検証済みソリューション：製造業

改訂：2023 年 9 月 27 日

ソリューションの概要

このガイドでは、Cisco DNA Center および Cisco SD-Access を使用する一般的な運用技術（OT）ネットワーク導入プロファイルに関するガイダンスを提供します。このガイドは、検証の参考資料として使用できます。

OT ネットワークは、過去 20 ～ 30 年間、Purdue モデル（1990 年にリリース）に従っており、そのリリース以降、ネットワーキング業界で大きな変化があり、それらのイノベーションは今日の OT 業界で活用されています。

ここでは、今日の自動化要件を満たすために、進化する大規模な製造業 IT/OT ネットワークで考慮する必要がある重要な事項について説明します。

復元力、冗長性、および高可用性

OT ネットワークは組織の機能にとって重要になっているため（多くの場合、OT ネットワークは企業の中核であるため）、厳密なネットワークレベルとサービスレベルの復元力を提供することが重要です。ネットワークレベルの復元力は、デュアルファブリック ボーダー ノード、デュアルファブリック コントロールプレーン ノード、デュアルアンカー ボーダーおよびコントロールプレーンノード、デュアル ワイヤレス コントローラ、ハードウェアスタックまたは StackWise Virtual を備えたファブリックスイッチ、IE 拡張ノードの REP リング、デュアルファブリック トランジット コントロール プレーン ノード（該当する場合）を含む堅牢なファブリックネットワーク設計で実現できます。サービスレベルの復元力は、次を展開することによって実現されます。

- Cisco DNA Center 3 ノードクラスタ。
- 複数のポリシー管理ノード（PAN）、モニタリングノード（MNT）、およびアクティブとスタンバイの Platform Exchange Grid（pxGrid） とポリシーサービスノード（PSN）を備えた分散型 Cisco Identity Services Engine（ISE）クラスタ。

セキュリティとネットワークのセグメンテーション

今日の OT ネットワークでは、セグメンテーション機能が制限されている場合があり、OT ネットワークの大部分は VLAN ベースです。より深いセグメンテーションが必要な場合、多くの組織は物理的に分離された OT ネットワークを作成します。この問題を解決するために、ネットワーク管理者は、物理的な分離の利点と単一ネットワークのシンプルさを備えている論理的なセグメント化を使用します。このセグメンテーションは、サイバーセキュリティの問題への対処にも役立ちます。セグメンテーションが IP アクセス制御リスト（ACL）によってインスタンス化される場合、ほとんどのシンプルな展開では、時間の経過とともに拡張、トラブルシューティング、および維持が困難になる可能性があります。

Cisco SD-Access アーキテクチャ内では、Cisco DNA Center と Cisco ISE は連動し、計画、設定、セグメンテーション、アイデンティティサービス、ポリシーサービスの自動化を実現します。Cisco ISE は、デバイスプロファイリング、アイデンティティサービス、ポリシーサービスを提供し、Cisco DNA Center と動的に情報を交換します。

Cisco SD-Access ソリューションは、マクロセグメンテーションを使用することで、IT デバイスと製造フロアにあるデバイスの間のデータプレーンとコントロールプレーンを完全に分離するニーズに対応します。異なるデバイスを作成し、異なるオーバーレイ仮想ネットワーク（VN）に配置することで、製造業の OT ネットワークで完全なデータの分離を実現し、さまざまな IT 部門間にセキュリティを提供できます。

Cisco SD-Access はグループベースのポリシー（GBP）のスケーラブルグループタグ（SGT）を使用したマイクロセグメンテーションを使用することで、同じ VN 内のエンドポイント間の詳細なデータプレーン分離のニーズにも対応します。Cisco DNA Center IT 管理者は、グループを作成し、従業員をロールごとにグループに配置し、各グループのメンバーが相互に対話する方法を制御するポリシーを定義します。

サイレントホストの処理

OT ネットワークにおける最大の問題の 1 つは、製造フロアにあるサイレントホストです。製造フロアの一部のエンドポイントはサイレントホストです。それらのサイレントエンドポイントでは、ネットワーク内のそれぞれのプレゼンスはブロードキャストされません。Cisco DNA Center は、レイヤ 2 フラッディング機能を介してサイレントホストに対するソリューションを提供します。レイヤ2フラッディングは、特定のオーバーレイサブネットのブロードキャスト、リンクローカル マルチキャスト、および ARP トラフィックのフラッディングを可能にします。この機能は、オーバーレイサブネットをアンダーレイの専用のマルチキャストグループにマッピングし、ターゲットのトラフィックをファブリックの Virtual Extensible LAN（VXLAN）でカプセル化して、送信先のアンダーレイ マルチキャスト グループにデータを送信します。このソリューションでは、アンダーレイで PIM Any-Source Multicast（PIM-ASM）が使用されます。これは、Cisco DNA Center の LAN 自動化ワークフローを使用して自動的に、または導入の後半のフェーズで手動で設定できます。このソリューションは、各種組み込み機能を備えたさまざまな OT デバイスに対応することで、OT ネットワークに柔軟性を提供します。

レイヤ 2 専用 VN（ファブリック外のゲートウェイ）

OT ネットワークの場合、さまざまなユースケースやビジネス目的用の多数のレイヤ 2 ネットワークが工場のフロアにあります。高レベルのセキュリティを実現するには、ファブリックネットワークの外部にあるファイアウォールでレイヤ2トラフィックを検査する必要があります。この要件は、すべてのトラフィックの最初のホップがファブリックの外部にある必要があることを意味します。この実装では、レイヤ2専用 VN とアンダーレイマルチキャスト機能を組み合わせて使用します。

ネットワークのアシュアランスと分析

ネットワーク管理者は、OT システムの動的なニーズに迅速に対応するために、ネットワークを効率的に管理およびモニターできます。導入環境では、ネットワーク、デバイス、アプリケーションのパフォーマンスを向上させるためにテレメトリを使用することで、ネットワーク関連やセキュリティ関連のリスクがプロアクティブに予測されます。Cisco DNA アシュアランス は Cisco AI Network Analytics を使用して、テレメトリデータを収集し、ネットワークデバイスのパフォーマンスをモニターし、検出された問題にフラグを付け、修復手順を提示します。

Cisco DNA アシュアランス および Cisco AI Network Analytics を使用することで、ネットワーク管理者は、ネットワークデバイスおよび接続されているエンドポイント（有線とワイヤレスの両方）の全体的な正常性をモニターできるだけでなく、デバイス、エンドポイント、および個々のアプリケーションの正常性を確認できます。この360度の分析により、管理者は、ワイヤレスラップトップの接続や OT デバイスのワイヤレス SSID への接続の問題など、ネットワーク要素が直面している個々の問題を特定できます。

Cisco AI エンドポイント分析

最新のセキュリティ脅威は、企業情報を得るために、エンタープライズ ネットワークの脆弱な単一のエントリポイントをエクスプロイトしようとします。エントリポイントが侵害されると、脅威はデバイス全体に数秒で水平拡散する可能性があります。Cisco SD-Access ソリューションのような、きめ細かいネットワーク セグメンテーションを行うことが、この種の脅威の水平拡散を防ぐためには推奨されます。従来の OT ネットワークには、無人搬送車（AGV）、プログラマブル ロジック コントローラ（PLC）、さまざまな製造機器や監視デバイスなど、数千台の類似デバイスが含ま

れています。ネットワーク上のすべてのデバイスを見つけて識別することは、時間がかかり、面倒な作業です。Cisco AI エンドポイント分析 は、パッシブ ネットワーク テレメトリ モニタリングとネットワークのディープ パケット インスペクションを通じて、タイプ、製造元、通信プロトコル、およびポート別にデバイスを識別することで、この問題に対処します。

Cisco DNA Center はエンドポイントの分類属性も Cisco ISE と共有します。新しいデバイスがアイデンティティベースの認証を介してオンボーディングされると、製造元とタイプによって自動的に識別されて、適切なグループに追加されます。セキュリティポリシーの定義と適用は、個々のエンドポイントではなくグループに適用した方が簡単です。グループベースのポリシーは、エンドポイントによるセキュリティ侵害などの新たな状況に合わせて簡単に編集でき、ネットワーク全体にグローバルに適用できます。

ハードウェアとソフトウェアの仕様

ソリューションは、次の表に示すハードウェアとソフトウェアで検証されています。サポートされているハードウェアの完全なリストについては、「Cisco Software-Defined Access Compatibility Matrix」を参照してください。

ロール	モデル名	ハードウェア プラットフォーム	ソフトウェア バージョン
Cisco DNA Center コントローラ	DN2-HW-APL-XL	Cisco DNA Center アプライアンス 3 ノードクラスタ	2.3.3.7
アイデンティティ管理、RADIUS サーバー	ISE-VM-K9	Cisco Identity Services Engine 仮想アプライアンス	3.1 パッチ 2
	SNS-3695-K9	Cisco ISE アプリケーション用の Secure Network Server（大規模）	
Cisco SD-Access ファブリック コントロール プレーン ノード	ASR1001-X	Cisco 1000 シリーズ アグリゲーション サービス ルータ	17.6.3a、17.6.4、17.9.2a
	C9500-24Y4C、C9500-24Q、C9300-48P、C9300-24P	Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9500 シリーズ スイッチ	17.6.4、17.9.3
Cisco SD-Access ファブリック ボーダー	C9500-24Y4C、C9500-40X、C9500-12Q、C9500-24Q、C9300-48P、C9300-24P	Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9500 シリーズ スイッチ	17.6.4、17.9.3
Cisco SD-Access ファブリック エッジ	C9300-48P、C9300-24P	Cisco Catalyst 9300 シリーズ スイッチ	17.6.4、17.9.3
Cisco SD-Access ワイヤレス コントローラ	C9800-80-K9	Cisco Catalyst 9800-80 ワイヤレスコントローラ	17.6.4、17.9.3

