



ワシントン DC オペレーショナルテ クノロジーマネジメント

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

Operational Technology.....	5
Operational Technology Management 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
SU ライセンスのインストール ITOM.....	8
OTM のサブスクリプション統計情報の表示.....	9
割り当てられたサブスクリプションユニットに対するリソース使用率の確認OTM.....	9
OTM サブスクリプションで使用する CI 数の確認.....	10
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.....	12
OTM SU ライセンス参照.....	13
Operational Technology Manager.....	17
Operational Technology Manager の探索.....	18
の構成 Operational Technology Manager.....	29
Operational Technology Manager 統合.....	43
Operational Technology Manager を使用する.....	108
Operational Technology Manager 参照.....	163
産業用プロセスマネージャー.....	165
産業用プロセスマネージャー の詳細.....	166
の構成 産業用プロセスマネージャー.....	168
での使用産業用プロセスマネージャーOperational Technology Manager.....	188
産業用プロセスマネージャー 参照.....	208
Operational Technology Vulnerability Response.....	214
Operational Technology Vulnerability Response の詳細.....	215
Operational Technology Vulnerability Response の構成.....	225
Operational Technology Vulnerability Response 統合.....	236
Operational Technology Vulnerability Response の使用.....	254
Operational Technology Vulnerability Response 参照.....	257
オペレーショナルテクノロジーインシデント管理.....	266
オペレーショナルテクノロジーインシデント管理 の詳細.....	267
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.....	269
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.....	280
オペレーショナルテクノロジーインシデント管理 参照.....	290
オペレーショナルテクノロジー変更管理.....	293
オペレーショナルテクノロジー変更管理 の詳細.....	294
オペレーショナルテクノロジー変更管理 の構成.....	296
オペレーショナルテクノロジー変更管理 の使用.....	306
オペレーショナルテクノロジー変更管理 参照.....	319
オペレーショナルテクノロジーのナレッジ管理.....	321
オペレーショナルテクノロジーのナレッジ管理 の詳細.....	322
オペレーショナルテクノロジーのナレッジ管理 の構成.....	322

オペレーショナルテクノロジーのナレッジ管理 の使用.....331

オペレーショナルテクノロジーのナレッジ管理 参照.....339

ドメイン分離と Operational Technology.....342

Operational Technology

ServiceNow for Operational Technology 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、生産現場での稼働時間を最大化Operational Technologyでできます。

コアオペレーションにおける **Operational Technology** メリットと工場労働者のエンパワメント



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.



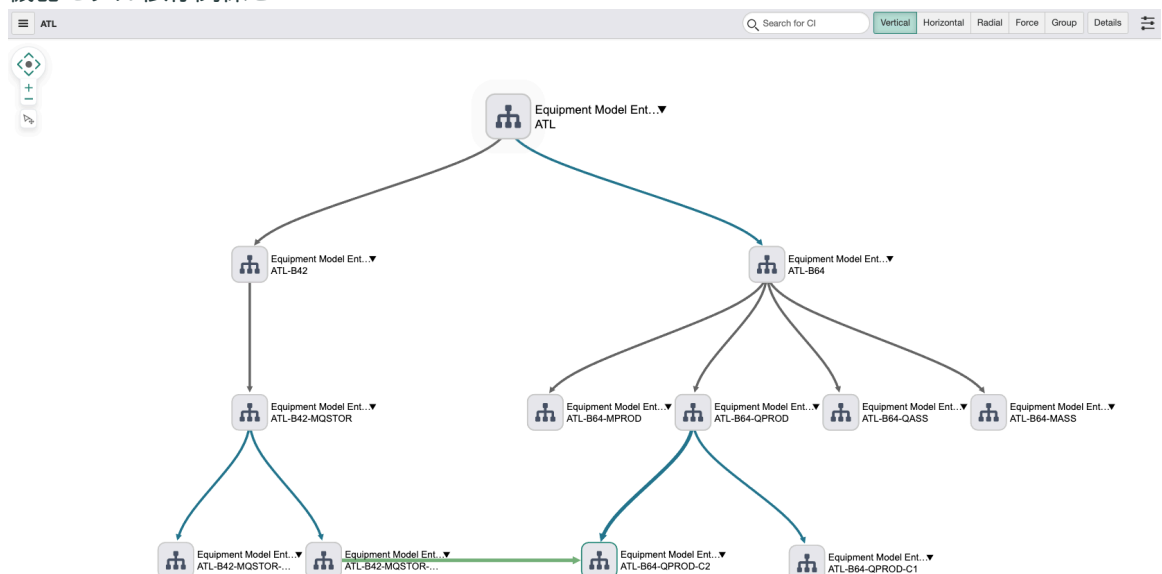
Factory Workers

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

Operational Technology Management による ServiceNow アップタイムの最大化と運用レジリエンスの構築

業界にオペレーショナルテクノロジーが導入される前は、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。彼らは、環境の全体像を把握し、そのすべてを保護、監視、管理することが困難であると感じていました。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かつコンテキスト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、システムの安全性を維持して稼働させ、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を評価し、優先順位を付け、対応できるようにすることもできます。

機器モデル依存関係ビュー



デジタル マップを使用することで、組織は産業運用プロセス、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より簡単かつ迅速に管理および評価できます。



注:

この Operational Technology Management ソリューションは、ではサポートされていません Now Mobile。

可視性の向上 	Operational Technology システムのコンテキストに応じた全体像を把握して、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、[ソリューションの概要](#) 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。
- 要求および設定 Operational Technology方法については、次を参照してください。
 - [の構成 Operational Technology Manager](#)
 - [の構成 産業用プロセスマネージャー](#)
 - [Operational Technology Vulnerability Response 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](#)
- がテーブルを管理および使用する共通サービスデータモデル (CSDM) 方法Operational Technologyの詳細については、「[Operational Technology テーブルと CSDM テーブル](#)」を参照してください。
- [の Operational Technology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 - Operational Technology リリースノート](#)。

アプリケーション

- Operational Technology Manager
- 産業用プロセスマネージャー
- Operational Technology Vulnerability Response
- 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
- サービス管理: IT Service Management 
- セキュリティ: Vulnerability Response 
- 可視性: IT Operations Management 

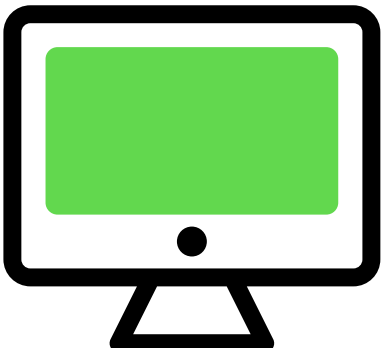
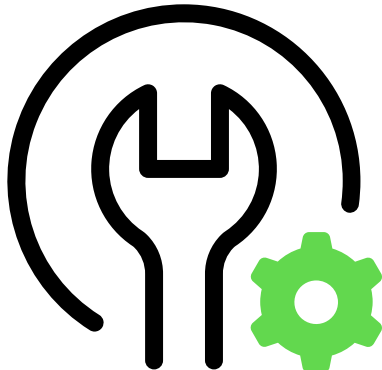
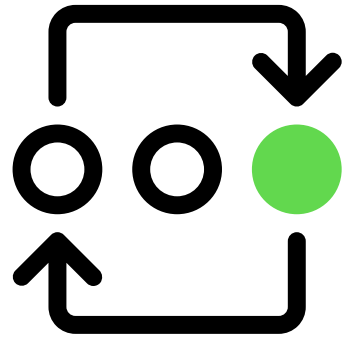
Operational Technology Management ライセンスとサブスクリプション

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の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サブスクリプションの使用OTM状況を計算して表示するため、重要な側面Operational Technology Management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、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のニーズに適応するための機能の拡張 OTM について情報に基づいた意思決定を行うことができます。OTMライセンスモジュールを使用して、製品 (ServiceNow OT Foundation、OT Visibility、ServiceNowServiceNow OT Vulnerability and Response) のサブスクリプション関連の詳細OTMにアクセスします。

開始するには

ライセンスの詳細を見るOTM	SU ライセンスのインストール ITOM 対象 OTM	ライセンス参照
		
サブスクリプション関連の詳細の詳細	プラグインの最新バージョンを更新します	ジョブスケジュール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

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

この ServiceNow プラットフォームは、製造業のライセンス管理に採用されています OTM。OTM には IT Operations Management (ITOM)、で見つかったライセンスと、ドメイン専用の OTM ライセンスが含まれます。

ライセンスと IT Operations Management (ITOM) 同様の方法でライセンスを監視し OTM ます。ServiceNow インスタンス内では、OTM **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。

SU ライセンスのインストール ITOM

[sn_itom_licensing] を ServiceNow ITOM SU Licensing 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ます。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の取得 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。システムが自動的にインストールされます ServiceNow ITOM SU Licensing。このアプリケーションの更新が利用可能 ServiceNow Store になると、通知を受け取ります。

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

- ジョブスケジュール
- テーブル

詳細については、「[の SU ライセンスとともに ITOM 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。



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ているアプリケーションサブスクリプションの数 OTM 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。
- 利用可能な最新バージョン ITOM の SU ライセンスをから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、組織のサブスクリプション使用率を評価し OTM、将来のサブスクリプション要件に備えます。

手順

1. 単品で購入したサブスクリプションのサブスクリプション情報 OTM を表示するには、次に移動します **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リソース使用率の確認OTM

製品で OTM 管理できるリソース統計を検討および分析し、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

を使用した**OTM ライセンスダッシュボード**場合のOTM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 日の平均を表示します。この機能は、日次カウントごとにドメイ

ン固有の情報と特定の CI リストを提供するため、リソース使用率を経時的に効果的に監視および分析できます。

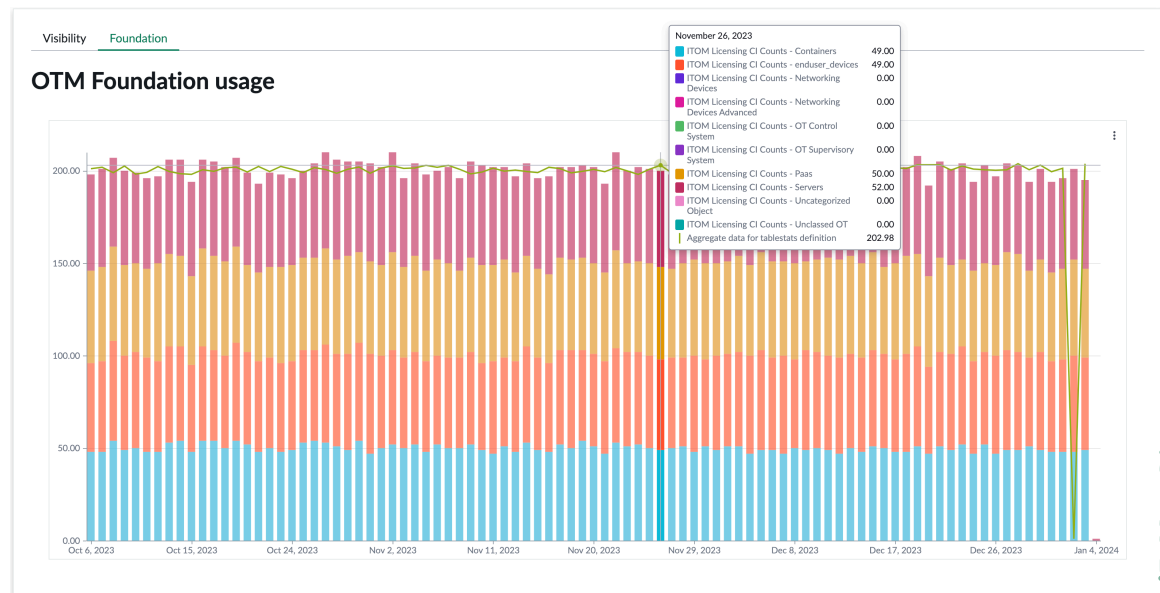
注:

SG-OT Excel によって管理される CI は、90 日より前、90 日以内、および 90 日より古い last_scan 日のライセンス消費についてカウントされ、一覧表示されます。

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、[基盤] を選択します。

OTM ライセンスダッシュボード



自動翻訳

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

直近 90 日間の CI データの日次カウントまたは平均を表示します。ServiceNowOT Foundation、OT Visibility、ServiceNowOT Vulnerability and Response は、ServiceNowアプリケーションがサポートするOTMライセンスリソースに関するインサイトを提供します。アプリケーションが検出、監視、およびプロビジョニングする OTM リソースは、CMDB に格納されている構成アイテム (CI) です。ライセンスモジュールは OTM、この CI 情報と組織で購入したサブスクリプションの情報を組み合わせて、アプリケーションで使用する OTM サブスクリプション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。
- 利用可能な最新バージョン ITOM の SU ライセンスをから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 ServiceNow に対して料金が発生します。サブスクリプションに含まれる OTM 製品と機能の詳細については、「」を参照してください [OTM へのサブスクリプション](#)。

ライセンス付与のために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) の日次カウントを計算し、その後、これらの CI カウント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で管理されている場合は、CI 数の重複を排除するための調整が行われます。
3. IT 構成アイテム (IT CI) が OT 構成アイテムとして分類される場合、CI は 1 回のみカウントされます (ライセンスではなく ITOM ライセンスの下で OTM)。
4. ライセンスモジュールは、アプリケーションの CI 数 OTM を統合して、過去 90 日間の日次 CI 数の平均を計算します。

i 注:

SG-OT Excel によって管理される CI は、90 日前以降、90 日以降、90 日以上前の last_scan 日のライセンス消費についてカウントされ、リストされます。

5. ライセンスモジュールは、アプリケーションの日次平均 CI 数 OTM と、顧客契約に記載されているライセンスの詳細を照合して、ライセンス関連の統計情報を生成します。

これにより、組織での購入したサブスクリプションユニットの利用状況に関する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: 90 日間にわたって収集された CI 数の平均を、CI タイプ別に分類して、個々の OTM アプリケーションごとに表示します。

i 注:

SG-OT Excel によって管理される CI は、90 日前以降、90 日以降、90 日以上前の last_scan 日のライセンス消費についてカウントされ、リストされます。

- 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: 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 の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数。

ドメイン別に分類された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 OTM。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.

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

各アプリケーション (ServiceNow OT Foundation、OT VisibilityServiceNow、ServiceNow OT Vulnerability and Response) についてOTM、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。
- 利用可能な最新バージョン ITOM の SU ライセンスをから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

生成された CI リストは、最新の日次 CI 数と強く関連しています。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. ライセンスされた CI を表示するアプリケーションを選択します。

- 基盤
- 可視性
- HLA
- 健全性

Application	Max Results	Status	Progress	Additional Filters for CIs
Foundation	10,000	Completed	1/10000	
Health	10,000		N.A.	
Visibility	10,000	Completed	1/10000	
HLA	10,000		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 (Populate licensable CIs)] 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。

レポートの処理が終了すると、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。

ITOM SKU の OTM [ライセンス可能な CI] ページには、ライセンスを持つ OTM 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、ライセンスとともに OTM インストールされるコンポーネント、製品のサブスクリプションフォーム OTM、およびライセンスダッシュボードの概要 OTM に関する貴重なインサイトを教えてください。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考資料にアクセスし、サブスクリプションとライセンス要件を効果的に管理 OTM するのに役立ちます。

の SU ライセンスとともに ITOM インストールされるコンポーネント OTM

SU ライセンス プラグインが有効になると OTM、いくつかのタイプのコンポーネント (ジョブスケジュールやテーブルなど) がインストールされます。

インストールされたジョブスケジュール

ジョブスケジュール	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	健全性の OTM ライセンス可能な CI のリストをコンパイルします。
ITOM Health ライセンス使用回数ストア	健全性の OTM 日次 CI 数を計算します。
OTOM ヴィジビリティライセンス CI リストストア	可視性のためにライセンス可能な CI のリストをコンパイルします OTM。
OTM 基盤ライセンス CI リストストア	Foundation のライセンス可能な CI のリストをコンパイルします OTM。
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 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	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。

テーブル	説明
[itom_lu_discovery_source_mapping]	
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。
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 of the リストが含まれています。
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 のリストが含まれています。
可視性 LU 一時 [visibility_lu_temp]	Discovery 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。
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

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。これにより、サブスクリプション管理を簡素化し、製品の使用状況を明確に OTM することができます。

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

アプリケーションの名前 OTM。

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なままになる期間。

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

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。ダッシュボードには、OTMアプリケーションごとに専用のレポートが用意されており、日次の使用回数と90日間のサブスクリプション・ユニットの平均使用率が視覚的に表示されます。ライセンスダッシュボードは OTM、ITOM ライセンスアプリケーションのバージョン 4.0 に不可欠なコンポーネントです。このダッシュボードには、 から ServiceNow Storeアクセスできます。

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、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バージョン履歴のリリースノート**」を参照してください。

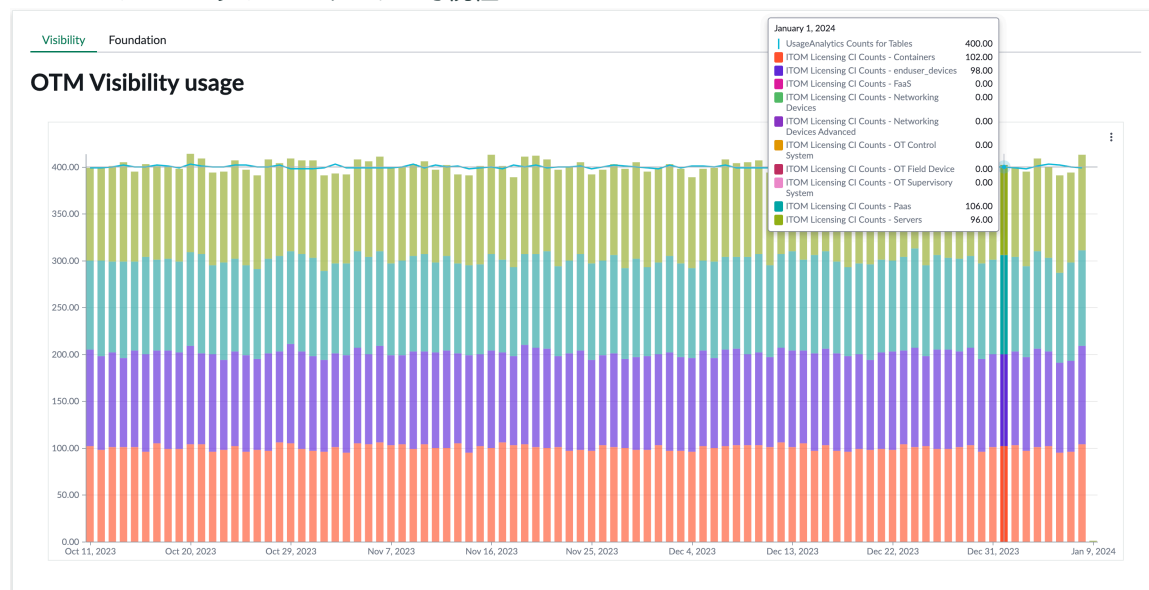
必要な Now Platform ロール

admin

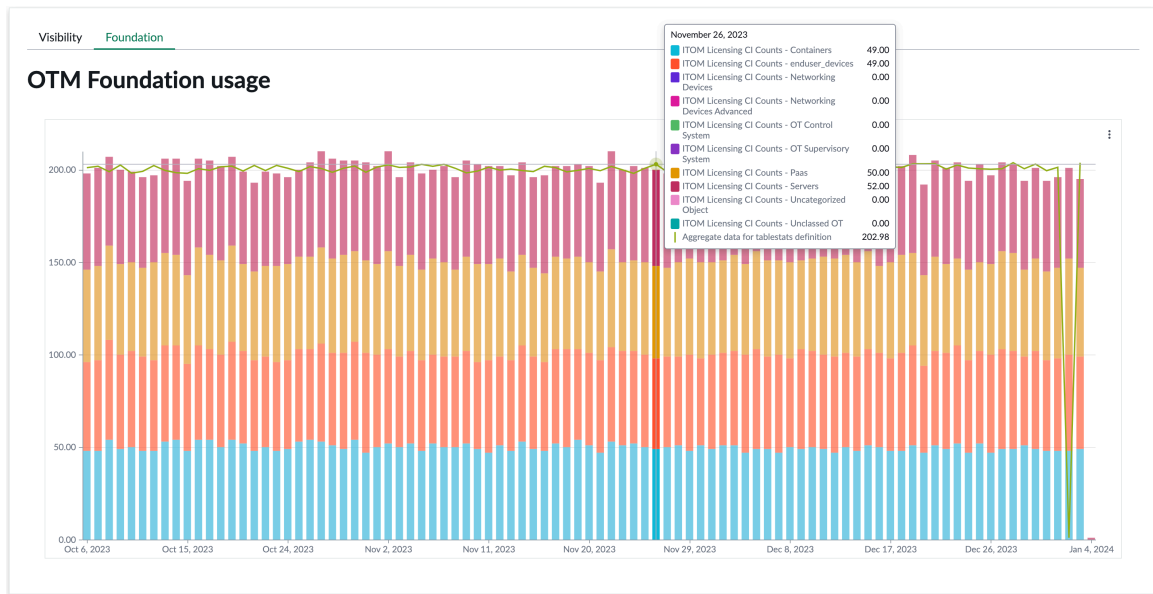
アセスメントダッシュボードへのアクセス

の OTM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 - 可視性



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。

データの表示方法

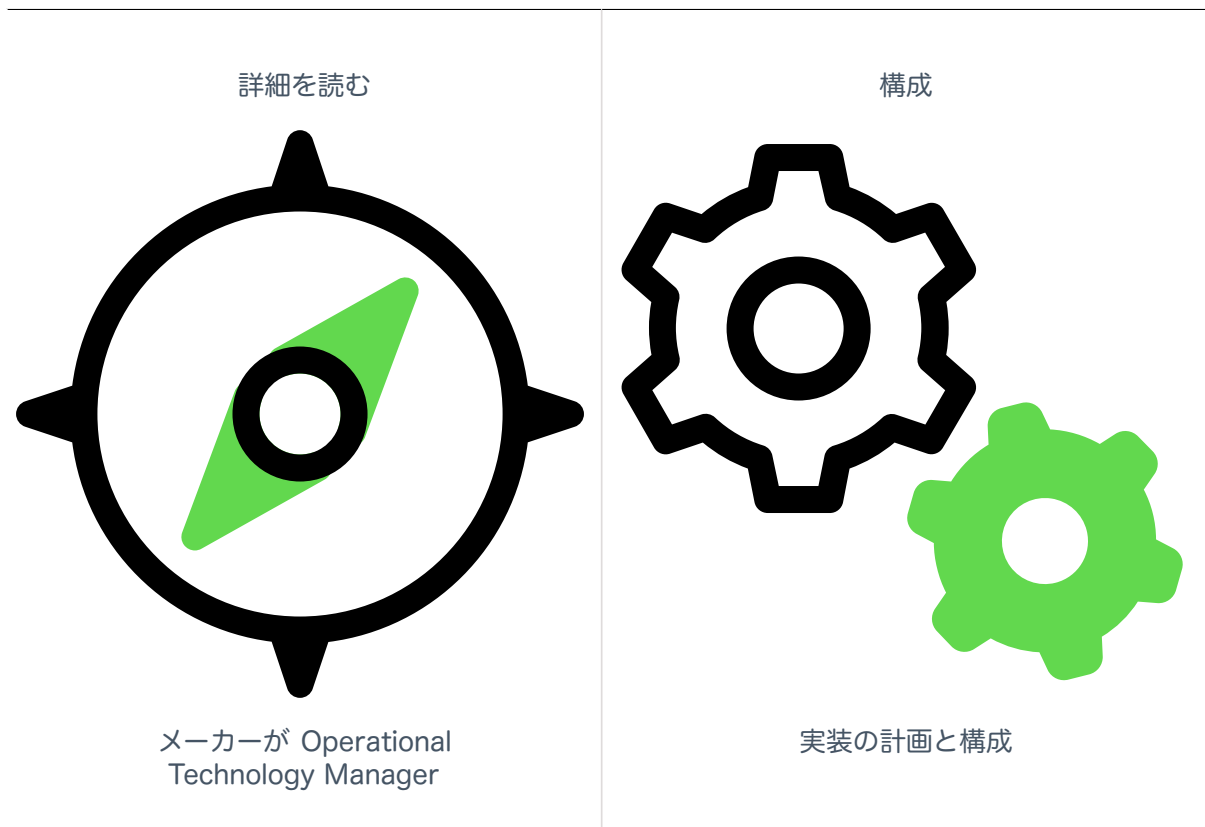
ダッシュボードには、次の可視化が含まれています。

タイトル	ソーステーブル	説明
OTM Visibility 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分析カウント [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	説明
		i 注: SG-OT Excel によって管理される CI は、90 日前以降、90 日前以降、90 日以上前のlast_scan日のライセンス消費についてカウントされ、リストされます。

Operational Technology Manager

アプリケーションはOperational Technology Manager、組織がソリューションを使用ServiceNow Operational Technology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。Operational Technology Manager は、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Now Platformの使用構成管理データベース (CMDB)をサポートしています。

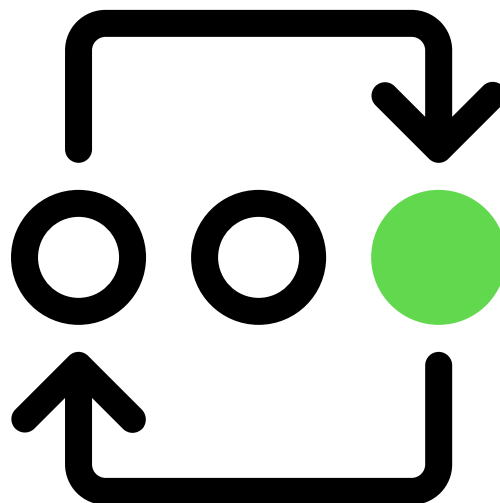


使用



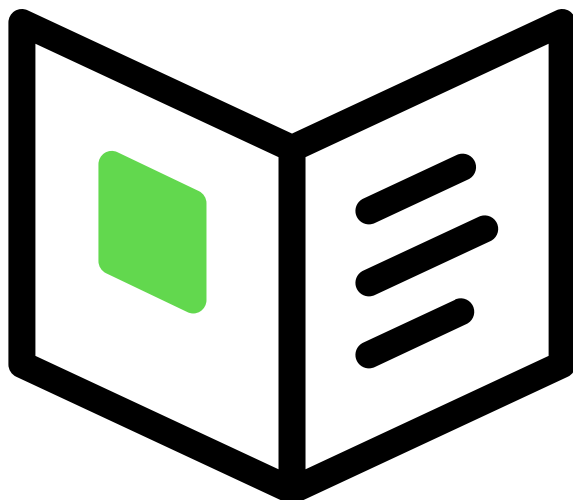
Operational Technology デバイスの
インポート、検出、およびレビュー

統合



他のアプリケーションと統合して拡張す
る Operational Technology Manager

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

Operational Technology Manager の探索

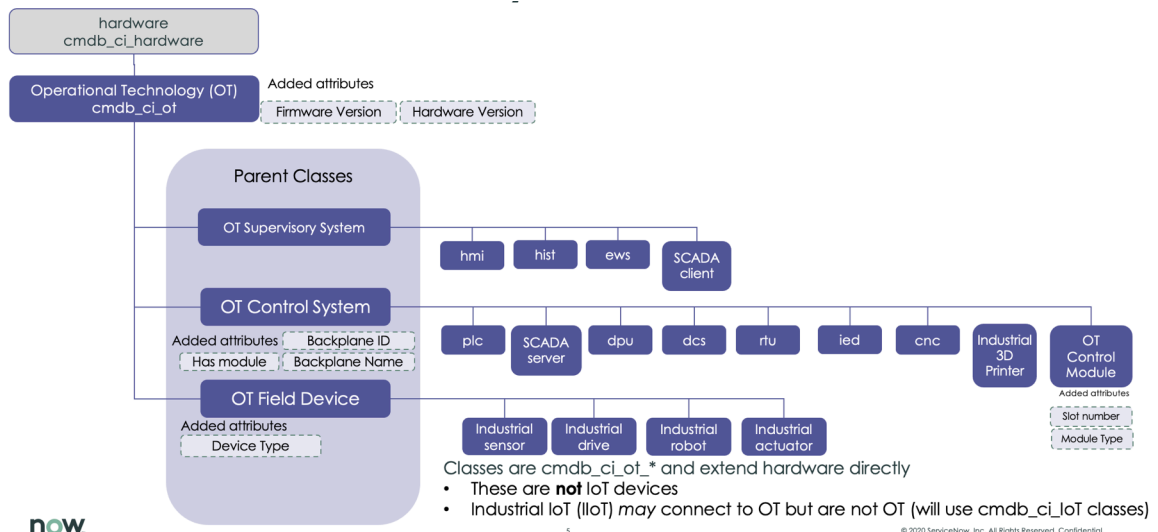
アプリケーションを使用して Operational Technology Manager、企業がソリューションを使用 ServiceNow Operational Technology できるようにするための基盤データと関係を作成する方法について説明します。

ではOperational Technology Manager、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Now Platformの使用構成管理データベース (CMDB)がサポートされています。

Operational Technology Manager (OT) 構成アイテム拡張クラス

Operational Technology Managerは、次の図に示すように、クラス階層を拡張する CMDB (OT) 構成アイテム (CI) 拡張クラスを使用しますOperational Technology。

OT CI 拡張クラスが OT デバイスと等しい



Operational Technology Manager 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 に入力し、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、「[オペレーション テクノロジ \(OT\) 拡張クラス](#)」を参照してください。

の CMDB CI クラス Operational Technology Manager

Operational Technology Manager は、CMDB CI Class Models アプリケーションの一部である 次の 構成管理データベース (CMDB) 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 CI クラスモデルアプリケーションを参照してください CMDB 。 [ServiceNow ストア](#)。

ワークフローの Operational Technology Manager CMDB CI クラス

クラス	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検出

既存の Operational Technology デバイス データを に Now Platform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)

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データをインポート Operational Technology できます サービスグラフ。抽出変換ロード (ETL) で 統合ハブ スプレッドシートを使用して、このデータを CMDB. 詳細については、「サービスグラフ コネクタ (Operational Technology Excel)」を参照してください。

Operational Technology 用の 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 レベルのデバイスを検出する Operational Technology には、for Operational Technology 機能を繰り返し実行 ディスカバリー します。これは、標準 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、これは ディスカバリー 通常、OT 検出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、「Operational Technology 用の 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、を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems。

サービスグラフ パートナーからの ServiceNow 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コネクタも提供しています サービスグラフ。

OT ネットワークと標準 IT ネットワークの違い

が 構成管理データベース (CMDB) ネットワーク内にある Operational Technology デバイスを処理する方法と、標準の情報技術 (IT) ネットワーク内のデバイスを処理する方法には違いがあります。

(ITOM) で Information Technology Operations Management 管理される構成アイテム (CI) は、では CMDB IT タイプとして分類されます。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に存在します。

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、次を参照してください [Operational Technology \(OT\) extension classes](#)。

次の図は、これらの違いを示しています。

Operational Technology 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、「」を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems。

Operational Technology [デバイスのランディングページ] タブ

[OT デバイス] ランディングページタブは、業種別 ワークスペース一元化された場所です。このタブを使用して、自分の Operational Technology Manager データ 産業用プロセスマネージャーを確認できます。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。

の 業種別 ワークスペース[OT デバイス] ランディングページタブでは、次のアクションを実行できます。

- 過去 1 週間に OT ネットワークで変更された OT デバイス情報を把握します。
- 産業施設全体の OT デバイス在庫の進捗状況を表示します。
- OT デバイスを有意義な方法で分析します。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。

ランディングページタブのコンテンツ

OT デバイスのランディングページタブで OT デバイスデータにアクセスするには、次に移動します: すべて > **Industrial Workspace** をクリックし、[ホーム] (🏠 アイコン) を選択して、[OT デバイス] タブを選択します。次の表で説明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、数、またはグラフのコンポーネントを選択します。

次の表では、[OT デバイス] ランディングページ 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 デバイスランディングページ (OT Devices landing page)] タブ

タイル	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。

[OT デバイスランディングページ (OT Devices landing page)] タブ (続く)

タイル	説明
	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 デバイスが検出されました	過去 7 暦日間に OT ネットワーク内の for Operational Technology およびその他の自動プロセスによってディスカバリー検出された新しい 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、マッピングされていない 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 (Unmapped)	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。 i 注: 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なため、このタイルは がインストールされている場合にのみ使用できます 産業用プロセスマネージャー。
カテゴリ別の OT デバイス	OT ネットワーク内の OT デバイスの数 (アサインされた OT デバイスタイプクラス別)。
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。

[OT デバイスランディングページ (OT Devices landing page)] タブ (続く)

タイトル	説明
	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。
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 レベル別に示す棒グラフ。 i 注: OT システムの Purdue レベルの詳細については、以下を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems 。
タイプ別の OT デバイス (トップレベル)	OT デバイスデータを OT デバイスタイプ別に分類した棒グラフ。
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 デバイスの数を割り当てられたメーカー別に示す円グラフ。
重要度別の OT デバイス	割り当てられた重要度別に OT ネットワーク内の OT デバイスの数を示す円グラフ。

OT ランディングページのフィルター

(OT) ランディングページのフィルター Operational Technology を使用して、ランディングページに表示するデータをサイト別または事業部門 (BU) 別に指定できます。たとえば、一度に複数のサイトの OT デバイスデータを表示できます。

概要

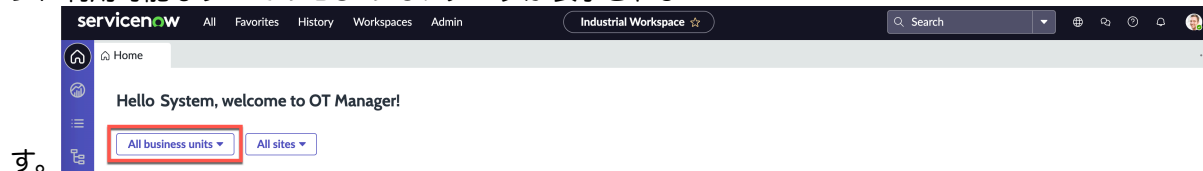
事業部門とサイトフィルターを使用すると、ランディングページに表示する OT デバイスまたは脆弱性データを指定できます。1 つ以上の事業部門とそれぞれの拠点を選択して、その OT データを 1 つの場所に 業種別 ワークスペース表示できます。

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、ランディングページに利用可能なすべての BU の OT データが表示されま



BU フィルターを設定すると、ランディングページには、選択した BU に含まれるすべてのサイトのデータが表示されます。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、選択した BU に関連付けられているサイトのみが含まれるようにサイトフィルターが更新されます。

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、「」を参照してください [OT ランディングページで事業部門とサイトフィルターを使用する](#)。

サイトフィルター

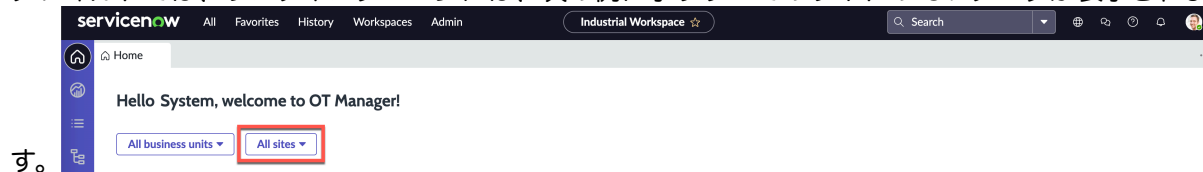
サイトフィルターを使用すると、次のアクションを実行できます。

- 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。
- サイトがアサインされていない OT データを表示します。

注:

OT デバイスにサイトが割り当てられていない場合、フィルターには [サイトが割り当てられていません] と表示されます。ランディングページ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、そのサイトに部署を割り当てる必要があります。

デフォルトでは、ランディングページには、次の例に示すすべてのサイトの OT データが表示されま



OT ランディングページで事業部門とサイトフィルターを使用する

(OT) ランディングページで事業部門 (BU) とサイトフィルター Operational Technology 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**.2. ホーム () アイコンを選択して、ランディングページを開きます。

3. 1 つ以上の BU の OT データを表示します。

- a. ランディングページのヘッダーで、[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 PT データを表示します。

- a. ランディング ページのヘッダーで、[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。ショートコードは、サイトの略語です。

OT デバイスのランディングページタブの設定

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、フィルターを含む **[OT デバイス]** ランディングページタブの設定を開始できるようにします。

の ガイド付きセットアップ**[OT デバイス]** ランディングページタブにアクセスするには、次に移動します: **すべて > Industrial Workspace 管理者 > ガイド付きセットアップ** をクリックし、の Operational Technology Manager**[OT デバイスランディングページ]** タブセクションを選択します。

[OT デバイス] ランディングページタブとそのコンテンツの詳細については、次を参照してください [Operational Technology \[デバイスのランディングページ\] タブ](#)。

次の表に、ガイド付きセットアップ**OT デバイス**のランディングページタブを設定できるタスクを示します。

OT デバイスのランディングページタブ ガイド付きセットアップ のタスク

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] ランディングページタブのすべてのパフォーマンスアナリティクスインジケータの日次データを収集して表示します。他のユーザーがランディングページタブを表示する前に、このステップ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レビューします。合計レコード数がデフォルト値の 100 万件を超えることが予想される場合は、レコードコレクション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] ランディングページ タブの事業部門フィルターに BU を表示します。

OT デバイスのランディングページタブ ガイド付きセットアップ のタスク (続く)

タスク	目的
	注: サイトに関連付けられている BU のみがランディングページに表示されます。
4. サイトを事業部門に割り当てます。	ユーザーがランディングページタブを BU でフィルタリングできるように、サイトを事業部門 (BU) にアサインします。

OT デバイスのデータ収集を構成する

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、(OT) デバイスのデータ収集 Operational Technology を構成します パフォーマンスアナリティクス。この構成により、OT データがランディングページ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 デバイスの日次データ収集ジョブがまだ実行されていない場合は、ランディングページタブに利用できるデータがなく、[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 デバイスの日次データコレクションジョブの実行を求める次の警告メッセージが表示されます。 OT

ⓘ No Data is shown on the dashboard because the 'OT Devices 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、管理者に問い合わせるように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 > データコレクター > パフォーマンスアナリティクス > ジョブ。
[OT デバイス] ランディングページ 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、[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、ランディングページ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、ジョブを最初の実行するとき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 デバイスのランディングページ] タブに、ユーザー用に収集された 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 ソースをレビューします。レコードコレクションを上書きして、ランディングページの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

を使用した パフォーマンスアナリティクス移行のため、**OT** デバイスのランディングページ 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の実行後にレコード数が 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の実行後にレコード数が 100 万件を超えた場合は、エラーメッセージが表示され、管理者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 データを上書きすることができます。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、次を参照してください [Indicator sources](#)。

注:

ジョブログには、インジケータソースに関するものでは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、ジョブログレコードを [レベル] 列でフィルタリングする必要があります。

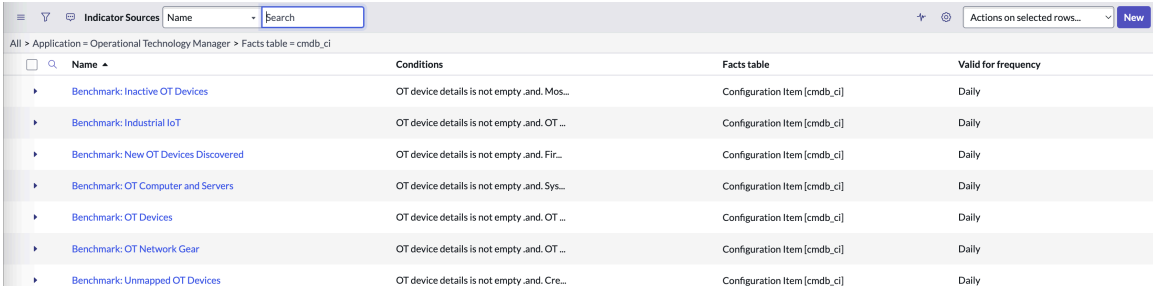
手順

1. 移動先 **すべて > 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. [フィルターを表示/非表示] () アイコンを選択してフィルターを適用し、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ー]
- [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。

