前提条件：オーケストレータ

Orchestrator の要件

（注） このセクションでは、Orchestratorサービスを有効にする場合の追加の要件とガイドラインについて説明します。前提条件とガイドライン セクションに記載されているプラットフォーム レベルの要件をすでに満たしていることを確認します。

- Nexus Dashboard リリース 3.1.1 以降、サービスを個別にダウンロードする必要がなくなったため、Cisco DC App Center 接続は Nexus Dashboard から削除されました。

  Orchestrator を展開するには、[ソフトウェアのダウンロード（Software Download）]ページから統合インストール イメージをダウンロードします。個々のサービスのインストール イメージは、Cisco DC App Center から入手できなくなりました。

- Cisco ACI ファブリックを管理するために Nexus Dashboard Orchestrator を展開する場合は、データ インターフェイスまたは管理インターフェイスから各サイトの APIC のインバンドまたはアウトオブバンド（OOB）インターフェイスまたは両方への接続を確立できます。

  ファブリック接続がNexusダッシュボードの管理インターフェイスからのものである場合は、特定のスタティック ルートを設定するか、管理インターフェイスが APIC インターフェイスの同じ IP サブネットの一部であることを確認する必要があります。

- Cisco NDFC ファブリックを管理するために Nexus Dashboard Orchestrator を展開する場合は、データネットワークから Cisco NDFC サイトにインバンドで到達できる必要があります。

- 両方のネットワークでノード間の接続が必要です。そして、次の追加のラウンドトリップ時間（RTT）要件があります。

表 *1 : Orchestrator RTT* の要件

接続	最大 RTT
管理対象 APIC サイトへ	500 ミリ秒
管理対象 NDFC サイトへ	150 ミリ秒

Orchestrator の通信ポート

上記の Nexus Dashboard クラスタ ノードに必要なポート（前のセクションに記載）に加えて、Orchestrator サービスには次のポートが必要です。

表 *2 : Nexus Dashboard Orchestrator* ポート（管理ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
SCP または SFTP	22	TCP	入力 / 出力	バックアップを保存し、ソフトウェア アップグレード イメージをダウンロードするためのリモート サーバー
HTTP	80	TCP	発信	外部ログストリーミングが有効になっている場合は、Splunk または syslog サーバー
HTTPS	443	TCP	入力 / 出力	外部ログストリーミングが有効になっている場合は、Splunk または syslog サーバー

表 *3 : Nexus Dashboard Orchestrator* ポート（データ ネットワーク）

サービス	ポート	プロトコル	方向 イン：クラスタに対して アウト：クラスタからファブリックまたは世界外に対して	接続
HTTPS	443	TCP	発信	スイッチと APIC の帯域内

オーケストレータのファブリック要件

次の追加のファブリック関連のガイドラインがオーケストレータ サービスに適用されます。

- Cisco Mini ACI ファブリックは、追加の設定を必要とせずに、一般的なオンプレミス サイトとしてサポートされます。

  このタイプのファブリックの導入と設定に関する詳細情報は、*Cisco Mini ACI* ファブリックおよび仮想 *APIC*に記述されています。

- リモート リーフ スイッチを含む ACI ファブリックを管理している場合は、次の制限が適用されます。
  - 物理リモート リーフ スイッチのみがサポートされます。
  - -EX および -FX 以降のスイッチのみが、リモート リーフ スイッチとしてサポートされています。
  - リモート リーフは、IPN スイッチを使用しないバックツーバック接続サイトではサポートされていません。
  - 1 つのサイトのリモート リーフ スイッチで別のサイトの L3Out を使用することはできません。
  - あるサイト（ローカル リーフまたはリモート リーフ）と別のサイトのリモート リーフ間のブリッジ ドメインの拡張はサポートされていません。

  また、Nexus Dashboard Orchestrator でサイトを追加して管理するには、その前に次のタスクを実行する必要があります。

  - サイトの APIC でリモート リーフの直接通信を直接有効にする必要があります。

    直接通信を有効にするには、サイトの APIC にログインし、**[システム（System）]**>**[システム設定（System Settings）]**>**[ファブリック全体の設定（Fabric Wide Setting）]**