ロール	モデル名	ハードウェア プラットフォーム	ソフトウェア バージョン
Cisco SD-Access 拡張ノード	IE-3400H-16T	Cisco Catalyst IE3400 高耐久性シリーズ	17.6.4、17.9.3
	IE-3300-8P2S	Cisco Catalyst IE3300 高耐久性シリーズ	17.6.4、17.9.3

ソリューションの導入例のシナリオ

以下のユースケースは、図 1 に示されているトポロジを使用して製造プロファイルに対して検証されています。

- サービスとネットワークの復元力
  - デュアル Cisco SD-Access ボーダーとデュアル コントロール プレーン ノード、ボーダー StackWise Virtual リンクとボーダー/エッジスタック、およびトランジットネットワークのデュアル トランジット コントロール プレーンにより、ネットワーク全体で高可用性を実現できます。フェールオーバーとネットワーク障害の回復が発生した場合、トラフィックフローの中断は生じないか、最小限である必要があります。
  - 管理者は、3 ノード高可用性モードで Cisco DNA Center を設定できます。Cisco DNA Center クラスタでサービスやノードの障害が発生した場合、ユーザーの介入なしでシステムが回復する必要があります。
  - Cisco ISE の分散展開モデルは、PAN、PSN、pxGrid サービスのフェールオーバーにより回復する必要があります。
  - 管理者は、Cisco ISE に到達できない場合にファブリックエッジに重要な VLAN を実装できます。
  - Cisco DNA Center は、オンデマンドまたはスケジュールに従い設定とデータをバックアップできます。バックアップファイルを Cisco DNA Center に復元して、以前の設定にロールバックできます。
- 機密性の高い OT ネットワークデータを保護する多層セキュリティの実装
  - 管理者は、ネットワークでの脅威の拡散を制限するために、ユーザー、ゲスト、モノのインターネット（IoT）デバイス、OT デバイスをそれぞれの論理ネットワークにセグメント化できます。
  - 管理者は、不正アクセスを防ぐために、有線およびワイヤレスのエンドポイントに対してクローズド認証オンボーディング（dot1x 認証）または MAC 認証バイパス（MAB）を有効にできます。
  - 管理者は、グループを作成し、ユーザーやエンドポイントを（アイデンティティに基づいて）グループに分け、グループ間のトラフィックを制御するグループベースのポリシーを定義できます。
  - 管理者は、工場のフロアに大規模なアクセス コントロール ポリシーを実装でき、クライアントのオンボーディング時にセキュリティグループ ACL（SGACL）がエッジデバイスに適切にインストールされます。
  - 管理者は、システムイベントが記録される監査ログを使用して Cisco DNA Center のアクティビティをモニターできます。監査ログには、発生したシステムイベント、発生した時刻と場所、イベントを開始したユーザーが含まれます。
  - 管理者は、Cisco DNA Center へのアクセス権限が異なる詳細なロールベースのユーザーを作成できます。

- シンプルな管理
  - Cisco DNA Center により、デバイスインベントリが一元管理され、ユーザーは IP アドレス、プロビジョニングステータス、ソフトウェアリリース、インベントリインサイトなどのデバイス情報を確認できます。
  - Cisco DNA Center では、管理者は、ソフトウェアイメージ管理（SWIM）機能を使用して、スイッチ、ルータ、拡張ノード、およびワイヤレスコントローラのゴールデンイメージをアップグレードできます。
  - Cisco DNA Center では、ファブリックボーダーとコントロールプレーンの RMA ワークフローにより、デバイスの交換がシームレスになります。
  - サイトのボーダーの L3 ハンドオフによる VLAN の消費の最適化により、拡張マルチサイト環境における VLAN の割り当ての柔軟性が管理者にもたらされます。
  - LAN 自動化の重複プールオプションにより、アンダーレイネットワークの異なるファブリックサイト間で同じアドレスを再利用でき、IP アドレスの使用が大幅に最適化されます。
- ネットワーク サービス
  - 管理者は、Cisco SD-Access ファブリックエンドポイントをサポートすることを目的としたレイヤ 2 専用 VN 機能を実装できます。セキュリティ上の理由から、ファブリックの外部に存在するネットワークに対する厳密なエントリポイント（ファイアウォールを経由するなど）があります。
  - 管理者は、拡張ノードを使用してネットワーク障害の回復時間が 50 ms 未満となる冗長性を実現でき、ファブリックサイトの Resilient Ethernet Protocol（REP）リングを設定できます。
  - 管理者は、ファブリックサイト内のブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）トラフィックだけでなく、サイレント OT デバイスを処理する L2 フラッディングを有効にできます。
- Cisco DNA アシュアランス と Cisco AI エンドポイント分析 を使用したネットワークとクライアントのモニター
  - 管理者は、Cisco DNA アシュアランス を使用してネットワークの正常性をモニターして、ネットワークの問題を特定できます。Cisco DNA アシュアランス は、リンクのダウン、AP のダウン、スイッチスタックメンバーのダウンなど、さまざまなネットワーク障害に起因する問題を報告できます。
  - 管理者は、Cisco DNA アシュアランス を使用して有線クライアントとワイヤレスクライアントの正常性をモニターし、クライアントのオンボーディングの問題を特定できます。
  - 管理者は、テレメトリデータロガー（TDL）ベースのアシュアランスを有効にして、クライアントの正常性を報告する際のスケールとパフォーマンスを向上できます。
  - 管理者は、多数の同時エンドポイントをモニターできます。アシュアランスチャートには、100,000 の同時エンドポイントと 250,000 の一時エンドポイントの情報が表示されます。
  - 管理者は、Cisco AI エンドポイント分析 を使用して、エンドポイントと IoT デバイスを識別およびプロファイリングできます。
  - 管理者は、ワイヤレスセンサーを使用してワイヤレスネットワークのパフォーマンスをモニターできます。
  - 管理者は、アプリケーションテレメトリを有効にし、Cisco DNA アシュアランス を使用して、遅延、ジッター、パケットドロップに関するアプリケーションの正常性をモニターできます。

- 管理者は、既存のエンドポイント間の通信を可視化して、新しいアクセス制御の導入の必要性と影響を評価できます。
- 管理者は、グループベースのポリシー分析機能を使用して、マイクロセグメンテーション ポリシーを作成および実装できます。

トポロジ

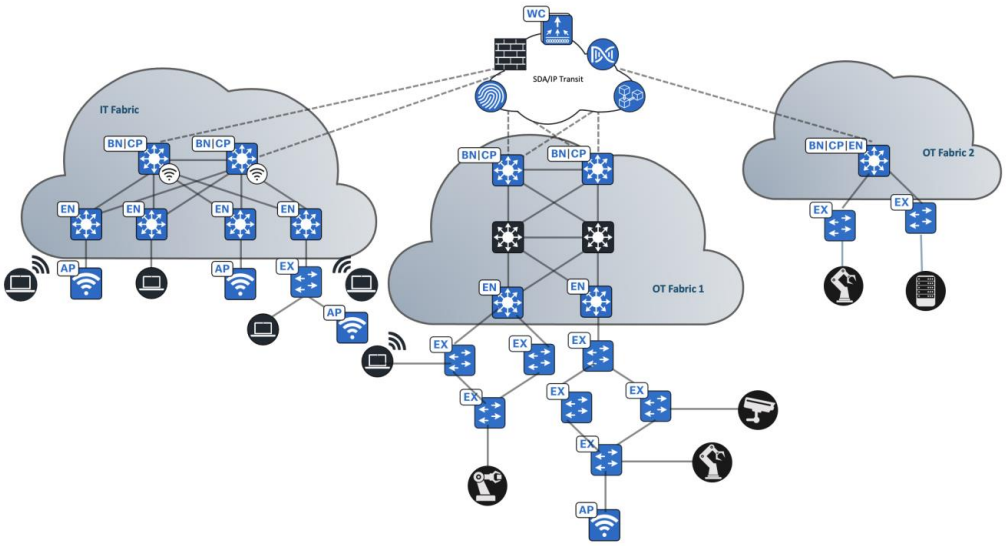
製造業プロファイルのテストトポロジには、1 つの IT ネットワークサイト、1 つの中規模 OT サイト、および 1 つの小規模 OT ネットワークを管理するための 3 ノード Cisco DNA Center クラスタが含まれています。Cisco SD-Access トランジットは、これらのネットワークを接続するために展開されます。次の図は、製造業ソリューションのテストベッドの論理トポロジを示しています。

テストベッドのセットアップには、次のコンポーネントがあります。

- IT ファブリックには、デュアル共存ボーダーおよびコントロールプレーンノード、ワイヤレスコントローラ、ファブリックエッジ、拡張ノードがあります。
- OT ファブリック 1 には、デュアルボーダー、デュアル専用コントロールプレーンノード、デュアル ワイヤレスコントローラ、10 個のファブリックエッジ、および 20 個の拡張ノードがあります。
- OT ファブリック 2 は、組み込みワイヤレスコントローラ ノードと拡張ノードを備えたハードウェアスタッキング上の一体型ファブリック（FiaB）を備えた小規模サイトです。
- Cisco SD-Access トランジットは、デュアルトランジット コントロール プレーン ノードで実装されます。IT ネットワークのボーダーは、Cisco SD-Access トランジットを介して他の OT サイトにインターネットアクセスを提供するように設定されています。

次の図は、ソリューションのテストベッドの論理トポロジを示しています。

図 *1*: ソリューションのテスト論理トポロジ



スケール

ソリューションのテストでは、次の表に示すスケールについて確認しました。ハードウェアキャパシティについては、*Cisco DNA Center* のデータシートを参照してください。

