改訂：2026 年 10 月 26 日

Cisco Nexus Hyperfabric — スタートアップガイド

Cisco Nexus HyperFabric

Cisco Nexus HyperFabric は、クラウドベースのサービスによって管理される物理ネットワークの設計と構築を可能にする、facric-as-a-service ソリューションです。ネットワークは 1 つのスイッチのように小さく始めて、それぞれが多くのスイッチのファブリックを持つ複数の場所に拡大できます。

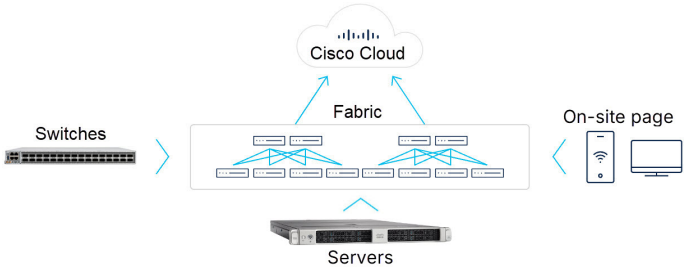
Cisco Nexus HyperFabric の設計、展開、および運用は、お客様とシスコの共有責任モデルに基づいています。シスコの自動化および運用スタッフが、クラウドベースのサービスを適切に機能させ、ソフトウェア アップグレード プロセスを管理します。お客様のスタッフは、スイッチのアップグレードのタイミングと、アプリケーション、ホスト、国内ネットワークとのすべての相互接続、およびクラウドベースのサービスへの接続のタイミングを直接制御します。

Cisco Nexus Hyperfabric 展開のコンポーネント

Cisco Nexus HyperFabric 展開を構成するのは、以下のコンポーネントです。

- Cisco Nexus HyperFabric サービス：スケーラブルで、グローバルに分散された、マルチテナントのクラウドベースの software-as-a-service（SaaS）ネットワーク インフラストラクチャ管理ソリューションです。Cisco Nexus HyperFabric サービスは、Cisco によってホストおよび運用されており、ファブリックのプロビジョニングと可視化のための単一ポイントです。組織は、デバイス テレメトリとサービスが存在する場所を決定する、特定の地理的リージョン内に作成されます。
- Cisco Nexus HyperFabric スイッチ：オンプレミスまたはコロケーション環境内のクラウド管理型 Cisco 6000 スイッチです。スイッチのブートストラップと管理は、クラウドベースのサービスによって処理されます。
- 高性能ファブリック：EVPN VXLAN、レイヤ 2 VLAN、または IPv4/IPv6 ルーティングを使用するメッシュ トポロジまたはスパイン リーフ トポロジです。
- グラフィカル ユーザ インターフェイス（GUI）および REST API：Cisco Nexus HyperFabric でタスクを実行するために使用できるインターフェイス。
- オンサイト ページ：ネットワーク ケーブル配線技術者が、ファブリック内のデバイスを要求、バインド、ケーブル接続するための段階的なタスクを提供します。このページでは、ファブリック トポロジのリアルタイム検証も提供されます。
- Cisco UCS サーバ：（オプション）クラウドでモニターされる Cisco UCSC-C225-M8N-1P サーバ（ストレージ用）および Cisco UCSC-885A-M8-HC1 サーバ（オンプレミスまたはコロケーション環境の GPU 用）。スイッチのブートストラップと管理は、クラウドベースのサービスによって処理されます。

図 *1 : Cisco Nexus HyperFabric* のコンポーネント



Cisco Nexus HyperFabric の仕組み

これは Cisco Nexus HyperFabric の仕組みの全体的なプロセスです。

1. Cisco Nexus HyperFabric チームと協力して、Cisco Nexus HyperFabric GUI で提供される自動設計ツールを使用してファブリックをオンラインで設計します。完成した設計は、新しいファブリックの ブループリント です。
2. ファブリックのブループリントが完了すると、Cisco Nexus HyperFabric は次の追加のリソースを生成します。
   - サーバとスイッチや、直接接続ケーブル（DAC）とアクティブ光ケーブル（AOC）などのプラガブルモジュールを含む、必要なファブリック コンポーネントを購入するための詳細な部品表（BoM）
   - 設置者がファブリックを配線するための完全なケーブル配線計画
3. コンポーネントを受け取ったら、**オンサイト**のページの指示に従って、設置担当者がそれらのコンポーネントを物理的に配線します。
4. 新しい各デバイスには、Cisco Nexus HyperFabric に接続できるエージェントが含まれています。1 つのスイッチの管理ポートを設定し、そのポートに外部インターネット接続を提供します。その後、スイッチは Cisco Nexus HyperFabric に接続します。このインターネットに接続されたスイッチは、「出口ノード」と呼ばれます。
5. エージェントにより、各デバイスはネイバーを検出して認証できます。各デバイスはファブリック内の出口ノードへのパスを検出します。デバイスは出口ノードを介してサービスと接続します。
6. デバイスを接続して準備ができたら、各デバイスを所有する組織を指定して、各デバイスをオンラインで Cisco に登録（「要求」）します。

（注）

場合によっては、デバイスが 組織によってすでに要求されていることもあります。

7. Cisco Nexus HyperFabric では、各物理スイッチをファブリック ブループリントの論理的な場所（「ノード」）に割り当てます（バインド）。スイッチをブループリントのノードにバインドすると、デバイスは Cisco Nexus HyperFabric から構成をダウンロードできます。
8. ファブリックが完全にプロビジョニングされたら、ローカル ホストとサーバをファブリックに接続できます。

デバイス テレメトリ

Cisco Nexus HyperFabric は、次のデバイス統計情報についてほぼリアルタイムのテレメトリを提供します。

- スイッチまたはサーバ：ポート ステータス、アサーション、およびトラフィック統計
- インターフェイス：ポート カウンタ、リンク ステータス、およびネットワーク設定
- 環境：ファン、PSU、およびその他のコンポーネントのスイッチごとのセンサー読み取り値
- 光ファイバおよびプラガブル：デジタル オプティカル モニタリング（DOM）統計

Nexus HyperFabric の使用例

Cisco Nexus HyperFabric の一般的な使用例には、小規模から中規模のブランチ オフィス、またはオンプレミス管理を必要としないリモート コロケーション サイトなどがあります。Cisco Nexus HyperFabric は、次のようなニーズを満たすのに最適です。

- 新しいデータセンターファブリックを展開または拡張する、または新しいデータセンターファブリックを簡単に構築できる。
- 基本的なネットワーク要件とコンピューティング接続を使用して、確実かつ迅速に展開する
- 新しいデータセンターネットワークを簡単に設計し、時間の経過とともに進化させる
- 1 つまたは 2 つのスイッチからなる小規模なスパインレス ファブリックを展開する
- AI クラスタへの新しいファブリックの展開を容易にする
- シームレスに展開し、分散データセンターをエッジまたはコロケーションに拡張する
- アーキテクチャを制限することなく、小規模でファブリックを開始してシームレスに拡張することを可能にする

サポートされるトポロジ

Cisco Nexus HyperFabric は次のネットワークトポロジをサポートします。

- 単一のスイッチまたは冗長スイッチ ペア詳細については、トポロジ：単一のリーフ スイッチまたは冗長スイッチ ペア （4 ページ）を参照してください。
- 小規模メッシュ ファブリック詳細については、トポロジ：2~6 台のリーフ スイッチがある小規模なメッシュ ファブリック （5 ページ）を参照してください。
- スパインおよびリーフ ファブリック。多層ファブリックを含むことができます。詳細については、トポロジ：1 ~ 4 台のスパイン スイッチと 1 台以上のリーフ スイッチを備えた 2 階層または 3 階層ファブリック （7 ページ）を参照してください。
- スーパー スパイン ファブリック。詳細については、トポロジ：スーパー スパイン ファブリック （9 ページ）を参照してください。

サイトが拡大した場合、Cisco Nexus HyperFabric の設計ツールに再アクセスして更新されたブループリントを作成することで、必要に応じてトポロジを変更できます。

トポロジのサブセクションの図では、ケーブル接続がさまざまなデバイスグループを結合する色付きの線で示されています。ケーブルの各数字は、デバイス グループ間の接続数を示します。

トポロジ：単一のリーフ スイッチまたは冗長スイッチ ペア

ホスト数が 50 未満のサイトでは、1 つのリーフスイッチで十分な場合があります。高可用性のために、冗長構成で 2 番目のスイッチを展開できます。

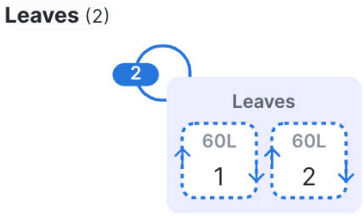
図 *2*：単一のリーフ スイッチ



図 *3*：冗長スイッチ ペアの図



図 *4*：冗長スイッチ ペア



冗長スイッチ ペアの構成の概要

次のステップのハイレベル リストでは、冗長スイッチ ペアの構成の概要を示します。

1. デフォルトのスイッチ階層で、そのグループのスイッチ数を 2 に設定します。
2. **[グループ接続（Group connections）]** の下の **[スイッチ グループ（Switch group）]** で、接続数を 2 に設定します。

トポロジ：2～6 台のリーフ スイッチがある小規模なメッシュ ファブリック

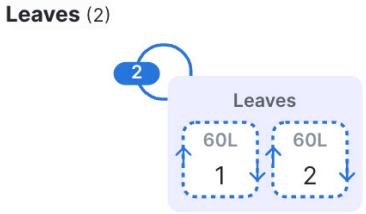
小規模メッシュ ファブリックは、エッジ データ センターや人工知能（AI）クラスタなどの小規模な高性能環境を対象としています。このファブリックには、スパイン スイッチのない 2～6 台の相互接続されたリーフ スイッチがあり、ほとんどの場合、ファブリック全体で同等の冗長性を確保するためにスイッチをペアで展開する必要があります。

存在するアップリンク ポートの数に応じて、拡張性を増大させることができます。6 台のリーフ スイッチを超えたら、2 階層ファブリックのスパイン スイッチ、または 3 階層ファブリックの場合にスパイン スイッチと別のリーフスイッチ階層を追加できます。多層ファブリックの詳細については、トポロジ：1~4 台のスパイン スイッチと 1 台以上のリーフ スイッチを備えた 2 階層または 3 階層ファブリック （7 ページ） を参照してください。

図 *5：2* 台のリーフ スイッチがある小規模なメッシュ ファブリックの図



図 *6：2* 台のリーフ スイッチがある小規模なメッシュ ファブリック



2 台のリーフ スイッチがある小規模なメッシュ ファブリックの構成の概要

この手順の概略的なリストでは、2 台のリーフ スイッチがある小規模なメッシュ ファブリックの構成の概要を示します。

1. デフォルトのスイッチ階層で、そのグループのスイッチ数を 2 に設定します。
2. **[グループ接続（Group connections）]** の下の **[スイッチ グループ（Switch group）]** で、接続数を 2 に設定します。

図 *7：4* 台のリーフ スイッチがある小規模なメッシュ ファブリックの図

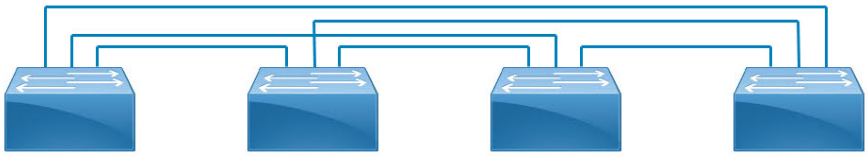


図 *8 : 4* 台のリーフ スイッチがある小規模なメッシュ ファブリック



4 台のリーフ スイッチがある小規模なメッシュ ファブリックの構成の概要

この手順の概略的なリストでは、4 台のリーフ スイッチがある小規模なメッシュ ファブリックの構成の概要を示します。

1. デフォルトのスイッチ階層で、そのグループのスイッチ数を 4 に設定します。
2. **[グループ接続（Group connections）]** の下の **[スイッチ グループ（Switch group）]** で、接続数を 1 に設定します。

図 *9 : 6* 台のリーフ スイッチがある小規模なメッシュ ファブリックの図

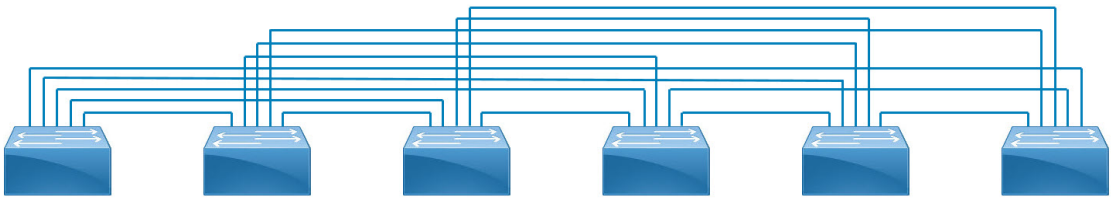
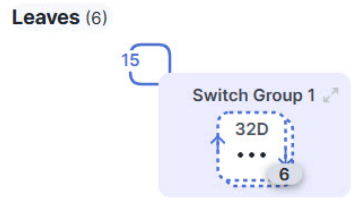


図 *10 : 6* 台のリーフ スイッチがある小規模なメッシュ ファブリック



6 台のリーフ スイッチがある小規模なメッシュ ファブリックの構成の概要

この手順の概略的なリストでは、6 台のリーフ スイッチがある小規模なメッシュ ファブリックの構成の概要を示します。

1. デフォルトのスイッチ階層で、そのグループのスイッチ数を 6 に設定します。
2. **[グループ接続（Group connections）]** の下の **[スイッチ グループ（Switch group）]** で、接続数を 1 に設定します。

トポロジ：1～4 台のスパイン スイッチと 1 台以上のリーフ スイッチを備えた 2 階層または 3 階層ファブリック

スパインおよびリーフ ファブリックは、最初の階層として 1～4 つのスパイン スイッチを持ち、第 2 階層として 1 つ以上のリーフ スイッチを持つ 2 階層トポロジにすることができます。また、第 2 階層のリーフスイッチに接続された第 3 階層として追加のリーフスイッチがある 3 階層トポロジも考えられます。

図 *11*：*2* つのスパイン スイッチと *2* つのリーフ スイッチを備えた *2* 階層ファブリックの図

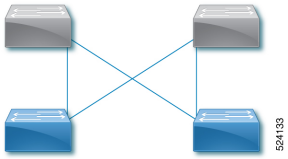
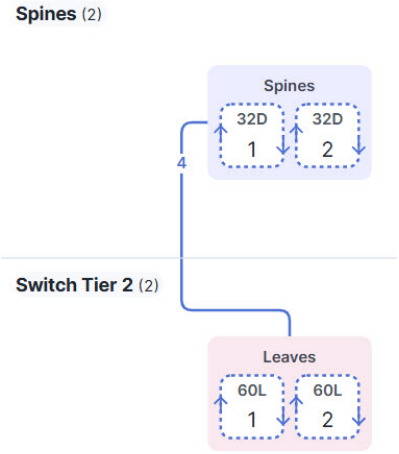


図 *12*：*2* つのスパイン スイッチと *2* つのリーフ スイッチを備えた *2* 階層ファブリック



2 つのスパイン スイッチと 2 つのリーフ スイッチを備えた 2 階層ファブリックの概要

このステップの概略リストでは、2 つのスパイン スイッチと 2 つのリーフ スイッチを備えた 2 階層ファブリックの構成の概要を示します。

1. スパイン スイッチでは、デフォルトのスイッチ階層を使用し、そのグループでスイッチの数量を 2 に設定します。
2. リーフ スイッチでは、新しいスイッチ階層を追加し、そのグループでのスイッチの数を 2 に設定します。
3. **[グループ接続（Group connections）]** の下の **[スイッチ グループ（Switch group）]** で、リーフ スイッチ グループからスパイン スイッチ グループへの接続数を 1 に設定します。

図 *13*：階層 *1* に *2* つのスパイン スイッチ、階層 *2* に *4* つのリーフ スイッチ、階層 *3* に *2* つのリーフ スイッチを備えた *3* 階層ファブリックの図

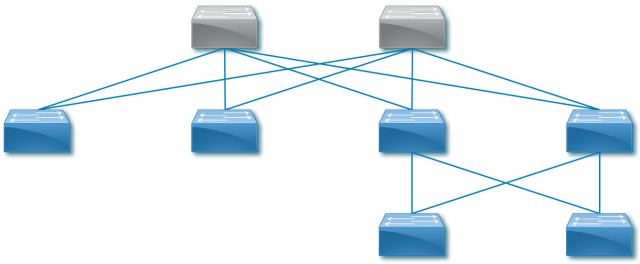
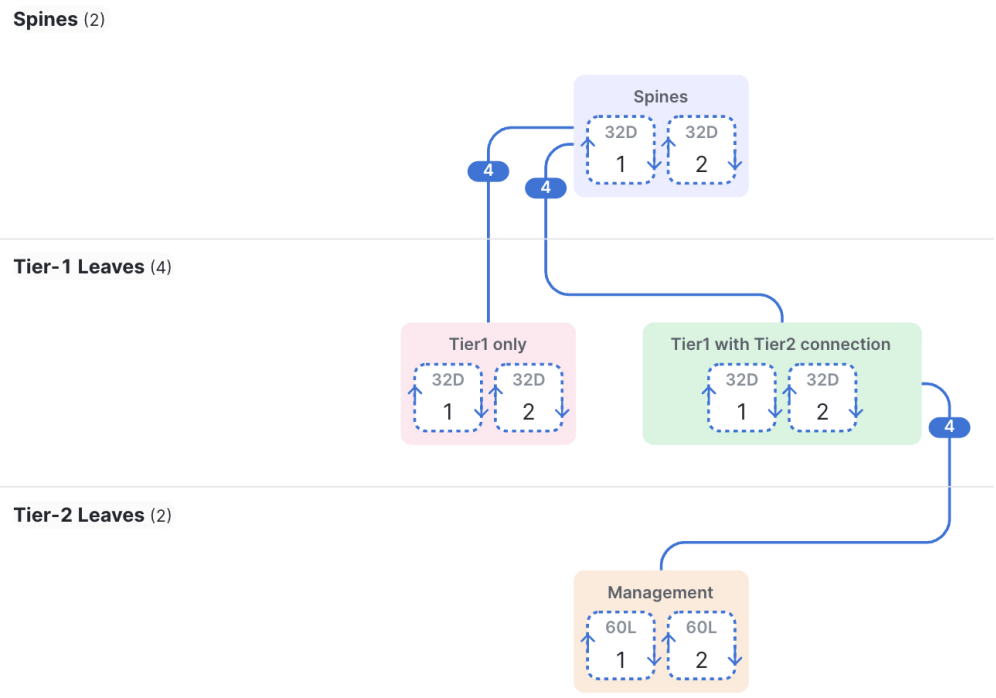


図 *14*：階層 *1* に *2* つのスパイン スイッチ、階層 *2* に *4* つのリーフ スイッチ、階層 *3* に *2* つのリーフ スイッチを備えた *3* 階層ファブリック



階層 1 に 2 つのスパイン スイッチ、階層 2 に 4 つのリーフ スイッチ、階層 3 に 2 つのリーフ スイッチを備えた 3 階層ファブリックの構成の概要

このステップの概略リストでは、階層 1 に 2 つのスパイン スイッチ、階層 2 に 4 つのリーフ スイッチ、階層 3 に 2 つのリーフ スイッチを備えた 3 階層ファブリックの構成の概要を示します

1. 階層 1 のスパイン スイッチでは、デフォルトのスイッチ階層を使用し、そのグループでスイッチの数量を 2 に設定します。
2. 階層 2 のリーフ スイッチでは、新しいスイッチ階層を追加し、そのグループでスイッチ数を 2 に設定してから、別のグループを追加し、そのグループでスイッチ数を 2 に設定します。
3. 階層 3 のリーフ スイッチでは、新しいスイッチ階層を追加し、そのグループでのスイッチ数を 2 に設定します。

4. **[グループ接続（Group connections）]** の下の **[スイッチ グループ（Switch group）]** で、接続数を示されているように設定します：
   - それぞれの階層 2リーフ スイッチ グループからスパイン スイッチ グループへ 1
   - 階層 3 リーフ スイッチ グループから 2 番目の階層 2 リーフ スイッチ グループへ 1

トポロジ：スーパー スパイン ファブリック

スーパー スパイン スイッチ トポロジは、同じファブリック内の複数のスパイン リーフの POD（配信ポイント）を相互接続するために使用される 3 層アーキテクチャです。スーパー スパイン レイヤは、スパイン レイヤの上の追加の階層として機能し、追加の相互接続性と拡張性を提供します。

図 *15*：スーパー スパイン ファブリックの図

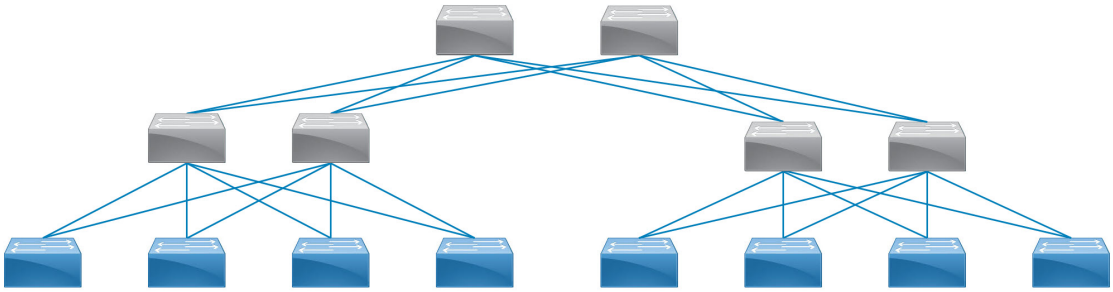
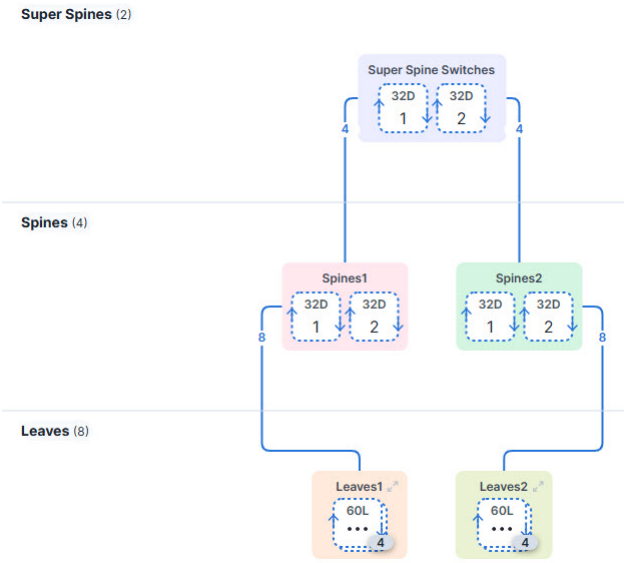


図 *16*：*2* つのスーパー スパイン スイッチ、*4* つの通常のスパイン スイッチ、および *8* つのリーフ スイッチを備えたスーパー スパイン ファブリック



スーパー スパイン ファブリックの構成の概要

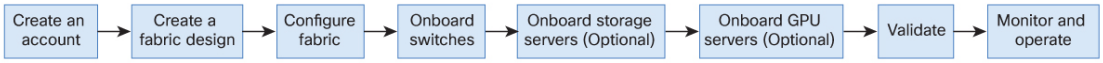
次に、スーパー スパイン ファブリックの構成の概要を示します。

1. スーパー スパイン スイッチでは、デフォルトのスイッチ階層を使用し、そのグループでスイッチの数量を 2 に設定します。
2. 通常のスパイン スイッチでは、新しいスイッチ階層を追加し、階層に2番目のグループを追加して、両方のグループでスイッチの数量を 2 に設定します。
3. リーフ スイッチでは、新しいスイッチ階層を追加し、階層に 2 番目のグループを追加して、両方のグループでスイッチ数量を 4 に設定します。
4. **グループ接続**の下の**スイッチ グループ**では、表示された接続数を設定します。
   - 各スパイン スイッチ グループからスーパー スパイン スイッチ グループに 1 つ
   - 最初のリーフ スイッチ グループから最初のスパイン スイッチ グループに 1 つ
   - 2 番目のリーフ スイッチ グループから 2 番目のスパイン スイッチ グループへ 1 つ

