



Cisco DNA Center SD-Access LAN 自動化導入ガイド

LAN 自動化：段階的な導入手順 2

ワークフロー 2

ステップ 1：計画 3

ステップ 2：設計 19

ステップ 3：検出 22

ステップ 4：プロビジョニング 33

既存の LAN 自動化スタックへのスイッチとリンクの追加 48

LAN 自動化のトラブルシューティング 53

追加情報：Cisco DNA Center 2.3.5 以降の LAN 自動化 53

LAN 自動化：段階的な導入手順

シスコの LAN 自動化を導入すると、ネットワーク運用がシンプルになり、IT スタッフが時間のかかる反復的なネットワーク設定作業から解放され、エラーのない標準のアンダーレイネットワークを作成できます。LAN 自動化により、従来のネットワーク計画と実装プロセスを必要とせずに、アンダーレイネットワークの構築が迅速化されます。

このガイドは Cisco DNA Center 2.3.3 に基づいています。ただし、ガイドの追加トピックでは、Cisco DNA Center 2.3.5 以降に基づく LAN 自動化プロセスに関する情報を提供します。

手順と例は、Cisco DNA Center バージョンによって異なる場合があります。LAN 自動化および関連機能の設定の詳細については、[Cisco DNA Center Documentation ポータル](#)の『*Cisco DNA Center User Guide*』を参照してください。

ワークフロー

シスコの LAN 自動化には、主に次のような利点があります。

- ゼロタッチプロビジョニング：ネットワークデバイスが動的に検出およびオンボーディングされ、工場出荷時の状態からネットワークに完全に統合されるまでが自動化されます。
- エンドツーエンドのトポロジ：新しいネットワークシステムとその物理接続を動的に検出するように、検出プロセスをモデル化してプログラミングできます。それらの新しいシステムをレイヤ3 IP アドレッシングおよびルーティングプロトコルを使用して自動化し、エンドツーエンドのルーティングトポロジを動的に構築できます。
- 復元力：シスコの LAN 自動化には、転送トポロジと冗長性を最適化するシステムとネットワークの設定パラメータが統合されています。シスコの LAN 自動化でシステムレベルの冗長性を確保し、ベストプラクティスを自動的に適用することで、計画的または計画外のネットワーク停止時もクラス最高水準の復元力が提供されます。
- セキュリティ：シスコ推奨のネットワークアクセスおよびインフラストラクチャの保護パラメータが自動的に適用され、最初の導入時点から妥協のないセキュリティが提供されます。
- コンプライアンス：LAN 自動化によって人的ミスや設定の誤りが排除され、IT リソースの浪費につながるルールや設定の不整合を減らすことができます。新しいシステムのオンボーディング時、LAN 自動化で Cisco DNA Center のグローバルに管理されるパラメータを自動化することにより、ネットワーク インフラストラクチャ全体でコンプライアンスが確保されます。

シスコの LAN 自動化ワークフローの4つの主要なステップに従って、企業の IT 管理者は新規ネットワークの準備、計画、および自動化を進めることができます。

手順

ステップ 1 計画：LAN 自動化における各種のロールについて理解します。サイトと IP プールの計画を立て、シードデバイスの前提条件を確認します。

ステップ2 設計：グローバルサイトを設計して構築します。グローバルなネットワークサービスとサイトレベルのネットワークサービスを設定します。グローバル デバイス クレデンシャルを設定します。グローバル IP アドレスプールを設計し、LAN 自動化プールを割り当てます。

ステップ3 検出：シードデバイスを検出します。

ステップ4 プロビジョニング：LAN 自動化を開始および停止します。

- a) LAN自動化の開始：シードデバイスに一時的な設定をプッシュし、デバイスを検出し、イメージをアップグレードし、検出されたデバイスに初期設定をプッシュします。
- b) LAN 自動化の停止：すべてのポイントツーポイントリンクをレイヤ3に変換します。

ステップ1：計画

アンダーレイネットワークを構築するための最初のステップはLAN 自動化の計画です。このセクションでは、シスコのLAN 自動化のサポートマトリックスをターゲットのアンダーレイネットワーク環境にあてはめて計画する必要がある項目について説明します。

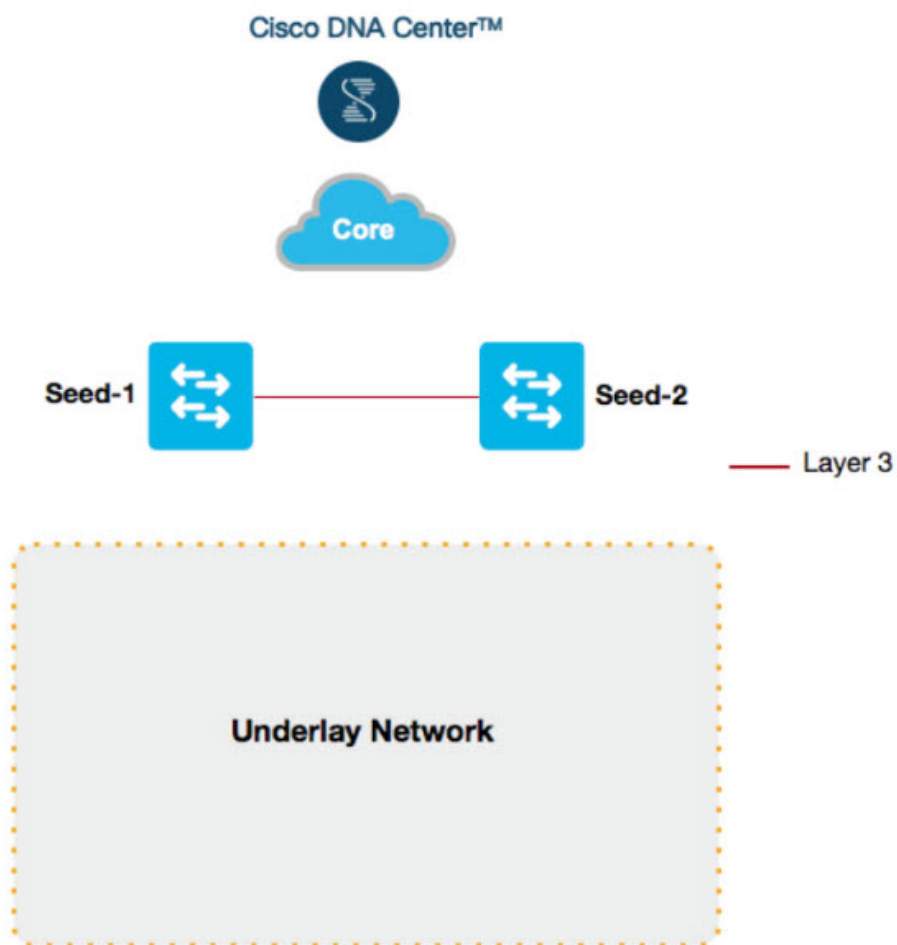
システム ロール

シードデバイス

シードデバイスは、ネットワークに事前に導入されたシステムであり、シスコのLAN 自動化でダウンストリームの新しいスイッチを検出してオンボードする最初のポイントとなります。シードデバイスは、シスコのプラグアンドプレイ (PnP) やゼロタッチプロビジョニングなどのテクノロジーで自動化することも、手動で設定することもできます。次の図は、IP コアの Cisco DNA Center の接続とLAN 自動化を使用して検出するアンダーレイネットワークの間のシードデバイスのネットワーク境界を示しています。

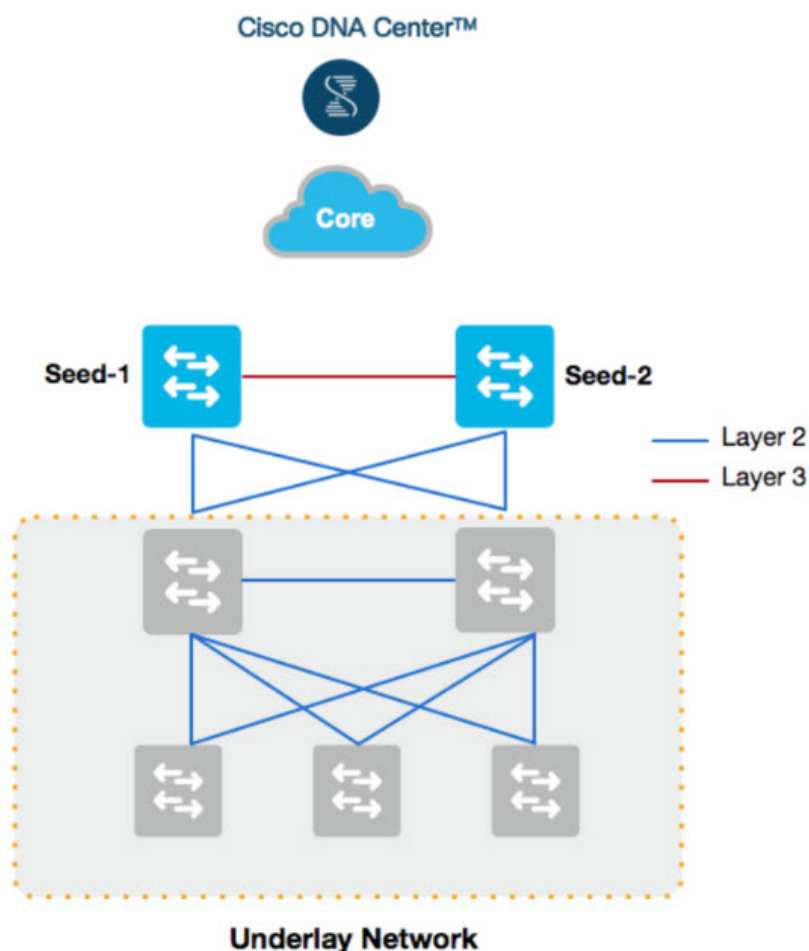
ピアシード（次の図の Seed-2）も LAN 自動化で自動化できます。必須となるシードデバイスは1つだけです。

デバイスの検出は、プライマリ シードデバイス インターフェイスでのみ行われます。



PnP エージェント

PnP エージェントは、工場出荷時の設定の Cisco Catalyst スイッチです。組み込みの Day-0 メカニズムにより、Cisco DNA Center と通信し、統合された PnP サーバの機能をサポートします。Cisco DNA Center によって、完全な Day-0 自動化を可能にする PnP プロファイルと設定のセットが動的に構築されます。次の図に、シードデバイスへの PnP エージェントの物理接続を示します。



自動化の境界

一般に、エンタープライズネットワークにおいては、構造化された階層型のネットワーク設計を構築し、すべてのネットワーク層で拡張性と冗長性を提供することを推奨します。3層アーキテクチャは大規模なエンタープライズキャンパスネットワークで実証されていますが、ネットワーク設計はネットワーク全体のサイズや物理的な接続などによって異なります。初期計画の一環として、ネットワーク管理者はシスコの LAN 自動化で自動化する物理トポロジを決定する必要があります。

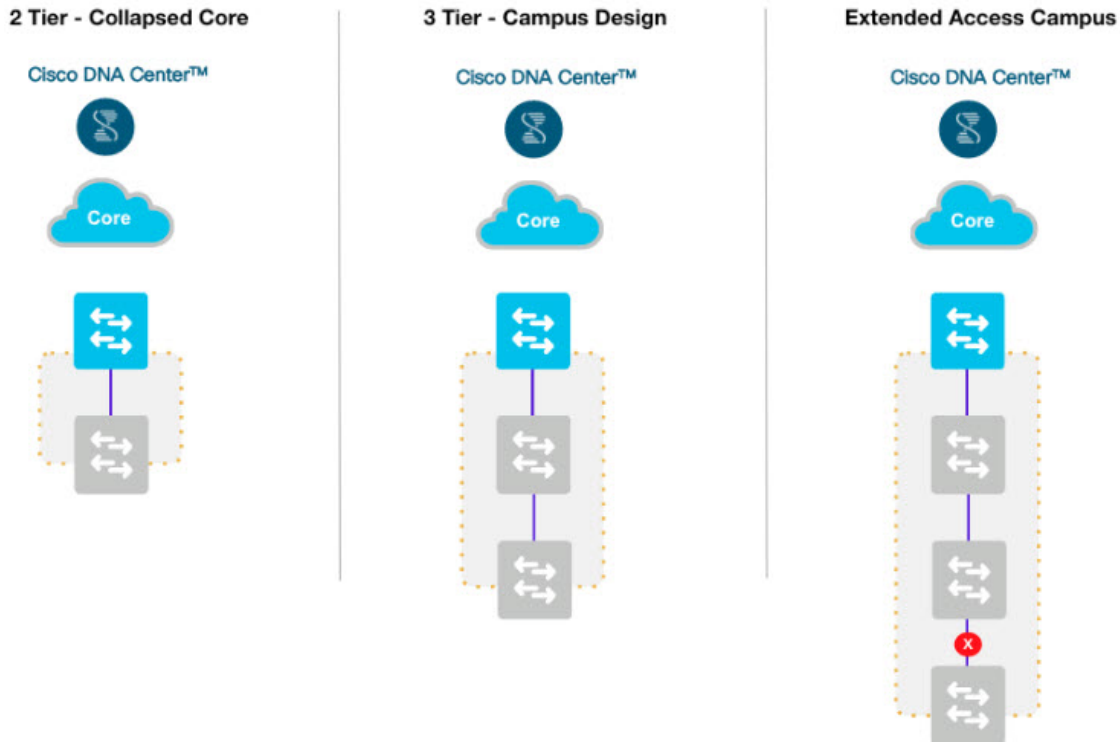
Cisco DNA Center の LAN 自動化では、初期の自動化の境界点にあるデバイスから最大 2 ホップまでサポートします。つまり、アンダーレイネットワークをアクセスレイヤまで構築するには、ネットワーク管理者はコアレイヤまたはディストリビューションレイヤから自動化の境界を開始する必要があります。2ホップを超える追加のネットワークデバイスも検出されることはありますが、自動化することはできません。

LAN 自動化は、直接接続されたネイバーでのみ開始されます。2つのシナリオについて考えてみます。

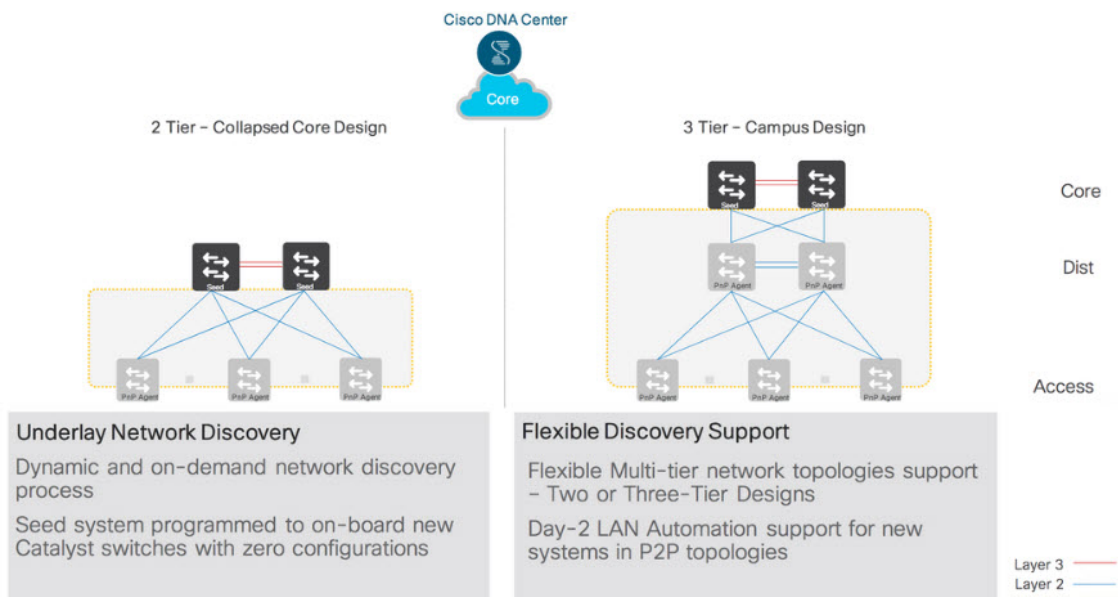
- シナリオ 1 : 3 層ネットワークで、ディストリビューションレイヤとアクセスレイヤのスイッチを LAN 自動化で自動化するとします。ディストリビューションレイヤのスイッチ（シードに直接接続されたスイッチ）は LAN 自動化に参加するため、ディストリビューションレイヤとアクセスレイヤの両方のスイッチが検出されて LAN 自動化で自動化されます。

- シナリオ 2：3 層ネットワークで、ディストリビューションレイヤとアクセスレイヤのスイッチを LAN 自動化で自動化するとします。ディストリビューションレイヤはすでに LAN 自動化で自動化されています。その後、アクセスレイヤのスイッチをネットワークに追加し、それらのスイッチを LAN 自動化で自動化します。ディストリビューションスイッチはすでに LAN 自動化で自動化されてリンクがレイヤ 3 に変換されているため、階層 1 のスイッチをシードとして使用することはできません。このシナリオでは、シードとしてディストリビューションを選択する必要があります。

次の図は、シスコの LAN 自動化でサポートされる自動化の境界を示しています。



次の図は、2 層および 3 層のネットワーク設計を示しています。

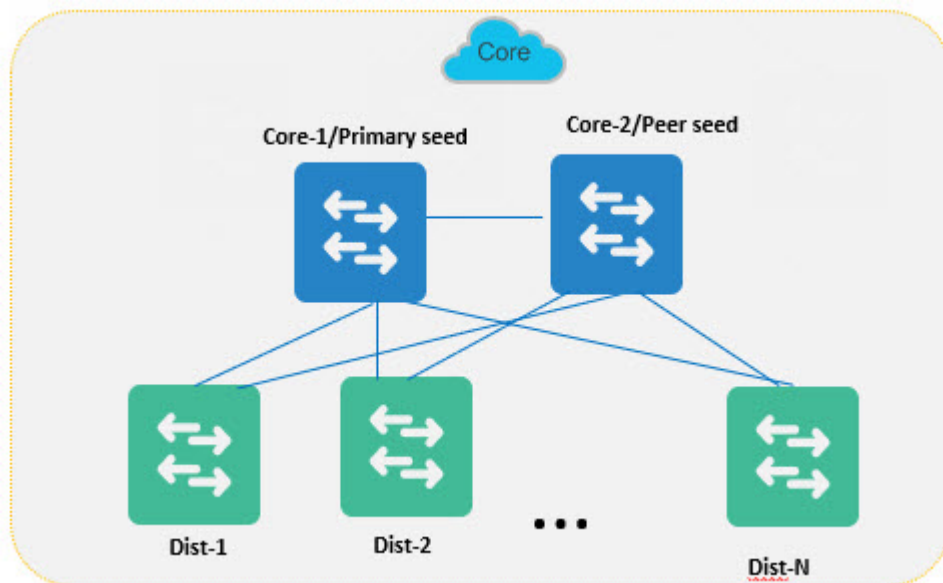


大規模なトポロジの段階的な LAN 自動化：最初のパス

大規模なトポロジを構築する際は、LAN 自動化を複数回実行します。最初のパスでは、コアデバイスをシードデバイスとして選択してディストリビューションスイッチを起動します。ディストリビューションスイッチが新しいデバイスとして起動します。



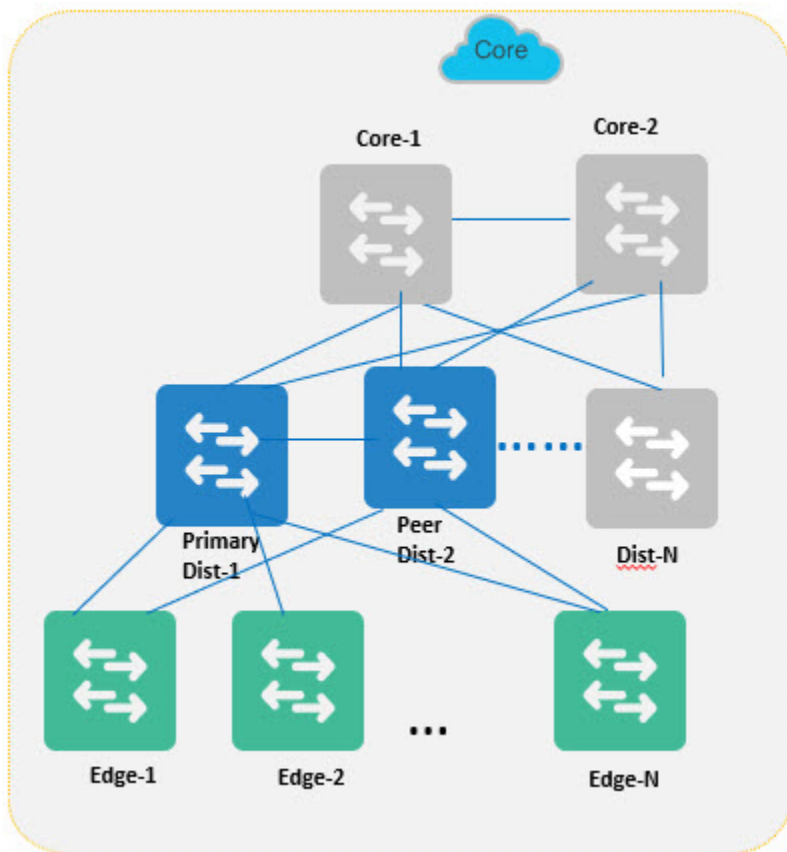
(注) N は一度に 50 デバイス以下とします。グループ内のすべてのスイッチを同時に起動することも順番に起動することもできます。