調整が必要なインジケータソースは、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する] 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. [フェッチされたレコードの最大数] 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

ランディングページ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** デバイス] ランディングページ 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] ランディングページの 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ことで、他のユーザーは [OT デバイス] ランディングページ タブの事業部門フィルターの下に BU を表示できます。

手順

1. 移動先 **すべて > 組織 > 事業部門**.
2. **[New (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

フィールド	説明
名前	事業部門の名前。
会社	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。
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。事業部門は、サイトレコードまたは [サイト] リストに追加できます。

部署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 (OT) ランディングページをフィルタリング Operational Technology 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

サイトは、次の方法で事業部門に割り当てることができます。

- 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割り当てます。
 - 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 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。[部署] 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。

の構成 **Operational Technology Manager**

Operational Technology Managerソリューションのデータ基盤を作成できるように、アプリケーションを構成しますServiceNow Operational Technology。

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。	処理で使用するOperational Technologyためにクラス階層を拡張し構成管理データベース (CMDB) ます。
2. をインストールします Operational Technology Manager。	Operational Technology Manager アプリケーションをインストールします。
3. ロールをアサインします Operational Technology 。	各ユーザーが使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. コネクタのインポート用に サービスグラフ Excel スプレッドシートを準備しMicrosoftます。	にNow Platformアップロードする Excel スプレッドシートを作成し、Microsoft既存のOperational Technologyデータを入力します。 詳細については、「 コネクタインポート用のサービスグラフ 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の準備 」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。	データを にアップロード Operational Technology します 構成管理データベース (CMDB)。 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。
6. for Operational Technology 関数を実行しますディスカバリー。	産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルにあるデバイスを検出 Operational Technology (OT) します。 for Operational Technologyの詳細についてはディスカバリー、を参照してください Operational Technology 用の ディスカバリー 。
7. パートナーが提供する ServiceNow Service Graph Connector をインストールします。	パートナーが提供するコネクタは、ServiceNow Storeで利用可能になったときにインストールServiceNow, Inc.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] の選択肢を使用します。	Excel スプレッドシートをインポートした後、または for Operational Technology 関数を実行しディスカバリーした後、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。

のフレームワークの実装CSDMOperational Technology

フレームワークに従うことで CSDM 、レポートと分析の一貫した精度という主要な目標を確実に達成し、(OT) 環境を感情的に管理 Operational Technology できるようになります。

CSDM OT フレームワーク

フレームワークの実装 CSDM 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。

Operational Technology 製品ビュー

Operational Technology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、主要なエンティティがコア 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Operational Technologyを理解することです。

Operational Technology Manager

企業が Operational Technology 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、「[Operational Technology Manager](#)」を参照してください。

産業用プロセスマネージャー

Operational Technology 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。

Operational Technology Vulnerability Response

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、「[Operational Technology Vulnerability Response](#)」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

を有効にします。

Operational Technology および CSDM テーブル

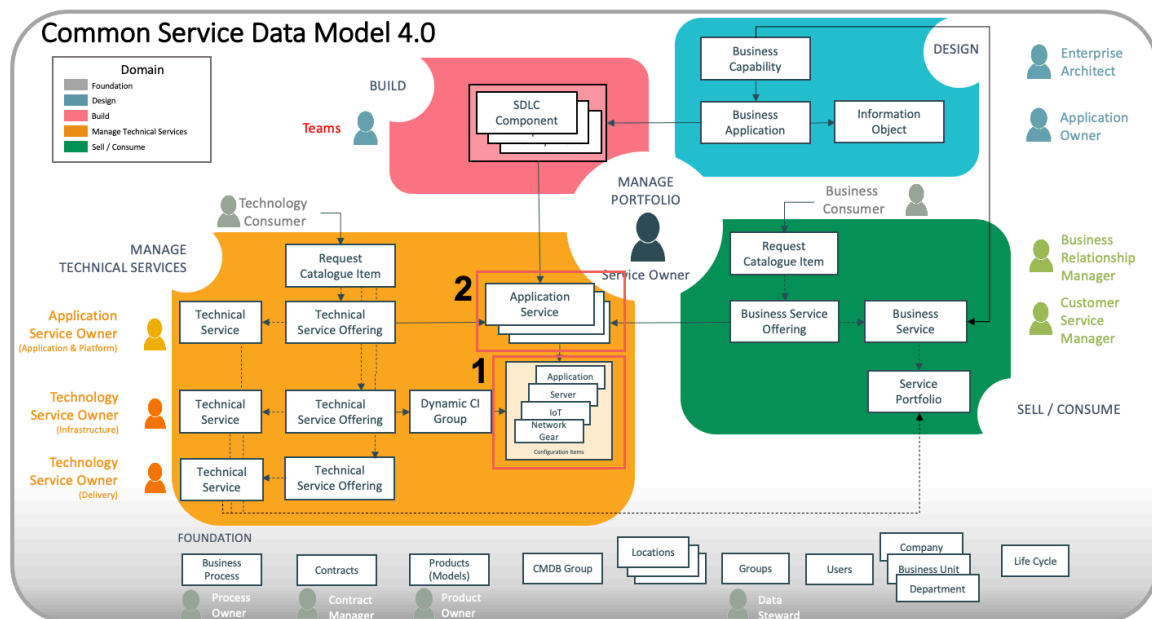
Operational Technology は CSDM テーブルを管理および使用します。いくつかの ServiceNow 製品は、Operational Technology のメリットを活用し、それに対して価値を付加します。

Operational Technology によって管理される CSDM テーブル

Operational Technology (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。

- Operational Technology 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。

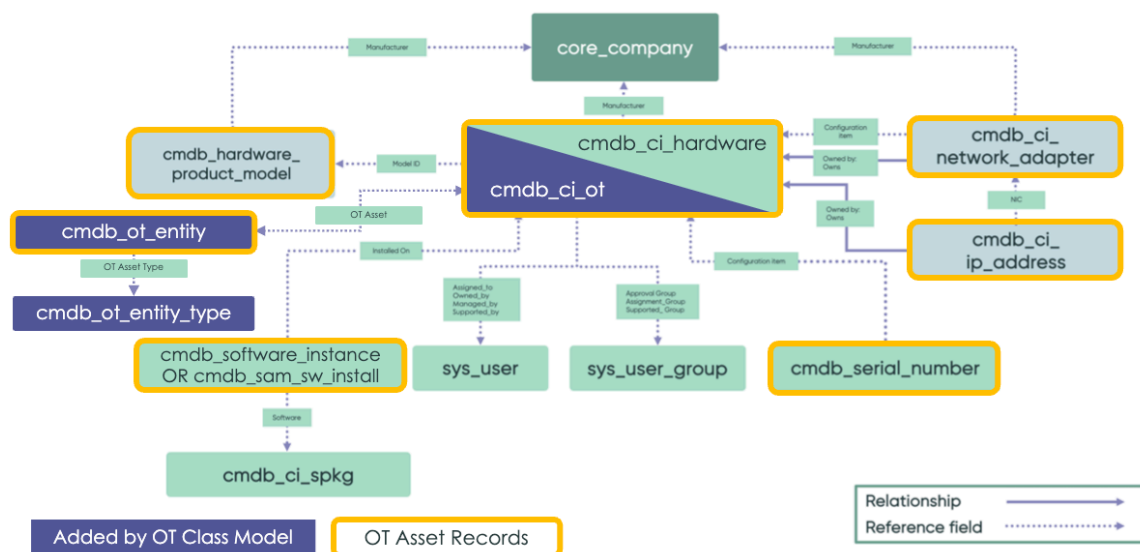


Operational Technology によって使用される CSDM テーブル

1. OT デバイス：

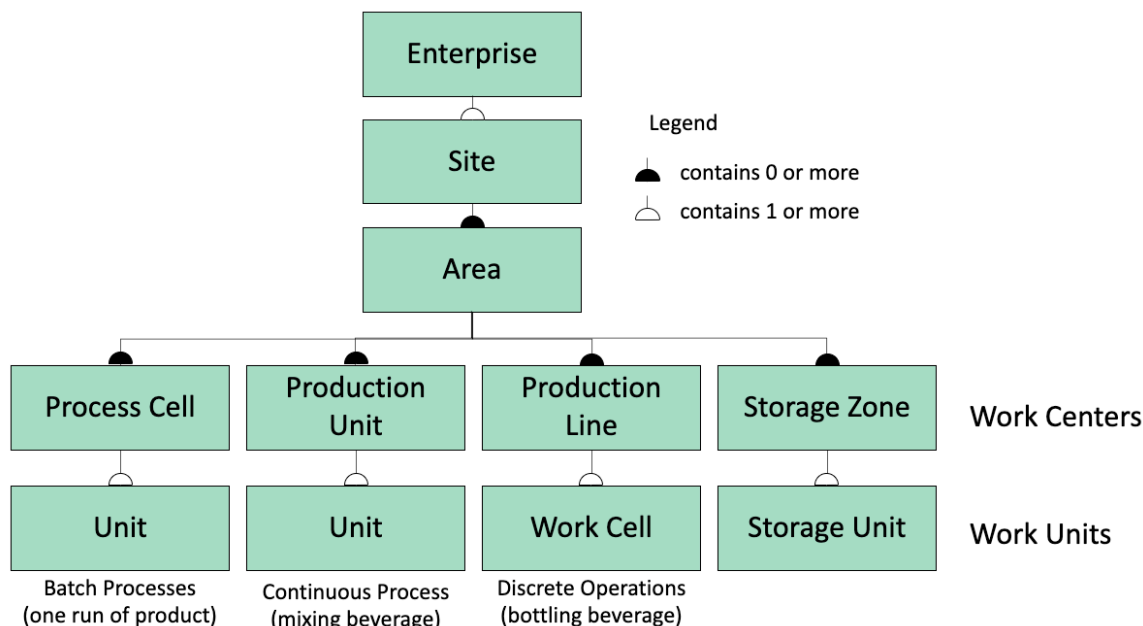
- ハードウェアを拡張することによって、Operational Technology ハードウェアクラス (cmdb_ci_ot) に対して構成アイテムクラスが作成されました。詳細については、「[Operational Technology \(OT\) extension classes](#)」を参照してください。
- OT デバイスの詳細 (cmdb_ot_entity) 参照を使用して OT デバイスの詳細を cmdb_ot_entity テーブルに追加することで、任意の CI クラス (関連する既存のハードウェアクラスおよび新しい OT クラス) を OT デバイスとして指定できます。OT 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。
- OT デバイスタイプでは、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：

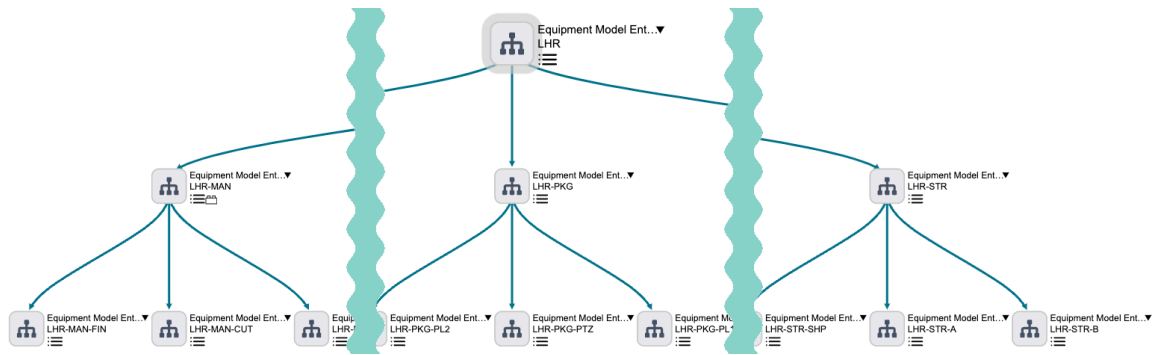
- a. 機器モデルエンティティクラスは、計算されたアプリケーションサービスを拡張し、次の目的で使用されます。
 - i. OT デバイスまたは機器モデルエンティティのサイトを表します。親のない機器モデルエンティティテーブル (cmdb_ci_ot_isa_entity) のレコードはサイトと見なされます。
 - ii. 生産プロセスの一部の ISA 機器モデルエンティティを表します。
- b. 機器モデルテンプレート (isa_entity_template) を使用して、産業環境にある機器モデルエンティティ間の関係をさらに記述することができます。
 - i. レベル (isa_entity_level) 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) はベースシステムに含まれています。

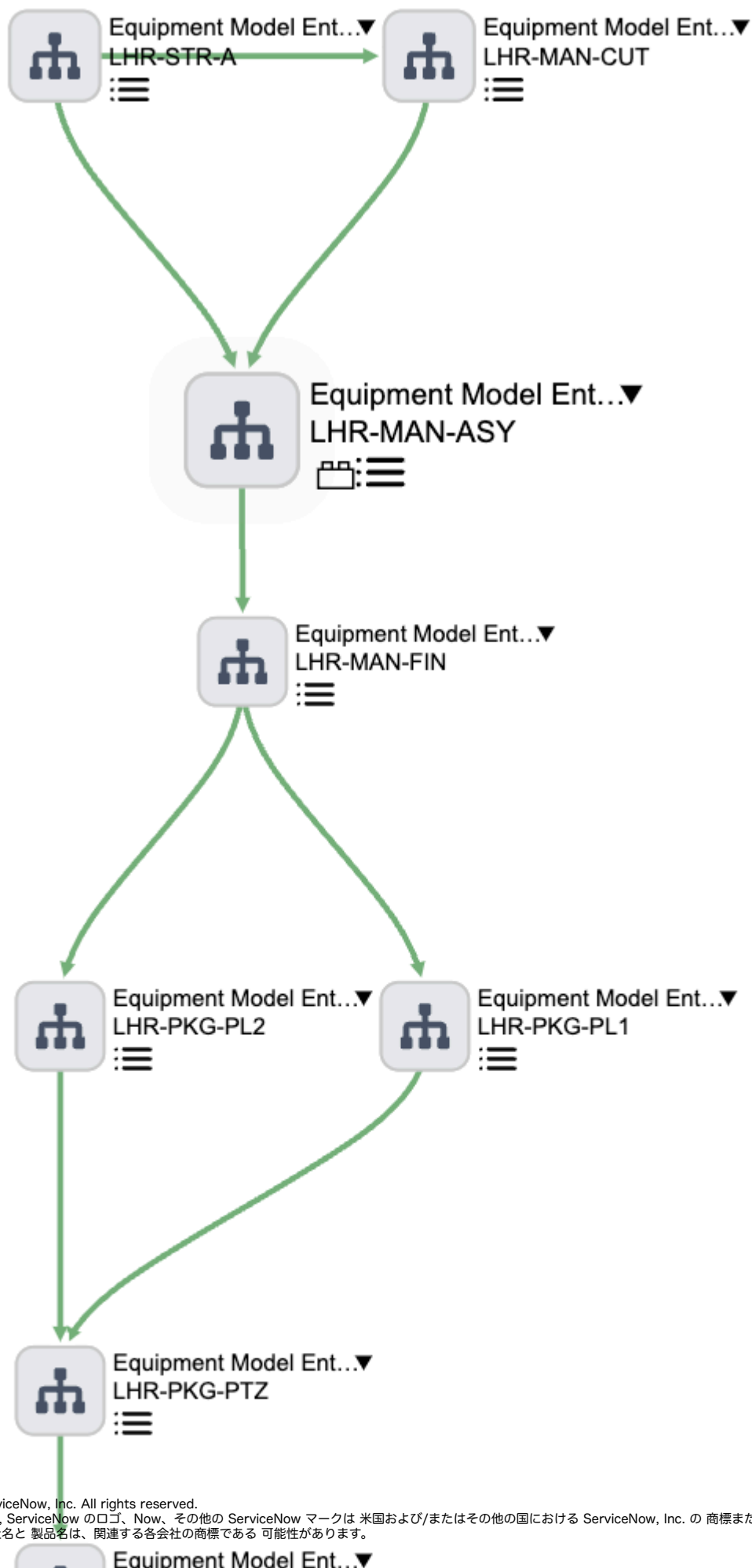


CSDM には、OT デバイスと機器モデルエンティティが互いにどのように関連しているかをより正確に区別する関係タイプ (Operational Technology固有) が含まれています。

- **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。





Operational Technology 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。

Operational Technologyのディスカバリー

Operational Technology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 Operational Technology Manager 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、業種別 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。

Operational Technology Vulnerability Response

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 (VI) レコードが作成されると、OT デバイスが VI 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正のための適切なローカルチームへの VI 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

を有効にします。

Operational Technology 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。

Operational Technology Manager のユースケース

このセクションでは、Operational Technology Manager のユースケースについて説明します。

Operational Technology Manager のユースケース

Operational Technology Manager アプリケーションは、Operational Technology 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。

の [OT デバイス] ランディングページタブには、業種別 ワークスペース 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] ランディングページタブの詳細については、次を参照してください [Operational Technology \[デバイスのランディングページ\] タブ](#)。

主な機能

- Operational Technology Manager 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 の検出は OT 固有のロールに制限され、OT 関連のメタデータを OT 検出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

Operational Technology Manager 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、Operational Technology 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。

Operational Technology Vulnerability Response のユースケース

Operational Technology Vulnerability Response 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。

主な機能

- 修正オーナーワークスペースは、脆弱性一致アイテム (VI) を本番プロセスにマッピングします。
- OT VI 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。
- VI で OT デバイスにアサインされたサイトに基づいて、修正オーナーに VI を自動アサインします。

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、Operational Technology Vulnerability Response 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？

の 業種別 ワークスペース [OT 脆弱性] ランディングページタブには、システムの脆弱性が要約されます。[OT 脆弱性] ランディングページタブの詳細については、次を参照してください [Operational Technology 脆弱性ランディングページタブ](#)。

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。

主な機能

ユーザーが業種別 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 デバイスや産業機器構成の変更に共同で取り組むことができます。

主な機能

- すべてのステークホルダーをつなぐデジタル化された変更ワークフロー。
- 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。
- およびOperational Technology Vulnerability Responseアプリケーションとオペレーショナルテクノロジーインシデント管理の統合オペレーショナルテクノロジー変更管理ワークフロー。
- 機器モデルエンティティの工場フロアの変更をダウンタイムスケジュールに合わせて調整します。

結果

次の例は、オペレーショナルテクノロジー変更管理 組織に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 修復オーナーは、脆弱性のグループを修正するための変更を開始したいと考えています。
- OT 構成とプラントエンジニアリングアクティビティを担当する OT 技術者は、産業フロアで誤動作しているロボットアームを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は、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 (OT) システムに関する情報 Operational Technology 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のに役立ちます。

主な機能

- ソリューションでOperational Technology Management既存のナレッジ管理 Now Platform の機能ものを使用する機能。
- 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ナレッジ記事を直接作成する機能。
- ナレッジマネージャーとナレッジユーザー用の OT ナレッジベースを構成する機能。
- でナレッジ記事を作成する機能。業種別 ワークスペース
- ナレッジ記事を公開、編集、廃止、または削除するための承認を要求する機能。
- 更新された情報を使用して既存のナレッジ記事を編集する機能。

結果

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

- 数年の経験を持つ OT エンジニアは、ガイドワーカーや経験の浅い技術者のために、OT デバイスの知識を 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労働者と技術者は、工場のフロアで問題に気付く、修正を説明するナレッジ記事を必要としています。

Operational Technology Request Management のユースケース

主な機能結果

Operational Technology 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。

Operational Technology 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。

Operational Technology (OT) 拡張クラスのインストール

の基盤Operational Technology Managerとなる (OT) 拡張クラスをインストールするOperational Technology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) を含むクラス階層を拡張し 構成管理データベース (CMDB) ます。AND サービスグラフ コネクタなどのディスカバリーアプリケーションは、これらのクラス拡張を使用して CI に入力し、さまざまなテクノロジーや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

Operational Technology Manager のインストール

管理者ロールをお持ちであれば、Operational Technology Manager 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ます。詳細については、次を参照してください。 [のエンタイトルメントの取得 ServiceNow 製品またはアプリケーション](#)。

i 注:

に必要な Operational Technology Manager 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

Operational Technology Manager 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

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表示の詳細については、「[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。

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 Operational Technology Manager 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、Operational Technology Manager 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 **Operational Technology Manager**

この Operational Technology Manager 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	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底 DAO クラス。
NIDSUtils	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。 Operational Technology (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の	デバイスに Discovery Operational Technology を使用する際に役立つユーティリティ。
OTBaseDAO(オーティープベースダオ)	すべての DAO クラスが Operational Technology 拡張する必要がある基底 DAO クラス。
OTFoundationConstant	他のスクリプトインクルードによって使用される定数のコレクション。
OTUtil	ユーティリティ メソッドの Operational Technology コレクション。
SGOTDeviceConstants	Service Graph Connector によって Operational Technology 使用される定数のコレクション。
SGOTDeviceTransformUtil	Service Graph Connector の Operational Technology 変換ユーティリティメソッドのコレクション。
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ためのベースパターン。
SGOTTroubleShootHelper	Service Graph Connector の構成を検証するためのヘルパーメソッド。
OTAssetFilterAjax	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 業種別 ワークスペースユーティリティクライアントスクリプト。
OTBulkEditHandler	フローアクションとジョブスケジュール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	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.

名前	説明
	getDeviceCMDBClassNameWithSysId;2. getComputerType です。

Operational Technology Manager ロールの割り当て

ユーザーにロールをアサインすると、Operational Technology Manager 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、Operational Technology Manager アプリケーションを使用できます。

サイト ユーザーを構成する場合は、機器モデル エンティティのサイト ユーザーのユーザー基準を作成して割り当てることができます。詳細については、「[管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)」を参照してください。

ロール	説明
Operational Technology ディスカバリー 管理者 [ot_discovery_admin]	for プロセスを実行できますディスカバリーが、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 Operational Technology (OT) エンティティにアクセスすることはできません構成管理データベース (CMDB)。Operational Technology詳細については、「 Operational Technology検出スケジュールを作成し、プロセスを実行するディスカバリー 」を参照してください。
Operational Technology Manager ビューアー [cmdb_ot_viewer]	(OT) デバイスレコードへの Operational Technology 読み取り専用アクセス。
Operational Technology Manager 編集者 [cmdb_ot_editor]	運用テクノロジー (OT) 拡張クラス に対する作成、読み取り、更新、および削除アクセス権。
Operational Technology Manager 管理者 [cmdb_ot_admin]	(OT) デバイスレコードに対する Operational Technology 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、「 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。

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。

Operational Technology Manager 統合

Operational Technology Manager 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、次のサードパーティ統合がサポートされています。

- Claroty CTD のサービスグラフコネクタ統合
- サービスグラフ(Azure)用Microsoft Defender for IoTコネクタ
- サービスグラフ コネクタ (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

Cloty Continuous Threat Detection (CTD) をアプリケーションと ServiceNow Operational Technology Manager 統合して、検出されたデバイスと Cloty CTD サイト (センサーまたはネットワーク侵入検知システムアプライアンス) をインポートします。

ストアでアプリを要求する

[ServiceNow ストア](#) 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メモ情報については、「[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

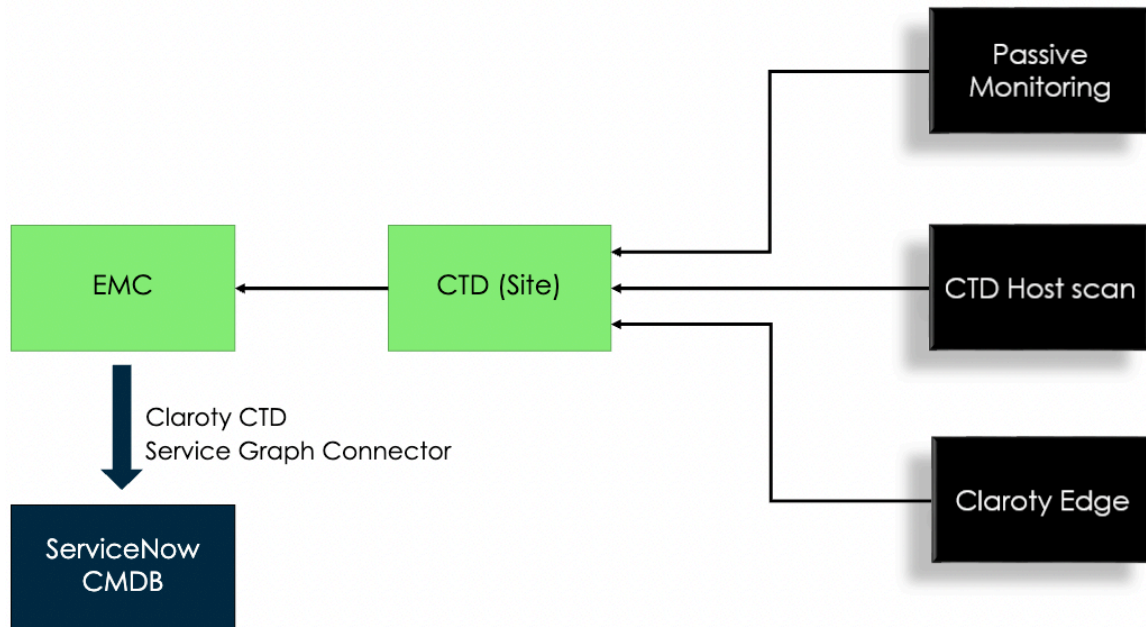
- Claroty CTD バージョン:2.0.1 以降
- サポートされている ServiceNow バージョン:
 - ユタ
 - バンクーバー
 - ワシントン

ユースケース

アプリケーションで Operational Technology Manager を使用してClaroty Continuous Threat Detection のサービスグラフコネクタ統合、次の情報を にインポートします。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測定基準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。統合ダッシュボードで CMDB の統合の監視の詳細については、「[」](#)を参照してください [Integration Commons for CMDB](#)。

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、構成アイテム (CI) クラス定義に変換されます ServiceNow CMDB。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、に含まれる Claroty CTD のサービスグラフコネクタ統合 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	スタギンテーブル
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	スタギングテーブル
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 パッケージのエントタイトルメントに基づいて ServiceNow 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、次の Claroty CTD のサービスグラフコネクタ統合 表に示すデフォルトのクエリパラメーターフィルターが使用されます。

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	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アドレスタイプはインポートされません。
ghost_exact	false	Claroty CTD にゴーストとして分類されたデバイスがある場合、デフォルト値が false に設定されているため、Claroty CTD 向けサービスグラフコネ

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	説明
		クタ統合で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

の Claroty CTD のサービスグラフコネクタ統合 ガイド付き設定を使用して、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 store app](#)。
- ITOM Discovery 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、「[Discovery 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. アプリケーションがアプリケーションピッカーを使用するように Claroty CTD のサービスグラフコネクタ統合 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、[開始するには] を選択します。
4. を構成する MID サーバーには、次の手順を実行します。
 - a. [接続と資格情報のセットアップ] セクションで、[MID Server を構成] タスクを選択します。
 - b. 構成が完了したら、[MID サーバー完了としてマーク] 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. [接続と資格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. [設定] 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. を使用している場合は、MID サーバーレコードの **[MID Server を使用]** チェックボックスをオンにします。

注:

を使用していない場合は、MID サーバー手順 5g に進みます。

- f. [詳細 MID サーバー 設定] 関連リストから、[MID 選択] を選択します MID サーバー。

- g. [更新] を選択します。

- h. 手順 5a から 5h を繰り返して、**Claroty CTD EMC Base** 認証 レコードを更新します。

6. 資格情報レコードを設定するには、次の手順を実行します。

- a. [接続と資格情報のセットアップ] セクションで、[資格情報の構成] タスクを選択します。

- b. [設定] を選択します。

- c. 資格情報テーブルの Claroty CTD EMC Base Auth レコードを開きます。

- d. [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. [接続と資格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、推奨される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は、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、非本番環境用に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。

イントラネットのレコード値

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 Server 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	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.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。デフォルト値はページあたり 500 レコードです。

プロパティ	説明
	i 注: ページあたりのデバイスの最大数は 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.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、前回の正常な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、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.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	説明
	注: インストールされた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.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を分単位で設定するプロパティ。時間が経過すると、Service Graph Connector は次のインポート中に新しい 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。 注: 値を変更して、同じトークンを最大 24 時間保持し、REST 呼び出しの数を減らすことができます。
sn_clarotyctdsgc.classify_based_on_os	の一部として OS Claroty CTD のサービスグラフコネクタ統合による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、Service Graph Connector 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、「」を参照してください 対象となる CMDB クラス。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は、Claroty タイプコードを 0\$1 として入力します。

プロパティ	説明
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 および 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 および 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. **[Save (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サイトの構成」セクションで、「CTDサイトのインポート」タスクを選択します。

b. **[設定]** 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 サイトの構成] セクションで、[NIDS の構成] 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 を設定したら、[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. **[設定]** を選択します。

c. [スケジュール設定済みデータインポート] テーブルで、[**SG-OT CTD** サイトのインポートスケジュール] 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午前 0 時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レビューまたは変更します。

アクション	説明
条件スクリプトの入力	[条件付き] を選択してインポートスケジュール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を変更する	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] テーブルでユーザーを参照します。

アクション	説明
	注: デフォルトでは、このフィールドは [システム管理者] 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 ロールを割り当てる必要があります。空のままにした場合、インポートスケジュールはログインしている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、すべてのレコードをインポートすることも、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インポートすることもできます。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. [Configure Import Schedules] セクションで、[Configure Devices Import Schedule] タスクを選択します。
- f. [設定] 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** デバイスのインポートスケジュール] 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。
 - デバイスは CTD サイトによって照会されます。Service Graph Connector 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レビューまたは変更します。

アクション	説明
条件スクリプトの入力	[条件付き] を選択してインポートスケジュール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を変更する	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	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] テーブルで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 [システム管理者] 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 ロールを割り当てる必要があります。空のままにした場合、インポートスケジュールはログインしている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、すべてのレコードをインポートすることも、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インポートすることもできます。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. [設定] を選択します。

- k. [スケジュール設定済みデータインポート] テーブルで、[**SG-OT CTD** ベースラインインポートスケジュール] 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実行し、必要に応じてインポートスケジュールをレビューまたは変更します。

アクション	説明
条件スクリプトの入力	[条件付き] を選択してインポートスケジュール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を変更する	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	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] テーブルで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 [システム管理者] 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 ロールを割り当てる必要があります。空のままにした場合、インポートスケジュールはログインしている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、すべてのレコードをインポートすることも、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インポートすることもできます。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. [設定] を選択します。

o. [スケジュール設定済みデータインポート] テーブルで、[**SG-OT CTD** インストール済みプログラムのインポートスケジュール] を選択して、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、毎日真夜中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実行し、必要に応じてインポートスケジュールをレビューまたは変更します。

アクション	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。
デフォルトのインポートスケジュールを変更する	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	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] テーブルで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 [システム管理者] 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 ロールを割り当てる必要があります。空のままにした場合、インポートスケジュールはログインしている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、すべてのレコードをインポートすることも、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インポートすることもできます。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: を Claroty CTD のサービスグラフコネクタ統合トラブルシューティングするには、次の手順を実行します。

- a. [[オプション] サービスグラフコネクタ for Claroty CTD のトラブルシューティング (Troubleshooting the Service Graph Connector for Claroty CTD)] セクションを選択します。
- b. [検証スケジュール設定済みジョブの実行] タスクで、[構成] を選択します。
- c. [今すぐ実行] を選択します。
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、検証結果によって問題が報告され、トラブルシューティング手順が提案されます。スケジュール設定済みジョブが終了するまで待ちます。
- d. ジョブスケジュールが完了したら、「[オプション] Claroty CTD 向け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。

注:

スケジュール設定済みスクリプトは、の初期設定 Claroty CTD のサービスグラフコネクタ統合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、次に移動します: 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** > **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、次の場所に移ります。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**.

の使用中に発生した問題のトラブルシューティングの詳細については、「」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 [Service Graph Connector Integration for Claroty CTD \(KB1502041\)](#) のトラブルシューティングシナリオ。

NIDS センサーの検証

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を準備します。センサーはデバイス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。Service Graph Connector 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

[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。[ライフサイクルステージステータス] フィールドが [使用中] に設定されている場合、検証は成功しています。

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割り当てるセンサーの値を追加します。
4. [NIDS 管理者構成] 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用に **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用に 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、すべてのデバイスの 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、属性のデフォルトのリストです。

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

サービスグラフ接続フレームワークの使用

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 Claroty CTD 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 か所に収集します。

始める前に

必要なロール: admin

このタスクについて

個別のデータソース、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 Claroty CTD のサービスグラフコネクタ統合 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 接続フレームワークでは、すべての関連データソースと Claroty CTD 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 (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 **Service Graph Connector Integration for Claroty CTD** 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. [Service Graph 接続] ページで、[**SG-OT Claroty CTD** 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、[**Service Graph** 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、[**Service Graph** 接続データソース] 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、[**Service Graph** 接続のスケジュール設定済みデータインポート] 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、[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 [状態] と [提案] に、失敗した手順の状態とトラブルシューティングの提案がそれぞれ表示されます。

CMDB でターゲットとなるクラス **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
Last discovered (最後に検出)	last_discovered
ファームウェアバージョン	firmware_version
OS バージョン	os、os_version

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	属性の名前
デバイスクラス名	device_class_name
初回確認日	first_seen
最終確認日	last_seen
最初の検出	first_discovered
シリアル番号	serial_number
モデル番号	model_number
メーカー	manufacturer
ベンダー	vendor

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
IP アドレス	ip_address
IP バージョン	ip_version

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

OT デバイスの詳細 [cmdb_ot_entity]

OT デバイスの詳細 [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	属性の名前
OT デバイスタイプ	ot_device_type
ビジネス上の重要度	business_criticality
OT 相関 ID	ot_correlation_id
Purdue レベル	purdue_level
ゾーン	zone

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	属性の名前
スロット	スロット
名前	名前
ファームウェアバージョン	firmware_version
モデル	モデル
シリアル番号	serial_number
メーカー	manufacturer
ベンダー	vendor

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	属性の名前
Last discovered (最後に検出)	last_discovered

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

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、アプリケーションに付属しています Claroty CTD のサービスグラフコネクタ統合。

i 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
eAVサーバー	(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ー = 48
eBluetoothデバイス	(空)	cmdb_ci_iot		eBluetoothデバイス = 41
電子ブロードキャスト	(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
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
eコントローラー	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eコントローラー = 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

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
eDomainController	(空)	cmdb_ci_server		eDomainController = 5
eエレクトリカルドライブ	産業用ドライブ	cmdb_ci_ot_industrial_drive	industrial_drive	eElectricalDrive = 68
eエンドポイント	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
eゲートウェイ	(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	eGPSClock = 37
eGPSDevice	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	歴史	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の	IED	cmdb_ci_ot_ied	led	eIED = 19
eインフュージョンポンプ	(空)	cmdb_ci_iot		電子注入ポンプ = 46
eMediaServer(イーメディアサーバー)	(空)	cmdb_ci_server		eMediaServer = 54
eMedicalデバイス	(空)	cmdb_ci_iot		eMedicalDevice = 47
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

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
eNTPServer	(空)	cmdb_ci_server		eNTPサーバ = 21
eOPCServer (英語)	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		eプロキシサーバー = 28
eRemotelIOの	OT フィールドデバイス	cmdb_ci_ot_field_device	ot_field_device	eRemotelIO = 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	eRobot = 57
eルーター	ルーター	cmdb_ci_ip_router		eルータ = 11
eRTU (英語)	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	eセンサー = 67
イースマートライト	(空)	cmdb_ci_iiot		eSmartLight = 51
eスマートフォン	(空)	cmdb_ci_iiot		eSmartPhone = 44
イースマートウォッチ	(空)	cmdb_ci_iiot		eSmartWatch = 45
eStorageArray(eストレージレイ)	(空)	cmdb_ci_server		eストレージレイ = 36
eStreamer	(空)	cmdb_ci_iiot		eStreamer = 52
eスイッチ	(空)	cmdb_ci_ip_switch		eスイッチ = 12
eSyslogServer	(空)	cmdb_ci_server		eSyslogServer = 25
eTerminalServer (英語)	(空)	cmdb_ci_server		eTerminalServer = 24
eTVScreen	(空)	cmdb_ci_iiot		eTVScreen = 40

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
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		eベンディングマシン = 43
eVideoRecorder (イービデオレコーダー)	(空)	cmdb_ci_server		eVideoRecorder = 64
eVirtualizationServer	(空)	cmdb_ci_server		eVirtualizationServer = 65
eVoip電話	(空)	cmdb_ci_comm_hardware		eVoip電話 = 39
eVoipサーバー	(空)	cmdb_ci_server		eVoipサーバー = 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
eバイオメトリックスキャナー	(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	eVisionカメラ = 76
eVisionController (英語)	OT コントロールシステム	cmdb_ci_ot_control_system	ot_control_system	eVisionController = 78
eVisionSensor (電子ビジョンセンサー)	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
eVulnerabilityスキャナー	(空)	cmdb_ci_server		eVulnerabilityScanner = 70

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

アプリケーションとServiceNow Operational Technology Manager統合Microsoft Defender for IoT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 ストア 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メモ情報については、「[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

- サポートされている Microsoft Defender for IoT センサーのバージョン：
 - 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

アプリケーションで ServiceNow Operational Technology Manager (Azure 用のMicrosoft Defender for IoTコネクタを使用してサービスグラフ、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

コネクタ (Azure) のサービスグラフMicrosoft Defender for IoT ガイド付き設定では、インスタンスの統合を構成するための整理された順序のタスクが提供されます。ガイド付きセットアップにアクセスするには、「[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測定基準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。統合ダッシュボードで CMDB 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

(Azure) データソースのMicrosoft Defender for IoT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、構成アイテム (CI) クラス定義に変換されServiceNow CMDB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、(Azure) アプリケーションからMicrosoft Defender for IoT定期的にデータをプルするように統合を構成できます。

次の表は、(Azure) プロジェクトに含まれるMicrosoft Defender for IoT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ています。

()Azure のデータ Microsoft Defender for IoT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 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 [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 [cmdb_ci_hpux_server]
- HVAC機器 [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]

() プロジェクトからMicrosoft Defender for IoTデータを取得するときにデータが保存される場所の詳細については、を参照してください対象となる **CMDB クラス**。Azure

サービスグラフ(**Azure**)の**Microsoft Defender for IoT**コネクタを設定します

(Azure) のMicrosoft Defender for IoTコネクタのサービスグラフガイド付き設定を使用して、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 store app](#)。
- ITOM Discovery 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、「[Discovery 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 コネクタ 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 ()Azure アプリケーションのMicrosoft Defender for IoTコネクタ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、[開始するには] を選択します。
4. リソースにアクセスする Azure には、次の手順を実行します。
 - a. [リソースへのアクセス Azure] 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. [接続と資格情報の構成] セクションで、[接続と資格情報のセットアップ] タスクを選択します。
 - b. [設定] 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 & 資格情報の作成] 関連リンクを選択します。
 - e. [接続および資格情報を作成] ウィンドウで、次のフィールドに入力します。

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 の値に置き換えます。

注:

トークンの生成が成功すると、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 フローに失敗しました 」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. [接続と資格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、推奨される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構成します。

プロパティ	説明
sn_msftd4iotazsgc.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_msftd4iotazsgc.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_msftd4iotazsgc.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。
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 (チェックボックスをオン)、デルタを取得するか (ボックスをオフ) を選択できます。 - デルタでは、で最後に成功したインポート CMDB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。 i 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	デバイスサポート用にこのプロパティを設定します。