Cisco Nexus HyperFabric のライフサイクル

Cisco Nexus HyperFabric に基づいてネットワークを設計、展開、および維持するには、シスコと協力して、図 17 : Cisco Nexus HyperFabric のライフサイクル （10 ページ） に示されているプロセスに従ってください。

図 *17 : Cisco Nexus HyperFabric* のライフサイクル



1. Cisco Nexus HyperFabric にログインします。

   クラウド管理型ネットワークを作成する最初のステップは、Cisco Nexus HyperFabric ポータルにログインし、ネットワーク ファブリックを設計および運用する組織を作成することです。Cisco Nexus Hyperfabric へのログイン （11 ページ） を参照してください。

2. ファブリック設計を作成します。

   Cisco Nexus HyperFabric では、Blueprint Designer を使用してファブリックを設計し、デバイスとトポロジを選択して、ファブリックのブループリントを作成します。ファブリック ブループリントの設計 （28 ページ） を参照してください。

3. ファブリックを設定（または変更）します。

   Blueprint Designer で、ファブリック デバイス間の相互接続を構成します。光ファイバ、直接接続ケーブル（DAC）、アクティブ光ケーブル（AOC）などのプラガブル モジュールを設定し、残りのポートをサーバやその他のネットワークデバイスへの接続用に設定します。「ファブリックの変更 （32 ページ）」を参照してください。

4. スイッチのオンボード

   Nexus HyperFabric スイッチがブループリントに従って物理的に設置され、配線されている場合、組織はスイッチを「要求」し、ブループリント内の論理位置（ノード）に「バインド」する必要があります。スイッチは、Cisco Nexus HyperFabric ポータルを介してクラウドで管理されるようになります。ファブリックのオンボード （48 ページ） を参照してください。

5. （オプション）サーバをオンボードします。

   サーバがブループリントに従って物理的に設置され、配線されている場合、組織はサーバを「要求」し、ブループリント内の論理位置（ノード）に「バインド」する必要があります。サーバは、Cisco Nexus HyperFabric ポータルを介してクラウドでモニターされるようになります。ファブリックのオンボード （48 ページ） を参照してください。

6. デザインを検証します。

   スイッチをファブリック ブループリントにバインドした後、トラフィックが正しく転送されることを確認します。

7. ファブリックをモニタおよび操作します。

   *Cisco Nexus Hyperfabric — ファブリックの構成*を参照してください。

Cisco Nexus HyperFabric へのアクセス

Cisco Nexus Hyperfabric へのログイン

クラウド管理型ネットワークの設計を開始するには、Cisco Nexus HyperFabricにログインする必要があります。

Nexus HyperFabric にログインするには、cisco.com のユーザ アカウントが必要です。これは https://id.cisco.com/ で作成できます。

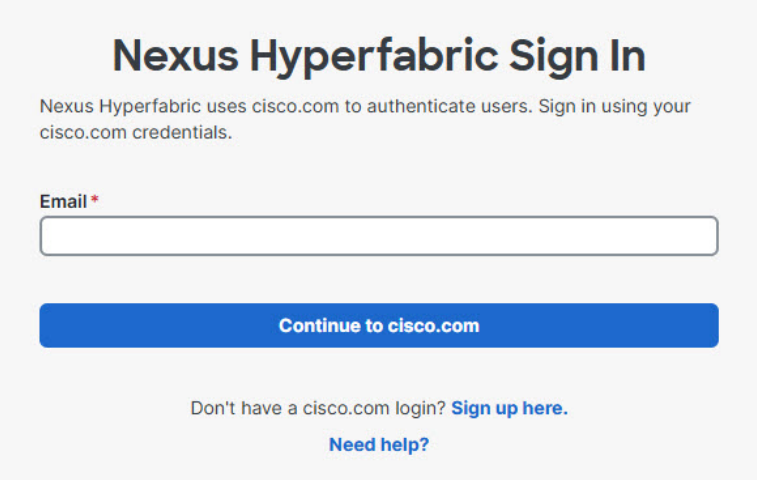
以下の手順に従って、Cisco Nexus HyperFabric にログインします。

ステップ 1 Webブラウザで https://hyperfabric.cisco.com/をポイントします。

ステップ 2 **[電子メール（Email）]** には、https://id.cisco.com/ で登録した電子メール アドレスを入力します。それから **[cisco.com に進む（Continue to cisco.com）]** を選択します。

お客様はシスコのシングル サインオン（SSO）サービスによって認証されます。Nexus HyperFabric のアカウントは、 cisco.com のユーザ アカウントに追加されます。

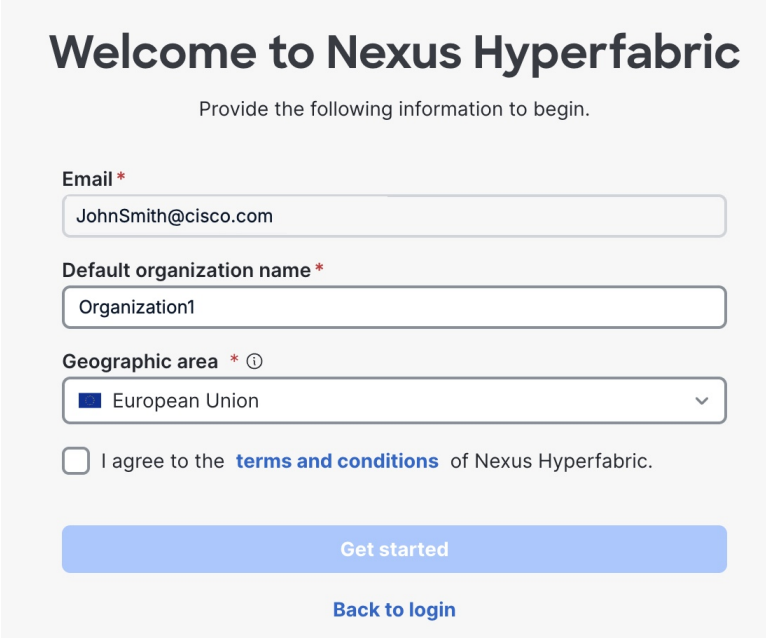
図 *18 : Cisco Nexus HyperFabric* のサインイン



1 つ以上の Nexus HyperFabric 組織の管理者である場合、最後にログインした組織のメイン ページに移動します。

a) https://id.cisco.com/ に登録済みの電子メール アドレスを持っていない場合は、**[ここでサインアップ（Sign up here）]** を選択して必要な情報を入力し、この手順を繰り返します。

ステップ 3 既存の組織の管理者でない場合、Nexus HyperFabric は組織を作成するように求めます。



a) 組織の名前を入力します。

デフォルトの組織名は、電子メールアドレスに「scratch」という単語を続けたものです。 「scratch」は、これが最初の組織であることを示しているだけで、それ以外は特別な意味はありません。この名前は変更でき、名前には限られた特殊文字を含めることができます。使用できる特殊文字のリストについては、組織の作成のガイドライン （26 ページ） を参照してください。

b) 組織が存在する地域を選択します。

欧州連合（EU）または米国（US）のいずれかを選択できます。地域によって、組織のデバイステレメトリとサービスが保存および処理される場所が決まります。詳細については、リージョンベースの組織 （25 ページ）を参照してください。

c) **[Nexus Hyperfabric の利用規約に同意します（I agree to the terms and conditions of Nexus Hyperfabric）]** を選択します。

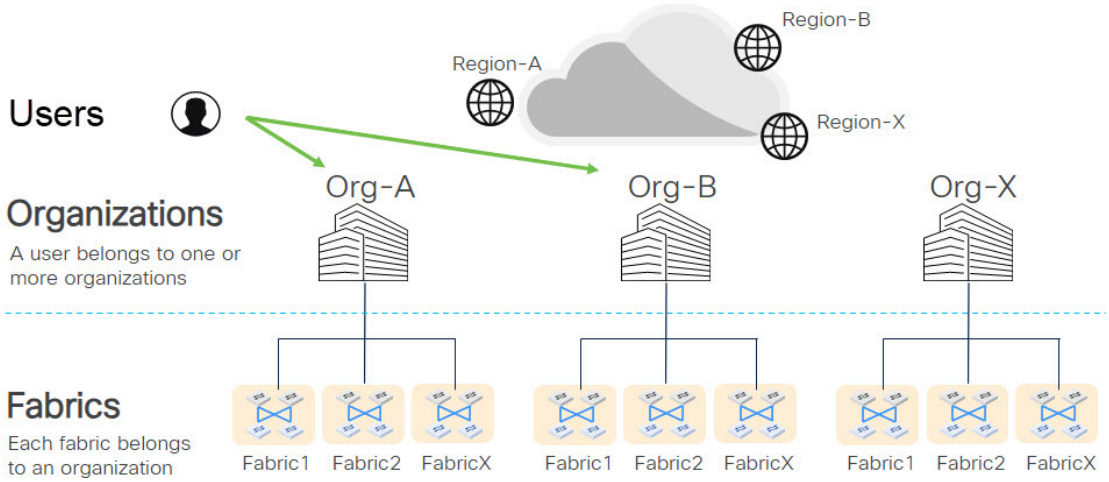
d) **[開始する（Get Started）]** を選択します。

Cisco Nexus HyperFabric は組織のメイン ページを表示します。

組織に新しいユーザを追加する

組織の管理者は、その組織に新しいユーザを追加できます。ユーザは複数の組織に属することができます。図 19 : 組織およびユーザ （13 ページ） は、ユーザと組織の関連付けを示しています。

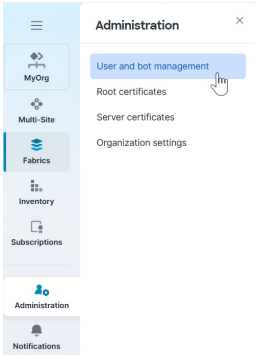
図 *19 :* 組織およびユーザ



新規ユーザを追加するには、次の手順に従います。

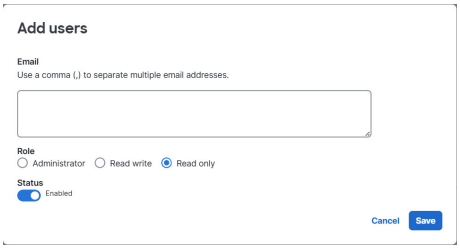
ステップ 1 **[管理（Administration）] > [ユーザ管理（User Management）]** を選択します。

図 *20 :* ユーザ管理



ステップ 2 **[+ ユーザの追加（+ Add User）]** を選択します。

図 *21 :* ユーザの追加



ステップ 3 新規ユーザの E メール アドレスを入力します。

電子メール アドレスをカンマ区切りのリストとして入力することができます。選択したロールとステータスの設定は、このリストのすべてのユーザーに適用されます。

ステップ 4 ロールを選択します：**[管理者（Administrator）]**、**[読み取り/書き込み（Read Write）]**、または **[読み取り専用（Read Only）]**。

ステップ 5 ユーザのステータスを選択します：**[有効（Enabled）]** または **[無効（Disabled）]**。

ステップ 6 **[保存（Save）]** を選択します。

組織への参加

既存の組織に参加できるのは、管理者が追加した場合のみです。追加すると、Nexus HyperFabric がトリガーされて電子メールで招待が送信されます。この手順では、管理者によって組織に追加されていることを前提としています。管理者がユーザーを追加する手順については、組織に新しいユーザを追加する （13 ページ） を参照してください。

組織に参加するには、次の手順に従います。

ステップ 1 招待電子メールを受信したら、電子メール内のリンクに移動します。

ステップ 2 Nexus HyperFabric にログインします。

ステップ 3 エンドユーザーライセンス契約（EULA）に同意します。

後ほど、他の組織に招待された場合には、 EULA への再度の同意は求められません。

アイデンティティ プロバイダー フェデレーション

アイデンティティ プロバイダー（IdP）フェデレーションでは、Cisco Nexus HyperFabric にログインするときシングルサインオン機能に使用する IdP を指定できます。特定のドメインを使用するように IdP フェデレーションを設定すると、そのドメインの一部であるすべてのユーザーは、会社の通常の（Cisco Connected Online 以外の）ID を使用して Nexus HyperFabric にログインできます。これらのユーザーは、会社の Nexus HyperFabric 組織にアクセスできます。

アイデンティティ プロバイダー フェデレーションの制限事項

アイデンティティ プロバイダー（IdP）フェデレーションには次の制限が適用されます。

- フェデレーテッド ユーザは、ユーザが管理者であるかどうかにかかわらず、組織を作成できません。
- フェデレーテッド ユーザは、API ベアラー トークンを作成できません。ベアラー トークンが必要な場合は、組織内のシスコ管理者に連絡して作成してもらってください。

アイデンティティ プロバイダー フェデレーションの構成

アイデンティティ プロバイダー フェデレーションを構成するには、次の手順を実行します。

ステップ 1 認証プロトコルを追加します。

追加する認証プロトコルの手順を参照してください。

- 認証プロトコルとして SAML を追加する （15 ページ）

- 認証プロトコルとして OpenID 接続を追加する （18 ページ）

ステップ 2 アイデンティティ プロバイダー フェデレーション用のドメインの追加 （22 ページ）。

ステップ 3 アイデンティティ プロバイダー フェデレーションのルーティング ルールの追加 （23 ページ）。

複数のルーティングルールを構成する場合は、この手順を繰り返します。

ステップ 4 アイデンティティ プロバイダー（IdP）にログインし、この IdP を使用して Nexus HyperFabric にログインできるユーザを追加します。

ユーザの追加方法については、IdP のマニュアルを参照してください。

ステップ 5 アイデンティティ プロバイダー フェデレーション構成の確認 （23 ページ）。

認証プロトコルとして SAML を追加する

この手順では、IdP フェデレーションで使用するために、Cisco Nexus HyperFabric で認証プロトコルとしてセキュリティアサーション マークアップ言語（SAML）を追加します。この手順では、例としてMicrosoft Entra を IdP として使用する手順を示しています。Microsoft Entra 固有の情報を IdP に応じて置き換えることで、選択した IdP を使用できます。正確な手順については、IdP のドキュメントを参照してください。

（注）

Microsoft Entra の手順は、予告なしに変更されることがあります。

認証プロトコルとして SAML を追加するには、次の手順を実行します。

ステップ 1 Nexus HyperFabric からサービス プロバイダーの詳細を収集します。

a) Nexus HyperFabric で、**[管理（Administration）]** > **[ユーザ管理（User Management）]** > **[外部（External）]** を選択します。

b) **[管理者ポータルの起動（Launch admin portal）]** を選択します。

Cisco Identity サイトが新しいタブで開きます。

c) Cisco Identity で、**[設定（Settings）]** > **[IdP の管理（Manage IdPs）]** > **[サービス プロバイダー (SP) (Service providers (SP))]** に移動します。

SAML サービス プロバイダー エリアには、IdP に入力する必要があるこの情報が含まれています。このリストは、必要な情報を指定します。

- **Entity ID**
- **アサーション コンシューマ サービス URL**
- **シングル サインアウト URL**（最初の URL のみ）

ステップ 2 IdP で、Nexus HyperFabric 用の新しいエンタープライズ アプリケーションを作成します。

Microsoft Entra の次のサブステップに従います。

a) Web ブラウザで https://entra.microsoft.com をポイントします。

b) **[エンタープライズ アプリ（Enterprise apps）]** > **[新しいアプリケーション（New Application）]**を選択します。
c) アプリケーション ギャラリーで **Cisco Webex** を検索し、Cisco Webex アプリを選択します。
d) アプリケーションの名前を入力し、その他のフィールドにも入力して、**[作成（Create）]** を選択します。

ステップ 3 SAML を使用してシングル サインオンをセットアップします。

Microsoft Entra の次のサブステップに従います。

a) **[エンタープライズ アプリ（Enterprise apps）]** > **[すべてのアプリケーション（All applications）]** > ***app_name***を選択します。

app-name は作成したアプリケーションの名前です。

b) **[シングル サインオン（Single sign-on）]** を選択し、シングルサインオン方式として **[SAML]** を選択します。
c) 表にリストされている Cisco Identity フィールドから値をコピーし、 Microsoft Entra の同等のフィールドに値を貼り付けます。

表 *1 : Cisco Identity* から *Microsoft Entra* へのマッピング

Cisco Identity	**Microsoft Entra**
Entity ID	**識別子（エンティティ ID）**
アサーション コンシューマ サービス URL	**応答 URL（Assertion Consumer Service URL とも呼ばれます）**
アサーション コンシューマ サービス URL	**サインオン URL**
サインアウト URL	**ログアウト URL**

ステップ 4 ユーザー属性と要求を構成します。

Microsoft Entra の次のサブステップに従います。

a) **[SAML を使用したシングル サインオンの設定（Set up Single Sign-On with SAML）]** から、**[属性と要求（Attributes & Claims）]** エリアで **[編集（Edit）]** を選択します
b) 表で指定されている要求を構成していることを確認します。

表 *2 :* 必要な要求

要求	**値**
emailaddress	`user.mail`
uid	`user.userprincipalname`

c) **[グループ要求の追加（Add a group claim）]**を選択し、表で指定されているように請求を構成します。

表 *3:* グループ要求のプロパティ

プロパティ	値
ユーザに関連付けられているどのグループを要求で返す必要があるか？	アプリケーションに割り当てられたグループ
ソース属性	クラウド専用グループの表示名

d) IdP が生成した要求名を保存します。

この要求名は、この手順の手順 8.h （18 ページ） で使用します。

ステップ 5 ユーザ グループを設定します。

Microsoft Entra の次のサブステップに従います。

a) **Microsoft Entra 管理センターの** ホームページから、**[グループ（Groups）]** > **[新しいグループ（New Group）]**を選択します。
b) 表で指定されている次の情報を入力します。

表 *4:* ユーザ グループのプロパティ

プロパティ	値
グループの種類	**[セキュリティ（Security）]**
グループ名	管理
グループの説明	**Hyperfabric 管理者グループ**
メンバーシップ タイプ	割り当て済み

c) **[作成（Create）]** を選択します。
d) 異なる Nexus HyperFabric ロール用に追加のユーザ グループを作成する必要がある場合は、グループごとにこの手順を 1 回繰り返します。

ステップ 6 Nexus HyperFabric アプリケーションにユーザ グループを割り当てます。

Microsoft Entra の次のサブステップに従います。

a) **[エンタープライズ アプリ（Enterprise apps）]** > **[すべてのアプリケーション（All applications）]** > ***app_name***を選択します。

app-name は作成したアプリケーションの名前です。

b) **[ユーザとグループ（Users and groups）]** を選択します。
c) **[ユーザ/グループの追加（Add user/group）]** を選択します。
d) 追加するグループを選択し、**[割り当て（Assign）]** を選択します。

少なくとも、作成した ADMIN グループを追加する必要があります。

ステップ 7 フェデレーション メタデータ XML 証明書ファイルをダウンロードします。

Microsoft Entra の次のサブステップに従います。

a) **[エンタープライズ アプリ（Enterprise apps）]** > **[すべてのアプリケーション（All applications）]** > ***app_name***を選択します。

app-name は作成したアプリケーションの名前です。

b) **[シングル サインオン（Single sign-On）]** を選択します。

c) **[SAML 証明書（SAML Certificates）]** で、**[フェデレーション メタデータ XML（Federation Metadata XML）]** の横にある**ダウンロード**アイコンを選択します。

ステップ 8 Cisco Identity で、**[設定（Settings）]** > **[IdP の管理（Manage IdPs）]** > **[アイデンティティ プロバイダー (IdP) (Identity providers (IdPs))]**に移動します。

a) **[+ IdPの追加（+ Add an IdP）]** を選択します。

b) **SAML**を選択から、 **次へ**を選択します。

c) **[ID プロバイダー (IdP) に接続する方法の選択 (Select a method to connect your identity provider (IdP))]** で、 **[IdP のメタデータのアップロード（Upload your IdP's metadata）]** を選択します。

d) **[IdP のメタデータのアップロード（Upload your IdP's metadata）]** では、 **未署名、自己署名、またはプライベート CA 署名の IdP メタデータファイル**を選択します。

e) **[ファイルをクリックするかこの領域にドラッグしてアップロード（Click or drag file to this area to upload）]** を使用して、以前にダウンロードしたフェデレーション メタデータ XML SAML 証明書ファイルをアップロードします。

f) **[次へ（Next）]** を選択します。

g) 横にある下矢印を選択して、**[カスタム要求、JIT 設定、およびリンク属性の構成 (オプション) (Configure custom claims, JIT settings, and linking attributes (optional))]** を展開します。

h) カスタム要求を選択 **+ カスタム要求の追加**、ステップ 4.d （17 ページ）()で保存した要求を入力し、Enter キーを押します。

Enter を押さない場合、要求は追加されません。

i) **[+ カスタム要求の追加（+ Add custom claim）]** を選択し、
`http://schemas.microsoft.com/ws/2008/06/identity/claims/groups` と入力し、Enter を押します。

このカスタム要求により、手順 4.d （17 ページ） で構成したアプリケーションロールが、Nexus HyperFabric のロールベース アクセス コントロール（RBAC）が正しく機能するためのトークンに含められます。

j) **[ジャストインタイム (JIT) の設定(Just-In-Time (JIT) settings)]** では、**[ユーザの作成またはアクティブ化（Create or activate users）]** と **[SAML 属性によるユーザの更新（Update user with SAML attributes）]** をオンにします。

これらの設定により、フェデレーションはユーザがログインするときにレコードをプロビジョニングし、リモート IdP がユーザを認証します。

k) 残りのフィールドは無視し、**[IdPの追加（Add IdP）]** を選択します。

認証プロトコルとして OpenID 接続を追加する

この手順では、アイデンティティプロバイダー（IdP）フェデレーションとして使用するために、Cisco Nexus HyperFabric で認証プロトコルとして OpenID 接続 を追加します。この手順では、例としてMicrosoft Entra を IdP として使用する手

順を示しています。Microsoft Entra 固有の情報を IdP に応じて置き換えることで、選択した IdP を使用できます。正確な手順については、IdP のドキュメントを参照してください。

（注）

Microsoft Entra の手順は、予告なしに変更されることがあります。

この手順に進む前に、Nexus HyperFabric で使用する OpenID 接続を構成します。構成方法については、IdP のマニュアルを参照してください。

OpenID 接続 を認証プロトコルとして追加するには、次の手順を実行します。

ステップ 1 Nexus HyperFabric からサービス プロバイダーの詳細を収集します。

a) Nexus HyperFabric で、**[管理（Administration）]** > **[ユーザ管理（User Management）]** > **[外部（External）]** を選択します。

b) **[管理者ポータルの起動（Launch admin portal）]** を選択します。

Cisco Identity サイトが新しいタブで開きます。

c) Cisco Identity で、**[設定（Settings）]** > **[IdP の管理（Manage IdPs）]** > **[サービス プロバイダー (SP) (Service providers (SP))]**に移動します。

このページから **リダイレクトURI** を収集します。

ステップ 2 IdP で、Nexus HyperFabric 用の新しいエンタープライズ アプリケーションを作成します。

Microsoft Entra の次のサブステップに従います。

a) Web ブラウザで https://entra.microsoft.com をポイントします。

b) **[エンタープライズ アプリ（Enterprise apps）]** > **[新しいアプリケーション（New Application）]**を選択します。

c) **[独自アプリケーションの作成（Create your own Application）]** を選択します。

d) アプリケーションの名前を入力し、その他のフィールドにも入力して、**[作成（Create）]**を選択します。

ステップ 3 作成したアプリケーションに関する情報を収集します。

クライアント ID とディスカバリ URL を収集します。

Microsoft Entra の次のサブステップに従います。

a) **[エンタープライズの登録（Enterprise registrations）]** > **[すべてのアプリケーション（All applications）]** > ***app_name***を選択します。

app-name は作成したアプリケーションの名前です。

b) アプリケーション（クライアント）ID を収集します。

c) **[エンドポイント（Endpoints）]** を選択し、**OpenID 接続メタデータ ドキュメント** の URL を収集します。

OpenID 接続メタデータ ドキュメントの URL は、ディスカバリ URL とも呼ばれます。

ステップ 4 クライアント シークレットを構成します。

Microsoft Entra の次のサブステップに従います。

a) アプリケーションの概要ページから、**[証明書とシークレット（Certificates & secrets）]** を選択します。
b) **[新しいクライアント シークレット（New client secret）]** を選択します。
c) 説明を入力し、期限日を選択してから、**[追加（Add）]** を選択します。
d) 生成されたクライアント シークレット値を収集します。