カテゴリ	値
デバイスインベントリ	5000
ファブリックサイトごとのデバイス	1000
建物とフロア	2000
ファブリックサイトごとの VN	64
ファブリックサイトの IP プール	500
ファブリックサイトごとのワイヤレスコントローラ	2
ファブリックサイト	500
インベントリの AP	12,000
エンドポイント	100,000（有線 80,000、ワイヤレス 20,000）
SSID	10
SGT	4000

カテゴリ	値
REP リング内の IE デバイス	18

ソリューションの重要事項

ここでは、ソリューションの展開に役立つテクニカルノートについて説明します。

オフィス外でのスペース拡張

製造業では、OT ネットワーク内のデバイスは、オフィス外や起伏の激しい場所に配置されることがよくあります。そのような場合、シスコの産業用イーサネット（IE）スイッチを拡張ノード（EN）として使用できます。Cisco SD-Access EN は、レイヤ 2 ポート拡張を提供し、既存のファブリックエッジノードへのポート密度を高めることで、モビリティを実現します。一方、それらの EN は、それぞれのスイッチに接続されているエンドポイントにセグメンテーションおよびグループベースのポリシーも提供します。Cisco DNA Center は、EN を検出、プロビジョニング、およびファブリックに追加するためのゼロタッチのプラグアンドプレイ自動ワークフローを提供することに注意してください。

Cisco DNA Center には、拡張ノードのサポートオプションとして、クラシック EN とポリシー拡張ノード（PEN）の 2 つがあります。PEN は、クラシック EN で提供される運用と管理に加えて、SGACL による SGT ポリシーの適用を直接サポートします。この SGACL のローカルサポートにより、PEN に水平方向のトラフィックを直接適用できます。

EN は、802.1Q トランクポートを介して単一のファブリックエッジスイッチに接続されます。このポートは、2 つ以上のリンクがアップストリーム ファブリック エッジで集約されている場合、EtherChannel として展開できます。トランクと EtherChannel の作成は Cisco DNA Center で自動化されています。ワークフローで EN がオンボーディングされたら、エンドポイント（ファブリックモード AP と他の Power over Ethernet（PoE）デバイスを含む）を EN に直接接続し、必要に応じて有線およびワイヤレスサービスをオフィス外のスペースに拡張できます。Cisco SD-Access EN の展開の詳細については、Cisco Extended Enterprise 非ファブリックおよび SD-Access ファブリック設計ガイド [英語] を参照してください。

REP リング

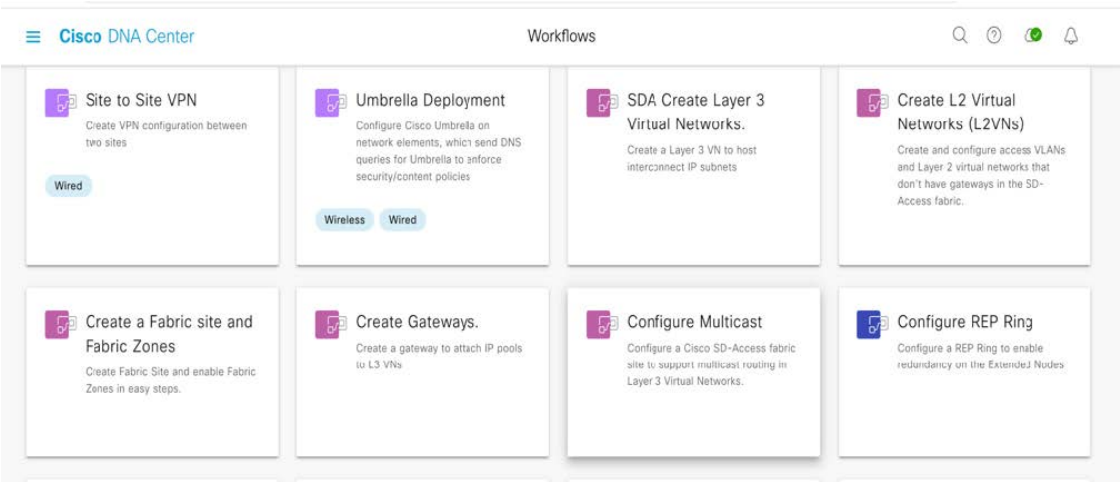
OT ネットワークは、IT ネットワークと比較して、ネットワークデバイスが地理的に遠い場所に分散している傾向があります。隣接するスイッチの間が数 km 離れている場合もあります。設置場所が地理的に分散しているため、すべてのアクセススイッチをディストリビューション レイヤまでケーブルで物理的に接続できないため、スター型トポロジの使用は非現実的であるか、コストがかかりすぎる可能性があります。OT ネットワークにはスター型トポロジのネットワークが含まれることが多いですが、リニアデイジーチェーンやリングトポロジなど、他のトポロジも含まれます。

一般に、製造業では、モーションアプリケーションにはゼロ損失と同期が必要ですが、アプリケーションの要件はあまり厳しくありません。たとえば、モーションアプリケーションの入出力動作は、最大 100 ミリ秒のレイヤ 2 コンバージェンス時間に耐えることができます。ほとんどの製造業では、このレベルの復元力と精度は必要ありません。シスコでは、OT ネットワークは通常、スパニングツリープロトコル（STP）のバリアントを備えた REP リングとして展開され、復元力を提供します。

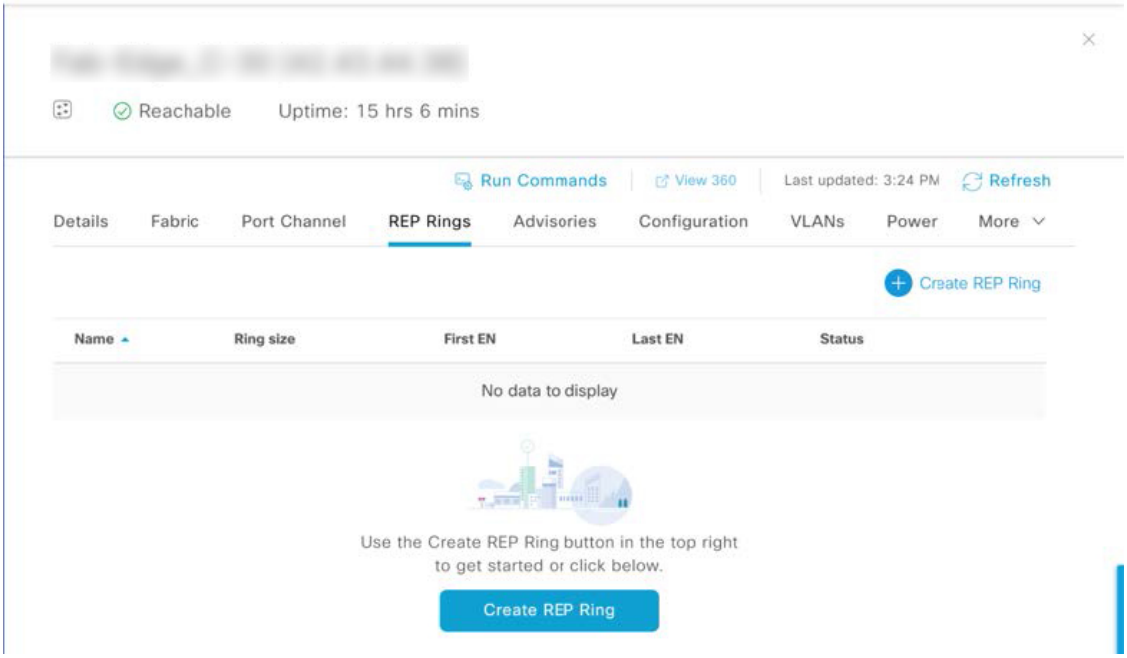
Cisco DNA Center には、Cisco SD-Access ファブリックサイトで REP リングを作成して展開するワークフローが用意されており、IE スイッチはファブリックエッジに接続され、2 つの EN のデイジーチェーンとしてオンボーディングされます。Cisco DNA Center を使用すると、次の手順に従って、この REP リングの自動化を完了できます。

手順

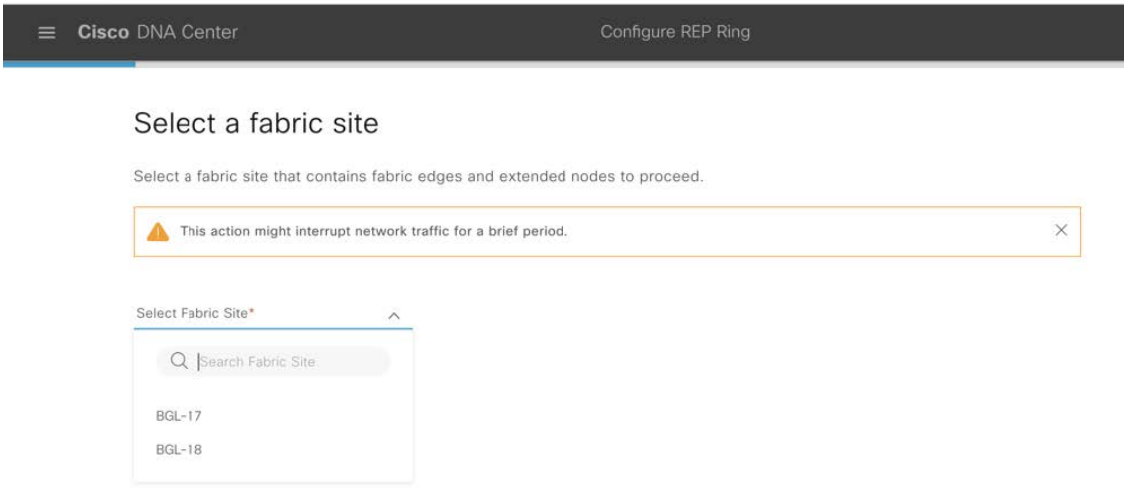
ステップ 1 メニューアイコン（☰）をクリックして、**[Workflows]** > **[Configure REP Ring]** の順に選択します。



