



Xanadu オペレーショナルテクノロジー 管理

最終更新日: 2025年12月17日

自動翻訳

これらの資料は、翻訳ソフトウェアを使用してお客様の便宜のために翻訳されています。正確な翻訳をご提供できるよう相当な努力を払っておりますが、いかなる自動翻訳も人間の翻訳者に代わることはなく、そのようなことは意図されておりません。翻訳は「現状のまま」提供されています。他言語への翻訳の的確性、信頼性または正確性については、明示または黙示を問わず、いかなる保証も行われません。翻訳ソフトには限界があるため、一部のコンテンツが正確に翻訳されていない場合があります。これらの資料の公用言語は英語です。翻訳の際に生じる相違または不一致は、コンプライアンスまたは履行の目的に関しては拘束力を有さず、法的効力はないものとします。

ここで示したいくつかの例と図は、説明の目的でのみ提供されています。ServiceNow 製品またはサービスへの実際の関連付けやつながりは意図されておらず、推測されるものではありません。

ServiceNow, ServiceNow のロゴ、Now、その他の ServiceNow マークは米国および/またはその他の国における ServiceNow, Inc. の商標または登録商標です。その他の会社名および製品名は、それぞれの所有者の商標です。

下記の ServiceNow ウェブサイト利用規約をお読みください。 www.servicenow.com/terms-of-use.html

自動翻訳

本社
2225 Lawson Lane
Santa Clara, CA 95054
United States
(408) 501-8550

目次

オペレーショナルテクノロジー.....	5
オペレーショナルテクノロジー管理 ライセンスとサブスクリプション.....	7
OTM へのサブスクリプション.....	8
インストール ITOM SU ライセンス.....	8
OTM のサブスクリプション統計情報の表示.....	10
割り当てられたサブスクリプションユニットに対する OTM リソースの使用状況を確認する.....	10
OTM サブスクリプションで使用する CI 数の確認.....	11
OTM サブスクリプションユニットを利用する CI を表示する.....	13
OTM SU ライセンス参照.....	14
オペレーショナルテクノロジーマネージャー.....	18
オペレーショナルテクノロジーマネージャーの詳細.....	19
オペレーショナルテクノロジーマネージャーの構成.....	22
オペレーショナルテクノロジーマネージャー統合.....	38
オペレーショナルテクノロジーマネージャーを使用する.....	116
オペレーショナルテクノロジーマネージャー参照.....	179
産業用プロセスマネージャー.....	182
産業用プロセスマネージャーの探索.....	183
産業用プロセスマネージャーの構成.....	185
での産業用プロセスマネージャーの使用 オペレーショナルテクノロジーマネージャー.....	206
産業用プロセスマネージャー参照.....	228
オペレーショナルテクノロジー脆弱性対応.....	234
オペレーショナルテクノロジー脆弱性対応の探索.....	235
オペレーショナルテクノロジー脆弱性ソリューション管理.....	236
オペレーショナルテクノロジー脆弱性対応の構成.....	237
オペレーショナルテクノロジー脆弱性対応統合.....	249
オペレーショナルテクノロジー脆弱性対応の使用.....	277
オペレーショナルテクノロジー脆弱性対応参照.....	284
オペレーショナルテクノロジーインシデント管理.....	285
オペレーショナルテクノロジーインシデント管理の探索.....	286
オペレーショナルテクノロジーインシデント管理の構成.....	289
オペレーショナルテクノロジーインシデント管理の使用.....	301
オペレーショナルテクノロジーインシデント管理参照.....	311
オペレーショナルテクノロジー変更管理.....	314
オペレーショナルテクノロジー変更管理の探索.....	315
オペレーショナルテクノロジー変更管理の構成.....	317
オペレーショナルテクノロジー変更管理の使用.....	328
オペレーショナルテクノロジー変更管理参照.....	341
オペレーショナルテクノロジーのナレッジ管理.....	343

オペレーショナルテクノロジーのナレッジ管理 の探索.....344

オペレーショナルテクノロジーのナレッジ管理の構成..... 345

オペレーショナルテクノロジーのナレッジ管理 の使用.....354

オペレーショナルテクノロジーのナレッジ管理 参照..... 361

オペレーショナルテクノロジー要求管理..... 364

オペレーショナルテクノロジー要求管理 の探索.....365

オペレーショナルテクノロジー要求管理の構成..... 366

オペレーショナルテクノロジー要求管理 の使用.....370

オペレーショナルテクノロジー要求管理 参照..... 371

産業用 ワークスペース.....376

産業用ワークスペースの探索.....377

の構成 産業用 ワークスペース.....392

産業用 ワークスペース の使用.....409

ドメインセパレーションと オペレーショナルテクノロジー.....421

オペレーショナルテクノロジー

ServiceNow for オペレーショナルテクノロジー を使用すると、デジタルワークフローを通じて、組織が運用を合理化し、生産性を向上させ、生産現場でオペレーショナルテクノロジーアップタイムを最大化できます。

概要

オペレーショナルテクノロジーとServiceNow オペレーショナルテクノロジー管理ソリューションの概要をご覧ください。

https://player.vimeo.com/video/957122379?h=d9c04a0637&badge=0&autopause=0&player_id=0&app_id=58479

オペレーショナルテクノロジー、コアオペレーション、工場労働者の能力強化におけるメリット



Operational Technology

Contextualize and safeguard your Operational Technology systems, connect to digital workflows, and respond quickly to threats.



Core Operations

Streamline and digitize standard operating procedures (SOPs) and enable shared knowledge and collaboration across the enterprise.



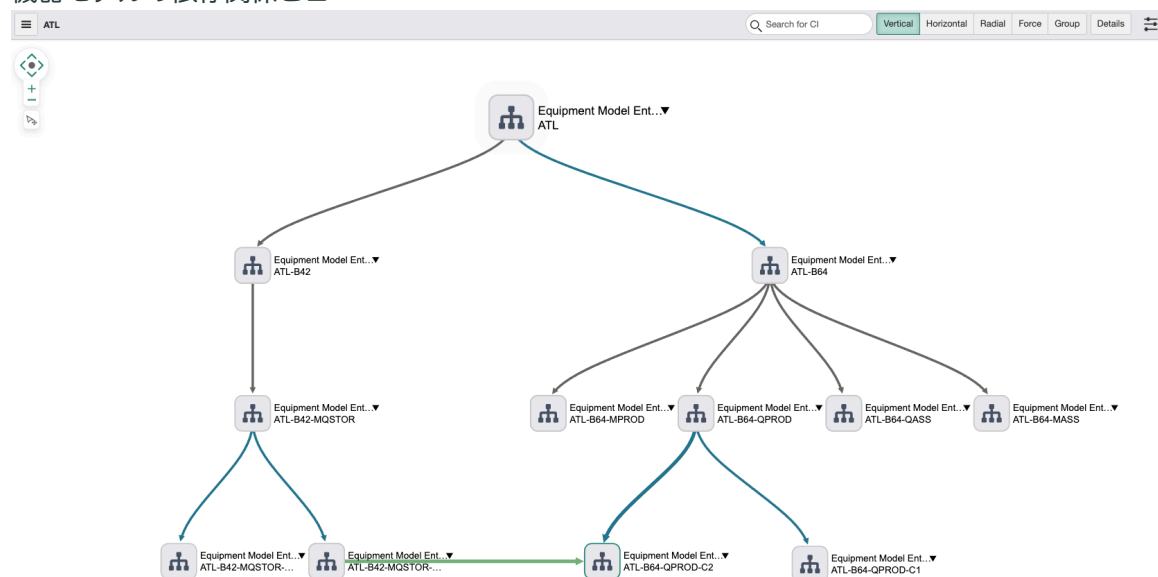
Factory Workers

Empower the workforce with digital tools and knowledge to adapt, collaborate, and excel in fast-changing conditions.

ServiceNow Operational Technology Management (オペレーショナルテクノロジー管理) でアップタイムを最大化し、運用レジリエンスを構築します

業界のオペレーショナルテクノロジーが登場する前は、メーカーは手動プロセスと従来の知識に依存して環境を維持していました。環境の全体像を把握し、そのすべてを保護、監視、管理することが難しいと感じていました。ServiceNow オペレーショナルテクノロジー管理ソリューションにより、産業組織はオペレーショナルテクノロジーシステムの完全で状況に応じたビューを取得できるようになりました。このビューを使用すると、システムの安全性と稼働を維持し、生産プロセスやデジタルワークフローに接続することができます。また、組織がイベントや脅威の評価、優先順位付け、対応を行うこともできます。

機器モデルの依存関係ビュー



デジタルマップを使用することで、組織は産業オペレーションプロセス、システム、および関係の可視性を高めることができます。このマップを使用すると、潜在的な生産への影響を簡単かつ迅速に管理および評価できます。

注: オペレーショナルテクノロジー管理ソリューションは Now Mobile[®] ではサポートされていません。

可視化の向上



オペレーショナルテクノロジーシステムの完全かつ状況に応じたビューを取得して、システムのセキュリティと稼働を維持できるようにします。

デジタルワークフロー



オペレーショナルテクノロジーシステムを生産プロセスとデジタルワークフローに接続します。

脆弱性管理



すべてを 1 か所で確認できるため、イベントや脅威の評価、優先順位付け、対応を行うことができます。

従業員の装備を整える

ローコードおよびノーコードのアプリケーションを構築して、従業員が共同で監視、拡張トラブルシューティング、問題解決、詳細な状況分析を実行できるようにします。

詳細については、[ソリューション概要](#) を参照してください。

開始するには

- [DemoNow](#) でデモされた機能をご覧ください。
- オペレーショナルテクノロジーの要求と設定の方法については、次を参照してください。
 - [オペレーショナルテクノロジーマネージャー](#) の構成
 - [産業用プロセスマネージャー](#) の構成
 - [オペレーショナルテクノロジー脆弱性対応](#)の構成
 - [オペレーショナルテクノロジーインシデント管理](#)の構成
 - [オペレーショナルテクノロジー変更管理](#)の構成
 - [オペレーショナルテクノロジーのナレッジ管理](#)の構成
- オペレーショナルテクノロジー が共通サービスデータモデル (CSDM)テーブルを管理および使用する方法の詳細については、「[オペレーショナルテクノロジーおよび CSDM テーブル](#)」を参照してください。
- オペレーショナルテクノロジー の最新リリースの詳細については、次を参照してください。
[ServiceNow Store - オペレーショナルテクノロジー リリースノート](#)。

アプリケーション

- [オペレーショナルテクノロジーマネージャー](#)
- [産業用プロセスマネージャー](#)
- [オペレーショナルテクノロジー脆弱性対応](#)
- [オペレーショナルテクノロジーインシデント管理](#)
- [オペレーショナルテクノロジー変更管理](#)
- [オペレーショナルテクノロジーのナレッジ管理](#)
- [オペレーショナルテクノロジー要求管理](#)
- サービス管理: [IT Service Management](#)
- セキュリティ: [脆弱性対応](#)
- 可視化: [IT Operations Management](#)

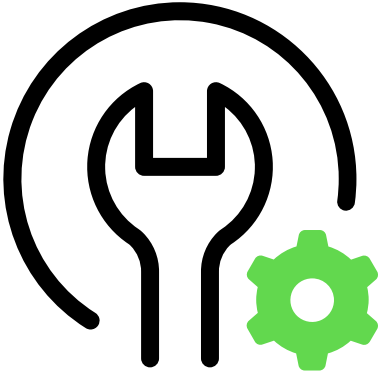
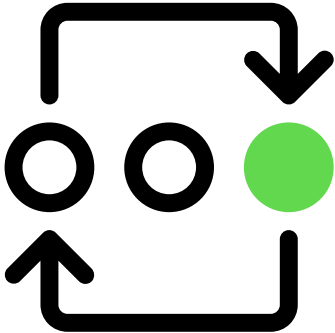
オペレーショナルテクノロジー管理 ライセンスとサブスクリプション

ServiceNow OTM[®]ライセンスは、監視対象のデバイスの数やサブスクリプション期間などの要素を含むサブスクリプションユニットに基づいてOTMサブスクリプションの使用状況を計算して表示するため、オペレーショナルテクノロジー管理 の重要な側面です。

概要

これにより、組織はコンプライアンスを確保し、リソースを効果的に割り当て、OTM 機能の拡張について情報に基づいた意思決定を行うことで、運用テクノロジーシステムを保護し、変化するセキュリティと運用ニーズに適応できます。OTM ライセンスモジュールを使用して、OTM製品 (ServiceNow OT Foundation、ServiceNow OT Visibility (OT ヴィジビリティ)、ServiceNow OT Vulnerability and Response (OT 脆弱性に対応) のサブスクリプション関連の詳細にアクセスします。

開始するには

OTMライセンスの詳細	の ITOM SU ライセンスのインストール OTM	ライセンス参照
 サブスクリプション関連の詳細について学習する	 プラグインの最新バージョンを更新する	 スケジュール済みジョブやテーブルなどのインストール済みコンポーネントに関する情報

自動翻訳

サポートへの連絡

連絡先 [カスタマーサービス & サポート](#)

OTM へのサブスクリプション

ServiceNowプラットフォームは、製造業のライセンス管理にOTMを採用しています。OTMには、IT Operations Management (ITOM)にあるライセンスと、OTMドメイン専用のライセンスが含まれます。

IT Operations Management (ITOM)ライセンスと同様の方法でOTMライセンスを監視します。ServiceNowインスタンス内でOTMは、**ITOM** ライセンスカテゴリメタデータ (**OTM** ライセンス > **CI** タイプ別のライセンス) ページで、[**SKU** タイプ] 列に **otm** の値が表示されます。既定では、ライセンス フィルターは [**SKU** タイプ に **otm** を含む] に設定されています。

インストール **ITOM SU** ライセンス

ServiceNow ITOM SU Licensing [sn_itom_licensing] をインストールまたは更新して、最新のライセンス機能を実際に使用できるようにします。このアプリケーションには、デモデータが含まれています。まだインストールされていない場合は、関連する ServiceNow Store アプリケーションとプラグインをインストールします。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「」を参照してください。[のエンタイトルメントを取得する ServiceNow 製品またはアプリケーション](#)。
- 依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性については、ServiceNow Store の [ITOM SU ライセンス](#) アプリケーションリストを確認してください。

必要なロール：admin

このタスクについて

2022 年第 1 四半期より前は、元のライセンスメカニズムはファミリーリリースの一部として提供されていました。それ以降は、ライセンスメカニズムは ServiceNow Store の ServiceNow ITOM SU Licensing を使用して提供されます。システムは自動的に ServiceNow ITOM SU Licensing をインストールします。このアプリケーションの更新が ServiceNow Store で利用可能になると、通知を受信します。

ITOM SU Licensing とともに次のアイテムがインストールされます。

- スケジュール済みジョブ
- テーブル

詳細については、「[ITOM SU ライセンスとともにインストールされるコンポーネントOTM](#)」を参照してください。

手順

1. 移動先 **すべて > システムアプリケーション > 利用可能なすべてのアプリケーション > すべて**.
2. フィルター基準と検索バーを使用して、アプリケーション (sn_itom_licensing) を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることがあります。

[更新] ボタンの横のリストに、使用可能なバージョンが表示されます。

3. リストからバージョンを選択し、[更新] を選択します。

表示されるインストールダイアログには、アプリケーションとともにインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエンタイトルメントを取得します。
5. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。
デモデータには、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードが含まれています。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

重要:

インストール時にデモデータを読み込んでおかないと、後から読み込むことはできません。

6. [更新] を選択します。

OTM のサブスクリプション統計情報の表示

組織で購入および消費された OTM アプリケーションサブスクリプションの数を表示し、リソース管理と運用テクノロジーの最適化に関する貴重なインサイトを提供します。

始める前に

- 組織に有効な OTM サブスクリプションがあることを確認します。
- から利用可能な最新バージョンの ITOM SU ライセンスをインストールしたことを確認します
[ServiceNow Store](#)。

必要なロール：sn_itom_license reader

このタスクについて

構成アイテム (CI) の割り当てとその割り当てレベルを評価して、組織の OTM サブスクリプション使用率を評価し、将来のサブスクリプション要件に備えます。

手順

1. 単品で購入した OTM サブスクリプションのサブスクリプション情報を表示するには、次の場所に移動します。 **OTM** ライセンス > ライセンスのサマリー。
2. **OTM 製品の [サブスクリプション] フォーム**の説明に従って、フォームに表示される詳細を確認します。

割り当てられたサブスクリプションユニットに対する OTM リソースの使用状況を確認する

OTM製品が管理できるリソース統計を確認および分析し、この情報をサブスクリプションユニットの平均割り当てと比較します。

始める前に

必要なロール：admin

このタスクについて

OTM ライセンスダッシュボードを使用して、OTMの詳細なライセンスデータの傾向を調べます。日次 CI 数を確認するか、過去 90 日間の日次カウントの平均を表示します。この機能により、ドメイン固有の情報と日次カウントごとに特定の CI リストが提供されるため、リソースの使用状況を経時的に効果的に監視および分析できます。

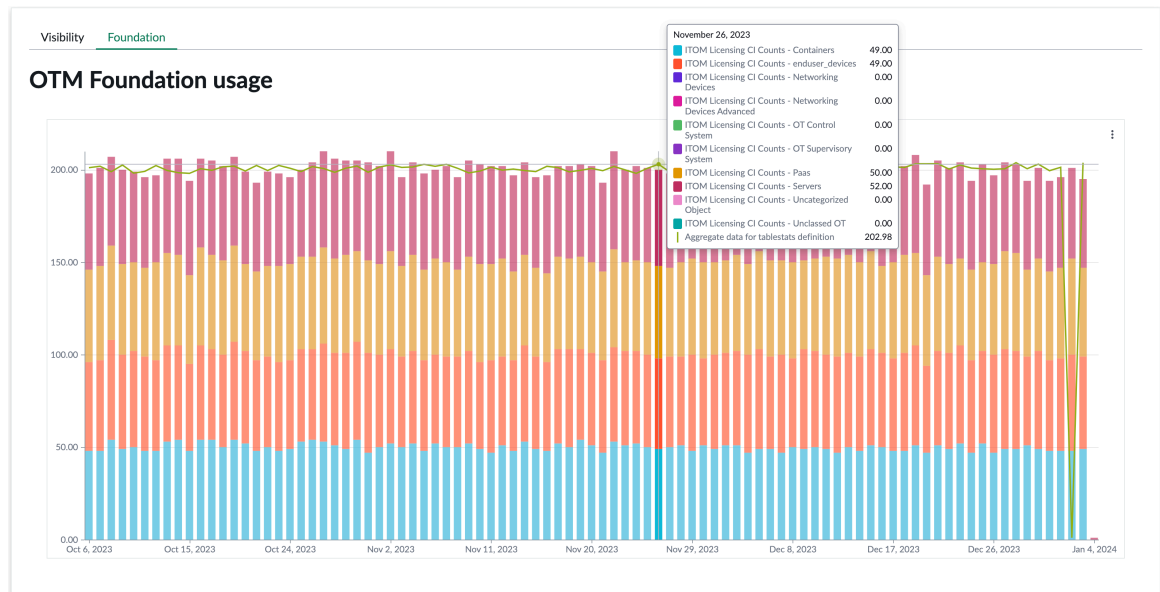
注:

SG-OT Excel によって管理されている CI は、90 日より前、90 日以上、または 90 日より古いlast_scan日付のライセンス消費としてカウントされ、リストされます。

手順

1. 移動先 **すべて > OTM ライセンス > OTM ライセンスダッシュボード**。
2. 関連するタブを選択して、OTM 製品のダッシュボードを表示します。
たとえば、[**Foundation** (基盤)] を選択します。

OTM ライセンスダッシュボード



3. バーをポイントすると、各カテゴリの CI の数が表示されます。
4. バーを選択すると、カウントされた CI のリストが表示されます。
5. 「OTM ライセンスダッシュボード」で説明されているダッシュボードを確認します。

OTM サブスクリプションで使用する CI 数の確認

CI データの直近 90 日間の日次カウントまたは平均を表示します。ServiceNow OT Foundation (OT 基盤)、ServiceNow OT Visibility (OT ヴィジビリティ)、ServiceNow OT Vulnerability and Response (OT 脆弱性対応) では、OTM アプリケーションがサポートするライセンス済みリソースに関するインサイトが得られます。アプリケーション OTM 検出、監視、およびプロビジョニングするリソースは、CMDB に格納されている構成アイテム (CI) です。OTM ライセンスモジュールは、この CI 情報と組織が購入したサブスクリプションに関する情報を組み合わせて、OTM アプリケーションによるサブスクリプションの使用に関する統計情報を生成します。

始める前に

- 組織に有効な OTM サブスクリプションがあることを確認します。
- から利用可能な最新バージョンの ITOM SU ライセンスをインストールしたことを確認します [ServiceNow Store](#)。

必要なロール：sn_itom_license reader

このタスクについて

ServiceNow OT Foundation、ServiceNow OT Visibility および ServiceNow OT Vulnerability and Response の使用に対して料金が発生します。OTM サブスクリプションに含まれる製品と機能の詳細については、「[OTM へのサブスクリプション](#)」を参照してください。

ライセンス目的でデータを収集して統合する手順には、次の一連のアクションが含まれます。

1. OTM ライセンスシステムは、各 OTM 製品によって管理される構成アイテム (CI) の日次数を計算し、その後、これらの CI 数を個別のライセンス可能な CI カテゴリに分類します。
2. 同一の構成アイテム (CI) が同じ OTM 製品内のさまざまな機能によって管理されている場合は、CI 数の重複を排除するために調整が行われます。

- IT 構成アイテム (IT CI) が OT 構成アイテム (OT) 構成アイテム (OT) として分類されている場合、CI は 1 回だけカウントされます。OTM ライセンスではカウントされ、ITOM ライセンスではカウントされません。
- ライセンスモジュールは、OTM アプリケーションの CI 数を統合して、過去 90 日間の日次 CI 数の平均を計算します。



注:

SG-OT Excel によって管理される CI は、90 日前以降、90 日以上前の last_scan 日付のライセンス消費用にカウントされ、一覧表示されます。

- ライセンスモジュールは、OTM アプリケーションの日次平均 CI 数を顧客契約に指定されたライセンスの詳細と照合して、ライセンス関連の統計情報を生成します。

その結果、購入したサブスクリプションユニットを組織でどのように利用しているかを示す統計情報を表示できます。

OTM アプリケーションごとに購入した CI 数とサブスクリプションについて、次の情報を表示します (個別)。

- 合計数: 個々の OTM アプリケーションについて、CI タイプ別に分類された、90 日間にわたって収集された CI 数の平均。



注:

SG-OT Excel によって管理される CI は、90 日前以降、90 日以上前の last_scan 日付のライセンス消費用にカウントされ、一覧表示されます。

- サブスクリプションユニット率: 比率によって、サブスクリプションを必要とする特定の CI カテゴリの CI の数が決まります。ライセンスモジュールは、顧客契約からこの比率情報を取得します。
- 消費されたサブスクリプションユニットの合計数: 各 OTM アプリケーション内の各 CI カテゴリに対して組織が使用しているサブスクリプションの数。この計算は、各 CI カテゴリ内の CI 数にサブスクリプションユニット率を適用することによって実行されます。
- 消費されたサブスクリプションユニットの合計数: すべての OTM アプリケーションによって消費されたサブスクリプションユニットの合計。

ドメイン別に分類され OTM サブスクリプションユニット (SU) の消費量にアクセスできます。このデータは、消費と経費をさまざまな組織に割り当てるのに役立ちます。

手順

1. 移動先 OTM ライセンス > ライセンスレポート。

ITOM Licensing CI Counts View: License_report CI Category Search				
All > SKU > OTM > Aggregated = true > Total Count > 0				
CI Category	Domain	Total Count	Subscription Unit Ratio	Total Subscription Units Consumed
Application: Visibility (6)				
Networking Devices	global	17	25:1	0
OT Control System	global	210	3:1	70
OT Field Device	global	19	10:1	1
OT Supervisory System	global	7	1:1	7
Servers	global	20	1:1	20
Unclassified OT	global	49	1:1	49
Sum				147
Sum				147

2. オプション: 過去 90 日間の日次 CI 数の平均を表示します。

3. オプション: 日次 CI 数を表示するには、フィルターを変更して [集計済み] を **false** に設定します。

(Optional) 必要に応じて、列をソートしてビューを変更できます。[作成日時] 列には、CI 情報が最後に更新された日時を示すタイムスタンプが表示されます。

OTM サブスクリプションユニットを利用する CI を表示する

ServiceNow OT Foundation、ServiceNow OT Visibility (OT ヴィジビリティ)、ServiceNow OT Vulnerability and Response (OT 脆弱性対応) の OTM アプリケーションのそれぞれについて、現在カウント可能な CI のリストを生成します。

始める前に

- 組織に有効な OTM サブスクリプションがあることを確認します。
- から利用可能な最新バージョンの ITOM SU ライセンスをインストールしたことを確認します [ServiceNow Store](#)。

必要なロール: sn_itom_license reader

このタスクについて

生成される CI リストは、直近の日次 CI 数と強く相関しています。ただし、最後の日次カウント以降に変更が発生した場合、生成されたリストの CI の数が最新の日次カウントと比較してわずかに不一致を示す可能性があります。

手順

1. 移動先 **すべて > OTM ライセンス > OTM のライセンス可能な CI** をレポート。
[ITOM のライセンス可能な CI をレポート] ページが表示されます。
2. ライセンス済み CI を表示するアプリケーションを選択します。
 - Foundation
 - ヴィジビリティ
 - HLA
 - 健全性

Application	Max Results	Status	Progress	Additional Filters for CIs
Foundation	10,000	Completed	1/10000	
Health	10,000	N.A.	N.A.	
Visibility	10,000	Completed	1/10000	
HLA	10,000	N.A.	N.A.	

3. 選択したアプリケーションのレポートを作成するには、[ライセンス可能な CI を入力] を選択します。
4. 確認メッセージに同意し、レポートを生成するには、[はい] を選択します。

新しいレポートで、以前に生成されたレポートのデータが置き換えられます。レポートをキャンセルするには、アプリケーションを選択し、[ジョブのキャンセル] オプションを選択します。

5. 数分待ってから、ページを更新します。
レポートの処理が完了すると、アプリケーションのステータスが [完了] と表示されます。

6. アプリケーションを選択し、[ライセンス可能な CI を表示] を選択します。

OTM SKU の [ライセンス可能な CI ITOM] ページに、OTMライセンスを持つ CI のリストが表示されます。

OTM SU ライセンス参照

参照トピックを使用して、OTM ライセンスとともにインストールされるコンポーネント、OTM 製品のサブスクリプションフォーム、および OTM ライセンスダッシュボードの概要に関する貴重なインサイトを得ることができます。サブトピックに移動して、これらの重要な各側面に関する特定のガイダンスと参照にアクセスし、OTM サブスクリプションとライセンス要件を効果的に管理するのに役立ちます。

ITOM SU ライセンスとともにインストールされるコンポーネントOTM

スケジュール済みジョブやテーブルなど、いくつかのタイプのコンポーネントが、OTM SU Licensing プラグインのアクティブ化とともにインストールされます。

インストールされるスケジュール済みジョブ

スケジュール済みジョブ	説明
ITOM 除外テーブル更新ストア	除外リストを更新します。
ITOM ライセンス集計ストア	過去 90 日間の日次 CI 数の平均を計算します。
ITOMHealthCIReporterWithOTOMCountOTOMStore	OTM 健全性のライセンス可能な CI のリストを編集します。
ITOM Health ライセンス使用回数ストア	OTM健全性の日次 CI 数を計算します。
OTOM ライセンス可視化 CI リストストア	OTM可視化のためにライセンス可能な CI のリストをまとめます。
OTM Foundation ライセンス CI リストストア	OTM Foundation のライセンス可能な CI のリストをまとめます。
OTM 基盤ライセンス使用回数ストア	OT Foundation の日次ライセンス可能な CI 数を計算します。

インストールされるテーブル

テーブル	説明
ITOM LU Discovery ソースマッピング [itom_lu_discovery_source_mapping]	各カテゴリのライセンス可能な検出ソースのリストが含まれています。
ITOM LU Governance アプリのマッピング [itom_lu_governance_app_mapping]	ガバナンスアプリケーションとそれぞれのライセンス可能な CI とのマッピングを含むレコードのリスト。
ITOM LU Governance CI [itom_lu_governance_ci]	Governance ライセンスでカウントされる CI のリストが含まれています。

テーブル	説明
ITOM ライセンス除外メタデータ [itom_license_exclusion_metadata]	さまざまなライセンスに適用可能な除外ルールの一覧が含まれています。
ライセンスの除外 [license_exclusion_list]	除外ルールに基づいてライセンス数から除外する必要がある CI の一覧が含まれています。
可視化 LU 一時 [visibility_lu_temp]	Discovery ライセンスでカウントされる CI の一覧が含まれています。
ITOM ライセンスカテゴリメタデータ [itom_lu_category_metadata]	ライセンスのメタデータが含まれています。
ITOM ライセンスの検出ソース [itom_lu_discovery_sources]	すべての検出ソースのカテゴリが含まれます。

OTM 製品の [サブスクリプション] フォーム

サブスクリプション管理を簡素化し、OTM 製品の使用状況を明確にすることを可能にする、当社製品のサブスクリプションフォームにある重要なフィールドとインジケータについて説明します。

個別に購入したアイテム (単品) に関する次のサブスクリプション統計情報を表示します。

名前

OTMアプリケーションの名前。

購入日

アプリケーションごとに購入したサブスクリプションの数。

キャパシティ定義 ID

アプリケーションからサブスクリプションユニットの日次消費データを取得するために使用される ID。

開始日/終了日

このサブスクリプションがアクティブである期間。

単品サブスクリプション

ライセンスモジュールは、次のようにサブスクリプションの利用量を計算して表示します。

単品サブスクリプション

[サブスクリプション] ウィンドウには、購入して割り当てられた、OTM アプリケーションへのサブスクリプションの情報が表示されます。

購入した単品サブスクリプションを表示する [サブスクリプション] ウィンドウ

Subscriptions

Name

Search

Actions on selected rows...

New

One or more of your custom applications is not mapped to a subscription. [Go to Custom Table Inventory](#) to map your applications to your purchased subscriptions.

Not all subscription services are monitored and not all of your purchased subscriptions may appear in the list. [More Info](#)

All > Sys ID = 77d9e0a687042d105a79c809cebb3541

☐	Name	Start date	End date	Purchased	Allocated
☐	Operational Technology Visibility - Subs...	2021-11-30	2024-11-29	25840	460

OTM ライセンスダッシュボード

OTM ライセンスダッシュボードを使用して、取得したサブスクリプションに関連するリソース消費とステータスを評価します。ダッシュボードは、各 OTM アプリケーション専用のレポートを提供し、日次使用回数と 90 日間のサブスクリプションユニットの平均使用率を視覚的に表示します。OTM ライセンスダッシュボードは、ServiceNow Store からアクセスできる ITOM ライセンスアプリケーションバージョン 4.0 の不可欠なコンポーネントです。

ストアでアプリを要求する

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースメモ情報については、「[ServiceNow Store バージョンの履歴リリースノート](#)」を参照してください。

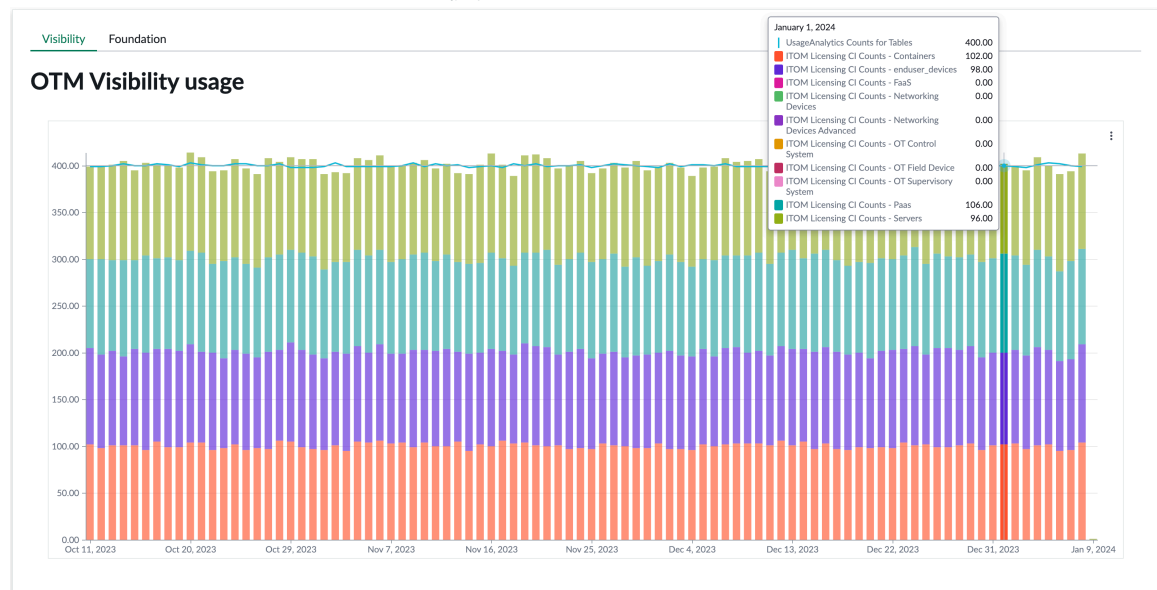
必要な Now Platform ロール

admin

アセスメントダッシュボードへのアクセス

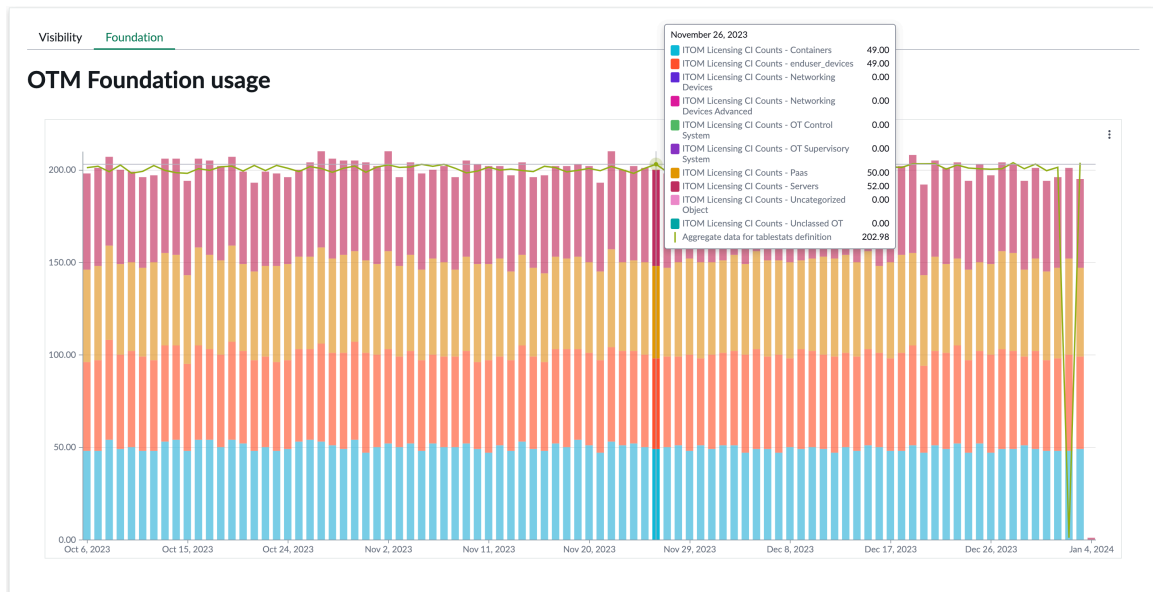
OTM用のダッシュボードを開くには、次の場所に移動します。すべて > **OTM ライセンス** > **OTM ライセンスダッシュボード**。

OTM ライセンスダッシュボード - 可視化



自動翻訳

OTM ライセンスダッシュボード:基盤



ユースケース

組織内のさまざまなユーザーがこのダッシュボードをどのように使用するかの例については、次のユースケースを参照してください。

ユーザー	ダッシュボードの使用方法
admin	さまざまな OTM 製品のリソース使用率を検証します。組織が特定のリソースで購入したサブスクリプションユニットの数を超えたケースを報告します。



注:

ServiceNowアプリケーションは、構成アイテム (CI) としてアプリケーションサービスを構成するデバイスおよびアプリケーションを参照します。

データの可視化

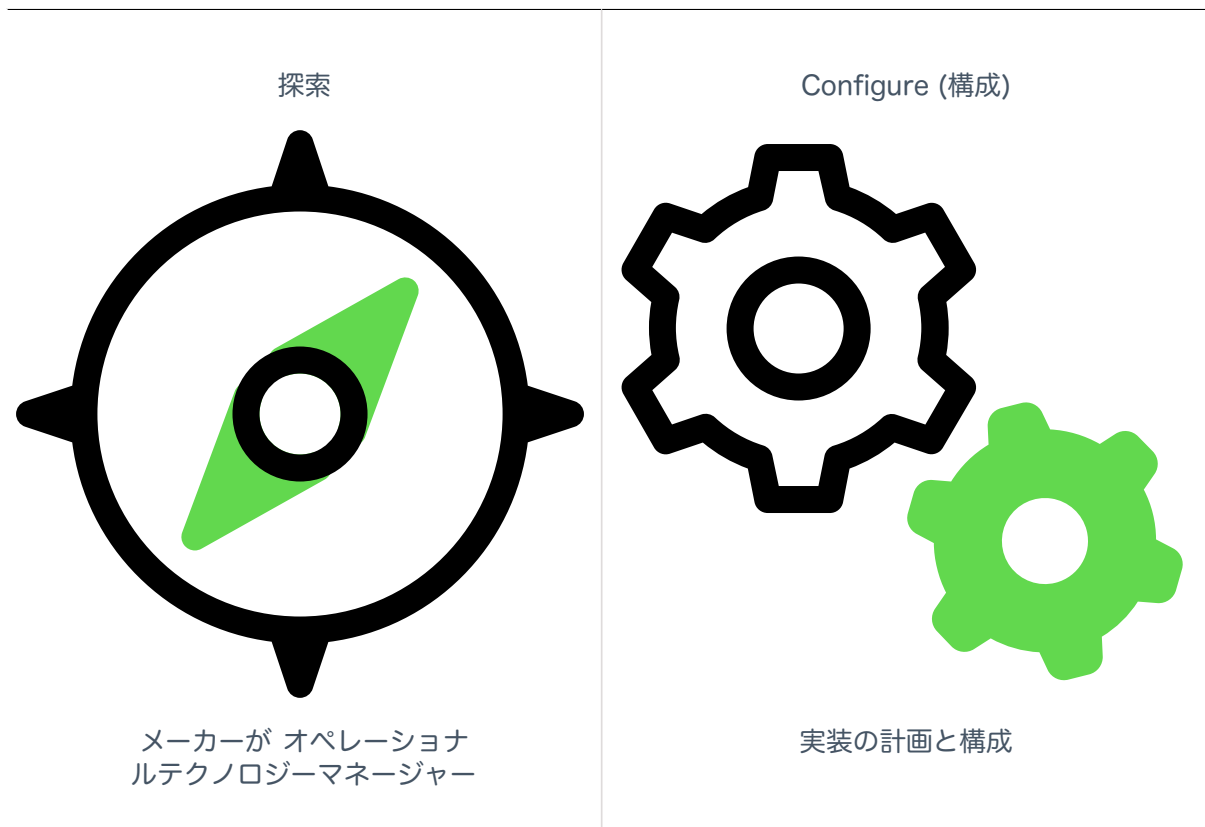
ダッシュボードには、次の可視化が含まれています。

タイトル	ソーステーブル	Description (説明)
OTM 可視化の使用状況と OTM 基盤の使用状況	ITOM ライセンス CI 数 [itom_lu_ci_counts] および テーブルの利用状況 アナリティクスカウント [usageanalytics_count]	ITOM アプリケーションごとに過去 120 日間のさまざまなライセンス可能なカテゴリの CI の数を表すバーを表示します。ダッシュボードには、過去 90 日間のサブスクリプションユニットの平均利用量を表す線も表示されます。

タイトル	ソーステーブル	Description (説明)
		i 注: SG-OT Excel によって管理される CI は、90 日前以降、90 日以上前の last_scan 日付のライセンス消費用にカウントされ、一覧表示されます。

オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー アプリケーションは、組織が ServiceNow® オペレーショナルテクノロジー ソリューションを使用できるようにするための基盤データと関係性を作成します。オペレーショナルテクノロジーマネージャー は、Now Platform での 構成管理データベース (CMDB)、サービスグラフ コネクタ、および ディスカバリー アプリケーションの使用をサポートしています。

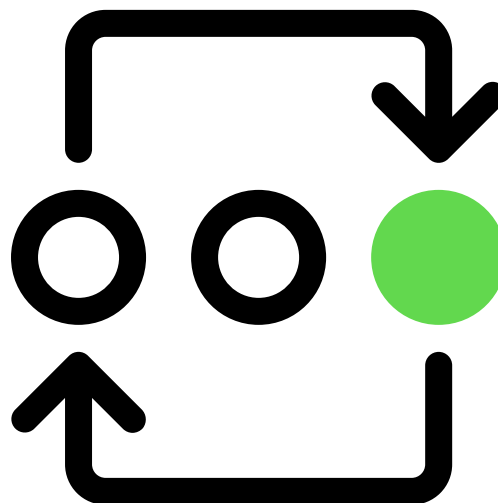


使用



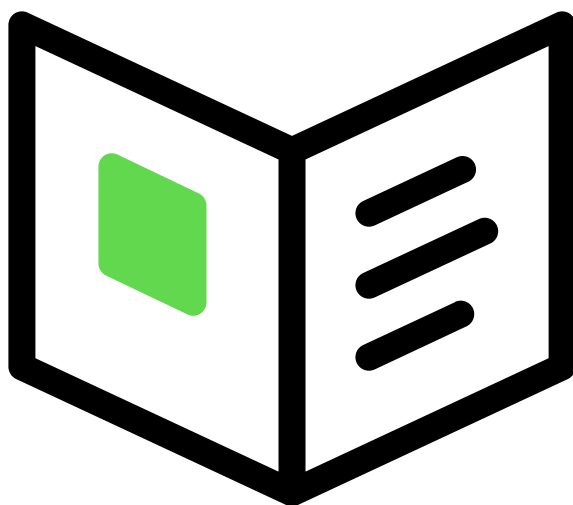
オペレーショナルテクノロジーデバイスのインポート、検出、およびレビュー

データ連携



他のアプリケーションとの統合による オペレーショナルテクノロジーマネージャー の拡張

参照



関連情報とアプリケーションの詳細を取得

オペレーショナルテクノロジーマネージャーの詳細

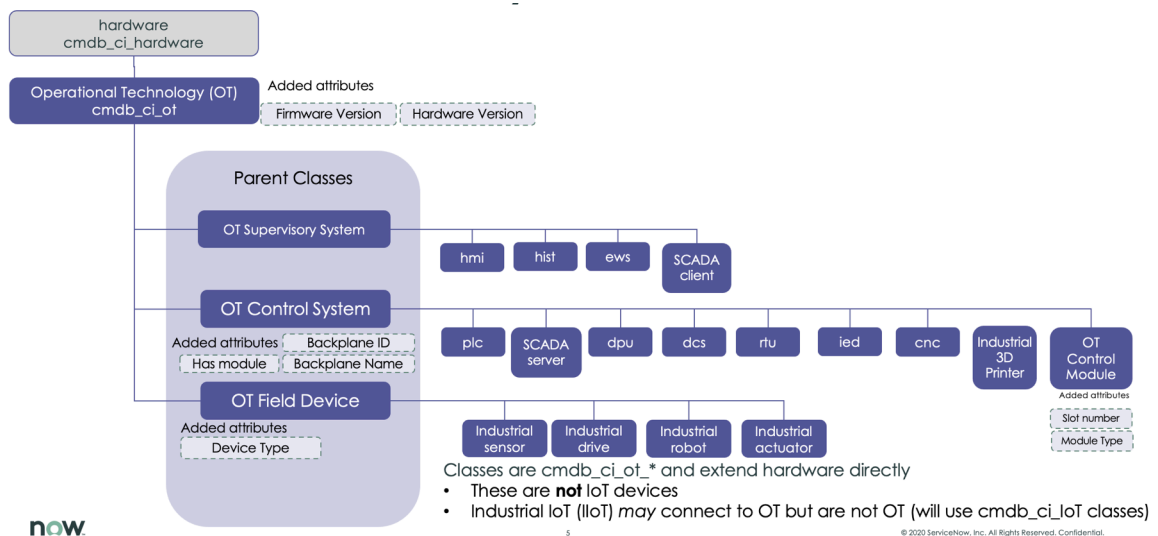
オペレーショナルテクノロジーマネージャー アプリケーションを使用して、企業が ServiceNow[®] オペレーショナルテクノロジー ソリューションを使用できるようにする基盤データと関係を作成する方法について説明します。

オペレーショナルテクノロジーマネージャーは、Now Platform での 構成管理データベース (CMDB)、サービスグラフ コネクタ、および ディスカバリー アプリケーションの使用をサポートします。

オペレーショナルテクノロジーマネージャー (OT) 構成アイテム拡張クラス

オペレーショナルテクノロジーマネージャー は オペレーショナルテクノロジー (OT) 構成アイテム (CI) 拡張クラスを使用して、次の図に示すように CMDB クラス階層を拡張します。

OT CI 拡張クラスが OT デバイスと等しい



オペレーショナルテクノロジーマネージャー クラスの説明、識別ルール、識別子エントリ、および依存関係 (該当する場合) が含まれます。サービスグラフ アプリケーションは、これらのクラス拡張を使用して CI を設定し、さまざまなテクノロジーとソフトウェアを検出します。詳細については、「[運用技術 \(OT\) 拡張クラス](#)」を参照してください。

の CMDB CI クラス オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー は 構成管理データベース (CMDB) CMDB CI クラスモデルアプリケーションの一部であるこれらの構成アイテム (CI) クラスを追加します。

注:

このアプリケーションの詳細については、次の場所にある CMDB CI Class Models アプリケーションを参照してください。 [ServiceNow ストア](#)。

オペレーショナルテクノロジーマネージャー ワークフローの CMDB CI クラス

クラス	Description (説明)	拡張された CI クラス
ネットワーク侵入検知システム	ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワーク監視アプライアンスと、それが検出するネットワーク上のデバイスとの間の関係を構築します。	cmdb_ci_nids

OT デバイスデータのインポートとディスカバリー

既存の オペレーショナルテクノロジー デバイスデータを Now Platformにアップロードするには、複数の方法があります。

サービスグラフ コネクタ (Excel)

サービスグラフ コネクタ (Excel) 機能を使用して、入力された Microsoft Excel フラットファイルスプレッドシートからオペレーショナルテクノロジーデータをインポートできます。統合ハブ抽出変換ロード (ETL) でスプレッドシートを使用して、このデータをCMDBにアップロードします。詳細については、「[サービスグラフオペレーショナルテクノロジー用コネクタ \(Excel\)](#)」を参照してください。

オペレーショナルテクノロジー のディスカバリー

産業用コントロールシステム (ICS) ネットワークで指定された Purdue レベルのオペレーショナルテクノロジーデバイスを検出するには、オペレーショナルテクノロジー機能のディスカバリーを繰り返し実行します。これは、標準のディスカバリープロセスと同様の方法で動作します。ただし、そのディスカバリーは通常、OT ディスカバリースケジュールの作成時に選択したレベルに応じて、Purdue レベル 3 ~ 3.5 で行われます。詳細については、「[オペレーショナルテクノロジー のディスカバリー](#)」を参照してください。

i 注:

産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。

サービスグラフServiceNow パートナーのコネクタ

ServiceNow パートナーは、既存の OT データのアップロードに使用できる サービスグラフ コネクタも提供しています。

OT ネットワークと標準的な IT ネットワークの違い

オペレーショナルテクノロジーネットワークと標準の情報技術(IT)ネットワークにあるデバイスを構成管理データベース (CMDB)が処理する方法には違いがあります。

Information Technology Operations Management (ITOM) で管理される構成アイテム (CI) は、CMDBでは IT タイプに分類されます。これらは、Purdue モデルのレベル 4 と 5、またはエンタープライズレベルで存在します。

OT データモデルで管理されるデバイスは、Purdue モデルのレベル 0 から 3.5 に存在し、OT デバイスには次の 2 つの主要コンポーネントがあります。

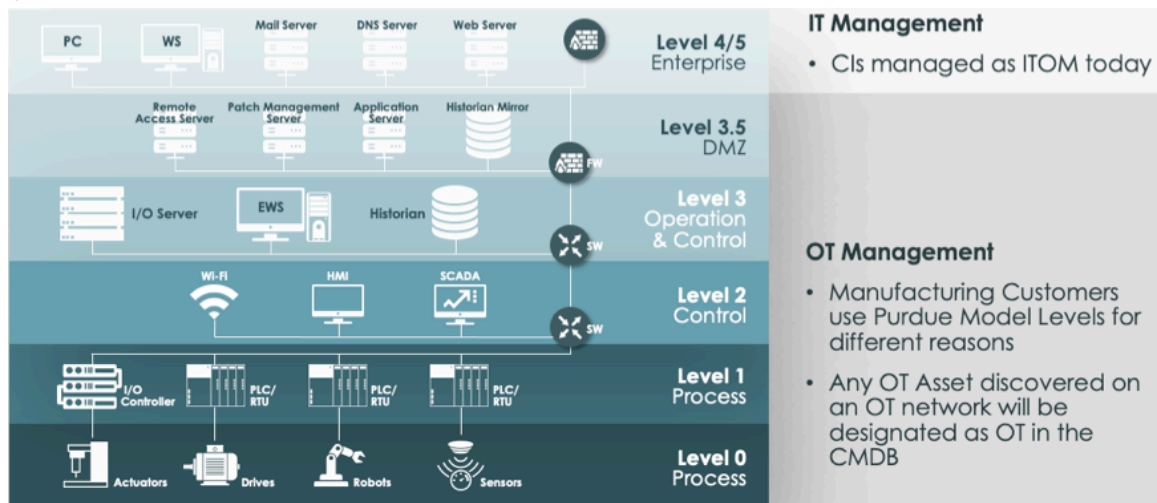
1. CI クラスレコード。これは、IT クラス、または OT クラスの CI です。
2. OT デバイスの詳細レコード。OT デバイスタイプ (機能) およびその他の OT 固有の属性を説明するものです。

i 注:

OT データモデルと拡張クラスの詳細については、「[Operational Technology \(OT\) extension classes](#)」を参照してください。

次の図は、これらの違いを示しています。

オペレーショナルテクノロジー **CMDB** クラスモデルは **Purdue** レベルをサポートします



注:

Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。

オペレーショナルテクノロジー マネージャー の構成

ServiceNow オペレーショナルテクノロジー ソリューションのデータ基盤を作成できるように、オペレーショナルテクノロジー マネージャー アプリケーションを構成します。

タスク	目的
1. オペレーショナルテクノロジー (OT) 拡張クラスをインストールします。	オペレーショナルテクノロジー処理で使用するために構成管理データベース (CMDB) クラス階層を拡張します。
2. インストール オペレーショナルテクノロジー マネージャー。	オペレーショナルテクノロジー マネージャー アプリケーションをインストールします。
3. オペレーショナルテクノロジー ロールをアサインします。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
4. サービスグラフ Connector インポート用の Microsoft Excel スプレッドシートを準備します。	Now Platformにアップロードするために、Microsoft Excel スプレッドシートを作成して既存のオペレーショナルテクノロジー データを入力します。 詳細については、「 サービスグラフ コネクタ インポート用のインポート前 OT ワークシート エントリーレビューツールを準備する 」を参照してください。
5. Excel スプレッドシートをインポートします。	オペレーショナルテクノロジー データを構成管理データベース (CMDB) にアップロードします。 詳細については、「 Excel テンプレートのインポート 」を参照してください。

タスク	目的
6. オペレーショナルテクノロジー関数のディスクバリーを実行します。	産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルにある オペレーショナルテクノロジー (OT) デバイスを検出します。 ディスクバリー for オペレーショナルテクノロジーの詳細については、「 オペレーショナルテクノロジーのディスクバリー 」を参照してください。
7. ServiceNow パートナーが提供するサービスグラフコネクタをインストールします。	ServiceNow Storeで利用可能になったServiceNow, Inc.パートナーが提供するコネクタをインストールします。
8. [オペレーショナルテクノロジー (OT)] メニューの [すべての OT デバイス] または [IP アドレス別のすべての OT デバイス] を選択します。	Excel スプレッドシートをインポートした後、または ディスカバリー for オペレーショナルテクノロジー 機能を実行した後、企業内の OT デバイスの詳細情報を編集または表示します。

の CSDM フレームワークの実装 オペレーショナルテクノロジー

CSDMフレームワークに従うことで、レポートとアナリティクスの一貫した精度という主要な目標を確実に達成し、オペレーショナルテクノロジー (OT) 環境を情動的に管理できるようになります。

CSDM OT のフレームワーク

CSDM フレームワークの実装は、段階的に完了する必要があります。詳細については、「[Implementing the CSDM framework in stages](#)」を参照してください。

オペレーショナルテクノロジー 製品ビュー

オペレーショナルテクノロジーは、ライフサイクルのさまざまな段階で OT デバイスと本番プロセスの幅広い管理に対応する製品をカバーしています。この製品ビューの目的は、主要エンティティ オペレーショナルテクノロジー コア 共通サービスデータモデル (CSDM) (CSDM) フレームワークでどのように機能するかを理解することです。

オペレーショナルテクノロジーマネージャー

企業が オペレーショナルテクノロジー ソリューションを使用できるようにするための基盤データと関係を作成します。詳細については、「[オペレーショナルテクノロジーマネージャー](#)」を参照してください。

産業用プロセスマネージャー

オペレーショナルテクノロジー ソリューションに必要な ISA-95 機器モデルデータ基盤を作成できます。詳細については、「[産業用プロセスマネージャー](#)」を参照してください。

オペレーショナルテクノロジー脆弱性対応

サイトレベルでの OT デバイスの脆弱性についての効果的な優先順位付けと修復が可能になります。詳細については、「[オペレーショナルテクノロジー脆弱性対応](#)」を参照してください。

オペレーショナルテクノロジーインシデント管理

エンジニアが OT デバイスと本番プロセスの問題を迅速に解決できるようになります。詳細については、「[オペレーショナルテクノロジーインシデント管理](#)」を参照してください。

オペレーショナルテクノロジー変更管理

組織が OT デバイスと本番プロセスに変更を実装できるようにします。詳細については、「[オペレーショナルテクノロジー変更管理](#)」を参照してください。

オペレーショナルテクノロジーのナレッジ管理

組織が、OT インシデントに関連するナレッジ記事で OT システムに関する情報を取得できるようになります。詳細については、「[オペレーショナルテクノロジーのナレッジ管理](#)」を参照してください。

オペレーショナルテクノロジー要求管理

OT サービスカタログにアクセスして OT カatalog アイテムを要求し、定義されたフローに基づいてそれらを履行できます。OT ワーカーはカタログアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型の要求が容易になります。詳細については、「[オペレーショナルテクノロジー要求管理](#)」を参照してください。

オペレーショナルテクノロジーと CSDM テーブル

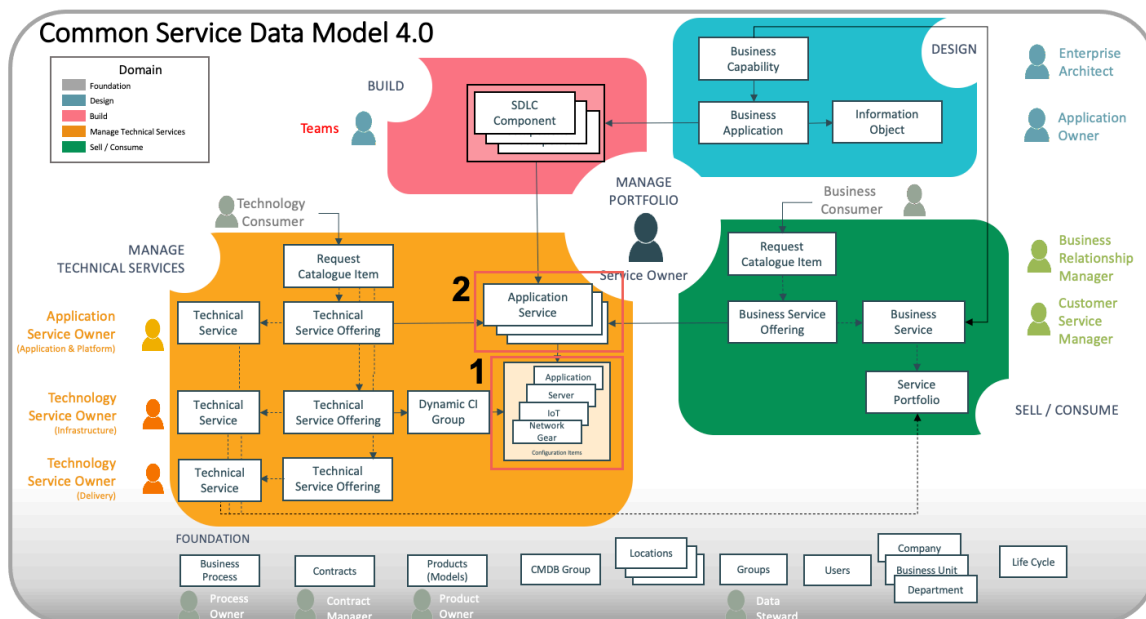
オペレーショナルテクノロジーは CSDM テーブルを管理および使用します。いくつかの ServiceNow 製品は、オペレーショナルテクノロジーのメリットを活用し、それに対して価値を付加します。

オペレーショナルテクノロジーによって管理される CSDM テーブル

オペレーショナルテクノロジー (OT) によって管理されるテーブルには、次の 2 つの主要なカテゴリがあります。

- オペレーショナルテクノロジー デバイス：OT (ICS または PCN) ネットワークで検出された構成アイテム。
- ISA 設備階層モデルエンティティ：OT デバイスによって自動化された産業プロセス。

この図の番号は、インシデント管理によって管理される CSDM テーブルに対応しています。

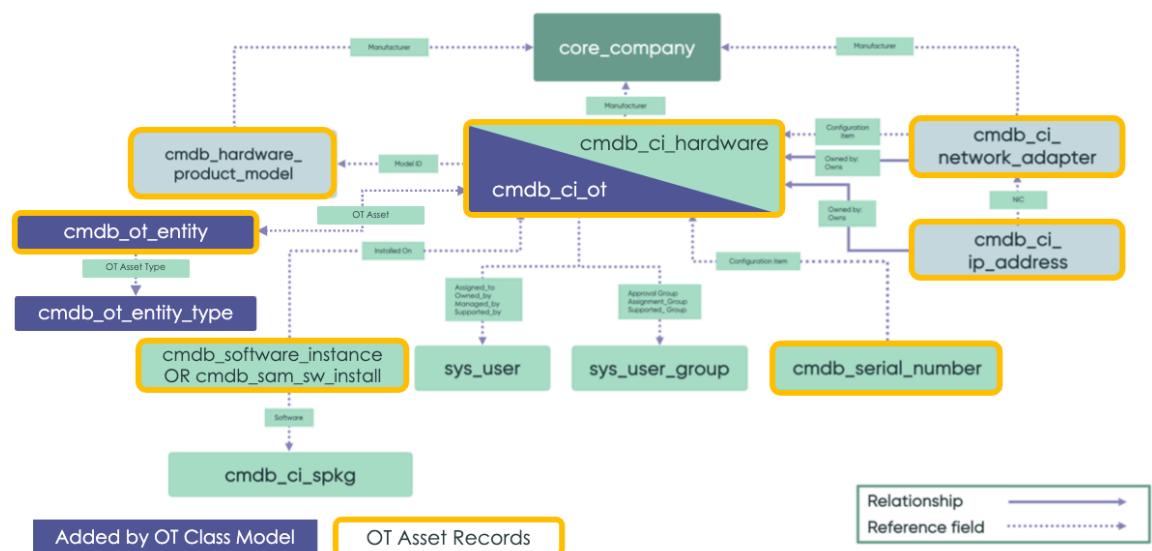


オペレーショナルテクノロジーによって使用される CSDM テーブル

1. OT デバイス：

- a. ハードウェアを拡張することによって、オペレーショナルテクノロジー ハードウェアクラス (cmdb_ci_ot) に対して構成アイテムクラスが作成されました。詳細については、「[Operational Technology \(OT\) extension classes](#)」を参照してください。
- b. OT デバイスの詳細 (cmdb_ot_entity) 参照を使用して OT デバイスの詳細を cmdb_ot_entity テーブルに追加することで、任意の CI クラス (関連する既存のハードウェアクラスおよび新しい OT クラス) を OT デバイスとして指定できます。OT デバイスの詳細には、Purdue レベルや OT デバイスタイプなどの OT 固有の特性が含まれています。
- c. OT デバイスタップでは、産業または生産プロセスを自動化する CI の機能を記述します。cmdb_ot_entity_type テーブルには、これらの機能またはロールが記述されています。

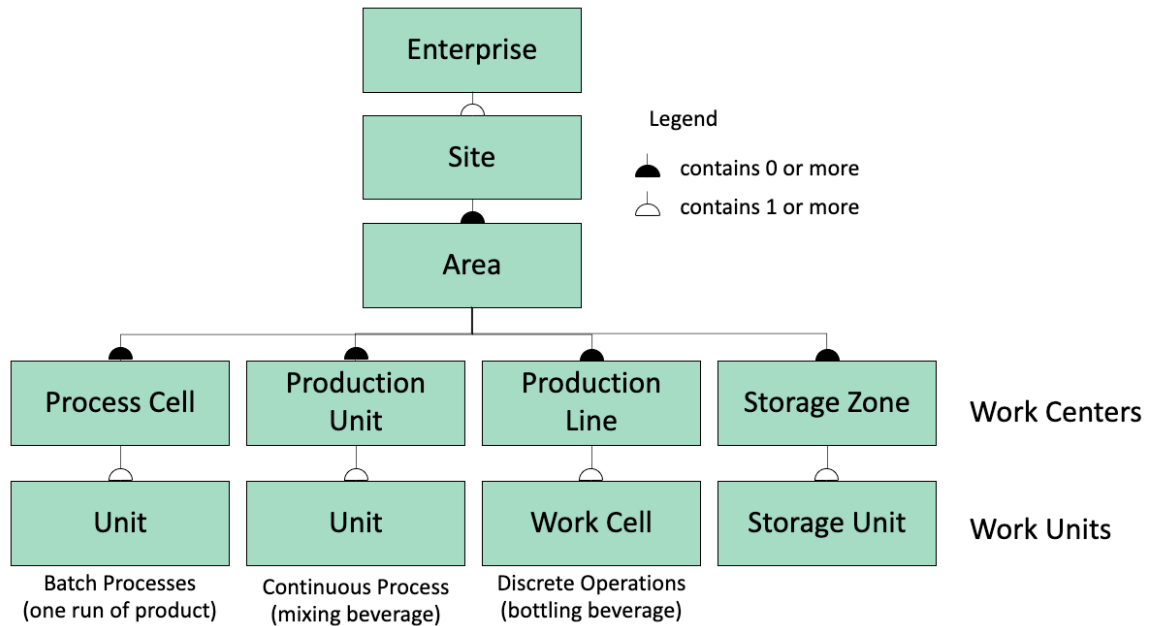
ここに示すように、単一の OT デバイスは少なくとも 2 つのレコード (1 つの CI レコードと 1 つの OT エンティティレコード) で表されます。デバイスには、最大 6 つのテーブルに 6 つ以上のレコードを含めることができます (たとえば、CI に複数の IP アドレスと MAC アドレスがある場合など)。



2. 設備モデルのエンティティ：

- a. 機器モデルエンティティクラスは、計算されたアプリケーションサービスを拡張し、次の目的で使用されます。
 - i. OT デバイスまたは機器モデルエンティティのサイトを表します。親のない機器モデルエンティティテーブル (cmdb_ci_ot_isa_entity) のレコードはサイトと見なされます。
 - ii. 生産プロセスの一部の ISA 機器モデルエンティティを表します。
- b. 機器モデルテンプレート (isa_entity_template) を使用して、産業環境にある機器モデルエンティティ間の関係をさらに記述することができます。
 - i. レベル (isa_entity_level) は、機器モデルエンティティの階層レベルを示します。デフォルトの ISA-95 テンプレートの場合、ここに表示されるレベル (エリア、作業センター、および作業単位) はベースシステムに含まれています。
 - ii. レベルタイプ (isa_entity_type) は、指定されたレベルの機器モデルエンティティによって表されるプロセスのタイプを示します。デフォルトの ISA-95 テンプレートの場合、ここに表示

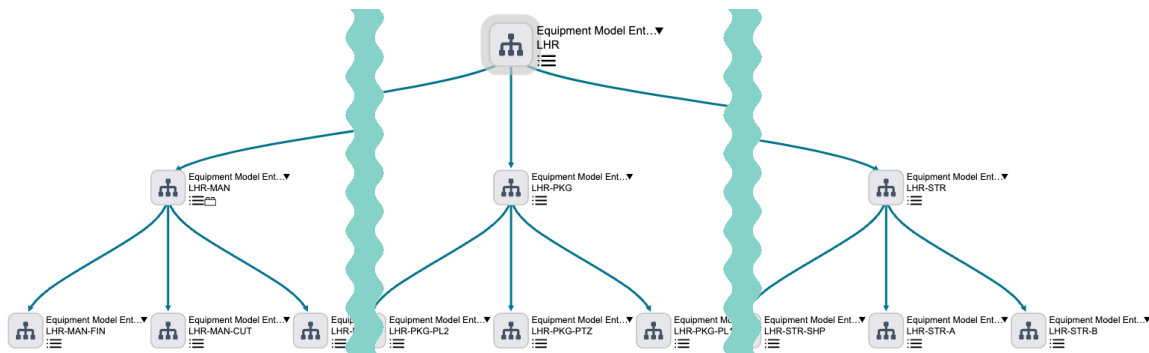
されているタイプ (プロセスセル、生産単位、生産ライン、およびストレージゾーン) はベ-
 スシステムに含まれています。

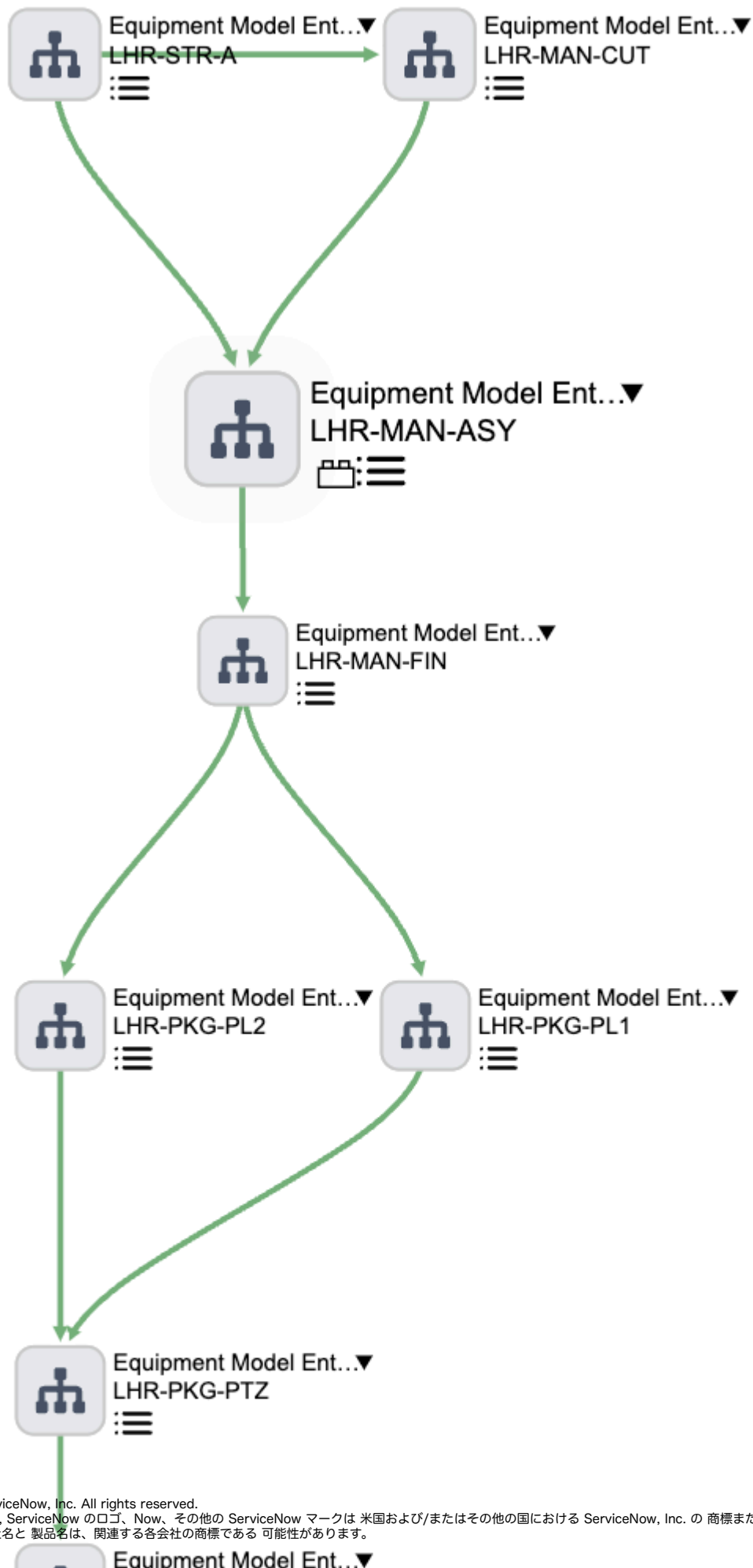


CSDM には、OT デバイスと機器モデルエンティティが互いにどのように関連しているかをより正
 確に区別する関係タイプ (オペレーショナルテクノロジー固有) が含まれています。

- **Producer for::Consumer of** : 機器モデルエンティティ間の生産プロセス (マテリアルフロー) を示します。
- **Contains Element::Element of** : 機器モデルエンティティ間の階層関係を示します。
- **Automated by::Automates** : OT デバイスと、OT デバイスが自動化する機器モデルエンティティの関係を示します。
- **Detects::Detected by** : どのネットワーク侵入検知システム (NIDS) クラス (cmdb_ci_nids) が OT ネットワーク上の OT デバイスを検出したかを示します。
- **Owns::Owned by** : OT コントロールモジュールが OT コントロールシステム (PLC、DCS など) によって所有されている場合の関係を示します。

次の依存関係マップは、OT デバイスと機器モデルエンティティの関係を示しています。





オペレーショナルテクノロジーに付加価値を提供する製品

OT を以下のいずれかの ServiceNow 製品と併用すると、OT の価値をさらに高めることができます。

オペレーショナルテクノロジーのディスカバリー

オペレーショナルテクノロジーのディスカバリーは、IT クラスのハードウェアおよびソフトウェア CI に関する詳細を提供し、OT スケジュールごとに Purdue レベルやサイトなどの追加の OT デバイスコンテキストを提供するように構成できます。OT のディスカバリーは オペレーショナルテクノロジーマネージャー 製品の一部です。

産業用プロセスマネージャー

OT デバイスが機器モデルエンティティにアサインされると、それらの間に *automated by::automates* 関係が作成されます。これは、産業用 ワークスペースで手動で行うか、[OT サブネットマッピング] メニューアイテムにある「ゾーンベースの IP ネットワークグループ間の自動マッピング (AMAZING)」機能を使用して、OT サブネットと機器モデルエンティティ間の関係を使用して行うことができます。

オペレーショナルテクノロジー脆弱性対応

サードパーティセキュリティプラットフォームとの OT 認定統合からレコードをインポートして脆弱性一致アイテム (VIT) レコードが作成されると、OT デバイスが VIT に関連付けられます。これにより、次の両方の機能が有効になります。

- マップされた機器モデルエンティティの重要度に基づくリスク計算。
- サイトベースのアサイン先グループによる修復のための適切なローカルチームへの VIT のアサイン。

オペレーショナルテクノロジーインシデント管理

OT のインシデント管理は、ほとんどの OT デバイスの IT とは別に実行されます。OT インシデントレコードにより、OT デバイスに関連する問題へのサイトベースのアクセスと表示が可能になります。

オペレーショナルテクノロジー変更管理

OT 変更要求により、OT デバイスまたは産業機器の構成を変更することができます。

オペレーショナルテクノロジーのナレッジ管理

オペレーショナルテクノロジーのナレッジ管理を使用すると、OT インシデントに関連するナレッジ記事で OT システムに関する情報をキャプチャできます。

オペレーショナルテクノロジー要求管理

OT サービスカタログにアクセスして OT カタログアイテムを要求し、定義されたフローに基づいてそれらを履行できます。OT ワーカーはカタログアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型の要求が容易になります。

オペレーショナルテクノロジーからメリットを得る製品

IT Service Management (ITSM)

サービスには、サイト、本番プロセス、OT デバイスのコンテキストと、その下に階層化された情報とテクノロジーがあります。

Information Technology Operations Management (ITOM)

管理対象の OT デバイスハードウェアおよびソフトウェアとともに、本番プロセスのビジネスコンテキストを理解します。

Security Operations

保護対象の OT デバイスハードウェアおよびソフトウェアとともに、本番プロセスのビジネスコンテキストを理解します。

ガバナンス、リスク、コンプライアンス (GRC)

監査人は、本番プロセスフローと、関連する情報オブジェクトをより適切に活用できます。これは、監査人が、監査のスコーピング、リスクの測定、および監査アクティビティの管理のための設計時のデータ機密性を理解するために役立ちます。

資産管理

ソフトウェアおよびハードウェアのライフサイクルプロセスが本番プロセスに及ぼす影響を管理します。

オペレーショナルテクノロジーマネージャーのユースケース

このセクションでは、オペレーショナルテクノロジーマネージャー のユースケースについて説明します。

オペレーショナルテクノロジーマネージャー のユースケース

オペレーショナルテクノロジーマネージャー アプリケーションは、オペレーショナルテクノロジーソリューションを使用できるようにするための基盤データと関係を作成します。Now Platform での構成管理データベース (CMDB)、サービスグラフ Connector、および ディスカバリー アプリケーションの使用をサポートしています。

産業用 ワークスペース の OT マネージャーダッシュボードの [OT デバイス] タブには、OT デバイスのインベントリの概要が表示されます。[OT デバイス] タブの詳細については、「[オペレーショナルテクノロジーマネージャー ダッシュボード](#)」を参照してください。

主要な機能

- オペレーショナルテクノロジーマネージャー は、CMDB クラス階層を拡張する OT 構成アイテム (CI) 拡張クラスを使用します。
- OT のディスカバリーは OT 固有のルールに制限され、OT 関連のメタデータを OT ディスカバリースケジュールに追加できます。
- サービスグラフ Connector (Excel) は、入力された Microsoft Excel フラットファイルスプレッドシートから OT データをインポートします。このデータは検証され、CMDB の OT デバイスの詳細を表すための適切なテーブルレコードと関係に変換されます。

結果

オペレーショナルテクノロジーマネージャー ユースケースでは、次のことができます。

- 産業環境における OT デバイスの依存関係を可視化します。
- サイト固有の RBAC を使用して、サイトごとに OT デバイスのライフサイクルを管理します。
- 確実なデータ基盤を作成し、インフラストラクチャの重要なレベルを定義します。

産業用プロセスマネージャー のユースケース

産業用プロセスマネージャー アプリケーションを使用して、オペレーショナルテクノロジーソリューションに必要な ISA-95 機器モデルデータ基盤を作成します。

主要な機能

産業用プロセスマネージャー ワークスペースでは、次の操作を実行できます。

- ISA-95 モデルを使用して、産業環境の各サイトの本番プロセスを記述します。
- 機器モデルエンティティとそれらの相互関係および OT デバイスとの関係を管理します。
- OT サブネットと機器モデルエンティティの関係を使用して、すべての OT デバイスの関係を自動化する機器モデルエンティティに自動的にマッピングします。

結果

産業用プロセスマネージャー を使用すると、各サイトの機器モデルのカスタムバージョンを作成できます。

オペレーショナルテクノロジー脆弱性対応 のユースケース

オペレーショナルテクノロジー脆弱性対応 により、サイトレベルでの OT デバイスの脆弱性についての効果的な優先順位付けと修復ができます。

主要な機能

- 修復オーナーワークスペースは、脆弱性一致アイテム (VIT) を本番プロセスにマッピングします。
- OT VIT のリスク計算は、OT デバイスによって自動化された機器モデルエンティティの重要度に基づいて行うことができます。
- VIT で OT デバイスにアサインされたサイトに基づく、修復オーナーへの VIT の自動アサイン。

結果

OT デバイスの CMDB 関係を活用することで、自動化する本番プロセスの重要度に基づいて脆弱なデバイスまたはアイテムを優先順位付けできます。

OT エンジニアまたは OT 脆弱性マネージャーは、オペレーショナルテクノロジー脆弱性対応 を使用して次のような質問の答えを見つけることができます。

- 使用している OT デバイスにどのような脆弱性があるか？ ☒
- OT 固有のリスクを使用して脆弱性の修正を優先するにはどうすればよいか？
- OT の脆弱性の修正に向けての進捗状況はどのようなものか？

産業用 ワークスペース の [OT 脆弱性] タブには、システムの脆弱性がまとめられます。[OT 脆弱性] タブの詳細については、「[オペレーショナルテクノロジーマネージャー ダッシュボード](#)」を参照してください。

オペレーショナルテクノロジーインシデント管理 のユースケース

OT インシデントは、OT ネットワーク上の OT デバイスによって提供されるサービスが中断されると発生します。インシデントが最初に作成されたときに OT デバイスが不明な場合があります。オペレーショナルテクノロジーインシデント管理 により、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

主要な機能

ユーザーが産業用 ワークスペースから OT インシデントを作成すると、OT インシデントを IT インシデントと区別するために、インシデントに OT のネットワークタイプが自動的にアサインされます。このフィールドは、デフォルトでは表示されません。

結果

オペレーショナルテクノロジーインシデント管理によって、エンジニアが OT デバイスと本番プロセスの問題を迅速に解決できるようになります。これにより、OT インシデントを IT インシデントとは別に管理できます。

オペレーショナルテクノロジー変更管理 のユースケース

オペレーショナルテクノロジー変更管理 を使用すると、チームメンバーが OT デバイスまたは産業機器の構成の変更に関与することが出来ます。

主要な機能

- すべてのステークホルダーを結び付ける、デジタル化変更ワークフロー。
- さまざまな変更管理プロセス (ワークフロー) を持つサイト。
- IT Change Management と オペレーショナルテクノロジー変更管理 は分離されていますが、必要に応じて組み合わせることが出来ます。
- オペレーショナルテクノロジーインシデント管理 および オペレーショナルテクノロジー脆弱性対応 アプリケーションと統合されたオペレーショナルテクノロジー変更管理ワークフロー。
- ダウンタイムスケジュールに合わせて調整された、設備モデルエンティティの工場フロアの変更。

結果

次の例は、組織に オペレーショナルテクノロジー変更管理 を適用する方法を示しています。

- OT デバイスの脆弱性の修正を担当する OT 修復オーナーが、一連の脆弱性を修正するための変更を開始する。
- OT 構成とプラントエンジニアリング活動を担当する OT 技術者が、故障したロボットアームを産業現場で修理するための変更を実行したいと考えています。
- 生産活動全体を担当する工場長が、エンジニアリングチームから要求された変更をレビューして承認したいと考えています。

オペレーショナルテクノロジーのナレッジ管理 のユースケース

オペレーショナルテクノロジーのナレッジ管理 は、OT インシデントに関連するナレッジ記事で オペレーショナルテクノロジー (OT) システムに関する情報をキャプチャするのに役立ちます。組織はこれらのナレッジ記事を使用して、ユーザーが適切な情報にアクセスし、ユーザーとの誤解を防ぐことができます。

主要な機能

- オペレーショナルテクノロジー管理ソリューションで既存のナレッジ管理 Now Platform 機能を使用する機能。
- OT インシデントに関連するすべてのナレッジベース記事を参照し、インシデントレコードから直接ナレッジ記事を作成する機能。
- ナレッジマネージャーとナレッジユーザー向けの OT ナレッジベースを構成する機能。
- 産業用 ワークスペースでナレッジ記事を作成する機能。
- ナレッジ記事の公開、編集、廃止、または削除の承認を要求する機能。
- 更新された情報で既存のナレッジ記事を編集する機能。

結果

次の例は、チームに オペレーショナルテクノロジーのナレッジ管理 を適用する方法を示しています。

- 数年の経験を持つ OT エンジニアが、ガイドワーカーや経験の浅い技術者のために、OT デバイスに関する知識を 1 か所に集めたいと考えています。
- 生産プロセスオペレーションを担当する最前線の作業員と技術者は、工場フロアの問題に気づき、修正方法を説明するナレッジ記事を必要としています。

オペレーショナルテクノロジー要求管理のユースケース

オペレーショナルテクノロジー要求管理を使用すると、OT サービスカタログにアクセスして OT カタログアイテムを要求し、定義されたフローに基づいてアイテムを履行できます。OT ワーカーはカタログアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型の要求が容易になります。

主要な機能

- 複数のカタログ要求を効率的に管理するための単一のビューを提供します。
- 透明性を高め、要求プロセスを迅速化し、自動通知と承認によって遅延を最小限に抑えます。
- カタログ要求の作成と更新に使用できる製品とサービスのメニューを管理します。

結果

次の例は、チームに オペレーショナルテクノロジー要求管理 を適用する方法を示しています。

- OT エンジニアは、さまざまな OT 製品やサービスの OT 要求を 1 か所で提出および管理できます。
- 工場長またはスーパーバイザーは、適切なチームと協力して、工場フロアで報告されたインシデントを修復できます。

オペレーショナルテクノロジーと CSDM の要素

CSDM の要素があるビジネスアプリケーションの管理に関連する用語。

オペレーショナルテクノロジー用語

用語	定義
機器モデル	出力または製品を生産するために生産工程がどのように編成されているかを説明するサービスレコード。
製品プロセス	機器モデルエンティティと、原材料から最終製品までのワークフローのさまざまなステージとの関係。
サイト	親を持たない親機器モデルエンティティレコード。サイトにアサインされた OT デバイスに読み取りまたは書き込みレベルのアクセスをアサインするために使用される、特別な機器モデルエンティティレコードです。
OT デバイス (サイトのアサイン)	サイトのアサインは、OT デバイスのロールベースセキュリティ (RBAC) に必要です。OT デバイスは 1 つのサイトにのみ属することができるため、これは OT デバイスレコードの OT デバイスの詳細 (cmdb_ot_entity) テーブル部分の選択リスト参照フィールドとして実装されます。
OT デバイス (automates::automated)	「automates::automated by」関係は、OT デバイスが本番プロセスにどのように関連しているかを示します。本番プロセスには、複数の機器モデルエンティティが含まれることがあります。
Windows	OT と IT のどちらのネットワークでも、Windows サーバーは cmdb_ci_win_server サーバーで表されます。

オペレーショナルテクノロジー用語 (続く)

用語	定義
	さらに、OT ネットワーク内の Windows サーバーは、[cmdb_ci_win_server.cmdb_ot_entity] フィールドに参照があり、OT での機能とその他の OT 特性 (Purdue レベル、サイトなど) を記述する cmdb_ot_entity テーブル内のレコードを指しています。

オペレーショナルテクノロジー FAQ

CSDM フレームワークの実装時にいくつかの疑問点が生じることがあります。

生産プロセスと機器モデルエンティティの違いは何ですか？

機器モデルエンティティとは、出力または製品を生産するために生産工程がどのように編成されているかを説明するために使用されるサービスレコードのことです。生産プロセスは、生の入力から完成品への材料の流れとして機器モデルエンティティ間の関係を示します。

サイトとは何ですか？

サイトとは、それ自体が親を持たない親機器モデルエンティティレコードのことです。サイトにアサインされた OT デバイスに読み取りまたは書き込みレベルのアクセスをアサインするために使用される、特別な機器モデルエンティティレコードです。

OT デバイスにサイトアサインと「*automates::automated by*」の両方の関係があるのはなぜですか？

サイトアサインは、OT デバイスのロールベースセキュリティ (RBAC) に必要です。OT デバイスは 1 つのサイトにのみ属することができるため、これは OT デバイスレコードの OT デバイスの詳細 (cmdb_ot_entity) テーブル部分の選択リスト参照フィールドとして実装されます。

automates::automated by 関係は、OT デバイスが本番プロセスにどのように関連しているかを示します。本番プロセスには、複数の機器モデルエンティティが含まれることがあります。

OT ネットワーク上と IT ネットワーク上の Windows サーバーの違いは何ですか？

どちらのタイプのネットワークでも、Windows サーバーは cmdb_ci_win_server サーバーで表されます。さらに、OT ネットワーク内の Windows サーバーの [cmdb_ci_win_server.cmdb_ot_entity] フィールドにある参照は、OT での機能と、その他の OT 特性 (Purdue レベル、サイトなど) を記述する cmdb_ot_entity テーブル内のレコードに向けたものです。

オペレーショナルテクノロジー (OT) 拡張クラスのインストール

オペレーショナルテクノロジーマネージャーの基盤である オペレーショナルテクノロジー (OT) 拡張クラスをインストールする必要があります。

これらのクラスモデルは、クラスの説明、識別ルール、識別子エントリ、および依存関係 (該当する場合) を含む 構成管理データベース (CMDB) クラス階層を拡張します。ディスカバリー コネクタや サービスグラフ コネクタなどのアプリケーションは、これらのクラス拡張を使用して CI を入力し、さまざまなテクノロジーとソフトウェアを検出します。

詳細については、[オペレーショナルテクノロジー \(OT\) 拡張クラス](#) を参照してください

オペレーショナルテクノロジーマネージャー のインストール

管理者ロールをお持ちであれば、オペレーショナルテクノロジーマネージャー アプリケーションをインストールできます。このアプリケーションには、デモデータが含まれています。まだインストールされていない場合は、関連する ServiceNow Store アプリケーションとプラグインをインストールします。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。

- ❗ **注:**
オペレーショナルテクノロジーマネージャーに必要なサブスクリプションの詳細については、「[Operational Technology Management \(OTM\) のサブスクリプション](#)」を参照してください

必要なロール：admin

このタスクについて

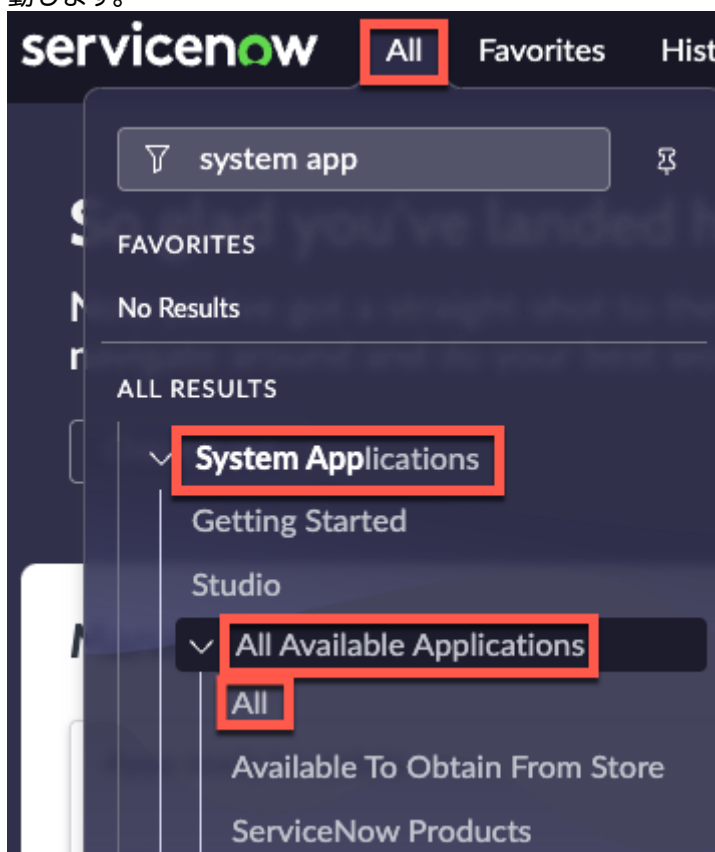
オペレーショナルテクノロジーマネージャー とともに次のアイテムがインストールされます。

- プラグイン
- ストアアプリケーション
- ロール
- テーブル
- スクリプトインクルード

オペレーショナルテクノロジーマネージャーとともにインストールされるコンポーネントの表示の詳細については、「[オペレーショナルテクノロジーマネージャーとともにインストールされるコンポーネント](#)」を参照してください。

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して オペレーショナルテクノロジーマネージャー アプリケーションを検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store への要求が必要になることがあります。

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

依存するプラグインとアプリケーションがインストールされる場合、現在インストールされている場合、またはインストールする必要がある場合は、表示されます。インストールする必要があるプラグインまたはアプリケーションがある場合は、オペレーショナルテクノロジーマネージャー をインストールする前にインストールする必要があります。

4. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。
デモデータには、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードが含まれています。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

i 重要:

インストール時にデモデータを読み込んでおかないと、後から読み込むことはできません。

5. [インストール] を選択します。

インストールされたスクリプトインクルード オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー プラグインは、次のスクリプトインクルードをインストールします。

名前	Description (説明)
ベースDAO	すべての DAO クラスが拡張する必要がある基本 DAO クラス。
NIDSUtil	cmdb_ci_nids デバイス用のユーティリティ。
OTDevicesMigrationUtils	指定されたクラスから更新されたクラステーブルにレコードを移行します。詳細については、次を参照してください。 オペレーショナルテクノロジー (OT) 拡張クラス 。
OT デバイス	[cmdb_ot_entity] テーブルおよび関連する [cmdb_ci] および [cmdb_rel_ci] テーブルに対して操作を実行するための実装クラス。
OTDeviceDAO	オペレーショナルテクノロジーデバイスでのディスクバリーの使用を支援するユーティリティ。
OTBaseDAO	オペレーショナルテクノロジー内のすべての DAO クラスが拡張する必要がある基本 DAO クラス。
OTFoundationConstants	他のスクリプトインクルードで使用される定数のコレクション。
OTUtil	オペレーショナルテクノロジーユーティリティメソッドのコレクションです。
SGOTDeviceConstants	オペレーショナルテクノロジーサービスグラフコネクタで使用される定数のコレクション。
SGOTDeviceTransformUtil	サービスグラフコネクタ オペレーショナルテクノロジー ための変換ユーティリティメソッドのコレクションです。
SGOTDataStreamBase	指定された入力で特定のデータストリームを呼び出す基本パターン。
SGOTTroubleShootHelper	サービスグラフコネクタの構成を検証するためのヘルパーメソッド。
OTAssetFilterAjax	産業用 ワークスペースのすべての OT デバイス リストビューからアプリケーションレコードと OT コントロールモジュールを除外するユーティリティクライアントスクリプト。

名前	Description (説明)
OTBulkEditHandler	フローアクションとスケジュール済みジョブによってトリガーされる IT から OT への一括編集 (変換) と OT デバイスの詳細の一括編集を処理するサーバー側スクリプト。
拡張ポイント	
SGOTDeviceImportExtensionPoint	次の 2 つのメソッドを含む SG OT デバイスインポート拡張ポイント:1. getDeviceCMDBClassNameWithSysId;2. getComputerType です。

オペレーショナルテクノロジーマネージャー ロールの割り当て

ユーザーにロールをアサインすると、オペレーショナルテクノロジーマネージャー アプリケーションの各機能やデータへのアクセスを制御できます。

始める前に

必要なロール: admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジーマネージャー アプリケーションを使用できます。

サイトユーザーを設定する場合は、機器モデルエンティティサイトユーザーのユーザー基準を作成してアサインすることができます。詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

ロール	Description (説明)
オペレーショナルテクノロジー ディスカバリー アドミニストレーター [ot_discovery_admin]	オペレーショナルテクノロジープロセスのディスカバリーを実行できますが、構成管理データベース (CMDB)にアクセスして、検出されたアイテムから作成された構成アイテム (CI) および関連オペレーショナルテクノロジー (OT) エンティティを表示することはできません。詳細については、「 オペレーショナルテクノロジー ディスカバリースケジュールを作成し、ディスカバリープロセスを実行します 」を参照してください。
オペレーショナルテクノロジーマネージャー ビュアー [cmdb_ot_viewer]	オペレーショナルテクノロジー (OT) デバイスレコードへの読み取り専用アクセス。
オペレーショナルテクノロジーマネージャー 編集者 [cmdb_ot_editor]	運用技術 (OT) 拡張クラス の  アクセス権を作成、読み取り、更新、および削除します。
オペレーショナルテクノロジーマネージャー アドミン [cmdb_ot_admin]	オペレーショナルテクノロジー (OT) デバイスレコードのアクセス権を作成、読み取り、更新、削除します。OT エンティティタイプ内の特定の構成を編集および管理することもできます。詳細については、「 運用技術 (OT) 拡張クラス  」を参照してください。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

オペレーショナルテクノロジーマネージャー 統合

オペレーショナルテクノロジーマネージャー アプリケーションには、サードパーティ統合のサポートが入っています。

現在、下記のサードパーティー統合をサポートしています。

- Claroty CTD のサービスグラフコネクタ統合
- サービスグラフMicrosoft Defender for IoT用コネクタ (Azure)
- サービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール)

Claroty CTD のサービスグラフコネクタ統合

Claroty Continuous Threat Detection (CTD) を ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションと統合して、検出されたデバイスと Claroty CTD サイト (センサーまたは Network Intrusion Detection System アプライアンス) をインポートします。

ストアでアプリを要求する

[ServiceNow Store](#) Web サイトにアクセスして、利用可能なすべてのアプリを表示し、要求をストアに送信する方法について確認してください。リリースされたすべてのアプリのこれまでのリリースノート情報については、「[ServiceNow Store のバージョン履歴リリースノート](#)」を参照してください。

サポートされているバージョン

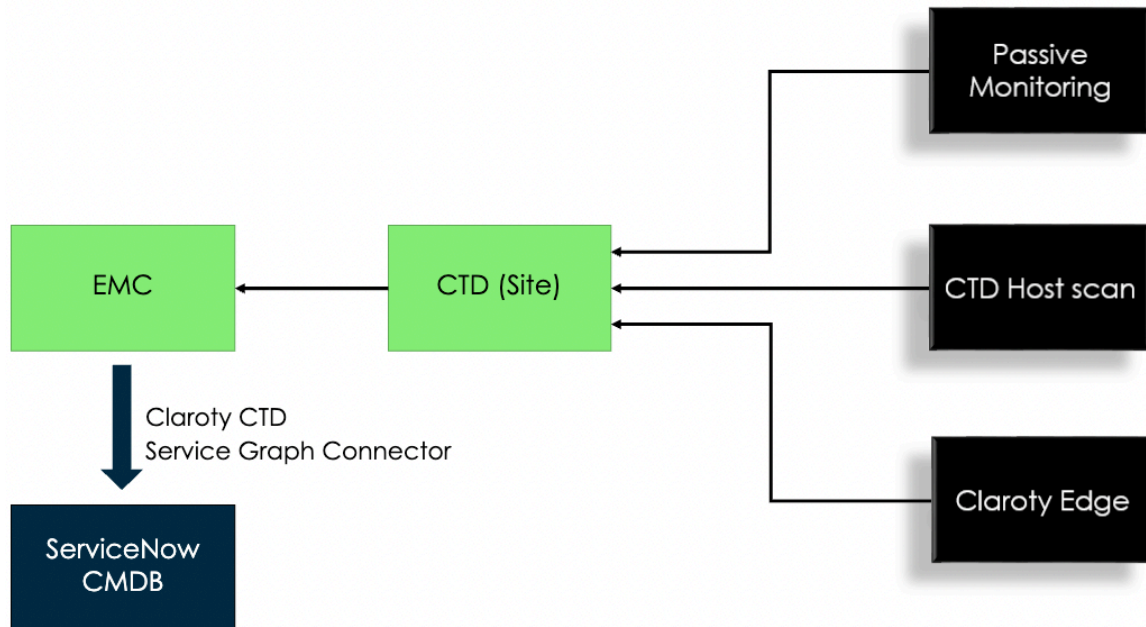
- Claroty CTD バージョン:2.0.1 以降
- サポートされている ServiceNow バージョン:
 - Utah
 - バンクーバー
 - ワシントン

ユースケース

オペレーショナルテクノロジーマネージャー アプリケーションでClaroty Continuous Threat Detection のサービスグラフコネクタ統合を使用して、次の情報を構成管理データベース (CMDB)

- サイト
- 各サイトで検出されたデバイス
- 接続 (またはベースライン)
- インストール済みプログラム

次の図は、Claroty CTD データを CMDB にインポートするための検出方法を示しています。



ガイド付きセットアップ

Claroty CTD のサービスグラフコネクタ統合 のガイド付きセットアップでは、インスタンスの統合を構成するための、整理され順序の付いたタスクが用意されています。ガイド付きセットアップにアクセスするには、「[ガイド付きセットアップの構成](#)」を参照してください。

CMDB 統合ダッシュボード

CMDB 共通統合 ストアアプリは、インストールされているすべての統合のステータス、処理結果、および処理エラーを一元的に表示するダッシュボードを提供します。すべての統合実行のメトリクスを確認することができます。特定の CMDB 統合、特定の期間、または特定の統合実行に関してビューをフィルタリングすることもできます。CMDB 統合ダッシュボードでの統合の監視の詳細については、「[Integration Commons for CMDB](#)」を参照してください。

データマッピング

Claroty CTD データソースのデータは、強力な変換エンジン (RTE) を使用してマッピングされ、ServiceNow CMDB 構成アイテム (CI) クラス定義に変換されます。データは、識別および調整エンジン (IRE) を使用して ServiceNow CMDB に挿入されます。

次の表に、Claroty CTD のサービスグラフコネクタ統合 に含まれるデータソースと、インポートされたデータがロードされる対応するステージングテーブルを示します。

Claroty CTD のデータソースとステージングテーブル

データソース	ステージングテーブル
SG-OT Claroty CTD デバイス	SG-OT Claroty CTD デバイスインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_devices_import]
SG-OT Claroty CTD ベースライン	SG-OT Claroty CTD ベースラインのインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_baselines_import]
SG-OT Claroty CTD プログラム	SG-OT Claroty CTD プログラムのインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_programs_import]

Claroty CTD のデータソースとステージングテーブル (続く)

データソース	ステージングテーブル
SG-OT Claroty CTD サイト	SG-OT Claroty CTD サイトのインポート [sn_clarotyctdsgc_sg_ot_claroty_ctd_sites_import]

ステージングテーブルからインポートされたデータは、次のターゲットテーブルに挿入されます。

- コンピューター [cmdb_ci_computer]
- ハードウェア [cmdb_ci_hardware]
- IP アドレス [cmdb_ci_ip_address]
- ネットワークアダプタ [cmdb_ci_network_adapter]
- OT デバイスの詳細 [cmdb_ot_entity]
- OT コントロールモジュール [cmdb_ci_ot_control_module]
- OT コントロールシステム [cmdb_ci_ot_control]
- シリアル番号 [cmdb_serial_number]

詳細については、「[対象となる CMDB クラス](#)」を参照してください。

のデフォルトのクエリパラメーター **Claroty CTD** のサービスグラフコネクタ統合

デフォルトでは、Claroty CTD のサービスグラフコネクタ統合にはクエリパラメーターフィルターが付属しています。これらの値は、IntegrationHub Enterprise パッケージの ServiceNow エンタイルメントに基づいて変更できます。

Claroty CTD からデータのインポートを開始すると、Claroty CTD のサービスグラフコネクタ統合は次の表にリストされているデフォルトのクエリパラメーターフィルターを使用します。

デフォルトのクエリパラメーターフィルター

クエリパラメーターフィルター	値	Description (説明)
approved_exact	true	approved_exact の値が true に設定されているため、Claroty CTD の未承認のデバイスはインポートされません。
valid_exact	true	valid_exact の値が true に設定されているため、Claroty CTD の無効なデバイスはインポートされません。
special_hint_exact	0	Claroty CTD で 0 (ユニキャスト) に設定されていない住所タイプはインポートされません。
ghost_exact	false	ゴーストとして分類されているデバイスが Claroty CTD にある場合、デフォルト値が false に設定されているため、Claroty CTD のサービスグラフコネクタ統合ではその

デフォルトのクエリパラメーターフィルター (続く)

クエリパラメーターフィルター	値	Description (説明)
		デバイスはインポートされません。

Claroty CTD のサービスグラフコネクタ統合の構成

Claroty CTD のサービスグラフコネクタ統合のガイド付きセットアップを使用して、統合ステップを進めます。

始める前に

依存関係と要件：

- 自動的にインストールされる [Integration Commons for CMDB](#) ストアアプリ。
- 自動的にインストールされる [CMDB CI Class Models](#)。
- ITOMディスカバリーライセンスプラグイン (com.snc.itom.discovery.license)。このプラグインを有効にする必要があります。
- ITOM Licensing プラグイン (com.snc.itom.license)。詳細については、「[ディスカバリーの要求](#)」を参照してください。
- 自動的にインストールされる Datastream Action プラグイン (com.glide.hub.action_type.datastream)。

必要なロール：admin

i 注:

Claroty CTD のサービスグラフコネクタ統合 の以前のバージョンを使用している場合は、古いコネクタからデータを移行しないでください。以前のバージョンをアンインストールし、新しい統合を実行する必要があります。

手順

1. アプリケーションピッカーを使用して、アプリケーションが Claroty CTD のサービスグラフコネクタ統合 に設定されていることを確認します。
詳細については、「[Application picker](#)」を参照してください。
2. 移動先 すべて > サービスグラフコネクタ **Claroty CTD** > ガイド付きセットアップ。
3. [はじめに] ページで、[開始] を選択します。
4. MID サーバーを設定するには、次の手順を実行します。
 - a. [接続と認証情報のセットアップ] セクションで、[MID サーバーを構成] タスクを選択します。
 - b. MID サーバー構成が完了したら、[完了としてマーク] を選択します。
5. 接続レコードを設定するには、次の手順を実行します。
 - a. [接続と認証情報のセットアップ] セクションで、[接続の構成] タスクを選択します。
 - b. [構成] を選択します。
 - c. 接続テーブルで Claroty CTD API レコードを開きます。
 - d. [接続 URL] フィールドに、Claroty CTD Enterprise Management Console (EMC) の URL の名前を入力します。
<https://192.168.1.100> など。

- e. MID サーバーを使用している場合は、レコードの **[MID サーバーを使用]** チェックボックスをオンにします。

注:

MID サーバーを使用していない場合は、手順 5g に進みます。

- f. [高度な MID サーバー 構成] 関連リストから、MID サーバー と MID 選択を選択します。
- g. [更新] を選択します。
- h. 手順 5a ~ 5h を繰り返して、**Claroty CTD EMC Base** 認証 レコードを更新します。

6. 認証情報レコードを設定するには、次の手順を実行します。

- a. [接続と認証情報のセットアップ] セクションで、[認証情報の構成] タスクを選択します。
- b. [構成] を選択します。
- c. 認証情報テーブルで Claroty CTD EMC Base 認証レコードを開きます。
- d. [**User name** (ユーザー名)] フィールドに、Claroty CTD EMC へのログインに使用したユーザー名を入力します。
- e. [パスワード] フィールドに、Claroty CTD EMC へのログインに使用したパスワードを入力します。
- f. [更新] を選択します。

7. 接続をテストするには、次の手順を実行します。

- a. [接続と認証情報のセットアップ] セクションで、[接続のテスト/検証] タスクを選択します。
- b. センサーのデータソースレコードの関連リンクセクションから [テスト接続] UI アクションを選択します。
接続テストが完了したら、結果を表示します。テスト結果が「成功」を返すまで、提案されたトラブルシューティング手順を実行する必要があります。
- c. 接続マネージャーに有効な証明書があることを確認してください。