この値は、IdP フェデレーションでの IdP のセットアップ時に**クライアント シークレット**して使用します。**[シークレット ID（Secret ID）]** カラムではなく、**[値（Value）]** カラムから値を取得してください。このページから移動すると値が非表示になるため、その前にシークレットを収集する必要があります。

ステップ 5 リダイレクト URI を構成します。

Microsoft Entra の次のサブステップに従います。

a) アプリケーションの概要ページから、**[認証（Authentication）]** を選択します。
b) **[リダイレクト URI の追加（Add Redirect URI）]** を選択します。
c) **[Web]** を選択し、手順 1.c （19 ページ） で収集したリダイレクト URI を入力します。
d) **[構成（Configuration）]** を選択します。

ステップ 6 アプリケーション ロールを構成します。

Microsoft Entra の次のサブステップに従います。

a) アプリケーションの概要ページから、**[アプリ ロール（App roles）]** を選択します。
b) **[アプリ ロールの作成（Create app role）]** を選択します。
c) フィールドに情報を入力します。

- **[表示名（Display name）]**：`Hyperfabric Admin` と入力します。
- **[許可されているメンバー タイプ（Allowed member types）]**：**[ユーザー/グループ（Users/Groups）]** を選択します。
- **[値（Value）]**：`ADMIN` と入力します。
- **[説明（Description）]**：`Hyperfabric 機能へのフル アクセス権を持つ Hyperfabric 管理者ロール（Hyperfabric Admin role with full access to Hyperfabric features）` と入力します。

d) **[適用（Apply）]** を選択します。
e) 追加のアプリケーション ロールを作成する場合は、この手順を繰り返します。

ステップ 7 ユーザーまたはグループをアプリケーションロールに割り当てます。

Microsoft Entra の次のサブステップに従います。

a) **Microsoft Entra 管理センター**のホームページから、**[エンタープライズ登録（Enterprise registrations）]** > **[すべてのアプリケーション（All applications）]** > ***app_name***を選択します。

app-name は作成したアプリケーションの名前です。

b) **[ユーザとグループ（Users and Groups）]** を選択します。
c) **[ユーザ/グループの追加（Add user/group）]** を選択します。
d) 目的のユーザまたはグループを選択し、`Hyperfabric Admin`などの適切なアプリケーション ロールに割り当てます。

ステップ 8 トークンに含めるアプリケーション ロールを構成します。

Microsoft Entra では、デフォルトでロール要求にアプリケーション ロールが含まれているため、この手順はMicrosoft Entraでは必要ありません。ただし、別のIdPを使用している場合は、アプリケーション ロールまたはユーザ グループ名がトークンに含まれていることを確認するために、カスタム/オプションの要求を追加する必要があります。正確な手順については、IdP のドキュメントを参照してください。

a) 手順 12.j （22 ページ） で使用する、IdP が生成した要求名を保存します。

ステップ 9 API 権限を構成します。

Microsoft Entra の次のサブステップに従います。

a) **Microsoft Entra 管理センター**のホームページから、**[エンタープライズ登録（Enterprise registrations）]** > **[すべてのアプリケーション（All applications）]** > ***app_name***を選択します。

app-name は作成したアプリケーションの名前です。

b) **[API 権限（API Permissions）]** を選択します。
c) **[権限（Permissions）]** を選択します。
d) **[Microsoft Graph]** > **[権限の委任（Delegate permissions）]**を選択します。
e) **電子メール**および **openid** の権限を確認し、**[権限の追加（Add permissions）]** を選択します。

ステップ 10 Nexus HyperFabric で、**[管理（Administration）]** > **[ユーザ管理（User Management）]** > **[外部（External）]** を選択します。

ステップ 11 **[管理者ポータルの起動（Launch admin portal）]** を選択します。

Cisco Identity サイトが新しいタブで開きます。

ステップ 12 Cisco Identity で、**[設定（Settings）]** > **[IdP の管理（Manage IdPs）]** > **[アイデンティティ プロバイダー (IdP) (Identity providers (IdPs))]**に移動します。

a) **[+ IdPの追加（+ Add an IdP）]** を選択します。
b) **[OpenID 接続（OpenID Connect）]** を選択し、**[次へ（Next）]** を選択します。
c) **[IdP 名（IdP name）]** には、リモート IdP の名前を入力します。
d) **[クライアント ID（Client ID）]** には、手順 3.b （19 ページ） で収集したクライアント ID を入力します。
e) **[クライアント シークレット（Client secret）]** には、手順 4.d （20 ページ） で収集したクライアント シークレットを入力します。
f) **[エンドポイント（Endpoints）]** では、**[検出 URL を使用（Use the discovery URL）]** を選択します。
g) **[検出 URL（Discovery URL）]** には、アプリケーションのURLを入力します。
h) **[Next]** を選択します。
i) 横にある下矢印を選択して、**[カスタム要求、JIT 設定、およびリンク属性の構成 (オプション) (Configure custom claims, JIT settings, and linking attributes (optional))]** を展開します。

j) **[+ カスタム要求の追加（+ Add custom claim）]** を選択し、手順 8.a （21 ページ） で収集した要求を入力し、Enter を押します。

Microsoft Entra を使用している場合は、要求として「ロール」を入力します。

Enter を押さない場合、要求は追加されません。

k) **[ジャストインタイム (JIT) の設定(Just-In-Time (JIT) settings)]** では、**[ユーザの作成またはアクティブ化（Create or activate users）]** と **[OIDC 要求によるユーザの更新（Update user with OIDC claims）]** をオンにします。

これらの設定により、フェデレーションはユーザがログインするときにレコードをプロビジョニングし、リモート IdP がユーザを認証します。

l) 残りのフィールドは無視し、**[IdPの追加（Add IdP）]** を選択します。

アイデンティティ プロバイダー フェデレーション用のドメインの追加

アイデンティティ プロバイダー フェデレーション用のドメインを追加するには、次のサブステップに従います。

ステップ 1 ブラウザで **Cisco Identity** をまだ開いていない場合は、次のサブステップに従います。

a) Cisco Nexus HyperFabricで、**[組織（Organization）]** > ***[org-name]***を選択します。

[org-name] は、認証プロトコルを追加した組織と同じです。

b) **[管理（Administration）]** > **[ユーザ管理（User Management）]** > **[外部（External）]** を選択します。

c) **[管理者ポータルの起動（Launch admin portal）]** を選択します。

Cisco Identity サイトが新しいタブで開きます。

ステップ 2 Cisco Identity で、**[設定（Settings）]** > **[ドメインの管理（Manage Domains）]**に移動します。

a) **[ドメインの追加（Add a domain）]** を選択します。

b) **[ドメイン名（Domain name）]** には、ドメインの名前を入力し、**[ドメインの追加（Add domain）]** を選択します。

- 指定されたドメインの一部であるユーザは、IdP フェデレーション用に構成したリモート アイデンティティ プロバイダー（IdP）を使用して認証されます。
- Nexus HyperFabric は、入力したドメイン名の完全一致を使用します。親ドメインを入力した場合、サブドメインは含まれません。

c) **[DNS 検証（DNS verification）]** トークンで、**[コピー（Copy）]** を選択します。

d) DNS サーバーの DNS レコードに移動し、TXT レコード セクションにトークンを貼り付けます。

これにより、ドメインを所有していることが確認されます。

e) Cisco Identity で、**[完了（Done）]** を選択します。

f) 追加したドメインを含む行の **[ドメイン（Domain）]** ページで、**[...]**>**[ドメインの検証（Verify domain）]** を選択します。

Cisco Identity がドメインを検証した後、ドメインのステータスが「Pending」から「Verified」に変わります。TXT レコードが不要になり、DNS サーバから検証トークンを削除できます。

Cisco Identity がドメインの検証に失敗した場合、DNS サーバはエラーをキャッシュします。DNS サーバは、**[存続可能時間 (TTL) (Time To Live (TTL))]** の設定で指定された時間が経過するとキャッシュをクリアします。この時点で、検証トークンを再度追加して、Cisco Identity にドメインの検証を要求することができます。

g) **[今はスキップ（Skip for now）]** を選択します。

アイデンティティ プロバイダー フェデレーションのルーティング ルールの追加

アイデンティティ プロバイダー フェデレーションのルーティング ルールを追加するには、次の手順を実行します。

ステップ 1 ブラウザで **Cisco Identity** をまだ開いていない場合は、次のサブステップに従います。

a) Cisco Nexus HyperFabric で、**[管理（Administration）]** > **[ユーザ管理（User Management）]** > **[外部（External）]** を選択します。

b) **[管理者ポータルの起動（Launch admin portal）]** を選択します。

Cisco Identity サイトが新しいタブで開きます。

ステップ 2 Cisco Identity で、**[設定（Settings）]** > **[IdP の管理（Manage IdPs）]** > **[ルーティング ルール（Routing rules）]**に移動します。

a) **[+ ルーティング ルールの追加（+ Add a routing rule）]** を選択します。

b) **[ルール名（Rule name）]** で、ルール名を入力します。

c) **[ルーティング タイプの選択（Select the routing type）]**で、**[ドメイン（Domain）]** を選択します。

d) **[これらが自分のドメインである場合（If these are your domains）]** では、追加したドメインを選択します。

複数のドメインを追加した場合は、複数のドメインを選択できます。

e) **[このアイデンティティ プロバイダーを使用する（Then use this identity provider）]** では、追加した IdP を選択します。

f) [**追加（Add）**] を選択します。**[ルーティング ルール（Routing Rules）]** ページが再び表示されます。

g) **[ルーティング ルール（Routing rules）]** テーブルで、追加したルーティング ルールの行について、 を選択します **[...]** > **有効化**。

ルールのステータスが「非アクティブ」から「アクティブ」に変わります。

アイデンティティ プロバイダー フェデレーション構成の確認

新しい IdP フェデレーションの目的のアイデンティティ プロバイダー（IdP）と Cisco Identity の構成が完了したら、テストを実行してフェデレーションが正常に機能することを確認できます。

アイデンティティ プロバイダーのフェデレーション設定を確認するには、次の手順を実行します。

ステップ 1 Cisco Identity で、**[設定（Settings）]** > **[IdP の管理（Manage IdPs）]** > **[アイデンティティ プロバイダー (IdP) (Identity providers (IdPs))]**に移動します。

ステップ 2 追加した IdP を選択します。

ステップ 3 右側に表示されるペインで、**[アクション（Action）] > [SSO セットアップのテスト（Test SSO Setup）]**を選択します。

テストでは、構成に問題があるかどうかが通知されます。

アイデンティティ プロバイダー フェデレーションの一般的なトラブルシューティング シナリオ

これらは、アイデンティティ プロバイダー（IdP）フェデレーションの一般的なトラブルシューティング シナリオの一部です。

IdP フェデレーションを作成した後、 Nexus HyperFabric にログインできなくなった

ほとんどの場合、カスタム要求を追加し忘れたか、要求を誤って入力したなど、何かを誤って構成しています。cisco.com の電子メールアドレスを使用して Nexus HyperFabric にログインします。その際、電子メールアドレスの先頭に「cisco/」を付けることで、誤って構成された IdP フェデレーションをバイパスます。たとえば、「cisco/myEmailAddress@cisco.com」となります。ログイン後に、構成を修正します。

すべての Nexus HyperFabric の管理者がリモートIdPから削除されたか、または Nexus HyperFabric 組織の唯一の管理者がアクティブなユーザーではない

組織内に少なくとも 1 人の Nexus HyperFabric 管理者がいる必要があります。この問題を解決するには、リモート IdP にログインし、新しい管理者を追加するか、既存のユーザを管理者ロールにアップグレードします。

新規の組織の作成

組織を作成するには、次の手順に従います。

ステップ 1 **[組織（Organization）] > [新しい組織の作成（Create new organization）]**を選択します。



ステップ 2 新しい組織の名前を入力します。

ステップ 3 組織が存在する地域を選択します。

欧州連合（EU）または米国（US）のいずれかを選択できます。地域によって、組織のデバイステレメトリとサービスが保存および処理される場所が決まります。

ステップ 4 **[保存（Save）]** を選択します。

リージョンベースの組織

リージョンベースの組織は、次のような Nexus HyperFabric 組織です：

- 作成時に単一の地理的リージョンにバインドされます
- デバイス テレメトリとサービスをそのリージョンにのみ保存し、その中で処理します。
- リージョンのデータ処理要件に合わせるのに役立ちます。

Cisco Nexus Hyperfabric は、組織作成のための次のリージョンをサポートします。

- 欧州連合（EU）
- アメリカ合衆国（US）

組織のリージョンを特定する方法

組織リストで、各組織名の横にリージョンのアイコンが表示されます。アイコンにより、組織が存在するリージョンを一目で見分けられます。

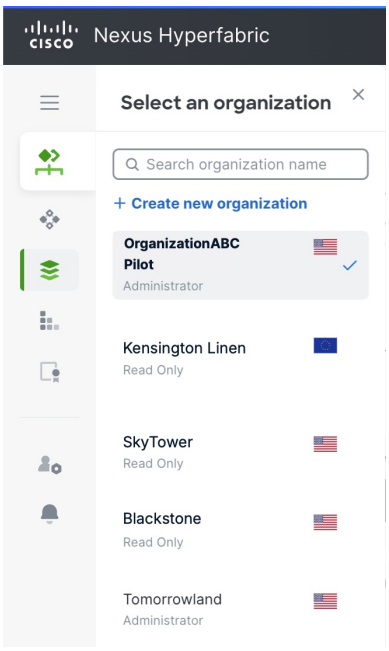


表 *5*: リージョンのアイコン

リージョンのアイコン	リージョン
	欧州連合

リージョンのアイコン	リージョン
	米国

組織の作成のガイドライン

Cisco Nexus HyperFabric で組織を作成する場合は、次のガイドラインに従ってください。

組織名のガイドライン

組織名は、次の要件を満たしている必要があります。

- 名前は 3ー120 文字で入力する必要があります。
- 組織名の最初以外または最後以外の文字としてであれば、次の特殊文字を含めることができます。
  - -
  - _
  - +
  - （スペース）
  - /
  - @
  - .
  - &

  パスフレーズに特殊文字を含めることはできません。

組織リージョンのガイドライン

組織のリージョンを選択する場合は、次のガイドラインに従います。

- 組織のテレメトリおよびサービスデータを配置する場所に基づいて、リージョンを選択します。
- Cisco Nexus Hyperfabric は、米国リージョンの組織に対してのみアイデンティティ プロバイダー フェデレーションをサポートします。EU リージョンで組織を作成する場合、ユーザーは cisco.com のログイン情報を使用してログインする必要があります。

注意

組織の作成後にリージョンを変更することはできません。

選択したリージョンは、組織に永続的に適用されます。ファブリック、デバイス、またはテレメトリデータを別のリージョンに置くには、そのリージョンに新しい組織を作成する必要があります。

組織の制限と所有権

次の制限と所有権のルールが組織に適用されます。

- 最大 10 の組織を作成できます。
- 組織を作成した後に、その組織を削除することはできません。
- デフォルトでは、自分が作成した組織の管理者になります。

ユーザ設定

REST API承認にベアラートークンを使用し、ユーザのデフォルトのタイム ゾーンと時間形式を変更する方法について説明します。

ベアラー トークン

ベアラー トークンにより、Cisco Nexus HyperFabric の REST API コールを使用する承認が付与されます。ベアラー トークンとその作成方法の詳細については、Cisco DevNet の Cisco Nexus HyperFabric API 認証 を参照してください。

ユーザのデフォルト タイム ゾーンの変更

Cisco Nexus HyperFabric が使用する優先時間形式とタイム ゾーンを選択できます。デフォルトでは、Nexus HyperFabric はイベント タイム スタンプをブラウザのローカル タイム ゾーンで表示します。

ステップ 1 GUI の右上にある自分のユーザ名をクリックします。
ステップ 2 **[タイムゾーン（Timezone）]** ドロップダウン リストから該当するタイムゾーンを選択します。
ステップ 3 時間形式を **[12hr]** または **[24hr]** に設定します。

GUI のすべてのタイムスタンプは、新しいタイム ゾーンとフォーマットで表示されます。

他のアプリケーションとのデータ共有

Nexus Hyperfabric から基本的なデバイス一覧、テレメトリ、および通知データを他のアプリケーションと共有する方法について説明します。

Cisco Cloud Control とのデータ共有

Cisco Cloud Control は、Cisco エコシステムの中央管理、自動化、および可視性の強化を提供する AI ネイティブのプラットフォームです。Nexus HyperFabric を有効にすることで、基本的なデバイス一覧、テレメトリ、および通知データを Cisco Cloud Control と安全に共有できます。

ステップ 1 **[管理（Administration）]** > **[組織の設定（Organization Settings）]** を選択します。
ステップ 2 データ共有を有効にします。

ファブリック ブループリントの設計

新しい組織を作成した場合、または既存の組織にファブリックを追加する必要がある場合、Cisco Nexus HyperFabric の Blueprint Designer を使用して新しいファブリックのブループリントを作成できます。

サポートされているファブリック トポロジについては、Nexus Hyperfabric の使用例を参照してください。

ポート チャネル、論理ネットワーク、ルーティング テーブルなどの追加設定の手順については、他の Cisco Nexus HyperFabric の記事で説明されています。

テンプレートを使用したファブリックの作成

事前定義されたトポロジを持つテンプレートを使用して、ファブリックを作成できます。作成するファブリックのサイズに基づいてテンプレートを選択します。

テンプレートを使用して新しいファブリックを作成するには、次の手順に従います。

ステップ 1 **[ファブリック（fabrics）]** を選択します。

ステップ 2 **[+新しいファブリックの追加（+Add new fabric）]** を選択し、**[テンプレートから新規（New from template）]** を選択します。

ステップ 3 **[テンプレート（Templates）]** ページで、**[AI クラスタ（AI cluster）]** または **[スイッチ ファブリック（Switch fabric）]** を必要に応じて選択します。

ステップ 4 必要なトポロジを持つテンプレートを選択します。

ステップ 5 デフォルトのファブリック名を変更する場合は、名前の横にある編集（✎）を選択し、新しい名前を入力して、**[更新（Update）]** を選択します。

ステップ 6 必要に応じてトポロジを変更してから、**[ファブリック ブループリントの保存（Save fabric blueprint）]** を選択します。

テンプレートを使用しないファブリックの作成

テンプレートを使用せずにファブリックを作成するには、次の手順に従います。

ステップ 1 **[ファブリック（fabrics）]** を選択します。

ステップ 2 **[+新しいファブリックの追加（+Add new fabric）]** を選択し、**[新しいファブリック（New fabric）]** を選択します。

a) ファブリック名を変更する場合は、デフォルト名の横にある編集（✎）を選択し、名前を変更して**[更新（Update）]**を選択します。

名前は一意である必要があり、3 ～ 120 文字を使用できます。名前にはハイフン（-）を含めることができますが、その他の特殊文字を含めることはできません。

デフォルトでは、ファブリックには 1 つのスイッチ階層があります。

b) ファブリックの権限付与レベルをアップグレードする場合は、**[アップグレード（Upgrade）]** を選択します。

ファブリックの現在の権限付与レベルが、ファブリック名の右側に表示されます。権限付与レベルの詳細については、Cisco Nexus Hyperfabric - サブスクリプションを参照してください。

ステップ 3 スイッチ階層を構成するには、次のサブステップに従います。

a) デフォルトのスイッチ階層名を変更する場合は、デフォルト名の横の編集（✎）を選択し、名前を変更してから **[更新（Update）]** を選択します。

デフォルトでは、スイッチ階層に 1 つのスイッチ グループがあります。

b) デフォルトのグループ名とショート ネームを変更する場合は、デフォルト名の横の編集（✎）を選択し、名前とショート ネームを変更してから **[更新（Update）]** を選択します。

c) グループの上部にあるドロップダウン リストからスイッチ モデルを選択します。

d) ハードウェア セットの名前を入力し、その他のフィールドに入力します。

Cisco Nexus HyperFabric では、デバイス名の一部としてハードウェア アセット名を使用します。

デフォルトでは、グループに 1 つのハードウェア アセットがあります。ハードウェア アセットをさらに追加する場合は、**[ハードウェア アセットの追加（Add hardware set）]** を選択してから、このサブステップを繰り返します。

e) 別のスイッチ グループを追加する場合は、**[グループの追加（Add group）]** を選択し、サブステップ 3.b （29 ページ） と後続のサブステップを繰り返します。

f) 別のスイッチ階層を追加する場合は、**[階層の追加（Add tier）]** を選択し、**[スイッチ（Switches）]** を選択して、この手順全体を繰り返します。

単一スイッチ ファブリックまたはメッシュ ファブリックをスイッチ モデルで設計する場合、スイッチ グループを 1 つだけ作成します。別のスイッチ モデルを追加する必要がある場合は、別のスイッチ グループを追加します。たとえば、2 つのスイッチ グループ（1 つはスパイン スイッチ用、もう 1 つはリーフ スイッチ用）を使用して、スパインとリーフのトポロジを作成できます。

スイッチを選択すると、Cisco Nexus HyperFabric によってトポロジが更新されます。

ステップ 4 **[グループ接続（Group connections）]** の **[スイッチ グループ（Switch groups）]** エリアで、ボックスを選択して、対応するスイッチ グループ間の接続を構成します。

スイッチ グループ間の接続がボックスのマトリックスで表示されます。マトリックスは、スイッチを相互にどのように接続するかを定義します。上部と側面のラベルにはスイッチ グループの名前が表示されます。ラベルは両軸でマッチします。

各ボックスには、スイッチ グループ ペアごとの接続数が表示され、A、B、または C などの文字が付いています。**[接続（Connections）]** プロパティは、接続数を指定します。これは、サブステップで示すように変更できます。各文字は、スイッチ PID の一意のペアを示しています。これにより、異常や構成ミスを一目で特定できます。

左のラベルで指定されたスイッチ グループのスイッチは、一番上のラベルで示されたスイッチ グループのスイッチの下に接続されます。例外は、スイッチグループが両方の軸で同じである場合です。この場合、そのグループのスイッチは相互接続されます。

例として、「スパイン」という名前のスイッチ グループに 2 つのスイッチがあり、「リーフ」という名前の別のスイッチ グループに 4 つのスイッチがあり、グループ間の **[接続（Connections）]** に「2」を指定す

るとします。これは、8組のスイッチがあることを意味します。2つの接続を指定したため、グループ間の合計接続数は 16 になります。

ボックスを選択すると、**[スイッチ グループ（Switch groups）]** エリアの右側にグループ接続のプロパティが表示されます。複数のボックスを選択すると、これらの各グループ接続を同時にレビューできます。

選択したスイッチ グループの接続に対して、次のサブステップを実行します。

a) 編集（✎）を選択して、プラガブル モジュールの PID を選択します。

[<switch_group> から <switch_group> の場合 PID を指定する（Select PIDS for <switch_group> to <switch_group>）] ダイアログが表示されます。最初のスイッチ グループの下部のテーブルから PID を選択し、**[ケーブル（Cable）]** を選択して PID を選択し、2 番目のスイッチ グループのラジオ ボタンを選択して PID を選択します。テーブルの上にあるフィールドを使用して、テーブルをフィルタリングできます。

