ネットワークのプロビジョニング

プロビジョニング

Cisco DNA Center でネットワークのポリシーを設定した後に、デバイスをプロビジョニングできます。この段階で、デバイスにオンボードし、デバイス間にポリシーを導入します。

プロビジョニングデバイスには、次の側面が含まれます。

- プラグ アンド プレイでのデバイスのオンボーディングと、デバイスのインベントリへの追加。
- 必要な設定とポリシーのインベントリ内デバイスへの展開。
- デバイスのサイトへの追加。
- ファブリック ドメインの作成とデバイスのファブリックへの追加。

Cisco DNA Center プロビジョニングでは IBNS 2.0 のみをサポートしています。これにより AAA 設定が変更され、関連するすべての認証コマンドがクラスベースのポリシー言語（CPL）制御ポリシーの対応するコマンドに変換されます。CPL 変換では、変換 CLI **authentication display [legacy|new-style]** が無効になるため、現在の設定をバックアップしておくことを推奨します。また、IBNS 2.0 に合わせた AAA 設定の更新をサポートするように変更管理期間を設定してください。

プラグ アンド プレイ プロビジョニングを使用したオンボードデバイス

プラグ アンド プレイ プロビジョニングは、最小限のネットワーク管理者およびフィールド担当者の関与で、新しいネットワーク デバイスを自動的かつリモートにプロビジョニングおよびオンボードする方法を提供します。

プラグ アンド プレイ プロビジョニングを使用すると、次の操作を実行できます。

- サイトの割り当て、サイト設定の展開、デバイス ソフトウェア イメージのインストール、およびカスタム オンボード設定の適用によって、デバイスをプロビジョニングする。
- インストールの前に、デバイス情報を入力し、プロビジョニング操作を選択してデバイスを計画します。デバイスはオンラインになると Cisco DNA Center に接続します。次に、デバイスのプロビジョニングとオンボーディングが自動で実行されます。
- 事前の計画なしにネットワーク上に表示される新しいデバイスである、要求されていないネットワーク デバイスをプロビジョニングします。
- Cisco スマート アカウントの Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリをプラグ アンド プレイに同期して、すべてのデバイスが Cisco DNA Center に表示されるようにします。
- ネットワーク デバイスの詳細なオンボーディング ステータスを表示します。

前提条件

プラグ アンド プレイ プロビジョニングを使用する前に、次の操作を実行します。

- メインの Cisco DNA Center の設定で、[System Settings] > [Settings] > [Cisco Credentials] を使って、シスコのログイン情報を設定します。詳細については、「Cisco Digital Network Architecture Center 管理者ガイド」の 「*Cisco* クレデンシャルの設定」 を参照してください。
- [System Settings] > [Settings] > [Device EULA Acceptance]を使用して、メインの Cisco DNA Center の設定でエンドユーザ ライセンス契約（EULA）に同意します。詳細については、*Cisco Digital Network Architecture Center* 管理者ガイド [英語] の 「Accept the License Agreement」を参照してください。
- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『 Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド [英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。

ここでは、プラグアンドプレイプロビジョニングの一般的な使用例とワークフローについて説明します。

計画されたプロビジョニング

管理者は、次のように新しいサイトまたはその他のネットワーク デバイス グループのプロビジョニングを計画できます。

1. ネットワーク階層内のサイトを定義します。About Network Hierarchyを参照してください。
2. 必要に応じて、デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。多くの場合、Day 0 設定をカスタマイズする必要がない限り、このようなテンプレートは必要ありません。デバイス設定の変更を自動化するテンプレートの作成 を参照してください。
3. 展開するデバイスのタイプについて、ネットワーク プロファイルを定義します。ネットワークプロファイルの作成 を参照してください。
4. 展開するデバイスのデバイスログイン情報（CLIおよびSNMP）を定義します。デバイス クレデンシャルについて を参照してください。
5. 必要に応じて、プロビジョニングするデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェア イメージのインポートを参照してください。
6. CSV ファイルを使用して一度にまたは一括で、計画したデバイスに関する詳細を追加します。デバイスの追加または編集 （10 ページ）またはデバイスの一括追加 （12 ページ）を参照してください。
7. デバイスが起動し、自動的にプロビジョニングされます。

要求されていないプロビジョニング。

計画前に新しいネットワーク デバイスをネットワークに追加すると、このネットワーク デバイスは要求のないデバイスとしてラベル付けされます。要求のないデバイスは、管理者が手動で追加することも、コントローラ ディスカバリの前提条件 （4 ページ） で説明されているいずれかの検出方法を使用して自動的に追加することもできます。管理者は、次の方法でデバイスをプロビジョニングできます。

1. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。デバイスの表示 （8 ページ） を参照してください。
2. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。プラグアンドプレイ対応デバイスのプロビジョニング （15 ページ） を参照してください。

Cisco スマート アカウントの同期およびプロビジョニング

ネットワーク デバイスは、シスコのプラグ アンド プレイ接続クラウド サービスによって Cisco スマート アカウントを通じて自動的に登録されます。管理者は Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。これにより、すべてのデバイスが Cisco DNA Center に表示されます。次に、これらのデバイスを要求してプロビジョニングすることができます。

1. スマートアカウントと同期するバーチャルアカウントを登録して同期します。バーチャル アカウント プロファイルの登録または編集 （13 ページ） を参照してください。
2. スマート アカウントからデバイス インベントリを同期します。スマート アカウントからのデバイスの追加 （14 ページ）を参照してください。
3. 要求のないデバイスでフィルタリングするか、名前で検索して、デバイス リストのデバイスを検索します。デバイスの表示 （8 ページ） を参照してください。
4. サイト、イメージ、設定テンプレート、またはプロファイルを割り当てて、デバイスを要求します。プラグアンドプレイ対応デバイスのプロビジョニング （15 ページ） を参照してください。
5. デバイスが起動し、自動的にプロビジョニングされます。

コントローラ ディスカバリの前提条件

プラグ アンド プレイによってデバイスのオンボーディングが自動化されます。デバイスは、Cisco DNA Centerコントローラを検出して接続できるようにする必要があります。デバイスは、次のいずれかの方法でコントローラを自動的に検出できるようにする必要があります。

- DHCP：DHCP コントローラ ディスカバリ （4 ページ）を参照してください。
- DNS：DNS コントローラ ディスカバリ （6 ページ）を参照してください。
- Cisco Plug and Play Connect クラウドサービス：Plug and Play Connect コントローラ ディスカバリ （6 ページ）を参照してください。

DHCP コントローラ ディスカバリ

シスコのネットワークデバイスは初回起動時にスタートアップ設定を使用しない場合、DHCP オプション 43 を使用して Cisco DNA Center コントローラの検出を試行します。

DHCP による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- DHCP サーバが Cisco Plug and Play のオプション 43 を使用して設定されている。このオプションにより、Cisco DNA Center コントローラの IP アドレスを持つネットワークデバイスが通知されます。

  DHCP サーバが文字列「ciscopnp」を含むオプション 60 を使用してデバイスから DHCP の検出メッセージを受信すると、オプション 43 の情報を含む応答をデバイスに返します。

デバイスの Cisco Plug and Play IOS エージェントは、応答から Cisco DNA Center コントローラの IP アドレスを抽出し、このアドレスを使用してコントローラと通信します。

DHCP オプション 43 は、DHCP サーバとして機能する Cisco ルータ CLI で、次のように設定された文字列の値で構成されます。

```
ip dhcp pool pnp_device_pool         <-- Name of DHCP pool
network 192.168.1.0 255.255.255.0    <-- Range of IP addresses assigned to clients
default-router 192.168.1.1           <-- Gateway address
option 43 ascii "5A1N;B2;K4;I172.19.45.222;J80"    <-- Option 43 string
```

このオプション 43 の文字列には、セミコロンで区切られた次のコンポーネントが含まれています。

- 5A1N;（プラグ アンド プレイ用の DHCP サブオプション、アクティブ動作、バージョン 1、デバッグ情報なし）。文字列のこの部分は変更する必要がありません。
- B2;（IP アドレスのタイプ）：
  - B1 = ホスト名
  - B2 = IPv4（デフォルト）
- I*xxx.xxx.xxx.xxx*;：Cisco DNA Center コントローラの IP アドレスまたはホスト名（大文字の i の後）。この例では、IP アドレスは 172.19.45.222 です。
- J*xxxx*：Cisco DNA Center コントローラへの接続に使用するポート番号。この例では、ポート番号は 80 です。HTTP のデフォルトはポート 80、HTTPS のデフォルトはポート 443 です。
- K4;：デバイスとコントローラの間で使用されるトランスポート プロトコル。
  - K4 = HTTP（デフォルト）
  - K5 = HTTPS
- T*trustpoolBundleURL*：デフォルト（Cisco DNA Centerコントローラ）以外の別の場所から trustpool バンドルを取得する場合は、このオプション パラメータを使用して trustpool バンドルの外部 URL を指定します。APIC-EM コントローラは、Cisco InfoSec Cloud（http://www.cisco.com/security/pki/）からバンドルを取得します。たとえば、10.30.30.10 の TFTP サーバからバンドルをダウンロードするには、パラメータを「Ttftp://10.30.30.10/ios.p7b」と指定します。

  trustpool セキュリティを使用していて、T パラメータを指定しない場合、デバイスは Cisco DNA Center コントローラから trustpool バンドルを取得します。
- Z*xxx.xxx.xxx.xxx*;（NTP サーバの IP アドレス）。trustpool セキュリティを使用してすべてのデバイスを同期させる場合、このパラメータは必須です。

DHCP の設定の詳細については、『*Cisco IOS Command Reference*』を参照してください。

DHCP オプション 43 が設定されていない場合、デバイスが DHCP サーバに接続できない場合、またはこの方法が別の理由で失敗する場合は、ネットワークデバイスは DNS を使用して検出を試行します。詳細については、DNS コントローラ ディスカバリ （6 ページ）を参照してください。

DNS コントローラ ディスカバリ

DHCP ディスカバリが Cisco DNA Center コントローラの IP アドレスを取得できない場合、ネットワークデバイスは DNS ルックアップ方式にフォールバックします。DHCP サーバから返されたネットワークドメイン名に基づき、事前設定されたホスト名「pnpserver」を使用して、コントローラの完全修飾ドメイン名（FQDN）を作成します。NTP のサーバ名は、事前設定されたホスト名 pnpserver に基づいています。

たとえば、DHCP サーバからドメイン名「customer.com」が返された場合、ネットワークデバイスは「pnpserver.customer.com」というコントローラの FQDN を作成します。次に、この FQDN の IP アドレスを解決するために、ローカル ネーム サーバを使用します。NTP サーバ名の FQDN は pnpntpserver.customer.com です。

DNS による検出方法の前提条件は次のとおりです。

- 新しいデバイスが DHCP サーバにアクセスできる。
- Cisco DNA Center コントローラがホスト名「pnpserver」を使用して展開されている。
- NTP のサーバ名はホスト名「pnpserver」で展開される。

Plug and Play Connect コントローラ ディスカバリ

DHCP または DNS による検出方法の使用がオプションでない場合は、Cisco Plug and Play Connect クラウド サービスによって、デバイスが Cisco DNA Center コントローラの IP アドレスを検出できます。ネットワークデバイスが起動すると、DHCP または DNS を介してコントローラを特定できない場合に、devicehelper.cisco.com に接続して Plug and Play Connect を試行し、組織に定義されている適切なコントローラの IP アドレスを取得します。通信を保護するために、デバイスは Plug and Play Connec に接続するときに、最初に Cisco trustpool バンドルをダウンロードしてインストールします。

次の手順では、検出に Plug and Play Connect を使用して、Cisco Plug and Play でシスコのネットワークデバイスを展開する方法についての概要を説明します。

始める前に

シスコの各種ネットワークデバイスは、Cisco Plug and Play をサポートし、Cisco Plug and Play Connect クラウドサービスに接続している Cisco IOS イメージを実行しています。

ステップ 1 ネットワーク管理者は、Cisco スマートアカウントの Web ポータルにある Plug and Play Connect を使用して、組織に適した Cisco DNA Center コントローラのコントローラ プロファイルを設定します。詳細については、web ポータルのスマートアカウントのマニュアルを参照してください。

ステップ 2 Cisco Commerce Workspace（CCW）を介してプラグアンドプレイ ネットワークデバイスを注文した場合、Cisco スマートアカウントが注文に割り当てられていれば、Plug and Play Connect を使用してネットワークデバイスが自動的に登録されます。Cisco Plug and Play で使用する各デバイスに、NETWORK-PNP-LIC オプションを追加します。

このオプションにより、デバイスのシリアル番号と PID がプラグアンドプレイ用にスマート アカウントで自動登録されます。デフォルト コントローラを指定済みの場合、注文の処理時にデバイスがそのコントローラに自動的に割り当てられます。

ステップ 3 または、Plug and Play Connect の Web ポータルからデバイスを手動で追加することもできます。

ステップ 4 Cisco DNA Center を、Cisco Plug and Play Connect のコントローラとして、リダイレクト サービス用に Cisco スマート アカウントに登録します。バーチャル アカウント プロファイルの登録または編集 （13 ページ）を参照してください。

CCW を通してプラグアンドプレイ ネットワーク デバイスを注文し、これらのネットワークデバイスがスマートアカウント経由で Plug and Play Connect に自動登録される場合には、この手順が必須です。

ステップ 5 Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。

Plug and Play Connect の Web ポータルに登録されたデバイスがコントローラに同期され、SmartAccount のソースとともにプラグ アンド プレイのデバイス リストに表示されます。

ステップ 6 新しく同期されたデバイスを要求します。プラグアンドプレイ対応デバイスのプロビジョニング （15 ページ） を参照してください。

ステップ 7 デバイス インストーラによって、シスコ ネットワークデバイスがインストールされ、電源が投入されます。

ステップ 8 デバイスは、Plug and Play Connect サービスをクエリして Cisco DNA Center コントローラを検出し、Cisco DNA Center でプラグ アンド プレイのシリアル番号によってコントローラを識別します。次に、要求プロセス中に計画された内容に従ってプロビジョニングされます。

（注） デバイスが定義済みの NTP サーバ **time-pnp.cisco.com** または **pool.ntp.org** と同期できない場合、デバイスは Plug and Play Connect のコンタクトに失敗します。この問題を解決するには、これらの 2 つのホスト名への NTP トラフィックをブロック解除するか、これら 2 つの NTP ホスト名を DNS サーバのローカル NTP サーバ アドレスにマップします。

プラグアンドプレイ導入ガイド

プラグアンドプレイを使用する場合は、次の推奨事項に従ってください。

- デバイスの起動順序：一般に、ルーティングとアップストリームデバイスは最初に展開する必要があります。ルータおよびすべてのアップストリームデバイスがアップされてプロビジョニングされると、スイッチとダウンストリームデバイスを展開できます。デバイスのプラグ アンド プレイ エージェントは最初のデバイスの起動時のみ、Cisco DNA Center

コントローラの自動検出を試みます。現時点で、デバイスがコントローラに接続できない場合、デバイス プロビジョニングは失敗するため、アップストリーム デバイスは最初にプロビジョニングする必要があります。

