées pour l'utilisateur en raison desquelles les résultats peuvent être affectés. Vous pouvez consulter les rôles limités dans le temps affectés à l'utilisateur ici.

Comparer les enregistrements de l'utilisateur

Voici quelques-unes des questions fréquemment posées lors de l'utilisation de la fonctionnalité Comparer l'enregistrement de l'utilisateur dans l'analyseur d'accès :

Forum Aux Questions

Questions	Explication
Comment lire les résultats dans l'onglet Détails ?	L'onglet Détails affiche les métadonnées associées à l'utilisateur 1 et à l'utilisateur 2
Comment accorder un rôle à un utilisateur ?	Dans l'onglet Utilisateurs, vous pouvez vérifier le rôle qui doit être accordé à l'utilisateur et affecter ce rôle.
Comment ajouter un utilisateur à un groupe ?	Dans l'onglet Groupes, vous pouvez vérifier le groupe auquel l'utilisateur doit être ajouté et ajouter l'utilisateur au groupe.
Qu'est-ce que l'option Afficher uniquement la différence ?	Lorsque vous cochez la case Afficher uniquement les différences, seuls les rôles ou le groupe qui sont différents entre l'utilisateur 1 et l'utilisateur 2 s'affichent.

Comparer l'accès de l'utilisateur

Voici quelques-unes des questions fréquemment posées lors de l'utilisation de la fonctionnalité Comparer l'accès de l'utilisateur dans l'analyseur d'accès :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forum Aux Questions

Questions	Explication
Comment lire les résultats sur la page de comparaison de contrôle d'accès ?	La page de comparaison des contrôles d'accès affiche les états d'évaluation pour différentes opérations ACL.
Quels sont les différents états d'évaluation ?	Lorsque l'on compare les contrôles d'accès entre les utilisateurs, les différents états d'évaluation sont les suivants : • Réussi • Bloqué
Qu'est-ce que l'option Afficher uniquement les différences ?	Lorsque vous cochez la case Afficher uniquement les différences, seul l'état d'évaluation de l'opération qui est différent entre l'utilisateur 1 et l'utilisateur 2 s'affiche.
Comment l'opération ACL est-elle évaluée ?	La liste de contrôle d'accès (ACL) est la règle pour les listes de contrôle d'accès qui restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Dans une ACL, la hiérarchie suivante est évaluée : • Rôle • Attribut de sécurité • Condition • Script
Comment lire les résultats sur la page d'affichage de la hiérarchie des rôles ?	La page d'affichage de la hiérarchie des rôles affiche le rôle affecté à l'utilisateur 1 et à l'utilisateur 2. Vous pouvez comprendre le rôle requis pour l'utilisateur pour une opération ACL particulière.
Comment puis-je voir les détails de l'utilisateur ?	Vous pouvez sélectionner l'icône **Utilisateur (nœud)** > **Actions supplémentaires** > **Afficher l'utilisateur** détails pour en savoir plus sur l'utilisateur.
Comment puis-je voir les détails du rôle ?	Vous pouvez sélectionner l'icône **Rôle (nœud)** > **Actions supplémentaires** > **Rôle d'affichage** détails pour en savoir plus sur le rôle.
Comment puis-je voir les détails des ressources auxquelles le rôle peut accéder ?	Vous pouvez sélectionner l'icône **Rôle (nœud)** > **Actions supplémentaires** > **Afficher toutes les ressources auxquelles le rôle a accès** pour connaître les ressources auxquelles le rôle peut accéder.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Forum Aux Questions (suite)

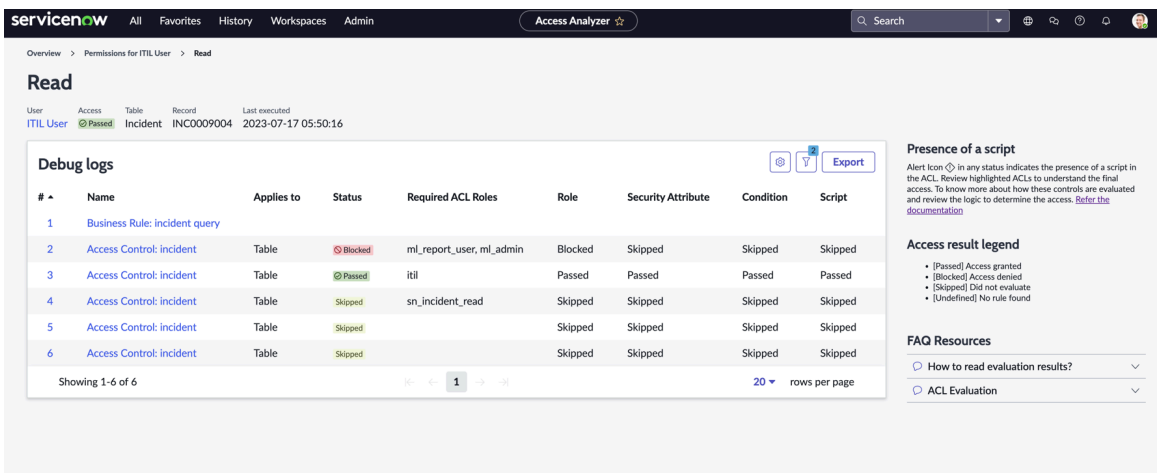
Questions	Explication
Comment puis-je voir les détails du groupe ?	Vous pouvez sélectionner l'icône **Groupe (nœud)** > **Actions supplémentaires** > **Afficher le groupe** pour en savoir plus sur le groupe.

Journaux de débogage d'analyseur d'accès

Les journaux de débogage affichent les détails de l'opération de sélection de résultat d'accès.

Champs dans les journaux de débogage

Les journaux de débogage dans l'analyseur d'accès affichent des informations sur l'opération sélectionnée pour comprendre les autorisations, les règles métier et les ACL associées à l'opération.



Les champs et leur description sont les suivants dans les journaux de débogage :

Journaux des débogages

Champs	Description
Nom	Les détails de la règle métier ou de l'ACL. Vous pouvez sélectionner la règle métier d'ACL pour plus d'informations.
Concerne	Les détails sur l'application de l'ACL au niveau d'un champ, d'un enregistrement ou d'une table.
Statut	État de l'ACL pour le rôle et l'autorisation associés.
Requiert une ACL	Rôle requis pour accéder au champ, à l'enregistrement ou à la table.
Rôle	Les détails sur le rôle bloqué, réussi ou ignoré pour le contrôle d'accès.
Attribut de sécurité	Les détails sur l'attribut de sécurité bloqué, réussi, ignoré pour le contrôle d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Journaux des débogages (suite)

Champs	Description
Condition	Le détail de la condition bloquée, réussie ou ignorée pour le contrôle d'accès.
Script	Les détails sur le script bloqué, réussi, ignoré pour le contrôle d'accès.
Personnalisé	Les détails sur l'ACL personnalisée, le cas échéant, pour le contrôle d'accès.
Application	État de l'application. Global ou Store.

Hiérarchie de l'évaluation

L'autorisation pour l'utilisateur, le groupe ou le rôle sélectionné est évaluée dans la hiérarchie suivante :

- Règle métier : une règle métier est un script de serveur configuré pour s'exécuter lorsqu'un enregistrement est affiché, inséré, supprimé ou lorsqu'une table est interrogée.
- Gestionnaire d'accès : une vérification interne du système à l'aide du code source masqué sur la plateforme.
- Filtration des données : un filtre de données est une forme de contrôle d'accès conçu pour fonctionner avec les règles de contrôle d'accès (ACL) existantes sur votre instance. Les filtres de données ne prennent en charge que l'opération de lecture.
- Liste de contrôle d'accès (ACL) : les règles des listes de contrôle d'accès (ACL) restreignent l'accès aux données en exigeant que les utilisateurs satisfassent à un ensemble d'exigences avant de pouvoir interagir avec ces données. Dans une ACL, la hiérarchie suivante est évaluée :
  - Rôle
  - Attribut de sécurité
  - Condition
  - Script

Évaluation de la liste de contrôle d'accès

Les ACL pour les opérations sont évaluées dans la séquence comme suit :

- Rôle
- Attribut de sécurité
- Condition
- Script

Présence d'un script

L'icône d'alerte quel que soit l'état indique la présence d'un script dans l'ACL. Examinez les ACL en surbrillance pour comprendre l'accès final.

Remarque :
Lors d'une requête d'analyseur d'accès, les règles métier sont exécutées en premier, puis la liste de contrôle d'accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Séquence d’exécution

La séquence d’exécution des résultats d’accès dans différents scénarios est la suivante :

- **Présence d’une ACL héritée ou générique** : au cours de la séquence d’exécution, les ACL héritées sont évaluées en premier, puis les ACL génériques.
- **Une ACL est transmise, les autres sont ignorées** : pendant l’exécution et l’évaluation de l’autorisation, si une ACL est réussie, l’exécution et l’évaluation de l’autre ACL sont ignorées. Parce que l’autorisation globale pour l’opération sélectionnée nécessite une ACL pour accéder à un champ, un enregistrement ou une table pour une identité.
- **Exécution des ACL au niveau du champ et des ACL au niveau de la table** : pendant l’exécution, les ACL au niveau du champ sont exécutées en premier, suivies des ACL au niveau de la table pour fournir des résultats plus granulaires lors de l’analyse de l’accès d’une identité.
- **Évaluation en présence d’une ACL scriptée** : en présence d’un script, l’accès global à l’opération est transmis avec une icône d’alerte pour indiquer le script dans l’ACL.

Simulateur d'accès

Le simulateur d'accès vous permet de simuler le changement de l'accès à la table spécifiée une fois qu'un rôle ou un groupe est affecté ou supprimé de l'utilisateur.

Explorer



Découvrez les fonctionnalités et la valeur commerciale d’Access Simulator.

Utiliser



Comprendre comment utiliser le simulateur d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurer



Savoir comment configurer Access Simulator.

Forum Aux Questions



Obtenez des détails sur les questions fréquemment posées pour le simulateur d’accès.

Exploration d’Access Simulator

Le simulateur d’accès vous permet de simuler le changement de l’accès à la table spécifiée une fois qu’un rôle ou un groupe est affecté ou supprimé de l’utilisateur.

Les administrateurs peuvent utiliser le simulateur d’accès pour simuler les besoins d’accès de leurs utilisateurs sur une table spécifiée et comprendre comment les contrôles d’accès changent pour un utilisateur. Cela permet de comprendre rapidement l’accès actuel des utilisateurs et de comprendre les impacts de la fourniture ou de la suppression de rôles aux utilisateurs.

https://player.vimeo.com/video/988627830?badge=0&autopause=0&player_id=0&app_id=58479

Le simulateur d’accès permet de simuler l’accès d’un utilisateur pour les scénarios suivants :

- Ajout d’un rôle à l’utilisateur
- Suppression d’un rôle de l’utilisateur
- Ajout de l’utilisateur à un groupe
- Suppression de l’utilisateur d’un groupe

Pour en savoir plus sur les paramètres du simulateur d’accès et activer l’option Prendre des mesures, reportez-vous à la section Configuration du simulateur d’accès (Prendre des mesures).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configuration du simulateur d’accès (Prendre des mesures)

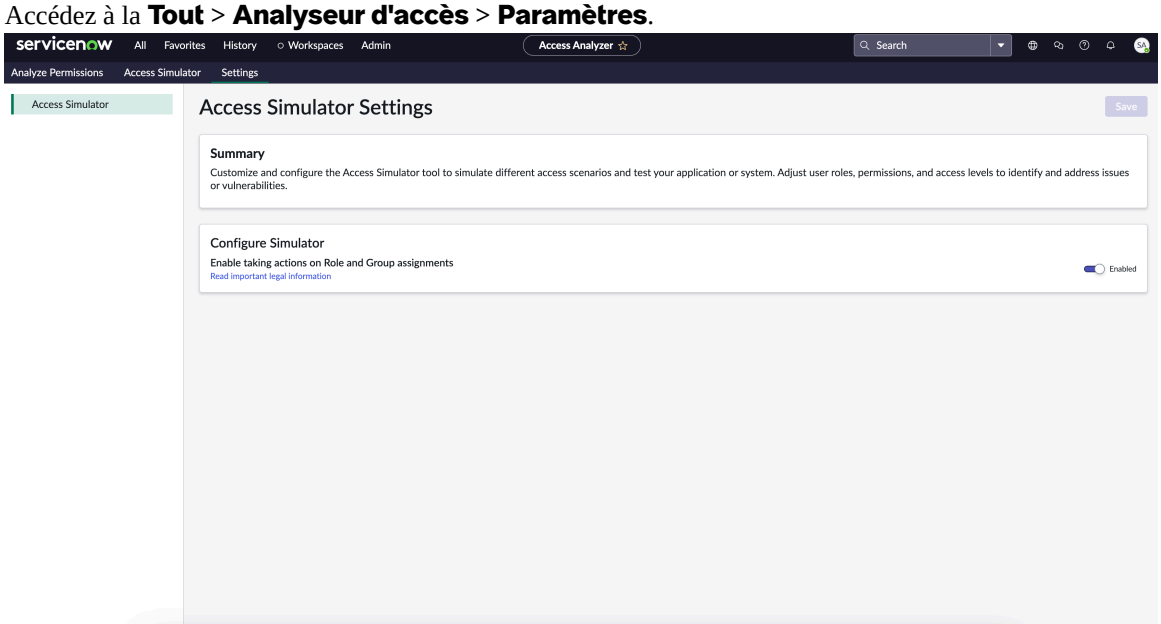
Configurez les options de prise d’actions pour terminer les affectations de rôle et de groupe que vous souhaitez ajouter après la simulation.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Paramètres**.



2. Sélectionnez le commutateur à activer.
   Lisez les informations juridiques avant d’activer le simulateur d’accès (Prendre des mesures).
3. Sélectionnez **Accepter**.
4. Sélectionnez **Enregistrer** pour enregistrer la configuration.

Utilisation du simulateur d’accès

Utilisez le simulateur d’accès pour simuler que l’accès de l’utilisateur à la table spécifiée changerait une fois qu’un rôle ou un groupe est affecté ou supprimé.

Avant de commencer

Rôle requis : administrateur

Activez la prise d’actions. Pour plus d'informations, consultez Configuration du simulateur d’accès (Prendre des mesures).

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez l’option **Simuler** sous chaque section en fonction des scénarios suivants :
   - Ajout d’un rôle à l’utilisateur
   - Suppression d’un rôle de l’utilisateur
   - Ajout de l’utilisateur à un groupe
   - Suppression de l’utilisateur d’un groupe

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Ajout d’un rôle à l’utilisateur

Utilisez le **rôle Simuler l’ajout** pour simuler les changements d’accès de l’utilisateur à une ressource (tables).

Avant de commencer

Rôle requis : administrateur

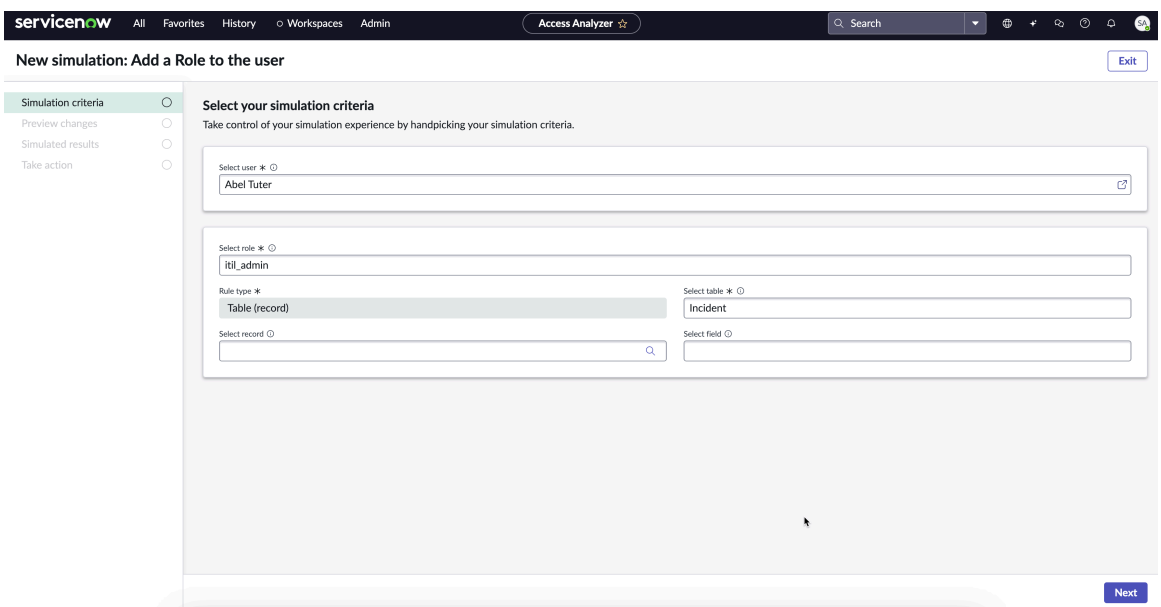
Activez la prise d’actions. Pour plus d'informations, consultez Configuration du simulateur d’accès (Prendre des mesures).

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Ajouter un rôle à l’utilisateur.
3. Spécifiez les champs suivants pour vos critères de simulation :

Ajouter un rôle à l'utilisateur

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d’utilisateur à sélectionner dans la liste. Dans cet exemple, **Abel Tuter**.
Sélectionner un rôle *	Spécifiez un rôle à sélectionner dans la liste. Dans cet exemple, **itil_admin**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d’enregistrement à sélectionner dans la liste (facultatif).
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ permet d’analyser l’autorisation, même au niveau du champ. Par exemple, Actif, Créé par, etc.

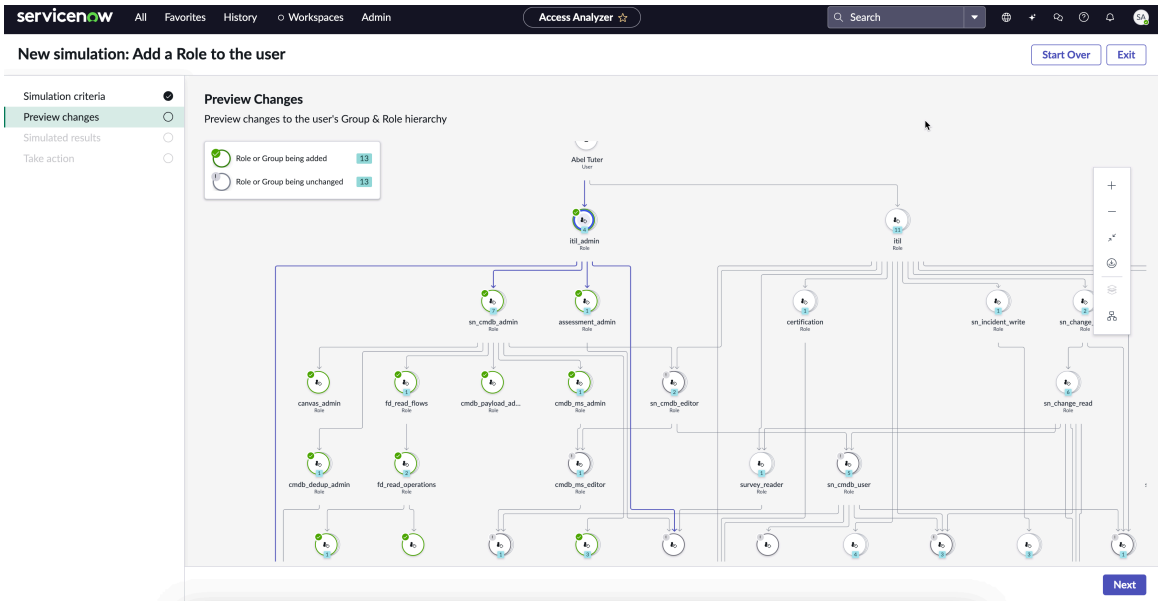


Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

4. Sélectionnez **Suivant**.

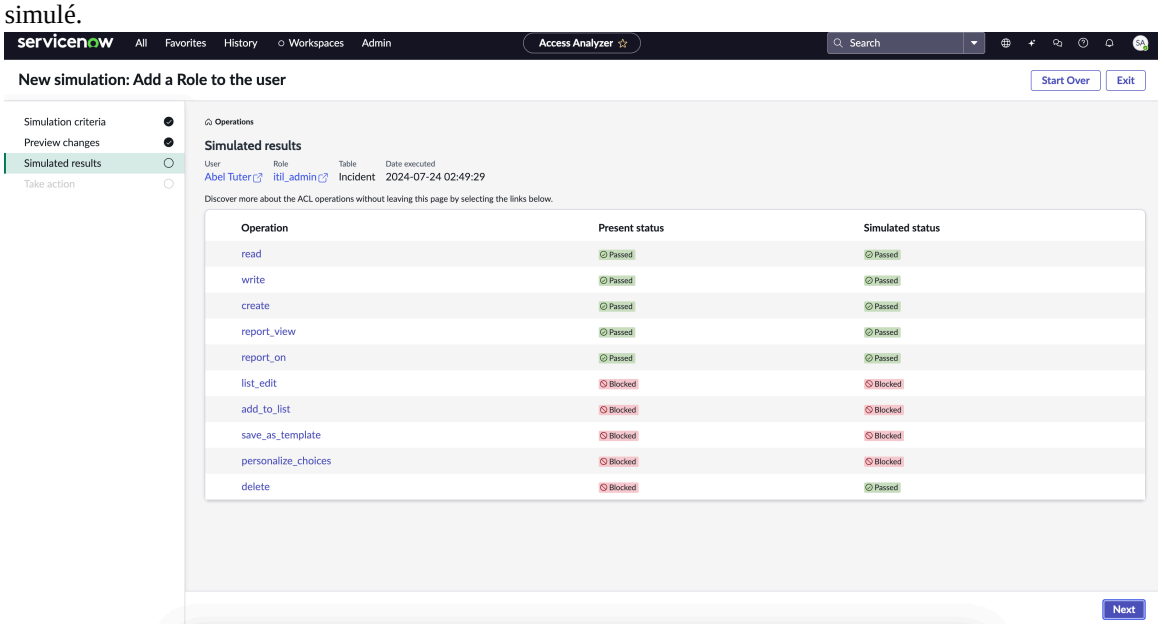
5. Prévisualisez les modifications.
   Les rôles nouvellement affectés sont simulés dans les changements apportés à l'aperçu. Vous pouvez valider les rôles et les rôles enfants qui sont ajoutés à l'utilisateur avant de passer à l'étape suivante.



Vous pouvez voir les nouveaux rôles qui sont ajoutés dans **itil_admin** rôle s'affiche avec les rôles existants de l'utilisateur.

6. Sélectionnez **Suivant**.

7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.



L'ajout du **itil_admin** permet à l'utilisateur d'effectuer une opération de suppression sur la table (incident).

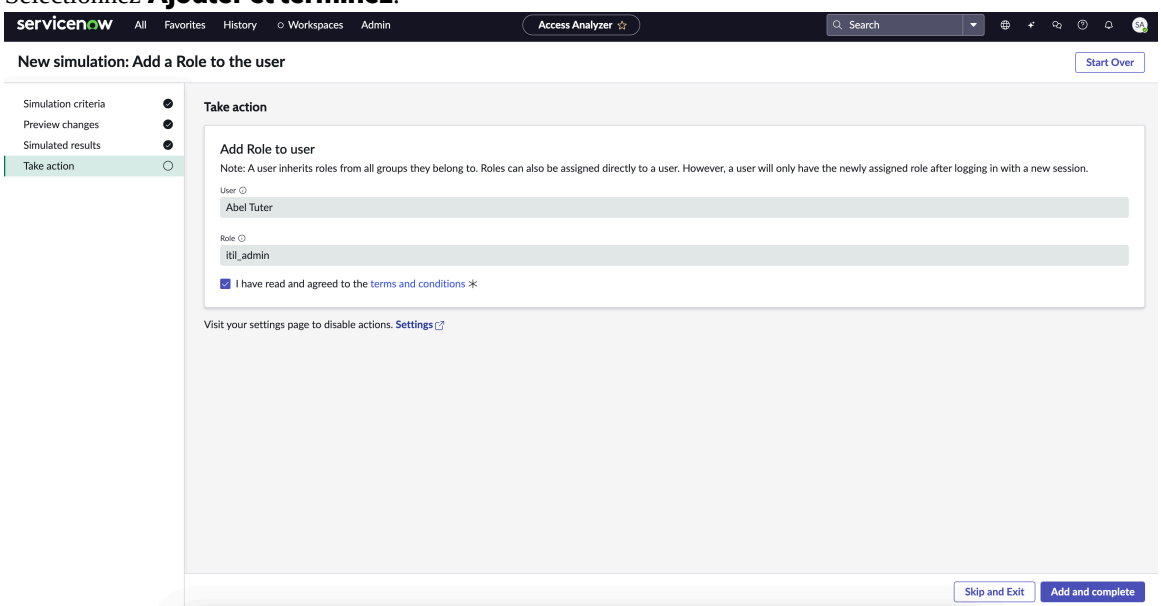
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez recommencer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Ajouter et terminez**.



Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer les actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

Les rôles sont ajoutés avec succès à l'utilisateur. Vous pouvez vérifier l'accès à l'aide de l'analyseur d'accès. Pour en savoir plus sur la vérification de l'accès d'un utilisateur, reportez-vous à la section Analyseur d'accès.

Suppression d'un rôle de l'utilisateur

Utilisez le **rôle Simuler la suppression** pour simuler les changements d'accès de l'utilisateur pour une ressource (tables).

