ファブリックネットワークのプロビジョニング

Cisco SD-Access ゼロトラスト セキュリティ ソリューション

ネットワークは、外部および内部の脅威から守らなければなりません。Cisco SD-Access は、職場にゼロトラストのセキュリティソリューションを提供します。Cisco SD-Access のゼロトラスト セキュリティ ソリューションは、ネットワーク上のあらゆる場所からすべてのユーザとデバイスへセキュアなアクセスを実現します。

Cisco SD-Access ゼロトラスト セキュリティ ソリューションには、次の機能が含まれています。

- すべてのエンドポイントの識別と検証：接続している各エンドポイントとの初期レベルの信頼を確立します。
- ポリシーとセグメンテーションの確立：エンドポイントとユーザータイプに基づいて、最小限の特権アクセスを保証します。
- エンドポイントの継続的な監視：エンドポイントを継続的に監視してコンプライアンスを確保します。
- 脅威の軽減：非準拠または悪意のある動作を示すエンドポイントを隔離できます。

Cisco SD-Access ゼロトラスト セキュリティ ソリューションは、職場でのネットワーク設定とお使いのサービスに応じて、柔軟にゼロトラストワークプレイスの実現を支援します。ユーザのネットワークへの接続を、ダイナミックなルールとセグメンテーションの自動化を用いて細かに設定できます。

Cisco SD-Access ゼロトラスト セキュリティ ソリューションは、次の機能を使用してネットワーク アクセス ポリシーを自動化します。

- エンドポイントの可視性：エンドポイントを識別してグループ化できます。トラフィックフロー分析を通じて相互作用をマッピングし、アクセスポリシーを定義します。
- トラストモニタリング：エンドポイントの動作を継続的に監視し、脆弱性をスキャンし、持続的なアクセスの信頼性を検証し、不正なエンドポイントや侵害されたエンドポイントを隔離します。
- ネットワーク セグメンテーション：マルチレベルでのセグメンテーションを通じて、グループベースのアクセスポリシーとセキュアなネットワークを確立します。

Cisco SD-Access ゼロトラスト セキュリティ ソリューションで、職場でのネットワーク設定とお使いのサービスに応じて、ゼロトラストワークプレイスを実現するあらゆる方法を模索できます。ネットワークの現状に応じて、ゼロトラストワークプレイスへ移行する最適な道筋を見つけ、それぞれのステップでもたらされる利点を検証できます。

[Zero Trust Overview] ダッシュボード

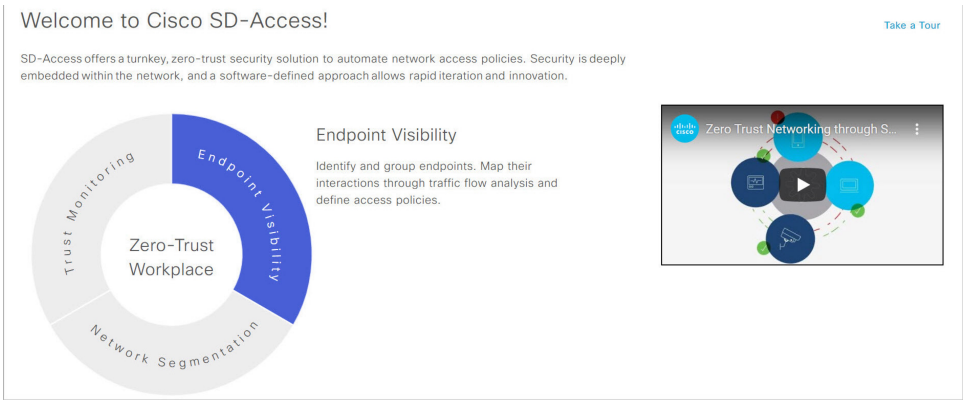
SD-Access の [Zero Trust Overview] ダッシュボードには、Zero Trust ワークプレイスへの移行の概要が示されます。このダッシュボードを表示するには、左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Zero Trust Overview]** の順に選択します。

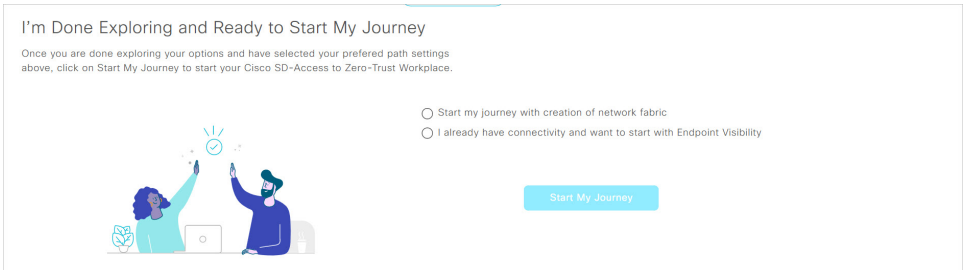
Zero Trust ワークプレイスへの移行には、次のフェーズがあります。

- 0 日目：Zero Trust ワークプレイスジャーニーの開始日。詳細については、[Zero Trust Overview] ダッシュボードの Day-Zero ビュー （3 ページ）を参照してください。
- n 日目：Zero Trust ワークプレイスジャーニーの継続的な監視と設定変更。詳細については、[Zero Trust Overview] ダッシュボードの n 日目ビュー （6 ページ）を参照してください。

[Zero Trust Overview] ダッシュボードの Day-Zero ビュー

SD-Access Zero Trust ワークプレイスへの移行の開始前、[Zero-Trust Overview] ダッシュボードの 0 日目ビューは、次のセクションで構成されます。





- [Welcome to Cisco SD-Access!]：このセクションには、完全な SD-Access Zero Trust ワークプレイスへの複数の道筋を簡潔に示す概要ビデオが用意されています。また、SD-Access Zero Trust ワークプレイスの中心となる次の項目を含む円もあります。

- エンドポイントの可視性
- 信頼のモニタリング
- ネットワークのセグメント化

各項目にカーソルを合わせると、詳細が表示されます。

- [Explore and start your journey to SD-Access Zero-Trust Workplace]：このセクションでは、ネットワーク設定とサービスに基づいて Zero Trust ワークプレイスへのさまざまな道筋を調べて、ネットワークに最適な道筋を特定できます。このセクションは、ネットワーク接続（Network Connectivity）とサービス（Services）のオプション、および道筋に関する詳細を含む円形のジャーニーマップで構成されています。ネットワーク接続とサービスについて選択したオプションに基づいて、ジャーニーマップには、Zero Trust ワークプレイスへの移行に利用できる道筋が表示されます。

  ジャーニーマップの各推奨ステップに関する詳細を表示するには、ジャーニーマップの周囲にある目的のステップにカーソルを合わせます。

- [I'm Done Exploring and Ready to Start My Journey]：道筋を調べて望ましい設定を選択した後、このセクションを使用して、Zero Trust ワークプレイスへの移行を開始できます。

SD-Access Zero Trust ワークプレイスジャーニーの開始

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Zero Trust Overview]** の順に選択します。

ステップ 2 [Explore and start your journey to SD-Access Zero-Trust Workplace] で、次の手順を実行します。

a) [Network Connectivity] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスへの移行でワイヤレスデバイスを使用するには、[With Wireless] を有効にします。
- Zero Trust ワークプレイスへの移行で Cisco Catalyst 9000 シリーズ デバイスを使用するには、[With CAT9K] を有効にします。または、Cisco DNA トラフィック テレメトリ アプライアンスを使用するには、[With Traffic Telemetry Appliance] を有効にします。

b) [Services] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスジャーニーで Cisco Identity Services Engine を使用するには、**[With ISE]** を有効にします。
- Zero Trust ワークプレイスジャーニーで Talos インテリジェンスを使用するには、**[With Talos]** を有効にします。
- Zero Trust ワークプレイスジャーニーでコントローラベースのアプリケーション認識（CBAR）を使用するには、**[With CBAR Enabled]** を有効にします。

c) （任意） ジャーニーマップの各推奨ステップに関する詳細を表示するには、ジャーニーマップの周囲にある目的のステップにカーソルを合わせます。

ステップ 3 **[I'm Done Exploring and Ready to Start My Journey]** で、次のオプションのいずれかを選択します。

- ファブリックネットワークを作成し、Zero Trust ワークプレイスへの移行を開始するには、[Start my journey with creation of network fabric] をクリックします。
- すでにファブリックネットワーク接続があり、エンドポイントの可視性から Zero Trust ワークプレイスへの移行を開始する場合は、[I already have connectivity and want to start with Endpoint Visibility] をクリックします。

ステップ 4 [Start My Journey] をクリックします。

ステップ 5 [Modify Journey Map] ダイアログボックスで、次の手順を実行します。

a) ジャーニーマップの設定を確認します。

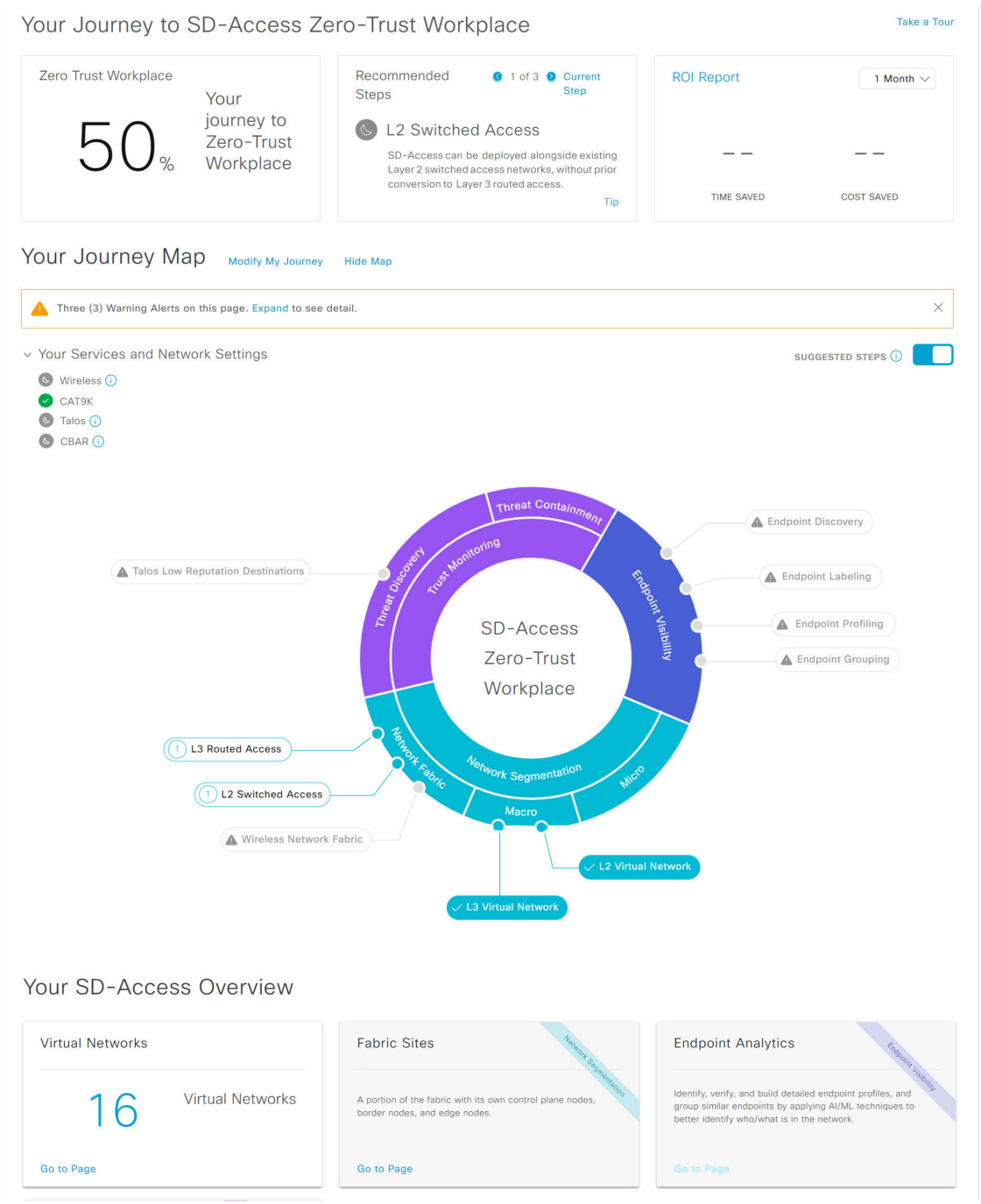
（注）
- Catalyst Center では、ネットワーク用に選択されたサービスが検出されない場合、メッセージが表示されます。
- Catalyst Center では、移行で選択されなかった追加のサービスが検出された場合、メッセージが表示されます。

b) （任意） 選択したサービスをジャーニーマップの設定から削除するには、該当するチェックボックスをオフにします。

c) [確認（Confirm）] をクリックします。

[Zero Trust Overview] ダッシュボードの *n* 日目ビュー

SD-Access Zero Trust ワークプレイスへの移行の開始後、[Zero Trust Overview] ダッシュボードの *n* 日目ビューは、次のセクションで構成されます。



- [Your Journey to SD-Access Zero Trust Workplace]：このセクションは、次のようなダッシュレットで構成されています。
  - [Zero Trust Workplace] ダッシュレットには、Zero Trust ワークプレイスへの移行の進行状況がパーセンテージで表示されます。
  - [Recommended Steps] ダッシュレットには、Zero Trust ワークプレイスへの移行で推奨される次のステップが表示されます。すべてのステップをスクロールするには、矢印

ボタン（ と ）を使用します。このダッシュレットには、一部のステップに関するヒントも表示されます。利用可能な場合は、[Tip] をクリックすると、該当するステップのヒントが表示されます。

- [ROI Report] ダッシュレットには、Zero Trust ワークプレイスへの移行を進めるうえで実行されたステップに基づいて、節約された時間とコストが表示されます。レポートの期間を選択するには、このダッシュレットのドロップダウンを使用します。レポートを表示するには、[ROI Report] をクリックします。

- [Your Journey Map]：このセクションには、Zero Trust ワークプレイスへの移行のネットワーク接続とサービス設定の詳細が表示されます。Zero Trust ワークプレイスへの移行を変更するには、[Modify My Journey] をクリックします。ジャーニーマップを非表示にするには、[Hide Map] をクリックします。

  このセクションには、進めている移行に関する警告アラートが表示されます（アラートがある場合）。アラートの詳細を表示するには、[Expand] をクリックします。選択したサービスがネットワークで現在利用できない場合に、そのサービスを移行から削除するには、該当する [Remove From Journey] オプションをクリックします。ネットワークで現在利用できないサービスを利用可能にするには、該当するハイパーリンクをクリックしてそのサービスを取得します。

  移行用に選択したサービスのリストを表示するには、[Your Services and Network Settings] ドロップダウンを展開します。サービスの横にある アイコンは、そのサービスがネットワークで現在利用可能であることを示しています。サービスの横にある アイコンは、そのサービスがネットワークで現在利用できないことを示しています。 該当する アイコンにカーソルを合わせると、利用できないサービスに関する詳細を含む [Update Needed] ダイアログボックスが表示されます。[Update Needed] ダイアログボックスでは、次の操作を実行できます。

  - 移行からサービスを削除するには、[Remove From Journey] をクリックします。
  - ネットワークで利用できないサービスを取得するには、該当するハイパーリンクをクリックします。

  ジャーニーマップの周囲にあるステップについて推奨される順番を表示するには、[Suggested Steps] トグルボタンを有効にします。

  ジャーニーマップの各ステップに関する詳細を表示するには、ステップにカーソルを合わせます。

  ステップの横にある アイコンは、その構成が未完了であることを示しています。ステップの横にある数字（例： ）は、ジャーニーマップにおける推奨ステップの順番を提案しています。ステップの横にある アイコンは、その構成が完了していることを示しています。

- [Your SD-Access Overview]：このセクションは、Zero Trust ワークプレイスへの移行の各機能領域のダッシュレットで構成されています。関連するウィンドウを開くには、該当する

[Go to Page] オプションをクリックします。各ダッシュレットの右上には、Zero Trust ワークプレイスへの移行の対応する中心項目が示されています。

SD-Access Zero Trust ワークプレイスジャーニーの変更

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Zero Trust Overview]** の順に選択します。

ステップ 2 [Your Journey Map] で、[Modify My Journey] をクリックします。

ステップ 3 [Explore and start your journey to SD-Access Zero-Trust Workplace] で、次の手順を実行します。

a) [Network Connectivity] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスへの移行でワイヤレスデバイスを使用するには、[With Wireless] を有効にします。
- Zero Trust ワークプレイスへの移行で Cisco Catalyst 9000 シリーズ デバイスを使用するには、[With CAT9K] を有効にします。または、Cisco DNA トラフィック テレメトリ アプライアンスを使用するには、[With Traffic Telemetry Appliance] を有効にします。

b) [Services] 設定で、必要なオプションを選択します。

- Zero Trust ワークプレイスジャーニーで Cisco Identity Services Engine を使用するには、**[With ISE]** を有効にします。
- Zero Trust ワークプレイスジャーニーで Talos インテリジェンスを使用するには、**[With Talos]** を有効にします。
- Zero Trust ワークプレイスジャーニーでコントローラベースのアプリケーション認識（CBAR）を使用するには、**[With CBAR Enabled]** を有効にします。

c) （任意） ジャーニーマップの各推奨ステップに関する詳細を表示するには、ジャーニーマップの周囲にある目的のステップにカーソルを合わせます。

ステップ 4 **[I'm Done Exploring and Ready to Start My Journey]** で、次のオプションのいずれかを選択します。

- ファブリックネットワークを作成し、Zero Trust ワークプレイスへの移行を開始するには、[Start my journey with creation of network fabric] をクリックします。
- すでにファブリックネットワーク接続があり、エンドポイントの可視性から Zero Trust ワークプレイスへの移行を開始する場合は、[I already have connectivity and want to start with Endpoint Visibility] をクリックします。