本番環境には有効な証明書をインストールする必要があります。非本番インスタンスまたは概念実証 (POC) インスタンスの場合、接続マネージャーに有効な証明書がない場合に統合が機能するようにシステムプロパティを構成できます。次の表に、非本番環境で構成できるシステムプロパティを示します。

非本番環境のシステムプロパティ

プロパティ	値
com.glide.communications.httpclient.verify_certificate	false に設定します。
com.glide.communications.httpclient.verify_certificate	false に設定します。
	このシステムプロパティを追加する必要がある場合は、「 システムプロパティの追加 」を参照してください。
com.glide.communications.trustmanager.trustall	true に設定します。

- d. MID セキュリティポリシーを確認します。
イントラネットレコードで、次の表の列に指定した値が表示されていることを確認します。

イントラネットレコード値

列	値
証明書チェーンチェック	false
ホスト名チェック	false
失効チェック	false

詳細については、「[MID サーバー証明書チェックポリシー](#)」を参照してください。

8. API リソースパス、ページネーションサイズ、および API キーの有効期限を設定するシステムプロパティを設定するには、次の手順を実行します。
- a. [システムプロパティの構成] セクションで、[構成] を選択します。
- b. 次の表のシステムプロパティを設定します。

プロパティ	Description (説明)
sn_clarotyctdsgc.resourcepath.site	サイトのリソースパスを設定するプロパティ: i 注: サイトのリソースパスは、CTD サイトおよびデバイスの Claroty CTD Enterprise Management Console (EMC) V4.4.3 API バージョンに対してデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.resourcepath.device	デバイスのリソースパスを設定するプロパティ: i 注: デバイスのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョン用にデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.pagesize.device	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするデバイスレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。

プロパティ	Description (説明)
	i 注: ページあたりの最大デバイス数は 500 です。
sn_clarotyctdsgc.resourcepath.baseline	ベースラインのリソースパスを設定するプロパティ: i 注: ベースラインのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョン用にデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.pagesize.baseline	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするベースラインレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。
sn_clarotyctdsgc.get_all_baselines	ベースラインのすべてのレコードをフェッチするか、前回成功したインポートの開始時刻以降の新しいレコードのみをフェッチするプロパティ。 i 注: ベースラインを初めてインポートするときは、このプロパティの設定に関係なく、すべてのレコードがインポートされます。
sn_clarotyctdsgc.resourcepath.entity	エンティティのリソースパスを設定するプロパティ: i 注: エンティティのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョン用にデフォルトで提供されます。別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.resourcepath.program	インストール済みプログラムのリソースパスを設定するプロパティ:

プロパティ	Description (説明)
	i 注: インストール済みプログラムのリソースパスは、CTD サイトおよびデバイスの CTD EMC V4.4.3 API バージョン用にデフォルトで提供されます。 別の API バージョンを使用する場合は、パスを上書きできます。
sn_clarotyctdsgc.pagesize.entity	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするエンティティレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。
sn_clarotyctdsgc.pagesize.program	Claroty CTD EMC へのページネーション REST 呼び出しでフェッチするプログラムレコードの数を設定するプロパティ。デフォルト値は 1 ページあたり 500 レコードです。
sn_clarotyctdsgc.api_token_life_in_minutes	API がアクティブと見なされる時間 (分) を設定するプロパティ。時間が経過すると、サービスグラフコネクタは次のインポート時に新しい API キーをフェッチします。デフォルト値は 0 で、REST 呼び出しごとに新しいトークンがフェッチされます。 i 注: 値を変更すれば、同じトークンを最大 24 時間保持し、REST 呼び出しの回数を減らすことができます。
sn_clarotyctdsgc.classify_based_on_os	Claroty CTD のサービスグラフコネクタ統合の一部として OS 別の分類をサポートするクラスのリストを提供するプロパティ。 フラグが True に設定されている場合、OS による分類がサポートされます。False に設定すると、サービスグラフコネクタは OS 別に分類されなくなります。例： <pre>{ "cmdb_ci_ip_switch":true, "cmdb_ci_nids":false }</pre>
sn_clarotyctdsgc.filter.asset_type_code	区切り文字 (\$) で区切られたデバイスタイプのコードのリストを提供するプロパティ。 Claroty のタイプとコードの詳細については、「対象となる CMDB クラス」を参照してください。たとえば、PLC および HMI デバイスタイプのみをインポートするに

プロパティ	Description (説明)
	は、Claroty タイプコードを 0\$1 として入力します。
sn_clarotyctdsgc.filter.asset_purdue_level	区切り文字 (\$) で区切られた Purdue レベルのリストを提供するプロパティ。たとえば、Purdue レベル 1 と 2 のデバイスのみをフィルタリングするには、Purdue レベル 1 と 2 のデバイスのみをフィルタリングするには、値を 1.0\$2.0 に設定します。

c. [保存] を選択します。

9. CTD サイトをインポートするには、次の手順を実行します。

a. [CTD サイトを構成] セクションで、[CTD サイトをインポート] タスクを選択します。

b. [構成] を選択します。

c. [今すぐ実行] ボタンを選択します。

10. ネットワーク侵入検知システム (NIDS) を構成するには、次の手順を実行します。

a. [CTD サイトを構成] セクションで、[NIDS を構成] タスクを選択します。

b. Claroty CTD からデバイスを取得するために使用する NIDS をセットアップしたら、[完了としてマーク] を選択します。

11. サイト、デバイス、ベースライン、およびインストール済みプログラムを実行するようにインポートスケジュールを構成するには、次の手順を実行します。

a. [インポートスケジュールの構成] セクションで、[サイトインポートスケジュールの構成] タスクを選択します。

b. [構成] を選択します。

c. [予定されているデータインポート] テーブルで、[**SG-OT CTD** サイトのスケジュール済みインポート] を選択します。

- デフォルトでは、サイトのインポートスケジュールは毎日深夜に実行されるように構成されています。

- デバイスをインポートする前に、CTD サイトをインポートして検証する必要があります。

d. 必要に応じて次のアクションを完了し、必要に応じてインポートスケジュールを確認または変更します。

アクション	Description (説明)
条件スクリプトの入力	[条件付き] を選択して、スケジュール済みインポートを実行するかどうかを決定する条件付きスクリプトを入力します。
デフォルトのインポートスケジュールの変更	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。

アクション	Description (説明)
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブル内のユーザーを参照します。 i 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを正常に行うには、選択したユーザーに admin ロールがアサインされている必要があります。空のままにすると、スケジュール済みインポートはログインユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、前回成功したインポートの開始時刻以降のすべてのレコードまたは新しいレコードのみをインポートできます。詳細については、「 ガイド付きセットアップの構成 」を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートを有効にします。
スケジュール変更を保存する	[更新] を選択して、スケジュールの変更を保存します。

- e. [インポートスケジュールの構成 (Configure Import Schedules)] セクションで、[デバイスインポートスケジュールの構成 (Configure Devices Import Schedule)] タスクを選択します。

- f. [構成] を選択します。

- g. [予定されているデータインポート] テーブルで、[**SG-OT CTD** デバイスのスケジュール済みインポート] を選択して、デバイスのインポートスケジュールを確認または変更します。

- デフォルトでは、デバイスのインポートスケジュールは毎日深夜に実行されるように設定されています。
- デバイスが CTD サイトによってクエリーされます。サービスグラフコネクタは、検証済みの CTD サイトによって検出されたデバイスのみクエリーを実行します。

- h. 必要に応じて次のアクションを完了し、必要に応じてインポートスケジュールを確認または変更します。

アクション	Description (説明)
条件スクリプトの入力	[条件付き] を選択して、スケジュール済みインポートを実行するかどうかを決定する条件付きスクリプトを入力します。

アクション	Description (説明)
デフォルトのインポートスケジュールの変更	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブル内のユーザーを参照します。 i 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを正常に行うには、選択したユーザーに admin ロールがアサインされている必要があります。空のままにすると、スケジュール済みインポートはログインユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、前回成功したインポートの開始時刻以降のすべてのレコードまたは新しいレコードのみをインポートできます。詳細については、「 ガイド付きセットアップの構成 」を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートを有効にします。
スケジュール変更を保存する	[更新] を選択して、スケジュールの変更を保存します。

- i. [インポートスケジュールの構成] セクションで、[ベースラインインポートスケジュールの構成] タスクを選択します。
- j. [構成] を選択します。
- k. [予定されているデータインポート] テーブルで、[**SG-OT CTD** ベースラインのスケジュール済みインポート] を選択して、ベースラインのインポートスケジュールを確認または変更します。デフォルトでは、ベースラインインポートスケジュールは親 OT コントロールシステムの実行後に実行されるように構成されています。
- l. 必要に応じて次のアクションを完了し、必要に応じてインポートスケジュールを確認または変更します。

アクション	Description (説明)
条件スクリプトの入力	[条件付き] を選択して、スケジュール済みインポートを実行するかどうかを決定する条件付きスクリプトを入力します。

アクション	Description (説明)
デフォルトのインポートスケジュールの変更	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブル内のユーザーを参照します。 i 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを正常に行うには、選択したユーザーに admin ロールがアサインされている必要があります。空のままにすると、スケジュール済みインポートはログインユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、前回成功したインポートの開始時刻以降のすべてのレコードまたは新しいレコードのみをインポートできます。詳細については、「 ガイド付きセットアップの構成 」を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートを有効にします。
スケジュール変更を保存する	[更新] を選択して、スケジュールの変更を保存します。

- m. [インポートスケジュールの構成 (Configure Import Schedules)] セクションで、[サイトインストール済みプログラムのインポートスケジュールの構成 (Configure Sites Installed Programs Import Schedule)] タスクを選択します。
- n. [構成] を選択します。
- o. [予定されているデータインポート] テーブルで、[**SG-OT CTD** インストール済みプログラムのスケジュール済みインポート] を選択して、インストール済みプログラムのインポートのスケジュールを確認または変更します。
デフォルトでは、インストール済みプログラムのインポートスケジュールは、毎日深夜に実行されるように設定されています。
- p. 必要に応じて次のアクションを完了し、必要に応じてインポートスケジュールを確認または変更します。

アクション	Description (説明)
条件スクリプトの入力	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。

アクション	Description (説明)
デフォルトのインポートスケジュールの変更	必要に応じて [実行] フィールドを設定して、デフォルトのインポートスケジュールを変更します。
ユーザーテーブルでのユーザーの参照	[実行方法] フィールドでユーザーを選択して、[ユーザー] テーブル内のユーザーを参照します。 i 注: デフォルトでは、このフィールドは [システムアドミニストレーター] に設定されています。インポートを正常に行うには、選択したユーザーに admin ロールがアサインされている必要があります。空のままにすると、スケジュール済みインポートはログインユーザーのロールを使用します。
インポートを実行	[今すぐ実行] を選択してインポートを実行します。構成されたシステムプロパティに基づいて、前回成功したインポートの開始時刻以降のすべてのレコードまたは新しいレコードのみをインポートできます。詳細については、ステップ 7c を参照してください。
インポートを有効にする	[アクティブ] チェックボックスをオンにして、インポートを有効にします。
スケジュール変更を保存する	[更新] を選択して、スケジュールの変更を保存します。

12. オプション: CMDBに構成アイテム (CI) が作成されると、資産レコードが作成されます。資産レコードには、CI のモデルカテゴリが含まれています。オペレーショナルテクノロジー (OT) のモデル カテゴリの詳細については、「[このモデルカテゴリ オペレーショナルテクノロジー](#)」を参照してください。OT デバイスのモデルカテゴリを表示するには、次の手順を実行します。
 - a. 移動先 **すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス**。
 - b. 資産レコードを表示する OT デバイスを選択します。
 - c. [Asset (資産)] フィールドの横の [**Preview this record** ()] を選択します。
 - d. [レコードを開く (**Open Record**)] を選択します。
13. オプション: Claroty CTD のサービスグラフコネクタ統合のトラブルシューティングを行うには、次の手順を実行します。
 - a. [オプション] Claroty CTD のサービスグラフコネクタのトラブルシューティングセクションを選択します。
 - b. [検証スケジュール済みジョブの実行] タスクで、[構成] を選択します。
 - c. [今すぐ実行] をクリックします。

このジョブは、SGC の構成と Claroty CTD への接続を検証するタスクを実行します。構成の問題が見つかった場合、検証結果から問題が報告され、トラブルシューティング手順が提案されます。スケジュール済みジョブが終了するまで待ちます。

- d. スケジュール済みジョブが完了したら、[オプション] Claroty CTD のサービスグラフコネクタのトラブルシューティング セクションに戻ります。
- e. [検証結果の確認] タスクで、[構成] を選択します。
このステップにより、前回のトラブルシューティング実行の実行ログと提案が開き、表示できるようになります。
- f. 必要に応じて提案に対処します。

i 注:

スケジュール設定済みスクリプトは、Claroty CTD のサービスグラフコネクタ統合 の初期設定後の任意の時点で使用できます。検証をトリガーするには、すべて > **Claroty CTD** のサービスグラフコネクタ > トラブルシューティング > トラブルシューティングを実行。検証結果を表示するには、次の場所に移動します。すべて > **Claroty CTD** のサービスグラフコネクタ > トラブルシューティング > 結果。

Claroty CTD のサービスグラフコネクタ統合 の使用中の問題のトラブルシューティングの詳細については、以下を参照してください。 [Claroty CTD のサービスグラフコネクタ統合 \(KB1502041\) のトラブルシューティングシナリオ](#)。

NIDS センサーの検証

インポートされたネットワーク IDS (NIDS) センサーを検証して、デバイスのインポートを準備します。センサーはデバイスのインポートの対象ではないため、学習モードでない場合にのみ検証に合格できます。

始める前に

CSDM プラグインをインストールすることをお勧めします。サービスグラフコネクタは、CMDB 標準に従ってライフサイクルデータモデルに沿っています。詳細については、「[Implementing the CSDM framework in stages](#)」を参照してください。

必要なロール:cmdb_nids_admin

このタスクについて

[**Life Cycle Stage** (ライフサイクルステージ)] フィールドと [**Life Cycle Stage Status** (ライフサイクルステージステータス)] フィールドは、センサーの学習モードをキャプチャするために使用されます。「ライフサイクルステージ」フィールドが「運用」に設定され、「ライフサイクルステージステータス」が「学習モード」に設定されている場合、検証は失敗します。[Life Cycle Stage Status (ライフサイクルステージステータス)] フィールドが [**In Use** (使用中)] に設定されている場合、検証は成功します。

手順

1. 移動先 すべて > ネットワーク **IDS** アプライアンス (**NIDS**) > センサー。
2. 検証するセンサーレコードを選択します。
3. [NIDS にアサインされたメタデータ (NIDS Assigned Meta Data)] セクションで、検出されたデバイスにアサインするセンサーの値を追加します。
4. [NIDS アドミン構成] セクションで、[ライフサイクルステージステータス] フィールドの値が [学習モード] になっていないことを確認します。
それ以外の場合、検証は失敗します。

5. **[NIDS ネットワークタイプ]** フィールドが NIDS ネットワークの場所に基づいて設定されていることを確認します。

たとえば、NIDS のデータセンター展開の場合は NIDS ネットワークタイプの **IT** を、産業用/OT ネットワーク上での産業用展開の場合は NIDS ネットワークタイプの **OT** を選択できます。

[OT] を選択すると、すべてのデバイスに対して OT デバイスの詳細が作成されます。

6. 属性が正しく入力されたら、[検証] を選択します。

i 注:

メモ: センサーからデバイスに渡される属性は、sn_cmdb_ci_class.nids_map_fields システムプロパティで定義されます。次のリストは、属性のデフォルトリストです。

- assigned_to
- 場所
- 会社
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- ゾーン
- isa_entity_site (産業用プロセスマネージャー アプリケーションがインストールされている場合のみ利用可能)

サービスグラフ 接続フレームワークを使用する

サービスグラフ接続フレームワークを使用して、Claroty CTD 用に作成された関連データソース、システムプロパティ、およびスケジュール設定済みデータインポートを 1 か所に集めます。

始める前に

必要なロール: admin

このタスクについて

Claroty CTD のサービスグラフコネクタ統合のデータソース、システムプロパティ、およびスケジュール設定済みデータインポートに個別に移動できるアプリケーションモジュールがあります。ただし、新しい サービスグラフ Connection フレームワークでは、Claroty CTD 用に作成されたすべての関連データソースとスケジュール設定済みデータインポートを 1 か所に集めることができます。関連リンクセクションを使用して、ソース (Claroty CTD) への接続をテストすることもできます。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープが **Claroty CTD** のサービスグラフコネクタ統合 アプリケーションに設定されていることを確認します。
2. 移動先 **すべて > Claroty CTD のサービスグラフコネクタ > Claroty CTD SGC 接続**。
3. [サービスグラフ接続] ページで、[**SG-OT Claroty CTD** のデフォルト接続] を選択します。

4. オプション: システムプロパティにアクセスするには、[サービスグラフ接続のプロパティ] タブを選択します。
5. オプション: データソースにアクセスするには、[サービスグラフ接続のデータソース] タブを選択します。
6. オプション: 予定されているデータインポートにアクセスするには、[サービスグラフ接続の予定されているデータインポート] タブを選択します。
7. オプション: Claroty CTD プラットフォームとの接続をテストするには、[**Test Connection** (テスト接続)] 関連リンクを選択します。
接続はいつでもテストできます。接続テストが完了すると、同じページの [ステータス] と [提案] に、失敗したステップのステータスとトラブルシューティングの提案が表示されます。

CMDB での対象となるクラス **Claroty CTD** のサービスグラフコネクタ統合

セットアップタスクを完了したら、Claroty CTD からデータをプルするように統合を定期的に構成できます。データは、構成アイテム [cmdb_ci] テーブルから拡張されたテーブルに保存されます。

コンピューター [cmdb_ci_computer]

コンピューター [cmdb_ci_computer] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
オペレーティングシステム	os
OS バージョン	os_version

外部システムメタデータ [cmdb_key_value_v2]

外部システムメタデータ [cmdb_key_value_v2] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
ディスカバリーソース	discovery_source
キー	key
ソースキー	source_key
URL 値	url_value
値のタイプ	value_type

ハードウェア [cmdb_ci_hardware]

ハードウェア [cmdb_ci_hardware] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性名
変更グループ	assignment_group
Support group (サポートグループ)	support_group

属性ラベル	属性名
Company (チェックアウト日時)	会社
Vendor (ベンダー)	ベンダー
名前	name
シリアル番号	serial_number
クラス	sys_class_name
最初の検出日	first_discovered
Location (ロケーション)	場所
モデル番号	model_number
最新の検出日	last_discovered
Supported by (サポート担当者)	supported_by
Assigned to (アサイン先)	assigned_to
グループによる管理	managed_by_group
Managed by (管理担当者)	managed_by
モデル ID	model_id
承認グループ	change_control
Owned by (オーナー)	owned_by
Manufacturer (メーカー)	manufacturer

ハードウェアに対して作成された関係

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owens::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]
ハードウェア [cmdb_ci_hardware]	Owens::Owned by	IP アドレス [cmdb_ci_ip_address]
ハードウェア [cmdb_ci_hardware]	参照	OT デバイス [cmdb_ot_entity]
ハードウェア [cmdb_ci_hardware]	参照	外部システムメタデータ [cmdb_key_value_v2]
ハードウェア [cmdb_ci_hardware]	参照	ソフトウェアインストール [cmdb_sam_sw_install]

IP アドレス [cmdb_ci_ip_address]

IP アドレス [cmdb_ci_ip_address] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
構成アイテムによって所有されている	owned_by_cmdb_ci
IP アドレス	ip_address

属性ラベル	属性の名前
IP バージョン	ip_version

IP アドレス用に作成された関係

親クラス	関係性タイプ	子クラス
IP アドレス [cmdb_ci_ip_address]		ネットワーク侵入検知システム [cmdb_ci_nids]
IP アドレス [cmdb_ci_ip_address]		ハードウェア [cmdb_ci_hardware]

ネットワークアダプタ [cmdb_ci_network_adapter]

ネットワークアダプタ [cmdb_ci_network_adapter] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
MAC アドレス	mac_address
名前	name

ネットワークアダプタ用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワーク侵入検知システム [cmdb_ci_nids] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
メーカー	manufacturer
名前	name
相関 ID	correlation_id
Description (説明)	short_description
ファームウェアバージョン	firmware_version
NIDS マネージャー接続ステータス	connection_state
Life Cycle Stage Status (ライフサイクルステータス)	life_cycle_stage_status
Life Cycle Stage (ライフサイクルステージ)	life_cycle_stage
検証済み	検証済み

NIDS 用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワーク侵入検知システム [cmdb_ci_nids]	Owens::Owned by	IP アドレス [cmdb_ci_ip_address]
ネットワーク侵入検知システム [cmdb_ci_nids]	検出::Detected by	ハードウェア [cmdb_ci_hardware]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性名\
ファームウェアバージョン	firmware_version
最新の検出日	last_discovered

OT デバイス [cmdb_ot_entity]

OT デバイス [cmdb_ot_entity] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性名
Purdue レベル	purdue_level
ISA エンティティサイト	isa_entity_site
OT ディスカバリーソース ID	ot_correlation_id
デバイスの重要度	business_criticality
ゾーン	ゾーン
OT デバイスタイプ	ot_asset_type

OT コントロールモジュール [cmdb_ci_ot_control_module]

OT コントロールモジュール [cmdb_ci_ot_control_module] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性名
Location (ロケーション)	場所
Supported by (サポート担当者)	supported_by
名前	name
シリアル番号	serial_number
スロット番号	slot_number
Manufacturer (メーカー)	メーカー
ファームウェアバージョン	firmware_version

属性ラベル	属性名
承認グループ	change_control
Assigned to (アサイン先)	assigned_to
最新のディスカバリー	last_discovered
モデル ID	model_id
モデル番号	model_number
Company (チェックアウト日時)	会社
Owned by (オーナー)	owned_by
Managed by (管理担当者)	managed_by
Support group (サポートグループ)	support_group
グループによる管理	managed_by_group
変更グループ	assignment_group
Vendor (ベンダー)	ベンダー

OT コントロールモジュール用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールモジュール [cmdb_ci_ot_control_module]	参照	OT デバイス [cmdb_ot_entity]

OT コントロールシステム [cmdb_ci_ot_control]

OT コントロールシステム [cmdb_ci_ot_control] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性名
モジュールあり	has_module
最新の検出日	last_discovered

OT コントロールシステム用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールシステム [cmdb_ci_ot_control]	Owns::Owned by	OT コントロールモジュール [cmdb_ci_ot_control_module]

シリアル番号 [cmdb_serial_number]

シリアル番号 [cmdb_serial_number] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
シリアル番号	serial_number

属性ラベル	属性の名前
シリアル番号タイプ	serial_number_type
有効	valid

シリアル番号用に作成された関係

親クラス	関係性タイプ	子クラス
シリアル番号 [cmdb_serial_number]	参照	ハードウェア [cmdb_ci_hardware]

ソフトウェア [cmdb_ci_spkg]

ソフトウェア [cmdb_ci_spkg] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
キー	key
バージョン	version
メーカー	manufacturer
名前	name

ソフトウェア用に作成された関係

親クラス	関係性タイプ	子クラス
ソフトウェア [cmdb_ci_spkg]	参照	ソフトウェアインスタンス [cmdb_software_instance]

ソフトウェアインスタンス [cmdb_software_instance]

ソフトウェアインスタンス [cmdb_software_instance] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
インストール日	install_date
インストール先	installed_on
名前	name

ソフトウェアインスタンス用に作成された関係

親クラス	関係性タイプ	子クラス
ソフトウェアインスタンス [cmdb_software_instance]	参照	ハードウェア [cmdb_ci_hardware]

ソフトウェアインストール [cmdb_sam_sw_install]

ソフトウェアインストール [cmdb_sam_sw_install] テーブルの次の属性は、収集されたデータによって設定されます。

属性ラベル	属性の名前
表示名	display_name
バージョン	version
ディスカバリソース	discovery_source

ソフトウェアインストール用に作成された関係

親クラス	関係性タイプ	子クラス
ソフトウェアインスタンス [cmdb_software_instance]	参照	ハードウェア [cmdb_ci_hardware]

デフォルトのクラスマッピング

デフォルトのクラスマッピングは、Claroty CTD のサービスグラフコネクタ統合 アプリケーションに付属しています。

注:

クラスマッピングはsn_clarotyctdsgcで確認できます。SGOTClarotyCTDConstants スクリプト。

Claroty CTD タイプ	ServiceNow タイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eAAAServer	(空)	cmdb_ci_server		eAAAServer = 61
eAccessControl	(空)	cmdb_ci_iot		eAccessControl = 50
eAccessPoint	(空)	cmdb_ci_ip_switch		eAccessPoint = 60
eADServer	(空)	cmdb_ci_server		eADServer = 33
eAutonomousVehicle (オートノマスビークル)	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eAutonomousVehicle = 58
eAVServer	(空)	cmdb_ci_server		eAVServer = 32
eバーコードスキャナー	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	電子バーコードスキャナ = 48
eBluetoothデバイス	(空)	cmdb_ci_iot		eBluetoothデバイス = 41
eブロードキャスト	(空)	cmdb_ci_netgear		電子ブロードキャスト = 4
eカメラ	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eカメラ = 42

Claroty CTD タイプ	ServiceNow タイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eCleaningデバイス	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eCleaningDevice = 55
eController	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eController = 20
eDataLogger	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eDataLogger = 66
eDBServer	(空)	cmdb_ci_server		eDBServer = 35
eDomainController	(空)	cmdb_ci_server		eDomainController = 5
eElectricalDrive	産業用ドライブ	cmdb_ci_ot_industrial_drive	industrial_drive	eElectricalDrive = 68
eEndpoint	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	eEndpoint = 2
eエンジニアリングステーション	EWS	cmdb_ci_ot_ews	ews	eエンジニアリングステーション = 14
eFileServer	(空)	cmdb_ci_server		eFileServer = 10
eファイアウォール	(空)	cmdb_ci_ip_firewall		eファイアウォール = 31
eフロントエンドプロセッサ	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eフロントエンドプロセッサ = 26
eGateway	(空)	cmdb_ci_ip_switch		eGateway = 15
eGPSCロック	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	eGPSCロック = 37
eGPSDeデバイス	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	eGPSDevice = 62
eHistorian	履歴担当者	cmdb_ci_ot_historian	historian	eHistorian = 9
eHMIの	HMI	cmdb_ci_ot_hmi	hmi	eHMI = 1
eHomeアシスタント	(空)	cmdb_ci_iot		eHomeAssistant = 53
eIED	IED	cmdb_ci_ot_ied	ied	eIED = 19
eInfusionPump(電子インフュージョンポンプ)	(空)	cmdb_ci_iot		eInfusionPump = 46
eMediaServer	(空)	cmdb_ci_server		eMediaServer = 54
eMedicalDevice(電子医療デバイス)	(空)	cmdb_ci_iot		eMedicalDevice = 47

Claroty CTD タイプ	ServiceNow タイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
電子顕微鏡	(空)	cmdb_ci_iot		電子顕微鏡 = 49
eモデム	(空)	cmdb_ci_netgear		eモデム = 27
eモータースターター	産業用ドライブ	cmdb_ci_ot_industrial_drive	industrial_drive	eMotorStarter = 69
eNetworkAccessStorage	(空)	cmdb_ci_server		eNetworkAccessStorage = 30
eネットワーキング	(空)	cmdb_ci_netgear		eネットワーク = 3
eNTPServer	(空)	cmdb_ci_server		eNTPServer = 21
eOPCServer	OPC サーバー	cmdb_ci_ot_opc_server	opc_server	eOPCServer = 16
EOT	オペレーショナルテクノロジーデバイス	cmdb_ci_ot	ot_base	EOT = 17
ePLCの	PLC	cmdb_ci_ot_plc	plc	ePLC = 0
eプリンター	(空)	cmdb_ci_printer		電子プリンタ = 6
eProxyServer	(空)	cmdb_ci_netgear		eProxyServer = 28
eRemotelIO(イーリモートIO)	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eRemotelIOの = 13
eReverseProxyServer	(空)	cmdb_ci_netgear		eReverseProxyServer = 29
eロボット	産業用ロボット	cmdb_ci_ot_industrial_robot	industrial_robot	eロボット = 57
eRouter	ルーター	cmdb_ci_ip_router		eRouter = 11
eRTU	RTU	cmdb_ci_ot_rtu	RTU	eRTU = 18
eSCADAClient	SCADA クライアント	cmdb_ci_ot_scada_client	scada_client	eSCADAClient = 7
eSCADAMaster	SCADA サーバー	cmdb_ci_ot_scada_server	scada_server	eSCADAMaster = 38
eSCADAServer	SCADA サーバー	cmdb_ci_ot_scada_server	scada_server	eSCADAServer = 8
eセンサー	産業用センサー	cmdb_ci_ot_industrial_sensor	industrial_sensor	電子センサー = 67
eSmartLight(イースマートライト)	(空)	cmdb_ci_iot		eSmartLight = 51
eスマートフォン	(空)	cmdb_ci_iot		eスマートフォン = 44
eSmartWatch(イースマートウォッチ)	(空)	cmdb_ci_iot		eSmartWatch = 45

Claroty CTD タイプ	ServiceNow タイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eStorageアレイ	(空)	cmdb_ci_server		eStorageArray = 36
eStreamer	(空)	cmdb_ci_iot		eStreamer = 52
eスイッチ	(空)	cmdb_ci_ip_switch		eSwitch = 12
eSyslogサーバ	(空)	cmdb_ci_server		eSyslogServer = 25
eTerminalServer	(空)	cmdb_ci_server		eTerminalサーバ = 24
eTVSシーン	(空)	cmdb_ci_iot		eTVScreen = 40
eUPSの	(空)	cmdb_ci_ups		eUPS = 63
eUserConsole	HMI	cmdb_ci_ot_hmi	hmi	eUserConsole = 22
eUserワークステーション	HMI	cmdb_ci_ot_hmi	hmi	eUserワークステーション = 23
eVendingMachine(ベンディングマシン)	(空)	cmdb_ci_iot		eVendingMachine = 43
eVideoレコーダー	(空)	cmdb_ci_server		eVideoRecorder = 64
eVirtualizationServer	(空)	cmdb_ci_server		eVirtualizationServer = 65
eVoip電話	(空)	cmdb_ci_comm_hardware		eVoipPhone = 39
eVoipServerの	(空)	cmdb_ci_server		eVoipServer = 56
eWebサーバ	(空)	cmdb_ci_server		eWebサーバ = 34
eWirelessLanController	(空)	cmdb_ci_netgear		eWirelessLanController = 59
電子バーコードリーダー	(空)	cmdb_ci_iot		電子バーコードリーダー = 77
eBiometricScanner(電子生体認証スキャナー)	(空)	cmdb_ci_iot		eBiometricScanner = 74
eDNSSサーバー	(空)	cmdb_ci_server		eDNSSサーバー = 75
eSNMPScanner	(空)	cmdb_ci_server		eSNMPScanner = 73
eSNMPServer	(空)	cmdb_ci_server		eSNMPServer = 72
eVisionカメラ	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eVisionCamera = 76

Claroty CTD タイプ	ServiceNow タイプ	クラス	OT エンティティタイプ	Claroty のタイプとコード
eVisionController (英語)	OT コントロールシステム	cmdb_ci_ot_control	ot_control_system	eVisionController = 78
eVisionセンサー	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eVisionSensor = 79
eVOIPAccessPoint	(空)	cmdb_ci_ip_switch		eVOIPAccessPoint = 71
eVulnerabilityScanner	(空)	cmdb_ci_server		eVulnerabilityScanner = 70

サービスグラフ **Microsoft Defender for IoT** 用コネクタ (Azure)

Microsoft Defender for IoT を ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションと統合して、OT デバイスとセンサーアプライアンスのインポートを自動化します。

ストアでアプリを要求する

[ServiceNow Store](#) Web サイトにアクセスして、利用可能なすべてのアプリを表示し、要求をストアに送信する方法について確認してください。リリースされたすべてのアプリのこれまでのリリースノート情報については、「[ServiceNow Store のバージョン履歴リリースノート](#)」を参照してください。

サポートされているバージョン

- 次の Microsoft Defender for IoT センサーバージョンをサポートします。
 - 22.2.3.22
 - 22.2.5.9
- サポートされている ServiceNow のバージョン：
 - Utah
 - バンクーバー
 - ワシントン

ユースケース

ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションで サービスグラフ Connector for Microsoft Defender for IoT (Azure) を使用して、OT デバイスとセンサーアプライアンスをインポートできます。

ガイド付きセットアップ

サービスグラフ Connector for Microsoft Defender for IoT (Azure) のガイド付きセットアップでは、インスタンスで統合を構成するための一連のタスクが整理されています。ガイド付きセットアップにアクセスするには、「[ガイド付きセットアップの構成](#)」を参照してください。

CMDB 統合ダッシュボード

CMDB 共通統合 ストアアプリは、インストールされているすべての統合のステータス、処理結果、および処理エラーを一元的に表示するダッシュボードを提供します。すべての統合実行のメトリクスを確認することができます。特定の CMDB 統合、特定の期間、または特定の統合実行に関してビューをフィルタリングすることもできます。CMDB 統合ダッシュボードでの統合の監視の詳細については、「[Integration Commons for CMDB](#)」を参照してください。

データマッピング

Microsoft Defender for IoT (Azure) データソースのデータは、強力な変換エンジン (RTE) を使用してマッピングされ、ServiceNow CMDB 構成アイテム (CI) クラス定義に変換されます。データは、識別および調整エンジン (IRE) を使用して ServiceNow CMDB に挿入されます。

セットアップが完了したら、Microsoft Defender for IoT (Azure) アプリケーションから定期的にデータをプルするように統合を構成できます。

次の表に、Microsoft Defender for IoT (Azure) プロジェクトに含まれるデータソースと、インポートされたデータがロードされる対応するステージングテーブルを示します。

データソースとステージングテーブル **Microsoft Defender for IoT (Azure)**

データソース	ステージングテーブル
SG-OT Azure D4IoT デバイスインポート	SG-OT Azure D4IoT デバイスインポート [sn_msftd4iotazsgc_sg_ot_azure_d4iot_devices_import]
SG-OT Azure D4IoT センサーインポート	SG-OT Msft D4IoT センサーインポート [sn_msftd4iotazsgc_sg_ot_azure_d4iot_sensors_import]

ステージングテーブルからインポートされたデータは、次のターゲットテーブルに挿入されます。

- AIX サーバー [cmdb_ci_aix_server]
- コンピューター [cmdb_ci_computer]
- 構成アイテム (CI) [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX サーバー [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- 外部システムメタデータ [cmdb_key_value_v2]
- ゲームコンソール [cmdb_ci_game_console]
- ハンドヘルドコンピューティングデバイス [cmdb_ci_handled_computing]
- 履歴担当者 [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX サーバー [cmdb_ci_hpux_server]
- 空調設備 [cmdb_ci_hvac]
- HyperV サーバー [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- 産業用アクチュエーター [cmdb_ci_ot_industrial_actuator]
- 産業用ドライブ [cmdb_ci_ot_industrial_drive]
- 産業用ロボット [cmdb_ci_ot_industrial_robot]
- 産業用センサー [cmdb_ci_ot_industrial_sensor]
- IoT デバイス [cmdb_ci_iot]
- IP アドレス [cmdb_ci_ip_address]
- IPカメラ [cmdb_ci_ip_camera]

- IP ファイアウォール [cmdb_ci_ip_firewall]
- IP 電話 [cmdb_ci_ip_phone]
- Linux サーバー [cmdb_ci_linux_server]
- ネットギア [cmdb_ci_netgear]
- ネットワークアダプタ [cmdb_ci_network_adapter]
- ネットワーク侵入検知システム [cmdb_ci_nids]
- オペレーショナルテクノロジー (OT) [cmdb_ci_ot]
- OSX サーバー [cmdb_ci_osx_server]
- OT コントロールモジュール [cmdb_ci_ot_control_module]
- OT コントロールシステム [cmdb_ci_ot_control]
- OT デバイスの詳細 [cmdb_ot_entity]
- OT フィールドデバイス [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- プリンター [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- シリアル番号 [cmdb_serial_number]
- サーバー [cmdb_ci_server]
- サーバー [cmdb_ci_server]
- Solaris サーバー [cmdb_ci_solaris_server]
- ソース [sys_object_source]
- Unix Server [cmdb_ci_unix_server]
- 無停電電源装置 (UPS) [cmdb_ci_ups]
- 無線アクセスポイント [cmdb_ci_wap_network]

Microsoft Defender for IoT (Azure) プロジェクトからデータをプルするときにデータが保存される場所の詳細については、「[対象となる CMDB クラス](#)」を参照してください。

サービスグラフ **Connector for Microsoft Defender for IoT (Azure)** を構成する

サービスグラフ Connector for Microsoft Defender for IoT (Azure) のガイド付きセットアップを使用して、統合手順を進めます。

始める前に

依存関係と要件：

- 自動的にインストールされる [Integration Commons for CMDB](#) ストアアプリ。
- 自動的にインストールされる [CMDB CI Class Models](#)。
- ITOM ディスカバリーライセンスプラグイン (com.snc.itom.discovery.license)。このプラグインを有効にする必要があります。
- ITOM Licensing プラグイン (com.snc.itom.license)。詳細については、「[ディスカバリーの要求](#)」を参照してください。
- 自動的にインストールされる Datastream Action プラグイン (com.glide.hub.action_type.datastream)。

必要なロール：admin

i 注:

以前のバージョンの サービスグラフ Connector for Microsoft Defender for IoT (Azure) を使用している場合は、古いコネクタからデータを移行しないでください。以前のバージョンをアンインストールし、新しい統合を実行する必要があります。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープが サービスグラフ Connector for Microsoft Defender for IoT (Azure) アプリケーションに設定されていることを確認します。
詳細については、「[Application picker](#)」を参照してください。
2. 移動先 すべて > **MSFT D4IoT (Azure)** のサービスグラフ > ガイド付きセットアップ。
3. [はじめに] ページで、[開始] を選択します。
4. Azureリソースにアクセスするには、次の手順を実行します。
 - a. [Azure リソースへのアクセス] タスクを選択します。
 - b. 説明の指示を完了したら、[完了としてマーク] を選択します。
5. 接続と資格情報を設定するには、次の手順を実行します。
 - a. [接続と認証情報の構成] セクションで、[接続と認証情報のセットアップ] タスクを選択します。
 - b. [構成] を選択します。
 - c. **SG-OT Azure** 接続レコードを選択します。
 - d. [新しい接続および資格情報の作成] 関連リンクを選択します。
 - e. [接続と認証情報を作成] ウィンドウで、次のフィールドに入力します。

Field (フィールド)	説明
接続名	接続レコードの表示名
接続 URL	Azure URL
OAuth クライアント ID	クライアント ID (アプリケーション ID) またはサービスプリンシパル ID
OAuth クライアントシークレット	サービスプリンシパルに関連付けられたクライアントシークレットキー
OAuth トークン URL	認証トークンを取得するための URL。URL の <tenantid> をテナント ID 値に置き換えます。

i 注:

トークンの生成に成功すると、新しいウィンドウに成功メッセージが表示されます。トークンの生成が成功しなかった場合、新しいウィンドウに「 OAuth フローが失敗しました 」というエラーメッセージが表示されます。表示された詳細を確認し、作成したレコードを編集してもう一度お試しください。

- f. **[OAuth トークンを作成して取得]** を選択します。

6. 接続をテストするには、次の手順を実行します。

- a. [接続と認証情報のセットアップ] セクションで、[接続のテスト/検証] タスクを選択します。
- b. センサーのデータソースレコードの関連リンクセクションから [テスト接続] UI アクションを選択します。
接続テストが完了したら、結果を表示します。テスト結果が「成功」を返すまで、提案されたトラブルシューティング手順を実行する必要があります。

7. システムプロパティを設定するには、次の手順を実行します。

- a. [システムプロパティの構成] セクションで、[構成] を選択します。
- b. 次のシステムプロパティを設定します。

プロパティ	Description (説明)
sn_msft4iotazsgc.resource_path	リソースパスプロパティを設定します。 ARG REST API バージョン 2021-03-01 の既定のリソース パスは /providers/Microsoft.ResourceGraph/resources です。
sn_msft4iotazsgc.pagesize.sensor	センサーのページサイズプロパティを設定します。 - Azure ARG REST API ではページネーションがサポートされているため、API ごとにページあたりのレコード数を選択できます。 - デフォルトは 1 ページあたり 1000 レコードです。 i 注: 1000 は、ページあたりの最大レコード数でもあります。
sn_msft4iotazsgc.pagesize.device	デバイスのページサイズプロパティを設定します。 - Azure ARG REST API ではページネーションがサポートされているため、API ごとにページあたりのレコード数を選択できます。 - デフォルトは 1 ページあたり 1000 レコードです。 i 注: 1000 は、ページあたりの最大レコード数でもあります。

プロパティ	Description (説明)
sn_msftd4iotazsgc.get_all_devices	▪ デバイスの場合、すべてのレコードをフェッチするか (ボックスをオン)、デルタをフェッチするか (ボックスをオフ) を選択できます。 ▪ デルタでは、CMDB内の前回の正常なインポートの開始時刻以降に作成または更新されたすべてのレコードをフェッチします。 注: デバイス統合を初めて実行すると、すべてのレコードがこのプロパティとは無関係にインポートされます。
sn_msftd4iotazsgc.convert_sensor_names_to_lower_case	デバイスインポート用にこのプロパティを設定します。 ▪ このシステムプロパティは、デバイスのインポート時に Microsoft Azure によって提供されたセンサー名を小文字に変換するために使用されます。 ▪ Microsoft Azure はクエリのデータが小文字形式であることを想定しているため、これは必須です。
sn_msftd4iotazsgc.filter.device_sub_types	サブタイプ別にデバイスのインポート中にデバイスをフィルタリングするには、このプロパティを設定します。 ▪ デバイスをフィルタリングする Microsoft Azure サブタイプのカンマ区切りリスト。 ▪ たとえば、PLC とサーバーのみをインポートするには、Microsoft Azure の DeviceSubType 属性から値を Server, PLC として指定します。
sn_msftd4iotazsgc.filter.device_tags	デバイスのインポート中にデバイスをデバイスタグでフィルタリングするには、このプロパティを設定します。 ▪ デバイスのフィルタリングに必要なタグのカンマ区切りリスト (大文字と小文字を区別する)。 ▪ たとえば、特定のタグを持つデバイスをインポートするには、Microsoft Azure の DeviceTags 属性の値のリストを指定します。
sn_msftd4iotazsgc.filter.custom_query	このプロパティを設定して、デバイスサブタイプおよびデバイスタグフィルターとは別に、デバイスインポート用のフィルターを追加します。

プロパティ	Description (説明)
	- 他の属性に基づいてフィルタリングするクエリ。 - これにより、他の属性をフィルタリングできます。詳細については、「Azure クエリ言語」を参照してください。

c. [保存] を選択します。

8. センサーをインポートするには、次の手順を実行します。

a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。

b. [構成] を選択します。

c. [アクティブ] を選択して、スケジュール設定済みデータインポートジョブをアクティブにします。

9. NIDS を構成するには、以下のステップを実行します。

a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。

b. 説明にリンクされている NIDS 構成が完了したら、[完了としてマーク] を選択します。

10. インポートスケジュールを設定するには、次の手順を実行します。

a. [Configure Import Schedules] セクションで、[Configure] を選択します。

b. [SG-OT Microsoft D4IoT Azure センサースケジュール済みインポート] を選択し、必要に応じてセンサーインポートスケジュールを確認または変更します。

i. [アクティブ] を選択して、センサーインポートスケジュールをアクティブ化します。

ii. デフォルトでは、センサーインポートスケジュールは毎日深夜に実行されるように設定されています。[実行] および [時間] フィールドを使用してスケジュールを変更します。

iii. このスケジュールを条件付きにするには、[条件付き] チェックボックスをオンにします。

iv. [今すぐ実行] を選択して手動インポートを開始します。

c. [SG-OT Microsoft Azure D4IoT デバイススケジュール済みインポート (SG-OT Microsoft Azure D4IoT Devices Scheduled Import)] を選択し、必要に応じてデバイスのインポートスケジュールを確認または変更します。

i. [アクティブ] を選択して、センサーインポートスケジュールをアクティブ化します。

ii. デフォルトでは、センサーインポートスケジュールは毎日深夜に実行されるように設定されています。[実行] および [時間] フィールドを使用してスケジュールを変更します。

iii. このスケジュールを条件付きにするには、[条件付き] チェックボックスをオンにします。

iv. [今すぐ実行] を選択して手動インポートを開始します。

注:

センサーごとにデバイスが照会されます。サービスグラフコネクタは、検証済みのセンサーによって検出されたデバイスのみクエリを実行します。詳細については、ステップ 9 を参照してください。

11. オプション: CMDBに構成アイテム (CI) が作成されると、資産レコードが作成されます。

資産レコードには、CI のモデルカテゴリが含まれています。オペレーショナルテクノロジー (OT) のモデル カテゴリの詳細については、「[のモデルカテゴリ オペレーショナルテクノロジー](#)」を参照してください。OT デバイスのモデルカテゴリを表示するには、次の手順を実行します。

- a. 移動先 **すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス**.
 - b. 資産レコードを表示する OT デバイスを選択します。
 - c. [Asset (資産)] フィールドの横の [**Preview this record** ()] を選択します。
 - d. [レコードを開く (**Open Record**)] を選択します。
12. オプション: サービスグラフ Connector for Microsoft Defender for IoT (Azure) のトラブルシューティングを行うには、次の手順を実行します。
- a. [オプション] Microsoft Defender for IoT のサービスグラフコネクタ (Azure) のトラブルシューティングのセクションを選択します。
 - b. [検証スケジュール済みジョブの実行] タスクで、[構成] を選択します。
 - c. [今すぐ実行] をクリックします。
このジョブは、SGC の構成と Microsoft Azure への接続を検証するタスクを実行します。構成の問題が見つかった場合、検証結果から問題が報告され、トラブルシューティング手順が提案されます。スケジュール済みジョブが終了するまで待ちます。
 - d. スケジュール済みジョブが完了したら、[オプション] Microsoft Defender for IoT のサービスグラフコネクタ (Azure) のトラブルシューティングのセクションに戻ります。
 - e. [検証結果の確認] タスクで、[構成] を選択します。
このステップにより、前回のトラブルシューティング実行の実行ログと提案が開き、表示できるようになります。
 - f. 必要に応じて提案に対処します。



注:

スケジュール設定済みスクリプトは、Claroty CTD のサービスグラフコネクタ統合 の初期設定後の任意の時点で使用できます。検証をトリガーするには、**すべて > MSFT D4IoT (Azure) のサービスグラフ > トラブルシューティング > トラブルシューティング**を実行。検証結果を表示するには、次の場所に移動します。 **すべて > MSFT D4IoT (Azure) のサービスグラフ > トラブルシューティング > 結果**。

次のタスク

Microsoft Defender for IoT (Azure) を ServiceNow サービスグラフ Connector for Microsoft Defender for IoT (Azure) に接続できるようになりました。詳細については、次を参照してください。 [Microsoft Defender for IoT \(Azure\) サブスクリプションを ServiceNow Service Graph Connector for Microsoft Defender for IoT \(Azure\) に接続する \(KB1587770\)](#)。

NIDS センサーの検証

ネットワーク IDS (NIDS) センサーがインポートされたら検証して、デバイスのインポートに備えます。学習モードでないセンサーはデバイスのインポートの対象ではないため、センサーは検証に合格します。

始める前に

CSDM プラグインをインストールすることをお勧めします。サービスグラフコネクタは、CMDB 標準に従ってライフサイクルデータモデルに沿っています。詳細については、「[Implementing the CSDM framework in stages](#)」を参照してください。

必要なロール:cmdb_nids_admin

i 注:

ServiceNow の NIDS アプライアンスは、Microsoft Defender for IoT (Azure) センサーを表します。

このタスクについて

[**Life Cycle Stage** (ライフサイクルステージ)] フィールドと [**Life Cycle Stage Status** (ライフサイクルステージステータス)] フィールドは、センサーの学習モードをキャプチャするために使用されます。「ライフサイクルステージ」フィールドが「運用」に設定され、「ライフサイクルステージステータス」が「学習モード」に設定されている場合、検証は失敗します。[Life Cycle Stage Status (ライフサイクルステージステータス)] フィールドが [**In Use** (使用中)] に設定されている場合、検証は成功します。

手順

1. 移動先 **すべて > ネットワーク IDS アプライアンス (NIDS) > センサー**。
2. 検証するセンサーレコードを選択します。
3. [NIDS にアサインされたメタデータ (NIDS Assigned Meta Data)] セクションで、検出されたデバイスにアサインするセンサーの値を追加します。
4. [NIDS アドミン構成] セクションで、[ライフサイクルステージステータス] フィールドの値が [学習モード] でないことを確認します。
それ以外の場合、検証は失敗します。
5. [NIDS ネットワークタイプ] フィールドが NIDS ネットワークの場所に基づいて設定されていることを確認します。
たとえば、NIDS のデータセンター展開の場合は NIDS ネットワークタイプの **IT** を、産業用/OT ネットワーク上での産業用展開の場合は NIDS ネットワークタイプの **OT** を選択できます。

[OT] を選択すると、すべてのデバイスに対して OT デバイスの詳細が作成されます。

6. 属性が正しく入力されたら、[検証] を選択します。

注:

メモ: センサーからデバイスに渡される属性は、sn_cmdb_ci_class.nids_map_fields システムプロパティで定義されます。次のリストは、属性のデフォルトリストです。

- assigned_to
- 場所
- 会社
- owned_by
- managed_by
- supported_by
- change_control
- support_group
- managed_by_group
- assignment_group
- ゾーン
- isa_entity_site (産業用プロセスマネージャー アプリケーションがインストールされている場合のみ利用可能)

サービスグラフ 接続フレームワークを使用する

サービスグラフ接続フレームワークを使用して、関連するデータソース、システムプロパティ、およびMicrosoft Azure用に作成されたスケジュール設定済みデータインポートを 1 か所に集めます。

始める前に

必要なロール: admin

このタスクについて

サービスグラフ Connector for Microsoft Defender for IoT (Azure) のデータソース、システムプロパティ、およびスケジュール設定済みデータインポートに個別に移動できるアプリケーションモジュールがあります。ただし、新しい サービスグラフ Connection フレームワークでは、すべての関連データソースと、Microsoft Azure 用に作成されたスケジュール設定済みデータインポートを 1 か所に集めることができます。関連リンクセクションを使用して、ソース (Microsoft Azure) への接続をテストすることもできます。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープが サービスグラフ Connector for Microsoft Defender for IoT (Azure) アプリケーションに設定されていることを確認します。
2. 移動先 **すべて > MSFT D4IoT (Azure)** のサービスグラフ > **Azure SGC** の接続。
3. [サービスグラフ接続] ページで、[**SG-OT Azure SGC** のデフォルト接続 レコード] を選択します。
4. オプション: システムプロパティにアクセスするには、[サービスグラフ接続のプロパティ] タブを選択します。
5. オプション: データソースにアクセスするには、[サービスグラフ接続のデータソース] タブを選択します。

6. オプション: 予定されているデータインポートにアクセスするには、[サービスグラフ接続の予定されているデータインポート] タブを選択します。
7. オプション: Microsoft Azure プラットフォームとの接続をテストするには、[テスト接続] 関連リンクを選択します。
接続はいつでもテストできます。接続テストが完了すると、同じページの [ステータス] と [提案] に、失敗したステップのステータスとトラブルシューティングの提案が表示されます。

CMDBサービスグラフ **Connector for Microsoft Defender for IoT (Azure)** の対象となるクラス

ガイド付きセットアップを完了したら、Microsoft Defender for IoT (Azure) プロジェクトから定期的にデータをプルするように統合を構成できます。データは、構成アイテム [cmdb_ci] テーブルから拡張されたテーブルに保存されます。

コンピューター [cmdb_ci_computer]

コンピューター [cmdb_ci_computer] テーブルの次の属性は、収集されたデータによって設定されます。

コンピューター [cmdb_ci_computer] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
オペレーティングシステム	os
OS アドレス幅 (ビット)	os_address_width
OS ドメイン	os_domain
OS バージョン	os_version

外部システムメタデータ [cmdb_key_value_v2]

外部システムメタデータ [cmdb_key_value_v2] テーブルの次の属性は、収集されたデータによって設定されます。

外部システムメタデータ [cmdb_key_value_v2] 属性

属性ラベル	属性の名前
ディスカバリーソース	discovery_source
キー	key
ソースキー	source_key
文字列値	string_value
URL 値	url_value
値のタイプ	value_type

ハードウェア [cmdb_ci_hardware]

ハードウェア [cmdb_ci_hardware] テーブルの次の属性は、収集されたデータによって設定されます。

ハードウェア [cmdb_ci_hardware] 属性

属性ラベル	属性の名前
クラス	sys_class_name
モデル番号	model_number
最新の検出日	last_discovered
Location (ロケーション)	場所
モデル ID	model_id
メーカー	メーカー
最初の検出日	first_discovered
Owned by (オーナー)	owned_by
承認グループ	change_control
グループによる管理	managed_by_group
Managed by (管理担当者)	managed_by
名前	name
Company (チェックアウト日時)	会社
Support group (サポートグループ)	support_group
変更グループ	assignment_group
Assigned to (アサイン先)	assigned_to
Supported by (サポート担当者)	supported_by

ハードウェアに対して作成された関係

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]
ハードウェア [cmdb_ci_hardware]	Owns::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]
ハードウェア [cmdb_ci_hardware]	参照	外部システムメタデータ [cmdb_key_value_v2]
ハードウェア [cmdb_ci_hardware]	参照	OT デバイス [cmdb_ot_entity]

IP アドレス [cmdb_ci_ip_address]

IP アドレス [cmdb_ci_ip_address] テーブルの次の属性は、収集されたデータによって設定されます。

IP アドレス [cmdb_ci_ip_address] 属性

属性ラベル	属性の名前
IP アドレス	ip_address

IP アドレス [cmdb_ci_ip_address] 属性 (続く)

属性ラベル	属性の名前
IP バージョン	ip_version
構成アイテムが所有	owned_by_cmdb_ci

IP アドレス用に作成された関係

親クラス	関係性タイプ	子クラス
IP アドレス [cmdb_ci_ip_address]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]
IP アドレス [cmdb_ci_ip_address]	参照	ハードウェア [cmdb_ci_hardware]

ネットワークアダプタ [cmdb_ci_network_adapter]

ネットワークアダプタ [cmdb_ci_network_adapter] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワークアダプター [cmdb_ci_network_adapter] 属性

属性ラベル	属性の名前
MAC アドレス	mac_address
名前	name
ディスカバリーソース	discovery_source

ネットワークアダプタ用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワーク侵入検知システム [cmdb_ci_nids] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワーク侵入検知システム [cmdb_ci_nids] 属性

属性ラベル	属性名
最初の検出日	first_discovered
NIDS ソース名	source_name
Life Cycle Stage (ライフサイクルステージ)	life_cycle_stage

ネットワーク侵入検知システム [cmdb_ci_nids] 属性 (続く)

属性ラベル	属性名
Life Cycle Stage Status (ライフサイクルステータス)	life_cycle_stage_status
名前	name
相関 ID	correlation_id
ファームウェアバージョン	firmware_version
完全修飾ドメイン名	fqdn
NIDS アサインゾーン	ゾーン
NIDS マネージャー接続ステータス	connection_state
検証済み	検証済み
Manufacturer (メーカー)	メーカー

NIDS 用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワーク侵入検知システム [cmdb_ci_nids]	検出::Detected by	ハードウェア [cmdb_ci_hardware]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] テーブルの次の属性は、収集されたデータによって設定されます。

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered

OT コントロールモジュール [cmdb_ci_ot_control_module]

OT コントロールモジュール [cmdb_ci_ot_control_module] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールモジュール [cmdb_ci_ot_control_module] 属性

属性ラベル	属性名
Vendor (ベンダー)	ベンダー
Support group (サポートグループ)	support_group
Serial number (シリアル番号)	serial_number

OT コントロールモジュール [cmdb_ci_ot_control_module] 属性 (続く)

属性ラベル	属性名
クラス	sys_class_name
最初の検出日	first_discovered
承認グループ	change_control
Managed by (管理担当者)	managed_by
グループによる管理	managed_by_group
変更グループ	assignment_group
Company (チェックアウト日時)	会社
ラック番号	rack_number
スロット番号	slot_number
Location (ロケーション)	場所
名前	name
ファームウェアバージョン	firmware_version
最新の検出日	last_discovered
Assigned to (アサイン先)	assigned_to
Owned by (オーナー)	owned_by
Supported by (サポート担当者)	supported_by
モデル ID	model_id

OT コントロールモジュール用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールモジュール [cmdb_ci_ot_control_module]	参照	OT デバイス [cmdb_ot_entity]

OT コントロールシステム [cmdb_ci_ot_control]

OT コントロールシステム [cmdb_ci_ot_control] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールシステム [cmdb_ci_ot_control] 属性

属性ラベル	属性名
モジュールあり	has_module
最新の検出日	last_discovered

OT コントロールシステム用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールシステム [cmdb_ci_ot_control]	Owns::Owned by	OT コントロールモジュール [cmdb_ci_ot_control_module]

OT デバイス [cmdb_ot_entity]

OT デバイス [cmdb_ot_entity] テーブルの次の属性は、収集されたデータによって設定されます。

OT デバイス [cmdb_ot_entity] 属性

属性ラベル	属性名
ISA エンティティサイト	isa_entity_site
OT ディスカバリーソース ID	ot_correlation_id
デバイスの重要度	business_criticality
Purdue レベル	purdue_level
ゾーン	ゾーン
OT デバイスタイプ	ot_asset_type

PLC [cmdb_ci_ot_plc]

PLC [cmdb_ci_ot_plc] テーブルの次の属性は、収集されたデータによって設定されます。

PLC [cmdb_ci_ot_plc] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
スイッチ位置	switch_position
スイッチリモート	switch_remote_mode

シリアル番号 [cmdb_serial_number]

シリアル番号 [cmdb_serial_number] テーブルの次の属性は、収集されたデータによって設定されます。

シリアル番号 [cmdb_serial_number] 属性

属性ラベル	属性の名前
シリアル番号	serial_number
シリアル番号タイプ	serial_number_type
有効	valid

シリアル番号用に作成された関係

親クラス	関係性タイプ	子クラス
シリアル番号 [cmdb_serial_number]	参照	ハードウェア [cmdb_ci_hardware]
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

サービスグラフ **Connector for Microsoft Defender for IoT (Azure)** の属性マッピングと分類

次の表に、センサーとデバイスの属性マッピングと分類を示します。

センサー属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
ID	文字列形式: /subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	- sys_object_source - cmdb_ci_nids	sys_object_source の SNK correlation_id	センサーの一意的 ID。
name	文字列	cmdb_ci_nids	name	センサーの名前。
properties.hostname	文字列	cmdb_ci_nids	fqdn	センサーのホスト名。
properties.ip	文字列	cmdb_ci_ip_address	ip_address	センサーの IP アドレス。
properties.learningMode	ブール値	cmdb_ci_nids	False または unavailable: ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステータス (life_cycle_stage_status): 使用中 真: ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステータス (life_cycle_stage_status): Learning	IoT センサーの学習モードステータス。

センサー属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
properties.mac	文字列	cmdb_ci_network_adapter	mac_address	センサーの MAC アドレス。
properties.sensorState	文字列	cmdb_ci_nids	connection_state	IoT センサーのステータス。
properties.sensorVersion	文字列	cmdb_ci_nids	firmware_version	IoT センサーのバージョン。
properties.upSince	文字列としての日付と時刻	cmdb_ci_nids	first_discovered	起動時間。
properties.zone	文字列	cmdb_ci_nids	ゾーン	IoT センサーのゾーン。

デバイス属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
ID	文字列形式: /subscriptions/ subscription-id>/providers/ <providers-id>/location/ <location>/ deviceGroups/ <device-Group>/ devices/<name-field>	- sys_object_source - cmdb_ot_entity - cmdb_key_value_v2	sys_object_source の SNK cmdb_ot_entity discovery_source_id	デバイスの一意の ID。
resourceGroup	(空)	cmdb_key_value_v2	(空)	リソースグループ
tenantId	(空)	cmdb_key_value_v2	(空)	テナント ID
properties.authorizationState	文字列	cmdb_key_value_v2	(空)	デバイスの認可済みステータス
properties.criticality	文字列	cmdb_ot_entity	business_criticality	デバイスの重要度
properties.deviceName	文字列	cmdb_ci	name	デバイスの名前。
properties.deviceSubType	文字列	cmdb_ci	sys_class_name	デバイスサブタイプの表示名。
properties.firstSeen	文字列としての日付と時刻	- cmdb_ci - cmdb_ci_ot_control_module(コントロールモジュールが存在する場合)	first_discovered	デバイスが初めて確認された時間。

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
properties.lastSeen	文字列としての日付と時刻	- cmdb_ci - cmdb_ci_ot_control_module(コントロールモジュールが存在する場合)	most_recent_discovery	デバイスが最後に確認された時刻。
properties.purdueLevel	文字列	cmdb_ot_entity	purdue_level	デバイスのPurdue レベル。
properties.operatingSystem.distribution	文字列	cmdb_ci_computeros		OS ディストリビューション
properties.operatingSystem.version	文字列	cmdb_ci_computeros_version		OS バージョン
properties.operatingSystem.platform	文字列	cmdb_ci_computeros_domain		OS プラットフォーム
properties.operatingSystem.architecture	文字列	cmdb_ci_computeros_address_width		OS アーキテクチャ
properties.additionalFields.plcKeyState	(空)	cmdb_ci_ot_plc	switch_position	PLC キーのステータス
properties.additionalFields.plcRunState	(空)	cmdb_ci_ot_plc	switch_remote_mode	PLC の実行状態
properties.hardware	オブジェクト	(空)	(空)	デバイスのハードウェアデータ
properties.hardwareModel	文字列	cmdb_ci	(空)	ハードウェアモデル
properties.hardwareSerialNumber	文字列	cmdb_serial_number	serial_number	ハードウェアのシリアル番号
properties.hardwareVendor	文字列	cmdb_ci	メーカー	ハードウェアベンダー
properties.nics	オブジェクトのレイ	(空)	(空)	デバイスのネットワークインターフェイスカードのリスト。
properties.nics[{}]	オブジェクト	(空)	(空)	ネットワークインターフェイスカードのプロパティ
properties.nics[{}].Address	文字列	cmdb_ci_ip_address	ip_address	IPv4 アドレス
properties.nics[{}].Address	文字列	cmdb_ci_network_adapter	mac_address	MAC アドレス
properties.slots	オブジェクトのレイ	(空)	(空)	バックプレーン内のデバイススロットのリスト。
properties.slots[{}]	オブジェクト	(空)	(空)	PLCバックプレーンのスロットデータ。

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
properties.slots[{}].firmwareVersion	文字列	cmdb_ci_ot_controlmodule	firmware_version	スロットのファームウェアバージョン。
properties.slots[{}].model	文字列	cmdb_ci_ot_controlmodule	model	スロットのモデル。
properties.slots[{}].rackNumber	整数	cmdb_ci_ot_controlmodule	rack_number	バックプレーンのラック番号
properties.slots[{}].serialNumber	文字列	cmdb_ci_ot_controlmodule	serial_number	スロットのシリアル番号。
properties.slots[{}].slotNumber	整数	cmdb_ci_ot_controlmodule	slot_number	ラック内のスロット番号。
properties.slots[{}].hardwareVendor	文字列	cmdb_ci_ot_controlmodule	hardware_vendor	スロットのハードウェアベンダー。

デバイスタイプの分類

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
アラームサイレン	(空)	(空)
警報システム	(空)	(空)
ATM	(空)	(空)
バックアップサーバー	(空)	(空)
バーコードスキャナー	(空)	(空)
DB サーバー	(空)	(空)
DCS コントローラ	産業	(空)

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
ドメイ ンコント ローラ	(空)	(空)
ドアコン トロール パネル	(空)	(空)
DVRの	(空)	(空)
エレベーター	(空)	(空)
エンジ ニアリン グステー ション	産業	(空)
火災警報	(空)	(空)
火災検知 器	(空)	(空)
ファイア ウォール	(空)	(空)
ゲームコ ンソール	(空)	(空)
履歴担当 者	(空)	(空)
HMI	産業	(空)
湿度セン サー	(空)	(空)
HVAC	(空)	(空)
I/O アダ プタ	(空)	(空)
IED	(空)	(空)
産業用包 装システ ム	(空)	(空)

自動翻訳

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
産業用ロ ボット	(空)	(空)
産業用は かり	(空)	(空)
インター ホン	(空)	(空)
IP カメ ラ	(空)	(空)
IP電話	(空)	(空)
範囲	(空)	(空)
Meter (測定)	(空)	(空)
モーショ ンディテ クター	(空)	(空)
マルチ キャスト/ブ ロード キャスト	(空)	(空)
NTP サーバ	(空)	(空)
ピープル カウン ターシス テム	(空)	(空)
物理的な 場所	(空)	(空)
PLC	産業	(空)
空圧装置	(空)	(空)

自動翻訳

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
プリン ター	(空)	(空)
プロト コルコン バーター	(空)	(空)
パンチク ロック	(空)	(空)
ロボッ トコント ローラ	(空)	(空)
ルーター	(空)	(空)
RTU	(空)	(空)
サーバー	サーバー	(空)
サーボド ライブ	(空)	(空)
スロット	(空)	(空)
スマート ライト	(空)	(空)
スマート フォン	(空)	(空)
スマート スイッチ	(空)	(空)

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
スマート テレビ	(空)	(空)
ストレージ	(空)	(空)
スイッチ	ネット ワークデ バイス	(空)
タブレッ ト	(空)	(空)
終着駅	(空)	(空)
サーモス タット	(空)	(空)
回転式改 札口	(空)	(空)
無停電電 源装置	(空)	(空)
可変周波 数ドライ ブ	(空)	(空)
VPN ゲート ウェイ	(空)	(空)
Wifiパイ ナップル	(空)	(空)
無線アク セスポイ ント	(空)	(空)
WLAN アクセス ポイント	ネット ワークデ バイス	(空)
ワークス テーショ ン	ワークス テーショ ン	(空)
不明	すべて	(空)

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
未分類	未分類ま たはすべ て	(空)
その他の タイプ	(空)	(空)
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• Windows サーバー • Windows Server バージョン 2004[8] • Windows Server、バージョン1909[9] • Windows Server、バージョン1903[9] • Windows サーバー 2019 • Windows サーバー 2016 • Windows Server 2012 R2 • Windows サーバー 2012 • Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003 R2 • Windows Server 2003 • Windows 2000 サーバー • Windows NT 4.0 サーバー • Windows NT 3.51 サーバー

デバイスタイプの分類 (続く)

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
		• Windows NT 3.5 サーバー • Windows NT 3.1 サーバー
上記のタイプ値 (指定 Network と IoT を除く)	(空)	• リナックス • arch • centos • Debian • 中折れ帽子 • SUSEの • Red Hat • RHEL • Ubuntuの • オラクル
上記のタイプ値 (指定 Network と IoT を除く)	(空)	AIX
上記のタイプ値 (指定 Network と IoT を除く)	(空)	ESX

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• HP/UX • HPUX
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• Hyper-V • hyperv • 超
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• Solaris • SunOS • SunOS
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• macOS X サーバー • macOS サーバー • OS X の • OSX

自動翻訳

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• UNIX • ヌー
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• 勝つ • windows • Microsoft • ウィンドウズ 1.0、1.02、1.03、1.04、2.03、2.10、2.11、3.0、3.1、3.2、7、8、8.1、10、98、95 • Windows 2000 の場合 • ワークグループ 3.11 の Windows • Windows Me • Windows NT 3.1、3.5、3.51、4.0 • Windows Vista の場合 • Windows XP の • Windows XP Professional x64 エディション
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	server

自動翻訳

サービスグラフ **Connector for Microsoft Defender for IoT** (オンプレミス管理コンソール)

Microsoft Defender for IoT (オンプレミス管理コンソール) を ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションと統合して、センサーアプライアンス、OT デバイス、ネットワーク接続のインポートを自動化します。

ストアでアプリを要求する

[ServiceNow Store](#) Web サイトにアクセスして、利用可能なすべてのアプリを表示し、要求をストアに送信する方法について確認してください。リリースされたすべてのアプリのこれまでのリリースノート情報については、「[ServiceNow Store のバージョン履歴リリースノート](#)」を参照してください。

サポートされているバージョン

- Microsoft Defender for IoT (オンプレミス管理コンソール) バージョン: 10.5.2 以降
- サポートされている ServiceNow のバージョン：
 - Utah
 - バンクーバー
 - ワシントン

ユースケース

ServiceNow オペレーショナルテクノロジーマネージャー アプリケーションで サービスグラフ **Connector for Microsoft Defender for IoT** (オンプレミス管理コンソール) を使用して、センサーアプライアンス、OT デバイス、ネットワーク接続をインポートできます。

ガイド付きセットアップ

サービスグラフ **Connector for Microsoft Defender for IoT** (オンプレミス管理コンソール) のガイド付きセットアップでは、インスタンスで統合を構成するための一連のタスクが整理されています。ガイド付きセットアップにアクセスするには、「[ガイド付きセットアップの構成](#)」を参照してください。

CMDB 統合ダッシュボード

CMDB 共通統合 ストアアプリは、インストールされているすべての統合のステータス、処理結果、および処理エラーを一元的に表示するダッシュボードを提供します。すべての統合実行のメトリクスを確認することができます。特定の CMDB 統合、特定の期間、または特定の統合実行に関してビューをフィルタリングすることもできます。CMDB 統合ダッシュボードでの統合の監視の詳細については、「[Integration Commons for CMDB](#)」を参照してください。

データマッピング

Microsoft Defender for IoT (オンプレミス管理コンソール) データ ソースからのデータは、強力な変換エンジン (RTE) を使用してマッピングされ、ServiceNow CMDB 構成アイテム (CI) クラス定義に変換されます。データは、識別および調整エンジン (IRE) を使用して ServiceNow CMDB に挿入されます。

セットアップが完了したら、Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションから定期的にデータをプルするように統合を構成できます。

次の表に、Microsoft Defender for IoT (オンプレミス管理コンソール) プロジェクトに含まれるデータソースと、インポートされたデータが読み込まれる対応するステージングテーブルを示します。

Microsoft Defender for IoT のデータソースとステージングテーブル (オンプレミス管理コンソール)

データソース	ステージングテーブル
SG-OT Microsoft D4IoT 接続インポート	SG-OT Msft D4IoT 接続インポート [sn_msftd4iotsgc_sg_ot_msft_d4iot_connections_import]
SG-OT Microsoft D4IoT デバイスインポート	SG-OT Msft D4IoT デバイスインポート [sn_msftd4iotsgc_sg_ot_msft_d4iot_devices_import]
SG-OT Microsoft D4IoT センサーインポート	SG-OT Msft D4IoT センサーインポート [sn_msftd4iotsgc_sg_ot_msft_d4iot_sensors_import]

ステージングテーブルからインポートされたデータは、次のターゲットテーブルに挿入されます。

- AIX サーバー [cmdb_ci_aix_server]
- コンピューター [cmdb_ci_computer]
- 構成アイテム (CI) [cmdb_ci]
- DCS [cmdb_ci_ot_dcs]
- ESX サーバー [cmdb_ci_esx_server]
- EWS [cmdb_ci_ot_ews]
- 外部システムメタデータ [cmdb_key_value_v2]
- ゲームコンソール [cmdb_ci_game_console]
- ハンドヘルドコンピューティングデバイス [cmdb_ci_handled_computing]
- 履歴担当者 [cmdb_ci_ot_historian]
- HMI [cmdb_ci_ot_hmi]
- HP-UX サーバー [cmdb_ci_hpux_server]
- 空調設備 [cmdb_ci_hvac]
- HyperV サーバー [cmdb_ci_hyper_v_server]
- IED [cmdb_ci_ot_ied]
- 産業用アクチュエーター [cmdb_ci_ot_industrial_actuator]
- 産業用ドライブ [cmdb_ci_ot_industrial_drive]
- 産業用ロボット [cmdb_ci_ot_industrial_robot]
- 産業用センサー [cmdb_ci_ot_industrial_sensor]
- IoT デバイス [cmdb_ci_iot]
- IP アドレス [cmdb_ci_ip_address]
- IPカメラ [cmdb_ci_ip_camera]
- IP ファイアウォール [cmdb_ci_ip_firewall]
- IP 電話 [cmdb_ci_ip_phone]
- Linux サーバー [cmdb_ci_linux_server]

- ネットギア [cmdb_ci_netgear]
- ネットワークアダプタ [cmdb_ci_network_adapter]
- ネットワーク侵入検知システム [cmdb_ci_nids]
- オペレーショナルテクノロジー (OT) [cmdb_ci_ot]
- OSX サーバー [cmdb_ci_osx_server]
- OT コントロールモジュール [cmdb_ci_ot_control_module]
- OT コントロールシステム [cmdb_ci_ot_control]
- OT デバイスの詳細 [cmdb_ot_entity]
- OT フィールドデバイス [cmdb_ci_ot_field_device]
- PLC [cmdb_ci_ot_plc]
- プリンター [cmdb_ci_printer]
- RTU [cmdb_ci_ot_rtu]
- シリアル番号 [cmdb_serial_number]
- サーバー [cmdb_ci_server]
- サーバー [cmdb_ci_server]
- Solaris サーバー [cmdb_ci_solaris_server]
- ソース [sys_object_source]
- Unix Server [cmdb_ci_unix_server]
- 無停電電源装置 (UPS) [cmdb_ci_ups]
- 無線アクセスポイント [cmdb_ci_wap_network]

Microsoft Defender for IoT (オンプレミス管理コンソール) プロジェクトからデータをプルするときのデータの保存場所の詳細については、「[対象となる CMDB クラス](#)」を参照してください。

サービスグラフ **Connector for Microsoft Defender for IoT** の構成 (オンプレミス管理コンソール)

サービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール) のガイド付きセットアップを使用して、統合手順を進めます。

始める前に

依存関係と要件：

- 自動的にインストールされる [Integration Commons for CMDB](#) ストアアプリ。
- 自動的にインストールされる [CMDB CI Class Models](#)。
- ITOMディスカバリーライセンスプラグイン (com.snc.itom.discovery.license)。このプラグインを有効にする必要があります。
- ITOM Licensing プラグイン (com.snc.itom.license)。詳細については、「[ディスカバリーの要求](#)」を参照してください。
- 自動的にインストールされる Datastream Action プラグイン (com.glide.hub.action_type.datastream)。

必要なロール：admin

i 注:

以前のバージョンの サービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール) がある場合は、古いコネクタからデータを移行しないでください。以前のバージョンをアンインストールし、新しい統合を実行する必要があります。

手順

1. アプリケーションピッカーを使用して、アプリケーションスコープが サービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションに設定されていることを確認します。
詳細については、「[Application picker](#)」を参照してください。
2. 移動先 **すべて** > サービスグラフコネクタ **Microsoft D4IoT** > ガイド付きセットアップ。
3. [はじめに] ページで、[開始] を選択します。
4. MID サーバーを設定するには、次の手順を実行します。
 - a. [接続と認証情報のセットアップ] セクションで、[MID サーバーを構成] タスクを選択します。
 - b. 説明にリンクされているMID サーバー構成が完了したら、[完了としてマーク] を選択します。
5. 接続および資格情報エイリアスレコードを更新するには、次の手順を実行します。
 - a. [接続と認証情報のセットアップ] セクションで、[接続と認証情報] タスクを選択します。
 - b. [構成] を選択します。
 - c. デフォルトのレコード **Microsoft D4IoT Base API** を開きます。
 - d. [接続] 関連リストから [新規] を選択して、新しい HTTP(s) 接続レコードを作成します。
 - e. [接続 URL] フィールドに、Microsoft Defender for IoT の Central Manager の URL の名前を入力します。
たとえば、 `https://192.168.1.100` などです。
 - f. オプション: MID サーバーを使用している場合は、次のすべてを選択します。
 - [MID サーバーを使用] ボックス
 - [MID サーバー詳細構成] 関連リストの **MID サーバー**
 - リストからの **MID** 選択
 - g. [認証情報] フィールドで、検索アイコンを選択して認証情報レコードリストを開きます。
 - h. [新規] を選択して、新しいレコードを作成します。
 - i. **API** キー認証情報タイプを選択します。
 - j. [**API** キー] フィールドに、Microsoft Defender for IoT 管理コンソールから提供された名前と API キーを入力します。
 - k. [送信] を選択して認証情報レコードを作成します。

Microsoft Defender for IoT管理コンソールでAPIキーを作成するには、Microsoft製品ドキュメントの <https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis> を参照してください。

1. [接続] フォームで、[送信] を選択して接続レコードの作成を終了します。

6. 接続をテストするには、次の手順を実行します。

- a. [接続と認証情報のセットアップ] セクションで、[接続のテスト/検証] タスクを選択します。
- b. センサーのデータソースレコードの関連リンクセクションから [テスト接続] UI アクションを選択します。
接続テストが完了したら、結果を表示します。テスト結果が「成功」を返すまで、提案されたトラブルシューティング手順を実行する必要があります。
- c. 接続マネージャーに有効な証明書があることを確認してください。

本番環境には有効な証明書をインストールする必要があります。非本番インスタンスまたは概念実証 (POC) インスタンスの場合、接続マネージャーに有効な証明書がない場合に統合が機能するようにシステムプロパティを構成できます。次の表に、非本番環境で構成できるシステムプロパティを示します。

非本番環境のシステムプロパティ

プロパティ	値
com.glide.communications.httpclient.verify_certificate	false に設定します。
com.glide.communications.httpclient.verify_certificate	false に設定します。 このシステムプロパティを追加する必要がある場合は、「 システムプロパティの追加 」を参照してください。
com.glide.communications.trustmanager_trustAll	true に設定します。

- d. MID セキュリティポリシーを確認します。
イントラネットレコードで、次の表の列に指定した値が表示されていることを確認します。

イントラネットレコード値

列	値
証明書チェーンチェック	false
ホスト名チェック	false
失効チェック	false

詳細については、「[MID サーバー証明書チェックポリシー](#)」を参照してください。

進行状況ウィンドウに完了コード [成功] が表示され、処理されたレコードの数が 接続マネージャー 内のセンサーの数と同じ数として表示される場合、接続は正しく設定されていることを示しています。

7. システムプロパティを設定するには、次の手順を実行します。

a. [システムプロパティの構成] セクションで、[構成] を選択します。

b. 次のシステムプロパティを設定します。

プロパティ	Description (説明)
sn_msftd4iotsgc.resourcepath.sensor	センサーリソースパスを設定します。 - センサーリソースパスは、V3 API バージョン用にデフォルトで提供されます。 - 別の API バージョンを使用する場合は、パスを上書きできます。
sn_msftd4iotsgc.resourcepath.device	- デバイスのリソースパスは、V3 API バージョンに対してデフォルトで提供されます。 - 別の API バージョンを使用する場合は、パスを上書きできます。
sn_msftd4iotsgc.resourcepath.connection	- 接続リソースパスは、V3 API バージョン用にデフォルトで提供されます。 - 別の API バージョンを使用する場合は、パスを上書きできます。
sn_msftd4iotsgc.pagesize.device	各デバイスおよび接続 API の 1 ページに表示するレコードの数を入力します。デフォルト値:ページあたり 50 レコード
sn_msftd4iotsgc.pagesize.connection	- 接続および認証情報レコードの設定時に構成された Microsoft D4IoT Base API とは異なる接続エイリアスを使用する場合は、このプロパティフィールドにカスタム接続エイリアスレコードのsys_idを入力できます。 - このプロパティのデフォルト値は空です。このプロパティフィールドを空白のままにすると、Microsoft D4IoT ベース API 接続エイリアスがデフォルトで使用されます。
sn_msftd4iotsgc.get_all_devices	デバイスのすべてのレコードをフェッチするか、前回成功したインポートの開始時刻以降の新しいレコードのみをフェッチするかを選択します。 i 注: 初めてデバイスをインポートすると、このプロパティの設定に関係なく、すべてのレコードがインポートされます。
sn_msftd4iotsgc.get_all_connections	接続のすべてのレコードをフェッチするか、CMDBで最後に成功したインポートの開始時刻以降の新しいレコードのみをフェッチするかを選択します。

プロパティ	Description (説明)
	i 注: 初めて接続をインポートするときは、このプロパティの設定に関係なく、すべてのレコードがインポートされます。
sn_msftd4iotsgc.ot.vr.integration.id	サービスグラフ for Microsoft Defender for IoT 統合で オペレーショナルテクノロジー脆弱性対応 アプリケーションを使用している場合は、OT VR インポートレコードの Sys ID を指定します。 i 注: オペレーショナルテクノロジー脆弱性対応 プラグインがインストールされていて、このプロパティフィールドが空白のままになっている場合、レコードで [アクティブ] が [true] に設定されていれば、Microsoft D4IoT デバイス CVE 統合 (デルタインポート) が実行されます。

c. [保存] を選択します。

8. センサーをインポートするには、次の手順を実行します。

a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。

b. [構成] を選択します。

c. [アクティブ] を選択して、スケジュール設定済みデータインポートジョブをアクティブにします。

9. NIDS を構成するには、以下のステップを実行します。

a. [センサーの構成 (NIDS)] セクションで、[センサーのインポート] タスクを選択します。

b. 説明にリンクされている NIDS 構成が完了したら、[完了としてマーク] を選択します。

10. インポートスケジュールを設定するには、次の手順を実行します。

a. [Configure Import Schedules] セクションで、[**Configure**] を選択します。

b. [**SG-OT Microsoft D4IoT** センサーのスケジュール済みインポート] を選択し、必要に応じてセンサーのインポートスケジュールを確認または変更します。

- デフォルトでは、センサーインポートスケジュールは毎日深夜に実行されるように設定されています。
- デバイスまたは接続をインポートする前に、センサーをインポートしてください。

c. [アクティブ] を選択して、センサーインポートスケジュールをアクティブ化します。

d. [**SG-OT Microsoft D4IoT** デバイスインポートスケジュール済み (**SG-OT Microsoft D4IoT Devices Scheduled Import**)] を選択し、必要に応じてデバイスインポートスケジュールを確認または変更します。

- デフォルトでは、デバイスのインポートスケジュールは毎日深夜に実行されるように設定されています。
- デバイスがセンサーによって照会されます。サービスグラフコネクタは、検証済みのセンサーによって検出されたデバイスを照会します。ネットワーク侵入検知システム (NIDS) アプリケーションの構成については、「[NIDS の検証](#)」を参照してください。

e. [アクティブ] を選択して、デバイスのインポートスケジュールをアクティブ化します。

f. [**SG-OT Microsoft D4IoT 接続インポートスケジュール済みインポート (SG-OT Microsoft D4IoT Connections Scheduled Import)**] を選択して、必要に応じて接続インポートスケジュールを確認または変更します。

- デフォルトでは、接続インポートのスケジュールは、デバイスのインポートが実行された後 (親の実行後) に実行されるように構成されています。
- 接続は、両方のデバイス (Microsoft API のソースと宛先、または CMDB の親と子) が既に CMDB にある場合にのみインポートされます。
- 接続をインポートする前にデバイスをインポートします。

CMDBサービスグラフ Connector for Microsoft Defender for IoT (オンプレミス管理コンソール) の対象となるクラス

ガイド付きセットアップを完了すると、Microsoft Defender for IoT (オンプレミス管理コンソール) プロジェクトから定期的にデータをプルするように統合を構成できます。データは、構成アイテム [cmdb_ci] テーブルから拡張されたテーブルに保存されます。

コンピューター [cmdb_ci_computer]

コンピューター [cmdb_ci_computer] テーブルの次の属性は、収集されたデータによって設定されます。

コンピューター [cmdb_ci_computer] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
オペレーティングシステム	os
OS アドレス幅 (ビット)	os_address_width
OS ドメイン	os_domain
OS バージョン	os_version

外部システムメタデータ [cmdb_key_value_v2]

外部システムメタデータ [cmdb_key_value_v2] テーブルの次の属性は、収集されたデータによって設定されます。

外部システムメタデータ [cmdb_key_value_v2] 属性

属性ラベル	属性の名前
ディスカバリーソース	discovery_source
キー	key

外部システムメタデータ [cmdb_key_value_v2] 属性 (続く)

属性ラベル	属性の名前
ソースキー	source_key
文字列値	string_value
URL 値	url_value
値のタイプ	value_type

ハードウェア [cmdb_ci_hardware]

ハードウェア [cmdb_ci_hardware] テーブルの次の属性は、収集されたデータによって設定されます。

ハードウェア [cmdb_ci_hardware] 属性

属性ラベル	属性の名前
クラス	sys_class_name
モデル番号	model_number
最新の検出日	last_discovered
Location (ロケーション)	場所
モデル ID	model_id
メーカー	メーカー
最初の検出日	first_discovered
Owned by (オーナー)	owned_by
承認グループ	change_control
グループによる管理	managed_by_group
Managed by (管理担当者)	managed_by
名前	name
Company (チェックアウト日時)	会社
Support group (サポートグループ)	support_group
変更グループ	assignment_group
Assigned to (アサイン先)	assigned_to
Supported by (サポート担当者)	supported_by

ハードウェアに対して作成された関係

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]
ハードウェア [cmdb_ci_hardware]	Owns::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]

ハードウェアに対して作成された関係 (続く)

親クラス	関係性タイプ	子クラス
ハードウェア [cmdb_ci_hardware]	参照	外部システムメタデータ [cmdb_key_value_v2]
ハードウェア [cmdb_ci_hardware]	参照	OT デバイス [cmdb_ot_entity]

IP アドレス [cmdb_ci_ip_address]

IP アドレス [cmdb_ci_ip_address] テーブルの次の属性は、収集されたデータによって設定されます。

IP アドレス [cmdb_ci_ip_address] 属性

属性ラベル	属性の名前
IP アドレス	ip_address
IP バージョン	ip_version
構成アイテムが所有	owned_by_cmdb_ci

IP アドレス用に作成された関係

親クラス	関係性タイプ	子クラス
IP アドレス [cmdb_ci_ip_address]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]
IP アドレス [cmdb_ci_ip_address]	参照	ハードウェア [cmdb_ci_hardware]

ネットワークアダプタ [cmdb_ci_network_adapter]

ネットワークアダプタ [cmdb_ci_network_adapter] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワークアダプター [cmdb_ci_network_adapter] 属性

属性ラベル	属性の名前
MAC アドレス	mac_address
名前	name
ディスカバリーソース	discovery_source

ネットワークアダプタ用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ネットワーク侵入検知システム [cmdb_ci_nids]
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

ネットワーク侵入検知システム [cmdb_ci_nids]

ネットワーク侵入検知システム [cmdb_ci_nids] テーブルの次の属性は、収集されたデータによって設定されます。

ネットワーク侵入検知システム [cmdb_ci_nids] 属性

属性ラベル	属性名
最初の検出日	first_discovered
NIDS ソース名	source_name
Life Cycle Stage (ライフサイクルステージ)	life_cycle_stage
Life Cycle Stage Status (ライフサイクルステータス)	life_cycle_stage_status
名前	name
相関 ID	correlation_id
ファームウェアバージョン	firmware_version
完全修飾ドメイン名	fqdn
NIDS アサインゾーン	ゾーン
NIDS マネージャー接続ステータス	connection_state
検証済み	検証済み
Manufacturer (メーカー)	メーカー

NIDS 用に作成された関係

親クラス	関係性タイプ	子クラス
ネットワーク侵入検知システム [cmdb_ci_nids]	検出::Detected by	ハードウェア [cmdb_ci_hardware]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	IP アドレス [cmdb_ci_ip_address]
ネットワーク侵入検知システム [cmdb_ci_nids]	Owns::Owned by	ネットワークアダプタ [cmdb_ci_network_adapter]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot]

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] テーブルの次の属性は、収集されたデータによって設定されます。

オペレーショナルテクノロジー (OT) [cmdb_ci_ot] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered

OT コントロールモジュール [cmdb_ci_ot_control_module]

OT コントロールモジュール [cmdb_ci_ot_control_module] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールモジュール [cmdb_ci_ot_control_module] 属性

属性ラベル	属性名
Vendor (ベンダー)	ベンダー
Support group (サポートグループ)	support_group
Serial number (シリアル番号)	serial_number
クラス	sys_class_name
最初の検出日	first_discovered
承認グループ	change_control
Managed by (管理担当者)	managed_by
グループによる管理	managed_by_group
変更グループ	assignment_group
Company (チェックアウト日時)	会社
ラック番号	rack_number
スロット番号	slot_number
Location (ロケーション)	場所
名前	name
ファームウェアバージョン	firmware_version
最新の検出日	last_discovered
Assigned to (アサイン先)	assigned_to
Owned by (オーナー)	owned_by
Supported by (サポート担当者)	supported_by
モデル ID	model_id

OT コントロールモジュール用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールモジュール [cmdb_ci_ot_control_module]	参照	OT デバイス [cmdb_ot_entity]

OT コントロールシステム [cmdb_ci_ot_control]

OT コントロールシステム [cmdb_ci_ot_control] テーブルの次の属性は、収集されたデータによって設定されます。

OT コントロールシステム [cmdb_ci_ot_control] 属性

属性ラベル	属性名
モジュールあり	has_module
最新の検出日	last_discovered

OT コントロールシステム用に作成された関係

親クラス	関係性タイプ	子クラス
OT コントロールシステム [cmdb_ci_ot_control]	Owns::Owned by	OT コントロールモジュール [cmdb_ci_ot_control_module]

OT デバイス [cmdb_ot_entity]

OT デバイス [cmdb_ot_entity] テーブルの次の属性は、収集されたデータによって設定されます。

OT デバイス [cmdb_ot_entity] 属性

属性ラベル	属性名
ISA エンティティサイト	isa_entity_site
OT ディスカバリーソース ID	ot_correlation_id
デバイスの重要度	business_criticality
Purdue レベル	purdue_level
ゾーン	ゾーン
OT デバイスタイプ	ot_asset_type

PLC [cmdb_ci_ot_plc]

PLC [cmdb_ci_ot_plc] テーブルの次の属性は、収集されたデータによって設定されます。

PLC [cmdb_ci_ot_plc] 属性

属性ラベル	属性の名前
最新のディスカバリー	last_discovered
スイッチ位置	switch_position
スイッチリモート	switch_remote_mode

シリアル番号 [cmdb_serial_number]

シリアル番号 [cmdb_serial_number] テーブルの次の属性は、収集されたデータによって設定されます。

シリアル番号 [cmdb_serial_number] 属性

属性ラベル	属性の名前
シリアル番号	serial_number
シリアル番号タイプ	serial_number_type
有効	valid

シリアル番号用に作成された関係

親クラス	関係性タイプ	子クラス
シリアル番号 [cmdb_serial_number]	参照	ハードウェア [cmdb_ci_hardware]
ネットワークアダプタ [cmdb_ci_network_adapter]	参照	ハードウェア [cmdb_ci_hardware]

サービスグラフ **Connector for Microsoft Defender for IoT** の属性マッピングと分類 (オンプレミス管理コンソール)

次の表に、センサーとデバイスの属性マッピングと分類を示します。

センサー属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
ID	文字列形式: /subscriptions/<subscription-id>/provider/<provider>/locations/<location>/sites/<site>/sensor/<sensor-name>	- sys_object_source - cmdb_ci_nids	sys_object_source の SNK correlation_id	センサーの一意の ID。
name	文字列	cmdb_ci_nids	name	センサーの名前。
properties.hostname	文字列	cmdb_ci_nids	fqdn	センサーのホスト名。
properties.ip	文字列	cmdb_ci_ip_address	ip_address	センサーの IP アドレス。
properties.learningMode	ブール値	cmdb_ci_nids	False または unavailable: ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステータス (life_cycle_stage_status): 使用中 真: ライフサイクルステージ (life_cycle_stage): 運用 ライフサイクルステー	IoT センサーの学習モードステータス。

センサー属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
			ジステータス (life_cycle_stage_status):Learning	
properties.mac	文字列	cmdb_ci_network_adapter	mac_address	センサーの MAC アドレス。
properties.sensorStatus	文字列	cmdb_ci_nids	connection_state	IoT センサーのステータス。
properties.sensorVersion	文字列	cmdb_ci_nids	firmware_version	IoT センサーのバージョン。
properties.upSince	文字列としての日付と時刻	cmdb_ci_nids	first_discovered	起動時間。
properties.zone	文字列	cmdb_ci_nids	ゾーン	IoT センサーのゾーン。

デバイス属性マッピング

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
ID	文字列形式: /subscriptions/ subscription-id>/providers/ <providers-id>/location/ <location>/ deviceGroups/ <device-Group>/ devices/<name-field>	- sys_object_source - cmdb_ot_entity - cmdb_key_value_v2	sys_object_source の SNK cmdb_ot_entity discovery_source_id	デバイスの一意の ID。
resourceGroup	(空)	cmdb_key_value_v2	(空)	リソースグループ
tenantId	(空)	cmdb_key_value_v2	(空)	テナント ID
properties.authorizedState	文字列	cmdb_key_value_v2	(空)	デバイスの認可済みステータス
properties.criticality	文字列	cmdb_ot_entity	business_criticality	デバイスの重要度
properties.deviceName	文字列	cmdb_ci	name	デバイスの名前。
properties.deviceSubtype	文字列	cmdb_ci	sys_class_name	デバイスサブタイプの表示名。
properties.firstSeen	文字列としての日付と時刻	- cmdb_ci - cmdb_ci_ot_control_module(コントロールモジュールが存在する場合)	first_discovered	デバイスが初めて確認された時間。

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
properties.lastSeen	文字列としての日付と時刻	- cmdb_ci - cmdb_ci_ot_control_module(コントロールモジュールが存在する場合)	most_recent_discovery	デバイスが最後に確認された時刻。
properties.purdueLevel	文字列	cmdb_ot_entity	purdue_level	デバイスのPurdue レベル。
properties.operatingSystem.distribution	文字列	cmdb_ci_computeros		OS ディストリビューション
properties.operatingSystem.version	文字列	cmdb_ci_computeros_version		OS バージョン
properties.operatingSystem.platform	文字列	cmdb_ci_computeros_domain		OS プラットフォーム
properties.operatingSystem.architecture	文字列	cmdb_ci_computeros_address_width		OS アーキテクチャ
properties.additionalFields.plcKeyState	(空)	cmdb_ci_ot_plc	switch_position	PLC キーのステータス
properties.additionalFields.plcRunState	(空)	cmdb_ci_ot_plc	switch_remote_mode	PLC の実行状態
properties.hardwareObject	オブジェクト	(空)	(空)	デバイスのハードウェアデータ
properties.hardwareModel	文字列	cmdb_ci	(空)	ハードウェアモデル
properties.hardwareSerialNumber	文字列	cmdb_serial_number	serial_number	ハードウェアのシリアル番号
properties.hardwareVendor	文字列	cmdb_ci	メーカー	ハードウェアベンダー
properties.nics	オブジェクトのレイ	(空)	(空)	デバイスのネットワークインターフェイスカードのリスト。
properties.nics[{}]	オブジェクト	(空)	(空)	ネットワークインターフェイスカードのプロパティ
properties.nics[{}].Address	文字列	cmdb_ci_ip_address	ip_address	IPv4 アドレス
properties.nics[{}].Address	文字列	cmdb_ci_network_adapter	adapter_mac	MAC アドレス
properties.slots	オブジェクトのレイ	(空)	(空)	バックプレーン内のデバイススロットのリスト。
properties.slots[{}]	オブジェクト	(空)	(空)	PLCバックプレーンのスロットデータ。

デバイス属性マッピング (続く)

ペイロードフィールド名	データタイプ	テーブルへのマッピング	フィールドにマップ	Description (説明)
properties.slots[{}].firmwareVersion	文字列	cmdb_ci_ot_controlmodule	firmware_version	スロットのファームウェアバージョン。
properties.slots[{}].model	文字列	cmdb_ci_ot_controlmodule	model	スロットのモデル。
properties.slots[{}].rackNumber	整数	cmdb_ci_ot_controlmodule	rack_number	バックプレーンのラック番号
properties.slots[{}].serialNumber	文字列	cmdb_ci_ot_controlmodule	serial_number	スロットのシリアル番号。
properties.slots[{}].slotNumber	整数	cmdb_ci_ot_controlmodule	slot_number	ラック内のスロット番号。
properties.slots[{}].hardwareVendor	文字列	cmdb_ci_ot_controlmodule	hardware_vendor	スロットのハードウェアベンダー。

デバイスタイプの分類

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
アラームサイレン	(空)	(空)
警報システム	(空)	(空)
ATM	(空)	(空)
バックアップサーバー	(空)	(空)
バーコードスキャナー	(空)	(空)
DB サーバー	(空)	(空)
DCS コントローラ	産業	(空)

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
ドメイ ンコント ローラ	(空)	(空)
ドアコン トロール パネル	(空)	(空)
DVRの	(空)	(空)
エレベーター	(空)	(空)
エンジ ニアリン グステー ション	産業	(空)
火災警報	(空)	(空)
火災検知 器	(空)	(空)
ファイア ウォール	(空)	(空)
ゲームコ ンソール	(空)	(空)
履歴担当 者	(空)	(空)
HMI	産業	(空)
湿度セン サー	(空)	(空)
HVAC	(空)	(空)
I/O アダ プタ	(空)	(空)
IED	(空)	(空)
産業用包 装システ ム	(空)	(空)

自動翻訳

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
産業用ロ ボット	(空)	(空)
産業用は かり	(空)	(空)
インター ホン	(空)	(空)
IP カメ ラ	(空)	(空)
IP電話	(空)	(空)
範囲	(空)	(空)
Meter (測定)	(空)	(空)
モーショ ンディテ クター	(空)	(空)
マルチ キャスト/ブ ロード キャスト	(空)	(空)
NTP サーバ	(空)	(空)
ピープル カウン ターシス テム	(空)	(空)
物理的な 場所	(空)	(空)
PLC	産業	(空)
空圧装置	(空)	(空)

自動翻訳

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
プリン ター	(空)	(空)
プロト コルコン バーター	(空)	(空)
パンチク ロック	(空)	(空)
ロボッ トコント ローラ	(空)	(空)
ルーター	(空)	(空)
RTU	(空)	(空)
サーバー	サーバー	(空)
サーボド ライブ	(空)	(空)
スロット	(空)	(空)
スマート ライト	(空)	(空)
スマート フォン	(空)	(空)
スマート スイッチ	(空)	(空)

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
スマート テレビ	(空)	(空)
ストレージ	(空)	(空)
スイッチ	ネット ワークデ バイス	(空)
タブレッ ト	(空)	(空)
終着駅	(空)	(空)
サーモス タット	(空)	(空)
回転式改 札口	(空)	(空)
無停電電 源装置	(空)	(空)
可変周波 数ドライ ブ	(空)	(空)
VPN ゲート ウェイ	(空)	(空)
Wifiパイ ナップル	(空)	(空)
無線アク セスポイ ント	(空)	(空)
WLAN アクセス ポイント	ネット ワークデ バイス	(空)
ワークス テーショ ン	ワークス テーショ ン	(空)
不明	すべて	(空)

デバイスタイプの分類 (続く)

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタ イプ名	オペレーティングシステム/ファームウェア
未分類	未分類またはすべて	(空)
その他のタイプ	(空)	(空)
上記のタイプ 値 (指定 Network と IoT を除く)	(空)	• Windows サーバー • Windows Server バージョン 2004[8] • Windows Server、バージョン1909[9] • Windows Server、バージョン1903[9] • Windows サーバー 2019 • Windows サーバー 2016 • Windows Server 2012 R2 • Windows サーバー 2012 • Windows Server 2008 R2 • Windows Server 2008 • Windows Server 2003 R2 • Windows Server 2003 • Windows 2000 サーバー • Windows NT 4.0 サーバー • Windows NT 3.51 サーバー

自動翻訳

デバイスタイプの分類 (続く)

Microsoft Azure デバイスサブタイプ名	Microsoft Azure デバイスタイプ名	オペレーティングシステム/ファームウェア
		• Windows NT 3.5 サーバー • Windows NT 3.1 サーバー
上記のタイプ値 (指定 Network と IoT を除く)	(空)	• リナックス • arch • centos • Debian • 中折れ帽子 • SUSEの • Red Hat • RHEL • Ubuntuの • オラクル
上記のタイプ値 (指定 Network と IoT を除く)	(空)	AIX
上記のタイプ値 (指定 Network と IoT を除く)	(空)	ESX

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• HP/UX • HPUX
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• Hyper-V • hyperv • 超
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• Solaris • SunOS • SunOS
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• macOS X サーバー • macOS サーバー • OS X の • OSX

デバイスタイプの分類 (続く)

Microsoft Azure デ バイスサ ブタイプ 名	Microsoft Azure デ バイスタ イプ名	オペレーティングシステム/ファームウェア
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• UNIX • ヌー
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	• 勝つ • windows • Microsoft • ウィンドウズ 1.0、1.02、1.03、1.04、2.03、2.10、2.11、3.0、3.1、3.2、7、8、8.1、10、98、95 • Windows 2000 の場合 • ワークグループ 3.11 の Windows • Windows Me • Windows NT 3.1、3.5、3.51、4.0 • Windows Vista の場合 • Windows XP の • Windows XP Professional x64 エディション
上記の タイプ 値 (指定 Network と IoT を 除く)	(空)	server

自動翻訳

オペレーショナルテクノロジーマネージャーを使用する

オペレーショナルテクノロジー (OT) 拡張クラスのインストールやユーザーロールのアサインなど、必要なすべてのセットアップタスクを完了したら、次のタスクを実行して、ServiceNow オペレーショナルテクノロジーソリューションの基盤データと関係を作成します。

タスク	目的
1. Microsoft Excel スプレッドシートに既存のオペレーショナルテクノロジー データを入力します。	Microsoft Excel スプレッドシートの正しい列に既存のデータを配置して、データのアップロードを確実に成功させます。
2. Excel スプレッドシートをインポートします。	既存の オペレーショナルテクノロジー データを構成管理データベース (CMDB) にアップロードします。
3. オペレーショナルテクノロジー関数のディスカバリーを実行します。	産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルにある オペレーショナルテクノロジー (OT) デバイスを検出します。
4. オペレーショナルテクノロジー (OT) メニューの選択を使用します。	企業内の OT デバイスの詳細情報の編集または表示を有効にします。

サービスグラフオペレーショナルテクノロジー 用コネクタ (Excel)

サービスグラフ コネクタ (Excel) 関数を使用すると、入力された Microsoft Excel フラットファイルスプレッドシートから既存のオペレーショナルテクノロジーデータをインポートできます。統合ハブ抽出変換ロード (ETL) で使用して、このデータを構成管理データベース (CMDB) にアップロードします。

インポートプロセスを実行する前に、Microsoft Excel スプレッドシートに既存の オペレーショナルテクノロジー データを入力する必要があります。統合ハブ ETL を使用して Microsoft Excel スプレッドシートをインポートすると、構成管理データベース (CMDB) に正しい構成アイテム (CI) レコードが作成されます。詳細については、「[運用技術 \(OT\) 拡張クラス](#)」を参照してください。

関連情報

[統合ハブ](#)

[統合ハブ ETL](#)

Microsoft Excel のサービスグラフコネクタの構成

入力された Microsoft Excel フラットファイルスプレッドシートから既存のオペレーショナルテクノロジーデータをインポートするように、Microsoft Excel のサービスグラフコネクタを構成します。

Microsoft Excel のサービスグラフコネクタのガイド付きセットアップを使用し、タスクを順番に完了して、Microsoft Excel のサービスグラフコネクタを構成します。

移動先 [すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ](#) をクリックし、次のガイド付きセットアップを開き、タスクを完了します。