Avant de commencer

Rôle requis : administrateur

Activez la prise d'actions. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Traduction automatique

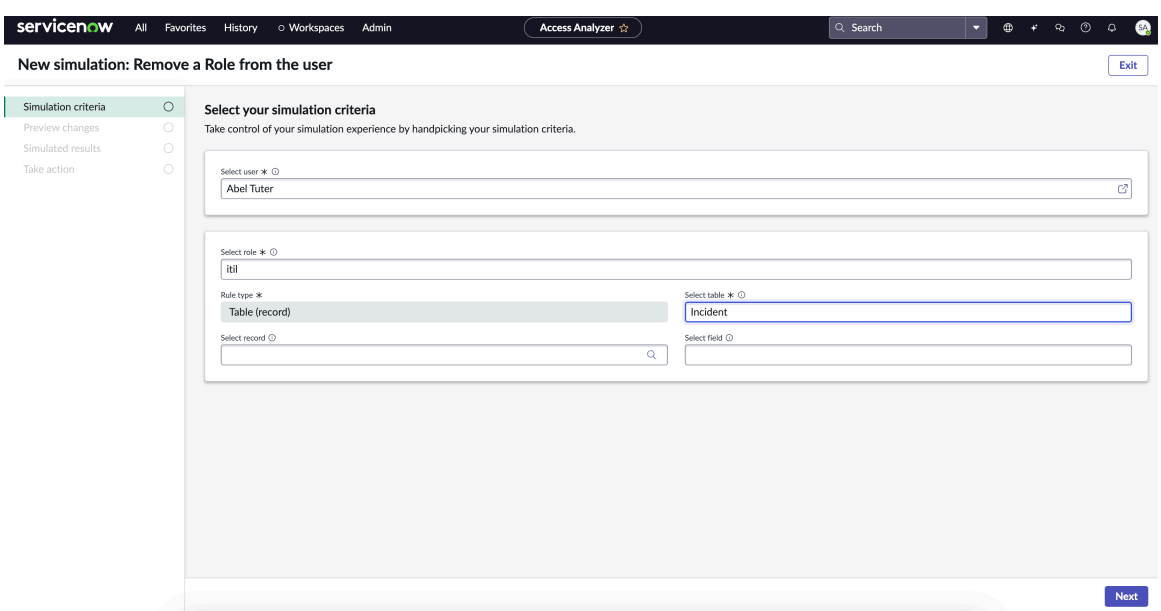
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Supprimer un rôle de l'utilisateur.
3. Spécifiez les champs suivants pour vos critères de simulation :

Supprimer un rôle de l'utilisateur

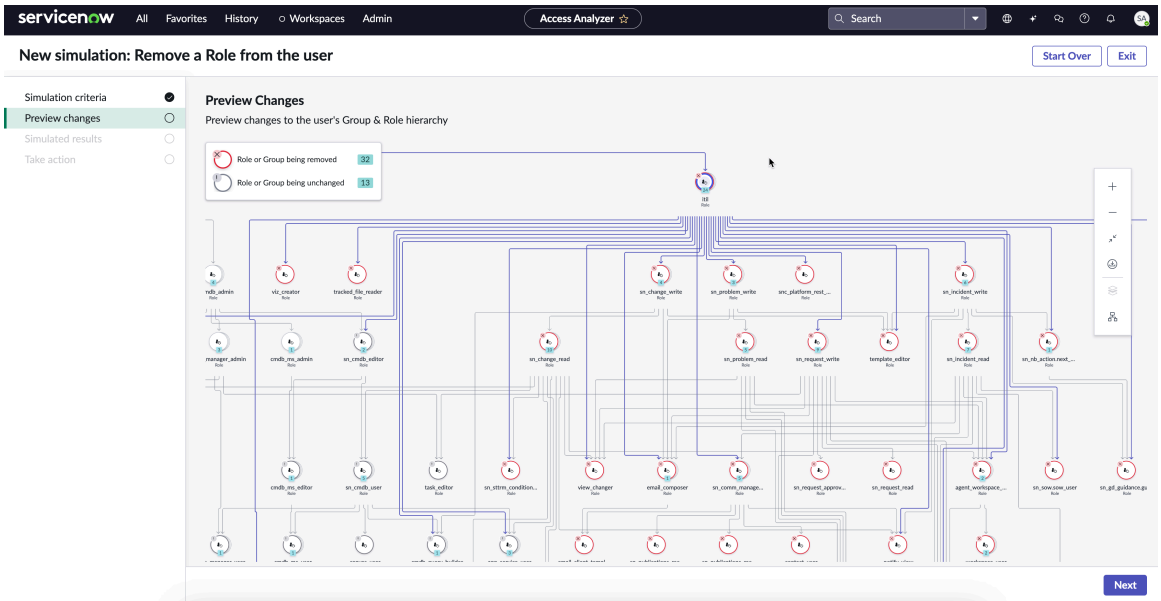
Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **Abel Tuter**.
Sélectionner un rôle *	Spécifiez un rôle à sélectionner dans la liste. Dans cet exemple, **itil**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ permet d'analyser l'autorisation, même au niveau du champ. Par exemple, Actif, Créé par, etc.



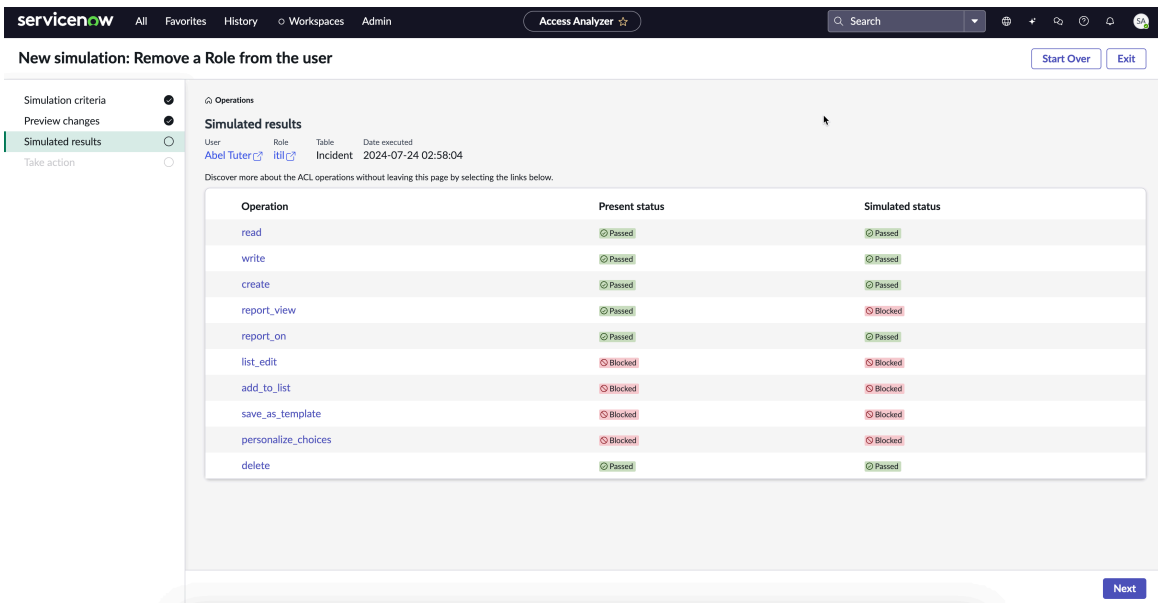
4. Sélectionnez **Suivant**.
5. Prévisualisez les modifications.
   Les rôles supprimés sont simulés dans les changements apportés à l'aperçu. Vous pouvez valider les rôles et les rôles enfants qui sont supprimés de l'utilisateur avant de passer à l'étape suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionnez **Suivant**.
7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.



Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez recommencer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Supprimer et terminer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer les actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

Les rôles sont supprimés avec succès de l'utilisateur. Vous pouvez vérifier l'accès à l'aide de l'analyseur d'accès. Pour en savoir plus sur la vérification de l'accès d'un utilisateur, reportez-vous à la section Analyseur d'accès.

Ajout de l'utilisateur à un groupe

Utilisez **l'option Simuler un ajout au groupe** pour simuler les changements d'accès de l'utilisateur pour une ressource (tables) lorsque l'utilisateur est ajouté à un groupe.

Avant de commencer

Rôle requis : administrateur

Activez la prise d'actions. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Procédure

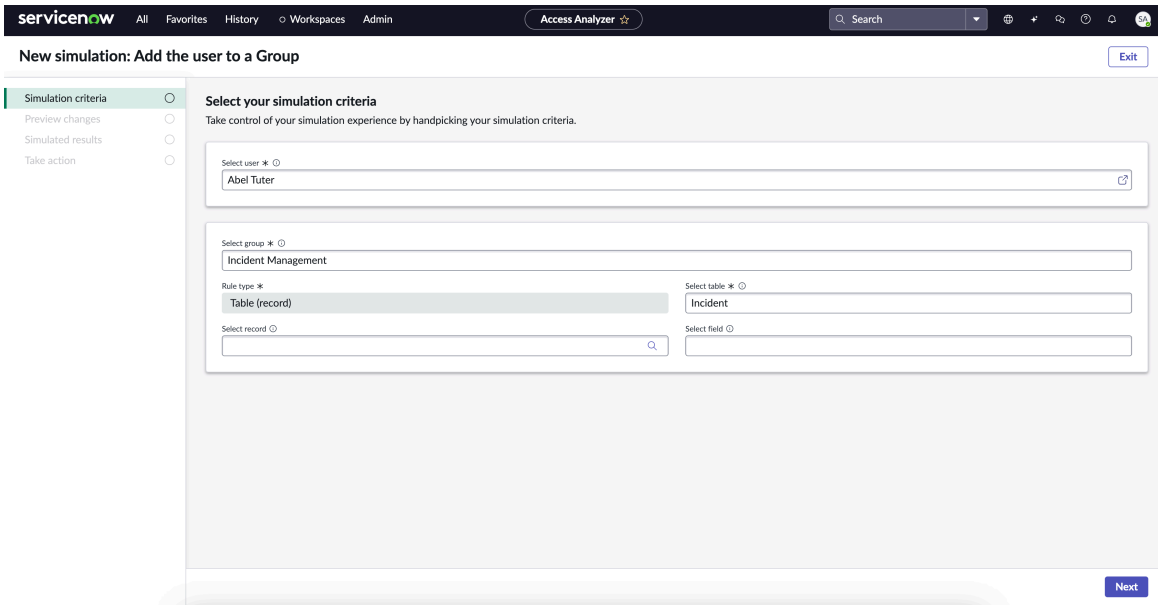
1. Accédez à la **Tout** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Ajouter l'utilisateur à un groupe.
3. Spécifiez les champs suivants pour vos critères de simulation :

Ajouter l'utilisateur à un groupe

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **Abel Tuter**.
Sélectionner un groupe *	Spécifiez un groupe à sélectionner dans la liste. Dans cet exemple, **Incident Management**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ permet d'analyser l'autorisation, même au niveau du champ. Par exemple, Actif, Créé par, etc.

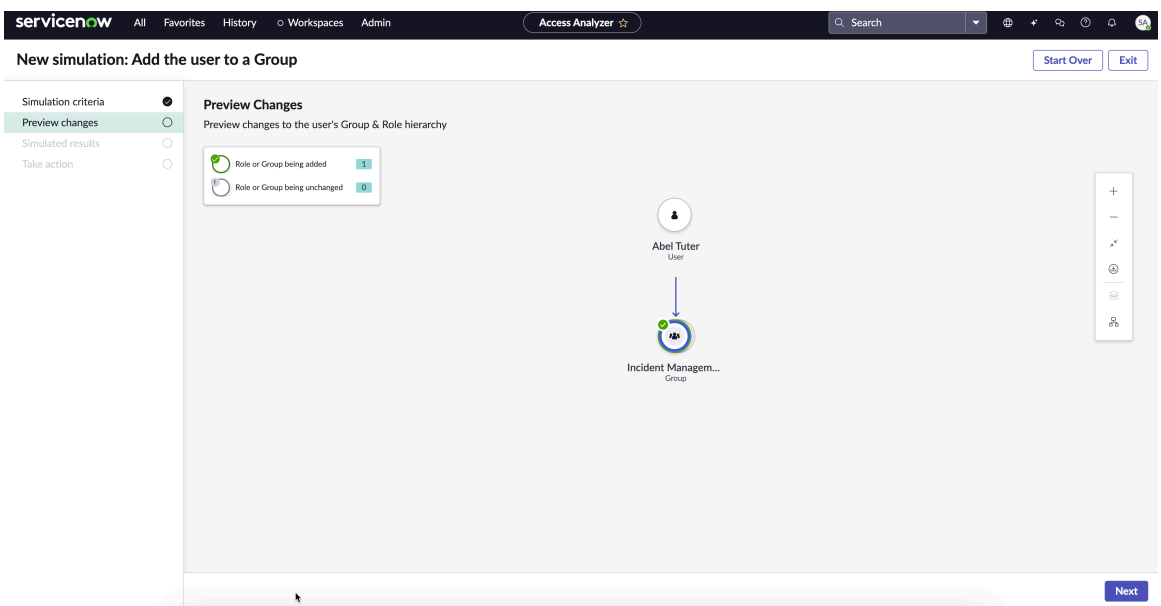
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



4. Sélectionnez **Suivant**.
5. Prévisualisez les modifications.

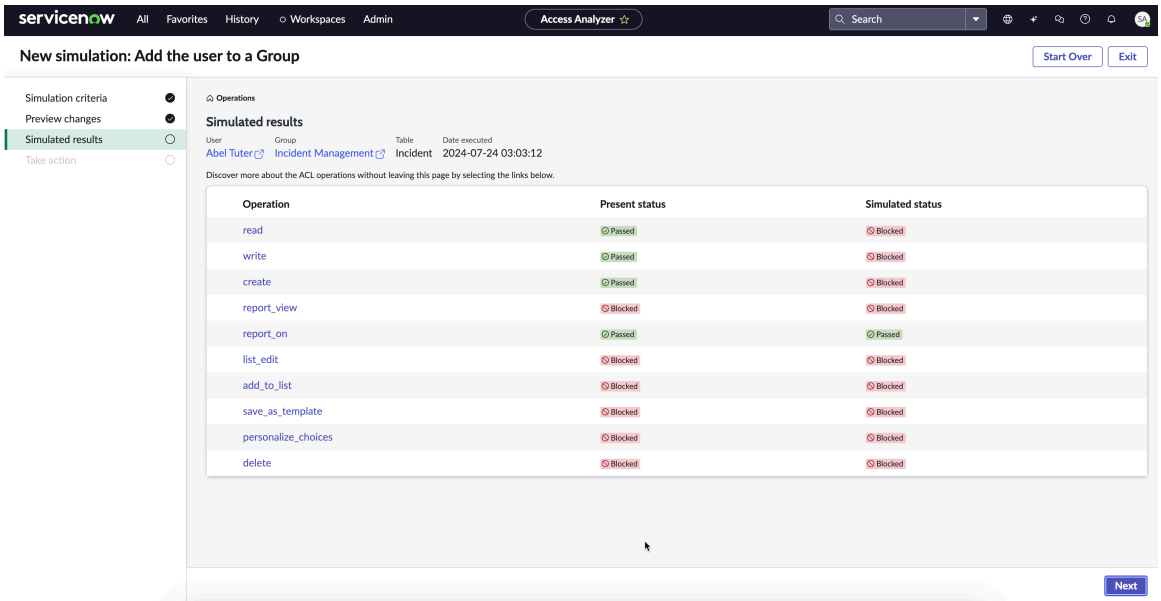
   Le groupe auquel l'utilisateur est affecté est simulé dans les modifications apportées à l'aperçu. Vous pouvez valider les changements avant de passer à l'étape suivante.



6. Sélectionnez **Suivant**.
7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez recommencer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Ajouter et terminez**.

Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer les actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

L'utilisateur est ajouté avec succès au groupe.

Suppression de l'utilisateur d'un groupe

Utilisez **l'option Simuler la suppression du groupe** pour simuler les changements d'accès de l'utilisateur à une ressource (tables) lorsque l'utilisateur est retiré d'un groupe.

Avant de commencer
Rôle requis : administrateur

Activez la prise d'actions. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).

Traduction automatique

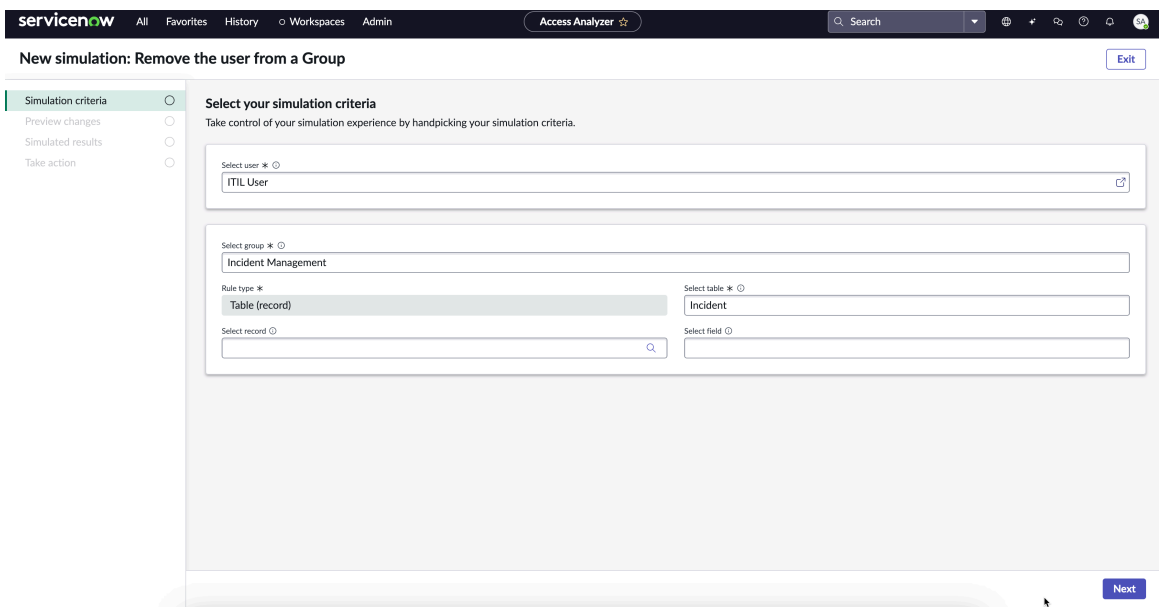
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Analyseur d'accès** > **Simulateur d'accès**.
2. Sélectionnez **Simuler** dans la section Supprimer l'utilisateur d'un groupe.
3. Spécifiez les champs suivants pour vos critères de simulation :

Supprimer l'utilisateur d'un groupe

Champ	Description
Sélectionner un utilisateur *	Spécifiez un nom d'utilisateur à sélectionner dans la liste. Dans cet exemple, **il s'agit de l'utilisateur ITIL**.
Sélectionner un groupe *	Spécifiez un groupe à sélectionner dans la liste. Dans cet exemple, **Incident Management**.
Type de règle *	Le type de règle est renseigné automatiquement et ne peut pas être modifié.
Sélectionner une table *	Spécifiez un nom de table à sélectionner dans la liste. Dans cet exemple, **Incident**.
Sélectionner un enregistrement	Spécifiez un nom d'enregistrement à sélectionner dans la liste.
Sélectionner un champ	Spécifiez un nom de champ à sélectionner dans la liste. Ce champ permet d'analyser l'autorisation, même au niveau du champ. Par exemple, Actif, Créé par, etc.



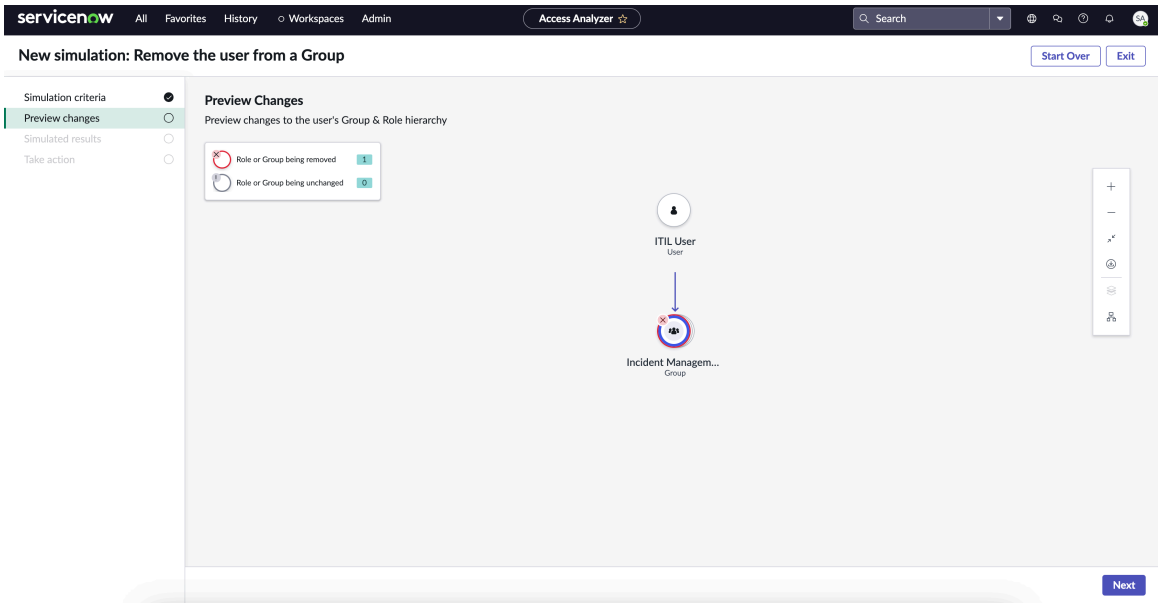
d

4. Sélectionnez **Suivant**.
5. Prévisualisez les modifications.

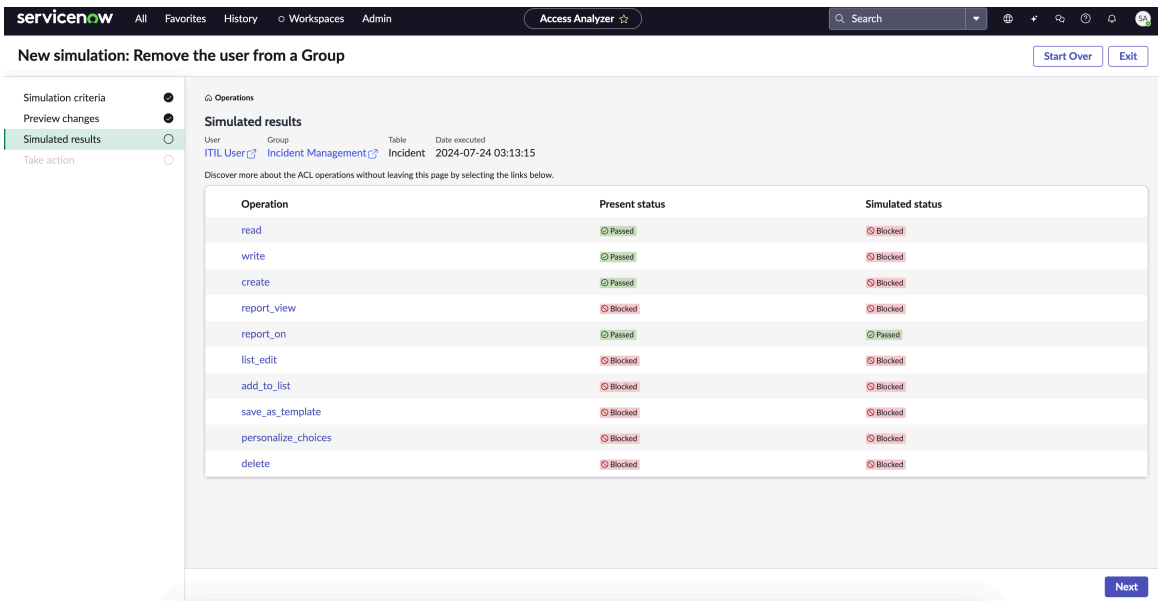
Le groupe à partir duquel l'utilisateur est supprimé est simulé dans l'aperçu des modifications. Vous pouvez valider les changements avant de passer à l'étape suivante.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Sélectionnez **Suivant**.
7. Validez **l'état actuel** et **l'état simulé** pour vérifier l'accès qui est **transmis** ou **bloqué** à l'utilisateur simulé.



Remarque :

- Si vous souhaitez en savoir plus sur l'ACL (opérations), sélectionnez les liens d'opération pour chaque enregistrement.
- Si vous souhaitez recommencer la simulation pour un autre rôle, sélectionnez **Recommencer**.
- Si vous souhaitez quitter la simulation, sélectionnez **Quitter**.

8. Sélectionnez **Suivant**.
9. Sélectionnez **Supprimer et terminer**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Si le simulateur d'accès n'est pas activé, vous ne pouvez pas terminer la simulation. Pour activer, sélectionnez **Activer les actions** et acceptez les informations juridiques.
- Si vous souhaitez masquer la simulation, sélectionnez **Masquer les actions**. Pour afficher et activer les actions, accédez aux paramètres. Pour plus d'informations, consultez Configuration du simulateur d'accès (Prendre des mesures).
- Si vous souhaitez quitter la simulation, sélectionnez **Ignorer et quitter**.

L'utilisateur a été supprimé avec succès de l'utilisateur.

Forum aux questions

Questions fréquemment posées sur l'utilisation du simulateur d'accès.

Forum aux questions

Questions	Explication
Comment puis-je commencer à utiliser le simulateur ?	Vous pouvez sélectionner l'option Simuler pour les différents scénarios que vous souhaitez simuler pour les utilisateurs et suivre les étapes.
Comment fonctionne le simulateur ?	Le simulateur d'accès simule l'accès à la table spécifiée pour l'utilisateur sélectionné et vous prévisualise les changements d'accès afin de prendre des décisions concernant la mise en service de l'accès.
Comment activer ou désactiver les actions dans le simulateur ?	Vous pouvez activer ou désactiver les actions dans le simulateur d'accès en accédant aux Paramètres ou pendant les étapes Prendre des mesures du processus de simulation.

Identité globale

Global Identity est un ServiceNow® produit qui permet d'identifier des utilisateurs uniques sur plusieurs instances.

Global Identity permet de gérer les utilisateurs, leurs attributs et d'autres données fondamentales sur ServiceNow® plusieurs ServiceNow® instances avec plusieurs instances.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorez l’ID fédéré



Découvrez les principales fonctionnalités et la valeur commerciale de Federated ID.

Accéder à l’ID fédéré



Accéder à l’ID fédéré.

Mise à jour des champs d’ID



Mettez à jour et configurez l’ID fédéré.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration de l'ID fédéré

Déterminez les utilisateurs dans plusieurs instances en fonction du nom d'utilisateur et de l'adresse e-mail, et fournissez un ID unique (ID fédéré) à l'utilisateur dans toutes les instances.

L'ID fédéré est utilisé pour identifier les utilisateurs sur plusieurs ServiceNow® instances. L'ID fédéré permet d'identifier l'utilisateur et de déterminer le nombre exact d'utilisateurs sur plusieurs instances. Pour plus d'informations, consultez ID fédéré.

Remarque :
Le nom d'utilisateur est requis pour générer des ID fédérés.