を選択し、**[リモート リーフ直接トラフィック転送を有効にする（Enable Remote Leaf Direct Traffic Forwarding）]** をオンにします。

（注） 有効にした後は、このオプションを無効にすることはできません。

- リモート リーフ スイッチの外部 TEP プールを設定する必要があります。

  1 つ以上の外部 TEP プールを設定するには、サイトの APIC にログインし、**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[ポッド ファブリック セットアップ ポリシー（Pod Fabric Setup Policy）]**に移動します。次に、サブネットを設定するポッドをダブルクリックし、**[外部 TEP（External TEP）]** 領域で **[+]** をクリックします。最後に、**[IP]**アドレスと**[予約アドレスの数（Reserve Address Count）]**を入力し、状態を [アクティブ（Active）] または [非アクティブ（Inactive）] に設定してから、**[更新（Update）]** をクリックしてサブネットを保存します。

  ルーティング可能な TEP プールを設定する場合は、 /22 から /29 の範囲のネットマスクを指定する必要があります。異なる時点を含め、複数の非連続外部 TEP プールを設定できます。

- リモート リーフ スイッチに接続しているレイヤ 3 ルータのインターフェイスに適用されている DHCP リレー設定で、APIC ノード（定義済み外部 TEP プールから割り当てられたもの）のルーティング可能な IP アドレスを追加する必要があります。

  各 APIC ノードのルーティング可能な IP アドレスは、APIC GUI の **[システム（System）]** > **[コントローラ（Controllers）]** > **[<controller-name>]**画面の **[ルーティング可能 IP アドレス（Routable IP Address）]** フィールドに表示されます。

- 次のセクションの説明に従って、ポッド プロファイル、ポリシー グループ、およびファブリック アクセス ポリシーを設定する必要があります。

ポッド プロファイルとポリシー グループ

各サイトの APIC には、ポッド ポリシー グループを持つポッド プロファイルが 1 つ必要です。サイトにポッド ポリシー グループがない場合は、作成する必要があります。通常、これらの設定はすでに存在していて、ファブリックを最初に展開したときに設定したとおりになっているはずです。

手順

ステップ 1 サイトの APIC GUI にログインします。

ステップ 2 ポッド プロファイルにポッド ポリシー グループが含まれているかどうかを確認します。

[ファブリック (Fabric)] > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[プロファイル (Profiles)]** > **[ポッドのプロファイルのデフォルト (Pod Profile default)]**に移動します。

ステップ 3 必要であれば、ポッド ポリシー グループを作成します。

a) **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[ポリシー グループ (Policy Groups)]**に移動します。

b) **[ポリシー グループ (Policy Groups)]** を右クリックし、**[ポッド ポリシー グループの作成 (Create Pod Policy Groups)]** を選択します。

c) 適切な情報を入力して、[Submit] をクリックします。

ステップ 4 新しいポッド ポリシー グループをデフォルトのポッド プロファイルに割り当てます。

a) **[ファブリック (Fabric)]** > **[ファブリック ポリシー (Fabric Policies)]** > **[ポッド (Pods)]** > **[プロファイル (Profiles)]** > **[ポッド プロファイルのデフォルト (Pod Profile default)]** に移動します。

b) デフォルトのプロファイルを選択します。

c) 新しいポッド ポリシー グループを選択し、**[更新 (Update)]** をクリックします。

ファブリック アクセス グローバル ポリシーの設定

このセクションでは、Nexus Dashboard クラスタにオンボードし、Nexus Dashboard Orchestrator で管理する前に、APIC サイトごとに作成する必要があるグローバル ファブリック アクセス ポリシーの設定について説明します。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

サイトを Nexus Dashboard Orchestrator で管理するには、いくつかのファブリック ポリシーを設定する必要があります。APIC の観点からは、ベアメタル ホストを接続していた場合と同様に、ドメイン、AEP、ポリシー グループ、およびインターフェイス セレクタを設定することができます。同じマルチサイト ドメインに属するすべてのサイトに対して、スパインスイッチインターフェイスをサイト間ネットワークに接続するための同じオプションを設定する必要があります。

