ファブリックネットワークのプロビジョニング

- ファブリックネットワークについて （1 ページ）
- ファブリックサイトの追加 （4 ページ）
- ファブリックへのデバイスの追加 （5 ページ）
- ボーダーノードとしてのデバイスの追加 （7 ページ）
- LISP Pub/Sub の設定 （9 ページ）
- IP のトランジット ネットワークの作成 （9 ページ）
- SDA トランジット ネットワークの作成 （10 ページ）
- ホスト オンボーディングの設定 （11 ページ）
- 認証テンプレートの選択 （12 ページ）
- ファブリックサイト内のポートの設定 （13 ページ）
- ファブリック ドメインのワイヤレス SSID の設定 （13 ページ）
- 仮想ネットワーク （14 ページ）
- ファブリックゾーンの設定 （18 ページ）
- 拡張ノードデバイスの設定 （22 ページ）
- ポートチャネルの設定 （24 ページ）
- マルチキャスト （27 ページ）

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。

Cisco DNA 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、トランジットサイトを使用して相互接続されます。

トランジットサイト

トランジットサイトとは、2つ以上のファブリックサイトを相互に接続したり、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。
- SDA 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。SDA 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。SDA 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（ブラウンフィールドチェック）：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、デバイスにループバック インターフェイスが設定されている必要があります。
- 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。Cisco DNA 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：Cisco DNA 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 Cisco DNA 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。

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、新しいファブリックサイトを作成できます。つまり、サイトのテレメトリ設定を構成するときには、[Monitor wired clients] を有効にしておく必要があります。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[Provision]** > **[SD ACCESS]** > **[Fabric Sites]** の順に選択します。

ステップ 2 [Fabric Sites] タブで、[Add fabric site] をクリックします。

または、最初の 2 つの手順の代わりに、Cisco DNA Center GUI で [Menu] アイコンをクリックし、**[Workflow]** > **[Create a Fabric Site and Fabric Zones]** を選択します。

ワークフローウィザードの指示に従います。

ステップ 3 [Create a Fabric Site] ウィンドウで、[Let's Do it] をクリックします。

ステップ 4 ファブリックサイトとして追加するエリア、建物、またはフロアを選択し、[Next] をクリックします。

ステップ 5 （オプション）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、[Yes Setup Zones] を選択します。

ファブリックゾーンを有効にするには、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 6 [Next] をクリックします。

ステップ 7 [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 8 [作成（Create）] をクリックします。

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、「Success!Your fabric site is created」というメッセージが表示されます。

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）。

1. Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Network Devices]** > **[Inventory]** の順に選択します。
2. [Inventory] ウィンドウに、検出されたデバイスが表示されます。
3. 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。
4. 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。
5. 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 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。
その結果表示されるウィンドウの [Fabric Sites] タブには、プロビジョニングされたすべてのサイトが表示されます。

ステップ 2 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 3 デバイスをクリックします。スライドインペインには、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	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。
Border	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	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。

デバイスを一体型ファブリックとして設定するには、[Control Plane]、[Border]、および [Edge] 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] と [Border] の両方を選択します。

ステップ 4 [Add] をクリックします。

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 （5 ページ）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。

ボーダーノードとしてデバイスを追加するには、次の手順を実行します。

ステップ 1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。
その結果表示されるウィンドウの [Fabric Sites] タブには、プロビジョニングされたすべてのサイトが表示されます。

ステップ 2 ボーダーノード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 3 デバイスをクリックします。

ステップ 4 表示されるスライドインウィンドウで、[Border] トグルボタンをクリックします。

ステップ 5 表示されたウィンドウで、[Layer 3 Handoff] タブをクリックします。

ステップ 6 [Enable Layer-3 Handoff] チェックボックスを選択します。

ステップ 7 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を変更することはできません。

ステップ 8 [Select IP 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。

IP プールは IP トランジットネットワークを追加する場合にのみ選択します。

ステップ 9 ボーダーデバイスで有効になっているトランジットネットワークを選択します。

a) ボーダーで SDA トランジットを有効にするには、[Select Transit/Peer Network] ドロップダウンリストからユーザーが作成した SDA トランジットドメインを選択します。