ガイド付きセットアップの使用の詳細については、「[ガイド付きセットアップ](#)」を参照してください。

タスク	目的
ユーザー	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
Staging table configuration (ステージングテーブルを構成)	CI の一意の名前を識別する際の構成要素を決定するために構成します。 システムのプロパティの詳細については、「SG-OT デバイスの Excel インポート処理に影響を与えるシステムプロパティ」を参照してください。
データを準備	既存のデータを適切な列に配置して、スプレッドシートを作成して準備します。 データの準備の詳細については、「サービスグラフ コネクタインポート用のインポート前 OT ワークシートエントリーレビューツールを準備する」を参照してください。
新しい OT デバイスを作成	ステージングテーブルのリストビューから [新規] ボタンをクリックして、新しい OT デバイスを手動で作成します。新しい OT デバイスの作成の詳細については、「
Validate records (レコードを検証)	インポートされたデータに対して検証を実行し、レコードの検証ステージを更新して検証コメントを入力します。 i 注: 検証を実行するためにリストのレコードを選択する必要はありません。検証は、ステージングテーブルに存在するすべてのレコードで実行されます。 レコードの検証の詳細については、「検証の管理」を参照してください。
Schedule Import (インポートのスケジュール)	ステージングテーブルからインポートセットテーブルにデータをインポートし、OT のリストビューとワークスペースで確認します。

インポート前の **OT** ワークシートエントリーレビューロールをアサイン

ユーザーまたはユーザーグループにロールをアサインして、Excel サービスグラフコネクタステージングテーブルと ETL を管理できるようにします。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジーマネージャー アプリケーションを使用できます。

ロール	Description (説明)
アドミニストレーター [cmdb_inst_admin]	- ETL を表示または編集できます。 - ステージングテーブルのレコードを表示できます。
アドミニストレーター [cmdb_OT_admin]	ステージングテーブルのレコードを表示または編集できます。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

で既存の OT レコードをプレビュー CMDB

ステージングテーブルから新しいレコードをインポートする前に、構成管理データベース (CMDB) 内の既存の オペレーショナルテクノロジー (OT) デバイスレコードをプレビューします。既存のレコードをプレビューすることで、関連のないレコードの調整や結合を回避できます。

始める前に

必要なロール: cmdb_ot_admin または admin

このタスクについて

ステージングテーブルから OT デバイスをインポートするときに、一致する構成アイテム (CI) が CMDB 内にある場合、既存のレコードが新しいレコードと調整または結合される可能性があります。一致する CI には、ホスト名、MAC アドレス、またはシリアル番号が含まれます。誤ってレコードを調整または結合しないように、ステージングテーブル内のレコードと一致する CI を共有する既存のレコードをプレビューできます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT Manager (OT マネージャー) > OT デバイスのインポート: ステージングテーブル**.
 検証コメントには、見つかった一致する CI の説明と、一致する CI へのリンクが含まれています。一致する CI が CMDB で見つかったと、[検証] ステータスが [部分的に有効] に設定されます。次の表に、一致する CI 検証コメントを示します。

一致する CI 検証コメント

一致する CI	検証コメント
ホスト名	別の CI で同じ変換済みの名前が見つかりました:<Link to CI>
MAC アドレス	別の CI で同じ MAC アドレス [MAC アドレス] が見つかりました:<Link to CI>
Serial number (シリアル番号)	別の CI で同じシリアル番号 [シリアル番号] が見つかりました: <Link to CI>

2. オプション: [Matching CI in the CMDB (CMDB 内の一致する CI)] 列から選択して、一致する CI を確認します。

簡単インポート

簡単インポートは、必要な列のみをインポートできる簡素化されたインポートプロセスです。

admin ロールを持つユーザーのみが簡単インポートを使用できます。現在のスコープ内のテーブルと、他のアプリケーションへの書き込みアクセス権を付与するテーブルにデータをインポートできます。

Excel テンプレートをダウンロードする

Microsoft Excel テンプレートをダウンロードして、Microsoft Excel スプレッドシートを作成し、既存のオペレーショナルテクノロジーデータを入力します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT Manager (OT マネージャー) > OT デバイスのインポート:ステージングテーブル**.
2. 列見出しを右クリックし、リストメニューから「インポート」を選択します。
3. レコードを [挿入] するか [更新] するかを選択します。

テンプレートのインポート

テンプレート	説明
挿入	このテンプレートを使用して、新しいレコードをテーブルに追加します。
更新	このテンプレートを使用して、テーブル内の既存のレコード内の値を変更します。このテンプレートには、リスト内のレコードごとに 1 行が含まれています。現在のリストフィルターによって、テンプレートに含まれるレコードが決まります。

Insert new records or update existing records using an Excel template file. Click Upload to preview the data to be imported. [More Info](#)

Import external data into SG OT Excel Staging

Do you want to insert or update data ? ☒ Insert ☐ Update

Do you want to create an Excel template to enter data ? ☒

Step 1: Create an Excel template file to enter data

Include all fields in the template? ☒

Create Excel template

Step 2: Upload the template file

Excel template file No file chosen

Upload

自動翻訳

4. リストに表示される列のみをテンプレートに含めるには、[すべてのフィールドをテンプレートに含める] チェック ボックスをオフにします。

テーブル内の特定のフィールドはシステムプロセスによって更新され、そのフィールドに値をインポートすることはできません。例として [作成者] フィールドがあります。このフィールドには、インポートを実行したログインユーザーがインポート中に入力されます。

このチェックボックスを選択したままにすると、リストで非表示になっている列も含め、テーブルのすべての列がテンプレートに含まれます。

5. [**Excel** テンプレートの作成] を選択します。

6. [エクスポートの完了] ページで、[ダウンロード] を選択して Microsoft Excel スプレッドシートをダウンロードします。

次のタスク

希望するアプリケーションを使用して、スプレッドシートを開きます。

注:

テンプレートには、テンプレートの使用方法を説明する [方向] タブが含まれています。

サービスグラフ コネクタインポート用のインポート前 **OT** ワークシートエントリーレビューツールを準備する

アップロードを成功させるには、既存のデータを正しい列に配置してスプレッドシートを準備することが重要です。

始める前に

必要なロール : admin

このタスクについて

手順

1. Microsoft Excel スプレッドシートの次の列に入力します。

注:

列名は変更できません。ステージングテーブルに列を追加できます。ステージングテーブルに新しいカスタムフィールドマッピングを追加する方法の詳細については、「[のステージングテーブルにカスタムフィールドマッピングを追加する サービスグラフ](#)」を参照してください。

スプレッドシートに入力する際のガイダンスについては、次の表を参照してください。スプレッドシートには多くの列が含まれています。例とフィールドの説明は、複数のセクションに分かれています。

- A から K までの列への入力
- 列 L から Y への入力
- AI による列 Z の入力
- AJ から AT までの列への入力
- AU から BD までの列への入力
- 列への入力 BE から BR
- BS から BW までの列への入力
- 1 桁目から 8 桁目への入力

列 A から K

列	必須列名	タイプ	説明と例
A	デバイスの重要度	文字列	ルールに基づく OT デバイスの重要度または重要度の測定。例： 「高」または「最重要」 - 中またはある程度重要 - 低またはやや重要 - なしまたは重要ではない
B	Assigned to (アサイン先)	文字列	この OT デバイスがアサインされているユーザーのメールアドレス。例:bob@example.com
C	バックプレーン ID	文字列	バックプレーンの識別と制御モジュールへのマッピングに使用される一意の ID。例:BPSN123
D	バックプレーン名	文字列	OT デバイスのバックプレーンの名前 (存在する場合)。例:バックプレーン #51、PLC1 バックプレーン
E	コントロールモジュールの親 ID	文字列	親コントロールシステムバックプレーンに対するコントロールモジュールの識別に使用される一意の ID。例:482bb239-05e8-4bad-ba59-925eb87ff06e
F	関連 ID	文字列	OT デバイスの識別に使用される一意の ID。correlation_id文字列を入力します。例: 482bb239-05e8-4bad-ba59-925eb87ff06e または 5123456。この列エントリは必須です。 - インポートされた各 OT デバイスには、一意のcorrelation_idが必要です。 - インポートする OT デバイスデータは通常、外部ソースシステムで作成され、各レコードに一意の識別子が割り当てられます。
G	カスタムフィールド 1	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。例: 再生品、中古品
H	カスタムフィールド 2	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。例:塗装、スタンプング
I	カスタムフィールド 3	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。
J	カスタムフィールド 4	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。
K	カスタムフィールド 5	文字列	(オプション)OT デバイスのカスタムデータは、CI の [属性] フィールドに保存されます。この列を使用して、分類やその他の目的でフリーフォームデータを OT デバイスに関連付けることができます。

列 L から Y

列	必須列名	タイプ	説明と例
L	Display name (表示名)	文字列	OT デバイスの表示名を入力するために使用されます。
M	機器モデルエンティティパス	文字列	OT デバイスがマッピングされている機器モデルエンティティのパス。
N	ファームウェアバージョン	文字列	OT デバイスのファームウェアバージョン (存在する場合)。例:12.0
O	最初の検出日	日時	OT デバイスがネットワーク上で最初に検出されたときの ISO 形式のタイムスタンプ。 例:YYYY-MM-DD HH:MM:SS。
P	ハードウェアバージョン	文字列	OT デバイスのハードウェアバージョン (存在する場合)。例:13.2
Q	モジュールあり	ブーリアン	モジュール付き制御システムの場合、このシステムにモジュールがあることを示します。 例:true、false
R	IO フィールドデバイスタイプ	文字列	この装置がフィールド装置の場合、入力、出力、またはその両方に使用するかどうかを示します。 例： - 入力 - output - input_output このデバイスは、入力と出力の両方として機能します。
S	IP アドレス 1	文字列	OT デバイスに関連付けられている最初の IP アドレス (存在する場合)。複数の IP アドレスがある

列	必須列名	タイプ	説明と例
			場合は、次の IP アドレス列 (IP アドレス 2) を使用します。 例:10.0.0.22、10.0.0.12
T	IP アドレス 2	文字列	OT デバイスに関連付けられている 2 番目の IP アドレス (存在する場合)。 例:192.168.100.1、192.168.100.5
U	IP アドレス 3	文字列	OT デバイスに関連付けられている 3 番目の IP アドレス (存在する場合)。
V	IP アドレス 4	文字列	OT デバイスに関連付けられている 4 番目の IP アドレス (存在する場合)。
W	IP アドレス 5	文字列	OT デバイスに関連付けられている 5 番目の IP アドレス (存在する場合)。
X	IP アドレス 6	文字列	OT デバイスに関連付けられている 6 番目の IP アドレス (存在する場合)。
Y	IP アドレス 7	文字列	OT デバイスに関連付けられている 7 番目の IP アドレス (存在する場合)。

自動翻訳

列 Z から AI

列	必須列名	タイプ	説明と例
Z	IP アドレス 8	文字列	OT デバイスに関連付けられている 8 番目の IP アドレス (ある場合)。
AAの	IP アドレス 9	文字列	OT デバイスに関連付けられている 9 番目の IP アドレス (存在する場合)。
AB	MAC アドレス 1	文字列	OT デバイスに関連付けられている最初の MAC アドレス (存在する場合)。複数の MAC アドレスがある場合は、次の MAC アドレス列(MAC アドレス 2)を使用します。 例:94:94:1d:01:6d:5f、cc:7c:4a:fb:2

列	必須列名	タイプ	説明と例
			i 注: OT デバイスの場合、次の 3 つのスプレッドシート列のうち少なくとも 1 つにエントリを作成する必要があります。これらの列のすべての値はスプレッドシートに対して一意である必要があります。 - MAC アドレス 1 - 名前 - Serial number (シリアル番号)
AC	MAC アドレス 2	文字列	OT デバイスに関連付けられている 2 番目の MAC アドレス (存在する場合)。例:e5:4d:c8:36:b1:2d
AD	MAC アドレス 3	文字列	OT デバイスに関連付けられている 3 番目の MAC アドレス (存在する場合)。
AE	MAC アドレス 4	文字列	OT デバイスに関連付けられている 4 番目の MAC アドレス (存在する場合)。
AF	MAC アドレス 5	文字列	OT デバイスに関連付けられている 5 番目の MAC アドレス (存在する場合)。
AGの	MAC アドレス 6	文字列	OT デバイスに関連付けられている 6 番目の MAC アドレス (ある場合)。
AH	MAC アドレス 7	文字列	OT デバイスに関連付けられている 7 番目の MAC アドレス (存在する場合)。
AI	MAC アドレス 8	文字列	OT デバイスに関連付けられている 8 番目の MAC アドレス (存在する場合)。

列 AJ から AT

列	必須列名	タイプ	説明と例
AJ	MAC アドレス 9	文字列	OT デバイスに関連付けられている 9 番目の MAC アドレス (存在する場合)。
AK	Manufacturer (メーカー)	文字列	OT デバイスのメーカーの名前。例:ロックウェル・オートメーション、デル
アル	メモ리카ードのシリアル 1	文字列	OT デバイスに取り付けられている最初のメモ리카ード (ある場合) のアサイン済みシリアル番号。メモ리카ードが複数ある場合は、次のメモ리카ードのシリアル列(メモ리카ードのシリアル2)を使用します。例:MMC DA362131、MemSN123
AM	メモ리카ードのシリアル 2	文字列	OT デバイスに取り付けられている 2 枚目のメモ리카ード (ある場合) のアサイン済みシリアル番号。例:MemSN123
ひとつの	メモ리카ードのシリアル 3	文字列	OT デバイスに取り付けられている 3 枚目のメモ리카ード (ある場合) のアサイン済みシリアル番号。
AO の	メモリサイズ 1	文字列	OT デバイスに取り付けられている最初のメモ리카ードのサイズ (ある場合)。例:256 GB または 1 GB
AP 通信	メモリサイズ 2	文字列	OT デバイスに取り付けられている 2 枚目のメモ리카ードのサイズ (ある場合)。例:256 GB または 1 GB
AQ	メモリサイズ 3	文字列	OT デバイスに取り付けられている 3 枚目のメモ리카ードのサイズ (ある場合)。例:256 GB または 1 GB
アール	メモリタイプ 1	文字列	OT デバイスに取り付けられているメモ리카ードのタイプ。メモ리카ードが複数ある場合は、複数の列を使用します。例:RAM
として	メモリタイプ 2	文字列	OT デバイスに取り付けられているメモ리카ードのタイプ。例:RAM
で	メモリタイプ 3	文字列	OT デバイスに取り付けられているメモ리카ードのタイプ。

列 AU から BD

列	必須列名	タイプ	説明と例
天文	モデル番号	文字列	OT デバイスのメーカーのモデル番号。例:ThinkServer TD230、XPS 15z

列	必須列名	タイプ	説明と例
単位			
AV の	モジュールタイプ	文字列	コントロールモジュールの機能の説明(このデバイスがコントロールモジュールの場合)。例:入力、出力
AW の	名前	文字列	OT デバイスのホスト名 (通常は FQDN の一部として)。例:PLC1、ドアアセンブリHMI、ロボット制御モジュール。 i 注: OT デバイスの場合は、これら 3 つのスプレッドシート列のうち少なくとも 1 つにエントリを作成する必要があります。これらの列のすべての値は、スプレッドシートに対して一意である必要があります。 - MAC アドレス 1 - 名前 - Serial number (シリアル番号)
斧	オペレーティングシステム	文字列	OT デバイスにインストールされているオペレーティングシステム (存在する場合)。例:Linux Fedora、Windows 10、Windows 2000、Mac OS 8。 i 注: OT デバイスの場合は、必須ではありませんが、次のスプレッドシート列にエントリを作成する必要があります。 - タイプ - 利用可能な場合、オペレーティングシステム - 利用可能な場合、ファームウェアバージョン
はい	OS バージョン	文字列	OT デバイスにインストールされているオペレーティングシステムの報告されたバージョン (存在する場合)。例:10.0、13.5.2 i 注: OT デバイスの場合は、必須ではありませんが、次のスプレッドシート列にエントリを作成する必要があります。 - type - 利用可能な場合は、os_version - 利用可能な場合、ファームウェアバージョン
アリゾナ州	OT ステージングタスク	文字列	ステージングテーブルの無効なレコードを修復するために作成されたタスク。
文学士	Purdue レベル	文字列	OT デバイスにアサインされた Purdue レベル。Purdue レベルを割り当てると、オペレーショナルテクノロジー機能のディスカバリーが正しい ICS レ

列	必須列名	タイプ	説明と例
			ベルで各アイテムを適切に配置し、正確なディスカバリー結果を生成できます。例:1、2、3
BB の	ラック 番号	文字 列	コントロールモジュールが取り付けられているラック。例:1、2、3
BC	Serial number (シリアル 番号)	文字 列	OT デバイスにアサインされたシリアル番号 (ある場合)。 例:SN545、SN998 i 注: OT デバイスの場合は、これら 3 つのスプレッドシート列のうち少なくとも 1 つにエントリを作成する必要があります。これらの列のすべての値は、スプレッドシートに対して一意である必要があります。 - MAC アドレス 1 - 名前 - Serial number (シリアル番号)
BD	シリアル 番号 タイプ	文字 列	通常は「system」の値に設定されますが、別のタイプのシリアル番号にすることもできます。例:uuid

列 BE から BR

列	必須列名	タイプ	説明と例
BE	簡単な説明	文字 列	OT デバイスの簡単な説明。例:ドア塗装セルのHMI、ドア組み立てロボットを制御します。
BF の	サイト	文字 列	機器モデルはサイトレベルで開始され、各産業サイトを説明する詳細な階層構造が含まれています。 詳細については、「 ISA-95 機器モデル 」を参照してください。
BG の	スロット番号	文字 列	コントロールモジュールの場合、このデバイスが制御システムのシャーシ内で占有するスロットを示します。例:1、2
BH	ソフトウェア のインストール 日 1	日時	アプリケーションソフトウェアが OT デバイスにインストールされた日付。日付が複数ある場合は、複数の列を使用します。 日付には UTC 形式のみを使用します。 例:YYYY-MM-DD HH:MM:SS
BIの	ソフトウェア のインストール 日 2	日時	アプリケーションソフトウェアが OT デバイスにインストールされた日付。日付が複数ある場合は、複数の列を使用します。 日付には UTC 形式のみを使用します。例:YYYY-MM-DD HH:MM:SS

列	必須列名	タイプ	説明と例
BJ の	ソフトウェア のインストール 日 3	日時	アプリケーションソフトウェアが OT デバイスにインストールされた 日付。日付が複数ある場合は、複数の列を使用します。 日付には UTC 形式のみを使用します。例:YYYY-MM-DD HH:MM:SS。
BK の	インストール されているソ フトウェア 1	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの名前 (存在する場合)。複数の名前がある場合は、複数の列を使用 します。例:ロックウェルHMIビジョン
BL の	インストール されているソ フトウェア 2	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの名前 (存在する場合)。
BM の	インストール されているソ フトウェア 3	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ アの名前 (存在する場合)。
BN の	ソフトウェア バージョン 1	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ ア (存在する場合) の報告されたバージョン。複数のバージョンがある 場合は、複数の列を使用します。 例:v1.2 または v2011 SP3 HF2 または 4.54.32145
ボー	ソフトウェア バージョン 2	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ ア (存在する場合) の報告されたバージョン。 例:v1.2 または v2011 SP3 HF2 または 4.54.32145
BP	ソフトウェア バージョン 3	文 字 列	OT デバイスにインストールされているアプリケーションソフトウェ ア (存在する場合) の報告されたバージョン。 例:v1.2 または v2011 SP3 HF2 または 4.54.32145
BQ	ステータス	文 字 列	OT デバイスのステータス: -- なし -- アサイン済みステータスはありません。 不在 OT デバイスが施設にありません。 In Maintenance (メンテナンス中) OT デバイスはメンテナンス中で、現在はオフラインで す。 In stock (在庫あり) OT デバイスの在庫が施設にあります。 インストール日時 OT デバイスが施設にインストールされています。 インストール待ち OT デバイスが施設へのインストールを保留していま す。

列	必須列名	タイプ	説明と例
			修理待ち OT デバイスは修理待ちですが、まだオンラインではありません。 Retired (廃止) OT デバイスは廃止されました。 Stolen (盗難) OT デバイスが盗まれました。 i 注: このフィールドの値は、CI フォームの [ライフサイクル ステージ] フィールドと [ライフサイクル ステージ ステータス] フィールドにマッピングされます。
ベッドルーム	Support group (サポートグループ)	文字列	この OT デバイスのプライマリサポートグループの名前。例: ドアサポート、企業ITサポート。

列 **BS** から **BW**

列	必須列名	タイプ	説明と例
理学士	変換済みの名前	文字列	ユーザーはこの列に入力しないでください。 デフォルトでは、変換された名前の値は、変換された列のシステムプロパティを使用して入力されます。 ユーザーは変換済みの名前を編集できません。 システムプロパティについては、「SG-OT デバイスの Excel インポート処理に影響を与えるシステムプロパティ」を参照してください。
BTの	タイプ	文字列	OT デバイス/構成アイテム (CI) のタイプ。 例: PLC、DCS

列	必須列名	タイプ	説明と例
			i 注: - 有効な CI タイプのリストと説明については、「オペレーションテクノロジー (OT) 拡張クラス」を参照してください。 - OT デバイスの場合は、必須ではありませんが、次のスプレッドシート列にエントリを作成する必要があります。 - type - os_version
BU	検証コメント	文字列	ユーザーはこの列に入力しないでください。 デフォルトでは、Excel からインポートされたステージングテーブルレコードで検証が実行された後に、検証コメントが入力されます。 レコードがインポートされても、検証コメントは更新されません。 ユーザーは検証コメントを編集できません。
バフ	検証ステータス	文字列	ユーザーはこの列に入力しないでください。 デフォルトでは、データがステージングテーブルにインポートされると、検証ステータスが設定されます。

列	必須列名	タイプ	説明と例
			OT デバイスのステータス: 検証の保留中 レコードがステージングテーブルにインポートされたときのデフォルトの状態。 無効 CMDB内で CI レコードを一意に作成することはできません。 部分的に有効 変換済みの名前、MAC アドレス 1、およびシリアル番号のいずれかに値がありません。他のすべてのフィールド(関連 ID、コントロールモジュール親ID)には値があります。 有効 すべての識別子が存在し、インポートの準備ができています。

列	必須列名	タイプ	説明と例
			インポート済み ステージングテーブルからインポートセットテーブルへのデータのインポートが完了しました。 ユーザーは検証ステータスを編集できません。
BWの	Vendor (ベンダー)	文字列	OT デバイスのベンダーの名前。

列1から8

列	必須列名	タイプ	選択肢列 (該当する場合)	説明と例
1	バックアップ構成ステータス	選択リスト	バックアップ有効、バックアップ無効、不明、適用外、計画済み、計画外	CI が関連するポリシーと一緒にバックアップサービスまたはアプライアンスに構成されているかどうかを示します。 例:バックアップが有効
2	バックアップ実行モード	選択リスト	手動、自動、手動または自動、不明	バックアップが定期的に自動的に実行されるように構成されているか、必要に応じて手動で実行されるように構成されているかを示します。 例:手動、自動
3	バックアップソース ID	文字列		外部または内部のバックアップサービスでデバイスを識別する、デバイスのバックアップサービスソース識別子。バックアップソース ID に

sn_otsm_sgc.excel.fields.for.transformed.name

- このプロパティにより、ユーザーは変換された名前を構築するためのフィールドを提供できます。
- フィールド値または列名はカンマで区切る必要があります。

この変換された名前は、ステージングテーブルから直接 [名前] フィールドの代わりに構成アイテム (CI) の名前として使用されます。デフォルトでは、名前フィールド値自体が変換された名前の値として使用されます。

- このプロパティは **sn_otsm_sgc** スコープに属し、このプロパティ名に自動的に追加されます。
- 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。

sn_otsm_sgc.excel.transformed.name.delimiter

- このプロパティは、システムプロパティ **fields.for.transformed.name** で指定された複数のフィールドまたは列の値を使用して変換済みの名前を計算するときに使用される区切り文字を指定します。
- **fields.for.transformed.name** プロパティで列名が 1 つだけ指定されている場合、区切り文字は使用されません。
- このプロパティは **sn_otsm_sgc** スコープに属し、このプロパティ名に自動的に追加されます。
- 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。

sn_otsm_sgc.excel.fields.for.validation.state.change

- このプロパティを使用すると、属性のカンマ区切りリストを指定して、検証ステータスが [検証保留中] に変更されるようにすることができます。デフォルト値は [空] です。



注:

MAC アドレス、シリアル番号、変換済みの名前、スロット番号 (OT コントロールモジュールの場合) などの識別子フィールドが変更されると、検証ステータスが [検証保留中] に変更されます。

- このプロパティはsn_otsm_sgcスコープに属し、このプロパティ名に自動的に追加されます。
- 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。

sn_otsm_sgc.enable.cmdb.validations

- このプロパティは、ステージングデバイスの CMDB 検証を有効にします。**True** に設定すると、ステージングデバイスは調整のために既存の CMDB CI に対して検証されます。
- このプロパティはsn_otsm_sgcスコープに属し、このプロパティ名に自動的に追加されます。
- 読み取りおよび書き込み操作には、admin、cmdb_ot_admin、および cmdb_inst_admin ロールが必要です。

Excel テンプレートのインポート

インポートテンプレートを新しいデータで更新した後、テンプレートをインスタンスにインポートして検証し、欠落しているデータ、重複しているデータ、無効なデータを見つけます。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT Manager (OT マネージャー) > OT デバイスのインポート:ステージングテーブル**.
2. 列見出しを右クリックし、メニューから「インポート」を選択します。

① Insert new records or update existing records using an Excel template file. Click Upload to preview the data to be imported. [More Info](#)

< Import external data into SG OT Excel Staging

Do you want to insert or update data ? ☒ Insert ☐ Update

Do you want to create an Excel template to enter data ? ☒

Step 1: Create an Excel template file to enter data

Include all fields in the template? ☒

Create Excel template

Step 2: Upload the template file

Excel template file No file chosen

Upload

3. インポートタイプとして [挿入] または [更新] を選択します。
4. [ファイルを選択] を選択して Microsoft Excel スプレッドシートを選択します。
5. [アップロード] を選択して、Microsoft Excel スプレッドシートをアップロードします。
6. [アップロードの進行状況] ページで、[インポートされたデータをプレビュー] を選択して、インポートされたデータを確認します。
7. テンプレートが検証に合格し、インポートされたプレビューが期待どおりである場合は、[インポートを完了] を選択してステージングテーブルにレコードをインポートします。

自動翻訳

OT デバイスを作成

[OT デバイスをインポート] ステージングテーブルで OT デバイスを手動で作成します。

始める前に

必要なロール:ot_staging_user、cmdb_ot_admin、または admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT マネージャーアドミン > OT デバイスのインポート：ステージングテーブル**.
2. [新規] ボタンを選択します。
3. [デバイスのタイプは何ですか? (**What is the type of the device?**)] リストから、OT デバイスタイプを選択します。
選択したデバイスタイプはフォームに自動的に追加されます。
4. [SG OT Excel ステージング:新規レコード] フォームで、必要に応じてフィールドに入力します。

[SG OT Excel ステージング:新規レコード] フォームのフィールド

Field (フィールド)	説明
Display name (表示名)	レコードに表示される OT デバイスの名前。 i 注: このフィールドには任意の文字列値を追加できます。複数のデバイスに同じ OT 表示名を付けることができます。これは OT デバイスを理解しやすくするためのものであり、ステージングテーブルから OT デバイスをインポートするときに生成される一意の CI 名とは異なります。
名前	CI で生成された一意の名前。
Purdue レベル	アサインされた Purdue レベル。レベル範囲は 0 から 5 です。 i 注: 産業用制御システムの Purdue レベルの詳細については、「 https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems 」を参照してください。
デバイスの重要度	デバイスに障害が発生した場合のサイトプロセスへの相対リスクの測定: ○ 1：最重要 ○ 4：重要ではない
関連 ID	デバイスが属するサイト。
サイト	デバイスが配置または割り当てられている最上位の親エンティティ、または産業サイト。

Field (フィールド)	説明
機器モデルエンティティパス	デバイスが存在する機器モデルエンティティパス。

5. オプション: 必要に応じて、次の関連リストに追加情報を追加します。

- 補足情報
- ネットワークアダプタ
- IP アドレス
- シリアル番号
- OS 情報
- コントロールシステム情報
- コントロールモジュール情報
- ソフトウェア情報
- メモリモジュール情報
- バックアップストア情報

6. **[Create OT Device (OT デバイスを作成)]** を選択します。

タスクの結果

OT デバイスが作成され、ステージングテーブルに追加されます。

検証の管理

検証では、ステージングテーブルにインポートされたデータを確認および管理できます。

実行する検証:

- 相関 ID (相関 ID) がありません
- タイプがコントロールモジュールの場合の親相関 ID がありません (コントロールモジュールの親 ID)
- シリアル番号がありません (シリアル番号)
- 変換済みの名前がありません (変換済みの名前)
- MAC アドレスがありません (列 MAC アドレス 1 で検証が実行されます)
- 欠損タイプ (Type)
- ラック番号 (ラック番号) がありません
- スロット番号 (スロット番号) がありません
- 機器モデルエンティティパスが存在しません (機器モデルエンティティパス)
- 指定されたサイト名が無効です (サイト名)
- 変換済みの名前 (変換済みの名前) の重複を検証

注:

コントロールモジュールでは、この検証はスキップされます。

- MAC アドレスの重複を検証 (MAC アドレス 1 のすべての列をチェック)
- シリアル番号列 (シリアル番号) の重複を検証

- 相関 ID 列 (相関 ID) の重複を検証
- ラック番号とスロット番号の重複を検証

i 注:

この検証は、コントロールモジュールのみを対象としています。

- モジュールありとコントロールモジュールの親 ID を検証

i 注:

この検証は、PLCと制御モジュールのみを対象としています。

- 無効なタイプの検証: `sn_otsm_sgc.SGOTAssetImportExtensionPoint` 拡張ポイント実装を通じて、デフォルトの Excel タイプと OT デバイスタイプのマッピングと比較します。

追加のマッピングがある場合は、ベースシステム

`sn_otsm_sgc.SGOTAssetImportExtensionPoint` 拡張ポイントの拡張ポイント実装を作成します。

デバイス分類のカスタム実装の追加の詳細については、「[デバイス分類のカスタム実装の追加](#)」を参照してください。

検証を実行

レコードの検証を実行して、欠損データ、重複データ、および無効なデータを見つけます。

始める前に

必要なロール: `ot_staging_user`、`cmdb_ot_admin`、または `admin`

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT Manager (OT マネージャー) > OT デバイスのインポート: ステージングテーブル**.
2. [Run Validations (検証を実行)] を選択して、ステージングテーブルで検証をトリガーします。

検証はすべてのレコードに対してバックグラウンドで実行されます。

データの検証にかかる時間は、ステージングテーブルに存在するレコードの数によって異なります。

3. 検証が完了したら、ステージングテーブルの [検証ステータス] 列でレコードのステータスを確認します。
4. レコードのステータスが部分的に有効または無効である場合は、次の操作を行います。
 - a. レコード内の欠落データを確認します。
 - b. レコードを修正します。
レコードは、ステージングテーブルのリストビューとビューのレコードで編集できます。
 - c. レコードを更新します。
 - d. 検証を実行します。

5. 不足しているデータが利用できない場合は、次の操作を行って特定のレコードのステータスを上書きし、そのレコードを有効として手動で設定します。

- a. レコードを選択してフォームを開きます。
- b. [有効に設定] を選択します。

i 注:

レコードを手動で有効に設定すると、調整の問題が発生し、CI が作成されない可能性があります。

OT ステージングタスクを使用して無効なレコードを修正する

オペレーショナルテクノロジー (OT) ステージングタスクを使用して、SG OT Excel ステージングテーブルの無効なレコードを修正します。OT ステージングタスクを使用すると、修正が必要な無効なレコードを追跡するのに役立ちます。

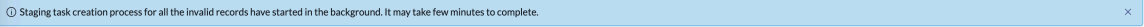
始める前に

必要なロール: cmdb_ot_admin、cmdb_ot_editor、ot_staging_user

このタスクについて

OT ステージングタスクを使用して、SG OT Excel ステージング (sg_ot_excel_staging) テーブルの無効なレコードを修正できます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT マネージャーアドミン > OT デバイスのインポート: ステージングテーブル**.
2. テーブルヘッダーで、[タスクの作成] ボタンを選択します。
以下の確認メッセージが表示されます。

3. ステージングタスクの作成プロセスが完了するまで待ちます。
ステージングタスクの作成が完了すると、テーブルの [OT ステージングタスク] 列に、無効なステージングレコードに関連する OT ステージングタスクが入力されます。
4. ステージングタスクレコードを確認および編集します。
 - a. [OT ステージングタスク] 列で、レコードを選択します。
 - b. ステージングタスクレコードフォームのフィールドに入力します (該当する場合)。

OT ステージングタスクレコードフォーム

Field (フィールド)	説明
ステータス	ステージングタスクのステータス。ステータスは、修復のいくつかの段階を通じてステージングタスクを移動させ、追跡します。
サイト	ステージングタスクが関連付けられているサイト。デフォルトのステージングタスクレコードの [サイト] フィールドは空です。空または無効なサイトフィールドを持つすべての無効なステージングレコードは、デフォルトのステージングタスクに関連付けられます。

Field (フィールド)	説明
	i 注: ステージングレコードの [サイト] フィールドを変更すると、関連するステージングタスクレコードが削除されます。
Description (説明)	ステージングタスクの詳細な説明。
作成者	ステージングタスクレコードを作成したユーザー。
Assigned to (アサイン先)	ステージングタスクを処理するユーザー。
アサイン先グループ	ステージングタスクを担当するアサイン先グループ。

c. [更新] を選択します。

5. オプション: SG OT Excel ステージングタスク (sg_ot_excel_staging_task) テーブルで作成された OT ステージングタスクレコードを表示するには、次の場所に移動します。すべて > 産業用ワークスペースアドミン > **OT** マネージャーアドミン > **OT** デバイスのインポート: ステージングタスクテーブル。

タスクの結果

これでステージングタスクレコードが作成され、修復を担当するユーザーにアサインされます。

データをインポートする時間間隔をスケジュールする

ステージングテーブルから CMDBにデータをインポートする時間間隔をスケジュールします。

始める前に

必要なロール: admin または cmdb_inst_admin

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > **OT Manager (OT マネージャー)** > **OT** デバイスのインポート: ステージングテーブル。
2. [SG OT Excel ステージング] ページで、[スケジュール済みインポート] を選択します。
3. [アクティブ] チェックボックスをオンにして、データをインポートする時間間隔をスケジュールします。
4. [今すぐ実行] を選択して、ステージングテーブルから CMDBにレコードをインポートします。

[検証] ステータスには、正常にインポートされたデータの [インポート済み] ステータスが表示されます。

ステージングテーブルでは、正常にインポートされたすべてのレコードがテーブルクリーナーによって削除されます。テーブルクリーナーの詳細については、「 」を参照してください。

ステージングテーブルを使用した Microsoft Excel スプレッドシートのインポート

簡単インポートを使用して Microsoft Excel スプレッドシートをステージングテーブルにインポートし、スプレッドシートからステージングテーブルに必要なデータを作成します。

始める前に

このプロセスには、統合ハブ ETL (com. sn_int_studio) プラグインが必要です。

このプロセスを実行する前に、インポートする Microsoft Excel スプレッドシートを適切に準備する必要があります。詳細については、「[サービスグラフ コネクタインポート用のインポート前 OT ワークシートエントリレビューツールを準備する](#)」を参照してください。

データをインポートする準備ができれば、構成管理データベース (CMDB) へのインポートをスケジュールできます。このプロセスにより、スプレッドシートに含まれる OT デバイスの 構成管理データベース (CMDB) に一意のレコードが作成されます。

必要なロール:cmdb_inst_admin、import_admin、import_scheduler、admin

このタスクについて

統合ハブ抽出変換ロード (ETL) を実行するときに、産業用 ガイド付きセットアップ に埋め込まれたコンテンツを参照して、追加のサポートを受けることもできます。

ステージングテーブルで検証を実行し、データの重複や不整合をチェックします。

産業用 ガイド付きセットアップにアクセスするには、産業用ワークスペースアドミン > ガイド付きセットアップ。

手順

1. 移動先 **すべて > 構成 > 統合ハブ ETL**.
2. **[CMDB アプリケーション:SG-OT Excel インポート ETL]** を選択します。
3. [ETL 変換マップアシスタント] フォームで、[ソースデータと基本的な詳細のインポート] を選択します。
4. [ETL 変換マップの基本情報を入力 (Provide Basic Information for the ETL Transform Map)] フォームの [サンプルインポートセット] フィールドで、[新しいインポートセットを自動ブル] を選択します。
5. 統合ハブ ETL フォームに戻ります。

i 注:

ETL 変換マップを作成するための残りの手順は、自動的に完了します。ただし、実際のインポートを実行する前に、特定のステップを選択してレビューすることができます。たとえば、[データの準備とプレビュー] を選択して、ネストされたデータ構造と生のソースデータを表示します。

i 注:

詳細については、「[ETL 変換マップの作成](#)」を参照してください。

6. 実際の Excel スプレッドシートのインポートを実行するには、[統合結果のテストとロールバック] を選択します。
7. **[Run Integration (統合の実行)]** を選択します。

i 注:

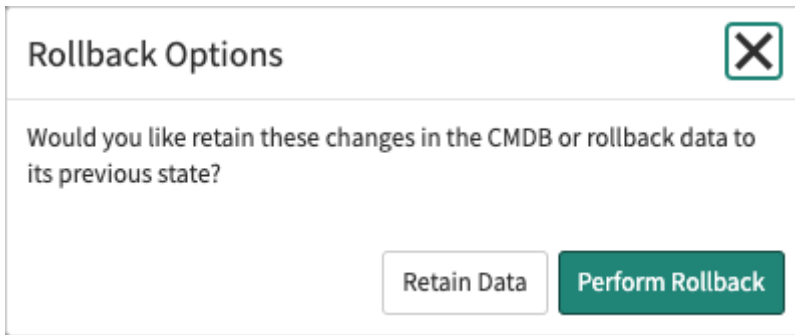
このインポートは 100 レコードをテストします。100 レコードを超える完全インポートを実行するには、インポートをスケジュールする必要があります。[インポートスケジュールを設定] を選択すると、定期的に設定されたスケジュールでインポートを実行するようにインポートをスケジュールできます。

データのインポートが完了すると、[テストとロールバックの統合結果] フォームが表示され、次のようなインポート統計情報が表示されます。

- マップされたクラス
- クラス間のリレーションシップ

- この統合実行から作成された新しいレコード。
- この統合実行から更新されたレコード。
- この統合実行から作成された部分的なレコード。
- この統合実行から作成された不完全なレコード。

8. [テストとロールバックの統合結果] フォームを終了します。
[ロールバックオプション] ダイアログボックスが表示されます。



The image shows a dialog box titled "Rollback Options" with a close button (X) in the top right corner. The main text asks: "Would you like retain these changes in the CMDB or rollback data to its previous state?". At the bottom, there are two buttons: "Retain Data" (light green) and "Perform Rollback" (dark green).

9. インポートされたデータを保持する場合は [データを保持] を選択し、インポートされたデータをロールバックして Microsoft Excel インポートを再試行する場合は [ロールバックを実行] を選択します。
10. スプレッドシートデータを Now Platformに正式にインポートするには:
- [インポートスケジュールの設定] を選択します。
 - [スケジュールの設定] を選択します。
 - [予定されているデータインポート] リストで、[スプレッドシートを使用した **SG-OT** デバイスのスケジュールインポート] を選択します。
 - [データインポートのスケジュール] フォームで、[今すぐ実行] を選択します。

次のタスク

すべての手順が完了したら、SG-OT デバイスインポート ETL ガイド付きセットアップのホームページで、[アクティブ化] を選択して ETL をアクティブ化します。

のステージングテーブルにカスタムフィールドマッピングを追加する サービスグラフ

ステージングテーブルにカスタムフィールドを追加し、Excel SGC を使用してステージングテーブルから CI フィールドにカスタムフィールドをマップします。

始める前に

フォーム レイアウトを構成するには、「[フォーム レイアウトの構成](#)」を参照してください。

ステージングテーブルにカスタムフィールドを作成するには、「[テーブルのフィールドを追加およびカスタマイズ](#)」を参照してください。

必要なロール：

- admin:スクリプトインクルードを変更したり、クラスまたはフィールドのマッピングを追加したり、ETL を変更したりできます。
- cmdb_inst_admin - 新しいクラスまたはフィールドのマッピングを追加し、ETL で変更することのみできます。

手順

1. ステージングテーブルにカスタム列が作成されたら、すべて > 産業用ワークスペースアドミン > **OT Manager (OT マネージャー)** > **OT デバイスのインポート:ステージングテーブル**.

2. Excel テンプレートをダウンロードします。

詳細については、「[Excel テンプレートのダウンロード](#)」を参照してください。

ステージングテーブルにレコードが存在する場合は、既存のレコードの列の値を編集できます。

3. Excel テンプレートを準備します。

詳細については、「[サービスグラフコネクタインポート用のインポート前 OT ワークシートエントリレビューツールの準備](#)」を参照してください。

4. Excel テンプレートをインポートします。

詳細については、「[Excel テンプレートのインポート](#)」を参照してください。

5. 移動先 すべて > 産業用ワークスペースアドミン > **OT Manager (OT マネージャー)** > **OT デバイスのインポート:スクリプトインクルード** をクリックし、SGOTAssetImportExcelConstants スクリプトインクルードを選択します。

6. スクリプトで、ステージングテーブルから新しい列名を更新し、SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap オブジェクト内の新しい ETL 列名を「<ETL 列名>:「<ステージングテーブルからの列名>」の形式で更新します。

この例では、コロン (:) の前の「u_my_custom_field」は ETL 列名 (ETL プレビューステップでは列として表示) を示し、コロンの後の「u_my_custom_field」はステージングテーブルの列名を示します。

新しい行の上の行の末尾にコンマ (,) が追加されていることを確認します。この例では、"custom_fields": "custom_fields" 行の後にカンマが追加されます。

```

SGOTAssetImportExcelConstants.importSetColumnsVsStagingColumnsMap = {
    // unique id used to uniquely identify the asset
    "id": "correlation_id",
    // Name of the asset
    "name": "transformed_name",
    // OperatingSystem of the asset
    //"operating_system": "os_version",
    // type of the asset.
    "type": "type",
    // if the asset has control module
    "has_module": "has_module",
    // id of the asset to which a control module belongs to (this is used in control module type asset).
    "control_module_parent_correlation_id": "control_module_parent_correlation_id",
    "ot_display_name": "display_name",
    "serial_number": "serial_number",
    "firmware_version": "firmware_version",
    "os_version": "os_version",
    "operating_system": "os",
    "assigned_to": "assigned_to",
    "manufacturer": "manufacturer",
    "model_number": "model_number",
    "serial_number_type": "serial_number_type",
    "purdue_level": "purdue_level",
    "asset_criticality": "asset_criticality",
    "short_description": "short_description",
    "vendor": "vendor",
    "equipment_model_entity_path": "equipment_model_entity_path",
    "first_discovered": "first_discovered",
    "hardware_version": "hardware_version",
    "status": "status",
    "backplane_name": "backplane_name",
    "backplane_id": "backplane_id",
    "slot_number": "slot_number",
    "rack_number": "rack_number",
    "module_type": "module_type",
    "device_type": "io_field_device_type",
    "support_group": "support_group",
    "site": "site",
    "ip_address": {
        "ip": "ip_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "mac_address": {
        "mac": "mac_address_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "memory": {
        "memory_card_serial": "memory_card_serial_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_size": "memory_size_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "memory_type": "memory_type_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    "software_installed": {
        "name": "software_installed_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "version": "software_version_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER,
        "install_date": "software_install_date_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    },
    // Do not change this. Key should match value of SGOTAssetImportExcelConstants.CUSTOM_FIELDS_COL_NAME_IN_IMPORT_SET
    "custom_fields": {
        "customfield": "customfield_" + SGOTAssetImportExcelConstants.STAGING.NESTED_COLUMN_DELIMITER
    }
}

```

7. [更新] を選択して、変更を保存します。
8. 移動先 すべて > 構成 > 統合ハブ **ETL**.
9. **[CMDB アプリケーション:SG-OT Excel インポート ETL]** を選択します。
10. [無効なマッピングデータが検出されました] ページが表示された場合は、[閉じる] を選択します。

11. ETL 変換マップアシスタントのガイド付きセットアップの [基本的な詳細を指定] セクションで、[ソースデータをインポート] を選択し、[基本的な詳細を入力] を選択します。

SG-OT Asset Excel Import

ETL Transform Map Assistant

Use this guided walkthrough to create and manage ETL Transform Map for integrating third-party data into CMDB.

1/1
Tasks

1. Specify Basic Details
Provide basic information for the ETL Transform Map.

✓ Import Source Data and Provide Basic Details

12. [サンプルインポートセット] フィールドで、[新しいインポートセットを自動プル] を選択します。

Specify Basic Details

← Provide Basic Information for the ETL Transform Map

Unsaved Changes

Save Mark as Complete

Provide the template with some basic properties, and select a data source to map to CMDB.

* CMDB Application ① SG-OT Excel Import

* Name ① SG-OT Asset Excel Import

Description ETL to import assets from Excel

* Data Source ① SG-OT Excel Import

Sample Import Set ① Auto-pull a new import set

13. [保存] を選択します。
「基本情報が正常に保存されました」というバナーが表示されます。
14. [Mark as Complete (完了としてマーク)] を選択します。
15. [ETL 変換マップアシスタント] ページの [マッピング用のソースデータの準備] セクションで、[データのプレビューと準備] を選択します。

now All Favorites History Workspaces

IntegrationHub ETL

Search

Prepare Source Data for Mapping

Preview and Prepare Data

Mark as Complete

Nested Data Structure

Tree Collection

object

object(1)

The table below displays raw source data. Click a column's action menu (≡) for specific data transformation options. You can also set columns to be ignored in mapping.

New Transform Show data structure

object	status_value	support_group	support_group_sys_id	type	u_my_custom_field	vendor	vendor_cleansed	vendor_name_cleansed
	get initial status value	Original Value	get support group sys id	Original Value	Original Value	Original Value	cleanse vendor	split - vendor cleansed
1				plc	My Custom value	Vendor E	48364f745328110594addecff7b127hj	Vendor E Vendor E

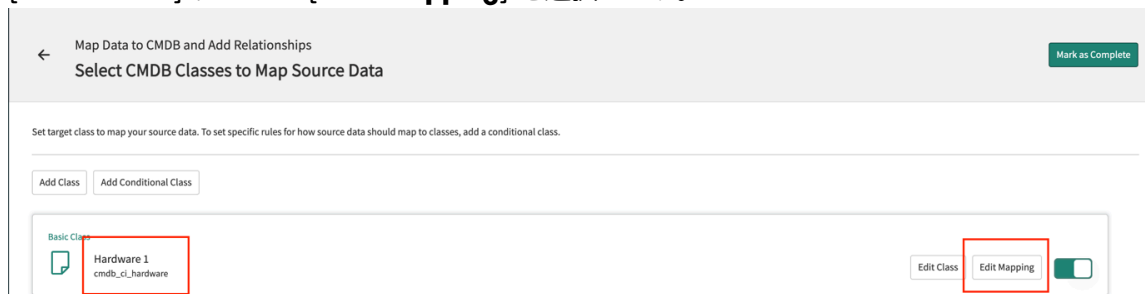
列が表示されない場合は、手順 11 から 14 を繰り返します。

16. [Mark as Complete (完了としてマーク)] を選択します。
17. [ETL 変換マップアシスタント] ページの [データを CMDB にマップしてリレーションシップを追加] セクションで、[ソースデータをマップする CMDB クラス] を選択します。
18. 列をターゲットクラスと属性にマップします。

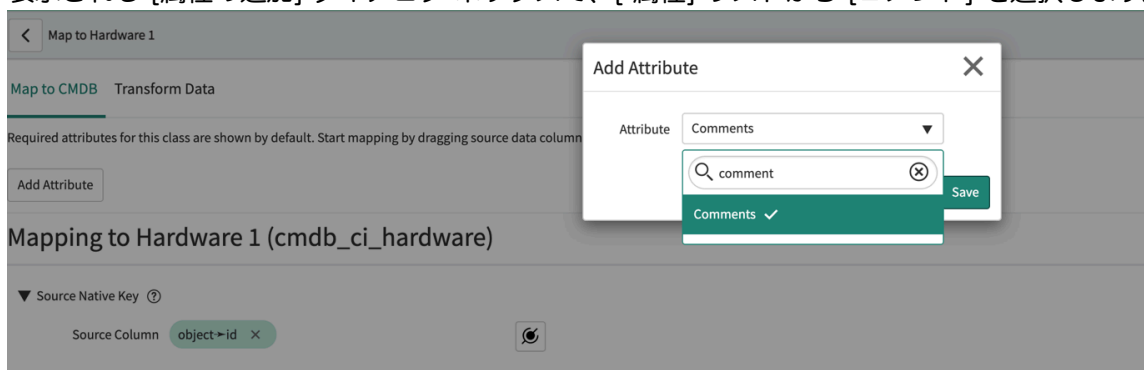
たとえば、「コメント」フィールドはハードウェア *cmdb_ci_hardware* クラスに存在します。このフィールドがマッピングされた後、その行のステージングテーブルの「コメント」列の値が空でない限り、ハードウェアの子クラスの「コメント」フィールドも更新されます。存在しない新しいフィールド、またはハードウェア *cmdb_ci_hardware* クラスに固有ではなく、代わりにオペレーショナルテクノロジー (*cmdb_ci_ot*) クラスのフィールドであるフィールドのマッピングを

追加する場合は、オペレーショナルテクノロジー (OT) 1 スタブにフィールドマッピングを追加します。

- a. フィールドマッピングを Hardware 1 クラスに追加します。
- b. [Hardware 1] クラスで [**Edit Mapping**] を選択します。



19. 表示される [属性の追加] ダイアログ ボックスで、[属性] リストから [コメント] を選択します。



20. [保存] を選択します。
「コメント」という名前の新しいフィールドが表示されます。スクロールしないとフィールドが表示されない場合があります。

Map to Hardware 1
Last Saved: 2021-10-28 13:29:49

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

Source Column	object→model_number_id_cleansed	
▼ Support group		
Source Column	object→support_group_sys_id	
▼ Manufacturer		
Source Column	object→manufacturer_sys_id_cleansed	
▼ First discovered		
Source Column	object→first_discovered_date_time_format	
▼ Class		
Source Column	object→asset_cmdb_class_sys_name	
▼ Comments		
Source Column		

21. [データ] ペインから、データピルを [コメント ソース列] フィールドにドラッグします。

now All Favorites History Workspaces IntegrationHub ETL

Map to Hardware 1
Last Saved: 2022-07-07 12:16:54

Successfully saved this mapping.

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

From collection object

Source Column	object→model_number_id_cleansed	
▼ Support group		
Source Column	object→support_group_sys_id	
▼ Manufacturer		
Source Column	object→manufacturer_sys_id_cleansed	
▼ First discovered		
Source Column	object→first_discovered_date_time_format	
▼ Class		
Source Column	object→asset_cmdb_class_sys_name	
▼ Comments		
Source Column	object→u.my_custom_field	

Data

serial_number_cleansed	SN0001
serial_number_snk	SN0001::6f6b81...
serial_number_type	system
serial_number_type_cleansed	system
serial_number_valid	true
sys_import_date_time_format	2022-07-07 06:4...
short_description	PLC with all the va...
site	Hyd Site
site_sys_id_computed	
slot_number	
status	installed
status_value	1
support_group	
support_group_sys_id	
type	plc
u.my_custom_field	My Custom value
vendor	Vendor E

ソース列アイコン () を選択して、そのデータマッピングフィールドを選択することもできます。
[ソース] 列にはデータピルが含まれています。

Map to Hardware 1
Last Saved: 2022-07-07 12:16:54

Map to CMDB Transform Data

Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)
From collection: object

Source Column	object.model_number_id_cleansed	
Support group	Source Column	object.support_group_sys_id
Manufacturer	Source Column	object.manufacturer_sys_id_cleansed
First discovered	Source Column	object.first_discovered_date_time_format
Class	Source Column	object.asset_cmdb_class_sys_name
Comments	Source Column	object.u.my_custom_field

22. [ETL 変換マップアシスタント] ページの [データを CMDB にマップし、関係性を追加する (Map Data to CMDB and Add Relationships)] セクションの [ソースデータをマップする **CMDB クラス (CMDB Classes to Map Source Data)**] に移動します。

Map to Hardware 1
Last Saved: 2021-10-28 13:40:03

Map to CMDB Transform Data

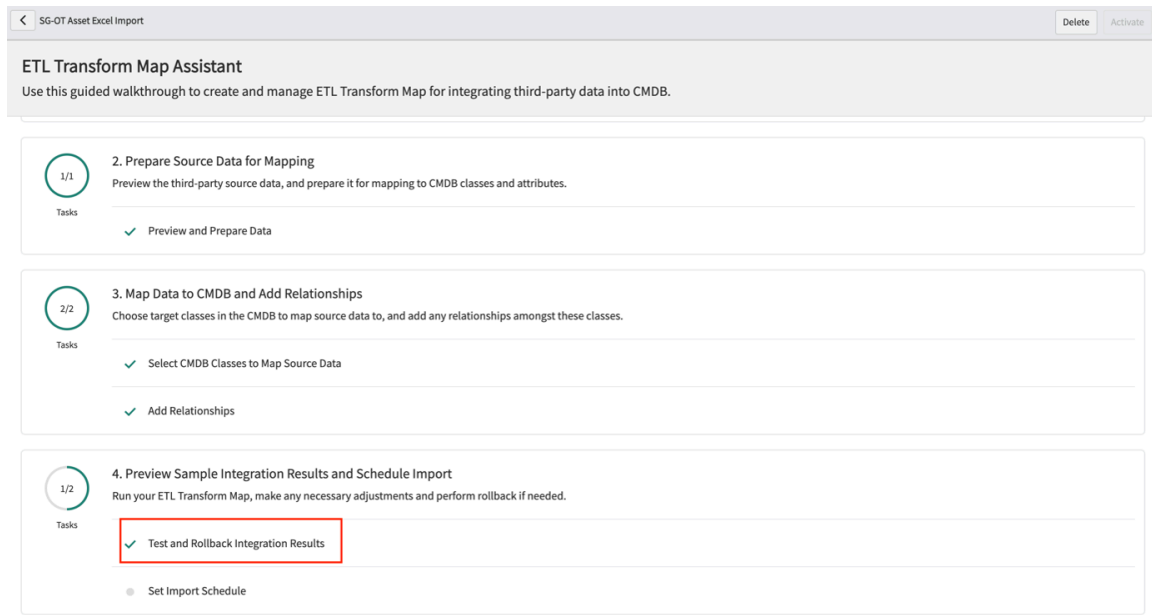
Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

Mapping to Hardware 1 (cmdb_ci_hardware)

Source Native Key	Source Column	object.id
Source Recency Timestamp	Source Column	
Name	Source Column	object.name

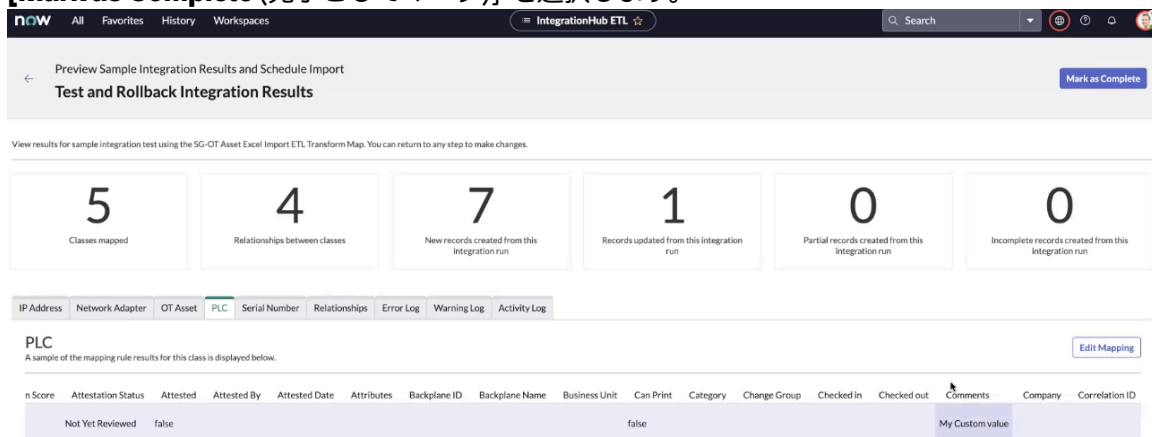
23. [Mark as Complete (完了としてマーク)] を選択します。
24. 次の手順に従って、新しいフィールドマッピングを確認します。
- ETL 変換マップアシスタントのホームページに移動します。
 - ガイド付きセットアップの [サンプル統合結果のプレビューとインポートのスケジュール] セクションで、[テストとロールバックの統合結果] を選択します。



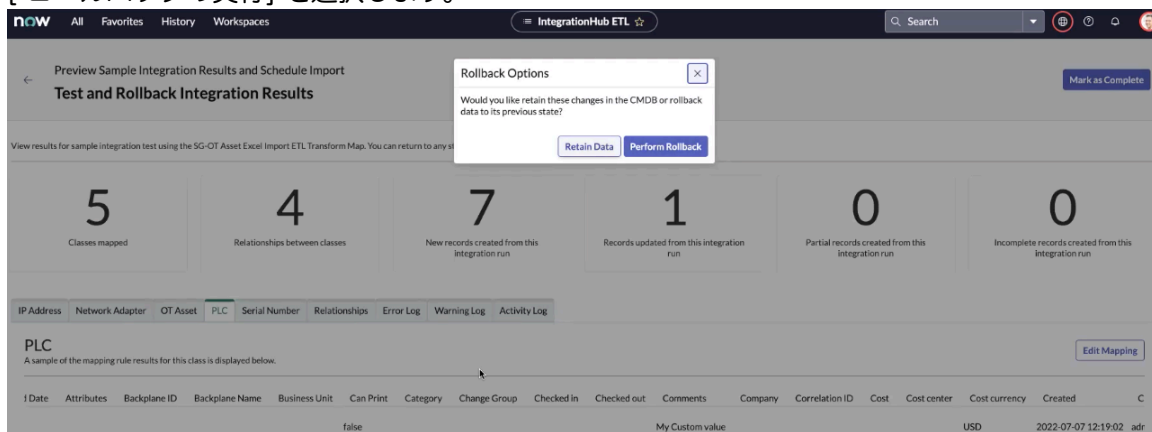
c. [**Run Integration** (統合の実行)] を選択します。

d. 実行が正常に終了したら、コメント値を指定した CI の [コメント] フィールドがステージングテーブルで更新されていることを確認します。

e. [**Mark as Complete** (完了としてマーク)] を選択します。



f. [**ロールバックの実行**] を選択します。



g. ETL がアクティブ化されていない場合は、[**アクティブ化**] を選択します。
新しい列フィールドマッピングが正常に追加され、検証されました。

デバイス分類のカスタム実装の追加

タイプ、os_version、およびfirmware_versionに基づいて、デバイスのベースシステム分類をカスタマイズします。

始める前に

sn_otsm_sgc.SGOTAssetImportExtensionPoint拡張ポイントのベースシステムは、sn_otsm_sgc.SGOTAssetImportUtil という名前のデフォルトの実装スクリプトを使用します。カスタマイズされた分類を追加するには、オペレーショナルテクノロジーのサービスグラフコネクタ (**Excel**) スコープで拡張ポイントの実装を作成します。

i 注:

ユーザーには、拡張ポイントの実装が 1 つだけが必要です。デフォルトの拡張ポイントではなくカスタム拡張ポイントを実装してアクティブ化する場合は、デフォルトの実装を非アクティブ化する必要があります。

必要なロール:cmdb_inst_admin、import_admin、import_scheduler、admin

手順

1. 移動先 すべての > システムの拡張ポイント > スクリプト化された拡張ポイント。
2. [sn_otsm_sgc.SGOTAssetImportExtensionPoint] を選択します。
3. [実装を作成] 関連リンクを選択します。
4. 拡張ポイント実装の名前を入力します。
5. [スクリプト] フィールドで、次の 2 つの関数を含むクラスオブジェクトが設定されていることを確認します。

getAssetCMDBSysClassNameWithOtEntityTypeSysId 拡張ポイントから返される結果が、コメントに記載されている形式に従っていることを確認してください。結果文字列形式を変更すると、インポートの失敗または不規則性が発生します。形式は、<cmdb class name>:::<ot entity type sys id> である必要があります。

オプション	説明
getAssetCMDBSysClassNameWithOtEntityTypeSysId(/ *string*/ type, /*string*/ osVersion, /*string*/ firmwareVersion)	このメソッドを実装して、デバイスが属する CMDB システムクラス名と、「:::」で連結された OT エンティティタイプsys_id返します。 未分類のデバイスの場合、OT デバイスタイプは ot_base に設定されます。
getComputerType(//*string*/ operatingSystem)	渡されたオペレーティングシステムに基づいて CMDB システムクラス名を返します。

6. 必要な変更をすべて行ったら、[更新] を選択します。
拡張ポイントの実装が作成されます。

次のタスク

関連リストの [実装] タブから、ベースシステム拡張ポイント実装を開いて非アクティブ化します。

デバイスのカスタム検証を追加する

OT デバイスの検証をカスタマイズします。

始める前に

sn_otsm_sgc のベースシステム。SGOTAssetCustomValidationExtensionPoint 拡張ポイントは、デフォルトの **sn_otsm_sgc** を使用します。SGOTExcelStagingAssetValidationProcessor 実装スクリプト。カスタマイズされた検証を追加するには、サービスグラフコネクタ for Operational Technology (Excel) スコープで拡張ポイントの実装を作成します。

必要なロール:cmdb_inst_admin、admin

手順

1. 移動先 すべて > システム拡張ポイント > スクリプト化済みの拡張点。
2. **[sn_otsm_sgc]** を選択します。SGOTAssetCustomValidationExtensionPoint。
3. [実装を作成] 関連リンクを選択します。
カスタム検証を追加できるスクリプトインクルードが作成されます。
4. カスタム検証を追加するには、次の検証シナリオを参照してください

	A	B	C	D	E	F	G	H	I	J
	Custom Validation									
1	Default Validation Partially Valid (sn_otsm_sgc.enable.cmdb.validations - True) Valid (sn_otsm_sgc.enable.cmdb.validations - True) Invalid (sn_otsm_sgc.enable.cmdb.validations - True) Partially Valid (sn_otsm_sgc.enable.cmdb.validations - False) Valid (sn_otsm_sgc.enable.cmdb.validations - False) Invalid (sn_otsm_sgc.enable.cmdb.validations - False) Partially Valid	Invalid (Override - False)	Valid (Override - False)	Partially Valid (Override - False)	Invalid (Override - True)	Valid (Override - True)	Partially Valid (Override - True)	No Implementation created (Override - True)	Implementation has different Name (Override - True)	Invalid state (Type) (Override - True)
2		Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
3		Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
4		invalid	invalid	invalid	invalid	Invalid	invalid	Invalid	Invalid	Same as Default state
5		Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
6		Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
7		invalid	invalid	invalid	invalid	Invalid	invalid	Invalid	Invalid	Same as Default state
8										

い。

5. [更新] を選択します。

Excel サービスグラフ コネクタをテストする

トラブルシューティングのアクションは、オペレーショナルテクノロジー デバイスまたはデータをインポートする際の一般的な問題の解決に役立ちます。システムログにアクセスして、これらのエラーのトラブルシューティングを行います。

これらのログは、問題をデバッグしたり、SGC ステップが適切に実行されていることを確認したりするために使用できます。

問題	ソリューション
SG-OT デバイスのデータのロード中に問題が発生した場合 Excel ETL ガイド付きセットアップで ETL をインポート	[関連リンク] リストから、データのロードを試みます。 1. SG-OT Excel インポートデータソースに移動し、[20 件のレコードのテストロード] または [すべてのレコードのロード] を選択します。 2. ETL に戻り、データのロードを再試行してください。
ETL ガイド付きセットアップから サービスグラフ コネクタをテスト実行した後、[部分的ペイロード] タブにエントリがある場合	次の条件が原因です。 • デバイスの必須フィールドの値がありません。 • 親デバイスが関連付けられていないコントロールモジュール - デバイスのタイプとコン

問題	ソリューション
	トロールモジュールの親 ID フィールドがステージングテーブルに正しく入力されていることを確認します。
ETL ガイド付きセットアップから サービスグラフ コネクタをテスト実行した後、[不完全なペイロード] タブにエントリがある場合	デバイスを識別するために一意に使用されるフィールドの値が欠落しているため。
Easy Import を実行した後、現在の実行からインポートされたレコードが表示される場合があります。検証が実行されると、現在のインポート実行のレコードだけでなく、ステージングテーブルのすべてのレコードで実行されます。	検証を実行する前に、ステージングテーブルのリストビューのパンくずリストで [すべて] をクリックする必要があります。
ステージングテーブルでタイムスタンプ列が空で表示される場合	ユーザーは UTC 形式 (YYYY-MM-DD hh:mm:ss) を使用して日付と時刻を入力する必要があります。
[検証を実行] ボタンをクリックした後、レコードの検証ステータスの更新が表示されない場合。	ユーザーは手動でページを更新する必要があります。
ユーザーがステージングテーブルのレコードの既存のデータを変更した場合、検証ステータスは [検証保留中] に設定されません。	次の属性が変更されると、検証ステータスは [検証保留中] に設定されます。 - 識別子フィールド (Mac アドレス (1-9)) - シリアル番号 - 名前 - 相関 ID - タイプ - コントロールモジュール親相関 ID - 変換済みの名前の計算で使用されるフィールド - ラック番号 - スロット番号 システムプロパティの詳細については、「 SG-OT デバイスの Excel インポート処理に影響を与えるシステムプロパティ 」を参照してください。
レコードがステージングテーブルにインポートされた後、変換済みの名前の計算に関連するシステムプロパティで行われた更新は、ステージングテーブルレコードには反映されません。	データをステージングテーブルにインポートする前に、システムプロパティを変更します。
ユーザーが少数のレコードを選択して [検証を実行] をクリックしたときに複数のエラーバナーが表示される場合。	検証は、ステージングテーブルで利用可能なすべてのレコードに対して実行されます。 検証対象として単一のレコードを選択しないでください。

問題	ソリューション
重複レコードが CMDB に存在する場合、ステージングテーブルはそれを重複として検出しません。	検証は、ステージングテーブルで使用可能なデータに対してのみ実行されます。 利用可能なデータの CMDB に対して検証は実行されません。
サイト名はスプレッドシートまたはステージングテーブルで提供されますが、スプレッドシートのインポート後は OT デバイスに表示されません。	CMDB 内の既存のサイトレコードのみが考慮されます。 サイトのentity_name (ISA 設備階層モデルエンティティ) は、Excel テーブルまたはステージングテーブルのサイト列に指定された値と一致する必要があります。 サイトのentity_nameが一致しない場合、値は空に設定されます。
ユーザーがデータソースで [すべての レコードをロード] をクリックしても、レコードはインポートセットにインポートされません。	ステージングテーブルに利用可能なレコードがありません。 レコードはステージングテーブルに存在しますが、レコードのステータスが [有効] または [部分的に有効] ではありません。 で Excel SGC に関連するすべてのログにアクセスする > システムログ > システムログ > すべて. [メッセージ] 列で文字列 SGOTExcel を検索します。

サービスグラフ コネクタで使用するスクリプトインクルードを表示します

アドミンとして、サービスグラフ コネクタに関連するスクリプトインクルードを表示します。

始める前に

サービスグラフ コネクターで使用するすべてのスクリプトのフィルター済みリストを表示します。

必要なロール:cmdb_ot_admin、cmdb_inst_admin、または admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT Manager (OT マネージャー) > OT デバイスのインポート：スクリプトインクルード。**
このリストには、名前が SGOTAsset または SGOTExcelStaging で始まるレコードが表示されます。
2. スクリプトのリストを表示します。

サービスグラフコネクタで使用するシステムプロパティにアクセスします

アドミンとして、サービスグラフ Connector に関連するシステムプロパティを表示します。

始める前に

サービスグラフ コネクターで使用するすべてのスクリプトのフィルター済みリストを表示します。

必要なロール:admin、cmdb_inst_admin、または cmdb_ot_admin

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > **OT** マネージャーアドミン > **OT** デバイスのインポート：システムプロパティ。
リストには、名前が **sn_otsm_sgc.excel** で始まるレコードが表示されます。
2. スクリプトのリストを表示します。

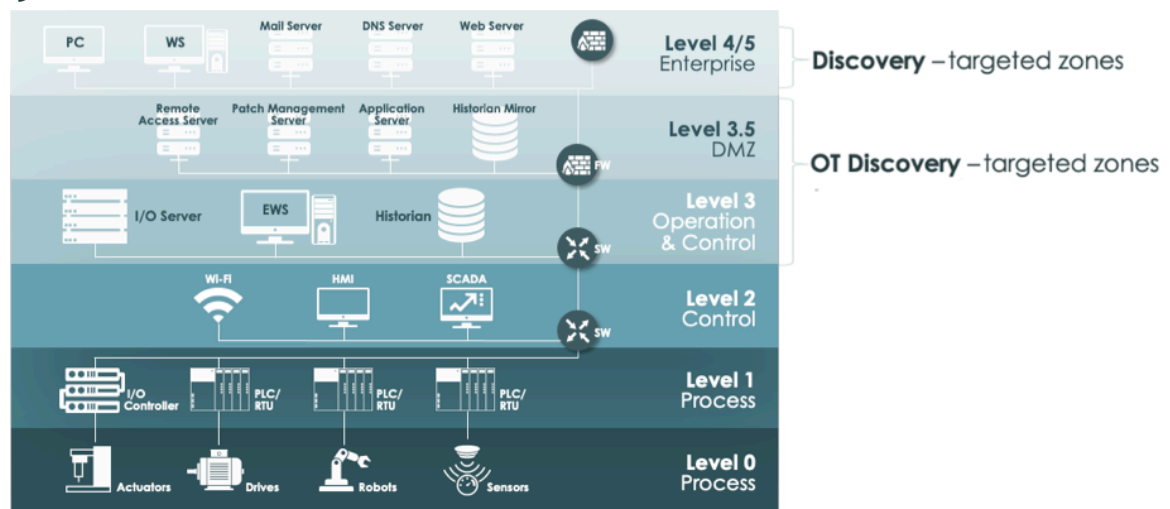
オペレーショナルテクノロジー のディスカバリー

ディスカバリー for オペレーショナルテクノロジー 機能を実行して、産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルにある IT クラス オペレーショナルテクノロジー (OT) デバイスを検出できます。IT クラスアイテムには、データセンターと工場の両方に存在するスイッチ、ルーター、およびコンピューターが含まれます。

標準的な ディスカバリー 処理が行われる場所

オペレーショナルテクノロジープロセスのディスカバリーは、標準のディスカバリープロセスと同様に動作します。

標準およびターゲットの **Purdue** レベル オペレーショナルテクノロジー ディスカバリー



Now Platform での標準的なディスカバリー処理は、通常、企業内の次の Purdue レベルで行われます。

処理済み **Purdue** レベル

Purdue レベル	Description (説明)
4	すべての情報技術 (IT) 機能など、サイトのビジネスとロジスティクス。
5	エンタープライズネットワーク:エンタープライズリソースプランニング (ERP) 機能が実行されます。



注:

産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。

オペレーショナルテクノロジー処理のディスカバリーが行われる場所と方法

対照的に、オペレーショナルテクノロジー処理のディスカバリーは、OT ディスカバリースケジュールの作成時に選択したレベルに応じて、次の Purdue レベルで実行できます。

処理済み Purdue レベル

Purdue レベル	Description (説明)
3.5	非武装地帯 (DMZ) または産業非武装地帯 (IDMZ)。従来の(IT)DMZと同様に、OT 指向の IDMZを使用すると、さまざまなセキュリティ要件を持つネットワークを安全に接続できます。
3	プラントまたはサイト全体の制御および監視機能が存在するサイトオペレーション。

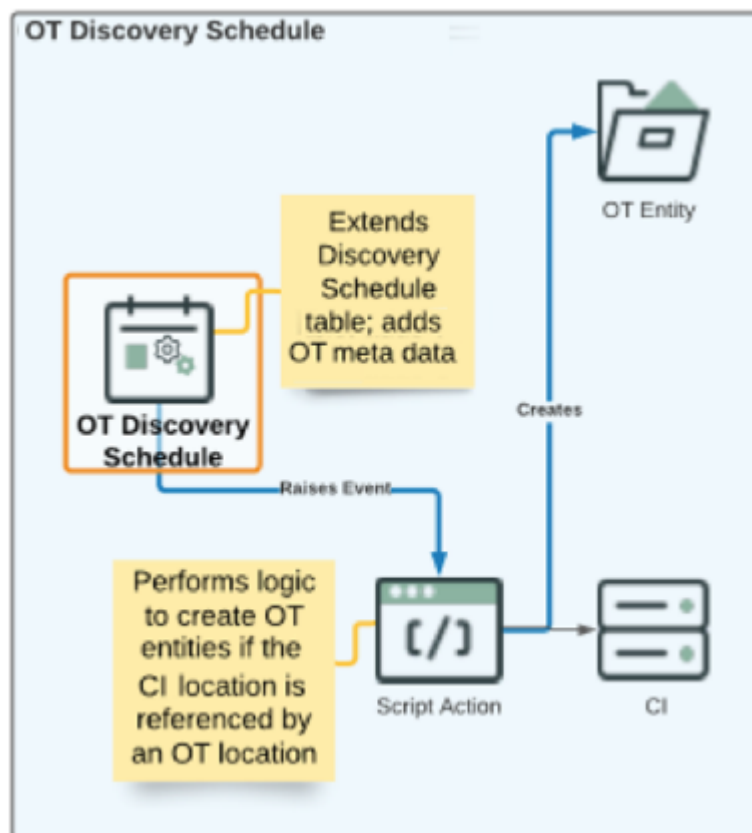
通常、ディスカバリー for オペレーショナルテクノロジー は ICS ネットワークの DMZ (または IDMZ、Purdue Level 3.5) で実行します。この Purdue レベルでは、通常、検出および管理する IT および OT クラスのコンピューターとサーバーがあります。



注:

産業オペレーションが中断される可能性を回避するには、ICS ネットワークで Purdue レベル 0 から 2 に対してディスカバリー プロセスを実行しないでください。

ディスカバリーオペレーショナルテクノロジー処理用



OT ディスカバリースケジュールを実行すると、次の処理が実行されます。

1. 割り当てられた IP アドレスを処理し、その中に存在するすべてのハードウェアアイテムを検出します。
2. 構成アイテム (CI) の検出が完了すると、内部で (discovery.device.complete) イベントがトリガーされます。このロジックは、OT エンティティ (cmdb_ot_entity) レコードが 構成管理データベース (CMDB)内に存在するかどうかを確認します。
 - 存在し、検出されたアイテムの関連属性が変更されている場合は、その CI に関連する OT エンティティが更新されます。
 - 存在しない場合は、作成されます。
3. 場所属性に加えて、定義された属性を OT ディスカバリースケジュールから CI および関連する OT エンティティレコードにプッシュします。
4. また、検出された OT デバイスにインストールされているアプリケーションの OT エンティティレコードも作成されます。OT ディスカバリーを通じて作成された OT エンティティレコードを持つアプリケーションを表示するには、Industrial Workspace リストビューに移動し、**[Operational Technology (OT) (オペレーショナルテクノロジー (OT))]** の下にある **[Applications (アプリケーション)]** リストを開きます。

関連情報

[運用技術 \(OT\) 拡張クラス](#)

[MID サーバー](#)

[ディスカバリー](#)

[プローブとセンサーを使用した水平ディスカバリープロセスフロー](#)

[水平検出のスケジュール](#)

ディスカバリー関連リンクとリストオペレーショナルテクノロジー

ディスカバリーオペレーショナルテクノロジーには、いくつかの関連リンクとリストが含まれています。

関連リンク

関連リンク	Description (説明)
クイック範囲	OT ディスカバリースケジュールの実行時にスキャンする IP アドレスとアドレス範囲。複数の形式 (ネットワーク、範囲、またはリスト) の IP アドレスをカンマ区切りの 1 つの文字列で入力します。使用中の MID サーバーは、指定された IP 範囲に接続する必要があります。 詳細については、「 ディスカバリースケジュールのクイック IP 範囲の作成 」を参照してください。
ディスカバリー 今	オペレーショナルテクノロジープロセスのディスカバリーをすぐに実行します。
Run Point Scan (ポイントスキャンを実行)	[ポイントスキャンを実行]ダイアログにアクセスします。詳細については、「 ポイントスキャンの実行 」をご参照ください。

関連リスト

関連リスト	Description (説明)
ディスカバリー IP 範囲	ディスカバリー スキャンおよび検出する IP アドレスとアドレス範囲。簡易 CI スキャン (動作なし) を使用している場合は、この関連リストを使用してこれらの IP アドレスを定義します。使用中の MID サーバーは、指定された IP 範囲に接続する必要があります。 注: セキュリティを強化するために、ディスカバリーターゲットの範囲を制限して不要なネットワークとデバイスを除外します。
ディスカバリー 範囲セット	OT ディスカバリースケジュールが 1 つ以上の Shazzam プローブを使用してスキャンする各範囲セットの定義。
ディスカバリー ステータス	現在および過去の OT ディスカバリースケジュールの実行結果の履歴。

関連情報

[MID サーバー](#)

[Shazzam プローブ、ポートプローブ、およびプロトコル](#)

[Shazzam プローブの作成](#)

オペレーショナルテクノロジーディスカバリースケジュールを作成し、ディスカバリープロセスを実行します

OT 機能のディスカバリーを実行する方法とタイミングを調整するオペレーショナルテクノロジー (OT) ディスカバリースケジュールを定義します。また、クイック ディスカバリー を即座に実行することも、実際に OT ディスカバリー を実行することもできます。

始める前に

ディスカバリー for オペレーショナルテクノロジー を実行する前に、次のアクションを実行します。

- 標準の ディスカバリー アプリケーションをインストールして構成します。詳細については、「[ディスカバリーのセットアップ](#)」を参照してください。
- CMDB CI クラスモデルプラグインをインストールします。詳細については、「[オペレーショナルテクノロジー \(OT\) 拡張クラスのインストール](#)」を参照してください。
- MID サーバーをインストールします。詳細については、「[MID サーバーのインストール](#)」を参照してください。

必要なロール:ot_discovery_admin

手順

- 移動先 すべて > **OT** ディスカバリー > **OT** ディスカバリースケジュール。
- クイック ディスカバリーを実行するか、OT ディスカバリースケジュールを選択または作成します。

3. フォームの [OT ディスカバリースケジュール] フィールドに入力します。
このフォームのほとんどのフィールドは、標準のディスカバリーフォームと同じか、同じように動作します。このトピックには、標準のディスカバリースケジュールとは異なるフィールドのみが表示されます。残りのフィールドの詳細については、「[水平ディスカバリーのスケジュール](#)」を参照してください
4. ディスカバリープロセスをすぐに実行するか、OT ディスカバリースケジュールを保存してレコードで指定した時間に実行します。

タスクの結果

オペレーショナルテクノロジープロセスのディスカバリーが実行されると、[ディスカバリースタタス] 関連リストに履歴レコードが作成されます。

インポートまたは検出後に **OT** デバイスを編集または表示する

オペレーショナルテクノロジー (OT) メニューのオプションを使用して、エンタープライズ内の OT デバイスの詳細情報を編集または表示します。

始める前に

次のいずれかの方法で、オペレーショナルテクノロジー デバイスデータをインポートします。

- オペレーショナルテクノロジー認定の サービスグラフ コネクタである 統合ハブ 抽出変換ロード (ETL) で Microsoft Excel スプレッドシートテンプレートを使用します。詳細については、「[スケーリングテーブルを使用した Microsoft Excel スプレッドシートのインポート](#)」を参照してください。
- オペレーショナルテクノロジーのディスカバリーを実行します。詳細については、「[オペレーショナルテクノロジーのディスカバリー](#)」を参照してください。
- ServiceNow Store の オペレーショナルテクノロジー 認定 サービスグラフ コネクタを使用します。

必要なロール:cmdb_ot_viewer、cmdb_ot_editor、cmdb_ot_admin、または admin

このタスクについて

cmdb_ot_viewerロールが割り当てられている場合は、OT デバイスのみを表示できます。cmdb_ot_editorまたはcmdb_ot_adminロールがアサインされている場合は、次の方法で OT デバイスレコードを編集できます。

- Now Platform で OT デバイスレコードを個別に編集します。
- 産業用 ワークスペースリストビューから複数の OT デバイスレコードを一括編集します。

手順

1. 1 つの OT デバイスレコード Now Platformを編集するには、次の手順に従います。
 - a. 移動先 **すべて > オペレーショナルテクノロジー (OT)** をクリックし、次のいずれかのメニュー項目を選択します。
 - すべての OT デバイス
 - デフォルトでは、このリストにはコントロールモジュールは含まれません。
 - IP アドレス別のすべての OT デバイス
 - [IP アドレス別のすべての OT デバイス] リストを表示するときは、次の点に注意してください。

- 複数の IP アドレスを持つ OT デバイスは、割り当てられた IP アドレスごとに 1 回表示されます。
- OT デバイスの名前を選択して、OT デバイスレコードを開きます。レコードに表示されている IP アドレスを選択すると、IP アドレスのみのレコードが開きます。
- このリストから新しい OT デバイスレコードを作成することはできません。

OT コントロールシステム

デフォルトでは、このリストにはコントロールモジュールは含まれません。

モジュール付き OT コントロールモジュール

モジュール付き OT コントロールシステムリストを表示するときは、次の点に注意してください。

- リストビューには、親制御システム別にグループ化されたすべての制御モジュールが表示されます。
- このリストから新しい OT デバイスレコードを作成することはできません。

b. [OT デバイス] 列で、編集する OT デバイスを選択します。

c. フォームのフィールドに入力します。

d. [更新] をクリックします。

2. 複数の OT デバイスレコード 産業用 ワークスペース一括編集するには、次の手順に従います。

a. 移動先 すべて > Industrial Workspace (産業用ワークスペース).

b. リスト ( ビューを開き、[オペレーショナルテクノロジー (OT)] で利用可能な次のいずれかのリストを選択します。

- OT 監督システム
- OT コントロールシステム
- OT フィールドデバイス
- OT コンピューターおよびサーバー
- OT ネットワーク機器
- 産業用 IoT (IIoT)
- 未分類の OT デバイス

c. 編集する各 OT デバイスの横にあるチェックボックスをオンにします。

i 注:

一括編集できるのは、同じ [クラス] フィールドを持つ OT デバイスのみです。クラスが異なる OT デバイスに一括編集機能を使用することはできません。

d. 構成アイテム (CI) フィールドを編集するには、[編集] ボタンを選択し、必要に応じてフォームフィールドを編集しま

 **OT Supervisory Systems** 24

Last refreshed 21m ago

     **Edit (7)**  **Export**

す。

i 注:

CI フィールドを一括編集できるレコードの最大数は、1 ページに表示されるレコード数です。

e. [更新] をクリックします。

f. OT デバイスの詳細を編集するには、[OT の詳細を編集] ボタンを選択し、必要に応じてフォームフィールドを編集します。

OT Supervisory Systems 24
Last refreshed 22m ago



注:

OT の詳細の一括編集はバックグラウンドジョブであり、完了するまでに時間がかかる場合があります。バックグラウンドジョブがビジー状態の場合、他の OT デバイスレコードを一括編集することはできません。

OT デバイスの関連アイテムと関連リスト

[すべての OT デバイス]、[IP アドレス別のすべての OT デバイス]、および [CI 別のすべての OT デバイス] メニューオプションには、いくつかの関連アイテムとリストが含まれています。

関連アイテム

このセクションには、この OT デバイスに関連付けられている関連アイテムまたは従属アイテムが一覧表示されます。

注:

すべての OT デバイスに次の関連リストが表示されるわけではありません。オペレーショナルテクノロジークラスまたは拡張クラスの OT デバイスの場合、次の関連リストが表示されません。Windows Server など、別のハードウェアクラスに分類された OT デバイスの場合、インスタンスアドミンは関連リストをフォームに追加する必要があります。

1. 関連レコードを表示するには、関連アイテムの名前 (メモリーモジュールなど) をクリックします。
2. この OT デバイスの構成アイテム (CI) 関係を追加するには、CI 関係の追加アイコン (CI  アイコン) をクリックします。検索フィールドを使用して、関係を作成する CI アイテムを検索します。
3. [依存関係ビュー] フォームにアクセスして OT デバイスの関係を図で表示するには、依存関係ビューを表示アイコン () をクリックします。
4. 関連アイテムの表示方法とフィルタリング方法を制御する設定を変更するには、設定アイコン ()

OT デバイス関連リスト

関連リスト	Description (説明)
IP アドレス	OT デバイスに関連付けられている IP アドレス、IP バージョン、ネットマスク、NIC 番号、および構成アイテム。
ネットワークアダプタ	名前、MAC アドレス、IP アドレス、ネットマスク、MAC メーカー、および動的ホスト構成プロトコル (DHCP) 対応インジケータ。これには、OT デバイスに関連付けられているネットワークアダプターのステータスが含まれます。
シリアル番号	OT デバイスに関連付けられているシリアル番号、有効性インジケータ、シリアル番号タイプ。
機器モデルエンティティ	OT デバイスによって自動化される機器モデルエンティティ。

OT デバイス関連リスト (続く)

関連リスト	Description (説明)
OT コントロールモジュール	タイプが OT コントロールシステムまたは拡張クラス (PLC など) の OT デバイスに関連付けられているコントロールモジュール。 表示される OT コントロールシステムレコードと「Owned by: Owns」関係を持つ各 OT コントロールモジュール。 プラットフォームで、ユーザーは OT コントロールモジュールを作成できます。 [モジュールタイプ] フィールドに応じて、次の入力/出力値から選択できます。 • なし • ローカル • リモート • Distributed
CMDB 360	CMDB 360 [cmdb_multisource_data] テーブル内の関連する CMDB 360 データ。
メモリモジュール	OT デバイスに関連付けられているメモリモジュールのシリアル番号、有効性インジケーター、シリアル番号タイプ。
インストールされているソフトウェア	OT デバイスにインストールされているアプリケーションソフトウェア (存在する場合)。
OT 脆弱性一致アイテム	OT デバイスに関連付けられている脆弱性一致アイテム。
OT インシデント	OT デバイスに関連付けられている OT インシデント。
OT 変更要求	OT デバイスに関連付けられている OT 変更要求。
外部システムメタデータ	ソースシステム内のデバイスの URL、ディスカバリーソース、および CI に関連付けられている更新済みデバイス。 URL は、サービスグラフコネクタを介してソースシステムによって自動的に入力されます。
OT プロトコル	これは、プロトコルコンバータクラスに適用されます。 プロトコルコンバータクラスに関連付けられているプロトコル、説明、ベンダー、およびバージョン。
バックアップ情報	現在の CI に関連付けられているバックアップ情報オブジェクト。

オペレーショナルテクノロジーデバイスフォーム

オペレーショナルテクノロジー (OT) デバイスフォームを使用して、企業内の OT デバイスの詳細情報を編集します。

オペレーショナルテクノロジーデバイスフォーム

Field (フィールド)	Description (説明)
OT 表示名	レコードに表示される OT デバイスの名前。 i 注: このフィールドには任意の文字列値を追加できます。複数のデバイスに同じ OT 表示名を付けることができます。これは OT デバイスを理解しやすくするためのものであり、ステージングテーブルから OT デバイスをインポートするときに生成される一意の CI 名とは異なります。
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で再生する機能でもあります。例： サーバーなどの IT デバイスは OT デバイスに変換でき、ネットワーク上で IT デバイスが果たす機能は HMI です。したがって、そのクラスはサーバーであり、そのデバイスタイプは HMI です。 i 注: 場合によっては、OT 機能のない OT デバイスや、デバイスタイプが不明な OT デバイスがあります。OT 機能のない OT デバイスの場合は、[OT 機能なし] を選択します。デバイスタイプが不明な OT デバイスの場合は、[不明] を選択します。
デバイスの重要度	デバイスの故障のサイトプロセスに対する相対リスクの測定値。例： • 1：最重要 • 4：重要ではない
サイト	デバイスが配置または割り当てられている最上位の親エンティティ、または産業サイト。
Purdue レベル	アサインされた Purdue レベル。範囲は 0 から 5 です。

オペレーショナルテクノロジーデバイスフォーム (続く)

Field (フィールド)	Description (説明)
	i 注: 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
ゾーン	デバイスが割り当てられているサイトの場所内のエリア。
クラス	OT デバイスにアサインされたクラスの名前。 i 注: CI クラスのリストと説明については、「オペレーションテクノロジー (OT) 拡張クラス」を参照してください。
ステータス	OT デバイスのステータス: -- なし -- アサイン済みステータスはありません。 不在 OT デバイスが施設にありません。 In Maintenance (メンテナンス中) OT デバイスはメンテナンス中で、現在はオフラインです。 In stock (在庫あり) OT デバイスの在庫が施設にあります。 インストール日時 OT デバイスが施設にインストールされています。 インストール待ち OT デバイスが施設へのインストールを保留しています。 修理待ち OT デバイスは修理待ちですが、まだオンラインではありません。 Retired (廃止) OT デバイスは廃止されました。 Stolen (盗難)

オペレーショナルテクノロジーデバイスフォーム (続く)

Field (フィールド)	Description (説明)
	OT デバイスが盗まれました。
ディスカバリー 源	OT デバイスデータの ディスカバリー ソース。たとえば、統合ハブ ETL を使用して Microsoft Excel スプレッドシートから OT デバイスをインポートした場合は、SG-OT Excel インポートです。詳細については、「 サービスグラフオペレーショナルテクノロジー用コネクタ (Excel) 」を参照してください。
インフラストラクチャ関係	OT デバイスと他の OT デバイスおよび機器モデルエンティティとの関係を表示します。
サービス関係	OT デバイスと機器モデルエンティティの関係を表示します。
CI タイムライン	OT デバイスに関連付けられた OT インシデント、OT 変更、監査履歴のタイムラインを表示します。
次のフィールドは、プログラマブルロジックコントローラー (PLC) クラスレコードにのみ適用されます。	
キースイッチ	キースイッチモード: - リモートモード PLCの設定を変更できます。 - ローカルモード デフォルトモードでは、PLCの構成を変更することはできません。
スイッチ位置	PLCのスイッチ位置には、次の位置があります。 • 実行 • プログラム • リモート • 停止 • テスト デフォルトでは、スイッチの位置は [なし] に設定されています。 スイッチ位置が リモートに設定されている場合、スイッチリモートモードが有効になります。
スイッチリモートモード	PLCのスイッチリモコンには、次のモードがあります。 • 実行 • プログラム

オペレーショナルテクノロジーデバイスフォーム (続く)

Field (フィールド)	Description (説明)
	• テスト • なし
資産	構成管理データベース (CMDB)に構成アイテム (CI) が作成されると、資産レコードが作成されます。資産レコードには、CI のモデルカテゴリが含まれています。オペレーショナルテクノロジー (OT) のモデル カテゴリの詳細については、「のモデルカテゴリ オペレーショナルテクノロジー」を参照してください。OT デバイスのモデルカテゴリを表示するには、次の手順を実行します。 1. 移動先 すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス. 2. 資産レコードを表示する OT デバイスを選択します。 3. [Asset (資産)] フィールドの横の [Preview this record ()] を選択します。 4. [レコードを開く (Open Record)] を選択します。

OT プロトコルを作成する

OT プロトコルテーブルは、名前、バージョンなど、ベンダー固有のプロトコルであるかどうかなど、プロトコルに関連する情報をユーザーがキャプチャするのに役立ちます。プロトコルは、産業用ネットワークに接続されたさまざまなデバイス間の通信媒体です。

始める前に

必要なロール:OT_admin および admin

手順

1. 移動先 **すべて > オペレーショナルテクノロジー (OT) > OT プロトコル**.
2. [OT プロトコル] ページで、[**新規**] をクリックします。
3. OT プロトコルフォームのフィールドに入力します。
4. プロトコルがベンダー固有のプロトコルである場合は、[**ベンダー固有**] チェックボックスをオンにします。
5. [送信] をクリックします。

OT プロトコルをプロトコルコンバーター CI にマッピングする

オペレーショナルテクノロジー (OT) プロトコルを産業用 ワークスペース内のプロトコルコンバーター構成アイテム (CI) に関連付けます。

始める前に

必要なロール:cmdb_ot_editor

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース) をクリックし、産業用 ワークスペース リストビューを開きます。
2. [すべての **OT** デバイス] リストで、プロトコルコンバーターレコードを選択します。
3. レコードで、[関連レコード] タブを選択します。
4. [OT プロトコル] 関連リストを選択します。
5. [追加] を選択します。
6. プロトコル コンバーター レコードに追加するプロトコルを選択し、[追加] をクリックします。プロトコルが関連リストに追加されます。
7. オプション: 関連リストからプロトコルレコードを削除するには、削除するレコードを選択して [**Remove** (削除)] をクリックします。

IT ハードウェアデバイスを **OT** デバイスに変換する

OT ネットワークに属する IT ハードウェアデバイスを特定したら、これらの IT 構成アイテム (CI) を OT デバイスに変換できます。

始める前に

必要なロール:cmdb_ot_admin または admin

このタスクについて

このタスクは、すべての IT ハードウェアデバイスに適用されます。

手順

1. IT CI を選択します。
たとえば、 **すべて > 構成 > ベースアイテム > コンピューター**。
2. OT デバイスに変換する IT ハードウェアデバイスを選択します。
3. [関連リンク] モジュールで、[**OT** デバイスの詳細を追加] を選択します。
[OT デバイス] フォームが表示されます。
4. OT デバイスの詳細フォームのフィールドに入力します。
5. [更新] を選択します。
6. 変換された OT デバイスを表示するには、 **すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス**。

タスクの結果

選択した IT ハードウェアデバイスが OT デバイスに変換されました。

または、複数の IT ハードウェアデバイスを選択し、一括編集で OT デバイスに変換することもできます。詳細については、「[一括編集で IT ハードウェアを OT デバイスに変換する](#)」を参照してください。

一括編集で IT ハードウェアを **OT** デバイスに変換する

複数の IT ハードウェアデバイスを選択し、一括編集でそれらを OT デバイスに変換すると、レコードをより迅速かつ効率的に編集できます。

始める前に

必要なロール:cmdb_ot_admin または admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > Industrial Workspace** (産業用ワークスペース).
2. 産業用 ワークスペースで、[すべての IT ハードウェア] リストに移動します。
3. オプション: [すべての IT ハードウェア] リストをフィルタリングする場合は、次のアクションを実行します。
 - リストの右上隅にあるフィルター 
 - リストに適用するフィルターを追加します。
 - [更新] を選択します。
4. 変換する各 IT ハードウェアデバイスの横にあるチェックボックスをオンにします。
リスト内のすべての IT ハードウェア デバイスを選択する場合は、[名前] 列の横にあるチェックボックスをオンにします。
5. [**Convert to OT devices** (OT デバイスに変換)] ボタンを選択します。
6. フォームのフィールドに入力します。

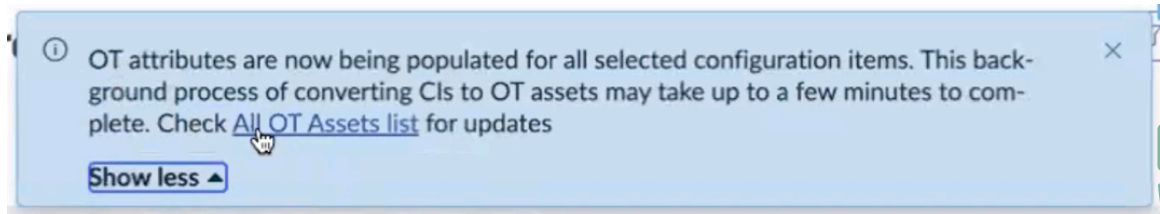
OT デバイスへの変換フォーム

Field (フィールド)	Description (説明)
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で再生する機能でもあります。例： サーバーなどの IT デバイスは OT デバイスに変換でき、ネットワーク上で IT デバイスが果たす機能は HMI です。したがって、そのクラスはサーバー であり、そのデバイスタイプは HMI です。 注: 場合によっては、OT 機能のない OT デバイスや、デバイスタイプが不明な OT デバイスがあります。OT 機能のない OT デバイスの場合は、[OT 機能なし] を選択します。デバイスタイプが不明な OT デバイスの場合は、[不明] を選択します。
デバイスの重要度	デバイスに障害が発生した場合のサイトプロセスへの相対リスクの測定: ○ 1：最重要 ○ 4：重要ではない
Purdue レベル	アサインされた Purdue レベル。レベル範囲は 0 から 5 です。

Field (フィールド)	Description (説明)
	注: 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
ゾーン	デバイスが割り当てられているサイトの場所内のエリア。
サイト	デバイスが配置または割り当てられている最上位の親エンティティ、または産業サイト。

7. [変換] を選択します。

プロセスが開始されたことを知らせる次のバナーが表示されます。[すべての OT デバイス] リストで更新を確認するには、バナー内のリンクを選択します。



タスクの結果

選択した IT ハードウェアデバイスが OT デバイスに変換されました。

IT を OT に再アサインするための一括更新ルールセット機能を使用して、IT ハードウェアを OT デバイスに自動的に変換するスケジュール済みジョブを作成することもできます。詳細については、「[IT レコードを OT デバイスに自動的に変換する](#)」を参照してください。

OT デバイスを一括編集で IT ハードウェアデバイスに変換する

オペレーショナルテクノロジー (OT) デバイスを一括編集して、OT デバイスの詳細を削除します。次に、OT デバイスを IT ハードウェアデバイスに変換します。

始める前に

必要なロール:cmdb_ot_admin または admin

このタスクについて

OT 機能がなく、IT ハードウェアデバイスとして分類する必要がある OT デバイスに遭遇した場合は、複数の OT デバイスを一括編集で選択して編集し、IT ハードウェアデバイスに変換できます。

手順

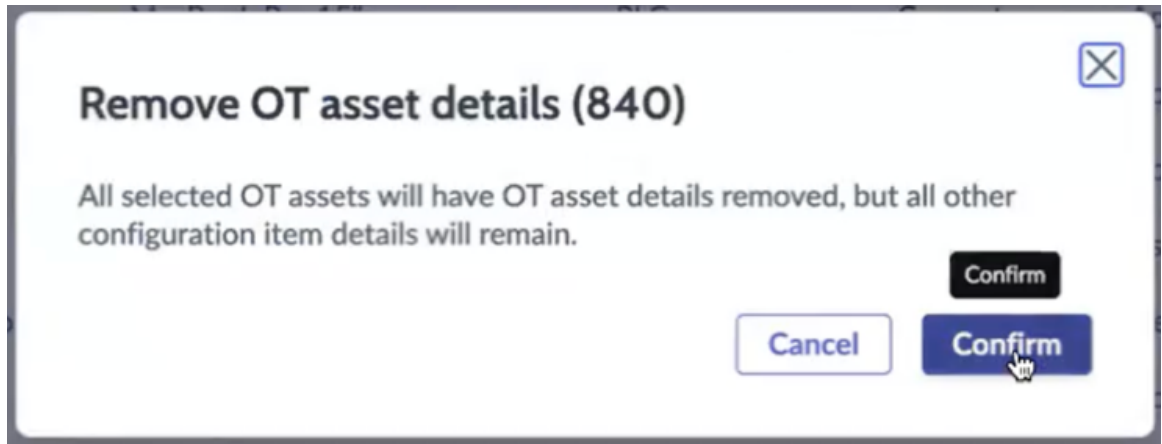
1. 移動先 **すべて > 産業用ワークスペースアドミン > Industrial Workspace**
2. Industrial ワークスペース の [All OT Devices (すべての OT デバイス)] リストビューに移動します。
3. IT ハードウェアデバイスに変換する OT デバイスを選択します。
リスト内のすべての OT デバイスを選択する場合は、[OT デバイス] 列の横にあるチェックボックスをオンにします。

4. [Remove OT device details (OT デバイスの詳細を削除)] ボタンを選択します。

OT デバイスの詳細を削除し、他のすべての構成アイテム (CI) の詳細を保持することを確認するダイアログ ボックスが表示されます。

注:

CI の詳細、ネットワークアダプター、または IP アドレスは削除されません。OT 固有のデータのみが削除されます。



5. [確認] を選択します。

タスクの結果

選択した OT デバイスから OT デバイスの詳細が削除され、OT デバイスが IT ハードウェアデバイスに変換されます。これらの IT ハードウェアデバイスは、Industrial Workspace の IT ハードウェアリストビューで表示できます。

IP アドレスを OT デバイ스에 マッピングする

SyncIPAddressToOT スケジュール済みジョブを使用して、利用可能なすべての OT デバイスの IP アドレス情報を更新および同期できます。SyncIPAddressToOT スケジュール済みジョブは、IP アドレス (cmdb_ci_ip_address) テーブルから IP アドレス情報を取得し、CI の IP アドレスフィールドに追加します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > スケジュール済みジョブ**.
2. [スケジュール済みジョブ] ページで、検索フィルターに「SyncIPAddressToOT」と入力し、Enter キーを押してスケジュール済みジョブを検索します。
3. [SyncIPAddressToOT] を選択します。
4. [Scheduled Script ExecutionSyncIPAddressToOT] ページで、[**Execute Now**] を選択します。

ネットワーク侵入検知システムアプライアンスの管理

cmdb_nids_admin または admin ロールを持っている場合は、Now Platformの NIDS メニューからネットワーク侵入検知システム (NIDS) クラスレコードにメタデータ属性を割り当てることができます。

ネットワーク侵入検知システムは、サポートされている統合からの IT および OT デバイスのインポートを管理するのに役立ちます。場所や NIDS ネットワークタイプなどのメタデータを NIDS レ

コードに割り当てると、検出された OT デバイスと IT デバイスを区別し、関連するメタデータが作成されたレコードに自動的に追加されます。cmdb_nids_admin または admin ロールを持つユーザーは、[**NIDS** にアサインされたメタデータ (**NIDS Assigned Meta Data**)] タブを編集し、アクティビティストリームでユーザーが行った変更を表示できます。

i 注:

テーブル内の NIDS レコードの手動作成は、レコードのリストビューまたはフォームビューから制限されます。

NIDS クラスレコードについて詳しくは、[ネットワーク侵入検知システム \(NIDS\) CI 拡張クラス](#) を参照してください。

NIDS レコードの [検証済み] フィールドが true に設定されている場合、NIDS フォームで NIDS の以下の属性のいずれかが変更されると、警告メッセージが表示されます。

- NIDS ネットワークタイプ
- NIDS ソース名
- NIDS ソース ID

detects::detected by 関係を持つ NIDS レコードが削除されると、警告メッセージが表示されます。

ネットワーク侵入検知システム (NIDS) のガイド付きセットアップを使用して、以下を実行できます。

- インスタンスにまだアカウントを持っていないユーザーのユーザーとロールの構成
- オペレーショナルテクノロジー (OT) 認定サービスグラフコネクタから NIDS レコードをインポートして、NIDS アプライアンスが OT ネットワークと IT ネットワークのどちらで実行されているかを指定する
- 検出されたデバイスをインポートできるように NIDS を検証します。NIDS の妥当性検査について詳しくは、[NIDS の検証](#)を参照してください。

NIDS ガイド付きセットアップにアクセスするには、次の場所に移動します。ネットワーク侵入検知システム (**NIDS**) > **NIDS** ガイド付きセットアップ。

デバイスを検出する NIDS センサーのマネージャーとしてアプライアンスを割り当てるには、ネットワーク侵入検知システム (**NIDS**) > マネージャー 該当する「管理コンソール」または「中央マネージャー」レコードを編集します。

- センサーリストを確認して、現在マネージャーとしてアサインされているデバイスがないことを確認します。
- センサーとして機能しないデバイスについては、[**is manager**] を **[True]** に変更します。