大規模なトポロジの段階的な LAN 自動化：最初のグループからの 2 回目のパス

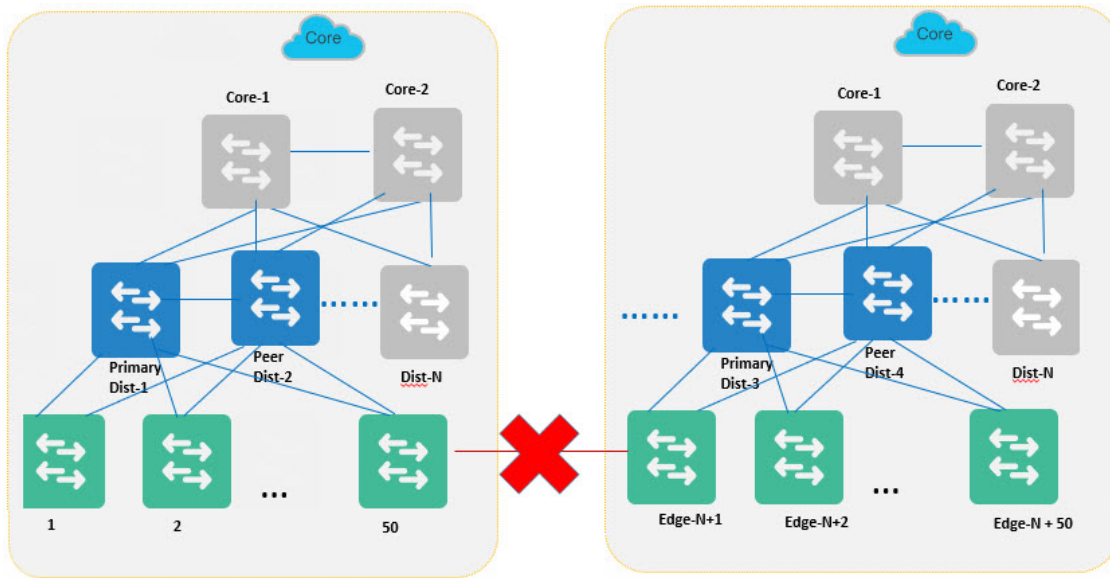
2 回目のパスでは、2 つのディストリビューションスイッチをシードデバイスとして選択して、エッジデバイスを新しいデバイスとして起動します。このセッションで起動する新しいデバイスについては、シードデバイスとして機能する 2 つのディストリビューションスイッチにすべて直接接続する必要があります。残りのディストリビューションスイッチについて、2 つずつのセットにしてこのプロセスを繰り返します。

1. ディストリビューションのセットごとに 2 回目のパスを繰り返して、アクセス/エッジスイッチを起動します (N は一度に 50 デバイス以下とします)。
2. エッジからはプライマリおよびピアのディストリビューションスイッチにのみアップリンクを接続します。
3. LAN 自動化セッションの実行時は IOT/拡張デバイスの電源を切ります。
4. ディストリビューションスイッチは他のディストリビューションスイッチに接続できます。
5. シードの下に 2 層までデバイスを配置できます。
6. 新しいデバイスは常にプライマリシードデバイスに接続します。ピアシードデバイスへの接続は任意です。



大規模なトポロジの段階的な LAN 自動化：2 つ目のグループからの 2 回目のパス

いずれかのグループに属するエッジデバイスを別のグループのエッジデバイスに接続することはできません。LAN 自動化セッションで新しく検出された PnP デバイスは、既存の非シードインベントリデバイスには接続できません。



リンク設定

- すべてのデバイスが Cisco DNA Center のインベントリに追加されたら、GUI で LAN 自動化セッションを「停止」することによって、レイヤ 3 リンクの設定プロセスを開始します。
- すべての PnP デバイスが Cisco DNA Center のインベントリに追加される前に誤って LAN 自動化を停止した場合、処理中のデバイスについてはリンクが設定されません。インベントリから処理中のデバイスを削除してから、新しい LAN 自動化セッションを開始し、処理中のデバイスを工場出荷時の状態に戻してリロードすることで、デバイスを再検出してリンクを設定する必要があります。
- このプロセスで、レイヤ 2 リンクのレイヤ 3 リンクへの変換が開始されます。これは、新しいデバイスのオンボーディング時に構築されたネットワークグラフをトラバースすることによって行われます。最初に、下位のデバイスリンクがレイヤ 3 IP アドレスに変換されます。次に、上位のデバイスリンクがレイヤ 3 IP アドレスに変換されます。ルータの IS-IS の設定も、このステップの間に接続リンクで行われます。このフェーズでは、上位層のリンクが設定されるまで、下位層のデバイスへの接続が一時的に失われる可能性があります。また、このフェーズでレイヤ 2 リンクがレイヤ 3 に変換されたときに、STP トポロジが変更されることがあります。
- このプロセスのアルゴリズムでは、最初に第 3 層のデバイス、次に第 2 層のデバイス、最後に第 1 層のデバイスの順に処理されます。
- 現在のセッションに参加しているデバイス間のリンクのみがレイヤ 3 リンクに変換されることに注意してください。新しく検出された PnP デバイスと既存の非シードインベントリデバイスの間のリンクはレイヤ 3 に変換されません。
- LAN 自動化デバイスがインベントリから削除される場合は、次のシナリオを検討してください。
 - シナリオ 1 : エッジデバイスがシングルホーム (1 つの中間ノードのみに接続) であり、中間ノードがインベントリから削除された場合、/31 ポイントツーポイントリンク IP アドレスは Cisco DNA Center (IPAM) から削除されますが、まだインベントリ内にあるため、エッジデバイスから構成を解除することはできません。これは、中間ノードとファブリックボーダー間のポイントツーポイント インターフェイスがエッジデバイス上のインターフェイスよりも前に設定されていないため、Cisco DNA Center からエッジデバイスに到達できない

くなる可能性があるためです。この場合、エッジデバイスの CLI にログインし、削除されたデバイスに接続されているインターフェイスをデフォルト設定に設定します。これにより、解放された IP アドレスがデバイス上にまだ存在するため、後の LAN 自動化ワークフロー中に IP アドレスが重複して割り当てられることが回避されます。後で、IP アドレスを手動で構成する代わりに、LAN 自動化ワークフローを使用して、エッジデバイスから新しい中間ノードまたは境界ノードへの新しいリンクを（必要に応じて）追加できます。

- シナリオ 2 : エッジデバイスがデュアルホーム（2つの中間ノードに接続）で、中間ノードの1つがインベントリから削除された場合、/31 ポイントツーポイントリンク IP アドレスが Cisco DNA Center (IPAM) から削除され、エッジデバイスからも設定解除されます。エッジデバイスで必要な手動設定はありません。

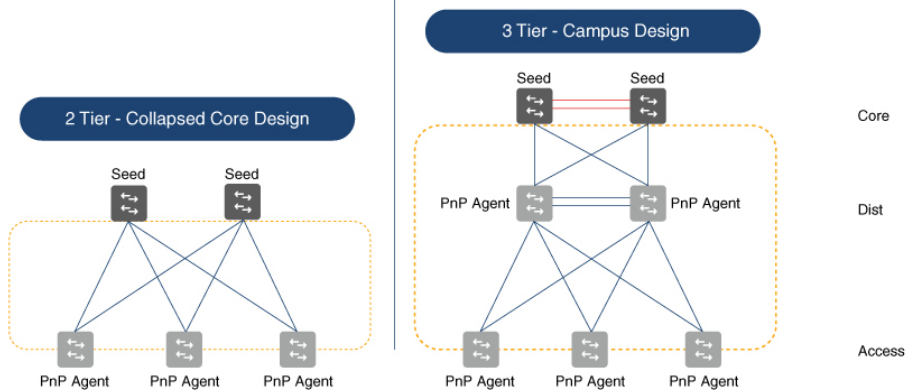
Cisco DNA Center 2.3.5 以降では、デインリンク設定（リンクの追加と削除）がサポートされています。詳細については、[インターフェイス間のリンクの作成（61 ページ）](#) を参照してください。

制約

- LAN 自動化では、PnP を介した StackWise Virtual (SV) スイッチのオンボーディングは自動化されません。StackWise Virtual スイッチは、シードデバイスとしてのみ使用できます。
- LAN 自動化では、スタック番号の再割り当てはサポートされていません。
- プラットフォームのサポートについては、リリースマトリックスを参照してください。

各種レイヤの各ロールでサポートされるスイッチ

次の図は、各種レイヤのシードおよび PnP エージェントでサポートされるデバイスファミリーを示しています。



Layer	Role	Supported Switch
Distribution	Distribution	Catalyst 3850, 6800, 9200, 9400, 9500, 9600
Access	PnP Agent	Catalyst 3650, 3850, 4500E, 9200, 9300, 9400, 9500, 9600

Layer	Role	Supported Switch
Core	Seed	Catalyst 3850, 4500E, 6800, 9200, 9300, 9400, 9500, 9600
Distribution	PnP Agent	Catalyst 3650, 3850, 4500E, 9000, 9200, 9300, 9500, 9600
Access	PnP Agent	Catalyst 3650, 3850, 4500E, 9200, 9300, 9400, 9500, 9600

431592

シスコ LAN 自動化製品サポートマトリックス

ロール ¹	製品モデル ²	ネットワークモジュール ³	Cisco IOS のバージョン	Cisco DNA Center のバージョン
シード PnP エージェント	C9600	シード：すべてのアップリンクとモジュールポートがサポートされます。 PnP エージェント：100G インターフェイスはサポートされていません。	17.3.2a 以降	1.3 以降
シード PnP エージェント	C9500-32C C9500-32QC C9500-24Y4C C9500-48Y4C	—	16.11.x 以降	1.3 以降

ロール ¹	製品モデル ²	ネットワークモジュール ³	Cisco IOS のバージョン	Cisco DNA Center のバージョン
シード PnP エージェント	C9500-12Q C9500-24Q C9500-40X C9500-16X	前面パネルポートの ⁴	—	—
シード PnP エージェント	C9404R C9407R C9410R	Sup-1 ⁵ Sup-1XL ³ Sup-1XL-Y ³ 任意のラインカード	—	—
シード PnP エージェント	C9300-24S C9300-24T C9300-24P C9300-24U C9300-48S C9300-48T C9300-48P C9300-48U C9300-24UX C9300-48UXM C9300-48UN	任意のアップリンクおよびモジュールポート	—	—
シード PnP エージェント	C9200L-24T C9200L-24P C9200L-48T C9200L-48P	任意のアップリンクおよびモジュールポート	—	1.2.8 以降
シード	C6807-XL	Sup6T 任意のアップリンクおよびモジュールポート	—	—
シード	C6880-X C6880-X-LE	任意のアップリンクおよびモジュールポート	—	—

ロール ¹	製品モデル ²	ネットワークモジュール ³	Cisco IOS のバージョン	Cisco DNA Center のバージョン
シード	C6816-X-LE C6832-X-LE C6824-X-LE-40G C6840-X-LE-40G	前面パネルの任意のポート	—	—
シード PnP エージェント	WS-C4503-E WS-C4506-E WS-C4507R+E WS-4510R+E	Sup9-E ³ Sup8-E 任意のアップリンクおよびモジュールポート	—	—
シード PnP エージェント	WS-C3850-24T WS-C3850-48T WS-C3850-24P WS-C3850-48P WS-C3850-48F WS-C3850-24U WS-C3850-48U WS-C3850-24XU WS-C3850-12X48U WS-C3850-12S WS-C3850-24S WS-C3850-12XS WS-C3850-24XS WS-C3850-48XS	任意のアップリンクおよびモジュールポート	—	—

ロール ¹	製品モデル ²	ネットワークモジュール ³	Cisco IOS のバージョン	Cisco DNA Center のバージョン
シード PnP エージェント	WS-C3650-24TS WS-C3650-48TS WS-C3650-24PS WS-C3650-48PS WS-C3650-48FS WS-C3650-24TD WS-C3650-48TD WS-C3650-24PD WS-C3650-24PDM WS-C3650-48PD WS-C3650-48FD WS-C3650-8X24PD WS-C3650-12X48FD WS-C3650-48TQ WS-C3650-48PQ WS-C3650-48FQ WS-C3650-48FQM WS-C3650-8X24UQ WS-C3650-12X48UQ WS-C3650-12X48UR WS-C3650-12X48UZ	任意のアップリンクおよびモジュールポート	—	—

¹ Cisco DNA Center 2.1.2 以降では、C9400、C9500、または C9600 の StackWise Virtual (SV) スイッチを LAN 自動化のシードとして設定できます。LAN 自動化では、PnP を介した StackWise Virtual スイッチのオンボーディングは自動化されません。StackWise Virtual スイッチは、シードデバイスとしてのみ使用できます。

² LAN 自動化は、ここにリストされている製品またはプラットフォームでのみサポートされます。

³ LAN 自動化では、専用の管理ポートはサポートされていません。C9500H および C9600 スイッチの場合、変換可能なポートはシードデバイスでのみ使用できます。スイッチが PnP デバイスとして使用されている場合、変換可能なポートは起動しません。

⁴ ブレークアウト ケーブル サポートは、シードデバイスでのみ使用できます。検出されたデバイスの場合、LAN 自動化はブレークアウトケーブルをサポートしません。これは、工場出荷時のデフォルトデバイスで PnP エージェントを停止する追加の設定が必要なためです。

⁵ 40G アップリンクは 16.11.1 以降でサポートされます。

設置場所の計画

Cisco DNA Center Design アプリケーションを使用して、必要なサイト、建物、およびフロアを作成します。新しいデバイスへのプライマリシードとピアシードの接続について、すべてのデバイスを同じサイトに含めるか階層にするかなどを検討します。また、さまざまなサイト、建物、フロアで IP プールを共有する方法についても検討してください。1つのオプションは、サイトごとに固有のプールを使用することです。別のオプションとして、階層内のすべてのサイトで共通の LAN プールを共有する方法もあります。デバイスを複数の LAN 自動化セッションでオンボーディングする場合は、階層内の各サイトに必要な IP プールが使用可能であることを確認してください。

次の制約事項に注意してください。

- リリース 1.1.x では、LAN 自動化の実行時、シード、ピアシード、および PnP デバイスに対して 1 つのサイトのみを選択できます。つまり、すべてのデバイスが 1 つのサイトに属している必要があります。
- デバイスのプロビジョニング後は、サイトを変更できません。そのため、デバイスをプロビジョニングする前に LAN 自動化を完了することを推奨します。

IP プールの計画

LAN 自動化用の IP プールを作成するには、まず Cisco DNA Center でグローバルプールを作成し、次にサイト固有の LAN IP プールを作成します。LAN 自動化での内部的な割り当ては次のようになります。

1. IP プールの一部が一時的な DHCP サーバ用に予約されます。このプールのサイズは、親 LAN プールのサイズによって異なります。たとえば、親プールが 192.168.10.0/24 の場合、DHCP サーバに割り当てられるサブプールのサイズは /26 になります。プールのサイズが /24 より大きい場合、DHCP プールのサイズはアルゴリズムに従って最大で /23 のサブプール (512 個の IP アドレス) まで増加します。したがって、/24 のプールであれば 64 個、/23 のプールであれば 128 個、/22 のプールであれば 256 個、それよりも大きければ 512 個の IP アドレスが DHCP サーバ用に予約されます。LAN 自動化を開始するための最小プールサイズは /25 で、DHCP プール用に予約されるサイズは /27 (32 個の IP アドレス) です。この IP プールの予約は一時的なもので、LAN 自動化検出セッションの間だけとなります。LAN 自動化検出セッションが完了すると、DHCP プールはリリースされ、IP が LAN プールに戻されます。通常は必要な IP の連続する最大のセグメントが DHCP プールに使用されるため、そのようなセグメントがプールに少なくとも 1 つ必要です。プールが断片化しすぎていると、DHCP プールを割り当てることができず、LAN 自動化セッションが IP プール割り当てエラーで終了します。
2. IP プールの別の部分は、/27 のサブプールサイズで内部的に予約されています。このサブプールは、Loopback0 および Loopback60000 に常に単一の IP を割り当てるためのものです。また、重複する別の IP プールが提供されていない場合、ポイントツーポイント L3 リンクの 2 つの連続する IP がこのサブプールから割り当てられます。この内部的に予約されたサブプールは、利用可能な IP がある限り、IP を提供するために LAN 自動化セッション全体で使用されます。IP が枯渇した場合は、新しい /27 サブプールが作成され、そのサブプールから IP が割り当てられます。これらのサブプールは、割り当てられたすべての IP が Cisco DNA Center で削除されるデバイスの一部として解放された場合にのみ解放されます。それ以外の場合、サブプールはプロセス全体で残り、削除できません。この内部サブプール割り当てロジックにより、IPAM での IP プールの使用では、デバイスに割り当てられた実際の IP ではなく、サブプールがカウントされます。
3. 共有またはリンク重複 IP プールがポイントツーポイント L3 リンクに提供されている場合、サイズ /27 のサブプールは、メイン IP プールではなく共有プールから内部的に予約されます。サブプールは、プールに割り当てられたすべての IP が解放されると自動的に削除されます。

専用（単一）IP プールを使用してアンダーレイネットワークを構築すると、LAN 自動化によって検出された各デバイスは、ポイントツーポイント接続用にインターフェイスごとに一意の /31 を取得し、Loopback0 およびアンダーレイマルチキャスト用に一意の /32 を取得します。

共有 IP プールは、マルチサイト展開で /31 IP アドレスの重複を許可することにより、200,000 を超えるエンドポイントを持つ大企業のアンダーレイネットワークでの IPv4 アドレス指定を最適化するために使用されます。異なるサイトのホストが /31 リンク上で重複した IP アドレスを取得する可能性があります。アンダーレイの /31 はファブリックサイトの外部にアドバタイズされないため、一意である必要はありません。ただし、/32 ループバックはすべてのデバイスに固有である必要があり、ネットワーク全体でデバイスを識別するためにグローバルルーティングテーブルにアドバタイズする必要があります。

LAN IP プールには、次の 2 つの有効なロールがあります。

- **[Link Overlapping IP Pool]**：このロールを持つプールは、LAN 自動化セッションではオプションです。指定した場合、IP アドレスはポイントツーポイント L3 リンクでのみ割り当てられます。このプールは、**[Shared IP Pool]** と呼ばれます。
- **[Main IP Pool]**：このロールを持つプールは、すべての LAN 自動化セッションに必須です。これは、ループバック、マルチキャスト、DHCP などの管理関連のすべての IP アドレッシングに使用されるプールです。**[Shared IP Pool]** が指定されていない場合、メイン IP プールが L3 リンク IP アドレッシングのデフォルトのフォールバックプールになります。

Discovered Device Site*	▼
Main IP Pool	▼ ⓘ
Link Overlapping IP Pool	▼ ⓘ
IS-IS Domain Password	ⓘ



(注) LAN 自動化セッションのシードデバイスが検出されたデバイスサイトとは異なるサイトにある場合、同じ共有 IP プールを同じシードおよび異なる検出されたデバイスサイトで使用することはできません。これは、同じシードデバイスへの重複 IP の割り当てを回避するためです。

IP プールの使用例

LAN 自動化で同じプールを使用して 10 台のデバイスを自動化し、各デバイスにプライマリシードへのリンクとセカンダリシードへのリンクを設定するとします。

プールは 192.168.199.0/24 とします。LAN 自動化が開始されると、/26 のプールが DHCP アドレス用に予約されます。この例では、192.168.199.1 ~ 192.168.199.63 が予約され、10 台のデバイスの VLAN 1 に割り当てられます。

次に、/27 プールがループバックアドレス用に予約されます。共有 IP プールがない場合、このプールはポイントツーポイントリンクにも使用されます。デバイスが 10 台でそれぞれに 2 つのリンクがあるため、合計で $2 \times 10 \times 4 = 80$ 個の IP アドレスがポイントツーポイントリンク用に予約され、10 個のループバックアドレスが予約されます。

合計では、10 個のデバイスに対して 100 個の IP アドレスが予約されます。各 VLAN 1 に 10 個、各ループバックに 10 個、デバイスとシードの間のポイントツーポイントリンクに 80 個です。

LAN 自動化を停止すると、VLAN 1 の IP アドレスはリリースされてプールに戻り、LAN 自動化セッションに割り当てられたアドレスは 90 個になります。

次の点に注意してください。

- 同じ IP プールを複数の検出セッションに使用できます。たとえば、検出セッションを 1 回実行して最初のデバイスのセットを検出します。検出の完了後、後続の LAN 自動化セッションに同じ IP プールを指定できます。同様に、1 つの検出セッションに 1 つの LAN プールを選択し、次の検出セッションに別の LAN プールを選択することもできます。
- LAN 自動化を開始するたびに、IP プールに使用可能な IP アドレスが 64 個あるかどうかチェックされます。同じプールで LAN 自動化を複数回実行する場合は、少なくとも /24 のプールを使用します。IP プールに対して LAN 自動化を 1 回だけ行う場合は、/25 のプールで十分です。
- デバイスに設定されているループバックや他のアドレスに属するアドレスプールなど、ネットワーク内の他の場所で使用されているアドレスプールは使用しないでください。

サイト固有の CLI と SNMP の設定

LAN 自動化を開始するには、CLI と SNMPv2 読み取り/書き込みまたは SNMPv3 の設定をサイトごとに設定する必要があります。Cisco DNA Center Design アプリケーションを使用してサイト固有の CLI および SNMP を設定し、LAN 自動化に使用するサイトの設定を保存します。クレデンシヤルは、グローバルレベルで設定すればサイトレベルで表示されます。特定のサイトのオプションボタンをクリックし、設定を保存して LAN 自動化に使用できるようにする必要があります。

シードデバイスの設定

シードデバイスを設定するときは、次の注意事項に従ってください。

- システムの最大伝送ユニット (MTU) の値は 9100 以上である必要があります。
- シードデバイスでは IP ルーティングをオンにします。
- Cisco DNA Center から LAN IP プールサブネットに IP で到達できるようにシードサービスと Cisco DNA Center の間のルーティングを設定します。
- PnP エージェントに接続されているデフォルトのインターフェイスを使用することをお勧めします。ピアシードデバイスの IP インターフェイスが PnP エージェントに接続されたインターフェイスに設定されている場合、それらのリンクは設定されません。PnP エージェントに接続されたピアデバイスのインターフェイスを設定する場合は、デフォルトのインターフェイスを使用し、ピアシードデバイスでインベントリ同期を実行します。LAN 自動化は、