- シスコのルータ トランク/アクセス ポートの設定：一般的なブランチ ネットワークには、ルータとスイッチが含まれます。1 つ以上のスイッチは WAN ルータに接続され、IP フォンやアクセス ポイントなどの他のエンドポイントはスイッチに接続します。スイッチがアップストリームルータに接続されると、次の導入モデルはプラグアンドプレイでサポートされます。
  - ダウンストリーム スイッチはルータのスイッチ ポートを使用してルータに接続されます。このタイプの接続では、ルータのスイッチ ポートをトランクまたはアクセス ポートとして設定できます。
  - ルータのルーテッド ポートを使用してダウンストリーム スイッチをルータに接続する。この場合、ルーテッド ポートはサブインターフェイスを使用して複数の VLAN をサポートできます。プラグアンドプレイのプロセス中、スイッチはそのポートを自動的にトランクポートとして設定します。大規模ブランチの場合は、ルータとダウンストリーム スイッチ間に複数の VLAN を設置する必要があります。このような使用例をサポートするには、スイッチをルーテッド ポートに接続する必要があります。
- 非 VLAN 1 設定：プラグアンドプレイは、VLAN 1 を使用して、デフォルトでデバイスをサポートします。1 以外の VLAN を使用するには、隣接するアップストリームデバイスでサポート対象のリリースが実行されていなければなりません。また、そのアップストリームデバイスに「**pnp startup-vlan** *x*」グローバル CLI コマンドを設定して、以降のプラグアンドプレイデバイスにこの CLI をプッシュする必要があります。隣接するアップストリーム デバイスでこのコマンドを実行した場合、そのアップストリーム デバイスでは VLAN メンバーシップの変更は行われません。ただし、アップストリームに接続された、以降のプラグアンドプレイデバイス上のアクティブインターフェイスは、指定された VLAN に変更されます。このガイドラインは、ルータとスイッチの両方に適用され、アクセスモードではなくトランクモードのシナリオでのみ使用する必要があります。

デバイスの表示

この手順では、プラグアンドプレイデバイスを表示する方法、デバイスでアクションを実行する方法、および新しいデバイスを追加する方法について説明します。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Devices] > [Plug and Play] の順に選択します。 > >

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 デバイスの名前をクリックします。

デバイスの詳細を示すウィンドウが表示されます。

ステップ 4 [Details]、[History]、[Configuration]、または [Stack] タブをクリックして、デバイスに関するさまざまな種類の情報を表示します。一部のタブには、クリックして詳細を表示できる追加のリンクがあります。

[スタック（Stack）] タブは、スイッチ スタック デバイスの場合にのみ表示されます。

ステップ 5 デバイスで特定のタスクを実行するには、ダイアログ ボックスの上部にある次のアクションをクリックします。使用可能なアクションは、デバイスの状態によって異なります。

- [Refresh]：デバイス状態情報を更新します。
- [Claim]：デバイスを要求しプロビジョニングします。プラグアンドプレイ対応デバイスのプロビジョニング （15 ページ） を参照してください。
- [Edit]：デバイスを編集します。デバイスの追加または編集 （10 ページ） を参照してください。
- [Reset]：デバイスがエラー状態になっている場合に、デバイスをリセットします。デバイスのリセット （24 ページ） を参照してください。
- [Delete]：デバイスを削除します。デバイスの削除 （24 ページ） を参照してください。

ステップ 6 複数のデバイスに対してアクションを実行するには、テーブルビューで各デバイスの横にあるチェックボックスをオンにし、[Actions] ドロップダウンメニューからアクションを選択します。

ステップ 7 [Add Device] をクリックして、新しいデバイスを追加します。

異なる方法でデバイスを追加する用法の詳細については、デバイスの追加または編集 （10 ページ）、デバイスの一括追加 （12 ページ）、または スマート アカウントからのデバイスの追加 （14 ページ） を参照してください。

デバイステーブルには、各デバイスについて、以下の表に示した情報が表示されます。すべての列はソートに対応しています。列ヘッダーをクリックすると、行が昇順にソートされます。列ヘッダーをもう一度クリックすると、行が降順にソートされます。

（注） デフォルトの列表示設定では一部の列が非表示になっています。これは、列の見出しの右端にある 3 つの点（ ⋮ ）をクリックするとカスタマイズできます。

表 *1*: デバイス情報

カラム	説明
#	行番号。
[Device Name]	デバイスのホスト名。このリンクをクリックすると、デバイスの詳細ウィンドウが開きます。スタックアイコンはスイッチスタックを示します。
[Serial Number]	デバイスのシリアル番号。
製品 ID	デバイスの製品 ID。

カラム	説明
[Source]	デバイスエントリの送信元： • [User]：ユーザが GUI または API を介してデバイスを追加しました。 • [Network]：コントローラに接続されたデバイスが要求解除されました。 • [SmartAccount]：デバイスはスマートアカウントから同期されました。
状態	• [Unclaimed]：デバイスはプロビジョニングされていません。 • [Planned]：デバイスはすでに要求されていますが、まだサーバと接続していません。 • [Onboarding]：デバイスオンボーディングが進行中です。 • [Provisioned]：デバイスは正常にオンボーディングされ、インベントリに追加されています。 • [Error]：デバイスにエラーがあり、プロビジョニングできませんでした。
オンボーディング状態	デバイスのオンボーディング状態。
[Site]	デバイスが関連付けられているサイト。
[Last Contact]	デバイスが最後にプラグ アンド プレイに接続した日時。
スマート アカウント	デバイスが関連付けられている Cisco スマート アカウント。
バーチャル アカウント	デバイスが関連付けられている（Cisco スマート アカウント内の）バーチャル アカウント。
[作成日時（Created）]	デバイスがプラグ アンド プレイに追加された日時。

デバイスの追加または編集

この手順では、[Plug and Play Devices] リストからデバイスを追加または編集する方法について説明します。代わりに、[編集（Edit）] をクリックしてデバイスの詳細ウィンドウからデバイスを編集することもできます。

表 2 : [デバイス（Device）] フィールド

フィールド	説明
[Serial Number]	デバイス シリアル番号（デバイスを編集している場合は読み取り専用）。
製品 ID	デバイス製品 ID（デバイスを編集している場合は読み取り専用）。
[Device Name]	デバイス名
SUDI 認証の有効化（Enable SUDI Authorization）	セキュアな固有デバイス識別子（SUDI）認証をサポートするデバイスで有効にします。
SUDI シリアル番号（SUDI Serial Numbers）	SUDI をサポートするデバイスには、シャーシのシリアル番号と SUDI シリアル番号（デバイス ラベルのライセンス SN と呼ばれる）の 2 つのシリアル番号があります。SUDI 認証を使用するデバイスを追加するときは、このフィールドに 1 つまたは複数の SUDI シリアル番号をカンマで区切って入力します。このフィールドは、[SUDI 認証の有効化（Enable SUDI Authorization）] がチェックされている場合にのみ表示されます。
このデバイスはスタックを表す（This Device Represents a Stack）	デバイスがスタックを表します（デバイスを編集している場合、この項目は読み取り専用です）。サポート対象のスタッカブル スイッチにのみ適用されます。

始める前に

デバイスにクレデンシャルが必要な場合は、グローバル デバイス クレデンシャルが [設計（Design）] > [ネットワーク設定（Network Settings）] > [デバイス クレデンシャル（Device Credentials）] ページで設定されていることを確認します。詳細については、グローバル CLI クレデンシャルの設定を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、[Provision] > [Devices] > [Plug and Play] > > の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 次のようにデバイスを追加または編集します。

- デバイスを追加するには、[Add Device] をクリックします。[Add Devices] ダイアログが表示されます。
- デバイスを編集するには、編集するデバイス名の横にあるチェック ボックスをオンにして、デバイス テーブルの上部にあるメニュー バーから [アクション（Actions）] > [編集（Edit）] をクリックします。**[デバイスの編集（Edit Device）]** ダイアログが表示されます。

ステップ 4 必要に応じてフィールドを設定します。詳細については上記の表を参照してください。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- デバイスを追加し、後で要求するには、[デバイスの追加（Add Device）] をクリックします。
- デバイスを追加し、すぐに要求するには、[追加＋要求（Add＋Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （15 ページ）、を参照してください。
- デバイスを編集する場合は、[デバイスの編集（Edit Device）] をクリックします。

デバイスの一括追加

この手順では、CSV ファイルからデバイスを一括で追加する方法を示します。

（注） プラグ アンド プレイにすでに存在するデバイスを追加する場合、既存のデバイスに対する変更はありません。

ステップ 1 Cisco DNA Centerのホームページで、[Provision] > [Devices] > [Plug and Play] > > の順に選択します。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 **[一括デバイス（Bulk Devices）]** タブをクリックします。

ステップ 4 **[ファイル テンプレートのダウンロード（Download File Template）]** をクリックしてサンプル ファイルをダウンロードします。

ステップ 5 各デバイスの情報をファイルに追加し、ファイルを保存します。デバイスタイプによっては、特定のフィールドが必須になることに注意してください。

ステップ 6 次のアクションのいずれかを実行して、CSV ファイルをアップロードします。

- ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップします。
- **[クリックして選択（click to select）]** が表示される場所をクリックしてファイルを選択します。

ステップ 7 **[デバイスのインポート（Import Devices）]** をクリックします。

CSV ファイル内のデバイスがテーブルにリストされます。

ステップ 8 インポートする各デバイスの横にあるチェックボックスをオンにするか、上部にあるチェックボックスをオンにしてすべてのデバイスを選択します。

ステップ 9 次のいずれかの操作を実行して、デバイスを追加します。

- デバイスを追加し、それらを後で要求するには、**[デバイスの追加（Add Devices）]** をクリックします。

- デバイスを追加し、それらをすぐに要求するには、[追加＋要求（Add＋Claim）] をクリックします。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （15 ページ）、を参照してください。

バーチャル アカウント プロファイルの登録または編集

この手順により、Cisco DNA Center コントローラを、リダイレクション サービス向けの Cisco スマート アカウントに、Cisco Plug and Play Connect のデフォルトのコントローラとして登録できます。また、これによって Cisco Plug and Play Connect クラウド ポータルから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

表 *3:* バーチャルアカウント フィールド

フィールド	説明
スマートアカウントの選択	Cisco スマート アカウント名
バーチャルアカウントの選択	バーチャルアカウント名バーチャルアカウントは、Cisco スマートアカウント内のサブアカウントです。
デフォルト コントローラ プロファイルとして使用	Cisco DNA Center コントローラを Cisco プラグアンドプレイ接続のクラウド ポータルにデフォルト コントローラとして登録するには、このボックスにチェックを付けます。
コントローラ IP または **FQDN**	この Cisco DNA Center コントローラの IP アドレスまたは完全修飾ドメイン名。
プロファイル名	コントローラのプロファイル名

始める前に

メインの Cisco DNA Center の設定で、[System] > [Settings] > [Smart Account] を使って、Cisco スマートアカウントのクレデンシャルを設定します。詳細については、『*Cisco Digital Network Architecture Center* 管理者ガイド』の「Configure Smart Account」 を参照してください。

ステップ 1 Cisco DNA Center のホームページで、**[System Settings]** > **[Settings]** > **[Cisco Credentials]**を選択します。

ステップ 2 [PnP Connect] タブをクリックします。

このテーブルには、登録されている Plug and Play Connect のバーチャル アカウント プロファイルがすべて一覧表示されます。

ステップ 3 次のように、バーチャル アカウント プロファイルを追加または編集します。

- バーチャルアカウントを登録するには、[追加（Add）] をクリックします。[register virtual account] ダイアログが表示されます。

- 登録済みのバーチャルアカウントプロファイルを編集するには、編集したいプロファイル名の横にあるラジオボタンをクリックし、テーブルの上にあるメニューバーの[プロファイルの編集（Edit Profile）]をクリックします。[バーチャル アカウントの編集（edit virtual account）]ダイアログが表示されます。

ステップ 4 上述の [Virtual Account Fields] テーブルを参照して、必要に応じてフィールドを設定します。

ステップ 5 次のいずれかの操作を実行して、設定を保存します。

- 新しいバーチャルアカウントプロファイルを登録する場合は、[登録（Register）]をクリックします。
- バーチャル アカウント プロファイルを編集する場合は、[変更（Change）] をクリックします。

次のタスク

Cisco Plug and Play Connect クラウド ポータルから、デバイス インベントリを Cisco DNA Center プラグ アンド プレイに同期します。詳細については、スマート アカウントからのデバイスの追加 （14 ページ）を参照してください。

スマート アカウントからのデバイスの追加

このタスクにより、Cisco Plug and Play Connect クラウド ポータルのスマート アカウントから Cisco DNA Center プラグ アンド プレイにデバイス インベントリを同期することができます。

バーチャル アカウント テーブルには、プロファイルごとに次の情報が表示されます。

表 *4:* バーチャル アカウント情報

カラム	説明
バーチャル アカウント	バーチャル アカウント名
スマート アカウント	バーチャル アカウントが関連付けられているスマート アカウント
同期ステータス	直近の同期プロセスのステータス

始める前に

Cisco プラグアンドプレイ接続クラウド ポータルからデバイスインベントリを同期する前に、バーチャルアカウントを登録する必要があります。バーチャル アカウント プロファイルの登録または編集 （13 ページ） を参照してください。

ステップ 1 Cisco DNA Center のホームページから、**[Provision]** > **[Devices]** > **[Plug and Play]**を選択します。

ステップ 2 [Add Device] をクリックします。

[デバイスの追加（Add Device）] ダイアログが表示されます。

ステップ 3 [スマートアカウントデバイス（Smart Account Devices）] タブをクリックします。

ステップ 4 デバイスを追加する Plug and Play Connect バーチャル アカウント プロファイルの名前の横にあるラジオ ボタンをクリックします。

ステップ 5 [同期（Sync）] をクリックして、このバーチャル アカウントの Cisco Plug and Play Connect から Cisco DNA Center プラグ アンド プレイに、デバイス インベントリを同期させます。

追加されたデバイスは、SmartAccount に設定されたソースとともに [プラグアンドプレイデバイス（Plug and Play Devices）] テーブルに表示されます。

次のタスク

新しく同期されたデバイスを要求します。デバイスの要求の詳細についてはプラグアンドプレイ対応デバイスのプロビジョニング （15 ページ）、を参照してください。

プラグアンドプレイ対応デバイスのプロビジョニング

デバイスのプロビジョニングまたは要求では、イメージとオンボーディングの設定をデバイスに展開するか、ワイヤレスデバイスのネットワークプロファイルを展開して、それをインベントリに追加してプロビジョニングします。デバイスの初起動を要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスをプロビジョニングするためのワークフローは、デバイスのタイプによって次のように異なります。

- スイッチとルータの参照資料： スイッチまたはルータ デバイスのプロビジョニング （15 ページ）
- ワイヤレス LAN コントローラ、アクセスポイント、センサの参照資料： ワイヤレスまたはセンサー デバイスのプロビジョニング （20 ページ）

スイッチまたはルータ デバイスのプロビジョニング

デバイスを要求すると、それをサイトに割り当て、イメージをインストールし、サイト設定とオンボーディングの設定を展開して、インベントリに追加することでプロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスが要求される場合、Cisco DNA Center からのシステム構成 CLI コマンドの一部はまずデバイスにプッシュされてから、定義した [Onboarding Configuration (Day-0)] テンプレートにプッシュされます。[Onboarding Configuration] テンプレートに同じ CLI コマンドがある場合、これらは最後に適用されるため、システム設定が上書きされます。システムによってプッシュされる CLI コマンドには、次のものがあります。

- デバイスのログイン情報（CLI および SNMP）
- SSH v2 および SCP サーバの有効化
- HTTP および HTTPS サーバの無効化

- スイッチでは、vtp モードの透過が有効になっています

（注） デバイスのデバイス可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加されたときに次の設定が追加されます。

- SNMP、NETCONF、Cisco TrustSec（CTS）ログイン情報
- IPDT の有効化
- コントローラ証明書
- SNMPトラップサーバ定義
- Syslog サーバ定義
- NetFlow コレクタ定義
- ワイヤレス ネットワーク アシュアランス