完了したら、**[選択（Select）]** を選択します。

b) **[接続（Connections）]** に、スイッチペアごとの接続数を入力します。

これは、スイッチ グループ間の接続の合計数ではありません。

c) **[ケーブル接続方法（Cabling strategy）]** の場合は、スイッチをケーブル接続する方法を選択します。

d) スイッチの自動ケーブル接続をオーバーライドする必要がある場合は、**[手動オーバーライド（Manual Overrides）]** エリアで、**[オーバーライドの追加（Add override）]** を選択し、**[接続オーバーライド（Connection override）]** を選択します。

左のオプション ボタンがデフォルトで選択されています。左側の並べて表示するで、ドロップダウン リストからデバイスとポートを選択し、テーブルからプラガブルを選択します。

[ケーブル（Cable）] を選択し、PID を選択します。

右のラジオ ボタンを選択します。右側の並べて表示するで、ドロップダウン リストからデバイスとポートを選択し、テーブルからプラガブルを選択します。

[選択（Select）] を選択します。

ステップ 5 ファブリックにサーバを含める場合は、次のサブステップに従います。

a) **[階層の追加（Add tier）]** を選択し、**[サーバ（Server）]**を選択します。

デフォルトでは、サーバ階層に 1 つのサーバ グループがあります。

b) デフォルトのサーバ階層名を変更する場合は、デフォルト名の横の編集（✎）を選択し、名前を変更してから **[更新（Update）]** を選択します。

c) デフォルトのグループ名とショート ネームを変更する場合は、デフォルト名の横の編集（✎）を選択し、名前とショート ネームを変更してから **[更新（Update）]** を選択します。

d) グループの上部にあるドロップダウン リストからサーバ モデルを選択します。

e) ハードウェア セットの名前を入力し、その他のフィールドに入力します。

Cisco Nexus HyperFabric では、デバイス名の一部としてハードウェア アセット名を使用します。

デフォルトでは、グループに 1 つのハードウェア アセットがあります。ハードウェア アセットをさらに追加する場合は、**[ハードウェア アセットの追加（Add hardware set）]** を選択してから、このサブステップを繰り返します。

f) 別のサーバ グループを追加する場合は、**[グループの追加（Add group）]** を選択し、サブステップ 5.c （30 ページ） と後続のサブステップを繰り返します。

g) 別のサーバ階層を追加する場合は、この手順全体を繰り返します。

h) ファブリックに GPU を備えたデバイスが含まれている場合は、**[East-West サーバ ポート接続のレール グループ管理（Manage rail groups for East-West server port connections）]** エリアで、**[レール グループの追加（Add rail group）]** を選択し、グループのフィールドに入力します。

- **[レール グループ名（Rail group name）]**：新しいグループ名を入力します。
- **[短縮名（Short name）]**：短い名前を入力します。
- **[幅（Width）]**：GPU サーバの数を入力します。
- **[カウント（Count）]**：8 を入力します。現在、これが唯一可能な値です。
- **[配置方法（Placement strategy）]**：方法を選択します。現在、サーバには **[分散（Distributed）]** のみ選択できます。
- **[スイッチ グループ（Switch group）]**：このレール グループを接続するスイッチ グループを選択します。

i) **[サーバ ポート グループからスイッチ グループへ（Server port groups to switch groups）]** 領域で、次の項目を構成します。

- **[プラガブル PID <-（Pluggable PID <–）]**：編集（✎）を選択、グループ サーバのプラガブルを選択します。同じダイアログ内で、**[プラガブル PID <-（Pluggable PID <–）]**（グループ サーバ）、**[ケーブル PID（Cable PID）]**、および **[プラガブル PID ->（Pluggable PID –>）]**（スイッチ グループまたはレール グループ）のプラガブルを選択できます。
- **[接続（Connections）]**：これは可能な接続の最大数です。この値は変更できません。サーバ ポート グループに接続しない場合は、**[スイッチ/レール グループ（Switch/rail group）]** から値を削除します（存在する場合）。
- **[ケーブル接続方法（Cabling strategy）]**：方法を選択します。
- **[ケーブル PID（Cable PID）]**：編集（✎）を選択し、ケーブルのプラガブルを選択します。同じダイアログ内で、**[プラガブル PID <-（Pluggable PID <–）]**（グループ サーバ）、**[ケーブル PID（Cable PID）]**、および **[プラガブル PID ->（Pluggable PID –>）]**（スイッチ グループまたはレール グループ）のプラガブルを選択できます。
- **[プラガブル PID <-（Pluggable PID <–）]**：編集（✎）を選択、スイッチ グループのプラガブルを選択します。同じダイアログ内で、**[プラガブル PID <-（Pluggable PID <–）]**（グループ サーバ）、**[ケーブル PID（Cable PID）]**、および **[プラガブル PID ->（Pluggable PID –>）]**（スイッチ グループまたはレール グループ）のプラガブルを選択できます。
- **[スイッチ/レール グループ（Switch/rail group）]**：スイッチ グループまたはレール グループを選択します。

ステップ 6 **[ファブリック ブループリントの保存（Save fabric blueprint）]** を選択します。

[ファブリック ブループリントの保存（Saving fabric blueprint）] ダイアログが表示され、Cisco Nexus HyperFabric がブループリントを生成したことが示されます。

ステップ 7 Cisco Nexus HyperFabric でケーブル配線計画を今すぐ作成する場合は、**[配線の実行（Run cabling）]** を選択します。それ以外の場合は、**[トポロジに進む（Continue to topology）]** を選択します。

ファブリックの変更

組織に対する管理者アクセス権または読み取り/書き込みアクセス権がある場合は、**[ファブリック（Fabrics）]** ページで既存のファブリックの設計を変更できます。展開されていないファブリック設計から設置され実行中のファブリックまで、どの段階でも、ファブリック ブループリントに変更を加えることができます。

[ファブリック（Fabrics）] ブループリント ページは、次の 2 つのモードのいずれかで動作します。

- 編集モード：これは、管理者アクセス権または読み取り/書き込みアクセス権を持つユーザーのデフォルト モードです。すべてのファブリック編集オプションが公開されます。
- 実行モード：これは、読み取り専用アクセス権を持つユーザーのデフォルト モードです。設定とステータスは表示されますが、編集オプションは表示されません。管理者アクセス権または読み取り/書き込みアクセス権を持っている場合にのみ、編集モードに切り替えることができます。

このマニュアルのすべての設定手順では、管理者または読み取り/書き込みアクセス権を持ってログインしており、メニューが編集モードになっていることを前提としています。

ファブリックの変更

この手順は、ファブリック構成を変更するための一般的なワークフローを提供します。

ファブリックを変更するには、次の手順に従います。

ステップ 1 **[ファブリック（Fabrics）]**を選択し、設定するファブリックをクリックします。

a) ファブリックが編集モードでない場合は、**[編集モードに切り替える（Switch to edit mode）]**（）を選択します。

ステップ 2 変更を行います。

変更内容を確認、確定、およびプッシュするまで、ファブリックに適用されません。

ステップ 3 変更を適用する準備ができたら、**[構成の確認（Review configuration）]** を選択します。

図 *22 :* 構成のレビュー



[構成のレビュー（Review configuration）] ページでは、前回のプッシュ以降の変更点に関する簡潔な説明のリストをレビューできます。これには変更者の ID と、変更が保存された日時が含まれます。

ステップ 4 変更を確認し、変更を適用する準備ができたら、**[コメントとプッシュ（Comment and push）]** を選択します。

ステップ 5 **[構成を送信する前のコメント（Comments before sending configuration）]** ダイアログボックスに、変更の理由を入力します。

ステップ 6 **[構成のプッシュ（Push Configuration）]** を選択します。

ステップ 7 変更のステータスをレビューします。

[ファブリック（Fabrics）] ブループリント ページのファブリック カードには、プッシュされた変更のステータスが表示されます。変更の適用に時間がかかる、または赤いアサーションが生成される場合があります。たとえば、インストール済みで実行中のファブリックに変更をプッシュし、その変更がファブリックの物理的なケーブル接続と競合している場合は、アサーションが発生します。

サイトでのファブリックの展開

Cisco Nexus HyperFabric は、ユーザーまたはネットワーク配線技術者が現場で実行する必要があるタスクをガイドする機能を提供することにより、ファブリック内のスイッチのケーブル配線作業を大幅に簡素化します。ネットワーク管理者は、Cisco Nexus HyperFabric を使用して、スイッチのケーブル配線計画を自動的に含むブループリントを作成します。専用の オンサイト ページに移動して、タスクをレビューおよびフォローして物理ファブリック トポロジをセットアップしたり、進行状況を追跡したりできます。

または、ネットワーク管理者が Cisco Nexus HyperFabric のオンサイト モバイル対応サイトの URL をネットワーク ケーブル接続技術者に提供することもできます。技術者はモバイル デバイスで URL を開いてブループリントをレビューし、それに従って物理ファブリック トポロジをセットアップするか、またはファブリックのステータスをレビューします。

サイトでのファブリックの展開の詳細については*Cisco Nexus Hyperfabric — サイトでのファブリックの展開*を参照してください。

Cisco Nexus HyperFabric オンサイトのモバイル対応サイトへの共有可能なリンクを取得する

次の手順を実行して、Cisco Nexus HyperFabric オンサイトのモバイル対応サイトへの共有可能なリンクを取得します。

ステップ 1 Cisco Nexus HyperFabric の GUI で、**[ファブリック（Fabrics）]** を選択し、リンクを取得するファブリックを選択します。

ステップ 2 **[オンサイト（On-site）]** の選択

ステップ 3 **[共有可能なリンク（Shareable link）]** を選択します。

ステップ 4 次のいずれかの方法を使用して、オンサイトのモバイル対応サイトに移動します。

- モバイル デバイスで QR コードをスキャンし、そのデバイスでオンサイトページを開きます。
- **[コピー（Copy）]** を選択して URL をコピーし、ネットワーク配線の技術者に URL を送信します。技術者は、モバイル デバイスを使用して URL にアクセスできます。

ケーブル配線

Cisco Nexus HyperFabric は、デバイスペアごとの接続数とケーブル接続戦略に基づいて、ファブリック内のデバイスをケーブル接続する方法を自動的に決定します。ケーブル接続戦略は 2 つの概念で構成されます。

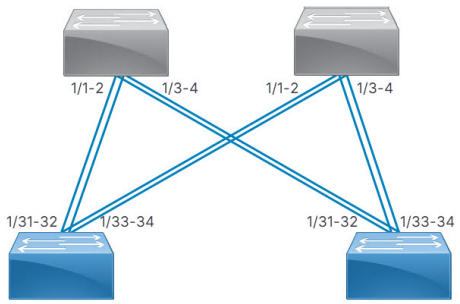
最初の概念は、次のとおりです。

- 厳格：Cisco Nexus HyperFabric は、選択した接続数で各デバイスペアを接続します。何らかの理由でデバイスに使用可能なポートが不足している場合、 Cisco Nexus HyperFabric は、ケーブル接続にエラーがあることを示しています。
- ベストエフォート：Cisco Nexus HyperFabric は、可能な場合は、選択した接続数で各デバイス ペアを接続します。ただし、何らかの理由でデバイスに十分な数の使用可能なポートがない場合、Cisco Nexus HyperFabric は、ペアのデバイスを、十分な数の使用可能なポートがある同じスイッチ グループ内の他のデバイスに接続します。

第 2 の概念は次のとおりです。

- 密度：Cisco Nexus HyperFabric は、デバイスの連続するポートをペアリングされたデバイスの連続するポートに接続します。連続するポートの数は、選択したデバイス ペアごとの接続数と同じです。 Cisco Nexus HyperFabric は、ペアリングされたデバイスごとに、連続するポートのこの接続を繰り返します。これはスイッチ間接続に使用されます。

  図 *23 : 2* つのスパインスイッチと *2* つのリーフ スイッチを使用したスイッチ間高密度ケーブル接続戦略

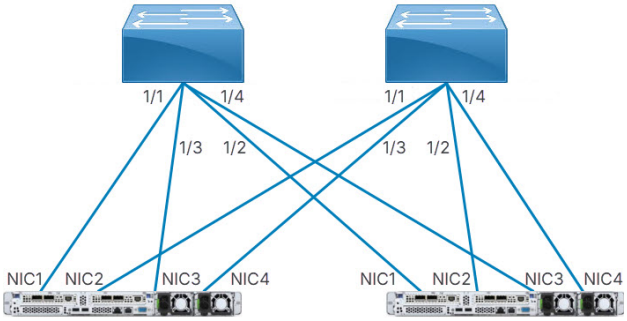


- 分散型：Cisco Nexus HyperFabric は、最初のサーバの最初のネットワーク インターフェイス カード（NIC）を最初のスイッチの最初のポートに接続し、次にサーバの 2 番目のNIC を2 番目のスイッチの最初のポートに接続します。サーバが 1 つの各スイッチの最初のポートに接続します。 Cisco Nexus HyperFabric は、後続のサーバでこのプロセスを繰り返しますが、NIC は各スイッチの次のポートに接続します。各サーバの NIC が各スイッチに接続された後、指定された接続数と等しい数の各サーバから各スイッチへの接続数が存在するようになるまで、プロセス全体が繰り返されます。

  GPU を備えたサーバ ポート グループも分散ケーブル戦略を使用します。レール グループ プロパティでは、これらのサーバの幅は GPU サーバの数と同じで、数は 8 です。

  GPUがある場合とない場合で、、同じスイッチに接続するには、各サーバで同じNIC番号を使用します。したがって、2 台のサーバ（server1 と server2）と 2 台のスイッチ（switch1 と switch2）があるファブリックの場合、両方のサーバの NIC1 は switch1 に接続され、両方のサーバの NIC2 は switch2 に接続します。

図 *24 : 2* つのリーフスイッチと *2* つのサーバによるスイッチからサーバへの分散ケーブル戦略



ファブリックに同じスイッチ グループまたはサーバ グループ内のデバイス間の接続が含まれている場合、Cisco Nexus HyperFabric はまず異なるグループのデバイス ペアにポートを割り当ててから、同じグループ内のデバイスにポートを割り当てます。

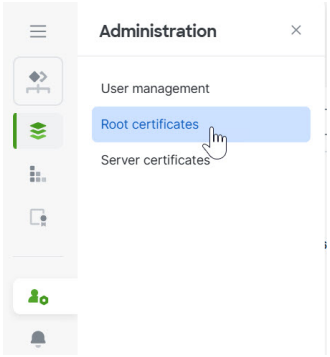
セキュアなトランスポート層のセキュリティ接続用にルート証明書を追加する

Cisco Nexus HyperFabric へのセキュアな Transport Layer Security（TLS）接続を確立するために組織によって発行されたルート証明書を信頼するようにスイッチを構成できます。

セキュアのトランスポート層のセキュリティ接続用にルート証明書を追加するには、次の手順を実行します。

ステップ 1 **[管理（Administration）] > [ルート証明書（Root certificates）]**を選択します。

図 *25 :* ルート証明書



ステップ 2 **[+ 証明書の追加（+ Add Certificate）]** を選択します。

図 *26 : [*証明書の追加（*Add Certificate*）*]* ダイアログ



ステップ 3 フィールドに入力し、**[保存（Save）]** を選択します。

[証明書（Certificate）] で、証明書を含むファイルをボックスにドラッグするか、ボックスを選択してファイルに移動し、ファイルを選択してから、**[開く（Open）]**を選択します。

スイッチ ポートの設定

スイッチ レベルでポートを構成する

ロールや速度、ブレークアウト ステータスなど、スイッチのポートのさまざまなプロパティを設定できます。ポート ロールは、ポートによって提供される接続のタイプを指定します。

スイッチ レベルでポートを設定するには、次の手順に従います。

ステップ 1 **[ファブリック（Fabrics）]** を選択し、スイッチを含むファブリックを選択します。

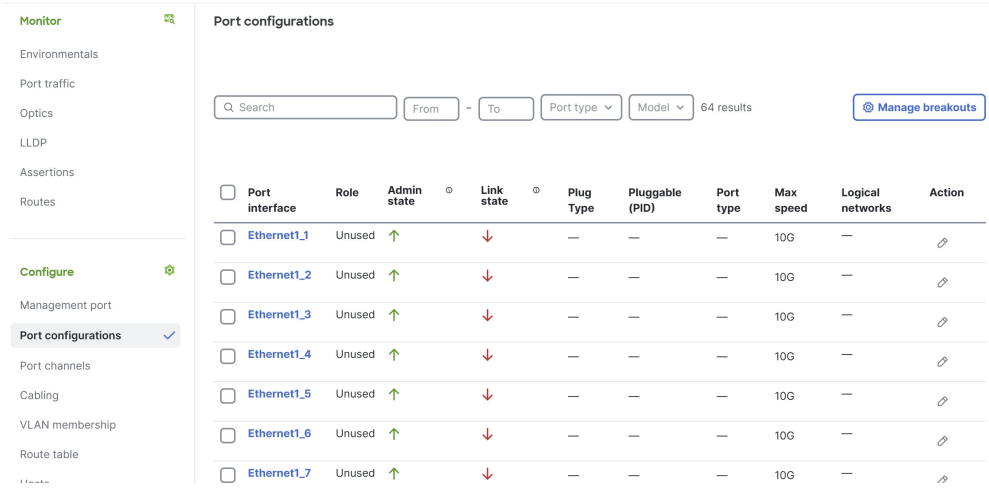
a) ファブリックが編集モードでない場合は、**[編集モードに切り替える（Switch to edit mode）]**（）を選択します。

ステップ 2 **[トポロジ（Topology）]** エリアで、構成するスイッチを選択し、スイッチ名を選択します。

ステップ 3 **[構成（Configure）]** エリアで、**[ポートの構成（Port configurations）]** を選択します。

ポート構成（Port configuration） テーブルには、スイッチのすべてのポートが一覧表示されます。

図 *27 :* ポート構成



ステップ 4 （任意）いずれかのポートのブレークアウトを有効または無効にする場合は、**[ブレークアウト管理（Manage breakouts）]** を選択します。

a) ブレークアウトを無効にするには、**[ブレークアウト オプション（Breakout option）]** で、**[無効化（Disable）]** を選択します。それ以外の場合は、目的のオプションを選択して、ブレークアウトを有効にします。

カッコ内の値は、各レーンの速度とポート当たりのレーン数を示しています。たとえば、値「2x 200G（50G X 4 lanes）」は、それぞれ 200G の速度の 2 つのポートを示しており、各ポートが 4 つの 50G レーンを使用します。これは、合計 400G の速度と 8 つのレーンを意味します。

接続されたスイッチのプラガブルの速度に対応するオプションを選択する必要があります。

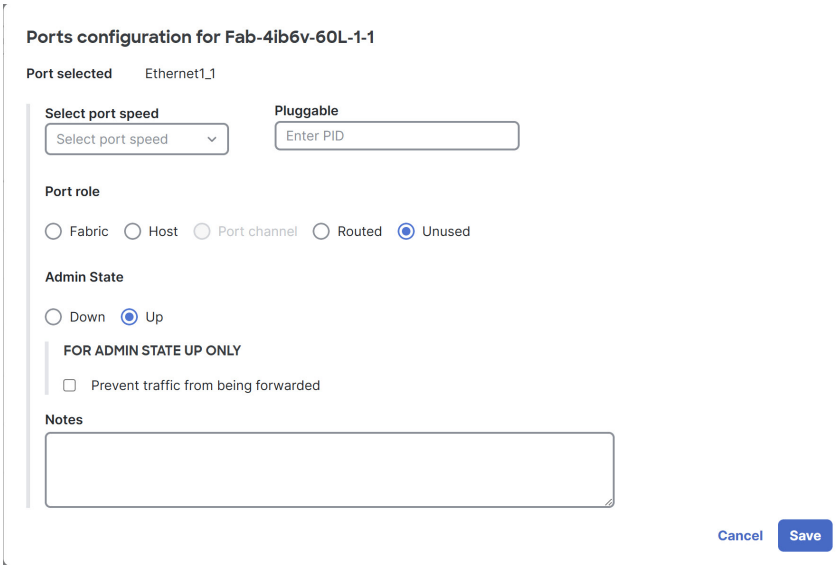
b) ブレークアウトを有効にした場合は、ケーブル タイプと光タイプを選択します。

c) **[保存]** を選択します。

ステップ 5 **[ポート構成（Port configurations）]** テーブルの **[アクション（Action）]** カラムで、構成するポートの編集ボタン（✎）をクリックします。

ポートを構成するためのダイアログ ボックスが開きます。

図 *28 :* ポートの構成



a) **[ポート速度の選択（Select port speed）]** で、ポートの速度を選択します。

カッコ内の値は、各レーンの速度とレーン数を示しています。たとえば、値「200G(50G x 4 lanes)」は、ポートの合計速度が 200G で、4 つの 50G レーンを使用することを示します。

デフォルトでは、ポートは最高速度でデータを送受信します。必要に応じて速度を抑えることができます。ブレークアウト ポートの速度は変更できません。

スイッチ ファブリック ポートで、デフォルト以外の速度を使用する場合は、適切な速度を選択する必要があります。たとえば、QSFP-DD ポートの場合、デフォルトの 400G の代わりに 40G、100G、または 200G を使用できます。

b) **[プラガブル（Pluggable）]** には、ポートのオプティックの製品 ID（PID）を入力します。

転送エラー修正（FEC）は、指定されたプラガブルに基づいて自動的に設定されます。FEC を手動で構成することはできません。

c) **[ポート ロール（Port role）]** で、ファブリック内の別のリーフまたはスパイン スイッチに接続するポートの **[ファブリック（Fabric）]** を選択します。

その他のポート タイプでは、ポートの目的に応じてロールを選択します。

- **[ファブリック（Fabric）]**：ファブリック スイッチ間の接続を提供し、ピア スイッチによる自動検出を可能にします。ファブリック内の別のリーフまたはスパイン スイッチに接続するポートには、これを選択します。
- **[ホスト（Host）]**：サーバまたはその他の一般的なネットワーク デバイスへのレイヤ 2 接続を提供します。
- **[ポート チャネル（Port channel）]**：ポートは、リンク集約グループ（LAG）とも呼ばれるポート チャネルのメンバーです。ポートをポート チャネルのメンバーに設定すると、そのロールが **[未使用（Unused）]** から **[ポート チャネル（Port channel）]** に自動的に変更されます。**ポート チャネル** ロールは、まずポート チャネルからポートを削除しない限り、このメニューでは変更できません。
- **[ルーテッド（Routed）]**：ルータまたはその他のネットワーク デバイスへのレイヤ 3 接続を提供します。

  スイッチでルーテッド ポートを設定するときに、VLAN タギングをイネーブルにすることを選択できます。イネーブルにするには、スタティックまたはダイナミック ルーティング プロトコルを使用して IPv4 および IPv6 パケットを別のデバイスに転送するために、レイヤ 3 インターフェイス上に 802.1Q VLAN サブインターフェイスを設定する必要があります。IP ルーティングにレイヤ 3 インターフェイスを使用できます。または、VLAN タギングを無効のままにした場合は、ルート テーブル（VRF）を選択し、ルートの IPv4 アドレスまたは IPv6 アドレスを指定します。追加のルーテッド ポートの設定手順については、以降のサブステップを参照してください。
- **[未使用（Unused）]**：ポートはトラフィックの転送や受信を行いません。

d) ポート ロールとして **[ルーテッド（Routed）]** を選択し、VLAN タギングを使用する場合は、**[VLAN タギングの有効化（Enable VLAN tagging）]** をオンに切り替えて、次の追加手順に従います。

1. **[サブ インターフェイスの追加（Add a sub Interface）]** を選択します。
2. **[VLAN タグ（VLAN tag）]** に、タグを入力します。

   同一の物理インターフェイス上の複数のサブインターフェイスに、同一の VLAN タグを割り当てないでください。
3. **[VRF の選択（Select VRF）]** で、VRF インスタンスを選択します。
4. **[IP アドレス（IP address ）]** フィールドに、IPv4 アドレスとマスク、IPv6 アドレス、またはその両方を入力します。

e) ポート ロールで **[ルーテッド（Routed）]** を選択し、VLAN タギングを使用しない場合は、**[VLAN タギングの有効化（Enable VLAN tagging）]** を無効にして、次の追加手順を実行します。