ステップ 5 [Modify My Journey] をクリックします。

ステップ 6 [Modify Journey Map] ダイアログボックスで、次の手順を実行します。

a) ジャーニーマップの設定を確認します。

（注）
- Catalyst Center では、ネットワーク用に選択されたサービスが検出されない場合、メッセージが表示されます。
- Catalyst Center では、移行で選択されなかった追加のサービスが検出された場合、メッセージが表示されます。

b) （任意） 選択したサービスをジャーニーマップの設定から削除するには、該当するチェックボックスをオフにします。
c) [確認（Confirm）] をクリックします。

ファブリックネットワークについて

ファブリックネットワークは、1 つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。ファブリックネットワークを使用すると、仮想ネットワークやユーザーおよびデバイスグループの作成、高度なレポート作成などが可能になります。その他の機能には、アプリケーション認識、トラフィック分析、トラフィックの優先順位付け、最適なパフォーマンスと運用効率のためのステアリングのインテリジェントサービスがあります。

Catalyst Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

ファブリックサイト

ファブリックサイトは、コントロールプレーン、ボーダー、エッジ、ワイヤレスコントローラ、ISE PSN のネットワークデバイスの固有のセットを持つ独立したファブリック領域です。異なるレベルの冗長性とスケールは、DHCP、AAA、DNS、インターネットなどのローカルリソースを含むことにより、サイトごとに設計することができます。

ファブリックサイトは、単一の物理的ロケーション、複数のロケーション、またはロケーションのサブセットのみをカバーすることができます。

- 単一の場所: ブランチ、キャンパスまたはメトロ キャンパス
- 複数の場所: メトロ キャンパス + 複数ブランチ
- ロケーションのサブセット: キャンパス内での構築または領域

Software-Defined Access ファブリックネットワークは、複数のサイトで構成されることがあります。各サイトは、優れた拡張性、復元力、生存性、およびモビリティを備えます。ファブリックサイトの全体的な集約は、多数のエンドポイントに対応し、モジュール方式で（または水平方向に）拡張します。複数のファブリックサイトは、トランジットを使用して相互接続されます。

トランジット

トランジットとは、2 つ以上のファブリックサイトを相互接続したり、ファブリックサイトと外部ネットワーク（インターネット、データセンターなど）を接続するサイトです。トランジットネットワークには 2 つのタイプがあります。

- IP トランジット：通常の IP ネットワークを使用して、外部ネットワークに接続するか 2 つ以上のファブリックサイトを接続します。IP トランジットは、従来型の IP ベース（VRF-LITE、MPLS）ネットワークを利用します。これには、サイト間での VRF と SGT の再マッピングが必要です。
- SD-Access トランジット：LISP/VxLAN のカプセル化を使用して 2 つのファブリックサイトを接続します。SD-Access トランジットエリアは、独自のコントロールプレーンノードを持つがエッジノードやボーダーノードはないファブリックの一部として定義できます。ただし、外部ボーダーを持つファブリックを使用することもできます。SD-Access トランジットを使用すると、エンドツーエンドポリシープレーンは SGT グループタグを使用して維持されます。

ファブリックの準備状況とコンプライアンスのチェック

ファブリックの準備状況チェック

ファブリックの準備状況チェックは、デバイスがファブリックに追加される準備が整っていることを確認するために、デバイス上で実行される事前プロビジョニングチェックのセットです。ファブリックの準備状況チェックは、デバイスのプロビジョニング時に自動的に実行されるようになりました。インターフェイス VLAN とマルチ VRF の設定チェックは、ファブリックの準備状況チェックの一環としては行われません。

ファブリックの準備状況チェックには、次の項目が含まれます。

- 接続チェック：エッジノードからマップサーバーへの接続、エッジノードからボーダーへの接続など、デバイス間で必要な接続を確認します。
- 既存の設定チェック：SD-Access を介してプッシュされる設定と競合する設定がデバイスにあり、それが後でエラーになる可能性がないかを確認します。
- ハードウェアバージョン：デバイスのハードウェアバージョンがサポートされているかどうかを確認します。
- イメージタイプ：サポートされているイメージタイプ（IOS XE、IOS、NXOS、Cisco Controller）を使用してデバイスが実行されているかどうかを確認します。
- ループバック インターフェイス：デバイス上のループバック インターフェイスの設定を確認します。SDA アプリケーションを使用するには、デバイスが番号 0 のループバックインターフェイスを持ち、デバイスに IP アドレスが設定されている必要があります。番号 0 のループバック インターフェイスがないと、Loopback0 がデフォルトでルーティングロケータ（RLOC）として使用されるため、ファブリック プロビジョニング エラーが発生する可能性があります。

- ソフトウェアライセンス：デバイスが適切なソフトウェアライセンスを使用して実行されているかどうかを確認します。
- ソフトウェアバージョン：デバイスが適切なソフトウェアイメージを使用して実行されているかどうかを確認します。

サポートされているソフトウェアバージョンの詳細については、「Cisco SD-Access Hardware and Software Compatibility Matrix」を参照してください。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。問題を修正し、デバイスのプロビジョニング ワークフローを続行できます。

ファブリック コンプライアンス チェック

ファブリック コンプライアンスとは、ファブリック プロビジョニング中に設定されたユーザー インテントに従って動作するデバイスの状態です。ファブリック コンプライアンス チェックは、次の条件に基づいてトリガーされます。

- 有線デバイスの場合は 24 時間ごと、ワイヤレスデバイスの場合は 6 時間ごと。
- 有線デバイスで設定が変更された場合。

  有線デバイスの設定変更によって SNMP トラップがトリガーされ、それによってコンプライアンスチェックがトリガーされます。Catalyst Center サーバーが SNMP サーバーとして設定されていることを確認します。

次のコンプライアンスチェックを実行し、デバイスがファブリックに準拠していることを確認します。

- 仮想ネットワーク：Catalyst Center 上の仮想ネットワークのユーザーインテントの現在の状態に準拠するように、必要な VRF がデバイスに設定されているかどうかを確認します。
- ファブリックロール：デバイスの設定が Catalyst Center のファブリックロールのユーザーインテントに準拠しているかどうかを確認します。
- セグメント：セグメントの VLAN 設定と SVI 設定を確認します。
- ポートの割り当て：VLAN および認証プロファイルのインターフェイス設定を確認します。

SD-Access の新しい自動化

強化された Cisco SD-Access ユーザーインターフェイス（UX）では、シンプルさ、柔軟性、豊富で直感的なコンテキストが統合されています。Cisco SD-Access UX では、ユーザー体験が強化され、次の機能が提供されます。

- 仮想ネットワークやファブリックサイトなどのファブリック要素間の関連付けの明確化
- 強化されたワークフロー

- ファブリック要素とその属性の簡潔なビュー

拡張 Cisco SD-Access UX では、次の機能が提供されます。

- [Fabric Sites]、[Virtual Networks]、および [Transits] を設定するための個別のページ。
- 各ページには、[Overview] ビューと [Table] ビューがあります。
- ページ上のテーブルをカスタマイズして、必要な列のみを表示できます。

  テーブルビューをカスタマイズするには、次の手順を実行します。

  - ウィンドウの右上隅にある歯車アイコンをクリックし、[Table Settings] を編集します。
  - [Table Settings] スライドインペインで、次の操作を実行します。
    - テーブルの密度を調整するには、[Table Appearance] をクリックします。
    - 表示する列を選択するには、[Edit Table Columns] をクリックします。
    - 後で使用できるカスタムビューとして設定を保存するには、[Yes] をクリックします。
    - 変更内容を保存して適用するには、[Apply] をクリックします。

- [Fabric Sites] の [Overview] ページには、ファブリックサイトとファブリックゾーンに関するヒントやインサイトに加えて、進行中のワークフローが表示されます。また、ファブリックサイト、ファブリックゾーン、ファブリックロールのデバイスの数、およびインベントリ内のデバイスの総数も表示されます。
- [Fabric Site] ページには、次の関連要素を設定および表示するためのタブがあります。
  - ファブリック インフラストラクチャ
  - レイヤ 3 仮想ネットワーク
  - レイヤ 2 仮想ネットワーク
  - エニーキャストゲートウェイ
  - ワイヤレス SSID
  - 認証テンプレート
  - ポートの割り当て
- [Virtual Networks] の [Overview] ページには、レイヤ 3 仮想ネットワーク、レイヤ 2 仮想ネットワーク、エニーキャストゲートウェイ、およびエクストラネットポリシーを設定するためのリンクがあります。また、レイヤ 3 仮想ネットワークの数、レイヤ 2 仮想ネットワークの数、エニーキャストゲートウェイの数、およびエクストラネットポリシーの数も表示されます。仮想ネットワークタスクのグラフィック表示により、タスクの進行状況の概要をすばやく確認できます。

- [Transits] の [Overview] ページには、SD-Access トランジット（LISP Pub/Sub および LISP/BGP）、SD-WAN トランジット、および IP ベースのトランジットの数が表示されます。このページには、進行中または展開済みのトランジットタスクがグラフィカルに表示されます。

ファブリック構成の可視化と制御

[Visibility and Control of Configurations] 機能は、計画したネットワーク構成をデバイスに展開する前にセキュリティを強化するソリューションを提供します。優れた可視化機能により、デバイス構成を展開する前にプレビューできます（CLI および NETCONF コマンドを使用）。強化された制御により、IT サービス管理（ITSM）チェックを通じて、信頼できる承認された構成のみをネットワークデバイスにプロビジョニングできます。

この機能の可視性コンポーネントはデフォルトで有効になっているため、デバイス構成をプレビューできます。この機能を無効にするには、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]** ウィンドウで [Configuration Preview] をクリックします。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Enable Visibility and Control of Configurations」[英語] を参照してください。

計画したネットワーク構成のセキュリティを強化するには、この機能の制御コンポーネントが有効になっていることを確認してください。この制御を有効にするには、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]** ウィンドウで [ITSM Approval] をクリックします。詳細については、『*Cisco Catalyst Center Administrator Guide*』の「Enable Visibility and Control of Configurations」[英語] を参照してください。

（注） タスク展開のスケジュール時に次のバナーメッセージが表示される場合、ワークフローで可視性と制御がサポートされます。

このワークフローでは、ネットワーク管理者などのユーザーがネットワークデバイスにワークフローを展開する前に、設定をプレビューできます。ワークフロー設定を構成するには、**[System]** > **[Settings]** > **[Visibility and Control of Configurations]** に移動します。

可視性のみを有効にする場合

[Visibility and Control of Configurations] ウィンドウで、[Configuration Preview] を有効にする場合、デバイス構成はプレビューしてから展開する必要があります。これは、デバイス構成をプレビューするまで、展開の [Now] および [Later] のスケジュールオプションがグレー表示（使用不可）になることを意味します。デバイス構成は、可視性がサポートされているワークフローのセグメントのプロビジョニング中、またはプロビジョニング後に **[Activities]** > **[Tasks]** ウィンドウでプレビューできます。これら 2 つのオプションにより、自分のペースで構成をプレビューできる柔軟性が得られます。

構成プレビューの生成を開始する前に、Catalyst Center によって、保留中の（競合する）操作に関するデバイス構成とデバイスのコンプライアンスがチェックされ、シームレスなプロビ

ジョニング操作が保証されます。保留中のすべての操作とデバイスのコンプライアンスの問題に対処して、ワークフローを続行できるようにしてください。詳細については、ネットワークデバイス プロビジョニングの事前チェックを参照してください。

事前チェックが完了すると、システムは選択したデバイスと設定を準備します。このプロセスには、時間がかかる場合があります。一方、[Exit and Preview Later] をクリックすると、後で [Tasks] ウィンドウで作業項目を確認できます。

[Preview Configuration] ウィンドウで最初にプレビュー構成を生成すると、最初にリストされたデバイスが自動的に選択されて、そのデバイスの構成プレビューが生成されます。このプレビューの生成中に、別のデバイスを選択して構成プレビューを生成できます。

[Preview Configuration] ウィンドウで構成を確認しながら、次の操作を実行できます。

- 左側のペインでデバイスを選択して、デバイスの構成をプレビューします。
- [View by Configuration Source] ドロップダウンリストを使用して、構成プレビューのデータをフィルタ処理します。
- トグルボタンをクリックして、計画された構成と実行中の構成の比較ビューを並べて表示するか、計画された構成のみを表示します。

（注） 並列比較ビューは YANG 構成の表示には対応していません。

- 並列比較ビューでは、一方の構成で1つのコマンドをクリックすると、もう一方の構成で対応するコマンドが強調表示されます。

（注） 次の制限事項に注意してください。

- システムでは、サブレベルのコマンドではなく、第 1 レベルのコマンドに対する並列強調表示のみがサポートされています。
- 構成間で強調表示を並べて表示するには、すべてのコマンドが完全に一致している必要があります。
- 一方の構成で No で始まるコマンドをクリックすると、もう一方の構成で一致をチェックするときに No の部分が無視されます。

- [Search Configuration] フィールドを使用して、表示された構成中の値を検索します。

[Preview Configuration] ウィンドウで構成を確認後、次の操作を実行できます。

- 構成の展開準備ができておらず、後で [Tasks] ウィンドウで確認する場合は、[Exit and Preview Later] をクリックします。

- 作業項目を破棄して現在のアクティビティに戻る場合は、[Discard] をクリックします。作業項目を破棄すると、後で復元することはできません。
- 生成された構成を保持し、他のすべてのリソースを破棄する場合は、[Discard] をクリックします。次に、[Discard] ダイアログボックスで、[Retain generated configs (if any)] チェックボックスをオンにして、[Accept] をクリックします。

  生成された構成を保持し、他のすべてのリソースを破棄すると、すべての構成をプレビューし、生成されていない構成を破棄することを選択したため、[Exit and Preview Later] の代わりに [Exit] が表示されます。

ヒント　構成のプレビューが失敗した場合は、生成された構成を保持し、他のすべてのリソースを破棄して、ユーザーまたはIT管理者が問題を詳細に調査できるようにすることを検討してください。

- リストされているすべてのデバイスの構成を送信する準備ができたら、[Deploy] をクリックします。

  複数のデバイスがある場合は、各デバイスをクリックして構成をプレビューする必要があります。ただし、[Deploy] をクリックすると、すべてのデバイスで構成がプレビューされていない場合でも、構成がすべてのデバイスにプッシュされます。

（注）　構成をプレビューすると、Catalyst Centerによって構成プレビューのスナップショットが作成されます。展開の操作がスケジュールされた後にネットワーク設定またはネットワークプロファイルに変更があった場合、その変更はデバイスのプロビジョニング中に反映されません。

- [Deploy] ではなく [Save Intent] が表示される場合、ワークフロー中に選択したパラメータはすでにデバイスに存在します。これらのパラメータをデータベースに保存するには、[Save Intent] をクリックします。デバイス構成の要件が満たされているため、構成はデバイスにプッシュされません。

可視化と制御を有効にする場合

[Visibility and Control of Configurations] ウィンドウで、[Configuration Preview] と [ITSM Approval] の両方を有効にする場合、計画したネットワーク構成をプレビューしてから IT 管理者に送信して、展開の承認を得る必要があります。計画したネットワーク構成は、可視性と制御がサポートされているワークフローのセグメントのプロビジョニング中、またはプロビジョニング後に **[Activities]** > **[Tasks]** ウィンドウで送信できます。これら 2 つのオプションにより、自分のペースで構成をプレビューできる柔軟性が得られます。

構成プレビューの生成を開始する前に、Catalyst Center によって、保留中の（競合する）操作に関するデバイス構成とデバイスのコンプライアンスがチェックされ、シームレスなプロビ

ジョニング操作が保証されます。保留中のすべての操作とデバイスのコンプライアンスの問題に対処して、ワークフローを続行できるようにしてください。詳細については、ネットワークデバイス プロビジョニングの事前チェックを参照してください。

事前チェックが完了すると、システムは選択したデバイスと設定を準備します。このプロセスには、時間がかかる場合があります。一方、[Exit and Preview Later] をクリックすると、後で [Tasks] ウィンドウで作業項目を確認できます。

[Preview Configuration] ウィンドウで最初にプレビュー構成を生成すると、最初にリストされたデバイスが自動的に選択されて、そのデバイスの構成プレビューが生成されます。このプレビューの生成中に、別のデバイスを選択して構成プレビューを生成できます。

デバイスの準備ができたら、[Preview Configuration] ウィンドウでデバイス構成をプレビューできます。リストの先頭にあるデバイスが自動的に選択され、そのデバイスの構成プレビューが生成されます。このプレビューの生成中に、別のデバイスを選択して構成プレビューを生成できます。

[Preview Configuration] ウィンドウで構成を確認しながら、次の操作を実行できます。

- 左側のペインでデバイスを選択して、デバイスの構成をプレビューします。
- [View by Configuration Source] ドロップダウンリストを使用して、構成プレビューのデータをフィルタ処理します。
- トグルボタンをクリックして、計画された構成と実行中の構成の比較ビューを並べて表示するか、計画された構成のみを表示します。

（注） 並列比較ビューは YANG 構成の表示には対応していません。

- 並列比較ビューでは、一方の構成で1つのコマンドをクリックすると、もう一方の構成で対応するコマンドが強調表示されます。

（注） 次の制限事項に注意してください。

- システムでは、サブレベルのコマンドではなく、第 1 レベルのコマンドに対する並列強調表示のみがサポートされています。
- 構成間で強調表示を並べて表示するには、すべてのコマンドが完全に一致している必要があります。
- 一方の構成で No で始まるコマンドをクリックすると、もう一方の構成で一致をチェックするときに No の部分が無視されます。