この手順では、[Plug and Play Devices] リストからデバイスを要求する方法について説明します。代わりに、[要求（Claim）] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド[英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、コントローラ ディスカバリの前提条件 （4 ページ）を参照してください。
- ネットワーク階層内のサイトを定義します。About Network Hierarchyを参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。SNMPv2c を使用している場合は、読み取りと書き込みの両方のログイン情報を指定する必要があります。デバイス クレデンシャルについて を参照してください。
- 必要に応じて、イメージを展開する場合は、プロビジョニングされるデバイスのソフトウェアイメージがアップロードされ、イメージリポジトリ内でゴールデンとしてマークされていることを確認します。ソフトウェア イメージのインポート を参照してください。

（注） Day-0 プロビジョニング中にプラグアンドプレイで使用されるイメージ展開プロセスは、後でデバイスイメージの更新時に使用されるプロセスと同じではありません。これはソフトウェアイメージのプロビジョニングで説明されています。プラグアンドプレイプロビジョニングでは、デバイスが工場出荷時のデフォルト状態にあると想定されているため、デバイスの事前チェック、自動フラッシュクリーンアップ、事後チェックは行われません。

- 必要に応じて、デバイスに適用する [Onboarding Configuration] テンプレートを定義します。このようなテンプレートには、ネットワーク上で管理できるようにデバイスをオンボードするための基本的なネットワーク設定コマンドが含まれています。Day-0 設定をカスタマイズする必要がない限り、ほとんどの場合、このようなテンプレートは必要ありません。デバイス設定の変更を自動化するテンプレートの作成 を参照してください。

（注） [Onboarding Configuration] テンプレートで `ip http client source-interface` CLI コマンドを使用できます。これにより、Cisco DNA Center は、特に複数の IP または VRF のシナリオにおいて、その IP アドレスをデバイスの管理 IP アドレスとして使用できます。

- デバイスのネットワークプロファイルを定義します。ネットワークプロファイルの作成を参照してください。

ステップ 1 Cisco DNA Center のホームページから、**[Provision]** > **[Devices]** > **[Plug and Play]**を選択します。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイステーブルの上にあるメニューバーで、[アクション（Actions）]>[要求（Claim）]をクリックします。

[Claim Devices] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。

ステップ 5 （オプション）必要に応じて、最初のカラムのデバイスのホスト名を変更します。

ステップ 6 [Select a Site] ドロップダウンリストから、各デバイスに割り当てるサイトを選択します。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。

ステップ 7 **[次へ (Next)]** をクリックします。
[Assign Configuration] ウィンドウが表示されます。

ステップ 8 （オプション）次のように、デバイステーブルに対するグローバルな変更を行います。

a) テーブルに表示されるカラムを変更するには、テーブル見出しの右端にある3つの点をクリックし、目的のカラムを選択します。[Apply] をクリックして、変更内容を保存します。

b) [Clear Images] をクリックして、デバイス用に設定されたデフォルトイメージをクリアします。イメージをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

c) [Clear Templates] をクリックして、デバイス用に設定されたデフォルトテンプレートをクリアします。テンプレートをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

d) デバイスに設定されているライセンスレベルをクリアするには、[Clear License Level] をクリックします。ライセンスレベルをクリアする各デバイスのチェックボックスをオンにして、[Clear] をクリックします。

e) デバイスの横にある [Actions] カラムの 3 つの点をクリックし、[Apply Image to Other Devices] または [Apply Template to Other Devices] を選択することで、あるデバイスのイメージまたはテンプレートを他のデバイスに適用できます。スタック構成のデバイスの場合は、[Apply License Level to Other Devices] をクリックして、デバイスのライセンスレベルを他のデバイスに適用できます。

ステップ 9 [Configuration] 列で、設定するデバイスの [Assign] をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。

b) （オプション）必要に応じて [Device Name] フィールドでデバイスのホスト名を変更します。

c) （オプション）[イメージ（Image）] ドロップダウン リストで、デバイスに適用するゴールデン ソフトウェア イメージを選択します。イメージリポジトリにこのデバイスタイプのゴールデンイメージが 1 つしかない場合は、そのイメージがデフォルトで選択されます。

d) （オプション）[テンプレート（Template）] ドロップダウン リストで、デバイスに適用する [オンボーディングの設定（onboarding configuration）] テンプレートを選択します。このデバイスタイプに対して定義されているオンボーディング設定テンプレートが 1 つしかない場合は、そのテンプレートがデフォルトで選択されます。

選択したテンプレートの横にある [Preview] をクリックすると、テンプレートが表示されます。

e) （オプション）スタックの番号を付け直す場合は、[Select a Cabling Scheme] ドロップダウンリストで、スタックのケーブル配線スキームを選択します。

この項目は、スタック構成をサポートしているスイッチが次のいずれかのケーブル配線スキームに従って接続されている場合にのみ表示されます。

図 *1:* ケーブル配線スキーム

f) （オプション）スタックの番号を付け直す場合は、[Select a Top of Stack serial Number] ドロップダウンリストで、スタックスイッチの先頭のシリアル番号を選択します。

この項目は、スタック構成をサポートしているスイッチがイメージに示すように接続されている場合にのみ表示されます。

g) （オプション）[Select a License Level] ドロップダウンリストで、スタックのライセンスレベルを選択します。

この項目は、スタック構成をサポートしているスイッチにのみ表示されます。

h) 変更した場合は、[Save] をクリックします。それ以外の場合は、[Cancel] をクリックしてリストに戻り、他のデバイスを設定します。

ステップ 10 プロビジョニングするデバイスを複数選択した場合は、リストにある次のデバイスの [Assign] クリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 11 **[次へ (Next)]** をクリックします。

[Provision Templates] ウィンドウが表示されます。ここでは、テンプレートに定義されたパラメータの値を指定できます。

ステップ 12 設定するデバイスの名前をクリックし、次の手順を実行します。

a) デバイスに設定テンプレートが割り当てられている場合は、テンプレートで定義されたパラメータの値を指定します。

各デバイスのフィールドに各パラメータの値を入力します。赤のアスタリスクは、必須フィールドを示します。

b) 選択したデバイスの起動設定に実行中の設定をコピーしたい場合、[Copy running config to startup config] チェックボックスをオンにします。

c) 複数のデバイスを選択してプロビジョニングした場合は、ウィンドウの左側にあるリストで次のデバイスをクリックし、パラメータ値を入力します。これを、すべてのデバイスに対して実行します。

ステップ 13 すべてのデバイスのパラメータ値を一括で指定するには、次の手順を実行します。

a) [**エクスポート (Export)**] をクリックして、CSV テンプレートファイルを保存します。

b) 各パラメータの値をファイルに追加して、ファイルを保存します。

c) [Import] をクリックします。

d) ドラッグ アンド ドロップ エリアにファイルをドラッグ アンド ドロップするか、[クリックして選択（click to select）] と表示されている場所をクリックしてファイルを選択します。
e) [Import] をクリックします。

ステップ 14 **[次へ (Next)]** をクリックします。

[Summary] ウィンドウが表示されます。ここで、デバイスに関する詳細や設定プレビューステータスを確認できます。

ステップ 15 設定プレビューが成功したかどうかを確認するには、各デバイスの [Day-0 Config] 列をチェックします。

プレビューでエラーが表示された場合は、デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。「テンプレートのプロビジョニング」手順に戻ってパラメータ値やテンプレートを変更したり、[Design] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。

ステップ 16 Day-0 Config 列のリンクをクリックして、デバイス、その設定、設定プレビューエラーの詳細を確認することができます。

ステップ 17 [要求（Claim）] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 18 [Yes] をクリックしてデバイスを要求します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary]には、デバイスにプッシュされる残りのネットワーク設定が表示されます。詳細については、デバイスのプロビジョニング （29 ページ）を参照してください。このプロセスは、[Design] エリアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイプロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS Cisco DNA Center の AAA クライアントとして ISE に追加されます (これらが設定されている場合)。

ワイヤレスまたはセンサー デバイスのプロビジョニング

デバイスを要求すると、デバイスにネットワークプロファイルを割り当て、それをインベントリに追加することでプロビジョニングされます。まだ起動していないデバイスを初めて要求する場合は、起動時に自動的にプロビジョニングされるようにデバイスを計画します。

デバイスが要求される場合、Cisco DNA Center からのシステム構成 CLI コマンドの一部はまずデバイスにプッシュされてから、定義した [Onboarding Configuration (Day-0)] テンプレートにプッシュされます。[Onboarding Configuration] テンプレートに同じ CLI コマンドがある場合、これらは最後に適用されるため、システム設定が上書きされます。システムによってプッシュされる CLI コマンドには、次のものがあります。

- デバイスのログイン情報（CLI および SNMP）
- SSH v2 および SCP サーバの有効化
- HTTP および HTTPS サーバの無効化

（注） デバイスのデバイス可制御性が有効になっている場合（デフォルトで有効）、デバイスがインベントリに追加されたときに次の設定が追加されます。

- SNMP、NETCONF、Cisco TrustSec（CTS）ログイン情報
- IPDT の有効化
- コントローラ証明書
- SNMP トラップサーバ定義
- Syslog サーバ定義
- NetFlow コレクタ定義
- ワイヤレス ネットワーク アシュアランス

この手順では、メインの [プラグアンドプレイ（Plug and Play）] タブからデバイスを要求する方法について説明します。代わりに、[要求（Claim）] をクリックしてデバイスの詳細ウィンドウからデバイスを要求することもできます。

始める前に

- プロビジョニングするシスコネットワークデバイスについて、サポートされているソフトウェアリリースがあり、工場出荷時のデフォルト状態になっていることを確認します。以前に設定されたネットワークデバイス、または不明な状態になっているネットワークデバイスを使用している場合は、『Cisco Digital Network Architecture Center のネットワーク プラグアンドプレイのトラブルシューティング ガイド [英語]』で、デバイスのクリーンアップとリセットの詳細を参照してください。
- プロビジョニングされているデバイスで Cisco DNA Center を検出して接続できることを確認します。詳細については、コントローラ ディスカバリの前提条件 （4 ページ）を参照してください。
- ネットワーク階層内のサイトを定義します。About Network Hierarchyを参照してください。
- デバイスの CLI および SNMP ログイン情報を定義します。デバイス クレデンシャルについてを参照してください。
- ワイヤレス アクセス ポイント デバイスをプロビジョニングするには、ワイヤレス アクセス ポイントを管理しているワイヤレス LAN コントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。これは、Mobility Express アクセスポイントでは必要ありません。

- センサー デバイスをプロビジョニングするには、センサーが Cisco DNA Center エンタープライズ IP アドレス（private/enp9s0）を介して到達可能であることを確認します。DHCP オプション 43 の文字列を使用すると、デバイスが Cisco DNA Center の未要求モードで到達可能になります。ただし、デバイスを要求するには、インターフェイス enp9s0 IP アドレスから到達可能である必要があります。DHCP サーバで ASCII 値「5A1D;B2;K4;I172.16.x.x;J80」を使用して、NTP サーバ（DHCP オプション 42）とベンダー固有の DHCP オプション 43 を設定します。ここで、172.16.x.x は enp9s0 インターフェイスに関連付けられた Cisco DNA Center の仮想 IP アドレスです。
- ワイヤレス アクセス ポイント デバイスのワイヤレス無線周波数プロファイルを定義します（Mobility Express アクセスポイントを除く）。ワイヤレス無線周波数プロファイルの作成 を参照してください。
- ワイヤレスセンサデバイスのバックホール設定を行います。バックホールの設定の管理 を参照してください。
- Mobility Express アクセスポイントの場合は、IP アドレスプールと管理インターフェイスを定義します。IP アドレス プールを設定する を参照してください。

ステップ 1 Cisco DNA Centerのホームページで、[Provision] > [Devices] > [Plug and Play] > > の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[フィルタ（Filter）] または **[検索（Find）]** オプションを使用して、特定のデバイスを見つけることができます。

ステップ 3 要求する 1 つ以上のワイヤレスデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイステーブルの上にあるメニューバーで、**[アクション（Actions）]** > **[要求（Claim）]** の順に選択します。

[デバイスの要求（Claim Devices）] ウィンドウが開き、最初の手順「サイトの割り当て」が表示されます。

ステップ 5 （任意） 必要に応じて、最初の列のデバイス名を変更します。

ステップ 6 （任意） 必要に応じて、2 番目の列のデバイスタイプを変更します。デバイスが使用しているモードに応じて、AP（アクセスポイント）または ME（Mobility Express）を選択できます。

誤ったモードを選択すると、デバイスのプロビジョニングエラーにつながります。この項目は、センサーデバイスには表示されません。

ステップ 7 [サイトの選択（Select a Site）] ドロップダウンリストから、各デバイスに割り当てるサイトとフロアを選択します。アクセスポイントデバイスは、ワイヤレスコントローラを備えたフロアに割り当てる必要があります。

同じサイトを最初のデバイスとしてすべての他のデバイスに適用するには、[Apply Site to All] チェックボックスをオンにします。あるデバイスのサイトを他のいくつかデバイスに割り当てるには、[Assign this Site to Other Devices] をクリックし、デバイスを選択して [Assign] をクリックします。ワイヤレスデバイスは、ビルディング自体ではなくビルディング内のフロアにのみ割り当てることができます。

ステップ 8 **[次へ (Next)]** をクリックします。
[設定（Configuration）] ウィンドウが表示されます。

ステップ 9 （任意）テーブルに表示される列を変更するには、テーブル見出しの右端にある3つの点をクリックし、目的の列を選択します。[Apply] をクリックして、変更内容を保存します。

ステップ 10 設定するデバイスの名前をクリックし、次の手順を実行します。

a) デバイス設定の概要を表示し、変更が不要な場合は [Cancel] をクリックします。
b) （任意） [デバイス名（Device Name）] フィールドで、必要に応じてデバイス名を変更します。
c) アクセスポイントデバイスの場合、**[RFプロファイル（RF Profile）]** ドロップダウンリストで、デバイスに適用する RF プロファイルを選択します。これは、1 つのプロファイルをデフォルトとして指定した場合に設定できます。
d) For a Mobility Express device, enter values in the following fields：**Management IP**, **Subnet Mask**, and **Gateway**.
e) ワイヤレスセンサーデバイスの場合、**[センサーの設定（Sensor Settings）]** ドロップダウンリストで、デバイスに適用するセンサー デバイス プロファイルを選択します。
f) 変更した場合は、[保存（Save）] をクリックします。それ以外の場合は、[キャンセル（Cancel）] をクリックしてリストに戻り、他のデバイスを設定します。
g) **[アクション（Actions）]** 列の **[他のデバイスに...を適用（Apply … to Other Devices）]** をクリックして、あるデバイスに割り当てた設定を同じタイプの他のデバイスに適用できます。

ステップ 11 複数のデバイスを選択してプロビジョニングした場合は、リストで次のデバイスをクリックし、この設定手順を繰り返します。これを、すべてのデバイスに対して実行します。

ステップ 12 **[次へ (Next)]** をクリックします。
[概要（Summary）] ウィンドウが表示されます。ここで、デバイスや設定に関する詳細を確認できます。

ステップ 13 設定プレビューが成功したかどうかを確認するには、各デバイスの **[Day-0 Config プレビューステータス（Day-0 Config Preview Status）]** 列をチェックします。

プレビューでエラーが表示された場合は、デバイスを要求する前に問題を解決してプロビジョニングエラーを回避する必要があります。[設定（Configuration）] 手順に戻って設定を変更したり、[設計（Design）] エリアに再度アクセスしてネットワーク設計の設定を更新したり、ネットワーク接続の問題を解決したりすることが必要になる場合があります。デバイスを管理しているワイヤレスLANコントローラがインベントリに追加され、ワイヤレスデバイスが割り当てられているサイトに割り当てられていることを確認します。