プロパティ	説明
	- このシステムプロパティは、デバイスのインポート時に提供された Microsoft Azure センサー名を小文字に変換するために使用されます。 - これは、小文字形式のクエリにデータが期待されるため、必要です Microsoft Azure。
sn_msftd4iotazsgc.filter.device_sub_types	サブタイプで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サブタイプのカンマ区切りリスト Microsoft Azure。 - たとえば、PLC とサーバーのみをインポートするには、DeviceSubType 属性から [サーバー、PLC] の値 Microsoft Azure を指定します。
sn_msftd4iotazsgc.filter.device_tags	このプロパティを設定して、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します。 - デバイスのフィルタリングに必要な大文字と小文字を区別するタグのカンマ区切りリスト。 - 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、の Microsoft AzureDeviceTags 属性から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。 - 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 照会言語」を参照してください。

c. **[Save (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. [設定] 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、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. 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. [インポートスケジュールの構成 (Configure Import Schedules)] セクションで、[構成] を選択します。
- b. [**SG-OT Microsoft Azure D4IoT** センサーインポートスケジュール] を選択して、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。
 - i. [アクティブ] を選択して、センサーのインポートスケジュールを有効にします。
 - ii. デフォルトでは、センサーのインポートスケジュールは毎日午前 0 時に実行されるように設定されています。[実行] フィールドと [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** デバイスインポートスケジュール] を選択して、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、センサーのインポートスケジュールを有効にします。
 - ii. デフォルトでは、センサーのインポートスケジュールは毎日午前 0 時に実行されるように設定されています。[実行] フィールドと [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:

デバイスはセンサーごとに照会されます。Service Graph Connector は、検証済み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: コネクタ(Microsoft Defender for IoT)Azureのトラブルシューティングサービスグラフを行うには、次の手順を実行します。

- a. [オプション] Microsoft Defender for IoT (Azure) 向けサービスグラフコネクタのトラブルシューティング ([オプション] Microsoft Defender for IoT (Azure) のトラブルシューティング)] セクションを選択します。
- b. [検証スケジュール設定済みジョブの実行] タスクで、[構成] を選択します。
- c. [今すぐ実行] を選択します。
このジョブは、SGC の構成とへの接続 Microsoft Azure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、検証結果によって問題が報告され、トラブルシューティング手順が提案されます。スケジュール設定済みジョブが終了するまで待ちます。
- d. ジョブスケジュールが完了したら、「[オプション] Microsoft Defender for IoT (Azure) 向けサービスグラフコネクタのトラブルシューティング ([オプション]Microsoft Defender for IoT (Azure))」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、の初期設定 Claroty CTD のサービスグラフコネクタ統合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、次に移動します: 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** > **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

これで、コネクタfor()Azureに接続Microsoft Defender for IoT()ServiceNow サービスグラフMicrosoft Defender for IoT Azureできます。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 Microsoft Defender for IoT \(Azure\) 用の ServiceNow Service Graph コネクタに接続する \(KB1587770\)](#)。

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。センサーはデバイス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。Service Graph Connector 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:

の ServiceNow 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

[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。[ライフサイクルステージステータス] フィールドが [使用中] に設定されている場合、検証は成功しています。

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割り当てるセンサーの値を追加します。
4. [NIDS 管理者構成] 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用に **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用に 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、すべてのデバイスの 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、属性のデフォルトのリストです。

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

サービスグラフ接続フレームワークの使用

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、および作成されたMicrosoft Azure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

(Azure) 用のMicrosoft Defender for IoTコネクタのデータソース、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サービスグラフ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 接続フレームワークでは、関連するすべてのデータソースと作成された Microsoft Azure 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、ソースへの接続 ()Microsoft Azure 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 ()Azure アプリケーションのMicrosoft Defender for IoTコネクタ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** 接続.
3. [Service Graph 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、[**Service Graph** 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、[**Service Graph** 接続データソース] 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、[**Service Graph** 接続のスケジュール設定済みデータインポート] タブを選択します。
7. オプション: プラットフォームとの Microsoft Azure 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 [状態] と [提案] に、失敗した手順の状態とトラブルシューティングの提案がそれぞれ表示されます。

CMDB()のMicrosoft Defender for IoT Azureコネクタでサービスグラフ対象となるクラス

ガイド付き設定を完了したら、()Azure プロジェクトからMicrosoft Defender for IoT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。

属性ラベル	属性の名前
運用体制	os
OS バージョン	os_version
OS ドメイン	os_domain
OS アドレス幅	os_address_width

構成アイテム [cmdb_ci]

構成アイテム [cmdb_ci] 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
ハードウェアベンダー	manufacturer
最新の検出	most_recent_discovery
最初の検出	first_discovered
名前	名前
表示名	sys_class_name

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
IP アドレス	ip_address

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	名前、Mac、mac_address

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	属性の名前
ファームウェアバージョン	firmware_version
モデル ID	model_id
ラック番号	rack_number
シリアル番号	serial_number
ベンダー	vendor
最新の検出	most_recent_discovery
最初の検出	first_discovered

OT デバイスの詳細 [cmdb_ot_entity]

OT デバイスの詳細 [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	属性の名前
Purdue レベル	purdue_level
資産の重要度	asset_criticality

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。

属性ラベル	属性の名前
スイッチ位置	switch_position
リモートモードの切り替え	switch_remote_mode

コネクタのMicrosoft Defender for IoT属性マッピングと分類 サービスグラフ (Azure)

次の表では、センサーとデバイスの属性マッピングと分類について説明します。

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	フィールドにマッピング	説明
ID	文字列形式: /subscriptions/ <subscripti- id>/provider/ <provider>/locations/ <location>/sites/ <site>/sensor/ <sensor-name>	• sys_object_source • cmdb_ci_nids	ceSNK (sys_object_source) • correlation_id	センサーの一意的 ID。
名前	文字列	cmdb_ci_nids	名前	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 または使用不可: 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 True : 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): 学習中	IoT センサーの学習モードステータス。
properties.mac	文字列	cmdb_ci_network_adapter	adapter 前、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。

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	フィールドにマッピング	説明
properties.zone	文字列	cmdb_ci_nids	zone	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	フィールドにマッピング	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	ceSNK (sys_object_source) cmdb_ot_entity の discovery_source_id	デバイスの一意的 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)	デバイスの許可済みステータス
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	名前	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ある場合)	first_discovered	デバイスが初めて確認された時刻。
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ある場合)	most_recent_discovery	デバイスが最後に確認された時間。
properties.purdueLevel	文字列	cmdb_ot_entity	purdue_level	デバイスの Purdue レベル。
properties.operatingSystem	文字列	cmdb_ci_computers	os	OS ディストリビューション

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	フィールドにマッピング	説明
properties.operatingSystem.version	文字列	cmdb_ci_computer	os_version	OS バージョン
properties.operatingSystem.platform	文字列	cmdb_ci_computer	os_domain	OS プラットフォーム
properties.operatingSystem.architecture	文字列	cmdb_ci_computer	os_address_width	OS アーキテクチャ
properties.additionalFields.plcKeyState	(空)	cmdb_ci_ot_plc	switch_position	PLC キーの状態
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・ハードウェア・データ
properties.hardware.model	文字列	cmdb_ci	(空)	ハードウェアモデル
properties.hardware.serialNumber	文字列	cmdb_serial_number	serial_number	ハードウェアのシリアル番号
properties.hardware.vendor	文字列	cmdb_ci	manufacturer	ハードウェアベンダー
properties.nics	オブジェクトの阵列	(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[{}].ipAddress	文字列	cmdb_ci_ip_address	ip_address	IPv4 アドレス
properties.nics[{}].macAddress	文字列	cmdb_ci_network_adapter	mac_address	MAC アドレス
properties.slots	オブジェクトの阵列	(空)	(空)	バックプレーン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。
properties.slots[{}].firmwareVersion	文字列	cmdb_ci_ot_control_module	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_control_module	model	スロットのモデル。
properties.slots[{}].rackNumber	整数	cmdb_ci_ot_control_rack	rack_number	バックプレーン内のラック番号
properties.slots[{}].serialNumber	文字列	cmdb_ci_ot_control_module	serial_number	スロットのシリアル番号。
properties.slots[{}].slotNumber	整数	cmdb_ci_ot_control_rack	slot_number	ラック内のスロット番号。

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	フィールドにマッピング	説明
properties.slots[0].name	Text	cmdb_ci_ot_control	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	(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	産業用	(空)
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	(空)	(空)
エレベーター	(空)	(空)
エンジンアリン	産業用	(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
グステー ション		
火災報知 器	(空)	(空)
火災検知 器	(空)	(空)
ファイア ウォール	(空)	(空)
ゲーム機	(空)	(空)
履歴担当 者	(空)	(空)
HMI	産業用	(空)
湿度セン サー	(空)	(空)
空調	(空)	(空)
I/O アダ プター	(空)	(空)
IED	(空)	(空)
産業用包 装システ ム	(空)	(空)
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)

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
IP カメ ラ	(空)	(空)
IP電話	(空)	(空)
範囲	(空)	(空)
メーター (Meter)	(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	産業用	(空)
空圧装置	(空)	(空)
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)

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
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)
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)

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
ターミナル駅	(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)
未分類	未分類またはすべて	(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
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 Server 2012 の場合 • 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 • 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)	• Linux • arch • centos • Debian • Fedora • Suse

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
		• Red Hat • RHEL • Ubuntu • Oracle
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
上記の タイプ 値 (指定 Network と IoT を除く)	(空)	• HP/UX • HPUX

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)	• Hyper-V • ハイパーV • ハイパー
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
上記の タイプ 値 (指定 Network と IoT を除く)	(空)	• Unix • Gnu

自動翻訳

デバイスタイプの分類 (続く)

Microsoft Azure デバイスタイプ名	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)	• 勝つ • windows • Microsoft • Windows 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、99 • Windows 2000 の場合 • Windows for Workgroups 3.11 (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

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

(オンプレミス管理コンソール) をアプリケーションとServiceNow Operational Technology Manager統合Microsoft Defender for IoT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 ストア](#) 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メモ情報については、「[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

アプリケーションで ServiceNow Operational Technology Manager Connector for Microsoft Defender for IoT (オンプレミス管理コンソール) を使用してサービスグラフ、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

Connector for Microsoft Defender for IoT (On-premises Management Console) のサービスグラフガイド付き設定では、インスタンスの統合を構成するための整理された順序のタスクが提供されます。ガイド付きセットアップにアクセスするには、「[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測定基準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。統合ダッシュボードで CMDB の統合の監視の詳細については、「[CMDB 統合の監視](#)」を参照してください [Integration Commons for CMDB](#)。

データマッピング

(オンプレミス管理コンソール) データ ソースの Microsoft Defender for IoT データは、強力な変換エンジン (RTE) を使用してマップされ、構成アイテム (CI) クラス定義に変換され ServiceNow CMDB に入ります。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、(オンプレミス管理コンソール) アプリケーションから Microsoft Defender for IoT 定期的にデータをプルするように統合を構成できます。

次の表は、(オンプレミス管理コンソール) プロジェクトに含まれる Microsoft Defender for IoT 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 テーブルの一覧です。

のデータ ソースとステージング テーブル (**Microsoft Defender for IoT** 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 [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 [cmdb_ci_hpux_server]
- HVAC機器 [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 Servercmdb_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]

(オンプレミス管理コンソール) プロジェクトから Microsoft Defender for IoT 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、「」を参照してください [対象となる CMDB クラス](#)。

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

Connector for Microsoft Defender for IoT (On-premises Management Console) のサービスグラフガイド付き設定を使用して、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 store app](#)。
- ITOM Discovery 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、「[Discovery 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 コネクタ (Microsoft Defender for IoT オンプレミス管理コンソール) 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 Connector for Microsoft Defender for IoT (On-premises Management Console) アプリケーションに設定されサービスグラフ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、[開始するには] を選択します。
4. を構成する MID サーバーには、次の手順を実行します。
 - a. [接続と資格情報のセットアップ] セクションで、[MID Server を構成] タスクを選択します。
 - b. 説明にリンクされている構成が完了したら、[MID サーバー完了としてマーク] 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. [接続と資格情報のセットアップ] セクションで、[接続と資格情報] タスクを選択します。
- b. [設定] 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 Central Manager の URL の名前を入力します。
たとえば、https://192.168.1.100。
- f. オプション: を使用している場合は、MID サーバー次のすべてを選択します。
 - [MID Server を使用] ボックス
 - [MID Server 詳細構成] 関連リストの **MID Server**
 - リストからの **MID** 選択
- g. [資格情報] フィールドで、検索アイコンを選択して [資格情報レコード] 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 キー資格情報] タイプを選択します。
- j. [API キー] フィールドに、管理コンソールから Microsoft Defender for IoT 提供された名前と API キーを入力します。
- k. [送信] を選択して資格情報レコードを作成します。
管理コンソールで Microsoft Defender for IoT API キーを作成するには、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Microsoft。
- l. [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. [接続と資格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、推奨される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は、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、非本番環境用に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。

イントラネットのレコード値

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 Server 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 [完了コードが成功] と表示され、処理されたレコードの数が接続マネージャーのセンサー数と同じ数として表示されると、接続が正しく設定されていることが示されます。

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構成します。

プロパティ	説明
sn_msfted4iotsgc.resourcepath.sensor	センサーの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_msfted4iotsgc.resourcepath.device	- V3 API バージョンには、デバイスリソースパスが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。

プロパティ	説明
sn_msftd4iotsgc.resourcepath.connection	- V3 API バージョンには、接続リソースパスが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 Devices and Connections API のページごと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	- 接続および資格情報レコードの設定時に構成した Microsoft D4IoT ベース 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、で CMDB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。 i 注: 初めて接続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.ot.vr.integration.id	統合用のMicrosoft Defender for IoTアプリケーションサービスグラフを使用している場合はOperational Technology Vulnerability Response、OT VR インポートレコードの Sys ID を指定します。

プロパティ	説明
	i 注: Operational Technology Vulnerability Response 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を空白のままにすると、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. **[Save (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. [設定] 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、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. 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. [インポートスケジュールの構成 (Configure Import Schedules)] セクションで、[構成] を選択します。

b. [**SG-OT Microsoft D4IoT** センサーのインポートスケジュール] を選択して、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、センサーのインポートスケジュールは毎日午前 0 時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ます。

c. [アクティブ] を選択して、センサーのインポートスケジュールを有効にします。

d. [**SG-OT Microsoft D4IoT** デバイスインポートスケジュール] を選択して、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午前 0 時に実行されるように設定されています。
- デバイスはセンサーによって照会されます。コネクタは サービスグラフ、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。Network Intrusion Detection System (NIDS) アプライアンスの構成については、「」を参照してください [NIDS の検証](#)。

e. [アクティブ] を選択して、デバイスのインポート スケジュールを有効にします。

f. 必要に応じて、[**SG-OT Microsoft D4IoT** 接続インポートスケジュール] を選択して、接続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、接続のインポートスケジュールは、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)がすでに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。

CMDBConnector for Microsoft Defender for IoT (On-premises Management Console) でサービスグラフ対象となるクラス

ガイド付き設定を完了したら、(オンプレミス管理コンソール) プロジェクトから Microsoft Defender for IoT 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。

属性ラベル	属性の名前
運用体制	os
OS バージョン	os_version
OS ドメイン	os_domain
OS アドレス幅	os_address_width

構成アイテム [cmdb_ci]

構成アイテム [cmdb_ci] 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
ハードウェアベンダー	manufacturer
最新の検出	most_recent_discovery
最初の検出	first_discovered
名前	名前
表示名	sys_class_name

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
IP アドレス	ip_address

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	名前、Mac、mac_address

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	属性の名前
ファームウェアバージョン	firmware_version
モデル ID	model_id
ラック番号	rack_number
シリアル番号	serial_number
ベンダー	vendor
最新の検出	most_recent_discovery
最初の検出	first_discovered

OT デバイスの詳細 [cmdb_ot_entity]

OT デバイスの詳細 [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	属性の名前
Purdue レベル	purdue_level
資産の重要度	asset_criticality

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。

属性ラベル	属性の名前
スイッチ位置	switch_position
リモートモードの切り替え	switch_remote_mode

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

次の表では、センサーとデバイスの属性マッピングと分類について説明します。

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	フィールドにマッピング	説明
ID	文字列形式: /subscriptions/ <subscripti- id>/provider/ <provider>/locations/ <location>/sites/ <site>/sensor/ <sensor-name>	• sys_object_source • cmdb_ci_nids	ceSNK (sys_object_source) • correlation_id	センサーの一意的 ID。
名前	文字列	cmdb_ci_nids	名前	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 または使用不可: 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 True : 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): 学習中	IoT センサーの学習モードステータス。
properties.mac	文字列	cmdb_ci_network_adapter	adapter 前、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。

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	フィールドにマッピング	説明
properties.zone	文字列	cmdb_ci_nids	zone	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	フィールドにマッピング	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	ceSNK (sys_object_source) cmdb_ot_entity の discovery_source_id	デバイスの一意的 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)	デバイスの許可済みステータス
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	名前	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ある場合)	first_discovered	デバイスが初めて確認された時刻。
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ある場合)	most_recent_discovery	デバイスが最後に確認された時間。
properties.purdueLevel	文字列	cmdb_ot_entity	purdue_level	デバイスの Purdue レベル。
properties.operatingSystem	文字列	cmdb_ci_computers	os	OS ディストリビューション

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	フィールドにマッピング	説明
properties.operatingSystem.version	文字列	cmdb_ci_computer	os_version	OS バージョン
properties.operatingSystem.platform	文字列	cmdb_ci_computer	os_domain	OS プラットフォーム
properties.operatingSystem.architecture	文字列	cmdb_ci_computer	os_address_width	OS アーキテクチャ
properties.additionalFields.plcKeyState	(空)	cmdb_ci_ot_plc	switch_position	PLC キーの状態
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・ハードウェア・データ
properties.hardware.model	文字列	cmdb_ci	(空)	ハードウェアモデル
properties.hardware.serialNumber	文字列	cmdb_serial_number	serial_number	ハードウェアのシリアル番号
properties.hardware.vendor	文字列	cmdb_ci	manufacturer	ハードウェアベンダー
properties.nics	オブジェクトの阵列	(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[{}].ipAddress	文字列	cmdb_ci_ip_address	ip_address	IPv4 アドレス
properties.nics[{}].macAddress	文字列	cmdb_ci_network_adapter	mac_address	MAC アドレス
properties.slots	オブジェクトの阵列	(空)	(空)	バックプレーン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。
properties.slots[{}].firmwareVersion	文字列	cmdb_ci_ot_control_module	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_control_module	model	スロットのモデル。
properties.slots[{}].rackNumber	整数	cmdb_ci_ot_control_rack	rack_number	バックプレーン内のラック番号
properties.slots[{}].serialNumber	文字列	cmdb_ci_ot_control_module	serial_number	スロットのシリアル番号。
properties.slots[{}].slotNumber	整数	cmdb_ci_ot_control_rack	slot_number	ラック内のスロット番号。

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	フィールドにマッピング	説明
properties.slots[]	文字列	HardwareVendor	cmdb_ci_ot_control.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	(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	産業用	(空)
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	(空)	(空)
エレベーター	(空)	(空)
エンジンアリン	産業用	(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
グステー ション		
火災報知 器	(空)	(空)
火災検知 器	(空)	(空)
ファイア ウォール	(空)	(空)
ゲーム機	(空)	(空)
履歴担当 者	(空)	(空)
HMI	産業用	(空)
湿度セン サー	(空)	(空)
空調	(空)	(空)
I/O アダ プター	(空)	(空)
IED	(空)	(空)
産業用包 装システ ム	(空)	(空)
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)

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
IP カメ ラ	(空)	(空)
IP電話	(空)	(空)
範囲	(空)	(空)
メーター (Meter)	(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	産業用	(空)
空圧装置	(空)	(空)
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)

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
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)
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)

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
ターミナル駅	(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)
未分類	未分類またはすべて	(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
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 Server 2012 の場合 • 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 • 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)	• Linux • arch • centos • Debian • Fedora • Suse

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
		• Red Hat • RHEL • Ubuntu • Oracle
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
上記の タイプ 値 (指定 Network と IoT を除く)	(空)	• HP/UX • HPUX

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)	• Hyper-V • ハイパーV • ハイパー
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
上記の タイプ 値 (指定 Network と IoT を除く)	(空)	• Unix • Gnu

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)	• 勝つ • windows • Microsoft • Windows 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、99 • Windows 2000 の場合 • Windows for Workgroups 3.11 (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

Operational Technology Manager を使用する

(OT) 拡張クラスのインストール Operational Technology 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、ソリューションの ServiceNow Operational Technology 基盤データと関係を作成します。

タスク	目的
1. Excel スプレッドシートに Microsoft 既存の Operational Technology データを入力します。	Excel スプレッドシートの Microsoft 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。

タスク	目的
2. Excel スプレッドシートをインポートします。	既存の Operational Technology 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. for Operational Technology 関数を実行しますディスカバリー。	産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルでデバイスを検出 Operational Technology (OT) します
4. (OT) メニューの選択 Operational Technology 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 コネクタ (Operational Technology Excel)

サービスグラフコネクタ (Excel) 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Operational Technologyデータをインポートできます。抽出変換ロード (ETL) で 統合ハブ これを使用して、このデータを 構成管理データベース (CMDB)。

インポートプロセスを実行する前に、Excel スプレッドシートに Microsoft 既存の Operational Technology データを入力する必要があります。ETL を使用して 統合ハブ Excel スプレッドシートをMicrosoftインポートすると、正しい構成アイテム (CI) レコード構成管理データベース (CMDB)が に作成されます。詳細については、「[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。

関連情報

[IntegrationHub](#)

[IntegrationHub ETL](#)

Service Graph Connector for Microsoft Excel 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 Operational Technology データをインポートするように Service Graph Connector for Microsoft Excel を構成します。

Service Graph Connector for Microsoft Excel のガイド付き設定を使用し、タスクを順番に完了して Service Graph Connector for Microsoft Excel を構成します。

移動先 **すべて > Industrial Workspace** 管理者 > ガイド付きセットアップをクリックし、次のガイド付き設定を開き、タスクを完了します。

ガイド付き設定の使用の詳細については、「[ガイド付き設定](#)」を参照してください。

タスク	目的
ユーザー	各ユーザーが使用できるアクションを制御するルールをアサインします。
ステージングテーブルの構成	CI の一意の名前を識別する際の構成要素を決定するように構成します。 システムのプロパティの詳細については、「 SG-OT デバイス 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。

タスク	目的
データを準備	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作成して準備します。 データの準備の詳細については、次を参照してください コネクタインポート用の サービスグラフ 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。
新しい OT デバイスを作成する	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、以下を参照してください。
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、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上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、次を参照してください 検証の管理。
スケジュールインポート	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 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 Service Graph Connector 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、Operational Technology Manager アプリケーションを使用できます。

ロール	説明
管理者 [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。
管理者 [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、既存の Operational Technology 構成管理データベース (CMDB) (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 存在する場合、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。レコードが誤って調整または結合されないようにするために、ステージングテーブル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 > Industrial Workspace 管理者 > 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。で一致する CI が見つかった CMDB と、[検証] ステータスは [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>
シリアル番号	別の CI で同じシリアル番号 [serial number] が見つかりました: <Link to CI>

2. オプション: [CMDB] 列の [一致する CI] から一致する CI を選択して表示します。

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。

管理者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、Excel スプレッドシートを作成し、Microsoft 既存の Operational Technology 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 > **Industrial Workspace** 管理者 > **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。

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

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、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 Excel スプレッドシートをダウンロードします Microsoft。

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。

i 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。

コネクタインポート用の サービスグラフ 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

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は、アップロードを成功させるために重要です。

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。

i 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、次を参照してください [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。

- 列 A から K の記入
- 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 までの列の記入

列 **A** から **K**

列	必須の列名	タイプ	説明と例
A	デバイスの重要度	文字列	ロールに基づく、OT デバイスの重要度または重要性の測定。例: ○ 「高」または「最重要」 ○ 中またはある程度重要

列	必須の列名	タイプ	説明と例
			「低」または「やや重要度が低い」 - なしまたは重要ではない
B	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、各レコードに一意の識別子をアサインする外部ソースシステムから取得されます。
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、スタンピング
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	必須の列名	タイプ	説明と例
L	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。

列	必須の列名	タイプ	説明と例
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	Datetime	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 (ある場合)。例:13.2
Q	モジュールあり	ブール	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	このデバイスがフィールドデバイスの場合、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： - input - 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

列	必須の列名	タイプ	説明と例
			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)。

列 Z から AI

列	必須の列名	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 (存在する場合)。
Aa	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	必須の列名	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 - 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	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 (存在する場合)。
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	必須の列名	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	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) のアサインされたシリアル番号。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 (存在する場合) のアサイン済みシリアル番号。例:MemSN123
AN	メモ리카ードのシリアル 3	文字列	OT デバイスにインストールされている 3 枚目のメモ리카ードに割り当てられたシリアル番号 (ある場合)。
Ao	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	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
Ar	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
As	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	必須の列名	タイプ	説明と例
Au	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
Av	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	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、これらの 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 - 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、必須ではない場合でも、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 - 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
ああ	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、必須ではない場合でも、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 - 可能な場合は、os_version - ファームウェアのバージョン (使用可能な場合)
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。

列	必須の列名	タイプ	説明と例
Ba	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、for 関数 Operational Technology がディスカバリー正しい ICS レ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	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	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 (存在する場合)。 例:SN545、SN998 i 注: OT デバイスの場合、これらの 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 - 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	必須の列名	タイプ	説明と例
Bve	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	サイト	文字列	設備モデルはサイトレベルから始まり、各工業用地を記述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	スロット番号	文字列	制御モジュールの場合、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	Datetime	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	ソフトウェアのインストール日 2	Datetime	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	必須の列名	タイプ	説明と例
Bj	ソフトウェアのインストール日 3	Datetime	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	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	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	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	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の報告済みバージョン (存在する場合)。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の報告済みバージョン (存在する場合)。 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の報告済みバージョン (存在する場合)。 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 -- 割り当てられた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。 メンテナンス中 OT デバイスはメンテナンス中で、現在オフラインです。 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 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 デバイスの施設へのインストールが保留中です。 修理待ち

列	必須の列名	タイプ	説明と例
			OT デバイスは修復を保留していますが、まだオンラインではありません。 廃止 OT デバイスは廃止されました。 盗難 OT デバイスが盗まれました。
Br	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。

BS から BW までの列

列	必須の列名	タイプ	説明と例
Bs	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。 システムのプロパティについては、「」を参照してください SG-OT デバイス Excel インポート処理に影響を与えるシステムプロパティ。
Bt	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	必須の列名	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、必須ではない場合でも、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 - 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、検証コメントは、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。
Bv	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	必須の列名	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ステータス。 無効 で Cmdbcli 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の親 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

列	必須の列名	タイプ	説明と例
			ができています。 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	ベンダー	文字列	OT デバイスのベンダーの名前。

2. Excel スプレッドシートに Microsoft 入力したら、簡単にアクセスしてアップロードできるように、既知の場所に保存します。

SG-OT デバイス Excel インポート処理に影響を与えるシステムプロパティ

SG-OT デバイスの Excel インポートプロセスは、正常に完了するために次のシステムプロパティに依存します。

sn_otsm_sgc.excel.fields.for.transformed.name

- このプロパティを使用すると、ユーザーは変換後の名前を構築するためのフィールドを指定できます。

- フィールド値または列名はコンマで区切る必要があります。

この変換後の名前は、ステージングテーブルから直接取得される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後の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** に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、検証ステータスを [検証保留中] に変更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を変更すると、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検証を有効にします CMDB 。**True** に設定すると、ステージング デバイスは既存の CI と照らしてCMDB検証され、調整を行います。
- 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、欠落しているデータ、重複しているデータ、無効なデータを検証して見つけます。

始める前に

必要なロール：admin

手順

1. 移動先 すべて > **Industrial Workspace** 管理者 > **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. [ファイルの選択] 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、Excel スプレッドシートをアップロードします Microsoft。
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のプレビュー」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、[インポートの完了] を選択してステージングテーブルにデータをインポートします。

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 > Industrial Workspace 管理者 > OT マネージャー管理者 > 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が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フィールド

フィールド	説明
表示名	レコードに表示される OT デバイスの名前。

フィールド	説明
	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 表示名を設定できます。これは、OT デバイスを理解しやすくするためのもので、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 によって生成される一意の名前。
Purdue レベル	割り当てられた 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、「」を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems。
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に対する相対リスクの測定値: ○ 1: 最重要 ○ 4: 重要ではない
相関 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アサインされている最上位の親エンティティまたは産業サイト。
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

6. [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

検証を使用すると、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 (コントロールモジュール親 ID) の場合、親相関 ID がありません
- 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)
- 変換後の名前 (変換後の名前) の重複を検証

i 注:

コントロールモジュールの場合、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 のすべての列を確認)
- 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。

- モジュールとコントロールモジュールの親 ID があることを検証

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: 拡張ポイント実装を通じて `sn_otsm_sgc.SGOTAssetImportExtensionPoint`、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、次を参照してください [デバイス分類のカスタム実装の追加](#)。

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、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 > Industrial Workspace 管理者 > 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. [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、そのレコードを手動で有効に設定します。
 - 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。

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て CI が作成されないことがあります。

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 > **Industrial Workspace** 管理者 > **OT マネージャー** 管理者 > **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。

① Staging task creation process for all the invalid records have started in the background. It may take few minutes to complete.
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で、該当する場合はフィールドに入力します。

OT ステージングタスクのレコードフォーム

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、いくつかの修復ステージ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。 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。
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。
アサイン先	ステージングタスクを実行するユーザー。
アサイン先グループ	ステージングタスクを処理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: に移動して、SG OT Excel ステージングタスク (sg_ot_excel_staging_task) テーブルに作成された OT ステージングタスクレコードを表示します すべて > **Industrial Workspace** 管理者 > **OT マネージャー** 管理者 > **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

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した。

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 に CMDB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 > Industrial Workspace 管理者 > 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、[インポートスケジュール] 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レコードを にインポートします CMDB。

正常にインポートされたデータの [検証] ステータスには [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て **Excel** スプレッドシートを **Microsoft** インポートする

簡単インポートを使用して 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 Microsoft 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、IntegrationHub 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 Excel スプレッドシートを適切に準備 Microsoft する必要があります。詳細については、「[コネクタインポート用の サービスグラフ 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。

データをインポートする準備ができれば、へのインポート 構成管理データベース (CMDB)をスケジュールできます。このプロセスでは、スプレッドシートに含まれている OT デバイスに対して一意のレコード 構成管理データベース (CMDB) 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

抽出変換ロード (ETL) を実行する 統合ハブ ときに、追加のサポートのために埋め込み 業種別 ガイド付きセットアップ コンテンツを参照することもできます。

ステージングテーブルで検証を実行して、データの重複や不整合をチェックします。

にアクセスするには、業種別 ガイド付きセットアップに移動します。 **Industrial Workspace** 管理者 > ガイド付きセットアップ。

手順

1. 移動先 **すべて > 構成 > IntegrationHub 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、[ソースデータのインポート] と [基本的な詳細] を選択します。

4. [ETL 変換マップの基本情報を入力してください] 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プル] を選択します。

5. ETL フォームに戻ります 統合ハブ。

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確認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. [統合の実行] を選択します。

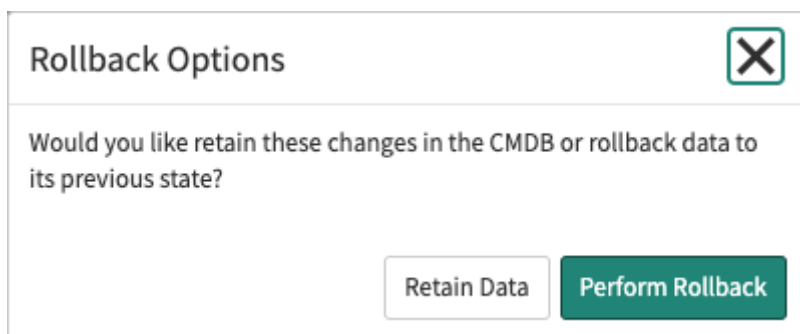
i 注:

このインポートでは 100 レコードをテストします。100 を超えるレコードの完全な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、定期的な設定スケジュールでインポートを実行するように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" and "Perform Rollback".

9. インポートされたデータを保持するには [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 Excel インポートを再試行Microsoftするには [ロールバックの実行] を選択します。

10. スプレッドシートデータを正式にインポートするには Now Platform:

- a. [インポートスケジュールの設定] を選択します。
- b. [スケジュールの設定] を選択します。
- c. [スケジュール設定済みデータインポート] リストで、[**SG-OT** デバイスのスプレッドシートを使用したインポートスケジュール] を選択します。
- d. [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ホームページから [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ピングします。

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、クラスや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の追加と、ETL での変更のみが可能です。

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、次に移動します。すべて > **Industrial Workspace** 管理者 > **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、「[Service Graph Connector 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 > **Industrial Workspace** 管理者 > **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の新しい列名と、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の列として表示) 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 > **IntegrationHub 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設定の [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

Save Mark as Complete

Unsaved Changes

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. [Save (保存)] を選択します。
[基本情報が正常に保存されました (Basic information saved successfully)] バナーが表示されます。
14. [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

	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	48364f7453281110594addeff7b127b1j Vendor E	Vendor E	4836

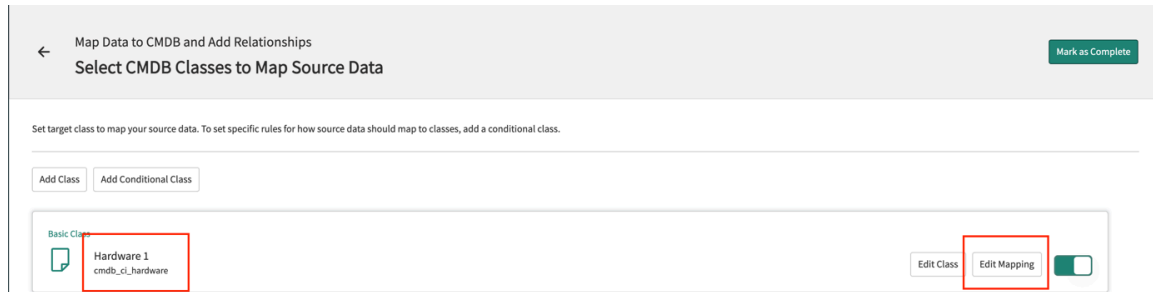
列が表示されない場合は、手順 11 ~ 14 を繰り返します。

16. [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、関係性を追加] 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。

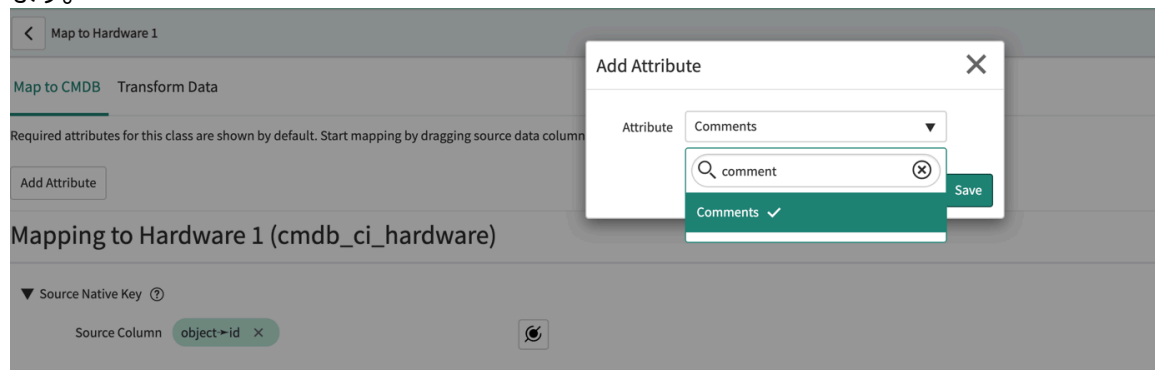
たとえば、「comments」フィールドは Hardware *cmdb_ci_hardware* クラスに存在します。このフィールドがマッピングされた後、その行のステージングテーブルの「コメント」列の値が

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. 「ハードウェア1」クラスで、「マッピングの編集」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. [Save (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] セクションの [ソースデータをマップする **CMDB** クラス] に戻ります。

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

Map to CMDB Transform Data

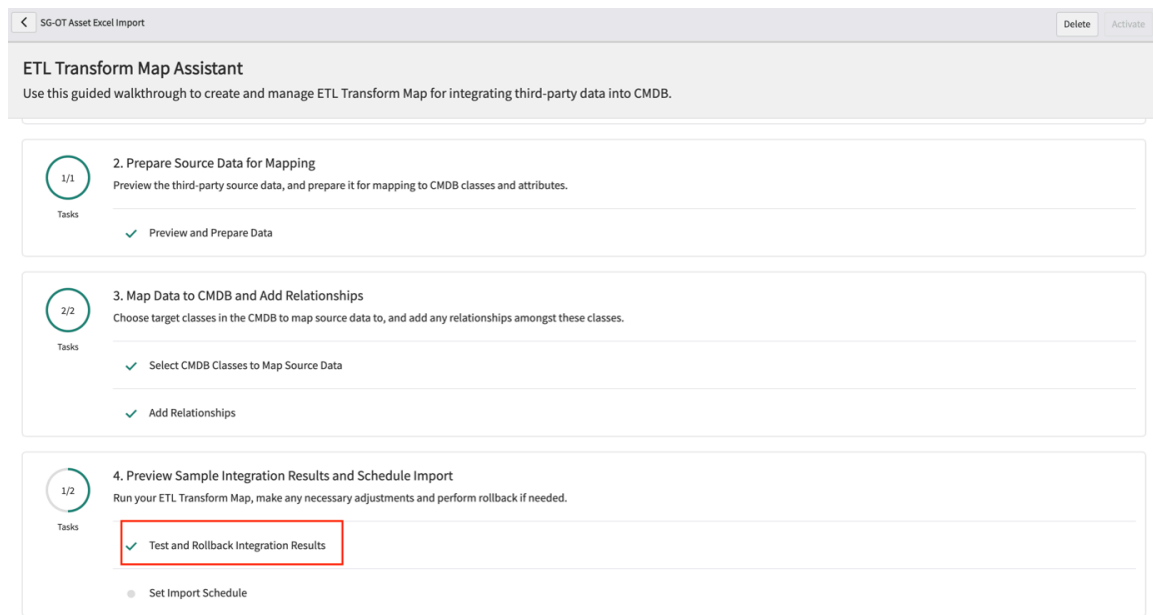
Required attributes for this class are shown by default. Start mapping by dragging source data columns or transformed data columns to their CMDB class attributes

Add Attribute

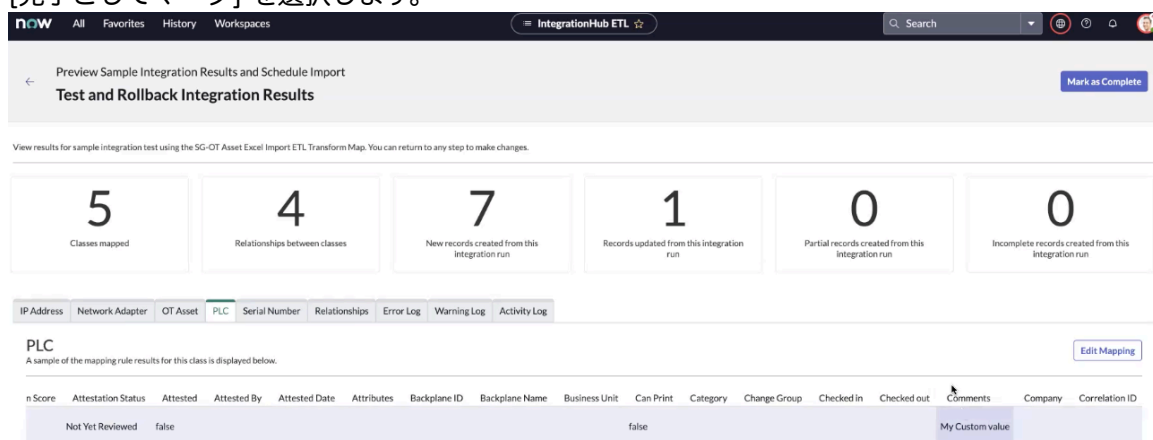
Mapping to Hardware 1 (cmdb_ci_hardware)