ポートがレイヤ 2 の場合にのみ機能します。Cisco Catalyst 6000 のポートはデフォルトでレイヤ 3 です。LAN 自動化を開始する前に、ポートをレイヤ 2 に変換します。

- シードデバイスではデバイスクレデンシャルと SNMP クレデンシャルを設定します。
- シードデバイスでレイヤ 3 インターフェイスが設定されている場合は、Cisco DNA Center で提供されるいずれの IP プールとも競合しないことを確認します。手動で設定されている IP アドレスを確認します。
- VLAN 1 で実行されている別の DHCP サーバに接続された他のインターフェイスがシードデバイスにないことを確認します。
- シードデバイスにループバックが設定されていない場合、LAN 自動化でシードにループバックが設定されます。
- LAN 自動化を実行する前にシードデバイスで設定の変更が行われた場合は、シードデバイスを Cisco DNA Center のインベントリと同期します。
- シードデバイスはサイトに割り当てます（シードデバイスを LAN 自動化用にプロビジョニングする必要はありません）。

シードデバイスの設定に関するその他の推奨事項を次に示します。

- **同じシードに接続されたサイトのデバイスについての複数の検出セッションの実行**：複数の検出セッションを実行して同じシードデバイスに接続された異なる建物やフロアのデバイスをオンボーディングする場合、次の検出セッションに参加しない PnP エージェントのポートをブロックすることを推奨します。

たとえば、シードデバイスが建物 23 にあり、フロア 1 とフロア 2 の PnP エージェントに接続されているとします。フロア 1 のデバイスは、Gig 1/0/10 ~ Gig 1/0/15 のインターフェイスで接続されています。フロア 2 のデバイスは、Gig 1/0/16 ~ Gig 1/0/20 のインターフェイスで接続されています。フロア 1 の検出セッションでは、Gig 1/0/16 ~ Gig 1/0/20 に接続されているポートをシャットダウンすることを推奨します。そうしないと、フロア 2 に接続されている PnP エージェントも、プライマリシードデバイスで実行されているサーバから DHCP IP を取得する可能性があります。これらのインターフェイスは検出セッションで選択されないため、PnP データベースに古いエントリとして残ります。フロア 2 の検出セッションを実行しても、それらのデバイスを PnP アプリケーションから削除して書き込み消去/リロードしないと検出は正しく機能しません。したがって、他の検出インターフェイスをシャットダウンすることを推奨します。

- **エンドポイント/クライアントの統合**：Cisco DNA Center 1.2.8以前では、検出するスイッチにクライアントが接続されていると、それらのクライアントの DHCP IP の競合によってプールが枯渇し、LAN 自動化が失敗することがあります。そのため、クライアントは LAN 自動化の完了後に接続することをお勧めします。

エンドポイント/クライアントの統合に関するこの制限は、Cisco DNA Center 1.2.10 以降には該当しません。クライアントがスイッチに接続した状態で LAN 自動化を実行できます。

PnP エージェントの初期状態

LAN 自動化で自動化するデバイスのライセンスレベルが Advantage であることを確認します。そうでない場合、一部のコマンドがプッシュされません。



- (注) Cisco DNA Center 2.3.5 以降では、C9000 および C3850 シリーズ スイッチの自動ライセンスアップグレードがサポートされています。

新しい PnP エージェントは、工場出荷時のデフォルトで LAN 自動化を開始する準備ができています。

既存のネットワークデバイスを再利用する場合は、次の点を確認してください。

- PnP エージェントには、LISP、IS-IS ルーティング、および CTS 関連の CLI をプッシュできるライセンスが必要です。現在のライセンスレベルは **show license** コマンドを使用して確認できます。必要に応じて、ライセンスをアップグレードします。
- PnP エージェントはクリーンな状態である必要があります。以前に実行したときの古い証明書やキーなどが残ってはいけません。
- スイッチコンソールから次の項目をクリアして、デバイスを工場出荷時のデフォルトに戻します。

```
[CLI config mode]

no pnp profile pnp-zero-touch
no crypto pki certificate pool
Also remove any other crypto certs shown by "show run | inc crypto"
crypto key zeroize
config-register 0x2102 or 0x0102 (if not already)
do write
end

[CLI exec mode]

delete /force nvram:*.cer
delete /force stby-nvram:*.cer (if a stack)
delete /force flash:pnp-reset-config.cfg
write erase
reload (enter no if asked to save)
```

Cisco IOS XE 16.12.x 以降の場合は、次を使用します。

```
[CLI exec mode]

pnp service reset no-prompt
```

ステップ 2: 設計

LAN 自動化の 2 番目のステップは設計です。設計フェーズでは、次のことを行います。

1. グローバルサイトを設計して構築します。
2. グローバルとローカルのネットワークサービスを設定します。
3. グローバル デバイス クレデンシャルを設定します。
4. グローバル IP アドレスプールを設計し、必要なサイトの LAN 自動化プールをグローバルプールから割り当てます。

サイトの設計と構築

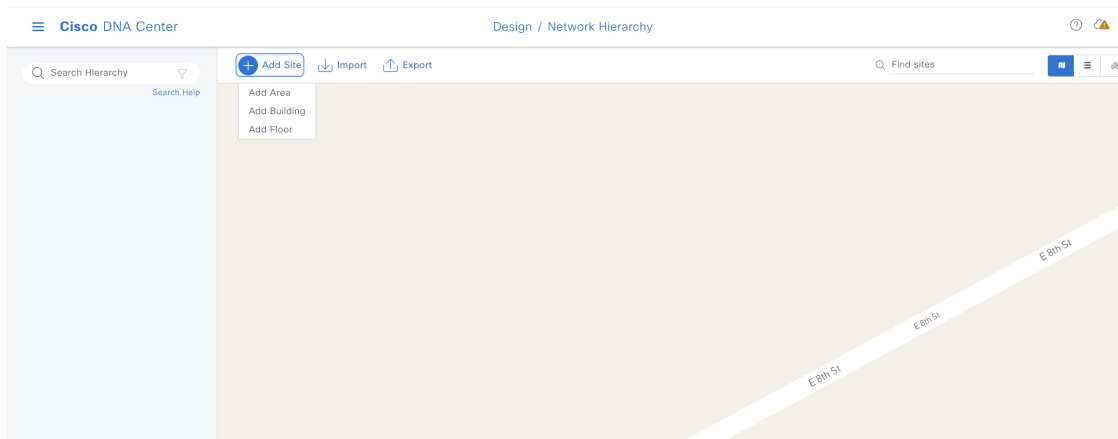
このセクションでは、サイトを設計して構築する方法について説明します。

手順

ステップ 1 Cisco DNA Center のホームページで、メニューアイコン（☰）をクリックして、**[Design] > [Network Hierarchy]** の順に選択します。

ステップ 2 サイトを作成し、ビルディングとフロアを追加します。

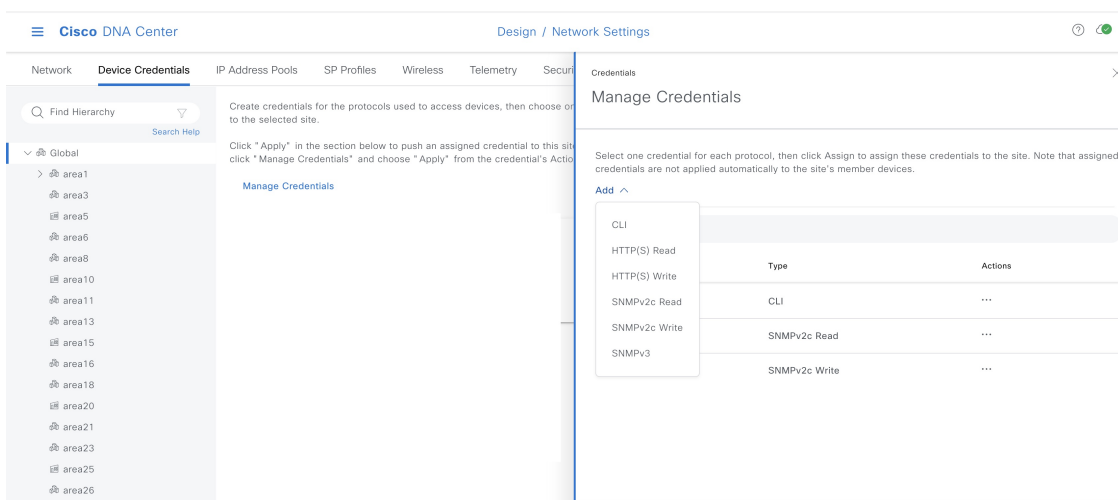
- サイトを作成するには、**[+Add Site] > [Add Area]** を選択します。
- ビルディングを追加するには、**[+Add Site] > [Add Building]** を選択します。
- フロアを追加するには、**[+Add Site] > [Add Floor]** を選択します。



ステップ 3 メニューアイコン（☰）をクリックして、**[Design] > [Network Settings] > [Device Credentials]** の順に選択します。

ステップ 4 **[Manage Credentials]** をクリックし、次のログイン情報を追加します。

- **CLI**
- **SNMPv2c 読み取り**



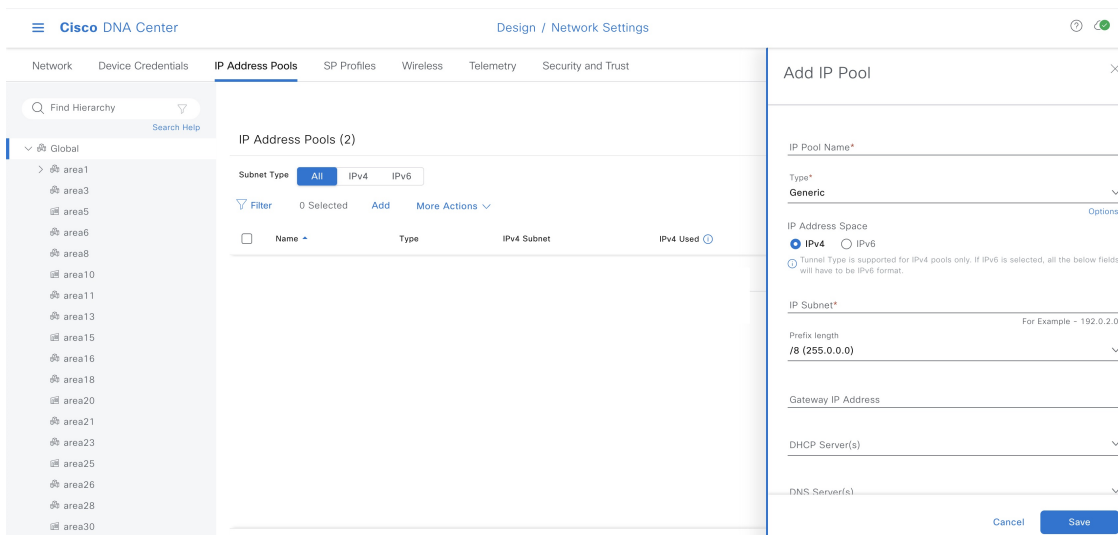
(注) すべてのサイトに同じデバイスクレデンシャルを使用する場合は、左側のナビゲーションツリーで [Global] をクリックし、クレデンシャルを設定します。

cisco というユーザ名は使用しないでください。

ステップ 5 メニューアイコン (☰) をクリックして、[Design] > [Network Settings] > [IP Address Pools] の順に選択します。

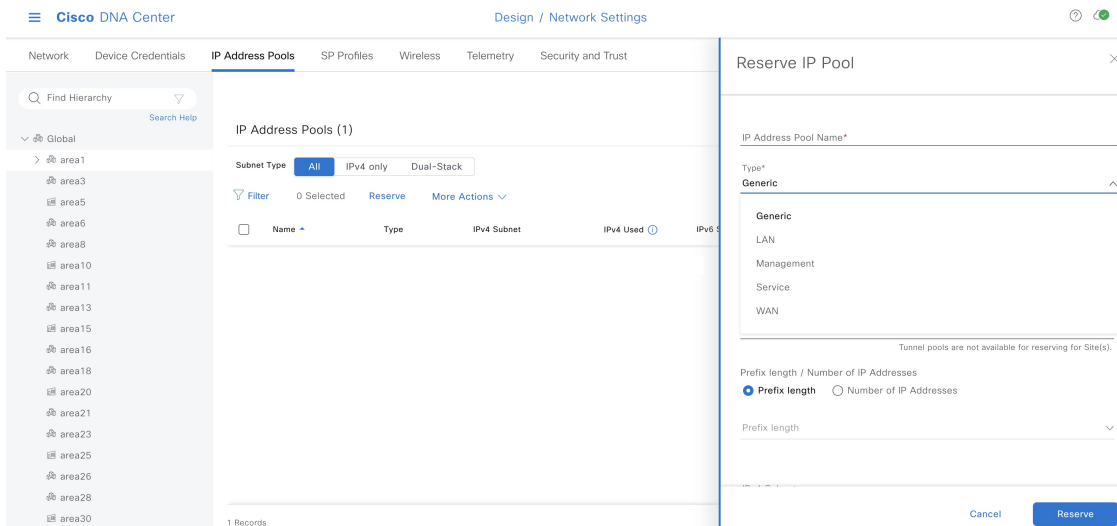
ステップ 6 左側の階層ツリーから、[Global] および [Add] をクリックします。

アンダーレイインフラストラクチャに使用する専用の IP アドレスプールを作成します。ネットワークすでに使用されているアドレスプールは使用しないでください。たとえば、デバイスに設定されているループバックや他のアドレスに属するアドレスプールは使用しないでください。



ステップ 7 左側の階層ツリーから、サイトを選択し、[Reserve] をクリックします。

ステップ 8 [Reserve IP Pool] ウィンドウで、[Type] ドロップダウンリストから [LAN] を選択します。



ステップ3：検出

アンダーレイネットワークを構築するための3番目のステップはデバイスの検出です。

検出プロファイルを作成して実行する前に、シードデバイスのアンダーレイ設定を確認します。

検出プロファイルの作成

このセクションでは、検出プロファイルを作成する方法について説明します。

手順

ステップ1 Cisco DNA Center ホームページから、メニューアイコン（☰）をクリックして、[Tools] > [Discovery] の順に選択します。

ステップ2 [Discovery] ウィンドウで、[Add Discovery] をクリックします。

ステップ3 [New Discovery] ウィンドウで、次の詳細を入力します。

- [Discovery Name]：検出プロファイルの名前。
- [IP Address/Range]：Cisco DNA Center からアクセス可能な任意のスイッチの任意のレイヤ3 インターフェイスまたはループバックをIPアドレスとして指定できます。プライマリシードとピアシードと一緒に検出する場合は、IP 範囲を入力します。該当するオプションボタンをクリックし、それに応じて詳細を入力します。
- [Credentials]：少なくとも1つのCLIと1つのSNMPのクレデンシャルを有効にします。クレデンシャルを追加するには [Add Credentials] をクリックします。

- **[Advanced]** : 検出スキャンで使用する1つまたは複数のプロトコルを指定します。[SSH] または [Telnet] を選択します。

(注) SSH を選択する場合は、シードが SSH 用に設定されていることを確認してください。

The screenshot shows the 'New Discovery' configuration interface in Cisco DNA Center. The 'Discovery Type' is set to 'CDP'. The 'IP Address' field is empty. The 'CDP Level' is set to '16'. The 'Preferred Management IP Address' is set to 'None'. There are 'Reset' and 'Discover' buttons at the bottom right.

ステップ 4 [Discover] をクリックします。

ステップ 5 検出スケジュールを選択し、[Start] をクリックします。

[Discoveries] ウィンドウでスキャンのステータスと結果を表示できます。

(注) 検出プロセスには少し時間がかかります。プロセスの完了後に障害が発生していないことを確認してください。

The screenshot shows the 'View All Discoveries' page. A summary card for the discovery 'discovered-via-SC...' shows it is 'Completed' with '2 Reachable Device(s)'. The 'Discovery Details' table is as follows:

CDP Level	None	LLDP Level	None
Protocol Order	ssh telnet	Retry Count	None
Timeout	30 second(s)	IP Address/Range	
IP Filter List	None	Preferred Management IP Address	None
New Device Only Configured	No	Recurring	No

The table of discovered devices is as follows:

IP Address	Device Name	Status	ICMP	SNMP	CLI	NETCONF
	Border-01	Success	Success	Success	Success	Success
	Border-02	Success	Success	Success	Success	Success

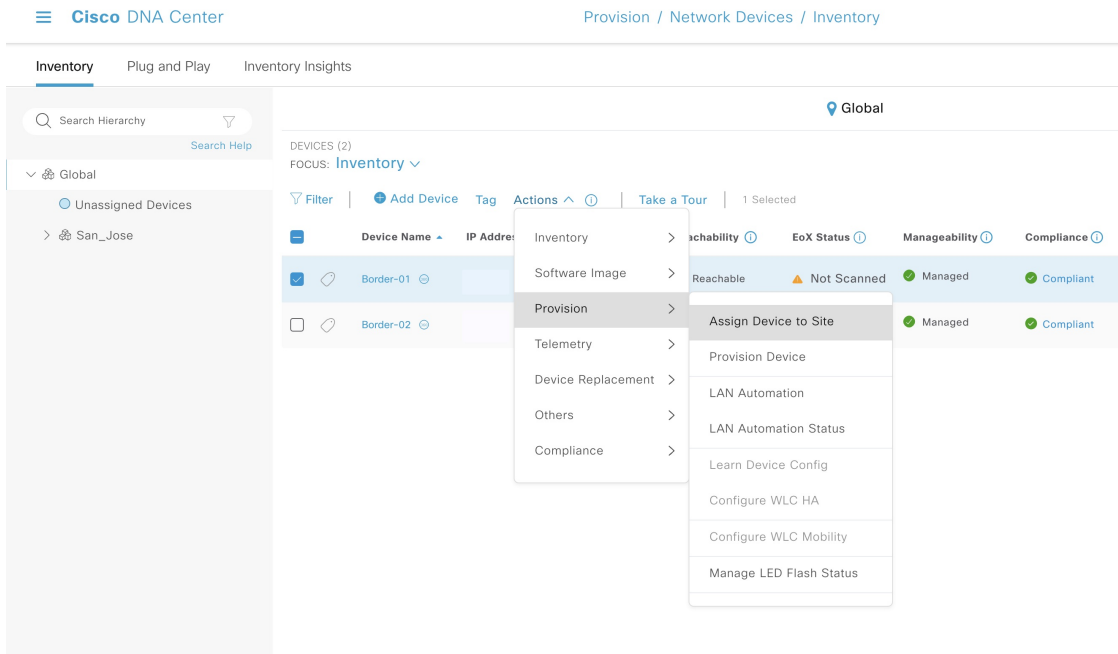
ステップ6 検出されたデバイスがインベントリに追加されたことを確認するには、メニューアイコン（☰）をクリックして、**[Provision] > [Inventory]** です。

(注) 検出されたデバイスの **[Reachability]** ステータスが **[Reachable]** であり、**[Manageability]** ステータスが **[Managed]** であることを確認します。

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes 'Cisco DNA Center' and 'Provision / Network Devices / Inventory'. Below this, there are tabs for 'Inventory', 'Plug and Play', and 'Inventory Insights'. A search bar is present with 'Search Hierarchy' and 'Search Help' options. The main content area displays a table of devices under the heading 'DEVICES (2)' and 'FOCUS: Inventory'. The table has columns for 'Device Name', 'IP Address', 'Device Family', 'Reachability', 'EoX Status', 'Manageability', and 'Compliance'. Two devices are listed: 'Border-01' and 'Border-02', both of which are 'Reachable', 'Not Scanned', 'Managed', and 'Compliant'.