ステップ 3 VLAN プールを指定します。

最初に設定するのは、VLANプールです。レイヤ3サブインターフェイスはVLAN4を使用してトラフィックにタグを付け、スパインスイッチをサイト間ネットワークに接続します。

a) 左側のナビゲーション ツリーで、**[プール (Pools)]** > **[VLAN]** を参照します。

b) **[VLAN]** カテゴリを右クリックし、**[VLAN プールの作成 (Create VLAN Pool)]** を選択します。

[**VLAN プールの作成 (CREATE VLAN Pool)**] ウィンドウで、次の項目を指定します。

- [**名前 (name)**] フィールドで、VLAN プールの名前 (たとえば、 `msite`) を指定します。

- [**Allocation Mode (割り当てモード)**]の場合は、[スタティック割り当て(Static Allocation)]を指定します。
- [**Encap ブロック(Encap Blocks)**] の場合は、単一の VLAN 4 だけを指定します。両方の [**Range (範囲)**] フィールドに同じ番号を入力することによって、単一の VLAN を指定できます。

ステップ 4 接続可能アクセス エンティティ プロファイル (AEP) を作成します。

a) 左側のナビゲーションツリーで、**[グローバル ポリシー (Global Policies)]** > **[接続可能なアクセス エントリ プロファイル (Attachable Access Entity Profiles)]** を参照します。

b) **[接続可能なアクセス エンティティ プロファイル (Attachable Access Entry Profiles)]** を右クリックして、**[接続可能なアクセス エンティティ プロファイルの作成 (Create Attachable Access Entity Profiles)]** を選択します。

[接続可能アクセス エンティティ プロファイルの作成(Create Attachable Access Entity Profiles)]] ウィンドウで、AEP の名前 (例：`msite-aep`) を指定します。

c) [**次へ(Next)]**] をクリックして [**送信(Submit)**] します。

インターフェイスなどの追加の変更は必要ありません。

ステップ 5 外部ルーテッド ドメインを設定します。

設定するドメインは、このサイトを追加するときに、Nexus Dashboard Orchestratorから選択するものになります。

a) ナビゲーション ツリーで、**[物理的ドメインと外部ドメイン (Physical and External Domains)]** > **[外部でルーテッド ドメイン (External Routed Domains)]** を参照します。

b) [**外部ルーテッド ドメイン(External Routed Domains)**] カテゴリを右クリックし、[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] を選択します。

[**レイヤ 3 ドメインの作成 (Create Layer 3 Domain)**] ウィンドウで、次の項目を指定します。

- [**名前 (name)**] フィールドで、ドメインの名前を指定します。たとえば、 `msite-l3`です。
- **関連付けられている接続可能エンティティ プロファイル**の場合は、ステップ 4で作成した AEP を選択します。
- **VLAN プール**の場合は、ステップ 3で作成した VLAN プールを選択します。

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

次のタスク

グローバル アクセス ポリシーを設定した後も、ファブリック アクセス インターフェイス ポリシーの設定 （7 ページ） の説明に従って、インターフェイス ポリシーを追加する必要があります。

ファブリック アクセス インターフェイス ポリシーの設定

このセクションでは、各 APIC サイトの Nexus Dashboard Orchestrator で行わなければならないファブリック アクセス インターフェイスの設定について説明します。

始める前に

サイトの APIC では、ファブリック アクセス グローバル ポリシーの設定 （5 ページ） の説明に従って、VLAN プール、AEP、および ドメインなどのグローバル ファブリック アクセス ポリシーを設定しておく必要があります。

手順

ステップ 1 サイトの APIC GUI に直接ログインします。

ステップ 2 メイン ナビゲーション メニューから、**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** を選択します。

前のセクションで設定した VLAN、AEP、およびドメインに加えて、サイト間ネットワーク (ISN) に接続するファブリックのスパイン スイッチ インターフェイスに対してインターフェイス ポリシーを作成します。