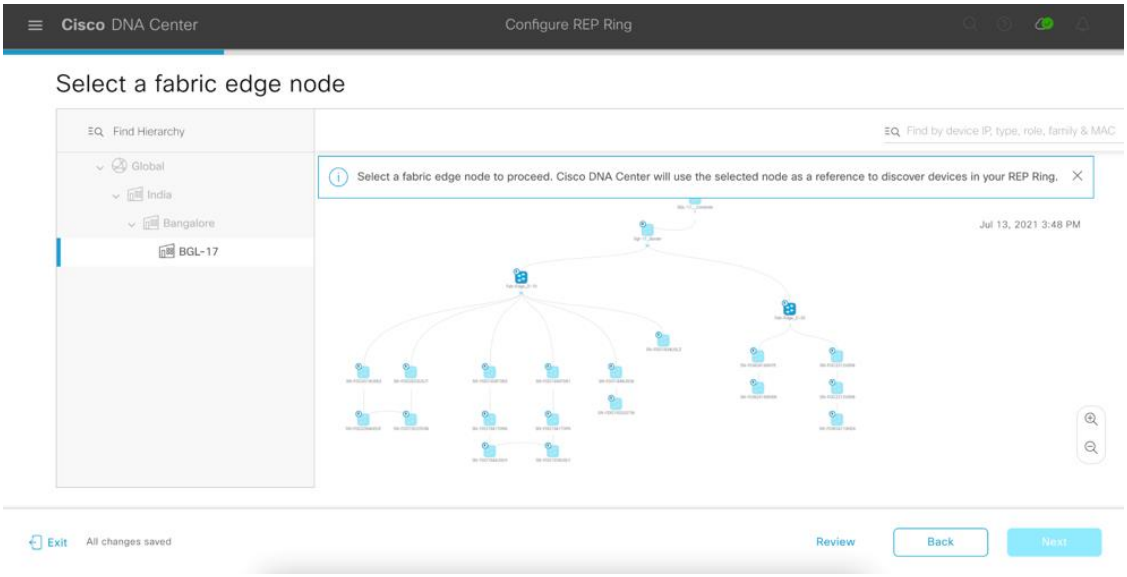
または、ファブリック サイト トポロジ ビューに移動して、REP リングを作成するファブリック エッジ ノードまたは FiaB ノードを選択することもできます。次に、[REP Rings] タブで、[Create REP Ring] をクリックします。



ステップ 2 [Select a fabric site] ページで、[Select Fabric Site] ドロップダウンリストからファブリック サイトを選択します。

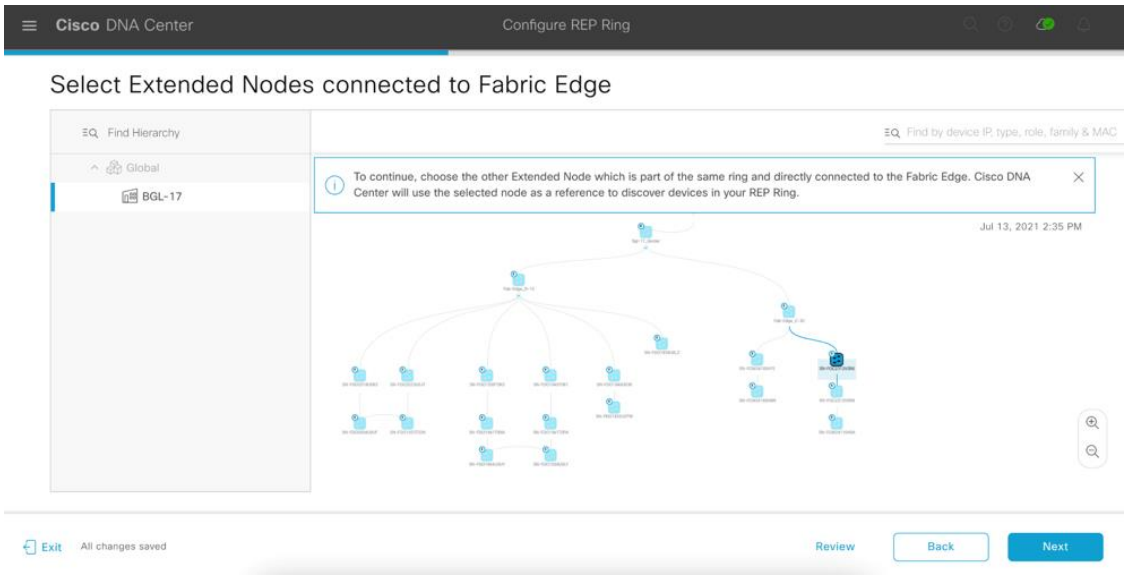


ステップ 3 [Select a fabric edge node] ページで、ファブリックエッジノードを選択します。

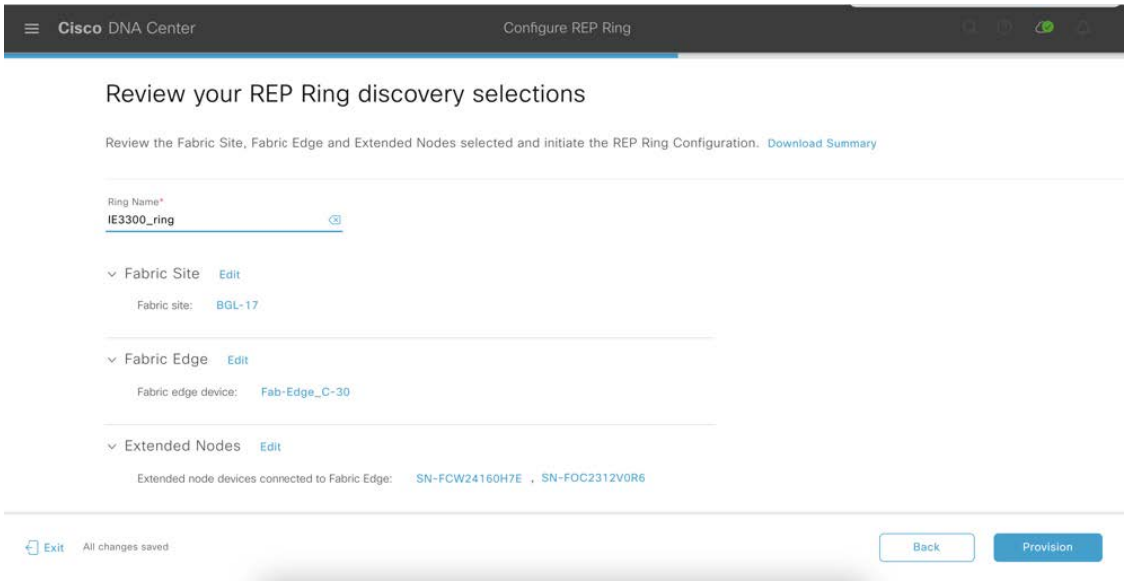


ステップ 4 [Select Extended Nodes connected to Fabric Edge] ページで、ファブリックエッジノードに接続する EN を選択します。

ファブリックエッジノードに接続する 2 つの EN を選択できます。



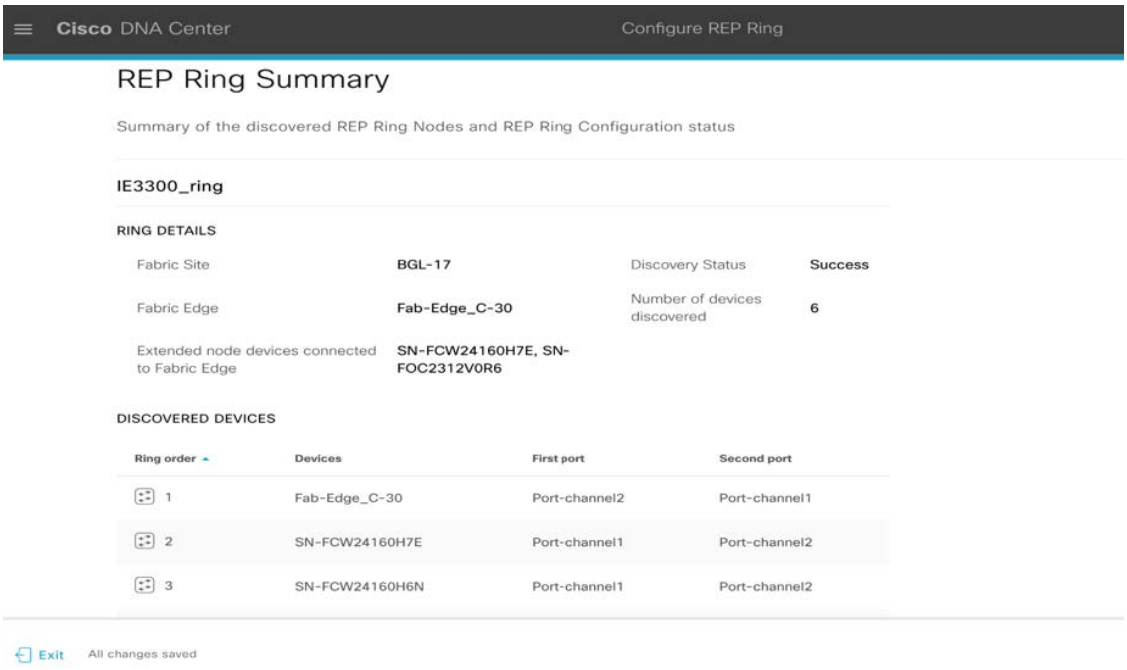
ステップ 5 [Review your REP Ring discovery selections] ページで、ファブリックサイト、エッジノード、および EN の構成を確認および編集します（必要な場合）。