NIDS によって割り当てられたメタデータを検出されたデバイスにコピーする NIDSUtils スクリプトインクルードについては、「[インストールされたスクリプトインクルード オペレーショナルテクノロジーマネージャー](#)」を参照してください。

関連情報

[ネットワーク侵入検知システム \(NIDS\) CI 拡張クラス](#)

[インストールされたスクリプトインクルード オペレーショナルテクノロジーマネージャー](#)

NIDS の検証

NIDS を検証して、センサーによって検出されたデバイスを ETL からインポートします。センサーはデバイスのインポートの対象ではないため、学習モードでない場合にのみ検証に合格できます。

始める前に

共通サービスデータモデル (CSDM) プラグインをインストールすることをお勧めします。サービスグラフコネクタは、構成管理データベース (CMDB) 標準に従ってライフサイクルデータモデルに沿っています。詳細については、「[Implementing the CSDM framework in stages](#)」を参照してください。

必要なロール:cmdb_nids_admin

このタスクについて

[**Life Cycle Stage** (ライフサイクルステージ)] フィールドと [**Life Cycle Stage Status** (ライフサイクルステージステータス)] フィールドは、センサーの学習モードをキャプチャするために使用されます。「ライフサイクルステージ」フィールドが「運用」に設定され、「ライフサイクルステージステータス」が「学習モード」に設定されている場合、検証は失敗します。[Life Cycle Stage Status (ライフサイクルステージステータス)] フィールドが [**In Use** (使用中)] に設定されている場合、検証は成功します。

手順

1. 移動先 **すべて > ネットワーク IDS アプライアンス (NIDS) > センサー**。
2. リストに管理コンソールまたは中央マネージャーがある場合は、以下のアクションを実行します。
 - a. [レコードの編集] をクリックします。
 - b. 「**NIDS アドミン構成**」タブで、「**NIDS マネージャーである**」を選択して、「検証済み」列を true に設定します。
3. [NIDS アドミン構成] セクションで、[ライフサイクルステージステータス] の値が [学習モード] でないことを確認します。
それ以外の場合、検証は失敗します。
4. **NIDS ネットワークタイプ**を選択します。

ネットワークタイプは、センサーの場所に基づいて選択する必要があります。

- i 注:**
ネットワークタイプ OT は OT デバイスレコードを作成します。ネットワークタイプ IT は OT デバイスレコードを作成しません。

5. [**NIDS にアサインされたメタデータ (NIDS Assigned Meta Data)**] タブで、NIDS によって検出されたすべてのデバイスが入力されていることを確認します。
6. [検証] をクリックします。

- i 注:**
ゾーン値は ETL によって入力されます。ゾーン値が NIDS レコードに手動で入力された場合、ETL によって入力された値が上書きされます。

NIDS レコードが検証されない場合、センサーによって検出されたデバイスは ETL からインポートされません。

次のタスク

あるいは、一括検証によって複数の NIDS センサーを検証することもできます。詳細については、「[複数の NIDS センサーの一括検証](#)」を参照してください。

複数の NIDS センサーの一括検証

一括検証によって複数の NIDS センサーを一度に検証することで、レコードをより迅速かつ効率的に編集できます。

始める前に

必要なロール:cmdb_nids_admin

このタスクについて

各 NIDS センサーを個別に検証する代わりに、一括検証を使用して複数の NIDS センサーを一度に検証できます。

i 注:

ディスクバリーソース別に NIDS センサーを慎重に確認し、一括検証中は注意して続行してください。

手順

1. 移動先 **すべて > ネットワーク IDS アプライアンス (NIDS) > センサー**.
2. 検証するセンサーレコードのチェックボックスをオンにします。
3. [センサーの検証 (**Validate Sensors**)] ボタンを選択します。

タスクの結果

検証したセンサーの ライフサイクルステータス が「使用中」の場合は、検証に成功したことを示すメッセージが表示されます。

選択したセンサーの [ライフサイクルステータス] が [学習モード] になっている場合、または [検証済み] 列が true に設定されている場合、学習モードの 1 つ以上のセンサーが検証されていないか、すでに検証されていることを警告するエラーメッセージが表示されます。一括検証を続行するには、[ライフサイクルステータス] 列を [使用中] に変更することを検討する必要があります。

オペレーショナルテクノロジーシステムサービスのモデル化

オペレーショナルテクノロジー (OT) システムサービスをモデル化して、分散制御システム (DCS) などの他の制御システムを作成できます。

OT システムサービスとは、物理プロセス、機械、および生産オペレーションを管理、制御、監視するために使用されるテクノロジーとシステムのカテゴリを指します。OT システムサービスは通常、製造、エネルギー、公益事業、輸送などの分野で採用されています。

OT システムサービスには次のものが含まれます。

- 分散制御システム (DCS)
- Supervisory Control and Data Acquisition (SCADA)
- 産業用制御システム (ICS)
- 安全計装システム (SIS)
- 製造実行システム (MES)
- プロセス制御システム
- 輸送管理システム
- エネルギー管理システム
- ビル管理システムサービス(BMS)

これらのシステムサービスは、産業プロセスが効率的かつ安全に実行されることを総合的に保証します。

DCS の例

OT システムサービスをモデル化して、他のコントロールシステムを作成できます。たとえば、分散制御システム (DCS) とすべての関連コンポーネント (PLC、制御モジュール、EWS、RTU、HMI、SCADA など) をモデル化できます。DCS は、プラントや生産工程の自動制御と運用のためのプラットフォームです。DCS によって、多数の異なるプロセスを行うプラント全体を調整および監督します。

DCS は、クローズドループ制御を使用するプロセス指向システムです。次の表では、DCS のコンポーネントについて説明します。

DCS のコンポーネント

コンポーネント	説明
オペレーターステーション	DCS の心臓部であるオペレーターは、プロセスを目で確認し、アラームとアラートを監視します。
サーバー、EWS、ヒストリアン	ハードウェア構成のデータ収集とデータ交換。
コントローラー、I/O モジュール	サーバーへのデータ交換。
フィールドデバイス	トランスミッター、スイッチ、アクチュエーター、バルブなどのデバイス。

DCS は、中央にある単一のコントローラーが制御機能処理する集中制御システムとは異なりますが、この中では各プロセス要素、マシン、またはマシンのグループが専用のコントローラーによって制御されます。

オペレーショナルテクノロジーシステムサービスの作成

オペレーショナルテクノロジー (OT) システムサービスを作成して、分散制御システム (DCS) とそのすべての関連コンポーネント (制御モジュールやプログラミングロジックコントロール (PLC) など) をモデル化します。

このタスクについて

次の場所で OT システムサービスを作成できます。

- Now Platform[OT Systems (OT システム)] リスト内
- 産業用 産業用ワークスペース リストビュー

始める前に

必要なロール：admin

手順

1. Now Platform で OT システムサービスを作成する場合は、次のアクションを実行します。

- 移動先 **すべて > オペレーショナルテクノロジー (OT) > OT システム**.
- [新規] を選択します。
- フォームで次のフィールドに入力します。

OT システムサービスフォーム

Field (フィールド)	説明
Display name (表示名)	OT システムサービスの表示名を入力するために使用されます。
名前	OT システムサービスのホスト名。

Field (フィールド)	説明
ISA エンティティサイト	OT システムサービスが属する ISA エンティティサイト。
Manufacturer (メーカー)	OT システムサービスのメーカーの名前。
モデル番号	OT システムサービスのメーカーのモデル番号。
簡単な説明	OT システムサービスの簡単な説明。
詳細	
Owned by (オーナー)	OT システムサービスのプライマリ所有者の名前。
Managed by (管理担当者)	OT システムサービスのプライマリマネージャーの名前。
事業上の重要度	システムサービスの重要度または重要度の測定。例： ▪ 「高」または「最重要」 ▪ 中またはある程度重要 ▪ 低またはやや重要 ▪ なしまたは重要ではない
サポートグループ	OT システムサービスのプライマリサポートグループの名前。
グループによる管理	OT システムサービスを管理するグループの名前。
運用ステータス	システムサービスのステータス。

- d. [送信] を選択します。
2. 産業用 ワークスペースリストビューで OT システムサービスを作成する場合は、次のアクションを完了します。
 - a. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース)。
 - b. リスト () アイコンを選択します。
 - c. **[Operational Technology (OT) (オペレーショナルテクノロジー (OT))]** モジュールで、**[OT Systems (OT システム)]** リストを選択します。
 - d. [新規] を選択します。
 - e. フォームで次のフィールドに入力します。

OT システムサービスフォーム

Field (フィールド)	説明
Display name (表示名)	OT システムサービスの表示名を入力するために使用されます。
名前	OT システムサービスのホスト名。
ISA エンティティサイト	OT システムサービスが属する ISA エンティティサイト。

Field (フィールド)	説明
Manufacturer (メーカー)	OT システムサービスのメーカーの名前。
モデル番号	OT システムサービスのメーカーのモデル番号。
簡単な説明	OT システムサービスの簡単な説明。
詳細	
Owned by (オーナー)	OT システムサービスのプライマリ所有者の名前。
Managed by (管理担当者)	OT システムサービスのプライマリマネージャーの名前。
事業上の重要度	システムサービスの重要度または重要度の測定。例： ▪ 「高」または「最重要」 ▪ 中またはある程度重要 ▪ 低またはやや重要 ▪ なしまたは重要ではない
サポートグループ	OT システムサービスのプライマリサポートグループの名前。
グループによる管理	OT システムサービスを管理するグループの名前。
運用ステータス	システムサービスのステータス。

f. [保存] を選択します。

次のタスク

これで、OT デバイスをシステムサービスに追加できるようになりました。詳細については、「[オペレーショナルテクノロジー システムサービスにデバイスを追加する](#)」を参照してください。

オペレーショナルテクノロジー システムサービスにデバイスを追加する

オペレーショナルテクノロジー (OT) デバイスを OT システムサービスに追加して、デバイスが属する機器モデルエンティティと OT システムサービスの間の関係を作成します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. リスト () アイコンを選択します。
3. **[Operational Technology (OT) (オペレーショナルテクノロジー (OT))]** モジュールで、**[OT Systems (OT システム)]** リストを選択します。
4. デバイスを追加する OT システムサービスを選択します。
5. **[関連レコード]** タブで、**[関連する OT デバイス]** 関連レコードを選択します。
6. **[追加]** を選択します。

7. 1 つ以上の OT デバイスの横にあるチェックボックスをオンにします。

8. すべての OT デバイスを選択したら、[追加] を選択します。

タスクの結果

OT デバイスを追加すると、次の関係が作成されます。

- 選択した構成アイテム (CI) と OT システムサービスの間の Depends on::Used by 関係
- OT システムサービスと CI の機器モデルエンティティの間の「Managed by::Manages」関係。

機器モデルエンティティへの オペレーショナルテクノロジー システムサービスのマッピング

スケジュール済みジョブを有効にして、オペレーショナルテクノロジー (OT) システムサービスを ISA 設備階層モデルエンティティにマッピングします。OT デバイスと機器モデルエンティティの関係が変更されると、スケジュール済みジョブは OT システムサービスと機器モデルエンティティの関係を再計算します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > スケジュール済みジョブ**.
2. フィルターを表示/非表示 ( アイコン) アイコンを選択します。
3. 次のフィルターを追加します。
[名前][次の値に等しい][OT システムを ISA エンティティにマッピング]
4. [**OT システムを ISA エンティティにマッピング (Map OT Systems to ISA Entities)**] スケジュール済みジョブレコードを選択します。
5. [アクティブ] フィールドの横のチェックボックスをオンにします。
6. [実行] フィールドで、ニーズに最も適したオプションを選択します。
7. [更新] を選択します。

オペレーショナルテクノロジーシステムサービスの依存関係マップの表示

オペレーショナルテクノロジー (OT) システムサービスの依存関係マップを表示して、選択した OT システムサービスの階層構造と、本番プロセス内の他のエンティティとの関係をグラフィカルに表示します。

このタスクについて

OT システムサービスの依存関係マップは、次の場所に表示できます。

- Now Platform OT システムサービスレコード内
- 産業用ワークスペース OT システムサービスレコード内

始める前に

必要なロール:cmdb_ot_editor

手順

1. Now Platform上の OT システムサービスの依存関係マップを表示するには、次のアクションを実行します。
 - a. 移動先 すべて > オペレーショナルテクノロジー (OT) > OT システム.
 - b. OT 依存関係マップを表示する OT システムサービスレコードを選択します。
 - c. [OT 依存関係マップを表示] を選択します。
2. 産業用ワークスペース内の OT システムサービスの依存関係マップを表示するには、次のアクションを完了します。
 - a. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
 - b. リスト () アイコンを選択します。
 - c. [Operational Technology (OT) (オペレーショナルテクノロジー (OT))] モジュールで、[OT Systems (OT システム)] リストを選択します。
 - d. OT 依存関係マップを表示する OT システムサービスレコードを選択します。
 - e. [OT 依存関係マップを表示] を選択します。

IT レコードを OT デバイスに自動的に変換する

IT を OT に再アサインするための一括更新ルールセット機能を使用して、IT ハードウェアをオペレーショナルテクノロジー (OT) デバイスに自動的に変換するスケジュール済みジョブを作成します。このスケジュール済みジョブは、一度に変換するすべての IT ハードウェアに OT エンティティの詳細を追加します。

始める前に

必要なロール：admin

このタスクについて

OT エンティティレコードを作成する IT ハードウェアとして分類された構成アイテム (CI) があります。次の一般的なガイドラインに従います。

- 使用するフィールドが、ステップ 3 ~ 4 のフィルター基準条件に適用されていることを確認します。パフォーマンス関連の問題を回避できるように、データセットが 100 万レコードを超えないことを確認します。
- ステップ 3 ~ 6 で、個別の CI クラスに対して個別のスケジュール済みジョブ定義を作成します。このようにして、各 CI レベルをフィルタリングし、OT エンティティのデフォルト値を定義できます。
- フィルターの [クラス] フィールドを使用して、ステップ 3 で特定の CI クラスのみをクエリします。



注:

ハードウェアクラスとその拡張クラスのみがソーステーブルで使用されます。

- [プレビュー] ボタンを使用して、ステップ 4 でさらにレビューするために選択したレコードを検証します。
- ステップ 5 の [OT エンティティのデフォルト構成] タブでデータを確認します。OT エンティティレコードは、これらのデフォルト値を使用して作成されます。

IT ハードウェアを OT デバイスに手動で変換することもできます。詳細については、「[一括編集で IT ハードウェアを OT デバイスに変換する](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > OT マネージャーアドミン > 自動化された IT OT** への一括変換。
2. [新規] を選択します。
3. [フィルター基準:OT デバイス] タブで、ソーステーブルとフィルター基準を設定して、変換する必要がある CI を特定します。

たとえば、COMP のプリフィックスを持ち、システムにインポートされるすべてのコンピューターについて OT エンティティの詳細を追加する場合は、ソーステーブルを **cmdb_ci_computer** として選択し、[名前] [次で始まる] **[COMP]**、[クラス] [コンピューター]、[**OT デバイスの詳細**] [空] などのフィルター基準を追加しま

す。

4. [プレビュー] ボタンを選択して、設定したフィルター条件から選択されたレコードの数を確認します。
これらのレコードには、OT デバイスタイプやデバイスの重要度などの OT エンティティの詳細が追加されます。
5. [**OT エンティティのデフォルト構成**] タブで、フィールドに入力します。
次の表のフィールドは、OT エンティティレコードまたは OT 関連のメタデータに追加されるデフォルト値を示しています。

[OT エンティティのデフォルト構成] フォーム

Field (フィールド)	Description (説明)
OT デバイスタイプ	OT デバイスが分類されるカテゴリタイプ。デバイスタイプは、デバイスが OT ネットワーク上で再生する機能でもあります。たとえば、サーバーなどの IT デバイスを OT デバイスに変換でき、ネットワーク上で HMI が果たす機能は HMI です。クラスはサーバーで、デバイスタイプは HMI です。 注: 場合によっては、OT デバイスに OT 機能がなかったり、デバイスタイプが不明であったりすることがあります。OT デバイスに OT 機能がない場合は、[OT 機能なし] を選択します。OT デバイスのデバイスタイプが不明な場合は、[不明] を選択します。
デバイスの重要度	デバイスに障害が発生した場合のサイトプロセスへの相対リスクの測定:

Field (フィールド)	Description (説明)
	○ 1 : 最重要 ○ 4 : 重要ではない
Purdue レベル	アサインされた Purdue レベル。レベル範囲は 0 から 5 です。 i 注: 産業用制御システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
ゾーン	デバイスが割り当てられているサイトの場所内のエリア。
サイト	デバイスが配置または割り当てられている最上位の親エンティティ、または産業サイト。

6. [実行] フィールドで、このジョブを実行するスケジュール時刻を選択します。

7. [アクティブ] フィールドの横にあるチェックボックスをオンにします。

8. [送信] を選択します。

オペレーショナルテクノロジーマネージャー 参照

参照トピックには、オペレーショナルテクノロジーマネージャー アプリケーションに関する追加情報が記載されています。

オペレーショナルテクノロジーマネージャーとともにインストールされるコンポーネント

オペレーショナルテクノロジーマネージャーアプリケーションをアクティブ化すると、ユーザーロールを含むいくつかのタイプのコンポーネントをインストールできます。

i 注:

アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストールされるロール

ロール	Description (説明)
オペレーショナルテクノロジー ディスカバリー アドミニストレーター [ot_discovery_admin]	オペレーショナルテクノロジープロセスのディスカバリーを実行できますが、構成管理データベース (CMDB)にアクセスして、検出されたアイテムから作成された構成アイテム (CI) および関連オペレーショナルテクノロジー (OT) エンティティを表示することはできません。詳細

ロール	Description (説明)
	については、「 オペレーショナルテクノロジー ディスカバリースケジュールを作成し、ディスカバリープロセスを実行します 」を参照してください。
オペレーショナルテクノロジーマネージャー ビューアー [cmdb_ot_viewer]	オペレーショナルテクノロジー (OT) デバイス レコードへの読み取り専用アクセス。
オペレーショナルテクノロジーマネージャー 編 集者 [cmdb_ot_editor]	運用技術 (OT) 拡張クラス の  アクセス権を作 成、読み取り、更新、および削除します。
オペレーショナルテクノロジーマネージャー ア ドミン [cmdb_ot_admin]	オペレーショナルテクノロジー (OT) デバイス レコードのアクセス権を作成、読み取り、更 新、削除します。OT エンティティタイプ内の 特定の構成を編集および管理することもできま す。詳細については、「 運用技術 (OT) 拡張ク ラス  」を参照してください。

のインストール済みソフトウェア オペレーショナルテクノロジー管理

オペレーショナルテクノロジー管理ソリューションのインストール済みソフトウェアは、ディスカバリー for オペレーショナルテクノロジー (OT) またはインストール済みソフトウェアをサポートする OT 認定サービスグラフコネクタから提供されます。

概要

CI にインストールされるソフトウェアは、ソフトウェア資産管理 (SAM) アプリケーションがインストールされているかどうかによって異なります。SAM を有効にすると、次のテーブルが作成されます。

- ソフトウェアディスカバリーモデル [cmdb_sam_sw_discovery_model]
- ソフトウェア モデル [cmdb_software_product_model]
- ソフトウェアインストール [cmdb_sam_sw_install]

SAM がアクティブ化されたときに、ソフトウェアインストールを管理するためのテーブル構造がどのように異なるかの詳細については、「[Discovery with Software Asset Management](#)」を参照してください。

ソフトウェア資産管理データを表示するようにコンピューター CI を構成することもできます。詳細については、「[Configure a CI to display Software Asset Management data](#)」を参照してください。

OT デバイスにインストールされているソフトウェアを表示する

産業用 ワークスペース内の OT デバイスにインストールされているソフトウェアは、次の場所で確認できます。

- [**OT デバイスにインストールされているソフトウェア (Software Installed on OT Devices)**] リストに移動します。すべて > オペレーショナルテクノロジー (OT) > OT デバイスにインストールされているソフトウェア。
- オペレーショナルテクノロジー (OT) モジュールの [産業用 ワークスペース] リストビューの [**OT デバイスにインストールされているソフトウェア**] リスト。
- OT デバイスレコードの [関連レコード] タブにある [インストールされているソフトウェア] リスト。

のモデルカテゴリ オペレーショナルテクノロジー

CMDBに構成アイテム (CI) が作成されると、資産レコードが作成されます。資産レコードには、CI のモデル・カテゴリが含まれています。

次の表では、オペレーショナルテクノロジー (OT) で利用可能なモデルカテゴリとその CI クラスについて説明します。

OT モデルカテゴリ

名前	CI クラス
産業	該当なし
工業一般	オペレーショナルテクノロジー (OT) [cmdb_ci_ot]
運用設備	運用機器 [cmdb_ci_oe]
OT コントロール	OT コントロールシステム [cmdb_ci_ot_control]
OT コントロール 3D プリンター	産業用 3D プリンター [cmdb_ci_ot_insustrial_3d_printer]
OTコントロールCNC	CNC [cmdb_ci_ot_cnc]
OT コントロール DCS	DCS [cmdb_ci_ot_dcs]
OT コントロール DPU	DPU [cmdb_ci_ot_dpu]
OT コントロール IED	IED [cmdb_ci_ot_ied]
OT コントロールモジュール	OT コントロールモジュール [cmdb_ci_ot_control_module]
OT コントロール PLC	PLC [cmdb_ci_ot_plc]
OT コントロール RTU	RTU [cmdb_ci_ot_rtu]
OT コントロール SCADA	SCADA サーバー [cmdb_ci_ot_scada_server]
OT コントロールサーバー	OPC サーバー [cmdb_ci_ot_opc_server]
OTフィールドアクチュエータ	産業用アクチュエーター [cmdb_ci_ot_industrial_actuator]
OT フィールドデバイス	OT フィールドデバイス [cmdb_ci_ot_field_device]
OT フィールドドライブ	産業用ドライブ [cmdb_ci_ot_industrial_drive]
OT フィールドロボット	産業用ロボット [cmdb_ci_ot_industrial_robot]
OT フィールドセンサー	産業用センサー [cmdb_ci_ot_industrial_sensor]
OT 監督	OT 監督システム [cmdb_ci_ot_overusery]
OT 監督 EWS	EWS [cmdb_ci_ot_ews]
OT 監督履歴担当者	履歴担当者 [cmdb_ci_ot_historian]
OT 監督 HMI	HMI [cmdb_ci_ot_hmi]
OT 監督 OPC	OPC クライアント [cmdb_ci_ot_opc_client]

OT モデルカテゴリ (続く)

名前	CI クラス
OT 監督 SCADA	cmdb_ci_ot_scada_client

関連情報

ネットワーク侵入検知システム (NIDS) 拡張クラス、OT 拡張クラス、および関連アプリケーションの詳細を確認します。

概要

拡張クラスは、オペレーショナルテクノロジー管理構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

Network Intrusion Detection System (NIDS) CI extension class

ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワーク監視アプライアンスと、それが検出するネットワーク上のデバイスとの間の関係を構築します。

Operational Technology (OT) extension classes

構成管理データベース (CMDB)は OT のクラスを更新します。

関連アプリケーション

CMDB CI Class Models

CMDB CI Class Models ストアアプリは、クラスの説明、識別ルール、識別子エントリ、および依存関係を含む、CMDB クラス階層を拡張するクラスモデルを追加します。

[store-future: BEGIN review]

のペルソナ オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャーには、アプリケーションに関連付けられたオペレーショナルテクノロジー (OT) ペルソナがあります。

[End]

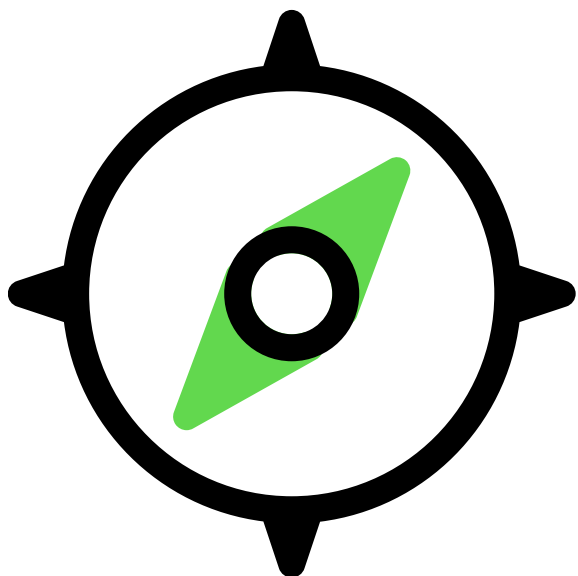
産業用プロセスマネージャー

産業用プロセスマネージャー アプリケーションを使用して、ServiceNow[®] オペレーショナルテクノロジーソリューションに必要な ISA-95 機器モデルデータ基盤を作成します。この 産業用プロセスマネージャー を使用すると、各サイトで独自のバージョンの機器モデルを作成できます。

 注:

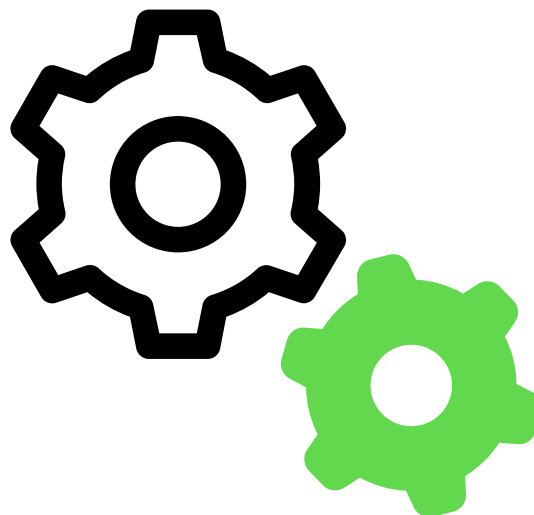
Manufacturing Process Manager は Industrial Process Manager for Vancouver に名前が変更されました。バージョン 1.0.9 以前を使用している場合、このアプリケーションは Manufacturing Process Manager という名称のままです。バージョン 2.0 を使用している場合、アプリケーションの名前は Industrial Process Manager (産業用プロセスマネージャー) です。

探索



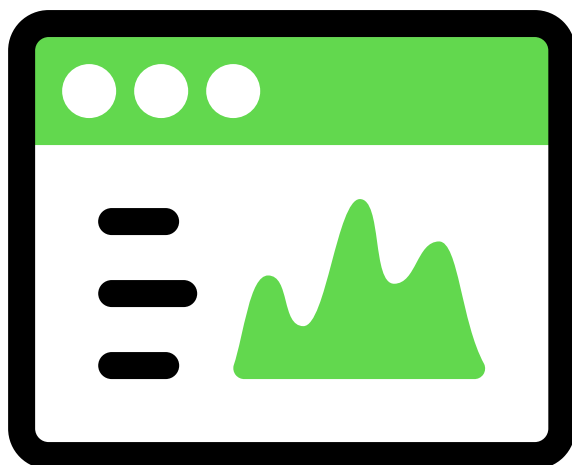
メーカーが 産業用プロセスマネージャー

Configure (構成)

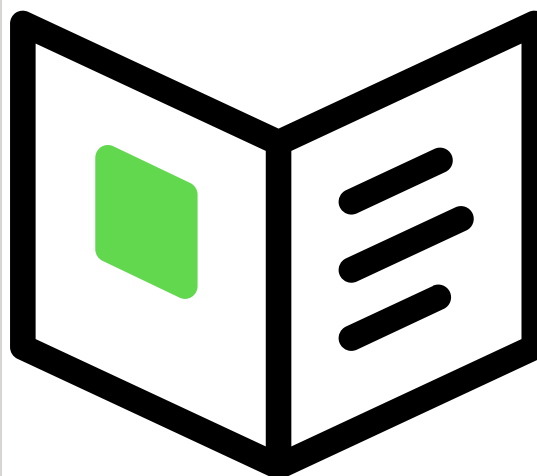


実装の計画と構成

使用

オペレーショナルテクノロジーデバイス
と機器モデルエンティティのレビュー

参照



関連情報とアプリケーションの詳細を取得

産業用プロセスマネージャー の探索

産業用プロセスマネージャーで使用される一般的な用語、略語、および ISA-95 機器モデル業界標準の詳細について説明します。

産業用プロセスマネージャー 一般的な用語

産業用プロセスマネージャーを開始する前に、このコンテンツで使用される一般的な用語と頭字語をいくつか見てみましょう。

一般的な用語と頭字語

用語	頭字語	定義
オペレーショナルテクノロジー	OT	物理的なプロセスを制御する産業オートメーションに使用されるテクノロジー。 i 注: オペレーショナルテクノロジーはモノのインターネット(IoT)ではありません。
国際オートメーション学会	ISA	ISA-95 機器モデルを含む、産業企業の標準を公開する組織。
抽出、変換、ロード	ETL	ソースシステムからデータを取得し、それを変換して、ターゲットシステムにアップロードするために使用される一般的な用語。

ISA-95 機器モデル

ISA-95 機器モデルは、産業施設とその中の生産設備を表す業界標準です。さまざまなレベルとレベルタイプで機器モデルテンプレートを定義することで、施設内の機器モデルエンティティを説明できます。

このテンプレートを使用すると、次のアクションを実行できます。

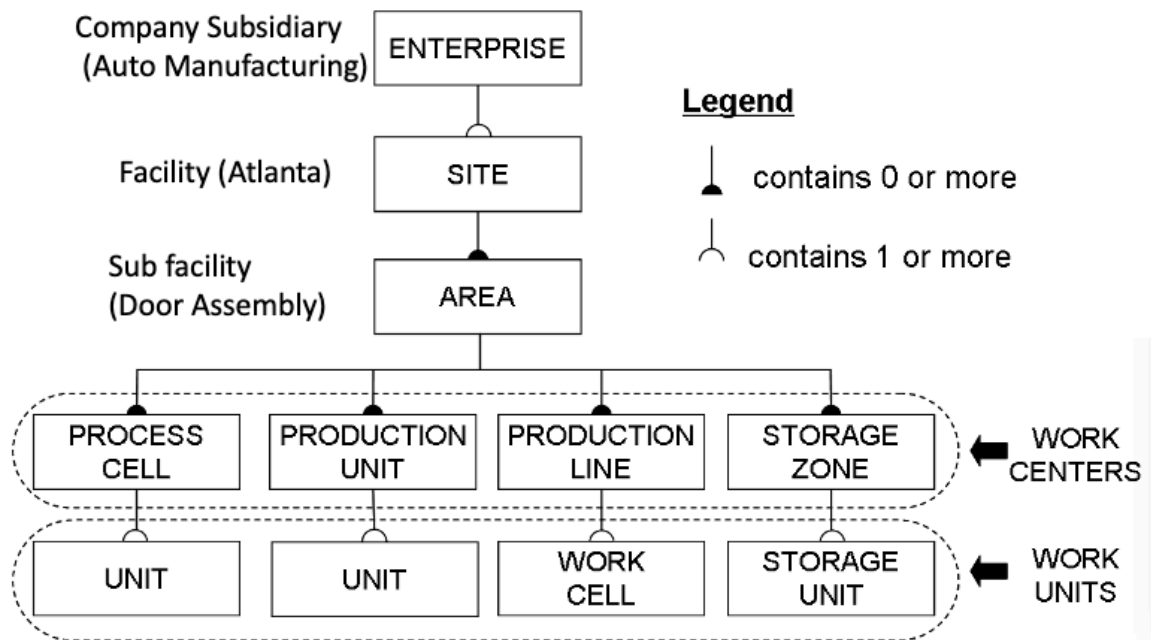
- 機器モデルエンティティをマッピングします。このマップを使用して、階層構造を作成します。
- 産業用のさまざまなサイトに合わせて複数の機器モデルを作成します。
- 各サイトにユーザーを割り当て、特定のサイトの機器モデル情報へのアクセス権を管理できるようにします。たとえば、アトランタのユーザーはアトランタのサイト情報にのみアクセスでき、ミシガン州のサイトのデータにはアクセスできないように指定できます。詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

機器モデルはサイトレベルで開始され、各産業サイトを説明する詳細な階層構造が含まれています。機器モデルテンプレートを適用して、このデータを階層的な順序で構造化します。

次の図は、産業用プロセスマネージャーのインストール時に提供される標準の ISA-95 デフォルトテンプレートの例です。このグラフィックは、アトランタにある自動車製造施設を表しています。

- サイトの下の下位レベルは、ドア組立エリア、独自の従属ワークセンター、および作業単位を表します。
- ワークセンターと作業単位レベルには、それぞれレベルタイプがあります。このモデルでは、作業区レベルには以下の 4 つの異なるレベルタイプがあります。
 - セルを処理
 - 生産単位
 - 生産ライン
 - ストレージゾーン

機器モデルテンプレートの例



設備モデルテンプレート

機器モデルテンプレートを作成して、機器モデルの特性評価を行ったり、類似したタイプの機器モデルエンティティをグループ化することで物理的な産業施設を説明するデータを構造化したりできます。

機器モデルテンプレートは、次のコンポーネントで構成されています。

機器モデルテンプレート

機器モデルテンプレートの名前と説明。

機器モデルテンプレートの階層レベル

機器モデルデータのソートと構造化に使用される割り当てられた階層レベル。

機器モデルテンプレートの階層レベルタイプ

階層レベル内のさまざまなタイプのエリア、機能、または生産プロセスを表すタイプ。

機器テンプレートの詳細と構造の図の例については、「[ISA-95 機器モデル と 機器モデルテンプレートの定義](#)」を参照してください。

産業用プロセスマネージャーの構成

産業用プロセスマネージャー アプリケーションを構成して、ServiceNow オペレーショナルテクノロジーソリューションに必要な機器モデルデータ基盤を作成できるようにします。

注:

admin ロールを持っている場合は、産業用 ガイド付きセットアップを使用して、産業用プロセスマネージャー アプリケーションのセットアップを進めることができます。

ガイド付きセットアップにアクセスするには、次の場所に移動します。産業用ワークスペース アドミン > ガイド付きセットアップ。

タスク	目的
1. ServiceNow Storeから産業用プロセスマネージャーを取り付けます。	産業用プロセスマネージャー アプリケーションとサポートプラグインをインストールします。
2. 産業用プロセスマネージャー ロールを割り当てます。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
3. サービスグラフ Connector インポート用の Excel スプレッドシートMicrosoft入力します。	Microsoft Excel スプレッドシートを作成し、Now Platformにアップロードするための既存の ISA-95 機器モデルデータを入力します。
4. Excel スプレッドシートをインポートします。	既存の ISA-95 機器モデルデータを 構成管理データベース (CMDB)にアップロードします。
5. ServiceNow パートナーが提供するサービスグラフ [service-graph] コネクタをインストールし、統合を使用して機器モデルデータをインポートします。	ServiceNow Storeで利用可能になったServiceNowパートナーが提供するコネクタをインストールし、機器モデルデータをインポートします。
6. 非管理者ロールを持つユーザーに機器モデルサイトへのアクセス権を付与します。	cmdb_ot_isa_viewerまたはcmdb_ot_isa_editorロールが割り当てられたユーザーのサイトアクセス権をアサインまたは削除します。
オプション:OT デバイスのマッピングを自動化する	OT デバイスから本番プロセスへのマッピングを自動化します。 注: マッピング機能を有効にするには、次のプラグインが必要です。 - オペレーショナルテクノロジーマネージャー - 産業用プロセスマネージャー

産業用プロセスマネージャー をインストールする

必要なエンタイトルメントと admin ロールがある場合は、産業用プロセスマネージャー アプリケーションと関連プラグインをインストールできます。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。

必要なロール：admin

このタスクについて

次のアイテムが 産業用プロセスマネージャー とともにインストールされます。

- プラグイン
- アプリケーションメニュー (ガイド付きセットアップを含む)
- ロール
- テーブル

産業用プロセスマネージャー アプリケーションとともにインストールされるコンポーネントの表示の詳細については、「[産業用プロセスマネージャーとともにインストールされるコンポーネント](#)」を参照してください。

i 注:

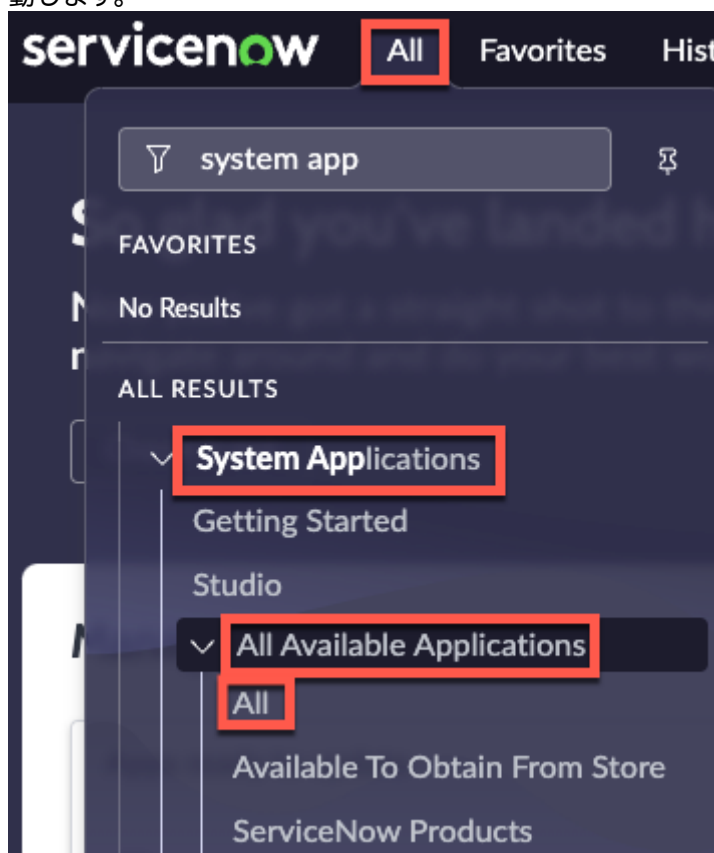
オペレーショナルテクノロジー ヴィジビリティのライセンスを持たないOperational Technology Service Managementユーザーの場合は、次の点に注意してください。

- 最新バージョンの オペレーショナルテクノロジーインシデント管理 がインストールされている場合は、 産業用プロセスマネージャー もインストールされます。
- 最新バージョンの オペレーショナルテクノロジー変更管理 がインストールされている場合は、 産業用プロセスマネージャー もインストールされます。

Operational Technology Service Managementエクスペリエンスにアクセスできるように、最新バージョンにアップグレードする必要があります。

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して、産業用プロセスマネージャー アプリケーションを検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store への要求が必要になることがあります。

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

依存するプラグインとアプリケーションがインストールされる場合、現在インストールされている場合、またはインストールする必要がある場合は、表示されます。インストールする必要があるプラグインまたはアプリケーションがある場合は、産業用プロセスマネージャーをインストールする前にインストールする必要があります。

4. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。
デモデータには、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードが含まれています。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

i 重要:

インストール時にデモデータを読み込んでおかないと、後から読み込むことはできません。

5. [インストール] を選択します。

産業用ワークスペースアドミン アプリケーションメニューとガイド付きセットアップ

アプリケーションと関連プラグインをインストールすると、産業用ワークスペースアドミン アプリケーションメニューを使用して、関連する オペレーショナルテクノロジーマネージャー、産業用プロセスマネージャー、オペレーショナルテクノロジーインシデント管理、オペレーショナルテクノロジー脆弱性対応、オペレーショナルテクノロジー変更管理、および オペレーショナルテクノロジーのナレッジ管理 機能にアクセスできるようになります。

産業用ワークスペースアドミン アプリケーションメニューコンテンツ

産業用ワークスペースアドミンアプリケーションメニューにアクセスするには、アプリケーションナビゲーターに「Industrial Workspace Admin」と入力します。オペレーショナルテクノロジー管理ソリューションは現在、次の 5 つのアプリケーションで構成されています。

- オペレーショナルテクノロジーマネージャー
- 産業用プロセスマネージャー
- オペレーショナルテクノロジー脆弱性対応
- オペレーショナルテクノロジーインシデント管理これには、以下が含まれます オペレーショナルテクノロジーのナレッジ管理
- オペレーショナルテクノロジー変更管理

i 注:

オペレーショナルテクノロジーインシデント管理 and オペレーショナルテクノロジー変更管理を使用する前に、まず オペレーショナルテクノロジーマネージャー または 産業用プロセスマネージャー アプリケーションをインストールする必要があります。

産業用ワークスペースアドミン アプリケーションメニューに表示されるオプションは、インストールされている OT アプリケーションと、ユーザーにアサインされたロールによって異なります。産業用プロセスマネージャーをインストールすると、産業用ワークスペースアドミンアプリケーションメニューで次の機能を使用できます。

- ガイド付きセットアップ
- すべての OT プロパティ
- 次の選択肢を含む OT マネージャー:

- OT マネージャーアドミン
- 産業用プロセスマネージャー
- OT インシデントアドミン
- オペレーショナルテクノロジー変更管理

アプリケーションのインストールと割り当てられたロールの詳細については、「[産業用プロセスマネージャー をインストールする](#)」と [産業用プロセスマネージャーユーザーロールのアサイン](#)」を参照してください。

産業用ワークスペースアドミン ガイド付きセットアップ

admin ロールを持っている場合は、ガイド付きセットアップを使用して、産業用プロセスマネージャー アプリケーションのセットアップを進めることができます。

ガイド付きセットアップにアクセスするには、次の場所に移動します。産業用ワークスペースアドミン > ガイド付きセットアップ。

ガイド付きセットアップでロック解除として表示される特定のステップは、インスタンスにインストールしたアプリケーションによって異なります。

産業用プロセスマネージャーのみがインストールされている場合は、次のセットアップ機能がロックされます。

- オペレーショナルテクノロジーマネージャーセットアップ手順。
- オペレーショナルテクノロジーマネージャーに依存する産業用プロセスマネージャーステップ。
- オペレーショナルテクノロジー脆弱性対応セットアップ手順。
- オペレーショナルテクノロジーインシデント管理セットアップ手順。
- オペレーショナルテクノロジー変更管理セットアップ手順。
- オペレーショナルテクノロジーのナレッジ管理セットアップ手順。

ガイド付きセットアップとその使用方法の詳細については、「[ガイド付きセットアップの使用](#)」を参照してください。

産業用プロセスマネージャーユーザーロールのアサイン

ユーザーにロールをアサインすると、産業用プロセスマネージャー アプリケーションの各機能やデータへのアクセスを制御できます。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、産業用プロセスマネージャー アプリケーションを使用できます。

ロール	Description (説明)
機器モデルビューアー [cmdb_ot_isa_viewer]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] テーブルレコードを表示することのみ可能です。詳細については、「 での 産業用プロセスマネージャー の使用 」と「 オペレーショナルテクノロジーマネージャー 」と「 機器モデルの管理 」を参照してください。

ロール	Description (説明)
機器モデルエディター [cmdb_ot_isa_editor]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] レコードを表示および編集できます。 詳細については、「での 産業用プロセスマネージャー の使用 オペレーショナルテクノロジーマネージャー」と「機器モデルの管理」を参照してください。
機器モデルアドミン [cmdb_ot_isa_admin]	cmdb_ot_isa_editor ロールを継承し、次のアクションも実行できます。 - 産業用ガイド付きセットアップを使用して、産業用プロセスマネージャーとオペレーショナルテクノロジーマネージャーを設定します。 - 機器モデルテンプレート [isa_entity_template]、[isa_entity_level]、および機器エンティティタイプ [isa_entity_type] テーブルレコードを編集する。 詳細については、「産業用ワークスペースアドミン アプリケーションメニューとガイド付きセットアップ」を参照してください。
機器モデルダウタイムプランナー [sn_isa_schedule_admin]	機器エンティティのスケジュールを作成、変更、および削除できます。スケジュールを機器エンティティに関連付けることもできます。
機器モデルビューアーすべて [cmdb_ot_isa_viewer_all]	すべての ISA Equipment Model (ISA 設備階層モデル) レコード (cmdb_ci_ot_isa_entity) と、関連する機器モデルテンプレートレコード (isa_entity_template、isa_entity_level、isa_entity_type) を表示できます。 cmdb_ot_adminに含まれるロール。
素晴らしい管理者 [sn_ot_amazing_admin]	すべての機器モデルエンティティの OT サブネットシステムプロパティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
アメージングエディター [sn_ot_amazing_write]	ユーザーに関連付けられているすべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
アメージングビューアー [sn_ot_amazing_read]	すべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を表示できます。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

OT システムプロパティの表示と編集

さまざまなアプリケーションの オペレーショナルテクノロジー (OT) に関連するすべてのシステムプロパティを表示および編集します。

始める前に

必要なロール：admin

このタスクについて

Now Platform の [すべての **OT** プロパティ] モジュールから、次の OT アプリケーションのシステムプロパティを変更できます。

- ディスカバリー対象 オペレーショナルテクノロジー
- 産業用プロセスマネージャー
- ISA 設備階層モデル
- オペレーショナルテクノロジーマネージャー
- オペレーショナルテクノロジーインシデント管理
- オペレーショナルテクノロジーのナレッジ管理
- オペレーショナルテクノロジー変更管理
- 産業用ワークスペース共通

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **すべての OT プロパティ**.
2. [システムのプロパティ] テーブルで、システムプロパティを編集するアプリケーションを選択します。
3. アプリケーションまたは機能の利用可能なシステムプロパティを必要に応じて編集します。
4. [更新] を選択します。

機器モデルテンプレートの定義

Now Platformで作成した機器モデルエンティティにアサインできるテンプレートを作成します。これらのテンプレートを使用して、機器モデルを特徴付けたり、類似したタイプの機器モデルエンティティをグループ化することで、物理的な産業施設を説明するデータを構造化したりすることができます。

機器モデルテンプレートを作成する

テンプレートの使用を識別して説明する機器モデルテンプレートレコードを作成します。機器モデルテンプレートを作成したら、その階層レベルとタイプを作成できます。

始める前に

必要なロール:cmdb_ot_isa_admin

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **産業用プロセスマネージャー** > **機器モデルテンプレート**.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。

機器モデルテンプレートフォーム

フィールド	説明
名前	機器モデルテンプレートの名前。
Description (説明)	機器モデルテンプレートの説明。
アプリケーション	選択したアプリケーションスコープ。このスコープがグローバルアプリケーションスコープである場合、[グローバル] が表示されます。

4. [送信] をクリックします。

次のタスク

機器モデルテンプレートの階層ソートレベルを作成します。

機器モデルテンプレートの階層ソートレベルを作成する

機器モデルテンプレートの階層レベルを作成してアサインします。機器テンプレートを機器モデルにアサインすると、これらのレベルによって、そこに表示されるデータがソートされて構造化されます。

始める前に

必要なロール：admin

このタスクについて

ソートのために機器モデルテンプレートにレベルを割り当てることができます。たとえば、サイト、エリア、作業区、その他のレベルを機器に割り当て、それぞれのソート順序を指定できます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルテンプレート**。
2. 機器モデルテンプレートを選択します。
3. [テンプレートレベル] 関連リストで、[新規] をクリックします。
4. フォームのフィールドに入力します。

[テンプレートレベル] フォーム

フィールド	Description (説明)
レベル名	機器モデルをアサインするレベルの名前。例： サイト 工業用地。 面 工業用地のエリア。 ワークセンター 工業用地の作業センター。
親	このレベルより上の機器モデルテンプレートレベルの識別子。空のままにすると、このレベルがモデルの最上位レベルになります。たとえば、次のアクションを実行できます。

フィールド	Description (説明)
	○ サイトレベルを作成する場合、親を持たない機器モデル階層の最上位レベルであれば、このフィールドを空のままにします。 ○ エリア レベルを作成し、それがサイト レベルの子である場合は、 サイト を親として選択します。 ○ ワークセンタレベルを作成し、それがエリアレベルの子である場合は、 エリア をその親として選択します。
アプリケーション	選択したアプリケーションスコープ。このスコープがグローバルアプリケーションスコープである場合、[グローバル] が表示されます。
テンプレート	選択した機器モデルテンプレートの名前。
順序	ソートのための機器モデル階層内のレベルの位置を示す番号。入力した最小の数値は、最上位の階層レベルを表します。たとえば、サイトが機器モデルテンプレートの階層の最上位レベルを表す場合は、[サイト] に 1 を入力します。

5. [送信] をクリックします。

次のタスク

機器モデルテンプレートの階層レベル内に詳細なタイプを作成します。

機器モデルレベルタイプを作成する

作成した各機器モデルテンプレートレベル内に詳細なレベルタイプを作成します。そのレベル内で作成する詳細レベルタイプは、そのレベル内の生産プロセスのタイプを表します。

始める前に

必要なロール：admin

このタスクについて

レベル内のさまざまなタイプの場所、エリア、または機能を表すタイプを作成できます。たとえば、ISA 95 テンプレートでは、作業区レベルには次のレベルタイプがあります。

- 生産セル
- 生産単位
- 生産ゾーン
- ストレージゾーン

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルテンプレート**。
2. 機器モデルテンプレートを選択します。
3. [テンプレートレベル] 関連リストで、機器モデルテンプレートレベルを選択します。
4. [テンプレートタイプ] 関連リストで、[新規] をクリックします。
5. フォームのフィールドに入力します。

[テンプレートレベルタイプ] フォーム

フィールド	Description (説明)
レベルタイプ名	選択した機器モデルテンプレートレベルにアサインするレベルタイプの名前。たとえば、生産セルを割り当てて、ワークセンタレベルの生産セルタイプを作成します。
レベル名	選択した機器モデルテンプレートのレベルの名前。
アプリケーション	選択したアプリケーションスコープ。このスコープがグローバルアプリケーションスコープである場合、[グローバル] が表示されます。
テンプレート	選択した機器モデルテンプレートの名前。

6. [送信] をクリックします。

機器モデルデータのインポート

スケジュール済みインポート機能を使用すると、入力された Microsoft Excel フラットファイルスプレッドシートから既存の機器モデルデータをインポートできます。これを使用して、ISA-95 機器モデルデータを 構成管理データベース (CMDB) にインポートできます。

機器モデルデータをインポートする前に、産業用プロセスマネージャー をインストールする必要があります。

機器モデルデータを Now Platform にインポートするには、いくつかの方法があります。

1. スプレッドシートを使用してデータをインポートする場合は、Microsoft Excel スプレッドシートに既存の ISA-95 機器モデルデータを入力し、スプレッドシートを使用した **SG** 設備モデルのスケジュール済みインポート を実行する必要があります。多くの従来のレコードシステムには、このデータを Excel スプレッドシートにエクスポートできる関数が含まれています。つまり、手動で入力する必要はありません。
2. いくつかの ServiceNow パートナーは、機器モデルデータを保存するサードパーティのレガシーレコードシステムへの統合も開発しています。
 - これらの統合が利用可能になったら、産業用プロセスマネージャーのオペレーショナルテクノロジー認定統合を検索して、ServiceNow Store で見つけることができます。
 - 環境に適用可能な統合をインストールし、必要に応じて実行します。

これらのインポート方法を使用することで、必要に応じて信頼できるソースに保存されているデータで Now Platform 内の既存の機器モデルを更新できます。新しくインポートされたデータの場合、Now Platform は機器モデルエンティティ CI クラスレコードを 構成管理データベース (CMDB) に自動的に作成します。

インポート処理に影響するシステムプロパティ

次のシステムプロパティは、Microsoft Excel スプレッドシートに機器モデルデータを入力する方法と、機器モデルのインポート - ETL プロセスが機能する方法に影響します。

`sn_isa_model.cmdb_relationships_sync_levels`

Now Platform にインポートして構成管理データベース (CMDB) で同期できる機器モデルのレベルの数を決定します。デフォルト値は 8 です。

`sn_isa_model.short_code_validation_max_length`

スプレッドシートのショートコード列の最大長を設定します。デフォルト値は 3 です。

sn_isa_model.user_search_matching_attribute

入力されたスプレッドシートからインポートされたユーザーデータ参照を、システムユーザー [sys_user] テーブルに保存されている対応するユーザーレコードと照合します。メールアドレスは各ユーザーレコードに固有であるため、デフォルトはユーザーのメールアドレスです。

glide.scriptable.excel.max_ファイル_サイズ

Excel ファイルの最大サイズをバイト単位で設定します。このプロパティはグローバルです。

i 注:

システムプロパティを追加または作成してシステムの動作を制御する方法の詳細については、「[システムプロパティの追加](#)」を参照してください。

Microsoft Excel スプレッドシートに機器モデルデータを入力する

Microsoft Excel スプレッドシートを作成し、既存の ISA 設備階層モデルデータを入力します。アップロードを成功させるには、既存のデータを正しい列に配置することが重要です。

Now Platform内の構成管理データベース (CMDB)が正しく入力される Microsoft Excel スプレッドシートを作成するには、次のアクションを実行します。

1. データソースレコードに添付されている Microsoft Excel スプレッドシートを使用して、アップロードするスプレッドシートを準備します。空のテンプレートを見つけるには、次のアクションを実行します。

a. 移動先 機器モデル: **ISA** > 備品を輸入します。モデル - データソース

b. **[Import Equipment Model - Data Source (機器モデルをインポート - データソース)] - [v2.xlsx (Import Equipment Model - Data Source -)]** をクリックします

i 注:

または、「機器モデルのインポート - データソース - v2.xlsx」スプレッドシートをダウンロードするには、Now Support ナレッジベースの記事「[ISA Equipment Model Excel Service Graph Connector \[KB0966600\]](#)」に必要な Microsoft Excel スプレッドシート」を参照してください。

2. 添付の「Import Equipment Model - Data Source - v2.xlsx」スプレッドシートをダウンロードして、テンプレートとそのワークシートの詳細を確認してください。

i 注:

v1 から v2 にアップグレードする ISA SGC ユーザーの場合は、以下の「**v1 から v2 へのアップグレード**」というセクションを参照してください。

機器モデルをインポート - データソース - スプレッドシート v2.xlsx

ワークシート名	目的
データインポート用の空のテンプレート	インポートする機器モデルデータを入力します。詳細な例は、このトピックの残りの部分で確認できます。
データ列の説明	このトピックに記載されている情報と同様に、スプレッドシートのデータ列について説明します。
インポート用のサンプルデータ	スプレッドシートにインポートする機器モデルの例を提供します。これらの例は、このトピックの残りの部分で確認できます。

3. Microsoft Excel スプレッドシートに入力したら、統合ハブ ETL 関数を実行するときに簡単にアクセスできるように、既知の場所に保存します。

注:

列名は変更できません。列を追加して、`sn_isa_model.user_search_matching_attribute` システムプロパティで指定されているように、所有者を一意に識別するための追加フィールドをサポートすることができません。

スプレッドシートへの入力

サンプルのオペレーショナルテクノロジーデータ (列 A から J)

1 つのスプレッドシートで複数のサイトからデータをインポートできます。この例の画像は、ATL と CTL の 2 つのサイトのデータを示しています。

	A	B	C	D	E	F	G	H	I	J
1	Path	Short Code	Entity Name	Location	Assigned to	Support Group	Description	Process criticality	Company	Template
2	ATL	ATL	Atlanta Site	Atlanta Car Facility	fred.luddy@example.com	Atlanta Plant Support	the site in Atlanta where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
3	ATL-B64	B64	Building 64	Atlanta Building 64	fred.luddy@example.com	Atlanta Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template
4	ATL-B42	B42	Building 42	Atlanta Building 42	fred.luddy@example.com	Atlanta Plant Support	similar to building 64 except with a 42 on the side	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
5	ATL-B64-MASS	MASS	Model M	Atlanta Building MASS	fred.luddy@example.com	Atlanta Plant Support	model S needs to be assembled somewhere	1 - most critical	Demo Car Corp	ISA 95 Default Template
6	ATL-B64-QASS	QASS	Model Q	Atlanta Building QASS	fred.luddy@example.com	Atlanta Plant Support	a place for the Q model to get assembled	1 - most critical	Demo Car Corp	ISA 95 Default Template
7	ATL-B64-MPROD	MPROD	Model MPROD	Atlanta Building MPROD	fred.luddy@example.com	Atlanta Plant Support	Model S also needs a production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
8	ATL-B64-QPROD	QPROD	Model QPROD	Atlanta Building QPROD	fred.luddy@example.com	Atlanta Plant Support	Model Q production line	1 - most critical	Demo Car Corp	ISA 95 Default Template
9	ATL-B42-MQSTOR	MQSTOR	Model M and Q	Atlanta Building MQSTOR	fred.luddy@example.com	Atlanta Plant Support	storage for the models we built	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
10	ATL-B64-QPROD-C1	C1	Cell 1	Atlanta Building C1	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 1	1 - most critical	Demo Car Corp	ISA 95 Default Template
11	ATL-B64-QPROD-C2	C2	Cell 2	Atlanta Building C2	fred.luddy@example.com	Atlanta Plant Support	Q prod assembly cell 2	1 - most critical	Demo Car Corp	ISA 95 Default Template
12	ATL-B42-MQSTOR-Z1	Z1	Zone 1	Atlanta Building Z1	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ for transfer	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
13	ATL-B42-MQSTOR-Z6	Z6	Zone 2	Atlanta Building Z6	fred.luddy@example.com	Atlanta Plant Support	storage zone for MQ to just store the stuff	2 - somewhat critical	Demo Car Corp	ISA 95 Default Template
14	CTL	CTL	California Site	California Car Facility	fred.luddy@example.com	California Plant Support	the site in California where we make cars	1 - most critical	Demo Car Corp	ISA 95 Default Template
15	CTL-C64	C64	Building 64	California Building 64	fred.luddy@example.com	California Plant Support	the building with the number 64 on the side	1 - most critical	Demo Car Corp	ISA 95 Default Template

列 A から J

列	名前	タイプ	Description (説明)	必須
A	パス	文字列	このエンティティとそのすべての親エンティティの短縮コードの連結。たとえば、ATL-B42-MQSTOR-Z1 は、次の短縮コードを連結したものです。 - アトランタサイトの ATL 短縮コード。 - 建物 B42 の B42 短縮コード。 - モデル M および Q の MQSTORE 短縮コード。 - モデル M および Q のゾーン 1 転送ストレージゾーンの Z1 短縮コード。	はい
B	短縮コード	文字列、英数字のみ	エンティティの簡単な説明コード。ショートコードの例については、前の「パス」列の説明を参照してください。 短縮コードは、 <code>sn_isa_model.short_code_validation_max_length</code> システムプロパティで指定された最大長を超えることはできません。	いいえ

列 A から J (続く)

列	名前	タイプ	Description (説明)	必須
C	エンティティ名	文字列	エンティティの正式名称。たとえば、都市名、建物番号、モデル番号などです。	はい
D	Location (ロケーション)	文字列	エンティティの場所。たとえば、アトランタにある機器モデルごとにアトランタビル 64 をリストします。Now Platform内の構成管理データベース (CMDB)に格納されている cmn-location 値。参照として使用します。	いいえ
E	Assigned to (アサイン先)	文字列	このエンティティレコードを所有および管理するアサインされた個人のメールアドレス。 i 注: <i>sn_isa_model.user_search_matching_attribute</i> システムプロパティで指定された設定に基づいて、追加の属性を使用できます。	いいえ
F	サポートグループ	文字列	このエンティティのメンテナンスと管理をサポートするグループの名前。	いいえ
G	Description (説明)	文字列	この機器モデルエンティティとその目的の詳しい説明。	いいえ
H	プロセスの重要度	文字列	エンティティが産業プロセスにとってどの程度重要かを示す指標。次に例を示します。 • 1 - 最重要。 • 2 - ある程度重要。	いいえ
I	Company (チェックアウト日時)	文字列	エンティティが属する会社の名前。Now Platform内のCMDBに格納されている cmn-location 値。参照として使用します。	いいえ
J	テンプレート	文字列	データのインポートに使用されるテンプレート。 i 注: データをインポートした後は、テンプレートを設定できません。	はい

v1 から v2 へのアップグレード

v1 から v2 にアップグレードする ISA SGC ユーザーの場合は、一意のパスを持つ新しい ISA 設備階層モデルエンティティをインポートし、既にパス値を持つ既存の ISA 設備階層モデルエンティティを修正スクリプトで更新できます。

データソースとインポートスケジュールを使用して機器モデルデータをインポートします

機器モデルデータを含む Microsoft Excel スプレッドシートを完成させたら、データソースとスケジュール済みインポートを使用して Now Platform にインポートします。

始める前に

このプロセスを実行する前に、インポートする Microsoft Excel スプレッドシートを準備する必要があります。詳細については、「[Microsoft Excel スプレッドシートに機器モデルデータを入力する](#)」を参照してください。

必要なロール:cmdb_inst_admin、import_admin

このタスクについて

このプロセスを実行すると、スプレッドシートに含まれる機器モデルレコードの 構成管理データベース (CMDB) 内に一意の機器モデルエンティティ CI クラスレコードが作成されます。

手順

1. 移動先 **すべて > 機器モデル : ISA > 備品** を入力します。モデル - データソース。
2. **SG 設備階層モデルデータソース**レコードで、作成した Microsoft Excel スプレッドシートを添付します。
 - a. [添付ファイルを管理] を選択します。
 - b. [添付ファイル] ダイアログ ボックスで、[ファイルの選択] を選択します。
 - c. 作成した Microsoft Excel スプレッドシートを選択し、[添付ファイル] ダイアログ ボックスを閉じます。
 - d. スプレッドシートを添付した後、[すべてのレコードをロード] 関連リンクを選択して、スプレッドシートからインポートテーブルにすべてのレコードをロードします。操作が完了すると、データがエラーなしでロードされた場合は、成功 完了コードを含む次の確認メッセージが表示されま

Progress

Name	ImportProcessor
State	Complete
Completion code	Success
Message	Processed: 25, inserts 0, updates 0, errors 0, empty and ignored 25, ignored errors 0 (0:00:00.087)

Next steps...

- [Import sets](#) Go to the import sets for this data load
- [Loaded data](#) Go to the newly imported data inside the staging table: sg_isa_entity_import
- [Run Robust Transform](#) Transform a loaded import set using a robust transform
- [Import log](#) View the import log

す。

e. 確認メッセージで、[強力な変換を実行] 関連リンクを選択します。

f. **[Transform]** を選択します。インポートが成功すると、成功 完了コードを含む次の確認メッセージが表示されます。

Progress

Name	Transforming: ISET0010001
State	Complete
Completion code	Success
Message	Transformation complete

Next steps...

[ISET0010001](#) Go to the import sets for this data load

[Transform history](#) Show the transform history, related errors and log

[Import log](#) View the import log

す。

管理者以外の機器モデルサイトアクセス権をアサインまたは削除する

アドミニストレーター以外の機器モデルサイトへのアクセスをアサインまたは削除します。ユーザー基準を作成して、特定のユーザーが特定のサイトの機器モデルエンティティにアクセスできるかどうかを決定できます。

始める前に

必要なロール：admin

このタスクについて

ユーザー基準を使用して、特定のユーザーが特定のサイトの機器モデルエンティティを読み取ったり編集したりできるかどうかを判断します。ユーザー基準レコードを作成したら、それをサイトにアサインして、機器モデルエンティティを読み取って編集できるユーザーを制御できます。さらに、ユーザーまたはグループに OT ロールをアサインして、同じサイトにアサインされている OT デバイスにアクセスできるようにすることができます。詳細については、「[オペレーショナルテクノロジー マネージャー ロールの割り当て](#)」を参照してください。

i 注:

バージョン 1.0.12 にアップグレードするユーザーの場合、サイトユーザーアクセスはユーザー基準とグループに移行されます。詳細については、「[ユーザー基準およびグループへのサイトユーザーアクセスの移行](#)」を参照してください。

手順

1. 移動先 [すべて > ナレッジ管理 > 管理 > ユーザー基準](#)
2. **[新規]** を選択します。
3. フォームのフィールドに入力します。
フィールド値の説明については、「[\[ユーザー基準\] フォーム](#)」を参照してください。

次のタスク

ユーザー基準を作成したら、サイトに割り当てることができます。サイトへの [編集可能] アクセス権の割り当ての詳細については、「[サイトへの \[編集可能\] アクセスのユーザー基準をアサインする](#)」を参照してください。サイトに [読み取り可能] アクセス権を追加する方法の詳細については、「[サイトへの読み取り可能アクセスのユーザー基準をアサインする](#)」を参照してください。

サイトへの読み取り可能アクセスのユーザー基準をアサインする

ユーザー基準をサイトにアサインして、選択したサイトに属する機器モデルエンティティを読み取ったり表示したりできるユーザーを定義します。

始める前に

必要なロール:cmdb_ot_isa_admin または admin

このタスクについて

[読み取り可能] アクセスのユーザー基準は、次の 2 つの場所でアサインできます。

- 機器モデルエンティティビューアクセステーブルから
- サイトレコードの [Can Read Equipment Models (機器モデルの読み取りが可能)] 関連リストから

手順

1. テーブルまたは関連リストに移動します。
2. [新規] を選択してレコードを作成します。
3. [サイト] フィールドで、必要な機器モデルサイトレコードを選択します。
4. [ユーザー基準] フィールドで、選択したサイトの機器モデルエンティティを読み取ったり表示したりできるユーザーを定義するユーザー基準を選択します。

i 注:

ユーザーがcmdb_ot_viewerロールを持っている場合、選択したサイトにアサインされているオペレーショナルテクノロジー (OT) デバイスを表示することもできます。

ユーザーがcmdb_ot_editorロールを持っている場合、ユーザーは選択したサイトにアサインされている OT デバイスを編集できます。

5. [送信] を選択します。

サイトへの [編集可能] アクセスのユーザー基準をアサインする

ユーザー基準をサイトにアサインして、選択したサイトに属する機器モデルエンティティを編集できるユーザーを定義します。

始める前に

必要なロール:cmdb_ot_isa_admin または admin

このタスクについて

編集可能アクセスのユーザー基準は、次の 2 つの場所でアサインできます。

- 機器モデルエンティティ編集アクセステーブルから
- サイトレコードの [機器モデルを編集可能] 関連リストから

手順

1. 次のいずれかに移動します。
2. [新規] を選択してレコードを作成します。
3. [サイト] フィールドで、必要な機器モデルサイトレコードを選択します。
4. [ユーザー基準] フィールドで、選択したサイトの機器モデルエンティティを編集できるユーザーを定義するユーザー基準を選択します。

i 注:

ユーザーがcmdb_ot_viewerロールを持っている場合、選択したサイトにアサインされているオペレーショナルテクノロジー (OT) デバイスを表示することもできます。

ユーザーがcmdb_ot_editorロールを持っている場合、ユーザーは選択したサイトにアサインされている OT デバイスを編集できます。

5. [送信] を選択します。

機器モデルエンティティのスケジュールを管理する

機器モデルエンティティのスケジュールは、産業用プロセスマネージャー アプリケーションを使用して管理できます。スケジュールを使用すると、1 つの機器モデルエンティティに対する複数のメンテナンスタスクを追跡できます。

概要

スケジュールを任意の機器モデルエンティティにリンクすることができます。機器モデルダウタイム計画者ロール (sn_isa_schedule_admin) を持っている場合は、機器モデルエンティティのスケジュールエントリを追加、変更、または削除し、次のタスクを実行できます。

- さまざまな機器モデルエンティティのスケジュールを管理します。
- これらのスケジュールを機器モデルエンティティに関連付けます。
- オペレーショナルテクノロジー (OT) インシデントまたは修復タスクに取り組めるように、スケジュールからタイムスロットを選択します。詳細については、[OT 修復タスクの開始時間の選択](#)を参照してください。

例

たとえば、1 つの機器モデルエンティティのスケジュールに複数のスケジュールエントリを設定するとします。これらのエントリは、異なるタスクを完了し、異なる時間に発生します。これを行うには、既存の機器モデルエンティティのスケジュールレコードの [スケジュールエントリ] 関連リンクでスケジュールエントリを作成します。

機器モデルエンティティに関連付けられたスケジュールが不要になった場合は、機器モデルエンティティレコードのスケジュール関連リンクを使用してスケジュールをデタッチできます。

機器モデルエンティティの既存のスケジュールを表示する場合は、機器モデルマネージャーまたはプラットフォームの計画されたダウタイムモジュールで表示できます。

機器モデルエンティティのスケジュールを作成する

産業用プロセスマネージャー アプリケーションを使用して機器モデルエンティティのスケジュールを作成します。これらのスケジュールを使用すると、複数の機器モデルエンティティを簡単に管理できます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **産業用プロセスマネージャー** > **機器モデルエンティティのスケジュール**.
2. [新規] を選択します。
3. フォームのフィールドに入力します。

機器モデルエンティティのスケジュールフォーム

フィールド	説明
名前	スケジュールの一意の名前です。
タイムゾーン	スケジュールのタイムゾーンです。[フローティング] を選択した場合、タイムゾーンは、アイテムにアクセスしているプロセスに対して相対的になります。 たとえば、アムステルダムのリソースマネージャーがフローティングスケジュールを 8:00 から 17:00 に設定した場合、カリフォルニア州サンノゼのユーザーにもそのスケジュールが 8:00 から 17:00 と表示されます。あるタイムゾーンでスケジュールを定義すると、異なるタイムゾーンのユーザーには、それぞれのタイムゾーンのスケジュールが表示されます。
タイプ	スケジュールの目的を説明するテキストラベル。
説明	スケジュールの説明。

4. [送信] を選択します。

次のタスク

これで、機器モデルエンティティスケジュールのエントリを作成できます。詳細については、「[スケジュールエントリの作成](#)」を参照してください。

スケジュールエントリの作成

産業用プロセスマネージャー アプリケーションで、既存の機器モデルエンティティのスケジュールのスケジュールエントリを作成します。1 つのスケジュールに対して複数のエントリを作成できます。スケジュールエントリを使用すると、1 つの機器モデルエンティティに対して複数のメンテナンスタスクを実行できます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて** > **産業用ワークスペースアドミン** > **産業用プロセスマネージャー** > **機器モデルエンティティのスケジュール**.
2. 既存の機器モデルエンティティスケジュールレコードを選択します。

3. [スケジュールエントリ] タブを選択します。
4. [新規] を選択します。
5. フォームのフィールドに入力します。

スケジュールエントリフォーム

フィールド	説明
名前	スケジュールエントリの一意の名前。
タイプ	スケジュールの目的を説明するラベル。
表示方法	カレンダーアプリケーションでのスケジュールエントリの表示方法を示すオプション。
繰り返し	スケジュールエントリの繰り返し間隔 (存在する場合)。繰り返し間隔を選択すると、他のフィールドが表示され、繰り返し間隔をさらに指定できます。
繰り返し間隔	スケジュールの繰り返し頻度 (週次、月次、または年次)。このフィールドは、[繰り返し] フィールドで [日次]、[週次]、[月次]、または [年次] が選択されている場合にのみ表示されます。
繰り返し：	週次スケジュールが繰り返される曜日。このフィールドは、[繰り返し] フィールドで [週次] が選択されている場合にのみ表示されます。
月次タイプ	月次スケジュールの繰り返し頻度。このフィールドは、[繰り返し] フィールドで [月次] が選択されている場合にのみ表示されます。次のオプションがあります。 - 毎月特定の日に繰り返します。 - 月の特定の週の特定の日に繰り返します。 - 月の最終日に繰り返します。 - 月の最終週の特定の曜日に繰り返します。
年次タイプ	年次スケジュールの繰り返し頻度。このフィールドは、[繰り返し] フィールドで [年次] が選択されている場合にのみ表示されます。次のオプションがあります。 - 年の特定の日に繰り返します。 - 浮動日に繰り返します。
浮動週	浮動年次スケジュールが繰り返される月の週。このフィールドは、[年次] フィールドで [フローティング] が選択されている場合にのみ表示されます。
浮動日	浮動年次スケジュールが繰り返される曜日。このフィールドは、[年次] フィールドで [フロー

フィールド	説明
	ティング] が選択されている 場合にのみ表示されます。
月	浮動年次スケジュールが繰り返される年の月。このフィールドは、[年次] フィールドで [フローティング] が選択されている 場合にのみ表示されます。
繰り返し期限	繰り返し終了日。このフィールドを空のままにすると、スケジュールが無期限に繰り返されます。

6. [送信] を選択します。

タスクの結果

スケジュールエントリが作成され、必要に応じてエントリを編集および更新できます。

スケジュールを機器モデルエンティティに関連付ける

産業用プロセスマネージャー アプリケーションを使用して、機器モデルエンティティの 1 つ以上のメンテナンススケジュールの作成、既存のスケジュールの編集、またはスケジュールの削除を行います。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 機器モデル: ISA > 機器モデルエンティティ**.
2. スケジュールに関連付ける機器モデルエンティティを選択します。
3. [スケジュール] タブを選択します。
4. オプション: 選択した機器モデルエンティティの新しいスケジュールを追加するには、次のアクションを実行します。
 - [新規] を選択します。
 - フォームに入力し、[送信] を選択します。
5. オプション: 選択した機器モデルエンティティのスケジュールを削除するには、次のアクションを実行します。
 - 削除するスケジュールを選択します。
 - [削除] を選択します。
6. オプション: 選択した機器モデルエンティティのスケジュールを編集するには、次のアクションを実行します。
 - 編集するスケジュールを選択します。
 - 変更を追加し、[更新] を選択します。

タスクの結果

メンテナンススケジュールが作成、削除、または編集されたとき。実行した手順に応じて、対象ユーザーは新しいスケジュールを表示したり、削除されたスケジュールが表示されなくなったり、スケジュールの編集済みバージョンを表示したりできます。

機器モデルエンティティにスケジュールを添付する

産業用プロセスマネージャー アプリケーションを使用して、既存のスケジュールを機器モデルエンティティに添付します。機器モデルエンティティにスケジュールを添付すると、スケジュールとそのエントリがそのエンティティに適用されます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 機器モデル : ISA > 機器モデルエンティティ**.
2. 機器モデルエンティティレコードを選択します。
3. [スケジュール] タブを選択します。
4. [編集] を選択します。
5. [コレクション] リストで、機器モデルエンティティに添付するスケジュールを選択します。
6. 中央の矢印を使用して、選択したスケジュールを [スケジュール] リストに移動します。
7. [保存] を選択します。

タスクの結果

添付されたスケジュールが機器モデルエンティティに適用されます。機器モデルエンティティレコードで添付されたスケジュールを表示および管理できます。

機器モデルエンティティからスケジュールをデタッチする

産業用プロセスマネージャー アプリケーションを使用して、機器モデルエンティティから既存のスケジュールをデタッチします。スケジュールが機器モデルエンティティに適用されなくなった場合は、簡単に削除して、そのエンティティに表示されないようにすることができます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 **すべて > 機器モデル : ISA > 機器モデルエンティティ**.
2. 機器モデルエンティティレコードを選択します。
3. [スケジュール] タブを選択します。
4. [編集] を選択します。
5. [スケジュール] リストで、機器モデルエンティティからデタッチするスケジュールを選択します。
6. 中央の矢印を使用して、選択したスケジュールを [コレクション] リストに移動します。
7. [保存] を選択します。

機器モデルエンティティのスケジュールを表示する

産業用プロセスマネージャーアプリケーションで既存の機器モデルエンティティのスケジュールを表示します。

始める前に

必要なロール:cmdb_ot_isa_viewer

このタスクについて

機器モデルエンティティのスケジュールは、作業場所に応じて 2 つの場所で表示できます。

- 機器モデルマネージャー
- プラットフォーム上の計画されたダウンタイムモジュール

手順

1. 機器モデルマネージャーで機器モデルエンティティのスケジュールを表示するには、次のアクションを実行します。
 - a. 機器モデルマネージャーに移動します。
 - b. 機器モデルエンティティレコードを選択します。
 - c. [スケジュールを表示] を選択します。
 - d. その機器モデルエンティティのダウンタイムスロットを表示します。
2. 計画されたダウンタイムモジュールで機器モデルエンティティのスケジュールを表示するには、次のアクションを実行します。
 - a. 移動先 すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 計画されたダウンタイム。
 - b. スケジュールと機器モデルエンティティの関連付けを表示します。

子スケジュールを追加

産業用プロセスマネージャーアプリケーションを使用して、既存の機器モデルエンティティのスケジュールに子スケジュールを追加します。子スケジュールを調整すると、親スケジュールにも適用されます。たとえば、特定の日のスケジュールされた時間を延長したり、スケジュールから休日を削除したりできます。

始める前に

必要なロール:sn_isa_schedule_admin

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルエンティティのスケジュール。
2. 既存の機器モデルエンティティのスケジュールのレコードを選択します。
3. [子スケジュール] タブを選択します。
4. [編集] を選択します。
5. [コレクション] リストで目的のスケジュールを選択します。
6. 中央の矢印を使用して、選択したスケジュールを [子スケジュール] リストに移動します。
7. [保存] を選択します。

タスクの結果

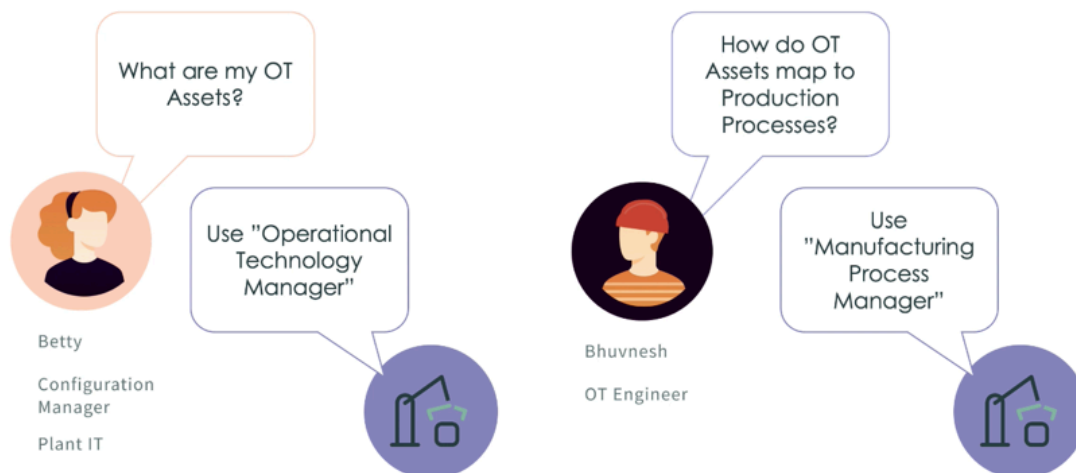
選択した子スケジュールが親スケジュールに適用されます。

での 産業用プロセスマネージャー の使用 オペレーショナルテクノロジー マネージャー

機器モデルのインポートなど、必要なすべてのセットアップタスクを完了すると、[産業用ワークスペースアドミン] メニューの [オペレーショナルテクノロジー マネージャー] および [産業用プロセスマネージャー] 機能を使用できます。これらの機能には、機器モデルマネージャーと Industrial Workspace が含まれます。

次の図は、企業の運用上の問題に関して産業担当者が尋ねる一般的な質問と、それに回答するために使用する Now Platform 機能を示しています。これらの機能は、担当者が産業施設内のデータ関係を視覚化するのに役立ちます。

運用上の問題に関する産業関係者の質問



構成マネージャーの Betty はエンタープライズレベルで作業しており、OT デバイスが企業内のどこにあるかを知りたいと考えています。この質問に答えるために、Configuration Manager は [産業用ワークスペースアドミン] メニューの オペレーショナルテクノロジーマネージャー 機能を使用できます。詳細については、「[産業用ワークスペースアドミン アプリケーションメニューとガイド付きセットアップ](#)」を参照してください。

OT エンジニアの Bhuvnesh は、現場レベルで作業しており、OT デバイスが特定の生産プロセスにどのようにマッピングされるかを知りたいと考えています。たとえば、「どのHMIとPLCが産業プロセスのこの特定の部分を制御しているか? この質問に答えるために、サイトレベルの OT マネージャーは、産業用ワークスペースアドミンメニューの産業用プロセスマネージャー機能を使用できます。

機器モデルの管理

機器モデルマネージャーを使用すると、ISA-95 機器モデルデータを確認および管理できます。これを使用して、インポートされた機器モデルデータを確認したり、機器モデルを手動で作成したりします。

機器モデルは、特定の施設の運用要素をマッピングします。たとえば、材料を保管し、それを使用して自動車を製造するアトランタの産業施設などです。機器モデルマネージャーを使用すると、特定の産業サイトの機器モデルエンティティを選択して表示し、次のタスクを実行できます。

- 機器モデルの階層と他のエンティティとの関係をグラフィカルに表示します。
- 上流または下流の生産プロセスを表示またはマッピングします。
- 子エンティティを確認します。
- 追加の OT デバイスをレビューするか、選択した機器モデルエンティティに関連付けます

i 注:

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、割り当てられたcmdb_ot_isa_editorまたはcmdb_ot_isa_viewerロールを持つユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

機器モデルの詳細の確認と更新

Now Platform にインポートした機器モデルの詳細を確認して更新し、情報が正しいことを確認します。新しい機器モデルエンティティを手動で作成し、それに詳細を追加することもできます。

始める前に

機器モデルデータを Now Platformにインポートします。詳細については、「[機器モデルデータのインポート](#)」を参照してください。

必要なロール:cmdb_ot_isa_viewer、cmdb_ot_isa_editor、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_viewerロールが割り当てられている場合は、機器モデルエンティティのみを表示できます。他のアサインされたcmdb_ot_isaロールがある場合は、機器モデルエンティティを編集することもできます。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**。
2. [**Equipment model view for** (次の機器モデルビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. 既存の機器モデルエンティティをレビューするか、作成します。
4. フォームで、フィールドを確認および更新します。

機器モデルの詳細フォーム

フィールド	Description (説明)
エンティティ名	機器モデルエンティティの名前。 i 注: 機器モデルエンティティの作成後に [エンティティ名] フィールドを更新できます。このフィールドを更新すると、ツリーコンポーネントとサイトフィルターも更新されます。 詳細については、「機器モデルエンティティのエンティティ名または親を更新する」を参照してください。
親	この機器モデルエンティティの親であるエンティティの名前 (存在する場合)。このフィールドは、親を持たない最上位の親エンティティでは空です。最上位の親エンティティはサイトと呼ばれます。

フィールド	Description (説明)
	i 注: 機器モデルエンティティの作成後に [親] フィールドを更新できます。 このフィールドを更新すると、ツリーコンポーネントとサイトフィルターも更新されます。詳細については、「機器モデルエンティティのエンティティ名または親を更新する」を参照してください。
テンプレート	手動で作成した機器モデルエンティティにアサインされる機器モデルテンプレート。 i 注: 統合ハブ ETL またはサードパーティ統合を使用して Now Platform にインポートした機器モデルに機器モデルテンプレートをアサインすることはできません。
レベル	データのソートと構造化の目的で、選択した機器モデルテンプレートからアサインされた階層レベル。次に例を示します。 サイト 工業用地。 面 工業用地のエリア。 ワークセンター 工業用地のワークセンター。 機器モデルエンティティに割り当てる機器レベルを検索して選択します。詳細については、「機器モデルテンプレートの階層ソートレベルを作成する」を参照してください。
タイプ	機器モデルテンプレートレベルにアサインされているレベルタイプの名前。たとえば、ワークセンターレベルの品目組立や生産セルなどです。詳細については、「機器モデルレベルタイプを作成する」を参照してください。
簡単な説明	この機器モデルエンティティとその目的の簡単な説明。
短縮コード	この機器モデルエンティティにアサインされている短縮コード。
パス	この機器モデルエンティティとそのすべての親エンティティの短縮コードの連結。たとえば、ATL-B42-MQSTOR-Z1 は、次の短縮コードを連結したものです。

フィールド	Description (説明)
	- アトランタサイトの ATL 短縮コード。 - 建物 B42 の B42 短縮コード。 - モデル M および Q の MQSTORE 短縮コード。 - モデル M および Q のゾーン 1 転送ストレージゾーンの Z1 短縮コード。
Location (ロケーション)	機器モデルエンティティの場所。たとえば、アトランタビル 64 は、そこに配置されている各関連機器モデルの場所です。機器モデルエンティティに割り当てる場所を検索して選択します。
Company (チェックアウト日時)	機器モデルエンティティに関連付けられている会社の名前。エンティティに割り当てる会社を検索して選択します。
Assigned to (アサイン先)	この機器モデルエンティティを操作および処理するアサインされたユーザー。エンティティに割り当てるユーザーを検索して選択します。
Managed by (管理担当者)	このエンティティレコードを所有し、管理を担当するアサインされた人物の名前。機器モデルエンティティにアサインするユーザーを検索して選択します。
プロセスの重要度	機器モデルエンティティが産業プロセスにとってどの程度重要かを示す指標。エンティティのプロセスの重要度を選択します。例： 1 - 最重要。 2 - ある程度重要。
サポートグループ	この機器モデルエンティティをサポートするグループの名前。機器モデルエンティティに割り当てるユーザーグループを検索して選択します。
管理担当者グループ	このエンティティレコードを所有し、管理を担当するアサイン先グループの名前。エンティティに割り当てるユーザーグループを検索して選択します。
Company (チェックアウト日時)	機器モデルエンティティが属する会社の名前。core_company値は、Now Platform内のCMDBに参照として格納されます。
運用ステータス	機器モデルエンティティの現在の運用ステータス： Operational (稼働中) 生産プロセスで完全に稼働しているエンティティ。 非稼働 生産プロセスで稼働していないエンティティ。

5. 関連リストタブで、関連する機器モデルデータを次のように確認します。

タスク	Description (説明)
機器モデル階層を表示する	「 機器モデル階層を表示する 」を参照してください。
機器モデルエンティティの上流の生産プロセスをマッピングします。	a. [上流プロセス] をクリックします。 b. 詳細については、「選択した機器モデルエンティティの上流の生産プロセスをマッピングします」を参照してください。
機器モデルエンティティの下流の生産プロセスをマッピングします。	a. [ダウンストリームプロセス] をクリックします。 b. 詳細については、「選択した機器モデルエンティティの下流の生産プロセスをマッピングします」を参照してください。
機器モデルエンティティの子エンティティを表示します。	a. 「子エンティティ」 (Child Entities) をクリックします。 b. 詳細については、「機器モデルエンティティの子エンティティのレビュー」を参照してください。
現在の機器モデルエンティティとその子エンティティに関連付けられている OT デバイスを表示します。	a. [マッピングされた OT デバイス] をクリックします。 b. 詳細については、「選択した機器モデルエンティティに関連付けられている OT デバイスを追加します」を参照してください。 i 注: デフォルトでは、このリストに OT コントロールモジュールは表示されません。

6. 機器モデルの詳細の確認と更新が完了したら、次のいずれかのアクションを実行します。

7. オプション: 機器モデルエンティティとその子エンティティに関連付けられたさまざまな OT データを表示するには、機器モデルエンティティレコードで次の関連リストを選択します。

- マッピングされた OT デバイス
- OT インシデント
- OT 変更要求
- 脆弱性一致アイテム
- 修復タスク

新しい機器モデルのエンティティを作成する

新しい機器モデルのエンティティを作成します。このタスクは、外部ソースから機器モデルデータをインポートするのではなく、Now Platform で直接新しい機器モデルエンティティを手動で作成する場合に実行します。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられたユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

手順

1. 移動先 [すべて](#) > [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > [機器モデルマネージャー](#)。
2. **[Equipment model view for (次の機器モデルビュー)]** フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. **[新しいエンティティの作成]** を選択します。
4. **[新しいエンティティを作成]** ウィンドウで、親エンティティを検索して選択します。



注:

親エンティティは、短縮コードまたは名前で検索できます。

5. フォームのフィールドに入力します。

[新しいエンティティの作成] フォーム

フィールド	説明
親	このエンティティの親であるエンティティの名前 (存在する場合)。 現在選択されている機器モデルが親エンティティとして表示されます。親を変更するには、作成しているエンティティの親であるエンティティを検索して選択します。
エンティティ名	機器モデルエンティティの名前。
短縮コード	このエンティティにアサインされた短縮コード。
エンティティタイプ	機器モデルテンプレートレベルにアサインされているレベルタイプの名前。たとえば、ワークセンタレベルの品目組立や生産セルなどです。 エンティティタイプを検索して選択します。詳細については、「 機器モデルレベルタイプを作成する 」を参照してください。

6. **[保存]** を選択します。
7. **[詳細]** フォームで、新しい機器モデルエンティティの残りの詳細を入力します。
詳細については、「[機器モデルの詳細の確認と更新](#)」を参照してください。

機器モデル階層を表示する

選択した機器モデルエンティティの階層構造と、生産プロセス内の他のエンティティとの関係をグラフィカルに表示します。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、割り当てられたcmdb_ot_isa_editorまたはcmdb_ot_isa_viewerロールを持つユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

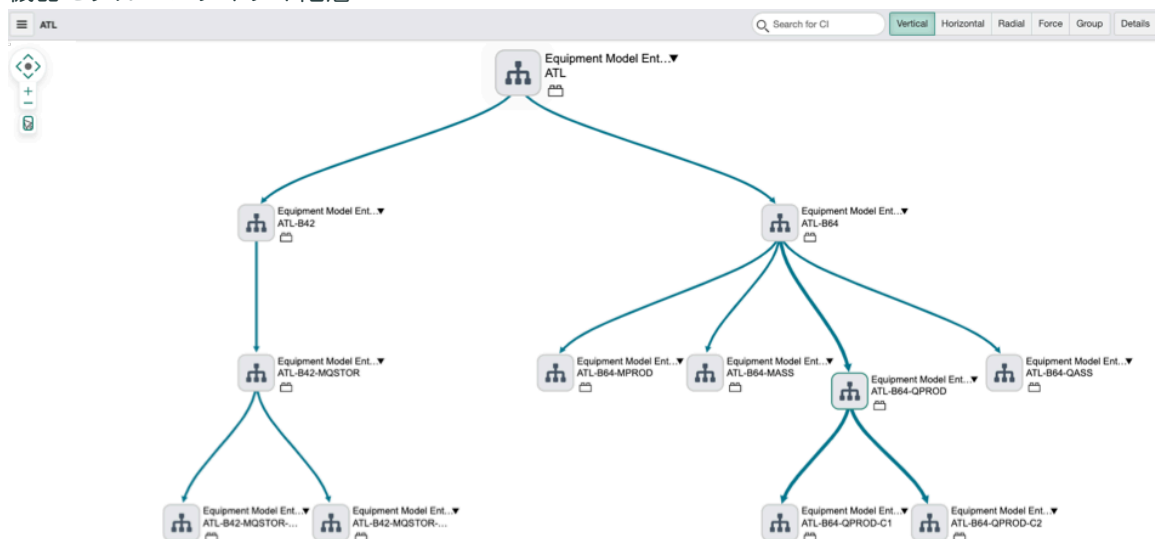
手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**。
2. [**Equipment model view for** (次の機器モデルビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. セレクターペインで、その階層と他のエンティティとの関係をグラフィカルに表示する機器モデルエンティティをクリックします。
たとえば、トップレベルのサイトエンティティをクリックすると、サイト全体の表現が表示されます。
4. 機器モデルエンティティの階層構造を表示するには、[**View hierarchy** (階層を表示)] をクリックします。

タスクの結果

選択した機器モデルエンティティについて、次のグラフィックが表示されます。現在選択されている機器モデルが、階層内の親エンティティとして表示されます。

機器モデルエンティティ階層



機器モデル OT デバイスマップを表示する

選択した機器モデルエンティティと、生産プロセス内の他の オペレーショナルテクノロジー (OT) デバイスとの関係をグラフィカルに表示します。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、割り当てられたcmdb_ot_isa_editorまたはcmdb_ot_isa_viewerロールを持つユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

手順

1. 移動先 [すべて](#) > [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > [機器モデルマネージャー](#).
2. [**Equipment mode view for** (次の機器モードビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. セレクターペインで、他のデバイスとの関係をグラフィカルに表示する機器モデルエンティティを選択します。
たとえば、トップレベルのサイトエンティティを選択して、サイト全体の表現を表示します。
4. 機器モデルエンティティとデバイスの関係を表示するには、[**OT デバイスマップを表示**] を選択します。

機器モデルの **OT** 依存関係マップを表示する

選択した機器モデルエンティティの階層構造と、生産プロセス内の他のエンティティやデバイスとの関係をグラフィカルに表示します。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、割り当てられたcmdb_ot_isa_editorまたはcmdb_ot_isa_viewerロールを持つユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

手順

1. 移動先 [すべて](#) > [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > [機器モデルマネージャー](#).
2. [**Equipment mode view for** (次の機器モードビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. セレクターペインで、その階層や他のデバイスやエンティティとの関係をグラフィカルに表示する機器モデルエンティティを選択します。
たとえば、トップレベルのサイトエンティティを選択して、サイト全体の表現を表示します。
4. 機器モデルエンティティと他のデバイスやエンティティとの関係の階層構造を表示するには、[**OT 依存関係マップを表示**] を選択します。

選択した機器モデルエンティティの上流の生産プロセスをマッピングします

上流プロセスを使用して、選択した機器モデルエンティティの上流生産プロセスをレビューします。機器モデルエンティティの新しい上流生産プロセスを作成してマッピングすることもできます。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_viewer、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられたユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

手順

1. 移動先 [すべて](#) > [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > [機器モデルマネージャー](#).
2. [**Equipment model view for** (次の機器モデルビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティをクリックします。
4. 機器モデルエンティティの上流生産プロセスを表示するには、[[上流プロセス](#)] をクリックします。
5. 機器モデルの上流の生産プロセスをレビューするか、新しいプロセスをマッピングします。
6. [送信] をクリックします。

選択した機器モデルエンティティの下流の生産プロセスをマッピングします

ダウンストリームプロセスを使用して、選択した機器モデルエンティティの下流の生産プロセスをレビューします。機器モデルエンティティの新しい下流生産プロセスを作成してマッピングすることもできます。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_viewer、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられたユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

手順

1. 移動先 [すべて](#) > [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > [機器モデルマネージャー](#).
2. [**Equipment model view for** (次の機器モデルビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティをクリックします。
4. 機器モデルエンティティの下流の生産プロセスを表示するには、[[下流プロセス](#)] をクリックします。
5. 機器モデルの下流の生産プロセスをレビューするか、新しいプロセスをマッピングします。

6. [送信] をクリックします。

機器モデルエンティティの子エンティティのレビュー

選択した機器モデルエンティティに関連付けられている子エンティティを確認します。上位レベルのエンティティに従属する関連エンティティの関係を確認できます。

始める前に

必要なロール:cmdb_ot_isa_editor、cmdb_ot_isa_admin

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、cmdb_ot_isa_editor ロールが割り当てられたユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

手順

1. 移動先 [すべて](#) > [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > [機器モデルマネージャー](#)。
2. [**Equipment model view for** (次の機器モデルビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
サイト名またはその短縮コードを入力してサイトを検索できます。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティをクリックします。
4. 機器モデルエンティティの子エンティティを表示するには、[**Child Entities** (子エンティティ)] をクリックします。
5. 新しい子エンティティを作成するには、[**Create new entity**] (新しいエンティティの作成)ボタンをクリックし、[Create new entity] (新しいエンティティの作成)フォームに詳細を入力します。
詳細については、「[新しい機器モデルのエンティティを作成する](#)」を参照してください。

選択した機器モデルエンティティに関連付けられている OT デバイスを追加します

OT デバイスを使用して、選択した機器モデルエンティティとその子エンティティに関連付けられている OT デバイスを確認します。他の OT デバイスを選択して、選択した機器モデルエンティティに関連付けることもできます。

始める前に

選択した機器モデルエンティティに追加の OT デバイスに関連付けるには、オペレーショナルテクノロジーマネージャー アプリケーションと 産業用プロセスマネージャー アプリケーションの両方をインストールする必要があります。

必要なロール:OT デバイスを追加するには、ログインユーザーは次のアサインされたロールの組み合わせを持っている必要があります。

- cmdb_ot_viewer、cmdb_ot_editor、またはcmdb_ot_adminロール
- cmdb_ot_isa_editorまたはcmdb_ot_isa_adminロール

注:

ユーザーロールの割り当ての詳細については、「[産業用プロセスマネージャーユーザーロールのアサイン](#)」を参照してください。

このタスクについて

cmdb_ot_isa_adminロールがアサインされたユーザーは、任意のサイトの機器モデルエンティティを表示できます。ただし、割り当てられたcmdb_ot_isa_editorまたはcmdb_ot_isa_viewerロールを持つユーザーは、管理者が特定のユーザーにアクセス権を付与したサイトにのみアクセスできます。サイト アクセスの許可の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
サイト名またはその短縮コードを入力してサイトを検索できます。
2. [**Equipment model view for** (次の機器モデルビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
3. セレクターペインで、機器モデル階層を展開し、表示するエンティティをクリックします。
4. 機器モデルエンティティとその子エンティティに関連付けられた OT デバイスを表示するには、[マッピングされた **OT** デバイス] をクリックします。
5. 関連付けられている OT デバイスを確認するか、選択した機器モデルエンティティに追加の OT デバイスに関連付けます。
6. [保存] をクリックします。

機器モデルエンティティのエンティティ名または親を更新する

機器モデル情報を最新の状態に保つために、必要に応じて機器モデルエンティティレコードのエンティティ名または親フィールドを更新します。

始める前に

必要なロール:cmdb_ot_isa_editor

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース).
2. 機器モデル ( ボタン)を選択します。
または、 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー**.
3. 更新する機器モデルエンティティレコードを選択します。
4. 必要に応じて [エンティティ名] フィールドまたは [親] フィールドを更新します。
5. [保存] を選択します。

タスクの結果

[エンティティ名] または [親] フィールドを更新すると、機器モデルマネージャーのツリーコンポーネントと、産業用 ワークスペースのオペレーショナルテクノロジー (OT) ランディングページのサイトフィルターフィールドも更新されます。

サイトのオペレーショナルテクノロジー脆弱性対応 アサイン先グループを一括編集する

一括編集機能を使用して、複数のサイトレコードの オペレーショナルテクノロジー脆弱性対応 (OT VR) アサイン先グループフィールドを一度に更新します。

始める前に

必要なロール:cmdb_ot_isa_admin

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. リスト ( ビューを開きます。
3. **Industrial Process Manager** (産業用プロセスマネージャー) モジュールで、[Sites (サイト)] リストを選択します。
4. 編集する各 OT サイトの横にあるチェックボックスをオンにします。
5. [編集] ボタンを選択します。
6. [**OT VR** アサイン先グループ] フィールドで、選択したサイトの オペレーショナルテクノロジー脆弱性対応 アサイン先グループを追加します。
7. [更新] を選択します。

タスクの結果

選択したサイトごとに **[OT VR アサイン先グループ (OT VR assignment group)]** フィールドが更新されます。

OT デバイスから機器モデルへの自動マッピング

OT デバイスの生産プロセスへのマッピングを自動化します。

OT マネージャーが脆弱性を経験した、または OT デバイスに関連するワークフローを管理する必要がある場合、自動化した本番プロセスに OT デバイスをどのように接続するかというコンテキストが、作業の優先順位付けにとって重要になります。OT デバイスから ISA 機器モデルエンティティへの自動マッピングにより、デバイスとプロセスの関係を表示できます。

i 注:

サイトごとに 1 つのサブネット範囲のみがサポートされます。2 つの異なるサイトが同じサブネットを持つことができます。たとえば、192.168.101.0/24 です。ただし、同じ サイトで同じ範囲の複数のサブネットはサポートされていません。このシナリオでは、手動マッピングを使用することをお勧めします。

主な特長

- 信頼できるソース (NetDB やファイアウォールなど) から OT サブネットをレコードとして ServiceNow インスタンスにアップロードして保存します。
- IP アドレスと OT サブネットを使用して、ISA エンティティへの OT デバイスのアサインを自動化する
- 複数のサイトでのプライベートIPアドレス範囲の再利用に関する問題を最小限に抑える

産業用ネットワークでは、サブネットを使用してプライベート IP アドレス空間を 1 つのサブネットに分割し、多くの場合、生産プロセスの一部または機器モデル エンティティに合わせて調整します。例: 缶詰ラインは、すべての機器がインテグレーターによってプログラムされた 192.168.101.0/24 ネットワーク上で動作します。制御システムや OT デバイスで使用される IP は、多くの場合、ラインの稼働に使用されるオートメーションソフトウェアにハードコードされています。サブネットがアトランタのサイトの缶詰ラインにマッピングされている場合、マネージャーは IP 192.168.101.66 の検出された PLC を缶詰ラインに自動的にマッピングできます。

マッピング機能は各サブネットを機器モデルエンティティに関連付け、OT の OT 認定統合または ServiceNow **Discovery for OT** (OT の ディスカバリー) からのインポート時に報告された IP アドレスに基づいて、機器モデルエンティティに関連付けられたサブネットに OT デバイスを自動的にマッピングできるようにします。

システムアドミニストレーターは OT サブネットマッピングレコードをインポートできます。ISA アドミニストレーターは、スケジュール済みジョブフローを通じて、機器モデルエンティティへのサブネットのマッピングを自動的に作成できます。ISA エディターは、個々の OT デバイスのマッピングをオンデマンドで手動で作成できます。

自動マッピング機能のペルソナ

自動マッピング機能は、次のペルソナを対象としています。

自動マッピングのペルソナ

ペルソナ	Description (説明)
システムアドミン	システムアドミニストレーターは、次のタスクを実行します。 - データを OT サブネットから機器モデルエンティティへのマッピングテーブルにインポートします - OT サブネットマッピングのスケジュール済みフローをアクティブ化、スケジュール、または手動でトリガーします
ISA アドミン	ISA アドミンは、[OT サブネットマッピング] リストビューから [すべての OT デバイスをマッピング] UI アクションを手動でトリガーします。
ISA エディター	ISA エディターは次のタスクを実行します。 - 特定のサイトの OT サブネットマッピングエントリーを手動で作成および更新します - 個々の OT デバイスを OT デバイスレコードの機器モデルエンティティにマッピングします - 複数の OT デバイスを OT サブネットマッピングレコードの機器モデルエンティティにマッピングします

プラグイン

マッピング機能を有効にするには、次のプラグインが必要です。

- オペレーショナルテクノロジーマネージャー
- 産業用プロセスマネージャー

必要なプラグインがインストールされている場合、ISA アドミニストレーターは 産業用プロセスマネージャー アプリケーションメニューからサブネットマッピング機能にアクセスできます。

自動マッピング機能のワークフロー

産業用プロセスマネージャーには、自動マッピング機能の自動フローが含まれています。

この機能には事前定義されたフローが含まれており、これを使用して機器モデルエンティティへの OT デバイスのアサインをスケジュールできます。

Flow Designer を使用することで、ビジネスニーズに合わせて事前定義されたフローをレビューして構成できます。

この機能で利用可能なフロー

次の表は、オペレーショナルテクノロジーマネージャー とともにインストールしたときに 産業用プロセスマネージャー で使用できる事前定義されたフローを示しています。

アプリケーション	フロー
産業用プロセスマネージャー インストールされている場合 オペレーショナルテクノロジーマネージャー	OT デバイスマッピングフロー

自動マッピング機能の一般的なユースケース

これらのユースケースは通常、自動マッピング機能に適用されます。

- OT マネージャーが既存の OT デバイスを所有しており、個々の OT デバイスをオンデマンドでマッピングしたいと考えている。
- OT アドミンは、有効な IP アドレスを持つ新しく検出された OT デバイスを機器モデルエンティティに自動的にマッピングしたいと考えています。

自動マッピング機能の一般的なワークフローを次に示します。

- システムアドミンは、Easy Import を使用して、Excel スプレッドシートから OT サブネットマッピングテーブルに OT サブネットデータをインポートします。
- 優れたアドミンがインポートされたデータレコードをレビューし、OT サブネットマッピングレコードをサイトやそのサイト内の機器モデルエンティティに関連付け (マッピング) します。
- 優れたアドミンは、スケジュール済みフローをアクティブ化またはトリガーして、インスタンス上のすべてのサイトの OT デバイスを自動的にマッピングします。
- Amazing エディターは、編集アクセス権を持つサイトに属するレコードを更新できます。