ステップ 3 スパイン ポリシー グループを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policie)]** > **[ポリシー グループ (Policy Groups)]** > **[スパイン ポリシー グループ (Spine Policy Groups)]** を参照します。

これは、ベアメタルサーバを追加する方法と類似していますが、リーフ ポリシー グループの代わりにスパイン ポリシー グループを作成する点が異なります。

b) **[スパイン ポリシー グループ (Spine Policy Groups)]** カテゴリーを右クリックして、**[スパイン アクセス ポート ポリシー グループの作成 (Create Spine Access Port Policy Group)]** を選択します。

[**スパイン アクセス ポリシー グループの作成 (Create Spine Access Port Policy Group)**]ウィンドウで、以下のとおり指定します。

- **[名前 (Name)]** フィールドの場合、ポリシー グループの名前を指定します。たとえば `Spine1-PolGrp` です。
- [**リンク レベル ポリシー (Link Level Policy)**] フィールドには、スパイン スイッチと ISN の間のリンク ポリシーを指定します。
- **[CDP ポリシー (CDP Policy)]** の場合、CDP を有効にするかどうかを選択します。
- **[添付したエンティティ プロファイル (Attached Entity Profiel)]**の場合、前のセクションで設定した AEP を選択します。たとえば `msite-aep` です。

c) [**送信 (Submit)**] をクリックします。

セキュリティ ドメインなどの追加の変更は必要ありません。

ステップ 4 スパイン プロファイルを設定します。

a) 左ナビゲーション ツリーで、**[インターフェイス ポリシー (Interface Policies)]** > **[ポリシー グループ (Profiles)]** > **[スパイン ポリシー グループ (Spine Profiles)]** を参照します。

b) **[プロファイル (Profiles)]** カテゴリを右クリックし、**[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のとおり指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前 (`Spine1`など) を指定します。
- **[インターフェイス セレクタ (Interface Selectors)]**では、+ 記号をクリックして、ISN に接続されるスパイン スイッチ上のポートを追加します。次に、**[スパイン アクセス ポート セレクターの作成 (Create Spine Access Port Selector)]** ウィンドウで、次のように指定します。
  - **[名前 (name)]** フィールドに、ポート セレクタの名前を指定します (例: `Spine1`)。
  - **[インターフェイス ID (Interface IDs)]** に、ISN に接続するスイッチ ポートを指定します (例 `5/32`)。
  - **[インターフェイス ポリシー グループ (Interface Policy Group)]** に、前の手順で作成したポリシー グループを選択します (例: `Spine1-PolGrp`)。

それから、**[OK]** をクリックして、ポート セレクタを保存します。

c) **[送信 (Submit)]** をクリックしてスパイン インターフェイス プロファイルを保存します。

ステップ 5 スパイン スイッチ セレクター ポリシーを設定します。

a) 左ナビゲーション ツリーで、**[スイッチ ポリシー (Switch Policies)]** > **[プロファイル (Profiles)]** > **[スパイン プロファイル (Spine Profiles)]** を参照します。

b) **[スパイン プロファイル (Spine Profiles)[** カテゴリを右クリックし、**[スパイン プロファイルの作成 (Create Spine Profile)]** を選択します。

[スパイン インターフェイス プロファイルの作成 (Create Spine Interface Profile)] ウィンドウで、次のように指定します。

- **[名前 (name)]** フィールドに、プロファイルの名前を指定します (例: `Spine1`)。
- **[スパインセレクタ (Spine Selectora)]**で、**[+]** をクリックしてスパインを追加し、次の情報を入力します。
  - **[名前 (name)]** フィールドで、セレクタの名前を指定します (例: `Spine1`) 。
  - **[ブロック (Blocks)]** フィールドで、スパイン ノードを指定します (例: `201`)。

c) **[更新 (Update)]** をクリックして、セレクタを保存します。

d) **[次へ (Next)]** をクリックして、次の画面に進みます。

e) 前の手順で作成したインターフェイス プロファイルを選択します。

たとえば、`Spine1-ISN`などです。

f) **[完了 (Finish)]** をクリックしてスパイン プロファイルを保存します。

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。