ステップ 14 [要求（Claim）] をクリックします。
確認のダイアログボックスが表示されます。

ステップ 15 **[はい（Yes）]** をクリックしてデバイスを要求し、プロビジョニングプロセスを開始します。

次のタスク

プロビジョニングプロセスを完了するには、デバイスがインベントリに追加された後、[Inventory] タブに移動し、デバイスを選択し、[Actions] > [Provision] > [Provision Device] をクリックします。すべての手順を実行し、[Summary]ステップで [Deploy] をクリックします。[Summary]には、デバイスにプッシュされる残りのネットワーク設定が表示されます。詳細については、デバイスのプロビジョニング （29 ページ）を参照してください。このプロセスは、[Design] エ

リアで設定した可能性のあるネットワーク設定をプッシュする場合に必要です。プラグアンドプレイプロビジョニング中は、デバイスのログイン情報とオンボーディング設定のみがデバイスにプッシュされます。[Inventory] からプロビジョニングが完了するまで、他のネットワーク設定はプッシュされません。さらに、デバイスは、RADIUS および TACACS Cisco DNA Center の AAA クライアントとして ISE に追加されます (これらが設定されている場合)。

デバイスの削除

デバイスを削除すると、デバイスはプラグアンドプレイのデータベースから削除されますが、リセットはされません。エラー状態のデバイスをリセットする場合は、[Reset] を使用します。

この手順では、[プラグアンドプレイ（Plug and Play）] タブからデバイスを削除する方法について説明します。代わりに、[削除（Delete）] をクリックしてデバイスの詳細ウィンドウからデバイスを削除することもできます。

（注） デバイスがプロビジョニングの状態の場合は、[Inventory] タブからのみ削除できます。

ステップ 1 Cisco DNA Centerのホームページで、[Provision] > [Devices] > [Plug and Play] > > の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 削除する 1 つ以上のデバイスの横にあるチェックボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、[アクション（Actions）] > [削除（Delete）] をクリックします。

確認のダイアログボックスが表示されます。

ステップ 5 [Yes] クリックして、このデバイスを削除することを確認します。

デバイスのリセット

デバイスのリセットはエラー状態のデバイスにのみ適用され、状態が [Unclaimed] にリセットされデバイスがリロードされますが、プラグアンドプレイ データベースからは削除されません。デバイスを削除する場合は、**[削除（Ddelete）]** を使用します。

（注） デバイスで保存された設定が工場出荷時のデフォルトまたは同様の最小限の設定である場合、このオプションを選択すると、デバイスはプロビジョニングプロセスを再起動します。ただし、デバイスに以前に保存されたスタートアップコンフィギュレーションがある場合は、これによってデバイスのプロビジョニングプロセスの再起動を回避できますが、工場出荷時のデフォルトにリセットする必要があります。ワイヤレスデバイスおよびセンサーデバイスでは、デバイスの状態だけがリセットされ、デバイスはリロードされません。

この手順では、**[プラグアンドプレイ（Plug And Play）]** タブからデバイスをリセットする方法について説明します。代わりに、[Reset] をクリックしてデバイスの詳細ウィンドウからリセットすることもできます。

ステップ 1 Cisco DNA Centerのホームページで、[Provision] > [Devices] > [Plug and Play] > > の順に選択します。

ステップ 2 テーブル内のデバイスを表示します。

[Filter] オプションを使用して、特定のデバイスを検索します。[Refresh] をクリックしてデバイスリストを更新します。

ステップ 3 リセットする 1 個以上のデバイスの横にあるチェック ボックスをオンにします。

ステップ 4 デバイス テーブルの上にあるメニュー バーで、**[Actions（アクション）] > [Reset（リセット）]** をクリックします。

確認のダイアログボックスが表示されます。

ステップ 5 次のいずれかのオプションを選択します。

- [Reset and keep current claim parameters]：現在の請求パラメータが維持され、デバイスは [Planned] 状態になります。
- [Reset and remove all claim parameters]：現在の請求パラメータを削除し、デバイスが [Unclaimed] 状態になります。

ステップ 6 [リセット（Reset）] をクリックします。

インベントリ内のデバイスの管理

ここでは、[Device Inventory] ウィンドウを使用して、サイトにデバイスを割り当て、デバイスタグを管理する方法について説明します。

[Device Inventory] ページを使用してデバイスを管理する方法の詳細については、インベントリの管理を参照してください。

デバイスをサイトに追加する

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。
[Inventory] ウィンドウには、**ディスカバリ**プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 サイトに割り当てるデバイスのチェックボックスをオンにします。

ステップ 3 [Actions] メニューから、**[Provision]** > **[Assign Device to Site]** を選択します。
[Assign Device to Site] スライドインペインが表示されます。

ステップ 4 [Assign Device To Site] スライドインペインで、デバイスの  アイコンの横にあるリンクをクリックします。
[Choose a floor] スライドイン ペインが表示されます。

ステップ 5 [Choose a floor] スライドインペインで、デバイスに割り当てるフロアを選択します。

ステップ 6 **[Save]** をクリックします。

ステップ 7 （任意） 複数のデバイスを選択して同じ場所に追加した場合は、最初のデバイスで [Apply to All] チェックボックスをオンにすると、残りのデバイスに同じ場所を割り当てることができます。

ステップ 8 [**Assign**] をクリックします。

デバイスのタグ付け

デバイス タグは属性またはルールに基づいてデバイスをグループ化することができます。単一のデバイスに複数のタグを設定できます。同様に、複数のデバイスに適用できる単一のタグもあります。

[プロビジョン（Provision）]ウィンドウのデバイスに対してタグを追加したり、削除できます。

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用するデバイスの横にあるチェックボックスをオンにして、[Tag Device] をクリックします。

ステップ 3 [タグ名（Tag Name）] フィールドにタグ名を入力します。

- 新しいタグを作成している場合は、 **[** 新規タグの作成（Create New Tag） **]** をクリックします。ルールを使用して新規タグを作成することもできます。詳細については、「ルールを使用してデバイスにタグ付けする （27 ページ）」を参照してください。
- 既存のタグを使用する場合は、一覧からタグを選択して、[Apply] をクリックします。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

ステップ 4 デバイスからタグを削除するには、以下のいずれか 1 つを行います。

- Click **Create New Tag**, unselect all tags, and then click **APply**.

- タグアイコンまたはタグ名にカーソルを合わせて、[X] をクリックし、デバイスからタグの関連付けを解除します。

ルールを使用してデバイスにタグ付けする

ルールを定義するタグに基づいてデバイスをグループ化することができます。ルールを定義するとき、Cisco DNA Center は指定したルールと一致するすべてのデバイスにタグを適用します。ルールはデバイス名、デバイスファミリ、デバイスシリーズ、IP アドレス、ロケーション、またはバージョンに基づくことができます。

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 タグを適用するデバイスの隣のチェックボックスをオンにして、**[デバイスのタグ付け（Tag Device）]** をクリックします。

ステップ 3 **[** タグ名（Tag Name） **]** フィールドにタグ名を入力し、**[** ルールによる新規タグの作成（Create New Tag with Rule） **]** をクリックします。

[新規 VRF の作成（Create New VRF） **]** ウィンドウが表示されます。

[タグ付きデバイスの合計数（Total Devices Tagged Count） **]** の下の **[** 手動で追加（Manually Added） **]** フィールドは、ステップ 2 で選択されたデバイスの合計数を示します。

ステップ 4 **[** 条件の追加（Add Condition） **]** をクリックして、ルールに必要なフィールドに記入します。

[一致するデバイス（Matching Devices） **]** の数は、この条件に一致するデバイスの数に応じて、自動的に変更されます。

追加条件を作成するためには、次の 2 つのオプションがあります。

- *And* 条件— **[** 条件の追加（Add Condition） **]** リンクをクリックします。**And** が条件の上に表示されます。
- *Or* 条件—既存の条件の隣の追加アイコン (+) をクリックします。**Or** は条件の隣に表示されます。

必要に応じていくつでも条件を追加できます。ルールを変更すると、指定したルールに一致するインベントリのデバイス数を反映して一致するデバイス数が変更されます。デバイス数でクリックして、ルールと一致するデバイスを表示できます。

ステップ 5 **[** 保存（Save） **]** をクリックして、定義されたルールと共にタグを保存します。

タグを適用するデバイス名の下に、タグ アイコンとタグ名が表示されます。

デバイスがインベントリに追加されると、定義したruleと一致する場合、タグは自動的にデバイスに適用されます。

デバイスタグの編集

以前に作成したデバイスタグを編集できます。

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

[デバイス名（Device Name）] 列のデバイス名の下に以前に作成したデバイスタグがありある場合はそれがリスト表示されます。

ステップ 2 デバイスを選択しないで、 [デバイスのタグ付け（Tag Device）] をクリックします。

以前に作成されたタグがリストされます。

ステップ 3 編集するタグをマウスオーバーして、タグ名の隣の鉛筆アイコンをクリックします。

代わりに、 [デバイスのタグ付け（Tag Device）] > [すべてのタグの表示（View All Tags）] を選択し、編集するタグの隣の鉛筆アイコンをクリックします。

ステップ 4 タグを変更し、 [保存（Save）] をクリックして変更を保存します。

タグの削除

デバイスタグまたはテンプレートタグは、デバイスまたはテンプレートに関連付けられていない場合にのみ削除できます。

始める前に

デバイスに（ルールを使用して）静的または動的に関連付けられているタグを削除します。

テンプレートに関連付けられているタグを削除します。

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。

デバイスインベントリのページには、ディスカバリ プロセス中に収集されたデバイス情報が表示されます。

ステップ 2 デバイスを選択しないで、[Tag Device] > [Manage Tags] をクリックします。

ステップ 3 削除するタグにマウスカーソルを合わせてから、タグ名の横にある削除アイコンをクリックします。

ステップ 4 タグの削除の警告メッセージで [Yes] をクリックします。

タグがデバイスまたはテンプレートに関連付けられている場合は、エラーメッセージがスローされます。デバイスまたはテンプレートに関連付けられているタグを除去し、タグを削除します。

デバイスのプロビジョニング

次の項では、シスコの多様なデバイスのプロビジョニング方法について説明します。

Cisco AireOS コントローラのプロビジョニング

始める前に

- シスコ ワイヤレス コントローラ をプロビジョニングする前に、次のグローバル ネットワーク設定を定義したことを確認します。
  - AAA、DHCP、および DNS などのネットワーク サーバ。

    詳細については、グローバル ネットワーク サーバの設定を参照してください。
  - CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。

    詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、およびグローバル HTTPS クレデンシャルの設定を参照してください。
  - IP アドレス プール

    詳細については、「IP アドレス プールを設定する」を参照してください。
  - SSID、ワイヤレス インターフェイス、およびワイヤレス無線周波数プロファイルなどのワイヤレス設定です。

    詳細については、「グローバル ワイヤレス設定の構成」を参照してください。
- インベントリに シスコ ワイヤレス コントローラ があることを確認します。ない場合は、[Discovery] 機能を使用して ワイヤレス コントローラ を検出します。
- サイトに シスコ ワイヤレス コントローラ が追加されたことを確認します。詳細については、「デバイスをサイトに追加する （26 ページ）」を参照してください。

Cisco DNA Center によって管理されている ワイヤレス コントローラ の設定に手動で変更を加えることはできません。Cisco DNA Center GUI からすべての設定を実行する必要があります。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devices]>[Inventory] ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。 >

ステップ 2 左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [DEVICE TYPE] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能な ワイヤレス コントローラ のリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 [Actions] ドロップダウンリストから、[Provision] > [Provision Device] を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 6 [Choose a site] をクリックして ワイヤレス コントローラ にサイトを割り当てます。

ステップ 7 [Add Sites] ウィンドウで、ワイヤレス コントローラ を関連付けるサイト名の横にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 8 [Apply] をクリックします。

ステップ 9 [Next] をクリックします。

[設定（Configuration） **]** ウィンドウが表示されます。

ステップ 10 Select a role for the ワイヤレス コントローラ：**Active Main WLC** or **Guest Anchor WLC**.

ステップ 11 [Select Primary Managed AP Locations] をクリックして、ワイヤレス コントローラ の管理 AP の場所を選択します。

ステップ 12 [Managed AP Location] ウィンドウで、サイト名の横にあるチェックボックスをオンにします。親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、親サイトの下にある子は自動的に選択されます。

（注） 管理 AP の場所を継承することで、サイトをその下のビルディングやフロアとともに自動で選択できます。1 つの ワイヤレス コントローラ で管理できるのは 1 つのサイトのみです。

ステップ 13 **[Save]** をクリックします。

ステップ 14 [Interface and VLAN Configuration] で [+ Add] をクリックして、アクティブメイン ワイヤレス コントローラ のインターフェイスと VLAN の詳細を設定します。

インターフェイスおよび VLAN の設定は、非ファブリックの ワイヤレス コントローラ プロビジョニングにのみ適用できます。

[インターフェイスと VLAN の設定（Configure Interface and VLAN） **]** ウィンドウが表示されます。

ステップ 15 **[** インターフェイス名（Interface Name） **]** ドロップダウン リストからインターフェイス名を選択します。

ステップ 16 [VLAN ID] フィールドに、VLAN の値を入力します。

ステップ 17 [Interface IP Address] フィールドに、インターフェイス IP アドレスの値を入力します。

ステップ 18 [Interface Net Mask (in bits)] フィールドに、インターフェイスのサブネットマスクを入力します。

ステップ 19 [Gateway IP Address] フィールドにゲートウェイ IP アドレスを入力します。

ステップ 20 [LAG/Port Number] ドロップダウンリストから、リンク集約またはポート番号を選択します。

ステップ 21 [OK] をクリックします。

ステップ 22 ゲスト アンカー ワイヤレス コントローラ の場合、[ゲスト SSID を DMZ サイトに割り当てる（Assign Guest SSIDs to DMZ site）] で [VLAN ID] を変更して、VLAN ID 設定を変更できます。

ステップ 23 [Mobility Group] で [Configure] をクリックして、ワイヤレス コントローラ をモビリティピアとして設定します。

詳細については、「モビリティ設定の概要 （59 ページ）」を参照してください。

[Configure Mobility Group] サイドパネルが表示されます。

ステップ 24 [Mobility Group Name] ドロップダウンリストで、 をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択します。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 25 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 26 [Mobility Peers] で [Add] をクリックして、ワイヤレス コントローラ をモビリティピアとして設定します。

ステップ 27 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、 Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 28 **[Save]** をクリックします。

ステップ 29 モビリティグループ名と RF グループ名をリセットするには、次のいずれかを実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > > **[Configuration]** ページの [Mobiliy Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

ステップ 30 **[次へ (Next)]** をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 31 [Devices] パネルでデバイスまたはテンプレートを検索できます。

ステップ 32 [wlanid] フィールドに、事前定義されたテンプレート変数の値を入力します。

ステップ 33 [Next] をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **デバイスの詳細**
- **ネットワーク設定（Network Settings）**
- **SSID**
- **管理サイト**
- **インターフェイス**

- **[Advanced Configuration]**
- モビリティ グループの設定

ステップ 34 [展開（Deploy）] をクリックして、コントローラをプロビジョニングします。

- 即座にデバイスを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 35 セカンダリコントローラをプロビジョニングします。

詳細については、「Cisco DNA Center からの N+1 高可用性の設定 （57 ページ）」を参照してください。

ステップ 36 展開が正常に完了すると、[デバイスインベントリ（Device Inventory）] ウィンドウの [ステータス（Status）] 列に「成功（SUCCESS）」と表示されます。

プロビジョニング後に何らかの変更を行う場合は、[Design] をクリックしてサイトのプロファイルを変更し、もう一度 ワイヤレス コントローラ をプロビジョニングします。

ステップ 37 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 38 [Device Inventory] ウィンドウで、[Provision Status] カラムの [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、さらに実行する必要があるアクションのリストを表示します。