ガイド付きセットアップを使用して OT デバイスの自動マッピングを構成する

産業用プロセスマネージャーガイド付きセットアップを使用して、OT デバイスを ISA 機器モデルエンティティに自動的にマッピングします。

始める前に

必要なロール：admin

このタスクについて

admin ロールを持っている場合は、産業用プロセスマネージャー ガイド付きセットアップを使用して、OT デバイスを ISA 設備階層モデルエンティティにマッピングする方法を順を追って説明できます。アクセスできるサイトの OT デバイスをマッピングできます。

手順

1. 移動先 すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ。
2. 産業用プロセスマネージャー アプリケーションの [開始] を選択します。
3. [OT デバイスを自動的にマッピング] タスクを選択します。
4. 次のタスク タブを選択し、[構成] を選択して構成タスクを完了します。

関連情報

[Guided setup](#)[OT デバイスから機器モデルへの自動マッピング](#)

すべての **OT** デバイスを機器モデルエンティティに自動的にマッピングする

優れたアドミンは、すべての OT デバイスから適切な ISA 機器モデルエンティティへの自動マッピングをトリガーできます。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [産業用プロセスマネージャー](#)

必要なロール:sn_ot_amazing_admin

手順

1. 移動先 [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > **OT** サブネットマッピング.
2. [すべての **OT** デバイスをマッピング] を選択して、[OT デバイスをマッピング] フローを実行します。

タスクの結果

OT デバイスは、すべての「アクティブ」な OT サブネットマッピングレコードにリストされている機器モデルエンティティに自動的にマッピングされます。マッピングがトリガーされた後、リストビューから情報メッセージで利用可能なリンクを選択して、マッピング結果を表示できます。

サブネット内のすべての **OT** デバイスをマッピング

OT アドミンは、選択したサブネット内のすべての OT デバイスの自動マッピングをトリガーできます。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [産業用プロセスマネージャー](#)

必要なロール:sn_ot_amazing_write

手順

1. 移動先 [産業用ワークスペースアドミン](#) > [産業用プロセスマネージャー](#) > **OT** サブネットマッピング.
2. [OT サブネットマッピング] リストから、デバイスをマッピングする OT サブネットマッピングレコードを開きます。
3. [サイト] フィールドと [機器モデルエンティティ] フィールドが正しく入力されていることを確認します。
4. このサイト内のすべての OT デバイスを選択した OT サブネットの IP アドレスに自動的にマッピングするには、[このサブネットの **OT** デバイスを マッピング] UI アクションを選択します。

タスクの結果

選択した IP 範囲内の IP アドレスを持つ OT デバイスが選択したサイトにある場合、サイト内のすべてのデバイスが OT サブネットにマッピングされます。マッピングがトリガーされた後、リストビューから情報メッセージで利用可能なリンクを選択して、マッピング結果を表示できます。

サイトにアサインされていない **OT** デバイスを表示する

サイトにアサインされていない オペレーショナルテクノロジー (OT) デバイスのリストを表示します。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [産業用プロセスマネージャー](#)

必要なロール:cmdb_ot_isa_editor および cmdb_ot_editor

このタスクについて

OT デバイスマッピングの一環として、機器モデルエンティティにマッピングする前に、デバイスをサイトにアサインする必要があります。これを行うには、サイトにアサインされていないすべての OT デバイスのリストを表示します。

手順

1. 移動先 **すべて > オペレーショナルテクノロジー (OT) > サイトアサインのない OT デバイス**。
2. デバイスをサイトに個別にアサインするには、デバイスレコードを選択し、[サイト] フィールドを更新します。
3. 一括編集を実行して [サイト] 列を更新し、複数のデバイスを同じサイトに割り当てるには、次の手順を実行します。
 - a. サイトにアサインする各 OT デバイスの横にあるチェックボックスをオンにします。
 - b. (サイト) 列ヘッダーで、[Column options (列オプション)] ボタンを選択し、[**Update Selected**] (選択項目を更新) を選択します。
 - c. [サイト] フィールドを更新します。
 - d. [更新] を選択します。

次のタスク

OT デバイスはサイトにアサインされていますが、機器モデルエンティティにはマッピングされていません。マッピングされていない OT デバイスのリストを表示して、デバイスのマッピングを完了することができます。詳細については、「[マッピングされていない OT デバイスを表示する](#)」を参照してください。

マッピングされていない **OT** デバイスを表示する

どの機器モデルエンティティにもマッピングされていない IP アドレスを持つ オペレーショナルテクノロジー (OT) デバイスのリストを表示します。

始める前に

次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [産業用プロセスマネージャー](#)

必要なロール:cmdb_ot_isa_editor および cmdb_ot_editor

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. オペレーショナルテクノロジー (OT) モジュールの 産業用 ワークスペース リストビューで、[マッピングされていない OT デバイス] リストを選択します。
このリストには、IP アドレスと、アサインされたサイトの機器モデルエンティティへのマッピングに使用できるその他のフィールドを含む OT デバイスレコードが表示されます。
3. オプション: [サイト] 列ヘッダーで、[フィルター] ボタンを選択し、[サイト別にグループ化] を選択します。
このフィルターを使用すると、マッピングされていない OT デバイスをサイト別に整理でき、複数のサイトを管理する場合に役立ちます。

次のタスク

これで、OT デバイスを機器モデルエンティティにマッピングできるようになりました。詳しくは、「[個々の OT デバイスを機器モデルエンティティにマッピングする](#)」を参照してください。

個々の OT デバイスを機器モデルエンティティにマッピングする

OT デバイスからアクセス可能なサイトの ISA 設備階層モデルエンティティへのオンデマンドマッピングを実行します。

始める前に

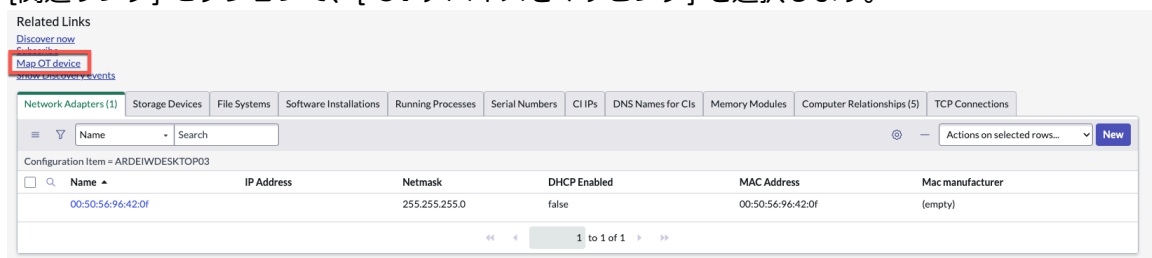
次のプラグインをインストールする必要があります。

- [オペレーショナルテクノロジーマネージャー](#)
- [産業用プロセスマネージャー](#)

必要なロール:sn_ot_amazing_write および cmdb_ot_viewer

手順

1. 移動先 すべて > オペレーショナルテクノロジー (OT) > すべての OT デバイス.
2. [OT デバイス] 列で、マッピングする OT デバイスを選択します。
3. [関連リンク] セクションで、[OT デバイスをマッピング] を選択します。



タスクの結果

選択したデバイスの IP アドレスとサイトに一致するアクティブな OT サブネットがある場合、デバイスがマッピングされます。

OT サブネットマッピングのスケジュール済みフローを構成する

OT デバイスマッピングフローを構成して、OT デバイスをサイトと機器モデルエンティティに自動的にマッピングします。

始める前に

次のプラグインをインストールする必要があります。

- オペレーショナルテクノロジーマネージャー
- 産業用プロセスマネージャー

必要なロール：admin

このタスクについて

OT デバイスマッピングフローをスケジュールに基づいて実行するように設定して、すべてのアクティブな OT サブネットマッピングレコードの OT デバイスを自動的にマッピングできます。

手順

1. 移動先 産業用ワークスペースアドミン > 産業用プロセスマネージャー > **OT** サブネットマッピングのスケジュール済みフロー。
2. オプション：サイトマッピングをアクティブ化します。
 - a. [フロー変数の設定] セクションを開きます。
 - b. [**Run Auto Assign Site**] の横にあるチェックボックスをオンにして、[**Save**] を選択します。
3. フローが定期的に行われるようにスケジュールするには、[トリガー] セクションのリンクを選択して間隔を定義します。
4. ヘッダーで [アクティブ化] を選択して、OT デバイスマッピングフローのスケジュールされた実行をアクティブ化します。
アクティブ化後、このフローをスケジュールに基づいて実行して、インスタンス上のすべてのアクティブな OT サブネットマッピングレコードの OT デバイスを自動的にマッピングできます。

OT サブネットマッピングを表示

機器モデルエンティティにアサインされたマッピング済みの OT サブネットをすべて表示します。

始める前に

必要なロール：

- sn_ot_amazing_write、cmdb_ot_isa_editor、cmdb_ot_viewerまたは
- sn_ot_amazing_admin、cmdb_ot_isa_editor、cmdb_ot_viewer

手順

1. 次のいずれかのオプションを使用して、機器モデルマネージャーに移動します。
 - 移動先 すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルマネージャー。
 - 移動先 すべて > **Industrial Workspace** (産業用ワークスペース). 機器モデル () アイコンを選択します。
2. 機器モデルビューからサイトを選択するか、機器モデル階層を展開してマッピングを表示するエンティティを選択します。
3. エンティティフォームで、[マッピングされた **OT** サブネット] 関連リストタブを選択します。
マッピングされた OT サブネットは、アクティブまたは非アクティブとして表示されます。アクティブな OT サブネットのみが スケジュール済みフローに含まれます。詳細については、「[OT サブネットマッピングのスケジュール済みフローを構成する](#)」を参照してください。
4. オプション：OT デバイスレベルでマッピングに使用される OT サブネットを表示するには、OT デバイスレコードの [**OT** サブネット] 関連リストを選択します。

次のタスク

[新しい OT サブネットマッピングレコードを作成します](#)

新しい **OT** サブネットマッピングレコードを作成します

機器モデルエンティティに関連付ける新しい OT サブネットマッピングを作成します。

始める前に

必要なロール:sn_ot_amazing_write または sn_ot_amazing_admin

i 注:

新しい OT サブネットマッピングレコードを作成する場合、デフォルトでは新しいレコードは非アクティブです。OT デバイスマッピングフローがトリガーされたときにレコードを自動的にマッピングするには、OT サブネットマッピングレコードがアクティブである必要があります。

手順

1. 移動先 産業用ワークスペースアドミン > 産業用プロセスマネージャー > 機器モデルエンティティ。
2. 新しいマッピングを作成するサイトまたは機器モデルエンティティを選択します。
3. [マッピングされた **OT** サブネット] 関連リストを選択し、[新規] を選択します。
4. フォームのフィールドに入力します。

OT サブネットから機器モデルエンティティへのマッピングフォーム

Field (フィールド)	説明
名前	サブネットのゾーンまたは VLAN 名。
サイト	[ルックアップ] で、利用可能なサイトのリストから ISA サイトを選択します (まだ入力されていない場合)。
タイプ	次のオプションからサブネットタイプを選択します。 • IP 範囲 - サブネット内の IP アドレスのサブセット • IP ネットワーク - サブネット全体 (CIDR 表記)
開始 IP アドレス	IP 範囲の開始 IP このフィールドは、[タイプ] が [IP 範囲] の場合に表示されます。
終了 IP アドレス	IP 範囲の終了 IP このフィールドは、[タイプ] が [IP 範囲] の場合に表示されます。
ソース名	NetDB やファイアウォールなど、ソースの名前。
ファイアウォール名	ゾーンを管理しているファイアウォールの名前 (該当する場合)。
Description (説明)	サブネットマッピングの説明。
アクティブ	OT サブネットマッピングのスケジュール済みフローの実行時にサブネットを自動マッピングに含めるには、[アクティブ] を選択します。

Field (フィールド)	説明
機器モデルエンティティ	ルックアップで、利用可能なエンティティのリストから機器モデルエンティティを選択します (まだ入力されていない場合)。
サブネット	サブネットアドレス (CIDR 形式) を入力します。このフィールドは、[タイプ] が [IP ネットワーク] の場合に表示されます。
Location (ロケーション)	サブネットレコードに場所を追加して、マッピングされた OT デバイスの場所を自動的に追加または更新します。 <i>i</i> 注: 場所 は、sn_otsm.subnet_mapping.location_auto_update システムプロパティに基づいてマッピングされます。OT サブネットマッピングに使用されるシステムプロパティの詳細については、「OT サブネットマッピング機能で使用するシステムプロパティ」を参照してください。
インターフェイス名	ファイアウォールインターフェイスの名前 (該当する場合)。
VLAN ID	該当する場合は、VLAN ID を指定します。

5. [送信] を選択します。

マッピングされたすべての **OT** デバイスを表示

機器モデルエンティティにマッピングされているすべての オペレーショナルテクノロジー (OT) デバイスのリストを表示します。

始める前に

必要なロール:sn_ot_amazing_write または sn_ot_amazing_admin

手順

移動先 **すべて** > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > マッピングされた **OT** デバイス。

このリストには、さまざまな機器モデルエンティティにマッピングされているすべてのデバイスが含まれています。[**Automates by :: Automates CI** (自動化担当者:: 自動化)] CI 関係は、親エンティティと子エンティティに適用されます。

OT サブネットマッピング機能で使用するシステムプロパティ

優れたアドミンは、OT サブネットマッピング機能をサポートするシステムプロパティを表示および構成できます。

優れたアドミンロールを持つユーザーは、次の場所に移動して OT サブネットマッピングプロパティ設定にアクセスできます。 産業用ワークスペースアドミン > 産業用プロセスマネージャー > **OT** サブネットマッピングのプロパティ。

OT サブネットマッピングのシステムプロパティ

プロパティ	Description (説明)
<code>sn_otsm.map_all_ot_assets.all_discovery_source</code>	すべてのディスカバリーソースの OT デバイスのマッピングを制御します。すべてのディスカバリーソースの OT デバイスをマッピングします。オンにすると、以下の特定のディスカバリーソースが上書きされます。デフォルトは [はい] (true) です。 デフォルト値: True
<code>sn_otsm.map_all_ot_assets.discovery_source</code>	指定されたディスカバリーソースの OT デバイスをマッピングします (カンマ区切り形式)。上記の [すべてのディスカバリーソースの OT デバイスをマッピング] がオフの場合にのみ適用されます。
<code>sn_otsm.subnet_mapping.auto_assign_ot_devices</code>	Owner/Owned by 関係に基づいて、すべての OT コントロールモジュールを機器モデルエンティティに自動的にアサインします。デフォルトは [はい] (true) です。
<code>sn_otsm.subnet_mapping.location_auto_update</code>	OT デバイスの場所をサブネットの場所を上書きします。オンにすると、サブネットにマッピングされたときに、サブネットの場所が OT デバイスの場所よりも優先されます。デフォルトは [はい] です。

産業用プロセスマネージャーとオペレーショナルテクノロジーマネージャーの両方がインストールされている場合にインストールされる自動マッピングコンポーネント

いくつかのタイプの自動マッピングコンポーネント (テーブル、システムプロパティ、スケジュール済みフローなど) も、産業用プロセスマネージャー がアクティブになるとインストールされます (オペレーショナルテクノロジーマネージャー もアクティブになります)。

これらの自動マッピングコンポーネントは、オペレーショナルテクノロジーマネージャー とともにインストールされるか、産業用プロセスマネージャー がとともにインストールされるときに使用可能になります。

テーブル

テーブル	Description (説明)
OT サブネットから機器モデルエンティティへのマッピング [ot_subnet_mapping]	OT サブネットと機器モデルエンティティのマッピングを保存します。

プロパティ

プロパティ	Description (説明)
<code>sn_otsm.map_all_ot_assets.all_discovery_source</code>	すべてのディスカバリーソースの OT デバイスのマッピングを制御します。

プロパティ (続く)

プロパティ	Description (説明)
	デフォルト値: True
sn_otsm.map_all_ot_assets.discovery_sources	指定されたディスカバリーソースの OT デバイスをマッピングします (カンマ区切り形式)。
sn_otsm.subnet_mapping.auto_assign_ot_controls	Control Rules 関係に基づいて、すべての OT コントロールモジュールを機器モデルエンティティに自動的にアサインします。デフォルトは [はい] (true) です。
sn_otsm.subnet_mapping.location_auto_update	OT デバイスの場所をサブネットの場所で上書きします。オンにすると、サブネットにマッピングされたときに、サブネットの場所が OT デバイスの場所よりも優先されます。デフォルトは [はい] です。

フローデザイナーフロー

アプリケーション	フロー
産業用プロセスマネージャーとオペレーショナルテクノロジーマネージャーとの統合	OT デバイスマッピングフロー

産業用プロセスマネージャー 参照

参照トピックには、産業用プロセスマネージャー アプリケーションに関する追加情報が記載されています。

産業用プロセスマネージャーとともにインストールされるコンポーネント

産業用プロセスマネージャーアプリケーションをアクティブ化すると、ユーザーロールを含むいくつかのタイプのコンポーネントをインストールできます。

i 注:

アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストールされるロール

ロール	Description (説明)
機器モデルビューアー [cmdb_ot_isa_viewer]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] テーブルレコードを表示することのみ可能です。詳細については、「 での 産業用プロセスマネージャー の使用 オペレーショナルテクノロジーマネージャー 」と「 機器モデルの管理 」を参照してください。
機器モデルエディター [cmdb_ot_isa_editor]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] レコードを表示および編集できます。

ロール	Description (説明)
	詳細については、「 での 産業用プロセスマネージャー の使用 オペレーショナルテクノロジーマネージャー 」と「 機器モデルの管理 」を参照してください。
機器モデルアドミン [cmdb_ot_isa_admin]	cmdb_ot_isa_editor ロールを継承し、次のアクションも実行できます。 - 産業用ガイド付きセットアップを使用し、産業用プロセスマネージャーとオペレーショナルテクノロジーマネージャーを設定します。 - 機器モデルテンプレート [isa_entity_template]、[isa_entity_level]、および機器エンティティタイプ [isa_entity_type] テーブルレコードを編集する。 詳細については、「産業用ワークスペースアドミン アプリケーションメニューとガイド付きセットアップ」を参照してください。
ISA サイトビューアー [cmdb_ot_isa_bypass_qbr]	OT 進捗スコアカードですべてのサイトを表示できます。
機器モデルダウンタイムプランナー [sn_isa_schedule_admin]	機器エンティティのスケジュールを作成、変更、および削除できます。スケジュールを機器エンティティに関連付けることもできます。
機器モデルビューアーすべて [cmdb_ot_isa_viewer_all]	すべての ISA Equipment Model (ISA 設備階層モデル) レコード (cmdb_ci_ot_isa_entity) と、関連する機器モデルテンプレートレコード (isa_entity_template、isa_entity_level、isa_entity_type) を表示できます。 cmdb_ot_adminに含まれるロール。
素晴らしい管理者 [sn_ot_amazing_admin]	すべての機器モデルエンティティの OT サブネットシステムプロパティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
アメージングエディター [sn_ot_amazing_write]	ユーザーに関連付けられているすべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を作成、変更、削除できます。
アメージングビューアー [sn_ot_amazing_read]	すべての機器モデルエンティティの OT サブネットレコード (ot_subnet_mapping) を表示できます。

ユーザー基準およびグループへのサイトユーザーアクセスの移行

ISA 設備階層モデルのバージョン 1.0.12 にアップグレードすると、サイトユーザーアクセスからユーザー基準およびグループへの移行が自動的に開始されます。

ISA 設備階層モデルのバージョン 1.0.12 にアップグレードすると、次の変更が発生します。

- ユーザー基準を使用して機器モデルエンティティサイトへの読み取りまたは書き込みレベルのユーザーアクセスを定義するサイトレベルのアクセス制御が改善されました。OT ビューアー (cmdb_ot_viewer) または OT エディター (cmdb_ot_editor) ロールの追加アサインにより、そのロールに応じてアサインされたサイト内の OT デバイスの表示や編集のアクセス権を持つことができます。
- ISA 設備階層モデルのバージョン 1.0.12 にアップグレードすると、既存のサイトユーザーレコードは、改善されたアクセス制御モデルにユーザー基準に従って移行され、同じアクセス許可が保持されます。ISA エンティティサイトユーザーレコードを持つサイトごとに、次の変更が行われます。
 - 表示アクセス権を持つユーザーの場合：
 - 新しいユーザー基準レコードが作成され、「**Read User Criteria for <サイト名> サイト#[システム生成]**」という名前が付けられます。
 - このサイトのすべてのサイトユーザーを含む新しいユーザーグループが作成され、「**Read Group for <サイト名> サイト [システム生成]**」という名前が付けられます。
 - 新しい [機器モデルエンティティ閲覧アクセス] テーブル (isa_entity_m2m_user_criteria_can_view) に、新しいユーザー基準とユーザーグループで新しいレコードが作成されます。
 - 編集アクセス権を持つユーザーの場合：
 - 新しいユーザー基準レコードが作成され、「**Edit User Criteria for <サイト名> サイト [システム生成]**」という名前が付けられます。
 - このサイトのすべてのサイトユーザーを含む新しいユーザーグループが作成され、「**Edit Group for <サイト名> サイト [システム生成]**」という名前が付けられます。
 - 新しい [機器モデルエンティティ編集アクセス] テーブル (isa_entity_m2m_user_criteria_can_edit) に、新しいユーザー基準とユーザーグループで新しいレコードが作成されます。
- サイトの機器モデルエンティティレコードの [サイトユーザー] アプリケーションメニューと [サイトユーザー] 関連リストが削除されます。
- すべてのサイトユーザー (isa_entity_site_user) レコードが非アクティブに設定されます。
- [サイトユーザー：読み取り可能] および [サイトユーザー：編集可能] アプリケーションメニュー項目が Now Platform に追加されます。
- [機器モデルの読み取りが可能] および [機器モデルの編集が可能] 関連リストがサイトの機器モデルエンティティレコードに追加されます。

[ユーザー基準] フォーム

[ユーザー基準] フォームを使用して、特定のユーザーが特定のサイトの機器モデルエンティティにアクセスできるかどうかを決定できます。

次の表で、ユーザー基準フォームのフィールドについて説明します。

[ユーザー基準] フォーム

フィールド	説明
名前	ユーザー基準の名前
簡単な説明	サイトの機器モデルエンティティにアクセスするためのユーザー基準の簡単な説明。
ユーザー	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできるユーザー。

[ユーザー基準] フォーム (続く)

フィールド	説明
	ユーザーのロック解除アイコン () を選択して、エンティティにアクセスできるユーザーを選択します。[自分を追加] アイコン () を選択して、自分をユーザーとして追加します。
グループ	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできるグループ。グループのロック解除アイコン () を選択して、グループを選択します。
ロール	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできるロール。グループのロック解除アイコン () を選択して、グループを選択します。
詳細	ユーザー基準のスクリプトを作成するオプション。
アプリケーション	自動的に グローバルに設定されるフィールド。
アクティブ	ユーザー基準を使用可能にするオプション。
会社	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできる会社。会社のロック解除アイコン () を選択して、会社を選択します。
場所	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできる場所。場所のロック解除アイコン () を選択して、場所を選択します。
部門	ユーザー基準を適用するときにサイトの機器モデルエンティティにアクセスできる部門。部門のロック解除アイコン () を選択して、部門を選択します。
すべて一致	ユーザー基準が適用されるときにすべての条件を必須にするオプション。条件は、[場所]、[部門] フィールドなどの前のフィールドで設定されます。

ISA 設備階層モデルシステムプロパティ

必要に応じて、ISA 設備階層モデルのシステムプロパティを有効にします。

ISA 設備階層モデルのシステムプロパティにアクセスするには、次の場所に移動します。 [すべて > 産業用ワークスペースアドミン > すべての OT プロパティ](#)。OT システムプロパティを表示および編集する方法の詳細については、「[OT システムプロパティの表示と編集](#)」を参照してください。

次の表に、ISA 設備階層モデルのシステムプロパティを示します。

ISA 設備階層モデルシステムプロパティ

システムプロパティ	Description (説明)	タイプ
sn_isa_model.cmdb_relationships	同期される CMDB 関係のレベル数。	整数
sn_isa_model.short_code_validation_max_length	短コード検証の最大長。	整数
sn_isa_model.user_search_match_criteria	検索条件内のユーザーと一致するユーザーテーブル [sys_user] の列。デフォルトでは、[ユーザー] テーブルの [メール] 列が使用されます。	文字列

の事前定義フィルター 産業用プロセスマネージャー

産業用プロセスマネージャー アプリケーションは事前定義されたフィルターを使用するため、産業用ワークスペースで利用可能な UI アクションを選択して機器モデルの依存関係マップを表示できます。

産業用プロセスマネージャーでは、次の事前定義フィルターを使用できます。

ISA 設備階層モデル:階層プロセス

選択した機器モデルエンティティの階層構造と、生産プロセス内の他のエンティティとの関係。

ISA 設備階層モデル:OT 依存関係マップ

選択した機器モデルエンティティの階層構造と、他のエンティティおよび オペレーショナルテクノロジー (生産プロセス内の OT デバイス) との関係。

ISA 設備階層モデル:OT デバイスマップ

選択した機器モデルエンティティと、生産プロセス内の他の OT デバイスとの関係をグラフィカルに表現したもの。

ISA 設備階層モデル:プロセス

選択した機器モデルエンティティとその生産プロセスとの関係のグラフィカル表現。

説明されている事前定義されたフィルターを使用して機器モデルの依存関係マップを表示するには、**Industrial Workspace** に移動して機器モデルビューを開きます。次に、依存関係マップを表示する機器モデルエンティティを選択できます。レコードを開くと、次の UI アクションが表示され、そこから選択できます。

- OT 依存関係マップを表示

i 注:

レコードヘッダーで [マップを表示] を選択して、OT デバイスレコードの OT 依存関係マップを表示することもできます。

- OT デバイスマップを表示
- 階層を表示
- プロセスを表示

組織の必要に応じて、事前定義されたフィルターを更新することもできます。詳細については、「[事前定義フィルターの変更](#)」を参照してください。

事前定義フィルターの変更

必要に応じて、ISA 設備階層モデルアプリケーションの事前定義フィルターを変更します。

始める前に

必要なロール：ecmdb_admin

手順

1. 移動先 **すべて > 依存関係ビュー > 事前定義フィルター**.
2. フィルター **[Application] [is] [ISA Equipment Model]** を適用します。
3. 編集する事前定義フィルターレコードを選択します。
4. 必要に応じて、[構成タイプ]、[CI フィルター]、および [関係タイプ] 関連リストを変更します。
これらの関連リストを変更する方法の詳細については、「[Create a predefined filter](#)」を参照してください。
5. [更新] を選択します。

サイトと場所

サイト属性と場所属性には、オペレーショナルテクノロジー (OT) のさまざまな用途があります。

サイト

サイトは ISA 設備階層モデルエンティティの一部であり、生産プロセスが行われる産業用サイトを表します。サイトは論理的であり、それを使用して機器モデルを定義できます。その後、その機器モデルを使用してアクセス制御を提供できます。アクセス制御の詳細については、「[管理者以外の機器モデルサイトアクセス権をアサインまたは削除する](#)」を参照してください。

サイトに場所を指定することはできますが、場所とは見なされません。どの OT デバイスにも場所があり、機器モデルエンティティサイトにアサインすることができます。

Location (ロケーション)

場所は、場所 (cmn_location) テーブルに格納されている値を参照します。これは、機器モデルまたはデバイスの物理的な場所です。たとえば、機器モデルの 1 つがサイトアトランタに属し、ジョージア州アトランタにある場合は、その場所を ジョージア州アトランタとしてリストします。

関連情報

ネットワーク侵入検知システム (NIDS) 拡張クラス、OT 拡張クラス、および関連アプリケーションの詳細を確認します。

概要

拡張クラスは、オペレーショナルテクノロジー管理構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

Network Intrusion Detection System (NIDS) CI extension class

ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワーク監視アプライアンスと、それが検出するネットワーク上のデバイスとの間の関係を構築します。

Operational Technology (OT) extension classes

構成管理データベース (CMDB)は OT のクラスを更新します。

関連アプリケーション

オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー アプリケーションを使用すると、複数のソースから OT デバイスデータを集計できるため、産業用ソリューションで使用される基本的なデータ関係を構築できます。

[store-future: BEGIN review]

のペルソナ 産業用プロセスマネージャー

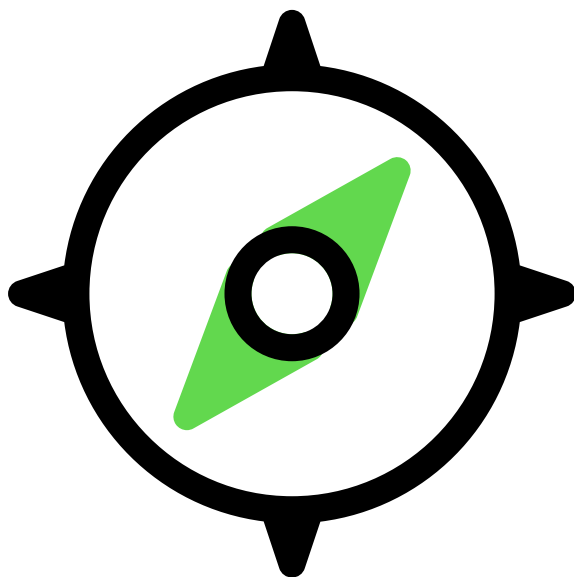
産業用プロセスマネージャーには、アプリケーションに関連付けられたオペレーショナルテクノロジー (OT) ペルソナがあります。

[End]

オペレーショナルテクノロジー脆弱性対応

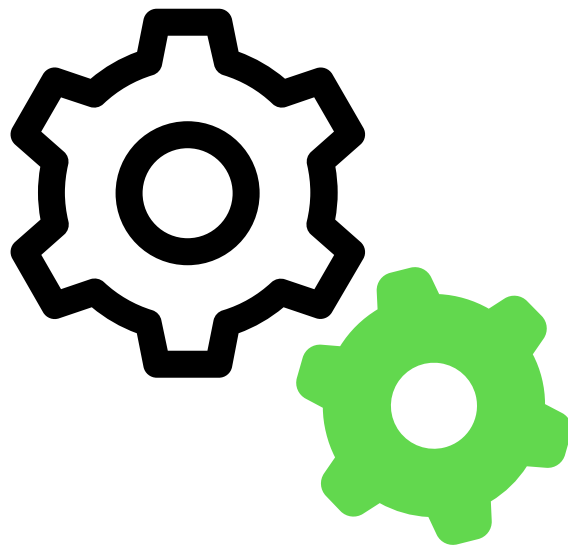
オペレーショナルテクノロジー脆弱性対応 により、サイトレベルでの OT デバイスの脆弱性の効果的な優先順位付けと修復が可能になります。OT デバイスの CMDB 関係を活用することで、脆弱なデバイスまたはアイテムを、自動化する本番プロセスの重要度に基づいて優先順位付けできます。

探索



オペレーショナルテクノロジー脆弱性対応 の探索

Configure (構成)



オペレーショナルテクノロジー脆弱性対応 の構成

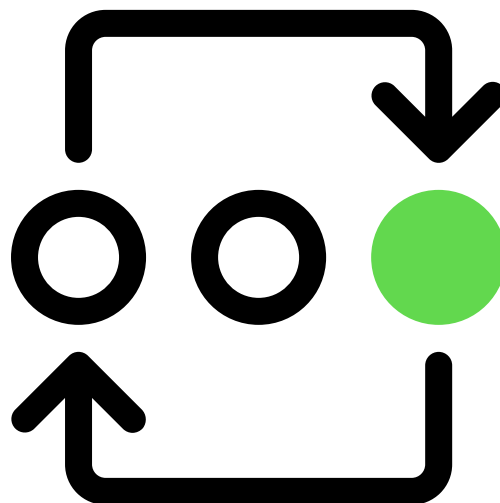
自動翻訳

使用



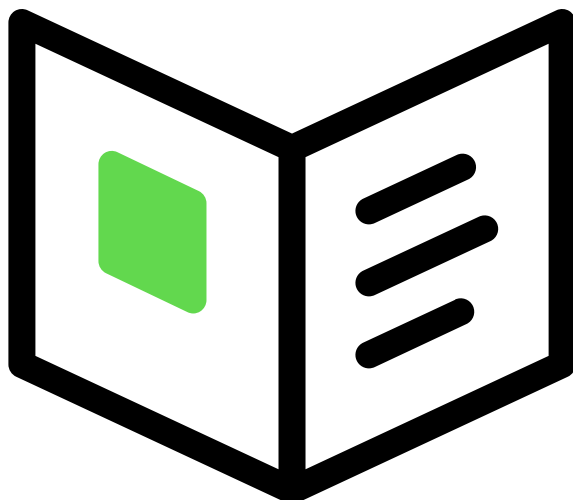
オペレーショナルテクノロジー脆弱性対応の使用

データ連携



他のアプリケーションとの統合による オペレーショナルテクノロジー脆弱性対応の拡張

参照



関連情報とアプリケーションの詳細を取得

自動翻訳

オペレーショナルテクノロジー脆弱性対応の探索

オペレーショナルテクノロジー脆弱性対応を工業生産プロセスの統合ソリューションとして使用します。

OT エンジニアまたは OT 脆弱性マネージャーは、オペレーショナルテクノロジー脆弱性対応を使用して次のような質問に対する答えを見つけることができます。

- 使用している OT デバイスにどのような脆弱性があるか？ ☒
- OT 固有のリスクを使用して脆弱性の修正を優先するにはどうすればよいのか？
- OT の脆弱性の修正に向けての進捗状況はどのようなものか？

修復タスクと脆弱性一致アイテムのステータス

ユースケースが複雑なため、脆弱性一致アイテム (VI) とその修復タスクのステータスが異なる場合があります。修復タスクと脆弱性一致アイテムのステータス、およびそれらのワークフローの詳細については、「[Vulnerability Response remediation task and vulnerable item states](#)」を参照してください。

主な機能

オペレーショナルテクノロジー脆弱性対応 では、次の主要な機能を使用できます。

- OT マネージャーダッシュボードの [OT Vulnerabilities (OT 脆弱性)] タブは、オペレーショナルテクノロジー脆弱性対応 アプリケーションからデータを確認することができる産業用 ワークスペース内の一元的な場所です。
- オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードは、初期分析と検出から封じ込めや修復までの OT VI のボリューム、パフォーマンス、進捗状況を追跡します。

オペレーショナルテクノロジー 脆弱性ソリューション管理

Xanadu バージョン以降、オペレーショナルテクノロジー (OT) 脆弱性ソリューション管理は オペレーショナルテクノロジー脆弱性対応 アプリケーション内で利用できる機能です。

多くの場合、セキュリティチームと IT チームは、脆弱性の検出結果を調査し、環境にとって最も効果的なソリューションを特定するために多大な時間と労力を費やします。大規模な組織では、脆弱性の発見を修復タスクに変換することは、脆弱性の量と複雑さのために手作業で時間がかかり、エラーが発生しやすいプロセスです。

OT 脆弱性ソリューション管理 は、環境内の脆弱性検出と、それらを修復する可能性のあるソリューションを自動的に関連付けます。脆弱性に適用される修復アクションを特定し、脆弱性リスクの重大度によって優先順位を付けることができます。また、OT の補完コントロールを使用することで、すぐにパッチを適用できない脆弱性によってもたらされるリスクを軽減できます。詳細については、「[の補完コントロールを使用 オペレーショナルテクノロジー](#)」を参照してください。

OT 脆弱性ソリューション管理 機能は、脆弱性対応 アプリケーションで利用可能な機能に基づいています。脆弱性ソリューション管理の詳細については、「[Vulnerability Solution Management](#)」を参照してください。

OT 脆弱性ソリューション管理 は、ソリューションインテリジェンス統合の汎用形式をサポートしています。ソリューションインテリジェンス統合の汎用フレームワークは、ソリューションベンダーからさまざまなファイル形式でデータを取り込みます。これらの形式は、情報の交換と処理を高速化します。また、標準化されたレポート形式での重要なセキュリティ関連情報の共有も向上します。サポートされているファイル形式は Common Security Advisory Framework (CSAF) で、これは JSON ベースの構造化された機械可読セキュリティアドバイザリーを提供するオープンソース標準です。米国サイバーセキュリティ社会基盤安全保障庁 (CISA)、Siemens、Hitachi、Schneider Electric などの主要ベンダーが CSAF 形式をサポートしています。

CSAF がサポートするソリューション管理には、次の主要な機能が含まれています。

- セットアップアシスタントによる構成。詳細については、「[Configure vulnerability solution providers](#)」を参照してください。
- ファイルインポートによる CSAF データのインポートのサポート。詳細については、「[Import Common Security Advisory Framework data through file import](#)」を参照してください。

- CSAF URL を介した CSAF データのインポートのサポート。詳細については、「[Import Common Security Advisory Framework \(CSAF\) data through CSAF URL](#)」を参照してください。OT 脆弱性ソリューション管理 を使用すると、次から CSAF データをインポートできます。
 - CSAF 形式をサポートし、CSAF URL ROLIE フィードを持つ個々のベンダー。ベンダーが提供する CSAF URL ROLIE フィードを使用して、CSAF データをインポートできます。たとえば、Siemens URL ROLIE フィードなどです。
 - CSAF アグリゲーターまたは信頼できるプロバイダー (ROLIE フィードをサポートする URL インポート経由)。信頼できるプロバイダーから複数のベンダーの CSAF データをインポートできます。たとえば、CISA は信頼できるプロバイダーであり、[CISA の GitHub CSAF リポジトリ](#)にある産業用コントロールシステム (ICS) CSAF アドバイザリから複数のベンダーの CSAF データをインポートできます。これらの脆弱性ソリューションは、共通脆弱性識別子 (CVE) に基づいて、正しいベンダーおよび脆弱性一致アイテム (VIT) に自動的にマッピングされます。信頼できるプロバイダーを使用すると、個々のベンダーの CSAF URL から CSAF データをインポートするために必要な時間と労力を削減できます。
- アドバイザリーまたは API を使用した CSAF データのインポートのサポート。詳細については、「[Import Common Security Advisory Framework data from advisories](#)」を参照してください。

- i 注:**
移動先 [すべて > 脆弱性対応 > Solutions \(ソリューション\) > すべて](#) 上記の方法を使用してインポートしたソリューションのリストを表示します。

脆弱性対応プラグインは、作成されたソリューションのメトリクスステータスを更新します。

関連情報

[での脆弱性一致アイテム \(VIT\) のソリューションの表示](#) [産業用ワークスペース](#)

オペレーショナルテクノロジー脆弱性対応の構成

オペレーショナルテクノロジー (OT) アサインルール、修正ターゲット、リスク算出、リスクロールアップ計算を設定してから、脆弱性一致アイテムレコードを作成するように統合を設定します。

- i 注:**
- sn_vul.vulnerability_admin ロールを持っている場合は、産業用 ガイド付きセットアップを使用して、オペレーショナルテクノロジー脆弱性対応 アプリケーションのセットアップを行うことができます。

ガイド付きセットアップにアクセスするには、次の場所に移動します。産業用ワークスペース アドミン > ガイド付きセットアップ。

タスク	目的
1. ServiceNow Storeからオペレーショナルテクノロジー脆弱性対応をインストールします。	オペレーショナルテクノロジー脆弱性対応 アプリケーションをインストールします。
2. 必要に応じて、アドミンユーザーまたはユーザーグループにロールをアサインします。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
3. OT 脆弱性修正オーナーにロールをアサインします。	OT 脆弱性修正オーナーが利用できるアクションを制御するロールをアサインします。

タスク	目的
4. アサイン先グループを作成し、ユーザーをサイトとグループに割り当てます。 1. 機器モデルマネージャーにあるサイトごとに、オペレーショナルテクノロジー脆弱性対応 サイトのアサイン先グループを作成します。 2. cmdb_ot_isa_viewer または cmdb_ot_isa_editor ロールを既に持っているユーザーをサイトにアサインします。 3. サイトのアサイン先グループにユーザーを追加します。	- OT 修正オーナーユーザーがサイトの脆弱性一致アイテムのみを表示できるようにします。 - ユーザーがアサインされているサイトの脆弱性一致アイテムを表示できるようにします。
5. OT 修復ターゲットルールを設定する。	- OT 脆弱性一致アイテムをサイトレベルのグループ、または分類に基づくグループにアサインします。 - 脆弱性一致アイテムの修正予定期間を定義します。
6. オペレーショナルテクノロジー脆弱性対応 アプリケーションのデモデータレコードをロードします。	OT 脆弱性一致アイテムの修復ターゲットを計算します。
7. OT リスク算出を設定する。	OT デバイス上の脆弱性一致アイテムのリスクを計算するときに使用する OT リスクファクターを決定します。
8. OT リスクロールアップ算出を設定する。	機器モデルエンティティの各レベルで OT デバイスのリスクスコアを計算します。
9. ご使用の環境 オペレーショナルテクノロジー適用可能な オペレーショナルテクノロジー脆弱性対応 アプリケーションの認定統合をインストールします。	OT 脆弱性管理の機能を強化する認定済みサードパーティアプリケーションを統合します。

オペレーショナルテクノロジー脆弱性対応のインストール

admin ロールを持っている場合は、オペレーショナルテクノロジー脆弱性対応 アプリケーションをインストールします。このアプリケーションには、デモデータが含まれています。まだインストールされていない場合は、関連するストアアプリケーションとプラグインをインストールします。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。
- アプリケーションがプラグインまたはその他のストアアプリケーションを必要とし、それがまだインストールされていない場合は、先にインストールしてください。
- オペレーショナルテクノロジー脆弱性対応 には次のプラグインが必要です。オペレーショナルテクノロジー脆弱性対応 をインストールする前に、これらのプラグインがアクティブ化されていることを確認してください。

必須の ServiceNow プラグイン

脆弱性対応 (sn_vul)

ServiceNow 脆弱性対応 アプリケーションは、脆弱性一致アイテムをインポートし、グループルールに従って自動的にグループ化することで、脆弱性を修復することができます。「[Vulnerability Response のインストール](#)」を参照してください。🔗

産業用プロセスマネージャー (sn_otsm)

ServiceNow 産業用ソリューションに必要な ISA-95 機器モデルデータ基盤を作成します。「[産業用プロセスマネージャー をインストールする](#)」を参照してください。

オペレーショナルテクノロジー マネージャー

オペレーショナルテクノロジー Manager アプリケーションは、企業が ServiceNow 産業用ソリューションを使用できるようにする基盤データと関係を作成します。オペレーショナルテクノロジーManager は、Now Platform での 構成管理データベース (CMDB)、サービスグラフコネクタ、およびディスカバリーアプリケーションの使用をサポートしています。[Operational Technology Manager \(OTM\) の設定](#)を参照してください。

必要なロール：admin

このタスクについて

次のアイテムは、オペレーショナルテクノロジー脆弱性対応 アプリケーションのインストールとともにインストールされます。

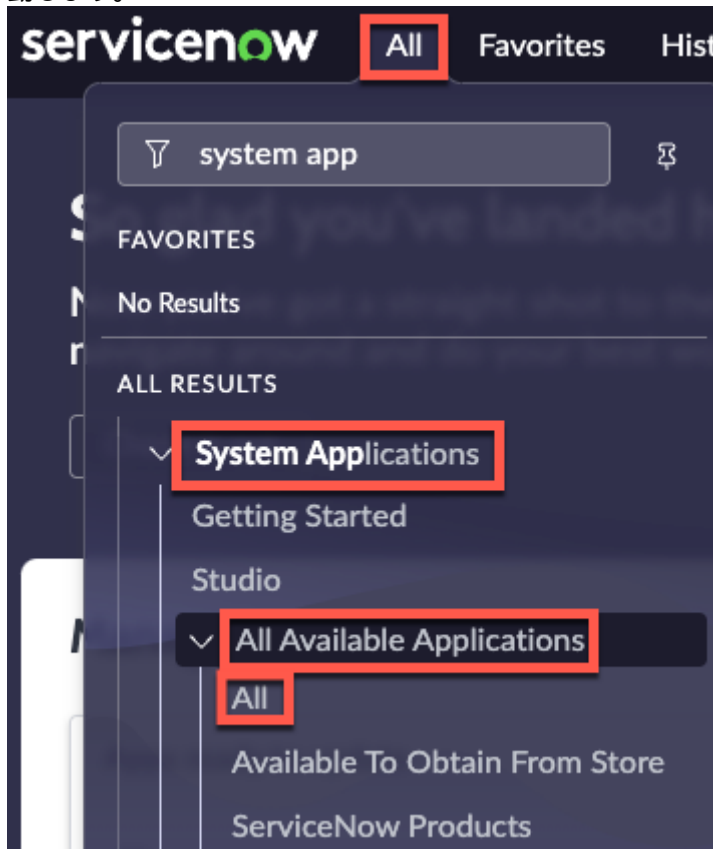
- プラグイン
- ストアアプリケーション
- ロール
- ビジネスルール

アプリケーションとともにインストールされるコンポーネントの表示の詳細については、以下を参照してください。

- [オペレーショナルテクノロジー脆弱性対応とともにインストールされるコンポーネント](#)
- [アプリケーションとともにインストールされているコンポーネントを検索します](#)🔗。

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して オペレーショナルテクノロジー脆弱性対応 アプリケーションを検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることもあります。

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. リストからバージョンを選択し、[インストール] を選択します。

表示されるインストールダイアログボックスには、アプリケーションと併せてインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエントリメントを取得します。
5. オプション: 利用できるデモデータをインストールするには、[デモデータのロード] チェックボックスをオンにします。
デモデータには、一般的なユースケース向けのアプリケーション機能を説明するサンプルレコードが含まれています。開発またはテストインスタンスで初めてアプリケーションをインストールする場合は、デモデータを読み込みます。

i 重要:

インストール時にデモデータを読み込んでおかないと、後から読み込むことはできません。

6. [インストール] を選択します。

オペレーショナルテクノロジー脆弱性対応 ロールの割り当て

ユーザーにロールをアサインすると、オペレーショナルテクノロジー脆弱性対応 アプリケーションの各機能やデータへのアクセスを制御できます。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジー脆弱性対応 アプリケーションを使用できます。

必要に応じて、アドミンユーザーまたはユーザーグループにロールをアサインします。

アドミンユーザーまたはグループへのロールのアサイン

ロール	Description (説明)
OT VR 統合ビューアー [sn_otvr.integration_viewer]	OT VR 統合レコードを表示できます。
OT VR 統合アドミン [sn_otvr.integration_admin]	OT VR 統合レコードを表示および編集できます。
OT 脆弱性修正オーナー [sn_otvr.remediation_owner]	修復タスクを作成できます。脆弱性一致アイテムの既存の修復タスクをスケジュールすることもできます。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

次のタスク

[サイトのアサイン先グループを作成する](#)。

サイトのアサイン先グループを作成する

機器モデルマネージャーにあるサイトごとに 1 つの オペレーショナルテクノロジー脆弱性対応 アサイン先グループを作成します。これにより、OT の修復オーナーであるユーザーは、自分のサイトの脆弱性一致アイテムに限って表示できるようになります。

始める前に

オペレーショナルテクノロジー脆弱性対応アサイン先グループを作成し、できれば関連するサイトと同じ名前で作成します。たとえば、サイトがミラノにある場合、グループに「ミラノの OT VR アサイン先グループ」という名前を付けます。

必要なロール:cmdb_ot_isa_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > 産業用プロセスマネージャー > サイト**.
2. サイトレコードを選択します。
サイトレコードは、それ自体が親を持たない親機器モデルエンティティです。
3. **[OT VR assignment group (OT VR アサイン先グループ)]** フィールドで、検索アイコンを選択すると既存のユーザーグループが表示されます。
4. 該当するアサイン先グループを選択します。
 - 目的のグループが存在する場合は、リストからそれを選択します。
 - 目的のグループが存在しない場合は、**[New (新規)]** を選択してグループを作成し、**[Submit (送信)]** を選択します。
5. サイト レコードに戻ったら、 **更新** を選択します。
新しい OT VR アサイン先グループが作成されます。

次のタスク

サイトにユーザーをアサインする

サイトにユーザーをアサインする

産業用プロセスマネージャー の構成時にまだ行っていない場合は、cmdb_ot_isa_viewer または cmdb_ot_isa_editor ロールを既に持っているユーザーをサイトにアサインします。

始める前に

OT デバイスが CMDB にある場合、サイトアクセスを構成して、OT デバイスの表示を、cmdb_ot_viewer、エディター、アドミンのいずれかのロールと、cmdb_ot_isa_viewerまたはエディターのロールの両方を持つユーザーに制限できます。

必要なロール:cmdb_ot_isa_admin

手順

1. [Equipment Model Entities (機器モデルエンティティ)] フォームから、親機器モデルエンティティを選択します。
機器モデルの詳細については、「[機器モデルの管理](#)」を参照してください。
2. [サイトユーザー] タブで、[新規] を選択します。
3. [ISA エンティティサイトユーザー] フォームのフィールドに入力します。
4. [送信] を選択します。
ユーザーがサイトに割り当てられます。

次のタスク

ユーザーのアサイン先グループへのアサイン

ユーザーのアサイン先グループへのアサイン

アサイン先グループにユーザーを追加すると、そのユーザーはアサインされたサイトの脆弱性一致アイテムを表示できるようになります。

始める前に

ユーザーがアサインしたサイトの脆弱性一致アイテムを表示できるようにするには、サイトの OT VR アサイン先グループにユーザーを追加します。

OT 脆弱性一致アイテムが作成されると、可視化は以下に制限される。

- VR 修正オーナー (sn_vul.remediation_owner) ロールを持つユーザー
- OT デバイスが属するサイトに関連付けられた オペレーショナルテクノロジー脆弱性対応 アサイン先グループのメンバーシップ

必要なロール：admin

手順

1. サイトの オペレーショナルテクノロジー脆弱性対応 アサイン先グループに対応するグループを開きます。
2. [Group Members (グループメンバー)] タブから、**[Edit (編集)]** を選択します。
3. [Collection (コレクション)] リストから、[Group Members List (グループメンバーリスト)] にユーザーを追加します。
4. [保存] を選択します。
ユーザーはグループにアサインされ、アサインされたサイトの脆弱性一致アイテムを表示できます。グループへのユーザーの追加など、管理タスクの詳細については、「[User administration](#)」を参照してください。

次のタスク

[脆弱性一致アイテムをグループにアサイン](#)。

脆弱性一致アイテムをグループにアサイン

OT 脆弱性アサインルールを構成します。

始める前に

OT 脆弱性一致アイテムは、修正戦略に応じて、サイトレベルのグループまたは分類に基づくグループにアサインできます。

必要なロール:sn_vul.manage_assignment_rules または sn_vul.vulnerability_admin

このタスクについて

脆弱性一致アイテムがインポートされると、脆弱性アサインルールに基づいて適切なグループにアサインされる。オペレーショナルテクノロジー脆弱性対応 には、OT 脆弱性アサインルールである オペレーショナルテクノロジー **(OT)** アサインルールが 1 つ付属しており、サイトに基づいて対応する OT VR アサイン先グループに OT 脆弱性一致アイテムレコード (VIT) をアサインします。OT VR アサイン先グループがどのサイトにも属していない場合、またはサイトにグループが指定されていない場合、ルールは OT VR のデフォルトのアサイン先グループにアサインされる。

脆弱性対応アサインルールの作成の詳細については、「[脆弱性対応アサインルールの作成または編集](#)」を参照してください。

手順

1. [Vulnerability Assignment Rules (脆弱性アサインルール)] リストから、**[Operational Technology (OT) assignment rule (オペレーショナルテクノロジー (OT) アサインルール)]** を選択します。
2. 修復戦略に基づいてルールを構成します。

- 修正戦略がすべての OT 脆弱性一致アイテムをサイトにアサインすることである場合は、OT VR アサインルールの実行順序を他のすべてのルールよりも小さくなるように設定します。
- クラスごとにアサインしてから他のすべてのクラスのサイトにアサインするという戦略の場合は、OT VR アサインルールの実行順序をすべてのクラスベースのルールよりも大きくなるように設定します。

3. 実行順序が更新されたら、OT VR アサインルールのアクティブ状態を **true** に設定します。

次のタスク

OT 修復ターゲットルールを構成する。

OT 修復タスクルールの設定

産業用 ワークスペース で作成された修復タスクでは、既存の修復タスクルールを更新して、インポートされた脆弱性一致アイテムによって OT デバイスが自動的に追加されないようにします。

始める前に

必要なロール:sn_vul.manage_group_rules または sn_vul.vulnerability_admin

脆弱性一致アイテムがインポートされると、構成された修復タスクルールに基づいてそのアイテムが修復タスクに追加されることがあります。IT と OT ネットワークの両方に 脆弱性対応 を使用する場合は、IT と OT ネットワーク間で修復のために脆弱性一致アイテムを異なる方法でグループ化するには、構成を変更する必要があります。オペレーショナルテクノロジー脆弱性対応 では、OT ネットワークの脆弱性を自動的にグループ化しないようにする方法を示すデモデータがロードされた修復タスクルールレコードのサンプルを提供します。

修正戦略に基づいて、新規または既存の修復タスクルールを設定します。

- IT 環境内の脆弱性のみを対象として修復タスクを自動作成するという修正戦略の場合は、既存の修復タスクルールそれぞれに、OT の脆弱性を除外する次の条件を追加します。
 - 構成アイテム。OT デバイスの詳細 = は空
- すべての OT 脆弱性一致アイテムの修正タスクを自動作成するという修正戦略の場合は、適切なルールを作成します。

OT VR デモデータに同梱されているサンプル:修復タスクルール:脆弱性 (OT を除外)

The screenshot shows the configuration page for a Remediation Task Rule named "Vulnerability (exclude OT)". The rule is currently inactive. The description states that this rule is necessary to avoid including OT assets in remediation tasks. The condition is set to "All of these conditions must be met", with two criteria: "Active" is "true" and "Configuration Item. OT asset details" is "empty". The rule is configured to group vulnerable items by "Assignment group" and "Vulnerability". The assignment section indicates that remediation tasks should be assigned by field, specifically by the "Assignment group".

手順

1. 移動先 脆弱性対応 > 管理 > 修復タスクルール。
2. 更新するルールの名前を選択します。
 - グループ内のすべての脆弱性一致アイテムが同じチーム、同じ修復アクション、同じ期間で修復されるようにルールを定義します。たとえば、脆弱性一致アイテムの「アサイン先グループ」、「脆弱性」、および CI の「使用対象」でグループ化します (例: 本番、ステージング、開発) (これらの環境のメンテナンス期間が異なる場合)。
 - 修復タスクルールの詳細については、「[脆弱性対応ワークスペース](#)」を参照してください。
 - 修復タスクの詳細については、「[IT 修復ワークスペースの詳細](#)」を参照してください。

OT 修復ターゲットルールを構成する

OT 脆弱性一致アイテムの修復ターゲットルールを設定します。

OT 脆弱性一致アイテムの修正ターゲット日を計算するには、オペレーショナルテクノロジー脆弱性対応 アプリケーションのデモデータレコードをロードし、修復ターゲットルールを設定します。

必要なロール:sn_vul.manage_remediation_target_rules または sn_vul.vulnerability_admin

産業環境ではメンテナンスを実行する機会が少ないため、OT 修復ターゲットが異なる場合があります。修復ターゲットルールは、最小のターゲットから最大のターゲットの順に適用されます。

他の脆弱性と同じ期間内に利用可能なメンテナンスウィンドウがない OT デバイスの脆弱性については、別の修復ターゲット日が必要になる場合があります。この状況で修復ターゲット日を構成する方法を示すために、重大なリスク評価に対してこれを管理する方法を示す 2 つのデモデータレコードが提供されています。

- 重大なリスク評価ルール (OT のみ):このルールでは、構成アイテムの条件を使用します。OT デバイスの詳細が空でない **AND** リスク評価 = 1:重大。[Target (days) (ターゲット (日数))] を更新し、レコードを有効化します。
- 重大なリスク評価ルール (OT を除外):重大なリスクの非 OT 項目にのみ短いターゲットを適用するには、最初に OT デバイスを除外する必要があります。このルールでは、条件 [構成アイテム] を使用します。OT デバイスの詳細が空で、かつリスク評価 = 1:重大。[Target (days) (ターゲット (日数))] を更新し、既存の重大なターゲットルールを無効にして、代わりにこのルールを有効にします。

i 注:

OT の重大なリスクの脆弱性が非 OT 修復ターゲットルールから除外されるように、これらのルールを両方ともアクティブ化する必要があります。

脆弱性対応アサインルールの作成の詳細については、以下を参照してください。

- [Vulnerability Response の修復ターゲットルール](#)
- [脆弱性対応修復ターゲットルールの作成または編集](#)

リスク算出の設定

リスク算出の設定

OT デバイス上の脆弱性一致アイテムのリスクを計算するときに使用する OT リスクファクターを決定します。

始める前に

オペレーショナルテクノロジー、追加要素として、OT デバイスの重要度、Purdue レベル、OT デバイスが自動化する本番プロセスの重要度などがあります。

必要なロール:sn_vul.manage_risk_score_configuration または sn_vul.vulnerability_admin

このタスクについて

このステップについては、オペレーショナルテクノロジー脆弱性対応 アプリケーションのデモデータに付属している OT 脆弱性算出を使用したデフォルトのリスク算出を参照してください。OT を使用したデフォルトのリスク算出は、OT 脆弱性一致アイテムと非 OT 脆弱性一致アイテムに対して異なる方法でリスクを計算する必要がある場合に使用されます。

i 注:

一度にアクティブにできる脆弱性算出は 1 つだけであるため、提供されているデフォルトのリスクルール (非 OT) は、OT 以外のすべての脆弱なアイテムのリスクを計算するための例として使用されます。

詳細については、「[Define fields and weights for the risk rule \(リスクルールのフィールドと重み付けを定義する\)](#)」を参照してください。

OT 脆弱性一致アイテムのリスクスコアを設定するには、デモデータの OT デフォルトリスクルールのリスクルールレコードの重み付けを調整します。デモデータの OT で利用可能なその他のフィールドは次のとおりです。

- 機器モデルエンティティの重要度:サービス事業上の重要度ルールを使用します。
- OT デバイスの重要度:構成アイテム (CI) の [OT デバイスの詳細] の [デバイスの重要度] ルールを使用します。
- Purdue レベル:[構成アイテム OT デバイスの詳細 Purdue レベル] フィールドを使用します。

手順

1. [脆弱性算出] に移動します。
2. [Vulnerability Calculators (脆弱性算出)] リストから、**[Default Risk Calculator with OT (OT を使用したデフォルトリスク算出)]** を選択します。
3. [Vulnerability Calculators Rules (脆弱性算出ルール)] リストから、編集するリスクルールを開きます。
たとえば、**[OT Default Risk Rule (OT デフォルトリスクルール)]** を選択します。
4. [Vulnerability Risk Rules (脆弱性リスクルール)] ページの [Risk Calculator Criteria (リスク算出基準)] セクションで、リスクルールフィールドを 1 つ選択します。
5. [リスクルール] フィールドレコードで、全体的なリスクスコア計算における重要性に従って、各基準の重み付けまたは重み付け % を更新します。
6. [更新] を選択します。

次のタスク

他のすべての脆弱性一致アイテムのリスクスコアを設定するには、既存のリスクルールを OT を使用したデフォルトリスク算出にコピーし、OT デフォルトリスクルールの後に実行する順序を設定します。

OT 脆弱性リスクロールアップ算出を構成する

OT 脆弱性リスクロールアップ計算を使用して、機器モデルの各レベルで OT デバイスのリスクスコアを計算します。全体的なリスクスコアは、親の機器モデルエンティティにロールアップされます。

始める前に

- スケジュール済みジョブを実行して、すべての機器モデルエンティティのリスクスコアを計算します。

i 注:

すべての機器モデルエンティティのリスクスコア計算は、日次スケジュールジョブの後続の実行に対してのみ行われます。

- に移動して、[Equipment Model Entities (機器モデルエンティティ)] リストの [Service Populator (Service Populator)] 列が **OTDynamicManualServicePopulator** に設定されていることを確認します。すべて > 機器モデル: **ISA** > 機器モデルエンティティ。他の値に設定されている場合は、*Update ISA entity service populator* オンデマンドジョブを実行する必要があります。
- 移動先 すべて > システム定義 > スケジュール済みジョブ。
- [Update ISA entity service populator] ジョブを選択します。
- [今すぐ実行] をクリックします。

i 注:

[Equipment Model Entities (機器モデルエンティティ)] リストに [Service Populator (Service Populator)] 列が表示されない場合は、リストをカスタマイズして追加できます。詳細については、「[Personalize a list](#)」を参照してください。

- 必要なロール: sn_vul.vulnerability_admin

このタスクについて

このステップについては、オペレーショナルテクノロジー脆弱性対応 アプリケーションのデモデータに付属する OT 脆弱性算出を使用した脆弱性ロールアップ算出を参照してください。

詳細については、「[Vulnerability Response Rollup Calculators \(脆弱性対応ロールアップ算出\)](#)」を参照してください。

機器モデルエンティティのリスクスコアを計算するには、次のフィールドの重み付けを設定します。

- 機器モデルエンティティに関連付けられた脆弱性一致アイテム (VIT) の最大リスクスコア。
- 機器モデルエンティティに関連付けられた VIT の平均リスクスコア。
- 機器モデルエンティティあたりの脆弱性一致アイテムの数。

手順

1. 移動先 すべて > 脆弱性対応 > 管理 > 脆弱性ロールアップ算出。
2. [Vulnerability Rollup Calculator (脆弱性ロールアップ算出)] リストから、**[Equipment Model Entity Rollup (機器モデルエンティティロールアップ)]** を選択します。
3. 必要に応じて、[Rollup Weights (ロールアップの重み付け)] セクションで、各基準の重み付けを更新します。
4. [更新] を選択します。

次のタスク

これで、機器モデルエンティティのレベルに関連付けられたリスクを計算できます。

1. すべての機器モデルエンティティのリスクロールアップを計算します。
 - a. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**.
 - b. [**Operational Technology Vulnerability Response** (オペレーショナルテクノロジー脆弱性対応)] を選択します。
 - c. [リスクロールアップ計算] セクションで、[リスクロールアップ構成] タスクを選択します。
 - d. [構成] を選択します。
 - e. ガイド付きセットアップで説明されている手順に従います。
2. *Risk Rollup for VITs by Equipment Model Entity* スケジュール済みジョブを構成します。
 - a. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**.
 - b. [**Operational Technology Vulnerability Response** (オペレーショナルテクノロジー脆弱性対応)] を選択します。
 - c. [リスクロールアップ計算] セクションで、リスクロールアップタスクの日次スケジュールジョブを選択します。
 - d. [構成] を選択します。
 - e. ガイド付きセットアップで説明されている手順に従います。



注:

デフォルトでは、ジョブは毎日実行されるように設定されています。これは、[実行]、[タイムゾーン]、および [時間] フィールドを編集することで、ビジネスニーズに合わせて変更できます。

3. リスクスコアロールアップ用にエンティティを設定します。
 - a. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**.
 - b. [**Operational Technology Vulnerability Response** (オペレーショナルテクノロジー脆弱性対応)] を選択します。
 - c. [リスクロールアップ計算] セクションで、[リスクスコアロールアップジョブにすべてのエンティティを設定] タスクを選択します。
 - d. [構成] を選択します。
 - e. ガイド付きセットアップで説明されている手順に従います。
4. 修復タスクで誤ったリスクスコアと評価を取得しないようにするには、サイトがアサインされていない **OT** デバイスロールアップレコードの [テーブル] フィールドを変更します。
 - a. 移動先 **すべて > システム定義 > スクリプト - バックグラウンド**.
 - b. [スクリプトを実行] フィールドで、次のスクリプトを追加します。

```
var gr = new GlideRecord('sn_vul_rollup');

gr.get('sys_id','24973dc4939e42900b1566f4548918eb');

gr.table = 'sn_ot_metric';

gr.update();
```

- c. [スクリプトを実行] を選択します。

- d. サイトがアサインされていない **OT** デバイスロールアップレコードの [テーブル] フィールドの値を確認し、スケジュール済みジョブを実行するには、すべて > 脆弱性対応 > 管理 > 脆弱性ロールアップ算出。
- e. [サイトがアサインされていない **OT** デバイスロールアップレコード (**OT Devices with No sites Assigned Rollup**)] レコードを選択します。
- f. [テーブル] フィールドが [**OT** メトリクス **[sn_ot_metric]**] に設定されていることを確認します。
- g. スケジュール済みジョブを実行します。

ジョブを実行すると、正しい VIT リスクスコアと評価が修復タスクにロールアップされます。

認定 脆弱性対応 統合のインストール

OT 脆弱性管理の機能を強化する認定済みサードパーティアプリケーションを統合します。

ServiceNow® Storeで オペレーショナルテクノロジー脆弱性対応 アプリケーションの オペレーショナルテクノロジー 認定統合を検索し、ご使用の環境に適用可能なものをインストールしてください。

オペレーショナルテクノロジー脆弱性対応 統合

オペレーショナルテクノロジー脆弱性対応 アプリケーションには、サードパーティ統合のサポートが入っています。

現在、下記のサードパーティー統合をサポートしています。

- 脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール)
- 脆弱性対応 Claroty CTD との統合。

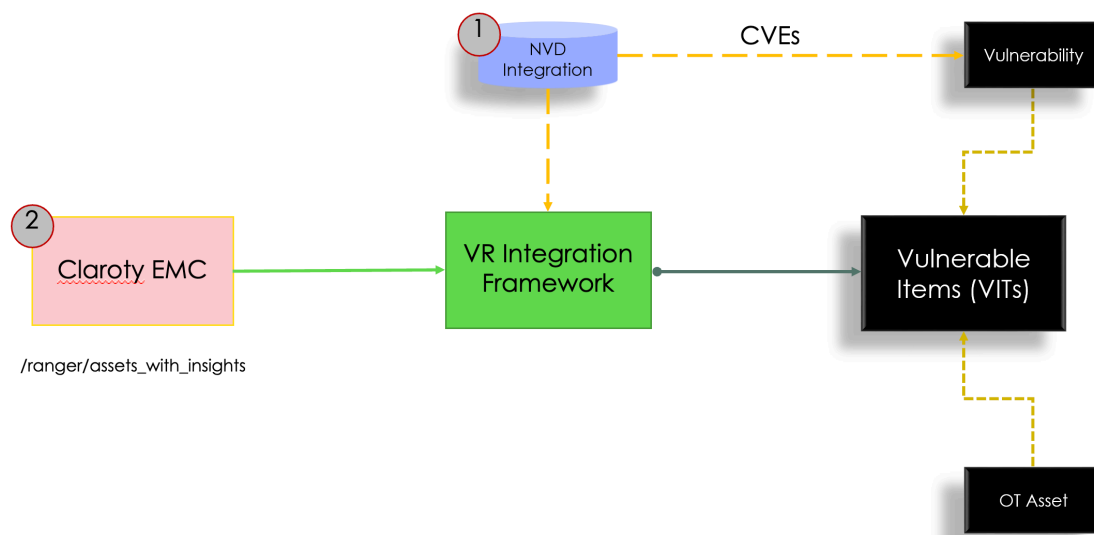
脆弱性対応 **Claroty CTD** との統合

脆弱性対応 Integration with Claroty Continuous Threat Detection (CTD) は、Claroty CTD からインポートされた脆弱性データを使用して、本番プロセス内でリスクベースのアクションを有効にします。

この 脆弱性対応ServiceNow® オペレーショナルテクノロジー脆弱性対応 アプリケーションとの統合を使用して、本番プロセスで使用する脆弱性を追跡、優先順位付け、および解決します。

次の画像は、脆弱性対応 と Claroty CTD の統合のプロセスを示しています。

脆弱性対応と Claroty CTD の統合のプロセス



脆弱性対応 と Claroty CTD の統合を実行する前に、脆弱性情報データベース (NVD) 統合を実行する必要があります。NVD 統合は、公開された共通脆弱性識別子 (CVE) を NVD からフェッチし、ServiceNowに入力します。次に、脆弱性対応 Integration with Claroty CTD アプリケーションを実行すると、各デバイスの脆弱性が特定され、脆弱性一致アイテム (VIT) が作成されます。

各 VIT には、オペレーショナルテクノロジー (OT) デバイスまたは構成アイテム (CI)、および検出された脆弱性との関係があります。脆弱性統合フレームワークが Claroty Enterprise Management Console (EMC) との接続を確立し、すべての OT デバイスの脆弱性を取得します。

注:

Claroty CTD EMC Platform Insights API の CVE は 10 個に制限されています。したがって、Claroty によって ServiceNow 提供される CVE は 10 件のみです。ただし、xDome プラットフォームにはこの制限がありません。

主な機能

- Claroty CTD から オペレーショナルテクノロジー (OT) デバイスに関連付けられた共通脆弱性識別子 (CVE) をインポートします。脆弱性一致アイテム (VIT) を作成して、OT デバイスの脆弱性データとそれが本番プロセスにどのように影響するかを一目で見られるようにします。
- 新しく検出された脆弱性のインポートを独自のスケジュールで自動的に実行する。
- アサインルールを使用して、リスクベースのアクションを実行できるローカルサイトベースのチームに、修復のために VIT を自動的にルーティングする。

脆弱性対応 Integration with Claroty CTD をインストール

Claroty CTD (sn_clarotyctdvr) との脆弱性対応統合をインストールし。このアプリケーションには、関連する ServiceNow Store アプリケーションとプラグインがインストールされます (まだインストールされていない場合)。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。
- 依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性については、ServiceNow Store の [Vulnerability Response Integration with Claroty CTD \(脆弱性対応と Claroty CTD\)](#) の統合) アプリケーションを確認してください。

- 脆弱性対応 Claroty CTD との統合には、次の ServiceNow Store アプリケーションが必要です。脆弱性対応 Integration with Claroty CTD をインストールする前に、これらのアプリケーションがインストールされていることを確認してください。

CMDB CI クラスモデルストアアプリ

この統合では、オペレーショナルテクノロジー [拡張クラス](#) CMDB CI クラスモデルアプリケーションの一部です。詳細については、「[CMDB CI Class Models](#)」を参照してください。

Claroty CTD のサービスグラフコネクタ統合

この統合では、オペレーショナルテクノロジーマネージャー アプリケーションを使用して、サイト、各サイトで検出されたデバイス、接続 (またはベースシステム)、およびインストールされたプログラムの 構成管理データベース (CMDB) へのインポートを自動化します。Claroty CTD のサービスグラフコネクタ統合をインストールするには、「[脆弱性対応 Integration with Claroty CTD をインストール](#)」を参照してください。

必要なロール：admin

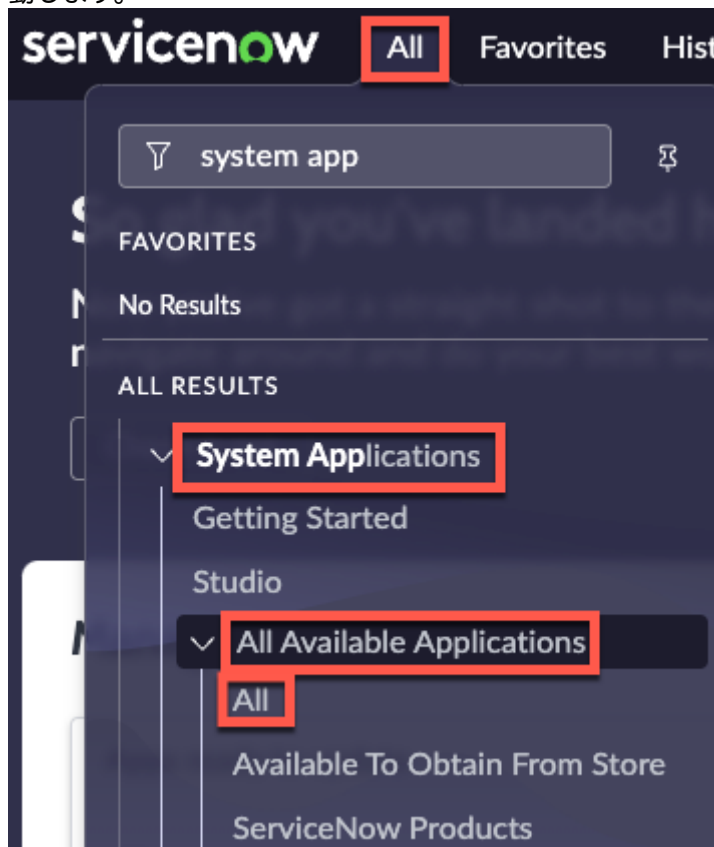
このタスクについて

脆弱性対応 Integration with Claroty CTD とともに次のアイテムがインストールされます。

- 脆弱性対応プラグイン
- NVD の脆弱性対応統合

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して、脆弱性対応 Integration with Claroty CTD アプリケーション (sn_clarotyctdvr) を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store に要求する必要がある場合があります。

[インストール] ボタンの横のリストに、使用可能なバージョンが表示されます。

3. リストからバージョンを選択し、[インストール] を選択します。

表示されるインストールダイアログボックスには、アプリケーションと併せてインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエントリメントを取得します。

5. [インストール] を選択します。

脆弱性対応 **Integration with Claroty CTD** のロールをアサイン

ユーザーにロールをアサインして、脆弱性対応 Integration with Claroty CTD アプリケーションの機能、性能、データへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次の表にリストされているロールが割り当てられている場合は、脆弱性対応 Integration with Claroty CTD アプリケーションを使用できます。

必要に応じて、アドミンユーザーまたはユーザーグループにロールをアサインします。

脆弱性対応 Integration with Claroty CTD アプリケーションで利用可能なロールの詳細については、「[脆弱性対応 Integration with Claroty CTD のロール](#)」を参照してください。

手順

Now Platformユーザー管理機能を使用して、ユーザーまたはグループにロールをアサインします。

脆弱性対応 **Integration with Claroty CTD** のロール

ロールは、脆弱性対応 Integration with Claroty CTD の機能へのアクセスを制御します。

次の表に、脆弱性対応 Integration with Claroty CTD のロールと権限を示します。

脆弱性対応 **Integration with Claroty CTD** のロール

ロール	Description (説明)
OT VR 統合ビューアー [sn_otvr.integration_viewer]	OT VR 統合レコードを表示できます。
OT VR 統合アドミン [sn_otvr.integration_admin]	OT VR 統合を構成して実行できます。
MID サーバー [mid_server]	MID サーバーを設定できます。

脆弱性情報データベース統合の実行

脆弱性情報データベース (NVD) 統合を実行して、米国国立標準技術研究所 (NIST) の NVD 製品からデータをインポートします。NVD 統合を実行すると、環境内で見つかった共通脆弱性識別子 (CVE) の重大度と詳細を判断する際に役立ちます。

始める前に

インスタンスで NIST NVD 統合を実行する前に、インストールと構成のステップを完了する必要があります。インストールと構成を完了すると、NVD 製品が オペレーショナルテクノロジー脆弱性対応 アプリケーションと適切に統合されます。

NVD プラグインをインストールするには、「[Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 **すべて > 脆弱性対応 > 管理 > 統合**.
2. [NIST NVD integration - API (CVE only) (NIST NVD 統合- API (CVE のみ))] レコードを選択します。

Name	Active	Class	Updated	Source Instance
Clarity CTD Vulnerability Closure Integration	false	Clarity CTD Vulnerability Integration	2023-06-09 09:52:27	Clarity CTD
Clarity CTD Vulnerability Detection Integration - Delta Import	false	Clarity CTD Vulnerability Integration	2023-06-22 10:23:09	Clarity CTD
Clarity CTD Vulnerability Detections - Full Import	true	Clarity CTD Vulnerability Integration	2023-06-22 10:23:16	Clarity CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solu...	2019-03-13 21:21:01	Microsoft Security Response Center Solu...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. [次以降にインポート] フィールドで、値を **NULL** に設定します。

4. [今すぐ実行] をクリックします。

脆弱性対応 Integration with Clarity CTD の構成

脆弱性対応 Integration with Clarity CTD を構成して、データのインポートを開始します。

Clarity CTD 脆弱性統合 ガイド付きセットアップ を使用して構成を完了します。

Clarity CTD 脆弱性統合 ガイド付きセットアップにアクセスするには、**Clarity CTD 脆弱性統合 > アドミン > セットアップ**.

Clarity CTD への接続

Clarity CTD に接続して、脆弱性統合のセットアップを開始します。

始める前に

セットアップを実行する前に、ナビゲーションバーで地球儀アイコン (🌐) を選択して、アプリケーションスコープを [脆弱性対応と **Clarity CTD** の統合] に変更します。

必要なロール：admin

手順

1. 移動先 **すべて > Clarity CTD 脆弱性統合 > アドミン > セットアップ**.
2. [Clarity CTD に接続] セクションで、[接続のセットアップ] タスクを選択します。

3. [接続のセットアップ] タスク ページで、[構成] を選択します。
[Claroty CTD Connection Manager (Claroty CTD 接続マネージャー)] ページが開きます。
4. フォームで次のフィールドに入力します。

[Claroty CTD に接続] フォーム

フィールド	Description (説明)
Claroty EMC URL	Claroty CTD Enterprise Management Console (EMC) の URL。
最小 CVSS スコア	該当する場合は、共通脆弱性スコアリングシステム (CVSS) スコアに基づいてインポートする脆弱性をフィルタリングできます。これは以上フィルターであるため、「9.0」と入力すると、統合は CVSS スコアが 9.0 ~ 10.0 の脆弱性をインポートします。
ユーザー名	Claroty アカウントのユーザー名。
パスワード	Claroty アカウントのパスワード。
MID サーバー	Claroty EMCがオンプレミスの場合は、MID サーバー が必要になる場合があります。その場合は、ここで MID サーバー を選択します。

5. [更新] を選択します。
6. [テスト接続] を選択します。
接続テストが成功すると、「結果 200」出力メッセージが表示されます。接続試行に失敗すると、Claroty から受信したエラーコードとメッセージが表示されます。

デルタインポート統合のアクティブ化

デルタインポート統合をアクティブ化して、Claroty CTD から脆弱性をインポートします。

始める前に

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[脆弱性情報データベース統合の実行](#)」を参照してください。

必要なロール：admin

このタスクについて

デルタインポート統合は、前回成功した統合実行からの脆弱性を Claroty CTD からインポートします。デフォルトでは、最初の実行で過去 90 日間のデータがインポートされます。[開始時間] フィールドをクリアすると、完全インポートになります。

手順

1. 移動先 すべて > **Claroty CTD 脆弱性統合** > アドミン > セットアップ。
2. [統合スケジュール済みジョブを構成] セクションで、[デルタインポート統合のアクティブ化] タスクを選択します。
3. [構成] を選択します。
4. デルタインポート統合レコードが [アクティブ] に設定されていることを確認します。
5. [実行] フィールドが [オンデマンド] に設定されていることを確認します。

6. オプション: 完全インポートを実行するには、[開始時間] フィールドをクリアします。

7. [更新] を選択します。

サービスグラフコネクタの後に脆弱性統合を実行する

Claroty CTD のサービスグラフコネクタを実行した後、Claroty CTD 脆弱性統合を実行します。サービスグラフコネクタを実行した直後に脆弱性統合を実行すると、Claroty CTD から最新の CMDB 情報が入力されます。

始める前に

サービスグラフ コネクタの後に実行する 脆弱性対応 統合を実行するには、Claroty CTD のサービスグラフコネクタ統合が構成され、アクティブになっている必要があります。

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[脆弱性情報データベース統合の実行](#)」を参照してください。

必要なロール: admin

手順

1. 移動先 すべて > **Claroty CTD 脆弱性統合** > アドミン > セットアップ。
2. [統合スケジュール済みジョブを構成] タスクで、[サービスグラフコネクタ後に実行] タブを選択します。
3. [構成] を選択します。
4. [SGC の後に実行 - Claroty CTD 脆弱性検出統合 - デルタインポート] レコードで、[アクティブ] オプションを選択してアクティブ化します。
5. [Run] フィールドが [**After Parent Runs**] に設定されていることを確認します。
6. [親] フィールドが [**SG-OT Claroty CTD 資産のインポートスケジュール**] に設定されていることを確認します。
7. [更新] を選択します。

自動クローズ統合のアクティブ化

自動クローズ統合をアクティブ化して、対応する ServiceNow 脆弱性検出をクローズします。

始める前に

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[脆弱性情報データベース統合の実行](#)」を参照してください。

必要なロール: admin

このタスクについて

脆弱性対応と Claroty CTD の統合に使用できるクローズ統合ジョブは 2 つあります。

- Claroty CTD の解決済み脆弱性クローズ統合
- Claroty CTD 完全脆弱性クローズ統合

Claroty CTD 解決済み脆弱性クローズ統合は、ServiceNow 構成管理データベース (CMDB)で解決済みとマークされた脆弱性一致アイテム (VIT) をチェックします。次に、これらの VIT について Claroty CTD にクエリを実行し、Claroty CTD から取得した応答に基づいて VIT をクローズします。

Claroty CTD 完全脆弱性クローズ統合は、ServiceNow CMDB内のステータス (解決済みかどうか) に関係なく、すべての VIT をチェックします。次に、Claroty CTD にすべての VIT を照会し、Claroty CTD に対応する CVE エントリがない VIT をクローズします。

手順

1. 移動先 **すべて > Claroty CTD 脆弱性統合 > アドミン > セットアップ**.
2. [統合スケジュール済みジョブを構成] タスクで、[自動クローズ統合のアクティブ化 (**Activate Auto-Closure Integration**)] タブを選択します。
3. [構成] を選択します。

注:

自動クローズ統合は、デルタインポート後に実行するように事前構成されているため、スケジュールは必要ありません。

4. [実行] フィールドが [オンデマンド] に設定されていることを確認します。
5. レコードが [アクティブ] に設定されていることを確認します。
6. [更新] を選択します。

Claroty CTD からの完全インポート統合の構成

Claroty CTD からデバイスの脆弱性インベントリ全体をインポートするように完全インポート統合を構成します。

始める前に

Claroty CTD レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[脆弱性情報データベース統合の実行](#)」を参照してください。

必要なロール：admin

このタスクについて

Claroty CTD 脆弱性検出 - フルインポート統合は、特定の日付に関係なく、Claroty CTD からデバイスの脆弱性インベントリ全体をインポートします。この統合は、日次デルタインポートで必要なすべての脆弱性データがインポートされていない場合に便利です。

注:

完全インポート統合では、最小 CVSS スコア構成が優先されます。CVSS 9.0 以上のみをインポートするように統合を構成した場合、完全インポートでは CVSS 9.0 以上のみをインポートします。

手順

1. 移動先 **すべて > Claroty CTD 脆弱性統合 > アドミン > セットアップ**.
2. [統合スケジュール済みジョブを構成] タスクで、[完全インポート統合を構成] タブを選択します。
3. [構成] を選択します。
4. [実行] フィールドが [オンデマンド] に設定されていることを確認します。
5. レコードが [アクティブ] に設定されていることを確認します。
6. [更新] を選択します。

システムプロパティの設定

脆弱性対応 Integration with Claroty CTD のシステムプロパティを設定して、必要に応じてプロパティを有効にできるようにします。

始める前に

セットアップを実行する前に、ナビゲーションバーで地球儀アイコン () を選択して、アプリケーションスコープを [脆弱性対応と **Claroty CTD** の統合] に変更します。

必要なロール:sn_otvr.integration_admin

手順

1. 移動先 **すべて > Claroty CTD 脆弱性統合 > アドミン > プロパティ**
2. 組織の必要に応じて、システムプロパティレコードを更新します。
脆弱性対応 Integration with Claroty CTD アプリケーション用にインストールされるシステムプロパティの詳細については、「[脆弱性対応 Integration with Claroty CTD のためにインストールされるプロパティ](#)」を参照してください。
3. [更新] を選択し、変更を保存します。

脆弱性対応 **Integration with Claroty CTD** のためにインストールされるプロパティ

脆弱性対応 Integration with Claroty CTD アプリケーションのシステムプロパティを有効にすることができます。

脆弱性対応 Integration with Claroty CTD システムプロパティにアクセスするには、次の場所に移動します **すべて > Claroty CTD 脆弱性統合 > アドミン > プロパティ**。

システムプロパティ

名前	説明	タイプ	デフォルト値
sn_clarotyctdvr.api_token_refresh_interval	Claroty CTD API トークンが有効である期間。デフォルトは 480 分 (8 時間) です。	整数	480
sn_clarotyctdvr.api_token_refresh_object	API トークンアクセスを確認します。	文字列	{"customer_name":"","first_name":"AP のサービ ス","id":1,"last_name":null,"mail":null,"p
sn_clarotyctdvr.auto_close_detection	Claroty CTD の古い脆弱性検出を自動クローズします。	true、false	false
sn_clarotyctdvr.auto_close_detection_interval	Claroty CTD の検出は、前回検出から指定された日数が経過すると自動的にクローズされます。	整数 days	90
sn_clarotyctdvr.default_page_size	Claroty CTD API からページごとにプルするレコードの数。	整数	500
sn_clarotyctdvr.detection_start_offset	Claroty CTD API からデータをインポートする場合、「開始時間」の前に指定された時間	整数 buffer	4

システムプロパティ (続く)

名前	説明	タイプ	デフォルト値
	数のバッファが追加されます。これにより、デルタインポートで欠落しているレコードがなくなります。		
sn_clarotyctdvr.integration_for_delta_days	Claroty CTD 統合の最初の実行時に過去数日間のデータがインポートされます。	整数	90
sn_clarotyctdvr.require_validation	脆弱性検出を作成するには、受信 CI が CMDB と一致する必要があります。	true、false	true

脆弱性対応 **Integration with Claroty CTD** のデータマッピング

このセクションでは、Claroty CTD API のフィールドを ServiceNow テーブルのフィールドにマッピングする方法を指定します。

脆弱性検出データマッピング

Claroty CTD フィールド	ServiceNow フィールド	メモ
	ソース	常に Claroty CTD に設定されます。
Identified_on	初回検出	
Last_updated	前回検出	
ステータス	ステータス	ステータス 0 は オープンを意味します。 ステータス 2 は、クローズ済み/修正済みを意味します。
Resource_id	Configuration item (構成アイテム)	構成アイテム (CI) は、sys_object_source テーブルでリソース ID を検索する CI ルックアップルールを使用して設定されます。たとえば、33.1 です。

脆弱性エントリーデータマッピング

脆弱性エントリーは、既存の共通脆弱性識別子 (CVE) レコードが National Vulnerability Database Entry [sn_vul_nvd_entry] テーブルに見つからない場合にのみ作成されます。Claroty CTD 統合で CVE を作成する必要がある場合は、テーブルにリストされている次のソースフィールドがマッピングされます。

Claroty CTD フィールド	ServiceNowフィールド	メモ
Cve_id	ID	例:CVW-2017-17562
タイトル	サマリー	統合によって [Claroty] がサマリーに追加され、Claroty によってバックフィルされた NVD CVE が表示されるようになります。たとえば、SIPROTEC の [Claroty] 認証バイパスの脆弱性などです。
CVSS	V3_base_score	
Published (公開済み)	Date_published	
変更あり	Last_modified	

脆弱性対応 Integration with Claroty CTD のエラー

脆弱性対応 Integration with Claroty CTD の作業中に、トラブルシューティングが必要なエラーが発生する可能性があります。

脆弱性検出統合 (データ検索)

エラーメッセージ	考えられる原因
ユーザー名とパスワードの組み合わせがないと Claroty CTD 統合を実行できません。	ユーザー名またはパスワードが統合構成に存在しません。
REST メッセージと REST メソッドを指定しないと統合を実行できません。	Claroty CTD 統合ジョブレコードで、REST メッセージまたは REST メソッドのフィールドが入力されていません。
Claroty CTD サーバーの URL を指定しないと統合を実行できません。	統合構成に URL が存在しません。
検出 API リソースパスを指定しないと統合を実行できません。	統合構成で、detection_api_resource_path パラメーターが入力されていません。デフォルトは /ranger/assets_with_insights です。
Claroty CTD から無効な応答コード {response code} を受信しました。	Claroty API からの応答が無効でした。たとえば、Claroty CTD から「Invalid response code 401 (無効な応答コード 401)」というメッセージを受信します。この無効な応答コードは、権限がなく、認証情報 (ユーザー名/パスワード) が無効である可能性が高いことを意味します。
JSON データから count_total プロパティを読み取れません。	ページネーションに使用された count_total が API 応答に存在しませんでした。Claroty CTD から無効なペイロードが受信されたことを意味する可能性があります。 Claroty CTD インスタンスが MID サーバー経由でアクセス可能であることを確認し、データソースの添付ファイル response.json ファイルを調べて count_total が存在することを確認します。

脆弱性検出統合 (データ処理)

エラーメッセージ	考えられる原因
添付ファイルの書き込み中にエラーが発生しました。	システムが応答データをデータソースに添付できませんでした。さらにサポートが必要な場合は、アドミニストレーターにお問い合わせください。 このエラーの一般的な原因は、MID サーバーユーザーに <code>sn_vul.vr_import_admin</code> ロールがないことです。
添付ファイルのコンテンツが null:添付ファイル <code>sys_id = {sys_id}</code> 。	データソースの添付ファイルの内容が null です。これは、Claroty API 自体の問題、または ServiceNowの問題を示している可能性があります。さらにサポートが必要な場合は、アドミニストレーターにお問い合わせください。
{sys_id} sys_id添付ファイルが見つかりませんでした。	データソースの添付ファイルが見つかりませんでした。前のエラーと同じ手順に従います。

脆弱性自動クローズ統合 (データ検索)

エラーメッセージ	考えられる原因
ユーザー名とパスワードの組み合わせがないと Claroty CTD 統合を実行できません。	ユーザー名またはパスワードが統合構成に存在しません。
REST メッセージと REST メソッドを指定しないと統合を実行できません。	Claroty CTD 統合ジョブレコードで、REST メッセージまたは REST メソッドのフィールドが入力されていません。
Claroty CTD サーバーの URL を指定しないと統合を実行できません。	統合構成に URL が存在しません。
検出 API リソースパスを指定しないと統合を実行できません。	統合構成で、 <code>detection_api_resource_path</code> パラメーターが入力されていません。デフォルトは <code>/ranger/assets_with_insights</code> です。
Claroty CTD から無効な応答コード {response code} を受信しました。	Claroty API からの応答が無効でした。たとえば、Claroty CTD から「Invalid response code 401 (無効な応答コード 401)」というメッセージを受信します。この無効な応答コードは、権限がなく、認証情報 (ユーザー名/パスワード) が無効である可能性が高いことを意味します。
JSON データから <code>count_total</code> プロパティを読み取れません。	ページネーションに使用された <code>count_total</code> が API 応答に存在しませんでした。Claroty CTD から無効なペイロードが受信されたことを意味する可能性があります。 Claroty CTD インスタンスが MID サーバー経由でアクセス可能であることを確認し、データソースの添付ファイル <code>response.json</code> ファイルを調べて <code>count_total</code> が存在することを確認します。

エラーメッセージ	考えられる原因
応答本文からの「objects」配列の解析中にエラーが発生しました。	Claroty CTD から無効なペイロードが受信されたことを意味すると考えられます。Claroty CTD インスタンスが到達可能であることを確認し、[Outbound HTTP Logs (送信 HTTP ログ)] をチェックして有効な応答があったかどうかを確認します。

脆弱性自動クローズ統合 (データ処理)

エラーメッセージ	考えられる原因
データディクショナリ JSON の解析に失敗しました。	データソース添付ファイルからのペイロードが無効な JSON でした。このエラーが発生する前に別のエラーが発生している可能性があります。Claroty CTD インスタンスが到達可能であることを確認し、[Outbound HTTP Logs (送信 HTTP ログ)] をチェックして有効な応答があったかどうかを確認します。

脆弱性対応 Microsoft Defender for IoT (Azure) との統合

Microsoft Defender for IoT (Azure) との 脆弱性対応 統合では、Microsoft Defender for IoT (Azure) からインポートされたデータを使用して、本番プロセスのコンテキストでリスクベースのアクションを有効にします。

ServiceNow オペレーショナルテクノロジー脆弱性対応 アプリケーションとの 脆弱性対応 統合を使用して、本番プロセスで使用されるデバイスの脆弱性を追跡、優先順位付け、および解決します。

主要な機能

- Microsoft Defender for IoT (Azure) から OT に関連付けられた CVE をインポートし、脆弱性一致アイテム (VIT) を作成して、本番プロセスのコンテキストで OT デバイスの脆弱性データを一目で見られるビューを作成します。
- 脆弱性のインポートを独自のスケジュールで自動的に実行します。
- アサインルールを使用すると、リスクベースのアクションを実行できるローカルサイトベースのチームに、修復のために VIT を自動的にルーティングできます。

脆弱性対応 for Microsoft Defender for IoT (Azure) をインストールする

admin ロールを持っている場合は、Microsoft Defender for IoT (Azure) の 脆弱性対応 をインストールできます。このアプリケーションには、関連する ServiceNow Store アプリケーションとプラグインがインストールされます (まだインストールされていない場合)。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。
- 次のものをレビュー [脆弱性対応 for Microsoft Defender for IoT \(Azure\)](#) 依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性に関する情報が ServiceNow Store にリストされているアプリケーション。

- 脆弱性対応 for Microsoft Defender for IoT (Azure) には、次の ServiceNow Store アプリケーションが必要です。脆弱性対応 Integration with Microsoft Defender for IoTをインストールする前に、これらのアプリケーションがインストールされていることを確認してください。

CMDB CI クラスモデルストアアプリ

この統合では、オペレーショナルテクノロジー [拡張クラス](#) CMDB CI クラスモデルアプリケーションの一部です。詳細については、「[CMDB CI Class Models](#)」を参照してください。

サービスグラフ コネクタ Microsoft Defender for IoT (Azure)

この統合では、オペレーショナルテクノロジーマネージャー アプリケーションを使用して、センサーアプライアンス、OT デバイス、ネットワーク接続のインポートを自動化します。サービスグラフをインストールするには、「[サービスグラフ Microsoft Defender for IoT用コネクタ \(Azure\)](#)」を参照してください。

必要なロール：admin

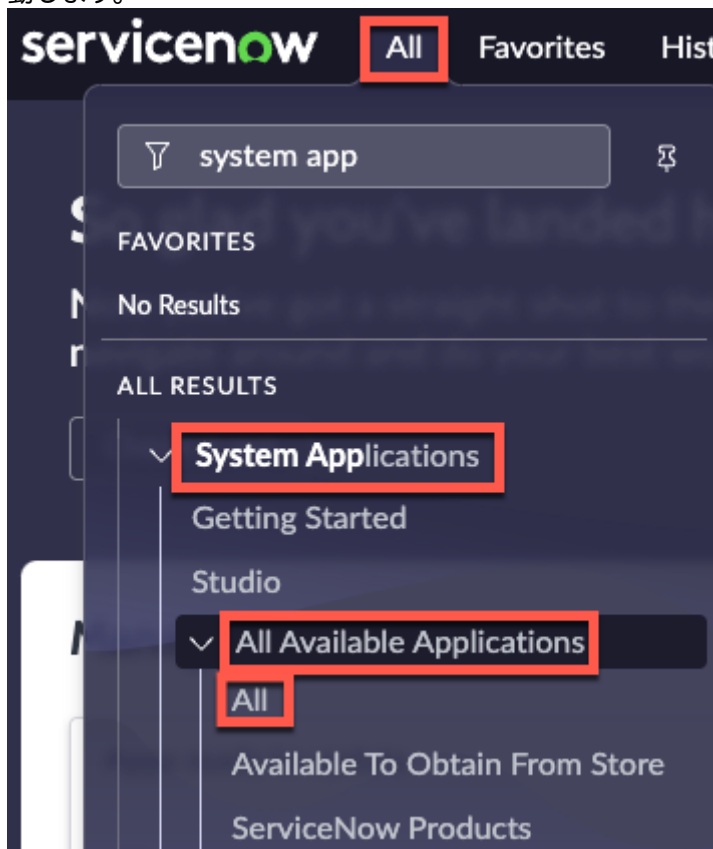
このタスクについて

次のアイテムは、脆弱性対応 for Microsoft Defender for IoT (Azure) とともにインストールされます。

- 脆弱性対応プラグイン
- NVD の脆弱性対応統合

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して、脆弱性対応 Integration for Microsoft Defender for IoT (Azure) を検索します。

名前またはアプリケーションスコープ ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、アプリケーションを同期するか、ServiceNow Store から要求してインスタンスにエンタイトルメントを付与する必要があります。

[インストール] ボタンの横のリストに、使用可能なバージョンが表示されます。

3. リストからバージョンを選択し、[インストール] を選択します。

表示されるインストールダイアログボックスには、アプリケーションと併せてインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエンタイトルメントを取得します。

5. [インストール] を選択します。

Microsoft Defender for IoT との脆弱性対応 統合 (Azure) のガイド付きセットアップに移動します。

脆弱性対応 Integration with Microsoft Defender for IoT (Azure) をインストールした後、ガイド付きセットアップに移動してアプリケーションの構成を確認します。

始める前に

ナビゲーションバーで地球儀アイコン (地球儀 ) を選択して、アプリケーションスコープを Vulnerability Response Integration with Microsoft Defender for IoT (Azure) に変更します。

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT** 脆弱性統合 > アドミン > ガイド付きセットアップ。
2. [Get Started (開始する)] を選択します。

Microsoft Defender for IoT に接続する (Azure)

Microsoft Defender for IoT (Azure) に接続して、脆弱性統合のセットアップを開始します。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT** 脆弱性統合 > アドミン > ガイド付きセットアップ。
2. [Microsoft Defender for IoT への接続 (Azure)] セクションで、[接続のセットアップ] タスクを選択します。
3. [接続のセットアップ] タスク ページで、[構成] を選択します。
[Microsoft Azure Defender for IoT への接続] ページが開きます。
4. フォームで次のフィールドに入力します。

[Microsoft Azure Defender for IoT への接続] フォーム

フィールド	Description (説明)
OAuth トークン URL	login.microsoftonline.com の OAuth 2.0 トークン URL。例: https://

フィールド	Description (説明)
	login.microsoftonline.com/<your tenant id>/oauth2/v2.0/token)。
OAuth クライアント ID	クライアント ID。
OAuth クライアントシークレット	クライアントシークレット。
ページサイズ制限	データの各ページでプルするレコードの最大数。デフォルトは 500 です。
最小 CVSS スコア	CVSS スコアがこの値以上の脆弱性のみがインポートされます。すべての脆弱性に対するデフォルトは 0.0 です。
サービスグラフコネクタのインポート後に実行	これは、Microsoft Defender for IoT (Azure) デバイスのインポートが完了した直後に脆弱性インポートを実行する推奨フィールドです。これにより、受信した脆弱性データを CMDB と照合できる可能性が最大限に高まります。 最も一般的な値は、SG-OT Microsoft Azure D4IoT デバイススケジュール済みインポートです。このフィールドを選択する場合は、[Azure D4IoT 脆弱性検出統合 - フルインポート] スケジュール済みジョブを [オンデマンドで実行] に設定したままにします。これにより、デバイスのインポートが完了すると、サービスグラフコネクタデバイスのインポートで子ジョブとして実行できるようになります。
日次インポート時間	[サービスグラフコネクタインポート後に実行] フィールドを使用していない場合は、このフィールドを使用して統合の日次インポート時間を設定できます。 i 注: [サービスグラフコネクタインポート後に実行] フィールドでインポートスケジュールが選択されている場合、このフィールドは使用できません。

5. [更新] を選択します。

6. [テスト接続] を選択します。

接続テストが成功すると、「結果 200」出力メッセージが表示されます。接続に失敗すると、Microsoft Defender for IoT (Azure) から受信したエラーコードとメッセージが表示されます。

脆弱性情報データベース統合の実行

脆弱性情報データベース (NVD) 統合を実行して、米国国立標準技術研究所 (NIST) の NVD 製品からデータをインポートします。NVD 統合を実行すると、Microsoft Defender for IoT (Azure) の脆弱性によって参照される基本的な共通脆弱性識別子 (CVE) データが提供され、環境内の脆弱性の重大度と詳細を判断するのに役立ちます。

始める前に

インスタンスで NIST NVD 統合を実行する前に、統合のインストールと構成のステップを完了する必要があります。インストールと構成を完了すると、NVD 製品が オペレーショナルテクノロジー脆弱性対応 アプリケーションと適切に統合されます。

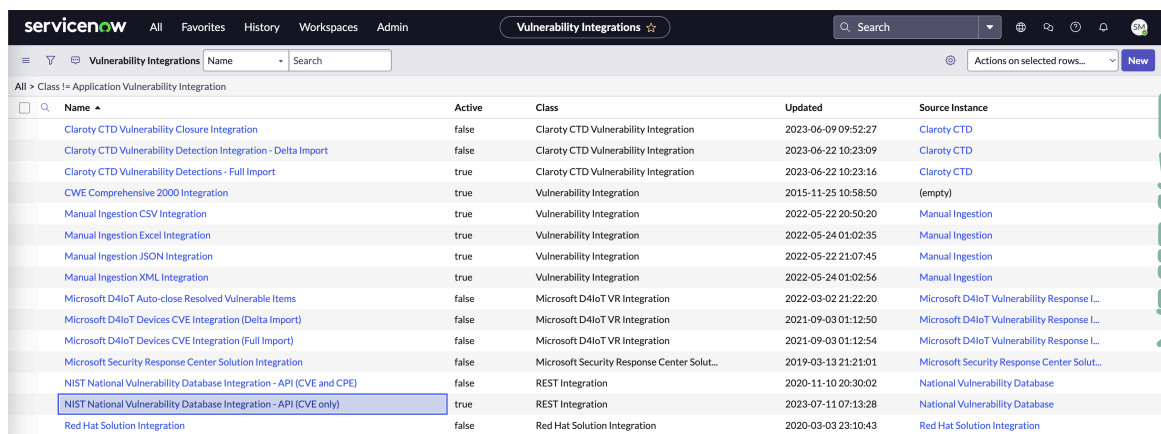
NVD プラグインをインストールするには、「[Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT** 脆弱性統合 > アドミン > ガイド付きセットアップ。
2. [統合を構成] セクションで、[脆弱性情報データベース (NVD) CVE エントリをインポート] タスクの横にある [構成] を選択します。
3. どちらがアクティブかに応じて、[NIST NVD 統合 - API (CVE のみ)] レコードまたは [NIST NVD 統合 - API (CVE および CPE)] レコードを選択します。

注：
NIST NVD 統合 - API (CVE のみ) レコードは、通常、デフォルトでアクティブになっています。



Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

4. レコードを編集するには、地球儀 (地球) を使用して、アプリケーションスコープを **[Vulnerability Response Integration with NVD]** に設定します。
5. [統合の詳細] タブの [次以降にインポート] フィールドで、値を過去の日付に設定します。

注：
これは、NVD の完全インポートが行われるために必要です。推奨される日付は 1999-01-01 00:00:00 です。

6. [保存] を選択します。
7. [今すぐ実行] をクリックします。

統合スケジュール済みジョブの構成

脆弱性データをインポートするスケジュール済みジョブをアクティブ化します。

始める前に

Microsoft Defender for IoT (Azure) レコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[脆弱性情報データベース統合の実行](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT 脆弱性統合** > アドミン > ガイド付きセットアップ。
2. [統合を構成] セクションで、[統合スケジュール済みジョブの確認とアクティブ化 (**Verify and Activate Integration Scheduled Jobs**)] タスクの横にある [構成] を選択します。
3. [**Azure D4IoT 脆弱性検出統合 - フルインポート (Azure D4IoT Vulnerability Detection Integration - Full Import)**] ジョブを選択します。
このジョブは、Microsoft Defender for IoT (Azure) から脆弱性検出をインポートします。
4. [アクティブ] フィールドの横のチェックボックスをオンにします。
追加の変更が必要な場合は、スケジュールを調整することもできます。[接続のセットアップ] タスクでサービスグラフコネクタのインポート後に実行するように脆弱性統合を構成した場合は、このジョブをオンデマンドで実行するように設定しておく必要があります。[接続のセットアップ] タスクの詳細については、「[Microsoft Defender for IoT に接続する \(Azure\)](#)」を参照してください。
5. [更新] を選択します。
6. **Azure D4IoT 脆弱性クローズ統合**ジョブを選択します。
Azure D4IoT 脆弱性クローズ統合 は、Microsoft Defender for IoT (Azure) から削除された検出を特定し、ServiceNowでクローズする検出ジョブです。
7. [アクティブ] フィールドの横のチェックボックスをオンにします。
[実行] フィールドを [オンデマンド] のままにしておくことをお勧めします。
8. [更新] を選択します。