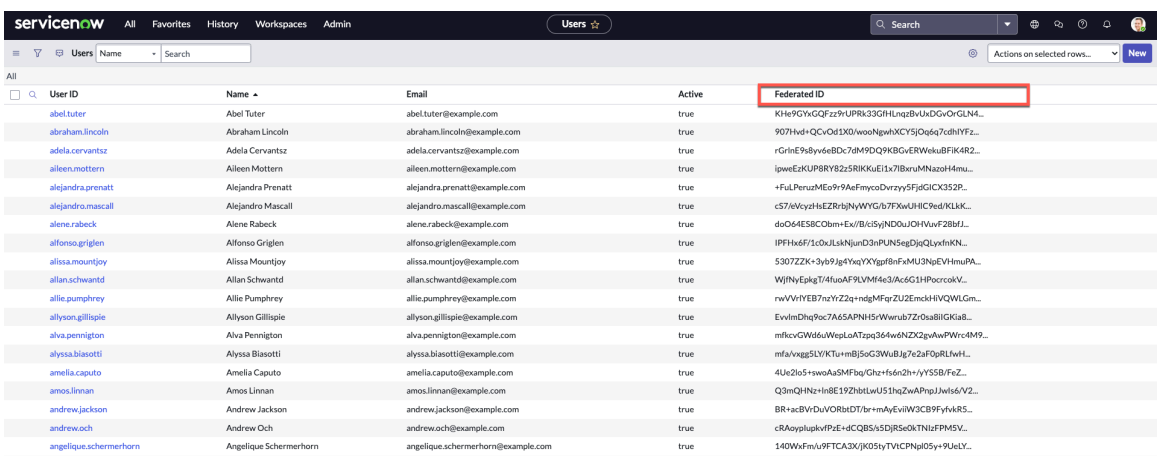
L'ID fédéré est un identificateur unique pour une identité à l'aide d'une fonction de hachage dans les ServiceNow® instances.

En utilisant **l'ID d'utilisateur** et **l'e-mail** de l'utilisateur dans les instances, l'ID fédéré est créé et affiché dans la table sys_user.

Après la mise à niveau vers la Xanadu version, le module d'extension Génération d'ID fédérés (com.glide.identity.globalid) est installé automatiquement sur toutes les instances.

Remarque :

- Le nom d'utilisateur est requis pour générer des ID fédérés.
- Le nom d'utilisateur et l'adresse e-mail sont utilisés pour générer des ID fédérés par défaut. Pour mettre à jour les champs permettant de générer des ID fédérés en fonction de vos besoins, reportez-vous à la section Mise à jour des champs d'ID.
- **Iamsync_admin** rôle est requis pour mettre à jour la configuration.
- Si des utilisateurs ont des noms d'utilisateur et une adresse e-mail en double, l'ID fédéré est généré pour un seul utilisateur. Si le nom d'utilisateur est nul ou vide, l'ID fédéré est nul.



Les changements de schéma après l'installation du module d'extension sont les suivants :

- Une nouvelle federated_id de colonne dans la table sys_user est créée.
- Nouvelle table : iamsync_type est renseigné automatiquement avec la configuration par défaut de la table sys_user .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

L'ID fédéré n'est pris en charge que pour la table sys_user et toutes les tables qui étendent la table sys_user.

Après la mise à niveau vers la Xanadu version, le module d'extension Génération d'ID fédérés (com.glide.identity.globalid) est installé automatiquement sur toutes les instances.

Accéder aux critères d'ID fédéré

Accédez aux critères d'ID fédéré pour connaître les champs d'ID utilisés pour générer l'ID fédéré.

Avant de commencer

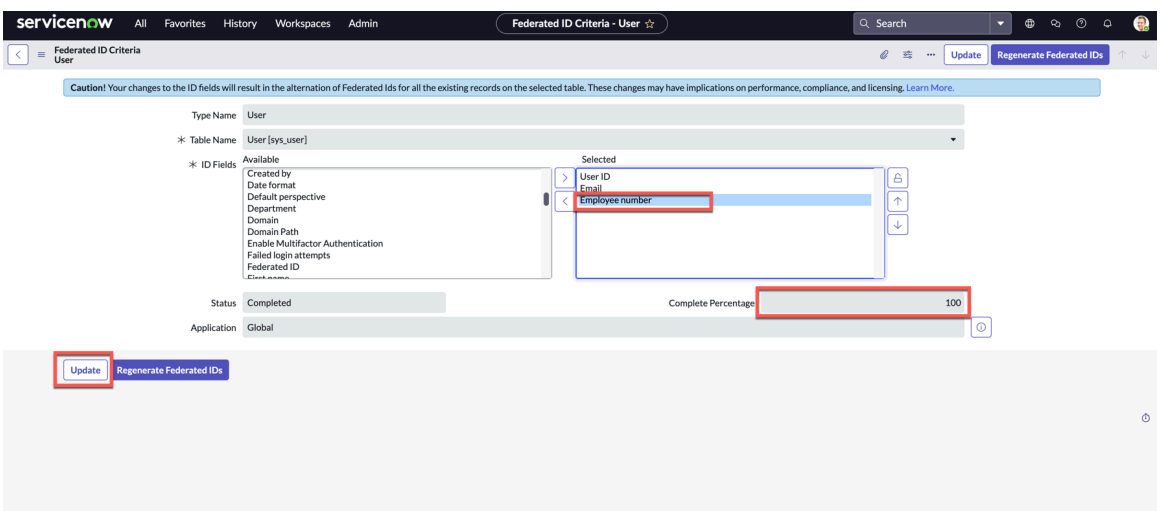
Rôle requis : iamsync_admin

Procédure

1. Accédez à la **Tout** > **Gérer l'ID fédéré** > **Critères d'ID fédéré**.
2. La page Critères d'ID fédérés affiche l'enregistrement avec les détails suivants :
   - Nom de type : **utilisateur**
   - Nom de la table : **Utilisateur [sys_user]**
   - Champs d'ID : **user_name (ID d'utilisateur), e-mail** (champs par défaut utilisés pour la génération d'ID fédérés).
   - État : **Terminé** (état de génération de l'ID fédéré). État disponible : **Prêt**, **En cours d'exécution**, **Terminé**, **Erreur**.

Remarque :

- Le nom d'utilisateur est requis pour générer des ID fédérés.
- Le nom d'utilisateur et l'adresse e-mail sont utilisés pour générer des ID fédérés par défaut.



Remarque :

Seuls les champs ID peuvent être mis à jour pour générer un nouvel ID fédéré pour les enregistrements existants. Pour en savoir plus, reportez-vous à la section Mise à jour des champs d'ID.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Mise à jour des champs d'ID

Mettez à jour les champs d'ID pour régénérer les ID fédérés en fonction des champs mis à jour.

Avant de commencer

Rôle requis : iamsync_admin

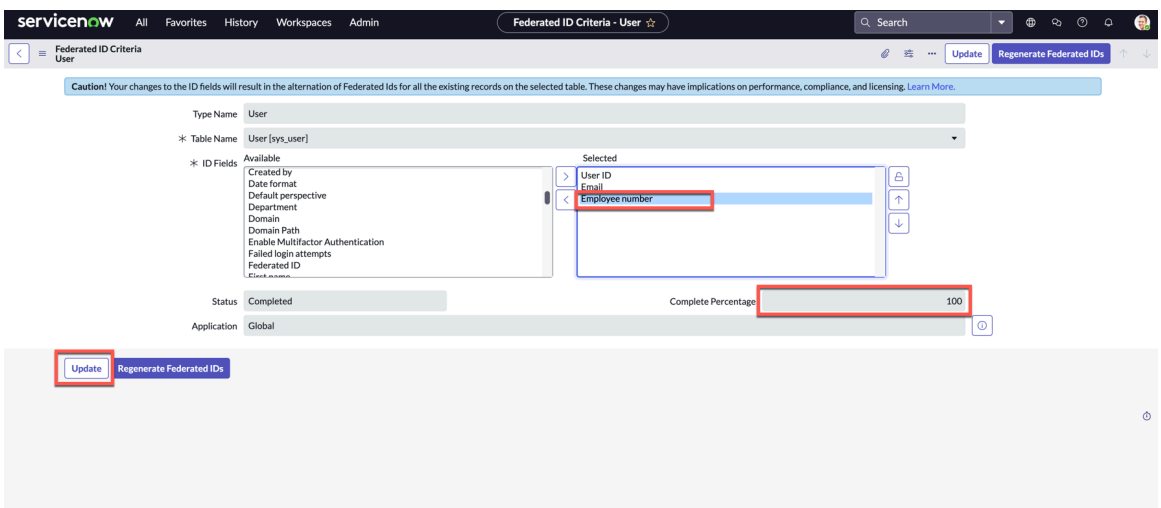
Remarque :
Tout changement apporté aux champs d'ID entraîne le changement des ID fédérés pour tous les enregistrements existants sur la table sélectionnée. Ces changements peuvent avoir des répercussions sur les performances, la conformité et l'octroi de licences.

Procédure

1. Accédez à la **Tout** > **Gérer l'ID fédéré** > **Critères d'ID fédéré**.
2. Sélectionnez le nom de type (**Utilisateur**).
3. Sélectionnez les nouveaux champs d'ID dans la page Utilisateur de critères d'ID fédérés que vous souhaitez ajouter à partir de la section Disponible à Sélectionné à l'aide des boutons fléchés.

   Par exemple, **Numéro d'employé**.

   Remarque :
   - Le nom d'utilisateur est requis pour générer des ID fédérés.
   - Le nom d'utilisateur et l'adresse e-mail sont utilisés pour générer des ID fédérés par défaut.
   - Si des utilisateurs ont des noms d'utilisateur et une adresse e-mail en double, l'ID fédéré est généré pour un seul utilisateur. Si le nom d'utilisateur est nul ou vide, l'ID fédéré est nul.



   Désormais, le **numéro d'employé** sélectionné devient un autre attribut pour générer l'ID fédéré.

4. Sélectionnez **Mettre à jour** pour générer les ID fédérés.

   Remarque :
   Sélectionnez **d'abord Mettre à jour** , puis vérifiez le pourcentage d'achèvement (100) avant de lancer une autre mise à jour.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Le pourcentage d'état indique la génération d'ID fédérés pour toutes les identités dans les instances.

Remarque :

- Tant que la tâche de mise à jour précédente n'est pas terminée, ne modifiez pas le champ.
- Les champs qui sont mis à jour doivent être de type chaîne.
- Les champs qui ne peuvent pas être sélectionnés en tant que champs d'ID sont les suivants :
  - Champs au niveau du système
  - Champs de Chiffrement Edge
  - Champs de mot de passe.

5. Accédez à la table sys_user pour afficher les nouveaux ID fédérés générés suite à la mise à jour des champs d'ID.

Remarque :
Sélectionnez **Régénérer les ID fédérés** si un utilisateur est créé ou mis à jour via des importations XML, des mises à jour de base de données de bas niveau, ou si l'instance ne fonctionne pas correctement. Si vous sélectionnez **Régénérer les ID fédérés**, régénère les ID de tous les utilisateurs, à l'aide des critères de champ ID actuels.

Identity Center

Vous permet de surveiller, de gérer et de minimiser les risques et les failles de sécurité fondés sur l'identité.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale d’Identity Center.

Activer



Découvrez comment activer Identity Center.

Mesures d’identité pour les administrateurs



Savoir comment les autorisations sont évaluées

Identity Center pour les utilisateurs



Obtenez des détails sur les questions fréquemment posées sur l’analyseur d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer Identity Center

Identity Center est une collection d'attributs d'utilisateur, d'accès, d'appareils, d'historique de connexion, d'activité de sécurité et bien plus encore.

Identity Center offre des options pour surveiller, gérer et minimiser les risques et les failles de sécurité liés à l'identité.

Identity Center est un guichet unique pour surveiller, gérer et minimiser les risques et les failles de sécurité fondés sur l'identité sur ServiceNow.

Pour activer Identity Center, installez le module d'extension Identity Center (com.snc.identity_center). Identity Center est disponible pour l'utilisateur final afin d'afficher les détails sur les sessions actives, l'historique de connexion et les appareils approuvés avec Identity Center. Pour plus d'informations, reportez-vous à la section Identity Center pour les utilisateurs.

Activation d'Identity Center

Pour Identity Center, installez le module d'extension Identity Center (com.snc.identity_center).

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Recherchez le module d'extension Identity Center (com.snc.identity_center) à l'aide des critères de filtre et de la barre de recherche.

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Identity Center pour les utilisateurs

Affichez les détails de vos sessions actives, de votre historique de connexion et de vos appareils approuvés avec Identity Center.

Identity Center est une collection d'attributs d'utilisateur, d'appareils, d'historique de connexion, d'activité de sécurité et bien plus encore. Il fournit une vue à volet unique de toutes les données avec des contrôles de sécurité et des fonctionnalités de notification supplémentaires.

Avec Identity Center, vous pouvez afficher les détails de vos sessions actives, de votre historique de connexion et de vos appareils approuvés.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pour accéder à l'Identity Center pour les utilisateurs, accédez à l'un des éléments suivants :

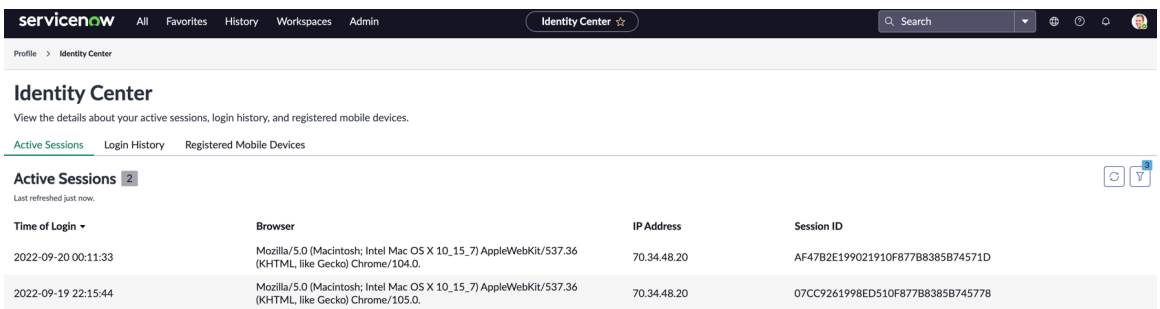
- Sur Now Platform, accédez à **Tout** > **Libre-service** > **Mon profil** et sélectionnez **Afficher Identity Center** dans la section Liens connexes.

  Remarque :
  Vous pouvez également accéder à votre profil en sélectionnant votre nom d'utilisateur dans l'en-tête de l'instance.



- Sur Now Support, sélectionnez le profil, puis sélectionnez **Afficher Identity Center** en bas de la page.

La page Identity Center s'affiche comme suit :



Identity Center comporte les onglets suivants :

- Sessions actives
- Historique de connexion
- Équipements mobiles enregistrés

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez sélectionner ces onglets pour afficher des détails tels que le navigateur, les adresses IP, les informations de relation de session, les informations de connexion, vos appareils mobiles enregistrés.

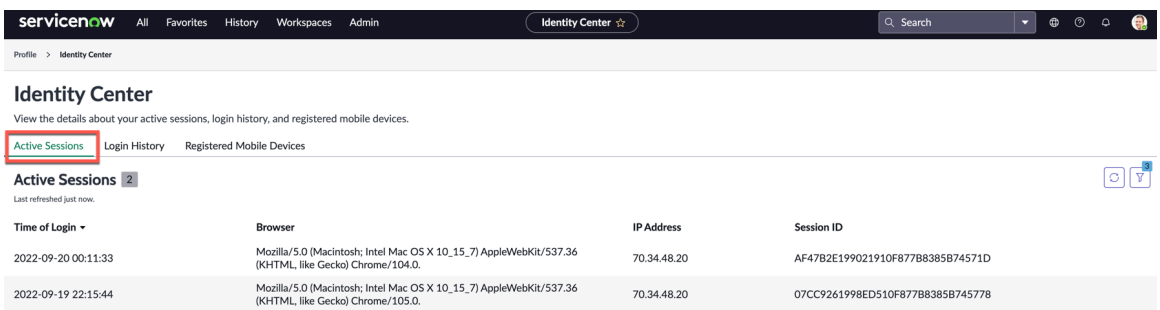
Afficher les sessions actives

Affiche les informations sur les sessions utilisateur.

Les sessions actives sont les sessions ouvertes sur l'instance actuelle ServiceNow® avec différents navigateurs ou appareils.

L'onglet Sessions actives de l'Identity Center vous permet d'identifier vos sessions en fonction du navigateur, de l'adresse IP et de l'ID de sessions. À l'aide de ces informations, vous pouvez effectuer les actions nécessaires, telles que prolonger ou mettre fin à la session.

L'utilisation de ces informations peut aider à déterminer si les sessions sont réelles et ne posent pas de problème de sécurité.



Afficher l'historique de connexion

Fournit des détails sur votre historique de connexion.

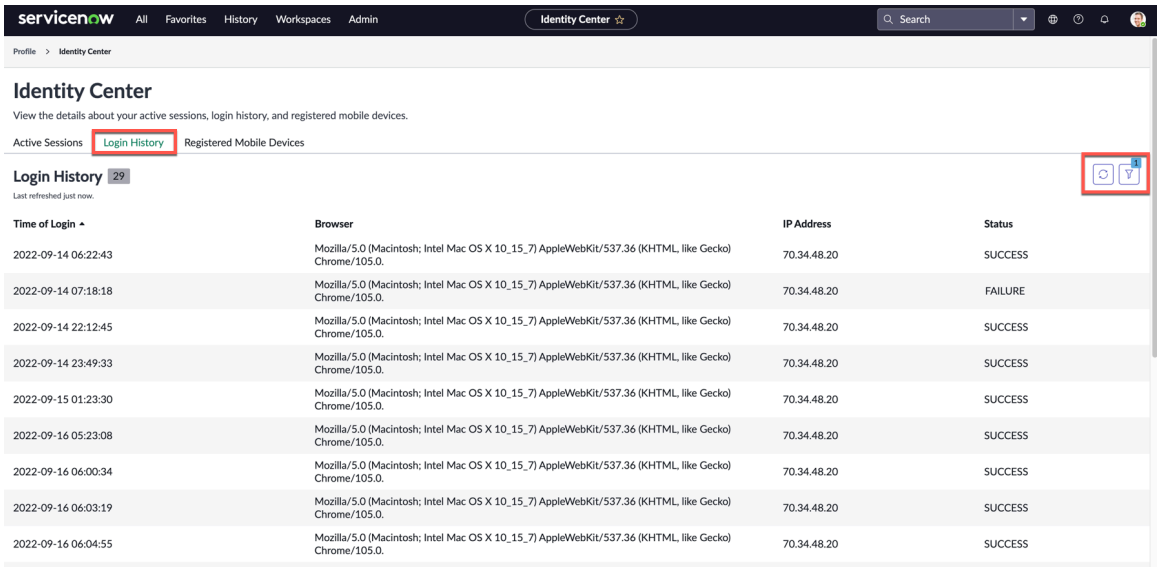
L'onglet Historique de connexion de l'Identity Center vous aide avec vos informations de connexion et l'état de votre connexion.

Vous pouvez utiliser les filtres pour spécifier des actions de connexion afin d'aider les enquêtes de sécurité. Le filtre peut aider à déterminer si l'activité était réelle ou suspecte et à signaler l'information à votre administrateur.

La pagination dans l'historique de connexion est de 20 par défaut et peut être définie sur un maximum de 100.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Voici quelques-uns des autres détails de l'historique de connexion :

- L'heure de connexion est l'heure de mise à jour à laquelle les équipements mobiles sont utilisés pour accéder à l'instance.
- Les enregistrements sont stockés dans Identity Center pendant 30 jours.

Afficher les équipements mobiles enregistrés

Fournissez des détails sur votre mobile enregistré sur l'instance ServiceNow .

L'onglet Équipements mobiles enregistrés dans Identity Center affiche les détails sur vos appareils enregistrés qui ont été utilisés pour accéder à l'instance ServiceNow .

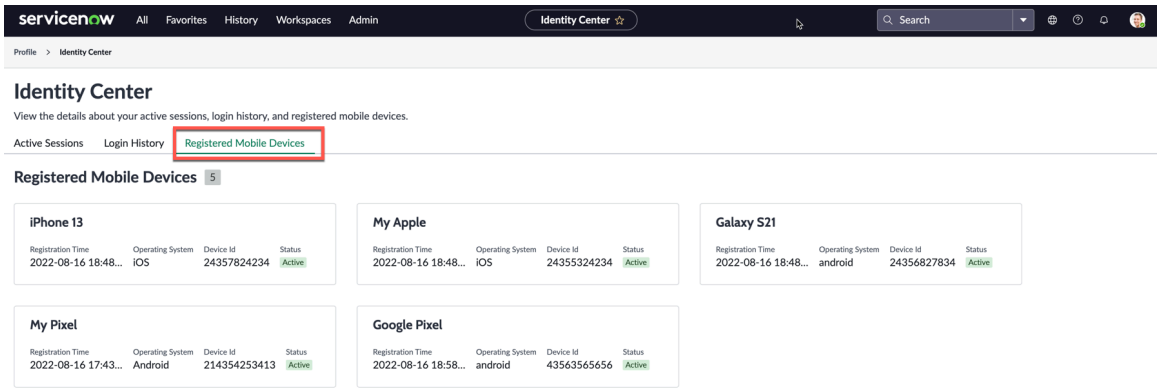
Si le module d'authentification adaptative est activé et qu'un appareil mobile enregistré est inscrit, Identity Center affiche les détails de vos appareils enregistrés.

En outre, il affiche également des détails sur les appareils tels que le système d'exploitation, l'ID de l'appareil et l'état de l'appareil, ainsi que l'heure d'enregistrement de l'appareil.

Pour enregistrer votre équipement mobile, vous devez vous assurer que le module d'extension Authentification adaptative (`com.snc.adaptive_authentication`) est installé et que vous avez activé votre fonctionnalité Application mobile de confiance. Pour plus d'informations, consultez Activer l'application mobile de confiance.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Mesures d’identité pour les administrateurs

Affichez les tendances des utilisateurs, des utilisateurs privilégiés, des sessions actives et du compte intégré sur votre ServiceNow instance.

Identity Metrics pour les administrateurs présente les tendances suivantes :

- Utilisateurs
- Utilisateurs privilégiés
- Comptes d’intégration ou non-humains
- Sessions actives
- Sessions inactives

Pour en savoir plus, consultez Mesures du Centre de sécurité.

Système de gestion des identités entre domaines (SCIM)

L’API SCIM (System for Cross-domain Identity Management) fournit des points de terminaison pour créer, lire, mettre à jour et supprimer des opérations sur les utilisateurs et les groupes à l’aide du protocole SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Fournisseur SCIM



Le fournisseur SCIM synchronise les changements apportés aux identités dans l'IdP, y compris la création, la mise à jour ou la suppression des enregistrements.

Client SCIM



Le client SCIM est utilisé pour créer, mettre à jour et supprimer des ressources d'identité dans un système qui prend en charge les demandes REST conformes à SCIM.

Traduction automatique

Le protocole SCIM est un protocole HTTP au niveau de l'application basé sur la norme HTTP (RFC7230). Utilisez cette API pour mettre en service et gérer les données d'identité, telles que les utilisateurs et les groupes. Utilisez l'API sur le Web et dans des environnements inter-domaines, tels que les fournisseurs de services d'entreprise à cloud ou les scénarios inter-cloud.

Pour accéder à cette API, vous devez activer le module d'extension SCIM v2 - ServiceNow® Cross-domain Identity Management (com.snc.integration.scim2).

Pour en savoir plus sur l'API SCIM, consultez l'API System for Cross-domain Identity Management (SCIM).

Fournisseur SCIM

Le fournisseur de services provisionne les utilisateurs et les groupes à l'aide de l'API SCIM.

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



En savoir plus sur le fournisseur SCIM.

Activer



Activer SCIM.

Personnalisation SCIM



Obtenez des détails sur la personnalisation de SCIM.

Définition de la source



En savoir plus sur la définition de source pour SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration du fournisseur SCIM

Le fournisseur de services provisionne les utilisateurs et les groupes à l'aide de l'API SCIM.

En tant que fournisseur SCIM, les ServiceNow schémas prennent en charge les API SCIM pour mettre en service les utilisateurs et les groupes.

Le fournisseur SCIM synchronise les changements apportés aux identités dans l'IdP, y compris la création, la mise à jour ou la suppression des enregistrements. Ces modifications sont automatiquement synchronisées avec le fournisseur selon le protocole SCIM. En outre, l'IdP peut lire les identités du fournisseur pour les ajouter à l'annuaire IdP. L'IdP peut alors détecter des valeurs incorrectes dans le fournisseur qui pourraient créer des failles de sécurité. La synchronisation permet aux utilisateurs finaux d'accéder de manière transparente aux applications qui leur sont affectées, avec des profils et des autorisations à jour.

Configurations du fournisseur SCIM

Pour configurer le fournisseur SCIM, effectuez les tâches suivantes :

- Activez le module d'extension **SCIM v2 - ServiceNow Cross-domain Identity Management** . Pour en savoir plus, reportez-vous à Activation du module d'extension SCIM.
- Activez les autres modules d'extension que d'autres modules d'extension requis pour SCIM :
  - OAuth 2.0
  - Fournisseur d'API REST
  - Politique d'accès REST API
- Ajoutez le rôle scim_admin dans le cadre du service SCIM.

> **⚠ Avertissement :**
> Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, dans lequel le scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Tables

Deux tables, sys_user et sys_group, contiennent les attributs SCIM qui ne sont pas mappés aux tables existantes ServiceNow . Pour en savoir plus sur les tables, reportez-vous aux tables spécifiques à SCIM .

Activation du module d'extension SCIM

Pour l'activation SCIM, installez le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2).

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtre et la barre de recherche pour rechercher le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management (com.snc.integration.scim2).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.

3. Sélectionnez **Installer** pour lancer le processus d'installation.

> **Remarque :**
> Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Didacticiel : Configurer SCIM pour l'attribution d'utilisateurs avec un fournisseur

La configuration de SCIM provisionne et annule automatiquement l'approvisionnement des utilisateurs et des groupes en ServiceNow utilisant le service de mise en service des fournisseurs.

Avant de commencer

Installez le module d'extension SCIM.