- [Search Configuration] フィールドを使用して、表示された構成中の値を検索します。

[Preview Configuration] ウィンドウで構成を確認後、次の操作を実行できます。

- 構成の展開準備ができておらず、後で**[Activities]** > **[Tasks]**ウィンドウで確認する場合は、[Exit and Preview Later] をクリックします。
- 作業項目をすべて破棄して現在のアクティビティに戻る場合は、[Discard] をクリックし、[Discard] ダイアログボックスで [Accept] をクリックします。作業項目を破棄すると、後で復元することはできません。
- 生成された構成を保持し、他のすべてのリソースを破棄する場合は、[Discard] をクリックします。次に、[Discard] ダイアログボックスで、[Retain generated configs (if any)] チェックボックスをオンにして、[Accept] をクリックします。

  生成された構成を保持し、他のすべてのリソースを破棄すると、すべての構成をプレビューし、生成されていない構成を破棄することを選択したため、[Exit and Preview Later] の代わりに [Exit] が表示されます。

ヒント　構成のプレビューが失敗した場合は、生成された構成を保持し、他のすべてのリソースを破棄して、ユーザーまたはIT管理者が問題を詳細に調査できるようにすることを検討してください。

- ITSM 承認を得るために構成を送信する準備ができたら、[Submit for Approval] をクリックします。

  複数のデバイスがある場合は、各デバイスをクリックして構成をプレビューする必要があります。ただし、[Submit for Approval] をクリックすると、すべてのデバイスで構成がプレビューされていない場合でも、構成がすべてのデバイスにプッシュされます。

（注）　構成をプレビューすると、Catalyst Centerによって構成プレビューのスナップショットが作成されます。展開の操作がスケジュールされた後にネットワーク設定またはネットワークプロファイルに変更があった場合、その変更はデバイスのプロビジョニング中に反映されません。

- [Submit for Approval] ではなく [Save Intent] が表示される場合、ワークフロー中に選択したパラメータはすでにデバイスに存在します。これらのパラメータをデータベースに保存するには、[Save Intent] をクリックします。設定はデバイスにプッシュされないため、ITSM の承認は必要ありません。

ファブリックサイトの追加

始める前に

IP デバイストラッキング（IPDT）がすでにサイトに設定されている場合にのみ、ファブリックサイトを作成できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します： **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

結果のウィンドウには、すでに作成されているすべてのファブリックサイトとその情報（正常性スコア、ファブリックゾーン、ファブリックデバイス、ファブリックロール、接続されたトランジットなど）が表形式で表示されます。

選択した列のみを表示するようにテーブルビューをカスタマイズできます。ウィンドウの右上隅にある歯車アイコンを使用して、[Table Settings] を編集し、[Apply] をクリックして変更を適用します。

ステップ 3 [Create Fabric Sites] をクリックします。

または、最初の 3 つの手順の代わりに、メニューアイコンをクリックして選択**[Workflow]** > **[Create Fabric Sites and Fabric Zones]** の順に選択します。

ステップ 4 [Create Fabric Sites] ウィンドウで、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 5 [Fabric Site Location] ウィンドウで、ファブリックゾーンとして追加するエリア、建物、またはフロアを選択します。

ステップ 6 [Wired Endpoint Data Collection] ウィンドウで、[Wired Endpoint Data Collection] チェックボックスがオンになっていることを確認します。

ステップ 7 [Authentication Template] ウィンドウで、次の手順を実行します。

a) ファブリックサイトの認証テンプレートを選択します。

- [Closed Authentication]：認証前のすべてのトラフィック（DHCP、DNS、ARP など）が廃棄されます。
- [Open Authentication]：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- [None]

b) （オプション）[Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass（MAB）] を選択します

- [802.1x Timeout（in seconds）]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。
- [Number of Hosts]：[Unlimited] または [Single] を選択します。
- [BPDU Guard]：このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジ プロトコル データ ユニット（BPDU）ガードを有効または無効にします。
- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択し、ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 8 （オプション）[Fabric Zones] ウィンドウで、次のいずれかのオプションを選択します。

- 後でファブリックゾーンを指定するには、[Setup Fabric Zones Later] をクリックします。
- ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックし、表示されたネットワーク階層からファブリックサイトを選択します。

ステップ 9 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 10 [Fabric Site Creation Scheduler] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、「ファブリック構成の可視化と制御」を参照してください。

ステップ 11 [展開（Deploy）] をクリックします。

[Fabric Site Creation Scheduler] ウィンドウで [Now] または [Later] を選択した場合、デバイス構成はスケジュールされた時刻に展開されます。[Tasks] ウィンドウでタスクを確認できます。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Fabric Site Creation Completed」というメッセージが表示されます。

次に、新しいファブリックサイトを作成するか [Task] ウィンドウでアクティビティを表示するかを選択できます。

ステップ 12 [Fabric Site Creation Scheduler] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、「ファブリック構成の可視化と制御」を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. スライドインペインで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Work Items] ウィンドウで作業項目のステータスを表示できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。設定が承認されると、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

ファブリックサイトの設定

ファブリックサイトを作成したら、ホストがファブリックサイトに接続するためのデバイス、仮想ネットワーク、および認証方式を設定できます。

[Provision] > **[SD-Access]** > **[Fabric Sites]**メニューでファブリックサイトを選択し、次のタブを使用します。

- [Fabric Infrastructure]：デバイスをファブリックロールに割り当てます。
- [Layer 3 Virtual Networks]：ファブリックサイトのレイヤ 3 仮想ネットワークを作成するか、既存のレイヤ 3 仮想ネットワークをファブリックサイトに割り当てます。
- [Layer 2 Virtual Networks]：ファブリックサイトのレイヤ 2 仮想ネットワークを作成するか、既存のレイヤ 2 仮想ネットワークをファブリックサイトに割り当てます。
- [Anycast Gateways]：ファブリックサイトのレイヤ 3 仮想ネットワークのエニーキャストゲートウェイを作成します。
- [Authentication Template] ：ファブリック用の認証テンプレートを選択します。認証テンプレートは、Cisco ISE から取得される一連の定義済みの設定です。

- [Wireless SSIDs] ：ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。ゲスト SSID またはエンタープライズ SSID を選択し、アドレスプールを割り当てることができます。
- [Port Assignment] ：ファブリックサイトに接続するデバイスのタイプに応じて、各ポートに固有の設定を適用します。

これらの各操作については、後のセクションで説明します。

次の制約事項に注意してください。

- Cisco SD-Access 展開環境では、AP、拡張ノード、およびユーザーデバイス（単一のコンピュータまたは単一のコンピュータと電話機など）と、トランクポートを必要とするデバイス（単一サーバーなど）のみがサポートされます。
- 内部スイッチまたは仮想スイッチを備えたサーバーはサポートされていません。
- その他のネットワーキング機器（ハブ、ルータ、スイッチなど）はサポートされていません。

ファブリックへのデバイスの追加

ファブリックサイトを作成すると、そのファブリックサイトにデバイスを追加できます。デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかも指定できます。

IP デバイストラッキング（IPDT）がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。

アクセスロールが割り当てられ、サイトで IPDT を有効にする前にプロビジョニングされたデバイスは、ファブリックに追加できません。このようなデバイスは、ファブリックサイトに追加する前に再プロビジョニングしてください。プロビジョニング ワークフローを調べて、デバイスでの [Deployment of IPDT] のステータスを確認します。

（注）

- ファブリックサイト内のデバイスをコントロールプレーンノードまたはボーダーノードとして指定する手順はオプションです。それらのロールがないデバイスもあります。ただし、各ファブリックサイトには、少なくとも 1 つのコントロール プレーン ノード デバイスと 1 つのボーダーノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大 6 つのコントロール プレーン ノードを追加できます。
- 現在、シスコ ワイヤレス コントローラは 2 つのコントロールプレーンノードとのみ通信します。

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

- **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウに、検出されたデバイスが表示されます。
- ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジビューにデバイスがグレー色で表示されます。
- ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。
- 問題解決の一環としてデバイスの設定を更新する場合は、デバイスで**[Inventory]** > **[Resync]** を実行して、デバイス情報を再同期してください。

（注） ファブリックの準備状況チェックに失敗しても、デバイスのプロビジョニングを続行できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します： **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、デバイスをクリックします。slide-in pane に、次の [Fabric] オプションが表示されます。

オプション	説明
エッジノード	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるボタンをトグルします。
ボーダー ノード	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるボタンをトグルします。
コントロール プレーン ノード	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるボタンをトグルします。

デバイスをファブリックインアボックスとして設定するには、[Control Plane Node]、[Border Node]、および [Edge Node] オプションを選択します。

デバイスをコントロールプレーンおよびボーダーノードとして設定するには、[Control Plane Node] と [Border Node] の両方を選択します。

ステップ 5 [Add] をクリックします。

ステップ 6 展開する前に構成コマンドをプレビューするには、「ファブリック構成の可視化と制御」セクションを参照してください。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付いた状態で表示されます。エラー通知の [詳細の表示（See more details）] をクリックして問題領域を特定し、修正します。

ボーダーノードとしてのデバイスの追加

ファブリックにデバイスを追加する場合、「ファブリックへのデバイスの追加（22ページ）」[英語]で説明したように、コントロールプレーン、ボーダーノード、またはエッジノードとして動作するようにさまざまな組み合わせで追加できます。

この項では、デバイスをボーダーノードとして追加し、次を設定する方法について説明します。

- ボーダーノードタイプ：内部、外部、または内部と外部（ステップ 9 （25 ページ））
- ボーダーノードの優先順位（ステップ 10 （25 ページ））
- ボーダーノードアフィニティ ID（ステップ 10 （25 ページ））
- ボーダーノードのスイッチ仮想インターフェイス（SVI）の TCP MSS 調整値（ステップ 10 （25 ページ））
- AS パスのプリペンド（ステップ 10 （25 ページ））
- 関連するトランジット：SD-Access トランジットまたは IP ベースのトランジット（ステップ 11 （26 ページ））
- レイヤ 3 ハンドオフの IP アドレスプールの割り当て（ステップ 11 （26 ページ））

始める前に

ボーダーノードアフィニティ ID 機能を使用するには、SD-Access LISP Pub/Sub トランジットを作成していることを確認します。詳細については、SD-Access トランジットの作成 （30 ページ）を参照してください。ローカルファブリックサイトに最初のコントロールプレーンノードを追加するときは、必ず LISP Pub/Sub コントロールプレーンプロトコルを選択してください。詳細については、LISP Pub/Sub の設定 （28 ページ）を参照してください。ボーダーノードは、Cisco IOS XE リリース 17.8.1 以降を実行している必要があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ボーダーノードを設定するファブリックサイトを選択します。
ネットワークインベントリ内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジビューでは、ファブリックロールで動作するすべてのデバイスは青色で表示されます。

ステップ 4 [Fabric Infrastructure] タブで、デバイスをクリックします。

ステップ 5 slide-in paneで、[Border Node] トグルボタンをクリックします。

ステップ 6 slide-in pane の結果、[Layer 3 Handoff] タブをクリックします。

ステップ 7 [Enable Layer-3 Handoff] チェックボックスを選択します。

ステップ 8 デバイスの [ローカル自律番号（Local Autonomous Number）] を入力します。

ローカル自律番号がデバイスですでに設定されている場合は、その番号が表示され、このフィールドは無効になります。デバイスですでに設定されているローカル自律番号は変更することができません。

ステップ 9 ボーダーノードのタイプを設定します。デフォルトでは、ボーダーノードは外部専用ボーダーノードとして指定され、外部ルートをインポートせずに、ファブリックサイトへのデフォルトゲートウェイとして機能します。

ボーダーノードは、デフォルトゲートウェイではなく、外部ルートのみをインポートする内部専用ボーダーノードとして設定できます。ボーダーノードには、内部ボーダーおよび外部ボーダーを組み合わせたロールを設定することもできます。

- ボーダーを外部専用ボーダーノードとして指定するには、[Default to all virtual networks] および [Do not import external routes] の両方のチェックボックスをオンにします。
- ボーダーを内部専用ボーダーノードとして指定するには、[Default to all virtual networks] および [Do not import external routes] の両方のチェックボックスをオフにします。
- ボーダーノードを内部および外部ボーダーとして指定するには、[Default to all virtual networks] チェックボックスをオンにします。このノードはファブリックのデフォルトゲートウェイとして機能し、BGP で学習したルートをファブリックサイトもインポートします（[Do not import external routes] チェックボックスはオンにしないでください）。

ボーダーノードタイプの詳細については、『Cisco SD-Access Solution Design Guide』[英語] を参照してください。

ステップ 10 SD-Access トランジットでボーダーノードの優先順位、アフィニティ ID、AS パスのプリペンド、TCP MSS 調整値およびネイティブマルチキャストを設定するには、[Advanced] をクリックして、次を設定します。

a) ボーダーノードの優先順位を変更するには、[Modify Border Priority] チェックボックスをオンにして、新しい優先順位値を入力します。

- 優先度の範囲は、1 ～ 10 です。
- 1 は最高の優先順位を示します。
- 10 は最も低い優先順位を示します。

• デフォルトの優先順位値は 10 です。

ファブリックサイトに 2 つ以上のボーダーノードが設定されている場合、トラフィックは優先順位の高いボーダーノードを介してルーティングされます。優先順位値が同じ場合、トラフィックはボーダーノード間で負荷分散されます。

b) （オプション）ボーダーノードアフィニティ ID を設定するには、[Modify Border Node Affinity-ID] チェックボックスをオンにして、次のフィールドに値を入力します。

• [Affinity-ID Prime]：相対的な prime 値が小さいほど、優先順位が高くなります。

• [Affinity-ID Decider]：2 つのボーダーノードの prime 値が同じ場合、ボーダーノードの優先順位を決定するタイブレーカーとして decider 値が使用されます。

アフィニティ ID は、他の利用可能なすべてのボーダーノードから受信した値の中でこのボーダーノードの値を考慮した相対値です。アフィニティ ID の相対値が低いほど、宛先ボーダーノードの優先順位が高くなります。デフォルトでは、アフィニティ ID 値はプロビジョニングされません。

受信したアフィニティ ID が等しい場合、優先順位を使用してボーダーノードの優先順位が決まります。

（注） アフィニティ ID 機能を適切に機能させるために、同じ SD-Access トランジットに接続されているすべてのボーダーノードにアフィニティ ID を設定していることを確認します。

c) BGP AS_PATH リストに付加する AS パスの数を定義するには、[AS Path Prepending] チェックボックスをオンにして、1 ～ 10 の値を入力します。

AS パスのプリペンドは、入力境界の選択に役立ちます。

d) レイヤ 3 ハンドオフ SVI の TCP 最大セグメントサイズ（MSS）値をカスタマイズするには、[TCP MSS Adjustment] チェックボックスをオンにして、必要な値を入力します。

[TCP MSS Adjustment] には 500 ～ 1440 の範囲内で値を入力できます。[TCP MSS Adjustment] の値は、IPv4 と IPv6 の両方の TCP セッションに適用されます。

（注） 境界デバイスがレイヤ 3 ハンドオフ用に設定されている場合にのみ、TCP MSS 値をカスタマイズできます。

e) （オプション）SD-Access トランジットに接続されている複数のサイトでネイティブマルチキャストを設定するには、[Enable Multicast over SD-Access Transit] チェックボックスをオンにします。

（注） SD-Access トランジットでも同様のチェックボックスを有効にしてください。

[Activities] > **[Audit Logs]** でボーダーノードの優先順位とアフィニティ ID の展開ログを表示できます。

ステップ 11 [Add Transit Site] にカーソルを合わせ、このボーダーノードに接続するトランジットを選択します。

[IP:BGP IP TRANSIT] では、仮想ネットワークの IP アドレスの割り当てを自動化するか、仮想ネットワークのローカルおよびピア IP アドレスを手動で割り当てるかを選択できます。両方を行うことはできません。

a) （オプション）Catalyst Center でボーダーノードとピア間の接続に IP アドレスを割り当てることができるようにするには、[Select IP Address Pool] ドロップダウンリストから IP アドレスプールを選択します。

（注） ローカルおよびピア IP アドレスを手動で割り当てた場合は、[Select IP Address Pool] が無効になります。

b) ハンドオフインターフェイスを設定するには、[Add External Interface] をクリックします。

表示されるウィンドウで、次の手順を実行します。

1. [External Interface] ドロップダウンメニューからインターフェイスを選択します。
2. [Remote AS Number] は、選択したトランジットまたはピアネットワークから自動的に導出されます。
3. （オプション）[Interface Description] フィールドに、インターフェイスの説明を入力します。
4. （オプション）[Actions] ドロップダウンリストから、[Enable All] または [Disable All] を選択します。
5. 仮想ネットワークの [Enable Layer 3 Handoff] トグルボタンをクリックします。この仮想ネットワークは、ボーダーノードによって BGP 経由でピアにアドバタイズされます。1 つ、複数、またはすべての仮想ネットワークを選択できます。
6. [VLAN ID] フィールドに、選択した仮想ネットワークの VLAN ID を入力します。
7. （オプション）選択した仮想ネットワークの IPv4 および IPv6 の [Local IP Address] および [Peer IP Address] を手動で割り当てるには、IP アドレスとサブネットマスクを CIDR 表記（IP アドレス/プレフィックス長）で入力します。

   （注） すでに IP プールを選択している場合、[Local IP Address] および [Peer IP Address] フィールドは無効になっています。

8. **[Save]** をクリックします。

c) [Add] をクリックします。

ステップ 12 （オプション）ファブリックサイトに従来のネットワークを接続している場合、または従来のネットワークから SD-Access ネットワークに移行する場合にのみ、この手順を実行します。[Layer 2 Handoff] タブをクリックします。

仮想ネットワークのリストと、各仮想ネットワークの IP アドレスプールの数が表示されます。

a) ハンドオフする仮想ネットワークをクリックします。

仮想ネットワークに存在する IP アドレスプールのリストと、従来のネットワークに接続できるインターフェイスのリストが表示されます。

b) [External Interface] ドロップダウンから、インターフェイスを選択します。
c) [Interface Description] に、オプションでインターフェイスの説明を入力します。
d) [External VLAN] フィールドに、ファブリックを拡張する必要がある VLAN 番号を入力します。

仮想ネットワークは単一のインターフェイスまたは複数のインターフェイスでハンドオフできます。セグメントのレイヤ 2 ハンドオフを 2 つの異なるデバイスで実行することもできます。いずれの場合も、ネットワークにループが形成されていないことを確認します。

ボーダーノードは従来のネットワークに接続されているため、ブロードキャストストーム、レイヤ 2 ループ、およびレイヤ 2 スイッチド アクセス ネットワークで発生する可能性のあるスパニングツリーの問題の影響を受けます。コントロールプレーンのノードサービスまたは他の外部ネットワークに接続するボーダーノードサービスの中断を防ぐため、ボーダーノードはレイヤ 2 ハンドオフ機能専用にすべきであり、他のファブリックロールまたはサービスと同じ場所に配置しないでください。

e) **[Save]** をクリックします。

ステップ 13 [Add] をクリックして設定を保存します。

ステップ 14 [Fabric Infrastructure] タブで [Deploy] をクリックして、ボーダーノードを設定します。

[Visibility and Control of Configurations] の設定に応じて、展開に使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、「ファブリック構成の可視化と制御」を参照してください。

LISP Pub/Sub の設定

最初のコントロールプレーンをファブリックに追加する場合にのみ、ファブリックサイトで LISP Pub/Sub を設定できます。

始める前に

ファブリックデバイスが Cisco IOS XE リリース 17.6.1 以降で動作することを確認します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します： **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリックサイトを選択します。

インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 [Fabric Infrastructure] タブの [List] ビューで、コントロールプレーンとして設定するデバイスをクリックします。

ステップ 5 スライドインペインで、[Control Plane Node] トグルボタンを有効にして、このプレーンを設定します。

ステップ 6 [Configure Control Plane] スライドインペインで、[LISP Pub/Sub] ルート配布プロトコルを選択し、[Add] をクリックします。

ステップ 7 [Add]をクリックします。

ステップ 8 [展開（Deploy）] をクリックします。

ステップ 9 [Modify Fabric] ウィンドウで、操作をスケジュールし、[Apply] をクリックします。

ファブリックサイトの LISP Pub/Sub の設定を確認するには、[SITE SUMMARY] ウィンドウで LISP Pub/Sub のステータスを確認します。

IP トランジットの作成

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します： **[Provision]** > **[Transits]**.