1. **[ルート テーブルの選択**（Select route table）]で、目的のルート テーブル（VRF）を選択します。
2. **[IP アドレス（IP addresses）]** フィールドに、1 つ以上の IPv4 または IPv6 アドレスとマスクを入力します。

   複数のアドレスを入力する場合は、各アドレスをカンマで区切ります。

f) **[管理状態（Admin state）]**で、**[アップ（Up）]** を選択してポートを有効にします。

- **[アップ（Up）]**：ポートはトラフィックを受信して転送します。これは、デフォルトの状態です。

  ポートを[アップ（Up）]にしてもトラフィックを転送しないように設定するには、**[トラフィックの転送を防止する（Prevent traffic from forwarding）]** チェックボックスをオンにします。

- **[ダウン（Down）]**：ポートはトラフィックの受信も転送も行いません。

g) **[保存]** を選択します。

ステップ 6 ファブリック内の別のリーフまたはスパイン スイッチまたはホストに接続するこのスイッチのすべてのポートについて、前の手順を繰り返します。

ステップ 7 ファブリックのすべてのリーフとスパイン スイッチでこの手順を繰り返します。

スイッチ レベルで複数のポートを設定する

ロールや速度など、スイッチ上の複数ポートのさまざまなプロパティを同時に設定できます。ポート ロールは、ポートによって提供される接続のタイプを指定します。

一部のプロパティの選択肢では、この手順で設定できない追加のプロパティが表示されます。これらの追加のプロパティを設定するには、ポートを個別に設定する必要があります。ここでは、この制限があるプロパティでの説明を示します。

スイッチ レベルで複数のポートを設定するには、次の手順に従います。

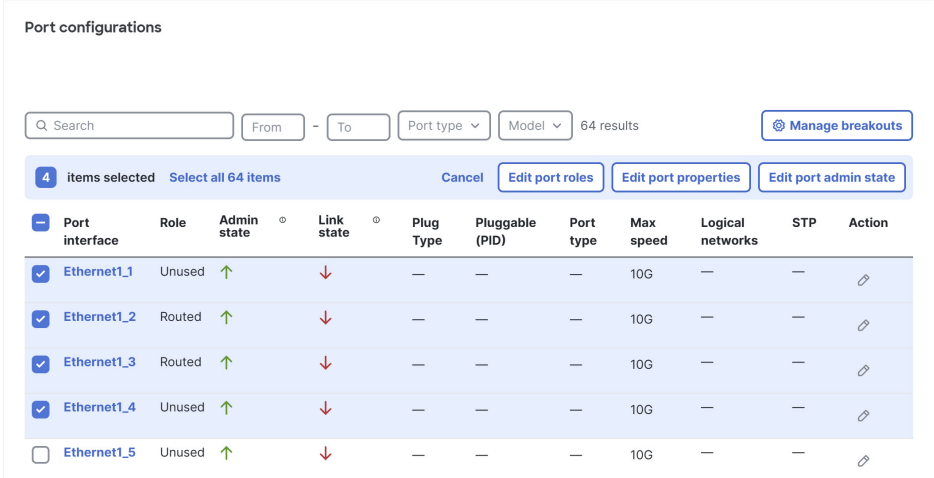
ステップ 1 **[ファブリック（Fabrics）]** を選択し、スイッチを含むファブリックを選択します。

a) ファブリックが編集モードでない場合は、**[編集モードに切り替える（Switch to edit mode）]**（）を選択します。

ステップ 2 **[トポロジ（Topology）]** エリアで、構成するスイッチを選択し、スイッチ名を選択します。

ステップ 3 **[構成（Configure ）]** エリアで、**[ポート構成（Port configurations）]** を選択し、各ポート ID の横にあるチェックボックスをオンにして、設定するポートを選択します。

図 *29*：選択された複数のポート



ステップ 4 ポートのロールを変更する場合は、**[ポートロールの編集（Edit port roles）]** を選択します。

a) **[ポート ロール（Port role）]**で、目的のロールを選択します。

- **[ファブリック（Fabric）]**：ファブリック スイッチ間の接続を提供し、ピア スイッチによる自動検出を可能にします。ファブリック内の別のリーフまたはスパイン スイッチに接続するポートには、これを選択します。
- **[ホスト（Host）]**：サーバまたはその他の一般的なネットワーク デバイスへのレイヤ 2 接続を提供します。グローバル スパニングツリーが有効になっている場合、この手順を使用して STP ブロッキング モードを選択することはできません。
- **[ポート チャネル（Port channel）]**：ポートは、リンク集約グループ（LAG）とも呼ばれるポートチャネルのメンバーです。ポートをポートチャネルのメンバーに設定すると、そのロールが **[未使用（Unused）]** から **[ポート チャネル（Port channel）]** に自動的に変更されます。**ポート チャネル** ロールは、まずポート チャネルからポートを削除しない限り、このメニューでは変更できません。
- **[ルーテッド（Routed）]**：ルータまたはその他のネットワーク デバイスへのレイヤ 3 接続を提供します。この手順を使用して、VLANの有効化または無効化、サブインターフェイスの追加、ルートテーブルの選択、IP アドレスの指定はできません。
- **[未使用（Unused）]**：ポートはトラフィックの転送も受信も行いません。ポートをポート チャネル メンバーとして構成する場合は、最初の状態でロールが **[未使用（Unused）]** である必要があります。

b) **[保存（Save）]** を選択します。

ステップ 5 ポートのプロパティを変更するには、**[ポートプロパティの編集（Edit port properties）]** を選択します。これらのプロパティには、ポート速度とプラガブル オプションが含まれます。

a) **[ポート速度の構成（Configure port speed）]** ドロップダウン リストから、ポートの速度を選択します。

カッコ内の値は、各レーンの速度とレーン数を示しています。たとえば、値「200G(50G x 4 lanes)」は、ポートの合計速度が 200G で、4 つの 50G レーンを使用することを示します。

デフォルトでは、ポートは最高速度でデータを送受信します。必要に応じて速度を抑えることができます。ブレークアウト ポートの速度は変更できません。

スイッチ ファブリック ポートで、デフォルト以外の速度を使用する場合は、適切な速度を選択します。たとえば、QSFP-DD ポートの場合、デフォルトの 400G の代わりに 40G、100G、または 200G を使用できます。

b) **[プラガブル（Pluggable）]** で、ポートの光ファイバの製品 ID（PID）を入力するか、表からプラガブルを選択します。以下のフィールドに検索およびフィルタ条件を入力して、特定の PID を見つけることができます。

c) **[保存（Save）]** を選択します。

ステップ 6 管理状態を変更する場合は、**[ポートの管理状態の編集（Edit port admin state）]** を選択します。

a) **[管理状態（Admin state）]**で、目的の管理状態を選択します。

- **[アップ（Up）]**：ポートはトラフィックを受信して転送します。これは、デフォルトの状態です。

ポートを[アップ（Up）]にしてもトラフィックを転送しないように設定するには、**[トラフィックの転送を防止する（Prevent traffic from forwarding）]** チェックボックスをオンにします。

- **[ダウン（Down）]**：ポートはトラフィックの受信も転送も行いません。

b) **[保存（Save）]** を選択します。

ファブリック レベルでのスイッチ ポートの構成

ファブリックの **[物理トポロジ（Physical topology）]** 領域に移動することで、ファブリック内の任意のスイッチの任意のポートを構成できます。このページを使用すると、さまざまなスイッチのポートを簡単に構成できます。

ファブリック レベルでポートを設定するには、次の手順に従います。

ステップ 1 **[ファブリック（Fabrics）]**を選択し、ポートを構成するスイッチを含むファブリックを選択します。

a) ファブリックが編集モードでない場合は、**[編集モードに切り替える（Switch to edit mode）]**（）を選択します。

ステップ 2 **[物理トポロジ（Physical topology）]** エリアで、**[ポート構成（Port configurations）]** を選択します。

[ポート構成（Port configurations）] テーブルには、ファブリック内のすべてのスイッチのすべてのポートが一覧表示されます。

ステップ 3 **[ポート設定（Port configurations）]** テーブルの上で、さまざまなフィールドとドロップダウン リストを使用してテーブルをフィルタリングできます。

- **[検索（Search）]**：入力した文字列が含まれる ID を持つポートのみがテーブルに表示されます。
- **[下限（From）]**：ポート番号が入力された整数以上であるポートのみがテーブルに表示されます。
- **[上限（To）]**：ポート番号が入力された整数以下であるポートのみがテーブルに表示されます。
- **[ポート タイプ（Port type）]**：選択したタイプのポートのみがテーブルに表示されます。
- **[モデル（Model）]**：選択したモデルのポートのみがテーブルに表示されます。

ステップ 4 **[アクション（Actions）]** カラムで、構成するポートの編集（）を選択します。

a) **[ポート速度の選択（Select port speed）]** ドロップダウン リストから、ポートの速度を選択します。

カッコ内の値は、各レーンの速度とレーン数を示しています。たとえば、値「200G(50G x 4 lanes)」は、ポートの合計速度が 200G で、4 つの 50G レーンを使用することを示します。

デフォルトでは、ポートは最高速度でデータを送受信します。必要に応じて速度を抑えることができます。ブレークアウト ポートの速度は変更できません。

スイッチ ファブリック ポートで、デフォルト以外の速度を使用する場合は、適切な速度を選択する必要があります。たとえば、QSFP-DD ポートの場合、デフォルトの 400G の代わりに 40G、100G、または 200G を使用できます。

b) **[プラガブル（Pluggable）]** には、ポートのオプティックの製品 ID（PID）を入力します。

転送エラー修正（FEC）は、指定されたプラガブルに基づいて自動的に設定されます。FEC を手動で構成することはできません。

c) **[ポート ロール（Port role）]** で、ファブリック内の別のリーフまたはスパイン スイッチに接続するポートの **[ファブリック（Fabric）]** を選択します。

その他のポート タイプでは、ポートの目的に応じてロールを選択します。

- **[ファブリック（Fabric）]**：ファブリック スイッチ間の接続を提供し、ピア スイッチによる自動検出を可能にします。ファブリック内の別のリーフまたはスパイン スイッチに接続するポートには、これを選択します。
- **[ホスト（Host）]**：サーバまたはその他の一般的なネットワーク デバイスへのレイヤ 2 接続を提供します。
- **[ポート チャネル（Port channel）]**：ポートは、リンク集約グループ（LAG）とも呼ばれるポート チャネルのメンバーです。ポートチャネルのメンバーになるようにポートを設定すると、そのロールが**未使用**から**ポート チャネル**に自動的に変更されます。**ポート チャネル** のロールは、まずポート チャネルからポートを削除しない限り、このメニューで変更することはできません。
- **[ルーテッド（Routed）]**：ルータまたはその他のネットワーク デバイスへのレイヤ 3 接続を提供します。

  スイッチでルーテッド ポートを設定するときに、VLAN タギングをイネーブルにすることを選択できます。イネーブルにするには、スタティックまたはダイナミック ルーティング プロトコルを使用して IPv4 および IPv6 パケットを別のデバイスに転送するために、レイヤ 3 インターフェイス上に 802.1Q VLAN サブインターフェイスを設定する必要があります。IP ルーティングにレイヤ 3 インターフェイスを使用できます。または、VLAN タギングを無効のままにした場合は、ルート テーブル（VRF）を選択し、ルートの IPv4 アドレスまたは IPv6 アドレスを指定します。追加のルーテッド ポートの構成手順については、以下のサブステップを参照してください。
- **[未使用（Unused）]**：ポートはトラフィックの転送や受信を行いません。

d) ポート ロールとして **[ルーテッド（Routed）]** を選択し、VLAN タギングを使用する場合は、**[VLAN タギングの有効化（Enable VLAN tagging）]** をオンに切り替えて、次の追加手順に従います。

1. **[サブ インターフェイスの追加（Add a sub Interface）]** を選択します。
2. **[VLAN タグ（VLAN tag）]** に、タグを入力します。

   同一の物理インターフェイス上の複数のサブインターフェイスに、同一の VLAN タグを割り当てないでください。
3. **[VRF の選択（Select VRF）]** で、VRF インスタンスを選択します。
4. **[IP アドレス（IP address ）]** フィールドに、IPv4 アドレスとマスク、IPv6 アドレス、またはその両方を入力します。

e) ポート ロールで **[ルーテッド（Routed）]** を選択し、VLAN タギングを使用しない場合は、**[VLAN タギングの有効化（Enable VLAN tagging）]** トグルをオフのままにして、次の追加手順を実行します。

1. **[ルート テーブルの選択**（Select route table）]で、目的のルート テーブル（VRF）を選択します。

2. **[IP アドレス（IP addresses）]** フィールドに、1 つ以上の IPv4 または IPv6 アドレスとマスクを入力します。

   複数のアドレスを入力する場合は、各アドレスをカンマで区切ります。

f) **[管理状態（Admin state）]**で、**[アップ（Up）]** を選択してポートを有効にします。

- **[アップ（Up）]**：ポートはトラフィックを受信して転送します。これは、デフォルトの状態です。

  ポートを[アップ（Up）]にしてもトラフィックを転送しないように設定するには、**[トラフィックの転送を防止する（Prevent traffic from forwarding）]** チェックボックスをオンにします。

- **[ダウン（Down）]**：ポートはトラフィックの受信も転送も行いません。

g) [保存（Save）] を選択します。

ファブリック レベルでの複数のポートの構成

ファブリックの **[物理トポロジ（Physical topology）]** エリアに移動して、ファブリック内の任意のスイッチ ポートを構成できます。このページを使用すると、同時に複数のスイッチのポートを簡単に構成できます。

一部のプロパティの選択肢では、この手順で設定できない追加のプロパティが表示されます。これらの追加のプロパティを設定するには、ポートを個別に設定する必要があります。ここでは、この制限があるプロパティでの説明を示します。

ファブリック レベルで複数のポートを設定するには、次の手順に従います。

ステップ 1 **[ファブリック（Fabrics）]** を選択し、ポートを構成するスイッチを含むファブリックを選択します。

a) ファブリックが編集モードでない場合は、**[編集モードに切り替える（Switch to edit mode）]**（）を選択します。

ステップ 2 **[物理トポロジ（Physical topology）]** で、**[ポート構成（Port configurations）]** を選択します。

[ポート構成（Port configurations）] テーブルには、ファブリック内のすべてのスイッチのすべてのポートが一覧表示されます。

ステップ 3 **[ポート設定（Port configurations）]** テーブルの上で、さまざまなフィールドとドロップダウン リストを使用してテーブルをフィルタリングできます。

- **[検索（Search）]**：入力した文字列が含まれる ID を持つポートのみがテーブルに表示されます。
- **[下限（From）]**：ポート番号が入力された整数以上であるポートのみがテーブルに表示されます。
- **[上限（To）]**：ポート番号が入力された整数以下であるポートのみがテーブルに表示されます。
- **[ポート タイプ（Port type）]**：選択したタイプのポートのみがテーブルに表示されます。
- **[モデル（Model）]**：選択したモデルのポートのみがテーブルに表示されます。

ステップ 4 各ポート ID の横にあるボックスをオンにして、構成するポートを選択します。ポートは異なるスイッチに属することができます。

ステップ 5 ポートのロールを変更する場合は、**[ポートロールの編集（Edit port roles）]** を選択します。

a) **[ポート ロール（Port role）]**で、目的のロールを選択します。

- **[ファブリック（Fabric）]**：ファブリック スイッチ間の接続を提供し、ピア スイッチによる自動検出を可能にします。ファブリック内の別のリーフまたはスパイン スイッチに接続するポートには、これを選択します。
- **[ホスト（Host）]**：サーバまたはその他の一般的なネットワーク デバイスへのレイヤ 2 接続を提供します。グローバル スパニングツリーが有効になっている場合、この手順を使用して STP ブロッキング モードを選択することはできません。
- **[ポート チャネル（Port channel）]**：ポートは、リンク集約グループ（LAG）とも呼ばれるポートチャネルのメンバーです。ポートをポートチャネルのメンバーに設定すると、そのロールが **[未使用（Unused）]** から **[ポート チャネル（Port channel）]** に自動的に変更されます。**ポート チャネル** ロールは、まずポート チャネルからポートを削除しない限り、このメニューでは変更できません。
- **[ルーテッド（Routed）]**：ルータまたはその他のネットワーク デバイスへのレイヤ 3 接続を提供します。この手順を使用して、VLANの有効化または無効化、サブインターフェイスの追加、ルートテーブルの選択、IP アドレスの指定はできません。
- **[未使用（Unused）]**：ポートはトラフィックの転送も受信も行いません。ポートをポート チャネル メンバーとして構成する場合は、最初の状態でロールが **[未使用（Unused）]** である必要があります。

b) **[保存]** を選択します。

ステップ 6 ポートのプロパティを変更するには、**[ポートプロパティの編集（Edit port properties）]** を選択します。プロパティには、ポート速度とプラガブルが含まれます。

a) **[ポート速度の設定（Configure port speed）]**で、ポートの速度を選択します。

カッコ内の値は、各レーンの速度とレーン数を示しています。たとえば、値「200G(50G x 4 lanes)」は、ポートの合計速度が 200G で、4 つの 50G レーンを使用することを示します。

デフォルトでは、ポートは最高速度でデータを送受信します。必要に応じて速度を抑えることができます。ブレークアウト ポートの速度は変更できません。

スイッチ ファブリック ポートで、デフォルト以外の速度を使用する場合は、適切な速度を選択する必要があります。たとえば、QSFP-DD ポートの場合、デフォルトの 400G の代わりに 40G、100G、または 200G を使用できます。

b) **[プラガブル（Pluggable）]** で、ポートの光ファイバの製品 ID（PID）を入力するか、表からプラガブルを選択します。以下のフィールドに検索およびフィルタ条件を入力して、特定の PID を見つけることができます。

c) **[保存]** を選択します。

ステップ 7 管理状態を変更する場合は、**[ポートの管理状態の編集（Edit port admin state）]** を選択します。

a) **[管理状態（Admin state）]**で、目的の管理状態を選択します。

- **[アップ（Up）]**：ポートはトラフィックを受信して転送します。これは、デフォルトの状態です。

ポートを[アップ（Up）]にしてもトラフィックを転送しないように設定するには、**[トラフィックの転送を防止する（Prevent traffic from forwarding）]** チェックボックスをオンにします。

- **[ダウン（Down）]**：ポートはトラフィックの受信も転送も行いません。

b) **[保存（Save）]** を選択します。

ポートの設定に関するガイドライン

Cisco HF6100-60L4D スイッチでは、 ポートグループ内のいずれかの SFP56 ポートの速度を設定すると、もう一方のポートの速度も同じ速度に設定されます。

設計を終了してコミットする

変更内容を確認、確定、およびプッシュするまで、ファブリックに適用されません。

設計を終了してコミットするには、次のステップに従います。

ステップ 1 **[構成のレビュー（Review configuration）]** を選択します。

ステップ 2 レビューリストで変更を確認します。

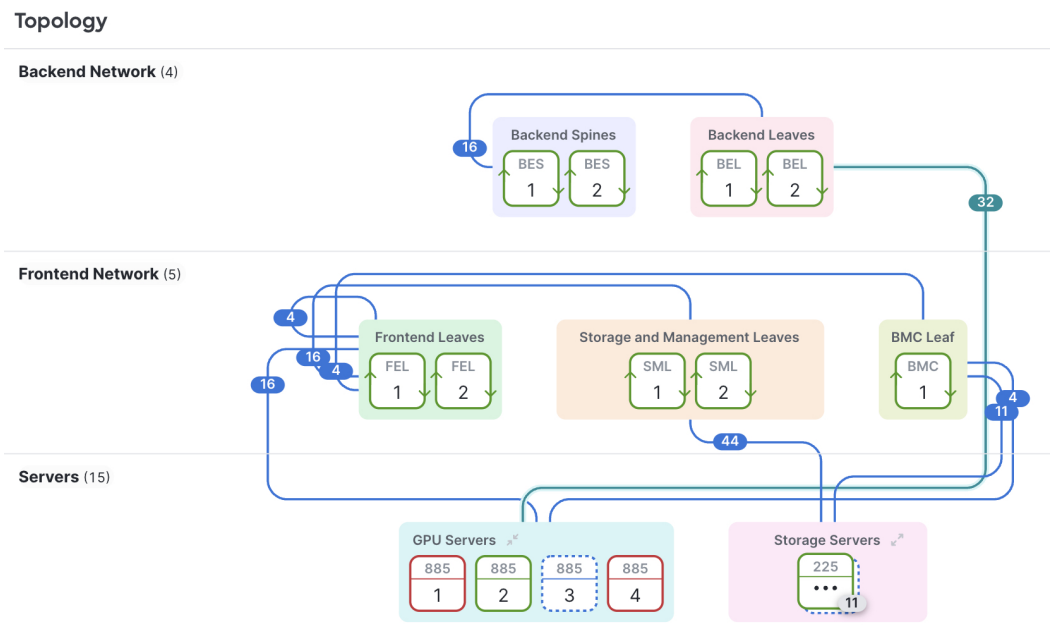
ステップ 3 **[コメントしてプッシュ（Comment and push）]** を選択します。

ステップ 4 **[構成を送信する前のコメント（Comments before sending configuration）]** ダイアログボックスに、変更の理由を入力します。

ステップ 5 **[構成のプッシュ（Push Configuration）]** を選択します。

このプッシュの一部としてデバイスをバインドした場合、デバイス アイコンの輪郭の色により、デバイスのアサーションを示します。デバイスに問題がなければ、緑色の輪郭が表示されるはずです。黄色の輪郭は、デバイスが予期しない状態になっており、問題が検出されていることを示していますが、その問題によって動作が中断することはありません。赤色の輪郭は、デバイスが予期しない状態になっており、動作の中断を引き起こす可能性のある問題が検出されたことを示しています。問題を調査する必要があります。

図 *30* : 構成をプッシュした後のファブリック トポロジ



発注と部品表について

展開

展開では、アセンブリ リストと部品表（BOM）の計算に関する情報が提供され、ファブリックに部品が必要かどうかが示されます。アセンブリ リストと BOM の CSV ファイルをエクスポートして、Cisco Nexus HyperFabric 外の参照用に使用できます。

展開情報のレビューまたはエクスポート

展開情報のレビュー、または参照として使用するために展開情報をCSVファイルにエクスポートすることもできます。次の情報をレビューまたはエクスポートできます。

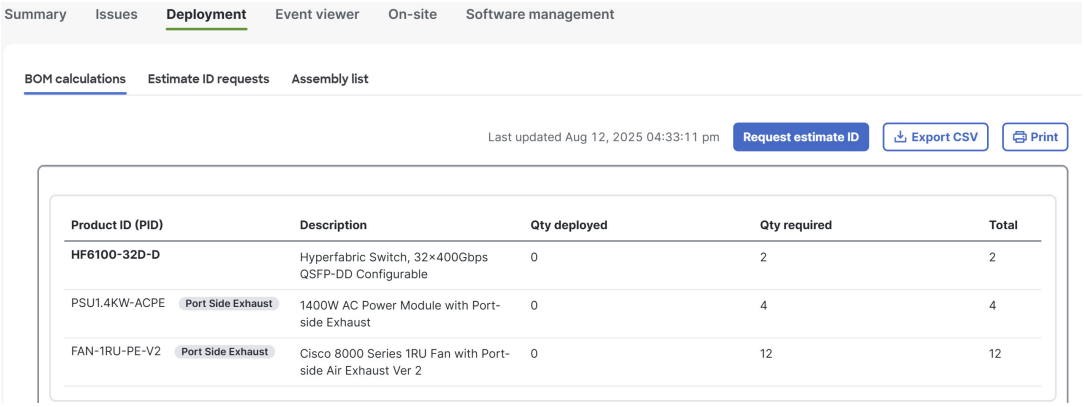
- ブループリント設計に従ってファブリックを構築するために製品を発注する際の部品表
- 各デバイスに必要なファン、電源、光ファイバなどのアクセサリのフルフィルメントをチェックするためのアセンブリ リスト