ステップ 39 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 40 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 41 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。

また、[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも表示されます。

ステップ 42 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

Cisco DNA Center からのシスコ WLC 高可用性の設定 Cisco DNA Center

シスコ ワイヤレス コントローラ高可用性（HA）を Cisco DNA Center から設定できます。現在、ワイヤレスコントローラ HA の形成がサポートされています。HA およびスイッチオーバーオプションの中断はサポートされていません。

ハイ アベイラビリティ用 Cisco ワイヤレス コントローラ設定の前提条件

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の検出機能とインベントリ機能が正常である必要があります。デバイスが管理状態になっている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 のサービスポートと管理ポートが設定されている必要があります。
- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長ポートが物理的に接続されている必要があります。

- ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の管理アドレスが同じサブネット内にある必要があります。ワイヤレスコントローラ 1 とワイヤレスコントローラ 2 の冗長管理アドレスも同じサブネット内にある必要があります。
- ワイヤレスコントローラで次のブート変数を手動で設定します。

```
config t
boot system bootflash::<device_iosxe_image_filename>
config-register 0x2102

show boot.  (IOSXE cli)

BOOT variable = bootflash:<device_iosxe_image_filename>,12;
Configuration register is 0x2102
```

シスコ ワイヤレス コントローラ HA の設定

ステップ 1 Cisco DNA Center のホームページから、[Provision] > [Devices] を選択します。

[Devices] > [Inventory] ウィンドウが表示され、検出されたデバイスが一覧表示されます。 >

ステップ 2 プライマリコントローラとして設定するコントローラ名の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから [Provision] > [Configure WLC HA] を選択します。 >

[High Availability] ページが表示されます。

ステップ 4 [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスをそれぞれテキストボックスに入力します。

冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、シスコ ワイヤレス コントローラ の管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがこのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 5 [Select Secondary WLC] ドロップダウンリストから、セカンダリコントローラを選択します。

ステップ 6 [HA の設定（Configure HA）] をクリックします。
HA 設定は、CLI コマンドを使用してバックグラウンドで開始されます。最初に、プライマリ ワイヤレス コントローラが設定されます。成功したら、セカンダリ ワイヤレス コントローラが設定されます。設定が完了したら、両方のワイヤレスコントローラが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 7 HA 設定を確認するには、[Devices] > [Inventory] > ページで、HA デバイスとして設定したデバイスをクリックします。

ステップ 8 [Wireless Info] タブをクリックします。

[Redundancy Summary] には、[Sync Status] が [In Progress] として表示されます。Cisco DNA Center で HA のペアリングが成功したことが検出されると、[Sync Status] が [Complete] に変わります。

これは、インベントリ ポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリ ワイヤレス コントローラ（ワイヤレスコントローラ 2）は、Cisco DNA Center から削除されます。このフローは、ワイヤレスコントローラでの正常な HA 設定を示しています。

高可用性プロセス中および完了後に起こること

1. Cisco WLC-1 および WLC-2 は、冗長管理、冗長ユニット、および SSO とともに設定されます。ワイヤレス コントローラはロールをアクティブまたはスタンバイとしてネゴシエートするために再起動します。設定は、アクティブからスタンバイに同期されます。
2. [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
   - SSO が有効になっています
   - ワイヤレス コントローラがアクティブ状態になっています
   - ワイヤレス コントローラがホット スタンバイ状態になっています
3. アクティブ ワイヤレス コントローラの管理ポートは、両方のコントローラによって共有され、アクティブ コントローラを指します。スタンバイ ワイヤレス コントローラのユーザー インターフェイス、Telnet、および SSH は機能しません。コンソールとサービス ポート インターフェイスを使用して、スタンバイ ワイヤレス コントローラを制御できます。

高可用性を設定および確認するためのコマンド

シスコ ワイヤレス コントローラ HA を設定するには、Cisco DNA Center で次のコマンドを送信します。

Cisco DNA Center で次のコマンドを ワイヤレス コントローラ 1 に送信します。

- **config interface address redundancy-management 198.51.100.xx peer-redundancy-management 198.51.100.yy**
- **config redundancy unit primary**
- **config redundancy mode sso**

Cisco DNA Center で次のコマンドを ワイヤレス コントローラ 2 に送信します。

- **config interface address redundancy-management 198.51.100.yy peer-redundancy-management 198.51.100.xx**
- **config redundancy unit secondary**
- **config port adminmode all enable**
- **config redundancy mode sso**

ワイヤレス コントローラ から HA 設定を検証するには、次のコマンドを使用します。

- HA 関連の詳細情報を確認する場合：**config redundancy mode sso**
- 設定済みのインターフェイスを確認する場合：**show redundancy summary**

ルーティングおよび NFV プロファイルのプロビジョニング

始める前に

ルーティングと NFV プロファイルをプロビジョニングする前に、次のグローバルネットワーク設定を定義したことを確認します。

- AAA、DHCP、および DNS などのネットワーク サーバ。詳細については、グローバル ネットワーク サーバの設定を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャル。詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、およびグローバル HTTPS クレデンシャルの設定を参照してください。
- IP アドレス プール詳細については、「IP アドレス プールを設定する」を参照してください。
- SP プロファイル。詳細については、「サービス プロバイダー プロファイルの設定」を参照してください。

（注） Cisco Firepower Threat Defense Virtual を NFV プロビジョニング フローを通じてプロビジョニングする場合、デフォルトのクレデンシャルユーザ名が保持され、パスワードはネットワーク設定でサイトに割り当てられたクレデンシャル プロファイルの設定に基づいて更新されます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devices] > [Inventory] ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [Routers] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能なデバイスのリストを取得します。

ステップ 4 プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。

ステップ 5 サイトで [Assign] をクリックすると、[Assign Device to Site] ウィンドウが表示されます。[Choose a Site] をクリックしてサイトを割り当てます。

ステップ 6 [Actions] ドロップダウンリストから、[Provision] > [Provision Device] を選択します。

NFVIS デバイスをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。

- [Router WAN Configuration] ウィンドウで詳細を確認します。[O] をクリックして WAN の IP アドレスを入力します。[+Edit Services] ウィンドウで詳細を確認します。**[次へ (Next)]** をクリックします。

  （注） vEDGE 関連サービスをプロビジョニングする前に、[system setting] ページで vManage 設定を構成する必要があります。詳細については、『Cisco Digital Network Architecture Center Administrator Guide』の「Configure vManage Properties」セクションを参照してください。

- [ENCS Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Custom Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Summary] ページで詳細を確認します。

ルータをプロビジョニングするには、次の手順を実行します。

- [Confirm Profile] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Router WAN Configuration] ウィンドウで詳細を確認します。
  - 回線インターフェイスとしてギガビットイーサネットを選択した場合は、[O] をクリックし、静的 IP アドレスを選択した場合は WAN IP アドレスを入力します。[DHCP] を選択した場合は、DHCP サーバの IP アドレスを入力します。プライマリ WAN がすでに PnP を使用して設定されている場合は、[Do Not Change] を選択して、ドロップダウンリストからプライマリ WAN として設定されているインターフェイスを選択します。
  - 回線インターフェイスとしてセルラーを選択した場合は、[O] をクリックして、[IP Negotiated] を選択し、ドロップダウンリストから [Interface Name] を選択して [Access Point Name (APN)] を入力します。サービスプロバイダーに応じて、[PAP] または [CHAP] の横にあるチェックボックスをオンにします。
  - 複数のサービスプロバイダーを利用している場合は、バックアップ WAN インターフェイスの [IP SLA Address] を入力します。

  仮想ルータをプロビジョニングしている場合、このウィンドウは表示されません。
- [Router LAN Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。

  You can now select one L3 interface or one or multiple L2 interfaces from **Interface(s**）drop down list.
- [Integrated Switch Configuration] ウィンドウで詳細を確認し、[Next] をクリックします。
- [Summary] ページで詳細を確認します。

ステップ 7 [展開（Deploy）] をクリックして、デバイスをプロビジョニングします。

展開が正常に完了すると、[デバイス インベントリ（Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。[SUCCESS] をクリックして詳細なプロビジョニング ログ ステータスを確認します。

VPC インベントリ収集

クラウドインベントリ収集が正常に完了すると、[Provision] セクションの [Cloud] タブに、収集した AWS VPC インベントリのビューが表示されます。左側のナビゲーションを展開して、クラウドプロファイルまたはアクセスキーのクラウド領域を表示できます。左側のナビゲーション項目をキーワードでフィルタ処理してクリックすると、選択した領域またはアクセスキーに対してのみ VPC が表示されます。

[VPC Inventory] ビューでは、VPC をクリックして、その VPC のサブネットや仮想インスタンスなどの詳細を確認することもできます。AWS VPC インベントリ収集は、すべてのインベントリ収集のデフォルト間隔で行われるようにスケジュールされており、クラウドアクセスキーの歯車メニューの [Sync] アクションを使用して、オンデマンドでトリガーすることもできます。インベントリ収集のステータスを表示するには、[VPC Inventory] ビューで [Show Sync Status] をクリックします。

シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング

始める前に

インベントリにシスコの AP があることを確認してください。ない場合は、ディスカバリ機能を使用して AP を検出します。詳細については、ネットワークの検出を参照してください。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devices] > **[Inventory]** ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。

ステップ 2 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 3 [Device Type] リストから [AP] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出され到達可能な AP のリストを取得します。

ステップ 4 プロビジョニングする AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 5 **[Actions]** ドロップダウンリストから、**[Provision]** > **[Provision]** を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 6 [Choose a floor] をクリックし、サイトに AP を割り当てます。

ステップ 7 [Choose a floor] ウィンドウで AP を関連付けるフロアを選択し、[Save] をクリックします。

ステップ 8 [Next] をクリックします。

[設定（Configuration）] ウィンドウが表示されます。

ステップ 9 デフォルトでは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Wireless Radio Frequency Profile]** でデフォルトとしてマークしたカスタム無線周波数プロファイルが、**[RF Profile]** ドロップダウンリストで選択されています。

[RF プロファイル（RF Profile）] ドロップダウンリストから値を選択して、AP のデフォルト RF プロファイル値を変更できます。オプションは、[High]、[Typical]、[Low] です。

選択した RF プロファイルに基づいて AP グループが作成されます。

ステップ 10 **[次へ (Next)]** をクリックします。

ステップ 11 [Summary] ウィンドウでデバイスの詳細を確認し、[Deploy] をクリックして AP をプロビジョニングします。

- 即座に AP を展開するには、[Now] オプションボタンをクリックし、[APply] をクリックします。
- 将来の日付と時刻で AP の展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 12 AP グループの作成または変更が進行中であることを示すメッセージが表示されます。

「プロビジョニング後にAPがリブートします。続行しますか? (After provisioning AP(s) will reboot. Do you want to continue?」というメッセージが表示されます。

ステップ 13 [OK] をクリックします。

展開が正常に完了した場合、[Inventory] ウィンドウの [Last Sync Status] 列に、[SUCCESS] と表示されます。

Cisco AireOS Mobility Express AP の Day 0 ワークフロー

始める前に

Cisco Mobility Express ワイヤレス ネットワーク ソリューションは、1 つ以上の 802.11ac Wave 2 Cisco Aironet シリーズのアクセスポイント（AP）と、ネットワーク内のその他の AP を管理する内蔵ソフトウェアベースの ワイヤレス コントローラ で構成されます。ワイヤレス コントローラ として機能している AP をプライマリ AP といい、このプライマリ AP によって管理される Cisco Mobility Express ネットワーク内のその他の AP を下位 AP といいます。

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。
- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、およびグローバル SNMPv3 クレデンシャルの設定を参照してください。
- WLAN、インターフェイス、RF プロファイルを作成します。

- DHCP サーバにオプション #43 とオプション #60 を設定します。これは Cisco DNA Center プラグアンドプレイサーバの IP アドレスです。これを使用して、AP は PnP サーバに接続し、設定をダウンロードします。
- インベントリに Mobility Express AP があることを確認してください。ない場合は、ディスカバリ機能を使用して検出します。詳細については、CDP を使用したネットワークの検出、Discover Your Network Using an IP Address Range、およびインベントリについてを参照してください。
- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

ステップ 1 Cisco Mobility Express は DHCP サーバに接続し、Cisco DNA Center プラグアンドプレイサーバに接続します。

ステップ 2 DHCP サーバは、オプション #43 を使用して IP アドレスを割り当てます。オプション #43 は、Cisco DNA Center プラグアンドプレイサーバの IP アドレスです。

ステップ 3 Mobility Express AP は PnP エージェントを開始し、PnP サーバに接続します。

（注） ネットワーク内に一連の Mobility Express AP がある場合、内部プロトコルを通過します。プロトコルは 1 つの Mobility Express AP を選択します。これは、シスコ ワイヤレス コントローラで、PnP サーバに到達するためのプライマリ AP として設定されます。

ステップ 4 [Provision] > [Devices] > [Plug and Play] タブで未要求 AP を検索します。 > >

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onbording Status] が [Initialized] になるまで待機する必要があります。

ステップ 5 この AP を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 6 デバイステーブルの上にあるメニューバーで、[Actions] > [Claim] の順に選択します。 >

[Claim Devices] ウィンドウが表示されます。

ステップ 7 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 8 **[次へ (Next)]** をクリックします。

ステップ 9 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 10 [Configuration for device name] ページで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 11 **[Save]** をクリックします。

ステップ 12 **[次へ (Next)]** をクリックします。

[概要（Summary）] ページが表示されます。

ステップ 13 [Summary] ページで [Claim] をクリックします。

Mobility Express AP が要求されると、設定された IP アドレスが Mobility Express AP に割り当てられます。

ステップ 14 要求されたデバイス（AP）と ワイヤレス コントローラ は、**[Provision]** > **[Device Inventory]** > **[Inventory]** ページで確認できるようになりました。

ステップ 15 また、CSV ファイルからデバイスを一括して追加することもできます。

詳細については、「デバイスの一括追加 （12 ページ）」を参照してください。

CSV を使用して Mobility Express AP を一括インポートすると、すべての Mobility Express AP が **[Device]** > **[Plug and Play]** ページに表示されます。VRRP プロトコルに基づいて、インポートされた Mobility Express AP のうち 1 台だけがプライマリ AP になって要求に応じ、残りは下位 AP になります。プライマリ AP を要求した後、下位 AP を要求する必要はありません。Cisco DNA Center は、[Plug and Play] ページから下位 AP をクリアしません。これらの下位 AP は、**[Devices]** > **[Plug and Play]**ページから手動で削除する必要があります。

ステップ 16 シスコ ワイヤレス コントローラ をプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （29 ページ） を参照してください。

ステップ 17 AP をプロビジョニングするには、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （37 ページ） を参照してください。

Cisco AireOS コントローラのためのブラウンフィールドのサポート

始める前に

（注） ブラウンフィールドのサポートは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスではなく Cisco AireOS ワイヤレス コントローラ デバイスに対応しています。

この手順では、Cisco DNA Center を使用して、ブラウンフィールド Cisco AireOS コントローラをプロビジョニングする方法を示します。

- 初めに、デバイスについてディスカバリを実行します。すべてのデバイスが [インベントリ（Inventory）] ウィンドウに表示されます。詳細については、ネットワークの検出およびインベントリについてを参照してください。
- ワイヤレス コントローラ は到達可能で、 [インベントリ（Inventory）] ウィンドウで管理状態でなければなりません。詳細については、インベントリについてを参照してください。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Device] > [Inventory] ウィンドウが表示されます。このウィンドウには、ネットワークで使用可能な検出済みのデバイスが一覧表示されます。 >

ステップ 2 [フィルタ（Filter）] をクリックして、選択したフィルタ フィールドに適切な値を入力します。たとえば、[デバイス名（Device Name）] フィルタの場合、デバイスの名前を入力します。