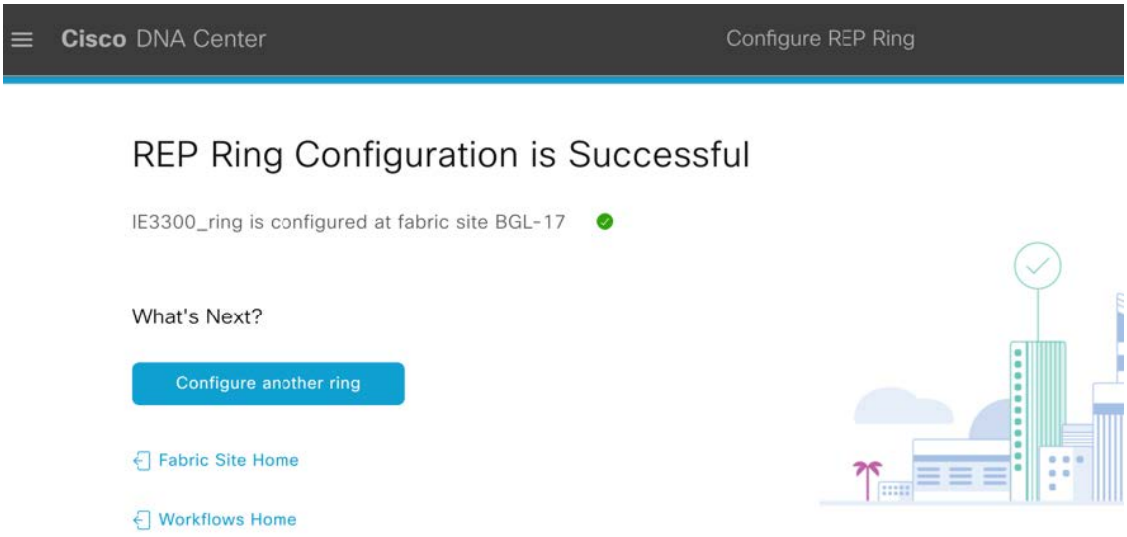
ステップ 6 準備ができたら、[Provision] をクリックします。

ステップ 7 [REP Ring Summary] ページで、[Next] をクリックします。

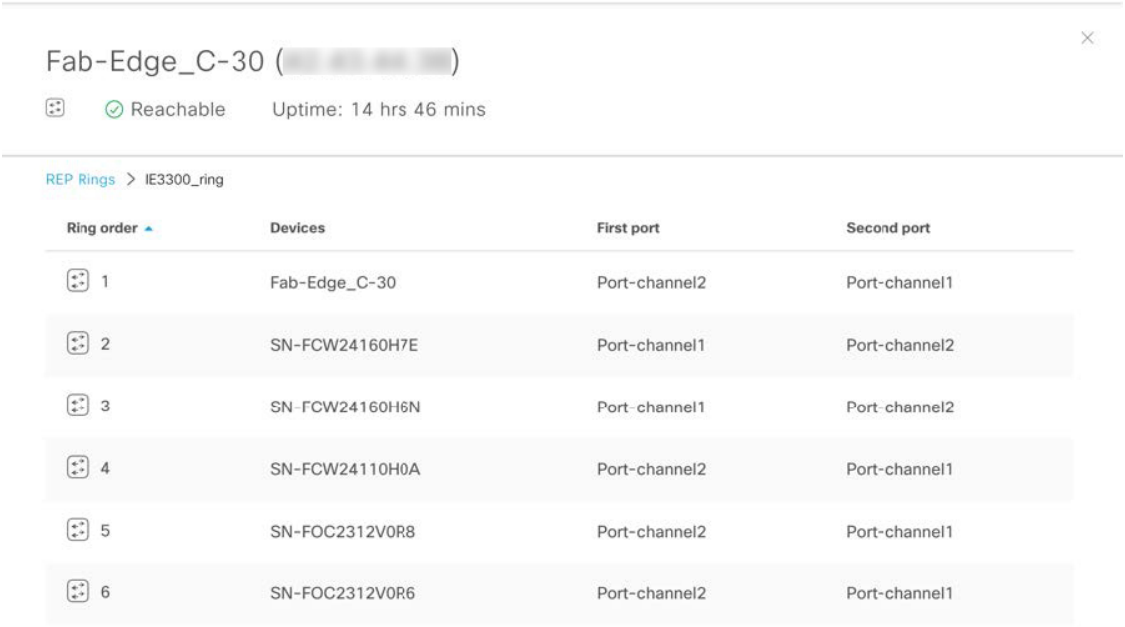
このページは、検出されたデバイスとともに、作成された REP リングの詳細情報が表示されます。



REP リングが作成されると、成功メッセージが表示されます。



ステップ 8 （任意）REP リングの作成を確認するには、ファブリック サイト ウィンドウに移動し、ファブリック エッジ ノードをクリックします。slide-in pane の [REP Ring] タブで、そのエッジ ノードに存在するすべての REP リングのリストを確認できます。



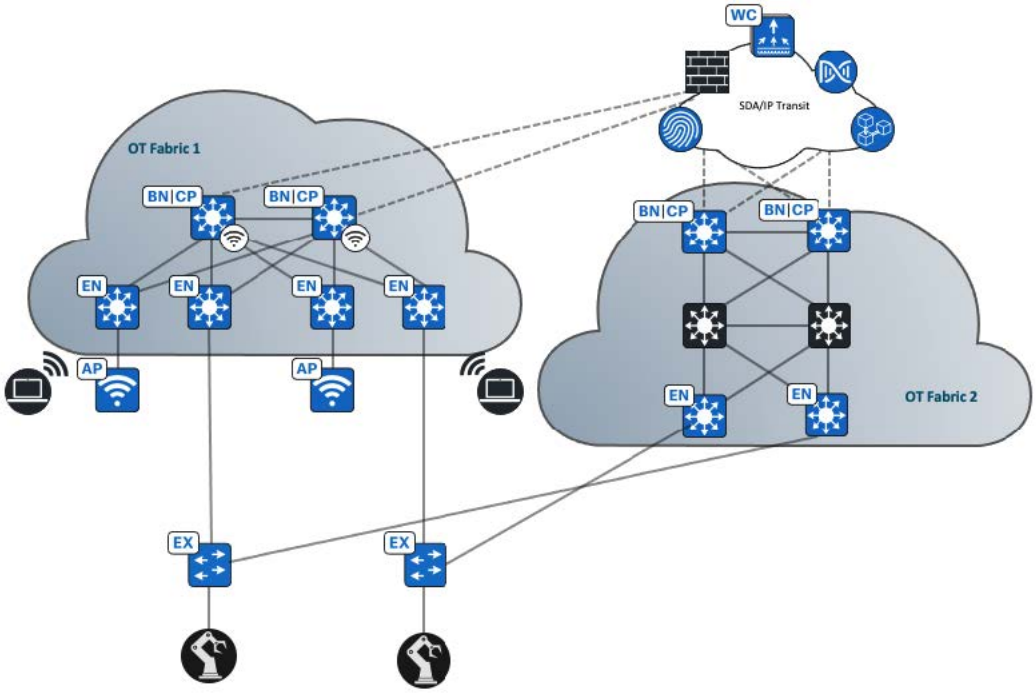
ゼロ損失冗長性：PRP を使用したデュアルファブリック

OT ネットワークは組織の機能にとって重要になっているため（多くの場合、OT ネットワークは企業の中核であるため）、OT ネットワークに復元力オプションを提供することが重要です。これらの冗長性スキームでは、ネットワークが回復し、トラフィックが再び流れるまでに数ミリ秒から数秒かかることがあります。製造フロアの品質管理システム（SAP など）がダウンしている場合（階層 1、階層 2、階層 3 の製造に関係なく）、製造ラインはダウンするため、ネットワークが影響を受けると、工場がダウンし、1 秒あたり数百万ドルの損失が生じる可能性があります。

ネットワーク障害から回復するために、メッシュトポロジやリングトポロジで接続されたネットワーク要素によって冗長性を提供できます。この場合、ネットワーク障害が発生するとネットワーク内が再構成され、トラフィックが再び流れるようになります。通常は、ブロックされたポートを開くことで流れます（これらのトポロジでは、RSTP、REP、MRP などのプロトコルが使用されることに注意してください）。ただし、製造業ではゼロパケット損失が要求されます。

Parallel Redundancy Protocol（PRP）は、国際規格の国際電気標準会議（IEC）62439-3 で定義されています。PRP は、イーサネットネットワークでヒットレス冗長性（障害後の回復時間ゼロ）を提供するように設計されています。PRP では異なるスキームが使用され、2 つのネットワーク インターフェイスを 2 つの独立し、分離されたパラレルネットワーク（LAN-A と LAN-B）に接続することで、（ネットワーク要素ではなく）エンドノードに冗長性が実装されます。各デュアル通信ノード（DAN）には、ネットワーク内にある他のすべての DAN への冗長パスがあります。

ソリューションは、Cisco SD-Access ネットワークで PRP を活用して、冗長 Cisco SD-Access ファブリックを作成し、メインサイトと冗長サイトの両方に EN を接続することで、パケット損失ゼロを実現することです。次のトポロジには、2 つの Cisco SD-Access ファブリックサイトが含まれています。



Cisco DNA Center は、EN オンボーディングおよび CLI テンプレートを使用して PRP 固有の設定を EN にプッシュすることで、このソリューションを実装します。この設定は、次の手順で実装できます。