Rôle requis : scim_admin

> **Avertissement :**
> Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, dans lequel le scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Pourquoi et quand exécuter cette tâche

Vous pouvez provisionner des utilisateurs à l'aide de SCIM à l'aide des méthodes d'authentification suivantes :

- Mise en service d'un utilisateur à l'aide de l'authentification de base
- Mise en service d'un utilisateur à l'aide d'OAuth

Mise en service d'un utilisateur à l'aide de l'authentification de base

La configuration de SCIM provisionne et annule automatiquement l'approvisionnement des utilisateurs et des groupes en ServiceNow utilisant le service de provisionnement des fournisseurs avec authentification de base.

Avant de commencer

Rôle requis : scim_admin

> **Avertissement :**
> Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, dans lequel le scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Vous devez activer le module d'extension SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès REST API** pour vérifier les détails des politiques d'accès REST API.
2. Sur la page Politique d'accès API, cliquez sur l'enregistrement **Politique d'API SCIM** .
3. Vérifiez que l'enregistrement **d'authentification de base de l'API SCIM** est disponible dans les sections Profils d'authentification.
4. Vérifiez si le champ **Authentification de base** est spécifié avec un enregistrement **de l'API SCIM** qui a été configuré ou vérifié précédemment en tant que registre d'application.
5. Créez les configurations requises du côté du fournisseur.
6. Testez la connexion pour vous assurer que le fournisseur peut se connecter à ServiceNow.

Remarque :
Si la connexion échoue, assurez-vous que votre ServiceNow compte dispose des autorisations d'administrateur et réessayez.

Mise en service d'un utilisateur à l'aide d'OAuth

Configurez le fournisseur pour les mises en service SCIM et l'annulation automatiques de l'approvisionnement des utilisateurs et des groupes en ServiceNow utilisant le service de mise en service des fournisseurs avec OAuth.

Avant de commencer

Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, dans lequel le scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Vous devez activer le module d'extension SCIM.

Procédure

1. Accédez à la **Tout** > **OAuth système** > **Registre d'application**.
2. Sur la page Registres d'application, cliquez sur l'enregistrement **de l'API SCIM** .
3. Vérifiez les détails de **l'enregistrement de l'API SCIM** .

   Ces détails doivent être fournis lors de la configuration de l'application ServiceNow sur Azure AD.
4. Accédez à la **Tout** > **Services web du système** > **Politiques d'accès REST API** pour vérifier les détails des politiques d'accès REST API.
5. Sur la page Politique d'accès API, cliquez sur l'enregistrement **Politique d'API SCIM** .
6. Vérifiez que l'enregistrement **SCIMAPIOAuthOnly** est disponible dans les sections Profils d'authentification.
7. Vérifiez si le champ **Entité OAuth** est spécifié avec un enregistrement **de l'API SCIM** qui a été configuré ou vérifié précédemment en tant que registre d'application.
8. Créez les configurations requises du côté du fournisseur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

9. Testez la connexion pour vous assurer que le fournisseur peut se connecter à ServiceNow.

Remarque :
Si la connexion échoue, assurez-vous que votre ServiceNow compte dispose des autorisations d'administrateur et réessayez.

Dépannage SCIM

Scénarios d'erreur courants lors de l'intégration à SCIM.

URL API REST non valide

Action : entrez une URL d'API valide. Serait en mesure de vérifier l'URL REST API dans **l'explorateur d'API REST**.

Aucune URL de redirection n'est définie dans l'instance ServiceNow

Action : saisissez une URL de redirection valide pour l'entité SCIM OAuth dans ServiceNow. Entrez l'URL de redirection lors de la configuration de l'entité OAuth dans ServiceNow.

Lorsque l'URL de redirection est différente de celle de la demande

Action : le **« redirect_url** » fourni dans « **Point de terminaison d'autorisation »** doit être identique à l'entité OAuth configurée dans ServiceNow.

Remarque :

Cette erreur se produit lorsqu'il y a une incompatibilité entre Azure « Point de terminaison d'autorisation » et ServiceNow « URL de redirection »

Lorsqu'un secret client non valide est transmis

Action : la valeur saisie dans « Secret client » doit être identique à celle de l'entité OAuth configurée dans ServiceNow.

Lorsqu'un « ClientId » non valide est transmis dans Azure « Authorization EndPoint »

Action : la valeur saisie pour le paramètre « client_id » dans « Point de terminaison d'autorisation » doit être identique à celle de l'entité OAuth configurée dans ServiceNow.

Personnalisation SCIM

Personnalisez les protocoles SCIM pour votre gestion des identités.

La personnalisation SCIM vous permet d'effectuer les opérations suivantes :

- Prise en charge des champs personnalisés sur les tables sys_user et sys_user_group via la génération dynamique de schémas d'extension.
- Offrez la possibilité de remplacer les mappages SCIM par défaut.

Un administrateur SCIM peut définir des schémas d'extension personnalisés pour les ressources utilisateur et groupe. Les attributs définis dans le schéma d'extension personnalisé peuvent être mappés à des champs dans les tables sys_user ou sys_user_group.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Configurations de la personnalisation SCIM

Pour la personnalisation SCIM, vous devez effectuer les tâches suivantes :

- Définissez un schéma d'extension personnalisé pour les utilisateurs et les groupes dans la table Schéma d'extension SCIM. Pour plus d'informations, Créer un schéma d'extension SCIMreportez-vous à la section .
- Créez des entités dans une définition ETL pour les attributs de schéma personnalisés. Les entités sont créées pour la table cible mappée avec les attributs sys_user ou sys_user_group. Pour plus d'informations, reportez-vous à la section Créer une définition SCIM ETL.
- Créez un mappage RTE entre ces deux entités. Pour plus d'informations, reportez-vous à la Créer une définition SCIM ETLprocédure 5 .
- Envoyer des attributs de schéma personnalisés avec des données dans la charge utile de la demande d'API SCIM.

L'API SCIM appelle le moteur RTE avec le mappage défini. Les données sont stockées dans les champs respectifs de la table cible tels que définis dans le mappage.

Propriétés et schémas de personnalisation SCIM

La personnalisation SCIM inclut les propriétés suivantes, les schémas pris en charge et les schémas non pris en charge.

Propriétés

La personnalisation SCIM ajoute les propriétés système suivantes.

Propriétés

Nom	Description
com.snc.integration.scim2.max.member.count	Le nombre maximal de membres SCIM.
com.snc.integration.scim2.resolve.external.id.conflict	Résoudre les ressources SCIM en fonction de la définition de source du client demandeur si plusieurs ressources sont trouvées avec un filtre SCIM d'ID externe. **Remarque :** Comme condition préalable, si la mise en service est effectuée à partir de plusieurs sources, celles-ci doivent être définies dans la table Définition de source SCIM. Si les sources ne sont pas définies ou si cette propriété est inactive, toutes les ressources correspondantes sont renvoyées avec une réponse de filtre d'ID externe.
com.snc.integration.scim2.user.etl.definition	ID de définition ETL de l'utilisateur SCIM.
com.snc.integration.scim2.group.etl.definition	ID de définition ETL du groupe SCIM.
com.snc.integration.scim2.rte.verbose.logging.enabled	Activer la journalisation détaillée pour les définitions RTE d'utilisateur et de groupe SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés (suite)

Nom	Description
com.snc.integration.scim2.string.field.validation.enable	Validation de la longueur des champs. Cette propriété active la validation au lieu de tronquer et d'enregistrer le champ.
com.snc.integration.scim2.provider.custom.script.id	ID de la bibliothèque de script pour personnaliser les réponses SCIM.

Schémas pris en charge

La personnalisation SCIM ajoute les schémas pris en charge suivants.

Schémas pris en charge

Schémas	Description	Préfixe	Exemple
urn:ietf:params:scim:schemas:core:2.0:User	Inclut les attributs principaux des ressources.	*urn:ietf:params:scim:schemas:core:2.0:User*	nom.deuxième prénom
urn:ietf:params:scim:schemas:extension:servicenow:2.0:User	Inclut les mappages de ServiceNow à SCIM (en anglais seulement)	*urn:ietf:params:scim:schemas:extension:servicenow:2.0:User*	servicenow.manager.value
urn:ietf:params:scim:schemas:extension:servicenow:custom:2.0:User	Inclut les attributs customisés qui ne sont pas mappés dans le cadre de l'extension principale ou du schéma d'extension ServiceNow .	*urn:ietf:params:scim:schemas:extension:servicenow:custom:2.0:User*	identificateur personnalisé.social

Schéma non pris en charge

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User: inclut les attributs couramment utilisés pour représenter les utilisateurs qui appartiennent à une entreprise ou une entreprise ou agissent en son nom.

Remarque :
Le schéma Enterprise est un schéma valide, mais ses attributs sont mappés à n'importe quelle table. Étant donné que la persistance de la base de données n'est pas prise en charge, aucune erreur ne s'affiche si un schéma d'entreprise est inclus dans le corps de la demande.

Créer un schéma d'extension SCIM

Créez des attributs personnalisés à mapper aux champs qui ne sont pas mappés dans le cadre du schéma principal ou du schéma d'extension ServiceNow .

Avant de commencer
Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle admin, où le rôle scmin_admin peut insérer de nouveaux enregistrements dans les tables afin de contourner la logique métier ou la protection ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

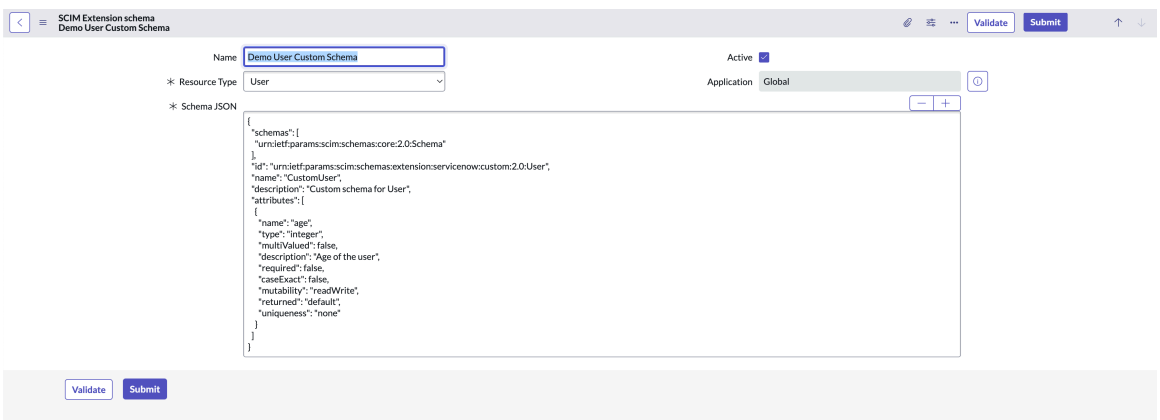
Procédure

1. Accédez à la **Tout** > **SCIM** > **Schémas d'extension SCIM**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

> **Remarque :**
> Un seul schéma d'extension peut être mappé au champ **Type de ressource** . Par exemple, Utilisateur en tant que type de ressource peut être mappé à un schéma d'extension utilisateur.

Schéma d'extension SCIM

Champ	Description
Nom	Nom du schéma des extensions.
Actif	Option permettant d'activer le schéma. Sélectionnez ce champ si l'enregistrement doit être considéré comme un schéma d'extension personnalisé. Un seul enregistrement de schéma d'extension personnalisé peut être actif à la fois pour un type de ressource spécifique, que ce soit pour le type Utilisateur ou Groupe.
Type de ressource	Type de ressource qui doit être mappé au schéma des extensions. Les options sont les suivantes : ○ **Utilisateur** ○ **Groupe**
Application	Le périmètre de l'application pour cet enregistrement.
JSON de schéma	Détails dans les schémas JSON. Pour plus d'informations sur la définition du schéma d'extension avec des attributs, consultez Datatracker .



4. Validez les attributs en cliquant sur **Valider**.
5. Cliquez sur **Envoyer**.

Résultats

Le schéma d'extension avec des attributs personnalisés liés au type de ressource Utilisateur ou Groupe est créé. Utilisez les définitions SCIM ETL pour mapper les

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

ressources en fonction du schéma d'extension sur la table sys_user et sys_user_group. Pour plus d'informations, consultez Créer une définition SCIM ETL.

Créer une définition SCIM ETL

Utilisez les définitions SCIM ETL pour mapper les attributs personnalisés sur les tables sys_user ou sys_user_group.

Avant de commencer
Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle admin, où le rôle scmin_admin peut insérer de nouveaux enregistrements dans les tables afin de contourner la logique métier ou la protection ACL.

Remarque :

- Les définitions ETL de groupe SCIM et d'utilisateur SCIM font partie du système de base pour le mappage des ressources. Vous pouvez utiliser les mêmes mappages de ressources et modifier les critères selon vos besoins, ou créer de nouveaux mappages de ressources.
- Il n'y a pas de prise en charge des champs [*] via RTE dans le mappage SCIM.

Procédure

1. Suivez les instructions des définitions Créer un chargement, une transformation d'extrait (ETL).
2. Ouvrez l'enregistrement nouvellement créé et affichez les détails.
3. Dans la section ETL Entities, créez une entité en cliquant sur **Nouveau**.
   Vous devez créer des entités pour les utilisateurs suivants :
   - scim-user : pour les champs qui proviennent de SCIM.
   - Table utilisateur (sys_user) ou groupe (sys_user_group) : pour les champs que vous souhaitez mapper à partir de la table de base de données avec SCIM. Par exemple, pour personnaliser les détails de l'utilisateur via SCIM, vous pouvez utiliser la table sys_user.

   a. Renseignez les champs du formulaire.

Formulaire Entité ETL

Champ	Description
Nom	Nom de l'entité ETL.
Application	Le périmètre de l'application pour cet enregistrement.
Table	Table cible pour l'entité ETL.
Définition	Entité ETL sélectionnée.
Chemin d'accès	Chemin d'accès unique pour cette entité. Ne spécifiez aucun chemin d'accès pour l'entité représentant la table de jeux d'importation. Lorsqu'une entité représente une collection, le chemin d'accès doit se terminer par un astérisque

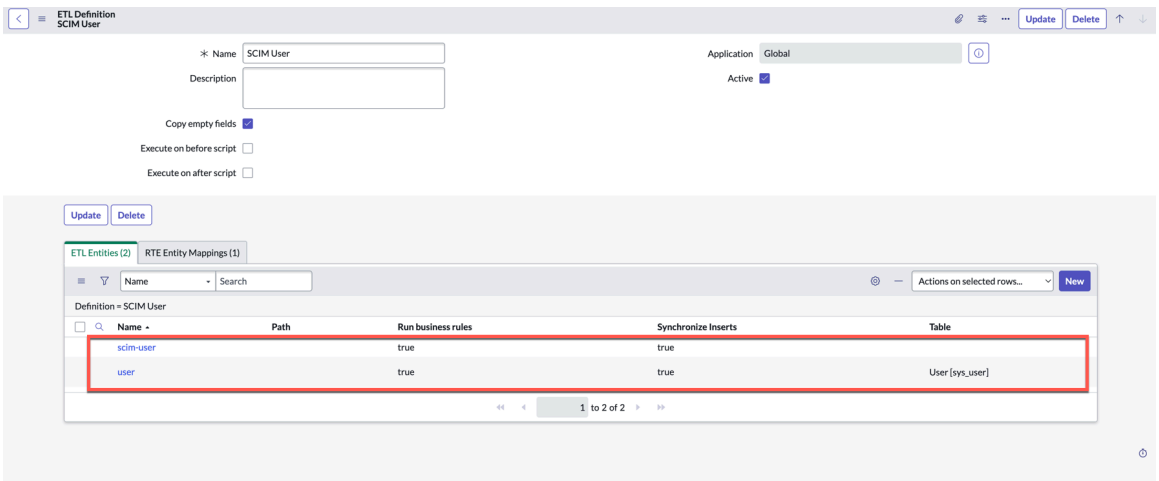
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	[*]. Cette exigence s’applique aux entrées intermédiaires et à l’entité de la table cible.
Synchroniser les insertions	Option permettant de garantir uniquement un enregistrement avec des valeurs de champ fusionnées uniques en synchronisant les insertions d’enregistrement.
Exécuter les règles métier	Option d’exécution des règles métier.

b. Cliquez sur **Envoyer**.

Les entités ETL sont créées pour les tables scim-user et user. Vous devez créer des champs d’entité ETL au sein de ces entités ETL et mapper les deux entités en créant un mappage d’entités RTE.



4. Créez les entités et mappez-les.

a. Ouvrez l’enregistrement soumis (scim-user et user).

b. Dans les champs Entité ETL, ajoutez les champs en cliquant sur **Nouveau**.

c. Renseignez les champs du formulaire.

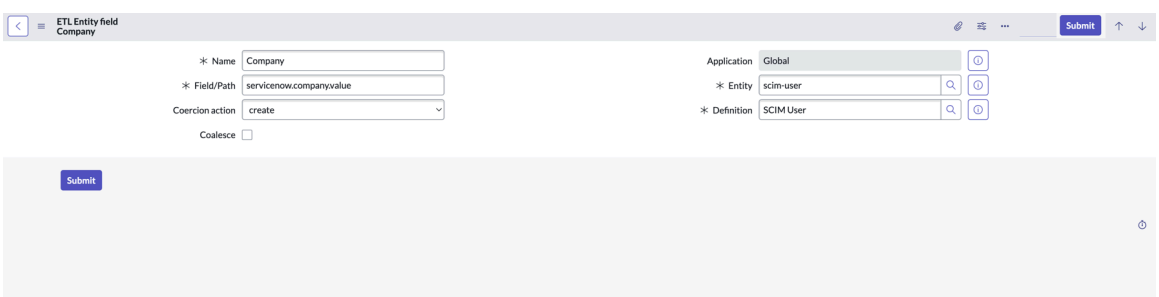
Formulaire Entité ETL

Champ	Description
Nom	Nom de la définition de champ Entité ETL.
Application	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Champ/chemin d'accès	Ce champ est soit une colonne, soit un chemin d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	▪ Le champ est un nom de colonne lorsque l'entité est la table d'importation ou la table cible. ▪ Le champ est un chemin d'accès lorsque le champ possède des structures imbriquées.
Entité	Entité à laquelle cette opération s'applique. Choisissez l'entité à l'aide de l'icône de recherche.
Action de forçage	Ce que le système doit faire si une référence ou un choix est introuvable. Les options sont les suivantes : ▪ **Créer** : permet de créer une référence ou un choix. Affectez la référence ou le choix à l'enregistrement actuel. ▪ **Rejeter** : n'enregistrez pas l'enregistrement complet dans la base de données. ▪ **Ignorer** : définir la valeur actuelle comme vide.
Définition	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Fusion	Option permettant d'interroger les enregistrements existants.



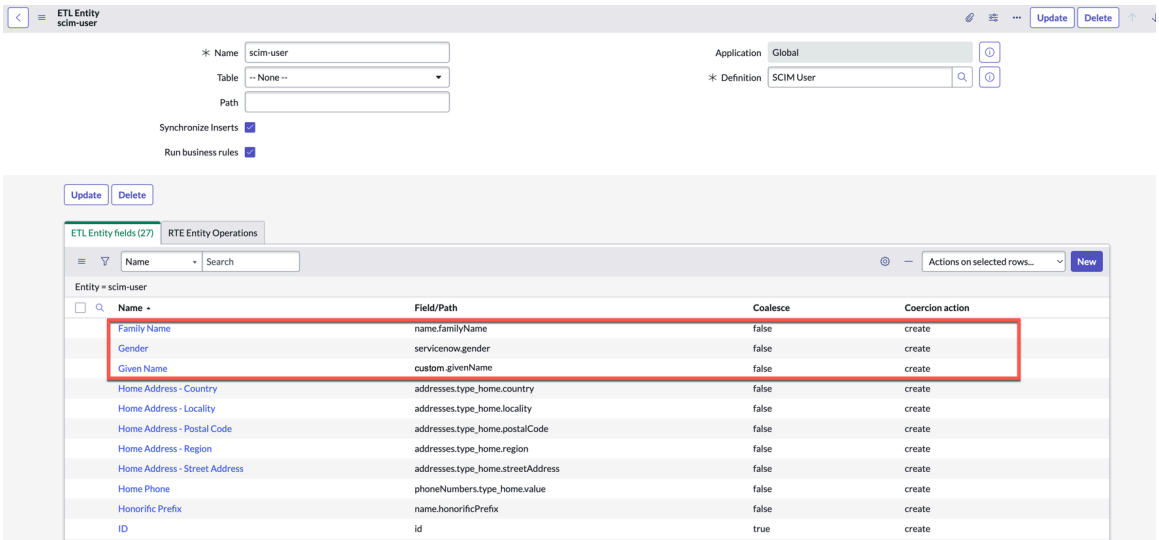
d. Soumettez les entrées en cliquant sur **Soumettre**.

Vous pouvez ajouter plusieurs entrées en tant que champ d'entité ETL en fonction de vos besoins.

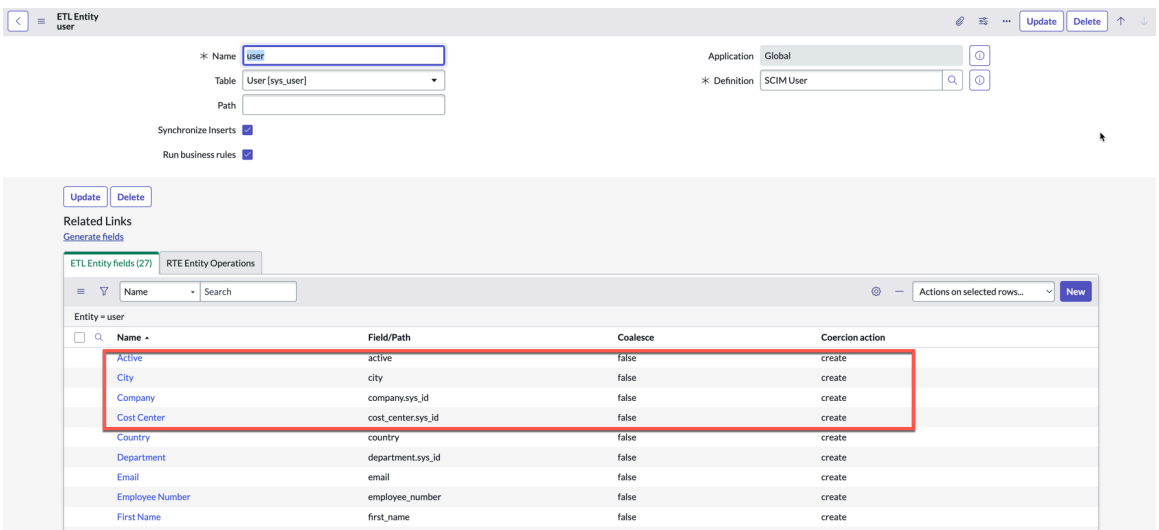
L'entité ETL scim-user peut avoir des entités avec l'extension principale (user), l'extension ou l'extension ServiceNow personnalisée.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



L'entité ETL utilisateur peut avoir des entités de la table de base de données. Par exemple, sys_user table.



Remarque :
Pour ajouter un filtre dans les champs SCIM entrants, utilisez un trait de soulignement (_). Ce trait de soulignement se traduit par un filtre d'égalisation. Par exemple, l'attribut `email.type_work.value` applique le filtre SCIM de l'e-mail `[type eq "work"].value`.

Une fois les champs créés dans les enregistrements d'entité ETL scim-user et user, vous devez créer un enregistrement de mappage d'entités RTE. Vous devez ensuite spécifier les définitions source et cible pour mapper les deux champs.

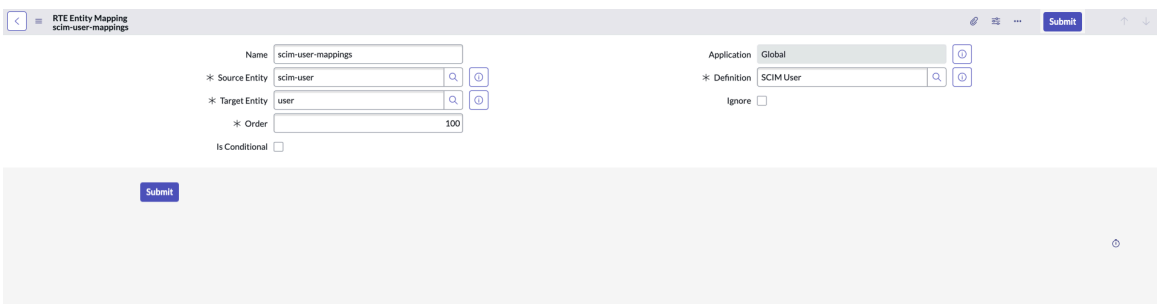
5. Dans la section Mappages d'entités RTE, créez un mappage d'entités en cliquant sur **Nouveau**
6. Renseignez les champs du formulaire.

Champ	Description
Nom	Nom du mappage.
Entité source	Entité source pour le mappage.

Traduction automatique

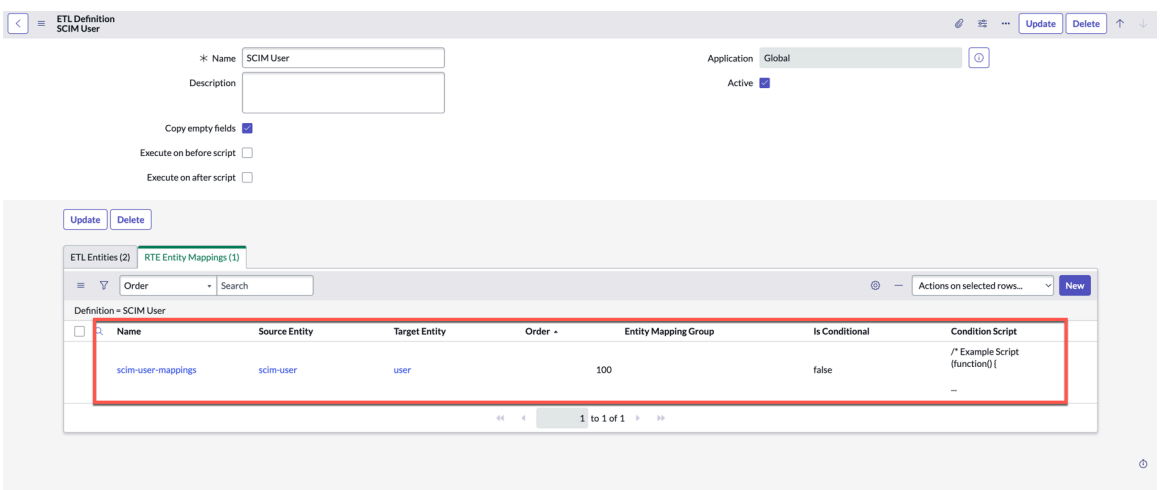
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Entité cible	Entité cible pour le mappage.
Ordre	Ordre dans lequel le mappage doit être traité.
Est conditionnel	Option permettant de désigner le mappage comme conditionnel.
Script de condition	Script qui définit les conditions à remplir pour le mappage.
Application	Le périmètre de l'application pour cet enregistrement.
Définition	Entité ETL sélectionnée à laquelle ce mappage appartient.
Ignorer	Option permettant de désigner si ce mappage d'entités ETL doit être ignoré lors de l'exécution d'intégrations de données à l'aide de la transformation robuste des ensembles de données à importer (RTE).