ステップ 2 [Create Transit] をクリックします。

ステップ 3 [Transit] スライドインペインで、トランジットネットワークの名前を入力します。

ステップ 4 [IP-Based] を選択します。
ルーティング プロトコルが BGP にデフォルトとして設定されます。

ステップ 5 トランジットネットワークの自律システム番号（ASN）を入力します。

ステップ 6 [Save] をクリックします。

ステップ 7 [Transit] スライドインペインで、[Visibility and Control of Configurations] の設定に応じて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

ステップ 8 [Apply] をクリックして IP トランジットを作成します。

ステップ 9 [Transit] スライドインペインで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて次の手順を実行します。

1. デバイス構成を確認します。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。
4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

SD-Access トランジットの作成

SD-Access トランジットを追加するには、次の手順に従います。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します： **[Provision]** > **[Transits]**.

ステップ 2 [Create Transit] をクリックします。

ステップ 3 [Transit] スライドインペインで、トランジットの名前を入力します。

ステップ 4 SD-Access の [Transit Type] を選択します。

LISP Pub/Sub コントロールプレーンのないファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP/BGP)] を選択してください。

LISP Pub/Sub コントロールプレーンのあるファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP Pub/Sub)] を選択してください。

[SD-Access (LISP Pub/Sub)] トランジットを他の Catalyst Center クラスタと共有する場合は、[Yes, Share] を選択してください。共有しない場合は、[No, keep it local] を選択してください。

（注） [Yes, Share] オプションは、**複数の Cisco DNA Center** パッケージがすべての Catalyst Center クラスタにインストールされている場合にのみ表示されます。

ステップ 5 ドロップダウンリストから [Transit Control Plane Node Site] を選択します。少なくとも 1 つのトランジット マップ サーバーを選択します。

ステップ 6 ドロップダウンリストからトランジットネットワークの [Transit Control Plane Node] を選択します。

ステップ 7 （オプション）追加のマップサーバーを構成するには、プラスアイコン（+）をクリックし、ステップ 5（30 ページ）とステップ 6 （30 ページ）を繰り返します。

ステップ 8 （オプション）LISP Pub/Sub ベースの SD-Access トランジットを介してネイティブ マルチキャストを構成するには、[Advanced Attributes] をクリックします。

[Advanced Attributes] スライドインペインで、[Multicast Over SD-Access Transit] チェックボックスをオンにします。

[Advanced Attributes] スライドインペインで、[Save] をクリックします。

（注） SD-Access トランジットに接続されている複数のサイトでネイティブマルチキャストを完全に設定するには、ボーダーノードで SD-Access トランジットを介するマルチキャストを有効にする必要があります。

ステップ 9 [保存（Save）] をクリックして、設定を保存します。

トランジットを作成すると、[Transits] ウィンドウに、新しく作成されたトランジットとその属性が表示されます。

（注） LISP/BGP コントロールプレーンを使用するファブリックサイトに [SD-Access (LISP Pub/Sub)] トランジットを追加することはできません。LISP Pub/Sub コントロールプレーンを使用するファブリックサイトに [SD-Access (LISP/BGP)] トランジットを追加することはできません。

ステップ 10 [Transit] スライドインペインで、[Visibility and Control of Configurations] の設定に応じて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

ステップ 11 [Transit] スライドインペインで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて次の手順を実行します。

1. デバイス構成を確認します。
2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

次のタスク

ファブリックサイトを SD-Access トランジットと相互接続するには、トランジットをボーダーノードに追加します。

認証テンプレートの選択

ファブリックサイト内のすべてのデバイスに適用される認証テンプレートを設定できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します： **[Provision]** > **[Fabric Sites]**.

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [fabric site] をクリックします。

ステップ 4 [Authentication Template] タブをクリックします。

ステップ 5 [Select Authentication Template] で、サイトの認証テンプレートを選択します。

- **オープン認証（Open Authentication）**：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。
- **クローズ認証（Closed Authentication）**：認証前のすべてのトラフィック（DHCP、DNS、ARP を含む）は廃棄されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- [None]

選択した認証テンプレートの設定を編集して、サイト固有の認証要件に対応することができます。

サイトレベルの認証を変更する前に、マクロまたは Autoconf を使用してアクセスポイントがオンボーディングされ、かつまだ定期的な再同期が行われていないファブリックデバイスがあれば再同期する必要があります。

ステップ 6 （オプション）選択した認証方式の設定を編集するには、[Edit] をクリックします。

a) スライドインペインで、次の手順を実行します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass（MAB）] を選択します
- [802.1x Timeout（in seconds）]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。

  Wake on LAN（WoL）は、次のシナリオでのみサポートされます。

  - 送信元（WoL イニシエータ）と宛先（スリープ状態のホスト）の両方が同じサブネット内にあり、レイヤ 2 フラッディングが有効になっている。
  - 送信元が、SD-Access ファブリックの外部にあるが、レイヤ 3 ハンドオフを介してファブリックに接続されているネットワーク内にあり、宛先が、IP ダイレクトブロードキャストが有効になっている SD-Access サブネット内にある。

  （注） 次のトポロジは、Wake on LAN をサポートしていません。

  - WoL イニシエータとスリープ状態のホストが、同じレイヤ 3 仮想ネットワーク内の異なるサブネット上にある。
  - WoL イニシエータが、SD-Access トランジットを介してスリープ状態のホストにルーティングする。

- [Number of Hosts]：[Unlimited] または [Single] を選択します。

  （注） [Number of Hosts] は、1 つのポートに接続できるデータホストの数を指定します。[Single] の場合、ポートでは 1 つのデータクライアントのみを保持できます。[Unlimited] の場合、ポートで複数のデータクライアントと 1 つの音声クライアントを保持できます。

- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

b) **[Save]** をクリックします。

保存された変更は、認証テンプレートが編集されているサイトにのみ適用されます。

ステップ 7 [展開（Deploy）] をクリックします。
ヒットレス認証変更機能を使用すると、ファブリックからデバイスを削除することなく、1 つの認証方式から別の認証方式に切り替えることができます。

ファブリックサイト内のポートの設定

[Port Assignment] タブで、ファブリックサイトの各アクセスデバイスを設定できます。デバイスの各ポートのネットワーク動作設定を指定できます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ポート割り当てを設定するファブリックサイトをクリックします。

ステップ 4 [Port Assignment] タブをクリックします。

ステップ 5 ファブリックデバイスのリストからデバイスを選択し、[Configure Port Assignments] をクリックします。

ステップ 6 [Connected Device Type] slide-in paneで、接続されているデバイスのタイプをクリックします。

オプション	説明
ユーザーデバイスとエンドポイント	ホストデバイスに接続するポートを設定します。
アクセス ポイント（AP）	アクセスポイントに接続するポートを設定します。
トランク	ポートをトランク ポートとして設定します。
サプリカントベースの拡張ノード	サプリカントベースの拡張ノードを受信するようにポートを設定します。

- ホストデバイスを接続するには、[User Devices and Endpoints] をクリックし、次の手順を実行します。
  1. [VLAN Name (Data)] ドロップダウンリストからデータの VLAN 名を選択します。
  2. [Security Group] ドロップダウンリストからセキュリティグループを選択します。

     セキュリティグループは、[None] 認証テンプレートでのみサポートされます。
  3. [VLAN Name (Voice)] ドロップダウンリストから音声の VLAN 名を選択します。
  4. [Authentication Template] ドロップダウンリストから認証タイプを選択します。
  5. コネクテッドデバイスに関する [Description] を入力します。
- アクセスポイントを接続するには、[Access Point] をクリックし、次の手順を実行します。
  1. [VLAN Name (Data)] ドロップダウンリストから VLAN 名を選択します。
  2. [Authentication Template] ドロップダウンリストから認証タイプを選択します。
  3. コネクテッドデバイスに関する [Description] を入力します。
- サプリカントベースの拡張ノードデバイスを接続するには、[Supplicant-Based Extended Node] をクリックします。
- トランクポートを接続するには、[Trunk] をクリックし、ポートの説明を [Description] に入力します。

ステップ 7 [Deploy Port Assignment] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。

- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

ステップ 8 [Deploy] をクリックしてポート割り当てを設定します。

ファブリックネットワークのワイヤレス SSID の設定

始める前に

ワイヤレスデバイスをファブリックサイトに追加してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [fabric site] をクリックします。

ステップ 4 [Wireless SSID] タブをクリックし、ホストがアクセス可能なネットワーク内のワイヤレス SSID を指定します。

ステップ 5 [Choose Pool] ドロップダウンリストから、SSID 用に予約されている IP アドレスプールを選択します。

このドロップダウンリストでは、レイヤ 3 およびレイヤ 2 セグメント用に設定されたワイヤレス IP アドレスプールを選択できます。

ステップ 6 [Assign SGT] ドロップダウンリストから、SSID のセキュリティグループを選択します。

ステップ 7 SSID でワイヤレスマルチキャストを有効にするには、[Enable Wireless Multicast] チェックボックスをオンにします。

ステップ 8 [展開（Deploy）] をクリックします。

ステップ 9 [Modify SSID Table] slide-in paneで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

ステップ 10 （任意） [Task Name] フィールドで、タスク名を更新します。

ステップ 11 [Apply] をクリックします。

[Modify SSID Table] slide-in paneで [Now] または [Later] を選択した場合、デバイス構成はスケジュールされた時刻に展開されます。[Tasks] ウィンドウでタスクを確認できます。

ステップ 12 [Modify SSID Table] slide-in paneで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

ファブリックでのワイヤレス メッシュ アクセス ポイントの設定

Cisco DNA Center リリース 2.3.7 以降、SD-Access ファブリックでワイヤレスメッシュ AP をオンボードできます。メッシュ AP は、ネットワーク要件に応じて、メッシュアクセスポイント（MAP）またはルートアクセスポイント（RAP）としてプロビジョニングできます。詳細については、「ワイヤレス メッシュ ネットワークについて」を参照してください。

始める前に

- 認証済みのアクセスポイント（AP）のリストを定義します。シスコ ワイヤレス コントローラのプロビジョニング中に AP 認証リストを選択できます。シスコ ワイヤレス コントローラは、AP 認証リストに含まれている AP からの要求にのみ応答します。認証され

た AP のリストを作成する方法については、「AP 認証リストの作成」を参照してください。

- メッシュ AP を管理およびプロビジョニングするための AP プロファイルを定義します。「Cisco IOS XE デバイスの AP プロファイルのメッシュ設定を行う」を参照してください。

ステップ 1 メッシュネットワークモードで使用する既存の AP がある場合は、最初に [Configure Access Point] ワークフローを使用して AP モードを [Bridge] に変更する必要があります。詳細については、「AP の設定」を参照してください。

ステップ 2 メッシュ AP をオンボードするには、AP 認証リストを使用してファブリック対応ワイヤレスコントローラをプロビジョニングします。「Cisco Catalyst 9800 シリーズワイヤレスコントローラのプロビジョニング」を参照してください。

次のタスク

AP をオンボードし、MAP または RAP のロールでプロビジョニングします。

仮想ネットワーク

仮想ネットワークは、共通物理ネットワークインフラストラクチャ内でトラフィックをセグメント化するために使用されるオーバーレイです。これは「マクロセグメンテーション」とも呼ばれます。レイヤー 2 仮想ネットワークはスイッチドトラフィックをセグメント化し、レイヤー 3 仮想ネットワークはルーテッドトラフィックをセグメント化します。Cisco SD-Access ファブリックに接続されている各エンドポイントは、静的エッジポート構成または Cisco Identity Service Engine からの動的ポリシーに基づいて、特定の仮想ネットワークに割り当てられます。仮想ネットワークのエンドポイントは、マイクロセグメンテーションポリシーによって明示的にブロックされていない限り、相互に通信できます。異なる仮想ネットワークにまたがるエンドポイントは、デフォルトでは、相互に通信できません。仮想ネットワーク間トラフィックの場合は、接続ポリシーを Cisco SD-Access ファブリックの外部（フュージョンデバイス上など）で実装する必要があります。

仮想ネットワークの一般的な使用例は、社内エンドポイントとビルディング管理システムの両方を含むオフィスビルです。社内エンドポイントは、照明、暖房、換気、空調などのビルディングシステムとは別にセグメント化する必要があります。このようなシナリオでは、ネットワーク管理者は、マクロセグメンテーションを使用して 2 つ以上の仮想ネットワークで社内エンドポイントとビルディングシステムをセグメント化することにより、ビルディングシステムと社内エンドポイントの間の不正アクセスをブロックできます。

レイヤ 3 仮想ネットワークは、複数のファブリックサイトやネットワークドメイン（ワイヤレス LAN、キャンパス LAN、および WAN）にまたがる場合があります。レイヤ 2 仮想ネットワークは、単一のファブリックサイト内に存在します。

レイヤ 3 仮想ネットワークの作成

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Workflows]** > **[Create Layer 3 Virtual Networks]** の順に選択します。

または、**[Provision]** > **[Virtual Networks]** で [Layer 3] タブに移動し、[Create Layer 3 Virtual Networks] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 3 [Layer 3 Virtual Networks] ウィンドウで、次の手順を実行します。

a) [Layer 3 Virtual Network name] フィールドに、レイヤー 3 仮想ネットワークの名前を入力します。

b) （任意）別のレイヤー 3 仮想ネットワークを作成するには、プラスアイコン（⊕）をクリックし、レイヤー 3 仮想ネットワークの名前を入力します。

ステップ 4 [Fabric Sites and Fabric Zones（Optional）] ウィンドウで、次のように構成します。

a) [Select Fabric Sites] をクリックして、ファブリックサイトを選択します。

仮想ネットワークは複数のファブリックサイトに割り当てることができます。ファブリックサイトを選択するには、次のいずれかを実行します。

- 必要なファブリックサイトの横にあるプラスアイコン（＋）をクリックします。
- ファブリックサイト名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックサイトを選択するには、**Shift**キーを押しながらファブリックサイト名をクリックし、[Add Selected] をクリックします。

- すべてのファブリックサイトを選択するには、[Add All] をクリックします。

作成したすべてのレイヤ 3 仮想ネットワークについて、この関連付けを繰り返します。

b) [**Assign**] をクリックします。

c) [Select Fabric Zones] をクリックして、次のいずれかを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコン（＋）をクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

d) [**Assign**] をクリックします。

ステップ 5 [Summary] ウィンドウで、レイヤー 3 仮想ネットワークの設定を確認します。

ステップ 6 [Deploy Layer 3 Virtual Networks] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

ステップ 7 [Deploy Layer 3 Virtual Networks] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、「ファブリック構成の可視化と制御」を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。
4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

レイヤ 2 仮想ネットワークの作成

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Workflows]** > **[Create Layer 2 Virtual Networks]** の順に選択します。

または、**[Provision]** > **[Virtual Networks]** で [Layer 2] タブに移動し、[Create Layer 2 Virtual Networks] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 3 [Configuration Attributes] ウィンドウで、以下を構成します。

a) [VLAN Name] フィールドに、VLAN 名を入力します。
b) [VLAN ID] フィールドに、VLAN ID を入力します。有効な VLAN ID の範囲は 2 ～ 4093 です。