手順

ステップ 1 通常のポート集約プロトコル（PAgP）ポートチャネルを介して拡張ノードをファブリック 1 に接続します。ファブリック 1 は、LAN 自動化プロセスによって PEN としてオンボーディングされます。

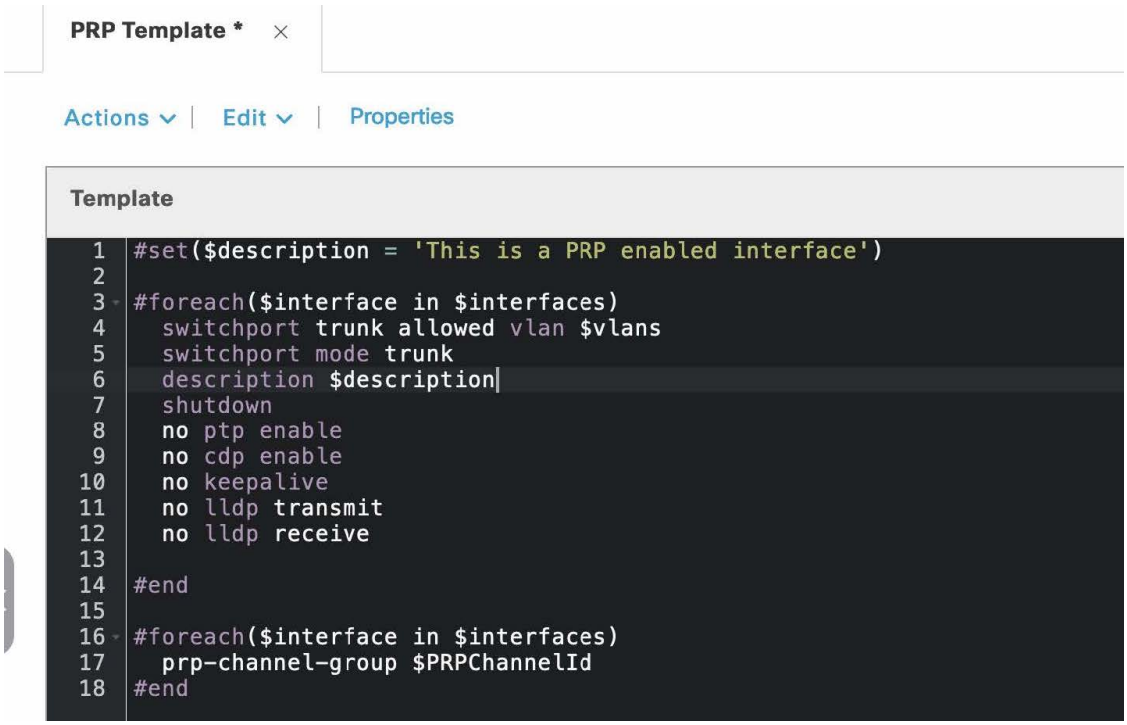
```
interface Port-channel1
description Extended2
switchport mode trunk
!
interface GigabitEthernet1/0/11
 switchport mode trunk
 cts manual
  policy static sgt 8000 trusted
 channel-group 1 mode desirable
```

ステップ 2 IE スイッチが正常にオンボードされると、ファブリック 2 エッジノードのダウンリンクポートが Cisco DNA Center GUI から PAgP トランクポートとして設定されます。

```
interface Port-channel1
 switchport mode trunk
 device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/0/13
 switchport mode trunk
 channel-group 1 mode desirable
```

ステップ 3 両方のファブリックサイトからのエッジが IE スイッチに接続され、プロビジョニングされたら、Cisco DNA Center プロビジョニング テンプレートを使用して PRP 設定を IE スイッチのアップリンクポートに適用できます。

PRP 設定については、次の Velocity テンプレートのサンプルを参照してください。

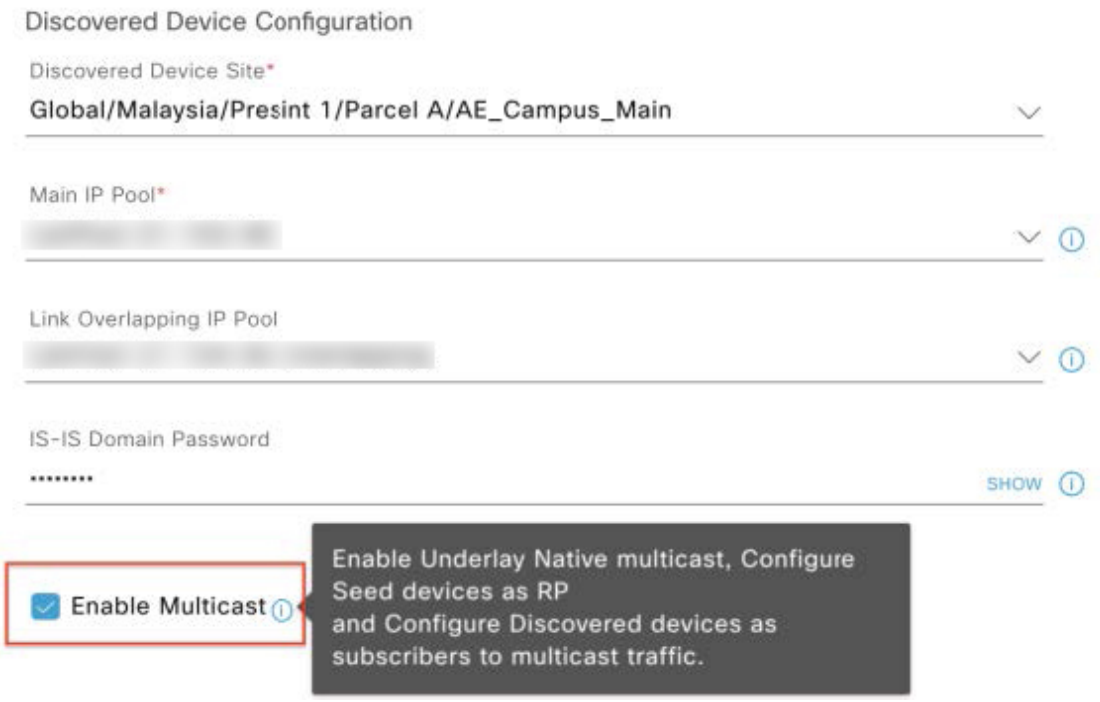


レイヤ 2 専用 VN（ファブリック外のゲートウェイ）

OT ネットワークの場合、さまざまなユースケースやビジネス目的用の多数のレイヤ 2 ネットワークが工場のフロアにあります。高レベルのセキュリティを実現するには、ファブリックネットワークの外部にあるファイアウォールでレイヤ 2 レベルのトラフィックを検査する必要があります。この要件は、すべてのトラフィックの最初のホップがファブリックの外部にある必要があることを意味します。この実装は、レイヤ 2 専用 VN とアンダーレイマルチキャスト機能の組み合わせを使用して実現されます。

アンダーレイマルチキャスト機能の場合、将来のファブリック マルチキャスト サービスの導入に備え、物理アンダーレイネットワークでマルチキャストを有効にします。LAN 自動化ワークフローの実行中にアンダーレイマルチキャストを有効にすることを強く推奨します。Cisco DNA Center には、LAN 自動化ワークフローの実行中に新しいデバイスのアンダーレイ PIM-ASM 設定を自動化するオプションがあります。このワークフローでは、シードデバイスで Loopback60000 が作成され、このアドレスがアンダーレイ マルチキャスト ネットワークのデフォルト ランデブー ポイントとして使用されます。図 2 に、LAN 自動化ワークフローを使用してアンダーレイマルチキャストを有効にする方法を示します。

図 *2 : LAN* 自動化ワークフローでのアンダーレイマルチキャストの有効化

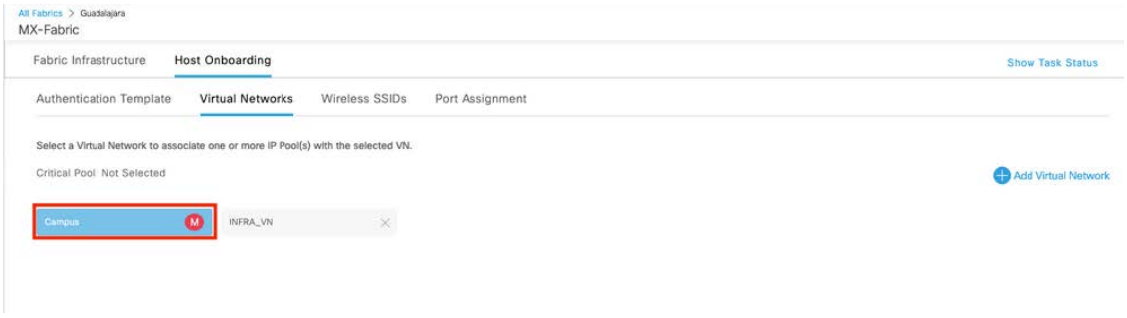


次の手順では、レイヤ 2 専用 VN ワークフローと展開を使用して、Cisco DNA Center の物理レイヤ 2 専用サービスでマルチキャストを有効にする方法を示します。