[Add] をクリックします。

b) ボーダーで IP トランジットを有効にするには、[Select Transit/Peer Network] ドロップダウンリストからユーザーが作成した IP トランジットドメインを選択します。

[Add] 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. デザイン階層から IP プールを選択します。選択したプールは、ボーダーノードと IP ピア間で IP ルーティングを自動化するために使用されます。
2. [インターフェイスの追加（Add Interface）] をクリックして、次の画面でインターフェイスの詳細を入力します。

3. ドロップダウン リストから [外部インターフェイス（External Interface）] を選択します。
4. [Interface Description] で、インターフェイスのカスタム説明を入力します。
5. [リモートAS番号（Remote AS Number）] を入力します。
6. リストで [仮想ネットワーク（Virtual Network）] をチェックします。この仮想ネットワークは、ボーダーによってリモート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。
7. **[Save]** をクリックします。

ステップ 10 デフォルトでは、ボーダーは外部ボーダーとして指定され、外部ルートをインポートせずに、すべての不明なトラフィックへのゲートウェイとして機能します。ボーダーを内部ボーダーとして設定すると、既知のトラフィックへのゲートウェイとして、特定の外部ルートをインポートするように設定できます。ボーダーには、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。

- ボーダーを外部ボーダーとして指定し、不明なネットワークへの接続を提供するには、[Default to all Virtual Networks] と [Do not Import External Routes] の両方のチェックボックスをオンにします。
- ボーダーを内部ボーダーとして指定し、特定のネットワークアドレスのゲートウェイとして動作させるには、[Default to all Virtual Networks] と [Do not Import External Routes] の両方のチェックボックスをオンにしないでください。
- この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。これは、エッジノードから送信されたすべての既知のトラフィックおよび不明なトラフィックへのゲートウェイとして機能します。（[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）。

ステップ 11 （オプション）ファブリックネットワークに非ファブリック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 SDA 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 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。

仮想ネットワークを選択すると、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が表示されます。非ファブリックデバイスを接続できるインターフェイスのリストも表示されます。

b) [External Interface] を選択してください。

Cisco DNA Center リリース 2.1.2.6 では、レイヤ 2 ハンドオフを実行できる複数のインターフェイスを選択できます。

c) [Interface Description] に説明を入力します。
d) ファブリックを拡張する必要がある [External VLAN] 番号を入力します。

Cisco DNA Center 2.1.2.6 より前のリリースでは、仮想ネットワークは 1 つのインターフェイスでのみハンドオフできます。複数のインターフェイス経由で同じ仮想ネットワークを処理することはできません。

Cisco DNA Center リリース 2.1.2.6 以降のリリースでは、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。

e) **[Save]** をクリックします。

ステップ 12 [Add] をクリックします。

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 Cisco DNA Center GUI で [Menu] アイコン（≡）をクリックして選択します、[SD ACCESS] で **[Provision]** > **[Fabric Sites]** の順に選択します。

ステップ 2 [Fabric Sites] タブで、LISP Pub/Sub を設定するサイトをクリックします。

[SITE] ウィンドウに、サイト要素の概要が表示されます。

ステップ 3 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 4 表示されるスライドインペインで、[Control Plane] トグルボタンをクリックして、このプレーンを設定します。

ステップ 5 [Configure Control Plane] ウィンドウで、[LISP PubSub] 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 6 [展開（Deploy）] をクリックします。

ステップ 7 [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 のトランジット ネットワークの作成

新しい IP トランジット ネットワークを追加するには、次の手順に従います。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（≡）をクリックし、**[Provision]** > **[Fabric]** の順に選択します。

ステップ 2 [Add Fabric or Transit/Peer Network] にマウスポインタを合わせます。

ステップ 3 ドロップダウンリストで [Transit/Peer Network] をクリックします。

ステップ 4 ネットワークのトランジットの名前を入力します。

ステップ 5 トランジット タイプとして、**IP ベース** 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 6 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 7 [Save] をクリックします。

SDA トランジット ネットワークの作成

新しい SDA トランジット ネットワークを追加するには、次の手順に従います。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[Provision]** > **[SD Access]** > **[Transits & Peer Networks]** の順に選択します。