[古い検出を自動クローズ] をアクティブ化

古い検出の自動クローズプロセスで使用されるシステムプロパティを構成して、環境内に存在しない脆弱性を自動的にクローズします。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT 脆弱性統合** > アドミン > ガイド付きセットアップ。
2. [古い検出を自動クローズ (オプション)] セクションで、[古い検出を自動クローズをアクティブ化] タスクを選択します。
3. [構成] を選択します。
4. [**Azure D4IoT VR 自動クローズプロパティ**] ページの [**Microsoft Azure Defender for IoT の古い検出を自動クローズしますか?**] フィールドで、[はい] を選択します。
5. [**Microsoft Azure Defender for IoT** の検出は更新されてから (値) 日後に自動的にクローズされる] フィールドに、検出が自動的にクローズされるまでの日数を入力します。
デフォルトは 90 です。
6. [保存] を選択します。

[古い検出を自動クローズ (**Auto-Close Stale Detections**)] ジョブのアクティブ化

スケジュール済みジョブをアクティブ化して、古い検出を定期的に自動クローズします。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > **Azure D4IoT** 脆弱性統合 > アドミン > ガイド付きセットアップ。
2. [古い検出を自動クローズ (オプション)] セクションで、[古い検出を自動クローズ] スケジュール済みジョブのアクティブ化 タスクを選択します。
3. [構成] を選択します。
4. [アクティブ] フィールドの横のチェックボックスをオンにします。
5. オプション: [実行] フィールドで、ニーズに合ったオプションを選択します。
デフォルトでは、このフィールドは [オンデマンド] に設定されていますが、必要に応じて変更できます。たとえば、[毎日] を選択し、表示される [時間] フィールドでその日の時間と分を選択できます。
6. [保存] を選択します。

脆弱性対応 **Integration with Microsoft Defender for IoT** のサポート (**Azure**)

データマッピングとエラー処理に関する質問については、このセクションを参照してください。

データマッピング

次の表では、Microsoft Defender for IoT (Azure) アプリケーションで脆弱性検出と脆弱性情報データベース (NVD) エントリに使用されるデータマッピングフィールドと、データが ServiceNow CMDB にインポートされた後に使用される同等のエントリがあるかどうかについて説明します。

脆弱性検出

[Microsoft Defender for IoT (Azure)] フィールド	ServiceNowフィールド
該当なし	source i 注: このフィールドは常に Microsoft Azure Defender for IoT に設定します。
name	detection_key
該当なし	status i 注: デフォルトでは、このフィールドはオープンを意味する 0 に設定されています。

NVD エントリ

[Microsoft Defender for IoT (Azure)] フィールド	ServiceNowフィールド
プロパティ/vulnerabilityId	ID
	source i 注: デフォルトでは、このフィールドは NVD に設定されています。

NVD エントリー (続く)

[Microsoft Defender for IoT (Azure)] フィールド	ServiceNowフィールド
プロパティ/説明	summary
プロパティ/スコア	スコア
プロパティ/exploitType	エクスプロイト有無 API データがエクスプロイトの存在を示している場合、統合はこのフィールドを [はい] に設定します。
プロパティ/exploitType	public_exploit API データがエクスプロイトの存在を示している場合、統合はこのフィールドを [はい] に設定します。

構成アイテム (CI) ルックアップ

CI ルックアップは、Microsoft Defender for IoT (Azure) の **deviceid** を使用して実行されます。サービスグラフコネクタによって入力されるsys_object_sourceテーブルで、一致する deviceid が検索されます。一致が見つかった場合、検出と脆弱性一致アイテムはその CI にリンクされます。

i 注:

デフォルトでは、脆弱性検出を挿入するには CI の一致が必要です。これにより、CMDB内の未分類のハードウェア CI を最小限に抑えることができます。この動作を変更するには、**sn_msft4iotazvr.require_ci_matchsystem** プロパティを **false** に設定します。このプロパティを false に設定すると、CI の一致が見つからない場合に、未分類のハードウェア CI を作成できます。

エラー処理

統合は、ほとんどが事前構成されているように設計されているため、Azure テナント ID、クライアント ID、クライアントシークレットを入力するだけで済みます。アプリケーションからのログメッセージは、**sn_msft4iotazvr** ソースのシステムログで表示できます。**sn_vul** ソースから、関連する追加のログメッセージが表示されることもあります。

統合実行が失敗した場合、統合実行の [メモ] フィールドにエラーが表示されます。ステータスは [完了] に設定され、サブステータスは [失敗] になります。

インポートキュー (sn_vul_ds_import_q_entry) テーブルには、処理待ちのすべての変換要求が含まれています。このテーブルをフィルタリングして、ステータスが [処理中] のアイテムのみを表示し、現在変換中のアイテムを表示できます。

次の表に、データ取得時およびデータ処理時のエラーメッセージと考えられる原因を示します。

脆弱性検出統合 (データ検索)

エラーメッセージ	考えられる原因
Cannot run integration without a REST message and REST method specified (REST	検出統合ジョブレコードで、 REST メッセージまたは REST メソッドのフィールドが入力されていません。

脆弱性検出統合 (データ検索) (続く)

エラーメッセージ	考えられる原因
メッセージと REST メソッドを指定しないと統合を実行できません)	
Microsoft Defender for IoT (Azure) oauth_client_idを指定しないと統合を実行できません	統合インスタンスでは、 OAuth クライアント ID が入力されていません。
Microsoft Defender for IoT (Azure) oauth_client_secretを指定しないと統合を実行できません	統合インスタンスでは、 OAuth クライアント シークレット が入力されていません。
Cannot run integration without the detection API resource path specified (検出 API リソースパスを指定しないと統合を実行できません)	統合インスタンスで、検出 API リソースパスが入力されていません。 デフォルトは https://management.azure.com/providers/Microsoft.ResourceGraph/resources です
指定された API バージョンで統合を実行できません	統合インスタンスでは、API バージョンは入力されません。 デフォルトは 2021-03-01 です。
Microsoft Defender for IoT (Azure) から無効な応答コード {response code} を受信しました	Microsoft API からの応答が無効です。 たとえば、Microsoft Defender for IoT (Azure) から受信した無効な応答コード 401 は、承認されていないことを意味します。認証情報または OAuth トークンが無効である可能性があります。
JSON 応答本文の解析に失敗しました	受信した JSON 応答は、解析できない場合は無効です。これは、データが受信されなかったことを意味します。認証情報が正しいこと、その他のエラーが発生していないことを確認します。
Error writing attachment (添付ファイル書き込みエラー)	システムは応答データをデータソースに添付できませんでした。さらにトラブルシューティングを依頼するために、システムアドミニストレーターに問い合わせる必要がある可能性があります。このエラーの一般的な原因は、MID サーバーまたは 実行 ユーザーに sn_vul.vr_import_admin ロールがないことです。
Attachment content is null: attachment sys_id = {sys_id} (添付ファイルの内容が null です: 添付ファイル sys_id = {sys_id})	データソースの添付ファイルの内容が null です。これは、Microsoft API 自体の問題、または ServiceNow の問題を示している可能性があります。より詳細なトラブルシューティングを

脆弱性検出統合 (データ検索) (続く)

エラーメッセージ	考えられる原因
	システムアドミニストレーターに依頼してください。
Could not find attachment with sys_id {sys_id} (sys_id {sys_id} の添付ファイルが見つかりませんでした)	データソース添付ファイルが見つかりませんでした。これは、Microsoft API 自体の問題、または ServiceNow の問題を示している可能性があります。より詳細なトラブルシューティングをシステムアドミニストレーターに依頼してください。

脆弱性検出統合 (データ処理)

エラーメッセージ	考えられる原因
脆弱性 ID がないと検出を作成できません	レコードに脆弱性 ID が存在しませんでした。これは、Microsoft API の問題が原因である可能性があります。

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール)

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) は、Microsoft Defender for IoT (オンプレミス管理コンソール) からインポートされたデータを使用して、本番プロセスのコンテキストでリスクベースのアクションを有効にします。

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションを使用して、本番プロセスで使用されるデバイスの脆弱性を追跡、優先順位付け、および解決します。

主要な機能

- OT デバイスに関連付けられた CVE を Microsoft Defender for IoT (オンプレミス管理コンソール) からインポートし、脆弱性一致アイテム (VIT) を作成して、OT デバイスの脆弱性データを本番プロセスのコンテキストとともに一目で見られるようにします。
- 新しく検出された脆弱性のインポートを独自のスケジュールで自動的に実行する。
- VIT のアサインルールを使用して、リスクベースのアクションを実行できるローカルサイトベースのチームに、修復のために VIT を自動的にルーティングできます。

脆弱性対応 for Microsoft Defender for IoTをインストールする (オンプレミス管理コンソール)

admin ロールを持っている場合は、脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) をインストールできます。このアプリケーションには、関連する ServiceNow Store アプリケーションとプラグインがインストールされます (まだインストールされていない場合)。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。
- 次のものをレビュー [脆弱性対応 for Microsoft Defender for IoT \(オンプレミス管理コンソール\)](#) 依存関係、ライセンスやサブスクリプションの要件、およびリリースの互換性に関する情報が ServiceNow Store にリストされているアプリケーション。

- 脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) には、次の ServiceNow Store アプリケーションが必要です。脆弱性対応 Integration with Microsoft Defender for IoTをインストールする前に、これらのアプリケーションがインストールされていることを確認してください。

CMDB CI クラスモデルストアアプリ

この統合では、オペレーショナルテクノロジー [拡張クラス](#) CMDB CI クラスモデルアプリケーションの一部です。詳細については、「[CMDB CI Class Models](#)」を参照してください。

サービスグラフ コネクタ Microsoft Defender for IoT (オンプレミス)

この統合では、オペレーショナルテクノロジーマネージャー アプリケーションを使用して、センサーアプライアンス、OT デバイス、ネットワーク接続のインポートを自動化します。サービスグラフをインストールするには、「[サービスグラフ Connector for Microsoft Defender for IoT \(オンプレミス管理コンソール\)](#)」を参照してください。

必要なロール：admin

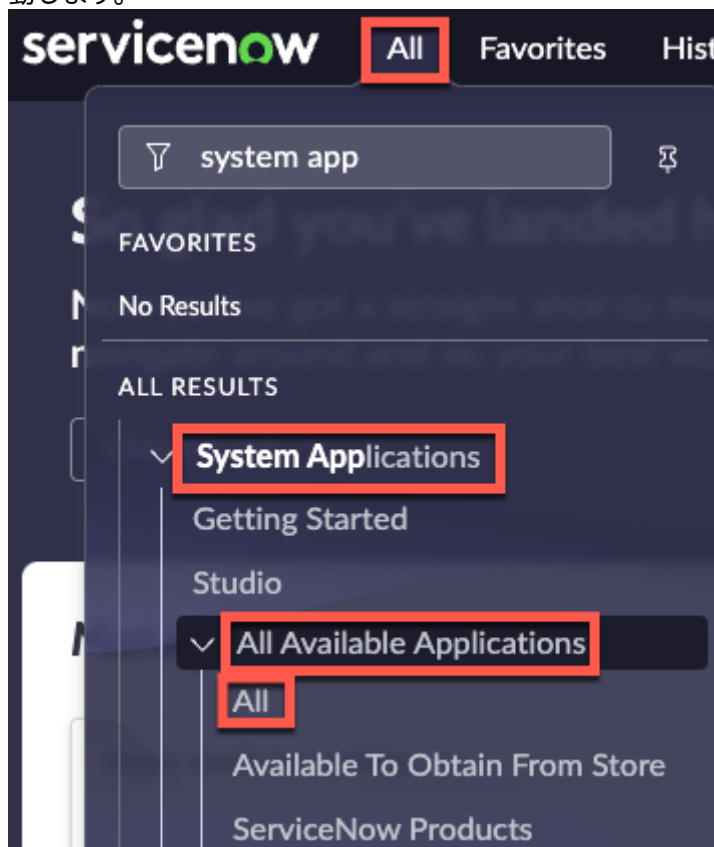
このタスクについて

次の項目は、脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) と共にインストールされます。

- 脆弱性対応プラグイン
- NVD の脆弱性対応統合

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して、Microsoft Defender for IoT (オンプレミス管理コンソール) の脆弱性対応を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることがあります。

[インストール] ボタンの横のリストに、使用可能なバージョンが表示されます。

3. リストからバージョンを選択し、[インストール] を選択します。

表示されるインストールダイアログボックスには、アプリケーションと併せてインストールされている依存関係が一覧表示されます。

4. プロンプトが表示された場合は、ServiceNow Store へのリンクに従って、依存関係のエントリメントを取得します。

5. [インストール] を選択します。

Microsoft Defender for IoT (オンプレミス管理コンソール) ロールの脆弱性対応の割り当て

ユーザーにロールを割り当てて、脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションの機能、性能、およびデータへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次の表に示すロールを持つユーザーは、脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションを使用できます。

必要に応じて、アドミンユーザーまたはユーザーグループにロールをアサインします。

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) ロール

ロール	Description (説明)
OT VR 統合ビューアー [sn_otvr.integration_viewer]	OT VR 統合レコードを表示できます。
OT VR 統合アドミン [sn_otvr.integration_admin]	OT VR 統合を構成して実行できます。
MID サーバー [mid_server]	MID サーバーを設定できます。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

脆弱性情報データベース統合の実行

脆弱性情報データベース (NVD) 統合を実行して、米国国立標準技術研究所 (NIST) の NVD 製品からデータをインポートします。NVD 統合を実行すると、環境内で見つかった共通脆弱性識別子 (CVE) の重大度と詳細を判断する際に役立ちます。

始める前に

インスタンスで NIST NVD 統合を実行する前に、インストールと構成のステップを完了する必要があります。インストールと構成を完了すると、NVD 製品がオペレーショナルテクノロジー脆弱性対応 アプリケーションと適切に統合されます。

NVD プラグインをインストールするには、「[Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 **すべて** > **脆弱性対応** > **管理** > **統合**.
2. [NIST NVD integration - API (CVE only) (NIST NVD 統合- API (CVE のみ))] レコードを選択します。

Name	Active	Class	Updated	Source Instance
Claroty CTD Vulnerability Closure Integration	false	Claroty CTD Vulnerability Integration	2023-06-09 09:52:27	Claroty CTD
Claroty CTD Vulnerability Detection Integration - Delta Import	false	Claroty CTD Vulnerability Integration	2023-06-22 10:23:09	Claroty CTD
Claroty CTD Vulnerability Detections - Full Import	true	Claroty CTD Vulnerability Integration	2023-06-22 10:23:16	Claroty CTD
CWE Comprehensive 2000 Integration	true	Vulnerability Integration	2015-11-25 10:58:50	(empty)
Manual Ingestion CSV Integration	true	Vulnerability Integration	2022-05-22 20:50:20	Manual Ingestion
Manual Ingestion Excel Integration	true	Vulnerability Integration	2022-05-24 01:02:35	Manual Ingestion
Manual Ingestion JSON Integration	true	Vulnerability Integration	2022-05-22 21:07:45	Manual Ingestion
Manual Ingestion XML Integration	true	Vulnerability Integration	2022-05-24 01:02:56	Manual Ingestion
Microsoft D4IoT Auto-close Resolved Vulnerable Items	false	Microsoft D4IoT VR Integration	2022-03-02 21:22:20	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Delta Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:50	Microsoft D4IoT Vulnerability Response L...
Microsoft D4IoT Devices CVE Integration (Full Import)	false	Microsoft D4IoT VR Integration	2021-09-03 01:12:54	Microsoft D4IoT Vulnerability Response L...
Microsoft Security Response Center Solution Integration	false	Microsoft Security Response Center Solut...	2019-03-13 21:21:01	Microsoft Security Response Center Solut...
NIST National Vulnerability Database Integration - API (CVE and CPE)	false	REST Integration	2020-11-10 20:30:02	National Vulnerability Database
NIST National Vulnerability Database Integration - API (CVE only)	true	REST Integration	2023-07-11 07:13:28	National Vulnerability Database
Red Hat Solution Integration	false	Red Hat Solution Integration	2020-03-03 23:10:43	Red Hat Solution Integration

3. [次以降にインポート] フィールドで、値を **NULL** に設定します。

4. [今すぐ実行] をクリックします。

Microsoft Defender for IoTの脆弱性対応を構成する (オンプレミス管理コンソール)

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) 統合のレコードを構成します。

始める前に

脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) のガイド付きセットアップを使用して、構成を完了します。ガイド付きセットアップにアクセスするには、次の場所に移動します。 **MSFT D4IoT 脆弱性統合** > **管理** > **ガイド付きセットアップ**。

必要なロール:sn_otvr.integration_admin および mid_server

手順

1. 移動先 **すべて** > **MSFT D4IoT 脆弱性統合** > **管理** > **構成管理**.
2. [新規] をクリックします。
3. フォームのフィールドに入力します。
フィールド値の説明については、「[Microsoft Defender for IoT VR 構成フォーム](#)」を参照してください。
4. [認証情報の保存と検証] をクリックします。

Microsoft Defender for IoT VR 構成フォーム

Microsoft Defender for IoT VR 構成フォームを使用して、脆弱性対応 for Microsoft Defender for IoT (オンプレミス管理コンソール) アプリケーションを構成します。

Microsoft Defender for IoT VR 構成フォーム

フィールド	説明
名前	構成の名前。
統合インスタンス	構成のインスタンス。 利用可能なデフォルトの統合インスタンスは Microsoft Defender for IoT 脆弱性対応 インスタンスです。
エンドポイント URL	Microsoft Defender for IoT 管理コンソールの URL。 例: https://10.10.0.222/external/v3/integration/devicecves
MID サーバー	統合に使用される MID サーバー。
API キー	Central Manager API にアクセスするために必要なトークン。 Microsoft Defender for IoT管理コンソールでの API キーの作成については、 「https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis」 を参照してください。
ページサイズ	Microsoft API 応答のページあたりのデバイス数。 デフォルトのページサイズは 50 です。
CVSS V2 スコア	設定された CVSS V2 スコア以上のスコアを持つ脆弱性は、CVE のインポートおよび脆弱性一致アイテム (VIT) レコードの作成の対象となります。 デフォルト値は 0 に設定されています。
解決済み VI の自動クローズ	VIT レコードが解決済みに設定されている場合、その OT デバイスの Microsoft Defender for IoT からの API 応答に CVE が表示されなくなったときに、VIT レコードを自動的に閉じることができます。
解決済み VI を再度開くまでの待機日数	VIT が解決された場合、ネットワーク内の OT デバイスの通信に基づいて脆弱性が解決されているかどうかを Microsoft Defender for IoT 確認するのにしばらく時間がかかる場合があります。 NIDS が VIT をクローズ済みと確認できない場合に、解決済み VIT を再オープンするまでの日数を定義します。

インポートスケジュールの構成

Microsoft Defender for IoTレコードにアクセスするためのインポートスケジュールを設定します。

始める前に

Microsoft Defender for IoTレコードのインポートをスケジュールする前に、NVD 統合を実行して問題を修正します。詳細については、「[脆弱性情報データベース統合の実行](#)」を参照してください。

必要なロール：admin

手順

1. 移動先 **すべて > MSFT D4IoT 脆弱性統合 > 管理 > 統合**.
2. レコードリストから、次のレコードを選択します。
 - 完全インポートスケジュールでは、すべての OT デバイスのすべての脆弱性がインポートされます。



注:

レコード数が増える可能性があるため、完全インポートスケジュールを頻繁に実行することはお勧めしません。

- デルタインポートのスケジュールは、デフォルトで Microsoft サービスグラフ Connections の統合後に実行されるように構成できます。「[OT 脆弱性対応 統合のシステム ID を構成する](#)」を参照してください。
- OT デバイスの脆弱性が解決された場合は、解決済み **VIT** インポートの自動クローズ スケジュールを使用します。脆弱性一致アイテム (VIT) がスキャナーからの確認に基づいて自動的に閉じます。

スコープが正しいアプリケーションにない場合、「このレコードを編集するにはここをクリックしてください」というメッセージがページの上部に表示されます。

3. レコードを編集するには、ここをクリックしてください。
4. [アクティブ] チェックボックスをオンにして、[アクティブ] を **true** に変更します。
5. 必要に応じて、ドロップダウンリストから [スケジュール] を選択します。
6. **[Execute Now (今すぐ実行する)]** をクリックします。

OT 脆弱性対応 統合のシステム ID を構成する

Microsoft SGC 接続の統合後に統合レコードを完全にインポートするようにシステム ID を構成します。

始める前に

必要なロール: admin

このタスクについて

脆弱性が報告されている可能性のあるすべての OT デバイスが CMDB に含まれるようにするには、この構成を強くお勧めします。

手順

1. 移動先 **すべて > サービスグラフコネクタ Microsoft D4 IoT > プロパティ**.

スコープが間違ったアプリケーションに設定されている場合、「このレコードを編集するにはここをクリックしてください (To edit this record click here)」というメッセージがページの上部に表示されます。

① This record is in the [Service Graph Connector Integration with Microsoft Azure Defender for IoT application](#), but [Global](#) is the current application. To edit this record click [here](#).

Microsoft Defender for IoT Integration Properties

Integration Configurations

The following system properties are used to configure the Microsoft Defender for IoT integration.

Sensor API resource path. Default value is "/external/v3/integration/sensors". ②

Device API resource path. Default value is "/external/v3/integration/devices". ②

Connection API resource path. Default value is "/external/v3/integration/connections". ②

(Optional) Override Connection Alias record sys_id used to connect the integration. Default value is empty. ②

The number of device records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. ②

The number of connection records to fetch in a paginated REST call to the Microsoft Defender for IoT Management Console. Default value is 50. ②

Get all devices. If not checked, then only devices created or updated since the last successful import will be imported. Default is No. ②

☐ Yes | No

Get all connections. If not checked, then only connections created or updated since the last successful import will be imported. Default is No. ②

☐ Yes | No

(Optional) Sys id of OT VR Integration (Scheduled Job) to execute after SG-OT Microsoft D4IoT Connections Import. ②

2. レコードを編集するには、ここをクリックしてください。

3. OT VR 統合のsys_idを使用してシステムプロパティ `sn_msft4iotsgc.ot.vr.integration.id` を構成します。

4. [保存] をクリックします。

古い検出の自動クローズの構成

[古い検出を自動クローズ] を有効にすると、サードパーティ統合によって最近検出されなかった古い脆弱性検出が自動的にクローズされます。

始める前に

必要なロール：admin

このタスクについて

古い検出は、重大なリスク脆弱性一致アイテム (VIT) を対象とする修復の結果である可能性が最も高いです。この修正は、さらに重要度が低く、[オープン] ステータスの複数の VIT にも対処しています。これらの VIT を [クローズ済み] に移動すると、Now Platform インスタンス内のアクティブな VIT と脆弱性グループの数が減少します。

手順

1. 移動先 **すべて > 脆弱性対応 > 管理 > 自動クローズ構成 > 古い検出**。

[古い構成を自動クローズ (Auto-Close Stale Configuration)] フォームが表示されます。

2. フィールドに入力します。

3. [古い検出を自動クローズする基準] フィールドで、[リストで最後に検出された検出] を選択します。

このオプションは、スキャナーによって検出が再度見つかった最新の日付を検索します。

i 注:

[前回スキャンされたデバイス] オプションは OT スキャナーには適用されません。

脆弱性対応 v22.0 以降では、検索の追加オプションを構成できます。詳細については、「[Create auto-close rules](#)」を参照してください。

4. モジュールを有効にするには、[アクティブ] チェックボックスをオンにします。

5. [最後に発見された検出 (日前)] フィールドに、古くなった検出の経過日数を入力します。

デフォルトは 90 日です。日数には任意の正の値を入力できます。この値は、Microsoft Defender for IoT によって提供された最終検出日と一致するために使用されます。[90] と [最後に発見された検出] が表示されている場合、過去 90 日間に検出されなかった脆弱性一致アイテムは自動的にクローズされます。

6. オプション: 保留された VIT または現在保留をレビュー中の VIT にマッピングされている古い検出を無視するには、[保留された VI の古い検出を無視する] チェックボックスをオンにします。このオプションを無効のままにすると、保留された VIT または保留をレビュー中の VIT にマッピングされた、基準に一致するすべての検出がクローズされます。保留された VIT またはこれらの検出に対応するレビュー中の VIT も、ロールアップロジックに基づいて自動的にクローズされます。ロールアップロジックの詳細については、「[Closing stale detections in Vulnerability Response](#)」を参照してください。

このオプションを有効にすると、保留された VIT または保留についてレビュー中の VIT にマッピングされる基準に一致する検出は、自動クローズ時にスキップされます。

7. オプション: [クローズされている VI の古い検出を無視する] チェックボックスをオフにします。デフォルトでは、このチェックボックスはオンになっており、このクローズ済み VIT に対する新しい検出が特定されたときにクローズ済み VIT が再オープンされないようにします。ロールアップロジックの詳細については、「[Closing stale detections in Vulnerability Response](#)」を参照してください。

8. [更新] を選択します。

スケジュール済みジョブ [Auto-Close Stale Detections] を毎日実行します。このジョブでは、選択された日付が「最後に検出があった日付」と「最後に資産がスキャンされた日付」のどちらであるかを判断します。当該検出のステータスが [古い] に移行します。[古い検出を自動クローズ] 機能では、アクティブな統合インスタンスにおいて古い検出をクローズするだけであるということがポイントです。アクティブな統合インスタンスに関連付けられている脆弱性一致アイテムや検出はクローズされます。脆弱性対応 v21.1 以降、スケジュール済みジョブは共通テーブル [sn_vul_cm_n_auto_close_rule] を考慮するように変更されました。

検出が [古い] とマークされた後、スキャナーがその検出の発見を再度報告すると、検出の [ステータス] フィールドは [オープン] に移行します。検出の対応する脆弱性一致アイテムも再オープンされます。

また、検出が [古い] とマークされていて、スキャナーがそれを [修正済み] であると判断した場合、検出は [クローズ済み] に移行します。ステータスは VIT にもロールアップされます。

オペレーショナルテクノロジー脆弱性対応の使用

サードパーティ統合からの脆弱性一致アイテムのインポートなど、必要なすべてのセットアップタスクを完了すると、産業用 ワークスペースから オペレーショナルテクノロジー脆弱性対応 アプリケーションを使用できます。

産業用 ワークスペース

オペレーショナルテクノロジー脆弱性対応を使用するには、産業用 ワークスペースから次のランディングページとメニューにアクセスします。

産業用 ワークスペースの詳細については、「[産業用 ワークスペース](#)」を参照してください。

OT マネージャーダッシュボードの [OT 脆弱性] タブ

産業用 ワークスペース の OT Manager (OT マネージャー) ダッシュボードの [OT Vulnerabilities (OT 脆弱性)] タブを使用して、次のデータを表示します。

- 過去 7 日間に作成された新しい OT 脆弱性一致アイテムの概要。
- リスクスコア別およびステータス別の OT 脆弱性一致アイテムの概要。
- 未対応の脆弱性一致アイテム (未アサインでオープン状態の OT 脆弱性一致アイテム)。
- 機器モデルの各レベルでの OT デバイスのリスクスコアの概要、および脆弱性一致アイテムのリスト。

[OT 脆弱性] タブの詳細については、「[オペレーショナルテクノロジーマネージャー ダッシュボード](#)」を参照してください。

の OTVR (PA) ダッシュボード 産業用 ワークスペース

OTVR (PA) ダッシュボードを使用して、脆弱性一致アイテムのボリューム、パフォーマンス、および初期分析と検出から封じ込めや修復までの進捗状況を追跡します。アサイン先グループ、エクスポイト、リスク評価、またはステータスでレポートをフィルタリングして、脆弱性エクスポージャーと影響を受けるサービスに関するインサイトを得ることができます。

OTVR (PA) ダッシュボードの詳細については、以下を参照してください。 [オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボード](#)

リストメニュー

[List (リスト)] メニューを使用して、自分がアクセスできるすべての OT 脆弱性一致アイテムレコードと、自分または自分がメンバーであるアサイン先グループにアサインされた修復タスクを表示します。

- OT 修復タスク
 - 自分にアサイン済み
 - 所属グループにアサイン済み
- OT 脆弱性一致アイテム
 - 自分にアサイン済み
 - 所属グループにアサイン済み
 - 自分の例外要求
 - すべての例外



注:

[すべての例外] リストには、ステータスが [却下] の例外も表示されます。

[OT 修復タスク] または [OT 脆弱性一致アイテム] リストメニューの下のレコードに移動して、OT 関連のコンテキストを取得します。レコードの履歴を表示するには、さまざまな作業メモ、コメン

ト、およびレコードの更新がキャプチャされるレコードの [アクティビティ] ウィンドウを表示します。[作成 (**Compose**)] ウィンドウで新しいコメントまたは作業メモを追加することもできます。

修復タスクの詳細については、「[修正タスクの作成](#)」を参照してください。

産業用 ワークスペース for オペレーショナルテクノロジー脆弱性対応 のリストビューの使用法の詳細については、「[IT 修復ワークスペースのリストビューの使用](#)」を参照してください。

機器モデルメニュー

機器マネージャーを使用して、OT 脆弱性一致アイテムを表示し、機器モデルエンティティにマッピングされている OT デバイスに関連付けられた修復タスクを表示および作成します。

関連情報

[脆弱性対応のワークスペース](#)

修正タスクの作成

機器モデルエンティティにマッピングされている OT デバイスに関連付けられた修復タスクを作成します。

始める前に

必要なロール:sn_otvr.remediation_owner

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. [機器モデル] ページを開きます。
3. [**Equipment model view for** (次の機器モデルビュー)] フィールドで、機器モデル情報を表示するサイトを選択します。
4. 適切な機器モデルエンティティを選択し、[**Vulnerable Items** (脆弱性一致アイテム)] 関連リストタブに移動します。
5. 修復タスクに追加する脆弱性一致アイテムレコードを選択し、[**Create remediation task** (修復タスクの作成)] を選択します。

The screenshot shows the ServiceNow interface for the 'Industrial Workspace'. The main view is 'Equipment model view for San Diego'. On the left, a sidebar shows the navigation tree with 'San Diego' and 'Airport' expanded, and 'Terminal 1' selected. The main content area displays the 'Terminal 1' view with tabs for 'Details', 'Upstream Process', 'Downstream Process', 'Child Entities', 'OT Assets (6)', 'OT Incidents (1)', 'OT Change Requests (7)', and 'Vulnerable Items (41)'. The 'Vulnerable Items' tab is active, showing a table of items. The table has columns: Number, Summary, OT asset, Manufacturer, Risk score, Risk rating, State, and Remediation task. The items listed are VIT0010001, VIT0010232, VIT0010235, VIT0010236, VIT0010237, and VIT0010238. Each item has a summary, OT asset, manufacturer (BizLink), risk score, risk rating (None, High, Medium, Low), and state (Open). A 'Create remediation task' button is located at the top right of the table. The bottom of the page shows 'Showing 1-20 of 41' and '20 rows per page'.

6. 修復タスクに必要なすべての詳細情報を入力します。

[Assignment group (アサイン先グループ)] フィールドは、サイトのアサイン先グループに基づいて自動的にアサインされます。

7. [Save (保存)] をクリックしてタスクレコードを作成します。

タスクの結果

修復タスクを作成すると、機器モデルエンティティのメンテナンススケジュールによって決定された次回の定期メンテナンス中にそのタスクが選択されます。機器モデルエンティティのスケジュールの詳細については、「[機器モデルの管理](#)」を参照してください。

修復タスクの開始時間を手動で選択することもできます。開始時刻の選択の詳細については、「[修復タスクの開始時間の選択](#)」を参照してください。

での脆弱性一致アイテム (VIT) のソリューションの表示 産業用ワークスペース

脆弱性一致アイテム (VIT) で、オペレーショナルテクノロジー (OT) 脆弱性ソリューション管理 によって提供される優先ソリューションまたは利用可能なすべてのソリューションを表示します。

始める前に

必要なロール：admin

手順

1. VITS のリストに移動します。

- 移動先 [すべて](#) > **Industrial Workspace** (産業用ワークスペース) > リストビュー () > OT 脆弱性一致アイテム。
- 移動先 [すべて](#) > **Industrial Workspace** (産業用ワークスペース) > 機器モデルビュー () > 脆弱性一致アイテム。

2. 表示されたリストから VIT を選択します。

3. VIT の [修正] セクションでは、優先ソリューションまたは VIT で利用可能なすべてのソリューションを表示できます。

VIT で利用可能なソリューションが複数ある場合は、[優先ソリューション] フィールドの  を選択して、VIT で利用可能なすべてのソリューションを検索して表示します。

関連情報

[オペレーショナルテクノロジー 脆弱性ソリューション管理](#)

修復タスクの開始時間の選択

機器モデルエンティティのスケジュールのタイムスロットを使用して、オペレーショナルテクノロジー (OT) 修復タスクの予定開始時間を選択します。

始める前に

必要なロール: sn_otvr.remediation_owner

このタスクについて

OT 修復タスクの開始時刻を 手動 選択するには、2 つの方法があります。

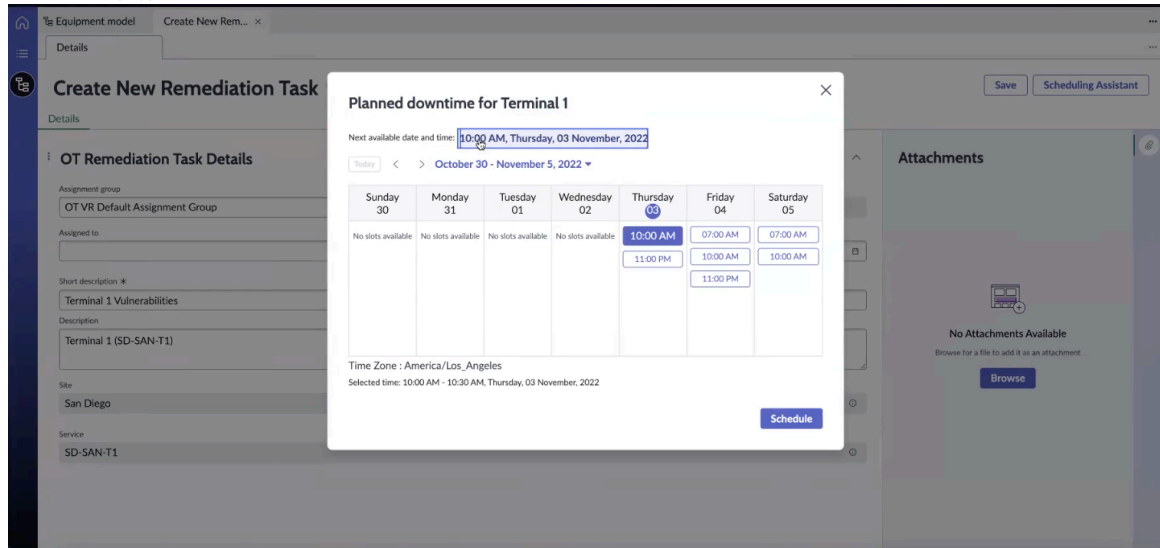
- 修復タスクの作成時に開始時間を選択するには、[新しい修復タスクを作成] フォームで [スケジュールアシスタント] を選択します。
- 既存の修復タスクを開き、そこからスケジュールを設定できます。

スケジュールアシスタントは、機器モデルエンティティのスケジュールのタイムスロットを使用します。詳細については、「[機器モデルエンティティのスケジュールを管理する](#)」を参照してください。

手順

1. 修復タスクの作成中に開始時間を選択する場合は、次のアクションを実行します。

- a. [修正タスクの作成](#)を参照し、ステップ 1 ～ 6 を完了します。
- b. [スケジュールアシスタント] を選択します。
- c. 修復タスクを実行する日時スロットを選択しま



す。

d. [Schedule] を選択します。

2. 既存の修復タスクの開始時間を選択する場合は、次のアクションを実行します。

- a. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
- b. リストビューで、**OT 修復タスク** > 自分にアサイン済み。
- c. リストから、開始時間を設定する修復タスクを選択します。
- d. [スケジュールアシスタント] を選択します。
- e. 修復タスクを実行する日時スロットを選択します。
- f. [Schedule] を選択します。

タスクの結果

設定された時間内に修復タスクが実行されます。

修復タスクを分割

ユーザーは、修復タスクレコードから脆弱性一致アイテム (VI) を分割して、修復タスクを作成できます。

始める前に

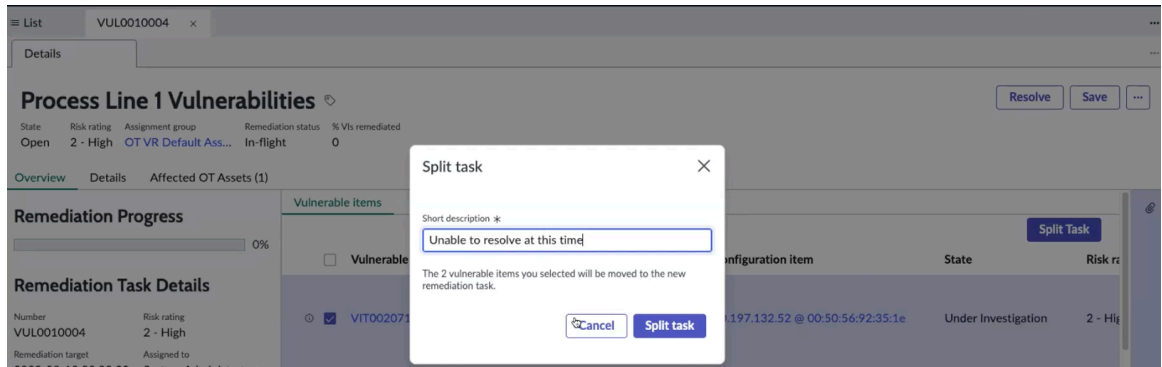
必要なロール: sn_otvr.remediation_owner

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース) > **OT 修復タスク** > 自分にアサイン済み。
2. リストから、新しい修復タスクに移動する VI を選択します。

3. [タスクを分割] をクリックします。
4. 表示されるダイアログで、[簡単な説明] フィールドに入力します。
リストから選択した VI の数が表示されます。

タスク分割メッセージ



5. [タスクを分割] を再度クリックします。

修復タスクの保留

修復タスクを保留して、後で解決できる例外要求を作成します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. 産業用 ワークスペースリストビューを開くには、リスト (☰) アイコンを選択します。
3. **[OT Remediation Tasks (OT 修復タスク)]** モジュールで、使用可能なリストのいずれかを選択します。
4. 保留する修復タスクを選択します。
5. [例外の要求] ボタンを選択します。
6. フォームのフィールドに入力します。

フィールド	説明
期限	保留ステータスが期限切れになり、修復タスクが再アクティブ化される日付を選択します。
理由	問題を保留する理由を入力します。次の選択肢があります。 ○ メンテナンス期間待ち ○ 誤検出 ○ 修正が利用不可 ○ リスクの受容

フィールド	説明
	○ コントロールの緩和を実施 ○ その他
追加情報	その他の関連情報を入力します。

7. [保存] を選択します。

タスクの結果

例外要求が作成されます。例外要求は、[OT 修復タスク] モジュールの [自分の例外要求] リストで確認できます。OT 修復タスクモジュールの [すべての例外] リストで、既存のすべての例外要求を表示することもできます。

の補完コントロールを使用 オペレーショナルテクノロジー

オペレーショナルテクノロジー (OT) の補完コントロールを使用して、すぐにパッチを適用できない脆弱性によってもたらされるリスクを軽減します。

このタスクについて

補完コントロールは、エクスプロイトが成功する可能性や影響を軽減するのに役立ちます。補完コントロールの詳細については、「[Understanding compensating controls for risk change](#)」を参照してください。

始める前に

必要なロール:sn_vul.vulnerability_admin または sn_vul.vulnerability_analyst

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース).
2. リスト () アイコンを選択します。
3. [ライブラリ] モジュールで、[補完コントロール] リストを選択します。
4. [新規] を選択します。
5. フォームで次のフィールドに入力します。

補完コントロールフォーム

フィールド	説明
名前	追加する補正コントロールの名前。
Description (説明)	追加する補正コントロールの説明。
アクティブ	選択すると、補正コントロールがアクティブになります。

6. [保存] を選択します。

での一般的な脆弱性エントリーの表示 産業用 ワークスペース

産業用 ワークスペース内の共通脆弱性エントリー (CVE) を表示して、補完コントロールに必要な情報にアクセスします。

始める前に

必要なロール：sn_vul.vulnerability_admin

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. リスト () アイコンを選択します。
3. [ライブラリ] モジュールで、[**CVE**] リストを選択します。

オペレーショナルテクノロジー脆弱性対応 参照

参照トピックには、オペレーショナルテクノロジー脆弱性対応 アプリケーションに関する追加情報が記載されています。

オペレーショナルテクノロジー脆弱性対応とともにインストールされるコンポーネント

オペレーショナルテクノロジー脆弱性対応 (com.sn_otvr) プラグインが有効になると、いくつかのタイプのコンポーネント (ユーザーロール、ビジネスルールなど) がインストールされます。

注:

アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

この機能ではデモデータを利用できます。

インストールされるロール

ロールタイトル [名前]	説明	含まれるロール
OT 脆弱性修正オーナー [sn_otvr.remediation_owner]	修復タスクを作成できます。脆弱性一致アイテムの既存の修復タスクをスケジュールすることもできます。	• cmdb_ot_isa_viewer • cmdb_ot_viewer • sn_vul.close_vi_vg • sn_vul.remediation_owner
OT VR 統合ビューアー [sn_otvr.integration_viewer]	オペレーショナルテクノロジー脆弱性対応統合レコードを表示できます。	なし
OT VR 統合アドミン [sn_otvr.integration_admin]	オペレーショナルテクノロジー脆弱性対応統合レコードを表示および編集できます。	• sn_sec_cmn.admin • sn_otvr.integration_viewer • sn_vul.read_all

インストールされるビジネスルール

ビジネスルール	テーブル	Description (説明)
OT VIT の修復タスクへの関連付け	修復タスク [sn_vul_vulnerability]	OT 修復タスクが作成されると、タスク > フィルターのグループ化構成で指定されたフィルター条件に従って、関連付けられた脆弱性一致アイテムがタスクにグループ化されます。

関連情報

ネットワーク侵入検知システム (NIDS) 拡張クラス、OT 拡張クラス、および関連アプリケーションの詳細を確認します。

概要

拡張クラスは、オペレーショナルテクノロジー管理構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

Network Intrusion Detection System (NIDS) CI extension class

ネットワーク侵入検知システム (NIDS) [cmdb_ci_nids] クラスは、パッシブネットワーク監視アプライアンスと、それが検出するネットワーク上のデバイスとの間の関係を構築します。

Operational Technology (OT) extension classes

構成管理データベース (CMDB)は OT のクラスを更新します。

関連アプリケーション

Vulnerability Response

オペレーショナルテクノロジー脆弱性対応 と統合すると、ServiceNow 脆弱性対応 アプリケーションはプロセスの重要度に基づいて OT の脆弱性を優先順位付けして解決するのに役立ちます。

CMDB CI Class Models

CMDB CI Class Models ストアアプリは、クラスの説明、識別ルール、識別子エントリ、および依存関係を含む、CMDB クラス階層を拡張するクラスモデルを追加します。

産業用プロセスマネージャー

産業用プロセスマネージャー アプリケーションを使用して、ServiceNow 産業用ソリューションに必要な ISA-95 機器モデルデータ基盤を作成し、各産業現場で独自のバージョンの機器モデルを作成できるようにします。

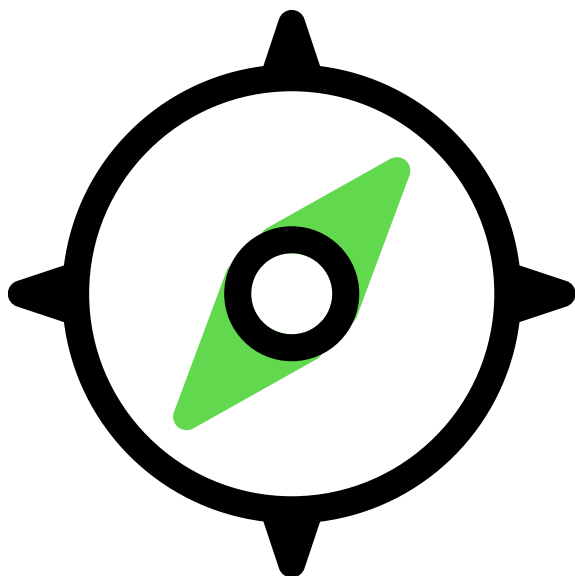
オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー アプリケーションを使用すると、複数のソースから OT デバイスデータを集計できるため、産業用ソリューションで使用される基本的なデータ関係を構築できます。

オペレーショナルテクノロジーインシデント管理

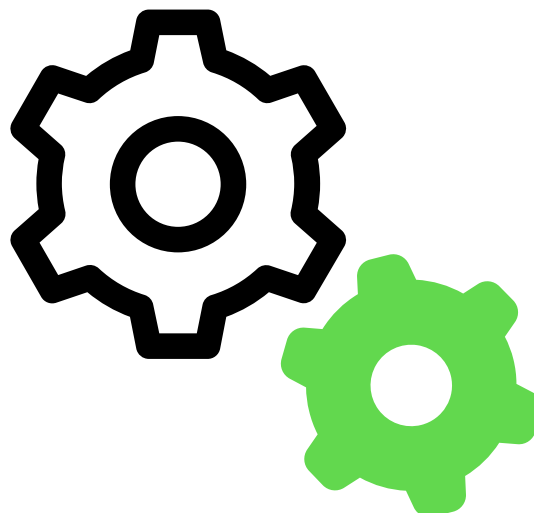
オペレーショナルテクノロジーインシデント管理 を使用すると、メーカーは OT デバイスインシデントをオープンからクローズまで管理できます。

探索



オペレーショナルテクノロジー
インシデント管理 の探索

Configure (構成)



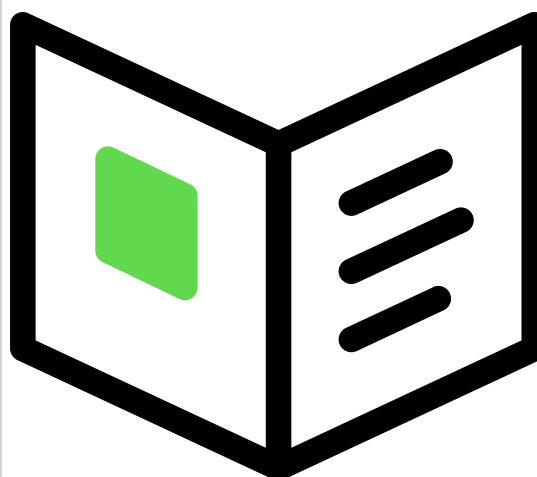
実装の計画と構成

使用



オペレーショナルテクノロジー
インシデント管理 の使用

参照



関連情報とアプリケーションの詳細を取得

オペレーショナルテクノロジーインシデント管理 の探索

オペレーショナルテクノロジーインシデント管理 アプリケーションの詳細を表示します。

主な機能

オペレーショナルテクノロジーインシデント管理 では、次の主要な機能を使用できます。

- OT インシデントを作成し、ワークフローを進めて、OT デバイスの影響を受ける生産プロセスを迅速に復元します。
- OT インシデントのコンテキストと生産プロセスへの影響を理解します。
- OT インシデントを IT インシデントと別にして監視し管理します。
- OT インシデント履行者に別のロールをアサインします。
- OT ユーザーエクスペリエンスの向上。
- オペレーショナルテクノロジーのナレッジ管理のサポート。詳細については、「[オペレーショナルテクノロジーのナレッジ管理](#)」を参照してください。

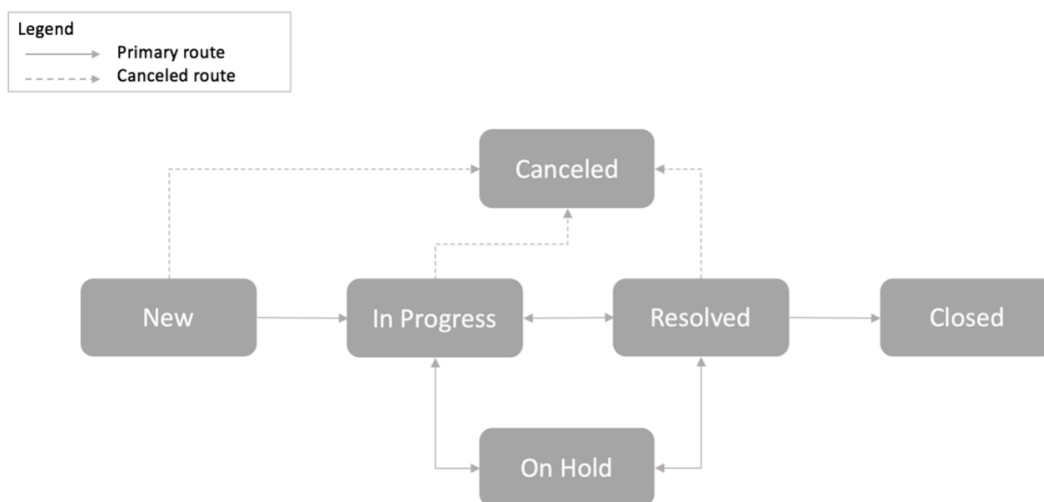
オペレーショナルテクノロジーインシデント管理

オペレーショナルテクノロジーインシデント管理 を使用すると、エンジニアはオペレーショナルテクノロジー (OT) デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジーインシデント管理 を使用すると、OT インシデントを IT インシデントとは別に管理できます。OT インシデントは、OT ネットワーク上の OT デバイスによって提供されるサービスが中断されると発生します。ときとして、インシデントが最初に作成されたときの OT デバイスが不明な場合があります。OT デバイスが不明な場合は、問題が発生した機器モデルエンティティに対してインシデントが発生する可能性があります。

OT インシデントマネージャーは、作成から終了までのインシデントのデフォルトのライフサイクルを管理する責任があります。OT Incident Management (インシデント管理) プロセスには多くのステータスがあり、それぞれのステータスがプロセスの成功と提供されるサービスの品質にとって重要です。さまざまな状況を次の図に示します。

オペレーショナルテクノロジーインシデント管理 プロセスステータス



インシデントのステータスは次のとおりです。

ステータス	説明
新規	インシデントはログに記録されていますが、調査はまだです。
処理中	インシデントはアサインされていて、調査中です。
保留中	詳しい情報、証拠、または解決策を提供するために、インシデントが一時的に別のエンティティに移行します。[保留中] オプションを選択すると、次の [保留理由] リストが表示されます。これらのリストオプションは、追加情報がどこから来ているのかを示します。 • 問い合わせユーザー待ち • 変更待ち • 問題待ち • ベンダー待ち 保留の理由が [Awaiting Caller] の場合、[Additional comments] セクションは必須です。 i 注: 問い合わせユーザーがインシデントを更新すると、[On Hold reason] フィールドがクリアされ、インシデントのステータスが [In Progress] に変わります。[アサイン先] フィールドに名前が記載されているユーザーとウォッチリストのユーザーにメール通知が送信されます。インシデントをクローズする前に、インシデントを 1 回以上保留にすることができます。
解決済み	インシデントが再発しないように、適切な修正が提供されます。
Closed (クローズ)	インシデントは所定の期間 [Resolved (解決済み)] の状況で経過すると、 [Closed (クローズ済み)] のマークが付けられ、問題なく解決したことが確定します。
キャンセル	インシデントはトリアーじされましたが、重複するインシデント、不要なインシデント、またはインシデントではないと判断されました。

産業用プロセスマネージャー との統合

オペレーショナルテクノロジーインシデント管理 を 産業用プロセスマネージャー と統合して、機器モデルエンティティに関するインシデントを報告します。

産業用プロセスマネージャー は、ServiceNow オペレーショナルテクノロジー ソリューションに必要な ISA-95 機器モデルデータ基盤を作成します。オペレーショナルテクノロジーインシデント管理と統合すると、本番プロセスに対するインシデントの影響を確認できます。

産業用プロセスマネージャー とともにインストールされる ISA Equipment Model プラグイン (sn_isa_model) は、指定されたロールのビューを有効にします。詳細については、「[ISA-95 機器モデル](#)」を参照してください。

OT デバイスレコードから OT インシデントが作成されると、次のことが起こります。

- OT インシデントフォームの **[OT device (OT デバイス)]** フィールドに、OT デバイスの値が入力されます。
- OT デバイスに関連付けられた機器モデルエンティティがある場合、その機器モデルエンティティは OT インシデントフォームの **[Equipment model entity (機器モデルエンティティ)]** フィールドに追加されます。
- OT インシデントフォームの **[Site (サイト)]** フィールドに、OT デバイスの値が入力されます。

機器モデルエンティティレコードから OT インシデントが作成されると、次のことが起こります。

- OT インシデントフォームの **[Equipment model entity (機器モデルエンティティ)]** フィールドに機器モデルエンティティの値が入力されます。
- OT インシデントフォームの **[Site (サイト)]** フィールドには、機器モデルエンティティのサイトが入力されます。

機器モデルエンティティレコードの **OT** インシデント関連リストには、そのエンティティで報告されたすべての OT インシデントが表示されます。フォーム上の **[Equipment model entity (機器モデルエンティティ)]** フィールドには、選択したサイトのエンティティのみを含めることができます。

オペレーショナルテクノロジーインシデント管理の構成

ServiceNow オペレーショナルテクノロジー ソリューションのデータ基盤を作成できるように、オペレーショナルテクノロジーインシデント管理 アプリケーションを構成します。

オペレーショナルテクノロジーインシデント管理 v2 は Tokyo P5 以降に依存しています。

注:

admin ロールを持っている場合は、ガイド付きセットアップを使用して、オペレーショナルテクノロジーインシデント管理 アプリケーションのセットアップを進めることができます。ガイド付きセットアップにアクセスするには、次の場所に移動します。産業用ワークスペースアドミン > ガイド付きセットアップ。

タスク	目的
1. ServiceNow Storeからオペレーショナルテクノロジーインシデント管理アプリケーションをインストールします。	オペレーショナルテクノロジーインシデント管理 アプリケーションとサポートプラグインをインストールします。
2. オペレーショナルテクノロジーインシデント管理 ロールを割り当てます。	ロールを割り当てて、各ユーザーが使用できるアクションをコントロールします。
3. OT インシデントを移行します。	OT インシデントをインシデントテーブルから OT インシデントテーブルに移行します。  注: この手順は、Paris、San Diego、または Tokyo から Utah にアップグレードする場合にのみ適用されます。

タスク	目的
4. OT インシデントのカテゴリとサブカテゴリを構成する。	必要に応じて、OT インシデントのカテゴリとサブカテゴリを構成します。
5. 状況モデルを設定します。	OT インシデントサイトのステータスモデルを構成します。
6. (オプション) アサインルールを作成します。	OT インシデントを適切なグループまたはユーザーに自動的にアサインするアサインルールを作成します。

オペレーショナルテクノロジーインシデント管理のインストール

admin ロールを持っている場合は、オペレーショナルテクノロジーインシデント管理 アプリケーション (sn_ot_inc_mgmt) をインストールできます。このアプリケーションは、関連する ServiceNow Store アプリケーションとプラグインをインストールします (まだインストールされていない場合)。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。
- オペレーショナルテクノロジーインシデント管理 には次のプラグインが必要です。オペレーショナルテクノロジーインシデント管理 をインストールする前に、これらのプラグインがアクティブ化されていることを確認してください。

必須の ServiceNow プラグイン

CMDB CI クラスモデル (sn_cmdb_ci_class)

CMDB CI Class Models (CMDB CI クラスモデル) ストアアプリは、クラスの説明、識別ルール、識別子エントリ、および依存関係を含む、CMDB クラス階層を拡張するクラスモデルを追加します。詳細については、「[CMDB CI クラスモデルストアアプリ](#)」を参照してください。

ISA Equipment Model (ISA 設備階層モデル) (sn_isa_model)

ISA-95 機器モデルエンティティおよびテンプレートのデータモデル詳細については、「[ISA-95 機器モデル](#)」を参照してください。

- オペレーショナルテクノロジーインシデント管理 には、次の ServiceNow Store アプリケーションのいずれかまたは両方が必要です。インストールする前に、これらのアプリケーションのうち少なくとも 1 つがインストールされていることを確認してください オペレーショナルテクノロジーインシデント管理。

必要な ServiceNow Store アプリケーション

オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー アプリケーションは、企業が ServiceNow オペレーショナルテクノロジー ソリューションを使用できるようにする基盤データと関係を作成します。オペレーショナルテクノロジーマネージャー は、Now Platform で構成管理データベース (CMDB)、サービスグラフコネクタ、およびディスカバリーアプリケーションの使用をサポートします。詳細については、「[オペレーショナルテクノロジーマネージャーの構成](#)」を参照してください。

産業用プロセスマネージャー

産業用プロセスマネージャー アプリケーションは、ServiceNow 産業用ソリューションに必要な ISA-95 機器モデルデータ基盤を作成し、各産業現場で独自のバージョンの機器モデルを作成できるようにします。詳細については、「[産業用プロセスマネージャー の構成](#)」を参照してください。

- 必要なロール：admin

このタスクについて

オペレーショナルテクノロジーインシデント管理 とともに次のアイテムがインストールされます。

- プラグイン
- ストアアプリケーション
- ロールと ACL

インストールされるロールと ACL の詳細については、「[オペレーショナルテクノロジーインシデント管理とともにインストールされるコンポーネント](#)」を参照してください。

i 注:

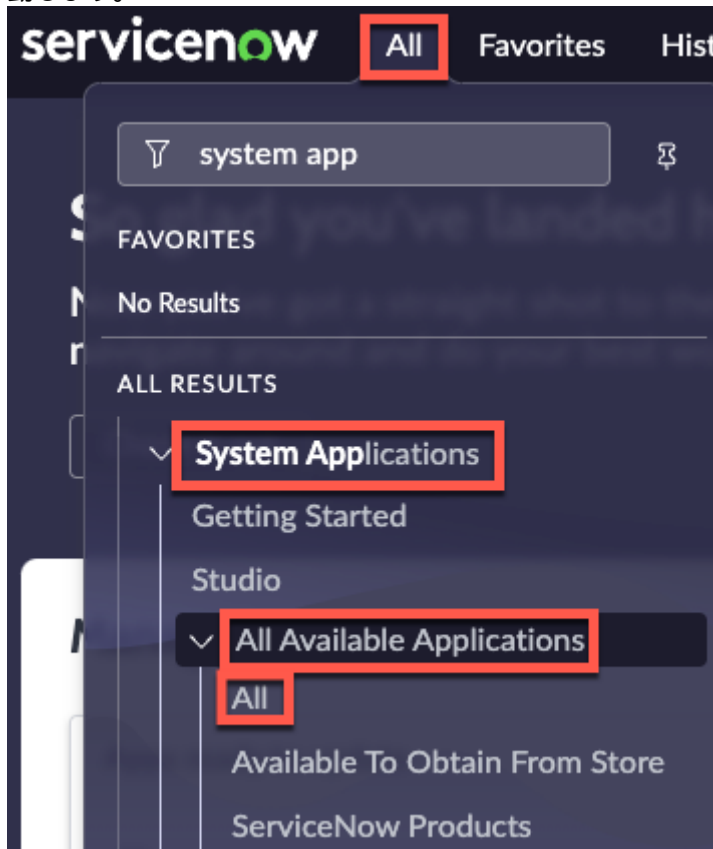
オペレーショナルテクノロジー ヴィジビリティのライセンスを持たないOperational Technology Service Managementユーザーの場合は、次の点に注意してください。

- 最新バージョンの オペレーショナルテクノロジーインシデント管理 がインストールされている場合は、産業用プロセスマネージャー もインストールされます。
- 最新バージョンの オペレーショナルテクノロジー変更管理 がインストールされている場合は、産業用プロセスマネージャー もインストールされます。

Operational Technology Service Managementエクスペリエンスにアクセスできるように、最新バージョンにアップグレードする必要があります。

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して、オペレーショナルテクノロジーインシデント管理 アプリケーション (sn_ot_inc_mgmt) を検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store へのリクエストが必要になることがあります。

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

依存するプラグインとアプリケーションがインストールされている場合、現在インストールされている場合、またはインストールする必要がある場合は、リストに表示されます。インストールする必要があるプラグインまたはアプリケーションがある場合は、オペレーショナルテクノロジーインシデント管理 をインストールする前にインストールする必要があります。

4. [インストール] を選択します。

インシデントを新しいインシデントテーブルに移行する

古いインシデントテーブルから新しいインシデントテーブルに オペレーショナルテクノロジー インシデントを移行します。インシデントを移行すると、古いテーブルが適用されなくなったことが オペレーショナルテクノロジーインシデント管理 アプリケーションに通知されます。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 産業用ワークスペースアドミン > ガイド付きセットアップ。
2. [オペレーショナルテクノロジーインシデント管理] カテゴリで、[開始] を選択します。
3. [Migrate OT Incidents (OT インシデントの移行)] セクションの横にある **[Configure (構成)]** を選択します。
4. [今すぐ実行] を選択して、移行を開始します。
5. オプション: このスケジュール済みジョブのアクティビティログを表示するには、次の場所に移動します すべて > システムログ > システムログ > すべて。

タスクの結果

オペレーショナルテクノロジーインシデントは新しいインシデントテーブルに移行され、オペレーショナルテクノロジーインシデント管理アプリケーションは古いテーブルを使用しなくなります。

ユーザーへのロールのアサイン

オペレーショナルテクノロジーインシデント管理アプリケーションでユーザーにロールをアサインして、機能やデータへのユーザーアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、オペレーショナルテクノロジーインシデント管理 アプリケーションを使用できます。

注:

OT インシデントユーザー [ot_incident_user] ロールは複製される。このロールがアサインされたユーザーに対して、スケジュール済みジョブ「新しい OT インシデントロールのアサイン」を実行して、新しい オペレーショナルテクノロジーインシデント管理 ロールをアサインすることができます。詳細については、「[ユーザーへの新しいロールのアサイン](#)」を参照してください。

ロール	Description (説明)
OT インシデントアドミン [sn_ot_incident_admin]	あらゆる機器モデルエンティティの OT インシデントレコードの作成、表示、削除、編集ができます。このロールを持つユーザーは、優先度 ルックアップルール と OT インシデントシステムプロパティを設定できます。
OT インシデントリーダー [sn_ot_incident_read]	OT インシデントレコードの表示のみ可能です。
OT インシデント履行者 [sn_ot_incident_write]	OT インシデントレコードを作成、表示、編集できます。

手順

Now Platformユーザー管理機能を使用して、ユーザーまたはグループにロールをアサインします。

ユーザーへの新しいロールのアサイン

オペレーショナルテクノロジーインシデント管理 アプリケーションのスケジュール済みジョブを通じて、OT インシデントユーザー [ot_incident_user] ロールを持っていたユーザーに新しいロールをアサインします。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

このタスクについて

OT インシデントユーザーロール [ot_incident_user] は廃止されました。スケジュール済みスクリプトの実行を通じて、ot_incident_userロールを持っていたユーザーに新しいロールを割り当てることができます。

手順

1. 移動先 **すべて** > システム定義 > スケジュール済みジョブ。
2. 検索バーで、[新しい **OT** インシデントロールのアサイン (**Assign New OT Incident Roles**)] スケジュール済みジョブを検索します。
3. [今すぐ実行] を選択して、スケジュール済みジョブを開始します。
4. オプション: このスケジュール済みジョブのアクティビティログを表示するには、次の場所に移動します **すべて** > システムログ > システムログ > **すべて**。

タスクの結果

スケジュール済みジョブが実行され、ユーザーに新しい オペレーショナルテクノロジーインシデント管理 ロールがアサインされます。

アサイン先グループの作成

OT インシデントレコードにアサインする オペレーショナルテクノロジー (OT) 固有のアサイン先グループを作成します。

始める前に

必要なロール：admin

このタスクについて

OT インシデントレコードの **[Assignment Group (アサイン先グループ)]** フィールドには、タイプが OT のアサイン先グループのみが表示されます。これは、オペレーショナルテクノロジー (OT) インシデントと情報技術 (IT) インシデントを分離するのに役立ちます。

OT インシデントレコードに表示する OT 固有のアサイン先グループを作成できます。

手順

1. 移動先 **すべて** > ユーザー管理 > グループ。
2. [新規] を選択します。
3. フォームのフィールドに入力します。

アサイン先グループフォーム

フィールド	説明
名前	アサイン先グループの名前
マネージャー	グループマネージャーまたはリード
タイプ	このグループのカテゴリです。[ターゲットレコードを選択] フィールドで、「OT」を検索して【タイプ】フィールドに追加します。
グループメール	グループのメール配布リストまたは連絡先のメールアドレス。
親	グループがメンバーとなっている他のグループ。
Description (説明)	アサイン先グループの説明

4. [送信] を選択します。

タスクの結果

これで、OT 固有のアサイン先グループがインシデントレコードに表示されるようになりました。

インシデントカテゴリとサブカテゴリ

オペレーショナルテクノロジー (OT) インシデントを分類することで、特定の OT インシデントの検索をグループ化して絞り込むことができます。

OT インシデントを作成できる場合は、次の表にリストされているカテゴリとサブカテゴリから選択できます。

インシデントカテゴリ

カテゴリ	サブカテゴリ
データベース	• DB2 • MS SQL Server • Oracle
ハードウェア	• OT の問題 • CPU • ディスク • キーボード • メモリー • 監視 • マウス

インシデントカテゴリ (続く)

カテゴリ	サブカテゴリ
問い合わせ/ヘルプ	• ウィルス対策 • メール • 内部アプリケーション
ネットワーク	• DHCP • DNS • IP アドレス • VPN • ワイヤレス
生産性	• マイナーストップ • 低速走行 • セットアップと調整 • ブレークダウン
品質	• 入荷する素材 • スタートアップの拒否 • プロセスの欠陥 - 定性的 • プロセスの欠陥 - 定量的
Safety	• ニアミス • 危険 • 安全性に関する懸念 • 事故
ソフトウェア	• メール • オペレーティングシステム

カテゴリまたはサブカテゴリを編集する

既存の オペレーショナルテクノロジー インシデントカテゴリとサブカテゴリを編集して、インシデントを分類します。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > 選択肢リスト**.
2. 条件フィルターを [テーブル] [次の値に等しい] **[sn_ot_incident]** および [要素] [次の値に等しい] [カテゴリ] または [要素] [次の値に等しい] [サブカテゴリ] に設定します。
3. カテゴリまたはサブカテゴリレコードを選択します。
4. 必要に応じてフォームを編集します。
5. [保存] を選択します。

タスクの結果

これで、既存のカテゴリまたはサブカテゴリへの変更がレコードに表示されます。

カテゴリまたはサブカテゴリを作成する

インシデントの分類に使用する オペレーショナルテクノロジー インシデントカテゴリまたはサブカテゴリを作成します。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > 選択肢リスト**.
2. カテゴリを作成するには、次のアクションを実行します。
 - a. [新規] を選択します。
 - b. [要素] フィールドに、「カテゴリ」という語を入力します。
 - c. [Label (ラベル)] フィールドに、カテゴリ名を入力します。
 - d. [Value (値)] フィールドに、カテゴリ値を入力します。
 - e. [Sequence (シーケンス)] フィールドに、シーケンス番号を入力します。
 - f. [送信] を選択します。
3. 新しいサブカテゴリを追加するには、次のアクションを実行します。
 - a. [新規] を選択します。
 - b. [要素] フィールドに「サブカテゴリ」という語を入力します。
 - c. [ラベル] フィールドに、サブカテゴリ名を入力します。
 - d. [値] フィールドに、サブカテゴリ値を入力します。
 - e. [Sequence (シーケンス)] フィールドに、シーケンス番号を入力します。
 - f. [送信] を選択します。

タスクの結果

新しいカテゴリまたはサブカテゴリは、オペレーショナルテクノロジー インシデントレコードで選択できます。

カテゴリまたはサブカテゴリを削除する

組織で使用されなくなった オペレーショナルテクノロジー インシデントカテゴリまたはサブカテゴリを削除します。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

手順

1. 移動先 **すべて > システム定義 > 選択肢リスト**.
2. 条件フィルターを [テーブル] [次の値に等しい] **[sn_ot_incident]** および [要素] [次の値に等しい] [カテゴリ] または [要素] [次の値に等しい] [サブカテゴリ] に設定します。
3. 削除するカテゴリまたはサブカテゴリレコードをポイントし、チェックボックスをオンにします。
4. [選択した行のアクション] メニューで、[削除] を選択します。

タスクの結果

削除されたカテゴリまたはサブカテゴリは、オペレーショナルテクノロジー インシデントレコードで使用できなくなります。

インシデント状況モデルの作成

サイトの オペレーショナルテクノロジー (OT) インシデント状況モデルを作成します。インシデント状況モデルを使用すると、関連するインシデントのライフサイクルを管理できます。

始める前に

- **Operational Technology Incident Management** (オペレーショナルテクノロジーインシデント管理) にアプリケーションスコープを設定します。
- 必要なロール：admin

このタスクについて

状況管理を使用することで、OT インシデントサイトとそのインシデントライフサイクルの状況モデルを設定できます。サイトごとに 1 つのモデルを作成できます。

状態管理と状態モデルの詳細については、「[状態管理](#)」を参照してください。

インシデントのライフサイクルの詳細については、「[オペレーショナルテクノロジーインシデント管理](#)」を参照してください。

手順

1. 移動先 **すべて > 状況管理 > ステータスモデル**.
2. **[OT Incident: Default Flow (OT インシデント:デフォルトフロー)]** モデルを選択します。
3. 条件を設定します。
4. 必要に応じて、State Transitions (状況移行) コンテキストメニューで、状況遷移レコードを構成します。

たとえば、[処理中] ステータス レコードの [入力条件] フィールドを編集する場合は、ステータス レコードを選択し、変更を追加して [更新] を選択します。

5. [更新] を選択します。

タスクの結果

現在、状況モデルは、インシデントレコードのライフサイクルを通じて予想されるレコードワークフローを正確に記述しています。

インシデントの優先度ルックアップルールの定義

オペレーショナルテクノロジーインシデントの影響度と緊急度を定義して、その優先度を計算します。その後、優先度計算を使用して作業に優先順位を付け、組織内でサービスレベルアグリーメント (SLA) を推進することができます。

始める前に

必要なロール:ot_incident_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > オペレーショナルテクノロジーインシデント管理 > 優先度ルックアップルール**.
2. [新規] を選択します。
3. フォームのフィールドに入力します。

優先度ルックアップルールフォーム

フィールド	説明
影響度	ビジネスプロセスに対するインシデントの影響度の測定。
緊急度	インシデントがビジネスに重大な影響を与えるまでに解決を遅らせることができる時間を測定します。
優先度	影響度と緊急度に基づくオプション。優先度によって、OT エンジニアがタスクにどれだけ迅速に対処すべきかが特定されます。
アプリケーション	ルールのスコープ。スコープは、すべてのアプリケーションとスコープ対象アプリケーションのどちらでルールを使用できるかを定義します。
アクティブ	ルールがアクティブかどうかを定義するオプション。
順番	ルールが [優先度] ルックアップリストに表示される順番。このフィールドは、最初に行われるルールを示します。

i 注:

優先度は、次の表のサンプルデータルックアップルールに従って計算されます。

優先度のデータルックアップルール

影響 ^{***} にそれぞれ変更します。	緊急度	優先度
1 - 高	1 - 高	1 - 重大
1 - 高	2 - 中	2 - 高
1 - 高	3 - 低	3 - 中
2 - 中	1 - 高	2 - 高
2 - 中	2 - 中	3 - 中
2 - 中	3 - 低	4 - 低
3 - 低	1 - 高	3 - 中
3 - 低	2 - 中	4 - 低
3 - 低	3 - 低	5 - 計画中

デフォルトでは、[優先度] フィールドは読み取り専用で、[影響度] と [緊急度] の値を選択して設定する必要があります。優先度の計算方法を変更するには、優先度ルックアップルールを変更するか、**[Priority is managed by Data Lookup - set as read-only]** (優先度はデータルックアップで管理される - 読み取り専用として設定) UI ポリシーを無効にして独自のビジネスロジックを作成します。

4. [送信] を選択します。

システムプロパティの設定

必要に応じてインシデントプロパティを有効にできるように、オペレーショナルテクノロジーインシデント管理 アプリケーションのシステムプロパティを設定します。

始める前に

- ナビゲーションバーで地球儀アイコン (🌐) を選択して、アプリケーションスコープを **Operational Technology Incident Management** に設定します。
- 必要なロール:sn_ot_incident_admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > オペレーショナルテクノロジーインシデント管理 > システムプロパティ**.
2. 組織の必要に応じて、次のプロパティを有効にします。
3. [保存] を選択して変更を保存します。

アサインルールの作成

アサインルールの 1 つ以上の条件に従って、オペレーショナルテクノロジー (OT) インシデントをグループまたはユーザーに自動的にアサインするアサインルールを作成します。OT インシデントをオープンした時点で実行されるアサインルールを使用します。

始める前に
必要なロール：admin

手順

1. 移動先 **すべて** > システムポリシー > ルール > アサイン。
2. [新規] を選択します。
3. フォームのフィールドに入力します。
フィールド値の説明については、「[\[アサインルール\] フォーム](#)」を参照してください。
4. [送信] を選択します。

次のタスク

アサインルールについては、「[Defining assignment rules](#)」を参照してください。

オペレーショナルテクノロジーインシデント管理の使用

オペレーショナルテクノロジーインシデント管理 アプリケーションに必要なすべてのセットアップタスクを完了すると、OT インシデントの管理を開始できます。

OT インシデントの管理

アサインされたユーザーロールに応じて、産業用 ワークスペース内の OT インシデントを管理できます。

産業用 ワークスペースでは、OT インシデントライターは次の場所から OT インシデントフォームを作成および更新できます。

- OT デバイスフォーム
- 機器モデルエンティティフォーム
- リストモジュール

産業用 ワークスペースでは、OT インシデントビューアーは次の場所で OT インシデントを表示できます。

- OT デバイスレコードの [関連レコード] タブにある [OT インシデント] 関連リスト
- 機器モデルエンティティレコードの **[OT Incidents (OT インシデント)]** タブ
- **OT インシデント** リストモジュールの下には、次のリストが表示されます。
 - 自分にアサイン済み
 - 自分のサイトに所属
 - すべて

OT インシデントアドミニストレーターは、産業用 ワークスペース 内の任意の OT インシデントレコードに移動して削除できます。

インシデントのアクセス制御

オペレーショナルテクノロジー (OT) データと情報技術 (IT) データを分離できるように、OT ユーザーのみが OT インシデントを表示できます。

次の表では、オペレーショナルテクノロジーインシデント管理 ロールを持つユーザーのロールと権限について説明します。

ロール	権限
sn_ot_incident_write	OT インシデントを作成、編集、および読み取ることができます。
sn_ot_incident_read	OT インシデントの読み取りのみ可能です。
sn_ot_incident_admin	任意の機器モデルエンティティのインシデントレコードを作成、表示、編集、削除できます。

アクセス制御ルールについて詳しくは、[アプリケーション管理アプリのアクセス制御ルール](#) を参照してください。

インシデントを報告

オペレーショナルテクノロジー (OT) インシデントレコードを作成して、予想される運用標準からの逸脱を報告します。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース).
2. デバイスレコードまたは機器モデルエンティティレコードを選択します。

i 注:
OT インシデントリストモジュールで OT インシデントを発生させることもできます。

3. [**OT Incidents (OT インシデント)**] タブを選択します。

4. [新規] を選択します。

5. フォームのフィールドに入力します。

デバイスレコードを選択した場合、[サイト] フィールドと [OT デバイス] フィールドは自動的に入力されます。機器モデルエンティティレコードを選択した場合、[サイト] および [機器モデルエンティティ] フィールドは自動的に入力されます。OT インシデントが OT インシデントリストモジュールから生成された場合、これらのフィールドはいずれも自動的に入力されません。

i 注:
組織は、インシデント管理プロセスに準拠するようにインシデントフォームとそのフィールドを構成しました。次の表に、一般的な OT インシデントフォームのフィールドを示します。

オペレーショナルテクノロジー インシデントフォーム

フィールド	説明
簡単な説明	インシデントの簡単な説明
説明	インシデントの詳細な説明
Number (番号)	Operational Technology Incident (OTINC) にプリフィックスされている、システムが生成した一意のインシデント番号。
問い合わせユーザー	問題について OT エンジニアに連絡したユーザー。

フィールド	説明
影響度	インシデントが産業プロセスに及ぼす影響の測定。
緊急度	インシデントがビジネスに重大な影響を及ぼすまでに、解決を遅らせることができる時間の指標。
ステータス	OT インシデントの状況。ステータスは、いくつかの解決の段階を通じてインシデントを移動させ、インシデントを追跡します。
カテゴリ	問題の種類。カテゴリを選択し、該当する場合は次にサブカテゴリを選択します。
サブカテゴリ	選択したカテゴリ内の問題の種類。
Watch list (ウォッチリスト)	コメントが追加されたときにこのインシデントに関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこのインシデントに関する通知を受け取るユーザー。
サイト	問題が発生したサイト。
OT デバイス	サイトで影響を受ける OT デバイス。
機器モデルエンティティ	サイトで影響を受ける機器モデルの機器モデルエンティティ。
Business impact (ビジネスへの影響度)	OT インシデントのビジネスインパクトに関する詳細情報。
アサイン先グループ	インシデントで動作するアサイン先グループ。タイプが OT のあらゆるグループがアサイン先グループになれます。
Assigned to (アサイン先)	このインシデントを担当するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。 [アサイン先グループ] フィールドに含まれ、 sn_ot_incident_write ロールを持つユーザーのみを選択できます。[アサイン先グループ] フィールドが空の場合は、sn_ot_incident_write ロールを持つ任意のサイトユーザーを選択できます。
親インシデント	このインシデントレコードの親インシデントの一意の番号。
追加コメント	必要に応じて追加する、問題に関する詳細情報。追加コメントは、インシデントを表示できるすべてのユーザーに表示されます。
作業メモ	インシデントの解決方法に関する情報、またはインシデントの解決手順 (該当する場合)。

6. [保存] を選択します。

タスクの結果

これで、アサイン先グループとアサイニーは、対処する必要がある OT インシデントがあることを認識しています。

インシデントを実行するタスクの作成

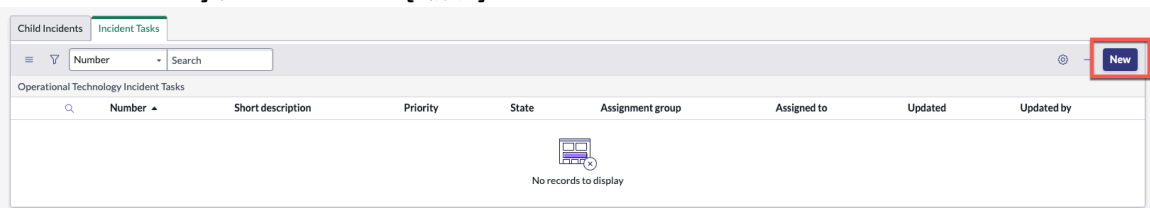
オペレーショナルテクノロジー (OT) インシデントを実行する一連のインシデントタスクを作成します。インシデントタスクは、インシデントの解決に必要な作業を分割し分類するのに役立ちます。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 **すべて > インシデント > オープン**。
2. タスクを作成する OT インシデントレコードを開きます。
3. [インシデントタスク] 関連リストで、[新規] を選択しま



す。

[インシデントタスク] 関連リストが表示されない場合は、追加する必要があります。

4. フォームのフィールドに入力しま

す。

インシデントタスクフォーム

フィールド	説明
番号	一意のシステム生成インシデントタスク番号。
インシデント	タスクが関連付けられているインシデント。
サイト	影響を受けるインシデントサイト。

フィールド	説明
	i 注: このフィールドは読み取り専用で、該当する場合は関連するインシデントサイトが自動的に入力されます。
設備モデルのエンティティ	影響を受ける機器モデルエンティティ。 i 注: このフィールドは読み取り専用で、該当する場合は、関連する機器モデルエンティティが自動的に入力されます。
OT デバイス	影響を受ける OT デバイス。 i 注: このフィールドは読み取り専用で、該当する場合は関連する OT デバイスが自動的に入力されます。
ステータス	インシデントの解決のいくつかの段階を通じてインシデントタスクを追跡するためのステータス。
優先度	インシデントタスクの優先度。
アサイン先グループ	インシデントタスクを担当するグループ。このフィールドを空のままにすると、インシデントは自動的にアサインされます。
Assigned to (アサイン先)	作業するようにインシデントタスクがアサインされているユーザー。 i 注: [アサイン先グループ] が変更された場合、[アサイン先] フィールドはクリアされます。
簡単な説明	インシデントタスクの簡単な説明。
Description (説明)	インシデントタスクの詳細な説明。
メモ	
作業メモリスト	作業メモが追加されたときにこのインシデントタスクに関する通知を受け取るユーザー。 i 注: 自分を追加アイコン [] をクリックして、自分を作業メモリストに追加します。

フィールド	説明
作業メモ	インシデントタスクの解決方法に関する情報、またはインシデントタスクを解決するために必要な手順 (該当する場合)。

5. [送信] を選択します。

タスクの結果

これで、関連する OT インシデントレコードのインシデントタスクを表示および編集できます。

インシデントタスクは、次の場所の 産業用 ワークスペース リストビューで表示できます。

- あなたにアサインされたインシデントタスク: **OT** タスク > 自分にアサイン済み
- グループにアサインされたインシデントタスク: **OT** タスク > 所属グループにアサイン済み
- 未アサインのインシデントタスク: **OT** タスク > 未アサイン

子インシデントを作成する

子 オペレーショナルテクノロジー (OT) インシデントレコードを作成して、報告された逸脱の一部をキャプチャし、個別に作業できるようにします。子インシデントを作成すると、同じ親に関連する複数のインシデントを整理するのに役立ちます。

始める前に

- [子インシデントの作成] 機能 (`com.snc.incident.create.child.enable`) プロパティを有効にします。詳細については、「[システムプロパティの設定](#)」を参照してください。
- 必要なロール: `sn_ot_incident_write`

このタスクについて

子インシデントにコピーされるフィールドは、`com.snc.sn_ot_incident.copy.attributes` システムプロパティを使用して設定されます。

手順

1. 産業用 ワークスペースの **OT** インシデントリストモジュールに移動します。
または、OT デバイスレコードまたは機器モデルエンティティレコードに移動して、[**OT** インシデント] タブを選択することもできます。
2. 子インシデントを作成する OT インシデントを開きます。
3. [子インシデント] 関連リストを選択します。
4. [新規] を選択します。
5. 子インシデントの詳細を入力します。
6. [保存] を選択します。

タスクの結果

これで、親インシデントレコードの子インシデントを表示および編集できます。

サイト全体のインシデントの可視化

オペレーショナルテクノロジー (OT) インシデント履行者ロール (`sn_ot_incident_write`) を使用すると、サイトに属するインシデントを表示、作成、または編集できます。また、他のサイトに属するインシデントを表示して、自分のサイトで同様のインシデントを解決することもできます。

概要

OT インシデント履行者ロール (sn_ot_incident_write) を持つユーザーは、次のタスクを実行できます。

- 自分にアサインされた OT インシデントレコードまたはサイトに属するインシデントを表示および編集します。
- OT インシデントを作成します。
- 他のサイトに属する OT インシデントを表示します。

OT インシデント履行者ロールのメリット

OT インシデント履行者であることの主な利点は、サイト全体のインシデントを読み取り専用で可視化できることです。サイト全体の他のインシデントを表示すると、サイトで同様のインシデントを解決するのに役立ちます。

注:

他のサイトの OT インシデントを編集することはできません。編集できるのは、自分のサイトに属するインシデントのみです。

インシデントを表示または編集する場所

産業用 ワークスペース のリストモジュールでは、次の OT インシデントリストを利用できます。

- 自分にアサイン済み:アサインされたインシデントレコードを表示および編集するには、次の場所に移動します。 **OT インシデント** > 自分にアサイン済み。
- 自分のサイトに所属:自分のサイトに属するインシデントレコードを表示および編集するには、次の場所に移動します。 **OT インシデント** > 自分のサイトに所属。
- さまざまなサイトの既存のインシデントレコードを表示するには、 **OT インシデント** > すべて。

インシデントとインシデントタスク間の同期

オペレーショナルテクノロジー (OT) インシデントタスクを使用して、他のステークホルダーと共同作業したり、他のステークホルダーからの作業を要求したりできます。OT インシデントとそのタスクは同期されるため、インシデントタスクのステータスはインシデントのステータスに応じて変化します。

`com.snc.incident.ot_incident_task.closure`プロパティは、関連するインシデントがクローズまたはキャンセルされたときに、オープン of インシデントタスクをクローズします。このプロパティは、OT インシデントのステータスに基づいて OT インシデントタスクで実行されるさまざまなアクションを担当します。

OT インシデントとそのオープン中の OT インシデントタスク間の同期は、以下のとおりです。

- OT インシデントがクローズされると、オープンされている OT インシデントタスクのステータスが [未完了でクローズ] に設定されます。
- OT インシデントがキャンセルされると、オープン中の OT インシデントタスクのステータスが [スキップしてクローズ] に設定されます。

インシデントメール通知

オペレーショナルテクノロジー (OT) インシデントのメール通知を使用して、インシデントが変更されたときにユーザーにアラートを送信します。

通知の一覧を次の表に示します。

OT インシデントメール通知

通知の名称	[When to send]	[Who receives it]	内容
コメントされたインシデント	余分のコメントが追加された場合	アサイン先、ウォッチリスト	件名: <インシデント #> - コメントが追加されました 本文:追加されたコメント インシデントへの URL
オープン済みで未アサインのインシデント	[Assigned to (アサイン先)] フィールドが空に変わり、[Active (アクティブ)] が true の場合	インシデントをオープンしたユーザー	件名:<インシデント #> - アサイン解除済み 本文:このインシデントで作業する人を特定してください インシデントへの URL
クローズ済みインシデント	インシデントがクローズされている場合	アサイン先グループ	件名: <インシデント #> - クローズ済み 本文:解決コードと解決メモ
変更されたインシデントの優先度	トリガーされた場合	アサイン先、アサイン先グループ、ウォッチリスト	件名:<インシデント #> - 優先度が変更されました 本文: 新しい優先度: <priority>
解決済みインシデント	インシデントの状態が解決済みに変わったとき	発信者、ウォッチリスト	件名:<インシデント #> - 解決済み 本文:解決コードと解決メモ
自分のグループに割り当てられたインシデント	[Assignment Group] フィールドが変更されたとき	アサイン先グループ、ウォッチリスト	件名: <インシデント #> - アサイン先グループ<アサインされました> 本文:優先度、簡単な説明、説明 インシデントへの URL

OT インシデントメール通知 (続く)

通知の名称	[When to send]	[Who receives it]	内容
自分にアサインされたインシデント	[Assigned to (アサイン先)] フィールドが変更されたとき	アサイン先、ウォッチリスト	件名:<インシデント #> があなたにアサインされました 本文:優先度、簡単な説明、説明 インシデントへの URL
自分のためにオープンされたインシデント	新規インシデントが作成させる場合	問い合わせユーザー	件名:<インシデント #> - 要求に応じてオープンされました 本文:優先度、簡単な説明、説明 インシデントへの URL
変更されたインシデントの状況	インシデントの状況が変わったとき	アサイン先、ウォッチリスト	件名:<インシデント #> - ステータスが変更されました 本文:簡単な説明、古いステータス、新しいステータス インシデントへの URL

OT インシデントレコードからのメールの作成

OT インシデントレコードで直接メールを作成して、インシデントについてチームや他のメンバーに最新情報を簡単に更新できるようにします。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. 産業用 ワークスペースリストビューを開きます。
3. OT インシデントリストモジュールで、利用可能なリストのいずれかを選択します。
4. メールを送信するインシデントレコードを選択します。
5. インシデントヘッダーで、[その他のアクション] ... を選択してメニューを開きます。 ボタンをクリックします。
6. [メールの作成] を選択します。
7. メールテンプレートのフォームに入力します。

[メールテンプレート] フォーム

フィールド	説明
ターゲット	メールの送信先のユーザー。 このフィールドは、OT インシデントレコードの [アサイン先] フィールドにユーザーを自動的に入力します。
[件名]	メールの件名。 このフィールドには、OT インシデントレコードの番号とその簡単な説明が自動的に入力されます。
本文	OT インシデントに関連するユーザーに送信する更新。

8. オプション: メールが応答の場合は、[応答テンプレート] フィールドで応答テンプレートを使用してメール本文を入力できます。
9. オプション: メールを下書きとして保存するには、[下書きとして保存] を選択します。
10. [メール送信] を選択します。

タスクの結果

メールは、メールテンプレートで指定したユーザーに送信されます。

インシデントを解決してクローズする

問題が修正されたら、オペレーショナルテクノロジー (OT) インシデントステータスを [解決済み] に設定できます。解決策に問題がなければ、インシデントをクローズできます。インシデントは、インシデントの自動クローズプロパティに基づいて、一定時間後に自動的にクローズされます。

始める前に

必要なロール:sn_ot_incident_write

手順

1. 移動先 **すべて** > **インシデント** > **オープン**。
2. 解決してクローズする OT インシデントを開きます。
3. [解決情報] 関連リストで、次のフィールドに入力します。

のフィールド

フィールド	説明
解決コード	解決済みケースを分類するための情報。
Resolution notes (解決メモ)	インシデントがどのように解決されたかを説明します。

4. [更新] をクリックします。

インシデントレコード内の関連するデバイスと機器モデルエンティティを編集する

関連する オペレーショナルテクノロジー (OT) デバイスと機器モデルエンティティを OT インシデントレコードに直接追加または削除します。インシデントと、その影響を受けるアイテムとの関係を追跡できます。

始める前に

必要なロール:sn_ot_incident_write または sn_ot_incident_admin

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. 産業用 ワークスペースリストビューを開きます。
3. OT インシデントリストモジュールで、利用可能なリストのいずれかを選択します。
4. 編集するインシデントレコードを選択します。
5. 関連する OT デバイスを追加または削除します。
これで、OT デバイスが [影響を受ける OT デバイス] 関連リストの変更レコードに追加されるか、変更レコードから削除されます。
6. [Impacted Equipment Model Entities (影響を受ける機器モデルエンティティ)] 関連リストで手順 4 と 5 を繰り返して、インシデントレコードに機器モデルエンティティを追加または削除します。

オペレーショナルテクノロジーインシデント管理 参照

参照トピックには、オペレーショナルテクノロジーインシデント管理 アプリケーションに関する追加情報が記載されています。

[アサインルール] フォーム

アサインルールは、アサインルールの 1 つ以上の条件に従って、オペレーショナルテクノロジー (OT) インシデントをグループまたはユーザーに自動的にアサインします。

次の表で、[アサインルール] フォームのフィールド値について説明します。

[アサインルール] フォーム

フィールド	説明
名前	アサインルールの説明的な名前です。
アクティブ	アサインルールをアクティブ化するオプション。
適用先	
テーブル	アサインルールを適用するレコードを格納したテーブルです。 注: OT インシデントに固有のアサインルールの場合は、[テーブル] フィールドを [オペレーショナルテクノロジーインシデント [sn_ot_incident]] に設定します。 このリストには、アサインルールと同じスコープ内にあるテーブルとデータベースビューのみが表示されます。タスクテーブルを拡張するカスタムテーブルを選択し、アサインルー

[アサインルール] フォーム (続く)

フィールド	説明
	ルが正しく機能するようにする場合は、<a href="https://<instance_name>.service-now.com/cache.do">https://<instance_name>.service-now.com/cache.do に移動してインスタンスキャッシュをクリアする必要があります。 i 重要: システムキャッシュをクリアすると、全体的なパフォーマンスに影響し、システムの応答時間が低下する可能性があります。キャッシュのフラッシュは営業時間中には実行せず、自動的に実行されるようにトリガーしないようにします。
条件	アサインルールが適用される条件。
アサイン先	
ユーザー	イベントがアサインされているユーザー。
グループ	イベントがアサインされているグループ。
スクリプト	
スクリプト	高度なアサインルール機能を指定するスクリプト。current.variable_pool 変数セットを使用できます。 i 注: スクリプトの入力が正しいことと、入力タイプがアサインルールスクリプトのフィールドタイプと一致していることを確認します。たとえば、アサインルールスクリプトが整数フィールドの値を設定し、スクリプトの値が文字列に設定されている場合、アサインルールによって予期しない結果が生じる可能性があります。
オプションのフィールド	
一致条件	任意 いずれかの条件が満たされると、アサインルールが適用されます。 すべて すべての条件が満たされると、アサインルールが適用されます。
実行順序	アサインルールが処理される順序。アサインルールが競合する場合、順番の値が小さいルールが大きい値のルールよりも優先されます。順序値が同じ番号に設定されている場合、最初に一致した条件を持つアサインルールが、最初に一致する条件がない他のアサインルールよりも優先されます。一致条件を備えた最初のアサインルールのみがレコードに対して実行されます。

オペレーショナルテクノロジーインシデント管理とともにインストールされるコンポーネント

オペレーショナルテクノロジーインシデント管理 (sn_ot_inc_mgmt) プラグインを有効にすると、ユーザーロールを含むいくつかのタイプのコンポーネントをインストールできます。

i 注:

アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストールされるロール

ロール	説明	含まれるロール
OT インシデントアドミン [sn_ot_incident_admin]	任意の機器モデルエンティティの OT インシデントレコードを作成、表示、削除、編集できます。優先度ルックアップルールと OT インシデントシステムプロパティを設定できます。	• cmdb_ot_isa_viewer_all • sn_ot_incident_write
OT インシデントリーダー [sn_ot_incident_read]	OT インシデントレコードの表示のみ可能です。	• cmdb_ot_viewer • cmdb_ot_isa_viewer
OT インシデント履行者 [sn_ot_incident_write]	OT インシデントレコードを表示、作成、編集できます。	sn_ot_incident_read

i 注:

OT インシデントユーザー [ot_incident_user] ロールは複製される。このロールを割り当てられたユーザーに対して、スケジュール済みジョブを実行して新しい オペレーショナルテクノロジーインシデント管理 ロールを割り当てることができます。詳細については、「[ユーザーへの新しいロールのアサイン](#)」を参照してください。

インストールされるテーブル

テーブル	説明
OT インシデント [sn_ot_incident]	サイト全体で報告された OT インシデントのリスト。
OT インシデントタスク [sn_ot_incident_task]	さまざまな OT インシデントで作成された OT インシデントタスクのリスト。
OT インシデント優先度ルールのルックアップ [dl_ot_inc_priority]	OT インシデントの優先度を計算するためのルールのリスト。

関連情報

OT 拡張クラスと関連アプリケーションに関する詳細情報を確認してください。

概要

拡張クラスは、オペレーショナルテクノロジー管理構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

[Operational Technology \(OT\) extension classes](#)

構成管理データベース (CMDB)は OT のクラスを更新します。

関連アプリケーション

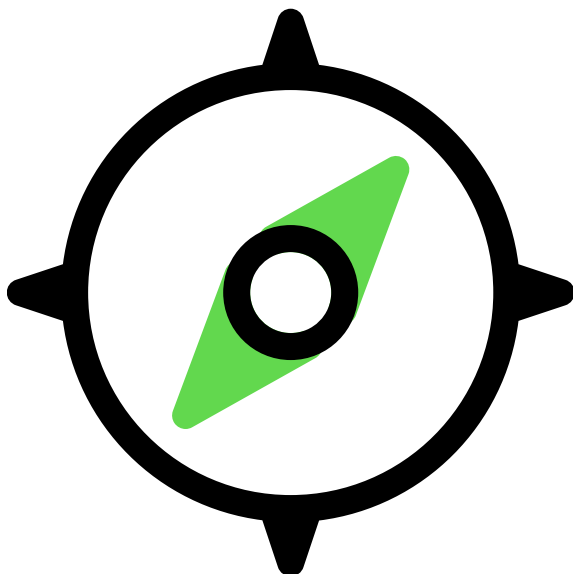
[IT Service Management](#)

ServiceNow IT Service Management アプリケーションを オペレーショナルテクノロジーインシデント管理 と統合すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジー変更管理

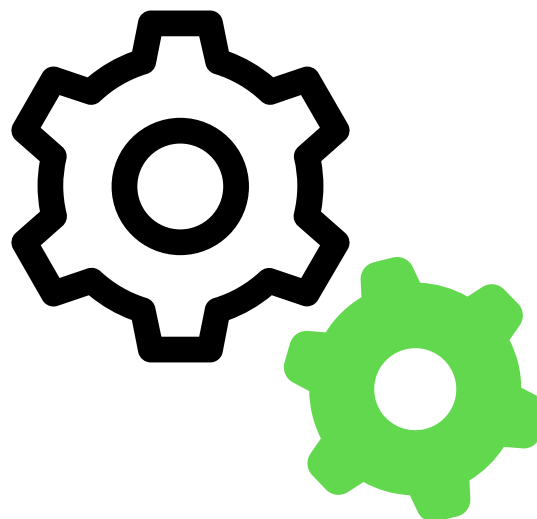
ServiceNow[®] オペレーショナルテクノロジー変更管理 アプリケーションを使用すると、組織はオペレーショナルテクノロジー (OT) デバイスと本番プロセスに変更を実装できます。

探索



オペレーショナルテクノロジー変更管理 の探索

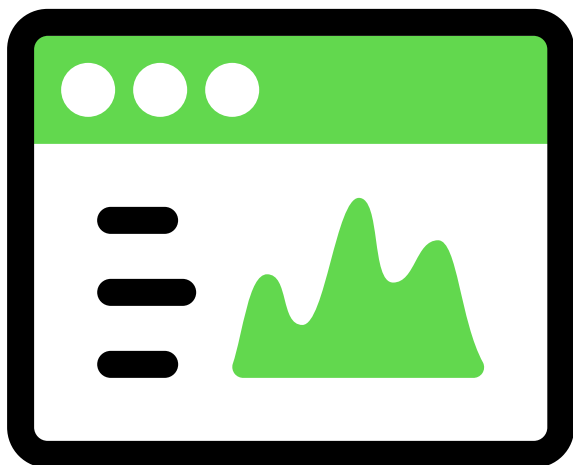
Configure (構成)



実装の計画と構成

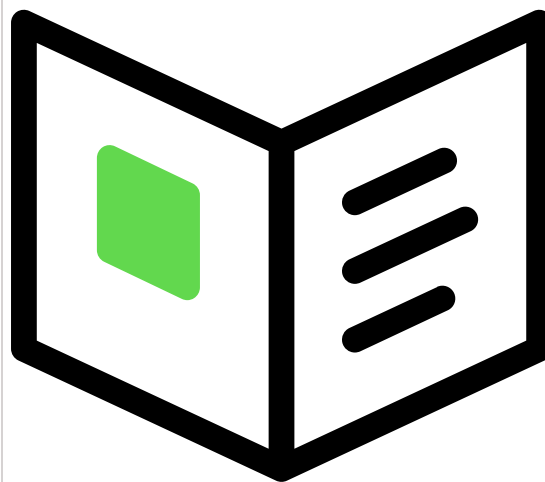
自動翻訳

使用



オペレーショナルテクノロジー変更管理 の使用

参照



関連情報とアプリケーションの詳細を取得

オペレーショナルテクノロジー変更管理 の探索

オペレーショナルテクノロジー変更管理 アプリケーションの詳細を表示します。

主な機能

オペレーショナルテクノロジー変更管理 アプリケーションでは、次の主要な機能を使用できます。

- すべてのステークホルダーを結び付ける、デジタル化変更ワークフロー。
- さまざまな変更管理プロセス (ワークフロー) を持つサイト。
- IT Change Management と オペレーショナルテクノロジー変更管理 は分離されていますが、必要に応じて組み合わせることができます。
- オペレーショナルテクノロジーインシデント管理 および オペレーショナルテクノロジー脆弱性対応 アプリケーションと統合されたオペレーショナルテクノロジー変更管理ワークフロー。
- ダウンタイムスケジュールに合わせて調整された、設備モデルエンティティの工場フロアの変更。

オペレーショナルテクノロジー変更管理を使用した生産プロセスの最適化

オペレーショナルテクノロジー変更管理 アプリケーションを使用すると、チームメンバーはオペレーショナルテクノロジー (OT) デバイスや産業機器の構成に対する変更に取り組むことができます。たとえば、最適化、生産プロセスの改変、脆弱性の修正などです。

概要

オペレーショナルテクノロジー変更管理 アプリケーションを使用すると、OT 変更要求を情報技術 (IT) 変更要求とは別に管理できます。ネットワークタイプ別に OT 変更要求と IT 変更要求を分離し、サイトごとに OT 変更要求を管理できます。

次の例は、組織に オペレーショナルテクノロジー変更管理 を適用する方法を示しています。

- OT デバイスの脆弱性の修正を担当する OT 修復オーナーが、一連の脆弱性を修正するための変更を開始する。
- OT 構成とプラントエンジニアリング活動を担当する OT 技術者が、故障したロボットアームを産業現場で修理するための変更を実行したいと考えています。
- 生産活動全体を担当する工場長が、エンジニアリングチームから要求された変更をレビューして承認したいと考えています。

OT 変更要求

OT 変更要求は、OT ネットワーク上の OT デバイスからのサービスが中断されたときに発生します。場合によっては、変更要求の作成時に OT デバイスが不明になることがあります。産業用ワークスペース から OT 変更要求を作成すると、その変更要求には **OT** のネットワークタイプが自動的にアサインされます。この属性は、OT 変更要求を IT 変更要求と区別するために使用されます。このフィールドはデフォルトでは表示されません。OT デバイスの詳細については、「[OT デバイスの関連アイテムと関連リスト](#)」を参照してください。

OT 変更要求の作成方法の詳細については、「[変更要求の作成](#)」を参照してください。

IT と OT の変更の分離

オペレーショナルテクノロジー変更管理 アプリケーションがインスタンスにインストールされたら、[ネットワークタイプ] を **[IT]**、**[OT]**、または [なし] から選択できます。新しい変更要求には、デフォルトで [ネットワークタイプ] の [なし] が割り当てられます。

オペレーショナルテクノロジー変更管理 モデルステータス移行

基本的な OT 変更モデルと高度な OT 変更モデルの両方について、オペレーショナルテクノロジー変更管理 モデル状況の移行を次の表に示します。OT 変更モデルの詳細については、「[変更要求を実行するための変更モデルを選択します](#)」を参照してください。

基本的な OT 変更モデルの状況

状況	説明
New (新規)	OT 変更要求が開始されます。
プラン	OT 変更要求は、次の基準で分析されます。 • Justification (理由) • 実装計画 • リスクと影響度の分析 • 取り消し計画 • テスト計画 • 変更のスケジュール設定
実装	ターゲットの OT デバイスで変更が実行されます。
クローズ済み	変更完了後、変更レコードがクローズされます。
キャンセル	変更レコードがキャンセルされ、変更は OT デバイスに適用されません。

高度な OT 変更モデルの状況

状況	説明
New (新規)	OT 変更要求が開始されます。
プラン	OT 変更要求は、次の基準で分析されます。 • Justification (理由) • 実装計画 • リスクと影響度の分析 • 取り消し計画 • テスト計画 • 変更のスケジュール設定
承認	レビュー担当者が OT 変更要求を承認または拒否します。
実装	ターゲットの OT デバイスで変更が実行されます。
実装後のレビュー	必要に応じて追加の OT 変更タスクを追加し、次のチェックを実行します。 • 電氣的チェック • ネットワークチェック • 品質チェック • 安全性チェック
クローズ	変更完了後、変更レコードがクローズされます。
キャンセル	変更レコードがキャンセルされ、変更は OT デバイスに適用されません。