7. Cliquez sur **Envoyer**.

L'exemple suivant montre un enregistrement créé pour mapper à la fois les enregistrements scim-user et user ETL Entity.



8. Ouvrez l'enregistrement soumis (scim-user-mappings) et créez un mappage entre les enregistrements scim-user et user ETL Entity.

   a. Dans la section Mappages de champs RTE, cliquez sur **Nouveau**.

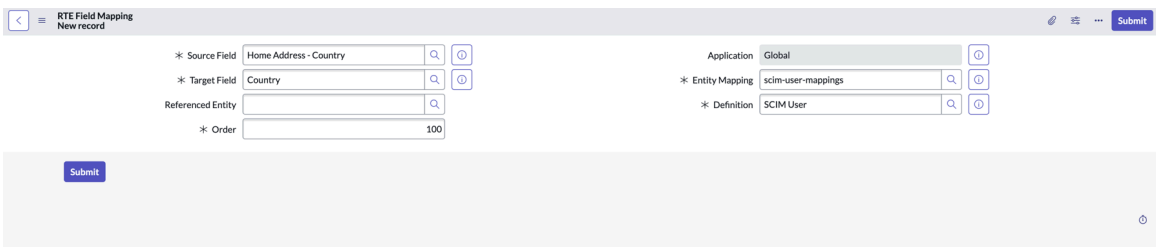
   b. Renseignez les champs du formulaire.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs de l'entité ETL

Champ	Description
Champ source	Le périmètre de l'application pour cet enregistrement.
Application	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Champ cible	Champ ETL de sortie pour l'opération si l'opération utilise une seule sortie.
Mappage d'entités	Mappage d'entités auquel cette opération s'applique.
Entité référencée	Entité référencée et opération à laquelle elle s'applique.
Définition	Entité ETL sélectionnée à laquelle appartient cette définition de champ.
Ordre	Ordre dans lequel l'opération s'exécute sur l'entité.



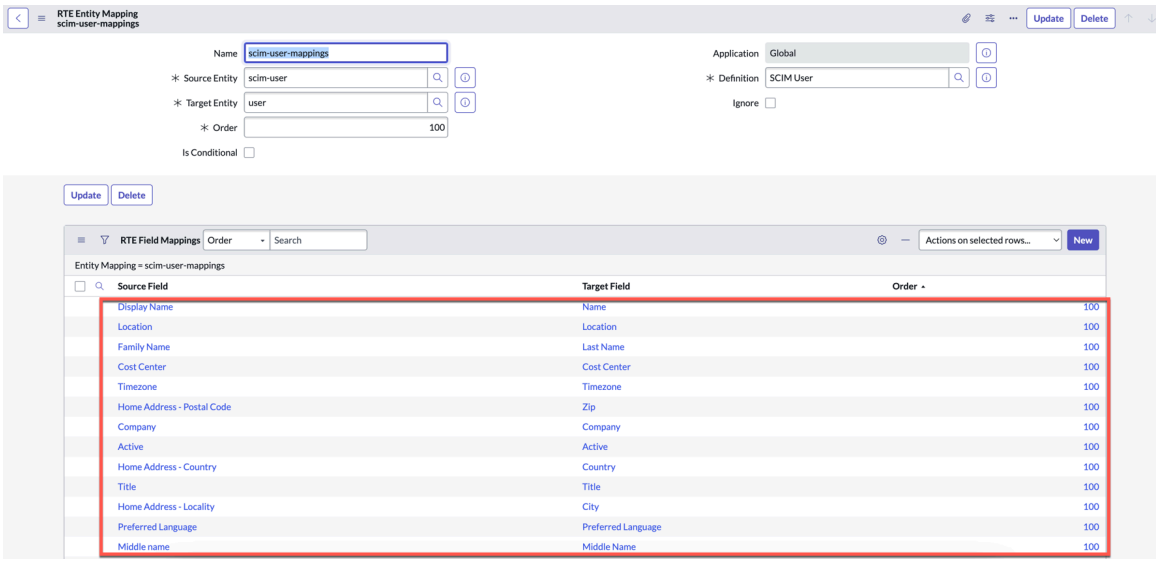
Le champ source **Adresse du domicile - Pays** (entité ETL scim-user) mappe le champ cible en tant que **Pays** (entité ETL utilisateur).

c. Soumettez les entrées en cliquant sur **Soumettre**.

Vous pouvez ajouter plusieurs entrées en tant que mappages d'entités RTE en fonction de vos besoins.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Les champs sources et les champs cibles sont mappés tels que configurés. Lorsque vous effectuez des opérations CRUD à l'aide de SCIM, les valeurs personnalisées sont mises à jour dans la table respective.

Résultats

Ces définitions et mappages ETL vous permettent d'extraire des données d'une table source, de transformer les données comme vous le souhaitez et de charger les données dans une table cible.

Information associée

Créer des définitions ETL (Extract Transform Load)

Gestion des champs non mappés

Vous pouvez gérer les champs non mappés dans la personnalisation SCIM de différentes manières.

Lors de la personnalisation SCIM, les champs qui ne font pas partie des tables sys_user et sys_user_group peuvent être mappés en exécutant les fonctions suivantes.

Personnaliser SCIM (créer ou mettre à jour)

Vous pouvez créer ou mettre à jour le client SCIM.

- L'administrateur SCIM peut ajouter des scripts personnalisés dans les scripts et *`onAfter`* pour les champs qui ne sont pas mappés dans la *`onBefore`* définition ETL ou RTE.
- L'administrateur SCIM peut remplacer les mappages RTE en ajoutant des scripts personnalisés dans les *`onBefore`* scripts et *`onAfter`* .
- Vous pouvez appeler une API scriptable dans le RTE *`onBefore`* ou *`onAfter`* des scripts pour accéder à la demande entrante et effectuer des transformations sur d'autres tables, listes et attributs non mappés.
- Vous pouvez utiliser cette *`sn_auth.SCIM2Util.getScimProviderCustomizationContext()`* méthode pour fournir le contexte de la requête SCIM qui contient l'objet *`scimResource`* . Le *`scimResource`* contexte représente les éléments suivants dans chaque opération :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- **POST** : ressource SCIM envoyée dans la charge utile de la demande.
- **PUT** : ressource SCIM actuelle de la base de données remplacée par la ressource SCIM envoyée dans la charge utile de la demande.
- **CORRECTIF** : ressource SCIM actuelle de la base de données après avoir effectué les opérations de correctif.

Voici un exemple de *`onAfter`* script.

```
(function onAfter(source, target, importLog) {

   var ctx = sn_auth.SCIM2Util.getScimProviderCustomizationContext();
   gs.info("scim context ee: " + JSON.stringify(ctx.scimResource));

   var roles = ctx.scimResource.roles;
   if(roles) {
      var removingRolesGR = new GlideRecord("sys_user_has_role");
      removingRolesGR.addQuery("user", target.sys_user[0].sys_id);
      removingRolesGR.query();
      removingRolesGR.deleteMultiple();

   for (var i = 0; i < roles.length; i++) {
      var addingRolesGR = new GlideRecord("sys_user_has_role");
      addingRolesGR.setValue("user", target.sys_user[0].sys_id);
      addingRolesGR.setValue("role", roles[i].value);
      addingRolesGR.setValue("state", "active");
      addingRolesGR.insert();
      }
      }
      var customUserExtn = new
 global.SCIMProviderCustomization().getCustomExtensionUrn('User');
      var salary = ctx.scimResource[customUserExtn].salary;
      if (salary) {
         var gr = new GlideRecord("u_user_salary");
         gr.addQuery("user", target.sys_user[0].sys_id);
         gr.query();
         if (gr.next()) {
            gr.setValue("salary", salary);
            gs.info("scim update: " + gr.update());
         } else {
         gr.setValue("salary", salary);
         gr.setValue("user", target.sys_user[0].sys_id);
         gr.insert();
         }
        }

})(source, target, importLog);
```

Personnaliser la réponse SCIM

Pour les appels d'API GET, toute réponse au client SCIM peut être personnalisée à l'aide du script en étendant le *`SCIMProviderCustomization`* script.

Tout en étendant le script, l'auteur peut remplacer les *`customizeUserResponse`* méthodes et *`customizeGroupResponse`* pour modifier les réponses des ressources utilisateur et groupe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

La *com.snc.integration.scim2.provider.customization.script.id* propriété permet au module d'extension SCIM d'utiliser le script qui doit être utilisé pour la personnalisation des réponses.

Voici un exemple d'extension du script de base.

```
var SCIMCustomizationScript = Class.create();
SCIMCustomizationScript.prototype = Object.extendsObject(SCIMProviderCustomization, {
   initialize: function() {
      SCIMProviderCustomization.prototype.initialize.call(this);
   },
   customizeUserResponse: function(context) {
      try {
         var rolesGR = new GlideRecord("sys_user_has_role");
         rolesGR.addQuery("user", context.scimResource.id);
         rolesGR.query();
         var i = 0;
         context.scimResource.roles = [];
         while (rolesGR.next()) {
            context.scimResource.roles[i] = {
               display: rolesGR.getElement('role.name').getValue(),
               value: rolesGR.getElement('role.sys_id').getValue()
            };
            i++;
         }
         var userGR = new GlideRecord("u_user_salary");
         userGR.addQuery("user", context.scimResource.id);
         userGR.query();
         if (userGR.next()) {
            var salary = userGR.getValue("salary");
            if (salary) {
               var customExtensionValue =
 SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
 context);
               customExtensionValue.salary = salary;
               SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this,
 "User", context, customExtensionValue);
            }
         }
      } catch (ex) {
         gs.error("err: " + ex);
      }
      return context;
   },
   customizeGroupResponse: function(context) {
      return context;
   },
   type: 'SCIMCustomizationScript'
});
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :

- Le paramètre que contiennent les `customizeUserResponse` méthodes and `customizeGroupResponse` est un objet de contexte avec un attribut appelé `scimResource`. Cet attribut possède tous les attributs d'un objet de ressource utilisateur ou groupe.
- Un include de script personnalisé ne peut être créé et consulté que par l'administrateur.
- Si une ressource utilisateur ou groupe est modifiée, vous devez renvoyer le contexte.
- S'il n'y a aucune modification d'attribut dans l'objet ressource, définissez la valeur vide ou renvoyez la `com.snc.integration.scim2.provider.customization.script.id` valeur null.
- Si certains attributs sont conservés dans le `onAfter` script, ils doivent être renseignés avec des valeurs de base de données dans l'objet `scimResource` à l'intérieur du script personnalisé. Cette action est requise afin que le système puisse effectuer les opérations suivantes :
  - Pour obtenir l'objet correct `scimResource` dans `onAfter` les scripts pendant l'opération PUT et PATCH.
  - Inclure les attributs qui ont persisté via le `onAfter` script dans la réponse au client.

Fonctions d'aide

Voici quelques-unes des fonctions d'assistance pour la personnalisation SCIM. Ces fonctions vous permettent de récupérer ou de définir différents types d'informations.

Fonctions d'aide

Fonction	Objectif
`SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");`	Récupère l'URN du schéma d'extension personnalisé.
`SCIMProviderCustomization.prototype.getServiceNowExtensionUrns.call(this, "User");`	Récupère l'URN des schémas d'extension ServiceNow extensions.
`SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User", context);`	Récupère le contenu de la personnalisation à partir de la réponse.
`SCIMProviderCustomization.prototype.getServiceNowExtensionNodeValue.call(this, "User", context);`	Récupère le contenu de la personnalisation à partir de la réponse
`SCIMProviderCustomization.prototype.setCustomExtensionNodeValue.call(this, "User", context, customExtensionValue);`	Définit le contenu de la personnalisation dans la réponse.

Voici un exemple d'utilisation de la fonction d'assistance :

```
var customExtensionUrn =
SCIMProviderCustomization.prototype.getCustomExtensionUrn.call(this, "User");
var customExtensionValue =
SCIMProviderCustomization.prototype.getCustomExtensionNodeValue.call(this, "User",
 context);
customExtensionValue.age = "18";
```

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