[デバイス（Devices）]テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 3 プロビジョニングする ワイヤレス コントローラ デバイス名の横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、[Provision] > [Learn Device Config] を選択します。 >

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 5 [Choose a site] をクリックして、コントローラにサイトを割り当てます。

ステップ 6 [Choose a site] ウィンドウで、ワイヤレス コントローラ を関連付けるサイトを選択し、[Save] をクリックします。

ステップ 7 **[次へ (Next)]** をクリックします。

ステップ 8 [Resolve Conflict] ウィンドウに、解決する必要がある Cisco DNA Center の競合する設定が表示されます。

ステップ 9 **[次へ (Next)]** をクリックします。

[Design Object] ウィンドウに、学習したすべての設定が一覧表示されます。

ステップ 10 左ペインで [ネットワーク（Network）] をクリックします。

右側のペインに、デバイス設定学習の一部として学習されたネットワーク設定と、次の情報が表示されます。

- [AAA サーバ（AAA Server）] の詳細。
- システム設定。AAA サーバの IP アドレスとプロトコルについての詳細情報を含みます。
- [DHCP Server] の詳細。

ステップ 11 AAA サーバの共有秘密を入力します。

ステップ 12 左ペインで [ワイヤレス（Wireless）] をクリックします。

右側のペインには、企業 SSID、ゲスト SSID、およびワイヤレスインターフェイスの詳細が一覧表示されます。

ステップ 13 事前共有キー（PSK）を使用する SSID の場合、事前共有キーを入力します。

ステップ 14 左ペインで [破棄された設定（Discarded Config）] をクリックします。

右ペインに、Cisco DNA Center 上で競合する設定、または既に存在する設定が一覧表示されます。破棄された設定エントリは、次のように分類されます。

- 設計エンティティの重複

- 無線ポリシーの不明なデバイス設定

ステップ 15 **[次へ (Next)]** をクリックします。

[ネットワーク プロファイル（Network Profile）] ウィンドウに、AP と WLAN の組み合わせに基づいて作成されたネットワーク プロファイルまたはサイト プロファイルが一覧表示されます。

ステップ 16 **[Save]** をクリックします。

「ブラウンフィールド設定に成功しました（`Brownfield Configuration is Successful`）」というメッセージが表示されます。

ステップ 17 **[設計（Design）]** > **[ネットワーク プロファイル（Network Profile）]** を選択して、サイトをネットワーク プロファイルに割り当てます。

ステップ 18 [ネットワーク プロファイル（Network Profile）] ページで [サイトの割り当て（Assign Site）] をクリックして、選択したプロファイルにサイトを追加します。

ステップ 19 [サイトをプロファイルに追加（Add Sites to Profile）] ウィンドウでドロップダウンリストからサイトを選択して、[保存（Save）] をクリックします。

ステップ 20 [プロビジョニング（Provision）] タブをクリックします。

ステップ 21 [フィルタ（Filter）] をクリックして、選択したフィルタ フィールドに適切な値を入力します。

[デバイス（Devices）]テーブルに表示されるデータは、選択したフィルタに従って自動で更新されます。

ステップ 22 プロビジョニングするコントローラ デバイス名の横にあるチェック ボックスをオンにします。

ステップ 23 [アクション（Actions）] ドロップダウン リストから、[プロビジョニング（Provision）]を選択します。

ステップ 24 [サイトの割り当て（Assign Site）] ウィンドウで詳細を確認して、[次へ（Next）] をクリックします。

[設定（Configurations）] ウィンドウが表示されます。

ステップ 25 [インターフェイスと VLAN の設定（Interface and VLAN Configuration）] で、[+ 追加（+ Add）] をクリックしてインターフェイスと VLAN の詳細を設定します。

ステップ 26 [インターフェイスと VLAN の設定（Configure Interface and VLAN）] ウィンドウで必要なフィールドを設定して、[OK] をクリックします。

ステップ 27 [Next] をクリックします。

ステップ 28 [Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- **デバイスの詳細**
- **ネットワーク設定（Network Settings）**
- **SSID**
- **管理サイト**
- **インターフェイス**

ステップ 29 [展開（Deploy）] をクリックして、デバイスをプロビジョニングします。

展開が正常に完了すると、[デバイス インベントリ（Device Inventory）] ウィンドウの [プロビジョニング ステータス （Provision Status）] 列に「成功（SUCCESS）」と表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定とプロビジョニング

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インテントベース ネットワーク用に構築された次世代のワイヤレスコントローラです。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは Cisco IOS XE ベースであり、Aironet の優れた RF 性能と Cisco IOS XE のインテントベースのネットワーキング機能を統合して、組織にクラス最高水準のワイヤレスエクスペリエンスを生み出します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラはモジュール型オペレーティングシステムに基づいて構築され、オープンでプログラマブルな API 機能が搭載されていて、0 日目から N 日目のネットワーク運用を自動化できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、次のような複数のフォームファクタで使用できます。

- Catalyst 9800-40 ワイヤレス コントローラ
- Catalyst 9800-80 ワイヤレス コントローラ
- Catalyst 9800-CL Cloud ワイヤレスコントローラ：プライベートクラウド（ESXi、KVM、Cisco ENCS、および Hyper-V に展開可能、以下で管理可能 Cisco DNA Center
- Catalyst 9300 シリーズ スイッチ、Catalyst 9400 シリーズ スイッチ、および Catalyst 9500H シリーズ スイッチ用 Catalyst 9800 組み込みワイヤレスコントローラ
- Cisco Catalyst 9800-L ワイヤレスコントローラ：中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされている仮想プラットフォームおよびハードウェア プラットフォームを一覧表示します。

プラットフォーム	説明
Cisco Catalyst 9800-80 ワイヤレス コントローラ	最大 6000 アクセスポイントと 64,000 クライアントをサポートします。 最大 80 Gbps のスループットをサポートし、2 ラックユニットスペースを使用します。 最大100-GEのアップリンクおよびシームレスなソフトウェア アップデートを搭載したモジュール型ワイヤレス コントローラ。
Cisco Catalyst 9800-40 ワイヤレス コントローラ	シームレスなソフトウェアアップデートを備えた、中小企業やキャンパスでの導入向けの固定ワイヤレスコントローラ。 最大 2000 アクセスポイントと 32,000 クライアントをサポートします。 最大 40 Gbps のスループットをサポートし、1 ラックユニットスペースを使用します。 4 つの 1-GE または 10-GE アップリンクポートを提供します。
Cisco Catalyst 9800-CL Cloud ワイヤレス コントローラ	Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、プライベートクラウドまたはパブリッククラウドに Infrastructure as a Service（IaaS）として導入できます。 Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラは、ハイアベイラビリティとセキュリティを実現するために構築された次世代のエンタープライズクラスの仮想ワイヤレスコントローラです。 Cisco Catalyst 9800-CL クラウド ワイヤレスコントローラの仮想フォームファクタは、ESXi、KVM、Cisco ENCS、および Hyper-V ハイパーバイザをサポートするプライベートクラウド向けです。
Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラ	Catalyst 9000 シリーズスイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラは、有線およびワイヤレスインフラストラクチャを一貫したポリシーと管理とともに提供します。 この導入モデルは、小規模キャンパスや分散型ブランチ向けの安全性に優れたソリューションである Cisco SD-Access でのみサポートされます。組み込みコントローラは、ファブリック モードでのみアクセス ポイント（AP）をサポートします。

プラットフォーム	説明
Cisco Catalyst 9800-L ワイヤレス コントローラ	Cisco Catalyst 9800-L ワイヤレスコントローラは、中小企業向けにシームレスなソフトウェアアップデートを提供します。Cisco Catalyst 9800-L ワイヤレスコントローラは 2 つのバリエーションで使用できます。銅線と光ファイバアップリンクのいずれかを選択でき、ネットワークの柔軟性が向上します。 • Cisco Catalyst 9800-L Copper シリーズ ワイヤレス コントローラ（9800-L-C RJ45） • Cisco Catalyst 9800-L ファイバ シリーズ ワイヤレス コントローラ（9800-L-F SFP）

次の表に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされているホスト環境を一覧表示します。

ホスト環境	ソフトウェア バージョン
VMware ESXi	• VMware ESXi vSphere 6.0 • VMware ESXi vSphere 6.5[1] • VMware ESXi vCenter 6.0 • VMware ESXi VCenter 6.5
KVM	• Red Hat Enterprise Linux 7.1 および 7.2 をベースとした Linux KVM • Ubuntu 14.04.5 LTS、Ubuntu 16.04.5 LTS
NFVIS	Cisco ENCS 3.8.1 および 3.9.1

[1] ESXi vSphere を使用した C9800-CL の .ova ファイルのインストールは機能しません。これは C9800 ova に限定されませんが、他の製品に影響します。シスコと VMware は、問題解決に向けて積極的に取り組んでいます。問題が修正されたかどうかを確認するには、シスコのアカウント担当者にお問い合わせください。VMware 6.5 および C9800-CL OVA ファイルの展開に固有の問題があります。「必要なディスクイメージがありません。（A required disk image was missing）」という警告が表示され、「VM の展開に失敗しました：postNFCData に失敗しました：ディスク以外のファイルに POST できません。（Failed to deploy VM: postNFCData failed: Cannot POST to non-disk files.）」というエラーで展開が失敗します。VMware ESXi 6.5 に C9800-CL をインストールするには、次のいずれかを実行します。1）ESXi 組み込み GUI を使用して C9800-CL の .iso ファイルをインストールする（ESXI 6.5 クライアントバージョン 1.29.0 はテスト済みで必須）。2）OVF ツールを使用して C9800-CL の .ova ファイルをインストールする。

次の表に、Cisco DNA Center でサポートされている Cisco Enterprise Network Function Virtualization Infrastructure Software（NFVIS）のバージョンを示します。

（注） Cisco Enterprise NFVIS デバイスは、N-1 から N へのアップグレードパスのみをサポートします。たとえば、Cisco Enterprise NFVIS Release 3.10.x から Cisco Enterprise NFVIS 3.11.x へのアップグレードのみがサポートされています。Cisco Enterprise NFVIS リリース 3.10.x から Cisco Enterprise NFVIS リリース 3.12.x へのアップグレードはサポートされていません。

Cisco Enterprise NFVIS バージョン	エンタープライズ ネットワーク コンピューティング システム（**ENCS**）デバイス プラットフォーム	注
• 3.10.1 • 3.10.2 • 3.10.3 • 3.11.1 • 3.11.2 • 3.11.3 • 3.12.2	• ENCS 5400 • UCS-E • UCS-C	Cisco Enterprise NFVIS 3.12.1 は、Cisco DNA Center のいずれのバージョンでもサポートされていません。 • Cisco Enterprise NFVIS 3.12.1 は、Cisco DNA Center のいずれのバージョンでもサポートされていません。これは、Cisco Enterprise NFVIS 3.12.1 では、警告 CSCvq66963 の修正を利用できないためです。 • Cisco DNA Center 1.3.3 を使用した、Cisco Enterprise NFVIS 3.11.x から Cisco Enterprise NFVIS 3.12.x へのアップグレードはサポートされていません。 • Cisco DNA Center 1.3.3 を使用した、Cisco Enterprise NFVIS 3.12.2 から Cisco Enterprise NFVIS 3.12.1 へのアップグレードはサポートされていません。 Cisco Enterprise NFVIS 3.12.2 は、Cisco DNA Center 1.3.3 でサポートされています。 • Cisco DNA Center 1.3.3 を使用した、Cisco Enterprise NFVIS 3.11.2 から 3.12.2 へのアップグレード。 • Cisco Enterprise NFVIS 3.12.2 は、Cisco DNA Center 1.3.3 でサポートされています。
• 3.11.1 • 3.11.2 • 3.11.3 • 3.12.2	ENCS 5100	Cisco 5100 エンタープライズ ネットワーク コンピューティング システム（ENCS）は、Cisco Enterprise NFVIS 3.10.x をサポートしていません。

Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、Cisco Digital Network Architecture Center 設置ガイド [英語] を参照してください。

2. ソフトウェアイメージのアップグレードに関する詳細については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラでのソフトウェアイメージのアップグレードのサポート（50 ページ） を参照してください。

3. Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

   確認するには、Cisco DNA Center のホームページで、歯車アイコン をクリックし、**[System Settings]** > **[Software Updates]** > **[Installed Apps]** を選択します。

4. Cisco Identity Services Engine と Cisco DNA Center を連動させます。統合後、関連する設定やデータとともに Cisco DNA Center が検出されたデバイスは、Cisco ISE にプッシュされます。

5. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。

   詳細については、CDP を使用したネットワークの検出またはDiscover Your Network Using an IP Address Rangeを参照してください。

   ワイヤレス管理 IP アドレスを手動で追加する必要があります。

   [Discovery] ウィンドウで Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して検出を実行する場合は、[Preferred Management IP] ドロップダウンリストから [Use Loopback] を選択して、デバイスのループバック インターフェイスの IP アドレスを指定します。

6. 検出されたデバイスが [Device Inventory] ページに [Managed] 状態で表示されていることを確認します。

   詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

   デバイスが [Managed] 状態になるまで待機する必要があります。

7. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアシュアランス接続を確認するには、次のコマンドを使用します。

   - **#show crypto pki trustpoints | sec DNAC-CA**

```
Trustpoint DNAC-CA
    Subject Name:
```

```
    cn=kube-ca
          Serial Number (hex): 00E***************
    Certificate configured.
```

- **#show crypto pki trustpoints | sec sdn-network**

```
Trustpoint sdn-network-infra-iwan:
    Subject Name:
    cn=sdn-network-infra-ca
        Serial Number (hex): 378***************
    Certificate configured.
```

- **#show telemetry ietf subscription all**

```
Telemetry subscription brief

  ID               Type        State       Filter type
  ------------------------------------------------------
  1011             Configured  Valid       tdl-uri
  1012             Configured  Valid       tdl-uri
  1013             Configured  Valid       tdl-uri
```

- **#show telemetry internal connection**

```
Telemetry connection

Address Port Transport State Profile
------------------------------------------------------------
IP address 25103 tls-native Active sdn-network-infra-iwan
```

- **#show network-assurance summary**

```
Network-Assurance                       : True
Server Url                              : https://10.***.***.***
ICap Server Port Number                 : 3***
Sensor Backhaul SSID                    :
Authentication                          : Unknown
```

8. 認証サーバとポリシーサーバの設定時に TACACS サーバを設定します。

   Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでユーザ名をローカルに設定している場合、TACACS の設定は必須ではありません。

9. サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロードを参照してください。

   新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

10. APの位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

    詳細については、「AP の追加、配置、および削除」を参照してください。

11. AAA（Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバが、ネットワーク全体のデフォルトになります。AAA サーバを追加するときに、TACACS サーバを追加できます。

    詳細については、グローバルネットワーク設定について、グローバル ネットワーク サーバの設定、および「AAA サーバの追加」を参照してください。

12. カスタムとして、親プロファイルでワイヤレス無線周波数プロファイルを作成します。

    詳細については、「ワイヤレス無線周波数プロファイルの作成」を参照してください。

13. IP アドレスプールをグローバルレベルで作成します。

    Cisco DNA Center Cisco DNA Center は、IP アドレスプールを使用して、SD-Access ネットワークの設定と展開を自動化します。

    IP アドレスプールを作成するには、IP アドレス プールを設定するを参照してください。

    プロビジョニングするビルディング用に IP アドレスプールを予約する必要があります。詳細については、「LAN アンダーレイのプロビジョニング」を参照してください。

14. エンタープライズおよびゲスト ワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義します。次に、Cisco DNA Center は地理的な場所全体でさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず SSID を作成し、次に作成した SSID をワイヤレス ネットワーク プロファイルに関連付ける必要があります。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

    詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成およびゲスト ワイヤレス ネットワークの SSID の作成を参照してください。

15. バックホールの設定を行います。詳細については、「バックホールの設定の管理」を参照してください。

16. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの [Policy] ウィンドウで、次のように設定します。

    - 仮想ネットワークを作成する。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、仮想ネットワークおよび仮想ネットワークの作成を参照してください。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加する。詳細については、「グループベースのアクセス コントロール ポリシーの作成」を参照してください。

17. 高可用性を設定します。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する （51 ページ）」を参照してください。

18. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。

    詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （65 ページ）」を参照してください。

19. Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでアプリケーションポリシーを設定および展開します。

    詳細については、アプリケーションポリシーの作成、アプリケーション ポリシーの展開、およびアプリケーション ポリシーの編集を参照してください。

（注） アプリケーションポリシーを展開する前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスをプロビジョニングする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、2 つの異なる SSID で異なるビジネスとの関連性を持つ2つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスの場合、アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは機能しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラでのソフトウェアイメージのアップグレードのサポート

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出します。

  Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ を検出するには、NETCONF を有効にしてポートを 830 に設定します。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するためのメカニズムです。これにより、コントローラでワイヤレスサービスが有効になります。

  詳細については、CDP を使用したネットワークの検出またはDiscover Your Network Using an IP Address Rangeを参照してください。

- デバイスが [Device Inventory] に [Managed] 状態で表示されていることを確認します。

  詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

ステップ 1 Cisco DNA Center のホームページで、[Design] > [Image Repository] を選択するか、 **のホームページで [Image Repository] をクリックします。** > Cisco DNA Center

ステップ 2 ローカルコンピュータまたは URL から、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェアイメージをインポートします。

詳細については、「ソフトウェア イメージのインポート」を参照してください。

ステップ 3 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て」を参照してください。

ステップ 4 デバイスファミリまたは特定のデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークできます。

詳細については、「ゴールデン ソフトウェア イメージの指定」を参照してください。

ステップ 5 ソフトウェアイメージをプロビジョニングするには、Cisco DNA Center のホームページで [Provision] をクリックします。

[Devices] > [Inventory] ウィンドウが表示されます。 >

ステップ 6 [Inventory] ウィンドウで、アップグレードするイメージ Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の横にあるチェックボックスをオンにします。

ステップ 7 [Actions] ドロップダウンから、[Software Image] > [Update Image] を選択します。 >

詳細については、ソフトウェア イメージのプロビジョニングを参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定する

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性（HA）を設定するための前提条件となるタスクを次に示します。

- 両方の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスが同じソフトウェアバージョンを実行していて、プライマリ Catalyst 9800 シリーズ ワイヤレス コントローラ上にアクティブなソフトウェアイメージがあります。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 のサービスポートおよび管理ポートが設定されています。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の冗長ポートが物理的に接続されています。
- インターフェイス設定、ルート追加、SSH 回線設定、netconf-yang 設定などの事前設定は、Catalyst 9800 シリーズ ワイヤレス コントローラ アプライアンスで完了します。
- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 と Catalyst 9800 シリーズ ワイヤレス コントローラ 2 の管理インターフェイスは同じサブネット内にあります。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 デバイスおよび Catalyst 9800 シリーズ ワイヤレス コントローラ 2 デバイスのディスカバリとインベントリは、Cisco DNA Center から正常に実行されます。
- デバイスは到達可能で、[Managed] 状態になっています。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

ステップ 2 **[Devices]** > **[Inventory]** ウィンドウが表示され、検出されたすべてのデバイスがこのウィンドウに一覧表示されます。

ステップ 3 特定のサイトで使用可能なデバイスを表示するには、左側のペインで [Global] サイトを展開し、関心のあるサイト、ビルディング、またはフロアを選択します。

選択したサイトで使用可能なすべてのデバイスが [Inventory] ウィンドウに表示されます。

ステップ 4 [Device Type] リストから [WLCs] タブをクリックし、[Reachability] リストから [Reachable] タブをクリックして、検出済みで到達可能なワイヤレス コントローラのリストを取得します。

ステップ 5 [Inventory] ウィンドウで目的の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 名をクリックし、プライマリコントローラとして設定します。

ステップ 6 [High Availability] タブをクリックします

デフォルトで選択された Catalyst 9800 シリーズ ワイヤレス コントローラがプライマリコントローラになり、[Primary C9800] フィールドはグレー表示されます。

ステップ 7 [Select Primary Interface] および [Secondary Interface] ドロップダウンリストから、HA 接続に使用するインターフェイスを選択します。

HA インターフェイスは次の目的で使用されます。

- IOSd が起動する前に、コントローラペア間の通信を有効にする。
- すべてのコントローラペアに IPC のトランスポートを提供する。
- コントローラペア間で交換される制御メッセージ全体の冗長性を有効にする。制御メッセージには、HA ロールの解決、キープアライブ、通知、HA 統計情報などがあります。

ステップ 8 [Select Secondary C9800] ドロップダウン リストから、HA ペアを作成するセカンダリコントローラを選択します。

ステップ 9 各フィールドに [Redundancy Management IP] と [Peer Redundancy Management IP] のアドレスを入力します。

（注） 冗長性管理 IP およびピア冗長性管理 IP に使用される IP アドレスは、Catalyst 9800 シリーズ ワイヤレス コントローラの管理インターフェイスと同じサブネットに設定する必要があります。これらの IP アドレスがそのサブネット範囲内で未使用の IP アドレスであることを確認します。

ステップ 10 [Netmask] フィールドに、ネットマスクアドレスを入力します。

ステップ 11 [HA の設定（Configure HA）] をクリックします。

HA設定は、CLIコマンドを使用してバックグラウンドで開始されます。最初に、プライマリコントローラが設定されます。成功すると、セカンダリコントローラが設定されます。HAが有効になると、両方のデバイスが再起動します。このプロセスは、完了するまで最大 2.5 分かかります。

ステップ 12 HA が開始されたら、[High Availability] タブの [Redundancy Summary] に、[Sync Status] が [HA Pairing is in Progress]として表示されます。HA ペアリングが成功したことを Cisco DNA Center が検出すると、[Sync Status] が [Complete] になります。

これは、インベントリ ポーラーまたは手動による再同期によってトリガーされます。これで、セカンダリコントローラ（Catalyst 9800 シリーズ ワイヤレス コントローラ 2）が Cisco DNA Center から削除されます。このフローは、Catalyst 9800 シリーズ ワイヤレス コントローラ での正常な HA 設定を示しています。

ステップ 13 手動でコントローラを再同期するには、**[Provision]** > **[Inventory]** ウィンドウで、手動で同期するコントローラを選択します。

ステップ 14 [アクション（Actions）] ドロップダウンリストから、[再同期（Resync）] を選択します。

ステップ 15 プロセスが完了した後に発生するアクションのリストを次に示します。

- Catalyst 9800 シリーズ ワイヤレス コントローラ 1 および Catalyst 9800 シリーズ ワイヤレス コントローラ 2 は、冗長性管理、冗長性単位、およびシングルサインオン（SSO）を使用して設定されます。デバイスは、ロールをアクティブコントローラまたはスタンバイコントローラとしてネゴシエートするために再起動します。設定はアクティブからスタンバイへと同期されます。
- [冗長性の概要の表示（Show Redundancy Summary）] ウィンドウで、次の設定を確認できます。
  - SSO は有効
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 1 がアクティブ状態である
  - Catalyst 9800 シリーズ ワイヤレス コントローラ 2 がスタンバイ状態である

ハイ アベイラビリティについて

高可用性（HA）によって、コントローラのフェールオーバーが原因で生じるワイヤレスネットワークのダウンタイムを短縮できます。Cisco DNA Center を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の高可用性を設定できます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで高可用性を設定するためのコマンド

ステップ 1 次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのプライマリで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

次に、HA シャーシインターフェイスの設定例を示します。

```
chassis ha-interface GigabitEthernet 3 local-ip 1.1.1.2 255.255.255.0 remote-ip
1.1.1.3
```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 2 次のコマンドを使用して、Catalyst 9800 シリーズ ワイヤレス コントローラのセカンダリで HA を設定します。

- **chassis ha-interface GigabitEthernet <redundancy interface num> local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行して、HA シャーシインターフェイスを設定します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.3 255.255.255.0 remote-ip
  1.1.1.2
  ```

ステップ 3 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

ステップ 4 Cisco Catalyst 9800-40 ワイヤレスコントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのプライマリに HA を設定するには、次のコマンドを使用します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3
  ```

- **reload** コマンドを実行して、変更が有効になるようにデバイスをリロードします。

ステップ 5 次のコマンドを使用して、Cisco Catalyst 9800-40 ワイヤレス コントローラおよび Cisco Catalyst 9800-80 ワイヤレス コントローラ デバイスのセカンダリに HA を設定します。

- HA シャーシインターフェイスを設定するには、**chassis ha-interface local-ip <redundancy ip> <netmask> remote-ip <peer redundancy ip>** コマンドを実行します。

  次に、HA シャーシインターフェイスの設定例を示します。

  ```
  chassis ha-interface local-ip 1.1.1.3 255.255.255.0 remote-ip 1.1.1.2
  ```

ステップ 6 **chassis clear** コマンドを実行して、すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアまたは削除します。

（注） **reload** コマンドを実行して、変更を反映するためにデバイスをリロードします。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性を確認するためのコマンド

次のコマンドを使用して、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの高可用性設定を確認します。

- **config redundancy mode sso** コマンドを実行して、HA 関連の詳細情報を確認します。
- **show chassis** コマンドを実行して HA ペアのシャーシ設定を表示します。これには、MAC アドレス、ロール、スイッチプライオリティ、および冗長 HA ペア内の各コントローラデバイスの現在の状態が含まれています。
- **show ip interface brief** コマンドを実行して、プラットフォームで設定されている設定モードではなく、デバイスで実行されている実際に稼働中の冗長モードを表示します。
- **show redundancy states** コマンドを実行して、アクティブコントローラとスタンバイコントローラの冗長性状態を表示します。
- **show redundancy summary** コマンドを実行して、設定されているインターフェイスを確認します。
- ハイアベイラビリティ設定の詳細を確認するには、**show romvar** コマンドを実行します。

N+1 高可用性

N+1 高可用性の概要

Cisco DNA Center では、シスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォームでの N+1 高可用性（HA）がサポートされています。

HA-SKU を使用した N+1 HA は、Cisco 2504、5500、7500、および 8500 シリーズのスタンドアロンワイヤレス コントローラおよび WiSM2 コントローラでサポートされています。

N+1 HA アーキテクチャは、低い導入コストで、地理的に離れたデータセンターのコントローラに冗長性をもたらします。

N+1 HA では、単一のシスコ ワイヤレス コントローラを複数のプライマリ コントローラのバックアップコントローラとして使用できます。これらのワイヤレス コントローラは互いに独立していて、インターフェイスの設定や IP アドレスを共有しません。

Cisco DNA Center Cisco DNA Center は、N+1 HA のプライマリおよびセカンダリ コントローラの設定をサポートします。

N+1 HA 設定は、グローバル レベルではなく AP レベルで実施されます。設定は AP に直接プッシュされます。

AP フォールバック オプションが有効の場合、プライマリ ワイヤレス コントローラが動作を再開すると、AP はバックアップ ワイヤレス コントローラからプライマリ ワイヤレス コントローラに自動的にフォールバックします。

（注） プライマリコントローラとセカンダリコントローラは、同じデバイスタイプである必要があります。たとえば、プライマリデバイスが Catalyst 9800 シリーズ ワイヤレス コントローラの場合は、セカンダリデバイスも Catalyst 9800 シリーズ ワイヤレス コントローラにする必要があります。

プライマリコントローラで高い優先順位が設定されている AP は、優先順位の低い AP が排除されることになっても、常に最初にバックアップコントローラに接続されます。

N+1 HA 設定には次の制限があります。

- N+1 HA 設定は、非ファブリック展開でのみサポートされます。
- VLAN ID の設定が原因で、セカンダリコントローラの自動プロビジョニングはサポートされていません。
- プライマリコントローラに変更を加えた場合、最新の設計の設定を使用してセカンダリコントローラを手動で再プロビジョニングする必要があります。
- Cisco DNA Center Cisco DNA Center では耐障害性はサポートされていません。
- アクセスポイントのステートフル スイッチ オーバー（AP SSO）機能は、N+1 HA ではサポートされていません。AP Control and Provisioning of Wireless Access Points（CAPWAP）ステートマシンは、プライマリコントローラに障害が発生したときに再起動されます。

Cisco DNA Center から N+1 高可用性を設定するための前提条件

- [Discovery] 機能を実行して、プライマリコントローラとセカンダリコントローラを検出します。

  詳細については、CDP を使用したネットワークの検出またはDiscover Your Network Using an IP Address Rangeを参照してください。

- ワイヤレス コントローラ が到達可能で、管理対象状態である必要があります。

  詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

- デバイス間のネットワーク接続性を確認します。プライマリコントローラがダウンした場合、AP が N+1 の設定に従ってセカンダリコントローラに参加できるようにする必要があります。

- 2 つのビルディングを作成して、両方のデバイスのプライマリおよびセカンダリの場所を管理します。たとえば、ビルディング A とビルディング B のような 2 つのビルディングを作成し、ビルディング A をコントローラ 1 のプライマリ管理場所かつコントローラ 2 のセカンダリ管理場所に設定し、ビルディング B をコントローラ 2 のプライマリ管理場所としてのみ設定できます。

  詳細については、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

- 設計フェーズ中にカバレッジヒートマップが可視化されるようにするには、フロアマップに AP を追加して配置します。

  詳細については、「AP の追加、配置、および削除」を参照してください。

- 2つの SSID を作成し、バックホール SSID として関連付けます。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成、ゲスト ワイヤレス ネットワークの SSID の作成、およびバックホールの設定の管理を参照してください。

Cisco DNA Center からの N+1 高可用性の設定

この手順では、非ファブリック展開環境において、シスコ ワイヤレス コントローラ および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォームに N+1 高可用性（HA）を設定する方法について説明します。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devicses] > **[Inventory]** ページが表示され、検出されたすべてのデバイスがこのページに一覧表示されます。

ステップ 2 プライマリコントローラとしてプロビジョニングするには、目的のコントローラの隣にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 4 プライマリコントローラのプライマリ管理 AP 場所を割り当てるには、[Choose a site] をクリックします。

ステップ 5 [Choose a site] ウィンドウで、サイトを選択して [Save] をクリックします。

ステップ 6 [Next] をクリックします。

[Configuration] ウィンドウが表示され、プライマリデバイスのプライマリ管理対象 AP の場所が表示されます。

ステップ 7 [Select Primary Managed AP Locations] をクリックして、プライマリコントローラの管理対象 AP のロケーションを追加または更新できます。

ステップ 8 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 9 インターフェイスと VLAN の詳細を設定します。

ステップ 10 [Configure Interface and VLAN] 領域で、IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 11 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 12 [Summary] ウィンドウでプライマリコントローラの管理対象 AP の場所およびその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 13 次に、セカンダリコントローラをプロビジョニングします。

ステップ 14 [Inventory] ウィンドウで目的のコントローラの隣にあるチェックボックスをオンにし、セカンダリコントローラとしてプロビジョニングします。

ステップ 15 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** を選択します。

[サイトの割り当て（Assign Site）] ウィンドウが表示されます。

ステップ 16 セカンダリコントローラの管理対象 AP の場所を割り当てるには、[Choose a site] をクリックします。

セカンダリコントローラの管理対象 AP の場所は、プライマリコントローラの管理対象 AP の場所と同じにする必要があります。

ステップ 17 [Choose a site] ウィンドウで、セカンダリコントローラを関連付けるサイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