（注） 1002 ～ 1005 および 2046 の VLAN ID は、予約済みの VLAN ID です。

c) [Traffic Type] エリアから、[Data] または [Voice] を選択します。
d) [Fabric-Enabled Wireless] チェックボックスをオンにして、ワイヤレスを有効にします。
レイヤー 2 仮想ネットワークでは、[Layer 2 Flooding] チェックボックスがデフォルトで有効になっています。
e) 別のレイヤー 2 仮想ネットワークを追加するには、プラス アイコン（⊕）をクリックして、3.a （40 ページ）～3.d （40 ページ）までを繰り返します。

ステップ 4 [Fabric Sites and Advanced Attributes] ウィンドウで、[Fabric Zones] ドロップダウンからレイヤー 2 仮想ネットワークのファブリックサイトを選択します。必要に応じて、このレイヤー 2 仮想ネットワークに関連付けるファブリックゾーンを選択するには、次の手順を実行します。

a) [Select Fabric Zones] をクリックして、次のいずれかを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコン（＋）をクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

作成したすべてのレイヤ 2 仮想ネットワークについて、この関連付けを繰り返します。

ステップ 5 （オプション）[Fabric Sites and Advanced Attributes] ウィンドウで、[Advanced Attributes] トグルボタンをクリックして、レイヤ 3 仮想ネットワークをこのレイヤ 2 仮想ネットワークに関連付けます。

ステップ 6 [Summary] ウィンドウで、レイヤ 2 仮想ネットワークの設定を確認します。

ステップ 7 [Create Layer2 Virtual Networks] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

ステップ 8 [Create Layer 2 Virtual Networks] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、「ファブリック構成の可視化と制御」を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

成功メッセージが表示された後にゲートウェイの作成を確認するには、[View Anycast Gateway] をクリックします。

ステップ 9 成功メッセージが表示された後にゲートウェイの作成を確認するには、[View Anycast Gateway] をクリックします。

[Virtual Networks] ウィンドウの [Anycast Gateway] タブに、ファブリックに含まれるすべてのエニーキャストゲートウェイの詳細が表示されます。

ファブリックサイトへのレイヤ 3 仮想ネットワークの関連付け

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Layer 3 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルで作成されたすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ 3 [Layer 3] タブで、ファブリックサイトの関連付けを編集したいレイヤ 3 仮想ネットワークの横にあるチェックボックスをオンにします。

（注） 最大 5 つのレイヤ 3 仮想ネットワークを編集できます。

ステップ 4 [More actions] にカーソルを合わせ、[Edit Fabric Site and Fabric Zone Associations] を選択します。

ステップ 5 [Fabric Sites and Fabric Zones（Optional）] ウィンドウで、次のように構成します。

a) [Select Fabric Sites] をクリックして、ファブリックサイトを選択します。

仮想ネットワークは複数のファブリックサイトに割り当てることができます。ファブリックサイトを選択するには、次のいずれかを実行します。

- 必要なファブリックサイトの横にあるプラスアイコン（＋）をクリックします。
- ファブリックサイト名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックサイトを選択するには、**Shift**キーを押しながらファブリックサイト名をクリックし、[Add Selected] をクリックします。

- すべてのファブリックサイトを選択するには、[Add All] をクリックします。

すべてのレイヤー 3 仮想ネットワークについて、この関連付けを繰り返します。

b) [**Assign**] をクリックします。

c) [Select Fabric Zones] をクリックして、次のいずれかを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコン（＋）をクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

d) [**Assign**] をクリックします。

ステップ 6 [Summary] ウィンドウで、レイヤー 3 仮想ネットワークサイトを確認します。

ステップ 7 [Update Layer 3 Virtual Networks] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

[Update] をクリックして、選択したサイトにレイヤ 3 仮想ネットワークを割り当てます。

ステップ 8 [Update Layer 3 Virtual Networks] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。

詳細については、「ファブリック構成の可視化と制御」を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

エニーキャストゲートウェイの作成

始める前に

レイヤ 3 仮想ネットワークが作成されていることを確認します。詳細については、レイヤ 3 仮想ネットワークの作成 （38 ページ）を参照してください。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Anycast Gateways] の数を示す数字をクリックします。

ステップ 3 [Anycast Gateway] タブで、[Create Anycast Gateway] をクリックします。

または、メニューアイコンをクリックして**[Workflows]** > **[Create Anycast Gateways]**の順に選択します。

ステップ 4 タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

ステップ 5 [Layer 3 Virtual Networks] ウィンドウで、ゲートウェイを追加する仮想ネットワークを 1 つ以上選択します。

- 必要なファブリックサイトの横にあるプラスアイコン（＋）をクリックします。
- ファブリックサイト名をクリックし、[Add Selected] をクリックします。

  （注） 複数のファブリックサイトを選択するには、**Shift**キーを押しながらファブリックサイト名をクリックし、[Add Selected] をクリックします。

- すべてのファブリックサイトを選択するには、[Add All] をクリックします。

ステップ 6 [Configuration Attributes] ウィンドウの左側のペインで、エニーキャストゲートウェイを作成するレイヤー 3 仮想ネットワークを選択し、次の手順を実行します。

a) [IP Address Pool] ドロップダウンリストから、IP アドレスプールを選択します。

b) INFRA_VN に対して、次の手順を実行します。

- [Pool Type] ドロップダウンリストから [AP] または [Extended Node] を選択します。
- [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] チェックボックスをオンにします。
- [VLAN ID] に仮想ネットワークのカスタム VLAN ID を入力します。
- サプリカントベースの拡張ノードをオンボードするには、[Supplicant-Based Extended Node Onboarding] チェックボックスをオンにします。

（注） このチェックボックスは、[Extended Node] プールタイプを選択した場合にのみアクティブになります。

c) IP ダイレクトブロードキャスト機能を有効にするには、[IP-Directed Broadcast] チェックボックスをオンにします。

（注）
- ダイレクトブロードキャストを有効にすると、Catalyst Centerのレイヤ 2 フラッディングが自動的に有効になります。
- ルータおよび Cisco Nexus 7000 シリーズ スイッチは、ダイレクトブロードキャストをサポートしていません。
- ダイレクトブロードキャストを有効にする前に、アンダーレイマルチキャストが有効になっていることを確認してください。

d) サブネット内ルーティングを有効にするには、[Intra-Subnet Routing] チェックボックスをオンにします。

（注） イントラサブネット ルーティングを有効にすると、Catalyst Centerの [Fabric-Enabled Wireless] チェックボックスと [Layer 2 Flooding] チェックボックスが自動的に無効になります。

e) エニーキャストゲートウェイの TCP 最大セグメントサイズ（MSS）値をカスタマイズするには、[TCP MSS Adjustment] チェックボックスをオンにして、必要な値を入力します。

[TCP MSS Adjustment] には 500 ～ 1440 の範囲内で値を入力できます。[TCP MSS Adjustment] の値は、IPv4 と IPv6 の両方の TCP セッションに適用されます。

[TCP MSS Adjustment] の値は、すべてのエニーキャスト ゲートウェイ スイッチ仮想インターフェイス（SVI）に適用されます。

f) [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] チェックボックスをオンにします。

g) [VLAN ID] に仮想ネットワークのカスタム VLAN ID を入力します。

（注）
- VLAN ID 1、1002 ー 1005、2046、および 4095 は予約済みで、使用できません。
- カスタム VLAN ID を指定しない場合は、Catalyst Center が 1021 ー 2020 の範囲の VLAN ID を生成します。

h) [Traffic Type] から、[Data] または [Voice] を選択します。

i) [Security Group] ドロップダウンリストからセキュリティグループを選択します。

j) この IP プールをクリティカル IP アドレスプールに含めるには、[Critical VLAN] チェックボックスをオンにします。

認証サーバーを使用できない場合、クリティカルプールがクローズド認証プロファイルに使用されます。認証サーバーがない場合、クリティカルプールにクリティカル VLAN が割り当てられ、未認証のすべてのホストがそのクリティカル VLAN に配置されます。

（注） クリティカル VLAN を有効にすると、Catalyst Centerが VLAN 名を自動的に生成します。

k) この IP プールをワイヤレス IP アドレスプールとして有効にするには、[Fabric-Enabled Wireless] チェックボックスをオンにします。

l) レイヤー 2 フラッディングを有効にするには、[Layer 2 Flooding] チェックボックスをオンにします。

（注） レイヤ 2 フラッディングにはアンダーレイマルチキャストが必要であり、これは LAN 自動化中に設定されます。LAN 自動化でアンダーレイをプロビジョニングしない場合は、アンダーレイマルチキャストを手動で設定します。

m) ファブリック対応のワイヤレスネットワークに接続されているブリッジモードの仮想マシンのオンボーディングを有効にするには、[Fabric Enabled Wireless] と [Multiple IP-to-MAC Addresses] チェックボックスをオンにします。

n) 1 つの有線ホストに複数の IPv4 アドレス（IP エイリアシング）を持たせるには、[Multiple IP-to-MAC Addresses] チェック ボックスのみをオンにします。

1 つの MAC アドレスに最大 1000 個の IPv4 アドレスを設定できます。

o) IP プールをさらに関連付けるには、プラスアイコン（  ）をクリックして上記の手順を繰り返します。

ステップ 7 [Fabric Zones (Optional)] ウィンドウで、次の手順を実行します。

a) [Select Fabric Zones] をクリックして、次のいずれかを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコン（  ）をクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリックゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

ステップ 8 [Summary] ウィンドウでエニーキャストゲートウェイの設定を確認します。

ステップ 9 [Create Anycast Gateway] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

[Deploy] をクリックして、エニーキャストゲートウェイを作成します。

ステップ 10 [Update Layer 3 Virtual Networks] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、「ファブリック構成の可視化と制御」を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

エクストラネットポリシー

レイヤ3仮想ネットワーク（VN）間でフュージョンデバイスを使用せずにルートリークできるエクストラネットポリシーを設定します。Cisco DNA Center で自動的にエクストラネットポリシーを作成し、エンドポイント（ホストまたはユーザー）から DHCP、DNS サーバー、インターネットなどの共有サービスへアクセスできるようになります。共有サービスはプロバイダー VN に接続します。共有サービスを使用するエンドポイントは、サブスクライバー VN に常駐します。エクストラネットポリシーは、プロバイダー VN とサブスクライバ VN 間の通信を確立します。

次の展開に関して、エクストラネットポリシーを作成、編集、および削除することができます。

- IP トランジットを使用した単一サイトファブリック
- SDA トランジットを使用したマルチサイトファブリック

エクストラネットポリシーの設定に関するガイドライン

エクストラネットポリシーを設定する前に、次のガイドラインを考慮してください。

- エクストラネットポリシーを設定するには、Cisco IOS XE 17.9.1 以降のリリースがデバイスで動作している必要があります。
- エクストラネットポリシーは、LISP Pub/Sub コントロールプレーンがあるファブリックサイトでのみサポートされます。
- SD-Access トランジットを使用するマルチサイトファブリックでエクストラネットポリシーを設定するには、すべてのサイトにプロバイダー VN がある必要があります。
- ネットワークで複数の VN ポリシーを設定する場合、同じ VN を複数のポリシーでプロバイダー VN にすることはできません。
- エクストラネットポリシーは、重複する IP プールをサポートしていません。
- ポリシー内のプロバイダー VN は、別の VN ポリシー内のサブスクライバ VN として設定することはできません。また、その逆もできません。
- エクストラネットポリシーが適用されるすべてのファブリックサイトにプロバイダー VN を追加してください。
- プロバイダー VN がファブリック外で互いにリークしないようにしてください。そうしないと、サブスクライバ VN 間でルートリークが発生する可能性があります。
- エクストラネットポリシーはルータデバイスではサポートされていません。

エクストラネットポリシーの作成

エクストラネットポリシーを作成するには、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Workflows]** > **[Create Extranet Policy]**の順に選択します。

または、**[Provision]** > **[Virtual Networks]**の [Extranet Policies] タブに移動します。[Extranet Policies] ウィンドウで、[Create Extranet Policy] をクリックします。

ステップ 2 画面上のガイダンスに従ってポリシーの名前を指定し、プロバイダー VN とサブスクライバ VN を選択します。

このエクストラネットポリシーを 1 つ以上のファブリックサイトに割り当てることができます。

SD-Access トランジットでファブリックサイトに接続するマルチサイト展開では、SD-Access トランジットによって接続されているすべてのファブリックサイトを選択してください。

ステップ 3 [Summary] ページで、エクストラネットポリシー構成を確認します。

変更を加えるには、変更する設定のグループの横にある [Edit] をクリックします。

ステップ 4 [Deploy Extranet Policy] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

ステップ 5 [Create] をクリックして、エクストラネットポリシーを作成します。

[Deploy Extranet Policy] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、「ファブリック構成の可視化と制御」を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

エクストラネットポリシーの編集

エクストラネットポリシーを編集して、サブスクライバVNの追加または削除、ファブリックサイトへのポリシーの割り当て、ファブリックサイトからのポリシーの削除を行うことができます。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Extranet Policies] タブで、編集するポリシーを選択し、**[More Actions]** > **[Edit Extranet Policy]** の順にクリックします。

ステップ 3 画面上のガイダンスに従ってポリシーを編集します。

エクストラネットポリシーの削除

エクストラネットポリシーを削除するには、次の手順を実行します。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Extranet Policies] タブで、削除するポリシーを選択し、**[More Actions]** > **[Delete Extranet Policy]** の順にクリックします。

ステップ 3 [Delete Extranet Policy] スライドインペインで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。。

- エクストラネットポリシーをすぐに削除するには、[Now] をクリックします。
- 将来の日付と時刻で削除操作をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

[Apply] をクリックして操作を実行します。

ファブリックゾーンの設定

ファブリックサイト（親サイト）は、ネットワークを簡単に管理できるように、より小さなサブネットによるファブリックゾーンに分割できます。ファブリックゾーンは、独自のエッジノードと拡張ノードを持つことができますが、コントロールプレーンとボーダーのために親サイトに接続します。以前の Catalyst Center のリリースから現在のリリースに移行した場合は、既存のファブリックサイトにファブリックゾーンを作成することができます。このファブリックゾーンは、親サイトのすべてのプロパティを継承します。

はじめる前に

- ネットワーク階層がグローバルサイトの下に作成されていることを確認します。
- 階層の最下位に位置していない親サイトを選択します。

次に、ファブリックゾーンを設定するためのワークフローの概要を示します。

1. 次のいずれかの方法でファブリックゾーンを作成します。
   - [Create a Fabric Site] ワークフローを使用して、ファブリックサイトとそのゾーンを作成します。詳細については、ファブリックサイトおよびそのファブリックゾーンの作成 （51 ページ）を参照してください。
   - 既存のファブリックサイトを編集して、ファブリックゾーンを追加します。詳細については、ファブリックサイト内のファブリックゾーンの作成 （53 ページ）を参照してください。
2. ファブリックゾーンにエッジノードと拡張ノードを追加します。詳細については、ファブリックへのデバイスの追加 （22 ページ）を参照してください。
3. ファブリックゾーンにレイヤ 3 仮想ネットワークとセグメントを割り当てます。詳細については、ファブリックゾーンへのレイヤ 3 仮想ネットワークの関連付け （54 ページ）を参照してください。

（注） ファブリックゾーンで使用できるのは親サイトの仮想ネットワークとセグメントのみです。

（注） ファブリックゾーンに追加されたセグメントは、親サイトでは更新できません。

親サイトのファブリックゾーンのエッジノードおよび拡張ノードは編集できません。

ファブリックゾーンのエッジノードは、親サイトのコントロールプレーンまたはボーダーとして設定できます。

ファブリックサイトおよびそのファブリックゾーンの作成

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Create Fabric Site] をクリックします。

または、メニューアイコンをクリックして**[Workflows]** > **[Create Fabric Site]**の順に選択します。

ステップ 3 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 4 [Fabric Site Location] ウィンドウで、ファブリックゾーンとして追加するエリア、建物、またはフロアを選択します。

ステップ 5 [Wired Endpoint Data Collection] ウィンドウで、[Wired Endpoint Data Collection] チェックボックスがオンになっていることを確認します。

ステップ 6 [Authentication Template] ウィンドウで、次の手順を実行します。

a) ファブリックサイトの認証テンプレートを選択します。

- [Closed Authentication]：認証前のすべてのトラフィック（DHCP、DNS、ARP など）が廃棄されます。
- [Open Authentication]：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- [None]

b) （オプション）[Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

- [First Authentication Method]：[802.1x] または [MAC Authentication Bypass（MAB）] を選択します
- [802.1x Timeout（in seconds）]：スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN]：[Yes] または [No] を選択します。
- [Number of Hosts]：[Unlimited] または [Single] を選択します。
- [BPDU Guard]：このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジ プロトコル データ ユニット（BPDU）ガードを有効または無効にします。
- [Pre-Authentication Access Control List]：トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 7 [Fabric Zones] ウィンドウで、ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックします。

ファブリックゾーンを有効にするには、ネットワーク階層でファブリックサイトを選択します。

ステップ 8 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 9 [Fabric Site Creation Scheduler] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、「ファブリック構成の可視化と制御」を参照してください。

ステップ 10 [展開（Deploy）] をクリックします。

[Fabric Site Creation Scheduler] ウィンドウで [Now] または [Later] を選択した場合、デバイス構成はスケジュールされた時刻に展開されます。[Tasks] ウィンドウでタスクを確認できます。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、成功メッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

ステップ 11 [Fabric Site Creation Scheduler] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。

   詳細については、「ファブリック構成の可視化と制御」を参照してください。

2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。

   （注） ITSM 承認のためにデバイス設定を送信し、すべての設定をプレビューせずにこれらの設定を展開できます。

3. スライドインペインで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。

4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

ITSM 承認のために設定を送信した場合は、[Work Items] ウィンドウで作業項目のステータスを表示できます。承認されていない場合は、ITSM承認のために作業項目を再送信する必要があります。設定が承認されると、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

ファブリックサイト内のファブリックゾーンの作成

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックゾーンを指定するファブリックサイトの [Actions] 列で、省略記号アイコン（ ••• ）の上にカーソルを置き、[Edit Fabric Zone] を選択します。