	Device Name	IP Address	Device Family	Reachability	EoX Status	Manageability	Compliance
<input type="checkbox"/>	Border-01		Switches and Hubs (WLC Capable)	Reachable	Not Scanned	Managed	Compliant
<input type="checkbox"/>	Border-02		Switches and Hubs (WLC Capable)	Reachable	Not Scanned	Managed	Compliant


ステップ7 インベントリからデバイスをサイトに割り当てるには、デバイスを選択し、**[Actions]** メニューから、**[Provision] > [Assign Device to Site]** の順に選択します。

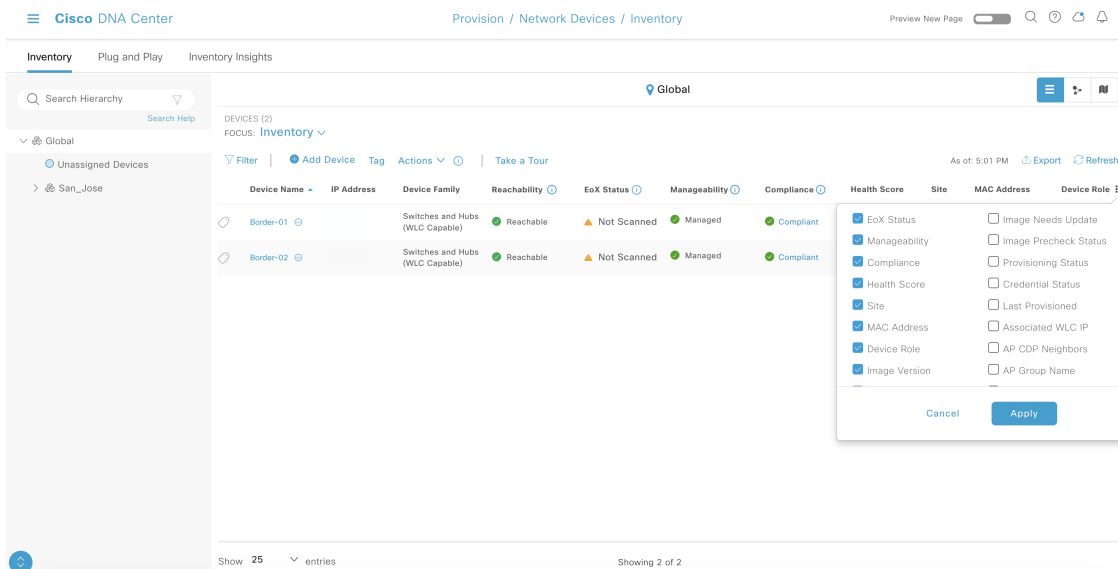


ステップ 8 [Assign Device to Site] ウィンドウで、サイトを選択し、[Apply] をクリックします。

Cisco DNA Center 1.2.6 以前の場合は、プライマリシードとピアシードの両方が同じサイトの同じフロアにあることを確認してください（物理的には異なるフロアにあってもかまいません）。

検出されたデバイスが選択したサイトに追加されます。

(注) [Inventory] ウィンドウの [Site] 列が表示されない場合は、 をクリックし、[Site] チェックボックスをオンにして [Apply] をクリックします。



LAN 自動化を開始する前の考慮事項

LAN 自動化プロセスを開始する前に、次の考慮事項について検討してください。

IP プールサブネットの到達可能性 Cisco DNA Center

LAN 自動化の検出では、LAN プールを使用して PnP エージェントに到達します。LAN プールから割り当てられる IP に Cisco DNA Center から到達できる必要があります。たとえば、LAN プールが 192.168.10.0 の場合、このサブネットに到達するための正しいルートが Cisco DNA Center に必要になります。到達可能性をテストするには、プライマリシードデバイス上に SVI (VLAN 1 インターフェイス) を作成し、Cisco DNA Center とシードの間で ping テストを実行します。次のサンプルコードを参照してください。

```
[On seed device]
Switch(config)#interface vlan1
Switch(config-if)#ip address 192.168.99.1 255.255.255.0
Switch(config-if)#end

[On Cisco DNA Center CLI console]
[Sat Jun 23 05:55:18 UTC] maglev@10.195.192.157
$ ping 192.168.99.1
PING 192.168.99.1 (192.168.99.1) 56(84) bytes of data.
64 bytes from 192.168.99.1: icmp_seq=1 ttl=252 time=0.579 ms
64 bytes from 192.168.99.1: icmp_seq=2 ttl=252 time=0.684 ms
64 bytes from 192.168.99.1: icmp_seq=3 ttl=252 time=0.541 ms

[On seed device]
Switch(config)#default int vlan 1
Interface Vlan1 set to default configuration
```

ping テストが失敗する場合、Cisco DNA Center でルートが正しく設定されていません。

LAN プールのスタティックルートの追加

Cisco DNA Center ハードウェアには複数の物理インターフェイスがあり、それぞれが異なるカテゴリの通信を提供します。推奨されるインターフェイス接続、IP ルーティング、およびスタティック割り当てについては、『[Cisco Digital Network Architecture Center Appliance Installation Guide](#)』を参照してください。シングルホーム設計では、Cisco DNA Center は IP ルーティングを提供するデフォルトゲートウェイでホスト機能を実行します。マルチホーム設計では、Cisco DNA Center にエンタープライズ側のインターフェイスを介した LAN 自動化ネットワークまでのスタティックルートが必要になります。

図 1: シングルホーム設計とマルチホーム設計の IP アドレッシング

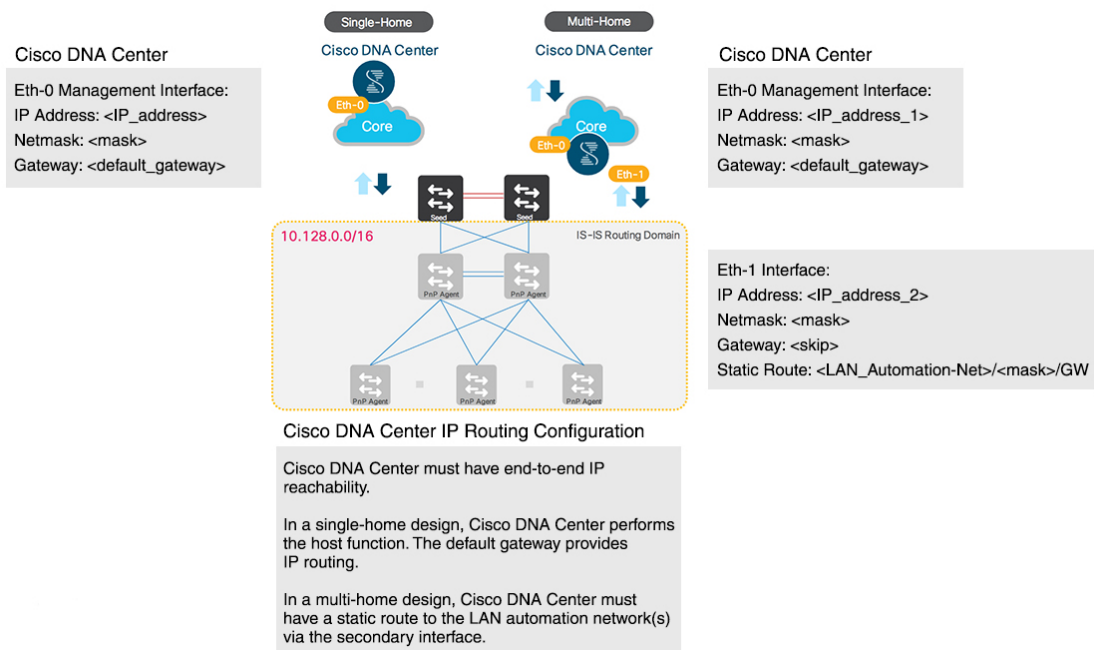
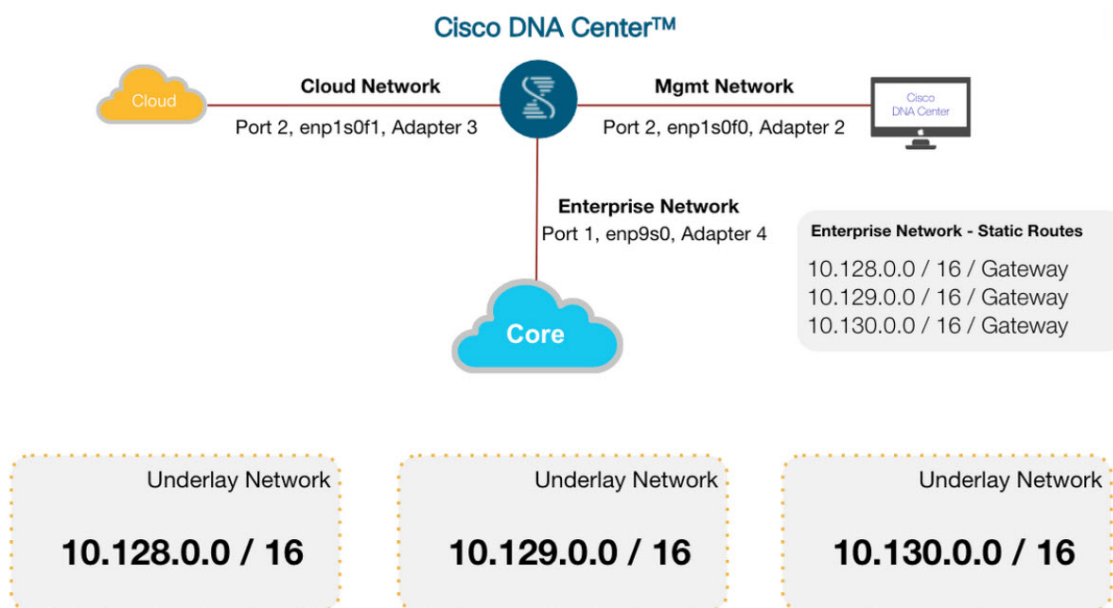


図 2: スタティック IP ルーティングの設計



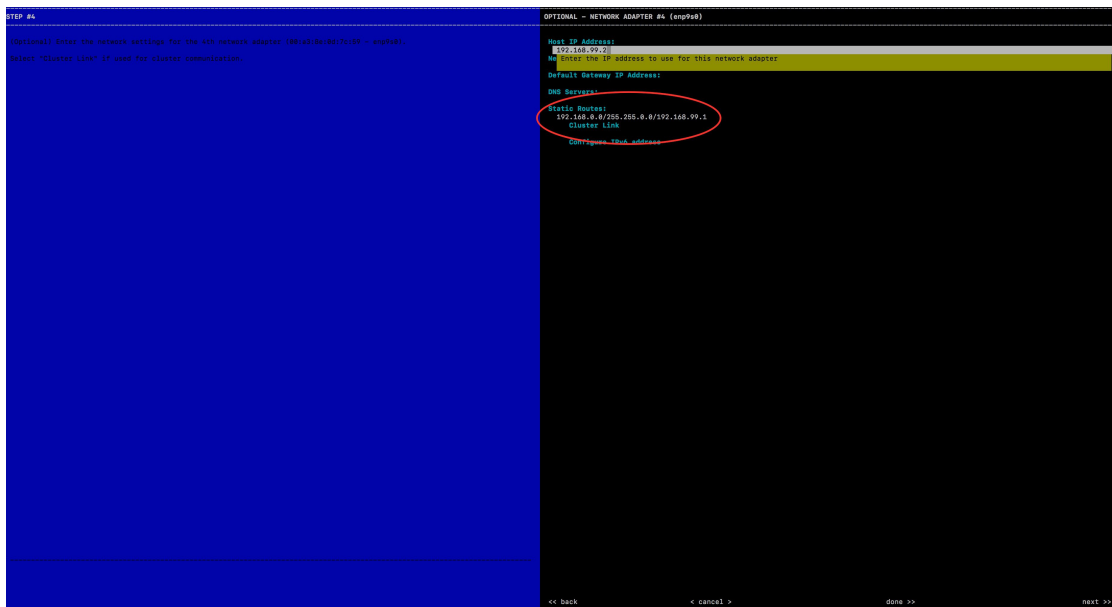
ネットワーク設計がマルチホーム設計の場合に IP 到達可能性の問題を解決する 1 つの方法として、Cisco DNA Center でスタティックルートを追加する方法があります。ネットワーク管理者は、Cisco DNA Center の初期設定時にスタティックルートを追加できるほか、後で `maglev` コマンドを使用して追加することもできます (Linux の `route` コマンドを使用してルートが変更された場合は `maglev` API で正しい情報が取得されないため、`route` コマンドは使用しないでください)。

シングルホーム設計の場合は、シードと Cisco DNA Center の間のルーティングを確認します。

Cisco DNA Center でスタティックルートを追加する手順は次のとおりです。

手順

ステップ1 Cisco DNA Center コンソールで、`sudo maglev-config update` コマンドを入力します。設定ウィザードが開きます。



ステップ2 スタティックルートを入力し、[Next] をクリックします。設定ウィザードでホストネットワーキングが検証されて設定されます。

ステップ3 スタティックルートを追加するための正しいインターフェイスが選択されていることを確認します。ルートを設定するためのインターフェイスが選択されていない場合は、正しいインターフェイスが表示されるまで [Next] をクリックします。

ステップ4 [Network Proxy] フィールドは空欄のままにします。プロキシの検証に失敗する場合は、プロキシ設定をスキップします。

ステップ5 [Proceed] をクリックして、コントローラに変更を適用します。
スタティックルートの追加には 5 ~ 6 分かかります。警告メッセージは無視してかまいません。

LAN 自動化を開始する前の PnP エージェントの初期状態

手順

ステップ1 LAN 自動化を開始する前に、PnP エージェントが **System Configuration Dialog** 状態であることを確認します。

```
FIPS: Flash Key Check : Key Not Found, FIPS Mode Not Enabled
cisco C9300-24T (X86) processor with 1418286K/6147K bytes of memory.
Processor board ID FCW2137G032
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
11264000K bytes of Flash at flash:.
0K bytes of WebUI ODM Files at webui:.
```

```
Base Ethernet MAC Address      : f8:7b:20:48:d8:80
Motherboard Assembly Number   : 73-17952-06
Motherboard Serial Number     : FOC21354B06
Model Revision Number         : A0
Motherboard Revision Number   : A0
Model Number                   : C9300-24T
System Serial Number          : FCW2137G032
```

```
%INIT: waited 0 seconds for NVRAM to be available
```

```
--- System Configuration Dialog ---
```

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

ステップ 2 Yes または **No** を入力せずに、デバイスを同じ状態のままにします。

(注) この最初のプロンプトでデバイスが停止せずに次に進む場合は、CLI コマンド `show ver | inc register` を使用してデバイスの `config-register` の値を確認します。場合によっては、値が `0x142` になっていることがあります。 `config-register` の値を `0x102` または `0x2102` に変更して設定を保存します。CLI を再度確認し、*Configuration register is 0x142 (will be 0x102 at next reload)* と表示されることを確認します。

値を `0x102` または `0x2102` に変更してデバイスをリロードした後も、デバイスが古い `config-register` の値で起動する場合は、デバイスで `no system ignore startupconfig switch all` を設定し、設定を保存してリロードします。

Cisco Catalyst 9000 シリーズ スイッチの場合は、`pnp service reset no-prompt` を使用します。

スタックに関する考慮事項

- スタックについても同じ手順に従います。スタック内のすべてのメンバーが起動したことを確認するための時間が余分にかかります。すべてのスイッチが起動するまで、LAN 自動化は開始しないでください。
- LAN 自動化は常にアクティブスイッチから開始されます。スタック内のすべてのスイッチを一緒に起動した場合、MAC アドレスが最小のスイッチがアクティブになります (スイッチプライオリティが設定されていない場合)。2 番目に小さいスイッチがスタンバイになります。お客様の要件によっては、常に最初のスイッチをアクティブにする必要がある場合もあります。この場合、すべてのスイッチを一緒に起動すると、最初のスイッチの MAC アドレスが最小でなければ、そのスイッチはアクティブになりません。必ず最初のスイッチをアクティブにするには、時間をずらして順番にスイッチを起動します。つまり、最初にスイッチ 1 を起動し、120 秒後にスイッチ 2 を起動します。これにより、スイッチが正しい順序でアクティブになり、スイッチ 1 がアクティブ、スイッチ 2 がスタンバイになります。ただし、リロードすると順序は維持されず、スイッチに MAC アドレスに応じてロールが割り当てられます。

- リロード後もスイッチの順序が維持されるようにするには、スイッチが常に同じ順序で起動するようにスイッチプライオリティを割り当てることを推奨します。最も高いプライオリティは15です。プライオリティが割り当てられている場合、スイッチのMACアドレスよりも優先されます。スイッチプライオリティを割り当てても、NVRAMの設定は変更されません。値はROMMONに書き込まれ、リロードや書き込み消去の後も保持されます。例として、次のサンプルコードを参照してください。

```
3850_edge_2#switch 1 priority ?
  <1-15> Switch Priority
3850_edge_2#switch 1 priority 14
WARNING: Changing the switch priority may result in a configuration change for that switch. Do
you want to continue?[y/n]? [yes]: y
```

一部の証明書はスイッチの起動時に設定されるため、プライオリティの割り当て後にスイッチのクリーンアップが必要になる場合があります。スイッチのクリーンアップについては、「[PNP エージェントの初期状態](#)」を参照してください。

(注) スタック内のすべてのスイッチが起動するまで、LAN 自動化は開始しないでください。

スタンバイ/メンバースイッチにコンソール接続している場合、画面に *console is now available, Press RETURN to get started* と表示されても、Enter キーを押さないでください。アクティブスイッチを監視し、**System Configuration Dialog** 状態になっていることを確認してください。

LAN 自動化がすでに実行されていて停止せずに続行する場合は、PnP エージェントに接続しているシードリンクを閉じます。このようにすると、リンクを起動する準備ができるまで検出は行われません。

管理ポートの取り外し

PnP エージェントはシードデバイスに直接接続します。PnP エージェントを他のネットワーク（管理ネットワークなど）や VLAN 1 上の別のサーバを介して DHCP を提供できるネットワークに接続しないでください。

シードポートがレイヤ 2 であることを確認

PnP エージェントに接続されるシードポートがレイヤ 2 であり、デフォルトとして設定されていることを確認します。たとえば、Cisco Catalyst 6500 および 9500H のポートはデフォルトではレイヤ 3 です。

プライマリシードのポートで STP がブロックされないことを確認

PnP エージェントに接続するプライマリシードのポートで STP がブロックされないことを確認します。

デバイスがインベントリに存在しないことを確認

このセクションの内容は、任意の時点で検出されたか LAN 自動化で自動化されたデバイスに適用されます。

次の LAN 自動化セッションで検出するデバイスがすでにインベントリに存在する場合、次の手順を実行してインベントリから削除します。

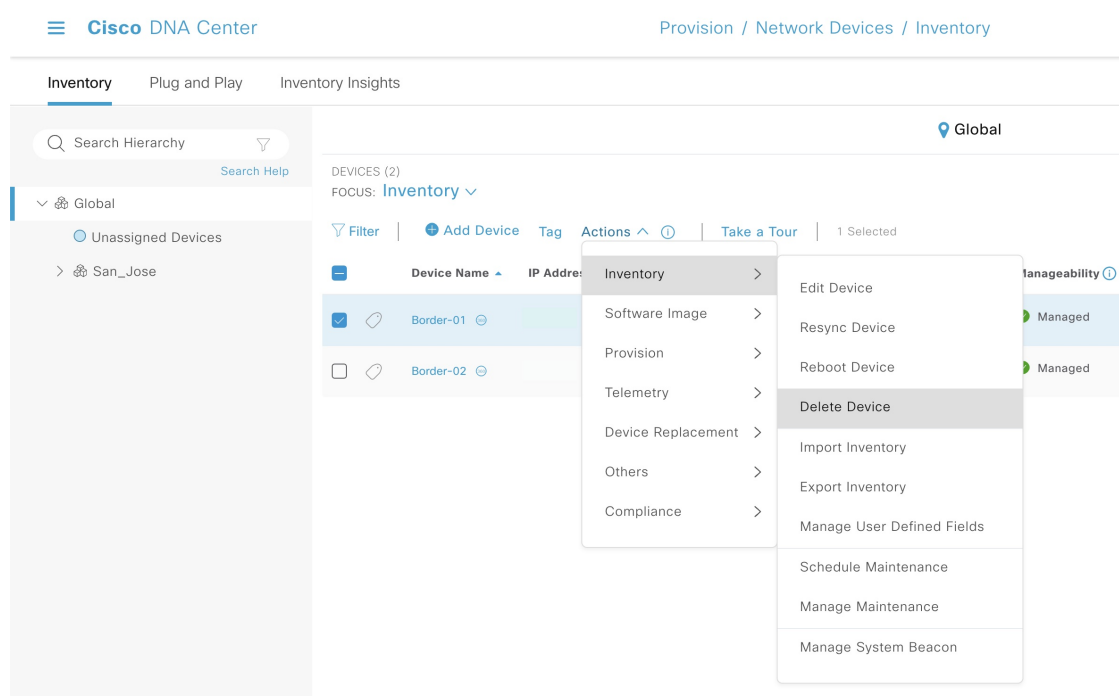
始める前に

デバイスがプロビジョニングされてファブリックに追加されている場合は、インベントリから削除する前にファブリックから削除してプロビジョニングを解除します。

手順

ステップ 1 Cisco DNA Center のホームページで、メニューアイコン (☰) をクリックして、**[Provision] > [Inventory]** の順に選択します。

ステップ 2 [Serial Number] 別にデバイスをフィルタ処理し、**[Actions]** ドロップダウンリストから **[Inventory] > [Delete Device]** の順に選択します。



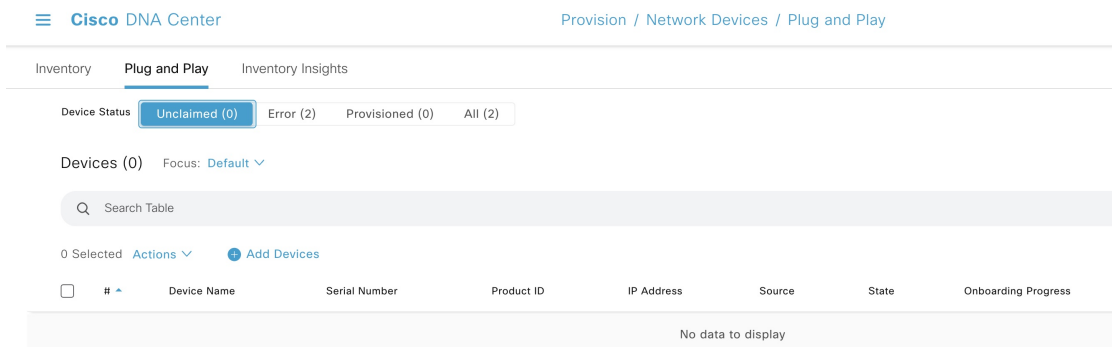
デバイスが PnP に存在しないことを確認

次回の LAN 自動化セッションで検出するデバイスがすでに PnP で使用可能になっている場合、検出の実行前に次の手順を実行して PnP から削除します。そうしないと、検出が正しく機能しません。

手順

ステップ 1 Cisco DNA Center ホームページで、メニューアイコン (☰) をクリックして、**[Provision] > [Plug and Play]** の順に選択します。

ステップ2 [Device Status] フィルタから、[Unclaimed] を選択します。[Unclaimed] で、検出するデバイス ([Serial Number]) が使用可能になっていないことを確認します。



ステップ3 デバイスが使用可能になっている場合は、デバイスにコンソール接続し、PnPプロファイルを削除します。

```
[on PNP agent]
```

```
3850_edge_2#show run | sec pnp-zero-touch
pnp profile pnp-zero-touch
transport https ipv4 192.168.99.2 port 443
```

```
3850_edge_2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
3850_edge_2(config)#no pnp profile pnp-zero-touch
3850_edge_2
```