オペレーショナルテクノロジー変更管理の構成

ServiceNow オペレーショナルテクノロジー (OT) ソリューションのデータ基盤を作成できるように、オペレーショナルテクノロジー変更管理 アプリケーションを構成します。

admin ロールを持っている場合は、ガイド付きセットアップを使用して オペレーショナルテクノロジー変更管理 アプリケーションのセットアップを指示できます。ガイド付きセットアップは、アプリケーションの構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

i 注:

オペレーショナルテクノロジー変更管理 は、Utah P4 以降のリリースに依存します。

ガイド付きセットアップにアクセスするには、産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表では、オペレーショナルテクノロジー変更管理 アプリケーションのガイド付きセットアップタスクとその目的について説明します。

タスク	目的
1. ServiceNow Storeからオペレーショナルテクノロジー変更管理アプリケーションをインストールします。	オペレーショナルテクノロジー変更管理 アプリケーションとサポートプラグインをインストールします。
2. オペレーショナルテクノロジー変更管理 ロールを割り当てます。	ロールを割り当てて、各ユーザーが使用できるアクションを制御します。
3. オペレーショナルテクノロジー変更管理 カテゴリを設定します。	組織に必要な OT 変更のカテゴリを構成します。
4. オペレーショナルテクノロジー変更管理 モデルを選択します。	組織の変更モデルを選択します。

オペレーショナルテクノロジー変更管理のインストール

admin ロールを持っている場合は、オペレーショナルテクノロジー変更管理 アプリケーション (sn_ot_chg_mgmt) をインストールできます。

始める前に

- アプリケーションとその関連するすべての ServiceNow Store アプリケーションに有効な ServiceNow エンタイトルメントがあることを確認してください。詳細については、「[ServiceNow 製品またはアプリケーションのエンタイトルメントの取得](#)」を参照してください。
- オペレーショナルテクノロジー変更管理 アプリケーションには次のプラグインが必要です。オペレーショナルテクノロジー変更管理 アプリケーションをインストールする前に、これらのプラグインがアクティブ化されていることを確認してください。

必須の ServiceNow プラグイン

CMDB CI クラスモデル (sn_cmdb_ci_class)

構成管理データベース (CMDB) CI クラスモデルストアアプリは、クラスの説明、識別ルール、識別子エントリ、依存関係など、CMDB クラス階層を拡張するクラスモデルを追加します。詳細については、「[CMDB CI クラスモデルストアアプリ](#)」を参照してください。

ISA Equipment Model (ISA 設備階層モデル) (sn_isa_model)

ISA-95 機器モデルエンティティおよびテンプレートのデータモデル詳細については、「[ISA-95 機器モデル](#)」を参照してください。

- オペレーショナルテクノロジー変更管理 アプリケーションには、次のServiceNow Storeアプリケーションのいずれかまたは両方が必要です。オペレーショナルテクノロジー変更管理 アプリケーションをインストールする前に、これらのアプリケーションのうち少なくとも 1 つがインストールされていることを確認してください。

必要な ServiceNow Store アプリケーション

オペレーショナルテクノロジーマネージャー

オペレーショナルテクノロジーマネージャー アプリケーションは、組織が オペレーショナルテクノロジー ソリューションを使用できるようにする基盤データと関係を作成します。オペレーショナルテクノロジーマネージャー アプリケーションは、Now Platform での 構成管理データベース (CMDB)、サービスグラフ コネクタ、および ディスカバリー アプリケーションの使用をサポートしています。詳細については、「

[オペレーショナルテクノロジーマネージャーの構成](#)を参照してください。

産業用プロセスマネージャー

産業用プロセスマネージャー アプリケーションは、ServiceNow[®] 産業用ソリューションに必要な ISA-95 機器モデルデータ基盤を作成し、各産業現場で独自のバージョンの機器モデルを作成できるようにします。詳細については、「[産業用プロセスマネージャー の構成](#)」を参照してください。

必要なロール：admin

このタスクについて

次のアイテムは、オペレーショナルテクノロジー変更管理 アプリケーションとともにインストールされます。

- プラグイン
- ストアアプリケーション
- ロールと ACL

インストールされるロールと ACL の詳細については、「[オペレーショナルテクノロジー変更管理とともにインストールされるコンポーネント](#)」を参照してください。

i 注:

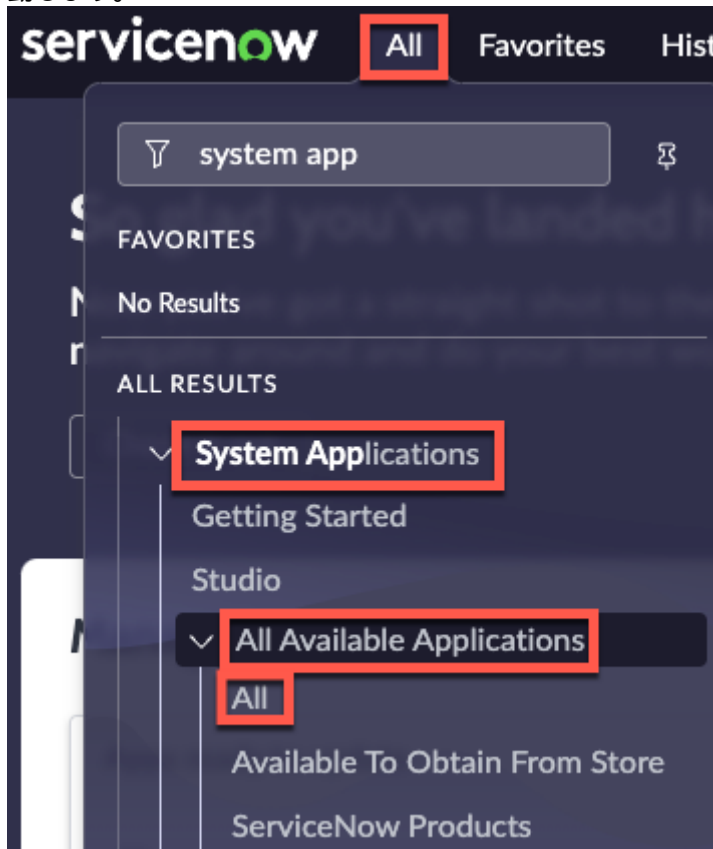
オペレーショナルテクノロジー ヴィジビリティのライセンスを持たないOperational Technology Service Managementユーザーの場合は、次の点に注意してください。

- 最新バージョンの オペレーショナルテクノロジーインシデント管理 がインストールされている場合は、産業用プロセスマネージャー もインストールされます。
- 最新バージョンの オペレーショナルテクノロジー変更管理 がインストールされている場合は、産業用プロセスマネージャー もインストールされます。

Operational Technology Service Managementエクスペリエンスにアクセスできるように、最新バージョンにアップグレードする必要があります。

手順

1. [すべて] > [システムアプリケーション] > [利用可能なすべてのアプリケーション] > [すべて]に移動します。



2. フィルター基準と検索バーを使用して、オペレーショナルテクノロジー変更管理 アプリケーションを検索します。

名前または ID でアプリケーションを検索できます。アプリケーションが見つからない場合は、ServiceNow Store に要求する必要がある場合があります。

[ServiceNow Store](#) Web サイトにアクセスして利用可能なすべてのアプリを表示し、ストアにリクエストを送信する方法について確認してください。リリースされたすべてのアプリのリリースノート情報については、「[ServiceNow Storeバージョン履歴のリリースノート](#)」を参照してください。

3. アプリケーションのインストールダイアログボックスで、アプリケーションの依存関係を確認します。

リストに表示されるのは、インストール予定である依存プラグインおよびアプリケーション、現在インストールされている依存プラグインおよびアプリケーション、またはインストールする必要がある依存プラグインおよびアプリケーションです。インストールする必要があるプラグインまたはアプリケーションがある場合は、オペレーショナルテクノロジー変更管理 アプリケーションをインストールする前にインストールする必要があります。

4. [インストール] を選択します。

オペレーショナルテクノロジー変更管理 ロールの割り当て

ユーザーにロールをアサインして、オペレーショナルテクノロジー変更管理 アプリケーションの機能やデータへのアクセスを制御できるようにします。

始める前に
必要なロール：admin

このタスクについて
次のテーブルにリストされているロールを持つユーザーは、アプリケーションを使用できます。

ロール	Description (説明)
変更マネージャー [sn_ot_change_manager]	OT 変更モデルレコードを管理できます。
変更管理者 [sn_ot_change_admin]	OT 変更レコードを作成、表示、削除、編集できます。カテゴリとシステムプロパティを設定できます。
変更書き込みユーザー [sn_ot_change_write]	OT 変更レコードを作成、表示、編集できます。 IT 変更タスクをアサインすることもでき、アサインされている IT 変更タスクを編集してクローズすることもできます。 詳細については、「 サイト全体の変更要求の管理 」を参照してください。
変更読み取りユーザー [sn_ot_change_read]	OT 変更レコードの表示のみ可能です。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

変更要求を実行するための変更モデルを選択します

組織のニーズに応じて、オペレーショナルテクノロジー (OT) 変更モデルを選択し、変更要求の実行を開始します。

始める前に
必要なロール:sn_ot_change_admin または admin

このタスクについて
次の 2 つの OT 変更モデルを使用できます。

- 基本的な OT 変更
- 高度な OT 変更

基本的な OT 変更モデルでは、承認なしの変更プロセスが使用されます。

OT 変更の基本モデルの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。

高度な OT 変更モデルでは、承認付きの変更プロセスが使用されます。変更承認ポリシーを作成し、変更要求をレビューする承認グループをアサインすることができます。変更承認の詳細については、「[オペレーショナルテクノロジー 変更承認](#)」を参照してください。

高度な OT 変更モデルの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

手順

1. 移動先 産業用ワークスペースアドミン > ガイド付きセットアップ。
2. Operational Technology Change Management (オペレーショナルテクノロジー変更管理) カテゴリで、**[Get Started (開始)]** を選択します。
3. [変更モデル] セクションの横にある [構成] を選択します。
4. 組織のニーズに合った変更モデルを選択します。
5. 必要に応じてレコードを編集します。

タスクの結果

変更モデルがシステムに適用され、OT 変更要求の作成を開始できます。

基本的な OT 変更モデルプレイブック

承認のない OT 変更が完了するまでに通過する必要がある基本的なオペレーショナルテクノロジー (OT) 変更モデルプレイブックのステージについて説明します。

開始

OT 変更要求の開始ステージでは、要求された変更の詳細をキャプチャし、必要に応じて変更をアサインできます。このステージには 3 つのタスクがあります。

変更の説明

Field (フィールド)	説明
簡単な説明	変更の簡単な説明
Description (説明)	変更の詳細。
カテゴリ	変更のタイプです。
サイト	変更が行われるサイト。
ウォッチリスト	コメントが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこの変更に関する通知を受け取るユーザー。

リスクをキャプチャ

Field (フィールド)	説明
優先度	変更にとどの程度迅速に対処すべきかを特定するための影響度と緊急度。
リスク	変更がもたらすリスクの量。
影響度	変更が産業プロセスに及ぼす影響の測定値。

変更をアサイン

Field (フィールド)	説明
要求者	変更を要求するユーザー。

変更をアサイン (続く)

Field (フィールド)	説明
アサイン先グループ	変更に対応するアサイン先グループ。タイプが OT のあらゆるグループがアサイン先グループになれます。
Assigned to (アサイン先)	この変更で作業するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。

プラン

OT 変更要求の計画ステージでは、変更の理由、実装計画、リスクと影響の計画、バックアウト計画、テスト計画、および変更をスケジュールする時間を追加できます。このステージには 6 つのタスクがあります。

理由を追加

Field (フィールド)	Description (説明)
Justification (理由)	変更を実施する必要がある理由。

実施計画を追加

Field (フィールド)	Description (説明)
実装計画	要求された変更の実装方法の詳細。

リスクと影響の分析を追加

Field (フィールド)	Description (説明)
リスクと影響度の分析	この変更に関連するリスクと影響の要因の詳細。

切り戻し計画を追加

Field (フィールド)	Description (説明)
バックアウトプラン	必要に応じて変更を元に戻す方法の詳細。

テスト計画を追加

Field (フィールド)	Description (説明)
テスト計画	実装された変更をテストする方法の詳細。

変更のスケジュール設定

Field (フィールド)	説明
開始予定日時	変更が行われた日付。

変更のスケジュール設定 (続く)

Field (フィールド)	説明
	i 注: [スケジュールアシスタント] ボタンを選択して開始予定日フィールドに自動的に入力することで、カレンダーで利用可能なダウンタイムスロットを選択することもできます。
終了予定日時	変更が終了する日付。 i 注: [スケジュールアシスタント] ボタンを選択して終了予定日フィールドに自動的に入力することで、カレンダーで利用可能なダウンタイムスロットを選択することもできます。

実装

OT 変更要求の実装ステージでは、次のタスクの詳細が提供されます。終了したら、このステージを完了としてマークできます。

変更を実行

ターゲットの OT デバイスで変更が実行され、完了した場合は完了としてマークします。

クローズ

クローズステージでは、変更が完了した後に変更レコードを閉じることができます。

変更レコードを閉じる

Field (フィールド)	Description (説明)
クローズコード	変更レコードがクローズされた理由。
クローズメモ	変更レコードのクローズに関するその他の詳細。

高度な OT 変更モデルプレイブック

高度なオペレーショナルテクノロジー (OT) 変更モデルプレイブック のステージについて説明します。このステージは、承認のある OT 変更が完了するまでに通過する必要があります。

開始

OT 変更要求の開始ステージでは、要求された変更の詳細をキャプチャし、必要に応じて変更をアサインできます。このステージには 3 つのタスクがあります。

変更の説明

Field (フィールド)	説明
簡単な説明	変更の簡単な説明
Description (説明)	変更の詳細。
カテゴリ	変更のタイプです。
サイト	変更が行われるサイト。
ウォッチリスト	コメントが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこの変更に関する通知を受け取るユーザー。

リスクをキャプチャ

Field (フィールド)	説明
優先度	変更にとどの程度迅速に対処すべきかを特定するための影響度と緊急度。
リスク	変更がもたらすリスクの量。
影響度	変更が産業プロセスに及ぼす影響の測定値。

変更をアサイン

Field (フィールド)	説明
要求者	変更を要求するユーザー。
アサイン先グループ	変更に対応するアサイン先グループ。タイプが OT のあらゆるグループがアサイン先グループになれます。
Assigned to (アサイン先)	この変更で作業するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。

プラン

OT 変更要求の計画ステージでは、変更の理由、実装計画、リスクと影響の計画、バックアウト計画、テスト計画、および変更をスケジュールする時間を追加できます。このステージには 6 つのタスクがあります。

理由を追加

Field (フィールド)	Description (説明)
Justification (理由)	変更を実施する必要がある理由。

実施計画を追加

Field (フィールド)	Description (説明)
実装計画	要求された変更の実装方法の詳細。

リスクと影響の分析を追加

Field (フィールド)	Description (説明)
リスクと影響度の分析	この変更に関連するリスクと影響の要因の詳細。

切り戻し計画を追加

Field (フィールド)	Description (説明)
バックアウトプラン	必要に応じて変更を元に戻す方法の詳細。

テスト計画を追加

Field (フィールド)	Description (説明)
テスト計画	実装された変更をテストする方法の詳細。

変更のスケジュール設定

Field (フィールド)	説明
開始予定日時	変更が行われた日付。 i 注: [スケジュールアシスタント] ボタンを選択して開始予定日フィールドに自動的に入力することで、カレンダーで利用可能なダウンタイムスロットを選択することもできます。
終了予定日時	変更が終了する日付。 i 注: [スケジュールアシスタント] ボタンを選択して終了予定日フィールドに自動的に入力することで、カレンダーで利用可能なダウンタイムスロットを選択することもできます。

承認

OT 変更要求の承認ステージでは、レビュー担当者が OT 変更を承認または拒否できます。このステージに含まれるタスクは 1 つだけです。

レビューとアクションの実行

Field (フィールド)	Description (説明)
[承認] ボタン	タスク フォームのテーブルに表示されるレビュー担当者の場合は、[承認] を選択して変更を受け入れます。
[拒否] ボタン	タスク フォームのテーブルに表示されているレビュー担当者の場合は、[拒否] を選択して変更を却下します。
コメント	変更の承認または拒否に関する追加情報。

変更承認の詳細については、「[オペレーショナルテクノロジー 変更承認](#)」を参照してください。

実装

OT 変更要求の実装ステージでは、以下のタスクの詳細が提供されます。終了したら、このステージを完了としてマークできます。

機能を停止

必要に応じて、ターゲットの OT デバイスの機能を停止した後に完了としてマークします。

LOTO を確認

ロックアウト/ターゲット(LOTO)は、メンテナンス中またはサービス中の機械の偶発的または意図しない起動を防ぐための安全手順です。LOTO が完了したら完了としてマークします。

変更を実行

ターゲットの OT デバイスで変更が実行され、完了した場合は完了としてマークします。

実施後のレビュー

OT 変更要求の実装後レビューステージでは、実行されたタスクをチェックし、レビュー中に特定された残作業に対して追加の OT 変更タスクを作成し、LOTO の取り消しプロセスを完了としてマークできます。

チェックを実行

Field (フィールド)	Description (説明)
電気チェックを実行	電気チェックの完了後に選択するチェックボックス。
ネットワークのチェックを実行	ネットワークチェックの完了後に選択するチェックボックス。
品質チェックを実行	品質チェックの完了後に選択するチェックボックス。
安全チェックを実行	安全チェックの完了後に選択するチェックボックス。

スピノフタスクを推奨

Field (フィールド)	Description (説明)
OT 変更タスク	OT 変更に関連する変更タスクのリスト。
ステータス	OT 変更のステータス。ステータスは、いくつかの解決段階を通じて変化し、変更を追跡します。
Assigned to (アサイン先)	この変更で作業するユーザー。アサイン先グループが変更されると、[アサイン先] フィールドはクリアされます。
簡単な説明	変更タスクの簡単な説明。

LOTO の取り消し

変更が実装され、レビューされた後、ロックアウトターゲットが取り消されたときに完了としてマークします。

スピノフタスク

スピノフタスクステージには、実装後レビューで完了する必要があるすべての変更タスクが一覧表示されます。

クローズ

クローズステージでは、変更が完了した後に変更レコードを閉じることができます。

変更レコードを閉じる

Field (フィールド)	Description (説明)
クローズコード	変更レコードがクローズされた理由。
クローズメモ	変更レコードのクローズに関するその他の詳細。

オペレーショナルテクノロジー変更管理 の使用

オペレーショナルテクノロジー変更管理 アプリケーションに必要なすべてのセットアップタスクを完了すると、オペレーショナルテクノロジー (OT) 変更要求の管理を開始できます。

変更要求の作成

サイトの変更を報告する オペレーショナルテクノロジー (OT) 変更要求を作成します。

始める前に

必要なロール:sn_ot_change_write

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. **[OT 変更要求]** リストビューで、開くリストを選択します。
3. **[新規]** を選択します。
4. 組織に適用する OT 変更モデルを選択します。

5. [**Create OT Change Record (OT 変更レコードの作成)**] を選択します。

6. チームが変更要求に取り組んでいる間、必要に応じてプレイブックを完成させます。

基本的な OT 変更モデルプレイブックの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。高度な OT 変更モデルプレイブックの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

i 注:

プレイブックを有効にしていない場合は、OT 変更要求レコードの [詳細] タブと [関連レコード] タブのみを表示できます。

変更要求を実行するための変更タスクの作成

オペレーショナルテクノロジー (OT) 変更要求を実行するための変更タスクを作成します。変更タスクは、変更要求中に実行する必要があるすべてのタスクをキャプチャするのに役立ちます。

始める前に

必要なロール:sn_ot_change_write

このタスクについて

変更タスクは、変更要求を実行して完了するために実行する必要がある個々のステップです。

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. タスクを作成する変更レコードを選択します。
3. [変更タスク] 関連リストで、[新規] を選択します。
[変更タスク] 関連リストが表示されていない場合は、追加する必要があります。
4. フォームのフィールドに入力します。

インシデントタスクフォーム

フィールド	Description (説明)
OT 変更タスク	
簡単な説明	変更タスクの簡単な説明。
Description (説明)	変更タスクの詳細。
OT デバイス	影響を受ける OT デバイス。
OT 変更要求	関連する OT 変更要求のレコード番号。
ステータス	変更実装のいくつかのステージを通じて変更タスクを追跡するためのステータス。
タイプ	変更のタイプです。
アサイン	
アサイン先グループ	変更タスクを担当するグループ。このフィールドを空のままにすると、変更タスクが自動的に割り当てられます。
Assigned to (アサイン先)	作業するように変更タスクがアサインされているユーザー。

フィールド	Description (説明)
OT 変更タスク	
	i 注: [アサイン先グループ] が変更された場合、[アサイン先] フィールドはクリアされます。
メモ	
ウォッチリスト	コメントが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモリスト	作業メモが追加されたときにこの変更に関する通知を受け取るユーザー。
作業メモ (プライベート)	顧客が利用できない作業メモ。

5. [保存] を選択します。

タスクの結果

関連する OT 変更レコードの変更タスクを表示および編集できます。

変更タスクは、次の場所の 産業用 ワークスペース リストビューで表示できます。

- 自分にアサインされたタスクの変更: **OT** タスク > 自分にアサイン済み
- グループにアサインされたタスクの変更: **OT** タスク > 所属グループにアサイン済み
- 未アサインの変更タスク: **OT** タスク > 未アサイン

OT デバイスの詳細から変更要求を作成する

OT デバイスレコードから オペレーショナルテクノロジー (OT) 変更要求を作成します。デバイスレコードから変更要求を作成すると、サイトまたはビジネスサービス、[OT デバイス] フィールドなど、変更要求レコードの情報が自動的に入力されます。

始める前に

必要なロール:sn_ot_change_write

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. [すべての OT デバイス] リストで、OT デバイスレコードを選択します。
3. [関連レコード] タブで、[OT 変更要求] 関連リストを選択します。
4. [新規] を選択します。
5. 組織に適用する OT 変更モデルを選択します。
6. [**Create OT Change Record (OT 変更レコードの作成)**] を選択します。
7. チームが変更要求に取り組んでいる間、必要に応じてプレイブックを完成させます。

基本的な OT 変更モデルプレイブックの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。高度な OT 変更モデルプレイブックの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

設定した条件に応じて、次のフィールドが自動的に入力されます。

- [**OT デバイス**] フィールドは、産業用プロセスマネージャー アプリケーションが有効になっている場合にのみ自動入力されます。
- 産業用プロセスマネージャーがインストールされている場合、OT デバイスにアサインされたサイトが [サイト] フィールドに表示されます。
- 産業用プロセスマネージャーが有効になっていて、OT デバイスに関連付けられているエンティティが 1 つしかない場合は、[**Equipment model entity** (機器モデルエンティティ)] フィールドが自動的に入力されます。



注:

複数のエンティティがデバイスに関連付けられている場合、[**Equipment model entity** (機器モデルエンティティ)] フィールドは空のままになります。

タスクの結果

変更要求が作成され、[アサイン先グループ]、[アサイン先]、および [ウォッチリスト] フィールドのユーザーに通知されます。

修復タスクからの変更要求の作成

OT 修復タスクから オペレーショナルテクノロジー (OT) 変更要求を作成します。修復タスクから変更要求を作成すると、[サイト] フィールドや [OT デバイス] フィールドなど、変更要求レコードの情報が自動的に入力されます。

始める前に

必要なロール:sn_ot_change_write または sn_otvr.remediation_owner

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. 変更要求を作成する修復タスクレコードを開きます。
3. 次の例に示すように、[**OT 変更を作成**] ボタンを選択しま

The screenshot displays the ServiceNow interface for a record titled 'California Vulnerabilities'. The record ID is VUL0010004. The interface includes a sidebar with navigation options, a main content area with details and a table of vulnerable items, and an attachments section.

Record Details:

- State: Open
- Risk rating: 3 - Medium
- Assignment group: OT VR Default Ass...
- Remediation status: In-flight
- % VIs remediated: 0

Buttons: Assign to me, Resolve task, **Create OT Change** (highlighted), Save, ...

Remediation Progress: 0%

Remediation Task Details:

- Number: VUL0010004
- Risk rating: 3 - Medium
- Assigned to: -
- Remediation target: -
- Created: 2023-05-25 07:00:00
- Updated: 2023-05-12 04:00:07
- Short description: California Vulnerabilities
- Description: California (CA)

Vulnerable Items Table:

Vulnerable item	Summary	Configuration item	State	Risk rating
VIT0010002	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka "Microsoft Graphics Components Remote Code Execution Vulnerability." This affects Windows 7, Microsoft Office, Microsoft Office Word Viewer, Office 365 ProPlus, Microsoft Excel Viewer, Microsoft PowerPoint Viewer, Windows Server 2019, Windows Server 2008 R2, Windows 10, Windows Server 2008.	PLC001	Open	3 - Medium

Attachments: No Attachments Available. Browse for a file to add it as an attachment. **Browse**

す。

i 注:

アクティブな変更モデルがない場合は、次のエラーが表示されま

✕ Error creating Change Request: No active change model available. Please contact your OT Change admin ✕

す。

4. 組織に適用する OT 変更モデルを選択します。

5. **[Next (次へ)]** をクリックします。

6. チームが変更要求に取り組んでいる間、必要に応じてプレイブックを完成させます。

基本的な OT 変更モデルプレイブックの詳細については、「[基本的な OT 変更モデルプレイブック](#)」を参照してください。高度な OT 変更モデルプレイブックの詳細については、「[高度な OT 変更モデルプレイブック](#)」を参照してください。

設定した条件に応じて、次のフィールドが自動的に入力されます。

- **[OT デバイス]** フィールドは、産業用プロセスマネージャー アプリケーションが有効になっている場合にのみ自動入力されます。
- 産業用プロセスマネージャーがインストールされている場合、OT デバイスにアサインされたサイトが **[サイト]** フィールドに表示されます。
- 産業用プロセスマネージャーが有効になっていて、OT デバイスに関連付けられているエンティティが 1 つしかない場合は、**[Equipment model entity (機器モデルエンティティ)]** フィールドが自動的に入力されます。

i 注:

複数のエンティティがデバイスに関連付けられている場合、**[Equipment model entity (機器モデルエンティティ)]** フィールドは空のままになります。

インシデントレコードからの変更要求の作成

OT インシデントレコードから オペレーショナルテクノロジー (OT) 変更要求を作成します。インシデントレコードから変更要求を直接作成すると、インシデントレコードからの新しい変更要求にデータが自動的にマッピングされます。

始める前に

必要なロール:sn_ot_incident_write、sn_ot_incident_admin、または sn_ot_change_write

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. OT インシデントリストモジュールで、利用可能なリストのいずれかを選択します。
3. OT 変更要求を作成するインシデントレコードを選択します。
4. **[Create OT Change (OT 変更を作成)]** ボタンを選択します。
[OT 変更を選択 (Select OT change)] フォームが開きます。
5. 組織に適用可能な変更モデルを選択します。
詳細については、「[変更要求を実行するための変更モデルを選択します](#)」を参照してください。
6. **[Create OT Change record (OT 変更レコードを作成)]** を選択します。
7. 必要に応じて、プレイブックと関連フォームに入力します。

プレイブックと関連フォームの詳細については、選択した OT 変更モデルに応じて「[基本的な OT 変更モデルプレイブック](#)」と [高度な OT 変更モデルプレイブック](#)」を参照してください。

i 注:

新しい変更要求の [Details (詳細)] 関連リストで、次のフィールドと関連リストに、関連する OT インシデントレコードの値が自動的に入力されます。

- サイト
- 設備モデルのエンティティ
- OT デバイス (CI)
- Short Description (簡単な説明)
- Description (説明)
- 優先度

i 注:

1 から 4 までの **[Priority]** フィールドの値は、新しい変更レコードで同じです。ただし、インシデントレコードの **[Priority]** フィールドの値が 5 だったのが、新しい変更レコードでは 4 に変更されます。

変更レコード内の関連するデバイスと機器モデルエンティティを編集する

関連する オペレーショナルテクノロジー (OT) デバイスと機器モデルエンティティを OT 変更レコードから直接追加または削除します。変更要求と影響を受けるアイテムとの関係を追跡できます。

始める前に

必要なロール:sn_ot_change_write または sn_ot_change_admin

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース).
2. 産業用 ワークスペースリストビューを開きます。
3. [OT 変更要求] リストモジュールで、利用可能なリストのいずれかを選択します。
4. 編集する変更レコードを選択します。
5. 関連する OT デバイスを追加または削除します。
これで、OT デバイスが [影響を受ける OT デバイス] 関連リストの変更レコードに追加されるか、変更レコードから削除されます。
6. ステップ 4 と 5 を繰り返して、[Impacted Equipment Model Entities (影響を受ける機器モデルエンティティ)] 関連リストで機器モデルエンティティを変更レコードに追加または削除します。

オペレーショナルテクノロジー 変更承認

オペレーショナルテクノロジー (OT) 変更承認により、レビュー担当者は要求された変更を承認し、必要に応じて改善を提案できます。

概要

高度な OT 変更モデルを使用した OT 変更承認により、承認者は変更要求を確認し、必要に応じて要求を編集し、変更要求を承認できます。

i 注:

変更承認は、高度な OT 変更モデルにのみ適用されます。基本的な OT 変更モデルには変更承認ポリシーは適用されません。

変更承認の要件

要件	Description (説明)
サイトレベル	変更が行われるサイトまたはエリア。
サイト承認グループ	変更要求をレビューおよび承認できる承認グループにアサインされたメンバー。
必要なロール	承認者にはsn_ot_change_readロールが必要です。
承認の割合	承認グループの 51% が変更を承認する必要があります。

OT 変更承認フロー

OT 変更の承認フローは次のとおりです。

1. 変更要求を作成します。
2. フローは変更モデルに基づいて呼び出されます。
3. フローは変更承認ポリシーを適用します。
4. さまざまな意思決定レコードが評価されます。
5. 一致する承認定義が実行されます。
6. サイトレベルの承認者のリストを変更レコードに追加します。

高度な OT 変更モデルには、変更承認ポリシーが含まれています。独自の承認ポリシーを作成することもできます。承認ポリシーの作成方法の詳細については、「[Create change approval policies](#)」を参照してください。

変更要求をレビューする承認者の追加

グループメンバーまたは承認者を承認グループに手動で追加して、オペレーショナルテクノロジー (OT) 変更要求をレビューします。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > ユーザー管理 > グループ**。
2. [Groups (グループ)] リストから **[OT Change Default Approvers (OT 変更のデフォルト承認者)]** グループを選択します。
3. [グループメンバー] 関連リストを選択します。
4. [編集] を選択します。
5. [コレクション] リストで、承認グループに追加するメンバーを選択します。
6. 中央の矢印を使用して、選択したメンバーを [OT 変更のデフォルト承認者] リストに移動します。
7. [保存] を選択します。

タスクの結果

新しいメンバーが承認グループに追加されました。これで、承認グループが変更要求をレビューできるようになります。

高度な OT 変更モデルプレイブックで OT 変更要求の開始ステージと計画ステージを完了すると、承認ステージで承認を要求できます。承認グループのメンバーは、次のいずれかの方法を使用して、産業用ワークスペース で変更要求レコードを開いて承認する必要があります。

- 変更要求レコードで、[**Approvers**] タブを選択し、[**State**] フィールドを [**Requested**] から適切なオプションに変更します。
- [**Playbook** (プレイブック)] タブで、[Approve (承認)] ステージを選択し、[**State** (ステータス)] フィールドを [**Requested** (要求済み)] から適切なオプションに変更します。

サイト全体の変更要求の管理

オペレーショナルテクノロジー変更管理 アプリケーションを使用して、自分のサイトまたは他のサイトに属する変更要求を表示、作成、または編集できます。他のサイトからの変更要求を表示することで、自分のサイトで同様の変更を実装できます。

概要

sn_ot_change_write ロールを持っている場合は、次のタスクを実行できます。

- 自分にアサインされている オペレーショナルテクノロジー (OT) 変更要求またはサイトに属する変更要求を表示および編集します。
- OT 変更要求を作成します。
- 他のサイトに属する OT 変更要求を表示します。

sn_ot_change_write ロールを持つことの主な利点は、サイト全体の変更を読み取り専用で表示できることです。サイト全体で他の変更を表示すると、サイトで同様の変更を実装するのに役立ちます。

注:

自分がアクセスできるサイトに属する OT 変更要求のみを編集できます。クロスサイト OT 変更要求の管理に必要な追加ロールの詳細については、以下のセクションを参照してください。

sn_ot_change_write ロールに必要なその他の OT ロールと権限

次の表では、sn_ot_change_write ロールを持つユーザーが自分のサイトまたは任意のサイトの変更要求にアクセスするために必要な追加のロールについて説明します。

sn_ot_change_write ロールに必要なその他のロール

ロール	権限
cmdb_ot_isa_editor ロールを持つ sn_ot_change_write	サイトの変更要求を作成および編集します。
cmdb_ot_isa_viewer ロールを持つ sn_ot_change_write	サイトの変更要求を作成および編集します。
sn_ot_change_write と cmdb_ot_isa_viewer_all	任意のサイトの変更要求を作成および編集します。
サイト ロールのない sn_ot_change_write	任意のサイトの変更要求を表示します。

sn_ot_change_read ロールに必要なその他の OT ロールと権限

次の表では、sn_ot_change_read ロールを持つユーザーが自分のサイトまたは任意のサイトの変更要求を表示するために必要な追加のロールと権限について説明します。

sn_ot_change_readユーザーロールに必要なその他のロール

ロール	権限
cmdb_ot_isa_editorロールを持つ sn_ot_change_read	サイトの変更要求を表示します。
cmdb_ot_isa_viewerロールを持つ sn_ot_change_read	サイトの変更要求を表示します。
sn_ot_change_readとcmdb_ot_isa_viewer_all	任意のサイトの変更要求を表示します。
サイト ロールのないsn_ot_change_read	任意のサイトの変更要求を表示します。

変更要求を表示または編集する場所

産業用 ワークスペース のリストモジュールでは、次の OT 変更要求リストを使用できます。

- 自分にアサイン済み:アサインされた変更レコードを表示および編集するには、次の場所に移動します。 **OT 変更要求** > 自分にアサイン済み。
- 自分のサイトに属する:自分のサイトに属する変更レコードを表示および編集するには、次の場所に移動します。 **OT 変更要求** > 自分のサイトに所属。
- さまざまなサイトの既存の変更レコードを表示するには、次の場所に移動します。 **OT 変更要求** > すべて。

サイト全体での変更モデルレコードの可視化

オペレーショナルテクノロジー (OT) 変更ロールとサイト ロールに応じて、自分のサイトまたは他のサイトの変更モデル レコードを表示、作成、または編集できます。

OT 変更モデルレコードのロールと可視化を変更する

次の表は、変更モデルレコードにアクセスするためのさまざまな OT 変更ユーザーのロールと権限を示しています。

sn_ot_change_writeロールを持つユーザーの権限

ロール	権限
cmdb_ot_isa_editor サイト ロールを持つ sn_ot_change_write	レコードに変更モデルを使用する。
cmdb_ot_isa_viewer サイト ロールを持つ sn_ot_change_write	レコードに変更モデルを使用する。
cmdb_ot_isa_viewer_all サイト ロールを持つ sn_ot_change_write	レコードに変更モデルを使用する。
サイト ロールのないsn_ot_change_write	変更モデルにはアクセスできません。

sn_ot_change_readロールを持つユーザーの権限

ロール	権限
cmdb_ot_isa_editor サイト ロールを持つ sn_ot_change_read	変更モデルにはアクセスできません。

sn_ot_change_read ロールを持つユーザーの権限 (続く)

ロール	権限
cmdb_ot_isa_viewer サイト ロールを持つ sn_ot_change_read	変更モデルにはアクセスできません。
サイト ロールのない sn_ot_change_read	変更モデルにはアクセスできません。
cmdb_ot_isa_viewer_all サイト ロールを持つ sn_ot_change_read	変更モデルにはアクセスできません。

sn_ot_change_manager ロールを持つユーザーの権限

ロール	権限
cmdb_ot_isa_editor サイト ロールを持つ sn_ot_change_manager	• 任意のサイトの変更モデルを作成、編集、削除します。 • 変更モデルを任意のサイトにアサインします。 • 任意のサイトから変更モデルを削除します。
cmdb_ot_isa_viewer サイト ロールを持つ sn_ot_change_manager	• 任意のサイトの変更モデルを作成、編集、削除します。 • 変更モデルを任意のサイトにアサインします。 • 任意のサイトから変更モデルを削除します。
サイト ロールのない sn_ot_change_manager	どのサイトの変更モデルも表示または編集できません。どのサイトにも関連付けられていないベースシステム変更モデルのみを表示できます。

sn_ot_change_admin ロールを持っている場合は、変更モデルを使用して、任意のサイトの変更要求を作成できます。

メール通知を変更する

オペレーショナルテクノロジー (OT) 変更要求または変更タスクが更新されたときに、メール通知を使用してユーザーにアラートします。

OT 変更要求と変更タスクの通知を次の表に示します。

OT 変更要求のメール通知

名前	[When to send]	[Who receives it]	内容
自分にアサインされた変更	[Assigned to (アサイン先)] フィールドが変更され、空でない場合	変更をアサインしたユーザー	件名:<変更要求 #> 通知 Body : 簡単な説明:<簡単な説明>

OT 変更要求のメール通知 (続く)

名前	[When to send]	[Who receives it]	内容
			ここをクリックして変更要求を表示:<変更要求の URL> サイト:<サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ> 説明:<説明>
自分のグループにアサインされた変更	[Assignment group] フィールドが変更され、空でない場合	アサイン先グループ	件名:<変更要求 #> がグループ <アサイン先グループ>にアサインされました Body : 簡単な説明:<簡単な説明> ここをクリックして変更要求を表示:<変更要求の URL> サイト:<サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ> 説明: <description>
コメントされた変更	変更要求にコメントが付けられたとき	- 要求者 - ウォッチリスト	件名:<変更要求 #> 件のコメントが追加されました Body : 簡単な説明:<簡単な説明> ここをクリックして変更要求を表示:<変更要求の URL> コメント:<変更要求に追加されたコメント>

OT 変更要求のメール通知 (続く)

名前	[When to send]	[Who receives it]	内容
作業メモされた変更	変更要求に作業メモが追加されたとき。	- 作業メモリスト - Assigned to (アサイン先) - アサイン先グループ	件名: <変更要求 #> 作業メモが追加されました Body : 簡単な説明:<簡単な説明> ここをクリックして変更要求を表示:<変更要求の URL> 作業メモ:<変更要求に追加された作業メモ>
承認された変更	変更要求が承認されたとき	- Assigned to (アサイン先) - アサイン先グループ	件名: <変更要求 #> が承認されました Body : 簡単な説明:<簡単な説明> <変更要求の URL> を表示するには、ここをクリックしてください 説明:<説明>
却下された変更	変更要求が却下されたとき	- Assigned to (アサイン先) - アサイン先グループ	件名:<変更要求 #> が却下されました Body : 簡単な説明:<簡単な説明> <変更要求の URL> を表示するには、ここをクリックしてください 説明:<説明>
保留中の変更	変更要求が保留になったとき	要求者	件名: <変更要求 #> が保留になりました Body : こんにちは <変更要求を作成したユーザー>、 要求した <変更要求 #> は保留になりました。要求が保留になってい

OT 変更要求のメール通知 (続く)

名前	[When to send]	[Who receives it]	内容
			る理由:<変更要求が保留になっている理由> 変更要求を表示するには、ここをクリックしてください: <変更要求の URL>
保留解除の変更	変更要求が保留になったとき	要求者	件名: <変更要求 #> が保留になりました Body : こんにちは <変更要求を作成したユーザー>、 要求した <変更要求 #> は保留解除され、[ステータス] フィールド <更新済み> ステータスになっています。 変更要求を表示するには、ここをクリックしてください: <変更要求の URL>

OT 変更タスクのメール通知

名前	[When to send]	[Who receives it]	内容
自分にアサインされたタスクの変更	[Assigned to (アサイン先)] フィールドが変更され、空でない場合	変更タスクをアサインされた人物	件名:<変更タスク #> 通知 -- <簡単な説明> Body : 簡単な説明:<簡単な説明> 変更タスクを表示するには、ここをクリックしてください:<変更タスクの URL> サイト: <サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ> 説明:<説明>

OT 変更タスクのメール通知 (続く)

名前	[When to send]	[Who receives it]	内容
自分のグループにアサインされたタスクの変更	[Assignment group] フィールドが変更され、空でない場合	アサイン先グループ	件名: 件名: <変更タスク #> 通知 -- <簡単な説明> Body : 簡単な説明:<簡単な説明> 変更タスクを表示するには、ここをクリックしてください:<変更タスクの URL> サイト: <サイト名> OT デバイス:<OT デバイス> 機器モデルエンティティ:<機器モデルエンティティ> 説明:<説明>
作業メモされた変更タスク	変更タスクに作業メモが追加されたとき	- 作業メモリスト - Assigned to (アサイン先) - アサイン先グループ	件名: <変更タスク #> 作業メモが追加されました -- <簡単な説明> Body : 簡単な説明:<簡単な説明> 変更タスクを表示するには、ここをクリックしてください:<変更タスクの URL> 作業メモ:<変更タスクに追加された作業メモ>

オペレーショナルテクノロジー変更管理 参照

参照トピックには、オペレーショナルテクノロジー変更管理 アプリケーションに関する追加情報が記載されています。

変更カテゴリ

オペレーショナルテクノロジー (OT) 変更要求を分類することで、特定の OT 変更要求をグループ化して検索を絞り込むことができます。カテゴリは、ステークホルダーが変更の内容を把握するためにも役立ちます。

OT 変更要求を作成できる場合は、次の表にリストされているカテゴリから選択できます。

OT 変更要求カテゴリ

カテゴリ	Description (説明)
ハードウェア	OT デバイスを追加、削除、または設定するための変更。
ソフトウェア	OT ソフトウェアを追加、削除、または設定するための変更。
サービス	OT サービスへの変更。
システムソフトウェア	OT システムソフトウェアへの変更。
アプリケーションソフトウェア	OT アプリケーションソフトウェアに対する変更。
ネットワーク	サブネット、IP アドレス、および MAC アドレスに対する変更。
通信	OT システムで使用される通信の変更。
ドキュメント	OT ドキュメントの変更。
ファームウェア	OT ファームウェアへの変更。
その他	上記のカテゴリではキャプチャされないその他の変更。

オペレーショナルテクノロジー変更管理とともにインストールされるコンポーネント

オペレーショナルテクノロジー変更管理 (sn_ot_chg_mgmt) アプリケーションをアクティブ化すると、ユーザーロールを含むいくつかのタイプのコンポーネントをインストールできます。

i 注:

アプリケーションファイルテーブルには、このアプリケーションとともにインストールされたコンポーネントがリストされています。このテーブルへのアクセス手順については、「[アプリケーションとともにインストールされているコンポーネントの検索](#)」を参照してください。

インストールされるロール

ロール	説明	含まれるロール
変更マネージャー [sn_ot_change_manager]	OT 変更モデルレコードを管理できます。	• sn_ot_change_write • sn_sttrm_condition_read
変更管理者 [sn_ot_change_admin]	OT 変更レコードを作成、表示、削除、編集できます。カテゴリとシステムプロパティを設定できます。	• cmdb_ot_isa_viewer_all • sn_ot_change_write
変更書き込みユーザー [sn_ot_change_write]	OT 変更レコードを作成、表示、編集できます。 IT 変更タスクをアサインすることもでき、アサインされている IT 変更タスク	• cmdb_ot_viewer • cmdb_ot_isa_viewer • sn_ot_change_read

ルール	説明	含まれるルール
	を編集してクローズすることもできます。 詳細については、「サイト全体の変更要求の管理」を参照してください。	
変更読み取りユーザー [sn_ot_change_read]	OT 変更レコードの表示のみ可能です。	• cmdb_ot_viewer • cmdb_ot_isa_viewer

関連情報

OT 拡張クラスと関連アプリケーションに関する詳細情報を確認してください。

概要

拡張クラスは、オペレーショナルテクノロジー管理構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

Operational Technology (OT) extension classes

構成管理データベース (CMDB)は OT のクラスを更新します。

関連アプリケーション

IT Service Management

ServiceNow IT Service Management アプリケーションを オペレーショナルテクノロジー変更管理 と統合すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジーのナレッジ管理

ServiceNow[®] オペレーショナルテクノロジーのナレッジ管理 は、 オペレーショナルテクノロジー (OT) システム、そのデバイス、および組織内の解決済みインシデントに関するナレッジの収集、整理、共有に役立ちます。



オペレーショナルテクノロジーのナレッジ管理 の探索

オペレーショナルテクノロジーのナレッジ管理 は、OT インシデントに関連するナレッジ記事で オペレーショナルテクノロジー (OT) システムに関する情報をキャプチャするのに役立ちます。組織は

これらのナレッジ記事を使用して、ユーザーが適切な情報にアクセスし、ユーザーとの誤解を防ぐことができます。

オペレーショナルテクノロジーのナレッジ管理のメリット

オペレーショナルテクノロジーのナレッジ管理 では、次の主要な機能を使用できます。

- オペレーショナルテクノロジー管理ソリューションで既存のナレッジ管理 Now Platform 機能を使用する機能。
- OT インシデントに関連するすべてのナレッジベース記事を参照し、インシデントレコードから直接ナレッジ記事を作成する機能。
- ナレッジマネージャーとナレッジユーザー向けの OT ナレッジベースを構成する機能。
- 産業用 ワークスペースでナレッジ記事を作成する機能。
- ナレッジ記事の公開、編集、廃止、または削除の承認を要求する機能。
- 更新された情報で既存のナレッジ記事を編集する機能。

オペレーショナルテクノロジーのナレッジ管理の構成

オペレーショナルテクノロジー (OT) ソリューションのデータ基盤を作成できるようにオペレーショナルテクノロジーのナレッジ管理を構成します。

admin ロールを持っている場合は、ガイド付きセットアップ を使用して オペレーショナルテクノロジーのナレッジ管理 のセットアップをガイドできます。ガイド付きセットアップ は、アプリケーションの構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

ガイド付きセットアップにアクセスするには、産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表に、ガイド付きセットアップ タスクとその オペレーショナルテクノロジーのナレッジ管理目的を示します。

i 注:

オペレーショナルテクノロジーのナレッジ管理はオペレーショナルテクノロジーインシデント管理アプリケーションに入っています。オペレーショナルテクノロジーインシデント管理 アプリケーション (バージョン 2.0.2) をインストールして構成していれば、オペレーショナルテクノロジーのナレッジ管理構成できます。追加に必要なロールはありません。

次の表は、セットアップと構成を正しく行うためにユーザーが完了する必要があるタスクを示しています。

オペレーショナルテクノロジーのナレッジ管理セットアップタスク

タスク	目的
ナレッジ管理ロールをオペレーショナルテクノロジーのナレッジ管理に割り当てます。	ロールを割り当てて、各ユーザーが使用できるアクションを制御します。
OT ナレッジベースを作成します。	OT ナレッジベースを構成して、マネージャーを追加し、アクセス権を設定します。

オペレーショナルテクノロジーのナレッジ管理セットアップタスク (続く)

タスク	目的
OT ナレッジベースに適用するユーザー基準を作成します。	OT ナレッジベースを閲覧または寄稿できるユーザーを決定するユーザー基準レコードを作成します。
ユーザー基準を OT ナレッジベースにアサインします。	ユーザー基準レコードを OT ナレッジベースにアサインして、ナレッジベース内のナレッジ記事を作成、読み取り、書き込み、および廃止できるユーザーを制御します。
非認証ユーザーの OT ナレッジベースへのアクセスを設定します。	非認証ユーザーがアクセスできる OT ナレッジベースをレビューします。アクセスは、ユーザー基準と <code>glide.knowman.block_access_with_no_user_criteria</code> プロパティ設定に基づきます。
ナレッジワークフローを OT ナレッジベースにアサインします。	公開および廃止プロセスのために、各 OT ナレッジベースに異なるナレッジワークフローをアサインします。
オペレーショナルテクノロジーのナレッジ管理に使用されるナレッジ管理プロパティを確認します。	適用可能な ナレッジ管理 プロパティを使用して、OT ナレッジベースの外観と機能を構成します。

オペレーショナルテクノロジーのナレッジ管理ユーザーへのロールのアサイン

ユーザーに ナレッジ管理 ロールをアサインして、オペレーショナルテクノロジーのナレッジ管理の機能やデータへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

ナレッジ管理ロールがアサインされている場合は、オペレーショナルテクノロジーのナレッジ管理機能を使用できます。

i 注:

ユーザー基準によってナレッジ記事へのアクセスが決定されます。詳細については、「[Managing access to knowledge bases and knowledge articles](#)」を参照してください。

オペレーショナルテクノロジーのナレッジ管理 に適用可能なナレッジ管理ロールの詳細については、「[オペレーショナルテクノロジーのナレッジ管理 ロール](#)」を参照してください。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

OT ナレッジベースを作成する

オペレーショナルテクノロジー (OT) ナレッジベースを作成して、OT ナレッジユーザーが OT インシデントに関連するコンテンツを保存、共有、管理するためのセルフサービスプラットフォームを提供します。

始める前に
必要なロール：admin

手順

1. 移動先 ナレッジ > 管理 > ナレッジベース.
2. [新規] を選択します。
3. ナレッジベースフォームのフィールドに入力します。
フィールド値の説明については、「[ナレッジベース フォーム](#)」を参照してください。
4. フォームヘッダーを右クリックし、[保存] を選択します。
5. 関連リストセクションで、OT ナレッジベースに関連する次のテーブルのアイテムを表示または設定します。

名前	説明
ナレッジ	このナレッジベースに保存されているナレッジ記事のリスト。
読込可能	読み取りアクセス権を付与し、基準に一致するユーザーが OT ナレッジベースの記事を読めるようにするユーザー基準のリスト。
寄稿可能	貢献者アクセス権を付与し、基準に一致するユーザーが OT ナレッジベースの記事を作成および変更できるようにするユーザー基準のリスト。
記事テンプレート	ナレッジ管理 Advanced (com.snc.knowledge_advanced) プラグインを有効にしている場合は、[記事テンプレート] 関連リストが表示されます。 記事テンプレートが関連リストにある場合、そのナレッジベースの記事は、リストされている記事テンプレートの 1 つを使用してのみ作成できます。 [Article Templates] 関連リストが空の場合、任意の記事テンプレートを使用して記事を作成できます。 [編集] を選択して、記事テンプレートをナレッジベースにマッピングします。 i 注: アドミン、ナレッジアドミニストレータ、およびナレッジマネージャーは、ナレッジベースの記事テンプレートを編集できます。
ナレッジ カテゴリ	OT ナレッジベースに関連付けられているナレッジカテゴリのリスト。

名前	説明
	i 注: カテゴリが非アクティブとしてマークされている場合、記事をカテゴリに関連付けることはできません。ただし、そのカテゴリの既存の記事には影響しません。

6. [送信] を選択します。

OT ナレッジベースのユーザー基準を作成する

ユーザー基準レコードを作成して、オペレーショナルテクノロジー (OT) ナレッジベースを閲覧または寄稿できるユーザーを決定します。

始める前に

必要なロール: user_criteria_admin

i 注:

ナレッジモジュールからユーザー基準レコードを作成するには、knowledge ロールに加えて user_criteria_admin ロールが必要です。アクセスの詳細については、「[Managing access to knowledge bases and knowledge articles](#)」を参照してください。

このタスクについて

ナレッジ管理のユーザー基準を使用して、特定のユーザーが OT ナレッジベースとナレッジ記事にアクセスできるかどうかを判断します。ユーザー基準レコードを作成したら、それを OT ナレッジベースにアサインして、ナレッジベースとその記事を読んだり寄稿したりできるユーザーを制御できます。さらに、記事レベルでユーザー基準をアサインして、それを読むことができるユーザーを制御できます。

手順

1. 移動先 **すべて > ナレッジ > 管理 > ユーザー基準**.
2. [新規] を選択します。
3. フォームのフィールドに入力します。

[ユーザー基準] フォーム

フィールド	説明
名前	ユーザー基準の一意の名前。
ユーザー	ユーザー基準に一致する必要があるユーザー。
グループ	ユーザー基準に一致する必要があるグループ。
ロール	ユーザー基準に一致するロール。

フィールド	説明
	i 注: - ロールの評価はセッションでキャッシュされるため、ルールを変更すると再度ログインする必要があります。 - ユーザー基準は、昇格された特権ルールに適用できません。
詳細	ユーザー基準フォームの [スクリプト] フィールドを含む詳細オプションを表示または非表示にするオプション。
スクリプト	true または false を返す追加のユーザー基準を定義するスクリプト。このフィールドは、[ユーザー基準] フォームで [詳細] オプションが選択されている場合に使用できます。 i 注: - スクリプトは、ユーザー基準が作成された範囲内で評価されます。 - スクリプトの評価はセッションにキャッシュされるため、評価を変更するには、再ログインする必要があります。スクリプト化されたユーザー基準がナレッジベースに対して定義されている場合、ナレッジベースへのユーザーアクセスはセッションごとに評価されます。セッションキャッシュのビルド後にスクリプトによって変更が生じた場合、その変更は次のセッションで有効になります。 <code>gs.getUser()</code> またはその他のセッション API は診断ツールで使用すると競合が発生するため、使用しないでください。スクリプトで利用可能な事前定義済みの <code>user_id</code> 変数を使用して、スクリプトを評価するために使用されているユーザーのユーザー ID を取得します。 - スクリプトは動的に評価されます。したがって、ユーザー基準にスクリプトを含めると、システムのパフォーマンスに影響を与える可能性があります。
アクティブ	ユーザー基準をアクティブ化/非アクティブ化するオプション。
会社	ユーザーレコードが一致する必要がある会社。
ロケーション	ユーザーレコードが一致する必要がある場所。
部門	ユーザーレコードが一致する必要がある部門。
すべて一致	入力された各ユーザー基準フィールドのすべての要素が一致する必要があるかどうかを判断するためのオプション。選択した場合、すべてのユーザー基準に一致するユーザーのみにアクセス権が付与されます。オフにした場合、ユーザーは、アクセス権が付与される 1 つ以上のユーザー基準のセットを満たす必要があります。 デフォルトでは、このチェックボックスはオフになっているため、いずれかの条件を満たせばアクセスできます。 たとえば、次の条件のユーザー基準レコードを考えてみましょう。 - 場所 A または B - 会社 C または D

フィールド	説明
	[すべて一致] を選択すると、次の条件をすべて満たすユーザーのみが一致します。たとえば、場所 A および会社 C に所属するユーザーです。 [すべて一致] が選択されていない場合、これらの条件のいずれかを満たすユーザーがマッチングされます。たとえば、場所 B のユーザー。 i 注: [すべて一致] を選択する場合は、決して満たされない矛盾した条件を作成しないようにしてください。たとえば、場所 A のすべてのユーザーが会社 G に対して作業している場合、この例の条件は決して満たせません。

4. [送信] を選択します。

次のタスク

これで、ユーザー基準を OT ナレッジベースにアサインできるようになりました。詳細については、「[ユーザー基準を OT ナレッジベースにアサインする](#)」を参照してください。

ユーザー基準を **OT** ナレッジベースにアサインする

ユーザー基準レコードを オペレーショナルテクノロジー (OT) ナレッジベースにアサインして、ナレッジベース内のナレッジ記事を作成、読み取り、書き込み、および廃止できるユーザーを制御します。

始める前に

必要なロール：knowledge_manager、knowledge_admin、または admin

このタスクについて

ユーザー基準を OT ナレッジベースにアサインして、読み取りまたは寄稿アクセスを制御できます。

手順

1. 移動先 **すべて > ナレッジ > 管理 > ナレッジベース**。
2. 管理する OT ナレッジベースレコードを選択します。
3. ユーザー基準を OT ナレッジベースに追加します。
 - a. 設定するユーザー基準に応じて、1 つ以上の関連リストを選択します。

関連リスト	説明
読込可能	ユーザーはナレッジベースにあるナレッジ記事を読むことができます。
読込不可	ユーザーはナレッジベースにあるナレッジ記事を読むことができません。
寄稿可能	ユーザーはナレッジベースにあるナレッジ記事を作成、変更、廃止できます。ナレッジベースへの寄稿アクセス権は、ナレッジベースのすべての記事への読み取りアクセス権も提供します。
寄稿不可	ユーザーはナレッジベースにあるナレッジ記事を作成、変更、廃止または読み取りできません。

b. 選択した関連リストで、必要なユーザー基準を追加します。

- admin ロールを持つユーザーとして、[新規] を選択し、必須フィールドを指定して [送信] を選択し、新しいユーザー基準レコードを追加します。
- knowledge_manager、knowledge_admin、または admin ロールを持つユーザーとして、[編集] を選択し、必要なユーザー基準を [コレクション] 列から [ナレッジ] 列に移動して [保存] を選択し、既存のユーザー基準レコードを追加します。

4. ナレッジ ベース フォームで、更新 を選択します。

非認証ユーザーの OT ナレッジベースへのアクセスをレビューする

ユーザー基準と `glide.knowman.block_access_with_no_user_criteria` プロパティ設定を使用して、非認証ユーザーがアクセスできる オペレーショナルテクノロジー (OT) ナレッジベースを確認します。

始める前に

必要なロール: knowledge_admin または admin

このタスクについて

ナレッジベースの非認証ユーザーを制限する場合は、ユーザー基準または `glide.knowman.block_access_with_no_user_criteria` プロパティ設定を使用できます。

手順

1. 移動先 **すべて > ナレッジ > 管理 > ナレッジベース**.
2. 非認証ユーザーがアクセスできる OT ナレッジベースを確認します。
3. オプション: ユーザー基準を使用してナレッジベースの非認証ユーザーを制限するには、ナレッジベースレコードを選択し、そのユーザー基準を更新します。
ユーザー基準の作成の詳細については、「[OT ナレッジベースのユーザー基準を作成する](#)」を参照してください。ユーザー基準の割り当ての詳細については、「[ユーザー基準を OT ナレッジベースにアサインする](#)」を参照してください。
4. オプション: `glide.knowman.block_access_with_no_user_criteria` プロパティ設定を使用して、ナレッジベースの認証されていないユーザーを制限します。
 - a. 移動先 **すべて > ナレッジ > アドミニストレーション > プロパティ**.
 - b. `glide.knowman.block_access_with_no_user_criteria` プロパティ設定を true に設定します。
 - c. [保存] を選択します。

OT ナレッジベースへのナレッジワークフローのアサイン

公開および廃止プロセスの各オペレーショナルテクノロジー (OT) ナレッジベースに異なるナレッジ管理ワークフローをアサインできます。

概要

オペレーショナルテクノロジーのナレッジ管理には、次の表に示すデフォルトのナレッジ管理ワークフローを使用して、OT ナレッジベースに適用できます。

注:

承認が必要なワークフローの場合、KBWorkflow スクリプトインクルードで `getApprovers()` 機能を編集することによって、どのユーザーが承認または廃止を行うことができるかを設定できます。

デフォルトのナレッジ管理 ワークフロー

ワークフロー	説明
ナレッジ - 公開承認	ナレッジベースのマネージャーに承認を要求します。承認中の記事は、承認後に公開済みステータスに移行する前のステータスが [レビュー中] になります。後で公開するように設定されている場合は、[スケジュール済み] ステータスに移行します。マネージャーが要求を却下した場合、ワークフローはキャンセルされ、記事はドラフト ステータスのままになります。 所有グループオプションが有効になっている場合、記事へのリンクを含むメール通知が所有グループのメンバーに送信され、承認されます。 所有グループオプションが有効になっていない場合、記事へのリンクを含むメール通知がナレッジベースマネージャーに送信され、承認されます。 記事が承認または却下されたことを知らせる通知が、記事の作成者または改訂者にも送信されます。 承認メール通知をオンにするには、<code>glide.knowman.enable_approval_notification</code> プロパティを true に設定します。 注: アクティブなユーザーのみが通知を受け取ります。
ナレッジ - 廃止承認	記事を廃止ステータスに移行する前に、ナレッジベースのマネージャーからの承認を要求します。マネージャーが要求を却下した場合、ワークフローはキャンセルされ、記事は [Published] ステータスのままになります。 所有グループオプションが有効になっている場合、記事へのリンクを含むメール通知が所有グループのメンバーに送信され、承認されます。 所有グループオプションが有効になっていない場合、記事へのリンクを含むメール通知がナレッジベースマネージャーに送信され、承認されます。
ナレッジ - すぐに公開	承認を必要とせずにドラフト記事を即時公開するか、後で公開するように設定されている場合は公開予定日に公開します。
ナレッジ - すぐ廃止	承認を要求せずに公開記事をすぐに廃止します。

デフォルトのナレッジ管理 ワークフロー (続く)

ワークフロー	説明
ナレッジ - ナレッジの公開	ナレッジ記事を [公開済み] ステータスに移行するサブフロー。独自のワークフローを定義している場合にこのサブフローを使用できます。
ナレッジ - ナレッジの廃止	ナレッジ記事を 廃止 ステータスに移行するサブフロー。独自のワークフローを定義している場合にこのサブフローを使用できます。

承認ワークフローのメール通知

承認ワークフローのメール通知を送信できます。

- 承認のために送信されたナレッジ記事について承認者に通知します。
- ナレッジ記事の承認ステータスを作成者に通知します

承認ワークフローのメール通知を送信するには、[記事承認ワークフロー内の承認者と作成者に通知を送信する] プロパティ (*glide.knowman.enable_approval_notification*) を有効にします。New York リリース以降、このプロパティはデフォルトで有効になっています。New York リリースより前のリリースバージョンの既存のお客様は、このプロパティを有効にしてメール通知を送信できます。このプロパティを有効にする前に、記事承認のカスタム通知を無効にします。*glide.knowman.enable_approval_notification* プロパティが利用できない場合、アドミニストレーターはプロパティを作成してその値を true に設定できます。詳細については、「[Knowledge Management properties](#)」を参照してください。

オペレーショナルテクノロジーナレッジベースのナレッジ管理プロパティの確認

アドミニストレーターは、ナレッジ管理プロパティを使用して、オペレーショナルテクノロジー (OT) ナレッジベースの外観と機能を設定できます。

ナレッジ管理プロパティにアクセスするには、次の場所に移動します。すべて > ナレッジ > アドミニストレーション > プロパティ。

次のテーブルにリストされているプロパティを使用して、ナレッジベースの不完全または不正確な記事にフラグを設定できるロールを制御します。

Glide.knowman.show_flag.roles プロパティ

プロパティ	Description (説明)
不完全/不正確な記事にフラグを設定できるロールのリスト (カンマ区切り形式) (<i>glide.knowman.show_flag.roles</i>)	に表示されるとおりにロール名を正確に入力します ユーザー管理 > ロール. [記事の評価セクションを表示] と [記事にフラグを設定] オプション プロパティの両方が選択されている場合、このプロパティにリストされているロールを持つユーザーには、記事ビューに [記事にフラグ設定] オプションが表示されます。 このプロパティにリストされているロールはすべて、[記事の評価セクションを表示できるロールのリスト] プロパティにもリストされている必要があります。

その他の使用可能な ナレッジ管理 プロパティの詳細については、「[Knowledge Management properties](#)」を参照してください。

オペレーショナルテクノロジーのナレッジ管理の使用

オペレーショナルテクノロジーのナレッジ管理に必要なすべてのセットアップタスクを完了すると、オペレーショナルテクノロジー (OT) インシデントに関連するナレッジ記事の管理を開始できます。

概要

オペレーショナルテクノロジーのナレッジ管理を使用することで、チームのニーズに応じてナレッジ記事を作成、編集、および廃止することができます。オペレーショナルテクノロジーインシデント管理 アプリケーションと併用すると、インシデントに関連する記事を参照したり、インシデントから記事を作成したりすることができます。

次の例は、チームに オペレーショナルテクノロジーのナレッジ管理 を適用する方法を示しています。

- 数年の経験を持つ OT エンジニアが、ガイドワーカーや経験の浅い技術者のために、OT デバイスに関する知識を 1 か所に集めたいと考えています。
- 生産プロセスオペレーションを担当する最前線の作業者と技術者は、工場フロアの問題に気づき、修正方法を説明するナレッジ記事を必要としています。

基本的な オペレーショナルテクノロジーのナレッジ管理 プロセス

次の ワークフロー では、オペレーショナルテクノロジーのナレッジ管理の基本的なプロセスについて説明します。

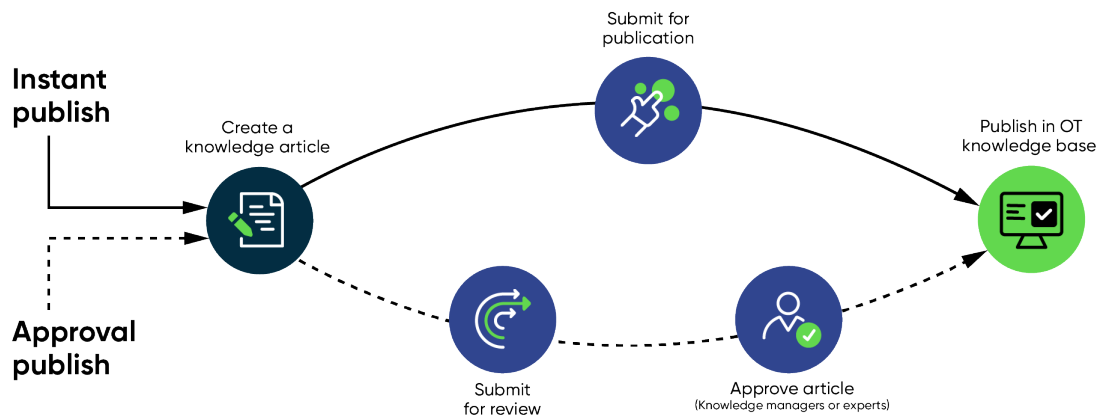
基本的な OT ナレッジのワークフロー



ナレッジ記事の公開

次の ワークフロー では、ナレッジ記事の作成方法と公開方法 (公開承認) と承認なし (即時公開) の両方について説明します。

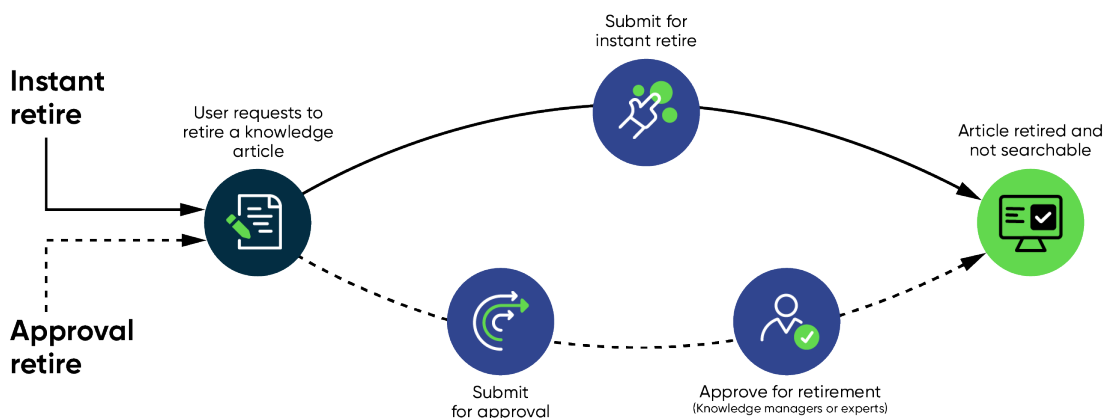
公開用ワークフロー



ナレッジ記事の廃止

次の ワークフロー では、ナレッジ記事を廃止する方法 (承認、廃止) と承認なし (即時廃止) の両方について説明します。すぐに廃止ワークフローでは、承認を必要とせずにすぐに記事を廃止できます。廃止承認ワークフローは、ナレッジマネージャーまたはエキスパートに承認要求を送信して、記事の廃止が必要であることを確認します。

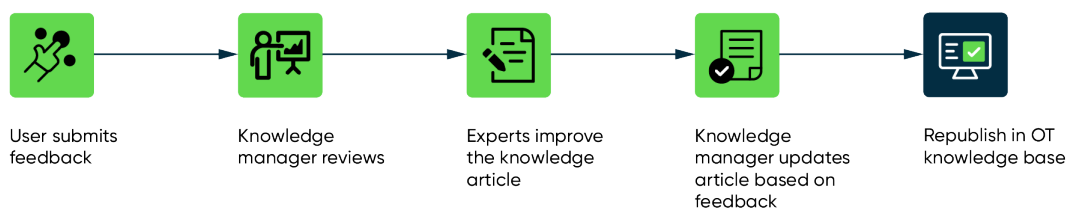
廃止用ワークフロー



ナレッジ記事への変更のレビューと承認

次の ワークフロー では、既存のナレッジ記事をユーザーフィードバックで更新する方法について説明します。

ユーザーフィードバックのワークフロー



ナレッジ記事

ナレッジ記事には、職場の最新情報、セルフヘルプ、トラブルシューティング手順、および OT チームがアクセスする必要があるその他の情報に関する情報が記載されています。たとえば、次のケースに対して次のナレッジ記事を作成できます。

- 組織全体で使用される標準運用手順テンプレート。
- インシデント中に学んだ教訓。
- さまざまな生産材料に注釈を付けた画像。

産業用 ワークスペース内のナレッジ記事は、次の方法で表示できます。

- 産業用 ワークスペースリストビューのナレッジモジュールの下。
- OT インシデントを開くときの [エージェントアシスト] ウィンドウ。
- 産業用 ワークスペースヘッダーのグローバル検索機能を使用する。

産業用 ワークスペースリストビューのナレッジモジュールでは、次のリストのナレッジ記事を表示できます。

- i 注:**
産業用 ワークスペースでこれらのリストモジュールを表示するには、ナレッジロールがアサインされている必要があります。

未公開記事

作成したものの、OT ナレッジベースでまだ公開されていない記事。

公開済みの記事

OT ナレッジベースに公開されている、作成した記事。

すべての記事

OT ナレッジベースで利用可能なすべての記事。

OT インシデントレコードからナレッジ記事を作成する

オペレーショナルテクノロジー (OT) インシデントとその解決に関連する情報を記録して保存するためのナレッジ記事を作成します。

始める前に

必要なロール:sn_ot_incident_write

- i 注:**
少なくとも 1 つのナレッジベースへの 寄稿可能 アクセス権も必要です。詳細については、[「OT ナレッジベースを作成する」](#)を参照してください。

このタスクについて

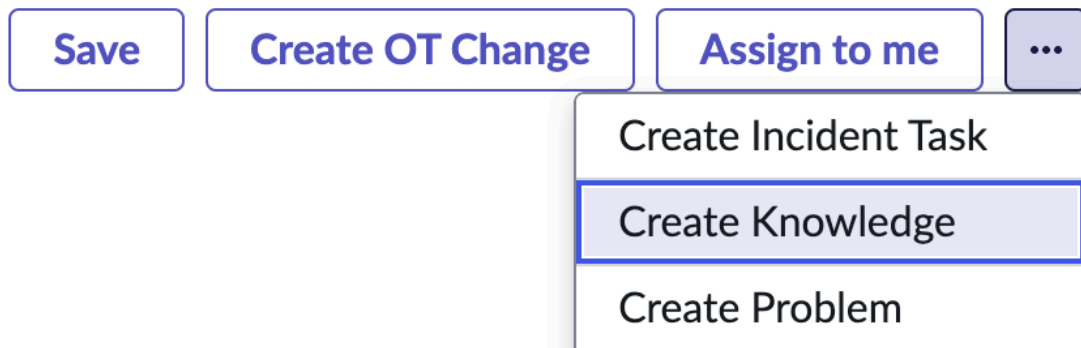
インシデントレコードから直接ナレッジ記事を作成すると、ナレッジ記事がコンテキスト情報の正しいインシデントにリンクされていることを確認できます。ナレッジ記事には、正しい手順、課題、およびソリューションが記載されており、チームが今後同様のインシデントを解決する際にも役立ちます。

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. OT インシデントモジュールのリストビューで、利用可能なリストのいずれかを開きます。
3. ナレッジ記事を作成する OT インシデントレコードを選択します。

4. [その他のアクション] アイコン (...) を選択してメニューを展開します。

5. [ナレッジを作成] を選択しま



す。

i 注:

[ナレッジを作成] ボタンを表示するには、インシデントレコードのステータスを [解決済み] に設定する必要があります。

6. フォームのフィールドに入力します。

ナレッジ記事フォーム

Field (フィールド)	説明
ナレッジベース	ナレッジ記事を含める必要があるナレッジベース。 i 注: OT ナレッジベースの可視化を正しく設定した場合、OT ユーザーはこの参照リストでナレッジベースを見つけることができます。
カテゴリ	ナレッジ記事の分類。
簡単な説明	ナレッジ記事のタイトルとして使用されるインシデント解決の簡単な説明。
記事本文	インシデントの手順、課題、および解決策を説明するナレッジ記事のコンテンツ。
有効期間終了日	ナレッジ記事の有効期限の日付。

7. [保存] を選択します。

ナレッジ記事はドラフトとして保存され、親 OT インシデントに添付されます。

8. [公開] を選択します。

タスクの結果

これで、ナレッジ記事が OT ナレッジベースで公開されました。ナレッジ記事を表示するには、インシデントレコードの [添付されたナレッジ] 関連リストを開きます。

i 注:

OT ナレッジベースの **[Publish workflow (公開ワークフロー)]** フィールドを **[Knowledge - Approval Publish (ナレッジ - 公開承認)]** に設定した場合、記事は公開前に承認される必要があります。

でのナレッジ記事の作成 産業用 ワークスペース

オペレーショナルテクノロジー (OT) インシデントに直接関連しないニーズとソリューションに記事の内容に対応するために役立つナレッジ記事を 産業用 ワークスペース で作成します。

始める前に

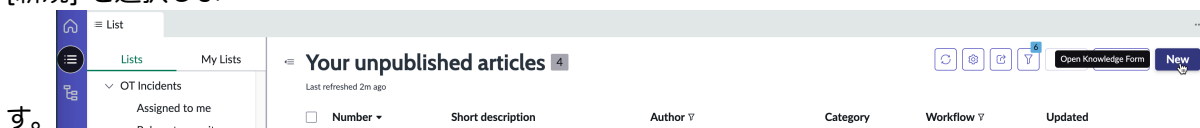
必要なロール: knowledge

i 注:

少なくとも 1 つのナレッジベースへの 寄稿可能 アクセス権も必要です。詳細については、「[OT ナレッジベースを作成する](#)」を参照してください。

手順

1. 移動先 **すべて > Industrial Workspace (産業用ワークスペース)**.
2. ナレッジモジュールのリストビューで、利用可能なリストの 1 つを開きます。
3. **[新規]** を選択しま



4. フォームのフィールドに入力します。

ナレッジ記事フォーム

Field (フィールド)	説明
ナレッジベース	ナレッジ記事を含める必要があるナレッジベース。 i 注: OT ナレッジベースの可視化を正しく設定した場合、OT ユーザーはこの参照リストでナレッジベースを見つけることができます。
カテゴリ	ナレッジ記事の分類。
簡単な説明	ナレッジ記事のタイトルとして使用されるインシデント解決の簡単な説明。
記事本文	インシデントの手順、課題、および解決策を説明するナレッジ記事のコンテンツ。
有効期間終了日	ナレッジ記事の有効期限の日付。

5. **[保存]** を選択します。
ナレッジ記事はドラフトとして保存され、親 OT インシデントに添付されます。
6. **[公開]** を選択します。

タスクの結果

これで、ナレッジ記事が OT ナレッジベースで公開されました。

注:

OT ナレッジベースの **[Publish workflow (公開ワークフロー)]** フィールドを **[Knowledge - Approval Publish (ナレッジ - 公開承認)]** に設定した場合、記事は公開前に承認される必要があります。

OT インシデントレコードからナレッジギャップを報告する

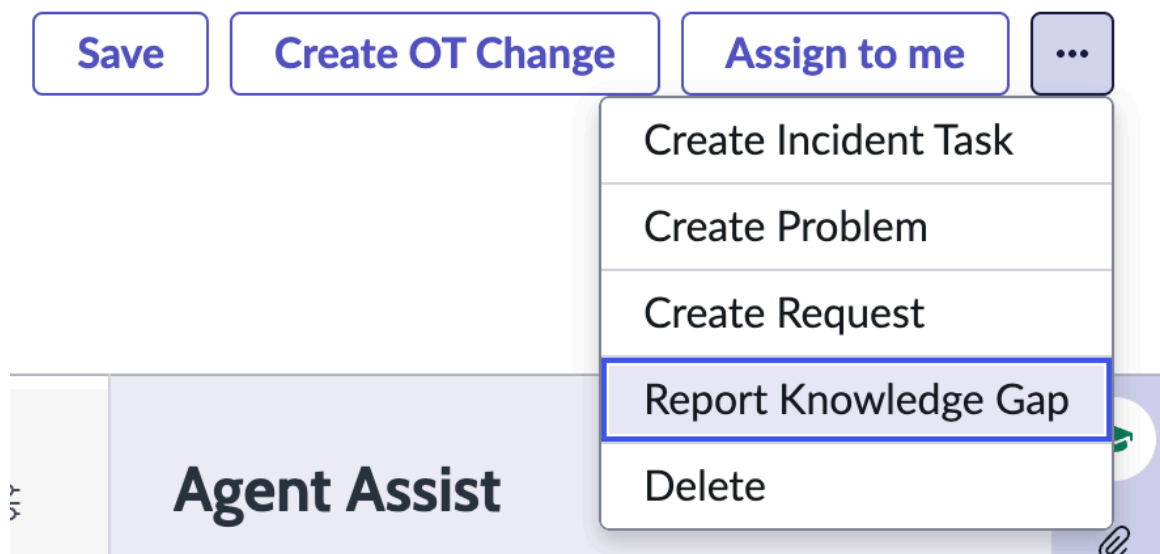
インシデントに関連するナレッジ記事が見つからない場合は、オペレーショナルテクノロジー (OT) インシデントからナレッジギャップを報告します。

始める前に

必要なロール:sn_ot_incident_read

手順

1. 移動先 **すべて > Industrial Workspace (産業用ワークスペース)**.
2. OT インシデントモジュールのリストビューで、利用可能なリストのいずれかを開きます。
3. ナレッジギャップを報告するインシデントレコードを選択します。
4. [その他のアクション] アイコン (...) を選択してメニューを展開します。
5. [ナレッジギャップを報告] を選択しま



6. フォームの [説明] フィールドにナレッジギャップの概要を入力します。

注:

[トピック] フィールドには、インシデントレコードの名前が自動的に入力されます。必要に応じて、このフィールドを変更できます。

7. [送信] を選択します。

タスクの結果

ナレッジギャップが報告され、フィードバックタスクが作成されます。

次のタスク

フィードバックタスクは、インシデントレコードの [ナレッジギャップ] 関連リストで表示できます。

フィードバックタスクを正しいユーザーまたはユーザーグループに割り当てるには、「[フィードバックタスクのアサイン](#)」を参照してください。

ナレッジ記事の公開または廃止要求の承認

ナレッジ記事の公開または廃止の要求を承認して、ナレッジベースを最新の状態に保ちます。

始める前に

必要なロール:knowledge_manager

このタスクについて

OT ナレッジベース受信のマネージャーとしてアサインされている場合は、ナレッジベースに属する記事の公開と廃止に関する承認要求を受信できます。

手順

1. 承認要求に関するメール通知を開きます。
2. メール内のリンクを選択して要求を開きます。
3. その要求を承認または却下します。
4. オプション: 却下された場合は、記事要求が却下された理由を説明するコメントを残します。

タスクの結果

承認要求を作成したユーザーにメールで通知されます。

フィードバックタスクのアサイン

フィードバックタスクをユーザーにアサインして、フィードバックタスクが対処され、関連するナレッジ記事が更新されるようにします。

始める前に

必要なロール:knowledge_manager

手順

1. 移動先 すべて > **Industrial Workspace** (産業用ワークスペース).
2. ナレッジモジュールのリストビューで、[未アサインの OT ナレッジギャップ] リストを開きます。
3. ユーザーまたはアサイン先グループにアサインするフィードバックタスクを選択します。
4. [アサイン先] フィールドで、フィードバックタスクをアサインするユーザーを追加します。
5. [保存] を選択します。

タスクの結果

これで、アサインされたユーザーは、ナレッジモジュールリストビューの [自分のフィードバックタスク] リストでフィードバックタスクを表示できるようになります。

他のアサイン済みフィードバックタスクを表示するには、産業用 ワークスペースのナレッジモジュールリストビューの下にある [アサイン済みフィードバックタスク] リストを選択します。

未アサインの OT ナレッジギャップを表示するには、産業用 ワークスペースの [ナレッジモジュール] リストビューの下にある [未アサインの OT ナレッジギャップ] リストを選択します。

OT インシデントの関連ナレッジ記事で情報を検索する

オペレーショナルテクノロジー (OT) インシデントレコードに添付されている関連するナレッジ記事で、適用可能な以前の解決策に関する情報を検索します。

始める前に

必要なロール:sn_ot_incident_read

i 注:

sn_ot_incident_readロールと、このインシデントのコンテキストに一致する記事を含むナレッジベースへの読み取りアクセス権が必要です。

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース).
2. OT インシデントモジュールのリストビューで、利用可能なリストを開きます。
3. 表示するインシデントレコードを選択します。
4. インシデントレコードで、[エージェントアシスト] ボタン  をクリックして、[エージェントアシスト] ウィンドウを開きます (まだ開いていない場合)。
5. ナレッジ記事全体を表示するには、[その他のアクション] ボタン  を
6. [全画面表示] を選択します。
7. オプション: オープンインシデントレコードにナレッジ記事を添付するには、[エージェントアシスト] ウィンドウで [添付] を選択します。
8. オプション: ナレッジ記事にフラグを設定するには、[エージェントアシスト] ウィンドウで [フラグ] を選択します。
9. オプション: ナレッジ記事を役に立つとマークするには、[その他のアクション] ボタン  を選択し、[役に立つ] を選択します。

オペレーショナルテクノロジーのナレッジ管理 参照

参照トピックには、オペレーショナルテクノロジーのナレッジ管理に関する追加情報が記載されています。

オペレーショナルテクノロジーのナレッジ管理 ロール

ナレッジ管理ロールをオペレーショナルテクノロジーのナレッジ管理ユーザーにアサインできます。

次の表に、ユーザーがオペレーショナルテクノロジーのナレッジ管理機能にアクセスできるようにユーザーにアサインできるナレッジ管理ロールを示します。

ナレッジ管理 適用可能なロール オペレーショナルテクノロジーのナレッジ管理

ロール	説明
knowledge	ナレッジロールは、デフォルトのナレッジベースに寄稿したり、ナレッジアプリケーションメニューにアクセスしたりできます。ナレッジロールは履行者ロールであり、要求者ロールではありません。 i 注: 要求者は、ナレッジ記事を表示したり、コメントしたり、フィードバックを提供したりすることができます。ただし、要求者は記事を作成または編集することはできません。

ナレッジ管理 適用可能なロール オペレーショナルテクノロジーのナレッジ管理 (続く)

ロール	説明
knowledge_manager	ナレッジマネージャーは、カテゴリの定義、重要な記事の固定、記事への変更の承認など、管理するナレッジベースの管理機能を実行できます。ナレッジベースのマネージャーとして選択されたユーザーは、このロールを自動的に受け取ります。 i 注: knowledge ロールは従属ロールとして提供されます。
knowledge_admin	ナレッジアドミニストレーターは、ナレッジ管理 システムの保守に関連するすべての管理タスクを実行できます。 i 注: - ナレッジアドミンとして選択されたユーザーは、スコープ付きナレッジベースを除くすべてのナレッジベースを変更できます。 - knowledge ロールは従属ロールとして提供されます。

ナレッジベース フォーム

新しいナレッジベースを作成するときは、次のフォームフィールドに入力します。

ナレッジベースフォームのフィールド

Field (フィールド)	説明
タイトル	OT ナレッジベースの一意の名前。
Article Validity (記事の有効期間)	記事が作成された日からのデフォルトの有効日数。
アイコン	OT ナレッジベースを説明する視覚的参照を提供する画像。画像は、記事検索結果ページで、このナレッジベースのすべての記事の横に表示されます。
コメントの無効化	コメントを無効化するオプション。選択すると、ユーザーは OT ナレッジベースの記事にコメントできなくなります。
提案の無効化	編集の提案を無効にするオプション。選択すると、ユーザーは OT ナレッジベースの記事の編集を提案できなくなります。
Disable category editing (カテゴリ編集の無効化)	OT ナレッジカテゴリの編集を無効にするオプション。選択すると、OT ナレッジマネージャー

ナレッジベースフォームのフィールド (続く)

Field (フィールド)	説明
	のみが OT ナレッジベースのナレッジカテゴリを追加または編集できます。
Disable rating (評価を無効化)	記事の評価を無効にするオプション。選択すると、ユーザーは OT ナレッジベースの記事を評価できません。
Disable mark as helpful (役に立つとマークするオプションを無効化)	役に立つとマークを無効にするオプション。選択すると、ユーザーは OT ナレッジベースの記事を役に立つとマークできなくなります。
Enable blocks (ブロックを有効化)	ナレッジブロック機能を有効にするオプション。選択すると、OT ナレッジベース内のナレッジ記事に追加するナレッジブロックを作成できます。
Checklist (チェックリスト)	OT ナレッジベースの記事の品質を評価するためのチェックリスト。
アプリケーション	OT ナレッジベースのアプリケーションスコープ。
所有者	OT ナレッジベースを担当するユーザー。ナレッジベースの所有者は、他のロールをナレッジベースにアサインできます。
マネージャー	OT ナレッジベースで管理機能を実行するユーザー。
公開用ワークフロー	ナレッジベースで記事を公開するためのワークフロー: • [ナレッジ - すぐに公開]:承認を要求せずにナレッジベースに記事を公開します。 • ナレッジ - 公開承認:記事を公開ステータスに移行する前に、ナレッジベースのマネージャーからの承認を要求します。
廃止用ワークフロー	OT ナレッジベースの記事を廃止するためのワークフロー: • ナレッジ - すぐに廃止:承認を要求せずにナレッジベースの記事を廃止します。 • [ナレッジ - 廃止承認 (Knowledge - Approval Retire)]:記事を廃止ステータスに移行する前に、ナレッジベースのマネージャーからの承認を要求します。
アクティブ	OT ナレッジベースがアクティブであることを示すオプション。選択しない場合、admin ロールを持つユーザーまたはナレッジアドミニストレーターのみが記事を作成、検索、または表示できます。
Description (説明)	

ナレッジベースフォームのフィールド (続く)

Field (フィールド)	説明
Set default knowledge field values (デフォルトのナレッジ フィールド値の設定)	OT ナレッジベースのデフォルトの構成設定。
関連製品	OT ナレッジベースコンテンツに関連する製品のリスト。

関連情報

OT 拡張クラスと関連アプリケーションに関する詳細情報を確認してください。

概要

拡張クラスは、オペレーショナルテクノロジー管理構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

[Operational Technology \(OT\) extension classes](#)

CMDBは OT のクラスを更新します。

関連アプリケーション

[Knowledge Management](#)

ナレッジ管理 アプリケーションを使用すると、ナレッジベースで情報を共有できます。これらのナレッジベースには、セルフヘルプ、トラブルシューティング、およびタスク解決などの情報をユーザーに提供する記事が含まれています。

[オペレーショナルテクノロジーインシデント管理](#)

オペレーショナルテクノロジーインシデント管理アプリケーションを使用すると、メーカーはインシデントがオープンされてから完了するまで、OT デバイスインシデントを管理できます。

[IT Service Management](#)

ServiceNow IT Service Management アプリケーションを オペレーショナルテクノロジーのナレッジ管理 と統合すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

オペレーショナルテクノロジー要求管理

オペレーショナルテクノロジー要求管理 では、カタログアイテムを要求し、定義されたフローに基づいてカタログアイテムを履行できます。



オペレーショナルテクノロジー要求管理 の探索

オペレーショナルテクノロジー要求管理 を使用すると、オペレーショナルテクノロジー (OT) サービスカタログにアクセスして OT カタログアイテムを要求し、定義されたフローに基づいてそれらを履行できます。OT ワーカーはカタログアイテムから OT 要求を作成して送信できます。これにより、一貫したエクスペリエンスが提供され、部門横断型の要求が容易になります。

オペレーショナルテクノロジー要求管理のメリット

オペレーショナルテクノロジー要求管理を使用すると、OT システムに次のメリットを適用し、チームがカタログ要求を管理するのに役立ちます。

- 複数のカタログ要求を効率的に管理するための単一のビューを提供します。
- 透明性を高め、要求プロセスを迅速化し、自動通知と承認によって遅延を最小限に抑えます。
- カatalog要求の作成と更新に使用できる製品とサービスのメニューを管理します。

OT システムへの オペレーショナルテクノロジー要求管理の適用

オペレーショナルテクノロジー (OT) システムにオペレーショナルテクノロジー要求管理を適用して、他のユーザーが OT 製品やサービスの OT 要求を作成および送信できるようにすることができます。

概要

オペレーショナルテクノロジー要求管理では、カタログアイテムを要求し、定義されたフローに基づいてカタログアイテムを履行できます。OT ワーカーは OT サービスカタログで要求を作成し、ニーズに最も適したカタログアイテムを選択できます。

ユースケース

次の表では、さまざまな OT ペルソナと、それらが オペレーショナルテクノロジー要求管理 をどのように使用できるかを示しています。

オペレーショナルテクノロジー要求管理のユースケース

ペルソナ	Description (説明)
OT エンジニア	オペレーショナルテクノロジー要求管理を使用して、さまざまな OT 製品やサービスの OT 要求を 1 か所で提出および管理できます。 要求できるカタログアイテムの例としては、サードパーティのリモートアクセス、新しい OT PC、新しい OT デバイス、新しい OT ホスト接続などがあります。
工場長またはスーパーバイザー	オペレーショナルテクノロジー要求管理を使用して適切なチームと連携し、工場フロアで報告されたインシデントを修復できます。

オペレーショナルテクノロジー要求管理の構成

オペレーショナルテクノロジー (OT) ソリューションのデータ基盤を作成できるようにオペレーショナルテクノロジー要求管理を構成します。

admin ロールを持っている場合は、ガイド付きセットアップを使用してオペレーショナルテクノロジー要求管理のセットアップを指示できます。ガイド付きセットアップは、アプリケーションまたは機能の構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

ガイド付きセットアップにアクセスするには、産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表に、ガイド付きセットアップ タスクとその オペレーショナルテクノロジー要求管理目的を示します。

i 注:

オペレーショナルテクノロジー要求管理 は Industrial Workspace Common に含まれていません。追加で必要なロールはありません。

次の表は、セットアップと構成を正しく行うためにユーザーが完了する必要があるタスクを示しています。

オペレーショナルテクノロジー要求管理セットアップタスク

タスク	目的
デモデータをロードします。	オペレーショナルテクノロジー要求管理用のデモデータをロードするには、Industrial Workspace Common プラグインのデモデータをロードする必要があります。デモデータをロードするには、次の手順を実行します。 1. 移動先 すべて > システム定義 > プラグイン。 2. 検索バーで、Industrial Workspace Common プラグインを検索します。 3. 結果がロードされたら、[Installed (インストール済み)] タブを選択し、[Industrial Workspace Common (産業用ワークスペース 共通)] ページを開きます。 4. クイックアクション で、デモデータのロードを選択します。
オペレーショナルテクノロジー要求管理 ロールをアサインします。	ロールを割り当てて、各ユーザーが使用できるアクションを制御します。
カタログビルダーを使用して、OT サービスカタログのカタログアイテムを作成します。	カタログビルダーを使用して OT サービスカタログのカタログアイテムを作成し、他のユーザーが OT 要求を送信してニーズに最適なカタログアイテムを選択できるようにします。
OT サービスカタログで作成したカタログアイテムのカタログアイテムカテゴリを追加します。	OT サービスカタログで作成するカタログアイテムのさまざまなカテゴリを選択して、OT カatalogアイテムを論理グループに整理します。
ワークフロースタジオ で OT 要求の実行フローを作成します。	OT 要求を履行するために、必要に応じてカタログアイテムの ワークフロースタジオ カタログタスクを含む実行フローを作成します。

オペレーショナルテクノロジー要求管理ユーザーへのロールのアサイン

ユーザーにロールをアサインして、オペレーショナルテクノロジー要求管理の機能やデータへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

ユーザーに割り当てることができる オペレーショナルテクノロジー要求管理 ロールの詳細については、「[オペレーショナルテクノロジー要求管理とともにインストールされるコンポーネント](#)」を参照してください。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

カタログアイテムカテゴリ

オペレーショナルテクノロジー (OT) サービスカタログで作成するカタログアイテムには、さまざまなカテゴリを選択できます。カテゴリは、OT カatalogアイテムを論理グループに整理するのに役立ちます。要求者が OT 要求を送信するときに、指定されたカテゴリに基づいてニーズに最適なカタログアイテムを選択できます。

必要に応じて、カテゴリとサブカテゴリを定義して OT カatalogアイテムを整理し、ユーザーが必要な製品やサービスを見つけられるようにすることができます。カタログアイテムカテゴリを定義する方法の詳細については、「[Create a category](#)」を参照してください。

オペレーショナルテクノロジー サービスカタログのカタログアイテムを作成する

カタログビルダーを使用して オペレーショナルテクノロジー (OT) サービスカタログのカタログアイテムを作成し、他のユーザーがカタログアイテム別に分類された OT 要求を送信できるようにします。

始める前に

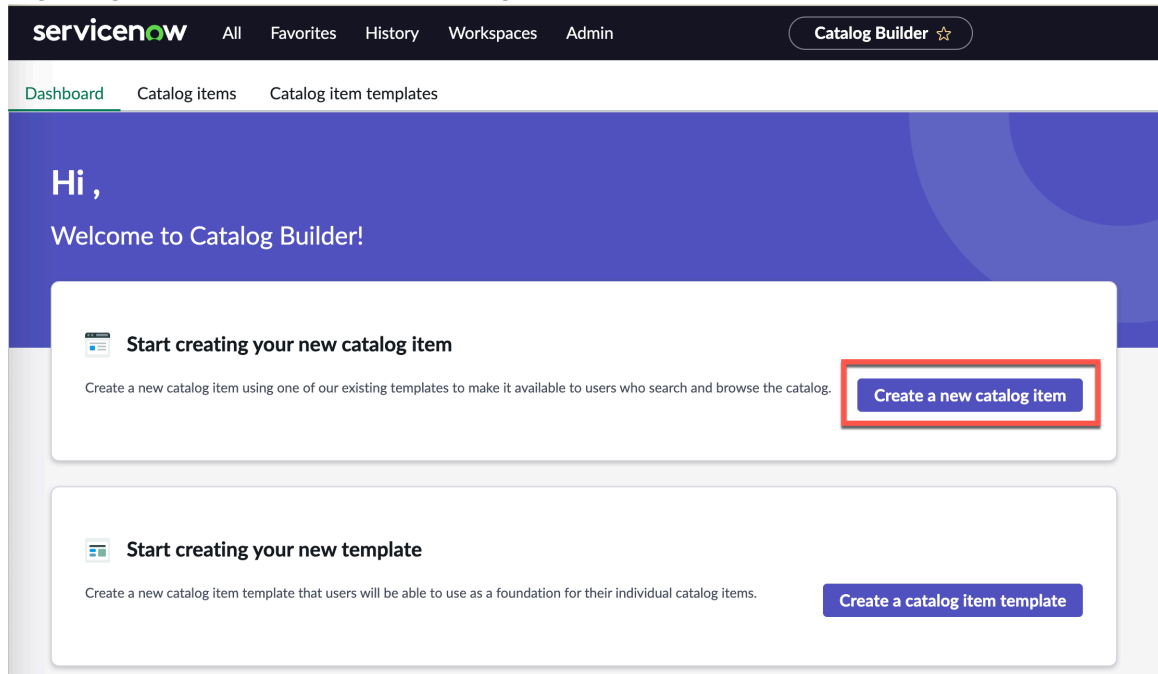
必要なロール：admin

このタスクについて

カタログビルダーで OT サービスカタログのカタログアイテムを作成できます。他のユーザーが OT 要求を送信するときに、ニーズに最適なカタログアイテムを選択できます。たとえば、OT デバイスへのリモートアクセスの要求は、OT サービスカタログで利用可能なカタログアイテムにすることができます。これにより、サードパーティは OT デバイスに関連する問題に取り組むことができます。

手順

1. 移動先 **すべて** > **サービスカタログ** > **カタログビルダー**。
2. [**ダッシュボード**] タブの [**新しいカタログアイテムの作成を開始**] で、[**新しいカタログアイテムの作成**] を選択しま



す。

または、[**カタログアイテム**] タブを選択して [**新規**] をクリックします。

3. [**はじめに**] ページで、[**続行**] を選択します。
4. [**Select your item template** (アイテムテンプレートを選択)] ページで、[**OT Catalog Item Template** (OT カatalogアイテムテンプレート)] を選択します。
5. [**Use this item template**] をクリックします。
6. [**カタログアイテムを作成**] フォームで、フィールドに入力します。

カタログアイテムフォームフィールドの詳細については、「[オペレーショナルテクノロジー カatalogアイテムフォーム](#)」を参照してください。

i 注:

[質問] セクションから OT カatalogアイテム変数セットを削除することはできません。OT カatalogアイテム変数セットは、OT 要求を他の要求と区別するものです。代わりに、[**Insert New Question** (新しい質問の挿入)] を選択することで、アイテムフォームの新しい質問を作成できます。新しい質問の挿入の詳細については、「[Create a question for a catalog item in Catalog Builder](#)」を参照してください。

7. オプション: カatalogアイテムをプレビューするには、[**プレビュー**] を選択します。
8. オプション: 進行状況を保存するには、[**保存**] を選択します。
9. [**Review and Submit** (確認と送信)] セクションが表示されたら、追加したカタログアイテム情報を確認して [**Submit** (送信)] を選択します。
10. 作成するカタログアイテムごとに手順 1 から 9 を繰り返します。

タスクの結果

カタログアイテムが作成され、他のユーザーが OT サービスカタログで OT 要求を作成するときに選択できるようになります。

オペレーショナルテクノロジー要求の実行フローの作成

オペレーショナルテクノロジー (OT) 要求を実行するために、必要に応じてカタログアイテムのワークフロースタジオカタログタスクを含む実行フローを作成します。

始める前に

必要なロール：admin

このタスクについて

実行フローをカタログアイテムにリンクできます。履行フローは、別のユーザーが OT 要求を送信したときにカタログタスクの作成と通知をトリガーします。

手順

1. 移動先 **すべて > プロセスの自動化 > Flow Designer**.
2. [フロー] ボタンを選択します。
3. [新規] ドロップダウンで [フロー] を選択します。
4. [プロパティ] フォームのフィールドに入力します。
プロパティフォームの詳細については、「[Create a flow in Workflow Studio](#)」を参照してください。
5. [フローを構築] を選択します。
6. フローにトリガーを追加します。
詳細については、「[Create a flow in Workflow Studio](#)」を参照してください。
7. アクション、フロー、サブフロー、またはグローロジックを追加します。
詳細については、「[Create a flow in Workflow Studio](#)」を参照してください。
8. [保存] を選択します。

タスクの結果

ワークフロースタジオ 実行フローのフロー、トリガー、およびアクションのドラフトを保存します。実行フローを選択してカタログアイテムに適用できるようになりました。

オペレーショナルテクノロジー要求管理の使用

オペレーショナルテクノロジー要求管理に必要なすべてのセットアップタスクを完了すると、ユーザーはオペレーショナルテクノロジー (OT) 要求の作成と管理を開始できます。

での オペレーショナルテクノロジー 要求の作成 産業用 ワークスペース

産業用 ワークスペース で オペレーショナルテクノロジー (OT) 要求を作成し、OT デバイスまたはインシデントに必要な製品またはサービスに対処します。

始める前に

必要なロール:任意の OT ユーザー

手順

1. 移動先 **すべて > Industrial Workspace (産業用ワークスペース)**.
2. 産業用 ワークスペースリストビューを開きます。
3. **[OT 要求]** リストモジュールで、[自分の要求] リストを選択します。

i 注:

[My Requests (自分の要求)] リストには、産業用 ワークスペースにアクセスできるすべての OT ユーザーがアクセスできます。

4. [新規] を選択します。
5. OT サービスカタログで、ニーズに最適な利用可能なカタログアイテムを 1 つ選択します。
6. 要求に応じて、フィールドに入力します。
7. [要求] を選択します。

次のタスク

OT 要求が送信されると、要求の詳細が記載されたメールが届きます。メールに記載されているリンクを使用して要求レコードを開き、そのステータスを追跡できます。要求を完了するために必要な追加のコンテキストを使用して、要求レコードを編集することもできます。

要求レコードに変更がある場合は、変更内容が記載されたメールで通知されます。たとえば、作業メモがレコードに追加された場合や、レコードのステータスが更新された場合などです。

オペレーショナルテクノロジー要求管理 リスト内の 産業用 ワークスペース

オペレーショナルテクノロジー (OT) 要求とカタログタスクは、産業用 ワークスペースリストビューで表示できます。

OT 要求

次のリストは、**[OT 要求]** モジュールの **[産業用 ワークスペース リスト]** ビューで OT 要求を表示してアクセスするために使用できます。

i 注:

これらのリストにアクセスするには、sn_request_read ロールが必要です。

OT 要求リスト

リスト	Description (説明)
自分の要求	ユーザーまたはアドミニストレーターがユーザーに代わって作成した OT 要求。
オープン中の要求アイテム	すべての OT 要求

OT カatalogタスク

OT カatalogタスクは、**[OT タスク]** モジュールで利用可能なリストで表示できます。OT カatalogタスクの場合、**[タスクタイプ]** 列の値は **[カatalogタスク]** です。

オペレーショナルテクノロジー要求管理 参照

参照トピックには、オペレーショナルテクノロジー要求管理に関する追加情報が記載されています。

オペレーショナルテクノロジー要求管理とともにインストールされるコンポーネント

オペレーショナルテクノロジー要求管理 を有効にすると、ユーザーロールやサービスカタログなど、いくつかのタイプのコンポーネントをインストールできます。

インストールされるロール

オペレーショナルテクノロジー要求管理のロール

名前	説明	ロールを含む
sn_request_read	要求 (sc_request)、要求アイテム (sc_req_item)、またはカタログタスク (sc_task) への読み取りアクセス。	NA
sn_request_write	要求 (sc_request、)、要求アイテム (sc_req_item)、またはカタログタスク (sc_task) への書き込みアクセス。	• task_editor • dependency_views • agent_workspace_user • view_changer • cmdb_read • cmdb_query_builder_read • sn_request_read
sn_request_comment_write	要求アイテム (sc_req_item) のコメントへの書き込みアクセス。 i 注: sn_request_comment_write ロールだけではコメントの書き込みアクセス権が付与されないため、テーブルへの書き込みアクセス権が必要です。	NA

インストールされたサービスカタログ

オペレーショナルテクノロジー要求管理サービスカタログ

名前	Description (説明)
OT サービスカタログ	ユーザーが OT 要求を送信するために提供されるサービスカタログ。

オペレーショナルテクノロジー カatalogアイテムフォーム

オペレーショナルテクノロジー (OT) サービスカタログの新しいカタログアイテムを作成するときは、次のフォームフィールドに入力します。

次の表では、OT カatalogアイテムフォームの各セクションで利用可能なフィールドについて説明します。

詳細

フィールド	Description (説明)
Basic Info (基本情報)	
アイテム名	カタログに表示される名前。
簡単な説明	サービスカタログホームページ、検索結果、注文フォームのタイトルバーに表示されるテキスト。
Item details (アイテムの詳細)	
画像	アイテムの画像。
Description (説明)	アイテムの完全な説明。この説明は、ユーザーがアイテムを選択するか、関連するプレビューリンクをクリックしたときにカタログに表示されます。 ビデオ、画像、社内ナレッジベース (KB) 記事へのリンク、外部情報源や指示書へのリンクを埋め込むことができます。