ステップ 4 [Edit Fabric Zones] ウィンドウで、エリア、建物、またはフロアを選択します。

ステップ 5 [Summary] ウィンドウでファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 6 [Fabric Site Update Scheduler] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、「ファブリック構成の可視化と制御」を参照してください。

ステップ 7 [Deploy] をクリックします。

ファブリックサイトとファブリックゾーンがプロビジョニングされるまでに数秒かかります。プロビジョニングされると、成功メッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

次のタスク

- 新しく作成したファブリックゾーンにエッジノードデバイスと拡張ノードデバイスのみを追加します。

ファブリックゾーンに割り当てられたデバイスを親サイトに割り当てることはできません。ただし、ファブリックゾーンに割り当てられたエッジノードデバイスを親サイトのコントロールプレーンまたはボーダーノードとして設定することは引き続き可能です。

- ファブリックゾーンに IP プールと仮想ネットワークを割り当てます。

ファブリックゾーンへのレイヤ3仮想ネットワークの関連付け

始める前に

ファブリックゾーンが作成されていることを確認します。

（注） ファブリックゾーンに追加できるのは親サイトのレイヤ 3 仮想ネットワークのみです。

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Virtual Networks]**。

ステップ2 [SUMMARY] で、[Layer 3 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 3 仮想ネットワークが示されます。

ステップ3 [Layer 3] タブで、ファブリックゾーンの関連付けを編集するレイヤー3仮想ネットワークの横にあるチェックボックスをオンにします。

（注） 最大 5 つのレイヤ 3 仮想ネットワークを編集できます。

ステップ4 [More actions] にカーソルを合わせ、[Edit Fabric Site and Fabric Zone Associations] を選択します。

ステップ5 [Fabric Sites and Fabric Zones（Optional）] ウィンドウで、次のように構成します。

a) [Select Fabric Zones] をクリックして、ファブリックゾーンを選択します。

仮想ネットワークは、ファブリックサイトの複数のファブリックゾーンに割り当てることができます。ファブリックゾーンを選択するには、次のいずれかを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコン（＋）をクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリック ゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

c) すべてのレイヤー 3 仮想ネットワークについて、この関連付けを繰り返します。

ステップ6 [Summary] ウィンドウで、レイヤー 3 仮想ネットワークゾーンを確認します。

ステップ7 [Created and Deploy（Step 1 of 2）] ウィンドウで、[Update] をクリックします。

ステップ 8 [Created and Deploy（Step 2 of 2）] ウィンドウで、[Deploy] をクリックして、レイヤ 3 仮想ネットワークをデプロイします。

ステップ 9 仮想ネットワークを確認するには、[View Layer 3 Virtual Networks] をクリックします。

[Virtual Networks] ウィンドウの [Layer 3] タブに、すべてのレイヤー 3 仮想ネットワークの詳細情報が表示されます。

ファブリックゾーンへのレイヤ 2 仮想ネットワークの関連付け

始める前に

（注） ファブリックゾーンに追加されたゲートウェイは、親サイトでは編集できません。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Layer 2 Virtual Networks] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのレイヤ 2 仮想ネットワークが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックサイトを選択し、[Select] をクリックします。

ステップ 5 [レイヤー2] タブで、ファブリックゾーンの関連付けを編集したいレイヤ 2 仮想ネットワークのチェックボックスをオンにします。

（注） 最大 5 つのレイヤー 2 仮想ネットワークを編集できます。

ステップ 6 [More actions] にカーソルを合わせ、[Edit Layer 2 Fabric Zone Associations] を選択します。

ステップ 7 [Associated Fabric Sites and Fabric Zones] ウィンドウで、次を構成します。

a) [Select Fabric Zones] をクリックして、ファブリックゾーンを選択します。

仮想ネットワークは、ファブリックサイトの複数のファブリックゾーンに割り当てることができます。ファブリックゾーンを選択するには、次のいずれかを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコン（＋）をクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリックゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

c) すべてのレイヤ 2 仮想ネットワークに、この関連付けを繰り返します。

ステップ 8 [Summary] ウィンドウで、レイヤ 2 仮想ネットワークの設定を確認して、[Create] をクリックします。

ステップ 9 [Create] ウィンドウで、[Deploy] をクリックして、レイヤー 2 仮想ネットワークを展開します。

レイヤ 2 仮想ネットワークがプロビジョニングされると、成功メッセージが表示されます。

ステップ 10 仮想ネットワークの作成を確認するには、[View Layer 2 Virtual Networks] をクリックします。[Virtual Networks] ウィンドウの [Layer 2] タブに、すべてのレイヤー 2 仮想ネットワークの詳細情報が表示されます。

ファブリックゾーンへのエニーキャストゲートウェイの関連付け

始める前に

ファブリックゾーンが作成されていることを確認します。

（注） 親サイトのエニーキャストゲートウェイのみをファブリックゾーンに追加できます。

ファブリックゾーンに追加されたエニーキャストゲートウェイは、親サイトでは更新できません。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Virtual Networks]**。

ステップ 2 [SUMMARY] で、[Anycast Gateways] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのエニーキャストゲートウェイが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックサイトを選択し、[Select] をクリックします。

ステップ 5 [Anycast Gateway] タブで、ファブリックゾーンの関連付けを編集するエニーキャストゲートウェイの横にあるチェックボックスをオンにします。

（注） 最大 5 つのエニーキャストゲートウェイを編集できます。

ステップ 6 [More actions] にカーソルを合わせ、[Edit Fabric Zone Associations] を選択します。

ステップ 7 [Fabric Zones (Optional)] ウィンドウで、次の手順を実行します。

a) [Select Fabric Zones] をクリックして、次のいずれかを実行します。

- 必要なファブリックゾーンの横にあるプラスアイコン（＋）をクリックします。
- ファブリックゾーン名をクリックし、[Add Selected] をクリックします。

（注） 複数のファブリックゾーンを選択するには、Shift キーを押しながらファブリックゾーン名をクリックし、[Add Selected] をクリックします。

- すべてのファブリック ゾーンを選択するには、[Add All] をクリックします。

b) [**Assign**] をクリックします。

ステップ 8 [Summary] ウィンドウでエニーキャストゲートウェイの設定を確認します。

ステップ 9 [Create] ウィンドウで、[Deploy] をクリックします。

ステップ 10 成功メッセージが表示された後にゲートウェイの作成を確認するには、[View Anycast Gateway] をクリックします。

[Virtual Networks] ウィンドウの [Anycast Gateway] タブに、すべてのエニーキャストゲートウェイの詳細が表示されます。

拡張ノードデバイスの設定

拡張ノードは、自動化されたワークフローによって設定されます。設定後、拡張ノードデバイスがファブリックトポロジビューに表示されます。[Port Assignment] タブを使用して、拡張ノードにポートを割り当てることができます。

（注） 拡張ノードは、GUI ベースのプロビジョニング ワークフローではオンボードできません。拡張ノードをオンボードするには、デバイス設定を工場出荷時の初期状態にリセットし、デバイスの電源をオンにした後に、SD-Access 自動化ワークフローを使用する必要があります。

デバイスは、拡張ノードネイバーの Cisco DNA ライセンスおよびデバイスの Cisco DNA ライセンスに応じてオンボードされます。

- ネイバーが Cisco DNA Essentials ライセンスで動作している場合、デバイスは、その Cisco DNA ライセンスに関係なく、標準の拡張ノードとしてオンボードされます。
- ネイバーが Cisco DNA Advantage ライセンスで動作している場合、デバイスは、Cisco DNA Essentials ライセンスがあれば、標準の拡張ノードとしてオンボードされます。
- ネイバーが Cisco DNA Advantage ライセンスで動作している場合、デバイスは、Cisco DNA Advantage ライセンスがあれば、ポリシー拡張ノードとしてオンボードされます。
- デバイスに複数のネイバーがあり、それらのネイバーに異なる Cisco DNA ライセンスレベルがある場合、デバイスは Cisco DNA ライセンスに関係なく、標準の拡張ノードとしてオンボードされます。

拡張ノードデバイスは、マルチキャストトラフィックをサポートします。

ポリシー拡張ノードは、仮想ネットワーク内のセキュリティポリシーをサポートする拡張ノードです。ポリシー拡張ノードのポート割り当て時に、[Group] を選択できます。

ポリシー拡張ノードデバイスには、Cisco IOS XE リリース 17.1.1s 以降を実行している Cisco Catalyst Industrial Ethernet（IE）3400、IE 3400 Heavy Duty シリーズ スイッチ、および Cisco Catalyst 9000 シリーズ スイッチがあります。

シスコ デジタルビルディング シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ、および Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチは、ポリシー拡張ノードとして構成することはできません。

拡張ノードの設定手順

Cisco Catalyst 9300、Cisco Catalyst 9400、および Cisco Catalyst 9500 シリーズスイッチは、ファブリックエッジとして設定されたときに拡張ノードをサポートします。

（注） ファブリックエッジノードとして設定されている Cisco Catalyst 9200 シリーズ スイッチは、拡張ノードデバイスをサポートしていません。

以下に、拡張ノードでサポートされている最小ソフトウェアバージョンを示します。

- Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチ：15.2(7)E0s（LAN ベースライセンスが有効になっている）

  IP サービスライセンスがある場合は、Switch Database Management（SDM）テンプレートを `dual-ipv4-and-ipv6 default` に手動で変更する必要があります。

- Cisco Catalyst IE 3400、3400 Heavy Duty（X-coded および D-coded）シリーズ スイッチ：Cisco IOS XE リリース 17.1.1s。
- Cisco Catalyst IE 3300 シリーズ スイッチ：Cisco IOS XE リリース 16.12.1s。
- Cisco Digital Building シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ：リリース 15.2(7)E0s。

ポリシー拡張ノードデバイス、およびポリシー拡張ノードをサポートするエッジノードデバイスで必要な最小ソフトウェアバージョンは Cisco IOS XE リリース 17.1.1 s です。

次の設定手順は、標準の拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ポリシー拡張ノードとしてデバイスを設定するには、デバイスとそれをサポートするエッジノードの両方で、Network Advantage と Cisco DNA Advantage のライセンスレベルが有効になっている必要があります。

ステップ 1 拡張ノードのネットワーク範囲を設定します。IP アドレスプールを設定する を参照してください。この手順では、IP アドレスプールを追加し、サイトレベルで IP プールを予約します。CLI および SNMP クレデンシャルが設定されていることを確認します。

ステップ 2 拡張 IP アドレスプールを INFRA_VN に割り当てます。エニーキャストゲートウェイの作成 （43 ページ）を参照してください。[Pool Type] として [Extended Node] を選択します。

Catalyst Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

ステップ 3 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Catalyst Center から到達可能であることを確認します。

（注） オプション 43 の詳細については、DHCP コントローラ ディスカバリを参照してください。

ステップ 4 ファブリックエッジデバイスに拡張ノードデバイスを接続します。拡張ノードデバイスからファブリックエッジへ複数のリンクを設定できます。

ステップ 5 拡張ノードに接続されているファブリックエッジノードでポートチャネルを作成します。リングまたはデイジーチェーン内の後続の拡張ノードに関して、それが接続している、前の拡張ノードでポートチャネルを作成します。

（注） この手順は、ファブリックのグローバル認証モードが [Open Authentication]、[Low Impact]、または [Closed Authentication] の場合にのみ完了してください。ファブリックサイトが [None] 認証モードに設定されている場合、ポートチャネルは、プラグ アンド プレイ プロビジョニングを使用した拡張ノードのオンボーディング中に自動的に作成されます。

ポートチャネルを作成するには、次の手順を実行します。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。
b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。
c) [fabric site] をクリックします。
d) [Fabric Infrastructure] タブで、ファブリックエッジノード（または接続に応じて拡張ノード）を選択します。
e) slide-in paneの [Port Channel] タブで、[Create Port Channel] をクリックします。
f) 次の手順を実行します。

- [Connected Device Type] ドロップダウンリストから [Extended Node] を選択します。
- 説明を入力します。
- [Port Aggregation Protocol (PAgP Desirable)] を選択します。

  Cisco IOS XE リリース 17.1.1s 以降、IE 3300 および IE 3400 デバイスは PAgP をサポートしています。
- Cisco IOS XE リリース 17.1.1s よりも前のバージョンを実行している場合は、IE 3300 および IE 3400 デバイスの [On] を選択します。

  （注） 拡張ノードのオンボーディングでは Link Aggregation Control Protocol（LACP）は機能しません。
- ポートチャネルとしてバンドルするポートを選択します。

g) [Done] をクリックします。

これで、ファブリックエッジノード（または拡張ノード）にポートチャネルが作成され、拡張デバイスがオンボードされます。

ステップ 6 以前の設定がない場合は、拡張ノードデバイスの電源をオンにします。拡張ノードデバイスに構成がある場合は、デバイス構成を工場出荷時のデフォルトにリセットしてリロードします。

Catalyst Center Cisco DNA Center では、拡張ノードデバイスをインベントリに追加し、同じサイトをファブリックエッジとして割り当てます。次に、拡張ノードデバイスがファブリックに追加されます。これで、拡張ノードデバイスがオンボードされ、管理できるようになりました。

設定が完了すると、拡張ノードがファブリックトポロジに、拡張ノードであることを示すタグ（X）とともに表示されます。

拡張ノードのポリシー拡張ノードへのアップグレード

Cisco SD-Access の自動化は、Catalyst Center Essentials ライセンスを持つポリシー拡張ノード対応デバイスを拡張ノードとしてオンボーディングします。ライセンスを Catalyst Center Advantage にアップグレードすることにより、この拡張ノードデバイスをポリシー拡張ノードに変換できます。

デイジーチェーンでは、アップストリームデバイスが拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

リングでは、隣接するノードが両方とも拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

ポリシー拡張ノードにアップグレードされたノードを、拡張ノードとして再構成することはできません。

拡張ノードをポリシー拡張ノードに変換するには、次の手順を実行します。

始める前に

- 拡張ノードがすでにオンボーディングされていることを確認してください。
- Catalyst Center でスマートライセンス認証情報を更新します。

ステップ 1 Catalyst Center ライセンスマネージャを使用して、デバイスでのライセンスレベルを Catalyst Center Essentials から Catalyst Center Advantage に変更します。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[Tools]** > **[License Manager]** の順に選択します。
b) [Devices] タブで、デバイスを選択します。
c) **[Actions]** > **[Change License]** > **[Change DNA License]** を選択します。
d) [Change DNA License Level] ウィンドウで、[Advantage] をクリックします。
e) [Confirm] をクリックします。
f) [Success] メッセージウィンドウで、[OK] をクリックします。

デバイスがリロードします。

ステップ 2 ノードが [Reachable] になり、[Managed] 状態になるのを待ちます。

[Provision] > **[Network Devices]** > **[Inventory]** ウィンドウに、すべてのデバイスの到達可能性ステータスが表示されます。

ステップ 3 「Netconf Connection Refused」エラーが表示された場合は、デバイスを再同期します。エラーが表示されなくなるまで、再同期プロセスを繰り返します。

a) **[Provision]** > **[Network Devices]** > **[Inventory]** ウィンドウで、デバイスを選択します。
b) **[Actions]** > **[Inventory]** > **[Resync Device]** の順に選択します。

ステップ 4 ポリシー拡張ノードへアップグレードします。

a) **[Provision]** > **[Fabric Sites]** ウィンドウで、デバイスがオンボーディングされているサイトを選択します。
b) [Fabric Infrastructure] タブで、デバイスをクリックしてその属性を編集します。
c) [Fabric] タブで、[Extended Node Attributes] の下の [Policy] トグルボタンをクリックします。
d) 表示される [Policy Extended Node Upgrade] ウィンドウで、[Upgrade] をクリックします。

拡張ノードの削除

このタスクでは、拡張ノード、ポリシー拡張ノード、および認証済み拡張ノードを削除する手順について説明します。

ステップ 1 ファブリックから拡張ノードデバイスを削除します。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。
b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。
c) 拡張ノードデバイスを含むファブリックサイトを選択します。
d) [Fabric Infrastructure] タブで、拡張ノードデバイスをクリックします。
e) スライドインペインで、[Remove From Fabric] をクリックします。
f) [Add] をクリックします。

ステップ 2 デバイスを [Inventory] から削除します。

インベントリからデバイスを削除する手順については、ネットワーク デバイスの削除を参照してください。

ステップ 3 サプリカントベースの拡張ノードデバイスの場合、ファブリックエッジノードまたは FIAB でポート割り当て設定を削除します。

拡張ノードおよびポリシー拡張ノードの REP リングトポロジの設定

拡張ノードによっ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するには、ファブリックサイトの Resilient Ethernet Protocol（REP）リングを設定します。

特に明記されていないかぎり、「拡張ノード」という用語はポリシー拡張ノードも表します。

REP リングでは、次のデバイスを設定できます。

- 拡張ノード：

  Cisco IOS 15.2(7)E3 以降のリリースが動作する Cisco Industrial Ethernet (IE) 4000、4010、5000 シリーズ スイッチ。

  Cisco IOS XE 17.3.3 以降のリリースが動作する Cisco Catalyst IE3300 シリーズ スイッチ。

- ポリシー拡張ノード：

  Cisco IOS XE 17.3.3 以降のリリースが動作する Cisco Catalyst IE3400、IE3400H シリーズ スイッチ。

REP リングの制約事項

- 拡張ノードを既存の REP リングに追加するには、最初に REP リングを削除します。REP リングを削除すると、Per VLAN Spanning Tree Protocol（PVSTP）が有効になり、レイヤ 2 ループが回避されます。次に、新しい拡張ノードをファブリックに追加し、REP リングを再度作成して、新しい拡張ノードを含めます。
- 特定の REP リング内の複数のリングおよびリングのリングはサポートされていません。
- REP リング内のノードには、デイジーチェーン方式で他のノードを接続できます。ただし、デイジーチェーンのノードには、ノードのリングを接続することはできません。
- REP リングまたはデイジーチェーンでは、拡張ノードとポリシー拡張ノードを混在させることはできません。REP リングまたはデイジーチェーンは、拡張ノードのみで、またはポリシー拡張ノードのみで構成されている必要があります。
- デフォルトでは、1 つの REP リングに最大 18 台のデバイスをオンボードできます。19 台以上のデバイスをオンボードするには、**spanning-tree vlan** *infra VN VLAN* **max-age 40** コマンドを使用して BPDU タイマーを増やします。このコマンドを設定するには、Cisco DNA Center のテンプレートを使用します。