Cisco IOS XE 16.12.x 以降の場合は、次を使用します。

```
pnp service reset no-prompt
```

ステップ4 [Unclaimed] セクションでデバイスのチェックボックスをオンにし、[Actions]>[Delete] をクリックします。

Advantage ライセンスを使用

PNP エージェントで実行している Cisco DNA Center のライセンスレベルが Advantage であることを確認します。

PNP エージェントがインストールモードであることを確認

LAN 自動化でイメージのアップグレードを行うには、PnP エージェントがインストールモードである必要があります。

LAN 自動化によるイメージのアップグレードはバックグラウンドで実行されます。

手順

ステップ1 PnP でデバイスが検出されると、検出されたデバイスのスイッチファミリー (Cisco Catalyst 9300 または 3850) に対してゴールデンイメージがマークされているかどうか Cisco DNA Center で確認されます。ゴールデンイメージが選択されているかどうかを確認するには、[Design] > [Image Repository] の順に選択します。

ゴールデンイメージがマークされていて、検出されたデバイスでゴールデンイメージが実行されていない場合は、検出デバイスがゴールデンイメージにアップグレードされます。それ以外の場合は、Cisco DNA Center によるイメージのアップグレードはスキップされ、デバイスの初期設定のプッシュに進みます。

ステップ 2 検出されたデバイスのイメージを LAN 自動化でアップグレードする場合は、デバイスがインストールモードで実行されていることを確認します。デバイスがバンドルモードの場合、LAN 自動化によるイメージのアップグレードは行われません。

ステップ 3 デバイスがバンドルモードの場合に LAN 自動化を続行するには、**[Design] > [Image Repository]** でその特定のスイッチファミリのゴールデンイメージを削除します。

ステップ 4: プロビジョニング

LAN 自動化プロセスの最後のステップはプロビジョニングです。次の 2 つの段階に分かれています。

1. デバイスの検出とオンボーディング (LAN 自動化の開始)。

LAN 自動化が開始されると、次の処理が行われます。

- ループバックと IS-IS の設定がプライマリとピアのシードデバイスにプッシュされ、一時的な設定がプライマリシードデバイスにプッシュされて、PnP エージェントの検出とオンボーディングが有効になります。



(注) Cisco DNA Center 2.3.3 以降では、IS-IS 設定の一部として `is-type level-2-only` をサポートしています。

- 新しいデバイスが検出されます。
- イメージがアップグレードされ、検出されたデバイスに設定がプッシュされます。



(注) イメージが更新されるのは、Cisco DNA Center のホームページの **[Design] > [Image repository]** で、そのスイッチタイプに対してゴールデンイメージがマークされている場合だけです。

LAN 自動化が開始されると、一時的な設定がプライマリシードデバイスにプッシュされ、PNP エージェントが検出されてオンボーディングされます。次に、PNP エージェントのイメージがアップグレードされ、ループバックアドレス、システム MTU、IP ルーティングなどの基本設定が PNP エージェントにプッシュされます。

2. インターフェイスの設定 (LAN 自動化の停止)。

LAN 自動化が停止されると、次の処理が行われます。

- 検出フェーズが終了し、シードデバイスと検出されたデバイスの間、および検出されたデバイス間 (最大 2 ホップ) のすべてのポイントツーポイントリンクがレイヤ 3 に変換されます。
- シードデバイスと検出されたデバイスから DHCP および VLAN 1 の一時的な設定がすべて削除されます。DHCP サブプールが LAN 自動化プールに戻されます。

LAN 自動化の開始

LAN 自動化では、プライマリシードデバイス、ピアシードデバイス、シードデバイスのサイト、LAN IP プール、およびインターフェイスを選択する必要があります。必要に応じて、デバイスのプレフィックス、ホスト名の CSV ファイル、設定可能な IS-IS パスワードなどを選択できます。

インターフェイスの選択

プライマリシードデバイスのインターフェイスは、新規デバイス検出および L3 設定に参加します。シードデバイスのインターフェイスは、LAN 自動化セッションでオンボーディングできる PnP エージェントを直接接続するためのフィルタを提供します。たとえば、直接接続された 4 つの PnP エージェントがあるとし、デバイス 1 は Gig1/0/10、デバイス 2 は Gig 1/0/11、デバイス 3 は Gig 1/0/12、デバイス 4 は Gig 1/0/13 で接続されています。検出インターフェイスの一部として Gig 1/0/11 と Gig 1/0/12 を選択した場合、LAN 自動化ではデバイス 1 とデバイス 2 のみが検出されます。デバイス 3 とデバイス 4 で PnP フローを開始しようとしても、これらは LAN 自動化セッションで選択されていないインターフェイスを介して接続されているためフィルタリングされます。このメカニズムにより、検出プロセスを制限できます。

インターフェイスの選択では、プライマリシードとピアシードの間のインターフェイスを選択してレイヤ 3 リンクを設定することもできます。プライマリシードとピアシードの間に複数のインターフェイスがある場合は、それらのインターフェイスの任意の組み合わせについてレイヤ 3 リンクを設定できます。インターフェイスが選択されていない場合、レイヤ 3 リンクは設定されません。

ピアシードインターフェイスを選択するオプションはありません。ピアシードと PnP エージェントの間のインターフェイスは、デバイスから収集されたトポロジ情報に基づいて自動的に推定されます。トポロジ情報は、デバイスで使用可能な CDP 情報に基づきます。

サイト選択

シードデバイスおよび PnP エージェントのサイトを選択できます。現在、シードデバイス用のサイトと PnP エージェント用のサイトが 1 つずつあります。

LAN プールの選択

LAN プールは、PnP エージェントのサイト情報に基づいて選択されます。LAN 自動化を開始するには、特定のサイトで使用可能な LAN プールのリストから LAN プールを選択します。複数の LAN 自動化セッションに同じ LAN プールを選択できます。たとえば、検出セッションを 1 回実行して最初のデバイスのセットを検出します。検出セッションの完了後、後続の LAN 自動化セッションに同じ IP プールを指定できます。同様に、検出セッションごとに異なる LAN プールを選択することもできます。必ず十分な残量がある LAN プールを選択してください。

IS-IS パスワード

- 値を入力する場合は、シードに設定されているものと同じパスワードを入力します。プライマリシードおよびピアシードに設定されたパスワードと異なる値を入力すると、エラーが返されます。
- プライマリシードとピアシードのパスワードが一致しない場合、エラーが返されます。

[IS-IS Password] フィールドに値を入力した場合：

- プライマリシードに IS-IS パスワードが設定されている場合、PnP デバイス（およびパスワードが未設定の場合はピアシード）にプライマリシードの IS-IS パスワードが設定されます。

- プライマリシードに IS-IS パスワードがなく、ピアにはある場合、PnP デバイスとプライマリシードにピアシードの IS-IS パスワードが設定されます。
- プライマリシードとピアシードに IS-IS パスワードが設定されていない場合、パスワードフィールドに値を入力すると、PnP デバイスとプライマリシードおよびピアシードにユーザが入力したパスワードが設定されます。

[IS-IS Password] フィールドを空欄のままにした場合：

- プライマリシードに IS-IS パスワードが設定されている場合、PnP デバイス（およびパスワードが未設定の場合はピアシード）にプライマリシードの IS-IS パスワードが設定されます。
- プライマリシードに IS-IS パスワードがなく、ピアにはある場合、PnP デバイスとプライマリシードにピアシードの IS-IS パスワードが設定されます。
- プライマリシードとピアシードに IS-IS パスワードが設定されていない場合、PnP デバイスと両方のシードにデフォルト値の「cisco」が使用されます。

ホスト名のマッピング

- [Default]：値を入力しない場合、**Switch** の後にループバックアドレスが続くホスト名が設定されます。たとえば、**Switch-192-168-199-100** のようになります。
- [Device Name Prefix]：デバイスのプレフィックスを使用して検出デバイスのホスト名が生成されます。LAN 自動化でサイトがカウントされ、プレフィックスと現在のサイトカウンタを使用して名前が生成されます。たとえば、デバイスのプレフィックスが *Building-23-First-Floor* の場合、*Building-23-First-Floor-1*、*Building-23-First-Floor-2* のようにデバイス名が生成されます。
- [Hostname Map File Format]：Cisco DNA Center では、次の例のような形式でホスト名とシリアル番号が指定された CSV ファイルが想定されます。スタックの LAN 自動化の場合、CSV ファイルを使用して 1 行に 1 つのホスト名と複数のシリアル番号を入力できます。シリアル番号はカンマで区切ります。



(注) デバイス名プレフィックスとホスト名マップファイルの両方が使用されている場合は、ホスト名マップファイルが優先され、デバイス名プレフィックスは使用されません。

A	B
Edge1	FCW2048Cxxx
Edge2	FCW2131Lxxx, FCW2131Gxxx, FCW2131Gxxx, FCW2131Gxxx
Edge3	FOC2052Xxxx, FCW2052Cxxx, FCW2052Fxxx
Edge4	FXS2131Qxxx

始める前に

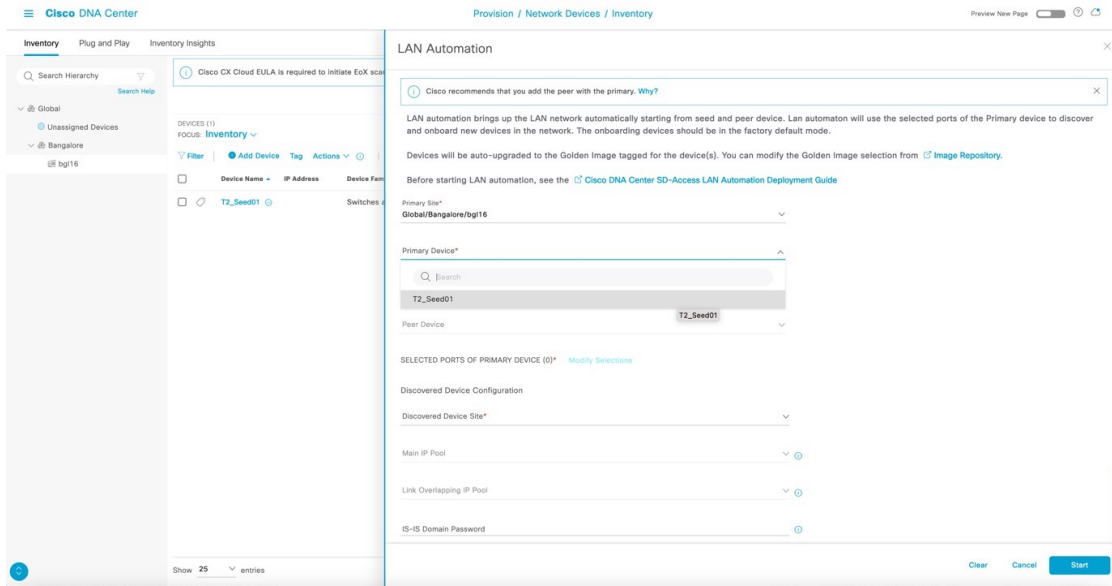
Cisco DNA Center 2.3.5 以降については、「[LAN 自動化のプロビジョン \(53 ページ\)](#)」を参照してください。

手順

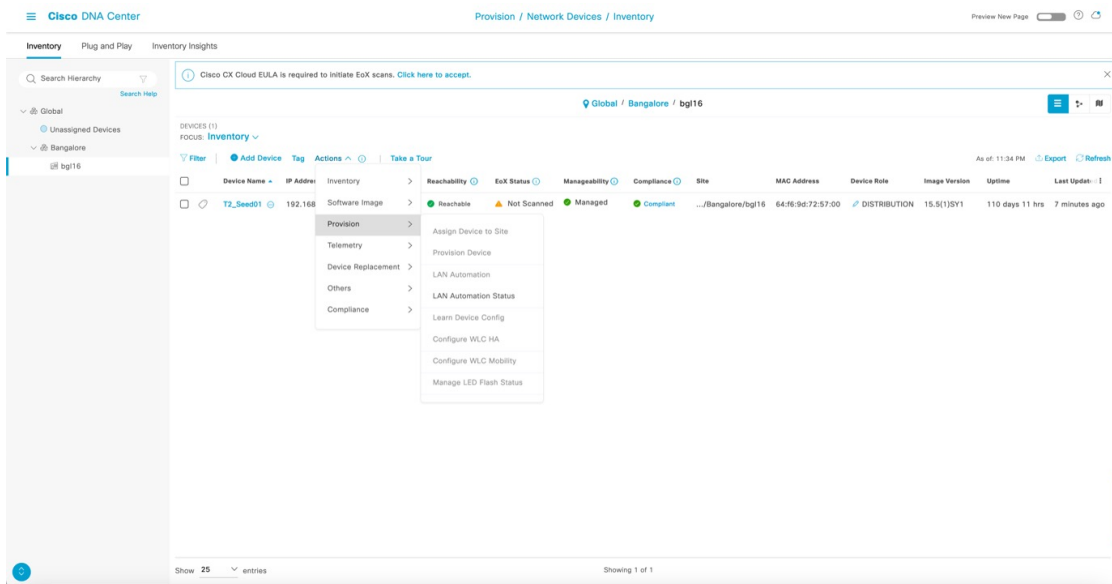
ステップ1 Cisco DNA Center GUI で、メニューアイコン（☰）をクリックして、[Provision] > [Network Devices] > [Inventory] の順に選択します。

ステップ2 [Inventory] ウィンドウで、[Actions] > [Provision] > [LAN Automation] の順に選択します。

ステップ3 必要な詳細を入力し、[Start] をクリックします。



ステップ4 LAN 自動化が開始されたら、[Lan Automation Status] をクリックして進行状況をモニタします。



Cisco DNA Center Provision / Network Devices / Inventory

Inventory Plug and Play Inventory Insights

LAN Automation Status

Summary Devices Logs

Discovered Site bg16

Primary Device T2_Seed01

Peer Device None

Primary Device Interfaces TenGigabitEthernet1/9

IP Pool LanPool

Link Overlapping IP Pool None

Advertise LAN Automation summary route into BGP Disabled

Multicast Disabled

Device Prefix None

Hostname File None

Status Seed Provisioned

Discovered Devices 0

Completed : 0 In Progress : 0 Error : 0

LAN 自動化が始まると、次の例のような設定がシードデバイスにプッシュされます。

プライマリシードの設定

```
!exec: enable
!  
system mtu 9100  
!  
ip multicast-routing  
ip pim ssm default  
!
```

ループバック IP と IS-IS の設定（セカンダリシードが設定されている場合、セカンダリシードにもループバック IP と IS-IS の設定がプッシュされます）。

```
interface Loopback0  
  ip address 10.4.210.123 255.255.255.255  
  description Fabric Node Router ID  
!  
router isis  
  net 49.0000.0100.0421.0123.00  
  domain-password *  
  ispf level-1-2  
  metric-style wide  
  nsf ietf  
  log-adjacency-changes  
  bfd all-interfaces  
  passive-interface Loopback0  
  default-information originate  
!  
interface Loopback0  
ip router isis  
  
clns mtu 1400  
  
ip pim sparse-mode  
exit  
!
```

DHCP プールの情報：

```
ip dhcp pool nw_orchestration_pool  
  network 10.4.218.0 255.255.255.192  
  option 43 ascii 5A1D;B2;K4;I10.4.249.241;J80;  
  default-router 10.4.218.1  
  class ciscopnp  
    address range 10.4.218.2 10.4.218.62  
!  
ip dhcp class ciscopnp  
  option 60 hex 6369736366f706e70  
!  
ip dhcp excluded-address 10.4.218.1  
!
```

VLAN 1 の設定：

```
vlan 1  
!  
interface Vlan1  
  ip address 10.4.218.1 255.255.255.192  
  no shutdown  
  ip router isis  
  clns mtu 4100  
  bfd interval 500 min_rx 500 multiplier 3  
  no bfd echo  
exit
```


プライマリシードの設定

```
!
```

検出に使用されるインターフェイスのスイッチポートの設定（この設定はプライマリシードデバイスの各検出インターフェイスにプッシュされます）。

```
interface TenGigabitEthernet1/1/8
  switchport
  switchport mode access
  switchport access vlan 1
```

```
!
```

```
interface TenGigabitEthernet1/1/7
  switchport
  switchport mode access
  switchport access vlan 1
```

```
exit
```

マルチキャストの設定（オプション。マルチキャストのチェックボックスがオンの場合にのみ設定されます）。

アンダーレイマルチキャストのランデブーポイント（RP）をボーダーにする必要がある場合は、ボーダースイッチをシードデバイスとして使用して、マルチキャストを有効にして LAN 自動化を開始してください。

ピアシードが設定されている場合、これらのマルチキャストの CLI がピアシードにもプッシュされます。同じ `rp-address` を使用して、プライマリシードとピアシードの両方で Loopback0 が設定されます。

```
interface Loopback0
  ip address 10.4.218.67 255.255.255.255
  ip pim sparse-mode
  ip router isis
```

```
ip pim register-source Loopback0
```

```
ip pim rp-address 10.4.218.67
```

セカンダリシードの設定

```
!exec: enable
!
system mtu 9100
!
ip multicast-routing
ip pim ssm default
!
interface Loopback0
 ip address 10.4.210.124 255.255.255.255
 description Fabric Node Router ID
!
router isis
 net 49.0000.0100.0421.0124.00
 domain-password *
 ispf level-1-2
 metric-style wide
 nsf ietf
 log-adjacency-changes
 bfd all-interfaces
 passive-interface Loopback0
 default-information originate
!
interface Loopback0
 ip router isis
 clns mtu 4100
 ip pim sparse-mode
 exit
!
```

(注) Cisco DNA Center 2.3.3 以降では、IS-IS 設定の一部として is-type level-2-only をサポートしています。

ステップ 5 デバイス検出の開始後、PnP エージェントのログを確認します。

(注) まだ PnP エージェントで Enter キーを押さないでください。

```
%INIT: waited 0 seconds for NVRAM to be available

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!

*Aug  2 23:13:50.440: %SMART_LIC-5-COMM_RESTORED: Communications with the Cisco Smart Software
Manager or satellite restored
*Aug  2 23:13:51.314: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1875844429 has been
generated or imported
*Aug  2 23:13:51.315: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Aug  2 23:13:51.355: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to
save new IOS PKI configuration
*Aug  2 23:13:51.418: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-1875844429.server
has been generated or imported
*Aug  2 23:13:52.071: %LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to administratively
down
*Aug  2 23:13:53.071: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to down
*Aug  2 23:14:00.112: %HMANRP-6-EMP_ELECTION_INFO: EMP active switch 1 elected: EMP_RELAY: Mgmt port
```

```
status DOWN, reelecting EMP active switch
```

```
*Aug 2 23:14:00.112: %HMANRP-6-EMP_NO_ELECTION_INFO: Could not elect active EMP switch, setting
emp active switch to 0: EMP_RELAY: Could not elect switch with mgmt port UP
*Aug 2 23:14:02.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 23:14:04 UTC Thu Aug
2 2018 to 23:14:02 UTC Thu Aug 2 2018, configured from console by vty0.
Aug 2 23:14:02.000: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
Aug 2 23:14:02.462: %PNP-6-PNP_DISCOVERY_DONE: PnP Discovery done successfully
Aug 2 23:14:07.847: %PKI-4-NOCONFIGAUTOSAVE: Configuration was modified. Issue "write memory" to
save new IOS PKI configuration
Aug 2 23:14:16.348: %AN-6-AN_ABORTED_BY_CONSOLE_INPUT: Autonomic disabled due to User intervention
on console. configure 'autonomic' to enable it.
%Error opening tftp://255.255.255.255/network-config (Timed out)
Aug 2 23:14:25.263: AUTOINSTALL: Tftp script execution not successful for V11.
```

ステップ6 デバイスが検出されると、検出されたデバイスのスイッチファミリーに対してゴールデンイメージがマークされているかどうかを Cisco DNA Center で確認されます。ゴールデンイメージがマークされていて、検出されたデバイスでゴールデンイメージが実行されていない場合は、最初に検出デバイスがゴールデンイメージにアップグレードされます。それ以外の場合は、Cisco DNA Center によるイメージのアップグレードはスキップされ、デバイスの初期設定がプッシュされます。次のログは、イメージがアップグレードされた場合のもので、

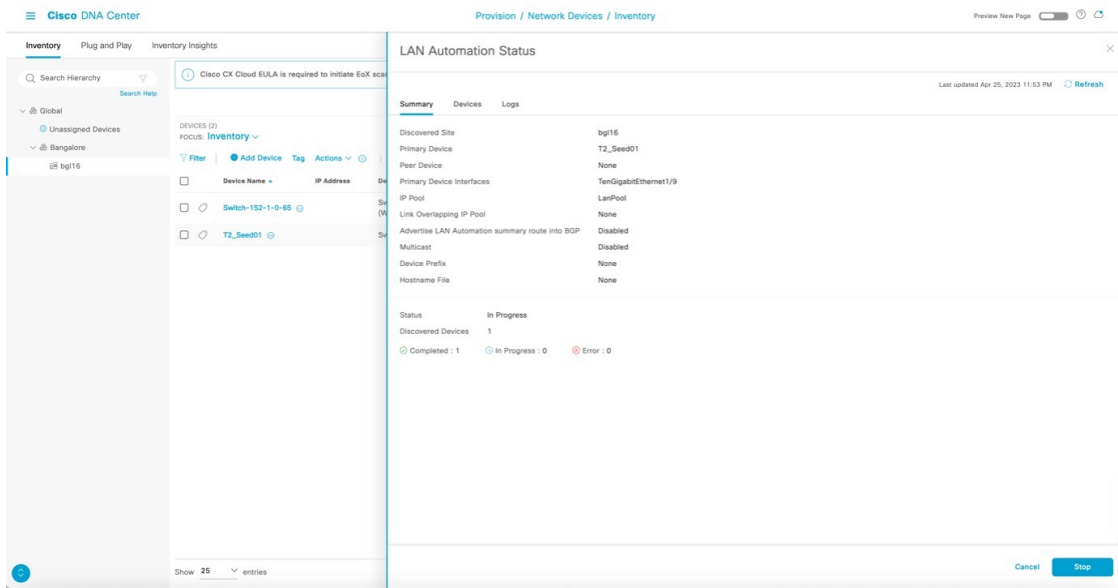
```
Oct 5 19:20:11.437: MCP_INSTALLER_NOTICE:
Installer: Source file flash:cat9k_iosxe.16.06.04s.SPA.bin is in flash, Install directly
Oct 5 19:20:12.450: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:20:12 provision.sh:
%INSTALL-5-OPERATION_START_INFO: Started install package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:20:22.778: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:20:22 packtool.sh:
%INSTALL-5-OPERATION_START_INFO: Started expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:21:26.034: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:21:26 packtool.sh:
%INSTALL-5-OPERATION_COMPLETED_INFO: Completed expand package flash:cat9k_iosxe.16.06.04s.SPA.bin
Oct 5 19:22:09.861: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 5 19:22:09 provision.sh:
%INSTALL-5-OPERATION_COMPLETED_INFO: Completed install package flash:{<package_name>}

***
*** --- SHUTDOWN NOW ---
***

Oct 5 19:22:20.950: %SYS-5-RELOAD: Reload requested by controller. Reload Reason: Image Install.
Chassis 1 reloading, reason - Reload command
Oct 5 19:22:30.501 FP0/0: %PMAN-5-EXITACTION:
Process manager is exiting: reload fp action requested
Oct 5 19:22:

Initializing Hardware...
```