▼ Source Native Key		
Source Column	object→id	
▼ Source Recency Timestamp		
Source Column		
▼ Name		
Source Column	object→name	

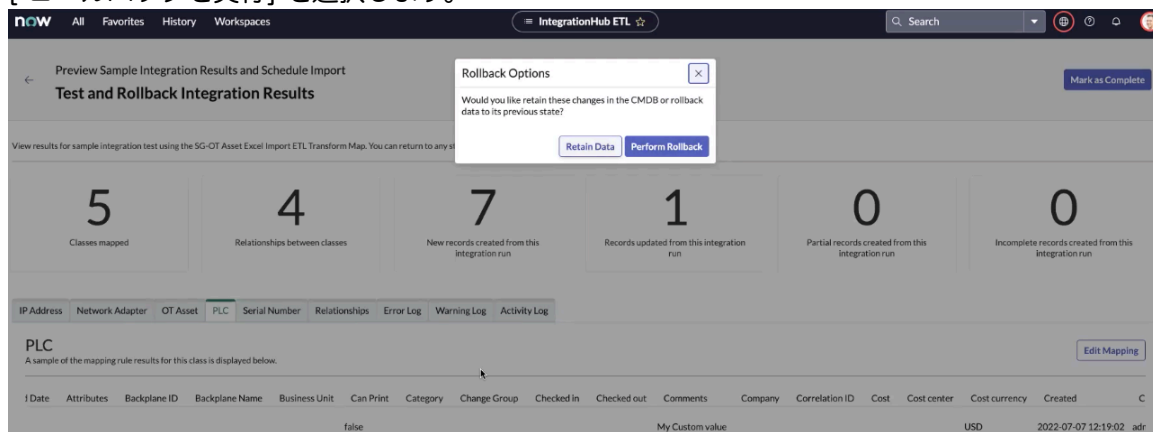
23. [完了としてマーク] を選択します。
24. 次の手順に従って、新しいフィールドマッピングを確認します。
- ETL 変換マップアシスタントのホームページに移動します。
 - ガイド付き設定の [サンプル統合結果のプレビューおよびインポートのスケジュール] セクションで、[統合結果のテストとロールバック] を選択します。



- c. [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. [完了としてマーク] を選択します。



- f. [ロールバックを実行] 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、デバイスの基本システム分類をカスタマイズします。

始める前に

拡張ポイントの `sn_otsm_sgc.SGOTAssetImportExtensionPoint` ベースシステムでは、という名前の `sn_otsm_sgc.SGOTAssetImportUtil` デフォルトの実装スクリプトが使用されます。カスタマイズされた分類を追加するには、**Service Graph Connector for Operational Technology (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 つのみ必要です。デフォル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 > システム拡張ポイント > スクリプト化済みの拡張ポイント**。
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
<code>getAssetCMDBSysClassNameWithOtEntityTypeSysId(/*string*/ type, /*string*/ osVersion, /*string*/ firmwareVersion)</code>	このメソッドを実装して、CMDB デバイスが属する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 <code>sys_id</code> を返します。 未分類のデバイスの場合、OT デバイスタイプは <code>ot_base</code> に設定されます。
<code>getComputerType(/*文字列*/ operatingSystem)</code>	渡されたオペレーティングシステムに基づいてシステムクラス名を返します CMDB。

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の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、Operational Technology 向け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。

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	Invalid	Valid	Partially Valid	Invalid	Valid	Partially Valid	No Implementation created	Implementation has different Name	Invalid state (Type)
2	Partially Valid	(Override - False)	(Override - False)	(Override - False)	(Override - True)	(Override - True)	(Override - True)		(Override - True)	(Override - True)
3	(sn_otsm_sgc.enable.cmdb.validations - True)	Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
4	Valid	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
5	Invalid	invalid	invalid	invalid	Invalid	Invalid	invalid	Invalid	Invalid	Same as Default state
6	(sn_otsm_sgc.enable.cmdb.validations - True)	Partially valid	Partially valid	Partially Valid	Invalid	Valid	Partially Valid	Partially Valid	Same as Custom validation state	Same as Default state
7	Valid	Valid	Valid	Valid	Invalid	Valid	Partially valid	Valid	Same as Custom validation state	Same as Default state
8	Invalid	invalid	invalid	invalid	Invalid	Invalid	invalid	Invalid	Invalid	Same as Default state
9	(sn_otsm_sgc.enable.cmdb.validations - False)	invalid	invalid	invalid	invalid	Invalid	invalid	Invalid	Invalid	Same as Default state

い。

5. [更新] を選択します。

Excel サービスグラフ コネクタのテスト

トラブルシューティングのアクションは、デバイスまたはデータをインポート Operational Technology する際の一般的な問題を解決するのに役立ちます。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
ETL ガイド付きセットアップでの SG-OT デバイス Excel インポート ETL のデータのロード中に問題が発生した場合	[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 [すべてのレコードをロード] 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コネクタをテスト実行した後、[サービスグラフ 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欠損値。 • 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

問題	ソリューション
	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コネクタをテスト実行した後、[サービスグラフ 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です。
簡単インポートが実行された後、現在の実行からインポートされたレコードがユーザーに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検証が実行されます。	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ブレッドクラムで [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の場合	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てもレコードの検証ステータスの更新が表示されない場合は、	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ても、検証ステータスは [検証処理待ち] 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の親相関 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、次のリンクを参照してください SG-OT デバイス Excel インポート処理に影響を与えるシステムプロパティ。
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、システムの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使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 1 つ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。 データ利用可能な CMDB に対して検証が実行されません。
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に OT デバイスには表示されません。	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 [データソースの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で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 すべて > 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。

コネクタによって サービスグラフ 使用されるスクリプトインクルードを表示します

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

始める前に

コネクタで使用されている サービスグラフ 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 > **Industrial Workspace** 管理者 > **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。

コネクタが サービスグラフ 使用するシステム・プロパティへのアクセス

管理者として、コネクタに関連する サービスグラフ システムプロパティを表示します。

始める前に

コネクタで使用されている サービスグラフ 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 > **Industrial Workspace** 管理者 > **OT マネージャー** 管理者 > **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。

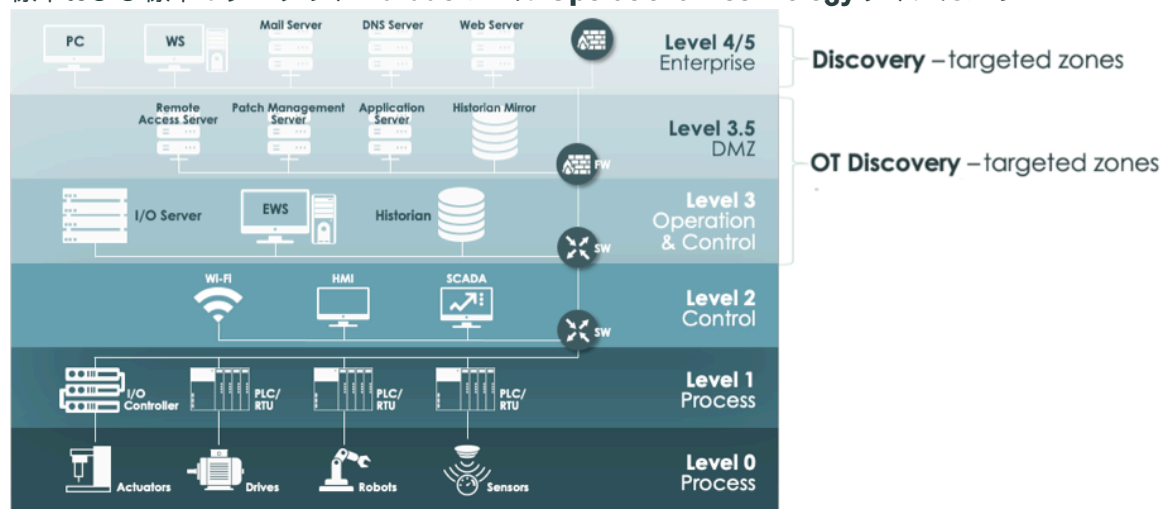
Operational Technology 用の ディスカバリー

for Operational Technology 関数を実行してディスカバリー、産業用コントロールシステム (ICS) ネットワーク内の指定された Purdue レベルで IT クラス Operational Technology (OT) デバイスを検出できます。IT クラスアイテムには、データセンターとファクトリ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 ディスカバリー 処理が行われる場所

ディスカバリー for Operational Technology プロセスは、標準の Discovery プロセスと同様の方法で動作します。

標準および標準のターゲット **Purdue レベル Operational Technology** ディスカバリー



でのNow Platform 標準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	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、を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems。

処理が行われる場所と方法ディスカバリー-Operational Technology

対照的に、処理はOperational Technology、ディスカバリー OT 検出スケジュールの作成時に選択したものに依拠して、次の Purdue レベルで実行できます。

処理済み **Purdue** レベル

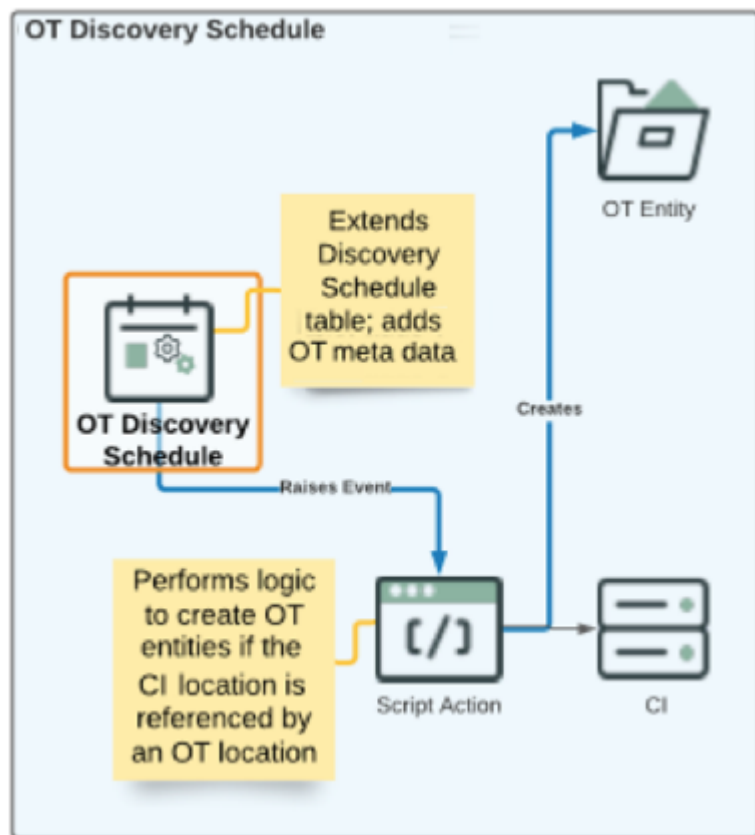
Purdue レベル	説明
3.5	非武装地帯 (DMZ) または産業非武装地帯 (IDMZ)。従来の(IT)DMZと同様に、OT 指向の IDMZを使用すると、さまざまなセキュリティ要件を持つネットワークを安全に接続できます。
3	プラントまたはサイト全体の制御および監視機能が存在するサイトオペレーション。

通常、ICS ネットワークの DMZ (または IDMZ、Purdue Level 3.5) で実行ディスカバリー-Operational Technology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:

産業運用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 ～ 2 に対してプロセスを実行し ディスカバリー ないでください。

ディスカバリー処理用Operational Technology



OT 検出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 アドレスを続行し、そこ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 構成管理データベース (CMDB) が 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、それに対して作成されます。
3. 場所属性に加えて、定義された属性を OT 検出スケジュールから 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 Discovery を介して作成された 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)]** の下の [アプリケーション] リストを開きます。

関連情報

[オペレーションテクノロジー \(OT\) 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検出プロセスフロー](#)

[水平検出のスケジュール](#)

ディスカバリー 関連 **Operational Technology** リンクと関連リスト

ディスカバリー には Operational Technology 、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	説明
クイック範囲	OT 検出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 アドレスをカンマで区切った 1 つの文字列に入力します。使用中の MID Server は、指定された IP 範囲に接続できる必要があります。 詳細については、「 Discovery 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	ディスカバリー for Operational Technology プロセスをすぐに実行します。
ポイントスキャンを実行	[ポイントスキャンの実行]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	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 Server は、指定された IP 範囲に接続できる必要があります。 注: セキュリティを強化するために、検出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 検出スケジュールが 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 検出スケジュール実行の結果の履歴。

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](#)

Operational Technology 検出スケジュールを作成し、プロセスを実行するディスカバリー

for an OT 機能を実行する方法とタイミングディスカバリーを調整する (OT) 検出スケジュールを定義します Operational Technology。また、即時 ディスカバリー クイック実行または実際の OT ディスカバリー 実行を実行することもできます。

始める前に

に対して実行ディスカバリーする前に、次のアクションを実行します:Operational Technology

- 標準 ディスカバリー アプリケーションをインストールして設定します。詳細については、「[Discovery のセットアップ](#)」を参照してください。
- CMDB CI Class Models プラグインをインストールします。詳細については、「[Operational Technology \(OT\) 拡張クラスのインストール](#)」を参照してください。
- MID Server をインストールします。詳細については、「[MID Server 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 検出 > OT 検出スケジュール**。
- クイック ディスカバリー実行、または OT 検出スケジュールを選択または作成します。
- フォームの [OT 検出スケジュール] フィールドに入力します。

4. ディスカバリープロセスをすぐに実行するか、OT 検出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

ディスカバリー for Operational Technology プロセスが実行されると、[ステータス] ディスカバリー 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の OT デバイスの編集または表示

(OT) メニューの Operational Technology オプションを使用して、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。

始める前に

次のいずれかの方法でデバイスデータをインポートします Operational Technology 。

- Microsoft認定された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) Operational Technology で 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、「[ステージングテンプレートを使用して Excel スプレッドシートを Microsoft インポートする](#)」を参照してください。
- 実行 ディスカバリー 対象 Operational Technology. 詳細については、「[Operational Technology 用の ディスカバリー](#)」を参照してください。
- Operational TechnologyからServiceNow Store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ロールがアサインされている場合は、OT デバイスのみを表示できます。アサインされたcmdb_ot_editorまたはcmdb_ot_adminロールがある場合は、次の方法で OT デバイスレコードを編集できます。

- で OT デバイスレコードを個別に編集します Now Platform。
- リストビューから複数の OT デバイスレコードを 業種別 ワークスペース 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ていません。

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ていません。

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. [Update (更新)] をクリックします。

2. 複数の OT デバイスレコード 業種別 ワークスペースを一括編集するには、次の手順に従います。

a. 移動先 すべて > Industrial Workspace.

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。



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 デバイスに対して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



す。



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. [Update (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下位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。クラスまたは拡張クラスの OT デバイス Operational Technology の場合、次の関連リストが表示されます。サーバーなどの Windows 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、インスタンス管理者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、関連項目の名前 (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 関係を追加] アイコン ([+] 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 ([図]) 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 ([設定]) をクリックします。

[OT デバイス] 関連リスト

関連リスト	説明
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。
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、およびシリアル番号タイプ。
メモリーモジュール	OT デバイスに関連付けられているメモリーモジュールのシリアル番号、有効性インジケータ、シリアル番号タイプ。
インストールされて	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 デバイス] 関連リスト (続く)

関連リスト	説明
いるソフトウェア	
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。
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。
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 コントロールモジュール	OT コントロールシステムタイプの OT デバイスまたは拡張クラス (PLC など) 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「所有者:所有」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
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、検出ソース、および CI に関連付けられている更新済みデバイス。 URL は、Service Graph Connector 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 コンバーター 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。

Operational Technology デバイスフォーム

Operational Technology (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。

Operational Technology デバイスフォーム

フィールド	説明
OT 表示名	レコードに表示される OT デバイスの名前。

Operational Technology デバイスフォーム (続く)

フィールド	説明
	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 表示名を設定できます。これは、OT デバイスを理解しやすくするためのもので、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的なリスクの測定値。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アサインさ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	割り当てられた Purdue 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、を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems。

Operational Technology デバイスフォーム (続く)

フィールド	説明
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 -- 割り当てられた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。 メンテナンス中 OT デバイスはメンテナンス中で、現在オフラインです。 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 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 デバイスの施設へのインストールが保留中です。 修理待ち OT デバイスは修復を保留していますが、まだオンラインではありません。 廃止 OT デバイスは廃止されました。 盗難 OT デバイスが盗まれました。
ディスカバリー ソース	ディスカバリー OT デバイスデータのソース。たとえば、ETL を使用して 統合ハブ Excel スプレッドシートから Microsoft OT デバイスをインポートした場合は、[SG-OT Excel インポート]。詳細については、「 サービスグラフ コネクタ (Operational Technology Excel) 」を参照してください。

Operational Technology デバイスフォーム (続く)

フィールド	説明
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の設定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。
リモートモードの切り替え	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 • テスト • なし

OT プロトコルを作成

OT プロトコルテーブルは、名前、バージョン、ベンダー固有のプロトコルかどうかなど、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. **[Submit (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

で 業種別 ワークスペース(OT) プロトコルをプロトコルコンバーター構成アイテム (CI) に関連付けOperational Technology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** リストビューを開きます業種別 ワークスペース
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 [削除] をクリックします。

IT ハードウェアデバイスの OT デバイスへの変換

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場合は、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、次に移動します: **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 OT デバイスに変換して、レコードをより迅速かつ効率的に編集できるようにします。

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 > Industrial Workspace 管理者 > Industrial Workspace**.
2. 業種別 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には、次のアクションを実行します。
 - フィルターの [ アイコンをクリックします。
 - 適用するフィルターをリストに追加します。
 - [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. [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。

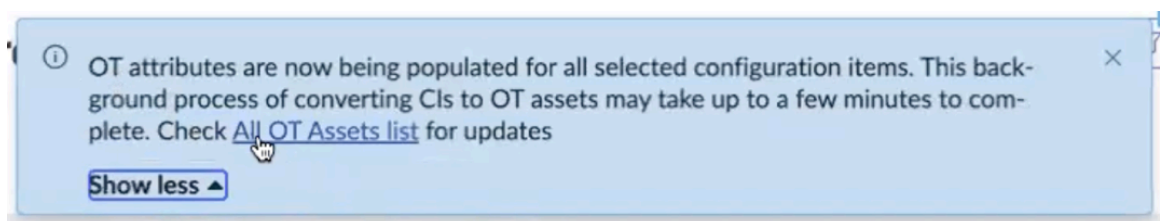
OT デバイスフォームに変換

フィールド	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。

フィールド	説明
	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に対する相対リスクの測定値: 1 : 最重要 4 : 重要ではない
Purdue レベル	割り当てられた Purdue レベル。レベル範囲は 0 から 5 です。 注: 産業用制御システムの Purdue レベルの詳細については、「」を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems 。
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アサインさ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ジョブスケジュール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](#)」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

(OT) デバイスを一括編集 Operational Technology 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

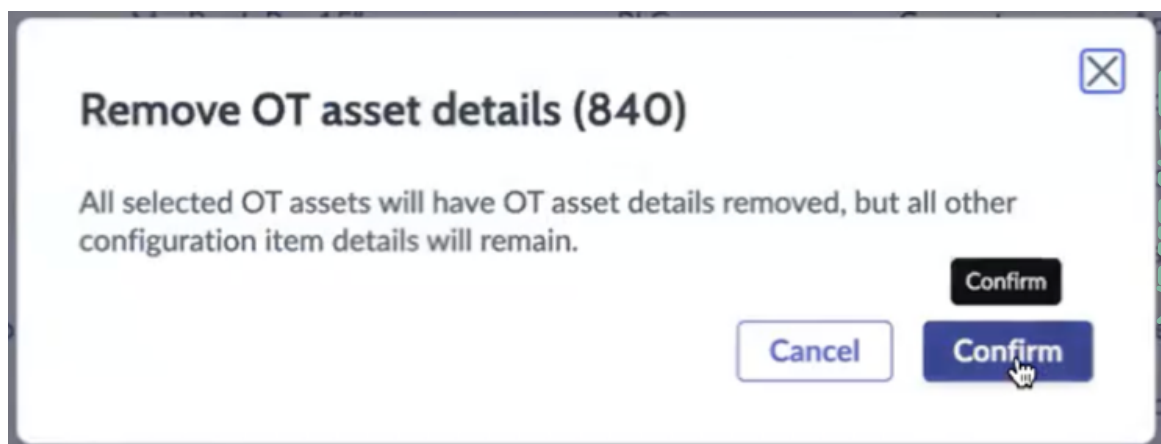
OT 機能を持たず、IT ハードウェアデバイスとして分類する必要がある OT デバイスが発生した場合は、複数の OT デバイスを一括編集で選択して編集し、IT ハードウェアデバイスに変換できます。

手順

1. 移動先 すべて > **Industrial Workspace** 管理者 > 産業用ワークスペース。
2. Industrial ワークスペースの [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. [**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。

i 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。



自動翻訳

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。

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、の Now PlatformNIDS 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を作成されたレコードに自動的に追加するのに役立ちます。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ています。

NIDS クラスレコードの詳細については、「[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 の次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

検出: 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 Guided Setup を使用して、次の操作を実行できます。

- インスタンスでまだアカウントを持っていないユーザーのためのユーザーとロールの設定
- (OT) 認定サービスグラフコネクタから Operational Technology 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 の妥当性確認の詳細については、[を参照してください NIDS の検証](#)。

NIDS Guided Setup 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 適用可能な「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割り当てら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の場合は、[**is manager**] を **True** に変更します。

検出されたデバイスに NIDS によって割り当てられたメタデータをコピーする NIDSUtils スクリプトインクルードについては、[を参照してください インストールされたスクリプトインクルード Operational Technology Manager](#)。

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 Operational Technology Manager](#)

NIDS の検証

NIDS を検証して、センサーによって検出された ETL からデバイスをインポートします。センサーはデバイス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

プラグインがインストールされていることをお勧めします 共通サービスデータモデル (CSDM)。Service Graph Connector は、標準に従って 構成管理データベース (CMDB) 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

[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。[ライフサイクルステージステータス] フィールドが [使用中] に設定されている場合、検証は成功しています。

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** 管理者構成] 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 Admin Configuration] セクションで、[**Life Cycle Stage Status**] の値が [Learning Mode] 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。
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** に割り当てられたメタデータ(**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 ETL からデバイスはインポートされません。

IT レコードを **OT** デバイスに自動的に変換

[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ジョブスケジュールを作成します。このジョブスケジュールは、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ってください。

- 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てください。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 万レコードを超えていないことを確認します。
- ステップ 3 ～ 6 の個別の CI クラスに対して、個別のスケジュール設定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ーします。

i 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確認します。
- 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 > Industrial Workspace 管理者 > OT マネージャー管理者 > 自動化された IT OT** への一括変換。
2. [New (新規)] を選択します。
3. [フィルター基準 - OT デバイス] タブで、変換する必要がある CI を識別するためのソーステーブルとフィルター基準を設定します。

たとえば、プリフィックスが COMP の、システムにインポートされるすべてのコンピューターの 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、フィルター基準を [名前] [次の値で始まる] **[COMP]**、[クラス] [次の値に等しい] **[コンピューター]**、および **[OT デバイスの詳細]** [空] として追加しま

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。
OT デバイスタイプやデバイスの重要度など、OT エンティティの詳細がこれらのレコードに追加されます。
5. [OT エンティティのデフォルト構成 (OT Entity Default Configuration)] 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

フィールド	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、ネットワーク上で再生される機能は 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 機能がないか、デバイスタイプが不明です。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に対する相対リスクの測定値: ○ 1: 最重要 ○ 4: 重要ではない
Purdue レベル	割り当てられた Purdue レベル。レベル範囲は 0 から 5 です。 注: 産業用制御システムの Purdue レベルの詳細については、「」を参照してください https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems。
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アサインさ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された時刻を選択します。

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。

Operational Technology Manager 参照

参照トピックには、Operational Technology Manager 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。

のインストール済みソフトウェア **Operational Technology Management**

ソリューションのインストール Operational Technology Management 済みソフトウェアは、Discovery for Operational Technology (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、(SAM) アプリケーションがインストールされ ソフトウェア資産管理 し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。

- ソフトウェア検出モデル [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 が有効化されたときのソフトウェア インストールを管理するためのテーブル構造の動作の違いの詳細については、次を参照してください [Discovery with Software Asset Management](#)。

コンピューターの CI を構成して、データを表示する ソフトウェア資産管理 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

OT デバイスに 業種別 ワークスペース 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。

- リストビューの 業種別 ワークスペース[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] タブの [インストールされているソフトウェア] リスト。

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てください。

概要

拡張クラスは、Operational Technology Management.構成管理データベース (CMDB)

[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) OT の更新クラス。

関連アプリケーション

[CMDB CI Class Models store app](#)

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 **Operational Technology Manager**

Operational Technology Manager Operational Technology アプリケーションに関連付けられた (OT) ペルソナ。

[End]

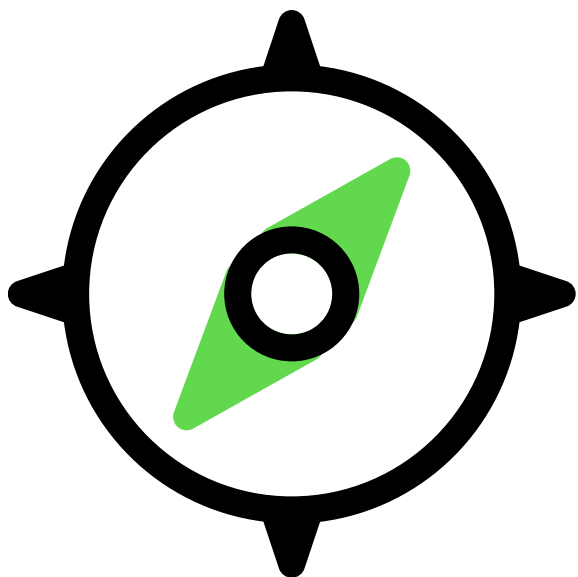
産業用プロセスマネージャー

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、ソリューションに必要な ISA-95 設備階層モデルデータ基盤ServiceNow Operational Technologyを作成します。を使用すると 産業用プロセスマネージャー、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。

i 注:

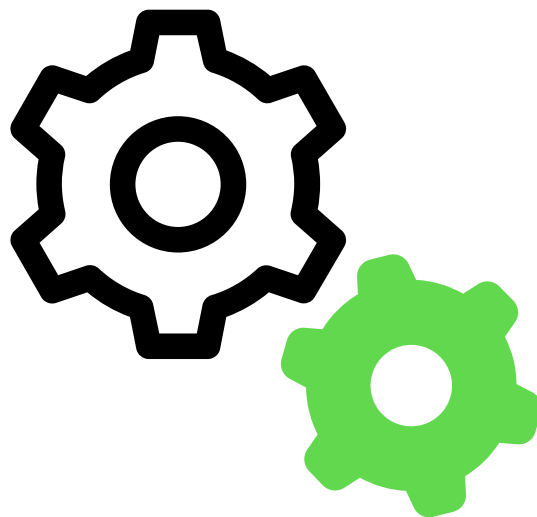
Manufacturing Process Manager は、Industrial Process Manager for Vancouver に名前が変更されました。バージョン 1.0.9 以前を使用している場合、アプリケーションは引き続き Manufacturing Process Manager と呼ばれます。バージョン 2.0 を使用している場合、アプリケーションは Industrial Process Manager と呼ばれます。

詳細を読む



メーカーが 産業用プロセスマネージャー

構成



実装の計画と構成

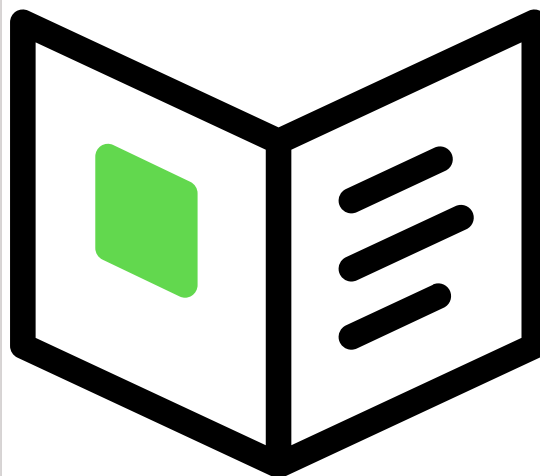
自動翻訳

使用



Operational Technology 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詳細

で使用される 産業用プロセスマネージャー一般的な用語、略語、および ISA-95 Equipment Model 業界標準の詳細については、を参照してください。

産業用プロセスマネージャー 一般的な用語

の使用を開始する 産業用プロセスマネージャー前に、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
Operational Technology	OT	物理プロセスを制御するために産業オートメーションで使用するテクノロジー。 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、産業企業向け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、それを変換してから、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記述できます。

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。

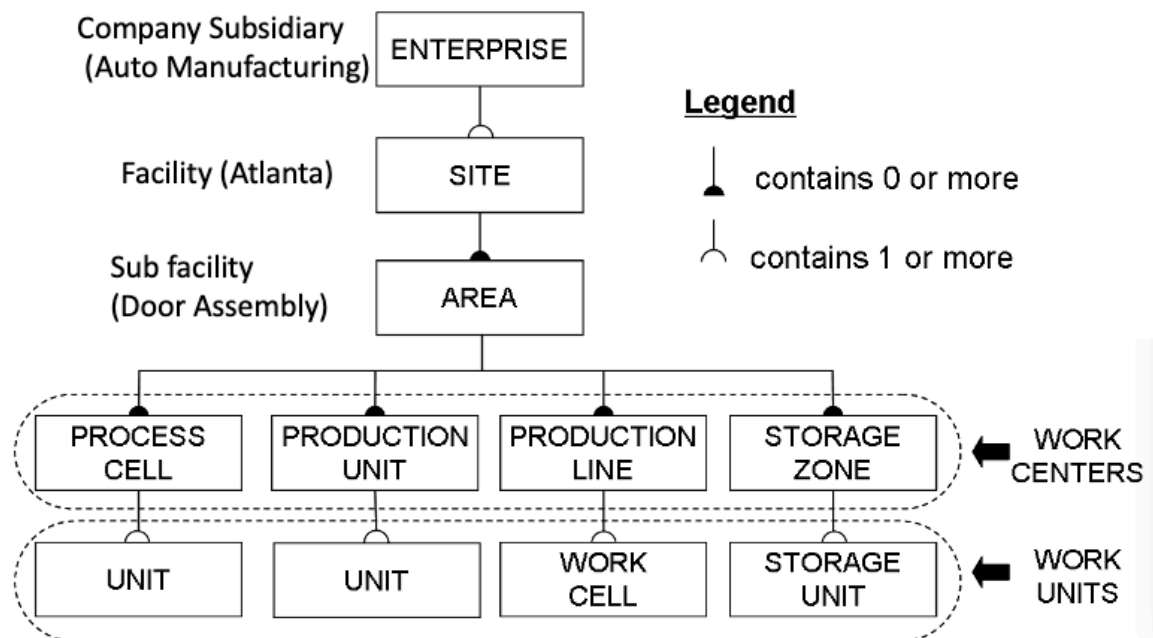
- 機器モデルエンティティをマッピングします。このマップを使用して、階層構造を作成します。
- 複数の産業サイトに対して複数の設備モデルを作成します。
- 各サイトにユーザーをアサインして、特定のサイトの機器モデル情報へのアクセスを管理できるようにします。たとえば、アトランタのユーザーがアトランタのサイト情報にのみアクセスでき、ミシガン州のサイトのデータにはアクセスできないように指定できます。詳細については、「[管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)」を参照してください。

設備モデルはサイトレベルから始まり、各工業用地を記述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、のインストール 産業用プロセスマネージャー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を製造する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、その従属ワークセンタ、および作業単位を表します。
- ワークセンタレベル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、ワークセンタレベルには 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
 - 本番ライン
 - 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して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ために使用できます。

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。

設備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。

設備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。

設備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。

装置テンプレートの詳細と構造の図の例については、「」および[設備モデルテンプレートの定義「」](#)を参照してください[ISA-95 機器モデル](#)。

の構成 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、アプリケーションを構成しますServiceNow Operational Technology。

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 業種別 アプリケーションのセットアップ 産業用プロセスマネージャー を進めることができます。

Guided Setup にアクセスするには、次の場所に移動します。 **Industrial Workspace** 管理者 > ガイド付きセットアップ。

タスク	目的
1. からをインストールし 産業用プロセスマネージャー ます ServiceNow Store。	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 産業用プロセスマネージャー ます。
2. ロールをアサインします 産業用プロセスマネージャー 。	各ユーザーが使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。
3. コネクタインポート用の サービスグラフ Excel スプレッドシートに入力Microsoftします。	Excel スプレッドシートを作成し、 Microsoft アップロードする Now Platform既存の ISA-95 設備階層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 設備階層モデルデータを に アップロードします 構成管理データベース (CMDB)。
5. パートナーが提供する ServiceNow 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。	で利用可能ServiceNow Storeになったときに パートナーが提供するコネクタをインストール しServiceNow、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 アクセスをアサインまたは削除 します。

タスク	目的
オプション:OT デバイスのマッピングを自動化する	OT デバイスの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。 - Operational Technology Manager - 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、アプリケーションと関連プラグインをインストール 産業用プロセスマネージャー 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ます。詳細については、次を参照してください。 [のエンタイトルメントの取得 ServiceNow 製品またはアプリケーション](#)。

必要なロール：admin

このタスクについて

次のアイテムがとともにインストールされます:産業用プロセスマネージャー

- プラグイン
- Guided Setup を含むアプリケーションメニュー
- ロール
- テーブル

アプリケーションとともに 産業用プロセスマネージャー 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、「」を参照してください [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](#)。

手順

- 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](#)。
- 産業用プロセスマネージャー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。

- 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

るプラグインまたはアプリケーションがある場合は、をインストールする 産業用プロセスマネージャー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。

Industrial Workspace 管理者 アプリケーションメニューと Guided Setup

アプリケーションと関連プラグインをインストールした後、Industrial Workspace 管理者アプリケーションメニューを使用して、関連するOperational Technology Manager、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Operational Technology Vulnerability Response、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ます。

Industrial Workspace 管理者 アプリケーションメニューの内容

アプリケーションメニューにアクセスする Industrial Workspace 管理者 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。この Operational Technology Management 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。

- Operational Technology Manager
- 産業用プロセスマネージャー
- Operational Technology Vulnerability Response
- オペレーショナルテクノロジーインシデント管理、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:

と 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オペレーショナルテクノロジーインシデント管理、まず または Operational Technology Manager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。

アプリケーションメニューに表示される Industrial Workspace 管理者 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、ユーザーに割り当てられているロールによって異なります。をインストールする 産業用プロセスマネージャー と、アプリケーションメニューで Industrial Workspace 管理者 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
- OT マネージャー。次の選択肢があります。
 - OT マネージャー管理者
 - 産業用プロセスマネージャー
 - OT インシデント管理者
 - 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、「」およびユーザーロールのアサイン産業用プロセス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 をインストールする。

Industrial Workspace 管理者 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アプリケーションのセットアップ 産業用プロセスマネージャーを進めることができます。

Guided Setup にアクセスするには、次の場所に移動します。 **Industrial Workspace** 管理者 > ガイド付きセットアップ。

ガイド付き設定でロック解除済みとして表示される具体的な手順は、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。

のみが 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、次のセットアップ機能はロックされます。

- セットアップ手順。Operational Technology Manager
- に依存するすべての産業用プロセスマネージャーステップ。Operational Technology Manager
- セットアップ手順。Operational Technology Vulnerability Response
- 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

Guided Setup とその使用方法の詳細については、「 [Guided Setup の使用](#)」を参照してください。

ユーザーロールのアサイン産業用プロセスマネージャー

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	説明
設備モデルビューア [cmdb_ot_isa_viewer]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] テーブルレコードのみを表示できます。詳細については、「 での使用産業用プロセスマネージャーOperational Technology Manager 」と「 機器モデルの管理 」を参照してください。
設備モデルエディタ [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、「 での使用産業用プロセスマネージャーOperational Technology 」

ロール	説明
	Manager と「 機器モデルの管理 」を参照してください。
機器モデル管理者 [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。 - 業種別 Guided Setup を使用して と 産業用プロセスマネージャー を設定します Operational Technology Manager。 - 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します。 詳細については、「Industrial Workspace 管理者 アプリケーションメニューと Guided Setup」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 設備階層モデルレコード (cmdb_ci_ot_isa_entity) および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た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[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すべての Operational Technology (OT) 関連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

の Now Platform[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。

- の検出 Operational Technology
- 産業用プロセスマネージャー
- ISA 設備階層モデル
- Operational Technology Manager
- 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

手順

1. 移動先 **すべて > Industrial Workspace 管理者 > 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. アプリケーションの必要に応じて、利用可能なシステムプロパティを編集します。
4. [更新] を選択します。

設備モデルテンプレートの定義

で Now Platform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の作成

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 > Industrial Workspace 管理者 > 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. **[New (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。
説明	機器モデルテンプレートの説明。

フィールド	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. [Submit (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の作成

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、これらのレベルで、表示されるデータがソートされ構造化されます。

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、その他のレベルを設備に割り当て、それぞれのソート順序を指定することができます。

手順

1. 移動先 **すべて > Industrial Workspace 管理者 > 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	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。 エリア 工業用地内のエリア。 ワークセンター 工業用地のワークセンター。
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。 ○ サイトレベルを作成している場合、それが親を持たない機器モデル階層のトップレベルである場合は、このフィールドを空のままにします。

フィールド	説明
	- 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、その親として サイト を選択します。 - 作業区レベルを作成し、それがエリア レベルの子である場合は、その親として エリア を選択します。
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	ソート目的で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が、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. [Submit (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で詳細なタイプを作成します。

機器モデルレベルタイプの作成

作成した各機器モデルテンプレートレベル内に詳細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記述します。

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、ワークセンタレベルには以下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 > Industrial Workspace** 管理者 > 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	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割り当て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. [Submit (送信)] をクリックします。

設備モデルデータのインポート

インポートスケジュール機能を使用すると、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、をインストールする 産業用プロセスマネージャー 必要があります。

機器モデルデータをに Now Platform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 設備階層モデルデータを入力し、**SG-Equipment Model Scheduled Import Using Spreadsheet** スケジュール設定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. また、複数の ServiceNow パートナーが、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を開発しています。
 - これらの統合が利用可能になったら、の認定統合産業用プロセスマネージャーを検索しOperational Technologyで見つけることができますServiceNow Store。
 - 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と、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、既存の Now Platform 設備階層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 機器モデルエンティティ CI クラスレコード 構成管理データベース (CMDB)が自動的に作成されます。

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、Excel スプレッドシートに機器モデルデータを入力する Microsoft 方法と、機器モデルのインポート - ETL プロセス機能に影響します。

`sn_isa_model.cmdb_relationships_sync_levels`

に Now Platform インポートして で 構成管理データベース (CMDB)同期できる機器モデルの何レベルかを決定します。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 [短縮コード] 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_file_size

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:

システムの動作を制御するためのシステムプロパティの追加または作成の詳細については、「[システムプロパティの追加](#)」を参照してください。

Excel スプレッドシートに Microsoft 機器モデルデータを入力します

Excel スプレッドシートを作成し Microsoft、既存の ISA 設備階層モデルデータを入力します。既存のデータを正しい列に配置することは、アップロードを成功させるために重要です。

にNow Platform正しく構成管理データベース (CMDB)入力された Excel スプレッドシートを作成するにはMicrosoft、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 Excel スプレッドシートを使用して Microsoft、スプレッドシートをアップロードする準備をします。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** > 輸入設備。モデル - データソース

b. **[Import Equipment Model - Data Source - v2.xlsx]** をクリックします。

i 注:

または、「設備階層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、のNow Support ナレッジベース「[ISA 設備階層モデル 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」を参照してください。

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

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	このトピックにある情報と同様に、スプレッドシートのデータ列の説明を提供します。
インポートするサンプルデータ	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. Excel スプレッドシートに Microsoft 入力したら、ETL 関数を実行する 統合ハブ 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。

i 注:

列名は変更できません。列を追加して、システムプロパティで `sn_isa_model.user_search_matching_attribute` 指定されている所有者を一意に識別するためのフィールドを追加できます。

スプレッドシートの入力

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**)

複数のサイトからデータを 1 つのスプレッドシートにインポートできます。サンプルイメージは、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	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。例えば、ATL-B42-MQSTOR-Z1 は、以下のショート・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	ショートコード	文字列、英数字のみ	エンティティの簡単な説明コード。短縮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、システムプロパティで <code>sn_isa_model.short_code_validation_max_length</code> 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	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。たとえば、都市名、建物番号、モデル番号などです。	はい
D	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。に格納されNow Platformている 構成管理データベース (CMDB) cmn-location 値で、これを参照として使用します。	いいえ
E	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ユーザーのメールアドレス。 i 注: システムプロパティで <code>sn_isa_model.user_search_matching_attribute</code> 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保守と管理をサポートするグループの名前。	いいえ
G	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対してどの程度重要または重要であるかを示す測定値。次に例を示します。 • 1 - 最重要。 • 2:ある程度重要。	いいえ
I	会社	文字列	エンティティが属する会社の名前。に格納されNow Platformている CMDB cmn-location 値で、これを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使用して Microsoft Excel スプレッドシートに入力したら、データソースとインポートスケジュールを使用してスプレッドシートをインポート Now Platform 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、「[Excel スプレッドシートに Microsoft 機器モデルデータを入力します](#)」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に対して、一意の機器モデルエンティティ CI クラスレコード 構成管理データベース (CMDB) が作成されます。

手順

1. 移動先 **すべて > 機器モデル : ISA > 輸入設備**。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す。

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. [変換] 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へのアクセス権のアサインまたは削除

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りまたは編集できるかどうかを決定します。ユーザー基準レコードを作成したら、それをサイトに割り当てて、機器モデルエンティティの読み取りと編集ができるユーザーを制御できます。さらに、OT ロールをユーザーまたはグループにアサインして、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、「[Operational Technology Manager 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. **[New (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

ユーザー条件を作成したら、それを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、「」を参照してください [サイトへの \[編集可能\] アクセスのユーザー基準を割り当てる](#)。サイトへの読込可能アクセス権の追加の詳細については、「」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の割り当て](#)。

サイトへの読み取り可能アクセスのユーザー基準の割り当て

ユーザー基準をサイトに割り当てて、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りまたは表示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

[読込可能] アクセスのユーザー基準は、次の 2 つの場所で割り当てることができます。

- 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 [機器モデルを読み取り可能] 関連リストから

手順

1. テーブルまたは関連リスト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読み取りまたは表示できるユーザーを定義するユーザー基準を選択します。

注:

ユーザーが cmdb_ot_viewer ロールを持っている場合、ユーザーは選択したサイトに割り当てられている (OT) デバイスを表示する Operational Technology こともできます。

ユーザーにcmdb_ot_editorロールがある場合、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割り当てる

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 つの場所で割り当てることができます。

- 機器モデルエンティティの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、ユーザーは選択したサイトに割り当てられている (OT) デバイスを表示する Operational Technology こともできます。

ユーザーに cmdb_ot_editor ロールがある場合、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の管理

アプリケーションを使用して 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を管理できます。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の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できます。機器モデルダウタイムプランナーロール (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。
- スケジュールからタイムスロットを選択して、(OT) インシデントまたは修正タスクを処理 Operational Technology できるようにします。詳細については、「[OT 修正タスクの開始時間の選択](#)」を参照してください。

例

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。

スケジュールを機器モデルエンティティに関連付ける必要がなくなった場合は、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、機器モデルワークスペース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行うことができます。

機器モデルエンティティのスケジュールの作成

アプリケーションで 産業用プロセスマネージャー 機器モデルエンティティ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 > Industrial Workspace 管理者 > 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. **[New (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。[浮動] 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です。 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 ~ 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 ~ 17:00 と表示されます。1 つの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の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

アプリケーションの既存の機器モデルエンティティのスケジュール 産業用プロセスマネージャー 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 > Industrial Workspace 管理者 > 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. **[New (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。
周期	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。次のオプションが含まれます： ○ 月の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。次のオプションが含まれます： ○ 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月。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。
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たら、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

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、またはアプリケーションでの 産業用プロセスマネージャー 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。
 - **[New (新規)]** を選択します。
 - フォームに入力し、[送信] を選択すること。
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を作成、削除、または編集します。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、編集されたバージョンのスケジュールを表示したりできます。

機器モデルエンティティへのスケジュールの添付

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 産業用プロセスマネージャー。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. **[Save (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

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。産業用プロセスマネージャー。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. 中央矢印を使用して、選択した集計表をコレクションリストに移動します。
7. **[Save (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の表示

アプリケーション内の 産業用プロセスマネージャー 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

作業場所に応じて、次の 2 つの場所で機器モデルエンティティのスケジュールを表示できます。

- 機器モデルワークスペース
- プラットフォーム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 ワークスペースで機器モデルエンティティ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. 機器モデルワークスペースに移動します。
 - b. 機器モデルエンティティレコードを選択します。
 - c. [スケジュールの表示] 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 > **Industrial Workspace** 管理者 > 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。

子スケジュールの追加

アプリケーションを使用して 産業用プロセスマネージャー、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 > **Industrial Workspace** 管理者 > 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. [Save (保存)] を選択します。

タスクの結果

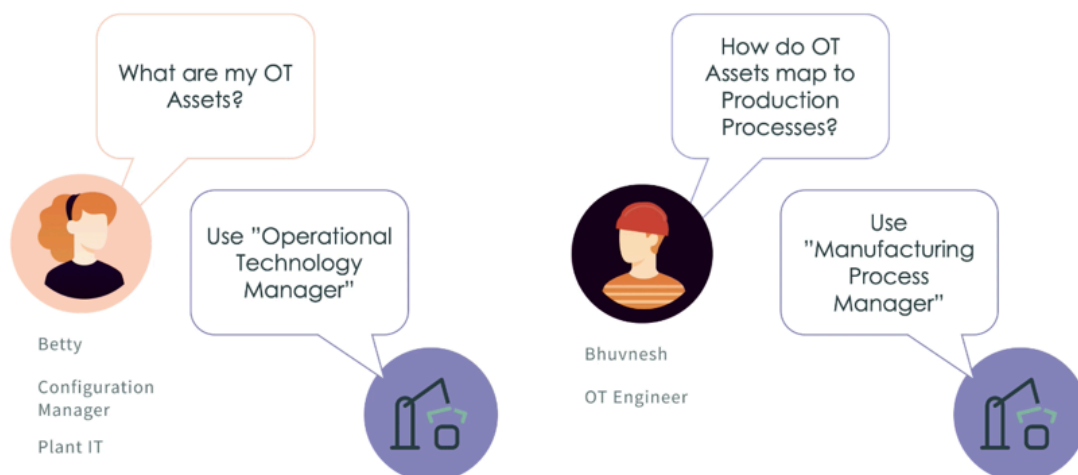
選択した子スケジュールが親スケジュールに適用されます。

での使用産業用プロセスマネージャーOperational Technology Manager

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、メニューの Industrial Workspace 管理者 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 Operational Technology Manager。これらの機能には、機器モデルワークスペースとワークスペースの Operational Technology Manager ランディングページが含まれます。

以下の図は、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 Now Platform、その質問に答えるために使用する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担当者の質問



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 はメニューの機能 Industrial Workspace 管理者を使用できます Operational Technology Manager。詳細については、「[Operational Technology \[デバイスのランディングページ\] タブ](#)」を参照してください。

OT エンジニアの Bhuvnesh は、サイト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やPLCが工業処理のこの特定の部分を制御しているのか? この質問に答えるために、サイトレベルの OT マネージャーはメニューの機能を使用できます産業用プロセスマネージャー Industrial Workspace 管理者。

機器モデルの管理

機器モデルワークスペースを使用すると、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、それらを使用して自動車を製造するアトランタの産業施設です。機器モデルワークスペースを使用すると、特定の産業サイトに対して選択した機器モデルエンティティを表示し、次のタスクを実行できます。

- 機器モデル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:

アサインされた `cmdb_ot_isa_admin` ロールを持つユーザーは、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、「[」](#)を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

機器モデルの詳細の確認および更新

にインポートした Now Platform 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できます。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、「[設備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 > Industrial Workspace 管理者 > 産業用プロセスマネージャー > 機器モデルワークスペース**.
2. [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確認するか、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	説明
エンティティ名	機器モデルエンティティの名前。
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。 i 注: 機器モデルエンティティが作成された後に [親] フィールドを更新できます。
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ている機器モデルテンプレート。 i 注: ETL またはサードパーティの統合を使用して統合ハブインポートしたNow Platform 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割り当てられる階層レベル。次に例を示します。 サイト 工業用地。 エリア 工業用地のエリア。

フィールド	説明
	ワークセンター 工業用地の作業区。 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の作成」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割り当てら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の作成」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。
ショート 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。例えば、ATL-B42-MQSTOR-Z1 は、以下のショート・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。
ロケーション	機器モデルエンティティの場所。たとえば、アトランタビルディング 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。
会社	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。
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割り当てられたユーザー。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。
管理担当者	このエンティティレコードを所有し、管理の責任を負っているアサインされたユーザーの名前。機器モデル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。
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対してどの程度重要であることを示す測定値。エンティティのプロセスの重要度を選択します。例：

フィールド	説明
	○ 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。
会社	機器モデルエンティティが属する会社の名前。core_company値は、の Now Platform に参照として格納CMDB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: 運用 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 本番プロセスで稼働していないエンティティ。

5. 次のように、関連リストタブで関連する機器モデルデータを確認します。

タスク	説明
機器モデル階層の表示	「 機器モデル階層の表示 」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. 「アップストリーム・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を確認します」を参照してください。

タスク	説明
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트롤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
- 修正タスク

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、で直接新しい Now Platform 機器モデルエンティティを手動で作成する場合に行います。

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

アサインされたcmdb_ot_isa_adminロールを持つユーザーは、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ているユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

手順

1. 移動先 **すべて > Industrial Workspace 管理者 > 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. [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] をクリックします。
4. 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。
ショート 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割り当てら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の作成 」を参照してください。

5. **[Save (保存)]** をクリックします。

6. [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および更新](#)」を参照してください。

機器モデル階層の表示

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

アサインされたcmdb_ot_isa_adminロールを持つユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

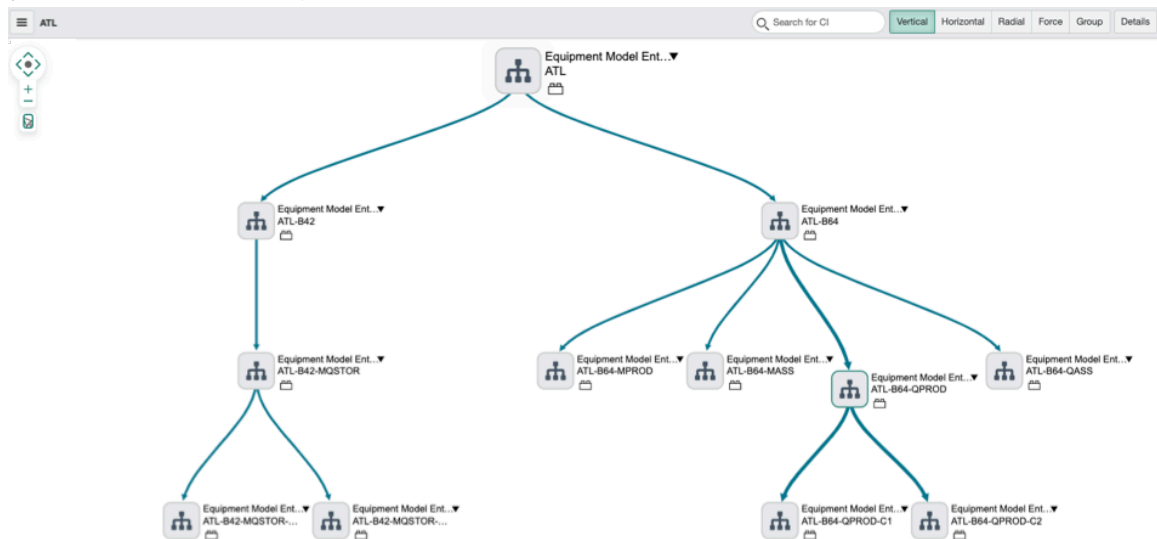
手順

1. 移動先 **すべて > Industrial Workspace 管理者 > 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. [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 サイト エンティティをクリックすると、サイト全体の表示が表示されます。
4. 機器モデルエンティティの階層構造を表示するには、**階層の表示** 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、次のグラフィック表示が表示されます。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



機器モデルの OT デバイスマップを表示

選択した機器モデルエンティティと、生産プロセスの他の Operational Technology (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

アサインされた cmdb_ot_isa_admin ロールを持つユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

手順

1. 移動先 **すべて > Industrial Workspace 管理者 > 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. [機器モード ビューの対象] 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のデバイスとの関係を表示するには、[**OT デバイスマップの表示**] を選択します。

機器モデルの OT 依存関係マップの表示

選択した機器モデルエンティティの階層構造と、生産プロセスの他のエンティティおよび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

アサインされたcmdb_ot_isa_adminロールを持つユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

手順

1. 移動先 **すべて > Industrial Workspace 管理者 > 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. [機器モード ビューの対象] 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、その階層と他のデバイスおよび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および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。また、機器モデルエンティティの新しいアップストリーム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

アサインされたcmdb_ot_isa_adminロールを持つユーザーは、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ているユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

手順

1. 移動先 **すべて > Industrial Workspace 管理者 > 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. [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 ウィンドウで、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. 機器モデルのアップストリーム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. [Submit (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生産プロセスをマッピングします

ダウ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。また、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

アサインされたcmdb_ot_isa_adminロールを持つユーザーは、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ているユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

手順

1. 移動先 すべて > **Industrial Workspace** 管理者 > 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. [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 ウィンドウで、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、新しいモデルをマッピングします。
6. [Submit (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を確認します

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

アサインされたcmdb_ot_isa_adminロールを持つユーザーは、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ているユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

手順

1. 移動先 すべて > **Industrial Workspace** 管理者 > 産業用プロセスマネージャー > 機器モデルワークスペース。
2. [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 ウィンドウで、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、[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、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 Operational Technology Manager 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、ログインユーザーに次のロールが割り当てられ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

i 注:

ユーザーロールの割り当ての詳細については、以下を参照してください [ユーザーロールのアサイン産業用プロセスマネージャー](#)。

このタスクについて

アサインされた cmdb_ot_isa_admin ロールを持つユーザーは、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、「」を参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

手順

1. 移動先 **すべて > Industrial Workspace** 管理者 > 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. [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 ウィンドウで、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. 関連付けられた OT デバイスをレビューするか、追加の OT デバイスを選択した機器モデルエンティティに関連付けます。
6. [保存] をクリックします。

OT デバイスの機器モデルへの自動マッピング

OT デバイスの本番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に遭遇する場合、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、OT デバイスが自動化する本番プロセスにどのように接続するかコンテキストは、作業の優先順位付けにとって重要です。OT デバイスの 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:

サイトごとにサポートされるサブネット範囲は 1 つだけです。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インスタンスに ServiceNow 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た ISA エンティティへの OT デバイスのアサインの自動化
- 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、すべての機器が積分器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、ラインの実行に使用される自動化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 サイトの缶詰ラインにマッピングされている場合、管理者は IP 192.168.101.66 で検出された 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 用 OT 認定統合または ServiceNow [Discovery](#) 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。

システム管理者は 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 管理者は、スケジュール設定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。

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。

- [Operational Technology Manager](#)
- [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 管理者は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 [産業用プロセスマネージャー](#) 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

には [産業用プロセスマネージャー](#)、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、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するために使用できます。

使用する [フローデザイナー](#)  を使用すると、ビジネスニーズに合わせて事前定義されたフローを確認および構成できます。

この機能で利用可能なフロー

次の表は、をインストールしOperational Technology Managerたときに使用できる産業用プロセスマネージャー定義済みのフローの一覧です。

アプリケーション	フロー
産業用プロセスマネージャー インストール時 Operational Technology Manager	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

通常、次のユースケースは自動マッピング機能に適用されます。

- OT マネージャーは既存の OT デバイスを持っており、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ます。
- OT 管理者は、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は次のとおりです。

- システム管理者は、[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。
- 優れた管理者は、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) ます。
- 優れた管理者は、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。

Guided Setup 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 Guided Setup 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、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、OT デバイスを ISA 機器モデルエンティティにマッピングする手順を順を追って行うことができます。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 > Industrial Workspace 管理者 > ガイド付きセットアップ**.
2. アプリケーションの [開始]産業用プロセスマネージャー 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 デバイスの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

優れた管理者は、すべての OT デバイスの適切な ISA 設備階層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。

- [Operational Technology Manager](#)
- [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 **Industrial Workspace** 管理者 > 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 デバイスのマッピング] 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 管理者は、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。

- [Operational Technology Manager](#)
- [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 **Industrial Workspace** 管理者 > 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] および [機器モデルエンティティ] フィールドに正しく入力されていることを確認します。
4. [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て、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** デバイスの表示

サイトにアサインされていない (OT) デバイスのリスト Operational Technology 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。

- [Operational Technology Manager](#)
- [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て [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、[列オプション] ボタンを選択し、[選択項目の更新] を選択します。
 - 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](#)」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

機器モデルエンティティにマッピングされていない IP アドレスを持つ (OT) デバイスのリスト Operational Technology 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。

- [Operational Technology Manager](#)
- [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**.
2. 業種別 ワークスペースオペレーショナルテクノロジー (**OT**) モジュールのリストビューで、[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にマッピングするため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、[サイトごとにグループ化] 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 デバイスをサイトごとに整理でき、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

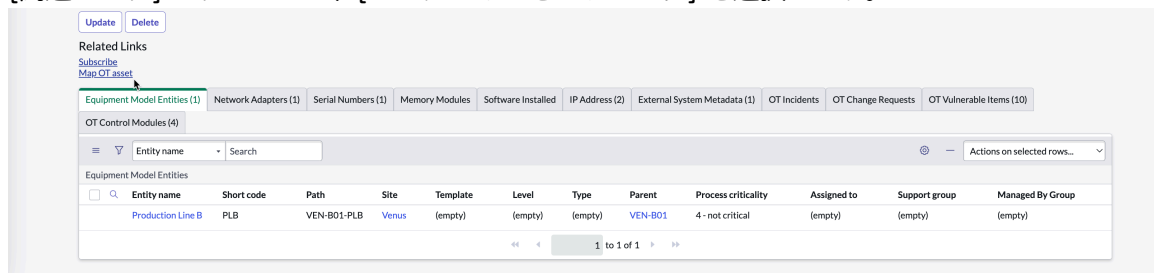
次のプラグインをインストールする必要があります。

- [Operational Technology Manager](#)
- [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。

- [Operational Technology Manager](#)
- [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 **Industrial Workspace** 管理者 > 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。
有効化後、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の表示

機器モデルエンティティにアサインされたすべてのマッピング済み OT サブネットを表示します。

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、ワークスペースに移動します。
 - 移動先 **すべて** > **Industrial Workspace** 管理者 > 産業用プロセスマネージャー > 機器モデルワークスペース。
 - 業種別ヘッダーのワークスペースメニューアイテムからワークスペースを選択します。
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 デバイスレコードで [**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](#)

新しい **OT** サブネットマッピングレコードを作成

新しい OT サブネットマッピングを作成して、機器モデルエンティティに関連付けます。

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と、デフォルトでは新しいレコードは非アクティブになります。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 **Industrial Workspace** 管理者 > 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

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、使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のソースの名前。
ファイアウォール名	ゾーンを管理するファイアウォールの名前 (該当する場合)。
説明	サブネットマッピングの説明。
アクティブ	[アクティブ] を選択すると、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が自動マッピングに含まれます。
機器モデルエンティティ	ルックアップから、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)。

フィールド	説明
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。
ロケーション	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するには、サブネットレコードに場所を追加します。 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、次を参照してください OT サブネットマッピング機能で使用されるシステムプロパティ。
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 Operational Technology (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 > Industrial Workspace 管理者 > 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されるシステムプロパティ

優れた管理者は、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。

優れた管理者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 **Industrial Workspace 管理者 > 産業用プロセスマネージャー > OT サブネットマッピングプロパティ**。

OT サブネットマッピングシステムプロパティ

プロパティ	説明
<code>sn_otsm.map_all_ot_assets.all_discovery_sources</code>	すべての検出ソースの OT デバイスのマッピングを制御します。すべての検出ソースの OT デバイスをマッピングします。オンにすると、以下の特定の検出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_sources</code>	指定された検出ソースの 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 [すべての検出ソースの 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>	Ownership 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。

と両方がインストールされるときに産業用プロセスマネージャー **Operational Technology Manager** 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、スケジュール設定済みフローなど) もアクティブになると Operational Technology Manager インストール産業用プロセスマネージャーされます。

これらの自動マッピング・コンポーネントは、とともにインストールされるか、またはインストール Operational Technology Manager される場合に産業用プロセスマネージャー使用可能です。

テーブル

テーブル	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]	機器モデルエンティティへの OT サブネットのマッピングを保存します。

プロパティ

プロパティ	説明
<code>sn_otsm.map_all_ot_assets.all_discovery_sources</code>	すべての検出ソースの OT デバイスのマッピングを制御します。 デフォルト値: True
<code>sn_otsm.map_all_ot_assets.discovery_sources</code>	指定された検出ソースの OT デバイスをマッピングします (カンマ区切り形式)。

プロパティ (続く)

プロパティ	説明
sn_otism.subnet_mapping.auto_assign_ot_controls	OT デバイスに属する OT モジュールに基づいて、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_otism.subnet_mapping.location_auto_update	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。

Flow Designer 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 Operational Technology Manager 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

いくつかのタイプのコンポーネント (ユーザーロールなど) が、アプリケーションのアクティブ化 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場合があります。

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
設備モデルビューア [cmdb_ot_isa_viewer]	アサインされた ISA 設備階層モデル [cmdb_ci_ot_isa_entity] テーブルレコードのみを表示できます。詳細については、「 での使用産業用プロセスマネージャーOperational Technology Manager 」と「 機器モデルの管理 」を参照してください。
設備モデルエディタ [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、「 での使用産業用プロセスマネージャーOperational Technology Manager 」と「 機器モデルの管理 」を参照してください。

ロール	説明
機器モデル管理者 [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。 - 業種別 Guided Setup を使用してと 産業用プロセスマネージャー を設定します Operational Technology Manager。 - 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します。 詳細については、「Industrial Workspace 管理者 アプリケーションメニューと Guided Setup」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 設備階層モデルレコード (cmdb_ci_ot_isa_entity) および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た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[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。

[ユーザー基準] フォーム (続く)

フィールド	説明
	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。
所在地	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 (場所の ) 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述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 > **Industrial Workspace** 管理者 > すべての **OT** プロパティ. OT システムの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、次を参照してください **OT システムプロパティの表示と編集**。

次の表では、ISA 設備階層モデルのシステムプロパティについて説明します。

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	説明	タイプ
sn_isa_model.cmdb_relationships	同期される関係のレベル。Byn の関係の CMDB 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_matching_attribute	システム内のユーザーと一致するユーザーテーブル [sys_user]	文字列

ISA 設備階層モデルシステムプロパティ (続く)

システムプロパティ	説明	タイプ
	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。	

の事前定義されたフィルター 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 では、事前定義されたフィルターを使用するため、で 業種別 ワークスペース利用可能な 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。

では 産業用プロセスマネージャー、次の定義済み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 Operational Technology (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 デバイスとの関係のグラフィカル表現。

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、「[事前定義されたフィルターの変更](#)」を参照してください。

事前定義されたフィルターの変更

組織の必要に応じて、ISA 設備階層モデルアプリケーションの事前定義された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 > Dependency Views > 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. 編集する事前定義された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、次のリンクを参照してください [Create a predefined filter](#)。
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は、(OT) の Operational Technology 用途が異なります。

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、次のリンクを参照してください [管理者以外の機器モデルサイトへのアクセス権のアサインまたは削除](#)。

サイトは場所を持つことができますが、場所とは見なされません。どの OT デバイスも場所を持ち、機器モデルエンティティサイトに割り当てることができます。

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、設備モデルの 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、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てください。

概要

拡張クラスは、Operational Technology Management.構成管理データベース (CMDB)

[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) OT の更新クラス。

関連アプリケーション

[Operational Technology Manager](#)

アプリケーションを使用すると Operational Technology Manager、複数のソースから OT デバイスデータを集計できるため、ソリューションで使用される 業種別 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

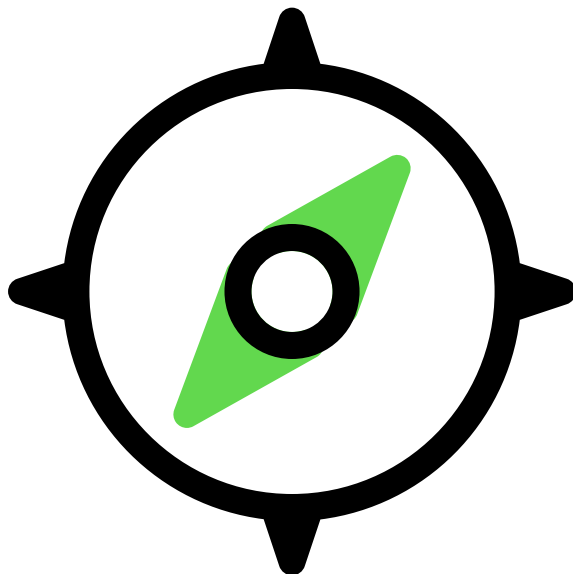
産業用プロセスマネージャーOperational Technology アプリケーションに関連付けられた (OT) ペルソナ。

[End]

Operational Technology Vulnerability Response

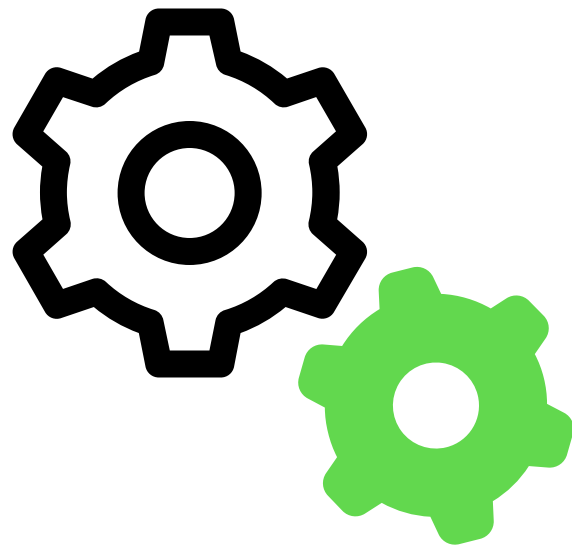
Operational Technology Vulnerability Response により、サイトレベルでの OT デバイスの脆弱性に対する効果的な優先順位付けと修復が可能になります。OT デバイスの CMDB 関係を活用することで、自動化する本番プロセスの重要度に基づいて脆弱なデバイスまたはアイテムに優先順位を付けることができます。

詳細を読む



Operational Technology
Vulnerability Response の詳細

構成



Operational Technology
Vulnerability Response の構成

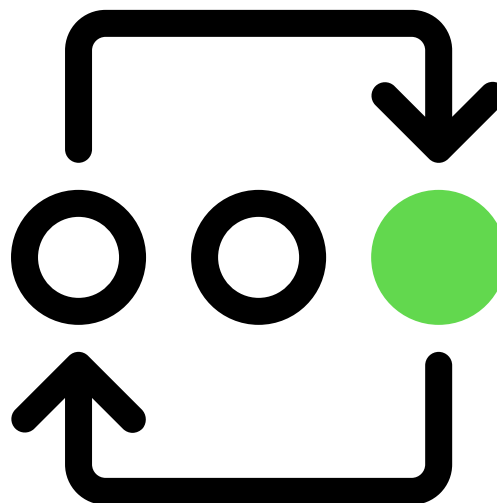
自動翻訳

使用



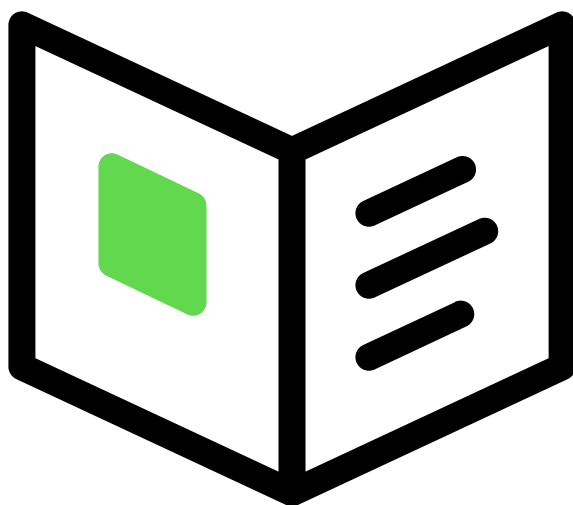
Operational Technology
Vulnerability Response の使用

統合



他のアプリケーションと統
合して拡張するOperational
Technology Vulnerability Response

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

Operational Technology Vulnerability Response の詳細

Operational Technology Vulnerability Response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、Operational Technology Vulnerability Response 次のような質問に対する回答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どのような進捗状況がありますか？

修復タスクと脆弱性一致アイテムのステータス

複雑なユースケースにより、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、「」を参照してください [Vulnerability Response remediation task and vulnerable item states](#)。

主な機能

を使用すると Operational Technology Vulnerability Response、次の主要な機能を使用できます。

- OT 脆弱性ランディングページは、アプリケーションからOperational Technology Vulnerability Responseデータを確認することができる一元的な場所です業種別 ワークスペース。
- (PA) ダッシュボードは Operational Technology Vulnerability Response 、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、および進捗状況を追跡します。

Operational Technology 脆弱性ランディングページタブ

[OT 脆弱性] ランディングページタブは、で一元化された場所です業種別 ワークスペース。このタブを使用して、アプリケーションから Operational Technology Vulnerability Response 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] ランディングページのタブでは、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表示する脆弱性リスクテーブル。

ランディングページタブのコンテンツ

[OT 脆弱性] ランディングページタブにアクセスするには、すべて > **Industrial Workspace** をクリックし、[ホーム] ( アイコンを選択して、[**OT 脆弱性**] タブを選択します。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、数、またはグラフのコンポーネントを選択します。

次の表では、[**OT 脆弱性**] ランディングページ タブのさまざまなタイルに表示される情報について説明します。

[OT 脆弱性ランディングページ (OT Vulnerabilities landing page)] タブ

タイル	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。
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要約した円グラフ。
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、脆弱性一致アイテムを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	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も強調表示されます。

OT ランディングページのフィルター

(OT) ランディングページのフィルター Operational Technology を使用して、ランディングページに表示するデータをサイト別または事業部門 (BU) 別に指定できます。たとえば、一度に複数のサイトの OT デバイスデータを表示できます。

概要

事業部門とサイトフィルターを使用すると、ランディングページに表示する 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拠点を選択して、その OT データを 1 つの場所に 業種別 ワークスペース表示できます。

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、ランディングページに利用可能なすべての BU の OT データが表示されま



BU フィルターを設定すると、ランディングページには、選択した BU に含まれるすべてのサイトのデータが表示されます。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、選択した BU に関連付けられているサイトのみが含まれるようにサイトフィルターが更新されます。

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、「」を参照してください [OT ランディングページで事業部門とサイトフィルターを使用する](#)。

サイトフィルター

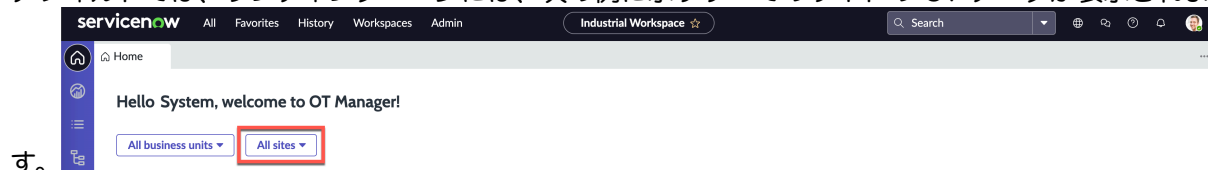
サイトフィルターを使用すると、次のアクションを実行できます。

- 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。
- サイトがアサインされていない OT データを表示します。

注:

OT デバイスにサイトが割り当てられていない場合、フィルターには [サイトが割り当てられていません] と表示されます。ランディングページ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、そのサイトに部署を割り当てる必要があります。

デフォルトでは、ランディングページには、次の例に示すすべてのサイトの OT データが表示されま



OT ランディングページで事業部門とサイトフィルターを使用する

(OT) ランディングページで事業部門 (BU) とサイトフィルター Operational Technology 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.**

2. ホーム () アイコンを選択して、ランディングページを開きます。

3. 1 つ以上の BU の OT データを表示します。

- ランディングページのヘッダーで、[すべての事業部門] メニューを選択します。
- 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 PT データを表示します。

- a. ランディング ページのヘッダーで、[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。ショートコードは、サイトの略語です。

OT 脆弱性ランディングページタブの設定

タスクを完了して ガイド付きセットアップ、組織のデータコレクション、インジケーターリソース、フィルターを含む **[OT 脆弱性]** ランディングページ タブの設定を開始できるようにします。

の ガイド付きセットアップ**[OT 脆弱性]** ランディングページタブにアクセスするには、次に移動します: **すべて > Industrial Workspace 管理者 > ガイド付きセットアップ** をクリックし、の Operational Technology Vulnerability Response**[OT 脆弱性ランディングページタブ]** セクションを選択します。

OT 脆弱性ランディングページタブとそのコンテンツの詳細については、次を参照してください[Operational Technology 脆弱性ランディングページタブ](#)。

次の表に、**[ガイド付きセットアップOT 脆弱性]** ランディングページタブを設定できるタスクを示します。

OT 脆弱性ランディングページタブ ガイド付きセットアップ のタスク

タスク	目的
1. OT 脆弱性日次データ収集ジョブを完了します。	[OT 脆弱性] ランディングページタブのすべてのパフォーマンスアナリティクスインジケーターの日次データを収集して表示します。他のユーザーがランディングページタブを表示する前に、このステップを完了する必要があります。
2. [オプション] インジケーターソースを確認します。	多数のレコードのインジケーターソースをレビューします。合計レコード数がデフォルト値の 100 万件を超えることが予想される場合は、レコードコレクション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

からすべてのインジケーターパフォーマンスアナリティクスの日次データを収集して表示できるように、(OT) 脆弱性一致アイテム (VI) のOperational Technologyデータ収集を構成します。この構成により、OT データがランディングページ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、ランディングページタブに利用できるデータがなく、[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。 OT

○ No Data is shown on the dashboard because the 'OT Vulnerable Items Daily Data Collection' job has not been run yet. [Run job now](#)

i 注:

admin ロールを持っていない場合は、管理者に問い合わせるように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 > データコレクター > パフォーマンスアナリティクス > ジョブ**.
[OT 脆弱性] ランディングページ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、**[スケジュール設定済みデータ収集]** テーブルに移動します。
2. フィルターを表示/非表示 ( を表示/非表示アイコン) アイコンを選択し、**[名前]** [次の値と同じ] **[OT 脆弱性一致アイテム日次データ収集]** 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、ランディングページ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、ジョブを最初に実行するとき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 脆弱性ランディングページタブに、ユーザー向けに収集された 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 ソースをレビューします。レコードコレクションを上書きして、ランディングページの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

を使用した パフォーマンスアナリティクス移行のため、**[OT 脆弱性]** ランディングページ 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 脆弱性一致アイテムの日次データコレクションジョブの実行後にレコード数が 100 万件を超えると、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、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、レコード数が 100 万件を超えた場合は、エラーメッセージが表示され、管理者にサポートを依頼す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 データを上書きすることができます。その後、他のユーザーにはエラー メッ

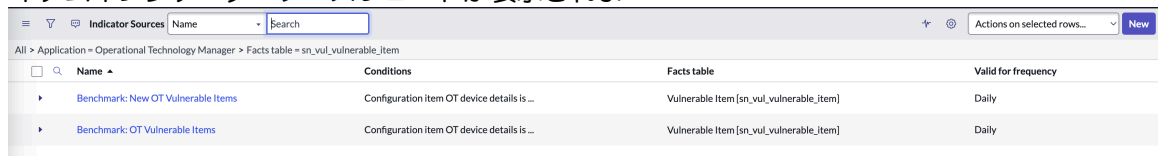
セージが表示されなくなり、インジケータ ソースのデータが表示されます。インジケータ ソースの詳細については、次を参照してください [Indicator sources](#)。

注:

ジョブログには、インジケータソースに関するものでは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 > 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. [フィルターを表示/非表示] () アイコンを選択してフィルターを適用し、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ー]
 - [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

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。
調整が必要なインジケータソースは、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する] 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. [フェッチされたレコードの最大数] フィールドで、値を [XM] に変更します。
6. [更新] を選択します。

Operational Technology Vulnerability Response (PA) ダッシュボード

(OT) 脆弱性一致アイテム (VI) の Operational Technology 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、エクスプロイト、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取得できます。

必須 Operational Technology および Operational Technology Vulnerability Response 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。

(PA) ダッシュボードを表示するには Operational Technology Vulnerability Response 、次に移動します: **すべて > Industrial Workspace** をクリックし、ナビゲーションパネルの **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。

Operational Technology Vulnerability Response (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	どの OT 脆弱性一致アイテムが最もリスクが高いかを判断することで、脆弱性の悪用によって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します。このダッシュボードでは、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、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。影響を受ける重大なデバイスや目立った脆弱性に関連する重要業績評価指標 (KPI) に注目できます。

[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、重要な測定基準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、改善が必要な領域を特定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] タブには、脆弱性のリスクとそのまん延、影響を受けるデバイス、修復ターゲットの遵守、および修復の進捗状況の KPI が表示されます。

[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 修正タスク
- 修正ターゲットを満たした OT VI
- OT VI 平均修正時間 (MTTR)
- 期限間近の OT の重大な修復タスク
- 経過時間別の OT VI
- 修復ターゲットステータス別のクローズ済み OT 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

[修復] タブ

[修復] タブは、修復アクションの進捗状況を把握し、修復を完了するため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重大な OT 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、過剰な修復の保留が原因で組織が負っているリスク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 OT 保留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なアイテムの OT 例外。

インジケータースソース

インジケータースソースは Operational Technology Vulnerability Response 、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ースソースの詳細については、次を参照してください (PA) [ダッシュボードの Operational Technology Vulnerability Response インジケータースソースとインジケータースソース](#)。

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、「[インジケータースソースを更新してより多くのレコードを収集する](#)」を参照してください。

インジケーター

アプリケーションの脆弱性修復 Operational Technology Vulnerability Response 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。ダッシュボードで使用されるインジケータースソースの詳細については、次を参照してください (PA) [ダッシュボードの Operational Technology Vulnerability Response インジケータースソースとインジケータースソース](#)。

インジケータースソースのレコード収集 オプションは、アプリケーションでは Operational Technology Vulnerability Response デフォルトで無効になっています。このオプションは、各インジケータースソース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ースソースは、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
- 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.非.クローズ済み
- 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
- 重大度
- 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、次を参照してください [Operational Technology Vulnerability Response \(PA\) ダッシュボードブレイクダウン](#)。

収集ジョブ

ダッシュボードは、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]脆弱性データの履歴収集
- [PA OT VR]修復タスクの日次収集
- [PA OT VR]脆弱性一致アイテムの日次収集 1
- [PA OT VR]脆弱性一致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、を参照してください [Operational Technology Vulnerability Response \(PA\) ダッシュボード収集ジョブ](#)。

データのビジュアル化

(PA) ダッシュボードでは、Operational Technology Vulnerability Response 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されるデータの可視化の詳細については、「」を参照してください [\(PA\) ダッシュボードで使用される Operational Technology Vulnerability Response データの可視化](#)。