リングの最後の 2 つのノードが同時にオンボードを試みると、まれに、これらのノード間にポートチャネルが作成されない場合があることに注意してください。REP リングが作成されると、リングの最後の 2 つのノード間にポートチャネルが確立されます。

特に明記されていないかぎり、次の手順は拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ファブリックエッジノードと拡張ノードがオンボードされていることを確認します。

REP リングの終端となっているファブリックエッジノードとそのインターフェイスを特定します。

（注） REP リング設定手順により、ネットワークトラフィックが短時間中断される可能性があります。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[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 ノードを選択し、[REP Rings] タブで [Create REP Ring] をクリックすることもできます。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Select a fabric site] ウィンドウで、エッジノードと拡張ノードの両方があるサイトを選択します。

ステップ 4 [Select a fabric edge node] ウィンドウで、ファブリックエッジノードを選択します。

ステップ 5 [Select Extended Nodes connected to Fabric Edge] ウィンドウで、ファブリックエッジノードに接続する拡張ノードを選択します。

ファブリックエッジノードに接続する 2 つの拡張ノードを選択できます。

ステップ 6 ファブリックサイト、エッジノード、および拡張ノードの選択を確認し、必要に応じて編集します。

ステップ 7 REP リングの設定を開始するには、[Provision] をクリックします。

[REP Ring Configuration Status] ウィンドウで、設定の進捗状況の詳細なステータスを確認できます。

ステップ 8 [REP Ring Summary] ウィンドウに、作成された REP リングの詳細情報が、検出されたデバイスとともに表示されます。

ステップ 9 REP リングの作成後、成功メッセージが表示されます。

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。

スライドインウィンドウの [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。

リスト内の REP リング名をクリックすると、リングに存在するデバイス、リングに接続する各デバイスのポートなどの詳細情報が表示されます。

REP リングステータスの表示

REP リング内のデバイスのステータスを表示するには、次の手順を実行します。

ステップ 1 Catalyst Center GUI でメニューアイコンをクリックして、**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [fabric site] をクリックします。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードまたはファブリックインアボックス（FIAB）クリックします。

slide-in pane に、選択したファブリックエッジノードまたは FIAB の詳細が表示されます。

ステップ 5 [REP Rings] タブで、[View] をクリックして [REP Ring Topology Status] を表示します。

[REP Topology Status] セクションには、REP リング内のすべてのデバイスの現在の状態が表示されます。[Role] 列に表示される状態は、[Open]、[Fail]、または [Alt] です。

[Open] は、デバイスリンクがアップしていて、トラフィックを転送していることを示します。

[Fail] は、デバイスリンクがダウンしていることを示します。

[Alt] は、デバイスリンクがアップしているが、ポートがトラフィックを転送できないことを示します。

REP リングの削除

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Infrastructure] タブで、REP リングを終了するファブリックエッジノードをクリックします。

スライドインウィンドウに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 3 [REP Rings] タブで、目的の REP リングの **[Actions (…)]** > **[Delete]**をクリックします。

これにより、REP リングが削除されます。

REP リングからのノードの削除

このタスクでは、REP リングから 1 つまたは複数の拡張ノードを削除する手順について説明します。

（注） 拡張ノードが削除された後、ダウンサイジングされた REP リングは既存のインターフェイスを使用して隣接デバイスへのリンクを作成する必要があります。

始める前に

ノードが属する REP リングが不完全でないことを確認してください。

ステップ 1 拡張ノードデバイスをネットワークから手動で削除します。

または、REP リング内のデバイスがダウンすると、[Fabric Infrastructure] ウィンドウに通知が表示されます。

ステップ 2 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 3 [Fabric Infrastructure] タブで、REP リングを終了するファブリックエッジノードをクリックします。

slide-in paneに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 4 [REP Rings] タブで、目的の REP リングについて、**[Actions (…)]** > **[Rediscover]**を選択します。

REP リングから拡張ノードデバイスが削除され、REP リングの表示が更新されます。

サプリカントベースの拡張ノードの設定

Authenticated Extended Node（AEN）とも呼ばれるサプリカントベースの拡張ノードは、IEEE 802.1x（Dot1x）サプリカント設定を受け取り、完全な認証と承認の後にのみ SD-Access ネットワークにオンボードされる拡張ノードデバイスです。サプリカントベースの拡張ノードデバイスをオンボードするには、ファブリックエッジのオーセンティケータポートをクローズド認証テンプレートで設定する必要があります。

次のプラットフォームは、サプリカントベースの拡張ノードオンボーディングをサポートしています。

ファブリックエッジまたは FIAB：

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9300、C9400、C9500、および C9500H スイッチ。

サプリカントベースの拡張ノード：

Cisco Catalyst 9000 シリーズ：Cisco IOS XE 17.7.1 以降で動作する C9200、C9300、C9400、C9500、および C9500H スイッチ。

サプリカントベースの拡張ノードの設定手順

始める前に

- Cisco ISE を構成して、リリース 3.1 以降で動作することを確認します。「サプリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定（68 ページ）」を参照してください。
- ファブリックエッジノードまたは FIAB デバイスをファブリックに追加し、それが Cisco IOS XE 17.7.1 以降で動作することを確認します。

- ファブリックエッジノードと Cisco ISE の間のパスに適切なパス MTU を設定します。値は 9100 をお勧めします。パス MTU は、LAN 自動化中、またはアンダーレイの構成時に、ファブリック内のすべてのデバイスに設定されることに注意してください。

ステップ 1 Catalyst Center で AAA サーバー設定を構成します。

a) **[System]** > **[Settings]** > **[External Services]** > **[Authentication and Policy Servers]** ウィンドウで、デバイス認証用の AAA サーバーとして Cisco ISE を定義します。

詳細な手順については、『Cisco DNA Center Administrator Guide』の「Configure Authentication and Policy Servers」を参照してください。

b) Cisco ISE サーバーをグローバルサイトに追加します。詳細については、Cisco ISE またはその他の AAA サーバーの追加を参照してください。

ステップ 2 （オプション）オンボーディング前にデバイスを認証するように Catalyst Center を構成します。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[System]** > **[Settings]** > **[Device Settings]** > **[PnP Device Authorization]** の順に選択します。

b) [Device Authorization] チェックボックスをオンにしてデバイスで許可を有効にします。

c) [Save] をクリックします。

ステップ 3 PKI 証明書を管理するように Catalyst Center アプライアンスを構成します。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：[System] > [Settings] > [Trust & Privacy] > [Certificate Authority] の順に選択します。 > > >

b) [Certificate Authority] ウィンドウで、[Use Cisco DNA Center] をクリックします。

c) [CA Management] タブで、[Download CA Certificate] をクリックします。

d) Cisco ISE の信頼できる証明書ストアに証明書を追加します。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html

外部証明書を使用する場合は、その証明書を Cisco ISE の信頼できる証明書ストアに追加します。

ステップ 4 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Catalyst Center から到達可能であることを確認します。

オプション 43 の詳細については、DHCP コントローラ ディスカバリを参照してください。

ステップ 5 ファブリックサイトで [Closed Authentication] を有効にし、ブリッジ プロトコル データ ユニット（BPDU）ガードを無効にします。

デフォルトでは、[Closed Authentication] を選択すると、すべてのダウンリンクアクセスポートに BPDU ガード設定がプッシュされます。拡張ノードのようなリモートスイッチが接続されている場合、BPDU ガードはポートをエラーディセーブルモードにプッシュします。BPDU ガードを無効にするには、クローズド認証の設定時に、[Enable BPDU Guard] チェックボックスをオフにします。

詳細については、「認証テンプレートの選択」 を参照してください。

ステップ 6 エニーキャストゲートウェイの作成 （43 ページ）に記載されているように、拡張 IP アドレスプールを INFRA_VN に割り当てます。

[Create Anycast Gateways] ワークフローで、[Pool Type] として [Extended Node] を選択し、[Supplicant-Based Extended Node Onboarding] チェックボックスをオンにします。

Catalyst Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

（注） 拡張 IP アドレスプールは、ファブリックエッジデバイスが Cisco IOS XE 17.7.1 以降で動作している場合にのみ正常に割り当てられます。Catalyst Center の以前のリリースからアップグレードした場合は、拡張 IP アドレスプールを構成する前に、サプリカントベースの拡張ノードの移行を完了する必要があります。

ステップ 7 ファブリックエッジデバイスまたは FIAB に拡張ノードデバイスを接続します。

オンボーディングの前にデバイスを認証することを選択した場合（ステップ 2）、電源をオンにした後、拡張ノードデバイスは [Pending Authorization] 状態になります。**[Provision]** > **[Plug and Play]** ウィンドウでデバイスのステータスを確認できます。

ステップ 8 （オプション）デバイスを認証します。

この手順は、デバイスが [Pending Authorization] 状態の場合にのみ実行してください。

a) 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Plug and Play]**。
b) [Plug and Play] ウィンドウで、サプリカントベースの拡張ノードデバイスを選択し、**[Actions]** > **[Authorize]** の順に選択します。

認証プロセスは、Cisco ISE で証明書ベースの EAP-TLS 認証を完了するために、サプリカントベースの拡張ノードデバイスをプロビジョニングします。認証後、Cisco ISE はサプリカントベースの拡張ノードデバイスに完全なアクセスを許可します。サプリカントベースの拡張ノードデバイスは、SD-Access ファブリックに完全にオンボードされます。

サプリカントベースの拡張ノードデバイスがファブリックにオンボードされた後は、ファブリック エッジサプリカント ポートへのアクセスは認証ステータスのみに基づきます。デバイスまたはポートがダウンすると、認証セッションがクリアされ、ポートでトラフィックが許可されなくなります。ポートが再び起動すると、IEEE 802.1x（Dot1x）認証プロセスを経て、SD-Access ネットワークへのアクセスが回復します。

障害のあるポートの交換

オーセンティケータ（ファブリックエッジまたは FIAB）ポートとサプリカントポート間のリンクがダウンした場合、障害のあるポートを交換し、[Port Assignment] メニューから新しいポートを設定できます。

ステップ 1 サプリカントポートを交換するには、次の手順に従います。

a) 新しいサプリカントポートの設定をクリアします。
b) 既存の設定を現在のサプリカントポートから新しいサプリカントポートにコピーして、802.1X 認証を可能にします。

ステップ 2 オーセンティケータポートを交換するには、次の手順に従います。

a) サプリカントポートをオーセンティケータの新しいインターフェイスに割り当てます。ポートの割り当てについては、「ファブリックサイト内のポートの設定 （33 ページ）」を参照してください。[Connected Device Type] として [Supplicant-Based Extended Node] を選択します。

b) オーセンティケータの古いインターフェイスの既存のポート割り当てをクリアします。

ステップ 3 オーセンティケータとサプリカントの古いポート間の物理接続を切断します。オーセンティケータとサプリカントの新しいポート間をケーブルで接続します。このリンクを確立します。

ステップ 4 オーセンティケータとサプリカントの新しいポート間のリンクが確立されたら、次の手順を実行します。

a) オーセンティケータとサプリカントの両方に対して **[Inventory]** > **[Resync Device]** を実行して、Catalyst Center のデバイス情報を再同期します。デバイス情報の再同期を参照してください。

b) 新しいサプリカントポートをオーセンティケータに割り当てます。ポートの割り当てについては、「ファブリックサイト内のポートの設定 （33 ページ）」を参照してください。[Connected Device Type] として [Authenticator Switch] を選択します。

c) 古いサプリカントポートのポート割り当てをクリアします。

サプリカントベースの拡張ノードをオンボードするためのCiscddentity Services Engine の設定

このタスクでは、Cisco Identity Services Engine（ISE）でサプリカントベースの拡張ノード（SBEN）デバイスをプロファイリングする方法について説明します。以下にリストされている手順は、Cisco ISE 設定手順の一部です。詳細については、『Cisco Identity Services Engine Administrator Guide』を参照してください。

始める前に

Cisco DNA Center から CA 証明書をダウンロードします。

ステップ 1 CA 証明書を Cisco ISE にインポートします。

Cisco ISE ホームページから、**[Administration]** > **[System]** > **[Certificates]** > **[System Certificate]** > **[Import]** を選択します。[Import] ウィンドウで、[Trust for client authentication and Syslog] チェックボックスがオンになっていることを確認します。詳細については、『Cisco Identity Services Engine Administrator Guide』の「Import the Root Certificates to the Trusted Certificate Store」セクションを参照してください。

ステップ 2 RADIUS 属性を使用して、次の認証プロファイルを設定します。

Cisco ISE メインメニューから、**[Policy]** > **[Policy Elements]** > **[Results]** > **[Authorization]** > **[Authorization Profiles]** を選択します。

次のプロファイルを構成します。

```
SBEN-DHCP:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_DHCP_ACL.in
```

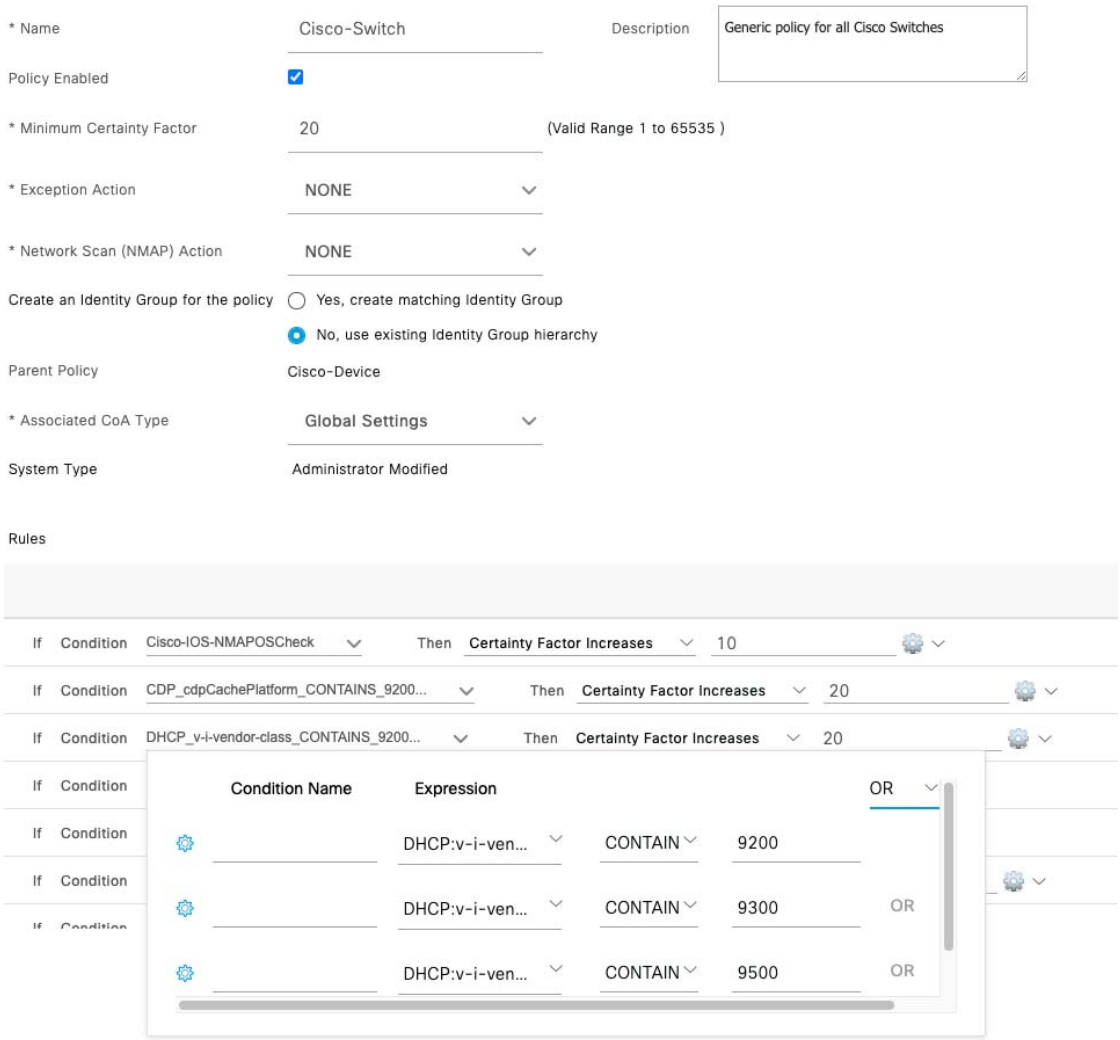
```
SBEN_LIMITED_ACCESS_AUTHZ:
Access Type = ACCESS_ACCEPT
Filter-ID = SBEN_MAB_ACL.in
cisco-av-pair = interface-template-name=SWITCH_SBEN_MAB_TEMPLATE

SBEN_FULL_ACCESS_AUTHZ :
Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=SWITCH_SBEN_FULL_ACCESS_TEMPLATE
```