Cisco DNA Center で設定の一部がプッシュされ、Cisco DNA Center によるデバイスのオンボーディングと管理が可能になります。[LAN Automation Status] に [In Progress] と表示され、[Discovered Devices Status] に検出中のすべてのデバイスの集約ステータスが表示されます。さらに、検出中の個々のデバイスのステータスが [Devices] タブに表示されます。



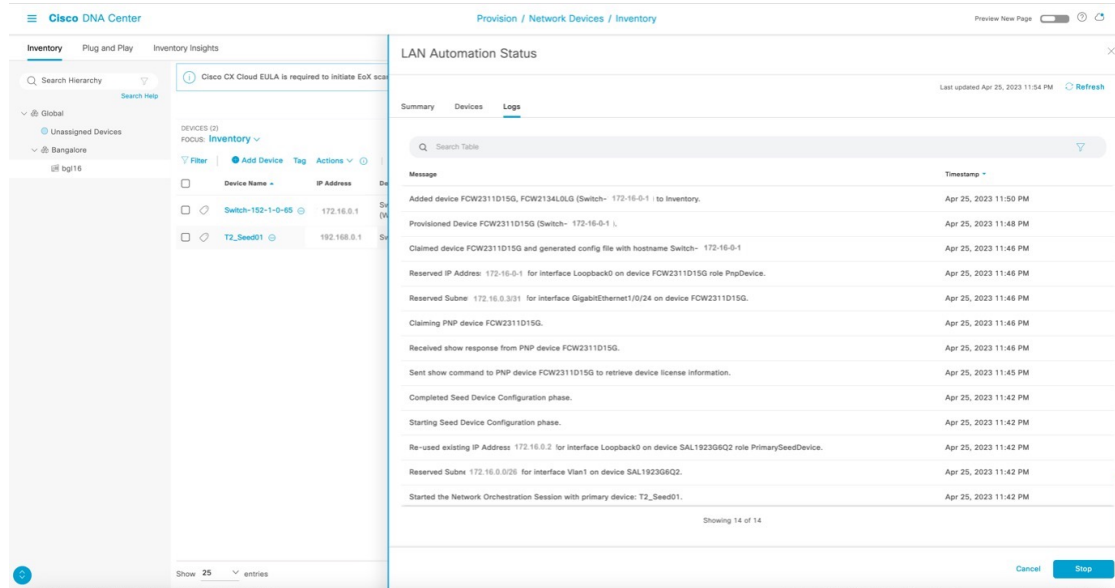
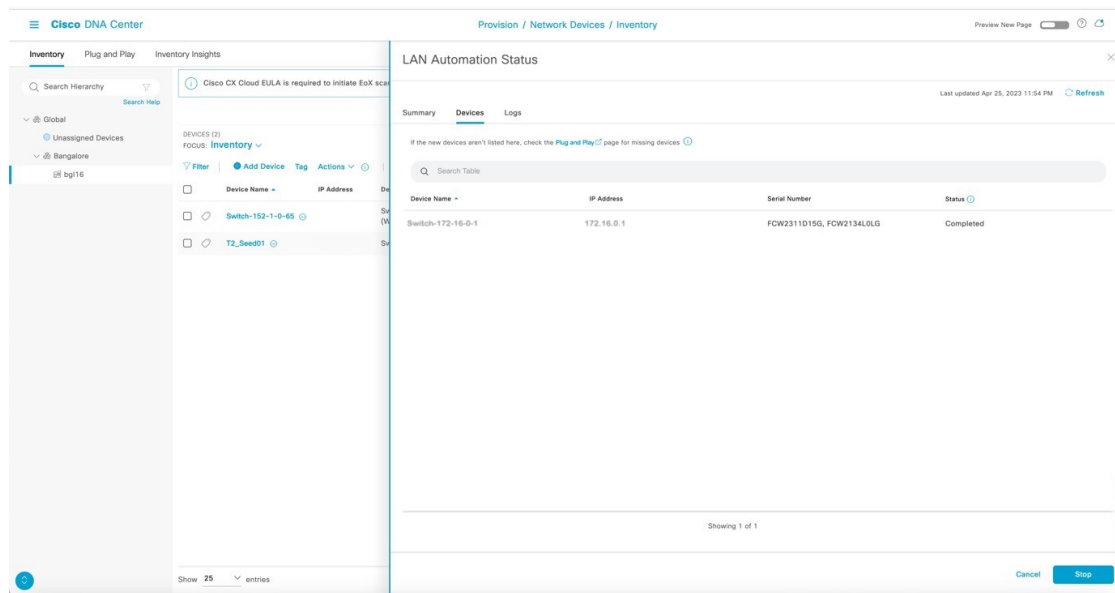
ステップ7 PnP エージェントのログを確認します。次の例に示すような情報が表示されます。このコンソールでは、必要に応じて **Return** キーを押してかまいません。**Return** キーを押すと、ホスト名が LAN 自動化を開始したときに [Hostname Mapping] フィールドに入力した値に変更されます。

```
Aug 2 23:14:50.682: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/3, changed state to up
Aug 2 23:14:51.487: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/24, changed state to up
Aug 2 23:14:51.681: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/3, changed
state to up
Aug 2 23:14:51.854: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/23, changed state to up
Aug 2 23:14:52.487: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/24, changed
state to up
Aug 2 23:14:52.855: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed
state to up
000123: Aug 2 23:16:17.345: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named dnac-sda has been generated
or imported
000124: Aug 2 23:16:17.423: Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...

000125: Aug 2 23:16:17.474: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed
state to up
000126: Aug 2 23:16:17.479: %CLNS-6-DFT_OPT: Protocol timers for fast convergence are Enabled.
000128: Aug 2 23:16:17.489: %bfd-6-BFD_IF_CONFIGURE: BFD-SYSLOG: bfd config apply, idb:Vlan1
000129: Aug 2 23:16:18.423: %CLNS-3-BADPACKET: ISIS: LAN L1 hello, packet (9097) or wire (8841)
length invalid from f87b.2077.b147 (Vlan1)
000130: Aug 2 23:16:18.502: %bfd-6-BFD_SESS_CREATED: BFD-SYSLOG: bfd_session_created, neigh
204.1.183.1 proc:ISIS, idb:Vlan1 handle:1 act
000131: Aug 2 23:16:19.269: %bfd-6-BFD_SESS_UP: BFD-SYSLOG: BFD session ld:1 handle:1 is going
UP
000132: Aug 2 23:16:19.494: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 0100.1001.0001 (Vlan1) Up, new
adjacency
000133: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: Op43 has 5A. It is for PnP
000134: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: After stripping extra characters in front of 5A,
if any

000135: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _pdon.2.ina=[Vlan1]
000136: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _papdo.2.eRr.ena
000137: Aug 2 23:16:20.289: %PNPA-DHCP Op-43 Msg: _pdon.2.eRr.pdo=-1
000138: Aug 2 23:16:30.010: %CLNS-5-ADJCHANGE: ISIS: Adjacency to 9324-SN-BCP-1 (Vlan1) Up, new
adjacency
```

すべてのデバイスが検出されると、[Discovered Devices] のステータスが [Completed] に変わり、検出されたデバイスがインベントリに追加されます。



ステップ 8 Cisco DNA Center のホームページで、メニューアイコン (≡) をクリックして、[Provision]> [Inventory] の順に選択し、シリアル番号でフィルタリングします。新しく検出されたスイッチが [Managed] として表示されます。

検出されたデバイスにプッシュされる設定例を次に示します。

```
!
archive
log config
logging enable
logging size 500
```

```

hidekeys
!
!
!
service timestamps debug datetime msec
!
service timestamps log datetime msec
!
service password-encryption
!
service sequence-numbers
!
! Setup NTP Server
! Setup Timezone & Daylight Savings
!
ntp server 10.4.250.104
!
! ntp update-calendar
!
! clock timezone <timezoneName> <timezoneOffsetHours> <timezoneOffsetMinutes>
! clock summer-time <timezoneName> recurring
!
! Disable external HTTP(S) access
! Disable external Telnet access
! Enable external SSHv2 access
!
no ip http server
!
no ip http secure-server
!
ip ssh version 2
!
ip scp server enable
!
line vty 0 15
! maybe redundant
login local
transport input ssh
! maybe redundant
transport preferred none
! Set VTP mode to transparent (no auto VLAN propagation)
! Set STP mode to Rapid PVST+ (prefer for non-Fabric compatibility)
! Enable extended STP system ID
! Set Fabric Node to be STP Root for all local VLANs
! Enable STP Root Guard to prevent non-Fabric nodes from becoming Root
! Confirm whether vtp mode transparent below is needed
vtp mode transparent
!
spanning-tree mode rapid-pvst
!
spanning-tree extend system-id
! spanning-tree bridge priority 0
! spanning-tree rootguard
! spanning-tree portfast bpduguard default
no udd enable
!
errdisable recovery cause all
!
errdisable recovery interval 300
!
ip routing
!Config below applies only on underlay orchestration
!
! Setup a Loopback & IP for Underlay reachability (ID)

```

```

! Add Loopback to Underlay Routing (ISIS)
!
interface loopback 0
description Fabric Node Router ID
ip address 10.4.218.97 255.255.255.255
ip router isis
!
!
! Setup an ACL to only allow SNMP from Fabric Controller
! Enable SNMP and RW access based on ACL
!
snmp-server view DNAC-ACCESS iso in
!
snmp-server group DNACGROUPAuthPriv v3 priv read DNAC-ACCESS write DNAC-ACCESS
!
snmp-server user admin DNACGROUPAuthPriv v3 auth MD5 C1sco123 priv AES 128 C1sco123
!
!
! Set MTU to be Jumbo (9100, some do not support 9216)
!
system mtu 9100
! FABRIC UNDERLAY ROUTING CONFIG:
!
! Enable ISIS for Underlay Routing
! Specify the ISIS Network ID (e.g. encoded Loop IP)
! Specific the ISIS domain password
! Enable ISPF & FRR Load-Sharing
! Enable BFD on all (Underlay) links
!
router isis
net 49.0000.0100.0421.8097.00
domain-password cisco
ispf level-1-2
metric-style wide
nsf ietf
! fast-reroute load-sharing level-1
log-adjacency-changes
bfd all-interfaces
! passive-interface loopback 0
!
!
!
interface vlan1
bfd interval 500 min_rx 500 multiplier 3
no bfd echo
!
!
!This config goes to subtended node

username lan-admin privilege 15 password 0 C1sco123
!
enable password C1sco123
!
!
hostname CL-9300_7
!
interface vlan1
ip router isis
!
!
end

```

(注) Cisco DNA Center 2.3.3 以降では、IS-IS 設定の一部として `is-type level-2-only` をサポートしています。

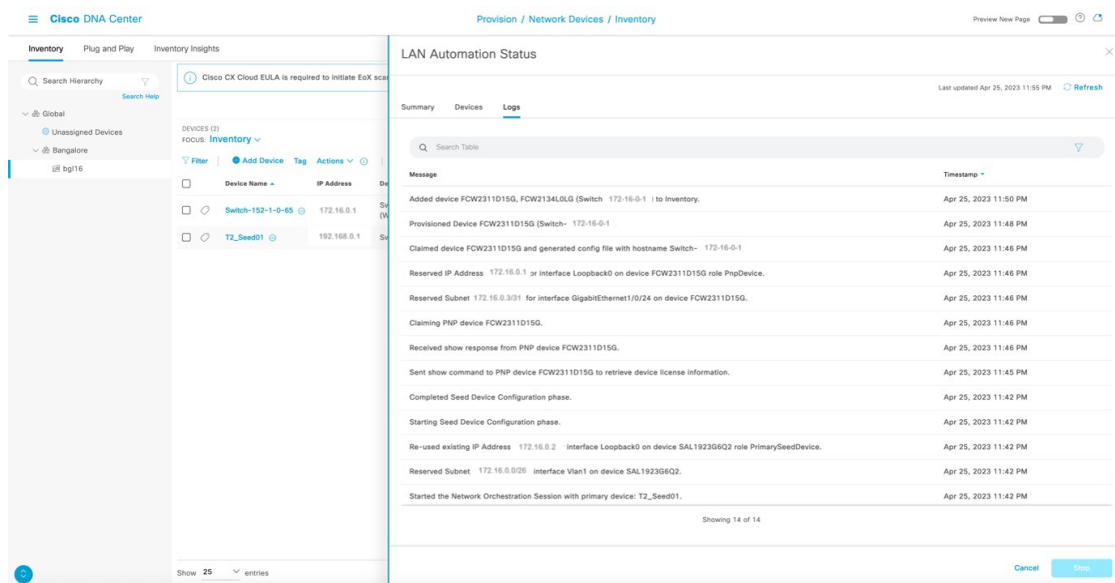
ステップ 9 [Discovered Devices] のステータスが [Completed] に変わり、検出されたすべてのデバイスがインベントリに [Managed] として表示されたら、LAN 自動化を停止できます。ただし、LAN 自動化を停止する前に [Topology] ページを表示し、検出されたデバイスとプライマリシードおよびピアシードの間のリンクが表示されていることを確認してください。[Tools] > [Topology] の順に選択し、シードと検出されたデバイスの間の物理リンクをクリックします。インターフェイスが正しいことを確認します。

物理リンクが表示されない場合は、物理リンクが接続されているシードデバイスを再同期します。再同期後、LAN 自動化を停止する前に [Topology] ページを再度表示して、リンクが表示されることを確認します。

LAN 自動化の停止

必要なすべてのデバイスが検出されたら、追加のデバイスが誤って検出されないように、LAN 自動化を停止できます。

[LAN Automation Status] ウィンドウで、[Stop] をクリックします。



[Stop] をクリックすると、次の処理が行われます。

- 残りの設定がネットワークデバイスにプッシュされます。これには、ポイントツーポイントリンクのレイヤ2からレイヤ3への変換が含まれます。
- VLAN 1 の設定が削除され、VLAN 1 の IP アドレスが LAN 自動化プールに戻されます。
- デバイスが Cisco DNA Center でオンボーディングされ、サイトに割り当てられます。

LAN 自動化の停止プロセスが開始されると、[LAN Automation Status] が [STOP in Progress] に変わります。

LAN 自動化が停止すると、次の例のような設定が検出デバイスにプッシュされます。

ネットワーク オーケストレーション サービスにより、すべてのリンクの状態を取得するためにシードデバイスと PnP デバイスの RESYNC が発行されます。最初の RESYNC の完了後、すべてのレイヤ 2 リンクにレイヤ 3 設定がプッシュされます。最後に、クラスタのリンク状態を再同期するために RESYNC が再発行されます。

ネットワーク オーケストレーションが停止すると、レイヤ 3 リンク設定がプッシュされます（インターフェイスペアごとに設定が適用されます）。

```
interface GigabitEthernet1/0/13
description Fabric Physical Link
no switchport
dampening
ip address 192.168.2.97 255.255.255.252
ip router isis
logging event link-status
load-interval 30
bfd interval 500 min_rx 50 multiplier 3
no bfd echo
isis network point-to-point
```

シードと検出デバイス間のすべてのポイントツーポイントリンク（ピアシードと検出デバイス間のリンクを含む）が設定されると、デバイスがサイトに追加されて Cisco DNA Center と同期されます。

LAN 自動化プロセスが完了し、[LAN Automation Status] が [Completed] に変わります。

LAN 自動化のログを確認します。

The screenshot displays the Cisco DNA Center interface. On the left, the 'Inventory' section shows a list of devices, including 'Switch-152-1-0-05' and 'T2_Sev01'. The main panel is titled 'LAN Automation Status' and shows a log of events. The log includes messages such as 'Completed LAN Automation.', 'Completed Final Resync.', 'Starting Final Resync for Devices.', 'Releasing SVI subnet: 172.16.0.0/25', 'Completed Device Cleanup.', 'Waiting for Device Cleanup to complete.', 'Starting Device Cleanup.', 'Completed L3 Conversion for the session's Tier-2 Devices.', 'Configuring L3 Interfaces for the session's Tier-2 Devices.', 'Completed Initial Resync.', 'Starting Initial Resync for Devices.', 'Stopping LAN Automation by user: admin.', and 'Added device FCW2311D15G, FCW2134L0LG (Switch- 172.16-0-1 to Inventory.' A 'Success' notification is visible at the bottom right, indicating 'Successful Stop Network Orchestration success.'

既存の LAN 自動化スタックへのスイッチとリンクの追加

このセクションでは、LAN 自動化スタックで新しいスイッチを追加する方法、既存のスイッチを追加する方法、リンクを設定する方法について説明します。

新しいスイッチの追加

このセクションでは、Cisco DNA Center に存在していない新規のスイッチを追加する方法について説明します。

LAN 自動化ですでに自動化されてプロビジョニングされた状態のスタックにスイッチを追加できます。この場合、新しいスイッチについて LAN 自動化を実行したり検出したりする必要はありません。

手順

- ステップ 1** スイッチが以前に Cisco DNA Center に含まれていなかったことを確認します（スイッチが検出されていたり、インベントリに存在してはなりません）。
- ステップ 2** 追加するスイッチのイメージとライセンスのバージョンがプロビジョニング済みのスタンドアロン/スタックと同じであることを確認します。イメージとライセンスのバージョンを確認するには、`show ver` コマンドと `show license right-to-use` コマンドを使用します。
- ステップ 3** スイッチのブートモードがスタックと同じであることを確認します。インストールモード（推奨）またはバンドルモードである必要があります。

```
9300_Edge_1#show ver | inc INSTALL
*  1 62  C9300-48U          16.6.3          CAT9K_IOSXE     INSTALL
   2 62  C9300-48U          16.6.3          CAT9K_IOSXE     INSTALL
   3 62  C9300-48U          16.6.3          CAT9K_IOSXE     INSTALL
   4 62  C9300-48U          16.6.3          CAT9K_IOSXE     INSTALL
```

- ステップ 4** スタックケーブルを使用して、新しいスイッチをスタックに接続します。接続したら、電源をオンにします。2～3分ほどで、新しいスイッチがスタックにスタンバイ（スタックの既存のスイッチが1つの場合）またはメンバー（スタックの既存のスイッチが2つ以上の場合）として追加されます。
- ステップ 5** `show ver` コマンドと `show switch` コマンドの出力を確認して、新しいスイッチが追加されたことを確認します。`show ver` コマンドの出力にすべてのスイッチのシリアル番号が表示されます。
- ステップ 6** スイッチがスタックに追加されたら、[Inventory] に移動し、元のプロビジョニング済みのスイッチ/スタックを選択して再同期を実行します。
- ステップ 7** 同期が完了すると、新しいシリアル番号が表示され、追加プロセスが完了します。

（注） 一度に複数のスイッチを追加できます。正しいケーブルを使用して、この手順を繰り返します。

次の図に、新しいスイッチを追加する前のシリアル番号を示します。

Inventory

Last updated: 4:14 pm Refresh Import Export Add

Filter Actions

Device Name	IP Address	Reachability Status	Serial Number	Uptime	Last Updated	Resync Interval	Last Sync Status	Site
3850_Edge_3	192.168.199.98	Reachable	FCW2133F05W, FOC2052X0C9, FCW2020F0A0	8 days 6 hrs 22 mins	7 minutes ago	00:25:00	Managed	...SJC24/SJC24-1
9500_Edge_1	192.168.199.97	Reachable	FCW2214L0S3, FCW2224C122	1 day 1 hrs 50 mins	6 minutes ago	00:25:00	Managed	...SJC24/SJC24-1
9500_border.ciscodna	192.168.210.1	Reachable	FCW2205A33L	5 days 6 hrs 24 mins	13 minutes ago	00:25:00	Managed	...SJC24/SJC24-1

Show 10 entries Showing 1 - 3 of 3

次の図に、新しいスイッチを追加した後のシリアル番号を示します。

Inventory

Last updated: 4:45 pm Refresh Import Export Add

Filter Actions

Device Name	IP Address	Reachability Status	Serial Number	Uptime	Last Updated	Resync Interval	Last Sync Status	Site
3850_Edge_3	192.168.199.98	Reachable	FCW2133F05W, FOC2052X0C9, FCW2020F0A0	8 days 6 hrs 49 mins	10 minutes ago	00:25:00	Managed	...SJC24/SJC24-1
9500_Edge_1	192.168.199.97	Reachable	FCW2214L0S3, FCW2224C122, FOC2224Q0UE, FCW2224C123	1 day 2 hrs 13 mins	12 minutes ago	00:25:00	Managed	...SJC24/SJC24-1
9500_border.ciscodna	192.168.210.1	Reachable	FCW2205A33L	5 days 6 hrs 52 mins	17 minutes ago	00:25:00	Managed	...SJC24/SJC24-1

Show 10 entries Showing 1 - 3 of 3

既存のスイッチの追加

このセクションでは、Cisco DNA Center にすでに存在する既存のスイッチを追加する方法について説明します。

以前に LAN 自動化で自動化されているスイッチ（別のスタックの一部またはスタンドアロンのスイッチ）や PnP で検出されているスイッチを追加する場合は、まずスイッチを物理的に取り外し、そのエントリーをインベントリおよび PnP アプリケーション/データベースから削除する必要があります。