Operational Technology Vulnerability Response の構成

(OT) アサインルール、修正ターゲット、リスク算出、およびリスクロールアップ計算を設定し Operational Technology 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。

注:

sn_vul.vulnerability_admin ロールを持っている場合は、ガイド付き設定を使用してアプリケーションのセットアップ Operational Technology Vulnerability Responseを進めることができます業種別。

Guided Setup にアクセスするには、次の場所に移動します。 **Industrial Workspace** 管理者 > ガイド付きセットアップ。

タスク	目的
1. からインストールしますOperational Technology Vulnerability ResponseServiceNow Store。	Operational Technology Vulnerability Response 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、管理者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。	各ユーザーが使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。
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使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。
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アサインします。 1. Operational Technology Vulnerability Response機器モデル マネージャーにある各サイトのサイト割り当てグループを作成します。 2. すでに cmdb_ot_isa_viewer または cmdb_ot_isa_editor ロールを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。

タスク	目的
5. OT 修正ターゲットルールを設定します。	- 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を修正するための予定期間を定義します。
6. アプリケーションのデモデータレコードを Operational Technology Vulnerability Response 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 リスク要因を決定します。
8. OT リスクロールアップ算出を設定します。	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. 環境に適用可能なアプリケーションの認定統合Operational Technology Vulnerability Response をインストールしOperational Technologyます。	認定されたサードパーティアプリケーションを統合して、OT 脆弱性管理の機能を強化します。

Operational Technology Vulnerability Response のインストール

admin ロールを持っている場合は、Operational Technology Vulnerability Response 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ます。詳細については、次を参照してください。[のエンタイトルメントの取得 ServiceNow 製品またはアプリケーション](#)。
- 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。
- Operational Technology Vulnerability Response には次のプラグインが必要です。Operational Technology Vulnerability Response 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、脆弱性を修復できるように、グループルールに従って脆弱性一致アイテムを自動的にインポートしてグループ化します。「[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)

ソリューションに必要な ISA-95 設備階層モデルデータ基盤を作成します ServiceNow 業種別。「[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。

Operational Technology マネージャー

Operational Technology Manager アプリケーションは、企業がソリューションを使用ServiceNow 業種別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。Operational TechnologyManager は、での Now Platform、サービスグラフコネクタ、および Discovery アプリケーションの使用構成管理データベース (CMDB)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

以下のアイテムは、アプリケーションのインストール Operational Technology Vulnerability Response 時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。

- [Operational Technology Vulnerability Response](#) 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. 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 Operational Technology Vulnerability Response 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。

**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。**Operational Technology Vulnerability Response ロールの割り当て**

ユーザーにロールをアサインすると、Operational Technology Vulnerability Response 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、Operational Technology Vulnerability Response アプリケーションを使用できます。

必要に応じて管理者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。

管理者ユーザーまたはグループへのロールのアサイン

ロール	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 統合管理者 [sn_otvr.integration_admin]	OT VR 統合レコードを表示および編集できます。

で 業種別 ワークスペースOT 脆弱性一致アイテムを修正するユーザーに、次のロールを追加します。

OT 脆弱性修正オーナーにロールをアサインする

ロール	説明
OT ビューアー [cmdb_ot_viewer]	OT デバイスレコードを読み取るための最小ロール。
OT ISA ビューアー [cmdb_ot_isa_viewer]	アサインされた機器モデルエンティティレコードを表示するための最小ロール。 また、レコードにアクセスする必要があるすべてのサイトにユーザーをアサインする必要があります。
VR 修正オーナー [sn_vul.remediation_owner]	脆弱性一致アイテムレコードを読み取り、編集できます。 修復タスクのアクティビティ履歴を表示できます。 メモの履歴を追加および表示できます。
VR クローズ [sn_vul.close_vi_vg]	脆弱性一致アイテムレコードを手動でクローズできます。

OT 脆弱性修正オーナーロールに加えて、修正 業種別 ワークスペースのために OT 脆弱性一致アイテムを機器モデルエンティティ別にグループ化するユーザー向けに、次のロールを追加します。

OT 脆弱性修正タスクユーザーのロールのアサイン

ロール	説明
VR 修正オーナー [sn_vul.remediation_owner]	修復タスクリストビューにアクセスできます。 分割タスク機能を実行できます。
修復タスクマネージャー [sn_vul.write_all]	すべての脆弱性一致アイテムと修復タスクを更新できます。
VR クローズ [sn_vul.close_vi_vg]	修復タスクをクローズできます。

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

[サイトアサイン先グループの作成](#)。

サイトアサイン先グループの作成

Equipment Model Manager で、サイトごとに 1 つの Operational Technology Vulnerability Response アサイン先グループを作成します。これにより、OT 修正オーナーユーザーはサイトの脆弱性一致アイテムのみを表示できます。

始める前に

アサイン先グループを作成し、Operational Technology Vulnerability Response であれば関連付け先の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は、グループに「ミラノ 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 > Industrial Workspace 管理者 > 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 アサイン先グループ**] フィールドで、検索アイコンを選択して既存のユーザーグループを表示します。
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、リストから選択します。
 - 目的のグループが存在しない場合は、[**新規**] を選択してグループを作成し、[**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

[ユーザーをサイトにアサインする](#)

ユーザーをサイトにアサインする

の構成時に cmdb_ot_isa_viewer または cmdb_ot_isa_editor ロールをすでに持っているユーザーをサイトにアサインしていない場合は、 を構成します 産業用プロセスマネージャー。

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、または admin ロールと、cmdb_ot_isa_viewer またはエディター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. [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アサインされます。

次のタスク

[ユーザーをアサイン先グループにアサインする](#)

ユーザーをアサイン先グループにアサインする

ユーザーをアサイン先グループに追加して、割り当てられた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。

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、可視性は以下に制限されます。

- 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アサイン先グループのメンバーシップ Operational Technology Vulnerability Response

必要なロール: admin

手順

1. サイトのアサイン先グループに対応する Operational Technology Vulnerability Response グループを開きます。
2. 「グループ・メンバー」タブで、「編集」を選択します。
3. [コレクション] リストから [グループ メンバー] リストにユーザーを追加します。
4. **[Save (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のグループへのアサイン](#)。

脆弱性一致アイテムのグループへのアサイン

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ます。Operational Technology Vulnerability Response には、OT 脆弱性アサインルールである **Operational Technology (OT)** アサインルールが 1 つ付属しています。このルールは、サイトに基いて OT 脆弱性一致アイテムレコード (VIT) を対応する OT VR アサイン先グループにアサインします。どのサイトにも属していない場合、またはサイトでグループが指定されていない場合、ルールは OT VR のデフォルトアサイン先グループにアサインされます。

Vulnerability Response アサインルールの作成の詳細については、「[Vulnerability Response 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. [脆弱性アサインルール] リストから、[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. 修正戦略に基づいて構成します。
 - 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ステータスを **true** に設定します。

次のタスク

[OT 修復ターゲットルールの構成](#)。

OT 修正タスクルールの構成

で 業種別 ワークスペース作成された修復タスクについては、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で 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をインポートすると、構成された修復タスクルールに基づいて修復タスクに追加できます。IT ネットワークと OT ネットワークの両方に使用する 脆弱性対応 場合、IT ネットワークと OT ネットワーク間で異なる方法で修正のために脆弱性一致アイテムをグループ化する場合は、構成を変更する必要があります。Operational Technology Vulnerability Response では、デモデータとともにロードされるサンプルの修復タスクルールレコードを提供し、OT ネットワークの脆弱性を自動的にグループ化から除外する方法を示します。

修正戦略に基づいて、新規または既存の修正タスクルールを設定します。

- 修正戦略が IT 環境内の脆弱性に対してのみ修正タスクを自動的に作成することである場合は、既存の各修正タスクルールに次の条件を追加して OT の脆弱性を除外します。
 - 構成アイテム。OT デバイスの詳細 = は空
- 修正戦略がすべての OT 脆弱性一致アイテムの修正タスクを自動的に作成することである場合は、適切なルールを作成します。

OT VR デモデータに同梱されるサンプル:修復タスクルール:脆弱性 (OT を除く)

A remediation task rule defines how a set of vulnerable items are automatically grouped for remediation. Define your rules such that all vulnerable items within a group are remediated by the same team, same remediation action, and same timeframe. For example, group by vulnerable item "Assignment group", "Vulnerability", and CI "Used for" (ex. Production, Staging, Development) if those environments have different maintenance windows. Vulnerable items that are not in the Open state are always excluded.

Name: Vulnerability (exclude OT) **Active:** ☐

Description: NOTE - this rule is necessary to avoid including OT assets automatically into remediation tasks - every remediation task rule will need to add an "AND" clause to do this. This is a copy of the existing "Vulnerability" remediation task rule, just renamed with the additional condition "Configuration Item - Ot asset details = is empty"

Case sensitive: ☐

Condition: All of these conditions must be met

AND

Active is true

OR

AND

Configuration item - Ot asset details is empty

Group by: Choose the vulnerable item fields to group by. If an extended table field is chosen, the field will be used only for vulnerable items that use the extended table.

Group vulnerable items from: Vulnerable Item Using field: Assignment group

And then from: Vulnerable Item Using field: Vulnerability

And then from: Vulnerable Item Using field: Click to select...

Assignment: If this rule groups vulnerable items by a user group field, such as vulnerable item "Assignment group", the remediation tasks can be assigned to match (Recommended). Use Assignment Rules to automatically set the vulnerable item "Assignment group" field for use in remediation task rules. Assign remediation tasks using the "Group by" field that specifies the desired user group field.

For example, a rule that groups on vulnerable item "Assignment group" could create separate groups for vulnerable items assigned to Windows Server, Database and Network. Each remediation task itself would then be assigned to Windows Server, Database and Network respectively.

Alternatively, remediation tasks created by this rule can be set to a static user group.

Assign remediation tasks by: Group by field

* Group by field: 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、および同じ期間によって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「使用目的」(例: 本番、ステージング、開発)で、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、「[Vulnerability Response 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探索](#)」を参照してください。

OT 修復ターゲットルールの構成

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、アプリケーションのデモデータレコードを Operational Technology Vulnerability Response ロードし、修正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

産業環境でメンテナンスを実行する機会はまだであるため、OT 修復ターゲットは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期間がない OT デバイスの脆弱性に対しては、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。ターゲット (日数) を更新し、レコードを有効にします。
- 重大なリスク評価ルール (OT を除く): 重大なリスクの非 OT アイテム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。ターゲット (日数) を更新し、既存の重要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 の重大なリスク脆弱性が OT 以外の修復ターゲットルールから除外されるようにするには、これらのルールの両方を有効にする必要があります。

Vulnerability Response 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](#)
- [Vulnerability Response 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 リスク要因を決定します。

始める前に

では Operational Technology、追加の要素として、OT デバイスの重要度、Purdue レベル、および OT デバイスが自動化する本番プロセスの重要度を含めることができます。

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、アプリケーションデモデータに付属 Operational Technology Vulnerability Response 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 を使用する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別々に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: サービスビジネス上の重要度ルールを使用します。
- OT デバイスの重要度: 構成アイテムの OT デバイスの詳細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] の [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. [脆弱性算出] リストから、[OT を使用したデフォルトリスク算出 (Default Risk Calculator with OT)] を選択します。
3. [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 デフォルトリスクルール] を選択します。
4. [脆弱性リスクルール] ページの [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の計算における重要度に従って、各条件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の構成

OT 脆弱性リスクロールアップ算出を使用して、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

- スケジュール設定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。

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、[機器モデルエンティティ] リストの [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、オンデマンドジョブを実行する *Update ISA entity service populator* 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] を選択します。

注:

[機器モデルエンティティ] リストに [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、アプリケーションデモデータに付属 Operational Technology Vulnerability Response 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 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. [脆弱性ロールアップ算出] リストから、[機器モデルエンティティのロールアップ] を選択します。
3. 必要に応じて、[ロールアップ重み付け] 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 > Industrial Workspace 管理者 > ガイド付きセットアップ**.
 - b. [Operational Technology Vulnerability Response] 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. [設定] を選択します。
 - e. ガイド付き設定で説明されている手順に従います。
2. ジョブスケジュール *Risk Rollup for VITs by Equipment Model Entity* を設定します。
 - a. 移動先 **すべて > Industrial Workspace 管理者 > ガイド付きセットアップ**.
 - b. [Operational Technology Vulnerability Response] 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. [設定] を選択します。
 - e. ガイド付き設定で説明されている手順に従います。

注:

デフォルトでは、ジョブは毎日実行す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のエンティティを設定します。
 - a. 移動先 **すべて > Industrial Workspace 管理者 > ガイド付きセットアップ**.
 - b. [Operational Technology Vulnerability Response] 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のエンティティ] タスクを選択します。
 - d. [設定] を選択します。
 - e. ガイド付き設定で説明されている手順に従います。

認定された脆弱性対応 統合をインストールする

認定されたサードパーティアプリケーションを統合して、OT 脆弱性管理の機能を強化します。

ServiceNow Store Operational Technologyアプリケーションの認定統合を検索し、ご使用の環境に適用可能な統合 Operational Technology Vulnerability Response をインストールします。

Operational Technology Vulnerability Response 統合

Operational Technology Vulnerability Response 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、次のサードパーティ統合がサポートされています。

- 脆弱性対応 向け 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 向け 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、(オンプレミス) から Microsoft Defender for IoT インポートされたデータを使用して、運用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、運用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。

主な機能

- OT デバイスに関連付けられた CVE を (オンプレミス管理コンソール) から Microsoft Defender for IoT 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の単一ビューを提供します。
- 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します。
- VIT の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するために、修復のためにローカルサイトベースのチームに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、インストール、関連 ServiceNow Store アプリケーション、およびプラグインが含まれます (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ます。詳細については、次を参照してください。 [のエンタイトルメントの取得 ServiceNow 製品またはアプリケーション](#)。
- をレビュー [脆弱性対応 向け 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ついては、の ServiceNow Store アプリケーションリストを参照してください。
- 脆弱性対応 for Microsoft Defender for IoT (On-premises Management Console) には、次の ServiceNow Store アプリケーションが必要です。と Microsoft Defender for IoT の統合をインストールする脆弱性対応前に、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ます。

CMDB CI Class Models ストアアプリ

この統合では、Operational Technology [拡張クラス](#)  CMDB CI Class Models アプリケーションの一部です。詳細については、「[CMDB CI Class Models store app](#) 」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、Operational Technology Manager 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。をインストールする サービスグラフには、「」を参照してください [サービスグラフ コネクタ \(Microsoft Defender for IoT オンプレミス管理コンソール\)](#)。

必要なロール：admin

このタスクについて

次の項目は、for Microsoft Defender for IoT (オンプレミス管理コンソール) と共に脆弱性対応インストールされます。

- Vulnerability Response プラグイン
- Vulnerability Response Integration with NVD

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. 脆弱性対応フィルター条件と検索バーを使用して (オンプレミス管理コンソール) を検索します Microsoft Defender for IoT。

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。

割り当て 脆弱性対応 先 **Microsoft Defender for IoT** (オンプレミス管理コンソール) ロール

ユーザーにロールを割り当てて、for Microsoft Defender for IoT (On-premises Management Console) アプリケーションの機能およびデータ脆弱性対応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。

必要に応じて管理者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	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 統合管理者 [sn_otvr.integration_admin]	OT VR 統合を構成して実行できます。
MID Server [mid_server]	を設定できます MID サーバー。

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。

National Vulnerability Database 統合の実行

National Vulnerability Database (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、お使いの環境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、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 製品がアプリケーションと適切に統合されます Operational Technology Vulnerability Response。

NVD プラグインをインストールするには、「」を参照してください [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#)。

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 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. [インポート開始日時] フィールドで、値を **NULL** に設定します。
4. [今すぐ実行] を選択します。

for Microsoft Defender for IoT の構成 脆弱性対応 (オンプレミス管理コンソール)

(オンプレミス管理コンソール) 統合の 脆弱性対応 Microsoft Defender for IoT 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。Guided Setup 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**.
2. **[New (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. **[資格情報の保存と検証]** 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 (On-premises Management Console) 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インスタンスです Microsoft Defender for IoT 脆弱性対応。
エンドポイント URL	管理コンソールの Microsoft Defender for IoT URL。 例: https://10.10.0.222/external/v3/integration/devicecves
MID Server	統合 MID サーバー に使用されます。
API キー	Central Manager API にアクセスするために必要なトークン。 管理コンソールでの Microsoft Defender for IoT API キーの作成については、「」を参照してください https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/references-work-with-defender-for-iot-apis 。
ページサイズ	API 応答の Microsoft ページあたりのデバイスの数。 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 (VI) レコードの作成で考慮されます。 デフォルト値は 0 に設定されています。

Microsoft Defender for IoT VR 構成フォーム (続く)

フィールド	説明
解決済み VI の自動クローズ	脆弱性一致アイテムレコードが解決済みに設定されている場合、その OT デバイスに対する API 応答に Microsoft Defender for IoT CVE が表示されなくなった場合に、自動的にクローズできます。
解決済み VI の再オープンまでの待機日数	VI が解決されても、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確認するには、しばらく Microsoft Defender for IoT 時間がかかる場合があります。 解決済み VI を NIDS が「クローズ済み」と確認できない場合に、解決済み VI を再オープンするまでの待機日数を定義します。

インポートスケジュールの構成

レコードにアクセスする Microsoft Defender for IoT 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

レコードの Microsoft Defender for IoT 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、「[National Vulnerability Database 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. レコードのリストから、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、接続の統合後に Microsoft サービスグラフ実行するように構成できます。「[OT 脆弱性対応 統合のシステム ID の構成](#)」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、解決済みの **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) は、スキャナーからの確認に基づいて自動的にクローズされます。

スコープが正しいアプリケーションにない場合は、ページの上部に「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. [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 の構成

SGC 接続の統合後に Microsoft 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 を設定します。

始める前に

必要なロール：admin

このタスクについて

この構成は、すべての OT デバイスが、それらに対して脆弱性が報告されている可能性がある CMDb 内にあることを確認するために強くお勧めします。

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は、ページの上部に「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

Save

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_msftd4iotsgc.ot.vr.integration.id を構成します。

4. [Save (保存)] をクリックします。

古い検出の自動クローズの設定

[古い脆弱性一致アイテムの自動クローズ (Auto-Close Stale Vulnerable Items)] 設定は、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一致アイテム (VIT) をクリーンアップ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

これらの古い検出は、重大なリスク VIT をターゲットとした修復に起因する可能性が高く、まだ「オープン」ステータスである可能性のある複数の重要度の低い 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、インスタンス内のアクティブな脆弱性一致アイテムと脆弱性グループの数が減少します Now Platform。

手順

1. 移動先 **すべて > 脆弱性対応 > 管理 > 自動クローズ構成**。

[自動クローズ構成] フォームが表示されます。

2. [古いアイテムの自動クローズ基準] 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。

i 注:

最後にスキャンされたデバイスは、OT スキャナーには適用されません。

[store-future: BEGIN review]このフィールドには、を所有し Microsoft Defender for IoT ているか Rapid7 インストールしているかに応じて、次のメッセージが表示されます。どちらのアプリケーションもインストールしていない場合、メッセージは表示されません。

インストールされているアプリケーション	メッセージ
Microsoft Defender for IoT	古い検出を自動クローズするには、スキャナーからの最新の「前回検出」検出情報が必要です。古い検出をクローズするには、Microsoft D4IoT デバイス CVE 統合 (フルインポート)、Rapid7 包括的脆弱性一致アイテム統合、および Rapid7 包括的脆弱性一致アイテム統合 - API が過去 7 日以内に正常に実行されていることを確認します。
Microsoft Defender for IoT および Rapid7	古い検出を自動クローズするには、スキャナーからの最新の「前回検出」検出情報が必要です。古い検出をクローズするには、Microsoft D4IoT デバイス CVE 統合 (フルインポート)、Rapid7 包括的脆弱性一致アイテム統合、および Rapid7 包括的脆弱性一致アイテム統合 - API が過去 7 日以内に正常に実行されていることを確認します。

[End]

3. 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てオンにします。

4. [日前] フィールドに、クローズする日数で古い VIT の経過時間を入力します。

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、から Microsoft Defender for IoT提供された最終検出日との照合に使用されます。[90] と [前回検出された脆弱性一致アイテム (**Vulnerable items last detected last detected**)] 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。

5. [更新] を選択します。

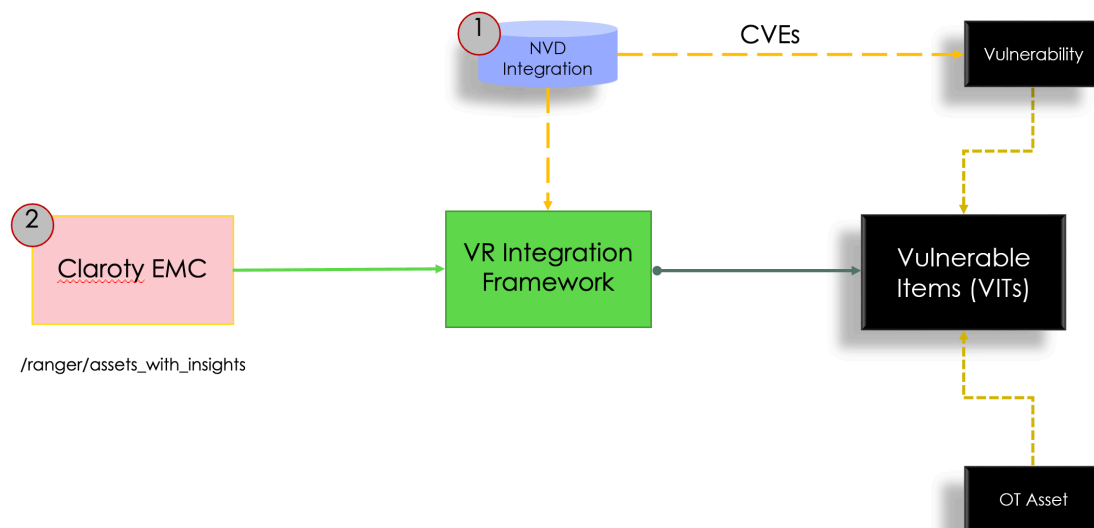
脆弱性対応 Claroty CTD との統合

脆弱性対応 Claroty Continuous Threat Detection (CTD) との統合では、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 アプリケーションと ServiceNow Operational Technology Vulnerability Response 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 Claroty CTD との統合のプロセスを示しています。

Vulnerability Response Integration with Claroty CTD のプロセス



Claroty CTD との統合を実行する脆弱性対応前に、National Vulnerability Database (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、に ServiceNow 入力します。次に、Integration with Claroty CTD アプリケーションを実行する脆弱性対応と、アプリケーションによって各デバイスの脆弱性が識別され、脆弱性一致アイテム (VI) が作成されます。

各 VI 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は、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プルします。

注:

Claroty CTD EMC Platform Insights API には 10 個の CVE の制限があります。したがって、Claroty から提供される ServiceNow 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はありません。

主な機能

- Claroty CTD から (OT) デバイスに関連付けられた Operational Technology 一般的な脆弱性とエクスポージャー (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単一のビューで確認できるようにします。
- 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します。
- 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します。

Integration with Claroty CTD のインストール脆弱性対応

脆弱性対応 Claroty CTD (sn_clarotyctdvr) との統合をインストールします。このアプリケーションには、インストール、関連 ServiceNow Store アプリケーション、およびプラグインが含まれています (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ます。詳細については、次を参照してください。 [エンタイトルメントの取得 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、の ServiceNow Store [Vulnerability Response Integration with Claroty CTD](#) アプリケーションリスト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。Integration with Claroty CTD をインストールする前に、脆弱性対応 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ます。

CMDB CI Class Models ストアアプリ

この統合では、Operational Technology [拡張クラス](#) CMDB CI Class Models アプリケーションの一部です。詳細については、「[CMDB CI Class Models store app](#)」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、Operational Technology Manager 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ているプログラムの 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。をインストールする Claroty CTD のサービスグラフコネクタ統合には、「」を参照してください [Integration with Claroty CTD のインストール脆弱性対応](#)。

必要なロール：admin

このタスクについて

Integration with Claroty CTD とともに 脆弱性対応 次のアイテムがインストールされます。

- Vulnerability Response プラグイン
- Vulnerability Response Integration with NVD

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、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。

Integration with Claroty CTD ロールのアサイン脆弱性対応

ユーザーにロールを割り当てて、Integration with the Claroty CTD アプリケーションの各機能およびデータ 脆弱性対応 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がアサインされたら、Integration with Claroty CTD アプリケーションを使用できます 脆弱性対応。

必要に応じて管理者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。

Integration with Claroty CTD アプリケーションで 脆弱性対応 利用可能なロールの詳細については、「」を参照してください [脆弱性対応 Integration with Claroty CTD ロール](#)。

手順

ユーザー管理機能を使用して、Now Platform 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 ロール

ロールは、Integration with Claroty CTD の機能 脆弱性対応 へのアクセスを制御します。

次の表では、Integration with 脆弱性対応 Claroty CTD のロールと権限について説明します。

脆弱性対応 Integration with Claroty CTD ロール

ロール	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 統合管理者 [sn_otvr.integration_admin]	OT VR 統合を構成して実行できます。
MID Server [mid_server]	を MID サーバー構成できます。

National Vulnerability Database 統合の実行

National Vulnerability Database (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、お使いの環境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、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 製品がアプリケーションと適切に統合されます Operational Technology Vulnerability Response。

NVD プラグインをインストールするには、「」を参照してください [Install the Vulnerability Response Integration with the NIST National Vulnerability Database](#)。

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 統合 - API (CVE のみ) レコードを選択します。

Vulnerability Integrations ☆					
All > Class != Application Vulnerability Integration					
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 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. [インポート開始日時] フィールドで、値を **NULL** に設定します。

4. [今すぐ実行] を選択します。

Integration with Claroty CTD の構成脆弱性対応

データのインポートを開始するには、脆弱性対応 Integration with Claroty CTD を設定します。

Claroty 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。

Claroty 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、次の場所に移動します。

Claroty CTD 脆弱性統合 > 管理者 > セットアップ。

Claroty CTD への接続

Claroty 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の地球儀アイコン () を選択して、アプリケーションスコープを **[Vulnerability Response Integration with Claroty CTD]** に変更します。

必要なロール：admin

手順

1. 移動先 すべて > **Claroty CTD** 脆弱性統合 > 管理者 > セットアップ。
2. [Claroty CTD に接続] セクションで、[接続の設定] 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 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	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、共通の脆弱性採点システム (CVSS) スコアに基づいてインポートされ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

フィールド	説明
	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、が必要になる MID サーバー 場合があります。その場合は、ここを選択します MID サーバー。

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、Results 200 出力メッセージが表示されます。接続に失敗すると、エラーコードと Claroty から受信した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、「[National Vulnerability Database 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の Claroty CTD から脆弱性をインポートします。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** > 管理者 > 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 (Activate Delta Import Integration)] タスクを選択します。
3. [設定] 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: フル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。

Service Graph Connector の後に脆弱性統合を実行

Claroty CTD 向け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。Service Graph Connector 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

コネクタの後にサービスグラフ実行する統合を実行するには脆弱性対応、を設定しClaroty CTD のサービスグラフコネクタ統合でアクティブにする必要があります。

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、「[National Vulnerability Database 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 > 管理者 > セットアップ。
2. [統合スケジュール済みジョブを構成 (Configure Integration Scheduled Jobs)] タスクで、[**Service Graph Connector** の後に実行 (**Run After Service Graph Connector**)] タブを選択します。
3. [設定] を選択します。
4. [SGC - Claroty CTD 脆弱性検出統合 - デルタインポート後に実行] 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、「[National Vulnerability Database 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

Vulnerability Response Integration with Claroty CTD では、次の 2 つのクローズ統合ジョブを使用できます。

- Claroty CTD 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、でServiceNow 構成管理データベース (CMDB)解決済みとして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 を照会し、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、でのステータス (解決済みかどうか) ServiceNow CMDBに関係なく、すべての VIT をチェックします。次に、すべての VIT について Claroty CTD 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 > 管理者 > 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. [設定] を選択します。



注:

自動クローズ統合は、デルタインポートの後に実行するように事前構成されているため、スケジュール設定は必要ありません。

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設定します。

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、「[National Vulnerability Database 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 - 完全インポート統合は、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 以降のみをインポートするように統合を設定した場合、完全インポートでは CVSS 9.0 以降のみがインポートされます。

手順

1. 移動先 **すべて > Claroty CTD 脆弱性統合 > 管理者 > 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. [設定] 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を設定します

Integration with Claroty CTD の脆弱性対応 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の地球儀アイコン () を選択して、アプリケーションスコープを [Vulnerability Response Integration with Claroty CTD] 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 > 管理者 > 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。
Integration with Claroty CTD アプリケーションに対して 脆弱性対応 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、次を参照してください [Integration with Claroty CTD のために脆弱性対応 インストールされるプロパティ](#)。
3. [更新] を選択し、変更を保存します。

Integration with Claroty CTD のために 脆弱性対応 インストールされるプロパティ

Integration with Claroty CTD アプリケーションのシステムプロパティ 脆弱性対応 を有効にすることができます。

Integration with Claroty CTD システムプロパティにアクセスする 脆弱性対応 には、次に移動します。すべて > **Claroty CTD** 脆弱性統合 > 管理者 > 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_expiry_in_minutes	Claroty CTD API トークンが有効な期間。既定値は 480 分 (8 時間) です。	整数	480
sn_clarotyctdvr.api_token_api_object	API トークンアクセスを確認します。	文字列	{"customer_name":"のサービス ","id":1,"last_r
sn_clarotyctdvr.auto_close_detection	Claroty CTD の新しい脆弱性検出を自動クローズします。	True、False	false
sn_clarotyctdvr.auto_close_detection_after_days	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 からプルするページごとのレコードの数。	整数	500
sn_clarotyctdvr.detection_delta_time	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レコードが欠落することがなくなります。	整数 buffer	4
sn_clarotyctdvr.integration_delta_time	脆弱性統合の最初の実行時に過去の日数のデータがインポートされます。	整数	90
sn_clarotyctdvr.require_cmdb	脆弱性検出を作成するには、受信 CI が一致 CMDB する必要があります。	True、False	true

Integration with Claroty CTD のデータマッピング脆弱性対応

このセクションでは、Claroty CTD API のフィールドをテーブルの ServiceNow フィールドにマッピングする方法について説明します。

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]/[修復済み] を意味します。
Resource_id	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によって設定されます。例:33.1。

脆弱性エントリーデータマッピング

脆弱性エントリーが作成されるのは、既存の共通脆弱性識別子 (CVE) レコードが脆弱性情報データベースエントリー [sn_vul_nvd_entry] テーブルにない場合のみです。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	統合により [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です。
CVSS	V3_base_score	
公開	Date_published	
変更	Last_modified	

Integration with Claroty CTD の脆弱性対応 エラー

Integration with Claroty CTD の脆弱性対応 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 統合を実行することはできません。	統合構成にユーザー名またはパスワードがありません。
REST メッセージと REST メソッドを指定せずに統合を実行することはできません。	Claroty CTD 統合ジョブレコードで、REST メッセージまたは REST メソッドフィールドが入力されません。
Claroty CTD サーバーの URL を指定せずに統合を実行することはできません。	統合構成に URL が存在しません。
検出 API リソースパスが指定されていないと統合を実行することはできません。	統合構成では、detection_api_resource_path パラメーターは入力されません。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、「無効な応答コード 401」というメッセージが Claroty CTD から受信します。この無効な応答コードは、権限がなく、資格情報 (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を受信したことを意味している可能性があります。 Claroty CTD インスタンスが MID Server を介して到達可能であることを確認し、データソース添付ファイル 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。

自動翻訳

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。	応答データをデータソースに添付できませんでした。詳細については、管理者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 Server ユーザーに sn_vul.vr_import_admin ロールがないことです。
添付ファイルのコンテンツが null です: 添付ファイル sys_id = {sys_id}。	データソース添付ファイルのコンテンツが null です。これは、Claroty API 自体の問題、または .ServiceNow 詳細については、管理者にお問い合わせください。
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。上記のエラーについても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 統合を実行することはできません。	統合構成にユーザー名またはパスワードがありません。
REST メッセージと REST メソッドを指定せずに統合を実行することはできません。	Claroty CTD 統合ジョブレコードで、REST メッセージまたは REST メソッドフィールドが入力されません。
Claroty CTD サーバーの URL を指定せずに統合を実行することはできません。	統合構成に URL が存在しません。
検出 API リソースパスが指定されていないと統合を実行することはできません。	統合構成では、detection_api_resource_path パラメーターは入力されません。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、「無効な応答コード 401」というメッセージが Claroty CTD から受信します。この無効な応答コードは、権限がなく、資格情報 (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を受信したことを意味している可能性があります。 Claroty CTD インスタンスが MID Server を介して到達可能であることを確認し、データソース添付ファイル 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。
応答本文からの「objects」アレイの解析中にエラーが発生しました。	可能性が高いということは、Claroty CTD から無効なペイロードを受信したことを意味します。Claroty CTD インスタンスが到達可能であることを確認し、送信 HTTP ログをチェックして有効な応答がある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、送信 HTTP ログをチェックして有効な応答があるかどうかを確認します。

Operational Technology Vulnerability Response 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したら、から業種別 ワークスペースアプリケーションを使用できますOperational Technology Vulnerability Response。

業種別 ワークスペース

使用する Operational Technology Vulnerability Responseには、から 業種別 ワークスペース次のランディングページとメニューにアクセスします。

の詳細については 業種別 ワークスペース、次のリンクを参照してください [Operational Technology \[デバイスのランディングページ\] タブ](#)。

[OT 脆弱性ランディングページ (OT Vulnerabilities landing page)] タブ

ランディングページの [OT 脆弱性] ランディングページタブ 業種別 ワークスペース 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サマリー。
- 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サマリー。
- 対処されていない脆弱性一致アイテム (まだアサインされておらず、オープンステータスの 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サマリーと脆弱性一致アイテムのリスト。

[OT 脆弱性] ランディングページタブの詳細については、次を参照してください [Operational Technology 脆弱性ランディングページタブ](#)。

リストメニュー

[リスト] メニューを使用して、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正タスクを表示します。

- OT 修正タスク
 - 自分のタスク
 - 自分のグループにアサイン済み
- OT 脆弱性一致アイテム
 - 自分のタスク
 - 自分の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、[却下] ステータスの例外も表示されます。

[OT 修正タスク] または [OT 脆弱性一致アイテム] リストメニューのレコードに移動して、OT 関連のコンテキストをさらに取得します。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] ウィンドウで新しいコメントや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、「」を参照してください [修復タスクの作成](#)。

for のリストビュー業種別 ワークスペースの使用の詳細については、「[IT 修復ワークスペースでのリストビューの使用](#)」を参照してください。Operational Technology Vulnerability Response

設備モデルメニュー

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

[Operational Technology Manager ワークスペースの確認](#)

[Vulnerability Response のワークスペース](#)

修復タスクの作成

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_vul.vulnerability_analyst または sn_vul.vulnerability_admin

手順

1. 移動先 すべて > **Industrial Workspace**.
2. 機器モデル ページを開きます。
3. [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、[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、[修復タスクの作成] を選択します。

The screenshot shows the ServiceNow 'Equipment model view for San Diego' page. The 'Vulnerable Items' tab is selected, displaying a table with the following data:

Number	Summary	OT asset	Manufacturer	Risk score	Risk rating	State	Remediation task
VIT0010001	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	0	5 - None	Open	
VIT0010232	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	
VIT0010235	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	
VIT0010236	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	40	3 - Medium	Open	
VIT0010237	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	20	4 - Low	Open	
VIT0010238	[Claroty] Rockwell sending a CIP connection request to an affected device and upon successful connection enables sending a new IP configuration	90.73.88.104 @ e5:ec:fe:3a:ee:2e	BizLink	80	2 - High	Open	

6. 修復タスクに必要なすべての詳細を入力します。

[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. [保存] を選択してタスク レコードを作成します。

次のタスク

修復タスクの開始時間を選択します。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。

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、(OT) 修正タスクの予定開始時間 Operational Technology を選択します。

始める前に

必要なロール： sn_vul.remediation_owner

このタスクについて

OT 修正タスクの開始時間を選択する方法は 2 つあります。

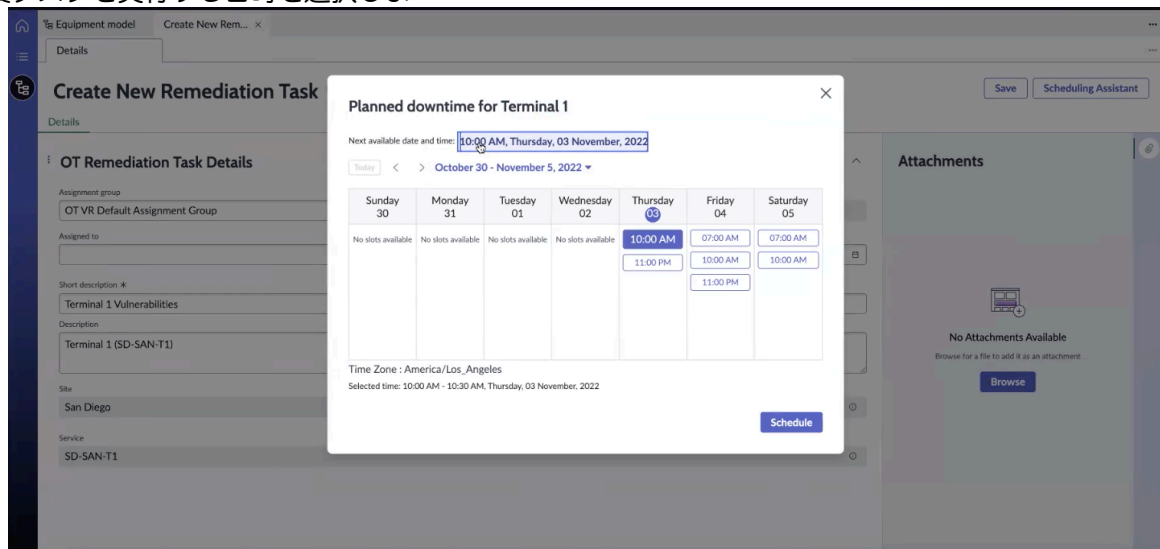
- 修復タスクの作成時に開始時間を選択するには、[新しい修復タスクを作成 (Create New Remediation Task)] フォームで [スケジュールアシスタント (**Scheduling Assistant**)] を選択します。
- 既存の修復タスクを開き、そこからスケジュールを設定できます。

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の管理](#)」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。

- ステップ 1 ～ 6 を参照 [修復タスクの作成](#) して実行します。
- [スケジュール アシスタント] を選択します。
- 修復タスクを実行する日時を選択しま



す。

- [スケジュール] 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。

- 移動先 **すべて > Industrial Workspace**.
- リストビューで、次の場所に移動します。 **OT 修正タスク > 自分のタスク**.