```
SCIMProviderCustomization.prototype.setCustomExtensionNodeValue call(this, "User", context,
 customExtensionValue);
```

Remarque :
RTE prend en charge la définition des données dans des tables autres que les tables sys_user et sys_user_group.

Création d'une définition de source

Créez une définition de source pour capturer des informations sur la source d'identité à partir de laquelle une ressource est mise en service.

Avant de commencer

Rôle requis : scim_admin

Avertissement :
Accordez ce rôle avec soin. Le rôle scim_admin équivaut à donner à l'utilisateur le rôle administrateur, dans lequel le scmin_admin peut ajouter ou mettre à jour des informations personnellement identifiables (PII).

Pourquoi et quand exécuter cette tâche

À l'aide d'une définition de source, la source d'identité de mise en service peut être mappée à une entité OAuth à l'aide de laquelle elle s'authentifie lors de la mise en service.

Après la création d'une définition source, toutes les ressources mises en service à partir de cette source d'identité sont mappées à son ID de définition source correspondant.

La définition de source capture les informations de source requises, par exemple en procédant comme suit :

- Identifie le client SCIM à partir duquel la ressource est mise en service.
- Résout les informations en double fournies par l'ID externe :
  - Si plusieurs sources d'identité mettent en service des ressources, deux ressources ou plus peuvent avoir la même valeur d'ID externe, car l'ID externe est uniquement unique à la source d'identité.
  - Si plusieurs ressources sont renvoyées avec un filtre SCIM d'ID externe, les ressources peuvent être résolues en fonction de la définition de source de la source d'identité demandeuse.

Remarque :
Une définition de source ne peut être créée que pour la source d'identité, qui utilise une méthode d'authentification OAuth.

Procédure

1. Accédez à la **Tout** > **SCIM** > **Définition de la source**.
2. Sur la page Définitions de source SCIM, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Définition de la source SCIM

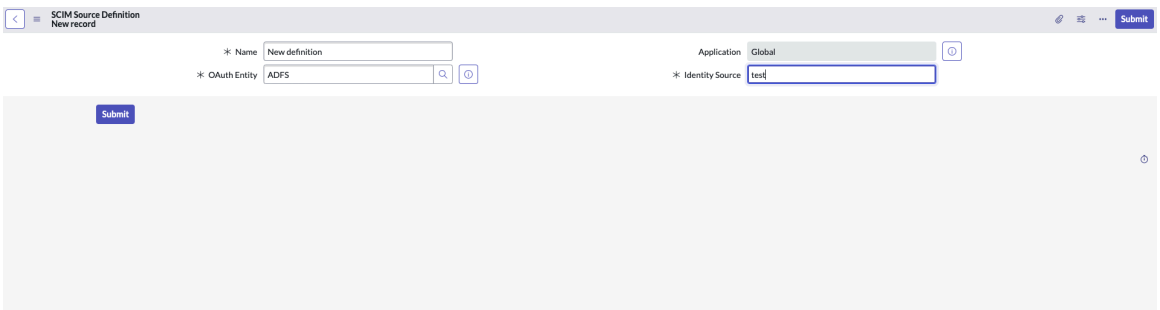
Champ	Description
Nom	Nom de la définition de source.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Application	Le périmètre de l'application pour cet enregistrement.
Entité OAuth	L’entité OAuth de l’utilisateur d’intégration. L’entité est utilisée pour la mise en service de l’utilisateur par le fournisseur de source d’identité.
Source d'identité	Le nom du fournisseur de la source d’identité. Par exemple, Azure AD, Okta, etc

Remarque :
Activez la propriété pour renvoyer uniquement les `com.snc.integration.scim2.resolve.externalid.conflict` ressources SCIM créées par la source d’identité demandeuse. Par défaut, toutes les ressources correspondantes avec un filtre d’ID externe sont renvoyées.



4. Cliquez sur **Envoyer**.

Résultats
La définition de source SCIM est créée. Utilisez les définitions SCIM ETL pour mapper les ressources en fonction du schéma d’extension sur la table sys_user et sys_user_group. Pour plus d'informations, consultez Créer une définition SCIM ETL.

Client SCIM

Le client SCIM facilite le provisionnement et les mises à jour des ressources d’identité par le biais d’opérations CRUD exposées par le point de terminaison SCIM sur un système externe.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



En savoir plus sur SCIM Client.

Activer



Activez le client SCIM.

Propriétés du client SCIM



Obtenez des détails sur la personnalisation de SCIM.

Dépannage



En savoir plus sur la définition de source pour SCIM.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration de SCIM Client

Le client SCIM facilite le provisionnement et les mises à jour des ressources d'identité par le biais d'opérations CRUD exposées par le point de terminaison SCIM sur un système externe.

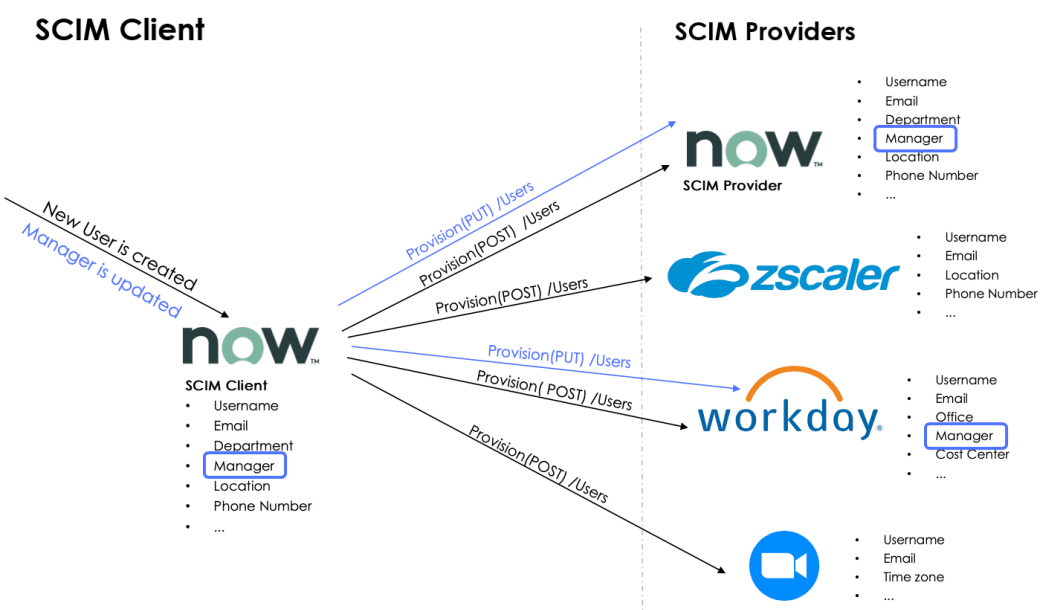
Le client SCIM est utilisé pour créer, mettre à jour et supprimer des ressources d'identité dans un système qui prend en charge les demandes REST conformes à SCIM. Le client est utilisé pour la gestion du cycle de vie de l'identité et pour la synchronisation des attributs d'identité entre ServiceNow les instances ou entre et ServiceNow d'autres fournisseurs SCIM.

Étant donné que les API sont exposées par le client, vous pouvez automatiser le processus de création, de mise à jour ou de suppression des ressources sur un ou plusieurs fournisseurs SCIM. Par exemple, si un développeur rejoint l'organisation, vous devez fournir l'accès à Git, à l'espace de travail, etc.

Le client SCIM vous permet d'effectuer les actions suivantes :

- Provisionnez les identités et l'accès pour l'appartenance à un utilisateur ou à un groupe.
- Synchronisez l'identité et les ressources connexes avec des systèmes conformes à SCIM.
- Intégrez n'importe quel fournisseur SCIM sur ServiceNow®.
- Annuler la mise en service des identités et de l'accès.

Le client SCIM fournit des API scriptables que le développeur d'intégration peut utiliser pour créer des workflows ou des automatisations afin d'effectuer des tâches spécifiques. Pour en savoir plus sur l'API scriptable, consultez API SCIM2Client .



Configurations pour le client SCIM

Pour configurer le client SCIM, effectuez les tâches suivantes :

- Créez un message REST pour tous les appels sortants d'un fournisseur SCIM particulier. Pour plus d'informations, consultez Créer un message REST.
- Créez un fournisseur SCIM pour extraire les informations sur les types de ressources et les schémas du fournisseur SCIM avec le message REST. Activez la configuration de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

méthode HTTP (PUT ou PATCH) pour mettre à jour une ressource dans le fournisseur SCIM. Pour plus d'informations, consultez Créer un fournisseur SCIM.

- Créez les mappages des attributs SCIM aux attributs d'un type de ressource et d'un ServiceNow fournisseur SCIM particuliers. Pour en savoir plus, reportez-vous à la section Créer un mappage des ressources de fournisseur SCIM.
- Effectuez le mappage du champ SCIM avec la table de base de données et le nom du champ. Transmettez la valeur par défaut ou écrivez un script pour extraire la valeur. Pour en savoir plus, reportez-vous à la section Créer un mappage d'attribut SCIM.

Activer le module d'extension client SCIM

Pour l'activation du client SCIM, installez le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client).

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à **Tout** > **Applications système** > **Toutes les applications disponibles** > **Toutes**.
2. Utilisez les critères de filtre et la barre de recherche pour rechercher le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client).

   Vous pouvez rechercher le module d'extension par son nom ou son ID. Si vous ne trouvez pas le module d'extension souhaité, vous devrez peut-être le demander au personnel ServiceNow.
3. Sélectionnez **Installer** pour lancer le processus d'installation.

   Remarque :
   Lorsque Séparation de domaine et l'administrateur délégué sont activés dans une instance, l'utilisateur administratif doit être dans le domaine **global**. Sinon, l'erreur suivante s'affiche : L'installation de l'application n'est pas disponible, car une autre opération est en cours d'exécution : activation du module d'extension pour <plugin name>.

Un message s'affiche une fois l'installation terminée.

Propriétés, tables, API scriptables et journaux du client SCIM

Le module d'extension SCIM v2 - ServiceNow Cross-domain Identity Management Client (com.snc.integration.scim2.client) inclut les propriétés système, tables, API scriptables et journaux suivants.

Propriétés

Le client SCIM ajoute les propriétés système suivantes.

Propriétés

Nom	Description
`com.snc.integration.scim2.client.log.request`	Cette propriété détermine s'il faut écrire tous les enregistrements du journal ou uniquement les enregistrements du journal d'erreurs. Les valeurs possibles sont **FAILURE** ou **ALL.**

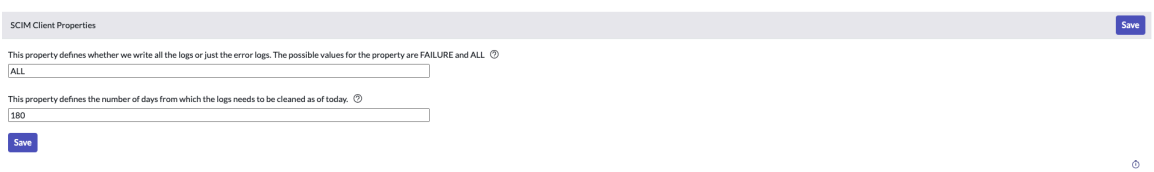
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Propriétés (suite)

Nom	Description
	Valeur par défaut : **TOUS**
com.snc.integration.scim2.client.log.cleanup.duration	Cette propriété détermine le nombre de jours d'effacement des journaux. Valeur par défaut : **180**

Pour définir les propriétés, accédez à **Tout** > **SCIM** > **Propriétés du client SCIM**.



Tables

Le client SCIM ajoute les tables suivantes.

Tables

Nom	Description
Fournisseur SCIM (sys_scim_provider)	Stocke les données de chaque fournisseur SCIM, telles que le nom, les définitions de ressources de message REST, etc.
Mappage des ressources de fournisseur SCIM (sys_scim_provider_resource_mapping)	Stocke les informations de la table principale pour chaque nom de fournisseur et de ressource.
Mappage de l'attribut SCIM (sys_scim_attribute_mapping)	Stocke les détails de la source d'où doit provenir chaque valeur d'attribut SCIM, tels que le champ de table, le script, etc.
Journal client SCIM (sys_scim_client_logs)	Stocke les états de chaque appel déclenché vers le fournisseur SCIM.

API pouvant contenir des scripts

L'API SCIM2Client appelle le fournisseur System for Cross-domain Identity Management (SCIM) (rôle serveur) pour créer, mettre à jour ou supprimer des données dans un fournisseur de service (SP). L'API scriptable du client SCIM doit être utilisée dans les scripts en cours d'exécution dans le contexte du système ou par un utilisateur administrateur système.

Par exemple, vous pouvez utiliser le script lors de l'exécution du workflow du concentrateur d'intégration en tant qu'utilisateur système, lors de l'exécution des travaux planifiés, etc.

Voici quelques-uns des cas d'utilisation des API scriptables :

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- En tant qu'administrateur, mettez en service des informations d'identité à partir de scripts en arrière-plan, de règles métier, d'appels d'include de script, de workflows, etc.
- En tant qu'administrateur, exécutez une tâche planifiée ou une tâche à la demande pour la mise en service de l'identité.
- Exécutez un workflow ou un sous-workflow avec l'étape Script à l'aide de l'appel d'API pouvant contenir des scripts de mise en service.
- Ajoutez le script de mise en service directement dans une règle métier ou un include de script. Le script peut être déclenché par des utilisateurs non-administrateurs. Ce cas d'utilisation fonctionne dans les situations suivantes :
  - L'utilisateur a accès au jeton, ce qui signifie qu'il a le rôle de générer le jeton à partir du modèle REST.
  - L'utilisateur peut récupérer les valeurs d'attribut SCIM à partir des tables mappées.

Pour en savoir plus sur l'API scriptable, consultez API SCIM2Client .

Journaux clients SCIM

Les journaux clients SCIM affichent l'état de mise en service des API SCIM. Pour afficher l'état de la mise en service, accédez à **Tout** > **SCIM** > **Journaux clients SCIM**.

Créer un message REST

Configurez un message REST pour tous les appels sortants d'un fournisseur SCIM particulier.

Avant de commencer

Rôle requis : administrateur

Procédure

1. Accédez à la **Tout** > **Services web du système** > **Sortant** > **Message REST**.
2. Cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Fournisseur SCIM

Champ	Description
Nom	Nom descriptif pour ce message.
Point de terminaison	URL de base du fournisseur SCIM. Par exemple, https://example.service-now.com/api/now/scim.
Type d'authentification	Type d'authentification à utiliser pour se connecter au fournisseur SCIM externe. Pour plus d'informations, consultez Authentification REST sortante .
En-têtes de messages REST	Type de contenu attendu du fournisseur SCIM externe. Par exemple, le nom de l'en-tête est le type de contenu dans le corps de la

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
	demande d'API suivante : Type de contenu : application/scim+json

4. Dans la liste connexe à Méthodes HTTP, cliquez sur **Nouveau**.
5. Configurez les méthodes HTTP suivantes.

Remarque :
Les URL comportent des variables que vous devez remplacer.

Méthodes HTTP

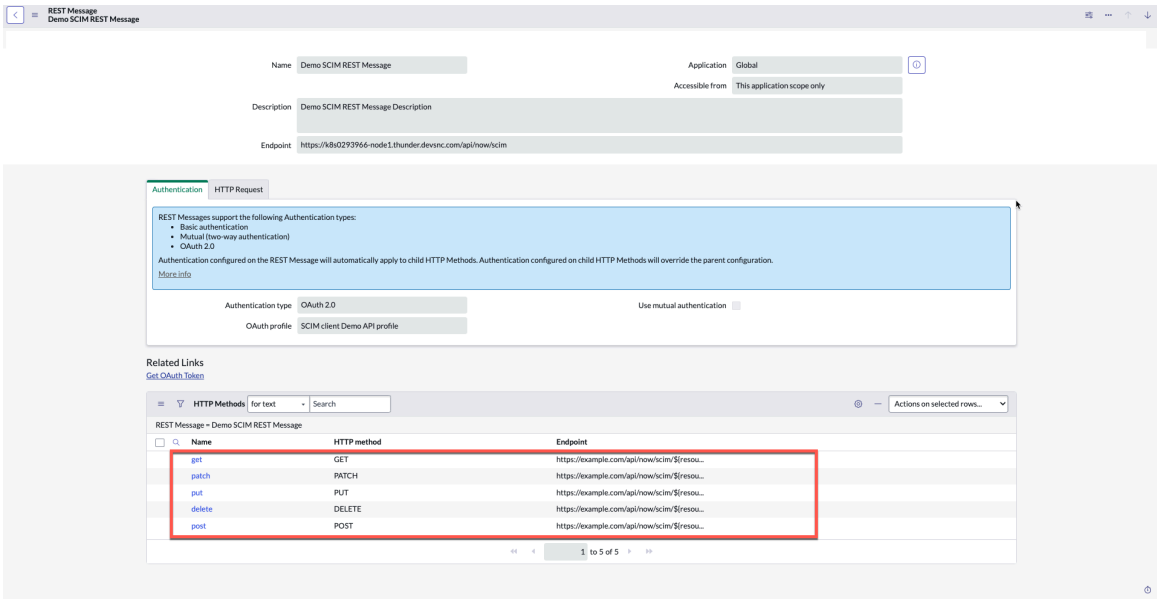
Méthodes	Exemple d'URL
GET	https://example.com/api/now/scim/${resourceName}
CORRECTIF	https://example.com/api/now/scim/${resourceName}/${resourceId}
PUT	https://example.com/api/now/scim/${resourceName}/${resourceId}
SUPPRIMER	https://example.com/api/now/scim/${resourceName}/${resourceId}
POST	https://example.com/api/now/scim/${resourceName}/${resourceId}

Remarque :

- Vous devez créer toutes les méthodes HTTP pour le fonctionnement du client SCIM.
- Un exemple de message REST est envoyé à partir du système de base.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



6. Cliquez sur **Envoyer**.

Résultats
L'enregistrement de message REST est créé.

Que faire ensuite
Utilisez le message REST pour créer un fournisseur SCIM. Pour plus d'informations, consultez Créer un fournisseur SCIM.

Pour en savoir plus sur la création d'un message REST, consultez Créer un message REST .

Créer un fournisseur SCIM

Créez un fournisseur SCIM pour extraire les informations sur les types de ressources et les schémas du fournisseur SCIM avec le message REST. Activez la configuration de la méthode HTTP (PUT ou PATCH) pour mettre à jour une ressource dans le fournisseur SCIM.

Avant de commencer
Remarque :
Un exemple de fournisseur SCIM fait partie du système de base. Vous pouvez l'utiliser et le configurer en fonction de vos besoins, ou créer un nouvel enregistrement.

Rôles requis : admin

Procédure
1. Accédez à la **Tout** > **Client SCIM** > **Fournisseur SCIM**.
2. Sur la page Fournisseurs SCIM, cliquez sur **Nouveau**.
3. Renseignez les champs du formulaire.

Formulaire Fournisseur SCIM

Champ	Description
Nom	Nom du fournisseur SCIM

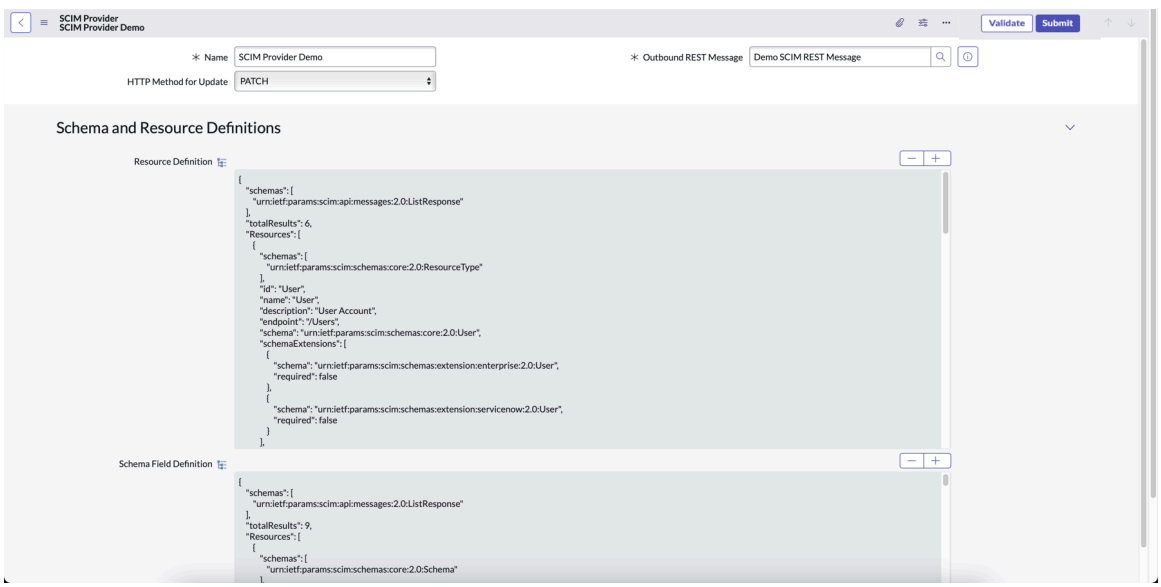
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ	Description
Message REST sortant	Message utilisé pour appeler l'API du fournisseur SCIM. Pour plus d'informations, consultez Créer un message REST.
Méthode HTTP pour la mise à jour	Type de méthode HTTPS utilisée pour mettre à jour le mappage des ressources. La méthode PATCH ou PUT peut être utilisée par le client lors de la mise à jour de la ressource d'identité lors de la mise à disposition d'une ressource déjà existante.

Remarque :

- Les champs **Définition de ressource** et **Définition du champ de schéma** sont récupérés à partir des */ResourceTypes/Schemas* points de terminaison et publics du fournisseur SCIM. Ces champs sont renseignés automatiquement une fois le message rest sélectionné.
- Si le message REST, les schémas ou les types de ressources sont mis à jour sur le fournisseur SCIM, cliquez sur **Actualiser** , puis sur **Mettre à jour** pour mettre à jour les champs **Définition de ressource** et **Définition du champ de schéma** .



4. Cliquez sur **Envoyer**.

Résultats

Les détails du fournisseur SCIM ont été créés avec succès. Utilisez le mappage des ressources du fournisseur SCIM pour mapper les détails du fournisseur SCIM aux ressources telles que les utilisateurs ou les groupes. Pour plus d'informations, consultez Créer un mappage des ressources de fournisseur SCIM.

Créer un mappage des ressources de fournisseur SCIM

Définissez les mappages des attributs SCIM aux attributs d'un ServiceNow type de ressource et d'un fournisseur SCIM particuliers.

Avant de commencer

Rôles requis : admin

Traduction automatique

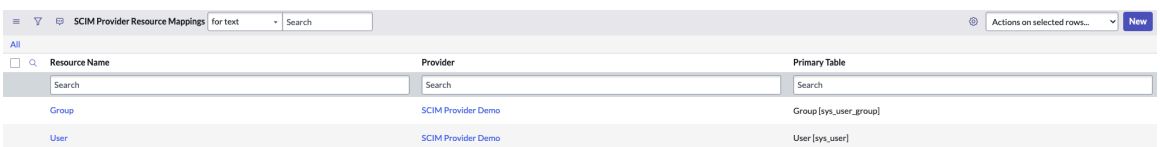
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Client SCIM** > **Mappage des ressources de fournisseur SCIM**.

   Le mappage des ressources du fournisseur SCIM est fourni avec le mappage Utilisateur et Groupe par défaut.

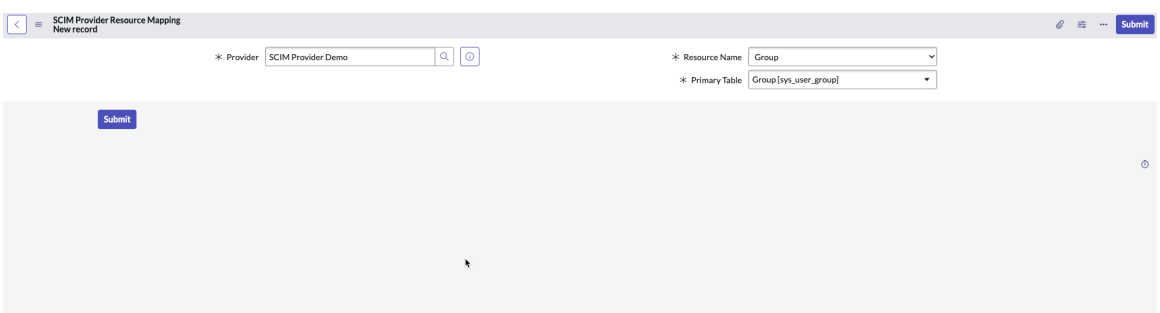
   Remarque :
   Les mappages d'utilisateur ou de groupe contiennent des exemples de mappages que vous pouvez utiliser comme référence. Vous pouvez également créer un mappage basé sur les ressources de l'utilisateur ou du groupe.



2. Créez un mappage des ressources en cliquant sur **Nouveau**.
3. Renseignez les champs du formulaire.

Mappage des ressources

Champs	Description
Fournisseur	Nom du fournisseur SCIM. Consultez le nom du fournisseur configuré lors de la création d'un fournisseur SCIM.
Nom de la ressource	Ressource pour laquelle le mappage doit être défini.
Table primaire	Table qui contient l'sys_id de la ressource en cours de mappage.



4. Cliquez sur **Envoyer**.

Résultats

L'enregistrement est créé et affiché dans la page Mappage des ressources de fournisseur SCIM. Utilisez les mappages d'attributs SCIM pour mapper davantage les attributs à partir des schémas. Pour plus d'informations, consultez Créer un mappage d'attribut SCIM.

Créer un mappage d'attribut SCIM

Créez un mappage d'attribut SCIM et utilisez-le comme source unique de ressource pour les champs de table ServiceNow .