インベントリからのスイッチの削除

スイッチがスタンドアロンの場合は、Cisco DNA Center のホームページで [Inventory] をクリックし、削除するスイッチを選択します。[Actions] > [Delete Device] の順に選択します。スイッチがスタックの一部である場合は、スイッチを物

理的に取り外してから、元のスタックを再同期します。同期が完了すると、取り外したスイッチのシリアル番号がインベントリに表示されなくなります。

PnPからのスイッチの削除

- スイッチがスタンドアロンの場合は、まずスイッチの `pnp profile pnp-zero-touch` の設定を解除し、[Device] で PnP データベースからエントリを削除します。
- スイッチがスタックの一部である場合は、スイッチを物理的に取り外します。取り外したスイッチに `pnp profile pnp-zero-touch` が設定されていないことを確認してから、[Device] で PnP データベースからエントリを削除します。

LAN 自動化停止後の追加リンクの設定

ここでは、以下を設定する際に使用する方法を示します。

- LAN 自動化停止後のプライマリシードデバイスとピアシードデバイスの間または分散デバイス間の追加リンク
- 新しく追加されたスタックスイッチからプライマリシードおよびピアシードへのアップリンク

デバイスで最初に LAN 自動化を実行したときに [Enable Multicast] オプションを選択した場合、追加のリンクを設定するときは [Enable Multicast] を選択しないでください。次の手順を実行して LAN 自動化が停止したら、新しく設定したレイヤ 3 ポートに移動し、インターフェイスで `ip pim sparse-mode` を手動で設定します。

始める前に

Cisco DNA Center 2.3.5 以降については、「[インターフェイス間のリンクの作成 \(61 ページ\)](#)」を参照してください。

手順

ステップ 1 `show cdp neighbors` コマンドの出力で、新しいリンクに接続されているネイバーが表示されていることを確認します。次の設定例では、スイッチ `9300_Edge-7` のポート `Ten 4/1/5` に接続される新しいリンクを示します。リンクのもう一方の端は、ポート `For 1/0/1` を介してスイッチ `9500_border-6` に接続します。

```
9300_Edge-7#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability  Platform  Port ID
9500_border.cisco.com
                  Ten 1/1/5       173        R S I      C9500-12Q For 1/0/1
9500_border-6.cisco.com
                  Ten 4/1/5       136        R S I      C9500-12Q For 1/0/1
```

ステップ 2 リンクの接続先のポート (`Ten 4/1/5` と `For 1/0/1`) にレイヤ 3 設定がないことを確認します。レイヤ 3 設定がある場合は、追加する新しいアップリンクに接続されたデフォルトのインターフェイスを使用し、両方のデバイスを再同期します。

ステップ 3 Cisco DNA Center のホームページで、[Provision] > [LAN Automation] の順に選択します。

- ステップ4** [Primary Device] フィールドに、新しいリンクの接続先のスイッチ（たとえば **9500_border-6**）を入力します。
- ステップ5** [Peer Device] フィールドに、新しいリンクを設定するスイッチ（たとえば **9300_Edge-7**）を入力します。
- ステップ6** アップリンクが接続するプライマリデバイスのポート、つまり PnP デバイスが接続されるポート（たとえば **For 1/0/1**）を選択します。
- ステップ7** 元のスタックのプロビジョニングに使用したのと同じ LAN 自動化プールを使用します。
- ステップ8** LAN 自動化を開始します。2分待ってから、LAN 自動化を停止します。新規デバイス検出は実行しないため、LAN 自動化プロセス全体を実行する必要はありません。LAN 自動化を停止すると、アップリンクに接続された両方のポートに同じ LAN 自動化プールから IP アドレスが設定されます。
- ステップ9** 次の例に示すように、LAN 自動化が停止して完了すると、両方のポートが LAN プールからレイヤ 3 用に設定されます。

```
9300_Edge-7#show run int t4/1/5
Building configuration...

Current configuration : 325 bytes
!
interface TenGigabitEthernet4/1/5
  description Fabric Physical Link
  no switchport
  dampening
  ip address 192.168.199.85 255.255.255.252
  ip router isis
  logging event link-status
  load-interval 30
  bfd interval 100 min_rx 100 multiplier 3
  no bfd echo
  isis network point-to-point

9500_border-6#show run int Fo1/0/1
Building configuration...

Current configuration : 327 bytes
!
interface FortyGigabitEthernet1/0/1
  description Fabric Physical Link
  no switchport
  dampening
  ip address 192.168.199.86 255.255.255.252
  ip router isis
  logging event link-status
  load-interval 30
  bfd interval 100 min_rx 100 multiplier 3
  no bfd echo
  isis network point-to-point
end
```

- (注) API に精通していれば、上記の IP アドレスの追加を API を使用して手動で実行することもできます。ただし、LAN 自動化を使用して IP アドレスを追加するとすべてのテーブルエントリが更新されるため、LAN 自動化を使用することを推奨します。LAN 自動化のもう 1 つの利点は、デバイスをインベントリから削除したときに関連するすべての IP アドレスが解放されることです。API を使用して手動で設定されている場合は IP アドレスは解放されません。

新しく追加されたスイッチへのアップリンクの移動

すでにプロビジョニングされているスタックから、LAN 自動化スタックに新しく追加されたスイッチにアップリンクを移動することはできません。

Cisco Catalyst 9400 での 40G インターフェイスの使用

16.11.1 以降の Cisco IOS では、次の条件を満たしていれば、起動時に 40G ポートが有効になります。

- スイッチが工場出荷時の Day-0 設定である必要があります（デバイスを Day-0 設定に戻す方法については、[PNP エージェントの初期状態（18 ページ）](#)を参照してください）。
- シングルスーパーバイザの場合、SUP ポート（ポート 1～8）のいずれにも 10G/1G SFP を挿入できません。ポート 9 または 10 に 40G QSFP を挿入する必要があります。
- デュアルスーパーバイザの場合、SUP ポート（ポート 1～8）のいずれにも 10G/1G SFP を挿入できません。ポート 9 にのみ 40G QSFP を挿入する必要があります。

LAN 自動化のトラブルシューティング

問題が発生した場合は、根本原因分析（RCA）ファイルを集集するとトラブルシューティングに役立ちます。CLI で次のように入力します。

```
$ sudo rca
```

3 ノードクラスタの場合は、各クラスタの RCA ファイルを集集します。

追加情報：Cisco DNA Center 2.3.5 以降の LAN 自動化

次のトピックでは、Cisco DNA Center 2.3.5 に基づく LAN 自動化プロビジョニングに関する情報を提供します。手順と例は、以降のバージョンでは異なる場合があります。

お使いの Cisco DNA Center バージョンの LAN 自動化設定および関連機能の詳細については、[Cisco DNA Center ドキュメント](#)ポータルの『*Cisco DNA Center User Guide*』を参照してください。

LAN 自動化のプロビジョン

LAN 自動化の開始と停止

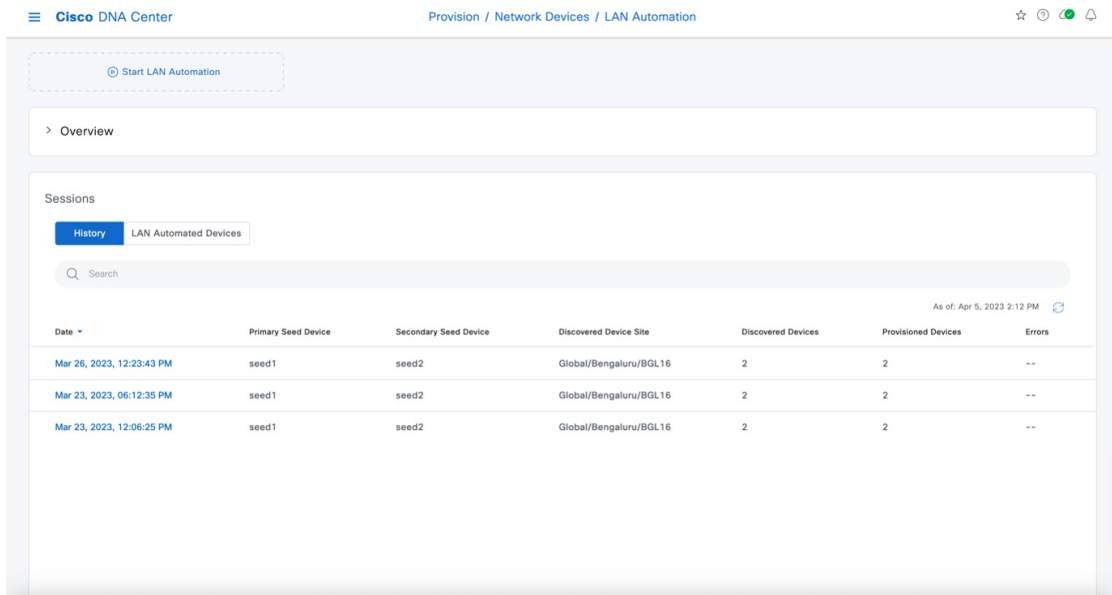
始める前に

次のトピックでは、Cisco DNA Center 2.3.5 に基づく LAN 自動化手順について説明します。手順は、Cisco DNA Center バージョンによって異なる場合があります。

手順

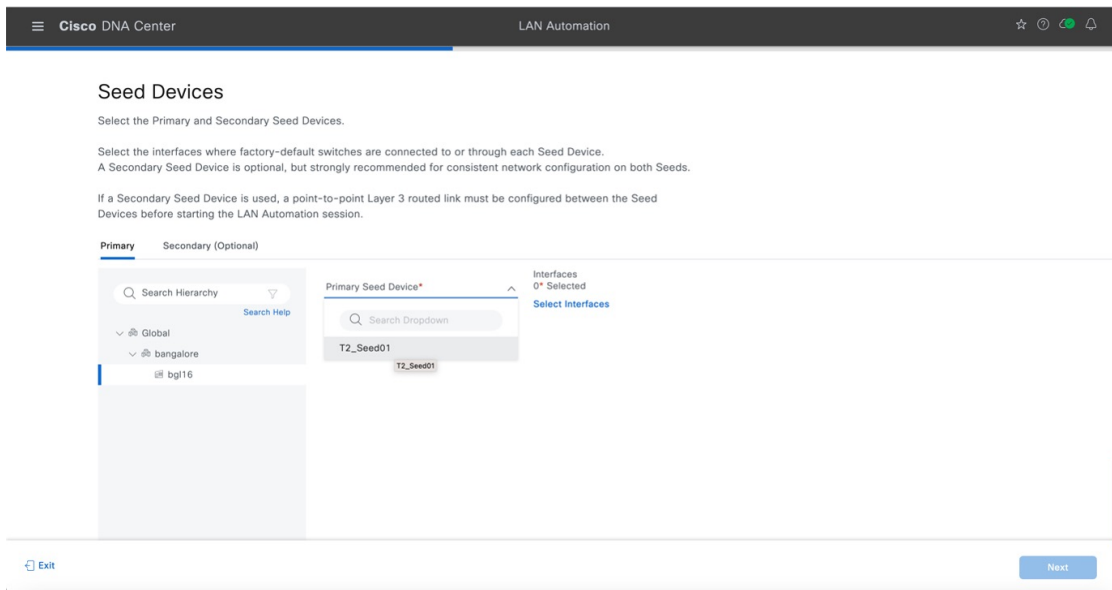
ステップ1 メニューアイコン (☰) をクリックして、[Provision] > [LAN Automation]。

ステップ2 [LAN Automation] ウィンドウで、[Start LAN Automation] をクリックします。



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

- [Primary Seed Device] とプラグアンドプレイ (PnP) インターフェイスを選択します。
- (オプション) [Secondary Seed Device] と PnP インターフェイスを選択します。



インターフェイスを選択するには、[Select Interfaces] ウィンドウでインターフェイスを選択し、[Add Selected] をクリックします。



Select Interfaces

Select Primary Seed Device Interfaces.

Add All		Remove All	
50 Unselected		2 Selected	
INTERFACE STATUS: UP		INTERFACE STATUS: UP	
<input type="checkbox"/>	GigabitEthernet1/0/1	<input checked="" type="checkbox"/>	GigabitEthernet1/0/3
<input type="checkbox"/>	GigabitEthernet1/0/7	INTERFACE STATUS: DOWN	
INTERFACE STATUS: DOWN		<input checked="" type="checkbox"/>	GigabitEthernet1/0/13
<input type="checkbox"/>	GigabitEthernet1/0/10		
<input type="checkbox"/>	GigabitEthernet1/0/11		
<input type="checkbox"/>	GigabitEthernet1/0/12		
<input type="checkbox"/>	GigabitEthernet1/0/14		
<input type="checkbox"/>	GigabitEthernet1/0/15		
<input type="checkbox"/>	GigabitEthernet1/0/16		
<input type="checkbox"/>	GigabitEthernet1/0/17		

Cancel

Select

ステップ 4 [Sessions Attributes] ウィンドウで、[Principal IP Address Pool] を選択し、必要に応じてその他の詳細を追加します。

Session Attributes

Select the Site where Discovered Devices will be assigned.
The available IP Address pools are based on the Discovered Device Site.
Advanced Session Attributes, and a Hostname Prefix are optional.

Discovered Devices Site

<input type="text" value="Search Hierarchy"/>	Principal IP Address Pool*	Link Overlapping IP Pool
<input type="text" value="Lan"/>	<input type="text" value="Lan"/>	<input type="text" value=""/>
<input type="text" value="IS-IS Domain Password (Optional)"/>	<input type="text" value=""/>	
<input checked="" type="checkbox"/> Enable Multicast	<input type="checkbox"/> Advertise LAN Automation Routes into BGP	

HOSTNAME MAPPING

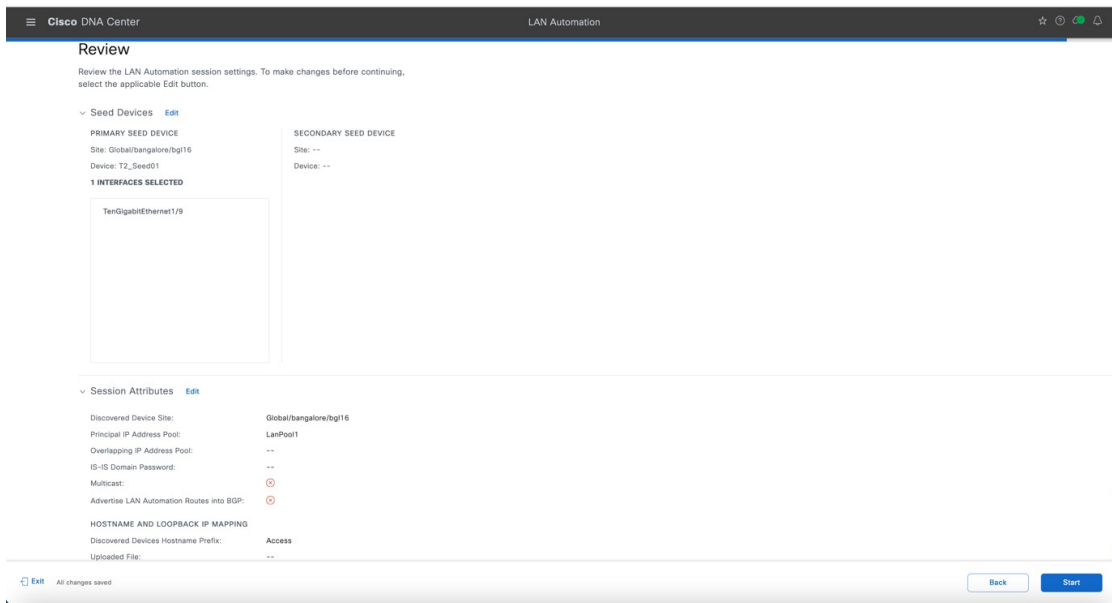
Discovered Devices Hostname Prefix

Choose a File

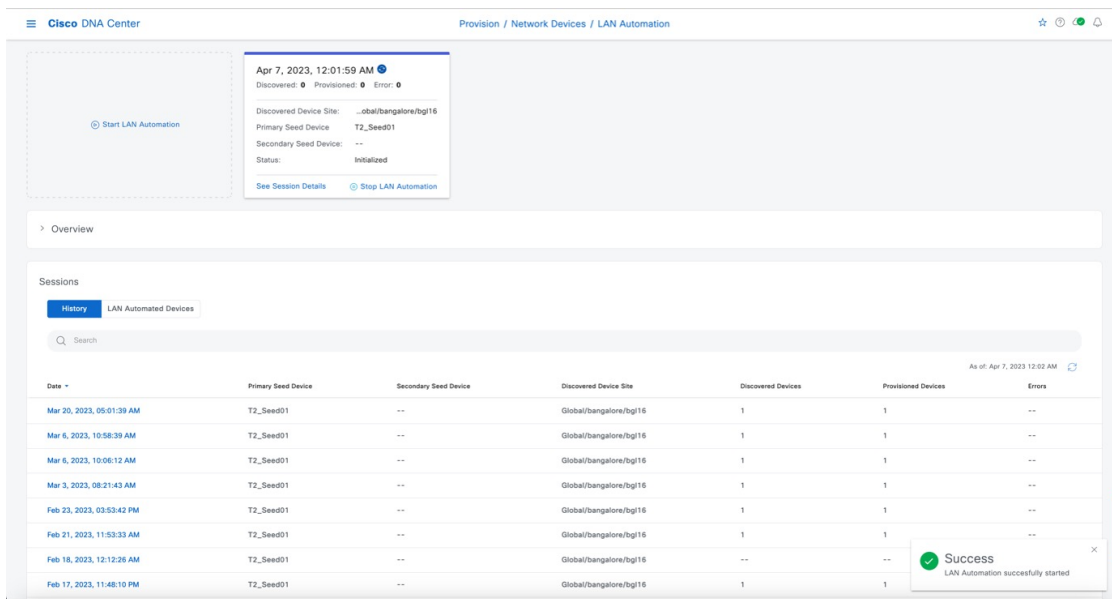
All changes saved

ステップ 5 [レビュー (Review)] をクリックします。

ステップ 6 設定を確認したら、[Start] をクリックして LAN 自動化を開始します。



LAN 自動化セッションが作成され、そのセッションのタイトルが [LAN 自動化] ウィンドウに表示されます。



セッションの詳細を表示するには、タイトルの [See Session Details] をクリックします。セッションのログを表示するには、セッションの詳細ウィンドウで [View Session Logs] をクリックします。

[LAN Automated Devices] タブには、LAN 自動デバイスの詳細が表示されます。検索フィールドを使用して、特定のテキストに基づいてデータをフィルタ処理できます。データをフィルタ処理するには、次のトグルボタンのいずれかをクリックします。

- [Seed Devices] : シードデバイスのデータを表示します。
- [Discovered] : 検出されたデバイスのデータを表示します。

- [Provisioned] : プロビジョニングされたデバイスのデータを表示します。
- [Error] : エラーのあるデバイスのデータを表示します。

The screenshot shows the Cisco DNA Center interface for LAN Automation. At the top, it displays 'Cisco DNA Center' and 'Provision / Network Devices / LAN Automation'. Below this, there's a summary for the current session: 'LAN Automation / Apr 7, 2023 12:01:59 AM', 'Stop LAN Automation' button, 'Status: In Progress', 'Discovered Device Site: Global/bangalore/bg16', 'Primary Seed Device: T2_Seed01 (192.0.2.1)', and 'Secondary Seed Device: --'. A 'View Session Logs' link is also present. Under 'View By', there are filters for 'Seed Devices: 1', 'Discovered: --', 'Provisioned: 1', and 'Error: --'. A search bar for devices is provided. Below the search bar, there are options to 'Add Link', 'Delete Link', and 'Edit Device'. A table of devices is shown with columns: 'Device Name', 'IP Address', 'Platform', 'Serial Number', and 'Status'. One device is listed: 'Access-4' with IP '172.16.0.1', Platform 'C9300-24T', and Serial Number 'FCW23110150'. The status is 'Provisioned' with a green progress bar. At the bottom, it shows '1 Records' and 'Show Records: 25'.

セッションの LAN 自動化を停止するには、タイトルの [Stop LAN Automation] をクリックします。

The screenshot shows the Cisco DNA Center interface for LAN Automation, specifically the 'Sessions' tab. At the top, it displays 'Cisco DNA Center' and 'Provision / Network Devices / LAN Automation'. Below this, there's a summary for the current session: 'Apr 7, 2023, 12:01:59 AM', 'Discovered: 0', 'Provisioned: 1', and 'Error: 0'. A 'Start LAN Automation' button is visible. Below the summary, there's a 'See Session Details' link and a 'Stop LAN Automation' button. The main content area shows 'Overview' and 'Sessions'. Under 'Sessions', there are tabs for 'History' and 'LAN Automated Devices'. A search bar is provided. Below the search bar, there's a table of sessions with columns: 'Date', 'Primary Seed Device', 'Secondary Seed Device', 'Discovered Device Site', 'Discovered Devices', 'Provisioned Devices', and 'Errors'. The table contains several rows of session data, including dates from Feb 17, 2023, to Mar 20, 2023, and various seed devices and device counts.