ステップ 3 [Profiling Policies] ウィンドウでデバイス プロファイリング ポリシーを定義します。

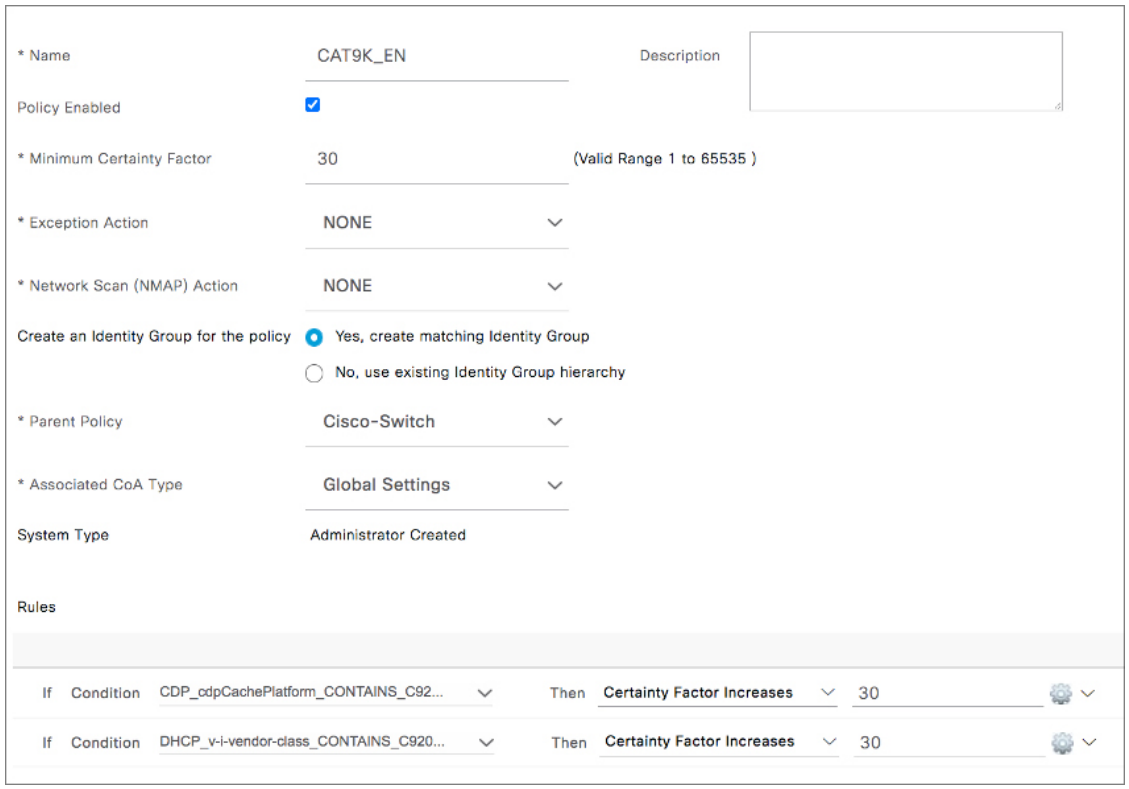
a) Cisco ISE のメインメニューから、**[Policy]** > **[Profiling]** > **[Profiling Policies]**を選択します。

b) [Profiling Policies] ウィンドウで、[Cisco-Device] : [Cisco-Switch] ポリシーの新しい [DHCP-v-i-vendor-class] 条件を追加します。



c) サプリカントデバイスの新しい子ポリシーを [Cisco-Switch] の下に作成し、[CdpCachePlatform] および [V-I-Vendor-Class] 条件を適用します。

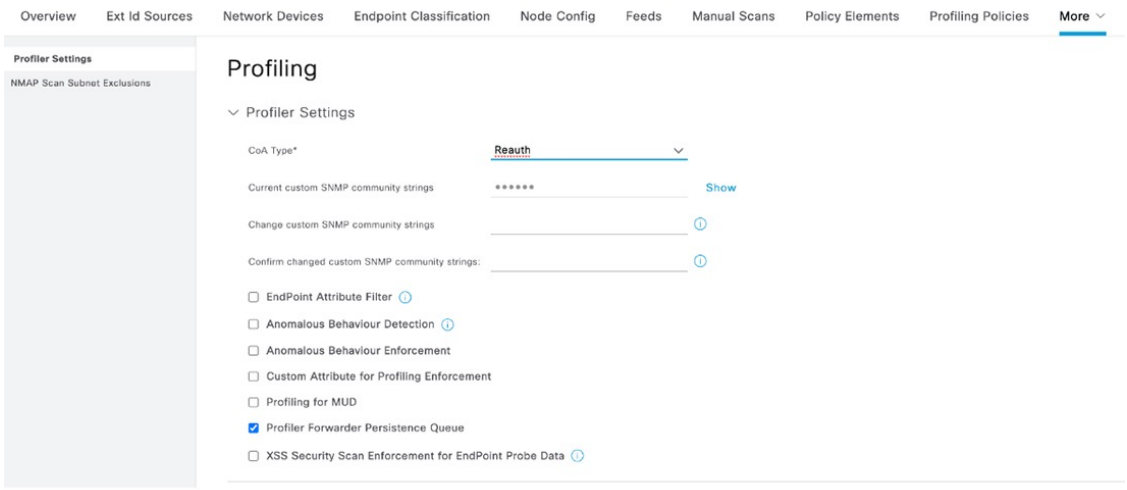
子ポリシーの [Minimum Certainty Factor] の値が親ポリシーの値よりも高いことを確認してください。



ステップ 4 グローバル認可変更（CoA）タイプを [Reauth] に設定します。

[CoA Type] を設定するには、Cisco ISE ホームページから、**[Work Centers]** > **[Profiler]** > **[Settings]**の順に移動します。

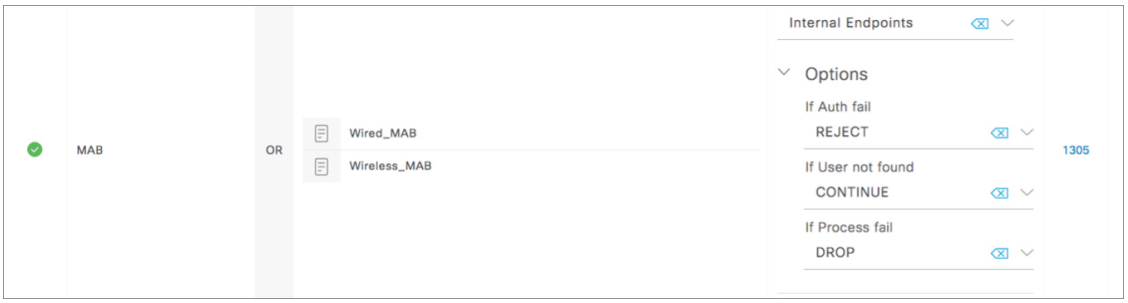
[CoA Type] ドロップダウンリストから [Reauth] を選択します。



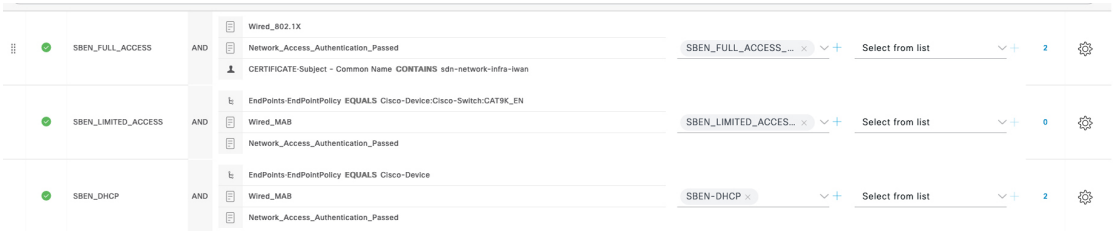
ステップ 5 [Authorization Policy] ウィンドウで認証ポリシーを定義します。

a) Cisco ISE ホームページから、**[Policy]** > **[Policy Sets]** > **[Default]** > **[Authorization Policy]**を選択します。

b) デフォルト MAB ポリシーの [If User not found] フィールドが [CONTINUE] オプションに設定されていることを確認します。



c) [Authorization Policy] ウィンドウで、サプリカントデバイスの認証ポリシーを構成し、ポリシーを以前に作成した認証プロファイル（SBEN-DHCP、SBEN_LIMITED_ACCESS_AUTHZ、SBEN_FULL_ACCESS_AUTHZ）に関連付けます。



ポートチャネルの設定

単一のエンティティとして機能するようにバンドルされたポートのグループは、ポートチャネルと呼ばれます。ファブリックエッジと、拡張ノードやサーバーなどリモート接続されたデバイスとの間のポートチャネルでは、接続の復元力と帯域幅が増加します。

ポート チャネルの作成

始める前に

認証はクローズド認証（[Closed Authentication]）である必要があります。

（注） 他の認証モードでは、次の手順は自動化されています。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ 2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 [Fabric Sites] ウィンドウで、ポートチャネルを設定するファブリックサイトをクリックします。

ステップ 4 [Port Assignment] タブで、[More Actions] にカーソルを合わせ、[Create Port Channel] をクリックします。

ステップ 5 [Select your fabric devices] ウィンドウで、ポートチャネルを作成する必要があるファブリックデバイスを選択します。

ステップ 6 ポートチャネルの数を指定し、各ポートチャネルを設定するには、[Determine number of port channels] ウィンドウで次のアクションを実行します。

a) [Connected Device Type] ドロップダウンリストから、接続済みのデバイスのタイプを選択します。

- ファブリックエッジノードと拡張ノードの間または 2 つの拡張ノードの間にポートチャネルを作成する場合は、[Extended Node] を選択します。
- 片側にファブリックエッジノードまたは拡張ノードがあり、反対側にサードパーティデバイスまたはサーバーポートがあるポートチャネルを作成するには、[Trunk] を選択します。

b) 新しいポートチャネルの説明を [Description] に入力します。

c) プロトコルを選択します。

- Cisco IOS XE リリース 16.12.1s および以前のリリースを実行する拡張ノードの場合は、プロトコルとして [On] を選択します。
- Cisco IOS XE リリース 17.1.1s および以降のリリースを実行する拡張ノードの場合は、プロトコルとして [Port Aggregation Protocol (PAgP)] を選択します。
- [Link Aggregation Control Protocol (LACP)] を拡張ノードのプロトコルとして選択しないでください。LACP モードでは、トランクポートまたはサーバーポートのみを接続できます。

ステップ 7 使用可能なインターフェイスのリストから、ポートチャネルとしてバンドルするインターフェイスを選択します。

（注） LACP モードで接続されたポートチャネルには、16 を超えるメンバーを含めることはできません。

PAgP モードで接続されたポートチャネルには 8 つを超えるメンバーを含めることはできません。

ステップ 8 [Summary] ウィンドウで、作成されたポートチャネルを確認します。

ステップ 9 [Deploy Port Channel] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

[Deploy] をクリックしてポートチャネルを設定します。

ポートチャネルの更新

始める前に

ポートチャネルを更新する前に、少なくとも1つのメンバーインターフェイスが存在することを確認します。

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ2 [Fabric Sites] タブ の [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ3 [Fabric Sites] ウィンドウで、ポートチャネルを更新するファブリックサイトをクリックします。

ステップ4 [Port Assignment] タブで、更新するポートチャネルをクリックします。

ステップ5 [More Actions] にカーソルを合わせ、[Edit Port Channel] をクリックします。

ステップ6 画面上のガイドラインに従って、ポートチャネル設定を更新します。

ポートチャネルにインターフェイスを追加したり、ポートチャネルの既存のインターフェイスを削除したりできます。

ステップ7 [Deploy Port Channel] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

[Deploy] をクリックしてポートチャネルを更新します。

ポートチャネルの削除

ステップ1 左上隅にあるメニューアイコンをクリックして次を選択します：**[Provision]** > **[Fabric Sites]**。

ステップ2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ3 [fabric site] をクリックします。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードをクリックします。

ステップ 5 slide-in paneで、[Port Channel] タブをクリックします。

[Port Channel] ビューには、既存のポートチャネルがすべて一覧表示されます。

ステップ 6 ポートチャネルのチェックボックスをオンにして、[Delete] をクリックします。

ステップ 7 プロンプトで [Yes] をクリックします。

マルチキャスト

マルチキャスト トラフィックは、次のような異なる方法で転送されます。

- ランデブー ポイントを使用した共有ツリー経由。この場合、PIM SM が使用されます。
- 最短パス ツリー（SPT）経由。PIM Source Specific Multicast（SSM）では SPT だけが使用されます。PIM SM は、受信側が接続しているエッジ ルータで送信元が認識されると SPT に切り替わります。

『IP マルチキャスト ルーティング テクノロジーの概要（IP Multicast Technology Overview）』を参照してください。

マルチキャストの設定

Catalyst Center には、仮想ネットワークでグループ通信またはマルチキャストトラフィックを有効にするためのワークフローが用意されています。このワークフローでは、ネットワークでのマルチキャスト実装（ネイティブマルチキャストまたはヘッドエンド レプリケーション）を選択することもできます。

（注） ボーダーがマルチサイト リモート ボーダーとして機能する仮想ネットワークでマルチキャストを有効にすることができます。このような仮想ネットワークでマルチキャストを設定すると、継承された仮想ネットワークにすでにセグメントが含まれている場合は、継承された仮想ネットワークのデバイスにもマルチキャストが設定されます。継承された仮想ネットワークにセグメントがない場合、マルチキャストは、最初のセグメントが作成された後にのみ展開されます。仮想ネットワークとその継承ネットワークが同じタイプのマルチキャスト実装を展開していることを確認してください。継承された仮想ネットワークのエッジノードデバイスをランデブーポイント（RP）として設定することはできません。

ステップ 1 左上隅にあるメニューアイコンをクリックして次を選択します：[Workflows] > [Configure Multicast] の順に選択します。

ステップ 2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ 3 [Fabric Site] ウィンドウのサイト階層ペインでサイトを選択します。

ステップ 4 [Replication Mode] ウィンドウで、ネットワークのマルチキャスト実装方式を次の中から選択します。

- **Native Multicast**
- **Head-end replication**

ステップ 5 [Virtual Networks] ウィンドウで、マルチキャストを設定する仮想ネットワークを選択します。

（注） 継承された仮想ネットワークを選択してマルチキャストを設定することはできません。

ステップ 6 [Multicast pool mapping] ウィンドウで、[IP Pools] ドロップダウンリストから IP アドレスプールを選択します。選択した IP アドレスプールは、選択した仮想ネットワークに関連付けられます。

ステップ 7 [Multicast Mode] ウィンドウで、実装するマルチキャストのタイプを選択します。

- **SSM**（送信元特定マルチキャスト）
- **ASM**（任意の固有のマルチキャスト）
- [SSM] と [ASM] を選択して両方を一緒に設定します。

ステップ 8 次の手順を実行します。

a) [SSM] を選択した場合は、仮想ネットワークごとに IP グループの範囲を追加して、SSM リストを設定します。仮想ネットワークに複数の IP グループ範囲を追加できます。

1. デフォルトでは、IPv4 アドレスの 232.0.0.0/8 の範囲が選択されています。必要に応じて IPv4 アドレスの範囲を変更できます。

   225.0.0.0 ～ 239.255.255.255 の IP グループ範囲を選択します。

2. IPv6 アドレスの場合、FF3x::/32 は SSM 用に予約されています。

b) [ASM] を選択したら、[Multicast Group to Rendezvous Point Mapping] ウィンドウで各仮想ネットワークのランデブーポイントを設定します。

1. ランデブーポイントのタイプ（[External] または [Fabric]）を選択します。
2. それぞれのタブでランデブーポイント（[IPv4 RP] と [IPv6 RP]）を選択します。
3. 任意の数の外部ランデブーポイントを定義できます。
4. 必要に応じて、グループからランデブーポイントへのマッピングを定義できます。ランデブーポイントに関連付けられている 1 つか複数の IPv4/IPv6 マルチキャストグループが存在する場合があります。
5. マッピングなし、またはありのランデブーポイントを設定できます。両方を一緒に設定することはできません。
6. IPv6 および IPv4 FF00:/8 と 225.0.0.0/8 ～ 239.0.0.0/8 それぞれのマルチキャストグループの範囲が許可されます。

ステップ 9 [Summary] ウィンドウで、マルチキャスト設定を確認します。設定を変更するには、[Edit] をクリックします。

ステップ 10 [Deploy Multicast] ウィンドウで、[Visibility and Control of Configurations] の設定に基づいて、使用可能なオプションを選択します。

- 設定をすぐに展開するには、[Now] をクリックします。
- 将来の日付と時刻で展開をスケジュールするには、[Later] をクリックし、展開する日付、時刻、タイムゾーンを定義します。
- 設定をプレビューするには、[Generate Configuration Preview] をクリックします。

  可視性のみが有効になっている場合、または可視性と制御の両方が有効になっている場合、[Generate Configuration Preview] がデフォルトで選択され、[Now] と [Later] がグレー表示（使用不可）になります。詳細については、ファブリック構成の可視化と制御 （14 ページ）を参照してください。

[Deploy] をクリックして設定を完了します。

ステップ 11 [Deploy Multicast] ウィンドウで [Generate Configuration Preview] を選択した場合は、[Visibility and Control of Configurations] の設定に応じて、次の手順を実行します。

1. デバイス構成を確認します。
2. 準備ができたら、[Deploy] または [Submit for Approval] をクリックします。構成の展開、または ITSM 承認のために送信する準備ができていない場合は、[Exit and Preview Later] をクリックします。
3. slide-in paneで、設定を展開するタイミングを指定し、タイムゾーンを選択します。可視性と制御が有効になっている場合は、IT 管理者へのメモを追加します。
4. [Submit] をクリックします。`

   設定が正常に送信されると、成功メッセージが表示されます。

   展開するタスクをプレビューしてスケジュールした場合は、[Tasks] ウィンドウでタスクを確認できます。

   ITSM 承認のために設定を送信した場合は、[Tasks] ウィンドウで作業項目のステータスを確認できます。承認されていない場合は、ITSM 承認のために作業項目を再送信する必要があります。承認されたタスクは、スケジュールされた時刻に展開され、[Tasks] ウィンドウで確認できます。

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。