- 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を選択します。
- f. [スケジュール] 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

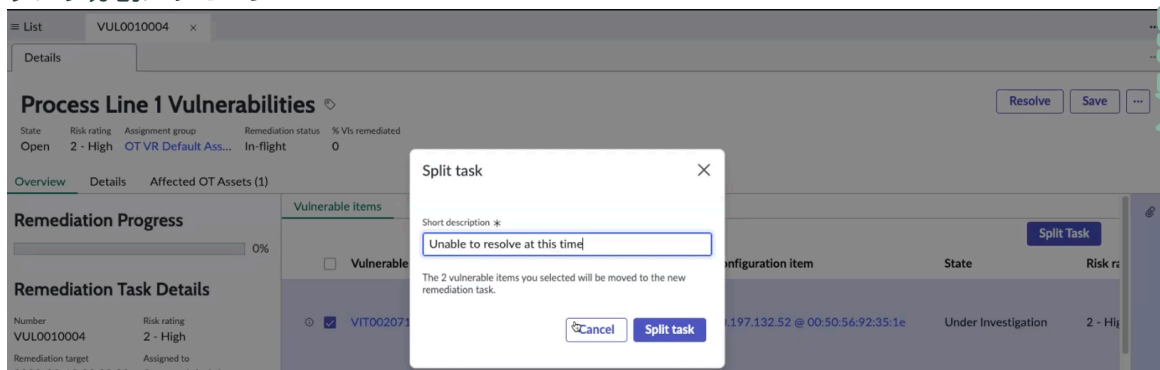
必要なロール： sn_vul.remediation_owner

手順

1. 移動先 **すべて > Industrial Workspace > OT 修正タスク > 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。

Operational Technology Vulnerability Response 参照

参照トピックには、Operational Technology Vulnerability Response 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。

Operational Technology Vulnerability Response とともにインストールされるコンポーネント

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、(com.sn_otvr) プラグインの Operational Technology Vulnerability Response アクティブ化とともにインストールされます。

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。

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	ロールを含む
OT VR 統合ビューアー [sn_otvr.integration_viewer]	統合レコードを表示できません Operational Technology Vulnerability Response。	なし
OT VR 統合管理者 [sn_otvr.integration_admin]	統合レコードを表示および編集 Operational Technology Vulnerability Response できます。	- sn_sec_cmn.admin - sn_otvr.integration_viewer - sn_vul.read_all

インストールされたビジネスルール

ビジネスルール	テーブル	説明
OT VIT を修復タスクに関連付ける	修復タスク [sn_vul_vulnerability]	OT 修正タスクが作成されると、task->Filter グループ化構成で指定されたフィルター条件に関して、関連する脆弱性一致アイテムをタスクにグループ化します。

(PA) ダッシュボードの Operational Technology Vulnerability Response インジケータソースとインジケータ

アプリケーションは Operational Technology Vulnerability Response 、インジケータソースとインジケータ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。

インジケータソース

インジケータは Operational Technology Vulnerability Response 、次のインジケータソースからデータを収集します。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、「[インジケータソースを更新してより多くのレコードを収集する](#)」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正タスクを含めます。

インジケータ

アプリケーションの脆弱性修復 Operational Technology Vulnerability Response 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。

インジケータの レコード収集 オプションは、アプリケーションでは Operational Technology Vulnerability Response 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。

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]
で、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]
で、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] 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、ユニット数値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]
で、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 の保留された重大な OT 脆弱性一致アイテムの数。[アクティブ]
で、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] で、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 修正タスク

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 修正タスクの数。[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 OT の保留されていない修正タスクの数。[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

$$(((\text{クローズされた脆弱なアイテム} > \text{修正ターゲット} = \text{ターゲット達成}) / (\text{クローズされた脆弱なアイテム})) * 100$$

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

$$[(\text{クローズされた脆弱なアイテムの所要時間合計}) / (\text{クローズされた脆弱なアイテム})]$$

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。[クローズ済み] で、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された脆弱性一致アイテムの合計期間を最小限に抑えることです。

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の数。[アクティブ] で、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。

インジケータソースを更新してより多くのレコードを収集する

インジケータソースから収集されるレコードが 100 万件を超えることが予想される場合は、インジケータソースを更新して、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、のデータ収集 業種別 ワークスペース時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 > 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 **[Application] [is] [Operational Technology Vulnerability Response]** を適用します。
3. 編集するインジケータ ソース レコードを選択します。
4. [レコードコレクション] セクションで、[レコードコレクションを上書き] 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。

Operational Technology Vulnerability Response (PA) ダッシュボードブレイクダウン

は Operational Technology Vulnerability Response ブレイクダウンを使用して、収集し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は、次のように分析されます。

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。

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

脆弱性一致構成アイテム (CI) のマネージャー。

保留の理由

脆弱性一致アイテムが修復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復予定期間。

修復ターゲットステータス

修復ターゲット日のある脆弱性一致アイテムのステータスが更新されました。

修復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満たさ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した。

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上のインジケーターに適用されます。

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.非.クローズ済み
 脆弱性一致アイテムのレポート。
 エクスプロイト攻撃ベクトル
 脆弱性一致アイテムのレポート。
 エクスプロイト有無
 脆弱性一致アイテムのレポート。
 エクスプロイトスキルレベル
 脆弱性一致アイテムのレポート。
 OT 経過時間範囲
 脆弱性一致アイテムのレポート。
 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。
 重大 度
 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のレポート。

Operational Technology Vulnerability Response (PA) ダッシュボード収集ジョブ

(PA) ダッシュボードは Operational Technology Vulnerability Response 、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、(PA) ダッシュボードに表示されるデータを収集します Operational Technology Vulnerability Response 。

[PA OT VR]脆弱性データの履歴収集

既存レコードの履歴データの収集ジョブ。

i 注:

脆弱性履歴データ収集は、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、日次データ収集ジョブは毎日スケジュールされた時刻に実行されます。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]脆弱性一致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、および重大な脆弱なアイテムについて毎日実行される収集ジョブ。

[PA OT VR]脆弱性一致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、および保留された重大な脆弱性一致アイテムについて毎日実行される収集ジョブ。

[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。

(PA) ダッシュボードで使用される **Operational Technology Vulnerability Response** データの可視化

(PA) ダッシュボードでは、Operational Technology Vulnerability Response 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、(PA) ダッシュボードに表示される Operational Technology Vulnerability Response 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	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 修正タスク	単一スコア	アクティブな (クローズされていない) OT 修正タスクの数。
修正ターゲットを満たした 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済み OT 脆弱性一致アイテムの割合。 修復ターゲットは、最後のオープン日に最後の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。
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。

[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	説明
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 修正タスクの数。 OT 修正タスクの修正ターゲット日は、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 修正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。
修復ターゲットステータス別のクローズ済み OT 脆弱性一致アイテム	棒グラフ	選択した時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	選択した時間スパンにおけるリスク評価によってグループ化されたアクティブな OT 脆弱性一致アイテムの数。

[修復] タブのデータの可視化

名前	タイプ	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 修正タスクの数。
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	リスク評価と修正ターゲットステータスごとにグループ化され

[修復] タブのデータの可視化 (続く)

名前	タイプ	説明
		たアクティブな OT 修正タスクの数。 このレポートでは、保留された OT 脆弱性一致アイテムが除外されます。
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 修正タスクの数。
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] タブデータの可視化

名前	タイプ	説明
理由別の OT 保留脆弱性一致アイテム	棒グラフ	保留の理由別にグループ化された、保留された OT 脆弱性一致アイテムの数。

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てください。

概要

拡張クラスは、Operational Technology Management.構成管理データベース (CMDB)

[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) OT の更新クラス。

関連アプリケーション

[Vulnerability Response](#)

Operational Technology Vulnerability Response 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 store app](#)

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](#)

この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、ソリューションに必要な ServiceNow 業種別 ISA-95 設備階層モデルデータ基盤を作成し、各産業サイトで独自のバージョンの設備モデルを作成できるようにします。

Operational Technology Manager

アプリケーションを使用すると Operational Technology Manager、複数のソースから OT デバイスデータを集計できるため、ソリューションで使用される業種別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 **Operational Technology Vulnerability Response**

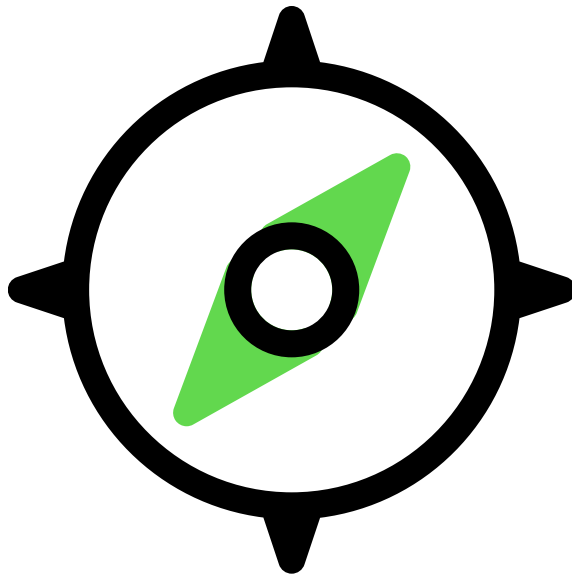
Operational Technology Vulnerability Response には、アプリケーションに関連付けられた (OT) ペルソナがあります Operational Technology。

[End]

オペレーショナルテクノロジーインシデント管理

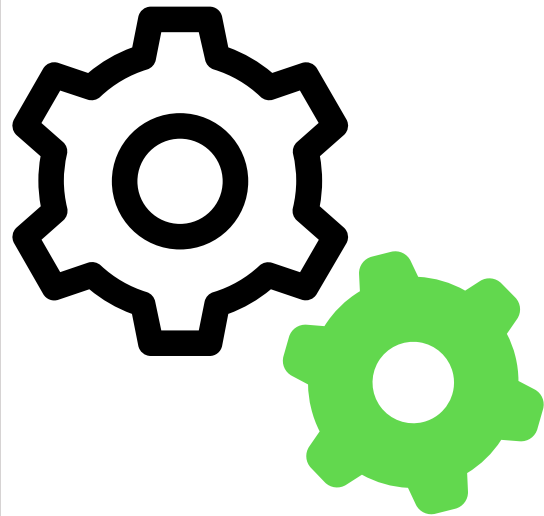
オペレーショナルテクノロジーインシデント管理を使用すると、メーカーは OT デバイスインシデントをオープンからクローズまで管理できます。

詳細を読む



オペレーショナルテクノロジー
インシデント管理の詳細

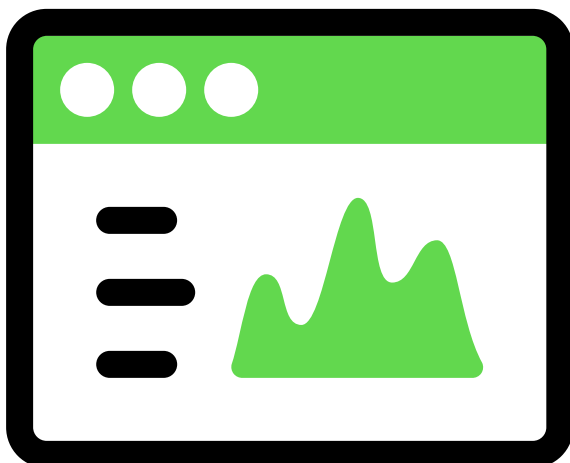
構成



実装の計画と構成

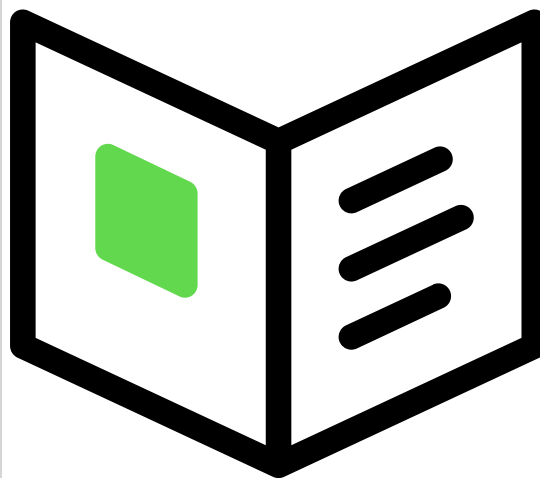
自動翻訳

使用



オペレーショナルテクノロジー
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詳細

アプリケーションの詳細 オペレーショナルテクノロジーインシデント管理 を確認します。

主な機能

を使用すると オペレーショナルテクノロジーインシデント管理、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、ワークフローを推進して、OT デバイスの影響を受ける本番プロセスを迅速に復元します。
- 生産プロセスに対する OT インシデントのコンテキストと影響を理解します。
- OT インシデントを IT インシデントとは別に監視および管理します。
- OT インシデント履行者に個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改善。
- のサポート。オペレーショナルテクノロジーのナレッジ管理詳細については、「[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。

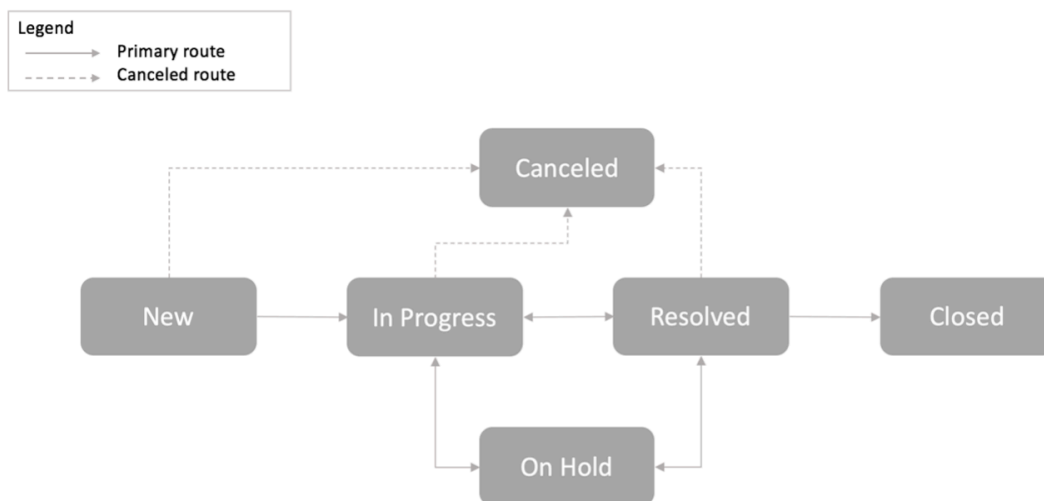
オペレーショナルテクノロジーインシデント管理

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。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。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を発生させることができます。

OT インシデントマネージャーは、作成からクローズ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 プロセスには多くのステータスがあり、それぞれ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。さまざまな状態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 プロセスのステータス



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。
対応中	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、インシデントの責任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、理由リストが表示されます。保留の理由が [問い合わせユーザー待ち] の場合は、[追加コメント] セクションが必要です。 i 注: 問い合わせユーザーがインシデントを更新した場合、[保留理由] フィールドがクリアされ、インシデントのステータスが [処理中] 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	インシデントに対して、再発を保証するための許容可能な修正が提供されます。

ステータス	説明
クローズ済み	インシデントは、特定の期間 [解決済み] ステータスを経過すると [クローズ済み] とマークされ、満足のいく解決を得られ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ジされましたが、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

と統合オペレーショナルテクノロジーインシデント管理 産業用プロセスマネージャーして、機器モデルエンティティの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、ソリューションに必要な ISA-95 設備階層モデルデータ基盤を作成します ServiceNow Operational Technology 。と オペレーショナルテクノロジーインシデント管理統合すると、本番プロセスに対するインシデントの影響を表示できます。

インストールされている 産業用プロセスマネージャー ISA 設備階層モデルプラグイン (sn_isa_model) により、指定されたロールのビューが有効になります。詳細については、「[ISA-95 機器モデル](#)」を参照してください。

OT インシデントが OT デバイスレコードから作成されると、以下が発生します。

- OT インシデントフォームの **[OT デバイス]** フィールドには、OT デバイスの値が入力されます。
- OT デバイスに機器モデルエンティティが関連付けられている場合、機器モデルエンティティが OT インシデントフォームの **[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 **[サイト]** フィールドには、OT デバイスのサイトが入力されます。

OT インシデントが機器モデルエンティティレコードから作成されると、次のようになります。

- OT インシデントフォームの **[機器モデルエンティティ]** フィールドには、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 **[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。フォームの 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

オペレーショナルテクノロジーインシデント管理ソリューションのデータ基盤を作成できるように、アプリケーションを構成しますServiceNow Operational Technology。

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アプリケーションのセットアップ オペレーショナルテクノロジーインシデント管理 を進めることができます。Guided Setup にアクセスするには、次の場所に移動します。 **Industrial Workspace** 管理者 > ガイド付きセットアップ。

タスク	目的
1. からアプリケーションをインストールし オペレーショナルテクノロジーインシデント管理 または ServiceNow Store。	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 オペレーショナルテクノロジーインシデント管理 または。
2. 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インシデント管理。	各ユーザーが使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。
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。
4. OT インシデントのカテゴリとサブカテゴリを設定します。	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設定します。
5. ステータス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 ロールをお持ちであれば、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ます。詳細については、次を参照してください。 [エンタイトルメントの取得 ServiceNow 製品またはアプリケーション](#)。
- 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 Class Models (sn_cmdb_ci_class)

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。詳細については、「[CMDB CI Class Models ストアアプリ](#)」を参照してください。

ISA 設備階層モデル (sn_isa_model)

ISA-95 設備階層モデルエンティティと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 ServiceNow Store のいずれかまたは両方のアプリケーションが必要です。をインストールする オペレーショナルテクノロジーインシデント管理前に、これらのアプリケーションの少なくとも 1 つがインストールされていることを確認します。

必要な ServiceNow Store アプリケーション

Operational Technology Manager

アプリケーションは Operational Technology Manager、企業がソリューションを使用 ServiceNow Operational Technology 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。Operational Technology Manager では、Configuration Management Database (CMDB)、Service Graph Connector、および Discovery アプリケーション Now Platformの使用がサポートされています。詳しくは、[Operational Technology Manager 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

アプリケーションは産業用プロセスマネージャー、ソリューションに必要な ServiceNow 業種別 ISA-95 設備階層モデルデータ基盤を作成し、各産業サイトで独自のバージョンの設備モデルを作成できるようにします。詳細については、「[の構成 産業用プロセスマネージャー](#)」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

注:

インストールされるロールと ACL の詳細については、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。

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. オペレーショナルテクノロジーインシデント管理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_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。

新しいインシデントテーブルへのインシデントの移行

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インシデントを移行 Operational Technology します。インシデントを移行すると、オペレーショナルテクノロジーインシデント管理古いテーブルが適用されなくなったことがアプリケーションに通知されます。

始める前に

- 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：admin

手順

1. 移動先 **Industrial Workspace** 管理者 > ガイド付きセットアップ。
2. カテゴリで オペレーショナルテクノロジーインシデント管理、[はじめに] を選択します。
3. [OT インシデントを移行] セクションの横にある [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: このジョブスケジュール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

インシデントは Operational Technology 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

アプリケーションのユーザーに オペレーショナルテクノロジーインシデント管理 ロールをアサインして、各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、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。

i 注:

OT インシデントユーザー [ot_incident_user] ロールは廃止されました。このロールがアサインされたユーザーに対して、ジョブスケジュール「新規 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 ロールをアサインできます。詳細については、「[ユーザーに新しいロールをアサインする](#)」を参照してください。

ロール	説明
OT インシデント管理者 [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。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みを表示できます。

ロール	説明
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

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

ユーザーに新しいロールをアサインする

アプリケーションのスケジュール設定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 オペレーショナルテクノロジーインシデント管理 割り当てます。

始める前に

- 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：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、[新規 **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、スケジュール設定済みジョブを開始します。
4. オプション: このジョブスケジュール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

ジョブスケジュールが実行され、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

Operational Technology OT インシデントレコードにアサインする (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 [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、インシデント (OT) と情報技術 (IT) を分離 Operational Technology 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. **[New (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。
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

インシデントを分類 Operational Technology (OT) 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、次の表に示す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

インシデントカテゴリ (続く)

カテゴリ	サブカテゴリ
	• 監視 • マウス
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	• 軽微な停止 • 実行速度の低下 • セットアップと調整 • ブレークダウン
品質	• 受信する資料 • 起動の拒否 • プロセスの欠陥 - 定性的 • プロセスの欠陥 - 定量的
安全	• ニアミス • 危険 • 安全上の懸念 • アクシデント
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 Operational Technology 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

- 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：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]** と [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. **[Save (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

インシデントを Operational Technology 分類するために使用する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

- 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：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. **[New (新規)]** を選択します。
 - b. [要素] フィールドに、「 **カテゴリ** 」という単語を入力します。
 - c. [ラベル] フィールドに、カテゴリ名を入力します。
 - d. [値] フィールドに、カテゴリ値を入力します。
 - e. [順序] フィールドに、順序番号を入力します。
 - 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. **[New (新規)]** を選択します。
 - b. [要素] フィールドに、「 **サブカテゴリ** 」という単語を入力します。
 - 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. [順序] フィールドに、順序番号を入力します。
 - f. [送信] を選択します。

タスクの結果

インシデントレコードで Operational Technology 新しいカテゴリまたはサブカテゴリを選択できます。

カテゴリまたはサブカテゴリを削除する

組織でそのカテゴリまたはサブカテゴリを使用しなくなった場合は、Operational Technology そのカテゴリまたはサブカテゴリを削除します。

始める前に

- 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：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]** と [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、インシデントレコードで Operational Technology 使用できなくなります。

インシデントステータスモデルの作成

Operational Technology サイトの (OT) インシデントステータスモデルを作成します。インシデントステータス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

- 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：admin

このタスクについて

ステータス管理を使用すると、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ステータスモデルを構成できます。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、「」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](#)。

手順

1. 移動先 すべて > 状態管理 > ステータスモデル。
2. **[OT インシデント:デフォルトのフロー]** モデルを選択します。
3. 条件を設定します。
4. [ステータス移行] コンテキストメニューで、必要に応じてステータス移行レコードを設定します。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、ステータスモデルは、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ます。

インシデントの優先度ルックアップルールを定義する

優先度を計算するための、インシデントの影響度と緊急度 Operational Technology を定義します。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 > Industrial Workspace 管理者 > Operational Technology Incident Management > 優先度ルックアップルール**。
2. **[New (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	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、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。優先度は、OT エンジニアがタスクにどれだけ迅速に対処すべきかを示します。
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を設定します

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

- 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 > Industrial Workspace 管理者 > Operational Technology Incident Management > システムのプロパティ**.
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。

アサインルールを作成

アサインルールの 1 つ以上の条件に従って (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 Operational Technology 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するには、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. **[New (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

アプリケーションに必要な オペレーショナルテクノロジーインシデント管理 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、で OT インシデント 業種別 ワークスペースを管理できます。

では、業種別 ワークスペース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

業種別 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の OT インシデントを表示できます。

- OT デバイスフォームの [OT インシデント] 関連リスト
- 機器モデルエンティティフォームの OT デバイスフォームの [OT インシデント] 関連リスト
- リストモジュールには、次のリストが表示されます。
 - 自分のタスク
 - 自分のサイトに所属
 - すべて

OT インシデント管理者は、任意の 業種別 ワークスペース 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

(OT) データと情報技術 (IT) データを分離 Operational Technology するために、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、ロールと、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
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できます。
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、および削除できます。

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

Operational Technology (OT) インシデントレコードを作成して、予想される標準的な運用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**.

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 インシデントを作成することもできます。

3. [**OT インシデント**] タブを選択します。

4. [**New (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すると、[サイト] および [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。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ています。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。

Operational Technology 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
番号	Operational Technology Incident (OTINC) がプリフィックスとして付いた、一意のシステム生成インシデント番号。
問い合わせユーザー	OT エンジニアに問題を連絡したユーザー。

フィールド	説明
影響	インシデントが産業プロセスに及ぼす影響度の測定値。
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の測定値。
ステータス	OT インシデントのステータス。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。
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	サイトの影響を受ける OT デバイス。
機器モデルエンティティ	サイトの影響を受ける機器モデル機器モデルエンティティ。
ビジネスへの影響度	OT インシデントのビジネスへの影響度に関する詳細情報。
アサイン先グループ	インシデントを担当するアサイン先グループ。アサイン先グループは、OT タイプの任意のグループにすることができます。
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、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. [Save (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ました。

インシデントを履行するタスクを作成する

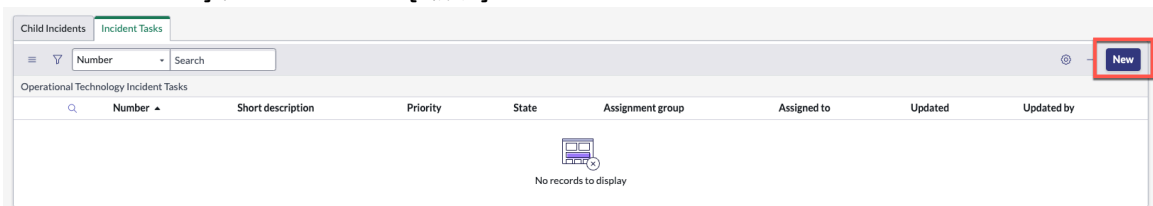
(OT) インシデントを実行する Operational Technology 一連のインシデントタスクを作成します。インシデントタスクは、インシデントの解決に必要な作業を分割して分類するのに役立ちます。

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	タスクが関連するインシデント。
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。
機器モデルエンティティ	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、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 (該当する場合)。
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ステージ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、インシデントが自動的にアサインされます。
アサイン先	担当するインシデントタスクが割り当てられているユーザー。 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。
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できます。

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の解決に必要な手順 (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るようになりました。

インシデントタスクは、次の場所のリストビューで 業種別 ワークスペース 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 Operational Technology (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

- [子インシデント機能の作成 (Create child incident feature)]
(`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を設定します](#)」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. 業種別 ワークスペース**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. **[New (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. **[Save (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内の子インシデントを表示および編集できるようになりました。

サイト全体のインシデントの可視性

Operational Technology (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。他のサイトに属するインシデントを表示して、サイトでの同様のインシデントの解決に役立てることもできます。

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になる主なメリットは、サイト全体のインシデントを読み取り専用で表示できることです。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。

i 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、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

次の OT インシデントリストは、 のリストモジュール 業種別 ワークスペースで利用できます。

- Assigned to me:次に移動して、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します。
OT インシデント > 自分のタスク。
- 自分のサイトに属している: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。
- 次に移動して、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します。 **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

(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協力して作業し、他のステークホルダーからの作業を要求することができます Operational Technology 。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。

この `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、オープンな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 OT インシデントタスク間の同期は次のように行われます。

- 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、オープンな 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

Operational Technology (OT) インシデントメール通知を使用して、インシデントに変更が加えられたときにユーザーにアラートを送信します。

通知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	送信時期	受信者	内容
コメントされたインシデント	余分なコメントが追加されたとき	アサイン先、ウォッチリスト	件名:&lt;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	[アサイン先] フィールドが空に変更され、[アクティブ] が true の場合	インシデントをオープンした担当者	件名:&lt;インシデント #> - 未アサイン 本文:このインシデントを担当する人を特定してください インシデントへの URL
クローズされたインシデント	インシデントがクローズされたとき	アサイン先グループ	件名:&lt;インシデント #> - クローズ済み 本文:解決コードと解決メモ
インシデントの優先度に変更されました	トリガーされたとき	アサイン先、アサイン先グループ、ウォッチリスト	件名:&lt;インシデント #> - 優先度に変更されました 本文: 新しい優先度: &lt;priority>
解決済みインシデント	インシデントのステータスが [解決済み] に変更されたとき	発信者、ウォッチリスト	件名:&lt;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	[アサイン先グループ] フィールドが変更された場合	アサイン先グループ、ウォッチリスト	件名:&lt;インシデント #> - &lt;アサイン先グループ> 本文:優先度、簡単な説明、説明 インシデントへの URL
自分に割り当てられたインシデント	[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:&lt;インシデント #> - あなたにアサインされました

OT インシデントメール通知 (続く)

通知の名称	送信時期	受信者	内容
			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	新しいインシデントが作成されたとき	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
インシデントステータスを変更されました	インシデントのステータスを変更されたとき	アサイン先、ウォッチリスト	件名:<インシデント #> - ステータスを変更されました 本文:簡単な説明、古い状態、新しい状態 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、インシデントについてチームや他のユーザーに最新情報を知らせます。

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**.
2. 業種別 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で、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
宛先	メールの送信先のユーザー (複数可)。

フィールド	説明
	このフィールドにより、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が自動的に入力されます。
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

メールテンプレートで指定したユーザーにメールが送信されます。

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、(OT) インシデントステータスを Operational Technology [解決済み] に設定できます。解決策に満足した場合は、インシデントをクローズできます。また、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、一定の時間が経過すると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。
解決メモ	インシデントがどのように解決されたかを示します。

4. [Update (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 Operational Technology (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から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**.
2. 業種別 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または削除されます。
6. [影響を受ける機器モデルエンティティ] 関連リストでステップ 4 と 5 を繰り返して、インシデントレコードの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、Operational Technology アサインルールの 1 つ以上の条件に従って、(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については、[テーブル] フィールドを [Operational Technology 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、アサインルールが正しく機能するようにするには、.service-now.com/cache.do">https://&lt;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。

アサインルールフォーム (続く)

フィールド	説明
	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、キャッシュのフラッシュを自動的に実行す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	イベントが割り当てられているユーザー。
グループ	イベントが割り当てられているグループ。
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てください。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た場合、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た場合、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番。アサインルールが競合する場合は、順序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を持た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

(sn_ot_inc_mgmt) プラグインを有効にする オペレーショナルテクノロジーインシデント管理 と、いくつかのタイプのコンポーネント (ユーザーロールなど) 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	ロールを含む
OT インシデント管理者 [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みを表示できます。	• 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] ロールは廃止されました。このロールを割り当てられたユーザーに対しては、スケジュール設定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、「[ユーザーに新しいロールをアサインする](#)」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 インシデントの下に作成された 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の詳細を確認してください。

概要

拡張クラスは、Operational Technology Management.構成管理データベース (CMDB)

[Operational Technology \(OT\) extension classes](#)

構成管理データベース (CMDB) OT の更新クラス。

関連アプリケーション

[IT Service Management](#)

IT Service Management アプリケーションを統合すると オペレーショナルテクノロジーインシデント管理、ServiceNow 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。

[store-future: BEGIN review]

のペルソナ オペレーショナルテクノロジーインシデント管理

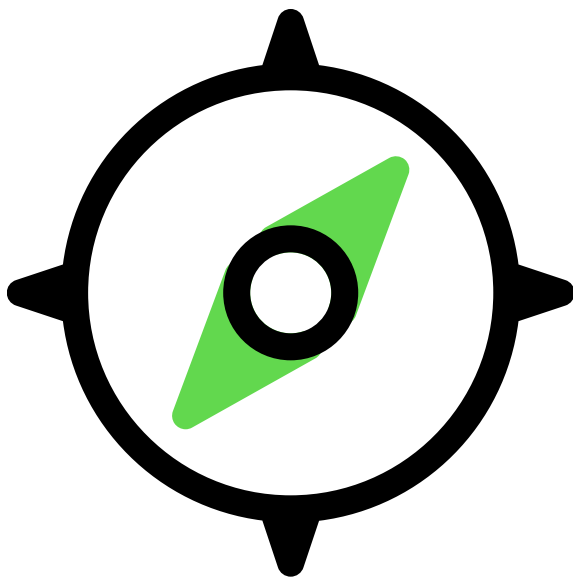
オペレーショナルテクノロジーインシデント管理 には、アプリケーションに関連付けられた (OT) ペルソナがあります Operational Technology 。

[End]

オペレーショナルテクノロジー変更管理

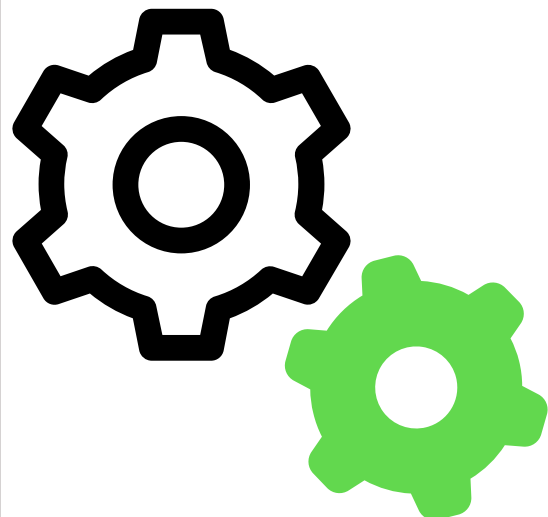
この ServiceNow オペレーショナルテクノロジー変更管理 アプリケーションを使用すると、組織は (OT) デバイスと本番プロセスに Operational Technology 変更を実装できます。

詳細を読む



オペレーショナルテクノロジー変更管理 の詳細

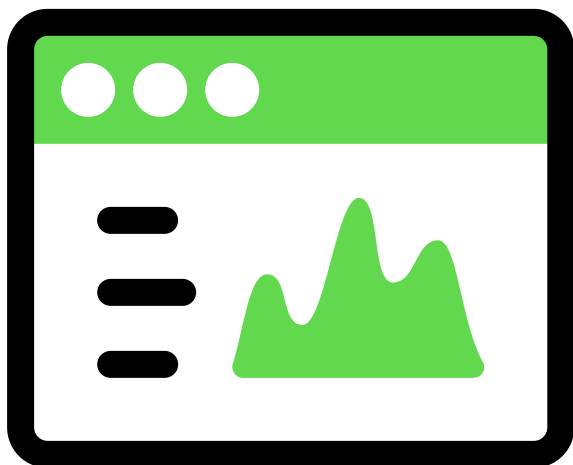
構成



実装の計画と構成

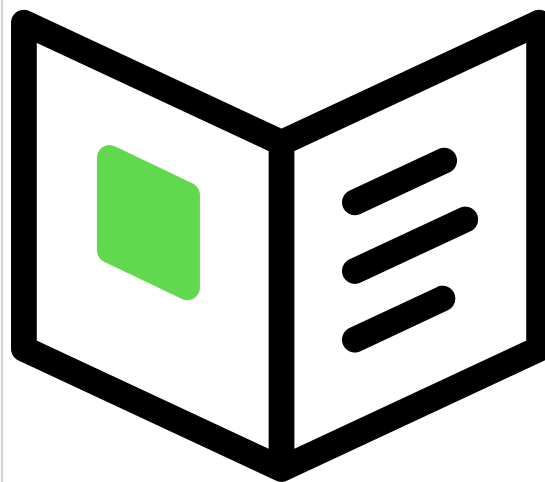
自動翻訳

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 の詳細

アプリケーションの詳細 オペレーショナルテクノロジー変更管理 を確認します。

主な機能

この 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つなぐデジタル化された変更ワークフロー。
- 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。
- およびOperational Technology Vulnerability Responseアプリケーションとオペレーショナルテクノロジーインシデント管理の統合オペレーショナルテクノロジー変更管理ワークフロー。
- 機器モデルエンティティの工場フロアの変更をダウンタイムスケジュールに合わせて調整します。

生産プロセスの最適化に使用オペレーショナルテクノロジー変更管理

この 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、運用テクノロジー (OT) デバイスや産業機器構成の変更に共同で取り組むことができます。これらの変更には、最適化、本番プロセスの変更、または脆弱性の修正が含まれます。

概要

この 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ことで、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 変更要求を IT 変更要求から分離し、サイトごとに OT 変更要求を管理できます。

次の例は、オペレーショナルテクノロジー変更管理 組織に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 修復オーナーは、脆弱性のグループを修正するための変更を開始したいと考えています。
- OT 構成とプラントエンジニアリングアクティビティを担当する OT 技術者は、産業フロアで誤動作しているロボットアームを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は、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ると発生します。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。から 業種別 ワークスペース OT 変更要求を作成すると、変更要求に **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、次を参照してください [OT デバイスの関連アイテムと関連リスト](#)。

OT 変更要求の作成方法の詳細については、次を参照してください [変更の要求の作成](#)。

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 **[なし]** の [ネットワークタイプ] 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

次の表に、基本的な OT 変更モデルと詳細な OT 変更モデルの両方のモデルステータス移行を示します オペレーショナルテクノロジー変更管理。OT 変更モデルの詳細については、次を参照してください [変更要求を実行する変更モデルを選択](#)。

基本的な OT 変更モデルのステータス

ステータス	説明
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。 • 理由 • 実装計画 • リスクと影響度の分析 • バックアウトプラン • テスト計画 • 変更をスケジュール
実装	変更はターゲットの OT デバイスで実行されます。
クローズ済み	変更が完了すると、変更レコードはクローズされます。
キャンセル	変更レコードはキャンセルされ、変更は OT デバイスに適用されません。

高度な OT 変更モデルのステータス

ステータス	説明
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。 • 理由 • 実装計画 • リスクと影響度の分析 • バックアウトプラン • テスト計画 • 変更をスケジュール
承認	レビュー担当者は OT 変更要求を承認または拒否します。
実装	変更はターゲットの OT デバイスで実行されます。
実施後のレビュー	必要に応じて OT 変更タスクを追加し、次のチェックを実行します。 • 電気チェック • ネットワークチェック • 品質チェック • 安全性チェック
クローズ済み	変更が完了すると、変更レコードはクローズされます。
キャンセル	変更レコードはキャンセルされ、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

オペレーショナルテクノロジー変更管理(OT) ソリューションのデータServiceNow Operational Technology基盤を作成できるようにアプリケーションを設定します。

admin ロールを持っている場合は、を使用してアプリケーションのセットアップオペレーショナルテクノロジー変更管理をガイドできますガイド付きセットアップ。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がカテゴリに整理されます。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。

にアクセスするには、ガイド付きセットアップに移動します。Industrial Workspace 管理者 > 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 アプリケーションのタスクとその目的 オペレーショナルテクノロジー変更管理 を示します。

タスク	目的
1. からアプリケーションをインストールし オペレーショナルテクノロジー変更管理 ます ServiceNow Store。	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 オペレーショナルテクノロジー変更管理 ます。
2. 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変更管理 。	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. カテゴリを設定します オペレーショナルテクノロジー変更管理 。	組織に必要な OT 変更のカテゴリを設定します。
4. 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 。	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 ロールをお持ちであれば、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ます。詳細については、次を参照してください。 [のエンタイトルメントの取得 ServiceNow 製品またはアプリケーション](#)。
- この 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。アプリケーションをインストールする オペレーショナルテクノロジー変更管理 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 Class Models (sn_cmdb_ci_class)

構成管理データベース (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。詳細については、「[CMDB CI Class Models ストアアプリ](#)」を参照してください。

ISA 設備階層モデル (sn_isa_model)

ISA-95 設備階層モデルエンティティと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。

- アプリケーションには オペレーショナルテクノロジー変更管理 、次 ServiceNow Store のいずれかまたは両方のアプリケーションが必要です。アプリケーションをインストールする オペレーショナルテクノロジー変更管理 前に、これらのアプリケーションの少なくとも 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

Operational Technology Manager

アプリケーションは Operational Technology Manager 、組織がソリューションを使用 Operational Technology 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。アプリケーションはOperational Technology Manager、サービスグラフ、構成管理データベース (CMDB)コネクタ、およびディスカバリーアプリケーションNow

Platformの使用をサポートしています。詳しくは、[Operational Technology Manager 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

アプリケーションは、産業用プロセスマネージャー、ソリューションに必要な ServiceNow 業種別 ISA-95 設備階層モデルデータ基盤を作成し、各産業サイトで独自のバージョンの設備モデルを作成できるようにします。詳細については、「[の構成 産業用プロセスマネージャー](#)」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

注:

インストールされるロールと ACL の詳細については、次を参照してください [オペレーショナルテクノロジー変更管理](#) とともにインストールされるコンポーネント。

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. オペレーショナルテクノロジー変更管理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。

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、アプリケーションの各機能やデータ オペレーショナルテクノロジー変更管理 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	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 変更タスクを編集および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。
読み取りユーザーの変更 [sn_ot_change_read]	OT 変更レコードの表示のみできます。

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。

変更要求を実行する変更モデルを選択

組織のニーズに応じて、Operational Technology 変更要求の実行を開始する (OT) 変更モデルを選択します。

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。

- OT 変更の基本
- OT 変更の詳細

OT 変更基本モデルは、承認なしで変更プロセスを使用します。

OT 変更基本モデルの詳細については、次を参照してください [基本的な OT 変更モデル Playbook](#)。

OT 変更詳細モデルでは、承認を伴う変更プロセスを使用します。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できます。変更承認の詳細については、次を参照してください [Operational Technology 変更承認](#)。

高度な OT 変更モデルの詳細については、次を参照してください [高度な OT 変更モデル Playbook](#)。

手順

1. 移動先 **Industrial Workspace** 管理者 > ガイド付きセットアップ。
2. [Operational Technology Change Management] カテゴリで、[**Get Started**] 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 Playbook

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) 変更モデルの Playbook 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

フィールド	説明
簡単な説明	変更の簡単な説明
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

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	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

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。アサイン先グループは、OT タイプの任意のグループにすることができます。
アサイン先	この変更を実行するユーザー。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

フィールド	説明
理由	変更を行う必要がある理由。

実施計画を追加

フィールド	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

フィールド	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要因の詳細。

切り戻し計画を追加

フィールド	説明
切り戻し計画	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

フィールド	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。

変更をスケジュール

フィールド	説明
開始予定日	変更が行われる日付。 i 注: [スケジュール アシスタント] ボタンを選択して [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	変更が終了する日付。

変更をスケジュール (続く)

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 [終了予定日] フィールドに自動的に入力することで、カレンダーで使用可能なダウタイム 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。完了したら、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、完了したら、完了としてマークします。

閉じる

[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

フィールド	説明
終了コード	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 Playbook

承認のある OT 変更が完了するまでに通過する必要がある、高度なオペレーショナルテクノロジー (OT) 変更モデル Playbook 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

フィールド	説明
簡単な説明	変更の簡単な説明
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。

変更の説明 (続く)

フィールド	説明
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

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	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

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。アサイン先グループは、OT タイプの任意のグループにすることができます。
アサイン先	この変更を実行するユーザー。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、リスクと影響度の計画、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

フィールド	説明
理由	変更を行う必要がある理由。

実施計画を追加

フィールド	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

フィールド	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要因の詳細。

切り戻し計画を追加

フィールド	説明
切り戻し計画	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

フィールド	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。

変更をスケジュール

フィールド	説明
開始予定日	変更が行われる日付。 i 注: [スケジュール アシスタント] ボタンを選択して [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スロットを選択することもできます。
終了予定日	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、カレンダーで使用可能なダウン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。このステージには 1 つのタスクのみが含まれます。

レビューとアクションの実行

フィールド	説明
[承認] ボタン	タスク フォームの表に表示されている校閲者の場合は、[承認] を選択して変更を受け入れます。
[拒否] ボタン	タスク フォームの表に表示されている校閲者の場合は、[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、次を参照してください [Operational Technology 変更承認](#)。

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。完了したら、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 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、完了したら、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りの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

フィールド	説明
電気チェックを実行	電気チェックが完了した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	品質チェックが完了した後に選択するチェックボックス。
安全チェックを実行	安全チェックが完了した後に選択するチェックボックス。

スピノフタスクを推奨

フィールド	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。
アサイン先	この変更を実行するユーザー。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、確認された後、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、完了する必要がある、実施後のレビューのすべての変更タスクが一覧表示されます。

閉じる

[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

フィールド	説明
終了コード	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

アプリケーションに必要な オペレーショナルテクノロジー変更管理 すべてのセットアップタスクを完了したら、(OT) 変更要求の管理 Operational Technology を開始できます。

変更の要求の作成

Operational Technology サイトの変更をレポートする (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**.
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. **[New (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. **[OT 変更レコードを作成]** を選択します。
6. チームが変更要求に取り組むときに、必要に応じて Playbook を完成させます。
基本的な OT 変更モデル Playbook の詳細については、次を参照してください [基本的な OT 変更モデル Playbook](#)。Advanced OT Change Model Playbook の詳細については、次を参照してください [高度な OT 変更モデル Playbook](#)。

変更要求を履行するための変更タスクの作成

(OT) 変更要求を履行 Operational Technology する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**.
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
OT 変更タスク	
簡単な説明	変更タスクの簡単な説明。
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白のままにすると、変更タスクが自動的にアサインされます。
アサイン先	担当する変更タスクが割り当てられているユーザー。 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。
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. **[Save (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、次の場所のリスト ビューで 業種別 ワークスペース 表示できます。

- 自分にアサインされたタスクを変更: **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を変更: **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

Operational Technology OT デバイスレコードから (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と [OT デバイス] フィールドなどの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.**
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. レコードで、[OT 変更要求] 関連リストを選択します。
4. **[New (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. **[OT 変更レコードを作成]** を選択します。
7. チームが変更要求に取り組むときに、必要に応じて Playbook を完成させます。

基本的な OT 変更モデル Playbook の詳細については、次を参照してください [基本的な OT 変更モデル Playbook](#)。Advanced OT Change Model Playbook の詳細については、次を参照してください [高度な OT 変更モデル Playbook](#)。

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、アプリケーションが有効になっている 産業用プロセスマネージャー 場合にのみ自動入力されます。
- がインストールされ 産業用プロセスマネージャー 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。
- 有効になっ 産業用プロセスマネージャー ている、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、[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、 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

Operational Technology OT 修正タスクから (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、変更要求レコードに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**.
2. 変更要求の作成元であ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

す。

The screenshot displays the 'California Vulnerabilities' record in ServiceNow. The top navigation bar shows 'List' and 'VUL0010004'. The record details include 'State: Open', 'Risk rating: 3 - Medium', 'Assignment group: OT VR Default Ass...', 'Remediation status: In-flight', and '% VIs remediated: 0'. The 'Overview' tab is active, showing 'Affected OT Assets (1)'. The 'Remediation Progress' bar is at 0%. The 'Remediation Task Details' section shows the task number VUL0010004, risk rating 3 - Medium, and various dates. The 'Vulnerable Items' table has one row with item VIT0010002, a summary of a remote code execution vulnerability, configuration item PLC001, and state Open with a 3 - Medium risk rating. The 'Attachments' section on the right shows 'No Attachments Available' with a 'Browse' button.