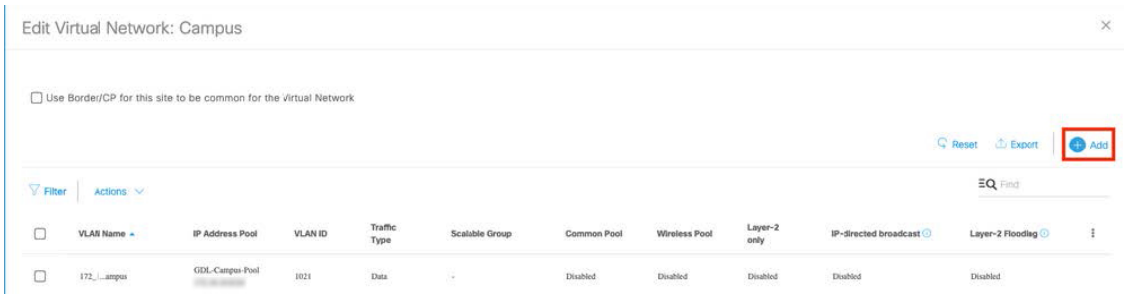
手順

ステップ 1 ファブリックサイトを選択し、そのファブリックサイトのウィンドウで、**[Hosting Onboarding]** > **[Virtual Networks]**を選択します。

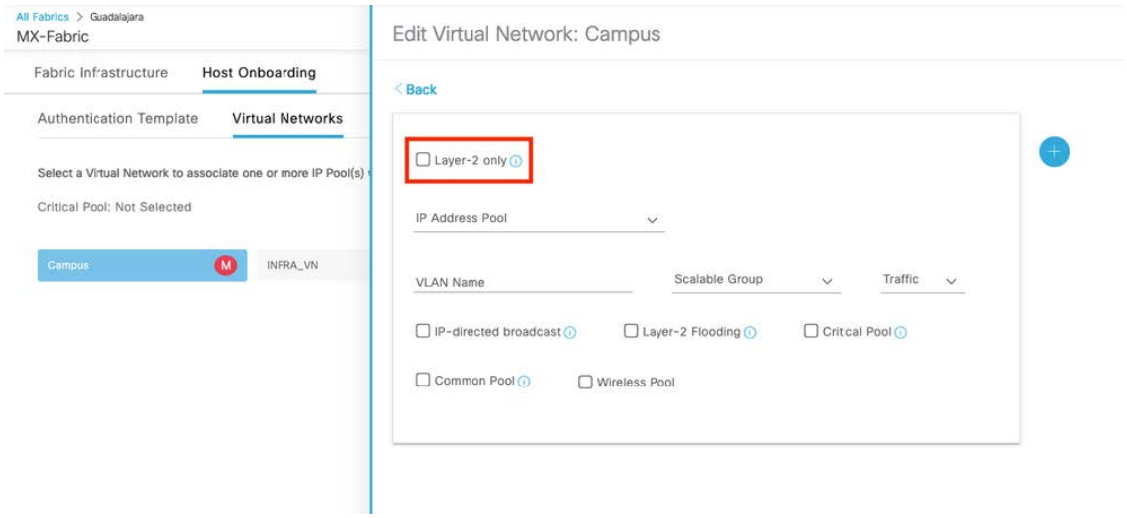
ステップ 2 レイヤ 2 専用サービスを追加する VN を選択します。



ステップ 3 [Edit Virtual Network: Campus] slide-in paneで、新しい IP プールを追加する場合と同様に [Add] をクリックします。

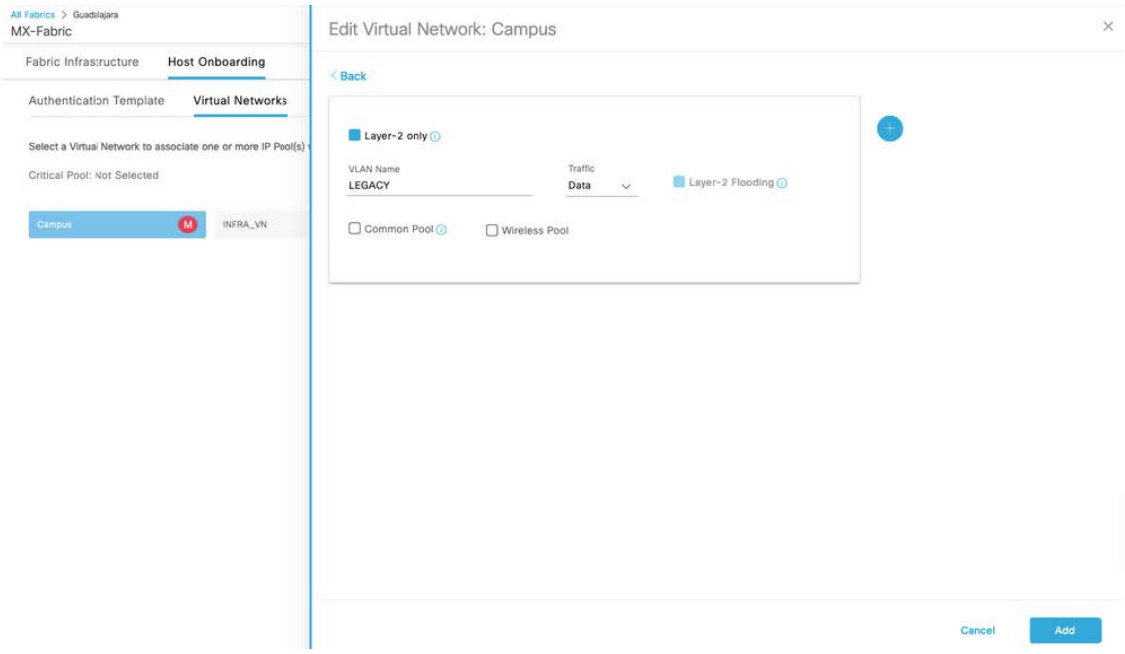


[Edit Virtual Network: Campus] slide-in paneに、[Layer-2 only] チェックボックスが表示されます。ここで、このセグメントがレイヤ 2 専用サービスであることを指定できます。

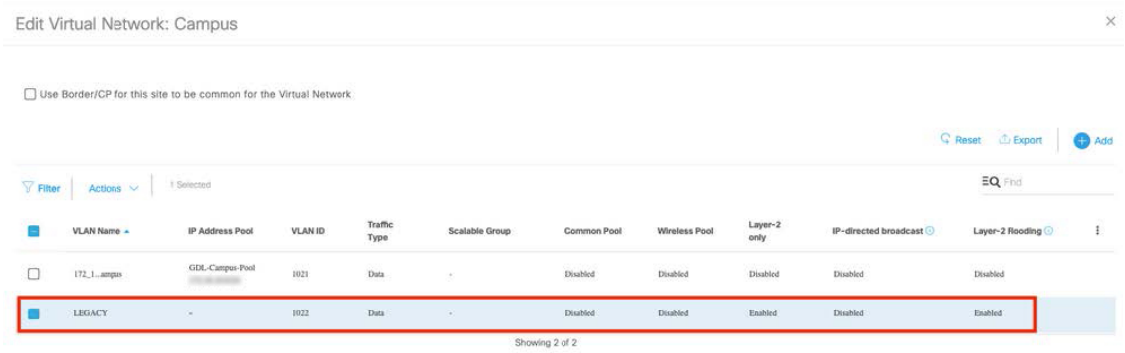


ステップ 4 [Layer-2 only] チェックボックスをオンにし、必要な情報を入力して、[Add] をクリックします。

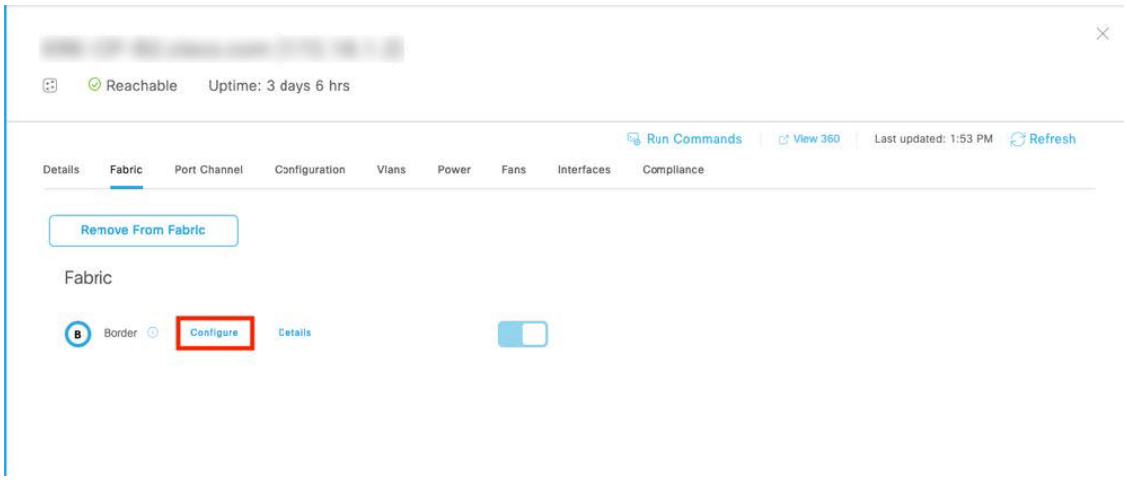
（注） Cisco DNA Center は、入力された名前を使用して外部 VLAN を識別し、ファブリック VLAN にマッピングします。



[Edit Virtual Network: Campus] slide-in paneには、レイヤ 2 専用セグメントが別の IP プールであるかのように表示されるようになりました。