ステップ 2 [Transits and Peer Networks] ウィンドウで、[Add Transit] をクリックします。

ステップ 3 [Transit/Peer Network] スライドインウィンドウで、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 [Transit/Peer Network Type] で SD-Access のトランジット/ピアネットワークタイプを選択します。

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 PubSub)] を選択してください。

SD-Access（LISP PubSub）トランジットを他の Cisco DNA Center 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） SD-Access（LISP Pub/Sub）トランジットは、他の 4 つの Cisco DNA Center ノードとだけ共有できます。

ステップ 5 ドロップダウンリストから [Site for the Transit Control Plane] 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**トランジット コントロール プレーン**を選択します。

ステップ 7 2 番目のマップサーバーを追加するには、手順 5 と手順 6 を繰り返します。

ステップ 8 [**保存（Save）**] をクリックします。

トランジットネットワークを作成すると、[Transits and Peer Networks] 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/BGP）** トランジットを追加することはできません。同様に、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。

次のタスク

ファブリックサイトを SDA 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。

ホスト オンボーディングの設定

[Host Onboarding] タブでは、ファブリック ドメインにアクセスできる各種デバイスまたはホストの設定を指定することができます。

[Host Onboarding] タブには次のサブタブがあります。

- [Authentication Template] タブ：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。認証テンプレートを選択したら、[Save] をクリックします。
- [Virtual Networks] タブ：IP アドレスプールを仮想ネットワーク（デフォルト、ゲスト、またはユーザー定義）に関連付け、[Update] をクリックします。表示される IP アドレス プールは、サイト固有のプールのみです。
- [Wireless SSIDs] タブ：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 を選択してアドレス プールを割り当て、[保存（Save）] をクリックできます。
- [Port Assignment] タブ：ファブリックドメイン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。これを行うには、固有の割り当てが必要なポートを選択し、[Assign] をクリックして、ドロップダウンリストからポートタイプを選択します。

  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、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）、および単一サーバー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。

認証テンプレートの選択

ファブリックドメイン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選択できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric]** の順に選択します。

ステップ 2 表示されたウィンドウで、ファブリックをクリックします。

ステップ 3 [Fabric Sites] ペインで、サイトを選択します。

ステップ 4 [Host Onboarding] タブをクリックします。

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

- **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。
- **認証なし**
- **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。

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、マクロまたは自動設定を使用して AP 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。

ウィンドウがスライドし、選択した認証方式のパラメータが表示されます：[First Authentication Order]、[802.1x to MAB Fallback]、[Wake on LAN]、[Number of hosts]。

（注） [Number of hosts] は、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。

必要な変更を行って、**[保存（Save）]** をクリックします。

編集ウィンドウが閉じます。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

[Select Port Assignment] タブで、ファブリックドメイン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。

（注） ここで行うポートの設定は、**[仮想ネットワーク（Virtual Networks）]** セクションで行ったデバイスの一般設定をオーバーライドします。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric]** の順に選択します。

ステップ 2 表示されたウィンドウで、ファブリックをクリックします。

ステップ 3 [Fabric Sites] ペインで、サイトを選択します。

ステップ 4 [Host Onboarding] タブで、[Port Assignment] タブをクリックします。

ステップ 5 左側のペインに表示されるファブリックデバイスのリストから、設定するデバイスを選択します。デバイスで使用可能なポートが右側のペインに表示されます。

ステップ 6 右側のペインで、デバイスのポートを選択し、[Assign] をクリックします。

ステップ 7 [Port Assignment] スライドインウィンドウで、次の項目を指定します。

- [IP Address Pool]：許可される IP アドレスプール
- [Scalable Group]：プロビジョニングされているグループ
- [IP Address Pool]：音声プールまたはデータプール
- [Authentication Template]：ポートで使用される認証テンプレート
- [Description]：ポートの説明

[更新（Update）] をクリックします。

ステップ 8 すべてのポートの割り当てが完了したら、[Deploy] をクリックします。

ファブリック ドメインのワイヤレス SSID の設定

ステップ 1 [Wireless SSID] セクションで、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 2 [Choose Pool] をクリックし、SSID の IP プール予約を選択します。

ステップ 3 [Assign SGT] ドロップダウンリストから、SSID のスケーラブルなグループを選択します。

ステップ 4 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。

仮想ネットワーク

仮想ネットワークは、独立したルーティングおよびスイッチング環境です。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。