展開情報をレビューまたはエクスポートするには、次の手順に従います。

ステップ 1 **[ファブリック（Fabrics）]** を選択し、目的のファブリックを選択します。

ステップ 2 **[展開（Deployment）]** > **[BOM 計算（BOM calculations）]** を選択します。

図 *31 : BOM* 計算

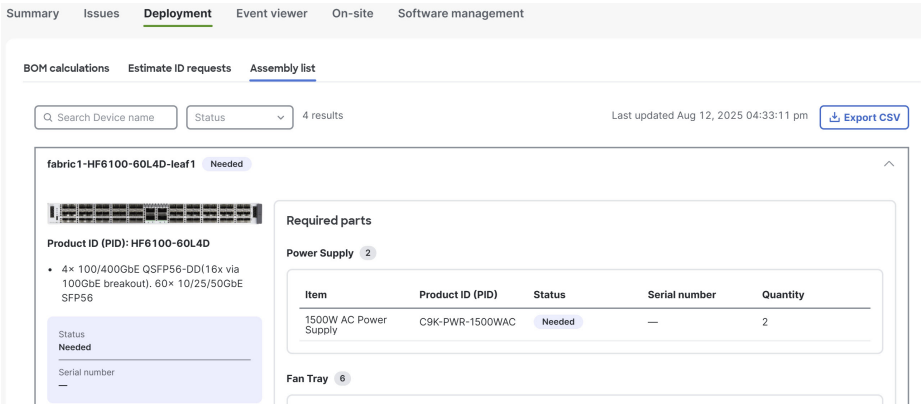


このページには、製品 ID（PID）の部品表（BOM）が表示されます。これは、ファブリック設計に必要なデバイスとアクセサリ、およびポート接続構成に基づく光ファイバを指定します。表は、必要な各 PID の数と、受け取って展開された数を示しています。

ステップ 3 （任意） BOM をカンマ区切り値（CSV）スプレッドシートとしてエクスポートするには、**[CSVのエクスポート（Export CSV）]** を選択します。

ステップ 4 **[アセンブリ リスト（Assembly list）]** を選択します。

図 *32 :* アセンブリ リスト



このページには、各デバイスに必要なファン、電源、光ファイバなどのアクセサリのリストが表示されます。この表には、部品が展開されているかどうか、および展開された部品のシリアル番号（ある場合）が表示されます。

ステップ 5 （任意） アセンブリ リストをカンマ区切り値（CSV）スプレッドシートとしてエクスポートするには、**[CSV のエクスポート（Export CSV）]** をクリックします。

部品表の見積 ID を要求する

部品表（BOM）の見積 ID を要求すると、 Cisco Nexus HyperFabric は Cisco Commerce Workspace（CCW）と通信して見積を作成し、見積 ID を含む電子メールを送信します。その後、パートナーまたはセールス チームの担当者と協力して、見積書について話し合って、部品を注文できます。

Cisco Nexus HyperFabric は見積 ID を 90 日間保持します。**[見積 ID リクエスト（Estimate ID requests ）]** ページから任意の BOM をダウンロードして、より長期間保存できます。見積 ID の有効期限が切れた場合は、新しい見積 ID を要求できます。

部品表の見積 ID を要求するには、次の手順に従います。

ステップ 1 **[ファブリック（fabrics）]** を選択します。

ステップ 2 見積 ID を取得する BOM を含むファブリックをクリックします。

ステップ 3 **[展開（Deployment）]** > **[BOM 計算（BOM calculations）]** を選択します。

ステップ 4 **[見積 ID のリクエスト（Request estimate ID）]** をクリックして 、次のサブステップを実行します。

a) **[見積 ID のリクエスト（Request estimate ID）]** ダイアログ ボックスで、 **[リクエストの送信（Submit request）]**をクリックします。

ダイアログ ボックスが閉じ、Cisco Nexus HyperFabric は「Cisco Nexus Hyperfabric <noreply@hyperfabric.cisco.com>」からの電子メールを送信します。電子メールの本文には、見積 ID と見積名が含まれます。

b) （オプション）この見積 ID および過去の見積 ID に関する情報を参照する場合は、**[展開（Deployment）]** > **[見積 ID のリクエスト（Estimate ID requests）]**を選択します。

このページから、**[アクション（Actions）]** カラムのダウンロードボタンを選択して、CSV ファイル形式で BOM をダウンロードできます。

ステップ 5 Cisco パートナーまたはセールス チームの連絡先に見積 ID を伝えます。

Cisco Nexus HyperFabric によって作成された見積書は読み取り専用です。連絡先は新しい見積 ID を持つ見積の複製を作成する必要があります。その後、担当者がコストの見積もりを行い、新しい ID を使用して注文を完了します。

ファブリックのオンボード

ファブリックのオンボード

この手順では、ファブリックをオンボードするために実行する必要があるタスクの概要を示します。

ファブリックをオンボードする前に、ファブリックを物理的に設置し、Cisco Nexus HyperFabric のブループリントと一致するようにファブリックを配線する必要があります。

ファブリックをオンボードするには、次の手順に従います。

ステップ 1 スイッチが Cisco Nexus HyperFabric クラウド サービスに接続できるようにします。

ステップ 2 組織にスイッチを要求します。

詳細については、デバイスの申請 （65 ページ）を参照してください。

ステップ 3 各スイッチをファブリック ブループリント内のその位置にバインドし、Cisco Nexus HyperFabric からその特定の構成を受信できるようにします。

詳細については、デバイスのバインド （67 ページ）を参照してください。

ステップ 4 AI クラスタを展開する場合は、次のサブステップに従います。

a) ストレージ用の Cisco UCSC-C225-M8N-1P サーバを要求します。

詳細については、デバイスの申請 （65 ページ）を参照してください。

b) UCSC-C225-M8N-1P サーバをバインドします。

詳細については、デバイスのバインド （67 ページ）を参照してください。

c) サーバに Cisco Nexus Hyperfabric エージェントをインストールします。

詳細については、 サーバへ Cisco Nexus Hyperfabric エージェントをインストールするを参照してください。

d) C885 および C880 サーバーの場合は、各サーバーに証明書を追加します。

詳細については、次のいずれかの手順を参照してください。

- デバイス オンボード トークンと Craft コンソールを使用してサーバに証明書を追加する （54 ページ）
- デバイス オンボード トークンと CSR 登録スクリプトを使用してサーバに証明書を追加する （56 ページ）
- ベアラー トークンと Craft コンソールを使用してサーバに証明書を追加する （58 ページ）
- ベアラー トークンと CSR 登録スクリプトを使用してサーバに証明書を追加する （62 ページ）

e) GPU 用の UCSC-885A-M8-HC1 サーバを要求します。

詳細については、デバイスの申請 （65 ページ）を参照してください。

f) UCSC-885A-M8-HC1 サーバをバインドします。

詳細については、デバイスのバインド （67 ページ）を参照してください。

オンボーディングの前提条件

インストールしたファブリックをオンボードする前に、次のものが必要です。

- スイッチが HTTPS（ポート 443）トラフィック用に接続できる実行中のインターネット接続
- 使用可能な DNS サーバー
- 構成済みのプロキシ サーバー（クラウドに到達する必要がある場合）
- ファブリック内のスイッチ用の少なくとも 1 つの管理 IPv4 または IPv6 アドレス

（注）

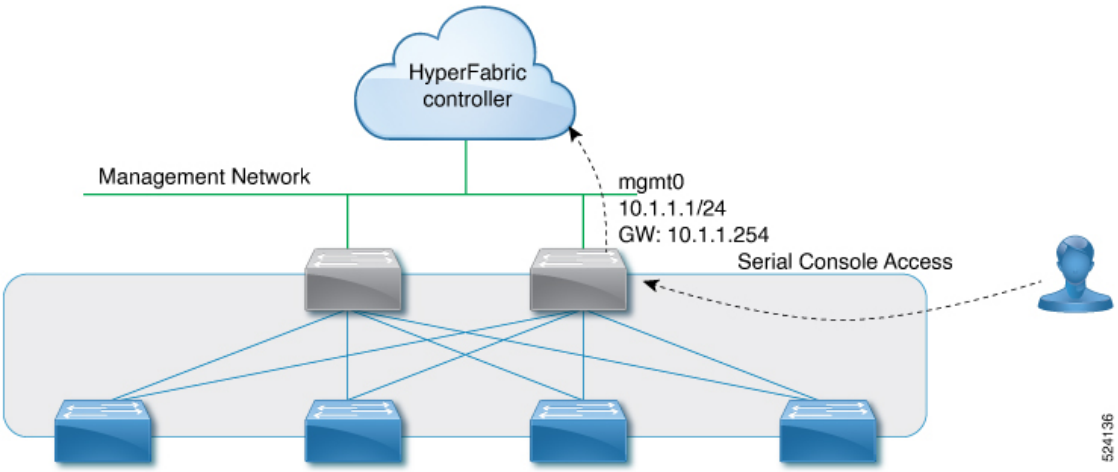
ファブリック内のすべてのスイッチを管理ネットワークに接続することを推奨します。

最初のスイッチを Cisco Nexus HyperFabric クラウド サービスに接続する

新しい Nexus HyperFabric スイッチの出荷時には、ネイバーを検出し、Cisco Nexus HyperFabric に接続できるようにするエージェントが含まれています。

次の図は、アウトオブバンド（OOB）管理ノードを Cisco Nexus HyperFabric に接続するための最初のスイッチの設定例を示しています。管理ノードの設定は、（使用可能な場合は）DHCP を介して、静的 IP アドレスが必要な場合はシリアル ポートの設定によって行うことができます。

図 *33*：アウトオブバンド管理ノードを *Cisco Nexus HyperFabric* に接続するための最初のスイッチの構成



通常、クラウドに物理的に接続する必要があるのは 1 台のスイッチのみです。このスイッチは自動的に Cisco Nexus HyperFabric に接続します。ファブリック内のネイバー スイッチによって検出されると、このスイッチはその可用性を「出口ノード」スイッチとして報告します。OOB 管理接続がない隣接スイッチは、出口ノード スイッチを介して Cisco Nexus HyperFabricに接続できます。

最初のスイッチを Cisco Nexus HyperFabric クラウド サービスに接続するには、次の手順に従います。

ステップ 1 物理サイトで、最初のインターネット接続を行うスイッチを選択します。このクラウド接続スイッチが出口ノードになります。

ステップ 2 スイッチの OOB 管理インターフェイスをインターネット接続に接続します。

ステップ 3 DHCP サーバーが存在する場合は、この手順の残りのステップをスキップできます。

スイッチはその DHCP 設定を受け取り、インターネット接続を介して Cisco Nexus HyperFabric に接続します。

ステップ 4 静的IPアドレスを設定する必要がある場合、またはプロキシを設定する必要がある場合は、次の接続パラメータを使用して、スイッチのシリアル コンソール ポートに端末を接続します。

- 115200 ボー
- パリティなし
- 8 データ ビット
- 1 ストップ ビット

ステップ 5 ユーザー名に「ttg-admin」、パスワードに「hfabric2025」を使用して、シリアル コンソールにログインします。

デフォルトのパスワードを変更するかどうかを尋ねられます。変更することを推奨します。

a) **[デフォルトパスワードの変更（Change default password）]** ダイアログで、 **[はい（Yes）]**を選択します。

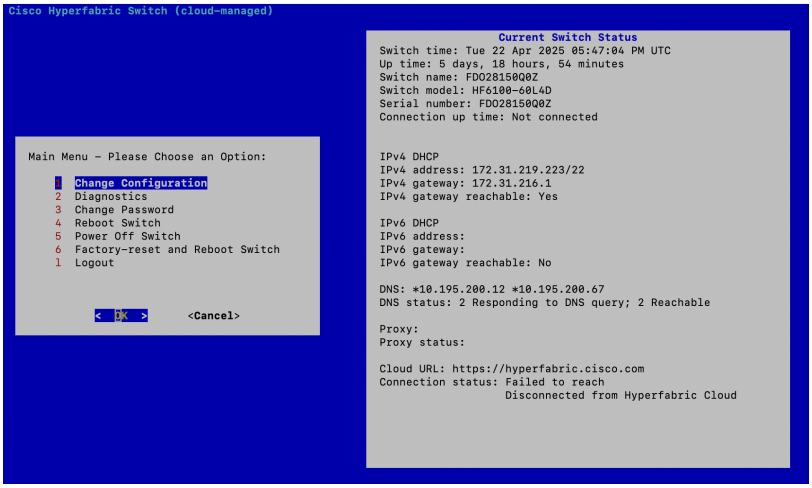
b) 現在のパスワード（「hfabric2025」）を入力してから、新しいパスワードを 2 回入力します。

```
Changing password for ttg-admin.
                                    Current password:
                                    New password:
                                    Retype new password:
                                    passwd: password updated successfully
                                    Press any key to continue
```

c) **[デフォルトのパスワードが正常に変更されました（Default password is changed successfully）]** ダイアログで、 **[OK]**を選択します。

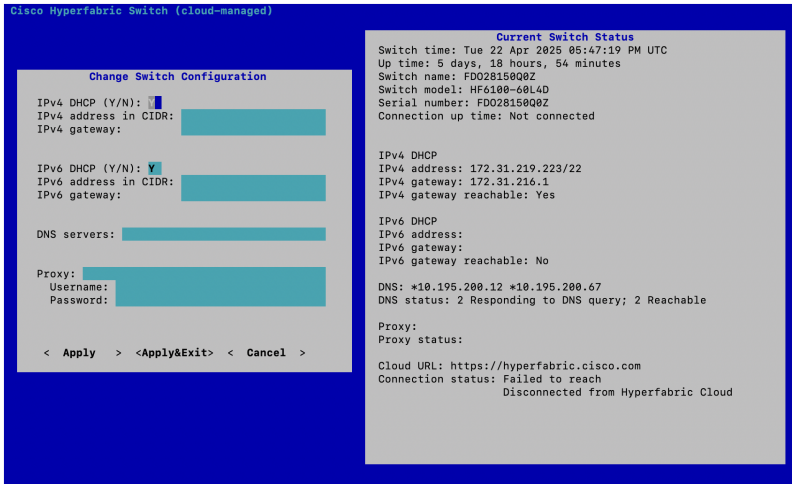
ステップ 6 コンソールメニューで、 **[設定の変更（Change Configuration）]**を選択します。

図 *34* : 構成の変更



a) 少なくとも 1 つの管理 IPv4 または IPv6 アドレスを設定します。DHCP サーバーが存在する場合は DHCP を選択できます。

図 *35 :* スイッチ構成の変更



b) 1 つまたは複数の DNS アドレスを構成します。

[DHCP] を選択した場合は、次の点に注意してください。

- DNS アドレスは必要ない場合もありますが、必要に応じて DNS アドレスを設定できます。
- スタティック DNS サーバー構成とダイナミック DNS サーバー構成の両方を設定することはできません。Cisco Nexus HyperFabric はダイナミック構成でスタティック構成を上書きします。

c) 必要に応じて、プロキシ設定を構成します。

ステップ 7 **[適用（Apply）]** を選択します。

a) コンソールを使用して、**[接続ステータス（Connection status）]** にスイッチが Cisco Nexus HyperFabric クラウドに接続されていると表示されていることを確認します。

隣接スイッチは、このスイッチを介して Cisco Nexus HyperFabric 接続を検出しアクセスできるようになります。

スイッチが接続されていない場合は、先に進む前に問題をトラブルシュート必要があります。

ヒント コンソールで、ゲートウェイ、DNS サーバー、および Cisco Nexus HyperFabric の到達可能性を確認できます。

サーバの準備

サーバに Cisco Nexus HyperFabric エージェントをインストールする

サーバを制御するために Nexus HyperFabric を有効にするには、サーバに Cisco Nexus HyperFabric エージェントをインストールする必要があります。

手順に従ってサーバに Cisco Nexus HyperFabric エージェントをインストールします。

ステップ 1 SSH を使用してサーバに接続します。

ステップ 2 NIC モードを使用するように NVIDIA BlueField-3（BF3）データ処理ユニットを構成します。

a) サーバで特権ポッドを作成します。

この例では、ノード名として「ec-e7-a7-11-f7-9c」を使用します。

```
admin@cluster3-centos-vm4:~$ oc get node
NAME                STATUS   ROLES                         AGE   VERSION
ec-e7-a7-11-f7-9c   Ready    control-plane,master,worker   58m   v1.32.9

admin@cluster3-centos-vm4:~$ oc debug node/ec-e7-a7-11-f7-9c --image=centos:10
Starting pod/ec-e7-a7-11-f7-9c-debug ...
To use host binaries, run `chroot /host`
Pod IP: 172.27.127.212
sh-5.2#
```

このコマンドの実行後にプロンプトを表示するには、Enter を押す必要がある場合があります。

b) **pciutils** と **mstflint** をインストールします。

```
sh-5.2# yum install -y pciutils mstflint
```

c) インターネットへの接続にプロキシ サーバを使用する必要がある場合は、`/etc/yum.conf` を編集します。

この例では、`/etc/yum.conf` のプロキシ構成を示しています。

```
sh-5.2# cat /etc/yum.conf
[main]
gpgcheck=1
installonly_limit=3
clean_requirements_on_remove=True
best=True
skip_if_unavailable=False
proxy=http://proxy.example.com:80
```

d) BF3 を NIC モードに変更します。

```
sh-5.2# lspci | grep ConnectX-7 | grep -v "\.1" | awk '{print $1}' | xargs -I {} mstconfig -y
\
-d {} set INTERNAL_CPU_OFFLOAD_ENGINE=1
```

e) ポッドを終了します。

```
sh-5.2# exit
```

ステップ 3 サーバの電源を再投入します。

a) サーバのベースボード管理コントローラ（BMC）に接続します。

b) サーバの電源を切り、30秒間待ちます。

c) サーバの電源をオンにします。

ステップ 4 サーバに Nexus HyperFabric エージェントをインストールします。

a) `hf_agent_deploy.yaml` をダウンロードします。

ここからファイルをダウンロードします：

https://cdn.hyperfabric.cisco.com/server/releases/agent/rhos/latest/hf_agent_deploy.yaml

b) `hf_agent_deploy.yaml` をサーバにコピーします。

c) hf_agent_deploy.yaml で **apply** コマンドを実行します。

```
admin@cluster3-centos-vm4:~$ oc apply -f hf_agent_deploy.yaml
namespace/cisco-hf created
serviceaccount/cisco-hf-agents-sa created
clusterrolebinding.rbac.authorization.k8s.io/cisco-hf-agents-privileged created
persistentvolume/cisco-hf-agents-pv created
persistentvolumeclaim/cisco-hf-agents-pvc created
daemonset.apps/cisco-hf-agents created
```

d) エージェントが正常にインストールされていることを確認します。

```
admin@cluster3-centos-vm4:~$ oc get pods -n cisco-hf
NAME                    READY   STATUS    RESTARTS   AGE
cisco-hf-agents-8pz6b   1/1     Running   0          13s

admin@cluster3-centos-vm4:~$ oc describe  pods -n cisco-hf
Name:         cisco-hf-agents-8pz6b
Namespace:    cisco-hf
Priority:     0
Node:         ec-e7-a7-11-f7-9c/172.27.127.212
Start Time:   Thu, 16 Oct 2025 16:27:46 -0700
<--- skipped --->
Events:
  Type     Reason            Age                    From               Message
  ----     ------            ----                   ----               -------
  Warning  FailedScheduling  4m48s (x2 over 4m50s)  default-scheduler  0/1 nodes are available:
 pod has unbound immediate PersistentVolumeClaims. preemption: 0/1 nodes are available: 1
Preemption is not helpful for scheduling.
  Normal   Scheduled         4m46s                  default-scheduler  Successfully assigned
cisco-hf/cisco-hf-agents-8pz6b to ec-e7-a7-11-f7-9c
  Normal   Pulling           4m45s                  kubelet            Pulling image
"public.ecr.aws/z9f4t0k6/hyperfabric/cisco_hf_agents:0.1.10"
  Normal   Pulled            4m39s                  kubelet            Successfully pulled image
 "public.ecr.aws/z9f4t0k6/hyperfabric/cisco_hf_agents:0.1.10" in 6.851s (6.851s including
waiting). Image size: 347159297 bytes.
  Normal   Created           4m38s                  kubelet            Created container:
hf-agents
  Normal   Started          4m38s                  kubelet            Started container hf-agents
```

デバイス オンボード トークンと Craft コンソールを使用してサーバに証明書を追加する

C885 または C880 サーバに Cisco Nexus HyperFabric エージェントをインストールしてから、サーバに証明書を追加する必要があります。デバイス オンボード トークンまたはベアラー トークンのいずれかを使用できます。また、Craft コンソールまたは CSR 登録スクリプトを使用できます。デバイス オンボード トークンを使用することをお勧めします。

デバイス オンボード トークンと Craft コンソールを使用してサーバに証明書を追加するには、次の手順を実行します。

ステップ 1 デバイス オンボード トークンを生成します。

トークンを生成するには、管理者ユーザである必要があります。

a) Nexus HyperFabric GUIで、ユーザ アバター（）を選択し、次に **[トークンの生成（Generate tokens）]** を選択します。

b) **[デバイス トークン（Device tokens）]** を選択し、**[デバイストークンの生成（Generate device token）]** を選択します。

c) **[コピー（Copy）]** を選択してデバイス オンボードトークン をコピーします。

ステップ 2 Craft コンソールを起動します。

a) SSH を使用し、サーバの管理 IP アドレスに admin として接続し、プロンプトが表示されたら admin パスワードを入力します。

```
$ ssh admin@management_ip_address
```

b) cisco_hf_agent Docker コンテナ内でインタラクティブな端末セッションを実行します。

```
$ docker exec -ti cisco_hf_agent bash
```

c) `main.sh` を実行します。

```
# /opt/cisco/bin/tortuga/craft-console/main.sh
```

ステップ 3 **[デバイス オンボード トークンの削除（Delete Device Onboard Token）]** を選択し、**[はい（Yes）]** を選択します。

新しいトークンを追加する前に、既存のトークンを削除する必要があります。トークンがまだ存在しない場合は、次のメッセージが表示されます：

```
token file not found: /run/drake/crypto/device-onboard-token
Failed to delete device onboard token.
Press any key to continue
```

いずれかのキーを押して、次のステップに進みます。

ステップ 4 サーバでデバイス オンボード トークンをプログラムして、証明書を追加します。

a) Craft コンソールで、**[デバイス オンボード トークンのプログラム（Program Device Onboard Token）]** を選択します。

b) コピーしたトークンを貼り付けて、Enter を押し、Ctrl+D を入力します。

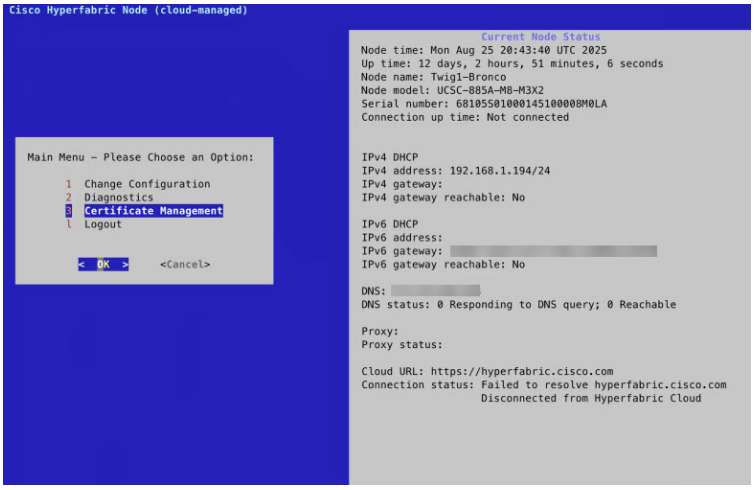
c) プロンプトが表示されたら、任意のキーを押します。

コンソールが **[証明書登録メニュー（Cert Enrollment Menu）]** に戻ります。

ステップ 5 証明書が存在することを確認します。

a) **[メイン メニュー（Main Menu）]**から、**[証明書管理（Certificate Management）]** を選択します。

図 *36 : Craft* コンソールのメイン メニュー



b) **[証明書ステータスのチェック（Check Certificate Status）]** を選択し、証明書が存在することを確認します。

コンソールに次の例のようなテキストが表示されます：

```
A valid certificate exists.
Press any key to continue
```

c) いずれかのキーを押します。

コンソールが **[証明書登録メニュー（Cert Enrollment Menu）]** に戻ります。

ステップ 6 **[デバイス オンボード トークンの削除（Delete Device Onboard Token）]** を選択し、**[はい（Yes）]** を選択します。