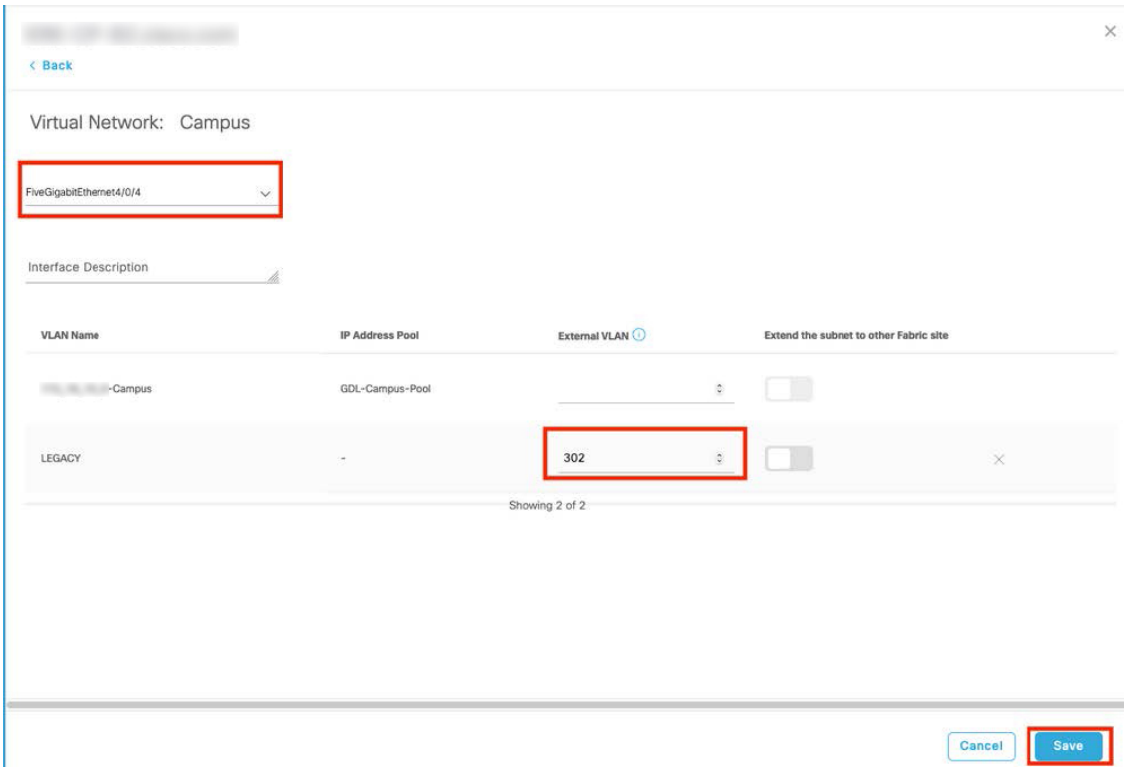
ステップ 5 [Fabric Infrastructure] に戻り、レイヤ 2 ボーダーとして追加するデバイスをクリックします。既存のボーダーを変更する場合は、[Border] オプションボタンを選択するか、[Configure] オプションボタンを選択します。



ステップ 6 slide-in paneで、[Layer 2 Handoff] タブをクリックして使用可能な VN のリストを表示し、目的の VN をクリックします。

ステップ 7 Fusion デバイスに接続するインターフェイスを選択し、外部 VLAN ID を指定して、[Save] をクリックします。

（注） 外部 VLAN ID は、外部ゲートウェイが属する VLAN です。



Cisco DNA Center によるファブリックデバイスの設定が完了すると、機能をテストできます。

Cisco AI エンドポイント分析

OT ネットワークでは、請負業者やベンダーのさまざまなデバイスを管理する必要があり、規模に加えて、セキュリティの問題も発生します。最新のセキュリティ脅威は、エンタープライズ ネットワークの有益な企業情報をエクスプロイトするための脆弱なエントリポイントを探します。ネットワーク内のすべてのデバイスを特定して追跡するのは、時間がかかり、面倒な作業です。Cisco AI エンドポイント分析 機能は、パッシブ ネットワーク テレメトリ モニタリングとディープ パケット インスペクションを通じて、タイプ、製造元、モデル、OS タイプ、通信プロトコル、およびポート別にデバイスを識別することで、この問題に対処します。この機能を使用すると、管理者は、属性に基づいてデバイスを分類するためのプロファイリングルールを作成できます。Cisco DNA Center は、機械学習と連携してスプーフィングされたエンドポイントを検出し、管理者が適切なアクションを判断できるようにします。

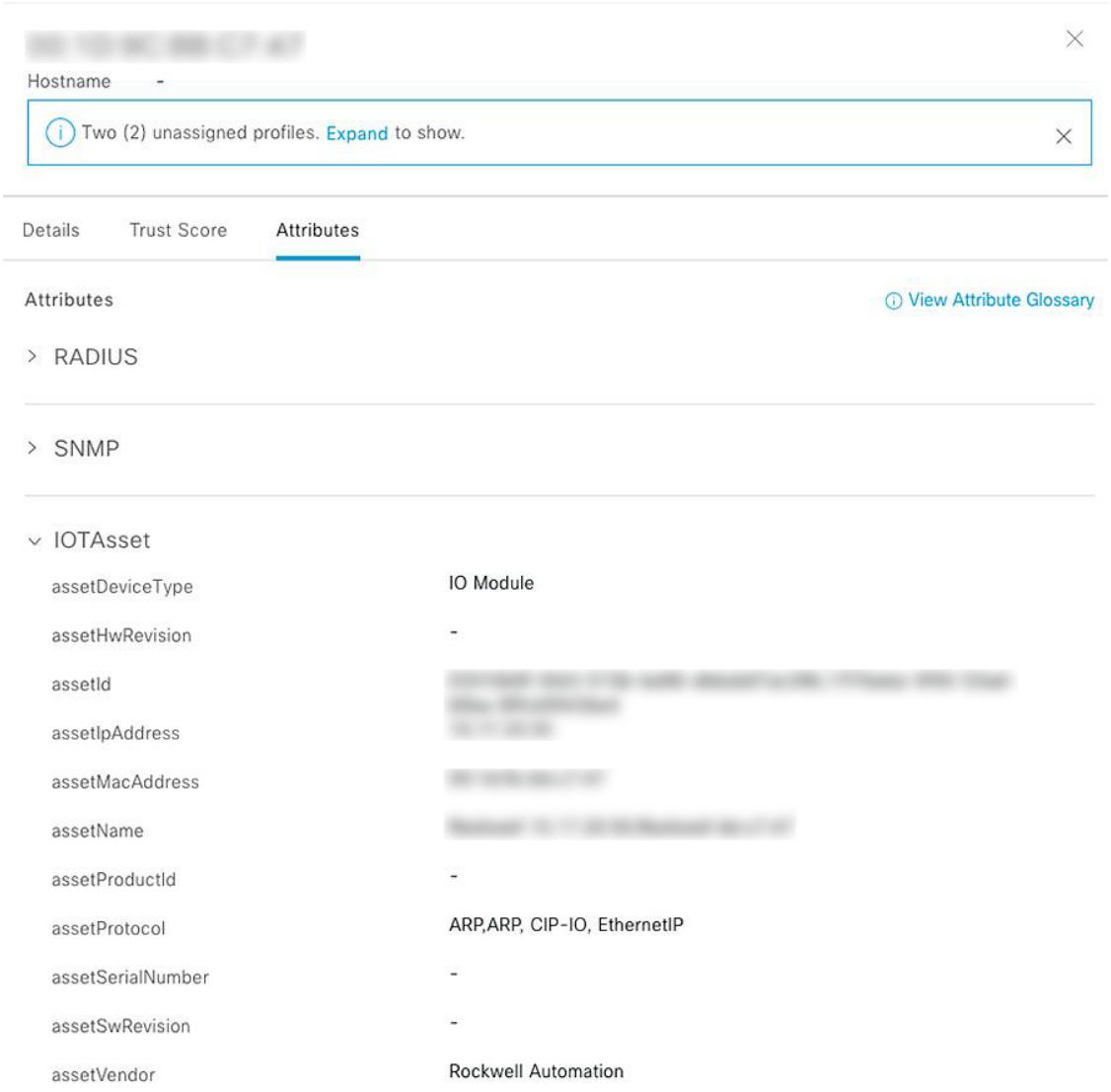
Cisco AI エンドポイント分析 は、Cisco DNA Center とともに実行される追加のアプリケーションです。アプリケーションはカタログサーバーからダウンロードしてインストールでき、その後、Cisco DNA Centerのシステム設定で有効にできます。Cisco DNA Center は、最新のエンドポイント分析モデルをダウンロードするためにクラウドに接続する必要があります。Cisco AI Endpoint Analytics を正常にインストールしたら、メニューアイコン（☰）をクリックして、[Policy] をクリックしてアクセスします。

Cisco AI エンドポイント分析 は、複数の方法を使用して悪意のあるエンドポイントを検出します。また、プロファイルラベルの変更、ネットワークアドレス変換（NAT）モードの検出、同時 MAC アドレス、ポスチャ、認証方式、および機械学習機能を使用して、偽のエンドポイントを識別してフラグを立てます。全体的な信頼スコアは、すべてのエン

ドポイントに対して生成されます。信頼スコアは、複数のリスクスコアの加重平均です。信頼スコアが低いほど、エンドポイントのリスクが高いことを意味します。

さらに、Cisco DNA Center はエンドポイントの分類属性を Cisco ISE と共有します。新しいデバイスがアイデンティティベースの認証を介してオンボーディングされると、製造元とタイプによって自動的に識別されて、適切なグループに追加されます。セキュリティポリシーの定義と適用は、個々のエンドポイントではなくグループに適用した方が簡単です。グループベースのポリシーは、エンドポイントによるセキュリティ侵害などの新たな状況に合わせて簡単に更新でき、ネットワーク全体にグローバルに適用できます。

次の図は、Cisco AI エンドポイント分析 に表示されているエンドポイントの詳細を示しています（特に [IOTAsset] 属性が強調表示されています）。



参照

- Cisco SD-Access Solution Design Guide (Cisco Validated Design)
- Cisco Software-Defined Access for Distributed Campus Prescriptive Deployment Guide
- Cisco Software-Defined Access Compatibility Matrix

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。