仮想ネットワークに入れることができるのは、割り当てられたユーザー グループのみです。仮想ネットワーク内で、ユーザーとデバイスは、アクセス ポリシーによって明示的にブロックされていなければ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ユーザーは、相互に通信できません。ただし、例外ポリシーを作成して、一部のユーザーに異なる仮想ネットワークをまたぐ通信を許可することができます。

一般的な使用例はビルディング管理です。照明、冷暖房空調（HVAC）システム、セキュリティ システムなどのビルディング システムからユーザー コミュニティをセグメント化する必要があります。このケースでは、ユーザー コミュニティとビルディング システムを 2 つ以上の仮想ネットワークにセグメント化して、ビルディング システムの不正アクセスをブロックします。

仮想ネットワークは、複数のサイト ロケーションやネットワーク ドメイン（ワイヤレス、キャンパス、および WAN）にまたがる場合があります。

デフォルトでは、Cisco DNA Center には単一の仮想ネットワークがあり、すべてのユーザーおよびエンドポイントがこの仮想ネットワークに属しています。Cisco DNA Center が Cisco Identity Services Engine（ISE）と統合されると、デフォルトの仮想ネットワークに Cisco ISE のユーザー グループおよびエンドポイントが移入されます。

Cisco DNA Center では、仮想ネットワークの概念はワイヤレス、キャンパス、および WAN ネットワークで共通です。仮想ネットワークが作成されたら、ワイヤレス、有線、または WAN 導入が組み合わされているサイトと関連付けることができます。たとえば、ワイヤレス デバイスと有線デバイスが含まれるキャンパス ファブリックがサイトで展開されている場合、仮想ネットワークの作成プロセスによってキャンパス ファブリックでサービス セット識別子（SSID）と Virtual Routing and Forwarding（VRF）の作成がトリガーされます。また、サイトに WAN ファブリックも展開されている場合、VRF がキャンパスから WAN に同様に拡張します。

サイトの設計および初期設定時に、ワイヤレス デバイス、有線スイッチ、および WAN ルータをサイトに追加できます。Cisco DNA Center は、仮想ネットワークと関連付けられたポリシーがサイトに対して作成されたことを検出し、それらを異なるデバイスに適用します。

レイヤ 3 仮想ネットワークの作成

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Workflows]** > **[Create Layer 3 Virtual Network]** の順に選択します。

または、[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択して [Layer 3 VNs] タブに移動し、[Create Layer 3 VN] をクリックすることもできます。

ステップ 2 [Add Virtual Network] ワークフローウィンドウで、[Let's Do it] をクリックします。

ステップ 3 [Create Layer 3 Virtual Networks] ウィンドウで、作成するレイヤ 3 仮想ネットワークの数を入力します。

ステップ 4 [Next] をクリックします。

ステップ 5 レイヤ 3 仮想ネットワークの名前を入力し、[Next] をクリックします。

ステップ 6 レイヤ 3 仮想ネットワークをファブリックサイトおよびファブリックゾーンに関連付けるには、ドロップダウンリストからレイヤ3仮想ネットワークを選択し、対応するドロップダウンリストからファブリックサイトを選択します。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。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。

または、[By Fabric Site] タブで、ファブリックサイトに複数の仮想ネットワークを割り当てることができます。

ステップ 7 [Next] をクリックします。

ステップ 8 この仮想ネットワークが複数のファブリックサイトに関連付けられている場合のトラフィックの出口動作を設定します。

a) デフォルトでは、[Local Exit] が選択されています。これにより、関連付けられている各ファブリックサイトのローカルボーダーを通過してトラフィックが出るようになります。

b) 仮想ネットワークを位置指定し、指定された境界でトラフィックが出られるようにするには、[Remote Exit] を選択します。

関連付けられているファブリックサイトのリストから、この仮想ネットワークにおけるすべてのトラフィックに関して出口として機能するボーダーを持つサイトを選択します。関連付けられている他のファブリックサイトは、この仮想ネットワークを継承します。