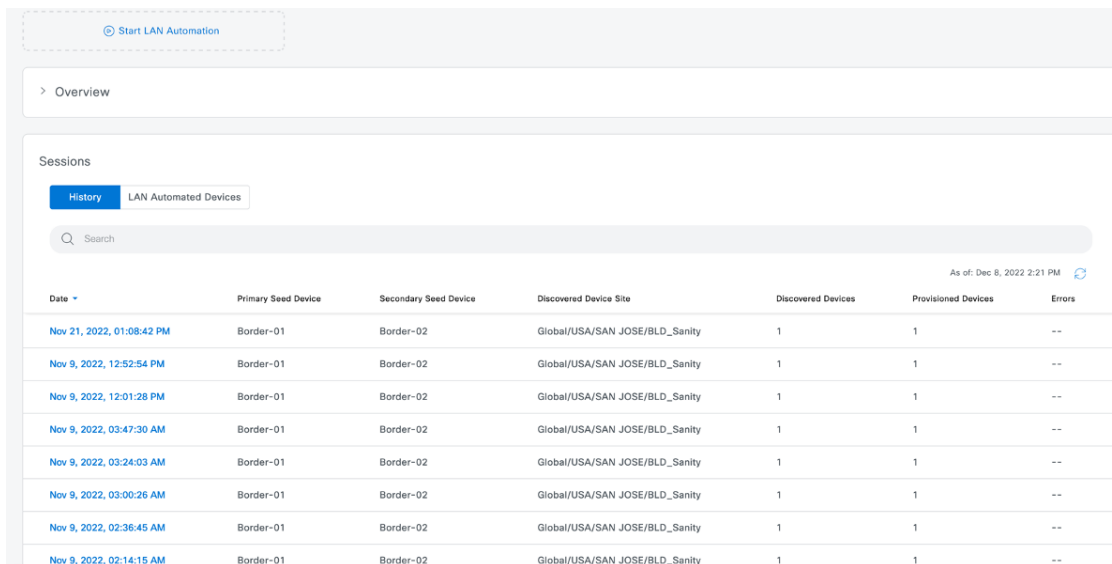
[History] タブには、ネットワーク内の LAN 自動化セッションの履歴が表示されます。検索フィールドを使用して履歴内の特定のテキストを検索できます。セッションの詳細を表示するには、ハイパーリンクが設定された日付をクリックします。

デバイスのログと構成を確認する

LAN 自動化セッションログ、デバイス固有のログ、およびデバイスにプッシュされた構成を表示します。

手順

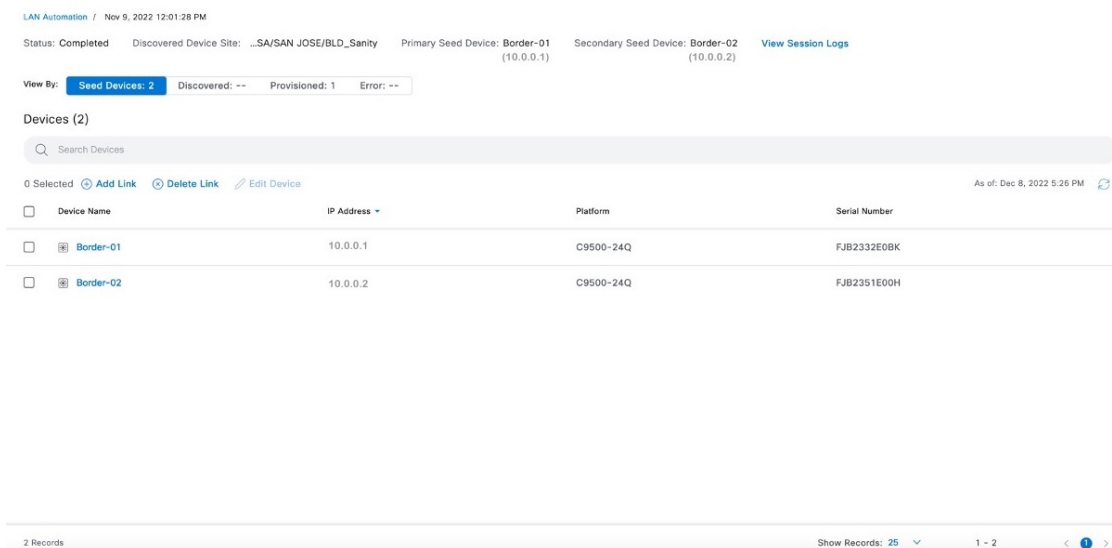
ステップ 1 [LAN Automation] ウィンドウで、[Sessions] 領域の [History] タブをクリックし、ハイパーリンクされた日付をクリックしてセッションの詳細を表示します。



The screenshot shows the 'Sessions' section of the LAN Automation interface. It features a 'History' tab and a search bar. Below is a table with columns for Date, Primary Seed Device, Secondary Seed Device, Discovered Device Site, Discovered Devices, Provisioned Devices, and Errors. The table contains eight rows of session data.

Date	Primary Seed Device	Secondary Seed Device	Discovered Device Site	Discovered Devices	Provisioned Devices	Errors
Nov 21, 2022, 01:08:42 PM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--
Nov 9, 2022, 12:52:54 PM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--
Nov 9, 2022, 12:01:28 PM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--
Nov 9, 2022, 03:47:30 AM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--
Nov 9, 2022, 03:24:03 AM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--
Nov 9, 2022, 03:00:26 AM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--
Nov 9, 2022, 02:36:45 AM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--
Nov 9, 2022, 02:14:15 AM	Border-01	Border-02	Global/USA/SAN JOSE/BLD_Sanity	1	1	--

ステップ 2 セッションのログを表示するには、セッションの詳細ウィンドウで [View Session Logs] をクリックします。



The screenshot shows the 'View Session Logs' window for a specific session. It displays the session status as 'Completed' and provides details for the discovered device site, primary and secondary seed devices, and a link to view session logs. Below this, there is a 'View By' section showing 'Seed Devices: 2', 'Discovered: --', 'Provisioned: 1', and 'Error: --'. The main part of the window is a table titled 'Devices (2)' with columns for Device Name, IP Address, Platform, and Serial Number. Two devices are listed: Border-01 and Border-02.

Device Name	IP Address	Platform	Serial Number
<input type="checkbox"/> Border-01	10.0.0.1	C9500-24Q	FJB2332E0BK
<input type="checkbox"/> Border-02	10.0.0.2	C9500-24Q	FJB2351E00H

LAN Automation / Nov 9, 2022 12:01:28 PM

Status: Completed Discovered Device Site: ...SA/SAN JOSE/BLD_Sanity Primary Seed Device: B...

View By: Seed Devices: 2 Discovered: -- Provisioned: 1 Error: --

Devices (2)

0 Selected Add Link Delete Link Edit Device

Device Name	IP Address
Border-01	10.0.0.1
Border-02	10.0.0.2

2 Records

Session Log

Search Devices

As of: Dec 8, 2022 2:23 PM

Message	Timestamp
Device FOC2422U025, FOC2422W01Y is deleted from inventory.	Nov 9, 2022, 12:49:43 PM
Released subnet 192.0.2.1/31	Nov 9, 2022, 12:49:41 PM
Released subnet 192.0.2.2/31	Nov 9, 2022, 12:49:41 PM
Released Loopback address 192.0.2.3 for Device FOC2422U025, FOC2422W01Y (STK).	Nov 9, 2022, 12:49:41 PM
Completed LAN Automation.	Nov 9, 2022, 12:28:31 PM
Completed Final Resync.	Nov 9, 2022, 12:28:31 PM
Starting Final Resync for Devices.	Nov 9, 2022, 12:27:11 PM
Releasing SVI subnet: 192.0.2.192/26	Nov 9, 2022, 12:27:11 PM
Completed Device Cleanup.	Nov 9, 2022, 12:27:11 PM
Waiting for Device Cleanup to complete.	Nov 9, 2022, 12:27:01 PM
Starting Device Cleanup.	Nov 9, 2022, 12:27:01 PM

44 Records Show Records: 25 1 - 25

ステップ3 デバイス固有のログと構成を表示するには、セッションの詳細ウィンドウでデバイス名をクリックします。トグルボタンを使用して、デバイスをフィルタリングします。デバイスの詳細が表示されます。

Border-01 (Primary Seed)

Device Model: Cisco Catalyst 9500 Series Switches Site: Global/USA/SAN JOSE/BLD_Sanity Primary Seed Device: Border-01 (10.0.0.1) Secondary Seed Device: Border-02 (10.0.0.2)

DETAILS

Session Attributes

Interfaces

Configuration Logs

Primary Seed Configs

Secondary Seed Configs

Discovered Device Configs

Session Logs

Primary Seed Logs

Secondary Seed Logs

Discovered Device Logs

Session Logs

Discovered Device Site: Global/USA/SAN JOSE/BLD_Sanity

Primary Seed: Border-01

Secondary Seed: Border-02

Primary Interfaces: FortyGigabitEthernet1/0/3

IP Pool: --

Link Overlapping IP Pool: --

Multicast:

Advertise LAN Automation Routes into BGP:

HOSTNAME AND LOOPBACK IP MAPPING

Device Prefix: --

Uploaded File: halleck_lo0_LAN_single.csv

ステップ4 デバイスにプッシュされた設定を表示するには、左側のペインで[Configuration Log]を展開し、デバイス設定を選択します。

Border-01 (Primary Seed) ✕

Device Model: Cisco Catalyst 9500 Series Switches | Site: Global/USA/SAN JOSE/BLD_Sanity | Primary Seed Device: Border-01 (10.0.0.1) | Secondary Seed Device: Border-02 (10.0.0.2)

DETAILS

- Session Attributes
- Interfaces
- Configuration Logs
 - Primary Seed Configs
 - Secondary Seed Configs
 - Discovered Device Configs
- Session Logs
 - Primary Seed Logs
 - Secondary Seed Logs
 - Discovered Device Logs
 - Session Logs

Primary Seed Configs

- L3 Delete Link Configuration for Interface FortyGigabitEthernet1/0/3 Nov 9, 2022, 12:49:42 PM


```

default interface FortyGigabitEthernet1/0/3
#INTERACTIVE
do write memory <IQ>confirm<R>y
#ENDS_INTERACTIVE

```
- DHCP Delete Configuration Nov 9, 2022, 12:27:02 PM
- SVI Delete Configuration Nov 9, 2022, 12:27:01 PM
- L3 Create Link Configuration for Interface FortyGigabitEthernet1/0/3 Nov 9, 2022, 12:26:43 PM
- SVI Create Configuration Nov 9, 2022, 12:01:33 PM
- DHCP Create Configuration Nov 9, 2022, 12:01:33 PM

STK (Discovered Device) ✕

Device Model: Cisco Catalyst 9300 Series Switches | Site: Global/USA/SAN JOSE/BLD_Sanity | Primary Seed Device: Border-01 (10.0.0.1) | Secondary Seed Device: Border-02 (10.0.0.2)

DETAILS

- Session Attributes
- Interfaces
- Configuration Logs
 - Primary Seed Configs
 - Secondary Seed Configs
 - Discovered Device Configs
- Session Logs
 - Primary Seed Logs
 - Secondary Seed Logs
 - Discovered Device Logs
 - Session Logs

Discovered Device Configs

- SVI Delete Configuration Nov 9, 2022, 12:27:01 PM


```

interface Vlan 1
no ip router isis
no cns mtu
no ip address
no bfd interval 500 min_rx 500 multiplier 3
ip redirects
no pnp profile pnp-zero-touch
#INTERACTIVE
no crypto pki trustpoint pnplabel<IQ>Are you sure you want to do this<R>yes
#ENDS_INTERACTIVE
#INTERACTIVE
do write memory <IQ>confirm<R>y
#ENDS_INTERACTIVE.

```
- L3 Create Link Configuration for Interface TenGigabitEthernet2/1/5 Nov 9, 2022, 12:26:52 PM
- L3 Create Link Configuration for Interface TenGigabitEthernet1/1/7 Nov 9, 2022, 12:26:41 PM

ステップ 5 デバイス固有のログを表示するには、左側のペインで [Session Logs] を展開し、デバイスログを選択します。

Border-01 (Primary Seed) ×

Device Model: Cisco Catalyst 9500 Series Switches | Site: Global/USA/SAN JOSE/BLD_Sanity | Primary Seed Device: Border-01 (10.0.0.1) | Secondary Seed Device: Border-02 (10.0.0.2)

DETAILS

- Session Attributes
- Interfaces
- Configuration Logs
 - Primary Seed Configs
 - Secondary Seed Configs
 - Discovered Device Configs
- Session Logs
 - Primary Seed Logs**
 - Secondary Seed Logs
 - Discovered Device Logs
 - Session Logs

Message	Timestamp
Completed Resync for Device FJB2332E0BK.	Nov 9, 2022, 12:50:03 PM
Sending Resync Message for Device FJB2332E0BK.	Nov 9, 2022, 12:49:53 PM
Completed Resync for Device FJB2332E0BK.	Nov 9, 2022, 12:28:31 PM
Sending Resync Message for Device FJB2332E0BK.	Nov 9, 2022, 12:27:11 PM
Generated DHCP Delete configuration for device FJB2332E0BK	Nov 9, 2022, 12:27:02 PM
Generated SVI Delete configuration for device FJB2332E0BK	Nov 9, 2022, 12:27:01 PM
Configuring L3 Link for Port FortyGigabitEthernet1/0/3 of Device FJB2332E0BK.	Nov 9, 2022, 12:26:43 PM
Completed Resync for Device FJB2332E0BK.	Nov 9, 2022, 12:26:40 PM

17 Records Show Records: 25 1 - 17

STK (Discovered Device) ×

Device Model: Cisco Catalyst 9300 Series Switches | Site: Global/USA/SAN JOSE/BLD_Sanity | Primary Seed Device: Border-01 (10.0.0.1) | Secondary Seed Device: Border-02 (10.0.0.2)

DETAILS

- Session Attributes
- Interfaces
- Configuration Logs
 - Primary Seed Configs
 - Secondary Seed Configs
 - Discovered Device Configs
- Session Logs
 - Primary Seed Logs
 - Secondary Seed Logs
 - Discovered Device Logs**
 - Session Logs

Message	Timestamp
Device FOC2422U025, FOC2422W01Y is deleted from inventory.	Nov 9, 2022, 12:49:43 PM
Released Loopback address 192.0.2.1 for Device FOC2422U025, FOC2422W01Y (STK).	Nov 9, 2022, 12:49:41 PM
Completed Resync for Device FOC2422U025, FOC2422W01Y.	Nov 9, 2022, 12:28:31 PM
Sending Resync Message for Device FOC2422U025, FOC2422W01Y.	Nov 9, 2022, 12:27:11 PM
Performing Cleanup for Device FOC2422U025, FOC2422W01Y.	Nov 9, 2022, 12:27:01 PM
Generated SVI Delete configuration for device FOC2422U025, FOC2422W01Y	Nov 9, 2022, 12:27:01 PM
Configuring L3 Link for Port TenGigabitEthernet2/1/5 of Device FOC2422U025, FOC2422W01Y.	Nov 9, 2022, 12:26:52 PM
Configuring L3 Link for Port TenGigabitEthernet1/1/7 of Device FOC2422U025, FOC2422W01Y.	Nov 9, 2022, 12:26:41 PM

22 Records Show Records: 25 1 - 22

インターフェイス間のリンクの作成

LAN 自動化が停止した後、インターフェイス間の追加リンクを設定します。

始める前に

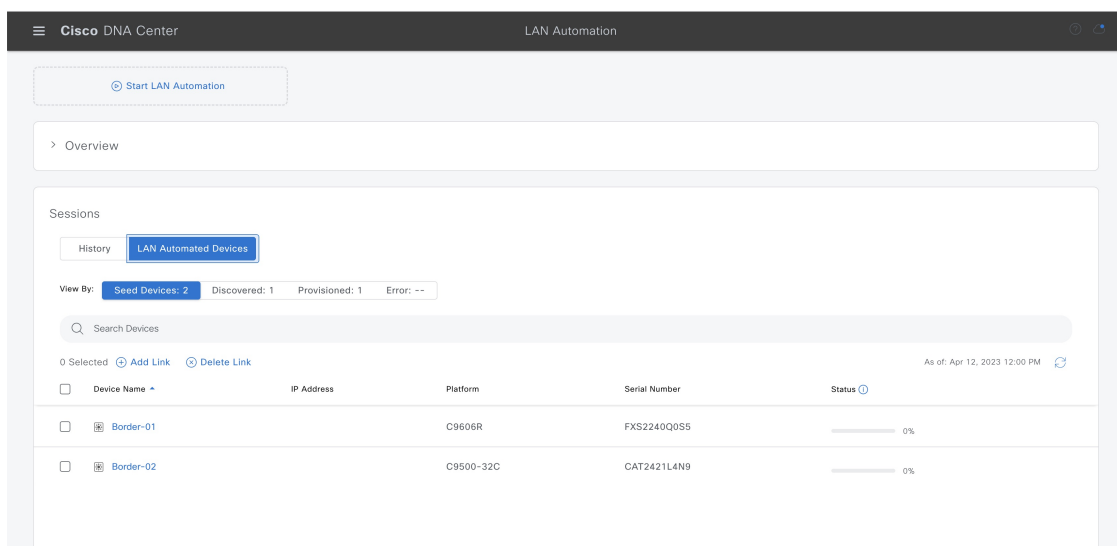
次のトピックでは、Cisco DNA Center 2.3.5 に基づいてインターフェイス間の追加リンクを設定する手順について説明します。手順は、Cisco DNA Center バージョンによって異なる場合があります。

手順

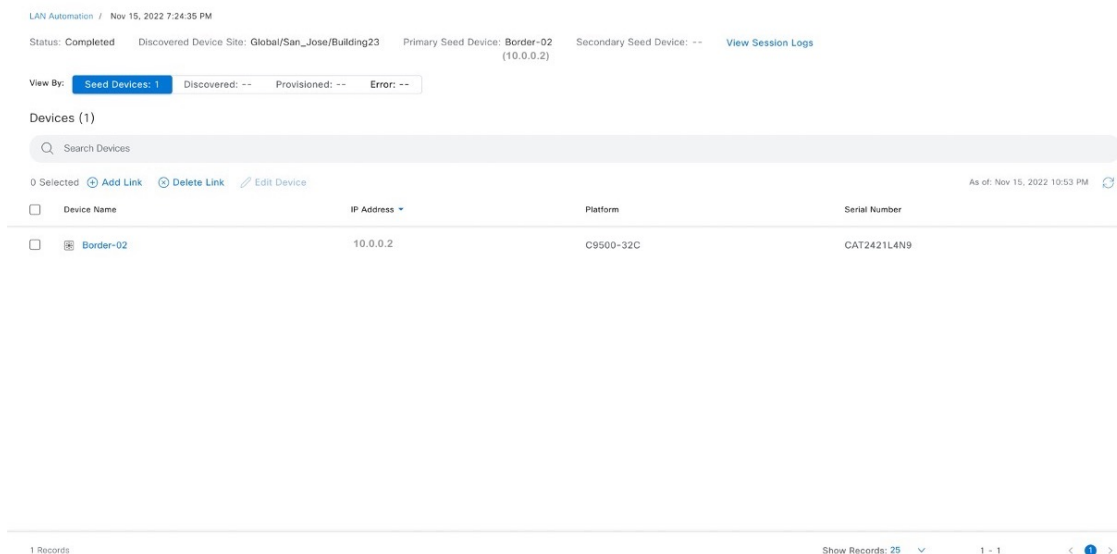
ステップ 1 メニューアイコン (☰) をクリックして、**[Provision] > [LAN Automation]**。

ステップ 2 次のいずれかのオプションを使用します。

- オプション 1 : [LAN Automation] ウィンドウの [LAN Automation Devices] タブで、[Add Link] をクリックします。



- オプション 2 : [History] タブで、セッションの日付をクリックしてセッションの詳細を表示し、[Add Link] をクリックします。



ステップ 3 [Add Link] のワークフローで次の手順に従います。

- a) リンクを確立する 2 つのデバイスを選択します。

Select Devices

Select the two devices where an additional interface will be provisioned using LAN Automation.
Note: Only devices in Reachable and Managed state in inventory are eligible for Link Addition.

● Device 1 ● Device 2

Search Hierarchy Search Help

- Global
- San_Jose
 - Building18
 - Building23

Device*
Border-01

Exit Next

- b) LAN 内の IP アドレスプールを選択します。IP アドレスプールが Cisco DNA Center から到達可能であることを確認します。

Select IP Address Pool

all pools with LAN are shown.

DEVICE 1
Border-01

DEVICE 2
Border-02

IP Address Pool*
Global/San_Jose(group-192net-lan... ▼

Exit All changes saved Back Next

- c) 接続を確立する両方のデバイスのインターフェイスを選択します。

Select Interface - Device 1

Select the interface on the first device.

This interface cannot currently have an IP Address or be bundled in a Port-Channel.

Link 1

Device 1 Interface: FortyGigabitEthernet1/0/11
Device 2 Interface: --

● Available Interface ● Selected Interfaces ○ Unavailable Interface

DEVICE 1
Border-01

Exit All changes saved Back Next

Select Interface - Device 2

Select the interface on the first device.

This interface cannot currently have an IP Address or be bundled in a Port-Channel.

Link 1

Device 1 Interface: FortyGigabitEthernet1/0/11
Device 2 Interface: HundredGigE1/0/11

● Available Interface ● Selected Interfaces ○ Unavailable Interface

DEVICE 2
Border-02

Exit All changes saved Back Next

- d) [Now] か [Later] をクリックし、リンクをプロビジョニングするタイミングを指定します。表示されるフィールドにタスクの名前を入力します。

Schedule Add Link Task

Specify the schedule details to begin the add link task.

Now Later

Task Name*

Add Link

[Exit](#) All changes saved

[Back](#)

[Next](#)

- e) [Summary] ウィンドウで、設定を確認します。変更するには、[Edit] をクリックします。

Summary

Review the link to be added and scheduler details. Click edit if you wish to make changes.

Review Link [Edit](#)

DEVICE 1

Border-01

INTERFACE

FortyGigabitEthernet1/0/11

DEVICE 2

Border-02

INTERFACE

HundredGigE1/0/11

Schedule Your Task [Edit](#)

Scheduler: Run Now

[Exit](#) All changes saved

[Back](#)

[Start Add Link](#)

- f) [Start Add Link] をクリックします。

[Link Configuration Started Successfully] ウィンドウが表示されます。

ステップ 4 設定のステータスを表示するには、[View Status in Activities] をクリックします。

次のタスク

リンクを削除するには、次の手順を実行します。

- [Delete link] をクリックします。

- デバイスとインターフェイスを選択します。
- [Start Delete Link] をクリックします。

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2022 Cisco Systems, Inc. All rights reserved.

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

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

翻訳について

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