証明書を追加した後で、トークンを削除する必要があります。

ステップ 7 クラスタがある場合は、クラスタ内のサーバごとに、この手順を繰り返します。

デバイス オンボード トークンと CSR 登録スクリプトを使用してサーバに証明書を追加する

C885 または C880 サーバに Cisco Nexus HyperFabric エージェントをインストールしてから、サーバに証明書を追加する必要があります。デバイス オンボード トークンまたはベアラー トークンのいずれかを使用できます。また、Craft コンソールまたは CSR 登録スクリプトを使用できます。デバイス オンボード トークンを使用することをお勧めします。

この手順は CSR 登録スクリプトを使用するためのものですが、一部の手順では Craft コンソールを使用します。

デバイス オンボード トークンと CSR 登録スクリプトを使用して サーバに証明書を追加するには、次の手順を実行します。

ステップ 1 Craft コンソールを起動します。

a) SSH を使用し、サーバの管理 IP アドレスに admin として接続し、プロンプトが表示されたら admin パスワードを入力します。

```
$ ssh admin@management_ip_address
```

b) cisco_hf_agent Docker コンテナ内でインタラクティブな端末セッションを実行します。

```
$ docker exec -ti cisco_hf_agent bash
```

c) `main.sh` を実行します。

```
# /opt/cisco/bin/tortuga/craft-console/main.sh
```

ステップ 2 **[デバイス オンボード トークンの削除（Delete Device Onboard Token）]** を選択し、**[はい（Yes）]** を選択します。

新しいトークンを追加する前に、既存のトークンを削除する必要があります。トークンがまだ存在しない場合は、次のメッセージが表示されます：

```
token file not found: /run/drake/crypto/device-onboard-token
Failed to delete device onboard token.
Press any key to continue
```

いずれかのキーを押して、次のステップに進みます。

ステップ 3 デバイス オンボード トークンを生成します。

トークンを生成するには、管理者ユーザである必要があります。

a) Nexus HyperFabric GUIで、ユーザ アバター（）を選択し、次に**[トークンの生成（Generate tokens）]**を選択します。

b) **[デバイス トークン（Device tokens）]**を選択し、**[デバイストークンの生成（Generate device token）]**を選択します。

c) **[コピー（Copy）]**を選択してデバイス オンボードトークンをコピーし、**[完了（Done）]**を選択します。

ステップ 4 サーバの CLI で、デバイス オンボードトークンをエクスポートします。

a) まだサーバに接続していない場合は、SSH を使用してサーバに接続します。

b) デバイス オンボード トークンをエクスポートします。

```
admin@cluster3-centos-vm4:~$ export DEVICE_ONBOARD_TOKEN="token"
```

コピーしたデバイス オンボード トークンをトークンの場所に貼り付けます。

ステップ 5 CSR 登録スクリプトを使用して、サーバに証明書を追加します。

a) セットアップに応じて、いずれかの CSR 登録スクリプトをダウンロードします。

Ubuntu または Red Hat を搭載したスタンドアロン サーバがある場合は、次の場所から `server-csr-enroll.sh` スクリプトをダウンロードします。

https://cdn.hyperfabric.cisco.com/server/releases/agent/utils/server-csr-enroll.sh

Kubernetes または OpenShift クラスタがある場合は、次の場所から `cluster-csr-enroll.sh` スクリプトをダウンロードします。

https://cdn.hyperfabric.cisco.com/server/releases/agent/utils/cluster-csr-enroll.sh

b) ダウンロードした CSR 登録スクリプトを実行し、必要に応じて、サーバまたはクラスタ内のすべてのサーバの証明書署名要求（CSR）に署名します。

次のコマンドの 1 つを実行します。

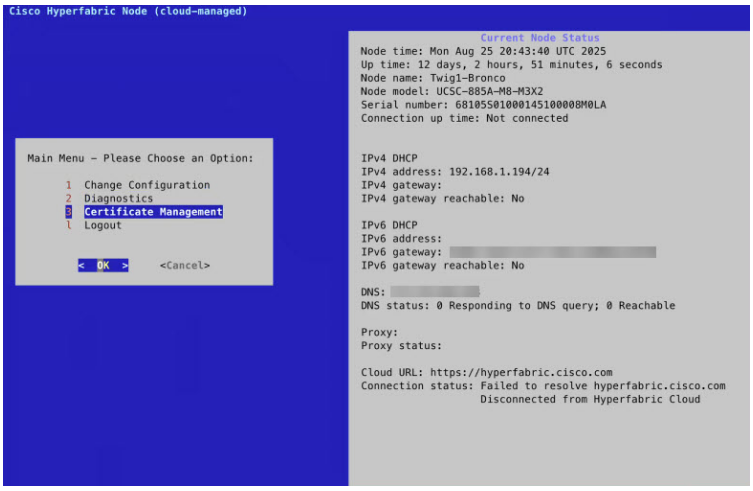
```
admin@cluster3-centos-vm4:~$ ./server-csr-enroll.sh [--force]
admin@cluster3-centos-vm4:~$ ./cluster-csr-enroll.sh [--force]
```

サーバまたはクラスタに証明書がすでにある場合は、**--force** を含めて証明書を上書きします。

ステップ 6 証明書が存在することを確認します。

a) Craft コンソールの**[メイン メニュー（Main Menu）]**から、**[証明書の管理（Certificate Management）]**を選択します。

図 *37 : Craft* コンソールのメイン メニュー



b) **[証明書ステータスのチェック（Check Certificate Status）]** を選択し、証明書が存在することを確認します。

コンソールに次の例のようなテキストが表示されます：

```
A valid certificate exists.
                name: 000b5043bca227a1bc8d3e72e05abc6d073e40341337ee67ab401a1db66db8df123
                Press any key to continue
```

c) いずれかのキーを押します。

コンソールが **[証明書登録メニュー（Cert Enrollment Menu）]** に戻ります。

ステップ 7 クラスタがある場合は、クラスタ内のサーバごとに、この手順を繰り返します。

ベアラー トークンと Craft コンソールを使用してサーバに証明書を追加する

C885 または C880 サーバに Cisco Nexus HyperFabric エージェントをインストールしてから、サーバに証明書を追加する必要があります。デバイス オンボード トークンまたはベアラー トークンのいずれかを使用できます。また、Craft コンソールまたは CSR 登録スクリプトを使用できます。デバイス オンボード トークンを使用することをお勧めします。

次の手順に従って、ベアラー トークンと Craft コンソールを使用してサーバに証明書を追加します。

ステップ 1 Craft コンソールを起動します。

a) SSH を使用し、サーバの管理 IP アドレスに admin として接続し、プロンプトが表示されたら admin パスワードを入力します。

```
$ ssh admin@management_ip_address
```

b) cisco_hf_agent Docker コンテナ内でインタラクティブな端末セッションを実行します。

```
$ docker exec -ti cisco_hf_agent bash
```

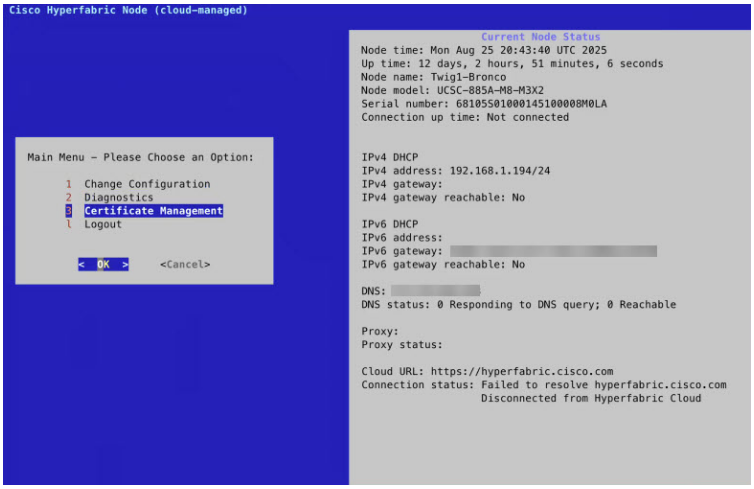
c) `main.sh` を実行します。

```
# /opt/cisco/bin/tortuga/craft-console/main.sh
```

ステップ 2 証明書が存在しないことを確認します。

a) **[メイン メニュー（Main Menu）]**から、**[証明書管理（Certificate Management）]** を選択します。

図 *38 : Craft* コンソールのメイン メニュー



b) **[証明書ステータスのチェック（Check Certificate Status）]** を選択し、証明書が存在することを確認します。

コンソールに次のテキストが表示されます。

```
Certificate does not exist; please generate a CSR, and import certificate.

                Failed to read TPM keys from nvram cannot execute /bin/bash: exit status 3
                Press any key to continue
```

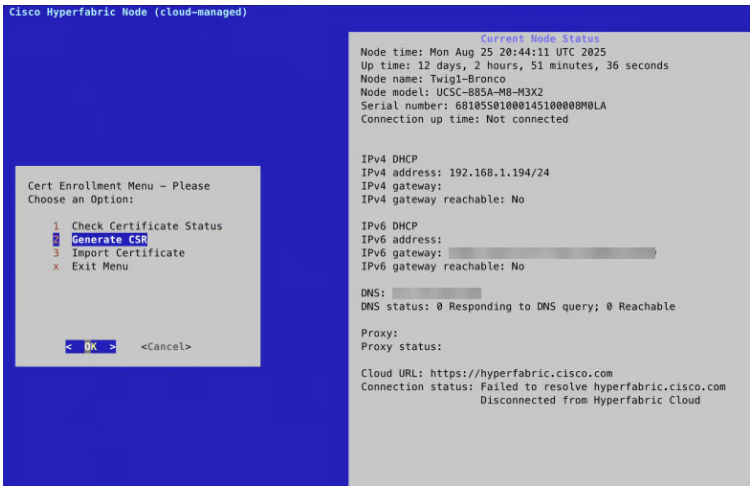
c) いずれかのキーを押します。

コンソールが **[証明書登録メニュー（Cert Enrollment Menu）]** に戻ります。

ステップ 3 証明書を生成します。

a) **[CSR の作成（Generate CSR）]** を選択します。

図 *39 : Craft* コンソールの証明書登録メニュー



しばらくすると、生成された証明書がコンソールに表示されます。

b) 証明書のテキスト（「BEGIN CERTIFICATE REQUEST」と「END CERTIFICATE REQUEST」の行を含む）を選択して、テキストをコピーします。

次に、証明書の例を示します。

```
-----BEGIN CERTIFICATE-----
                    pG8jZQ3XkDYTq5mF2sH9rVb1Lw6uJcN0eA7vXoBzS4iTnPfRxWlE3yKjG6hCvM1q
                    LdF2tUzN8mB7pXoS5cJaQkV9gWlR6yEpTzU4iFbM0hCxN2vL3sYwQ7uJdK8nV1rX
                    zW4bLmP5tGqS9jAfE6hR0xUoI2vYlZ3cNwQ8pJ/K1mV7rLxT4eFiP9bHzW6uJqD5
                    yCkN0tRvL3sXwA8mBpS2fJgQ7hUeK4nVzT1wL5uJrD9cHnM2pXqV.yLkS6tFbE0z
                    W8vJqN7xLrC5mUdG1hPzS4tWfKjQ6VbY4kN2XcP9mEzA3wUoF7sTnH1lD8rSgL0p
                    JvB5yMZxR2uKfW6qCjI3hOaT7eVnS9lQwG5dXpF1cJzK8bNvU4oRsL0yMhP3kTqV
                    6xWjF2nZcD7lBaE9mPtG1vRzS4wXoN5jQkH8uCzI2pLrY7sTnV0fJbA3dMpE6qQx
                    W9kJcO1hLwS8vPzF5tNfU2yGmB7rXoL0nD4uKjT3cVaE6pQwS9hM1/FzL7bJvN8x
                    WfR2lCoG5tUeK0n/jT4yVqS6dLwA1xMzB9uFrN2vCjH3kUoS5tWpQ8rLzEZ3qBf8
                    uH6rP.j1xW5Lk2VnRzG9aD7tSmX0C4wEoTgJvN5bF1yKsU2hQlM8pO6dXcS3nLrA
                    0zVjI7uG4kP9yTqWbM6cF2vJoS1hE8xLwR3pNfK5dU0mJzA7tYgQnV4lB9wXfC2s
                    H5rP6uKjT1oD8qS0vN3yLpI7bZxR4nWfM6tU2cG5aH9jEoT0pV3lDsK8wQmJ1yLz
                    S7uN4xFbR6qC2nP5oH0kVtG3dJ8yM1vWzA7rQjL4sXnE9pU6oS2hT5cKfNkF8vN2
                    yR7jQ1tXpZ6wLsH3oD9uB5eV4aGmT0lJcW8zM2/SnY7qK1pXrI6hV3dU9bS5oL4j
                    A0nGvT8wE2cFzM7tQpN1yJkR6lW3sD9uB5a/4xH0mJfC8oS2nY7qK1vXrT6pE3zI
                    9bL5jW4hU0lGmA8dF2yR7tQ.N1oKcV6wS3nJ9uB5aL4xG0mHfT8vN2yR7jQ1tXpZ
                    6wLsH3oD9uB5eV4aGmT0lJcW8zM2fSnY7qK1pXrI6hV3dU9bS5oL4jA0nGvT8wE2
                    cFzM7tQpN1yJkR6lW3sDpG8jZQ3XkDYTq5mF2sH9rVb1Lw6uJcN0eA7vXoBzS4iT
                    nPfRxWlE3yKjG6hCvM1qLdF2tUzN8mB7pXoS5cJaQkV9gWlR6yEpTzU4iFbM0hCx
                    N2vL3sYwQ7uJdK8nV1rXzW4bLmP5tGqS9jAfE6hR0xUoI2vYlZ3cNwQ8pJsK1mV7
                    rLxT4eFiP9bHzW6uJqD5yCkN0tRvL3sXwA8mBpS2fJgQ7hUeK4nVzT1wL5uJrD9c
                    HnM2pXq/3yLkS6tFbE0zW8vJqN7xLrC5mUdG1hPzS4tW.KjQ6VbY4kN2XcP9mEzA
                    3wUoF7sTnH1lD8rSgL0pJvB5yMZxR2uKfW6qCjI3hOaT7eVnS9lQwG5dXpF1cJzK
                    8bNvU4oRsL0yMhP3kTqV6xWjF2nZcD7lBaE9mPtG/vRzS4wXoN5jQkH8uCzI2pLr
                    Y7sTnV0fJbA3dMpE6qQxW9kJcO1hLwS8vPzF5tNfU2yGmB7rXoL0nD4uKjT3cVaE
                    6pQwS9hM1yFzL7bJvN8xWfR2lCoG5tUeK0nPjT4yVqS6dLwA1xMzB9uFrN2vCjH3
                    kUoS5tWpQ8rLzEZ3qBf8uH6rPYj1xW5Lk2VnRzG9aD7tSmX0C4wEoTgJvN5bF1yK
                    sU2hQlM8pO6dXcS3nLrA0zVjI7uG4kP9yTqWbM6cF2vJoS1hE8xLwR3pNfK5dU0m
                    JzA7tYgQnV4lB9wXfC2sH5rP6uKjT1oD8qS0vN3yL/I7bZxR4nWfM6tU2cG5aH.j
                    EoT0pV3lDsK8wQmJ1yLzS7uN4xFbR6qC2nP5oH0kVtG3dJ8yM1vWzA7rQjL4sXnE
                    9pU6oS2hT5cKfNkF8vN2yR7jQ1tXpZ6wLsH3oD9uB5eV4aGmT0lJcW8zM2fSnY7q
                    K1pXrI6hV3dU9bS5oL4jA0nGvT8wE2cFzM7tQpN1yJkR6lW3sD9/B5aV4xH0mJfC
                    8oS2nY7qK1vXrT6pE3zI9bL5jW4hU0lGmA8dF2yR7tQpN1oKcV6wS3nJ9uB5aL4x
-----END CERTIFICATE-----
```

```
W3.1X39e83zEKT2yskG=
-----END CERTIFICATE-----
```

c) Cisco Nexus HyperFabric GUIで、**[管理（Administration）]** > **[サーバ証明書（Server certificates）]**を選択します。

図 *40*：新しいサーバ証明書署名要求（*CSR*）



d) 左側のフィールドに証明書を貼り付けてから、**[送信（Submit）]** を選択します。

証明書が右側のフィールドに表示されます。

図 *41*：新しいサーバ証明書署名要求（*CSR*）の発行



e) 右側のフィールドの横にある **[コピー（Copy）]** を選択します。

ステップ 4 証明書をサーバにインポートします。

a) Craft コンソールで、**[証明書のインポート（Import Certificate）]** を選択します。

コンソールに次のテキストが表示されます：

```
Paste your certificate text below.
                When you are done, press Enter, then type Ctrl-D.
```

b) 証明書の内容を貼り付けて Enter、そして CTRL+D を押します。

プロセスが完了するまでに約 1 分かかります。その後、コンソールに次の例のようなテキストが表示されます：

```
-----BEGIN CERTIFICATE-----
                pG8jZQ3XkDYTq5mF2sH9rVb1Lw6uJcN0eA7vXoBzS4iTnPfRxWlE3yKjG6hCvM1q
                LdF2tUzN8mB7pXoS5cJaQkV9gWlR6yEpTzU4iFbM0hCxN2vL3sYwQ7uJdK8nV1rX
                zW4bLmP5tGqS9jAfE6hR0xUoI2vYlZ3cNwQ8pJ/K1mV7rLxT4eFiP9bHzW6uJqD5
                yCkN0tRvL3sXwA8mBpS2fJgQ7hUeK4nVzT1wL5uJrD9cHnM2pXqV.yLkS6tFbE0z
                W8vJqN7xLrC5mUdG1hPzS4tWfKjQ6VbY4kN2XcP9mEzA3wUoF7sTnH1lD8rSgL0p
                JvB5yMZxR2uKfW6qCjI3hOaT7eVnS9lQwG5dXpF1cJzK8bNvU4oRsL0yMhP3kTqV
                6xWjF2nZcD7lBaE9mPtG1vRzS4wXoN5jQkH8uCzI2pLrY7sTnV0fJbA3dMpE6qQx
                W9kJcO1hLwS8vPzF5tNfU2yGmB7rXoL0nD4uKjT3cVaE6pQwS9hM1/FzL7bJvN8x
                WfR2lCoG5tUeK0n/jT4yVqS6dLwA1xMzB9uFrN2vCjH3kUoS5tWpQ8rLzEZ3qBf8
                uH6rP.j1xW5Lk2VnRzG9aD7tSmX0C4wEoTgJvN5bF1yKsU2hQlM8pO6dXcS3nLrA
                0zVjI7uG4kP9yTqWbM6cF2vJoS1hE8xLwR3pNfK5dU0mJzA7tYgQnV4lB9wXfC2s
                H5rP6uKjT1oD8qS0vN3yLpI7bZxR4nWfM6tU2cG5aH9jEoT0pV3lDsK8wQmJ1yLz
                S7uN4xFbR6qC2nP5oH0kVtG3dJ8yM1vWzA7rQjL4sXnE9pU6oS2hT5cKfNkF8vN2
```

```
yR7jQ1tXpZ6wLsH3oD9uB5eV4aGmT0lJcW8zM2/SnY7qK1pXrI6hV3dU9bS5oL4j
A0nGvT8wE2cFzM7tQpN1yJkR6lW3sD9uB5a/4xH0mJfC8oS2nY7qK1vXrT6pE3zI
9bL5jW4hU0lGmA8dF2yR7tQ.N1oKcV6wS3nJ9uB5aL4xG0mHfT8vN2yR7jQ1tXpZ
6wLsH3oD9uB5eV4aGmT0lJcW8zM2fSnY7qK1pXrI6hV3dU9bS5oL4jA0nGvT8wE2
cFzM7tQpN1yJkR6lW3sDpG8jZQ3XkDYTq5mF2sH9rVb1Lw6uJcN0eA7vXoBzS4iT
nPfRxWlE3yKjG6hCvM1qLdF2tUzN8mB7pXoS5cJaQkV9gWlR6yEpTzU4iFbM0hCx
N2vL3sYwQ7uJdK8nV1rXzW4bLmP5tGqS9jAfE6hR0xUoI2vYlZ3cNwQ8pJsK1mV7
rLxT4eFiP9bHzW6uJqD5yCkN0tRvL3sXwA8mBpS2fJgQ7hUeK4nVzT1wL5uJrD9c
HnM2pXq/3yLkS6tFbE0zW8vJqN7xLrC5mUdG1hPzS4tW.KjQ6VbY4kN2XcP9mEzA
3wUoF7sTnH1lD8rSgL0pJvB5yMZxR2uKfW6qCjI3hOaT7eVnS9lQwG5dXpF1cJzK
8bNvU4oRsL0yMhP3kTqV6xWjF2nZcD7lBaE9mPtG/vRzS4wXoN5jQkH8uCzI2pLr
Y7sTnV0fJbA3dMpE6qQxW9kJcO1hLwS8vPzF5tNfU2yGmB7rXoL0nD4uKjT3cVaE
6pQwS9hM1yFzL7bJvN8xWfR2lCoG5tUeK0nPjT4yVqS6dLwA1xMzB9uFrN2vCjH3
kUoS5tWpQ8rLzEZ3qBf8uH6rPYj1xW5Lk2VnRzG9aD7tSmX0C4wEoTgJvN5bF1yK
sU2hQlM8pO6dXcS3nLrA0zVjI7uG4kP9yTqWbM6cF2vJoS1hE8xLwR3pNfK5dU0m
JzA7tYgQnV4lB9wXfC2sH5rP6uKjT1oD8qS0vN3yL/I7bZxR4nWfM6tU2cG5aH.j
EoT0pV3lDsK8wQmJ1yLzS7uN4xFbR6qC2nP5oH0kVtG3dJ8yM1vWzA7rQjL4sXnE
9pU6oS2hT5cKfNkF8vN2yR7jQ1tXpZ6wLsH3oD9uB5eV4aGmT0lJcW8zM2fSnY7q
K1pXrI6hV3dU9bS5oL4jA0nGvT8wE2cFzM7tQpN1yJkR6lW3sD9/B5aV4xH0mJfC
8oS2nY7qK1vXrT6pE3zI9bL5jW4hU0lGmA8dF2yR7tQpN1oKcV6wS3nJ9uB5aL4x
W3.1X39e83zEKT2yskG=
-----END CERTIFICATE-----

Certificate imported successfully
drake: stopped
drake: started
Press any key to continue
```

c) いずれかのキーを押します。

コンソールが **[証明書登録メニュー（Cert Enrollment Menu）]** に戻ります。

ステップ 5 証明書が存在することを確認します。

a) **[証明書ステータスのチェック（Check Certificate Status）]** を選択し、証明書が存在することを確認します。

コンソールに次の例のようなテキストが表示されます：

```
A valid certificate exists.
                name: 000b5043bca227a1bc8d3e72e05abc6d073e40341337ee67ab401a1db66db8df123
                Press any key to continue
```

b) いずれかのキーを押します。

コンソールが **[証明書登録メニュー（Cert Enrollment Menu）]** に戻ります。

ステップ 6 クラスタがある場合は、クラスタ内のサーバごとに、このサブステップを繰り返します。

ベアラー トークンと CSR 登録スクリプトを使用してサーバに証明書を追加する

C885 または C880 サーバに Cisco Nexus HyperFabric エージェントをインストールしてから、サーバに証明書を追加する必要があります。デバイス オンボード トークンまたはベアラー トークンのいずれかを使用できます。また、Craft コンソールまたは CSR 登録スクリプトを使用できます。デバイス オンボード トークンを使用することをお勧めします。