ステップ 9 [Next] をクリックします。

ステップ 10 仮想ネットワークを設定する前に、[Summary] ウィンドウで仮想ネットワークの設定を確認します。

ステップ 11 仮想ネットワークのコンテキストを作成するには、[Create] をクリックします。

ステップ 12 選択したサイトに仮想ネットワークを割り当てるには、[Deploy] をクリックします。

ステップ 13 仮想ネットワークの作成を確認するには、[View All Virtual Networks] をクリックします。

ステップ 14 [Virtual Networks] ウィンドウに、ファブリックに含まれるすべてのレイヤ 3 仮想ネットワークの詳細情報が表示されます。

レイヤ 2 仮想ネットワークの作成

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Workflows]** > **[Create Layer 2 Virtual Network]** の順に選択します。

または、[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択して [Layer 2 VNs] タブに移動し、[Create Layer 2 VN] をクリックすることもできます。

ステップ2 [Create L2 Virtual Network] ウィンドウで、[Let's Do it] をクリックします。

ステップ3 ファブリックに接続する VLAN の数を入力します。

ステップ4 [Next] をクリックします。

ステップ5 [Configure VLANs] ウィンドウで、次の手順を実行します。

a) 各 VLAN の **VLAN 名**とオプションの **VLAN ID** を入力します。

b) [Traffic Type] ドロップダウンリストから、[Data] または [Voice] を選択します。
レイヤ 2 仮想ネットワークではフラッディングがデフォルトで有効になっています。

c) [Next] をクリックします。

ステップ6 [Select your CPs for each L2VN] ウィンドウで、作成した各レイヤ 2 仮想ネットワークのファブリックサイトとレイヤ 3 仮想ネットワークを選択します。

レイヤ 2 仮想ネットワークが複数のファブリックサイトに展開されている場合、Cisco DNA Center は、共通プールを使用してサブネットを拡張します。

ステップ7 [Next] をクリックします。

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ます。[作成（Create）] をクリックします。

ステップ9 レイヤ 2 仮想ネットワークのプロビジョニングを確認するために、[Submit] をクリックします。

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 レイヤ2仮想ネットワークの作成を確認するには、[Virtual Network Overview] をクリックします。[Virtual Networks] ウィンドウの [Layer 2] タブには、ファブリックに含まれるすべてのレイヤ2仮想ネットワークの詳細情報が表示されます。

ファブリックサイトへのレイヤ3仮想ネットワークの追加

ステップ1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ2 [Virtual Networks] ウィンドウの [SEGMENTS] で、**レイヤ 3 仮想ネットワーク**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、目的のレイヤ 3 仮想ネットワークについて、**[Actions (…)]** > **[Add to fabric site]** の順にクリックします。

ステップ4 [Select Fabric Site] スライドインウィンドウで、サイトを選択し、[Select] をクリックします。

この仮想ネットワークを別のファブリックサイトに追加するには、次の手順を実行します。

レイヤ 3 仮想ネットワークへのゲートウェイの追加

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Virtual Networks] ウィンドウの [SEGMENTS] で、**レイヤ 3 仮想ネットワーク**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、目的のレイヤ 3 仮想ネットワークについて、**[Actions (…)]** > **[Add gateways]** の順にクリックします。

[Add Pools to an L3VN] ウィンドウに、選択したレイヤ 3 仮想ネットワークが割り当てられているすべてのサイトが表示されます。

ステップ 4 [Add Pools to an L3VN] ウィンドウの左側のペインで、ゲートウェイを作成するレイヤ 3 仮想ネットワークを選択し、次の手順を実行します。

a) ドロップダウンリストから [IP Pool] を選択します。

（注） ファブリックサイトと同じサイトレベルで予約されている IP プールからのみ選択できます。ネットワーク設定を設計するときに、IP アドレスプールを予約できます。

b) [VLAN Name] に有効な VLAN 名を入力するか、[Auto generate VLAN name] を選択します。

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

VLAN ID については、次の点に注意してください。

- 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、Cisco DNA Center が 1021 ー 2020 の範囲の VLAN ID を生成します。

d) [Traffic Type] ドロップダウンリストから、[Data] または [Voice] を選択します。

e) [Scalable Group] ドロップダウンリストからグループを選択します。

f) レイヤ 2 フラッディングを有効にするには、[Flooding] トグルボタンをクリックします。

（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。

g) 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] トグルボタンをクリックします。

クリティカルプールは、認証サーバーを使用できない場合に、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。

h) 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、[Wireless] トグルボタンをクリックします。

i) IP ダイレクトブロードキャスト機能を有効にするには、[Directed Broadcast] トグルボタンをクリックします。

（注）
- IP ダイレクトブロードキャストを有効にする前に、レイヤ 2 フラッディングを有効にしてください。
- ルータおよび Nexus 7000 シリーズ スイッチは、IP ダイレクトブロードキャストをサポートしていません。
- IP 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。