Location (ロケーション)

フィールド	Description (説明)
カタログ	
選択されているカタログ	このアイテムが表示されるカタログ。
カテゴリ	
選択されたカテゴリ	アイテムのカテゴリ。カテゴリは、[カタログ] フィールドの入力後にのみ選択できます。 カタログ検索では、サービスポータルのカテゴリに割り当てられたアイテムのみが検索されます。
トピック	
選択されたトピック	アイテムのトピック。カタログアイテムが公開されたら、要求者は追加したトピックを使用してカタログアイテムを検索し、アクセスすることができます。

質問

フィールド	Description (説明)
OT カatalogアイテム変数セット	
サイト	カタログアイテムの影響を受けるサイト。

設定

フィールド	Description (説明)
ポータルの設定	
送信ボタンラベル	要求者がカタログアイテムフォームへの入力を完了した後の [送信] ボタンのラベル。
[カートに追加] ボタンを非表示	選択すると、アイテムに [カートに追加] ボタンが表示されません。ウィジェットの [カートに追加を表示する] インスタンスオプションが false に設定されている場合、この設定は無視されます。 この設定は、[要求の方法] が [要求] または [送信] の場合はデフォルトで選択されています。 アップグレードシナリオでは、プラットフォームで [カートなし] フィールドが選択されている場合は、CatalogPortalSettingsMigration スクリプトインクルードを実行して、この設定を [ポータル設定] タブの [カートに追加] フィールドを非表示にします。 i 注: カタログアイテムと注文ガイドに適用されます。
[下書きとして保存する] ボタンを非表示	選択すると、アイテムに [ドラフトとして保存] ボタンが表示されません。
数量セクターを非表示	選択すると、カタログアイテムに [量] リストが表示されません。 これは、[要求の方法] が [要求] または [送信] の場合はデフォルトで選択されています。 アップグレードのお客様の場合、プラットフォームで [数量なし] フィールドが選択されている場合は、CatalogPortalSettingsMigration 移行スクリプトを実行して、この設定を [ポータル設定] タブの [数量を非表示にする] フィールドに更新します。 i 注: カタログアイテムに適用されます。 注文ガイドは、含まれているカタログアイテムからこの設定を継承します。
配送時間を非表示	選択すると、カタログアイテムに [配送時間] フィールドが表示されません。 これは、[要求の方法] が [送信] の場合はデフォルトで選択されています。

設定 (続く)

フィールド	Description (説明)
	i 注: カタログアイテムに適用されます。 注文ガイドは、含まれているカタログアイテムからこの設定を継承します。
[添付ファイル] ボタンを非表示	選択すると、カタログアイテムに [添付ファイルを追加] ボタンが表示されません。 i 注: カタログアイテムとレコードプロデューサーに適用されます。 注文ガイドは、含まれているカタログアイテムからこの設定を継承します。
添付を必須に設定	選択すると、カタログアイテムに添付ファイルを追加することが必須になります。 i 注: カタログアイテムとレコードプロデューサーに適用されます。

アクセス

フィールド	説明
利用可能 (Available for)	
アクセスを許可するユーザー基準	カタログアイテムにアクセスできるユーザー基準を選択します。
利用不可	
アクセスを拒否するユーザー基準	カタログアイテムにアクセスできないユーザー基準を選択します。

達成

フィールド	Description (説明)
実行方法	
プロセスエンジン	アイテム要求履行の順序。
選択されたフロー	アイテム要求の実行方法を定義するフロー。 i 注: このフィールドは、[プロセスエンジン] フィールドで [フローデザイナーフロー] を選択した場合にのみ表示されます。

達成 (続く)

フィールド	Description (説明)
選択したワークフロー	アイテム要求の実行方法を定義するワークフロー。 i 注: このフィールドは、[プロセスエンジン] フィールドで [ワークフロー] を選択した場合にのみ表示されます。

関連情報

オペレーショナルテクノロジー (OT) 拡張クラスと関連アプリケーションの詳細を確認してください。

概要

拡張クラスは、オペレーショナルテクノロジー管理構成管理データベース (CMDB)でどのように機能するかを理解するのに役立ちます。

[Operational Technology \(OT\) extension classes](#)

CMDBは OT のクラスを更新します。

関連アプリケーション

[Request Management](#)

要求管理を使用すると、定義されたフローに基づいてカタログアイテムを要求して実行できます。

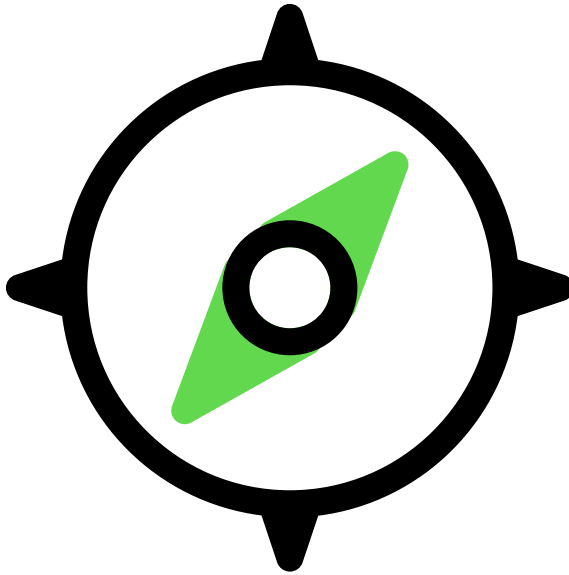
[IT Service Management](#)

ServiceNow IT Service Management アプリケーションを使用すると、エンジニアは OT デバイスと本番プロセスの問題を迅速に解決できます。

産業用 ワークスペース

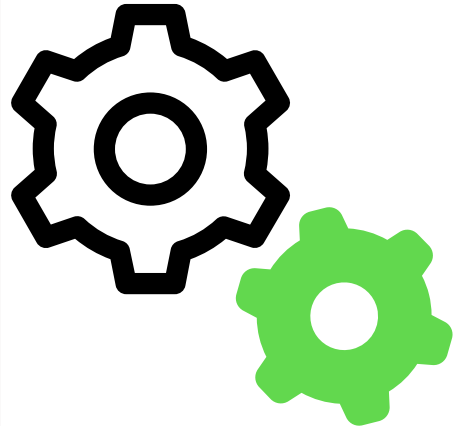
産業用 ワークスペース は、オペレーショナルテクノロジー (OT) ユーザーが OT データを管理するために必要なツールを提供するユーザーインターフェイスです。

探索



産業用ワークスペースの探索

Configure (構成)



実装の計画と構成

使用



Industrial Workspace の使用

自動翻訳

産業用ワークスペースの探索

産業用 ワークスペース は、オペレーショナルテクノロジー (OT) ユーザーが OT データを管理するために必要なツールを提供するユーザーインターフェイスです。

産業用 ワークスペース 航法

産業用 ワークスペースは次のページに分かれています。

産業用 ワークスペースページ

ページ	Description (説明)
OT アクション指向ランディングページ	ホーム (🏠) アイコンを選択すると、OT アクション指向ランディングページに移動します。ランディングページは、OT ネットワークに関連する重要なタスクを追跡するのに役立ちます。
OT マネージャーダッシュボード	OT マネージャーダッシュボード (📊) アイコンを選択すると、 [OT デバイス] タブと [OT 脆弱性] タブを含む OT マネージャーダッシュボードに移動します。OT マネージャーダッシュボードでは、OT デバイスと脆弱性一致アイテムに関連するデータを表示できます。
OTVR (PA) ダッシュボード	ダッシュボード (📊) アイコンを選択すると、オペレーショナルテクノロジー脆弱性対応 (OTVR) PA ダッシュボードに移動します。OTVR (PA) ダッシュボードは、OT 脆弱性一致アイテムのボリューム、パフォーマンス、および初期分析と検出から封じ込めまたは修復までの進捗状況を追跡します。
OT 進捗状況スコアカード	OT 進捗スコアカード (📊) アイコンを選択すると、OT 進捗スコアカードに移動します。OT 進捗状況スコアカードを使用すると、サイトデータを 1 つのビューで比較できます。
Industrial Workspace リストビュー	リスト (📋) アイコンを選択すると、産業用ワークスペースリストビューに移動し、OT データレコードに関連するすべてのリストにアクセスできます。次のリストモジュールとそれ以降のリストにアクセスできます。 • オペレーショナルテクノロジー (OT) • 情報技術 (IT) ハードウェア • 産業用プロセスマネージャー • OT インシデント • OT 変更要求 • OT 修復タスク • OT 脆弱性一致アイテム • OT タスク • ナレッジ

産業用 ワークスペースページ (続く)

ページ	Description (説明)
機器モデルマネージャー	機器モデル () アイコンを選択すると、機器モデルマネージャーに移動し、サイトとその機器モデルデータを表示できます。

オペレーショナルテクノロジー アクション指向のランディングページ

オペレーショナルテクノロジー (OT) アクション指向ランディングページを使用して、OT ネットワークに関連する重要なタスクを追跡できます。

概要

OT アクション指向ランディングページは、OT エンジニアなどのユーザーが、自分、自分のサイト、またはグループにアサインされたタスクを表示するのに役立ちます。ランディングページには、サインインしているユーザーが優先する必要がある重要なアクションが呼び出され、既存の OT インシデント、OT 変更要求、OT 修復タスク、OT 脆弱性一致アイテム、およびその他のタスクの概要が含まれています。

ランディングページには、日常のタスクと重要なアクションの詳細ビューが表示されます。[重要なアクション] セクションの各タスクには、作成日順にソートされたタスクが表示されます。タスクが重要な場合は、[重要なアクション] セクションに表示されます。

OT アクション指向ランディングページにアクセスするには、すべて > **Industrial Workspace** (産業用ワークスペース) をクリックし、ホーム () アイコンを選択します。

ランディングページのコンテンツ

次のセクションでは、OT アクション指向ランディングページで表示できるコンテンツについて説明します。

重要なアクション

[重要なアクション] セクションには、重要と見なされ、できるだけ早く対処する必要がある OT タスクまたはアクションが含まれています。タスクは 作成日 順に整理され、サインインしているユーザーにアサインされた、最近作成された重要なタスクが最初に表示されます。

このセクションに表示されるタスクは、[概要] セクションからブルされた、アクションを実行できる最も重要なタスクです。タスクの重要度は、次の基準によって決定されます。

- その優先度は「重大」です
- タスクが修復タスクであり、そのリスク評価が重大である。

このセクションに含まれるタスクは、次のように編成されています。

- サインインしているユーザーに直接割り当てられているすべてのタスクが最初に表示されます。
- ユーザーのグループにアサインされ、どのユーザーにもアサインされていないタスクが後に表示されます。
- グループまたはユーザーに割り当てられていないが、サインインしているユーザーがアクセスできるサイトに割り当てられているタスクは、最後に表示されます。

概要

[Overview (概要)] セクションには、OT インシデント、変更要求、修復タスク、脆弱性一致アイテム、およびユーザー、自分のグループ、またはサイトにアサインされたその他のタスクの概要が含まれています。

次のフィルターを使用して、レコードの [アサイン先]、[アサイン先グループ]、および [サイト] フィールドに基づいて表示されるレコードを表示できます。

あなたの仕事

自分にアサインされたレコード。

グループの作業

自分のグループにアサインされたレコード。

サイトの作業

自分のサイトにアサインされたレコード。

次の表では、[概要] セクションのタイルについて説明します。

概要タイル

タイル	Description (説明)
あなたにアサインされた OT インシデント/グループにアサインされた OT インシデント/サイトにアサインされた OT インシデント	自分、自分のアサイン先グループ、またはサイトのいずれかにアサインされた OT インシデントレコードの数。 すべての OT インシデントレコードのリストを表示するには、[すべてのレコード] を選択します。 ステータスまたはタイプに基づいてレコードのリストのみを表示するには、利用可能なグラフのそれぞれのセクションを選択します。たとえば、優先度に基づいてインシデントレコードのみを表示する場合は、グラフの [重大] セクションを選択します。
あなたにアサインされた OT 変更要求 / グループにアサインされた OT 変更要求 / サイトにアサインされた OT 変更要求	自分、自分のアサイン先グループ、またはサイトのいずれかにアサインされた OT 変更要求レコードの数。 すべての OT 変更要求レコードのリストを表示するには、[すべてのレコード] を選択します。 ステータスに基づいてレコードのリストのみを表示するには、利用可能なグラフの該当するセクションを選択します。たとえば、スケジュールされている変更要求レコードのみを表示する場合は、グラフの [スケジュール済み] セクションを選択します。
あなたにアサインされた OT 修復タスク / グループにアサインされた OT 修復タスク / サイトにアサインされた OT 修復タスク	自分、自分のアサイン先グループ、またはサイトのいずれかにアサインされた OT 修復タスクレコードの数。 すべての OT 修復タスクレコードのリストを表示するには、[すべてのレコード] を選択します。 ステータスに基づいてレコードのリストのみを表示するには、利用可能なグラフの該当するセクションを選択します。たとえば、レビュー中の修復タスクレコードのみを表示する場合は、グラフの [レビュー中] セクションを選択します。
自分にアサインされた OT 脆弱性一致アイテム / グループにアサインされた OT 脆弱性一致アイテム	自分、自分のアサイン先グループ、またはサイトのいずれかにアサインされた OT 脆弱性一致アイテムレコードの数。

概要タイル (続く)

タイル	Description (説明)
れた OT 脆弱性一致アイテム / サイトにアサインされた OT 脆弱性一致アイテム	すべての OT 脆弱性一致アイテムレコードのリストを表示するには、[すべてのレコード] を選択します。 リスク評価に基づいてレコードリストのみを表示するには、利用可能なグラフの該当するセクションを選択します。たとえば、優先度の高い脆弱性一致アイテムレコードのみを表示する場合は、グラフの [高] セクションを選択します。
あなたにアサインされたその他の OT タスク / グループにアサインされたその他の OT タスク / サイトにアサインされたその他の OT タスク	自分、アサイン先グループ、またはサイトのいずれかにアサインされた他の OT タスクレコードの数。 他のすべての OT タスクレコードのリストを表示するには、[すべてのレコード] を選択します。 優先度に基づいてレコードリストのみを表示するには、利用可能なグラフのそれぞれのセクションを選択します。たとえば、優先度が低いと見なされる OT タスクのみを表示する場合は、グラフの低セクションを選択します。

OT CMDB 健全性

OT CMDB Health は、構成管理データベース (CMDB)内のデバイスの健全性を監視および維持するのに役立ちます。OT デバイスの数をタイプ別に整理して表示できます。

i 注:

このセクションは、オペレーショナルテクノロジーマネージャー がインストールされている場合にのみ表示されます。

次の表では、[OT CMDB 健全性] セクションのタイルについて説明します。

OT CMDB ヘルスタイル

タイル	Description (説明)
未分類の OT デバイス	OT デバイスタイプカテゴリが割り当てられていない OT ネットワーク内の OT デバイスの数。 未分類の OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。
未アサインの OT デバイス	ユーザーにアサインされていない OT ネットワーク内の OT デバイスの数。 未アサインの OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。
マッピングされていない OT デバイス	どのサイトにもマッピングされていない OT ネットワーク内の OT デバイスの数。 マッピングされていない OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。

OT CMDB ヘルスタイル (続く)

タイル	Description (説明)
	i 注: このタイルは、産業用プロセスマネージャー がインストールされていて、サインインしているユーザーが cmdb_ot_isa_viewer ロールを持っている場合にのみ使用できます。このタイルを使用するには、組織に OT デバイスを本番プロセスにマッピングするための機器モデルが必要です。
サイトがアサインされていません	サイトにアサインされていない OT ネットワーク内の OT デバイスの数。 i 注: このタイルは、サインインしているユーザーが cmdb_ot_isa_viewer ロールを持っている場合にのみ使用できます。 サイトのない OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。
IP アドレスなし OT デバイス	IP アドレスが割り当てられていない OT ネットワーク内の OT デバイスの数。 IP アドレスのない OT デバイスレコードのリストを表示するには、[すべてのレコード] を選択します。

オペレーショナルテクノロジーマネージャー ダッシュボード

オペレーショナルテクノロジー (OT) Manager ((OT) マネージャー) ダッシュボードを使用すると、OT デバイスと脆弱性データを一元的に管理できます。OT マネージャーダッシュボードには、[**OT Devices (OT デバイス)**] タブと [**OT Vulnerabilities (OT 脆弱性)**] タブがあり、それぞれのデータの整理とアクセスが容易になります。

[OT デバイス] タブ

[**OT Devices (OT デバイス)**] タブは、産業用 ワークスペース の OT マネージャーダッシュボードの一元的な場所です。このタブを使用して、オペレーショナルテクノロジーマネージャー および 産業用プロセスマネージャー データを確認できます。これを使用して、OT ネットワーク内の OT デバイスと機器モデルエンティティの詳細情報を確認または編集することもできます。

産業用 ワークスペース の OT マネージャーダッシュボードの [**OT デバイス**] タブでは、次のアクションを実行できます。

- 過去 1 週間に OT ネットワークで OT デバイス情報がどのように変更されたかを把握します。
- 産業施設全体の OT デバイスインベントリの進行状況を表示します。
- OT デバイスを意味のある方法で分析します。たとえば、本番プロセスにマッピングされている本番デバイスの数に関するインサイトを得ることができます。

[OT デバイス] タブの内容

[**OT デバイス**] タブで OT デバイスデータにアクセスするには、すべて > **Industrial Workspace** (産業用ワークスペース)をクリックし、OT マネージャーダッシュボード () アイコンを選択して、[**OT デバイス**] タブを選択します。次の表に記載されているタイルの重要業績評価指標 (KPI) グラフにアクセスするには、タイルの数値、カウント、またはグラフコンポーネントを選択します。

次の表では、[**OT デバイス**] タブのさまざまなタイルに表示される OT デバイスデータについて説明します。

[OT デバイス] タブ

タイル	Description (説明)
過去 7 日間の更新	過去 7 暦日間に OT ネットワークで発生した OT デバイスに関連する重大な変更の数。 i 注: ジョブが正常に実行された場合は、最後のコレクションの終了時刻を示す Last updated: タイムスタンプがあります。 ジョブが失敗した場合は、前回の実行の終了時刻を示す [前回の実行] タイムスタンプがあります。
新しい OT デバイスの検出	過去 7 暦日間に オペレーショナルテクノロジーおよびその他の自動化プロセスのために ディスカバリーによって検出された新しい OT デバイスの数。
非アクティブな OT デバイス	過去 7 暦日間に OT ネットワークに表示されていない OT デバイスの数。これらのデバイスは非アクティブと見なされます。
OT デバイスの概要	OT ネットワーク内の未分類、未アサイン、未マッピングの OT デバイスの数。 i 注: ジョブが正常に実行された場合は、最後のコレクションの終了時刻を示す Last updated: タイムスタンプがあります。 ジョブが失敗した場合は、前回の実行の終了時刻を示す [前回の実行] タイムスタンプがあります。
未分類	OT デバイスタイプカテゴリがアサインされていない OT ネットワーク内の OT デバイスの数。
未アサイン	ユーザーにアサインされていない OT ネットワーク内の OT デバイスの数。
マップ解除	どのサイトにもマッピングされていない OT ネットワーク内の OT デバイスの数。

[OT デバイス] タブ (続く)

タイル	Description (説明)
	i 注: OT デバイスを本番プロセスにマッピングするための機器モデルが組織にある必要があるため、このタイルは 産業用プロセス マネージャー がインストールされている場合にのみ使用できます。
カテゴリ別の OT デバイス	アサインされた OT デバイスタイプクラス別の、OT ネットワーク内の OT デバイスの数。
監督システム	監督システムカテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
コントロールシステム	コントロールシステムカテゴリにアサインされている OT ネットワーク内の OT デバイスの数。 i 注: コントロールモジュールはこの数に含まれていません。
フィールドデバイス	フィールドデバイスカテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
コンピューターとサーバー	[コンピューターとサーバー] カテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
ネットワーク機器	ネットワーク機器カテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
Industrial IoT (産業用 IoT)	産業用モノのインターネット (IoT) カテゴリにアサインされている OT ネットワーク内の OT デバイスの数。
Purdue レベル別の OT デバイス	OT ネットワーク内の OT デバイスの数を、割り当てられた Purdue レベル別に表示する棒グラフ。 i 注: OT システムの Purdue レベルの詳細については、「https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lv1sec10/the-purdue-model-for-industrial-control-systems」を参照してください。
タイプ別の OT デバイス (トップレベル)	OT デバイスタイプ別に OT デバイスデータを分類した棒グラフ。

[OT デバイス] タブ (続く)

タイトル	Description (説明)
メーカー別の OT デバイス (トップレベル)	OT ネットワーク内の OT デバイスの数を、アサインされたメーカー別に示す円グラフ。
重要度別の OT デバイス	OT ネットワーク内の OT デバイスの数を、割り当てられた重要度別に示す円グラフ。

[OT 脆弱性] タブ

[**OT Vulnerabilities (OT 脆弱性)**] タブは、産業用 ワークスペース の OT マネージャーダッシュボードの一元的な場所です。このタブを使用して、オペレーショナルテクノロジー脆弱性対応 アプリケーションからデータを確認できます。また、これを使用して、OT ネットワーク内の OT 脆弱性の詳細情報を確認または編集することもできます。

[**OT 脆弱性**] タブでは、次のアイテムを表示できます。

- 新しい OT 脆弱性一致アイテムの数。
- 対処されていない脆弱性一致アイテム。
- ステータス別に整理された脆弱性一致アイテム。
- リスク評価別に整理された脆弱性一致アイテム。
- 既存の機器モデルエンティティ、脆弱性一致アイテム、およびリスクスコアを示す脆弱性リスクテーブル。

[OT 脆弱性] タブの内容

[**OT 脆弱性**] タブにアクセスするには、すべて > **Industrial Workspace** (産業用ワークスペース)をクリックし、OT マネージャーダッシュボード () アイコンを選択して、[**OT 脆弱性**] タブを選択します。タイトルの重要業績評価指標 (KPI) グラフにアクセスするには、タイトルの数値、カウント、またはグラフコンポーネントを選択します。

次の表では、[**OT 脆弱性**] タブのさまざまなタイトルに表示される情報について説明します。

[OT 脆弱性] タブ

タイトル	Description (説明)
OT 脆弱性概要	OT 脆弱性データを含むセクション。 i 注: ジョブが正常に実行された場合は、最後のコレクションの終了時刻を示す Last updated: タイムスタンプがあります。ジョブが失敗した場合は、前回の実行の終了時刻を示す [前回の実行] タイムスタンプがあります。
新しい OT 脆弱性一致アイテム	システムで見つかった新しい OT 脆弱性一致アイテムの数。
未対応の脆弱性一致アイテム	オープンでユーザーにアサインされていない OT 脆弱性一致アイテムの数。

[OT 脆弱性] タブ (続く)

タイル	Description (説明)
リスク評価別の脆弱性一致アイテム	脆弱性一致アイテムとその重要度をまとめた円グラフ。
ステータス別の脆弱性一致アイテム	すべての脆弱性一致アイテムをステータス別に表示する棒グラフ。対処されている脆弱性の数と、さらに調査が必要な脆弱性の数を解釈できます。たとえば、[調査中] カテゴリが比較的高い場合は、これらの脆弱性一致アイテムに最初に対処することで、これらのアイテムに優先順位を付けることができます。
脆弱性リスク	
機器モデルエンティティ	サイトの機器モデルエンティティとその脆弱性一致アイテムのリスクスコアを表示するテーブル。また、最もリスクの高い領域と脆弱性一致アイテムの数も強調表示されます。
サイトにアサインされた OT デバイスはありますか	どのサイトにもアサインされていない OT デバイスのリスクスコアと脆弱性一致アイテムの数を表示するテーブル

オペレーショナルテクノロジー 進捗状況スコアカード

オペレーショナルテクノロジー (OT) 進捗スコアカードを使用すると、サイト間でデバイスと脆弱性一致アイテムのデータを比較できます。

概要

OT 進捗状況スコアカードは、サイトデータを比較できる 産業用 ワークスペース 内の一元的な場所です。サイトデータには、OT デバイスデータと脆弱性データの両方が含まれます。OT 進捗状況スコアカードを使用すると、サイトの進捗状況を追跡し、注意が必要なサイトを特定できます。

次の オペレーショナルテクノロジー アプリケーションのサイトデータを表示することもできます。

- オペレーショナルテクノロジーマネージャー
- オペレーショナルテクノロジー脆弱性対応
- オペレーショナルテクノロジーインシデント管理
- オペレーショナルテクノロジー変更管理

スコアカードのコンテンツ

OT 進捗状況スコアカードにアクセスするには、すべて > **Industrial Workspace** (産業用ワークスペース) をクリックし、**OT 進捗スコアカード** () アイコンを選択します。

次の表では、OT 進捗スコアカードの各列について説明します。

OT 進捗状況スコアカード列

列	Description (説明)
全体スコア (%)	スコアカードのインジケーターによって決定されるサイトの進捗状況。重み付けを編集して、

OT 進捗状況スコアカード列 (続く)

列	Description (説明)
	インジケーターが全体のスコアにどの程度寄与するかを制御できます。詳細については、「 オペレーショナルテクノロジー進捗スコアカードのシステムプロパティの設定 」を参照してください。
で予想される OT デバイスの割合 CMDB	構成管理データベース (CMDB) に含まれると予想される OT デバイスの割合。 i 注: 値が -1 の場合、[CMDB で予想される OT デバイスの割合 (%)] インジケーターの 1 つ以上の値に、[OTPSC 属性] テーブルの [予想される OT デバイス] 属性がありません。予想される OT デバイスを構成する方法については、「サイトに想定される OT デバイスを構成する」を参照してください。
分類済み OT デバイス (%)	分類された OT デバイスの割合。分類済み OT デバイス (%) には、cmdb_ci_otとして分類された OT デバイスは含まれません。
アサイン済み OT デバイス (%)	次のフィールドに値を持つ OT デバイスの割合: - Assigned to (アサイン先) - Owned by (オーナー) - 管理担当者 - Supported by (サポート担当者) - 承認グループ - 管理対象グループ - サポート担当者 (Support by) - 変更グループ
OT デバイスデータの完全性 (%)	データ目標を達成する OT デバイスの割合。このメトリクスは、CMDB 健全性ダッシュボード - 完全性スコア計算ジョブに依存し、CI クラスマネージャーで必須フィールドと推奨フィールドを設定する必要があります。詳細については、「Set up and configure CMDB Health」を参照してください。 完全性は、次のメトリクスによって決定される KPI です。 必須 必須として定義されたフィールドが入力されていない CI の割合を測定します。欠損フィールドは不完全としてタグ付けされ、この CI の

OT 進捗状況スコアカード列 (続く)

列	Description (説明)
	一部の情報が欠落していることが示されます。 推奨 推奨として設定されているフィールドが入力されていない CI の割合を測定します。 データの完全性の詳細については、CMDB Health KPIs and metrics  i 注: 値が -1 の場合、CMDB 健全性ダッシュボード - 完全性スコア計算ジョブはまだ実行されていません。または、ジョブが未完了ステータスで実行されました。
マッピングされた OT デバイス (%)	機器モデルエンティティにマッピングされた OT デバイスの割合。 i 注: 値が 0 の場合、OT デバイスは見つかりません。
バックアップされた OT デバイス (%)	バックアップレコードが作成された OT デバイスの割合。 i 注: 値が 0 の場合、OT デバイスは見つかりません。
アサインされた OT 脆弱性一致アイテム (%)	クローズも対処もされていない OT 脆弱性一致アイテムの割合。 i 注: 値が 0 の場合、OT デバイスは見つかりません。
承認された OT 変更要求 (%)	送信され承認された OT 変更要求の割合。 i 注: 値が 0 の場合、OT デバイスは見つかりません。
OT コンテキストのある OT インシデント (%)	OT デバイスまたは機器モデルデータを含む OT インシデントの割合。 i 注: 値が 0 の場合、OT デバイスは見つかりません。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード

オペレーショナルテクノロジー (OT) 脆弱性一致アイテム (VI) のボリューム、パフォーマンス、および初期分析と検出から封じ込めや修復までの進捗状況を追跡します。アサイン先グループ、エクспロイト、リスク評価、またはステータスでレポートをフィルタリングして、脆弱性エクスポージャーと影響を受けるサービスに関するインサイトを得ることができます。

必要な オペレーショナルテクノロジー と オペレーショナルテクノロジー脆弱性対応 ロール

このダッシュボードは、cmdb_ot_viewer、cmdb_ot_isa_viewer_all、および sn_vul.remediation_owner ロールを持っている場合に使用できます。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードを表示するには、すべて > **Industrial Workspace** (産業用ワークスペース) をクリックし、ナビゲーションパネルで ダッシュボード (📊) アイコンを選択します。

ユースケース

次の表は、組織内のさまざまなユーザーがこのダッシュボードをどのように使用できるかの例を示しています。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのユースケース

ユーザー	ダッシュボードの使用方法
OT サイトマネージャー、OT アナリスト、脆弱性修復オーナー	最もリスクが高い OT 脆弱性一致アイテムを特定することで、脆弱性の悪用による増加するセキュリティインシデントに組織が対処できるように支援します。このダッシュボードには OT 脆弱性一致アイテムのアクティビティがグラフィカルに表示されるため、修正計画とステータスの進捗状況を設計するのに役立ちます。重要業績評価指標 (KPI) は、影響を受ける重大なデバイスと目立った脆弱性に関連付けられています。

[ダッシュボード] タブ

経時的な傾向データを示すレポートと、リアルタイム データを含むレポートを表示できます。また、重要なメトリクスの傾向を定期的に表示して、ビジネスプロセス全体を分析したり、改善が必要な領域を特定したりすることもできます。

[脆弱性一致アイテム] タブ、[修復] タブ、および [例外] タブの内容について説明します。

[脆弱性一致アイテム] タブ

[脆弱性一致アイテム] タブでは、脆弱性のリスクとそのまん延、影響を受けるデバイス、修復ターゲットへの遵守、および修復の進捗状況を確認できます。

[脆弱性一致アイテム] タブでは、次のレポートを表示できます。

- OT 脆弱性一致アイテム (VI)
- OT 脆弱性構成アイテム (CI)
- OT 修復タスク
- 修正ターゲットを満たした OT VI

i 注:

データは、先月、3 か月単位、6 か月単位、年単位、または全期間で表示できます。

- OT VI 平均修正時間 (MTTR)

i 注:

データは、先月、3 か月単位、6 か月単位、年単位、または全期間で表示できます。

- 期限間近の OT の重大な修復タスク
- 経過時間別の OT VI
- OT クローズ済み修復ターゲットステータス別の脆弱性一致アイテム
- リスク評価別の OT 脆弱性一致アイテム
- アサイン先グループ別の重大な OT 脆弱性一致アイテム
- アサイン先グループ別の期限切れの重大な OT 脆弱性一致アイテム

[修正] タブ

[修正] タブは、修復アクションの進捗状況を把握し、修復アクションの完了に最も支援が必要なサポートチームを確認するのに役立ちます。

[修復] タブでは、次のレポートをリアルタイムで表示できます。

- リスク評価とステータス別の OT 修復タスク
- リスク評価とターゲットステータス別の OT 修復
- 未アサインの OT 修復タスク
- 未アサインの OT 脆弱性一致アイテム
- アサイン先グループ別の OT の重大な修復タスク
- アサイン先グループ別の期限切れの重大な OT 修復タスク

[例外] タブ

[例外] タブは、修復が過度に延期される可能性があるため組織がリスクを負っている場所を把握するのに役立ちます。

[例外] タブでは、次のレポートをリアルタイムで表示できます。

- 理由別の保留された OT 脆弱性一致アイテム
- アサイン先グループ別の重大な脆弱性一致アイテムの OT 例外。

インジケータソース

オペレーショナルテクノロジー脆弱性対応インジケータは、次のソースからデータを収集します。

- OTVI.アクティブ
- OTVI.クローズ済み
- OTRT.アクティブ

ダッシュボードに使用されるインジケータソースの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードのインジケータソースとインジケータ](#)」を参照してください。

インジケータソースから 100 万件を超えるレコードが収集されることが予想される場合は、インジケータソースの [レコード収集] セクションで予想される数を上書きする必要があります。詳細については、「[多数のレコードのインジケータソースを確認する](#)」を参照してください。

インジケータ

オペレーショナルテクノロジー脆弱性対応 アプリケーションでの脆弱性修復の進捗状況を測定および追跡するために、いくつかのインジケータが使用されます。ダッシュボードで使用されるインジケータの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードのインジケータソースとインジケータ](#)」を参照してください。

インジケータの レコード収集 オプションは、オペレーショナルテクノロジー脆弱性対応 アプリケーションではデフォルトで無効になっています。このオプションは、各インジケータに対して大量のデータを収集するときに発生する可能性があるパフォーマンスの問題を回避するためにオフになっています。

ブレイクダウン

ブレイクダウンは、収集されたレコードを定性的属性でフィルタリングしてグループ化します。ダッシュボードのインジケータは、次のように分析されます。

- 経過時間
- クローズした経過時間
- Assignment Group (アサイン先グループ)
- CI マネージャー
- 保留の理由
- エクスプロイト攻撃ベクトル
- エクスプロイト有無
- エクスプロイトスキルレベル
- 修復ターゲットルール
- 修復ターゲットステータス
- 修復ターゲットステータス (クローズ済み)
- リスク評価
- 重大度
- ステータス

ブレイクダウンソースは、ブレイクダウンに含まれる一意の値を指定します。一意の値は、ブレイクダウン要素と呼ばれます。ダッシュボードは、次のブレイクダウンソースを使用します。

- アサイン先グループ
- 保留.理由.未.クローズ
- エクスプロイト攻撃ベクトル
- エクスプロイト有無
- エクスプロイトスキルレベル

- OT 経過時間範囲
- 修復ターゲットステータス
- 修復ターゲットステータス (クローズ済み)
- Remediation.Target.Rule
- リスク評価
- 過酷
- 状態
- Vulnerable.Item.CI.Manager

ブレイクダウンとブレイクダウン ソースの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードのブレイクダウン](#)」を参照してください。

収集ジョブ

ダッシュボードでは、次の収集ジョブを使用して、ダッシュボードに表示される OT 脆弱性データを収集します。

- [PA OT VR]過去の脆弱性データ収集
- [PA OT VR]修復タスクの日次収集
- [PA OT VR]脆弱なアイテムの日次収集 1
- [PA OT VR]脆弱なアイテムの日次収集 2
- [PA OT VR]脆弱な構成アイテム (CI) の日次収集

収集ジョブの詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボード収集ジョブ](#)」を参照してください。

データの可視化

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードでは、データの可視化を使用して OT 脆弱性データを表示します。たとえば、システム内の OT 脆弱性一致アイテムの合計数は、**OT 脆弱性一致アイテム (VI)** ウィジェットに単一スコアで表示されます。

ダッシュボードで使用するデータの可視化の詳細については、「[オペレーショナルテクノロジー脆弱性対応 \(PA\) ダッシュボードで使用するデータの可視化](#)」を参照してください。

の構成 産業用 ワークスペース

オペレーショナルテクノロジー (OT) データを管理できるように産業用 ワークスペースを設定します。

admin ロールを持っている場合は、ガイド付きセットアップを使用して 産業用 ワークスペース のセットアップをガイドできます。ガイド付きセットアップ は、アプリケーションまたは機能の構成を支援するツールです。構成アクティビティをカテゴリに整理します。これらのカテゴリには、セットアップタスクに関する情報、各タスクを完了するための手順、および構成を実行するインスタンス内のページへのリンクが含まれています。役立つヘルプコンテンツへのリンクも提供されます。

ガイド付きセットアップにアクセスするには、産業用ワークスペースアドミン > ガイド付きセットアップ。

次の表に、産業用 ワークスペースのガイド付きセットアップタスクとその目的を示します。

産業用 ワークスペース セットアップタスク

タスク	目的
産業用 ワークスペースロールをアサインします。	産業用 ワークスペースを構成する必要があるユーザーに、産業用ワークスペースの構成 [configure_industrial_workspace] ロールを割り当てます。
ホームページ宛先ルールを確認します。	ユーザー基準に基づいて、ユーザーを 産業用 ワークスペース 内の別のページにリダイレクトします。
OT アクション指向ランディングページの構成タスクを完了します。	ユーザーが 産業用 ワークスペースのランディングページにアクセスできるように、OT アクション指向のランディングページを構成します。
OT 進捗スコアカードの構成タスクを完了します。	ユーザーがサイトデータと 産業用 ワークスペース内の進捗状況の比較を開始できるように、OT 進捗状況スコアカードを構成します。
OT マネージャーダッシュボードの [OT 脆弱性] タブと [OT デバイス] タブの構成タスクを完了します。	ユーザーが 産業用 ワークスペース内のダッシュボードにアクセスできるように、OT マネージャーダッシュボードのタブを構成します。
オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードの構成タスクを完了します。	産業用 ワークスペースの オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードを構成します。

産業用 ワークスペースロールをアサインする

ユーザーに 産業用 ワークスペース ロールをアサインして、ワークスペースの機能やデータへのユーザーのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次のテーブルにリストされているロールを持つユーザーは、OT アクション指向ランディングページと OT 進捗スコアカードの ガイド付きセットアップ にアクセスできます。

OT 進捗状況スコアカードロール

ロール	Description (説明)
Industrial Workspace の構成 [configure_industrial_workspace]	OT アクション指向ランディングページと OT 進捗スコアカードの 産業用 ワークスペース と ガイド付きセットアップ にアクセスできます。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

のホームページ宛先ルールを確認します 産業用 ワークスペース

産業用 ワークスペースのホームページ宛先ルールを確認します。

始める前に
必要なロール：admin

このタスクについて

ホームページ宛先ルールは、ユーザー基準に基づいてユーザーを 産業用 ワークスペース 内の異なるページにリダイレクトします。ホームページ宛先ルールの詳細については、「[産業用 ワークスペース ホームページ宛先ルール](#)」を参照してください。

手順

1. [すべて] に移動します。
2. [フィルター] フィールドに「sys_homepage_destination_rule.list」を追加します。
3. Enter キーを押します。
4. ユーザー基準を編集する次の 産業用 ワークスペース ホームページ宛先ルールのいずれかを選択します。
 - OT 進捗状況スコアカードページ
 - MFG ホームページ
 - 製造 OT マネージャーダッシュボードページ

注:
OT マネージャーダッシュボードページのルールは、オペレーショナルテクノロジー マネージャー がインストールされている場合にのみ表示されます。

 - 製造 ISA 設備階層モデルページ

注:
[製造 ISA 設備階層モデルページ (MFG ISA Equipment Model Page)] ルールは、産業用プロセスマネージャー がインストールされている場合にのみ表示されます。
5. [ユーザー基準] フィールドで、ユーザー基準をコピーします。
6. 選択した 産業用 ワークスペース のページにユーザーをリダイレクトするユーザー基準を適用するには、次の手順を実行します。
 - a. 移動先 すべて > ユーザー基準.
 - b. リストビューの検索バーで、手順 5 でコピーしたホームページ宛先ルールのユーザー基準を検索します。
 - c. リダイレクトする必要なユーザーがユーザー基準と一致するように、ユーザー基準レコードを変更します。
 - d. [更新] を選択します。

タスクの結果

ユーザー基準レコードで定義されたユーザー、グループ、およびロールが、産業用 ワークスペース内の選択したページに自動的にリダイレクトされるようになりました。

オペレーショナルテクノロジーのアクション指向ランディングページの設定

ユーザーが重要なタスクにアクセスできるように、産業用 ワークスペース で オペレーショナルテクノロジー (OT) アクション指向ランディングページを設定します。

次の表に、OT アクション指向ランディングページの ガイド付きセットアップ タスクとその目的を示します。

OT アクション指向ランディングページのセットアップタスク

タスク	目的
1. OT アクション指向ランディングページのシステムプロパティを設定します。	sn_mfg_common.landing_page_important_actions_limit システムプロパティを使用して、[重要なアクション]の下に表示されるカードの数を変更します。

オペレーショナルテクノロジーアクション指向ランディングページのシステムプロパティを設定します

必要に応じてプロパティを有効にできるように、オペレーショナルテクノロジー (OT) アクション指向ランディングページのシステムプロパティを設定します。

始める前に

必要なロール:configure_industrial_workspace

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ワークスペースのシステムプロパティ**。
2. 必要に応じて、次のプロパティを編集します。

システムプロパティ	Description (説明)
sn_mfg_common.ランディング_ページ_重要_アクション_制限	OT アクション指向ランディングページの [重要なアクション] セクションでフェッチされる重要なアクションの最大数。デフォルトは 50 です。

3. [保存] を選択します。

オペレーショナルテクノロジー進捗スコアカードの設定

ユーザーがサイトデータと進捗状況を比較できるように、産業用 ワークスペースでオペレーショナルテクノロジー (OT) 進捗スコアカードを設定します。

次の表に、OT 進捗スコアカードの ガイド付きセットアップ タスクとその目的を示します。

OT 進捗状況スコアカードセットアップタスク

タスク	目的
1. OT 進捗スコアカードのロールをアサインします。	OT 進捗スコアカードのロールをユーザーにアサインして、OT 進捗スコアカードの機能とデータへのアクセスを制御できるようにします。
2. [PA OTPSC] 月次データ収集ジョブを完了します。	[OT 進捗状況スコアカード] タブの パフォーマンスアナリティクス からすべてのインジケータの日次データを収集して表示します。他のユーザーがこのタブのデータを表示する前に、この手順を完了する必要があります。
3. [オプション] インジケータソースを確認します。	多数のレコードのインジケータソースを確認します。合計レコード数がデフォルト値の 100

OT 進捗状況スコアカードセットアップタスク (続く)

タスク	目的
	万を超えることが予想される場合は、レコード収集を上書きする必要があります。
4. OT 進捗スコアカードのシステムプロパティを設定します。	OT 進捗状況スコアカードに表示されるしきい値と、計算済みスコアを決定するために使用されるコンポーネントを構成します。

オペレーショナルテクノロジー進捗スコアカードロールのアサイン

オペレーショナルテクノロジー (OT) 進捗スコアカードロールをユーザーにアサインして、OT 進捗スコアカードの機能やデータへのアクセスを制御できるようにします。

始める前に

必要なロール：admin

このタスクについて

次の表にリストされているロールを持つユーザーは、OT 進捗スコアカードを使用できます。

OT 進捗状況スコアカードロール

ロール	Description (説明)
OT 進捗状況スコアカードビューアー [ot_progress_scorecard_viewer]	利用可能なすべてのサイトデータを含む OT 進捗スコアカードを表示できます。
OT 進捗状況スコアカードエディター [ot_progress_scorecard_editor]	利用可能なすべてのサイトデータを含む OT 進捗スコアカードを表示および編集できます。

手順

Now Platform ユーザー管理機能を使用して、ユーザーとグループにロールをアサインします。

完全性スコア計算の検証

オペレーショナルテクノロジー (OT) 進捗スコアカードに **OT デバイスデータの完全性 (%)** インジケーターを含める場合は、**CMDB ヘルスダッシュボード:完全性スコア計算**がアクティブ化されていることを検証します。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ**。
2. [**Industrial Workspace** (産業用ワークスペース)] セクションで、[**OT Progress Scorecard (OT 進捗状況スコアカード)**] を選択します。
3. [完全性スコア計算の検証] タスクで、[構成] を選択します。
4. [CMDB Health Dashboard - Completeness Score Calculation Scheduled Script Execution] レコードで、次のアイテムを検証します。

- a. [アクティブ] チェックボックスがオンになっていることを検証します。
- b. 月末のレポートで正確なスコアが収集されるようにするには、[実行] フィールドが構成されていることを検証します

5. [更新] を選択します。

完全性の計算方法の詳細については、『[CMDB Health KPIs and metrics](#)』の「完全性」セクションを参照してください。

オペレーショナルテクノロジー進捗スコアカードのデータ収集の構成

パフォーマンスアナリティクス からすべてのインジケータの日次データを収集して表示できるように、オペレーショナルテクノロジー (OT) 進捗状況スコアカードのデータ収集を構成します。この構成により、OT データがスコアカードに正確に表示されます。

始める前に

必要なロール：admin

このタスクについて

[PA OTPSC] 月次データ収集ジョブを実行しない場合、OT 進捗状況スコアカードに使用できるデータは得られません。admin ロールを持っている場合は、ジョブの実行を求める警告メッセージが表示されます。

注:

admin ロールを持っていない場合は、アドミニストレータに問い合わせるよう求める警告メッセージが表示されます。

手順

1. 移動先 **すべて > データコレクタ > Performance Analytics (パフォーマンスアナリティクス) > ジョブ**.
OT 進捗状況スコアカードが表示されている場合は、エラーメッセージで [今すぐジョブを実行] を選択して、[スケジュール済みデータ収集] テーブルに移動します。
2. フィルターを表示/非表示 ( アイコン) アイコンを選択し、[名前] [次の値に等しい] [[PA OTPSC] 月次データ収集] のフィルターを追加して、フィルターを適用します。
3. [ジョブパラメーター] セクションの [アクティブ] フィールドの横にあるチェックボックスをオンにしてデータの収集を開始し、[時間] フィールドで時間をスケジュールします。
[今すぐ実行] ボタンを使用して、データを手動で収集できます。そうしないと、タブを表示したときにデータが表示されません。[今すぐ実行] ボタンは、ジョブを初めて実行する場合にのみ使用してください。この時点以降に収集されるデータは、スケジュールされた時刻に収集する必要があります。
4. デフォルトのスケジュール収集時間が有効かどうかを確認します。
デフォルトの時刻は毎月初めの 00:00:00 です。デフォルトの収集時間を変更する場合は、ジョブのアクティブ化後に変更できます。この変更については、必ずユーザーに通知してください。

タスクの結果

OT 進捗スコアカードに、ユーザーの正しいサイトデータが表示されるようになりました。

注:

OT 進捗状況スコアカードは パフォーマンスアナリティクス を使用します。パフォーマンスアナリティクス スコアは 5 か月間のみ保存されます。スコアを 5 か月以上保存してサイトデータを比較する場合は、[Activating your Performance Analytics subscription](#) をご覧ください。

多数のレコードのインジケータースソースを確認する

多数のレコードが必要な場合は、インジケータースソースを確認します。レコード収集を上書きして、オペレーショナルテクノロジー (OT) 進捗スコアカードにデフォルト値の 100 万件よりも多くのレコードが表示されるようにすることができます。

始める前に

必要なロール：admin

このタスクについて

パフォーマンスアナリティクス による移行のため、OT 進捗状況スコアカードの各インジケーターには、デフォルトで 100 万件のレコードのみを表示できます。admin ロールを持っていて、[PA OTPSC] 月次データ収集を実行した後にレコードが 100 万を超えると、エラーメッセージが表示されてジョブログが表示されます。

i 注:

admin ロールがなく、[PA OTPSC] 月次データ収集ジョブの実行後にレコードが 100 万を超えると、アドミニストレーターに問い合わせよう指示するエラーメッセージが表示されません。

admin ロールを持っている場合は、エラーメッセージのリンクからジョブログ関連リストを確認し、情報をフィルタリングして、エラーが発生しているインジケータースソースを確認できます。エラーのあるインジケータースソースを見つけたら、多数のレコードのインジケータースソースを変更し、インジケータースソースデータを上書きできます。その後、他のユーザーにはエラーメッセージが表示されなくなり、インジケータースソースのデータが表示されます。インジケータースソースの詳細については、「[Indicator sources](#)」を参照してください。

i 注:

新しいインジケーターを作成する必要がある場合は、Industrial Workspace Common に含まれるサイトブレイクダウンを使用する必要があります。オペレーショナルテクノロジーマネージャーアプリケーションのサイトブレイクダウン部分は廃止されました。

ジョブログには、インジケータースソースに関連しないエラーが含まれている場合があります。[レベル] 列でジョブログレコードをフィルタリングし、インジケータースソースに関するエラーメッセージを見つける必要があります。

手順

1. 移動先 **すべて > Performance Analytics** (パフォーマンスアナリティクス) > **ソース > インジケータースソース**。
2. フィルターを適用するには、[フィルターを表示/非表示 () アイコンを選択し、次のフィルターを追加します。
[アプリケーション][次の値に等しい][産業用ワークスペース共通]
3. 変更する必要があるインジケータースソースレコードを選択します。
どのインジケータースソースを調整する必要があるかは、エラーメッセージのジョブログリンクから確認できます。
4. [レコード収集] タブで、[レコード収集を上書き] フィールドの横にあるチェックボックスをオンにします。
5. [フェッチされるレコードの最大数 (**Maximum number of fetched records**)] フィールドで、値を XM に変更します。
6. [更新] を選択します。

オペレーショナルテクノロジー進捗スコアカードのシステムプロパティの設定

必要に応じてプロパティを有効にできるように、オペレーショナルテクノロジー (OT) 進捗スコアカードのシステムプロパティを設定します。

始める前に

必要なロール:configure_industrial_workspace

手順

1. 移動先 **すべて > 産業用ワークスペースアドミン > ワークスペースのシステムプロパティ**。
2. 必要に応じて、次のプロパティを編集します。

システムプロパティ	Description (説明)
OT 進捗状況スコアカード構成	
sn_mfg_common.otpsc.page_title	OT 進捗状況スコアカードに表示されるページタイトル。デフォルトは [OT 進捗状況スコアカード (OT Progress Scorecard)] です。
sn_mfg_common.otpsc.high_threshold	スコアカードに表示されている進捗状況バーの最大しきい値に達しました。このしきい値を超えるスコアはすべて緑色で示されます。
sn_mfg_common.otpsc.low_threshold	スコアカードに表示される進捗状況バーで到達した最低しきい値。しきい値を下回るスコアはすべて赤で示されます。
sn_mfg_common.otpsc.records_per_page	ページごとに表示されるレコードの数。デフォルトは 10 です。
OT 進捗状況スコアカードインジケータ	
sn_mfg_common.otpsc.ot_device_indicator_sysids	インジケータ sys_ids OT デバイス式をカンマ区切りリストで計算するために使用されます。
sn_mfg_common.otpsc.ot_incident_indicator_sysids	インジケータ sys_ids OT インシデントの計算式をカンマ区切りリストで計算するために使用されます。
sn_mfg_common.otpsc.ot_change_indicator_sysids	インジケータ sys_ids OT 変更の計算式をカンマ区切りリストで計算するために使用されます。
sn_mfg_common.otpsc.otvr_indicator_sysids	インジケータ sys_ids OTVR 計算式をカンマ区切りリストで計算するために使用されます。
インジケータ別 OT 進捗状況スコアカードの重み付け	
sn_mfg_common.otpsc.expected_ot_devices_weightage	CMDB メトリクスで予想される OT デバイスの割合 (%) が全体スコア (%) に寄与する重み付け。
sn_mfg_common.otpsc.classified_ot_device_weightage	分類済み OT デバイス (%) メトリクスが全体スコア (%) に寄与する重み付け。
sn_mfg_common.otpsc.assigned_ot_device_weightage	アサイン済み OT デバイス (%) メトリクスが全体スコア (%) に寄与する重み付け。

システムプロパティ	Description (説明)
sn_mfg_common.otpsc.ot_data_completeness_weightage	OT デバイスデータの完全性 (%) メトリクスが全体スコア (%) に寄与する重み付け。
sn_mfg_common.otpsc.mapped_ot_device_weightage	マッピングされた OT デバイス (%) メトリクスが全体スコア (%) に寄与する重み付け。
sn_mfg_common.otpsc.backed_up_ot_device_weightage	バックアップされた OT デバイス (%) メトリクスが全体スコア (%) に寄与する重み付け。
sn_mfg_common.otpsc.assigned_ot_vulnerable_items_weightage	アサインされた脆弱性一致アイテム (%) メトリクスが全体スコア (%) に寄与する重み付け。
sn_mfg_common.otpsc.approved_ot_change_requests_weightage	承認済み OT 変更要求 (%) メトリクスが全体スコア (%) に寄与する重み付け。
sn_mfg_common.otpsc.ot_incidents_with_ot_context_weightage	OT コンテキストのある OT インシデント (%) メトリクスが全体スコア (%) に寄与する重み付け。

3. [保存] を選択します。

サイトに想定される **OT** デバイスを構成する

OT 進捗状況スコアカードの **CMDB** で予想される **OT** デバイス の割合インジケータを使用できるように、サイトで予想される OT デバイスの数を構成します。

始める前に

必要なロール: ユーザー基準によって関連サイトにアサインされたサイトアクセス権を持つ

ot_progress_scorecard_editor および cmdb_ot_isa_viewer

注:

ユーザー条件によるサイト アクセスの詳細については、「[このホームページ宛先ルールを確認します 産業用 ワークスペース](#)」を参照してください。

手順

1. 移動先 [すべて > 産業用ワークスペースアドミン > OT 進捗状況スコアカード属性](#).

2. サイトでレコードを作成する必要がある場合は、次のアクションを完了します。

a. [新規] を選択します。

b. [サイト] フィールドにサイトを追加します。

c. [値] フィールドに、そのサイトで予想される OT デバイスの数を追加します。

注:

この値に OT コントロールモジュールを含めないでください。

d. [保存] を選択します。

3. サイトのレコードが存在し、想定されるデバイスを変更する場合は、次のアクションを実行します。

a. 編集するレコードを選択します。

b. [値] フィールドで、そのサイトで予想される OT デバイスの数を変更します。



この値に OT コントロールモジュールを含めないでください。

c. [更新] を選択します。

OT マネージャーダッシュボードの [OT デバイス] タブの設定

ガイド付きセットアップタスクを完了して、組織のデータコレクション、インジケータリソース、フィルターを使用して [OT デバイス] タブの設定を開始できるようにします。

OT マネージャーダッシュボードの [OT デバイス] タブのガイド付きセットアップにアクセスするには、すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ をクリックし、[オペレーショナルテクノロジーマネージャー] の下の [OT デバイス] タブセクションを選択します。

[OT デバイス] タブとその内容の詳細については、「[オペレーショナルテクノロジーマネージャーダッシュボード](#)」を参照してください。

次の表に、[OT デバイス] タブに設定できるガイド付きセットアップタスクを示します。

タスク ガイド付きセットアップ [OT デバイス] タブ

タスク	目的
1. OT デバイスの日次データ収集ジョブを完了します。	[OT デバイス] タブの パフォーマンスアナリティクス からすべてのインジケータリソースの日次データを収集して表示します。他のユーザーがこのタブのデータを表示する前に、この手順を完了する必要があります。
2. [オプション] インジケータリソースを確認します。	多数のレコードのインジケータリソースを確認します。合計レコード数がデフォルト値の 100 万を超えることが予想される場合は、レコード収集を上書きする必要があります。
3. 事業部門 (BU) を作成します。	事業部門 (BU) を作成して、[OT デバイス] タブの事業部門フィルターに BU を表示します。 注: サイトに関連付けられている BU のみがダッシュボードに表示されます。
4. サイトを事業部門に割り当てます。	サイトを事業部門 (BU) にアサインして、ユーザーがタブに表示されるデータを BU でフィルタリングできるようにします。

OT デバイスのデータ収集を構成する

パフォーマンスアナリティクス からすべてのインジケータリソースの日次データを収集して表示できるように、オペレーショナルテクノロジー (OT) デバイスのデータ収集を構成します。この構成により、OT マネージャーダッシュボードの OT デバイス タブに OT データが正確に表示される。

始める前に

必要なロール: admin

このタスクについて

OT デバイスの日次データコレクションジョブがまだ実行されていない場合は、[OT デバイス タブに利用可能なデータがなく、最終更新 日のタイムスタンプが

非表示になります。admin ロールを持っている場合は、OT デバイスの日次データコレクションジョブを実行するように求める次の警告メッセージが表示されます。

す:  No Data is shown on the dashboard because the 'OT Devices Daily Data Collection' job has not been run yet. [Run job now](#)

いません

注:

admin ロールを持っていない場合は、アドミニストレーターに問い合わせるよう求める警告メッセージが表示されます。

手順

1. 移動先 **すべて > データコレクタ > Performance Analytics (パフォーマンスアナリティクス) > ジョブ**。
[OT デバイス] タブが表示されている場合は、エラーメッセージで [今すぐジョブを実行] を選択することで、[スケジュール済みデータ収集] テーブルに移動できます。
2. フィルターを表示/非表示 ( アイコン) アイコンを選択してフィルターを適用し、[名前] [次の値に等しい] [OT デバイスの日次データ収集] のフィルターを追加します。
3. [ジョブパラメーター] セクションの [アクティブ] フィールドの横にあるチェックボックスをオンにしてデータの収集を開始し、[時間] フィールドで時間をスケジュールします。
[今すぐ実行] ボタンを使用して、データを手動で収集できます。そうしないと、[OT デバイス] タブを表示したときにデータが表示されません。[今すぐ実行] ボタンは、ジョブを初めて実行する場合にのみ使用してください。この時点以降に収集されるデータは、スケジュールされた時刻に収集する必要があります。
4. デフォルトのスケジュール収集時間が有効かどうかを確認します。
デフォルトの時刻は毎日 00:00:00 です。デフォルトの収集時間を変更する場合は、ジョブのアクティブ化後に変更できます。この変更については、必ずユーザーに通知してください。

タスクの結果

[OT デバイス] タブに、ユーザーに対して収集された OT デバイスの正しいデータが表示されるようになりました。

次のタスク

これで、インジケータソースを確認し、デフォルトのレコードコレクションを上書きする必要があるかどうかを判断できます。詳細については、「[多数のレコードのインジケータソースを確認する](#)」を参照してください。

多数のレコードのインジケータソースを確認する

多数のレコードが必要な場合は、インジケータソースを確認します。レコード収集を上書きして、[OT デバイス] タブにデフォルト値の 100 万件よりも多くのレコードが表示されるようにすることができます。

始める前に

必要なロール: admin

このタスクについて

パフォーマンスアナリティクス による移行のため、[OT デバイス] タブの各インジケータにはデフォルトで 100 万件のレコードのみを表示できます。admin ロールを持っていて、OT デバイスの日次データコレクションジョブを実行した後にレコードが 100 万件を超えた場合、エラーメッセージが表示されてジョブログに移動します。

注:

admin ロールがなく、OT デバイスの日次データ収集ジョブを実行した後にレコードが 100 万件を超えた場合は、アドミニストレーターに問い合わせるよう指示するエラーメッセージが表示されます。

admin ロールを持っている場合は、エラーメッセージ内のリンクからジョブログ関連リストを確認し、情報をフィルタリングして、エラーが発生しているインジケータソースを確認できます。エラーのあるインジケータソースを見つけたら、多数のレコードのインジケータソースを変更し、インジケータソースデータを上書きできます。その後、他のユーザーにはエラーメッセージが表示されなくなり、インジケータソースのデータが表示されます。インジケータソースの詳細については、「[Indicator sources](#)」を参照してください。

注:

新しいインジケータを作成する必要がある場合は、Industrial Workspace Common に含まれるサイトブレイクダウンを使用する必要があります。オペレーショナルテクノロジーマネージャアプリケーションのサイトブレイクダウン部分は廃止されました。

ジョブログには、インジケータソースに関連しないエラーが含まれている場合があります。インジケータソースに関するエラーメッセージを見つけるには、[レベル] 列でジョブログレコードをフィルタリングする必要があります。

手順

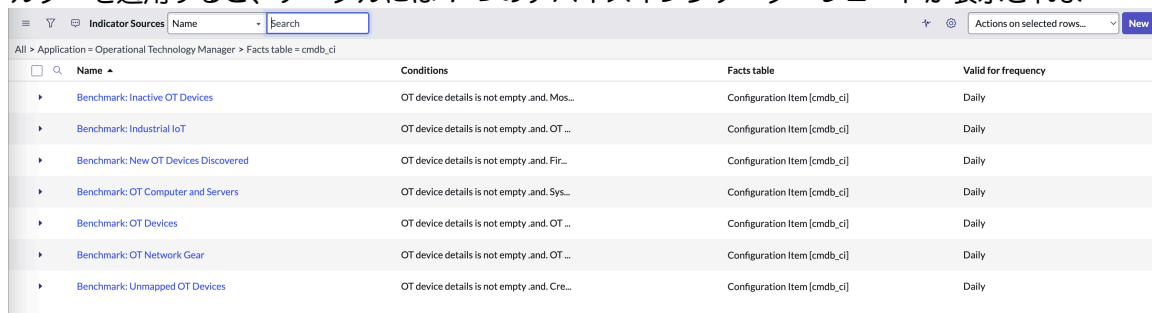
1. 移動先 **すべて > Performance Analytics** (パフォーマンスアナリティクス) > ソース > インジケータソース。

2. フィルターを適用するには、[フィルターを表示/非表示] () アイコンを選択し、次のフィルターを追加します。

○ [アプリケーション][次の値に等しい][オペレーショナルテクノロジーマネージャ]

○ [ファクトテーブル][次の値に等しい][cmdb_ci]

フィルターを適用すると、テーブルには 7 つのデバイスインジケータレコードが表示されま



Name	Conditions	Facts table	Valid for frequency
Benchmark: Inactive OT Devices	OT device details is not empty and. Mos...	Configuration Item [cmdb_ci]	Daily
Benchmark: Industrial IoT	OT device details is not empty and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: New OT Devices Discovered	OT device details is not empty and. Fir...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Computer and Servers	OT device details is not empty and. Sys...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Devices	OT device details is not empty and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: OT Network Gear	OT device details is not empty and. OT ...	Configuration Item [cmdb_ci]	Daily
Benchmark: Unmapped OT Devices	OT device details is not empty and. Cre...	Configuration Item [cmdb_ci]	Daily

す。

3. 変更する必要があるインジケータソースレコードを選択します。

どのインジケータソースを調整する必要があるかは、エラーメッセージのジョブログリンクから確認できます。

4. [レコード収集] タブで、[レコード収集を上書き] フィールドの横にあるチェックボックスをオンにします。

5. [フェッチされるレコードの最大数 (**Maximum number of fetched records**)] フィールドで、値を XM に変更します。

6. [更新] を選択します。

次のタスク

ダッシュボードに適用する事業部門 (BU) を作成します。詳細については、「[事業部門の作成](#)」を参照してください。

事業部門の作成

事業部門 (BU) を作成して OT マネージャダッシュボードの [OT デバイス] タブの事業部門フィルターを有効にします。BU を作成すると、組織機能を定義するのに役立ちます。

始める前に
必要なロール：admin

このタスクについて
admin ロールを持っている場合は、サイトにマッピングする BU を作成することで、[OT デバイス] タブに事業部門フィルターを表示できます。このアクションを実行すると、他のユーザーは [OT デバイス] タブの事業部門フィルターで BU を表示できます。

手順

1. 移動先 **すべて > 組織 > 事業部門**.
2. [新規] を選択します。
3. フォームのフィールドに入力します。

[事業部門] フォーム

Field (フィールド)	説明
名前	事業部門の名前。
Company (チェックアウト日時)	この事業部門に関連する会社 (存在する場合)。
業務部門長	事業部門の責任者。
Description (説明)	事業部門の説明。
親	その他の事業部門。[親] フィールドは、事業部門を階層要素として作成します。
階層レベル	事業部門のレベルを示す番号またはテキスト。
関連リスト	
部門	この事業部門を構成する部門。必要な数の部門を追加します。

4. [送信] を選択します。
5. オプション: 必要なすべての BU が作成されるまで、ステップ 2 ~ 4 を必要な回数だけ繰り返します。

タスクの結果

事業部門が作成されます。BU は、サイトレコードまたは [サイト] リストに追加できます。

事業部門へのサイトのアサイン

サイトを事業部門にアサインして、事業部門とそれにアサインされているサイトで オペレーショナルテクノロジー (OT) マネージャーダッシュボード をフィルタリングできるようにします。

始める前に
必要なロール：admin

このタスクについて
サイトを事業部門に割り当てるには、次の方法があります。

- サイトレコードを直接編集する。
- [サイト] テーブルで複数のサイトレコードを選択し、[事業部門] 列を更新します。

手順

1. 移動先 **すべて > 機器モデル : ISA > サイト**.
2. サイトレコードを編集して、サイトを事業部門にアサインします。
 - a. サイトレコードを選択して開きます。
 - b. [事業部門] フィールドで、事業部門を追加します。
 - c. [更新] を選択します。
3. [サイト] テーブルで複数のサイトレコードを選択し、[事業部門] 列を更新します。
 - a. [サイト] テーブルで、事業部門に割り当てる各サイトの横にあるチェックボックスをオンにします。
 - b. [事業部門] 列で、列 のオプション ボタンを選択し、 選択項目の更新 を選択します。



注:

[事業部門] 列は、ISA サイトビューでのみ表示されます。[事業部門] 列が表示されない場合は、[サイト] テーブルビューが [表示:ISA サイト] に設定されていることを確認します。

- c. [事業部門] フィールドで、事業部門を追加します。
- d. [更新] を選択します。

OT マネージャーダッシュボードの [OT 脆弱性] タブの設定

ガイド付きセットアップタスクを完了すると、組織のデータ収集、インジケータリソース、フィルターを使用して **[OT 脆弱性]** タブの設定を開始できます。

OT Manager (OT マネージャー) ダッシュボードの **[OT Vulnerabilities (OT 脆弱性)]** タブのガイド付きセットアップにアクセスするには、**すべて > 産業用ワークスペースアドミン > ガイド付きセットアップ** をクリックし、[オペレーショナルテクノロジー脆弱性対応] の下の **[OT 脆弱性]** タブセクションを選択します。

[**OT 脆弱性**] タブとその内容の詳細については、「[オペレーショナルテクノロジーマネージャーダッシュボード](#)」を参照してください。

次の表に、**[OT 脆弱性]** タブに設定できるガイド付きセットアップタスクを示します。

タスク ガイド付きセットアップ **[OT 脆弱性]** タブ

タスク	目的
1. OT 脆弱性の日次データ収集ジョブを完了します。	[OT 脆弱性] タブの パフォーマンスアナリティクス からすべてのインジケータの日次データを収集して表示します。他のユーザーがこの タブでデータを表示する前に、この手順を完了する必要があります。
2. [オプション] インジケータリソースを確認します。	多数のレコードのインジケータリソースを確認します。合計レコード数がデフォルト値の 100 万を超えることが予想される場合は、レコード収集を上書きする必要があります。

OT 脆弱性一致アイテムのデータ収集を構成する

オペレーショナルテクノロジー (OT) 脆弱性一致アイテム (VI) のデータ収集を構成して、パフォーマンスアナリティクスからすべてのインジケータの日次データを収集して表示できるようにします。この構成により、OT データが **[OT 脆弱性]** タブに正確に表示されます。

始める前に

必要なロール：admin

このタスクについて

OT 脆弱性一致アイテムの日次データコレクションジョブがまだ実行されていない場合は、タブに利用可能なデータがなく、[最終更新日] タイムスタンプが非表示になります。admin ロールを持っている場合は、OT 脆弱性一致アイテムの日次データコレクションジョブを実行するように求める次の警告メッセージが表示されます。[

ⓘ No Data is shown on the dashboard because the 'OT Vulnerable Items Daily Data Collection' job has not been run yet. [Run job now](#)

注:

admin ロールを持っていない場合は、アドミニストレーターに問い合わせるよう求める警告メッセージが表示されます。

手順

1. 移動先 **すべて > データコレクタ > Performance Analytics (パフォーマンスアナリティクス) > ジョブ**.
[**OT 脆弱性**] タブが表示されている場合は、エラーメッセージで [今すぐジョブを実行] を選択して、[スケジュール済みデータ収集] テーブルに移動します。
2. フィルターを表示/非表示 ( アイコン) アイコンを選択し、[名前] [次の値に等しい] [OT 脆弱性一致アイテムの日次データ収集] のフィルターを追加して、フィルターを適用します。
3. [ジョブパラメーター] セクションの [アクティブ] フィールドの横にあるチェックボックスをオンにしてデータの収集を開始し、[時間] フィールドで時間をスケジュールします。
[今すぐ実行] ボタンを使用して、データを手動で収集できます。そうしないと、タブを表示したときにデータが表示されません。[今すぐ実行] ボタンは、ジョブを初めて実行する場合にのみ使用してください。この時点以降に収集されるデータは、スケジュールされた時刻に収集する必要があります。
4. デフォルトのスケジュール収集時間が有効かどうかを確認します。
デフォルトの時刻は毎日 00:00:00 です。デフォルトの収集時間を変更する場合は、ジョブのアクティブ化後に変更できます。この変更については、必ずユーザーに通知してください。

タスクの結果

[**OT 脆弱性**] タブに、ユーザーに対して収集された OT 脆弱性一致アイテムの正しいデータが表示されるようになりました。

次のタスク

これで、インジケータソースを確認し、デフォルトのレコードコレクションを上書きする必要がありますかどうかを判断できます。詳細については、「[多数のレコードのインジケータソースを確認する](#)」を参照してください。

多数のレコードのインジケータソースを確認する

多数のレコードが必要な場合は、インジケータソースを確認します。レコード収集を上書きして、デフォルト値の 100 万件よりも多くのレコードが **[OT 脆弱性]** タブに表示されるようにすることができます。

始める前に

必要なロール：admin

このタスクについて

パフォーマンスアナリティクス による移行のため、[OT 脆弱性] タブの各インジケータにはデフォルトで 100 万件のレコードしか表示できません。admin ロールを持っていて、OT 脆弱性一致アイテムの日次データコレクションジョブを実行した後にレコードが 100 万件を超えた場合、エラーメッセージが表示されてジョブログが表示されます。

注:

admin ロールがなく、OT 脆弱性一致アイテムの日次データコレクションジョブを実行した後にレコードが 100 万件を超えた場合は、エラーメッセージが表示され、アドミニストレーターにサポートを求めるように指示されます。

admin ロールを持っている場合は、エラーメッセージのリンクからジョブログ関連リストを確認し、情報をフィルタリングして、エラーが発生しているインジケータソースを確認できます。エラーのあるインジケータソースを見つけたら、多数のレコードのインジケータソースを変更し、インジケータソースデータを上書きできます。その後、他のユーザーにはエラーメッセージが表示されなくなり、インジケータソースのデータが表示されます。インジケータソースの詳細については、「[Indicator sources](#)」を参照してください。

注:

新しいインジケータを作成する必要がある場合は、Industrial Workspace Common に含まれるサイトブレイクダウンを使用する必要があります。オペレーショナルテクノロジーマネージャアプリケーションのサイトブレイクダウン部分は廃止されました。

ジョブログには、インジケータソースに関連しないエラーが含まれている場合があります。[レベル] 列でジョブログレコードをフィルタリングし、インジケータソースに関するエラーメッセージを見つける必要があります。

手順

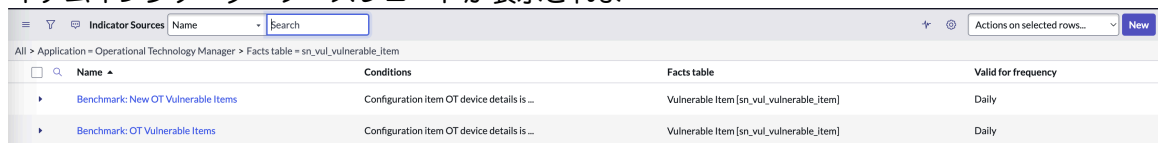
1. 移動先 すべて > **Performance Analytics** (パフォーマンスアナリティクス) > ソース > インジケータソース。

2. フィルターを適用するには、[フィルターを表示/非表示] () アイコンを選択し、次のフィルターを追加します。

○ [アプリケーション][次の値に等しい][オペレーショナルテクノロジーマネージャ]

○ [ファクトテーブル][次の値に等しい][sn_vul_vulnerable_item]

フィルターを適用すると、テーブルには 2 つの脆弱性一致アイテムインジケータソースレコードが表示されます。



Name	Conditions	Facts table	Valid for frequency
Benchmark: New OT Vulnerable Items	Configuration item OT device details is ...	Vulnerable Item [sn_vul_vulnerable_item]	Daily
Benchmark: OT Vulnerable Items	Configuration item OT device details is ...	Vulnerable Item [sn_vul_vulnerable_item]	Daily

す。

3. 変更する必要があるインジケータソースレコードを選択します。

どのインジケータソースを調整する必要があるかは、エラーメッセージのジョブログリンクから確認できます。

4. [レコード収集] タブで、[レコード収集を上書き] フィールドの横にあるチェックボックスをオンにします。

5. [フェッチされるレコードの最大数 (**Maximum number of fetched records**)] フィールドで、値を XM に変更します。

6. [更新] を選択します。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードの設定

ユーザーが重要なタスクにアクセスできるように、産業用 ワークスペースでオペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードを設定します。

次の表に、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのガイド付きセットアップタスクとその目的を示します。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードセットアップタスク

タスク	目的
1. データ収集ジョブを構成します。	OTVR (PA) ダッシュボードの パフォーマンス アナリティクス からすべてのインジケータの日次データを収集して表示します。他のユーザーがこのタブのデータを表示する前に、この手順を完了する必要があります。
2. [オプション] インジケータソースを確認します。	多数のレコードのインジケータソースを確認します。合計レコード数がデフォルト値の 100 万を超えることが予想される場合は、レコード収集を上書きする必要があります。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのデータ収集の構成

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに表示されるデータのデータ収集を構成します。スケジュール済みジョブは、特定の時間または繰り返しスケジュールで実行できる自動化された作業です。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > データコレクタ > Performance Analytics (パフォーマンスアナリティクス) > ジョブ**.
2. フィルターを適用するには、[フィルターを表示/非表示] () アイコンを選択し、次のフィルターを追加します。
 - [アプリケーション][次の値に等しい][オペレーショナルテクノロジー脆弱性対応]
 - [クラス][次の値に等しい][スケジュールされたデータ収集]
 フィルターを適用すると、次のスケジュール済みジョブが表示されます。
 - [PA OT VR]過去の脆弱性データ収集

注:

[PA OT VR] 履歴脆弱性データ収集ジョブは、一度だけ実行する必要があるオンデマンドジョブです。履歴データが収集された後、毎日スケジュールされた時刻に日次データ収集ジョブが実行されます。履歴データの詳細については、「[Collect historical data](#)」を参照してください。

- [PA OT VR]修復タスクの日次収集
- [PA OT VR]脆弱なアイテムの日次収集 1
- [PA OT VR]脆弱なアイテムの日次収集 2
- [PA OT VR]脆弱な構成アイテム (CI) の日次収集

3. データの収集を開始するには、スケジュール済みジョブレコードを選択します。
4. [ジョブパラメーター] セクションの [アクティブ] フィールドの横にあるチェックボックスをオンにし、[時間] フィールドで時間をスケジュールします。
[今すぐ実行] ボタンを使用して、データを手動で収集できます。そうしないと、タブを表示したときにデータが表示されません。[今すぐ実行] ボタンは、ジョブを初めて実行する場合にのみ使用してください。この時点以降に収集されるデータは、スケジュールされた時刻に収集する必要があります。
5. デフォルトのスケジュール収集時間が有効かどうかを確認します。
デフォルトの時刻は毎日 00:00:00 です。デフォルトの収集時間を変更する場合は、ジョブのアクティブ化後に変更できます。この変更については、必ずユーザーに通知してください。
6. スケジュール済みジョブごとに手順 3 ～ 5 を繰り返します。

タスクの結果

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに、ユーザーにとって正しいデータが表示されるようになりました。

次のタスク

これで、インジケータソースを確認し、デフォルトのレコードコレクションを上書きする必要がありますかどうかを判断できます。詳細については、「[多数のレコードのインジケータソースを確認する](#)」を参照してください。

多数のレコードのインジケータソースを確認する

インジケータソースから 100 万件を超えるレコードが収集されることが予想される場合は、インジケータソースを確認して更新し、予想されるレコード数を上書きします。このアクションは、産業用 ワークスペースのデータを収集するときのシステムパフォーマンスの問題を回避するのに役立ちます。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > Performance Analytics** (パフォーマンスアナリティクス) > **インジケータ > インジケータ (自動)**。
2. フィルター **[Application] [is] [Operational Technology Vulnerability Response]** を適用します。
3. [インジケータソース] 列で、編集するインジケータソースレコードを選択します。
4. [レコード収集] セクションで、[レコード収集を上書き] フィールドの横にあるチェックボックスをオンにします。
5. [フェッチされるレコードの最大数] フィールドに、デフォルト値の 100 万レコードより大きい数を追加します。
たとえば、200 万です。
6. [更新] を選択します。

産業用 ワークスペース の使用

産業用 ワークスペースに必要なすべてのセットアップタスクを完了すると、ユーザーは OT アクション指向ランディングページ、OT マネージャーダッシュボード、OT 進捗スコアカード、OTVR (PA) ダッシュボードでオペレーショナルテクノロジーデータの管理を開始できます。

産業用 ワークスペース ホームページ宛先ルール

アサインされたロールに応じて、ホームページ宛先ルールを使用して 産業用 ワークスペース 内の異なるページにリダイレクトされます。これにより、必要なデータに迅速かつ効率的にアクセスできるようになります。

概要

各宛先ルールは、アサインされたロールに基づいて、さまざまな OT ユーザーを 産業用 ワークスペース 上の異なるページにリダイレクトします。ロールによっては 1 ページのデータにアクセスできない場合があるため、データを表示できるページにユーザーをリダイレクトすると、産業用 ワークスペースをより適切にナビゲートするのに役立ちます。たとえば、オペレーショナルテクノロジー マネージャーエディター [cmdb_ot_editor] ロールを持つユーザーは、OT アクション指向ランディングページでデータを表示できないため、空のランディングページのみが表示されます。代わりに、該当する OT デバイスデータを表示できる OT マネージャーダッシュボードにリダイレクトされます。

産業用 ワークスペース ホームページ宛先ルールの説明

次の表では、産業用 ワークスペース ホームページ宛先ルールとその宛先について説明します。

ホームページ宛先ルール

ルール	宛先	リダイレクトされるロール	Description (説明)
OT 進捗状況スコアカードページ	now/mfg/ot-progress-scorecard/ (OT 進捗状況スコアカード)	ot_progress_scorecard	OT 進捗スコアカードルールでは、ルールに記述されているロールを持つユーザーがログインすると、OT 進捗スコアカードに直接移動します。
MFG ホームページ	now/mfg/home (OT アクション指向ランディングページ)	- sn_ot_incident_read - sn_ot_change_read - sn_vul.remediation_owner - cmdb_ot_viewer	MFG ホームページルールでは、ルールで説明されているロールを持つユーザーがログインすると、OT アクション指向ランディングページに直接移動します。
製造 OT マネージャーダッシュボードページ	now/mfg/ot-manager-dashboard (OT マネージャーダッシュボード)	cmdb_ot_viewer	[MFG Manager Dashboard Page (製造マネージャーダッシュボードページ)] ルールにより、ルールに記述されているロールを持つユーザーは、ログイン時に OT マネージャーダッシュボードに直接移動します。

ホームページ宛先ルール (続く)

ルール	宛先	リダイレクトされるロー ル	Description (説明)
			i 注: OT マネージャー ダッシュボード ページのルール は、オペレー ショナルテクノロ ジーマネージャー がインストールさ れている場合にの み表示されます。
製造 ISA 設備階層モデ ルページ	now/mfg/isa- equipment-model (機 器モデルマネージャー)	cmdb_ot_isa_viewer	製造 ISA 設備階層モ デルページのルールで は、ルールに記載さ れているルールを持 つユーザーがログイン すると、機器モデルマ ネージャーに直接移動 します。 i 注: [製造 ISA 設 備階層モデル ページ (MFG ISA Equipment Model Page)] ルールは、産業 用プロセスマネー ジャー がインス トールされている 場合にのみ表示さ れます。

オペレーショナルテクノロジー マネージャーダッシュボードフィルター

オペレーショナルテクノロジー (OT) Manager ダッシュボードのフィルターを使用して、サイト別または事業部門 (BU) 別にダッシュボードに表示するデータを指定できます。たとえば、複数のサイトの OT デバイスデータを一度に表示できます。

概要

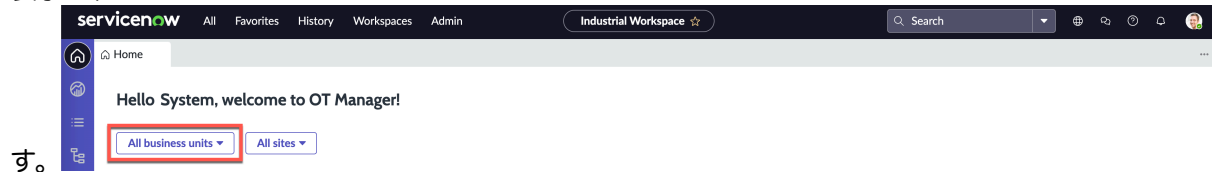
事業部門とサイトフィルターを使用すると、ダッシュボードに表示する OT デバイスまたは脆弱性データを指定できます。1 つ以上の事業部門とそれぞれのサイトを選択して、産業用 ワークスペース内の 1 つの場所で OT データを表示できます。

事業部門フィルター

事業部門 (BU) フィルターを使用すると、次のアクションを実行できます。

- すべての事業部門の OT データを表示します。
- 特定の事業部門の OT データを表示します。
- 複数の事業部門の OT データを表示します。

デフォルトでは、次の例に示すように、ダッシュボードに利用可能なすべての BU の OT データが表示されま



す。BU フィルターを設定すると、選択した BU に含まれるすべてのサイトのデータがダッシュボードに表示されます。その後、次のセクションで説明する [すべてのサイト] メニューからサイトを選択できます。BU フィルターを変更して別の BU を選択すると、サイトフィルターが更新され、選択した BU に関連付けられているサイトのみが含まれます。

BU およびサイトフィルターの使用方法の詳細については、「[事業部門とサイトのフィルターを使用する](#)」を参照してください。

サイトフィルター

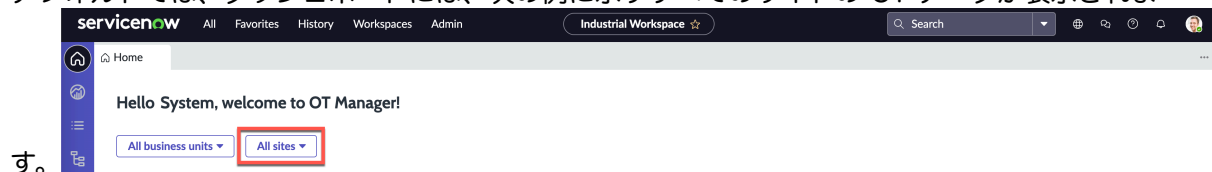
サイトフィルターを使用すると、次のアクションを実行できます。

- すべてのサイトの OT データを表示します。
- 特定のサイトの OT データを表示します。
- 複数のサイトの OT データを表示します。
- サイトが割り当てられていない OT データを表示します。

注:

OT デバイスにサイトがアサインされていない場合、フィルターには [サイトがアサインされていません (**No site assigned**)] と表示されます。ダッシュボードに正しいサイトを表示するには、デバイスにサイトを割り当ててから、そのサイトに事業部門を割り当てる必要があります。

デフォルトでは、ダッシュボードには、次の例に示すすべてのサイトの OT データが表示されま



事業部門とサイトのフィルターを使用する

オペレーショナルテクノロジー (OT) マネージャーダッシュボードの事業部門 (BU) とサイトフィルターを使用して、事業部門またはサイトでデータをフィルタリングします。

始める前に

必要なロール: admin

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース).
2. OT マネージャーダッシュボードを開きます。

3. 1 つ以上の BU の OT データを表示します。

- a. ヘッダーで、[すべての事業部門] メニューを選択します。
- b. リストから、データを表示する 1 つ以上の BU を選択します。検索機能を使用して、特定の BU を検索できます。

4. 1 つ以上のサイトの OT データを表示します。

- a. ヘッダーで、[すべてのサイト] メニューを選択します。
- b. 一覧から、データを表示する 1 つ以上のサイトを選択します。



注:

検索機能を使用して、特定のサイトを検索できます。検索バーにサイトの名前または短縮コードを入力します。短縮コードは、サイトの略語です。

オペレーショナルテクノロジー 進捗状況スコアカードフィルター

オペレーショナルテクノロジー (OT) 進捗スコアカードのフィルターを使用して、スコアカードに表示するデータをサイト、事業部門 (BU)、または日付別に指定できます。

概要

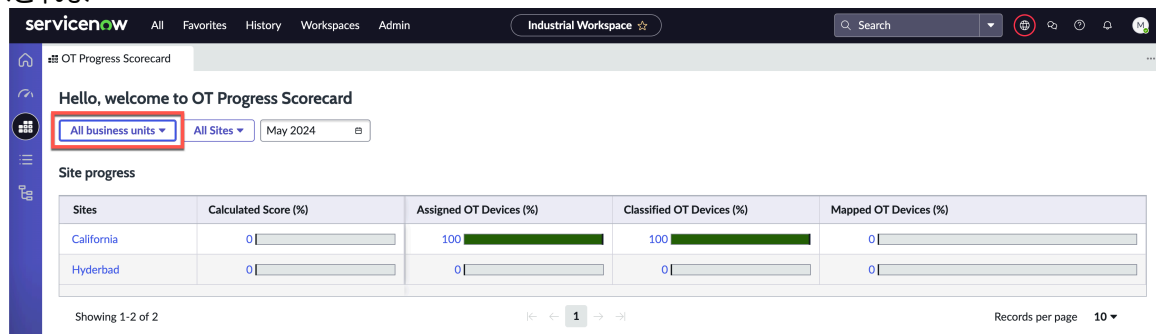
事業部門、サイト、および日付フィルターを使用すると、OT 進捗状況スコアカードに表示するスコアカードメトリクスを指定できます。1 つ以上の事業部門、それぞれのサイト、および特定の暦月でフィルタリングできます。

事業部門フィルター

事業部門 (BU) フィルターを使用すると、次のアクションを実行できます。

- すべての事業部門のスコアカードメトリクスを表示します。
- 特定の事業部門のスコアカードメトリクスを表示します。
- 複数の事業部門のスコアカードメトリクスを表示します。

デフォルトでは、次の例に示すように、スコアカードには利用可能なすべての BU のメトリクスが表示されます。



す。

BU フィルターを設定すると、選択した BU に含まれるすべてのサイトのデータがスコアカードに表示されます。その後、次のセクションで説明する [すべてのサイト] メニューからサイトを選択できます。BU フィルターを変更して別の BU を選択すると、サイトフィルターが更新され、選択した BU に関連付けられているサイトのみが含まれます。

BU およびサイトフィルターの使用方法の詳細については、「[オペレーショナルテクノロジー進捗スコアカードフィルターの使用](#)」を参照してください。

サイトフィルター

サイトフィルターを使用すると、次のアクションを実行できます。

- すべてのサイトのスコアカードメトリクスを表示します。
- 特定のサイトのスコアカードメトリクスを表示します。
- 複数のサイトのスコアカードメトリクスを表示します。

デフォルトでは、スコアカードには、次の例に示すすべてのサイトのメトリクスが表示されま

OT Progress Scorecard

Hello, welcome to OT Progress Scorecard

All business units All Sites May 2024

Site progress

Sites	Calculated Score (%)	Assigned OT Devices (%)	Classified OT Devices (%)	Mapped OT Devices (%)
California	0	100	100	0
Hyderabad	0	0	0	0

Showing 1-2 of 2 Records per page 10

す。

日付フィルター

日付フィルタを使用すると、選択した年の特定の暦月のスコアカードメトリクスを表示できます。デフォルトでは、スコアカードには前月と前年のメトリクスが表示されます。

- 注:**
- [PA OTPSC] 月次データ収集ジョブがまだ実行されていない場合、スコアカードにはスコアが 0 と表示されます。[PA OTPSC] 月次データ収集ジョブの詳細については、「[オペレーショナルテクノロジー進捗スコアカードのデータ収集の構成](#)」を参照してください。

OT Progress Scorecard

Hello, welcome to OT Progress Scorecard

All business units All Sites May 2024

Site progress

Sites	Calculated Score (%)	Assigned OT Devices (%)	Classified OT Devices (%)	Mapped OT Devices (%)
California	0	100	100	0
Hyderabad	0	0	0	0

Showing 1-2 of 2 Records per page 10

オペレーショナルテクノロジー進捗スコアカードフィルターの使用

オペレーショナルテクノロジー (OT) 進捗スコアカードの事業部門 (BU) とサイトフィルターを使用して、事業部門、サイト、または日付でデータをフィルタリングします。

始める前に

必要なロール：admin

手順

1. 移動先 **すべて > Industrial Workspace** (産業用ワークスペース)。
2. OT 進捗スコアカードを開きます。
3. 1 つ以上の BU のスコアカードメトリクスを表示します。

- a. ヘッダーで、[すべての事業部門] メニューを選択します。
 - b. リストから、データを表示する 1 つ以上の BU を選択します。検索機能を使用して、特定の BU を検索できます。
4. 1 つ以上のサイトのスコアカードメトリクスを表示します。
- a. ヘッダーで、[すべてのサイト] メニューを選択します。
 - b. 一覧から、データを表示する 1 つ以上のサイトを選択します。

注:

検索機能を使用して、特定のサイトを検索できます。検索バーにサイトの名前または短縮コードを入力します。短縮コードは、サイトの略語です。

5. カレンダー日付のスコアカードメトリクスを表示します。

- a. ヘッダーで、カレンダー () アイコンを選択します。
- b. データを使用する月と年を選択します。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのインジケータースソースとインジケーター

オペレーショナルテクノロジー脆弱性対応 アプリケーションは、インジケータースソースとインジケーターを使用してデータを収集し、脆弱性修復の進捗状況を追跡します。

インジケータースソース

オペレーショナルテクノロジー脆弱性対応インジケーターは、次のインジケータースソースからデータを収集します。インジケータースソースから 100 万件を超えるレコードが収集されることが予想される場合は、インジケータースソースの [レコード収集] セクションで予想される数を上書きする必要があります。詳細については、「[多数のレコードのインジケータースソースを確認する](#)」を参照してください。

OTVI.アクティブ

sn_vul_vulnerable_item テーブルを使用し、OT システム内のすべてのアクティブな脆弱性一致アイテムを含めます。

OTVI.クローズ済み

sn_vul_vulnerable_item テーブルを使用し、OT システム内のすべてのクローズ済み脆弱性一致アイテムを含めます。

OTRT.アクティブ

sn_vul_vulnerability テーブルを使用し、OT システム内のすべてのアクティブな修復タスクを含めます。

インジケーター

オペレーショナルテクノロジー脆弱性対応 アプリケーションでの脆弱性修復の進捗状況を測定および追跡するために、いくつかのインジケーターが使用されます。

インジケーターの レコード収集 オプションは、オペレーショナルテクノロジー脆弱性対応 アプリケーションではデフォルトで無効になっています。このオプションは、各インジケーターに対して大量のデータを収集するときに発生する可能性があるパフォーマンスの問題を回避するためにオフになっています。

OT 脆弱性一致アイテム

データソース OTVI の OT 脆弱性一致アイテムの数。[アクティブ]
は、sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の脆弱性一致アイテムの数を最小限に抑えることです。

重大な OT 脆弱性一致アイテム

データソース OTVI の重大な OT 脆弱性一致アイテムの数。[アクティブ]
は、sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の重大な脆弱性一致アイテムの数を最小限に抑えることです。

未アサインの OT 脆弱性一致アイテム

[アサイン先グループ] フィールドと [アサイン先] フィールドの両方が空であるすべてのアクティブな OT 脆弱性一致アイテム。目標は、未アサインの脆弱性一致アイテムの数を最小限に抑えることです。

クローズ済み OT 脆弱性一致アイテム

クローズ済み OT 脆弱性一致アイテムインジケータは、ユニット数で毎日測定されます。目標は、システム内のクローズ済みの脆弱性一致アイテムの数を最大化することです。

保留された OT 脆弱性一致アイテム

データソース OTVI の保留された OT 脆弱性一致アイテムの数。[アクティブ]
は、sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の保留された脆弱性一致アイテムの数を最小限に抑えることです。

保留された重大な OT 脆弱性一致アイテム

データソース OTVI の重大な保留された脆弱なアイテムの OT の数。[アクティブ]
は、sn_vul_vulnerable_itemテーブルを使用します。目標は、保留された重大な脆弱性一致アイテムの数を最小限に抑えることです。

保留されていない期限切れの重大な OT 脆弱性一致アイテム

データソース OTVI の保留されていない期限切れの重大な OT 脆弱性一致アイテムの数。[アクティブ] は、sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の保留されていない期限切れの重大な脆弱性一致アイテムの数を最小限に抑えることです。

OT 修復タスク

データソース OTRT の OT 修復タスクの数。[アクティブ] で、sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の修復タスクの数を最小限に抑えることです。

保留されていない期限切れの重大な OT 修復タスク

データソース OTRT の保留されていない期限切れの重大な OT 修復タスクの数。[アクティブ] で、sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の保留されていない期限切れの重大な修復タスクの数を最小限に抑えることです。

保留されていない OT 修復タスク

データソース OTRT の保留されていない OT 修復タスクの数。[アクティブ] で、sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の保留されていない修復タスクの数を最小限に抑えることです。

保留されていない重大な OT 修復タスク

データソース OTRT の保留されていない重大な OT 修復タスクの数。[アクティブ] で、sn_vul_vulnerabilityテーブルを使用します。目標は、システム内の保留されていない重大な修復タスクの数を最小限に抑えることです。

未アサインの OT 修復タスク

[アサイン先グループ] と [アサイン先] フィールドの両方が空であるすべてのアクティブな修復タスク。目標は、システム内の未アサインの修復タスクの数を最小限に抑えることです。

修復ターゲットを満たした脆弱なアイテムの割合

$$\left(\frac{[[\text{クローズされた脆弱なアイテム} > \text{修正ターゲット} = \text{ターゲット達成}]]}{[[\text{クローズされた脆弱なアイテム}]]} \right) * 100$$

目標は、システム内の修復ターゲットを満たす脆弱性一致アイテムの割合を最大化することです。

OT 脆弱性一致アイテム平均修復時間

$$\frac{[[\text{クローズされた脆弱なアイテムの所要時間合計}]]}{[[\text{クローズされた脆弱なアイテム}]]}$$

クローズ済み脆弱性一致アイテムの OT 合計期間

データソース OTVI のクローズ済み脆弱性一致アイテムの OT 合計期間の数。
[Closed]:sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内のクローズ済み脆弱性一致アイテムの合計期間を最小限にすることです。

OT 脆弱性構成アイテム

データソース OTVI の OT 脆弱性一致構成アイテム (OTVI) の数。[アクティブ]
は、sn_vul_vulnerable_itemテーブルを使用します。目標は、システム内の脆弱な構成アイテムの数を最小限に抑えることです。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードのブレイクダウン

オペレーショナルテクノロジー脆弱性対応はブレイクダウンを使用して、収集されたレコードをフィルタリングしてグループ化します。

ダッシュボードのインジケーターには、次のブレイクダウンが適用されます。

経過時間

日/時間/分形式で表示される脆弱性一致アイテムの経過時間。

クローズした経過時間

ステータスが [クローズ済み] に変更されたときの脆弱性一致アイテムの経過時間。

Assignment Group (アサイン先グループ)

脆弱性一致アイテムまたは修復タスクのアサイン先グループ。

CI マネージャー

脆弱な構成アイテム (CI) のマネージャー。

保留の理由

脆弱性一致アイテムが修正のために保留される理由。

エクスプロイト攻撃ベクトル

脆弱性のエクスプロイトの最も脆弱な攻撃ベクトル。

エクスプロイト有無

脆弱性に関連付けられているエクスプロイト。

エクスプロイトスキルレベル

脆弱性を利用するために必要な最低のスキルレベル。

修復ターゲットルール

脆弱性一致アイテムの修正の予定期間。

修復ターゲットステータス

脆弱性一致アイテムのステータスが修正ターゲット日とともに更新されました。

修正ターゲットステータス (クローズ済み)

修復ターゲット日が守られたときに脆弱性一致アイテムのステータスが更新されます。

リスク評価

脆弱性一致アイテムを [重大]、[高]、[中]、[低]、および [なし] に分類する数値化されたリスクスコア。

重大度

脆弱性の重大度を正規化したもの。

ステータス

脆弱性一致アイテムまたは修復タスクのステータス。

次のブレイクダウンソースは、脆弱性一致アイテムレポート、修復タスクレポート、またはその両方のタイプのレポートのダッシュボードのインジケータに適用されます。

アサイン先グループ

脆弱性一致アイテムと修復タスクのレポート。

保留.理由.未.クローズ

脆弱性一致アイテムレポート。

エクスプロイト攻撃ベクトル

脆弱性一致アイテムレポート。

エクスプロイト有無

脆弱性一致アイテムレポート。

エクスプロイトスキルレベル

脆弱性一致アイテムレポート。

OT 経過時間範囲

脆弱性一致アイテムレポート。

修復ターゲットステータス

脆弱性一致アイテムと修復タスクのレポート。

修復ターゲットステータス (クローズ済み)

脆弱性一致アイテムと修復タスクのレポート。

Remediation.Target.Rule

脆弱性一致アイテムと修復タスクのレポート。

リスク評価

脆弱性一致アイテムと修復タスクのレポート。

過酷

脆弱性一致アイテムと修復タスクのレポート。

状態

脆弱性一致アイテムと修復タスクのレポート。

Vulnerable.Item.CI.Manager

脆弱性一致アイテムレポート。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボード収集ジョブ

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードは、収集ジョブを使用して、ダッシュボードに表示されるデータを収集します。

次の収集ジョブは、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに表示されるデータを収集します。

[PA OT VR]過去の脆弱性データ収集

既存レコードの履歴データの収集ジョブ。

i 注:

履歴脆弱性データ収集は、一度だけ実行する必要があるオンデマンドジョブです。履歴データが収集された後、毎日スケジュールされた時刻に日次データ収集ジョブが実行されます。詳細については、「[Collect historical data](#)」を参照してください。

[PA OT VR]修復タスクの日次収集

毎日発生する修復タスクデータの収集ジョブ。

[PA OT VR]脆弱なアイテムの日次収集 1

保留されていない期限切れの重大な脆弱性一致アイテム、保留された脆弱なアイテム、脆弱なアイテム、および重大な脆弱性一致アイテムに対して毎日発生する収集ジョブ。

[PA OT VR]脆弱なアイテムの日次収集 2

未アサインの脆弱性一致アイテム、クローズされた脆弱性一致アイテム、クローズされた脆弱性一致アイテムの合計期間、および重大な保留された脆弱性一致アイテムについて毎日発生する収集ジョブ。

[PA OT VR]脆弱な構成アイテム (CI) の日次収集

毎日発生する脆弱性一致 CI データの収集ジョブ。

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードで使用されるデータの可視化

オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードでは、データの可視化を使用して OT 脆弱性データを表示します。

次の表では、オペレーショナルテクノロジー脆弱性対応 (PA) ダッシュボードに表示されるデータの可視化について説明します。

[脆弱性一致アイテム] タブのデータの可視化

名前	タイプ	Description (説明)
OT 脆弱性一致アイテム (VI)	単一スコア	アクティブな (クローズされていない) OT 脆弱性一致アイテムの数。
OT 脆弱性構成アイテム (CI)	単一スコア	1 つ以上のアクティブな OT 脆弱性一致アイテムに関連付けられている構成アイテム (CI) の数。
OT 修復タスク	単一スコア	アクティブな (クローズされていない) OT 修復タスクの数。
修正ターゲットを満した OT VI	単一スコア	現在の四半期と前の四半期の修正ターゲット日を達成した、クローズされた OT 脆弱性一致アイテムの割合。 修正ターゲットは、最終オープン日に最終オープン日からの日数 (24 時間単位として測定) を加算して計算されます。

[脆弱性一致アイテム] タブのデータの可視化 (続く)

名前	タイプ	Description (説明)
OT VI 平均修正時間 (MTTR)	単一スコア	OT 脆弱性一致アイテムを修正 (クローズ) する平均時間 (30 日間の実行平均として表示)。 i 注: [クローズした経過時間] の値は、データの収集時に計算されます。値は、last_opened の日付と収集ジョブの日時の差です。
期限間近の OT の重大な修復タスク	単一スコア	修正ターゲット日が近づいているアクティブな OT 修復タスクの数。 OT 修復タスクの修復ターゲット日は、グループ内のアクティブな脆弱性一致アイテムに属する最も近い期日に設定されます。 修復ターゲットは、最後のオープン日に日数 (24 時間単位として測定) を加算して計算されます。 このレポートでは、保留された OT 修復タスクは除外されます。
経過時間別の OT VI	ヒートマップ	経過時間 (日数) 別にグループ化された OT のアクティブな脆弱性一致アイテムの数。
OT クローズ済み修復ターゲットステータス別の脆弱性一致アイテム	棒グラフ	選択した期間スパンにおける修正ターゲットステータス別にグループ化された、クローズされた OT 脆弱性一致アイテムの数。 i 注: [クローズした経過時間] の値は、データの収集時に計算されます。値は、last_opened の日付と収集ジョブの日時の差です。
リスク評価別の OT 脆弱性一致アイテム	棒グラフ	選択した期間スパンにおけるリスク評価によってグループ化さ

[脆弱性一致アイテム] タブのデータの可視化 (続く)

名前	タイプ	Description (説明)
		れたアクティブな OT 脆弱性一致アイテムの数。

[修正] タブのデータの可視化

名前	タイプ	Description (説明)
リスク評価とステータス別の OT 修復タスク	ヒートマップ	リスク評価とステータス別にグループ化されたアクティブな OT 修復タスクの数。
リスク評価とターゲットステータス別の OT 修復タスク	ヒートマップ	リスク評価と修復ターゲットステータス別にグループ化されたアクティブな OT 修復タスクの数。 このレポートでは、保留された OT 脆弱性一致アイテムは除外されます。
未アサインの OT 修復タスク	単一スコア	アサインまたはアサイン先グループのないアクティブな OT 修復タスクの数。
未アサインの OT 脆弱性一致アイテム	単一スコア	アサインまたはアサイン先グループのないアクティブな OT 脆弱性一致アイテムの数。

[例外] タブのデータの可視化

名前	タイプ	Description (説明)
理由別の保留された OT 脆弱性一致アイテム	棒グラフ	保留の理由によってグループ化された、保留された OT 脆弱性一致アイテムの数。

ドメインセパレーションと オペレーショナルテクノロジー

オペレーショナルテクノロジー アプリケーションでは、ドメインセパレーションがサポートされています。ドメインセパレーションでは、データ、プロセス、および管理タスクをドメインと呼ばれる論理的なグループに分けることができます。どのユーザーがデータを表示できるか、データにアクセスできるかなど、このアプリケーションのいくつかの側面を制御できます。

サポートレベル：ベーシック

- アプリケーションサービスプロバイダーのユースケースに合わせてデータが適切なドメインに送られるようにするビジネスロジックが存在します。
- このアプリケーションは、ドメインセパレーションを完全にサポートしています。ドメインセパレーションには、ユーザーインターフェイス、キャッシュキー、レポート、ロールアップ、および集計からのドメインの分離が含まれます。
- インスタンスのオーナーは、複数のテナント間で正常に機能するようにアプリケーションをセットアップする必要があります。

サンプルユースケース：サービスプロバイダーがチャットを使用してテナント顧客のメッセージに回答する場合、お客様がサービスプロバイダーの応答を確認できるようにする必要があります。

サポートレベルの詳細については、「[アプリケーションでのドメインセパレーションのサポート](#)」」を参照してください。

概要

オペレーショナルテクノロジーアプリケーションは、依存関係アプリケーションのドメインセパレーション機能を継承します。各アプリケーションは独自のドメインセパレーション関係を持つことができるため、オペレーショナルテクノロジー アプリケーションに関連付ける特定のサポートレベルはありません。詳細については、「[Domain separation and Workflow Studio](#)」」を参照してください。

関連情報

[サービスプロバイダーのドメインセパレーション](#) 