- 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

す。

Error creating Change Request: No active change model available. Please contact your OT Change admin

4. 組織に適用する OT 変更モデルを選択します。
5. [次へ] を選択します。
6. チームが変更要求に取り組むときに、必要に応じて Playbook を完成させます。

基本的な OT 変更モデル Playbook の詳細については、次を参照してください [基本的な OT 変更モデル Playbook](#)。Advanced OT Change Model Playbook の詳細については、次を参照してください [高度な OT 変更モデル Playbook](#)。

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、アプリケーションが有効になっている 産業用プロセスマネージャー 場合にのみ自動入力されます。
- がインストールされ 産業用プロセスマネージャー 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。
- 有効になっ 産業用プロセスマネージャー ている場合、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、[**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、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

Operational Technology OT インシデントレコードから (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、データがインシデントレコードからの新しい変更要求に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.**
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 変更要求の作成元になるインシデントレコードを選択します。
4. [**OT 変更を作成**] ボタンを選択します。
[OT 変更を選択] 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変更モデルを選択](#)」を参照してください。
6. [**OT 変更レコードを作成**] を選択します。
7. 必要に応じて Playbook と関連フォームに入力します。
Playbook 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以下を参照してください。[基本的な OT 変更モデル](#) [Playbook](#)[高度な OT 変更モデル](#) [Playbook](#)。

i 注:

新しい変更要求の [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
- 機器モデルエンティティ
- OT デバイス (CI)
- 簡単な説明
- 説明
- 優先度

i 注:

1 ~ 4 の [優先度] フィールド値は、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 [優先度] フィールドの値 5 は、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 Operational Technology (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_change_write または sn_ot_change_admin

手順

1. 移動先 **すべて > Industrial Workspace.**
2. 業種別 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または削除されます。
6. ステップ 4 と 5 を繰り返しますが、[影響を受ける機器モデルエンティティ] 関連リストで、変更レコードに対して機器モデルエンティティを追加または削除します。

Operational Technology 変更承認

(OT) 変更承認により Operational Technology、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

詳細な 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レビューし、必要に応じて要求を編集して、変更要求を承認できます。

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 変更モデルに適用される変更承認ポリシーはありません。

変更承認要件

要件	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割り当てられたメンバー。
必要なロール	承認者にはsn_ot_change_readロールが必要です。
承認率	変更を進めるには、承認グループの 51% がその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、次を参照してください [Create change approval policies](#) .

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、(Operational Technology 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. [グループ] リストから、[**OT 変更のデフォルト承認者 (OT Change Default Approvers)**] 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. [Save (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した。

サイト全体の変更要求の管理

この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 オペレーショナルテクノロジー 変更管理 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た (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 Operational Technology 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。サイト間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:

他のサイトの OT 変更要求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変更要求のみです。

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として、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を示しています。

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

次の OT 変更要求リストは、 のリストモジュール 業種別 ワークスペースで利用できます。

- 自分にアサイン済み:次に移動して、アサインされた変更レコードを表示および編集します。 **OT** 変更要求 > 自分のタスク。
- 自分のサイトに属している: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、 **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。

サイト間での変更モデルレコードの可視性

(Operational Technology OT) 変更ロールとサイトロールに応じて、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。

変更モデルレコードに対する **OT** 変更ロールと可視性

次の表では、さまざまな OT 変更ユーザーが変更モデルレコードにアクセスするためのロールと権限について説明します。

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。
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、および削除します。 - 任意のサイトに変更モデルをアサインします。 - すべて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、および削除します。 - 任意のサイトに変更モデルをアサインします。 - すべて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	どのサイトについても変更モデルを表示または編集することはできません。どのサイトにも関連付けられていないベースシステムの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。

メール通知の変更

メール通知を使用して、(OT) 変更要求または変更タスクが更新されたときに Operational Technology ユーザーに警告します。

OT 変更要求と変更タスクの通知を次の表に一覧表示します。

OT 変更要求のメール通知

名前	送信時期	受信者	内容
自分にアサインされた変更	[担当者] 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: &lt;変更要求 #>通知 Body (本文): 簡単な説明:&lt;簡単な説明> ここをクリックして変更要求を表示:&lt;変更要求の URL> サイト: &lt;サイト名> OT デバイス: &lt;OT デバイス> 機器モデルエンティティ:&lt;機器モデルエンティティ> 説明: &lt;説明>
自分のグループにアサインされた変更	[アサイン先グループ] 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:&lt;変更要求 #>がグループ &lt;アサイン先グループ>にアサインされました Body (本文): 簡単な説明:&lt;簡単な説明> ここをクリックして変更要求を表示:&lt;変更要求の URL> サイト: &lt;サイト名> OT デバイス: &lt;OT デバイス> 機器モデルエンティティ:&lt;機器モデルエンティティ> 説明:&lt;description>

OT 変更要求のメール通知 (続く)

名前	送信時期	受信者	内容
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 (本文): 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>
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 • 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 (本文): 簡単な説明:<簡単な説明> 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> 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	• 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 (本文): 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	• 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 (本文): 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	送信時期	受信者	内容
			&lt;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: &lt;説明>
保留中の変更	変更要求が保留になっているとき	要求者	件名:&lt;変更要求 #> が保留されました Body (本文): こんにちは &lt;変更要求を作成したユーザー>、 要求した &lt;変更要求 #> は保留中になりました。要求が保留されている理由は、&lt;変更要求が保留されている理由>です。 変更要求を表示するには、ここをクリックしてください: &lt;変更要求の URL>
保留解除の変更	変更要求が保留にされたとき	要求者	件名:&lt;変更要求 #> が保留になりました Body (本文): こんにちは &lt;変更要求を作成したユーザー>、 要求した &lt;変更要求 #> は保留になり、[&lt;更新済みステータス フィールド> 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: &lt;変更要求の URL>

OT 変更タスクのメール通知

名前	送信時期	受信者	内容
自分にアサインされたタスクの変更	[担当者] フィールドが変更され、空でない場合	変更タスクがアサインされている人物	件名:&lt;変更タスク #>通知 -- &lt;簡単な説明> Body (本文): 簡単な説明:&lt;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:&lt;変更タスクの URL> サイト: &lt;サイト名> OT デバイス: &lt;OT デバイス> 機器モデルエンティティ:&lt;機器モデルエンティティ> 説明: &lt;説明>
自分のグループにアサインされたタスクの変更	[アサイン先グループ] 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: &lt;変更タスク #>通知 -- &lt;簡単な説明> Body (本文): 簡単な説明:&lt;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:&lt;変更タスクの URL> サイト: &lt;サイト名> OT デバイス: &lt;OT デバイス> 機器モデルエンティティ:&lt;機器モデルエンティティ> 説明: &lt;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 - アサイン先 - アサイン先グループ	件名:&lt;変更タスク #>作業メモが追加されました -- &lt;簡単な説明> Body (本文):

OT 変更タスクのメール通知 (続く)

名前	送信時期	受信者	内容
			簡単な説明:&lt;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:&lt;変更タスクの URL> 作業メモ:&lt;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

(OT) 変更要求を Operational Technology 分類することで、特定の OT 変更要求の検索をグループ化して絞り込むことができます。カテゴリは、利害関係者が変更の内容を知るのにも役立ちます。

OT 変更要求を作成できる場合、次の表に記載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	説明
ハードウェア	OT デバイスを追加、削除、または構成するための変更。
ソフトウェア	OT ソフトウェアを追加、削除、または構成するための変更。
サービス	OT サービスの変更。
システムソフトウェア	OT システムソフトウェアの変更。
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の変更。
ネットワーク	サブネット、IP アドレス、MAC アドレスの変更。
電気通信	OT システムで使用されるテレコミュニケーションの変更。
ドキュメント	OT ドキュメントの変更。
ファームウェア	OT ファームウェアの変更。
その他	上記のカテゴリで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

(sn_ot_chg_mgmt) アプリケーションのアクティブ化 オペレーショナルテクノロジー変更管理 とともに、いくつかのタイプのコンポーネント (ユーザーロールを含む) をインストールできます。

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。

インストールされるロール

ロール	説明	ロールを含む
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 変更タスクを編集および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。	- cmdb_ot_viewer - cmdb_ot_isa_viewer - sn_ot_change_read
読み取りユーザーの変更 [sn_ot_change_read]	OT 変更レコードの表示のみできます。	- 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の詳細を確認してください。

概要

拡張クラスは、Operational Technology Management.構成管理データベース (CMDB)

[Operational Technology \(OT\) extension classes](#)

構成管理データベース (CMDB) OT の更新クラス。

関連アプリケーション

[IT Service Management](#)

IT Service Management アプリケーションを統合すると オペレーショナルテクノロジー変更管理、ServiceNow 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。

[store-future: BEGIN review]

オペレーショナルテクノロジー変更管理 のペルソナ

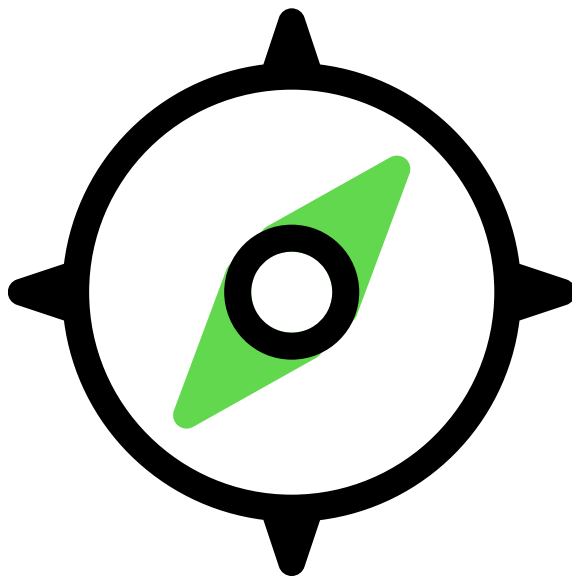
オペレーショナルテクノロジー変更管理 には、アプリケーションに関連付けられた (OT) ペルソナがあります Operational Technology 。

[End]

オペレーショナルテクノロジーのナレッジ管理

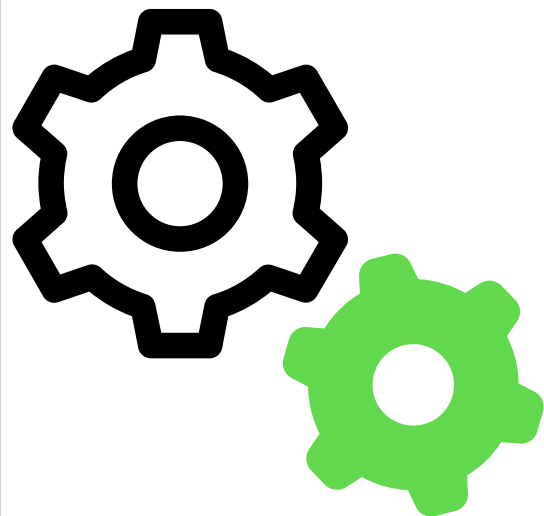
ServiceNow[®] オペレーショナルテクノロジーのナレッジ管理 は、(OT) システム、そのデバイス、および組織内の解決済みインシデントに関する Operational Technology ナレッジの収集、整理、共有に役立ちます。

詳細を読む



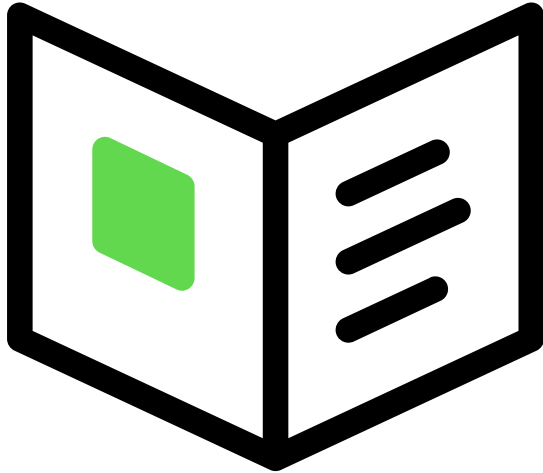
オペレーショナルテクノロジーのナレッジ管理 の詳細

構成



実装の計画と構成

自動翻訳

使用	参照
 オペレーショナルテクノロジーのナレッジ管理の使用	 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のナレッジ管理の詳細

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 (OT) システムに関する情報 Operational Technology 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のに役立ちます。

オペレーショナルテクノロジーのナレッジ管理のメリット

を使用すると オペレーショナルテクノロジーのナレッジ管理、次の主要な機能を使用できます。

- ソリューションでOperational Technology Management既存のナレッジ管理 Now Platform の機能ものを使用する機能。
- 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ナレッジ記事を直接作成する機能。
- ナレッジマネージャーとナレッジユーザー用の OT ナレッジベースを構成する機能。
- でナレッジ記事を作成する機能。業種別 ワークスペース
- ナレッジ記事を公開、編集、廃止、または削除するための承認を要求する機能。
- 更新された情報を使用して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

(OT) ソリューションのデータOperational Technology基盤を作成できるように構成オペレーショナルテクノロジーのナレッジ管理します。

admin ロールを持っている場合は、を使用してセットアップオペレーショナルテクノロジーのナレッジ管理を進めることができます。ガイド付きセットアップは、ガイド付きセットアップ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がカテゴリに整理されます。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ステップ、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。

アクセス ガイド付きセットアップするには、 に移動します **Industrial Workspace** 管理者 > 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 の オペレーショナルテクノロジーのナレッジ管理タスクとその目的を示します。

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。アプリケーション (バージョン 2.0.2) がインストールされ、構成されているオペレーショナルテクノロジーのナレッジ管理限りオペレーショナルテクノロジーインシデント管理、構成できます。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常に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
にロールをアサイン ナレッジ管理 します 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、アクセスを構成します。
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 ナレッジベースを読んだり寄稿したり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 ナレッジベースに割り当てて、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構成します。	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 glide.knowman.block_access_with_no_user_criteria プロパティ設定に基づいています。
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。
ナレッジ管理で使用するオペレーショナルテクノロジーのナレッジ管理プロパティを確認します。	OT ナレッジベースの外観と機能を適用可能なナレッジ管理 プロパティで構成します。

ユーザーへのロールの オペレーショナルテクノロジーのナレッジ管理 アサイン

ユーザーにロールをアサイン ナレッジ管理 して、各機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 オペレーショナルテクノロジーのナレッジ管理。

始める前に

必要なロール : admin

このタスクについて

ロールがアサイン ナレッジ管理 されている場合は、その機能を使用できます オペレーショナルテクノロジーのナレッジ管理。

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。

に適用可能なオペレーショナルテクノロジーのナレッジ管理ロールの詳細についてはナレッジ管理、次のリンク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 ロール](#)。

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 ナレッジベースの作成

Operational Technology (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. **[New (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記入します。
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むことができ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	ナレッジ管理詳細 (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。

名前	説明
	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。 [記事テンプレート] 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: 管理者、ナレッジ管理者、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。 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の作成

ユーザー基準レコードを作成して、(OT) ナレッジベースを読んだ Operational Technology り寄稿したり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

の ナレッジ管理 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決定します。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割り当て、その記事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. **[New (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。 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、ロ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、昇格された特権ロ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構築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。

フィールド	説明
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。選択すると、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、満たされた条件があれば一致するようにこのチェックボックスはオフになっています。 たとえば、次の条件のユーザー基準レコードを考えます。 - 場所 A または B - 会社 C または D [すべて一致] を選択すると、これら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一致します。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 ナレッジベースに割り当てることができます。詳細については、「[OT ナレッジベースにユーザー基準をアサインする](#)」を参照してください。

OT ナレッジベースにユーザー基準をアサインする

ユーザー基準レコードを (OT) ナレッジベースに Operational Technology 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、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 ナレッジベースに割り当てて、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. OT ナレッジベースにユーザー基準を追加します。
 - 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。

関連リスト	説明
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、[保存] を選択して、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

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、Operational Technology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。

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、次のリンクを参照してください [OT ナレッジベースのユーザー基準の作成](#)。ユーザー基準の割り当ての詳細については、「」を参照してください [OT ナレッジベースにユーザー基準をアサインする](#)。
4. オプション: プロパティ設定を使用して、ナレッジベースの非認証ユーザーを制限します `glide.knowman.block_access_with_no_user_criteria`。
 - 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. プロパティ設定を `glide.knowman.block_access_with_no_user_criteria true` に設定します。
 - c. [Save (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ために、各 Operational Technology (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

次の表のデフォルトの ナレッジ管理 ワークフローを OT ナレッジベースに オペレーショナルテクノロジーのナレッジ管理 使用して適用できます。

i 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 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。承認中の記事のステータスは [レビュー中] で、承認後に [公開済み] ステータスに移行します。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ために、記事の作成者または改訂者にも通知が送信されます。 承認メール通知をオンにするには、このプロパティを <code>glide.knowman.enable_approval_notificationtrue</code> に設定します。 i 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 [公開] ステータスのままになります。

デフォルト ナレッジ管理 ワークフロー (続く)

ワークフロー	説明
	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。
ナレッジ - ナレッジの公開	ナレッジ記事を [公開] 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するときに、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するときに、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。

- 承認を受ける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。このリリース以降 New York、このプロパティはデフォルトで有効になっています。リリースより前の New York 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。プロパティが *glide.knowman.enable_approval_notification* 利用できない場合、管理者はプロパティを作成し、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。

ナレッジベースのプロパティ **Operational Technology** の確認ナレッジ管理

管理者は、プロパティを使用して ナレッジ管理 (OT) ナレッジベースの外観と機能 **Operational Technology** を設定できます。

プロパティにアクセスする ナレッジ管理 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ルールを制御します。

Glide.knowman.show_flag.roles プロパティ

プロパティ	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) (glide.knowman.show_flag.roles)	に表示される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、次を参照してください [Knowledge Management properties](#)。

オペレーショナルテクノロジーのナレッジ管理の使用

に必要な オペレーショナルテクノロジーのナレッジ管理すべてのセットアップタスクを完了すると、(OT) インシデントに関連する Operational Technology 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と、チームのニーズに応じてナレッジ記事を作成、編集、廃止できます。このアプリケーションで使用する オペレーショナルテクノロジーインシデント管理 と、インシデントに関連する記事を参照し、インシデントから記事を作成できます。

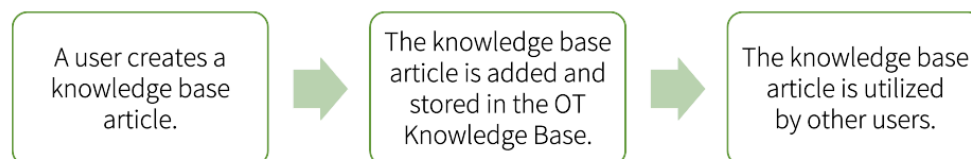
次の例は、チームに適用する オペレーショナルテクノロジーのナレッジ管理 方法を示しています。

- 数年の経験を持つ OT エンジニアは、ガイドワーカーや経験の浅い技術者のために、OT デバイスの知識を 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労働者と技術者は、工場のフロアで問題に気付く、修正を説明するナレッジ記事を必要としています。

[store-future: BEGIN review]

基本 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

ここでは ワークフロー、の オペレーショナルテクノロジーのナレッジ管理基本的な処理について説明しま



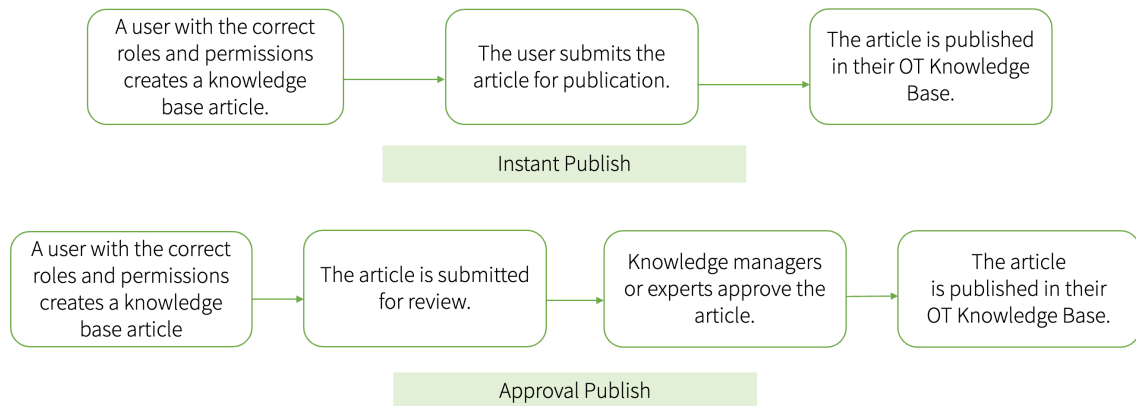
す。

[End]

[store-future: BEGIN review]

ナレッジ記事の公開

次に ワークフロー、ナレッジ記事を作成して公開する方法 (公開承認) と承認なし (すぐに公開) の両方について説明しま



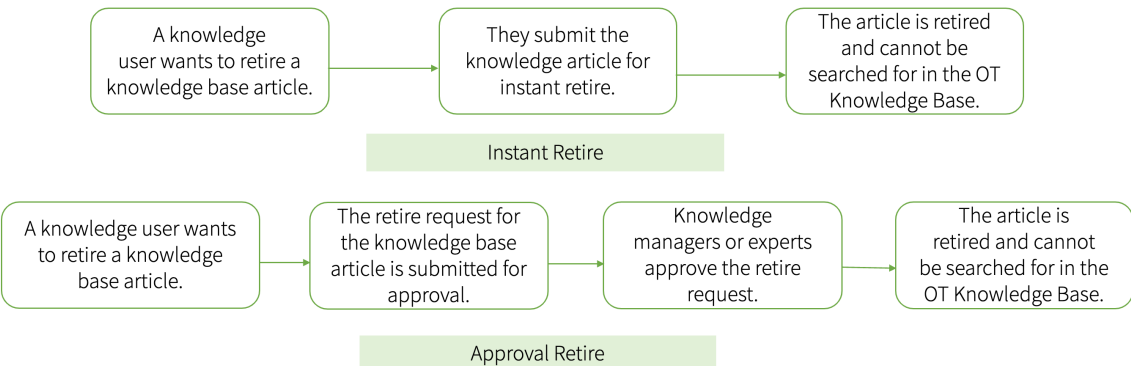
す。

[End]

[store-future: BEGIN review]

ナレッジ記事の廃止

以下 ワークフロー では、(廃止を承認) 承認がある場合と承認しない場合 (すぐに廃止) の両方でナレッジ記事を廃止する方法について説明します。すぐに廃止ワークフローを使用すると、承認を必要とせずに記事をすぐに廃止できます。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



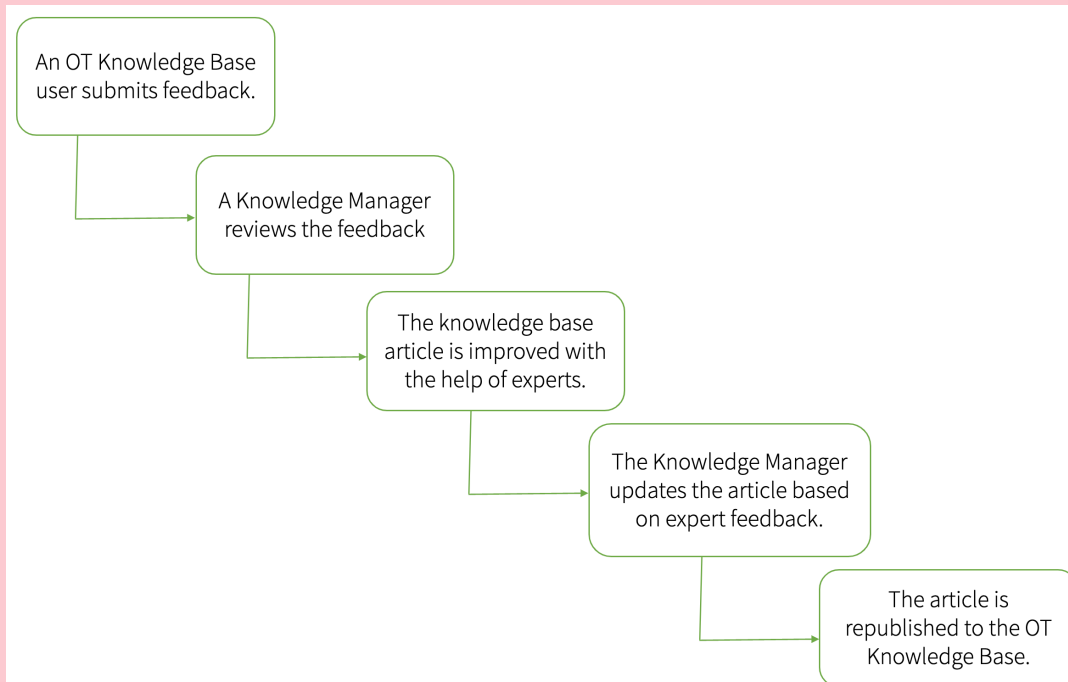
す。

[End]

[store-future: BEGIN review]

ナレッジ記事への変更のレビューおよび承認

既存の ワークフロー ナレッジ記事をユーザーからのフィードバックで更新する方法について説明します。



す。

[End]

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、次のケースについて、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。
- さまざまな生産資料に注釈を付ける画像。

ナレッジ記事は、次の方法で 業種別 ワークスペース 表示できます。

- リストビューの 業種別 ワークスペース ナレッジモジュールの下。
- OT インシデントを開くときの [エージェント支援] ウィンドウ。
- ヘッダーでグローバル検索機能を使用する。業種別 ワークスペース

リストビューのナレッジモジュール 業種別 ワークスペース では、次のリストのナレッジ記事を表示できます。

- i 注:**
 で 業種別 ワークスペースこれらのリストモジュールを表示するには、knowledge 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

OT ナレッジベースでまだ公開されていない、作成した記事。

公開済みの記事

OT ナレッジベースに公開される、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のナレッジ記事の作成

ナレッジ記事を作成して、(OT) インシデントとその解決に関連する Operational Technology 情報を記録および保存します。

始める前に

必要なロール:sn_ot_incident_write

注:

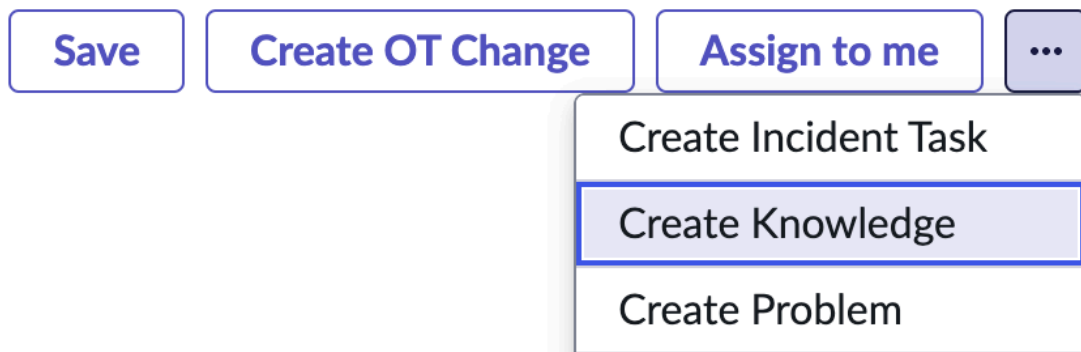
少なくとも 1 つのナレッジベースに対する 寄稿可能 アクセス権も必要です。詳細については、「[OT ナレッジベースの作成](#)」を参照してください。

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、コンテキスト情報を得るためにナレッジ記事が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含まれている場合に、チームが今後同様のインシデントを解決するのに役立ちます。

手順

1. 移動先 **すべて** > **Industrial Workspace**.
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] ボタン ... 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。

注:

[**Create Knowledge**] 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 [**Resolved**] 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

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。

フィールド	説明
	注: OT ナレッジベースの可視性を適切に設定した場合、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、およびソリューションを説明するナレッジ記事のコンテンツ。
有効期限	ナレッジ記事の有効期限。

7. [Save (保存)] を選択します。

ナレッジ記事が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 ナレッジベースに公開されました。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 [公開ワークフロー] フィールドを [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 業種別 ワークスペース

で 業種別 ワークスペース ナレッジ記事を作成して、(OT) インシデントに直接関連 Operational Technology しないニーズとソリューションに記事のコンテンツに対応します。

始める前に

必要なロール : knowledge

i 注:

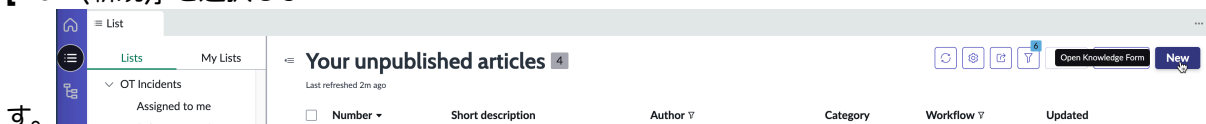
少なくとも 1 つのナレッジベースに対する 寄稿可能 アクセス権も必要です。詳細については、「[OT ナレッジベースの作成](#)」を参照してください。

手順

1. 移動先 **すべて > Industrial Workspace.**

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. [New (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

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性を適切に設定した場合、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、およびソリューションを説明するナレッジ記事のコンテンツ。
有効期限	ナレッジ記事の有効期限。

5. [Save (保存)] を選択します。

ナレッジ記事が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 ナレッジベースに公開されました。

i 注:

OT ナレッジベースの [公開ワークフロー] フィールドを [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のナレッジギャップの報告

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、Operational Technology (OT) インシデントからナレッジギャップを報告します。

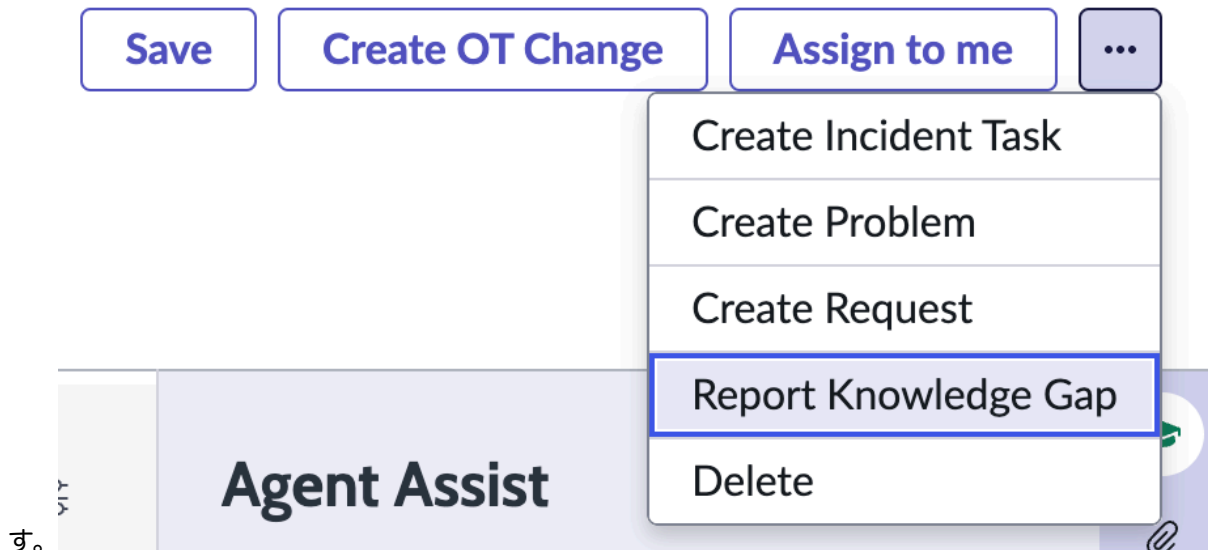
始める前に

必要なロール:sn_ot_incident_read

手順

1. 移動先 **すべて > Industrial Workspace.**
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] ボタン ... 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。

i 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方法については、「」を参照してください [フィードバックタスクの割り当て](#)。

ナレッジ記事の公開または廃止要求の承認

ナレッジ記事を公開または廃止する要求を承認して、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の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、記事の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割り当て

フィードバックタスクをユーザーに割り当てて、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ていることを確認します。

始める前に

必要なロール:knowledge_manager

手順

1. 移動先 **すべて > Industrial Workspace.**
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割り当てるフィードバックタスクを選択します。
4. [担当者] フィールドで、フィードバックタスクを割り当てるユーザーを追加します。
5. [Save (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した。

アサインされた他のフィードバックタスクを表示するには、の 業種別 ワークスペース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、の 業種別 ワークスペース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 インシデントに関連するナレッジ記事で情報を検索する

適用可能な以前の解決策の (OT) インシデントレコードに Operational Technology 添付されている関連ナレッジ記事の情報を検索します。

始める前に

必要なロール:sn_ot_incident_read

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.**
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、[エージェント支援] ボタン [] をクリックして、[エージェント支援] 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 []
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、[エージェント支援] 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、[エージェント支援] 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ったとマークするには、[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

ユーザーに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アサインナレッジ管理できます。

次の表に ナレッジ管理、ユーザーが機能にアクセスできる オペレーショナルテクノロジーのナレッジ管理 ようにアサインできるロールを示します。

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	knowledge ロールは、デフォルトのナレッジベースに寄稿することができ、また、ナレッジアプリケーション メニューにアクセスすることができます。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できません。
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、管理してい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	ナレッジ管理者は、システムの保守 ナレッジ管理 に関連するすべての管理タスクを実行できます。

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 (続く)

ロール	説明
	注: - ナレッジ管理者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場合は、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フィールド

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。
記事の有効期間	記事が作成された日付以降に有効なデフォルトの日数。
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の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ません。
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。
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。
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ません。
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。
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。

ナレッジベースフォームフィールド (続く)

フィールド	説明
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 ナレッジベースの責任を負うユーザー。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割り当てることができます。
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:承認の必要なし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: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管理者のみが記事を作成、検索、または表示できます。
説明	
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構成設定。
関連製品	OT ナレッジベースの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の詳細を確認してください。

概要

拡張クラスは、Operational Technology Management.構成管理データベース (CMDB)

[Operational Technology \(OT\) extension classes](#)

CMDB OT の更新クラス。

関連アプリケーション

[Knowledge Management](#)

この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

この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

IT Service Management アプリケーションを統合すると、オペレーショナルテクノロジーのナレッジ管理、ServiceNow 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。

ドメイン分離と Operational Technology

Operational Technology アプリケーションでは、ドメイン分離がサポートされています。ドメイン分離では、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、Domain Separation を完全にサポートしています。ドメイン分離には、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分離のサポート](#)

概要

Operational Technology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分離機能を継承します。各アプリケーションは独自のドメイン分離関係を持つことができるため、アプリケーションに Operational Technology 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 Flow Designer](#)

関連情報

[サービスプロバイダーのドメイン分離](#)