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

k) [Next] をクリックします。

ステップ 5 [Summary] ウィンドウで、エンドポイントの接続設定を確認します。

ステップ 6 [Provisions in progress] ウィンドウで、[Submit] をクリックします。

ステップ 7 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、[Virtual Network overview] をクリックします。

ステップ 8 [Virtual Networks] ウィンドウ の [Segments] の下にある [Layer 2 VNs] タブに、すべてのレイヤ 2 仮想ネットワークとその詳細情報が表示されます。

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。Cisco DNA Center の以前のリリースから移行した場合は、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 and Fabric Zones] 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 （19 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、既存のファブリックサイトでのファブリックゾーンの作成 （20 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 （5 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。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あることに注意してください。詳細については、「ファブリックゾーンへの仮想ネットワークの追加 （20 ページ）」を参照してください。

（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 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。

ステップ 2 [Fabric Sites] タブで、[Add Fabric Site] をクリックします。

または、最初の 2 つの手順を実行する代わりに、Cisco DNA Center GUI で [Menu] アイコンをクリックし、**[Workflow]** > **[Create a Fabric Site and Fabric Zones]** の順に選択します。

ワークフローウィザードの指示に従います。

ステップ 3 [Create a Fabric Site] ウィンドウで、[Let’s Do it] をクリックします。

ステップ 4 ファブリックサイトとして追加するエリア、建物、またはフロアを選択し、[Next] をクリックします。

ステップ 5 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、[Yes Setup Zones] を選択します。

ファブリックゾーンを有効にするには、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 6 [Next] をクリックします。

ステップ 7 [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 8 [作成（Create）] をクリックします。

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。「**Success!**Your fabric site is created」という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。

既存のファブリックサイトでのファブリックゾーンの作成

ステップ 1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。

ステップ 2 [Fabric Sites] タブで、ファブリックサイトを選択します。

[Site] ウィンドウで、**[More Actions]** > **[Edit Fabric Zone]** をクリックします。

ステップ 3 [Designate fabric zones] 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、ビルディング、またはフロアを選択します。

ステップ 4 [Next] をクリックします。

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 [作成（Create）] をクリックします。

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。「**Success!**Your fabric site is created」という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デバイスと拡張ノードデバイスだけを追加します。

  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仮想ネットワークの追加

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。

ファブリックゾーンに追加できるのは親サイトの仮想ネットワークだけであることに注意してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Virtual Networks] ウィンドウの [SEGMENTS] で、**レイヤ 3 仮想ネットワーク**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 [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、ファブリックゾーンを選択します。

ステップ 5 [Layer 3] タブで、[Add Layer 3 VN] をクリックします。

ステップ 6 [Add Virtual Network] スライドインペインで、ファブリックゾーンに追加する仮想ネットワークを選択します。[更新（Update）] をクリックします。

ファブリックゾーンへのレイヤ 2 仮想ネットワークの追加

始める前に

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更新できないことに注意してください。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します[SD ACCESS] で **[Provision]** > **[Virtual Networks]** の順に選択します。

ステップ 2 [Virtual Networks] ウィンドウで、**レイヤ 2 仮想ネットワーク**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、ファブリックゾーンを選択します。

ステップ 5 [Layer 2] タブで、[Add Layer 2/ Gateways] をクリックします。

ステップ 6 [Select L2VNs/Gateway] スライドインペインで、ゲートウェイを設定するファブリックゾーンのレイヤ 3 仮想ネットワークを選択します。

ステップ 7 [Next] をクリックします。

ステップ 8 [L2VNs/Gateway(s)] ドロップダウンリストから、目的のゲートウェイを選択します。

ステップ 9 [Add] をクリックします。

拡張ノードデバイスの設定

拡張ノードはレイヤ2スイッチモードで動作するデバイスで、ファブリックテクノロジーをネイティブにはサポートしていません。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。拡張ノードでの [Port Assignment] は、[Host Onboarding] ウィンドウで実行できます。