この手順は CSR 登録スクリプトを使用するためのものですが、一部の手順では Craft コンソールを使用します。

次の手順に従い、ベアラー トークンと CSR 登録スクリプトを使用して サーバに証明書を追加します。

ステップ 1 ベアラー トークンを生成します。

トークンを生成するには、管理者ユーザである必要があります。ベアラー トークンの詳細については、「Cisco DevNetでの 認証」を参照してください。

a) Nexus HyperFabric GUIで、ユーザ アバター（）を選択し、次に**[トークンの生成（Generate tokens）]**を選択します。
b) **[API ベアラー トークン（API bearer tokens）]**を選択し、**[ベアラー トークンの追加（Add a bearer token）]**を選択します。
c) フィールドに入力し、**[トークンの生成（Generate Token）]**を選択します。
d) **[コピー（Copy）]**を選択してデバイス トークンをコピーし、**[完了（Done）]**を選択します。

ステップ 2 サーバの CLI で、デバイス オンボードトークンをエクスポートします。

a) まだサーバに接続していない場合は、SSH を使用してサーバに接続します。
b) デバイス オンボード トークンをエクスポートします。

```
admin@cluster3-centos-vm4:~$ export DEVICE_ONBOARD_TOKEN="token"
```

コピーしたデバイス トークンをトークンの場所に貼り付けます。

ステップ 3 CSR 登録スクリプトを使用して、サーバに証明書を追加します。

a) セットアップに応じて、いずれかの CSR 登録スクリプトをダウンロードします。

Ubuntu または Red Hat を搭載したスタンドアロン サーバがある場合は、次の場所から `server-csr-enroll.sh` スクリプトをダウンロードします。

https://cdn.hyperfabric.cisco.com/server/releases/agent/utils/server-csr-enroll.sh

Kubernetes または OpenShift クラスタがある場合は、次の場所から `cluster-csr-enroll.sh` スクリプトをダウンロードします。

https://cdn.hyperfabric.cisco.com/server/releases/agent/utils/cluster-csr-enroll.sh

b) ダウンロードした CSR 登録スクリプトを実行し、必要に応じて、サーバまたはクラスタ内のすべてのサーバの証明書署名要求（CSR）に署名します。

次のコマンドの 1 つを実行します。

```
admin@cluster3-centos-vm4:~$ ./server-csr-enroll.sh [--force] [-p http://proxy.example.com:80]
admin@cluster3-centos-vm4:~$ ./cluster-csr-enroll.sh [--force] [-p http://proxy.example.com:80]
```

サーバまたはクラスタに証明書がすでにある場合は、**--force** を含めて証明書を上書きします。

プロキシを使用している場合は、**-p**を含めます。

ステップ 4 Craft コンソールを起動します。

a) SSH を使用し、サーバの管理 IP アドレスに admin として接続し、プロンプトが表示されたら admin パスワードを入力します。

```
$ ssh admin@management_ip_address
```

b) cisco_hf_agent Docker コンテナ内でインタラクティブな端末セッションを実行します。

```
$ docker exec -ti cisco_hf_agent bash
```

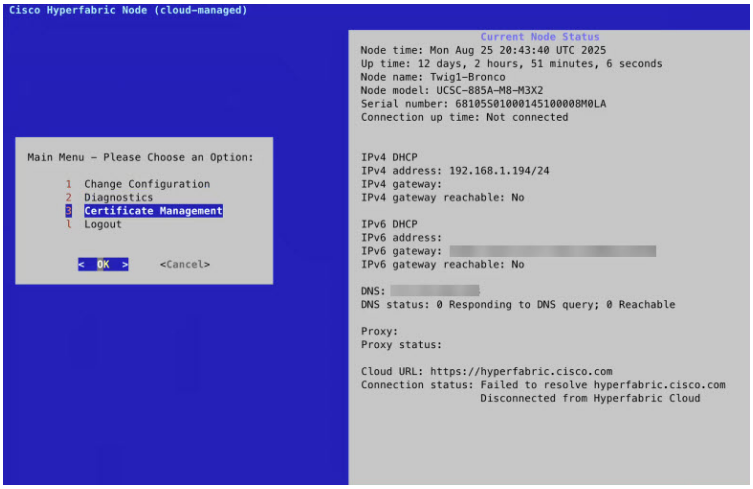
c) `main.sh` を実行します。

```
# /opt/cisco/bin/tortuga/craft-console/main.sh
```

ステップ 5 証明書が存在することを確認します。

a) **[メイン メニュー（Main Menu）]**から、**[証明書管理（Certificate Management）]** を選択します。

図 *42 : Craft* コンソールのメイン メニュー



b) **[証明書ステータスのチェック（Check Certificate Status）]** を選択し、証明書が存在することを確認します。

コンソールに次の例のようなテキストが表示されます：

```
A valid certificate exists.
                name: 000b5043bca227a1bc8d3e72e05abc6d073e40341337ee67ab401a1db66db8df123
                Press any key to continue
```

c) いずれかのキーを押します。

コンソールが **[証明書登録メニュー（Cert Enrollment Menu）]** に戻ります。

ステップ 6 クラスタがある場合は、クラスタ内のサーバごとに、この手順を繰り返します。

Cisco Nexus HyperFabric エージェントのインストールに関する考慮事項

以下の考慮事項は、Cisco Nexus HyperFabric エージェントのインストールに適用されます。

- サーバのホスト オペレーティング システムとして OpenShift CoreOS をインストールした後にのみ、サーバにエージェントをインストールできます。
- Nexus HyperFabric エージェントをインストールしたサーバを、構成管理とテレメトリのために Nexus HyperFabric クラウド コントローラに接続します。ポートの使用方法に関係なく、そのカーネルで使用可能なサーバ ルーティング テーブルに応じて、エージェントは任意のポートを使用できます。たとえば、ポートをイーストウェストのトラフィック、ノースサウスのトラフィック、および管理に使用できます。通信が管理インターフェイスを介して行う必要がある場合は、それに応じてルーティング テーブルを設定する必要があります。エージェントがクラウド コントローラに直接到達できない場合、エージェントはファブリックの終了ノードによって、コントローラに到達します。

Cisco Nexus Hyperfabric サーバ エージェントと ISO イメージ

この表は Cisco Nexus HyperFabric でサーバを使用する必要があるエージェントと ISO イメージのダウンロード場所を示しています。

表 *6*：サーバ エージェントと *ISO* イメージ

エージェントまたは ISO イメージ	ダウンロードの場所
UCS エージェント インストーラ	適切なパッケージをダウンロードします。 RPM：https://cdn.hyperfabric.cisco.com/server/releases/agent/latest/ucs_agent_installer_latest.rpm DEB：https://cdn.hyperfabric.cisco.com/server/releases/agent/latest/ucs_agent_installer_latest.deb
Nexus HyperFabric の展開エージェント 詳細については、サーバに Cisco Nexus HyperFabric エージェントをインストールする （52 ページ）を参照してください。	https://cdn.hyperfabric.cisco.com/server/releases/agent/latest/hf_agent_deploy.yaml

デバイスの申請

配信時には、新しいデバイスは所有者や組織に関連付けられていません。デバイスを展開する前に、Cisco Nexus HyperFabric を介してデバイスを要求し、デバイスを展開するファブリックを所有する組織に追加する必要があります。

（注）

場合によっては、出荷前にデバイスがすでに組織に対して要求されていることがあります。その場合は、要求の手順をスキップできます。

デバイスを要求するには、デバイスへの物理的アクセスおよび管理的アクセスが必要です。

デバイスの要求に関する制限事項

デバイスの要求には、次の制限が適用されます。

- 要求コードを使用して、ファブリックの最初のデバイスを要求する必要があります。
- 要求コードを使用せずにデバイスを要求する場合、Cisco Nexus HyperFabric が検出したスイッチのみを要求できます。検出プロセスは、すでに要求されている Nexus HyperFabric スイッチに直接接続されているスイッチに限定されます。これらの直接接続されたデバイスのみが検出されたリストに表示され、要求に使用できます。

要求コードを使用したスイッチの要求

要求コードを使用して、ファブリックの最初のスイッチを要求する必要があります。要求コードを使用して後続のスイッチを要求することも、要求コードを使用せずに検出されたスイッチを要求することもできます。要求コードを使用せずにスイッチを要求する方法については、要求コードを使用せずに検出されたデバイスを要求する （66 ページ）を参照してください。

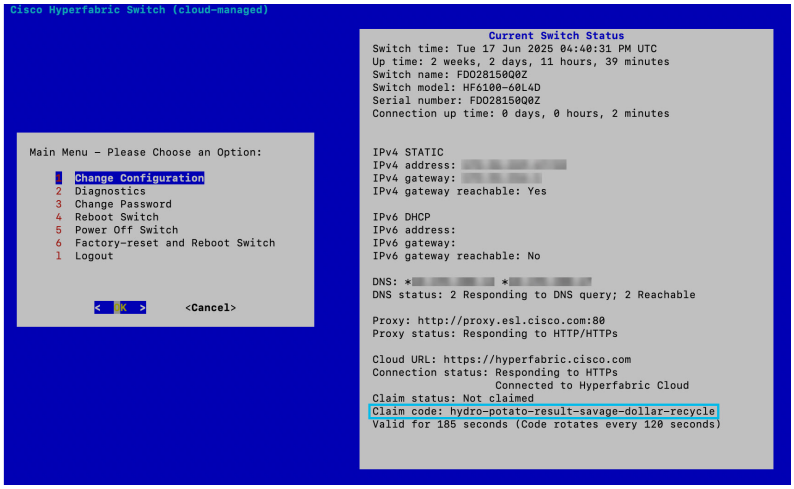
要求コードを使用してスイッチを要求するには、次の手順に従います。

ステップ 1 シリアルコンソールを使用してスイッチにログインし、シリアルコンソールのメニューに表示される要求コードを取得します。

複数のスイッチを要求する場合は、要求するすべてのスイッチからコードを取得します。

コードの有効期間は 4 分間ですが、コンソールに表示される要求コードは 2 分ごとに変更されます。

図 *43* : 要求コードの例



ステップ 2 Cisco Nexus HyperFabric の GUI で、**[インベントリ（Inventory）]** > **[デバイス インベントリ（Device Inventory）]** を選択します。

ステップ 3 **[デバイスの要求（Claim devices）]** を選択します。

ステップ 4 要求コードを入力し、**[要求（Claim）]** をクリックします。

複数のスイッチを要求する場合は、コードをカンマまたは改行で区切って入力します。

その後、スイッチは要求どおりに現在の組織に登録されます。他のファブリック スイッチが設置されて接続されると、最初のスイッチに接続されている要求のないスイッチが検出されます。

要求コードを使用せずに検出されたデバイスを要求する

要求コードを使用してファブリックの最初のデバイスを要求する必要があります。つまり、最初のデバイスにはこの手順を使用できません。ただし、要求コードを使用せずに、追加の検出済みデバイスを要求することはできます。要求コードを使用して最初のデバイスまたは後続のデバイスを要求する方法については、要求コードを使用したスイッチの要求 （65 ページ） を参照してください。

ベースボード管理コントローラ（BMC）ポートを使用してサーバを要求することはできません。

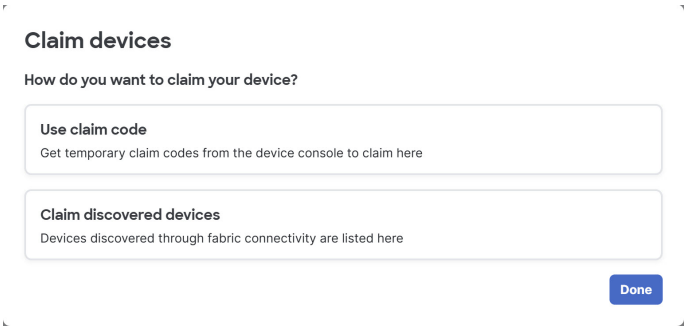
要求コードを使用せずに検出されたデバイスを要求するには、次の手順に従います。

ステップ 1 **[インベントリ（Inventory）]** > **[デバイス インベントリ（Device Inventory）]** を選択します。

ステップ 2 **[デバイスの要求（Claim devices）]** をクリックします。

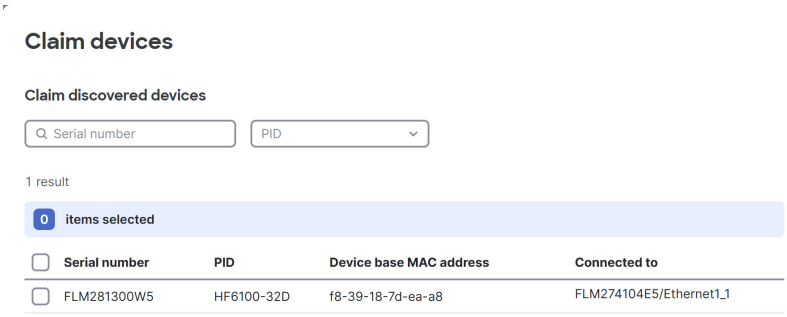
ステップ 3 **[検出デバイスの要求（Claim detected devices）]** をクリックします。

図 *44* : デバイスの要求



ステップ 4 1 つまたは複数のスイッチを選択し、**[要求（Claim）]** をクリックします。

図 *45* : デバイスの要求



その後、スイッチは要求どおりに現在の組織に登録されます。

オプションで、**[シリアル番号（Serial number）]** フィールドを使用して特定のシリアル番号を持つデバイスを検索し、**[PID]** ドロップダウンから選択した製品 ID を持つスイッチ をフィルタ処理できます。

デバイスのバインド

Cisco Nexus HyperFabric では、各物理スイッチをファブリック ブループリント内の論理的な位置（ノード）に割り当てる必要があります（「バインド」）。スイッチがブループリントのノードにバインドされていれば、Cisco Nexus HyperFabric から設定をダウンロードできます。

要求されたものの、組織のファブリックにまだバインドされていないスイッチは、実際のファブリックにバインドされるまで、待機場（「ヌル」ファブリック）にバインドされていると見なされます。

（注）

最初のデバイスをファブリックにバインドすると、Cisco Nexus HyperFabric は 、ファブリックのバージョンをそのデバイスで実行されているソフトウェア バージョンに設定します。待機場内のデバイスは自動的に最新バージョンにアップグレードされるため、ファブリックのバージョンは最新リリースに設定されます。

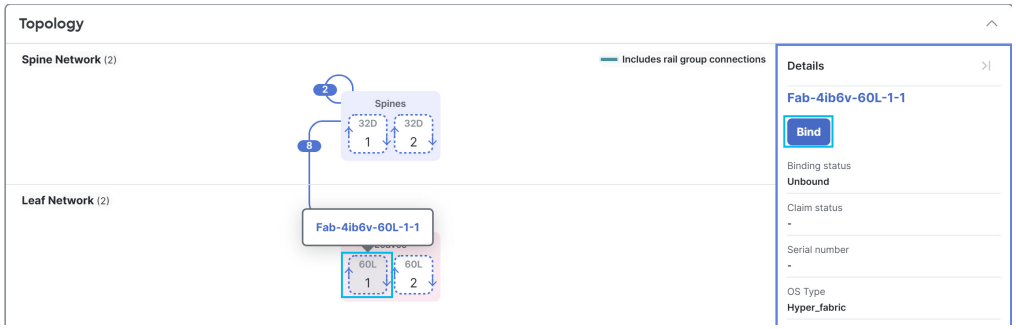
デバイスをバインドするには、次の手順に従います。

ステップ 1 **[ファブリック（Fabrics）]**を選択し、スイッチを含むファブリックを選択します。

a) ファブリックが編集モードでない場合は、**[編集モードに切り替える（Switch to edit mode）]**（）を選択します。

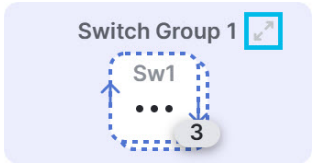
ステップ 2 **[トポロジ（Topology）]**エリアで、バインドするスイッチの位置をクリックし、スイッチ情報ペインで**[バインド（Bind）]** をクリックします。

図 *46*：トポロジ



グループに 3 つ以上のデバイスがある場合は、位置を選択する前にグループを展開する必要があります。

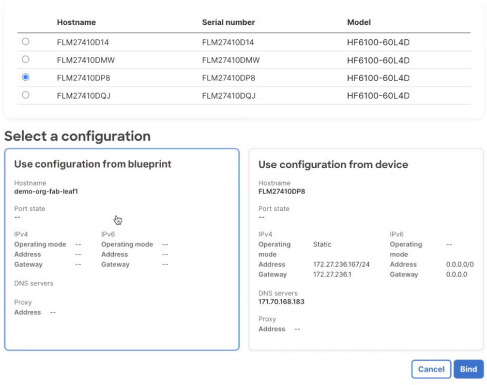
図 *47*：スイッチ グループの展開



ステップ 3 トポロジ内のこの位置に割り当てる物理スイッチを選択します。

結果のダイアログに、デバイス設定の 2 つのオプションが表示されます。

図 *48*：構成を選択します。



ステップ 4 構成を選択します。

- **[ブループリントからの構成を使用（Use configuration from blueprint）]**：ブループリントで定義された構成を使用します。これを選択した場合は、ブループリントで定義済みの構成でスイッチをクラウ

ドに接続できることを確認してください。*Cisco Nexus Hyperfabric* — スイッチの構成ドキュメントの「管理インターフェイスの構成」の手順を参照してください。

- **[デバイスからの構成を使用（Use configuration from device）]**：シリアル ポートを介して構成された現在のデバイス設定を使用します。Cisco Nexus HyperFabric はデバイスの設定でブループリントを更新します。

ステップ 5 デバイスをファブリック ブループリントのこの論理的な場所にバインドするには、**[バインド（Bind）]** を選択します。

デバイスのバインド操作が正常に完了すると、トポロジ エリアのデバイス アイコンが青色になります。

ステップ 6 残りのデバイスをバインドするには、これらの手順を繰り返します。

ステップ 7 デバイスのクラウド接続ステータスを確認します。

a) ページの左上近くにあるファブリックの名前を選択して、ファブリックのページに戻ります。

b) **[物理トポロジ（Physical topology）]** エリアで、**[クラウド接続（Cloud connectivity）]** を選択します。

このページでは、次のプロパティを確認できます。

- **[送信元IP：ポート（Source IP:Port）]**：送信元 IP アドレスとポート。
- **[宛先 IP：ポート（Destination IP:Port）]**：宛先 IP アドレスまたは宛先ポート
- **[接続パス（Connection path）]**：スイッチがクラウドに接続するときに通過するパス。表示される値は次のとおりです。
  - **[管理ポート（Management port）]**：パスはスイッチの管理ポート経由です。
  - ***[switch_name]***：パスは、指定されたスイッチを経由します。これは出口ノードです。
  - ***[port_ID]***：パスはスイッチのインバンド管理ポートを経由します。ポートの ID が表示されます。
- **[証明書チェーン（Certificate chain）]**：スイッチのトランスポート層セキュリティ（TLS）証明書が有効か無効かを指定します。証明書が無効な場合は、**[無効（Invalid）]** を選択して 、問題に関する情報を受信します。

QR コードをスキャンしてスイッチの詳細をレビューする

Cisco 6000 シリーズ スイッチには、固有の QR コードが記載されたステッカーが付いています。QR コードは、スイッチのシリアル番号を含む起動 URL を提供します。モバイル デバイスを使用してコードをスキャンし、URL を開いて Cisco Nexus HyperFabric GUI のスイッチの詳細ページに移動できます。

QR コードの詳細については、Cisco Nexus Hyperfabric シリーズ – QR コードドキュメントを参照してください。

QR コードをスキャンしてスイッチの詳細をレビューするには、次の手順に従います。

ステップ 1 モバイルデバイスを使用して QR コードをスキャンします。

ステップ 2 コードで提供される URL に移動します。

次のいずれかの結果が発生します。

- Cisco Nexus HyperFabric GUI にログインしていない場合は、ログインページにリダイレクトされます。ログインすると、ログイン中に QR コードをスキャンした場合と同様にプロセスが続行されます。他の可能な結果を参照してください。
- Cisco Nexus HyperFabric GUI にログインし、ログインした組織によってスイッチが要求されている場合、スイッチの詳細を示す GUI ページが表示されます。
- Cisco Nexus HyperFabric GUI にログインしているが、スイッチが要求されていない場合、またはスイッチがログインしていない組織によって要求されている場合、スイッチの詳細にはアクセスできません。

設計を終了してコミットする

変更内容を確認、確定、およびプッシュするまで、ファブリックに適用されません。

設計を終了してコミットするには、次のステップに従います。

ステップ 1 **[構成のレビュー（Review configuration）]** を選択します。

ステップ 2 レビューリストで変更を確認します。

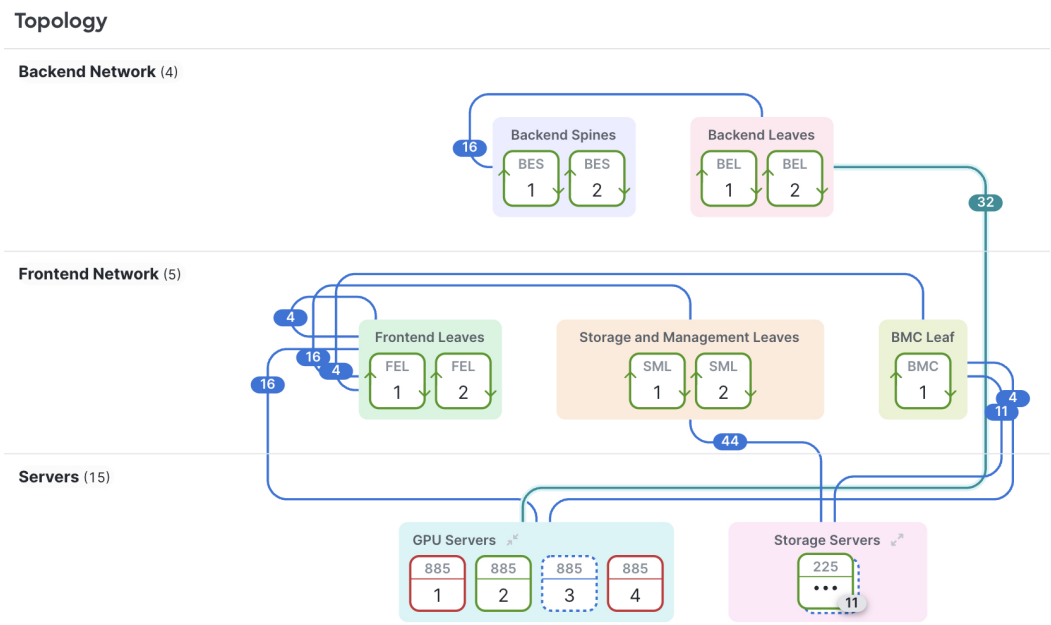
ステップ 3 **[コメントしてプッシュ（Comment and push）]** を選択します。

ステップ 4 **[構成を送信する前のコメント（Comments before sending configuration）]** ダイアログボックスに、変更の理由を入力します。

ステップ 5 **[構成のプッシュ（Push Configuration）]** を選択します。

このプッシュの一部としてデバイスをバインドした場合、デバイスアイコンの輪郭の色により、デバイスのアサーションを示します。デバイスに問題がなければ、緑色の輪郭が表示されるはずです。黄色の輪郭は、デバイスが予期しない状態になっており、問題が検出されていることを示していますが、その問題によって動作が中断することはありません。赤色の輪郭は、デバイスが予期しない状態になっており、動作の中断を引き起こす可能性のある問題が検出されたことを示しています。問題を調査する必要があります。

図 *49* : 構成をプッシュした後のファブリック トポロジ



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。