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Avant de commencer
Rôles requis : admin

Pourquoi et quand exécuter cette tâche
Voici les types de mappage d'attributs et leurs descriptions.

Types de mappage d'attribut

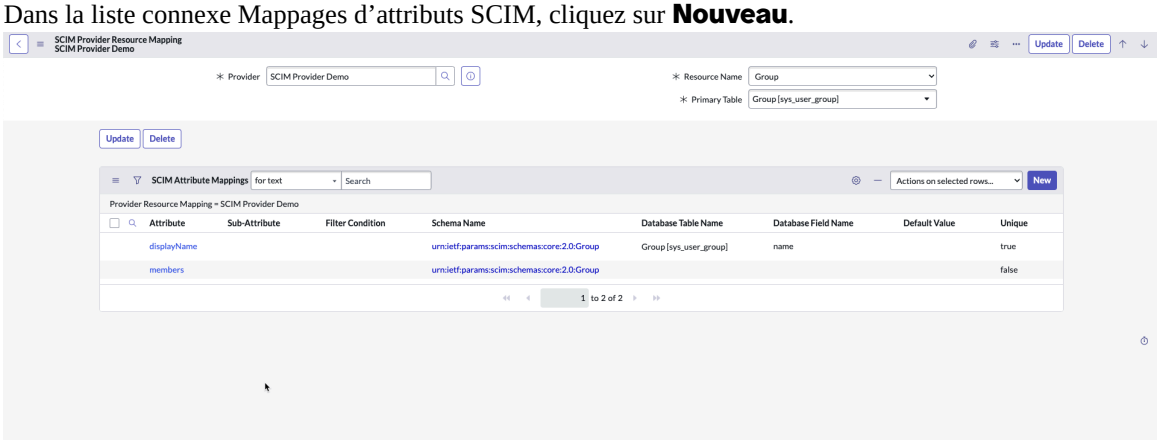
Type de mappage d'attribut	Description
Direct	L'attribut SCIM est renseigné à l'aide des champs Nom de table de **base de données** et **Nom de champ de base de données** .
Constante	L'attribut SCIM est renseigné à l'aide d'une valeur par défaut spécifiée.
Script/Personnalisé	L'attribut SCIM est renseigné à l'aide de la valeur de retour d'un script. Cet attribut nécessite l'activation de l'option Exécuter le script.

Remarque :

- L'attribut password n'est pas pris en charge
- Un exemple de mappage d'attributs pour les ressources Utilisateur et Groupe fait partie du système de base. Vous pouvez utiliser et configurer les mappages en fonction de vos besoins, ou vous pouvez créer un nouvel enregistrement.

Procédure

1. Accédez à la **Tout** > **Client SCIM** > **Mappage des ressources de fournisseur SCIM**.
2. Sélectionnez le mappage de ressources SCIM créé pour la configuration.
3. Dans la liste connexe Mappages d'attributs SCIM, cliquez sur **Nouveau**.



4. Renseignez les champs du formulaire.

Formulaire Mappages d'attributs SCIM

Champs	Description
Mappage des ressources de fournisseur	Mappage d'attributs pour une combinaison fournisseur-ressource.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
	Si ce champ n'est pas renseigné automatiquement, utilisez l'option de recherche. Sélectionnez l'enregistrement Mappage des ressources de fournisseur.
Nom du schéma	Nom de schéma de l'attribut SCIM pour lequel le mappage doit être défini. Par exemple, *urn:ietf:params:scim:schemas:core:2.0:User*.
Attribut	Attribut pour lequel le mappage doit être défini. Par exemple, *userName*.
Sous-attribut	Sous-attribut (le cas échéant) pour lequel le mappage doit être défini. Par exemple, s'il existe un attribut de type complexe comme *name.familyName*, alors l'attribut est **name** et le sous-attribut est **familyName**.
Type de champ	Le type de données Attribut SCIM. Ce champ est renseigné automatiquement à partir des schémas définis par le fournisseur SCIM. Par exemple, **booléen**.
Multivaleur	Plusieurs valeurs affectées à l'attribut. Un attribut peut avoir plusieurs valeurs, comme e-mail professionnel, e-mail personnel ou un autre e-mail. Par exemple, *emails*. Ce champ est renseigné à l'aide des schémas définis par le fournisseur SCIM.
Condition de filtre	Certains attributs à valeurs multiples peuvent contenir des informations supplémentaires qui peuvent être spécifiées à l'aide d'une condition de filtre. Les choix de condition de filtre sont renseignés à l'aide des schémas définis par le fournisseur SCIM. Par exemple, l'attribut *phoneNumbers* a plusieurs types comme travail, mobile, domicile, et ainsi de suite

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
Unique	Option permettant d'identifier de façon unique une ressource entre les systèmes du client SCIM et du fournisseur SCIM. Les attributs à valeurs multiples ne peuvent pas être marqués comme uniques. Par exemple, pour une ressource utilisateur, l'attribut *username* peut être rendu unique.
Nom de table de base de données	Utilisez ce champ pour mapper le nom de la table attributaire au nom de la ServiceNow table. Si vous choisissez le mappage d'attribut direct, vous devez définir ce champ. Par exemple, l'attribut *username* SCIM peut être mappé au champ **Utilisateur** dans le champ Nom de table **de base de données** .
Nom du champ de base de données	Le champ Nom de champ de base de données mappe l'attribut SCIM au ServiceNow nom de champ à mapper avec l'attribut SCIM. Si vous choisissez le mappage d'attribut direct, vous devez définir ce champ. Par exemple, l'attribut *username* SCIM peut être mappé au champ **ID d'utilisateur** dans le champ **Nom du champ de base de données** .
Valeur par défaut	Détails sur la valeur par défaut transmise au fournisseur SCIM. Peut être utilisé sile mappage d'attribut direct du champ renvoie null, ou si la valeur par défaut peut être utilisée pour retourner une valeur codée en dur. Dans le cas d'une valeur codée en dur, le nom de la table de base de données et le nom de champ doivent être **Aucun**. Par exemple, la valeur sous-attribut principale de l'e-mail professionnel peut être codée en dur comme **vrai**.
Exécuter le script	Option permettant d'extraire la valeur de l'attribut via le script. Cette option est requise pour les attributs à valeurs multiples qui ne contiennent

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champs	Description
	pas de condition de filtre. Pour un type complexe d'attribut, un script peut fournir la valeur au niveau d'un attribut ou d'un sous-attribut. Par exemple, l'attribut **Members** de la ressource de groupe n'a aucune condition de filtre. Par conséquent, l'option de script doit être définie au niveau de l'attribut parent de l'attribut **Membres** .
Script	Script utilisé pour extraire la valeur de l'attribut. Le type de script renvoyé doit être une chaîne ou un JSON converti en chaîne. La sortie du script doit être au format approprié, tel que prévu par le fournisseur pour cet attribut.

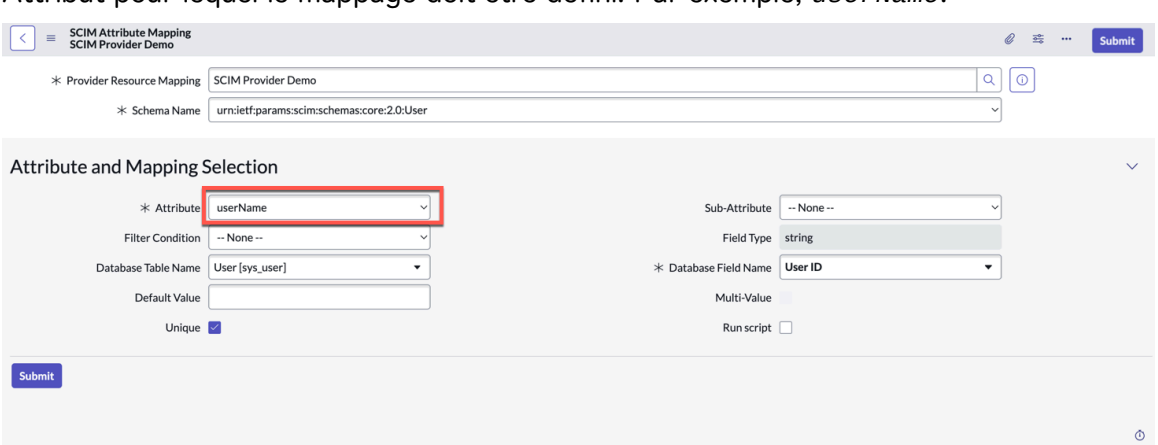
5. Cliquez sur **Envoyer**.

Références de mappage d'attribut

Les mappages d'attributs vous permettent d'utiliser les attributs comme source unique de ressource pour les champs de table ServiceNow .

Attribut

Attribut pour lequel le mappage doit être défini. Par exemple, *`userName`*.



Sous-attribut

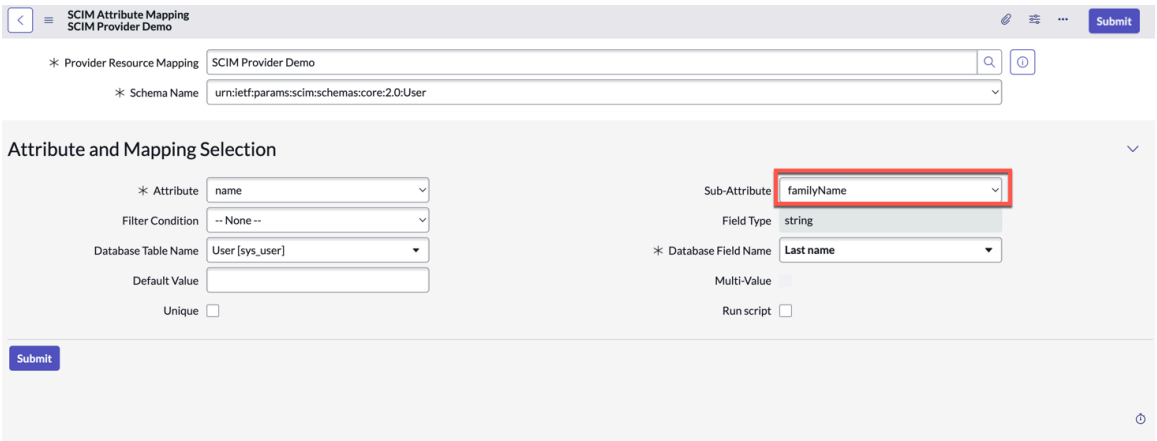
Sélectionnez le sous-attribut, le cas échéant, pour lequel un mappage doit être défini.

Par exemple, s'il existe un attribut de type complexe comme *`name.familyName`*, alors l'attribut est *`name`* et le sous-attribut est *`familyName`*.

Pour les attributs simples tels que le nom d'utilisateur, la valeur **du sous-attribut** est **Aucun**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

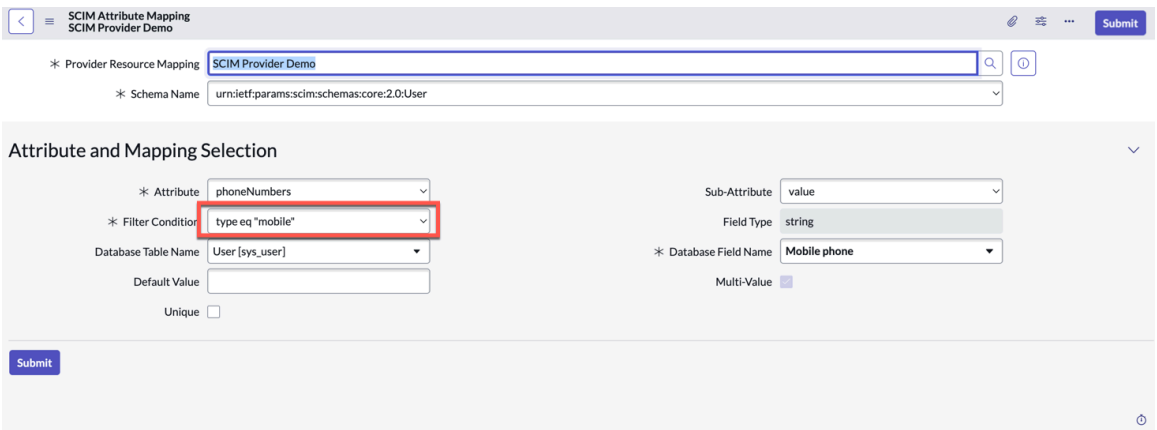


Condition de filtre

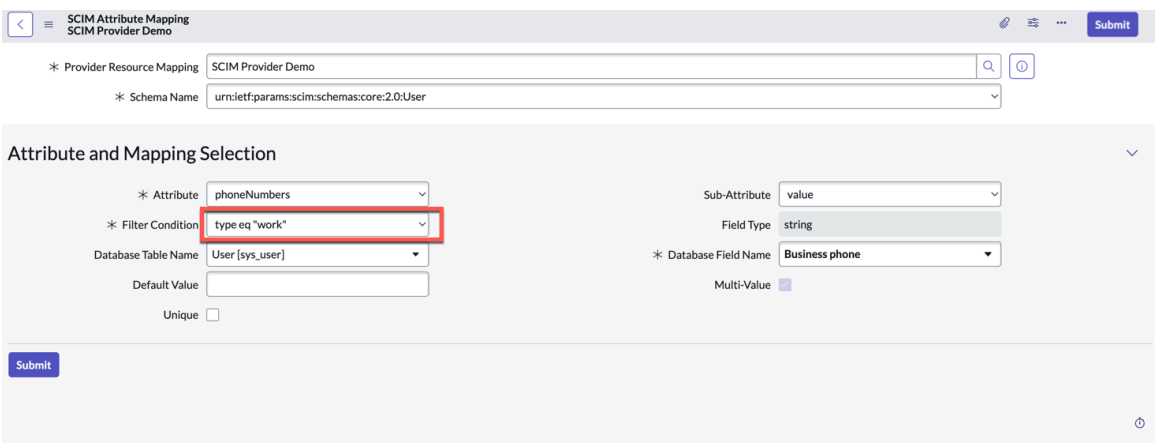
Un attribut à valeurs multiples peut contenir des informations supplémentaires qui peuvent être spécifiées à l'aide d'une condition de filtre. Les choix de la condition de filtre sont renseignés à l'aide des schémas définis par le fournisseur SCIM.

Par exemple, l'attribut *phoneNumbers* a plusieurs types comme travail, mobile, domicile, etc.

Vous pouvez spécifier une condition de filtre à partir d'un ensemble de valeurs possibles. Par exemple, l'attribut *phoneNumber* peut avoir une condition de **filtre de type eq « mobile »**.



À la place, l'attribut *phoneNumber* peut avoir une condition de filtre de **type eq « work »**.



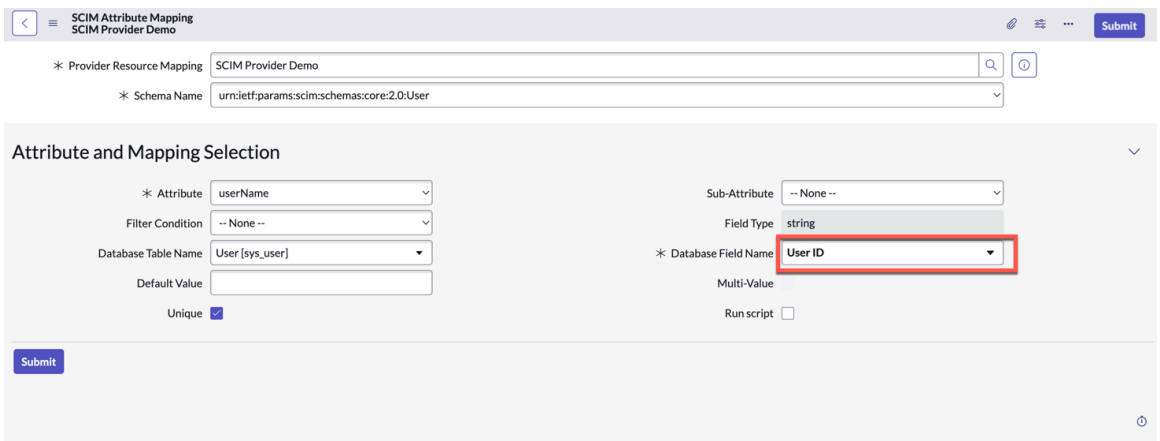
Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

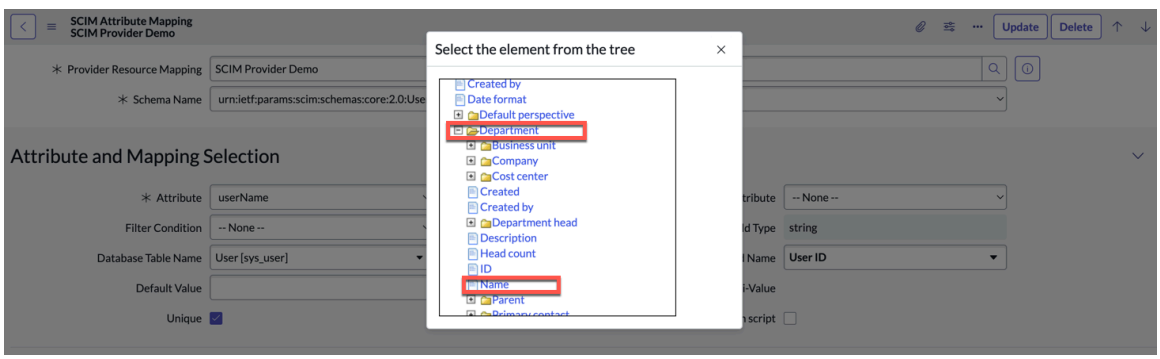
Nom du champ de base de données

Si l'option de mappage d'attribut direct est choisie, cet attribut doit être défini. Le champ **Nom de champ de base de données** représente le nom de ServiceNow champ mappé avec l'attribut SCIM.

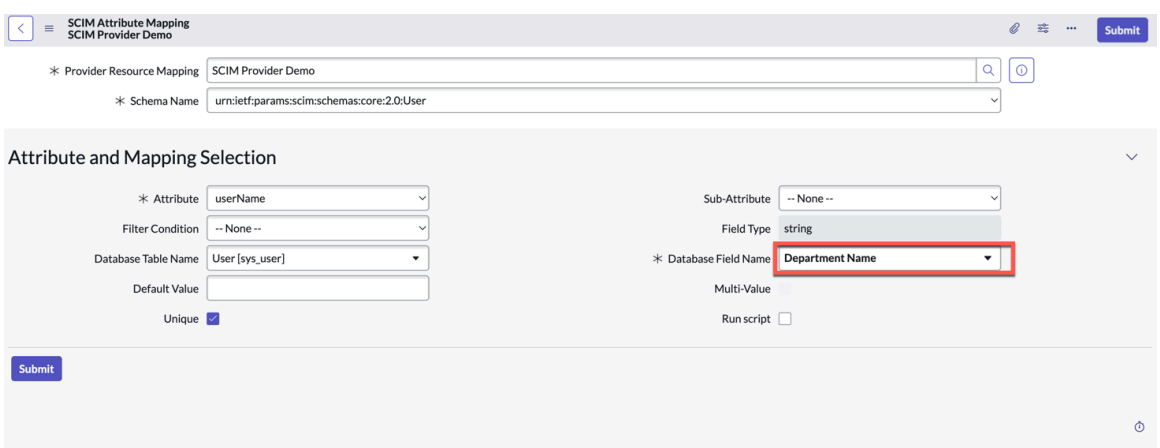
Par exemple, l'attribut *username* SCIM peut être mappé à un utilisateur en tant que champ Nom de la **table de base de données** et au champ ID de l'utilisateur en tant que champ **Nom du champ Base de données** .



Vous pouvez également remonter pas à pas à l'aide du **nom du champ de base de données**. Par exemple, l'attribut SCIM **du département** peut être mappé au champ **Nom du département** .



Ici, la table de base de données est **Utilisateur** et le nom du champ Base de données est **Nom de département**.



Traduction automatique

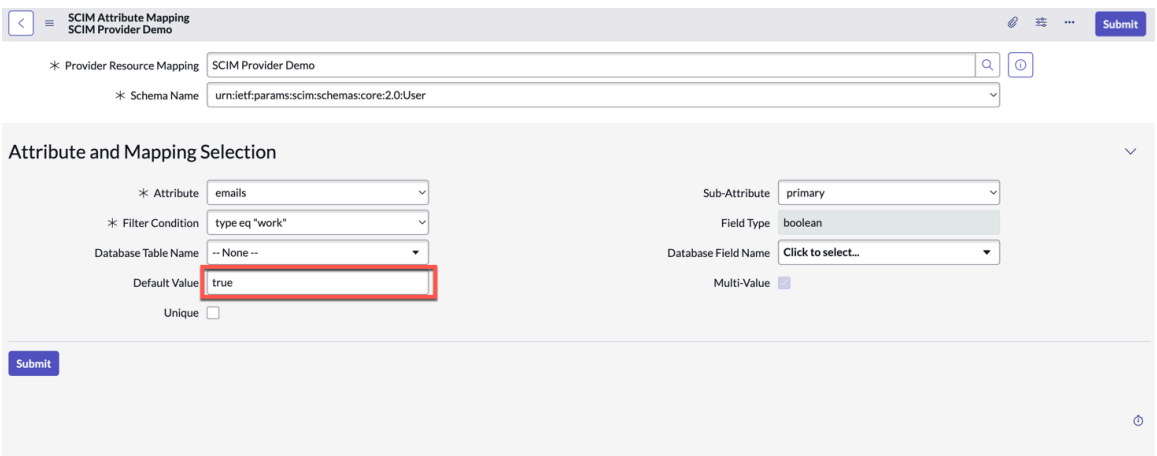
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Valeur par défaut

La valeur par défaut est transmise au fournisseur SCIM si le mappage d'attribut direct de ce champ renvoie null. La valeur par défaut peut également être utilisée pour renvoyer une valeur codée en dur.

Dans le cas d'une valeur codée en dur, le nom de la table de base de données et le nom de champ doivent être **Aucun**.

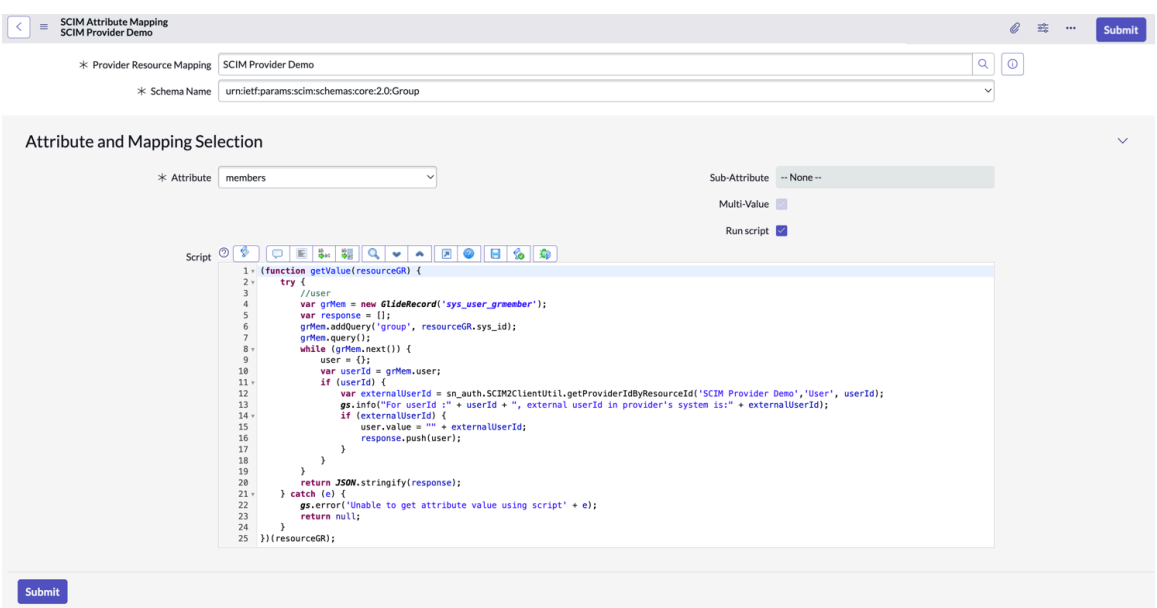
Par exemple, la valeur du sous-attribut primaire de l'e-mail professionnel peut être codée en dur comme **vrai**.



Script

Le script est utilisé pour extraire la valeur de l'attribut. Le type de retour du script doit toujours être une chaîne de caractères, ou un JSON converti en chaîne. La sortie du script doit être au format approprié, tel que prévu par le fournisseur pour cet attribut.

Voici un exemple de script pour un attribut à valeurs multiples.

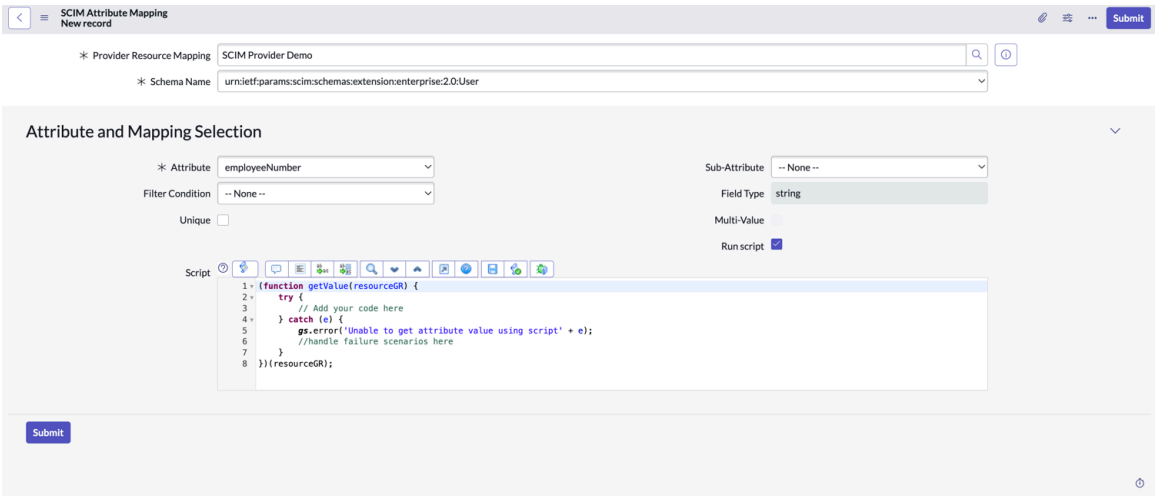


La sortie du script doit avoir un tableau JSON stringifié.

Ce qui suit est un exemple de script d'un attribut à valeur simple.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La sortie du script doit être une chaîne de caractères.

Dépannage du client SCIM

Les actions de dépannage peuvent aider à résoudre les problèmes courants lors de la configuration ou de l'exécution du client SCIM.

Dépannage

Problème	Action
La réponse contient le message suivant : `"message":"Unable to access the table core_company with id: 0c441abbc6112275000025157c651c89, Please cross check the Access control rules"`	Le message s'affiche si l'API est appelée dans un contexte utilisateur et que l'utilisateur n'a pas accès à la table. Vous devez vous assurer que l'API scriptable est appelée dans le contexte système.
La réponse contient le message suivant : `{"message":"User Not Authenticated","detail":" Required to provide Auth information"}`	• Assurez-vous que le jeton est généré via le message REST correspondant et qu'il est valide. • Assurez-vous que l'API scriptable est appelée dans le contexte système.
La réponse contient le message suivant : `Script execution failed, the reason is: Cannot cast java.lang.Integer to java.lang.String`	Dans le mappage d'attributs SCIM, si le champ est défini pour être récupéré à partir d'un script présentant ce problème, assurez-vous que le type de retour doit toujours être une chaîne.
La réponse contient le message suivant : `"status": "400", "scimType": "invalidValue",`	Pour tout attribut SCIM qui attend l'ID, cet ID est toujours du système du fournisseur. Assurez-vous que l'ID transmis dans la charge utile est valide dans le système du fournisseur.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Dépannage (suite)

Problème	Action
"detail": "Manager id : 02826bf03710200044e0bfc8bcbe5ds8 doesn't exist"	

Zones à vérifier pour le dépannage

Voici quelques-unes des zones qui peuvent être vérifiées pour détecter les erreurs de dépannage lors de l'utilisation du client SCIM :

- Si un problème est détecté lors de l'exécution de l'une des API scriptables, consultez la section Journaux du client SCIM.

Champs de journaux

Champ	Description
ID de demande	ID unique qui représente une API pouvant contenir des scripts appelée.
Fournisseur SCIM	Nom du fournisseur pour lequel l'API est appelée.
Ressource	Nom de la ressource pour laquelle l'API est appelée.
ID de ressource	L'ID pour lequel l'API est appelée. Pour la suppression, l'ID représente l'ID de ressource dans le système fournisseur et l'ID se trouve dans le système client.
Action	API qui s'appelle
Statut	État du journal en tant que réussite ou échec
Message	Message de réussite ou d'erreur. Le message d'erreur peut provenir du fournisseur SCIM ou être dû à des problèmes de configuration dans le client SCIM.

- Vérifiez le corps de la demande en configurant et en visualisant les appels sortants. Pour plus d'informations, consultez Journalisation des services Web sortants .
- Mettez à jour les niveaux de journal en ajoutant le type de contenu, en testant l'exemple et en accédant au formulaire Méthode HTTP correspondant dans le message REST du fournisseur correspondant.
- Si le corps de la demande est tronqué, augmentez la limite à l'aide de la propriété `glide.outbound_http.content.max_limit`système .

Audit d'identité et d'accès

Utilisez l'audit d'identité et d'accès pour comprendre les changements apportés aux utilisateurs, aux groupes, aux rôles et aux ACL.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Explorer



Découvrez les fonctionnalités et la valeur commerciale de l’audit d’identité et d’accès.

Configurer



Comprendre comment configurer l’audit d’identité et d’accès.

Résultats d'audit



Affichez les résultats de l’audit d’identité et d’accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Exploration de l'audit d'identité et d'accès

Utilisez l'audit d'identité et d'accès pour comprendre les changements apportés aux utilisateurs, aux groupes, aux rôles et aux ACL.

L'audit d'identité et d'accès permet de comprendre les informations essentielles sur qui a modifié quoi, où et quand dans les comptes, les groupes et les rôles des utilisateurs.

Permet de détecter les utilisateurs malveillants et de suivre les activités inhabituelles dans l'instance et de respecter les ServiceNow® normes de conformité pour pouvoir suivre les changements d'accès.

Identity and Access Audit (Identity Security Audit) est un module d'extension (`com.glide.security.audit`) qui s'installe automatiquement.

La fonctionnalité d'audit peut être activée ou désactivée en activant ou en désactivant la propriétésystème `glide.identity.security.audit.enabled` . par défaut, cette propriété est définie sur `true`.

L'audit d'identité et d'accès vous permet d'effectuer les actions suivantes :

- Consultez les changements apportés au cours des 30 derniers jours aux utilisateurs, groupes, attributs ACL de rôle, appartenances aux rôles, appartenances à des groupes et rôles ACL.
- Suivez les changements dans votre ServiceNow instance.
- Contribuez à atténuer les risques potentiels liés à la sécurité et à la réglementation.
- Démontrer la conformité avec les auditeurs des différents groupes au sein de l'organisation.
- Démontrez que l'organisation n'est pas vulnérable aux menaces liées à un manque de visibilité dans le groupe d'utilisateurs et aux changements de rôles.

Profils d'utilisateur dans Identity Access and Audit

Les différents profils d'utilisateur dans l'audit d'identité et d'accès sont les suivants :

- **Administrateur** : affichez les enregistrements d'audit et la configuration.
- **Administrateur de sécurité** : affichez ces pistes d'audit. Modifiez la configuration pour activer ou désactiver l'audit pour une certaine table ou modifiez les champs en cours d'audit.

Tables d'audit

Les tables suivantes peuvent être auditées à l'aide de l'audit d'identité et d'accès :

- Groupe [sys_user_group]
- Rôle [sys_user_role]
- Contrôle d'accès [sys_security_acl]
- Utilisateur [sys_user]
- Rôle de groupe [sys_group_has_role]
- Rôle d'utilisateur [sys_user_has_role]
- Rôles d'accès [sys_security_acl_role]

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

- Rôle contenu [sys_user_role_contains]
- Membre du groupe [sys_user_grmember]

Modules d'audit d'identité et d'accès

L'audit d'identité et d'accès comporte les modules suivants sur l'instance ServiceNow :

Module	Description
Résultats d'audit	Affiche les audits qui se sont produits dans l'instance ServiceNow .
Configurer la table et les champs	Configurez les tables et les champs système avec les champs disponibles provenant de l'audit d'identité et d'accès.
Configurer la période de conservation	Configurez la période de conservation des données auditées. La période maximale pouvant être définie est de 30 jours.
Pistes d'utilisateurs	Affiche les audits des utilisateurs.
Pistes de groupes	Affiche les audits des groupes.
Pistes des rôles	Affiche les audits des rôles.
Pistes ACL	Affiche les audits des ACL.

Résultats de l'audit d'identité

Affiche les audits qui se sont produits dans l'instance ServiceNow® .

Résultats d'audit affiche les changements apportés aux utilisateurs, aux groupes, aux rôles et aux ACL de l'instance ServiceNow .

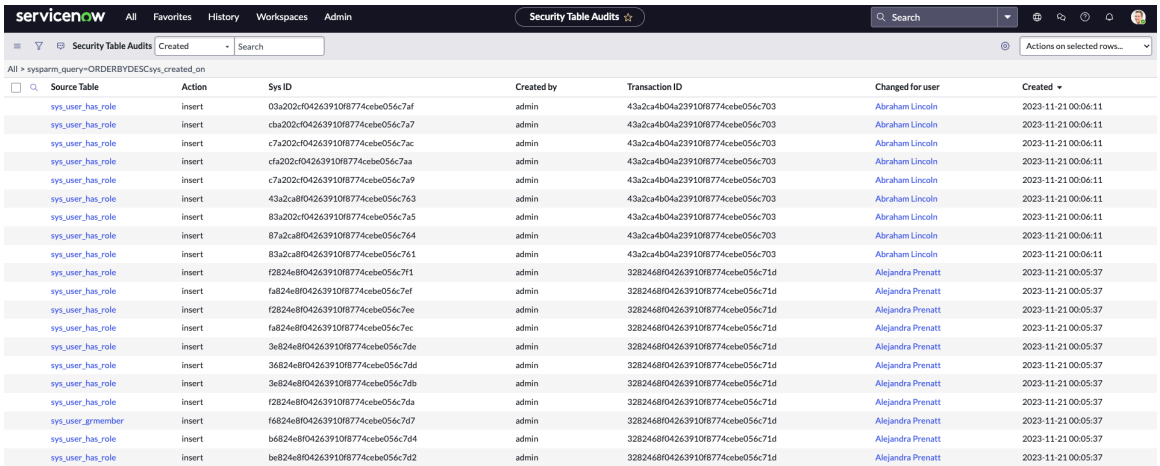
Pour accéder aux résultats d'audit, naviguez **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Résultats d'audit**. La page Audits de table de sécurité s'affiche avec les informations suivantes.

Audits de tables de sécurité

Nom de colonne	Description
Table source	Détails de la table source où l'audit a eu lieu.
Action	Décrit l'action d'audit.
Sys_id	Détails sur la sys_id de l'enregistrement audité.
Créé par	Détails de l'audit qui a été créé par.
ID de transaction	ID unique qui représente chaque action de l'audit particulier effectué.
Utilisateur concerné par le changement	Nom de l'utilisateur au moment de l'audit.
Créé	Heure et date d'exécution de l'audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Pistes d'utilisateurs

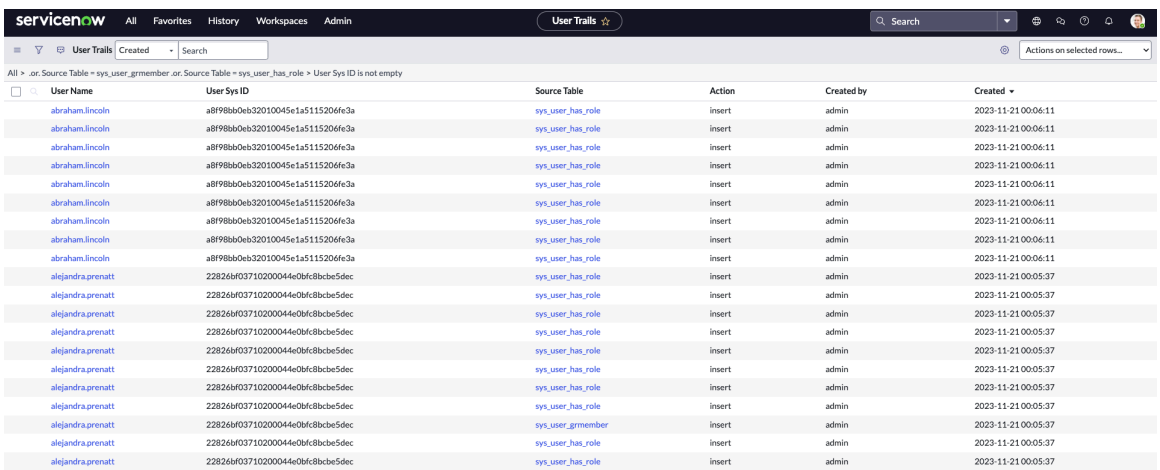
Affiche les audits des utilisateurs dans l'instance ServiceNow® .