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がサポートされています。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。

Cisco IOS XE 17.1.1s 以降のバージョンのソフトウェアを実行している Cisco Catalyst 産業用イーサネット 3400 および IE 3400 Heavy Duty シリーズスイッチは、ポリシー拡張ノードデバイスです。

Cisco 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 産業用イーサネット 4000、4010、5000 シリーズスイッチは、ポリシー拡張ノードデバイスではありません。ポート割り当て時の [Cisco TrustSec] と [Group] の選択はサポートされていません。

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。

ポリシー拡張ノードをサポートするエッジノードでサポートされているソフトウェアの最小バージョンは Cisco IOS XE 17.1.1 s です。

（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：IOS XE 17.1.1s
- Cisco Catalyst IE 3300 シリーズ スイッチ：IOS XE 16.12.1s
- Cisco Digital Building シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ：15.2(7)E0s

ポリシー拡張ノードを設定する前に、次のことを確認してください。

- 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 17.1.1 s です。
- ポリシー拡張ノードとそれをサポートするエッジノードの両方で、Network Advantage と 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。レイヤ 3 仮想ネットワークへのゲートウェイの追加 （17 ページ）を参照してください。[Pool Type] で [Extended] を選択します。

Cisco DNA 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 Cisco DNA 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]、[Low Impact]、または [Closed] の場合にのみ完了してください。ファブリックサイトが [No Authentication] 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) [Provision] > [Fabric Sites] > [Fabric Infrastructure] に移動し、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。タイトルにデバイス名の付いたウィンドウがスライド表示されます。
b) [Port Channel] タブで、[Create Port Channel] をクリックします。
c) 次のすべてのフィールドに入力します。

- [Connected Device Type] ロップダウンリストから [Extended Node] を選択します。
- [Port Aggregation Protocol (PAgP)] 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 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。
- 拡張ノードのオンボーディングでは Link Aggregation Control Protocol（LACP）は機能しないことに注意してください。
- 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。

d) [Done] をクリックします。

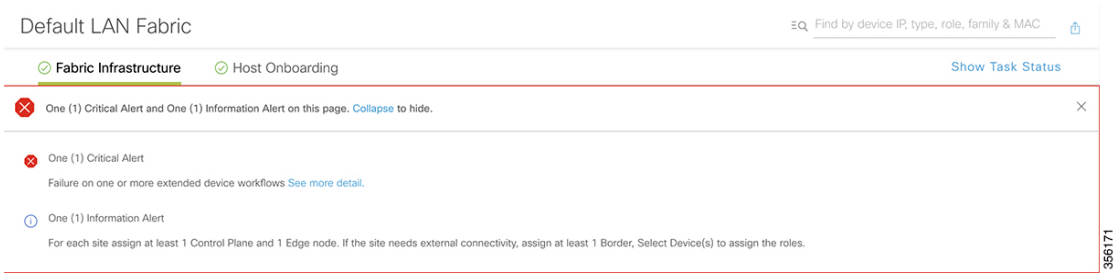
これで、ファブリックエッジノード（または拡張ノード）にポートチャネルが作成され、拡張デバイスがオンボードされます。

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設定がある場合は、以前の設定の書き込み消去を実行して、拡張ノードデバイスをリロードします。

Cisco DNA 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。

拡張ノードの設定中にワークフローでエラーが発生した場合は、[Topology] ウィンドウにバナーでエラー通知が表示されます。



[See more details] をクリックしてエラーを確認します。

[Task Monitor] ウィンドウがスライド表示され、拡張ノード設定タスクのステータスが表示されます。

[See Details] をクリックして、エラーの原因および考えられるソリューションを確認します。

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

認証がクローズド認証の場合にのみ、次の手順を実行します。他の認証モードでは、次の手順が自動化されていることに注意してください。

ステップ 1 [SD ACCESS] の下でCisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric Sites]**の順に選択します。