Les pistes d'utilisateurs affichent les changements d'attribut d'identité, d'appartenance au rôle et d'appartenance au groupe pour un utilisateur.

Pour accéder aux parcours d'utilisateurs, accédez à **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes d'utilisateurs**. La page Parcours d'utilisateurs s'affiche avec les informations suivantes.

Pistes d'utilisateurs

Noms d'utilisateur	Nom de l'utilisateur.
ID système de l'utilisateur	Détails sur l'utilisateur sys_id pour l'enregistrement audité.
Table source	Détails sur la table source où l'audit a été effectué.
Action	Décrit l'action d'audit.
Créés par	L'utilisateur qui a effectué le changement.
Créé	Heure et date d'exécution de l'audit.



Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pistes de groupes

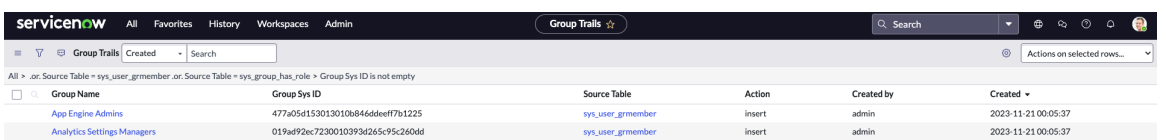
Affiche les audits des groupes dans l'instance ServiceNow® .

Les pistes de groupe affichent les changements d'attributs, d'membres et de rôles pour un groupe.

Pour accéder aux parcours de groupe, accédez à **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes de groupes**. La page Pistes de groupe s'affiche avec les informations suivantes.

Pistes de groupes

Nom de groupe	Nom du groupe.
ID système du groupe	Des détails sur le groupe sys_id pour l'enregistrement audité.
Table source	Détails sur la table source où l'audit a été effectué.
Action	Décrit l'action d'audit.
Créés par	L'utilisateur qui a effectué le changement.
Créé	Heure et date d'exécution de l'audit.



Pistes des rôles

Affiche les audits des rôles dans l'instance ServiceNow® .

Les pistes de rôle affichent les changements d'attributs et les changements de relations parent-enfant pour un rôle.

Pour accéder aux pistes de rôles, accédez à **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes des rôles**. La page Pistes d'accès aux rôles s'affiche avec les informations suivantes.

Pistes des rôles

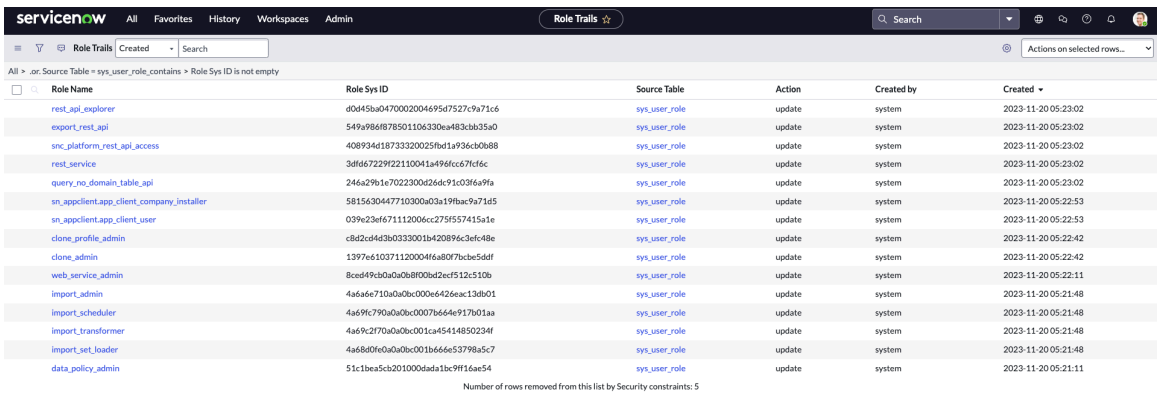
Nom de rôle	Nom du rôle.
ID système du rôle	Détails sur le rôle sys_id pour l'enregistrement audité.
Table source	Détails sur la table source où l'audit a été effectué.
Action	Décrit l'action d'audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Pistes des rôles (suite)

Créés par	L’utilisateur qui a effectué le changement.
Créé	Heure et date d’exécution de l’audit.



Pistes ACL

Affiche les audits des ACL dans l’instance ServiceNow® .

Les pistes ACL affichent les changements d’attributs et les changements de relations de rôle requis pour une ACL.

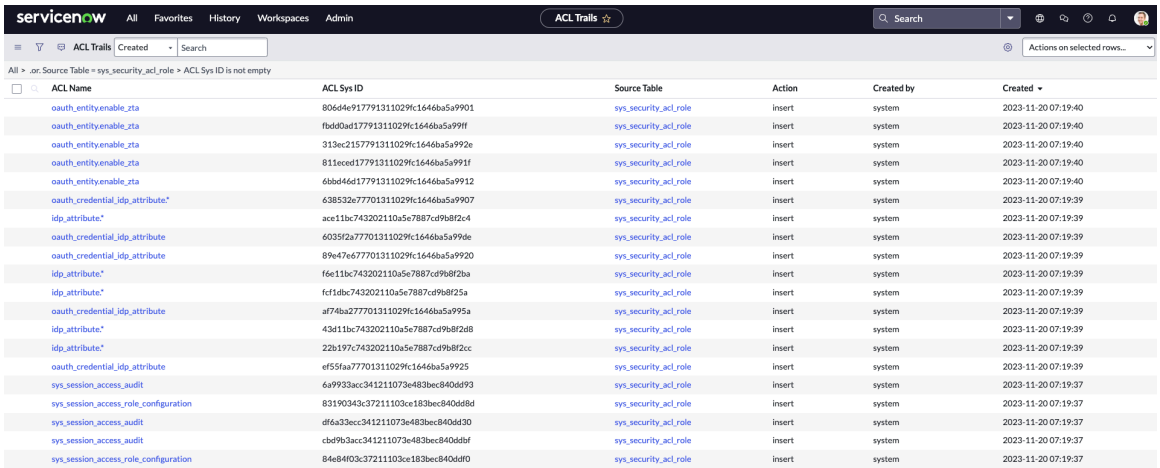
Pour accéder aux pistes ACL, accédez à **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Pistes ACL**. La page Pistes ACL s’affiche avec les informations suivantes.

Pistes ACL

Nom ACL	Nom de l’ACL.
ID système ACL	Détails sur l’ACL sys_id pour l’enregistrement audité.
Table source	Détails sur la table source où l’audit a été effectué.
Action	Décrit l’action d’audit.
Créés par	L’utilisateur qui a effectué le changement.
Créé	Heure et date d’exécution de l’audit.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d’autres pays
D’autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



Champs auditables de sécurité

Affiche les détails au niveau de la table et du champ qui seront audités dans l'instance ServiceNow® .

Champs auditables de sécurité affiche les détails des tables et des champs qui seront audités dans l'instance ServiceNow .

Pour accéder à la page Champs auditables de sécurité, accédez à **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Configurer les tables et les champs**. La page Champs auditables de sécurité s'affiche avec les informations suivantes.

Champs auditables de sécurité

Nom de colonne	Description
Table à Audit	Détails de la table qui fait l'objet d'un audit.
Destination de stockage d'audit	Détails de la destination où les détails de l'audit sont stockés.
Liste des champs	L'audit sera effectué pour les champs spécifiés dans la liste.
Créer	Auditez les changements associés à l'opération de création.
Mettre à jour	Auditez les changements associés à l'opération de mise à jour.
Supprimer	Auditez les changements associés à l'opération de suppression.
Actif	Auditez uniquement si la configuration de la table est active.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

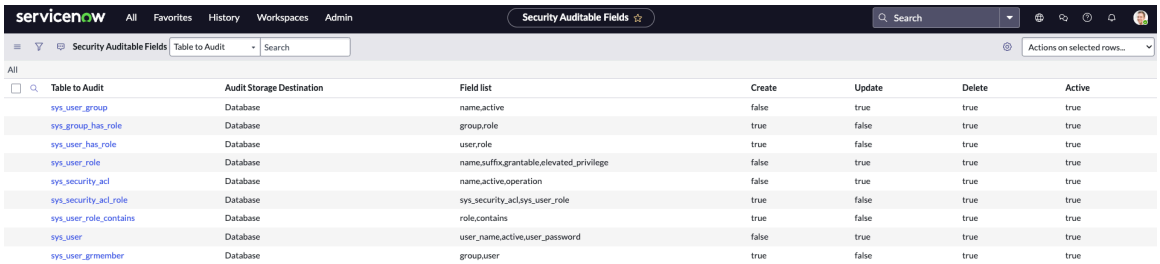


Table to Audit	Audit Storage Destination	Field list	Create	Update	Delete	Active
sys_user_group	Database	name,active	false	true	true	true
sys_group_has_role	Database	group,role	true	false	true	true
sys_user_has_role	Database	user,role	true	false	true	true
sys_user_role	Database	name,suffix,grantable,elevated_privilege	false	true	true	true
sys_security_acl	Database	name,active,operation	false	true	true	true
sys_security_acl_role	Database	sys_security_acl,sys_user_role	true	false	true	true
sys_user_role_contains	Database	role,contains	true	false	true	true
sys_user	Database	user_name,active,user_password	false	true	true	true
sys_user_grmember	Database	group,user	true	false	true	true

Les tables suivantes peuvent être auditées à l'aide de l'audit d'identité et d'accès :

- Groupe [sys_user_group]
- Rôle [sys_user_role]
- Contrôle d'accès [sys_security_acl]
- Utilisateur [sys_user]
- Rôle de groupe [sys_group_has_role]
- Rôle d'utilisateur [sys_user_has_role]
- Rôles d'accès [sys_security_acl_role]
- Rôle contenu [sys_user_role_contains]
- Membre du groupe [sys_user_grmember]

Configuration des tables et des champs

Audit d'identité et d'accès pour comprendre les changements apportés à un utilisateur, à un groupe, à un rôle et à un ACL.

Avant de commencer

Rôle requis : security_admin

Vous devez élever votre rôle au rang d'administrateur de sécurité pour configurer les tables et les champs pour l'audit d'identité et d'accès.

Les tables suivantes peuvent être configurées pour l'audit :

- Groupe [sys_user_group]
- Rôle [sys_user_role]
- Contrôle d'accès [sys_security_acl]
- Utilisateur [sys_user]
- Rôle de groupe [sys_group_has_role]
- Rôle d'utilisateur [sys_user_has_role]
- Rôles d'accès [sys_security_acl_role]
- Rôle contenu [sys_user_role_contains]
- Membre du groupe [sys_user_grmember]

Traduction automatique

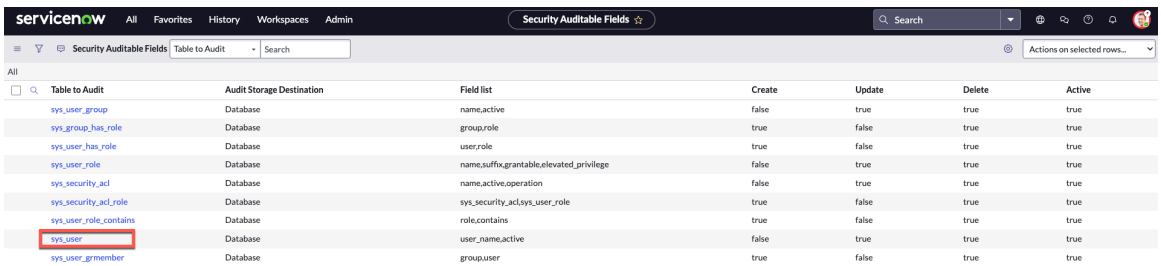
© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Remarque :
Pour comprendre quels champs peuvent être configurés pour les tables, reportez-vous à la section Champs pris en charge et non pris en charge pour l'accès à l'identité et l'audit.

Procédure

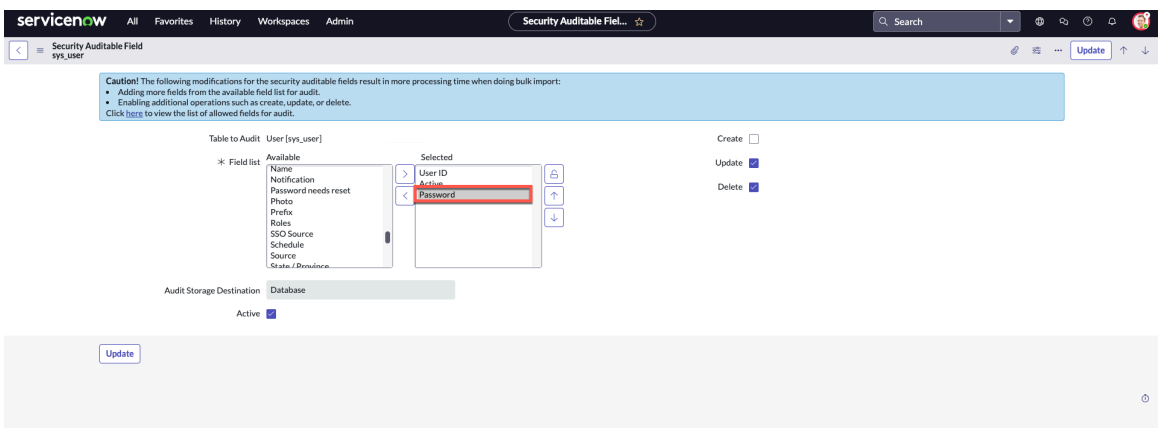
1. Accédez à la **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Configurer les tables et les champs**.
2. Sélectionnez la table à partir de laquelle vous souhaitez auditer un champ.

   Par exemple, **sys_user**.



3. Ajoutez le champ à auditer.

   Par exemple, **Mot de passe**.



Remarque :
Les modifications suivantes apportées aux champs auditables de sécurité entraînent une augmentation du temps de traitement lors de l'importation en bloc :

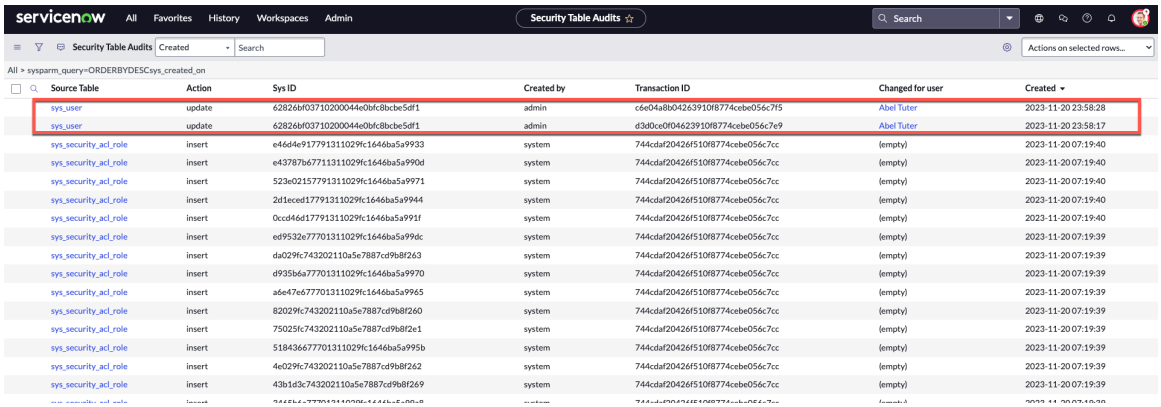
- Ajouter d'autres champs à partir de la liste de champs disponibles pour l'audit.
- Activation d'opérations supplémentaires telles que créer, mettre à jour ou supprimer.

4. Mettez à jour l'enregistrement.

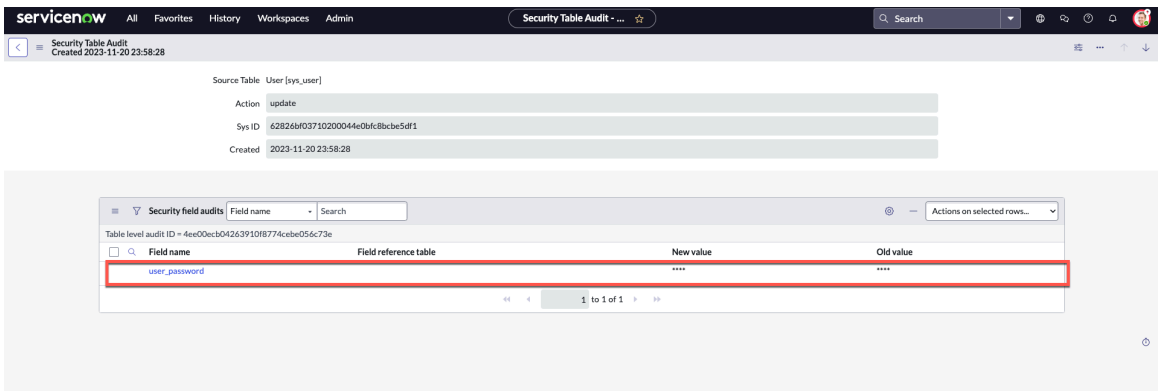
   Toute modification apportée au champ Mot de passe ajoute un nouvel enregistrement aux audits de la table de sécurité. Dans cet exemple, l'audit montre un champ de mot de passe modifié pour l'utilisateur **Abel Tuter**.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



La sélection de l'enregistrement créé affiche les détails des changements.



Configurer la période de conservation

Configurez la période de conservation pour l'audit d'identité et d'accès.

Avant de commencer

Rôle requis : administrateur

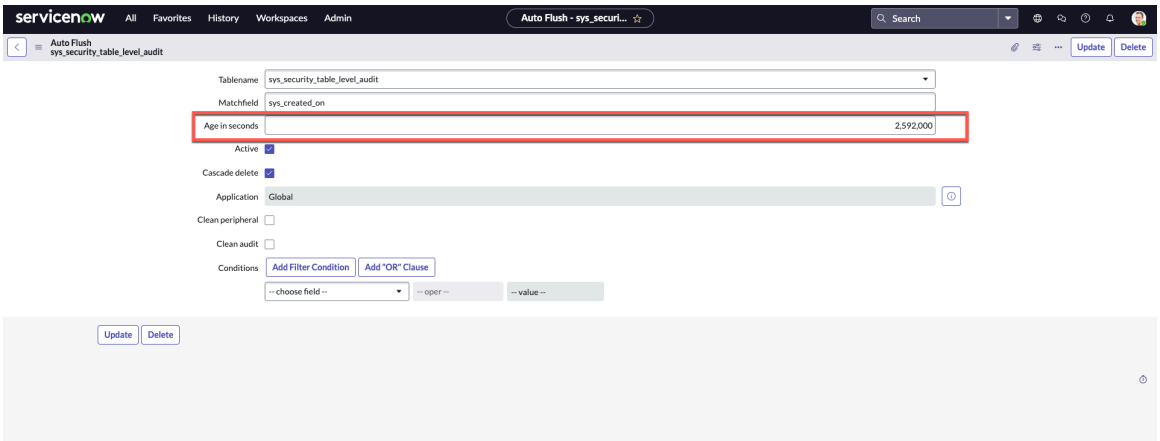
Procédure

1. Accédez à la **Tout** > **Sécurité de système** > **Audit d'identité et d'accès** > **Configurer la période de conservation**.
2. Sur le formulaire, vous pouvez modifier l'âge en quelques secondes.

> **Remarque :**
> Le nombre maximal de jours pour l'audit d'identité et d'accès est de 30 jours (2 592 000 secondes).

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.



3. Cliquez sur Enregistrer ou Mettre à jour pour enregistrer ou mettre à jour l'enregistrement.

Champs pris en charge et non pris en charge pour l'accès à l'identité et l'audit

Liste des champs pris en charge et non pris en charge pour l'audit.

La validation des champs d'audit empêche de choisir certains champs dans la table field_list de la configuration de l'audit des champs de sécurité (sys_sec_field_audit_config).

Champ pris en charge ou non pris en charge pour l'audit

Table	Champs pris en charge ou non pris en charge
Toutes les tables	Champs qui ne sont pas pris en charge : • Créé le (sys_created_on) • Créé par (sys_created_by) • Mis à jour par (sys_updated_by) • Date de mise à jour (sys_updated_on)
L'utilisateur a un rôle (sys_user_has_role)	Champs pris en charge : • Utilisateur • Rôle • Hérité • Nombre
Utilisateur (sys_user)	Champs qui ne sont pas pris en charge : • Dernière connexion (last_login) • Heure de la dernière connexion (last_login_time) • Dernière connexion Équipement (last_login_device)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Champ pris en charge ou non pris en charge pour l'audit (suite)

Table	Champs pris en charge ou non pris en charge
	• Activer l'authentification multifacteur (enable_multifactor_authn) • Perspective par défaut (default_perspective) • Intégration du calendrier (calendar_integration) • ID fédéré (federated_id) • Réinitialisation du mot de passe requise (password_needs_reset) • Échecs (failed_attempts) • Dernier mot de passe (last_password) • Serveur LDAP (ldap_server) • Verrouillé (locked_out) • Notification (notification) • Rôles (roles) • Domaine (sys_domain) • Chemin de domaine (sys_domain_path) • Format d'heure (time_format) • ID d'utilisateur haché (hashed_user_id) • Nom de classe (sys_class_name) • Nombre de changements (sys_mod_count)

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

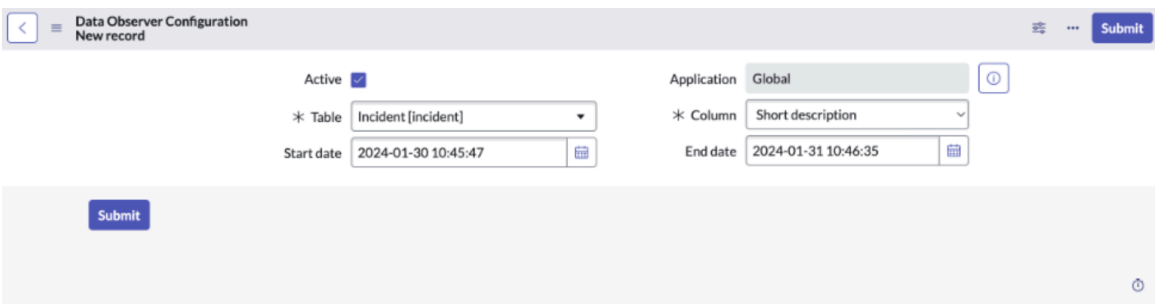
Accéder à l'observateur

Utilisez l'observateur d'accès pour comprendre les données d'accès des personnes et des processus sur votre instance.

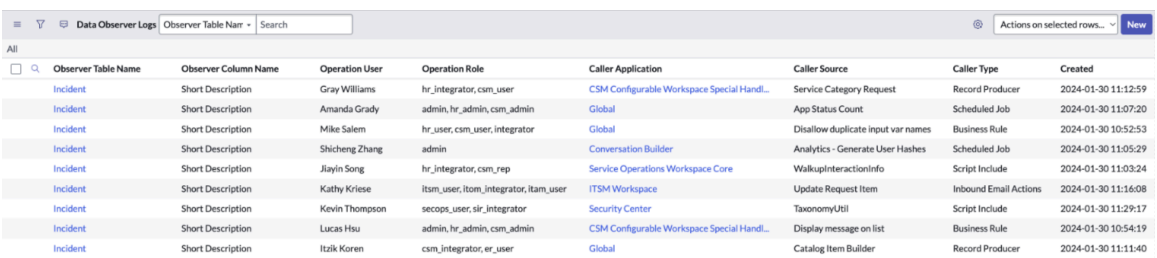
Avec Access Observer, les administrateurs de sécurité peuvent :

- Identifiez les entités telles que les utilisateurs, les rôles, les applications incluses dans le périmètre et les scripts qui accèdent à vos données.
- Utilisez cette connaissance préalable pour savoir comment appliquer au mieux la sécurité afin de limiter les accès inutiles à vos données, tout en confirmant celles qui nécessitent un accès tout en continuant à fonctionner normalement.
- Évitez les interruptions d'automatisation en visualisant une vue claire de la façon dont vos données sont accessibles avant d'apporter des modifications de sécurité.
- Répondez au besoin de fournir des informations sur la façon dont le chiffrement est appliqué sur votre instance.

Configurez l'observateur d'accès en créant des enregistrements de configuration d'observateur d'accès. Dans ces enregistrements, vous définissez une table et une colonne spécifiques à observer et l'heure à laquelle la colonne est observée.



Retrouvez les résultats de vos observations sur la table d'enregistrement du journal de l'observateur d'accès. Sur cette table, vous pouvez voir un enregistrement détaillant chaque fois que la colonne spécifiée est consultée.



Observer Table Name	Observer Column Name	Operation User	Operation Role	Caller Application	Caller Source	Caller Type	Created
Incident	Short Description	Gray Williams	hr_integrator, csm_user	CSM Configurable Workspace Special Handl...	Service Category Request	Record Producer	2024-01-30 11:12:59
Incident	Short Description	Amanda Grady	admin, hr_admin, csm_admin	Global	App Status Count	Scheduled Job	2024-01-30 11:07:20
Incident	Short Description	Mike Salem	hr_user, csm_user, integrator	Global	Disallow duplicate input var names	Business Rule	2024-01-30 10:52:53
Incident	Short Description	Shicheng Zhang	admin	Conversation Builder	Analytics - Generate User Hashes	Scheduled Job	2024-01-30 11:05:29
Incident	Short Description	Jiayin Song	hr_integrator, csm_rep	Service Operations Workspace Core	WalkupInteractionInfo	Script Include	2024-01-30 11:03:24
Incident	Short Description	Kathy Kriese	itsm_user, itom_integrator, itam_user	ITSM Workspace	Update Request Item	Inbound Email Actions	2024-01-30 11:16:08
Incident	Short Description	Kevin Thompson	secops_user, sir_integrator	Security Center	TaxonomyUtil	Script Include	2024-01-30 11:29:17
Incident	Short Description	Lucas Hsu	admin, hr_admin, csm_admin	CSM Configurable Workspace Special Handl...	Display message on list	Business Rule	2024-01-30 10:54:19
Incident	Short Description	Itzik Koren	csm_integrator, er_user	Global	Catalog Item Builder	Record Producer	2024-01-30 11:11:40

Configurer l'observation relative à l'accès

Créez un enregistrement d'observation d'accès pour examiner l'accès à une colonne de données pendant une fenêtre de temps spécifiée.

Avant de commencer
Rôle requis : security_admin

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Procédure

1. Accédez à la **Tout** > **Accéder à l'observateur** > **Accéder à une configuration d'observateur**.
2. Sélectionnez **Nouveau** pour créer un enregistrement.
3. Renseignez les champs du formulaire.

Accéder aux champs de configuration d'observateur

Champ	Description
Actif	Indique si l'enregistrement est actif ou non. Votre enregistrement est automatiquement marqué comme actif pendant la période d'observation et inactif dans le cas contraire.
Application	L'application incluse dans le périmètre de l'enregistrement. Ce champ est en lecture seule.
Table	Table contenant la colonne à observer
Colonne	Colonne de la table sélectionnée à observer.
Démarrer la tâche immédiatement	Si cette option est sélectionnée, l'observation commence dès la création de l'enregistrement.
Date/heure de fin	Heure à laquelle l'observation prend fin.
Date/heure de début	Heure à laquelle l'observation commence. Ce champ est uniquement visible si **l'option Démarrer la tâche immédiatement** n'est pas sélectionnée.

4. Sélectionnez **Soumettre** pour enregistrer l'enregistrement.

Que faire ensuite

Une fois que la fenêtre d'observation que vous avez définie a démarré, vous pouvez voir chaque cas où la colonne a été consultée détaillée dans les enregistrements de la table Journal de l'observateur d'accès [sys_data_ob_log].

Examiner les journaux de l'observateur d'accès

Utilisez les informations contenues dans les enregistrements du journal de l'observateur d'accès pour obtenir un aperçu de la façon dont vos données sont consultées.

Une fois que vous avez configuré un ou plusieurs enregistrements d'observation d'accès, votre instance commence à créer des enregistrements de journal d'observateur d'accès avec des détails sur l'accès aux colonnes que vous avez choisies. Vous pouvez trouver ces enregistrements sur votre instance à l'adresse **Tout** > **Accéder à l'observateur** > **Accéder au journal de l'observateur**.

Accéder aux résultats du journal de l'observateur

Utilisez la table suivante pour comprendre les informations présentées dans les journaux.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.

Accéder aux champs du journal de l'observateur

Champ	Description
Nom de la table de l'observateur	La table sélectionnée dans l'enregistrement d'observation d'accès qui a généré cet enregistrement.
Nom de la colonne Observateur	Colonne sélectionnée dans l'enregistrement d'observation d'accès qui a généré cet enregistrement.
Utilisateur de l'opération	Utilisateur ayant accédé à la colonne
Rôle de l'opération	Rôles de l'utilisateur ayant accédé à la colonne
Application de l'appelant	Application incluse dans le périmètre à partir de laquelle les données ont été consultées.
Type d'appelant	Type d'élément ayant accédé à la colonne, tel que le créateur d'enregistrement, la tâche planifiée ou la règle métier.
ID de document de la source de l'appelant.	
Source de l'appelant	Élément ayant accédé à la colonne. Utilisé le long du champ **Type d'appelant** pour voir ce qui a spécifiquement accédé à la colonne. Par exemple, si le type d'appelant est `Règle métier`, la source de l'appelant est le nom de la règle métier qui a accédé à la colonne.
Hachage primaire	
Nombre de répétitions	
Pile Java	
Pile JavaScript	
ID de session	ID de la session au cours de laquelle la colonne a fait l'objet d'un accès.

Traduction automatique

© 2025 ServiceNow. Tous droits réservés.
ServiceNow, le logo ServiceNow et les autres marques ServiceNow sont des marques commerciales et/ou des marques déposées de ServiceNow, Inc. aux États-Unis et/ou dans d'autres pays
D'autres noms de sociétés et de produits peuvent être la propriété des sociétés respectives auxquelles ils sont associés.