ステップ 2 表示された [Fabric Sites] ウィンドウで、ファブリックサイトをクリックします。

ステップ 3 [Fabric Infrastructure] タブに、すべてのファブリックデバイスが表示されます。

ステップ 4 ファブリックエッジノードをクリックします。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ 5 [Port Channel] タブで、[Create Port Channel] をクリックします。

ステップ 6 [Connected Device Type] ドロップダウンから、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。

ステップ 7 新しいポートチャネルの適切な説明を [Description] に入力します。

ステップ 8 適切な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 9 表示されたポートの一覧から、バンドルするポートを選択します。

（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 10 [Done] をクリックします。

作成した新しいポートチャネルがウィンドウに表示されます。

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 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]** > **[Fabric]** の順に選択します。

ステップ2 表示されたウィンドウで、ファブリックをクリックします。

ステップ3 [Fabric Sites] ペインで、サイトを選択します。

ステップ4 [Fabric Infrastructure] タブをクリックすると、すべてのファブリックデバイスが表示されます。

ステップ5 ファブリックエッジノードをクリックします。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ6 [Port Channel] タブを選択します。

ステップ7 表示されるポートチャネルのリストから、更新するポートチャネルを選択します。

結果のウィンドウに、選択したポートチャネルのすべてのインターフェイスとステータスが表示されます。

ステップ8 ポートチャネルで必要な更新を実行します。

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9 [Done] をクリックします。

ポートチャネルの削除

ステップ1 Cisco DNA Center GUI で、[Menu] アイコン（☰）をクリックし、**[Provision]** > **[Fabric]** > **[Fabric Infrastructure]** の順に選択します。

ステップ2 ポートチャネルを削除するデバイスをクリックします。

デバイス名の付いたウィンドウがスライド表示されます。

ステップ3 [Port Channel] タブをクリックします。

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

ステップ4 ポートチャネルを選択し、[Delete] をクリックします。

ステップ5 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

Cisco DNA 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。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します**[Provision]**。
すべてのプロビジョニングされたファブリックドメインがウィンドウに表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。ファブリックに設定されているすべてのサイトが表示されます。マルチキャストを設定するサイトを選択します。

ステップ 3 [Fabric Sites] ペインで、選択したサイトの横にある歯車アイコンをクリックします。

ステップ 4 ドロップダウンリストから [Configure Multicast] を選択します。

マルチキャスト構成のワークフローの最初のウィンドウが表示されます。

ステップ 5 [Enabling Multicast] ウィンドウで、ネットワークのマルチキャスト実装方式（[Native Multicast] または [Head-end replication]）を選択し、[Next] をクリックします。

ステップ 6 [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。[Next] をクリックします。

ステップ 7 [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。[Next] をクリックします。

ステップ 8 [Select multicast type] 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、[Next] をクリックします。

- **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）

ステップ 9 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. 225.0.0.0 ～ 239.255.255.255 の IP グループ範囲を選択します。
   2. IP グループの [Wildcard Mask] を入力します。
   3. [Next] をクリックします。

b) [ASM] を選択した場合は、ランデブーポイント（RP）のタイプを選択します。

   - **内部 RP**
   - **外部 RP**

[次へ (Next)] をクリックします。

ステップ 10 ランデブーポイントを設定するには、次の手順を実行します。

内部ランデブーポイントを設定する場合は、次のようにします。

a) 内部ランデブーポイントとして設定する必要があるデバイスを選択します。選択した 2 番目のランデブーポイントは、冗長ランデブーポイントになります。**[次へ (Next)]** をクリックします。
b) 一覧表示されている各仮想ネットワークに内部ランデブーポイントを割り当てます。[Next] をクリックします。

外部ランデブーポイントを設定する場合は、次のようにします。

a) [Setup your External RP] ウィンドウで、外部ランデブーポイントの IPv4 または IPv6 アドレスを入力します。

   （オプション）2 番目の IPv4 または IPv6 アドレスのセットを入力できます。

   [Next] をクリックします。

b) [Select which RP IP Address(es) to utilize] ウィンドウで、各仮想ネットワークの IP アドレスを選択します。

   [Next] をクリックします。

ステップ 11 構成を送信する前に、[Summary] ウィンドウに表示されているマルチキャスト設定を確認し、必要に応じて変更します。

[Finish] をクリックして、マルチキャストの設定を完了します。

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。