ステップ 18 **[次へ (Next)]** をクリックします。

[Configuration] ウィンドウが表示され、セカンダリデバイスのプライマリ管理対象 AP の場所とセカンダリ管理対象 AP の場所が表示されます。

ステップ 19 [Select Secondary Managed AP Locations）] をクリックして、セカンダリコントローラの管理対象 AP の場所を追加または更新できます。

ステップ 20 [Managed AP Location] ウィンドウで、サイト名の隣にあるチェックボックスをオンにして、[Save] をクリックします。

親サイトまたは個々のサイトのいずれかを選択できます。

ステップ 21 セカンダリコントローラのインターフェイスと VLAN の詳細を設定します。

ステップ 22 [Configure Interface and VLAN] 領域で、セカンダリコントローラの IP アドレスとサブネットマスクの詳細を設定し、[Next] をクリックします。

ステップ 23 [Advanced Configuration] ウィンドウで、事前定義されたテンプレート変数の値を設定し、[Next] をクリックします。

ステップ 24 [Summary] ウィンドウで、セカンダリコントローラの管理対象 AP の場所やその他の設定の詳細を確認し、[Deploy] をクリックします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 25 プライマリおよびセカンダリコントローラの管理対象場所を確認するには、**[Provision]** > **[Devices]** > **[Inventory]** ウィンドウでプロビジョニングしたコントローラのデバイス名をクリックします。

ステップ 26 [Device details] ウィンドウで、[Managed ap locations] タブをクリックして、プライマリおよびセカンダリの管理対象場所の詳細を表示します。

ステップ 27 プライマリコントローラの AP をプロビジョニングします。

ステップ 28 **[Devices]** > **[Inventory]** ウィンドウで、プロビジョニングする AP の隣にあるチェックボックスをオンにします。

ステップ 29 [Actions] ドロップダウンリストから、**[Provision]** > **[Provision]** を選択します。

ステップ 30 [Assign Site] ウィンドウで、[Choose a Floor] をクリックして、プライマリの管理対象場所からフロアを選択します。

ステップ 31 [Next] をクリックします。

[設定（Configuration）] ウィンドウが表示されます。

ステップ 32 デフォルトでは、**[Design]** > **[Network Settings]** > **[Wireless]** > **[Wireless Radio Frequency Profile]** でデフォルトとマークしたカスタム RF プロファイルが、**[RF Profile]** ドロップダウンリストで選択されています。

[RF プロファイル（RF Profile）] ドロップダウンリストから値を選択して、AP のデフォルト RF プロファイル値を変更できます。

ステップ 33 **[次へ (Next)]** をクリックします。

ステップ 34 [Summary] ウィンドウで、詳細を確認します。

ステップ 35 [Deploy] をクリックして、プライマリ AP をプロビジョニングします。

ステップ 36 AP グループの作成または変更が進行中であることを示すメッセージが表示されます。

「プロビジョニング後にAPがリブートします。続行しますか?（`After provisioning AP(s) will reboot. Do you want to continue?`」というメッセージが表示されます。

ステップ 37 [OK] をクリックします。

展開が成功すると、[Device Inventory] ウィンドウの [Last Sync Status] 列に、[SUCCESS] と表示されます。

モビリティ設定の概要

Cisco DNA Center のモビリティ設定では、一連の シスコ ワイヤレス コントローラ をモビリティグループにグループ化して、ワイヤレスクライアントのシームレスなローミング体験を実現できます。

モビリティグループを作成すると、ネットワーク内で複数のワイヤレスコントローラを有効にして、コントローラ間またはサブネット間のローミングが発生した際に、動的に情報を共有してデータトラフィックを転送できます。異なるモビリティグループ名を同じ無線ネットワーク内の異なる ワイヤレス コントローラ に割り当てると、モビリティグループによって、1 つの企業内の異なるフロア、ビルディング、キャンパス間でのローミングを制限できます。

Cisco DNA Center では、 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラなどのさまざまなプラットフォーム間でモビリティグループを作成できます。

モビリティ設定の注意事項と制約事項：

- [Provision] ページでは、モビリティを設定するために複数のコントローラを選択することはできません。
- グループ名をデフォルトにしてモビリティグループを作成することはできません。これにより、モビリティおよび RF グループ名がデフォルトとしてリセットされ、すべてのピアが削除されます。
- アンカーコントローラでモビリティグループ名を設定することはできません。
- Cisco AireOS コントローラでモビリティグループを設定しているときに仮想 IP アドレスが変更された場合は、ワイヤレス コントローラ を手動で再起動する必要があります。
- 同じモビリティグループ名を持つワイヤレスコントローラは、自動的に 1 つのモビリティグループにグループ化され、互いにピアとして追加されます。
- Cisco AireOS コントローラでモビリティグループを設定するときに、ワイヤレス コントローラ に IP アドレス 192.0.2.1 がない場合、 Cisco DNA Center は仮想 IP アドレス（192.0.2.1）をすべての ワイヤレス コントローラ にプッシュします。
- ゲストアンカーコントローラをモビリティグループに明示的に追加しないでください。プロビジョニングされたゲストアンカーコントローラは、[mobility configuration] ページでピアを追加している間、ドロップダウンリストに表示されません。
- ワイヤレス コントローラ をゲストアンカーとしてプロビジョニングする場合は、それがモビリティグループに追加されていないことを確認します。

モビリティ設定ワークフロー

次に、シスコ ワイヤレス コントローラ でモビリティを設定するために使用できるワークフローを示します。

- モビリティ設定は、[Provision] ページの [Configuration] ウィンドウで使用できます。
- モビリティを設定するには、モビリティグループ名、RF グループ名、およびモビリティピアを使用して ワイヤレス コントローラ をプロビジョニングする必要があります。
- ワイヤレス コントローラ のプロビジョニング中に適用される設定は、そのグループに設定されているすべてのモビリティピアに自動的に複製されます。
- ワイヤレス コントローラ を再同期して、最新のトンネルステータスを取得します。

モビリティ設定の使用例

次の使用例では、コントローラ間のモビリティの設定手順について説明します。

使用例 1

シスコ ワイヤレス コントローラ 1、 ワイヤレス コントローラ 2、および ワイヤレス コントローラ 3 は、モビリティグループ名（デフォルト）を使用して Cisco DNA Center に新たに追加されていて、まだプロビジョニングされていません。

1. モビリティグループ名、RF グループ名を設定し、ワイヤレス コントローラ 2 および ワイヤレス コントローラ 3 をピアとして追加することによって、ワイヤレス コントローラ 1 をプロビジョニングします。
2. ワイヤレス コントローラ 2 をプロビジョニングします。

   [Provision] ウィンドウでは、ワイヤレス コントローラ 2 のモビリティ設定がグループ名とピアとともに自動的に入力されます。
3. ワイヤレス コントローラ 3 をプロビジョニングします。
4. すべての ワイヤレス コントローラ をプロビジョニング後、ワイヤレス コントローラ を再同期して、最新のトンネルステータスを受信します。

使用例 2

異なるモビリティグループ名を持つシスコ ワイヤレス コントローラ 1、ワイヤレス コントローラ 2、および ワイヤレス コントローラ 3はすでに Cisco DNA Center に追加され、プロビジョニングされています。

1. モビリティグループ名、RF グループ名を設定してワイヤレス コントローラ 1 をプロビジョニングし、ピアとしてワイヤレス コントローラ 2 およびワイヤレス コントローラ 3 を追加します。
2. モビリティ設定は、 ワイヤレス コントローラ 2、 ワイヤレス コントローラ 3 などの他のピア間で自動的に複製されます。
   - ワイヤレス コントローラ 1 のプロビジョニングが成功すると、ワイヤレス コントローラ 2 と ワイヤレス コントローラ 3 がピアとして ワイヤレス コントローラ 1 に追加されます。
   - ワイヤレス コントローラ 1 と ワイヤレス コントローラ 3 は、ワイヤレス コントローラ 2 のピアとして追加されます。
   - ワイヤレス コントローラ 1 と ワイヤレス コントローラ 2 は、ワイヤレス コントローラ 3 のピアとして追加されます。

N+1 ローリング AP アップグレードについて

ローリング AP アップグレード機能は、N+1 ハイアベイラビリティ設定の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でのみサポートされます。この機能は、ワイヤレス LAN ネットワーク内の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に関連付けられている AP のソフトウェアイメージをアップグレードするのに便利です。ゼロダウンタイムを実現するために、N+1 ローリング AP アップグレード機能を使用して、段階的に AP をアップグレードすることができます。

プライマリコントローラは、無線リソース管理ネイバー AP マップを使用して、候補の AP を識別します。アップグレードプロセスは、イメージが候補の AP に事前ダウンロードされている間に、ソフトウェアイメージをプライマリコントローラにダウンロードすることから始まります。候補の AP がアップグレードされて再起動されると、これらの AP は、セカンダリコン

トローラに段階的に参加します。すべての AP がセカンダリコントローラに参加した後、プライマリコントローラは再起動します。これらの AP は、再起動された後、段階的にプライマリコントローラに再度参加します。

次に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のローリング AP アップグレードを設定するための前提条件を示します。

- 2 つの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（1 つはプライマリコントローラ、もう 1 つはセカンダリとして）の N+1 ハイアベイラビリティ設定。
- プライマリコントローラと N+1 コントローラの設定は同じで、ネットワーク内の同じ場所を管理します。
- N+1 コントローラではすでにゴールデンイメージが実行されているため、ローリング AP アップグレードはダウンタイムなしで動作します。

  ゴールデンイメージは、ネットワークデバイスの標準化されたイメージであり、Cisco DNA Center は Cisco.com からイメージを自動的にダウンロードします。イメージの標準化は、デバイスのセキュリティと、デバイスのパフォーマンスの最適化に役立ちます。
- N+1 コントローラはに到達可能であり、Cisco DNA Center で [Managed] 状態になっています。
- 両方のコントローラが同じモビリティグループの一部であり、プライマリコントローラと N+1 コントローラの間にモビリティトンネルが確立されます。プライマリコントローラと N+1 コントローラ間のアップグレード情報は、モビリティトンネルを介して交換されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのローリング AP アップグレードを設定するためのワークフロー

始める前に

（注） N+1 ローリング AP アップグレードは、ファブリック以外の導入でのみサポートされています。

ステップ 1 Cisco DNA Center を設置します。

詳細については、Cisco Digital Network Architecture Center 設置ガイド [英語] を参照してください。

ステップ 2 Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

確認するには、Cisco DNA Center のホームページで、歯車アイコン をクリックし、**[System Settings]** > **[Software Updates]** > **[Installed Apps]** を選択します。

確認するには、Cisco DNA Center のホームページで、歯車アイコン をクリックし、**[System Settings]** > **[Software Updates]** > **[Installed Apps]** を選択します。

ステップ 3 ディスカバリ機能を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを検出します。

Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。

詳細については、CDP を使用したネットワークの検出またはDiscover Your Network Using an IP Address Rangeを参照してください。

ステップ 4 検出されたデバイスが [Device Inventory] ウィンドウに [Managed] 状態で表示されていることを確認します。

詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

デバイスが [Managed] になるまで待機する必要があります。

ステップ 5 サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロードを参照してください。

新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

ステップ 6 AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

詳細については、「AP の追加、配置、および削除」を参照してください。

ステップ 7 プライマリ管理対象 AP の場所、およびローリング AP アップグレードが有効になっており、モビリティグループがセカンダリコントローラをピアとして設定されている状態で、プライマリコントローラをプロビジョニングします。

これを行うには、**[Provision]** > **[Devices]** > **[Inventory]** を選択し、プライマリコントローラ名の隣にあるチェックボックスをオンにします。

ステップ 8 モビリティグループ設定で、モビリティピアとして N+1 コントローラを設定します。

詳細については、「モビリティ設定の概要 （59 ページ）」を参照してください。

ステップ 9 プライマリコントローラのプライマリ管理対象 AP の場所を N+1 コントローラのセカンダリ管理対象 AP の場所として設定することによって、N+1 HA コントローラをプロビジョニングします。これにより、セカンダリコントローラが N+1 コントローラとして設定されます。

詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （65 ページ）」を参照してください。

ステップ 10 プライマリコントローラに関連付けられている AP をプロビジョニングします。

詳細については、「シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （37 ページ）」を参照してください。

ステップ 11 ソフトウェアイメージをリポジトリにインポートします。

詳細については、「ソフトウェア イメージのインポート」を参照してください。

ステップ 12 ソフトウェアイメージをデバイスファミリに割り当てます。

詳細については、「デバイスファミリへのソフトウェアイメージの割り当て」を参照してください。

ステップ 13 デバイスファミリまたはデバイスロールの星印をクリックして、ソフトウェアイメージをゴールデンとしてマークします。

詳細については、「ゴールデン ソフトウェア イメージの指定」を参照してください。

ステップ 14 イメージをアップグレードする前に、両方のデバイスでイメージの準備状況チェックが成功していることを確認してください。

また、[N+1 Device Check] と [Mobility Tunnel Check] のステータスに緑色のチェックマークが付いていることも確認してください。

- イメージ更新の準備状況チェックを実行するには、**[Provision]** > **[Devices]** > **[Software Images]** を選択します。
- イメージをアップグレードするデバイスを選択します。
- デバイスの事前チェックが成功すると、[Image Precheck Status] 列の [Status] リンクに緑色のチェックマークが付きます。デバイスのアップグレード準備状況の事前チェックのいずれかが失敗した場合、[Image Precheck Status] リンクのマークが赤色に変わり、そのデバイスの OS イメージは更新できません。先に進む前に [Status] リンクをクリックし、エラーを修正します。

ステップ 15 プライマリコントローラでアップグレードを開始します。

ステップ 16 **[Provision]** > **[Devices]** > **[Software Images]** ページで、プライマリコントローラの隣にあるチェックボックスをオンにします。

ステップ 17 [Actions] ドロップダウンリストから、**[Software Image]** > **[Update Image]** を選択します。

詳細については、「ソフトウェア イメージのプロビジョニング」を参照してください。

ステップ 18 イメージのアップグレードの進行状況をモニタするには、[Software Image] 列で [In Progress] をクリックします。

[Device Status] ページには、次の情報が表示されます。

- [Distribution Operation]：イメージ配信プロセスに関する情報が表示されます。イメージは Cisco DNA Center からプライマリデバイスにコピーされます。アクティブ化操作は、配信プロセスが完了すると開始されます。
- [Activate Operation]：アクティブ化操作の詳細が表示されます。このプロセス中に、ローリング AP アップグレードが開始されます。
- [Rolling AP Upgrade Operation]：ローリング AP アップグレードタスクが完了したかどうか、保留中の AP の数、再起動中の AP の数、N+1 コントローラに接続している AP の数など、ローリング AP アップグレードの概要が表示されます。

[View AP Status] をクリックすると、プライマリコントローラ、N+1 コントローラ、デバイス名、現在のステータス、および反復に関する詳細が表示されます。

Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のプロビジョニングを行う前に、Cisco DNA Center で Cisco Catalyst 9800 ワイヤレスコントローラを設定するためのワークフロー （47 ページ） の手順を完了したことを確認します。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devices] > [Inventory] > ウィンドウに、検出されたデバイスのリストが表示されます。

ステップ 2 サイトに関連付ける Catalyst 9800 シリーズ ワイヤレス コントローラ 名の横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Provision] > [Assign Device to Site] を選択します。 >

ステップ 4 [Assign Device To Site] ウィンドウで、[Choose a Site] をクリックし、Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けるサイトを選択します。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。このチェックボックスをオフにすると、個々のサイトの選択を解除できます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。

ステップ 8 設計フェーズ中に追加された設定を使用して、デバイスをプロビジョニングします。

ステップ 9 **[Provision]** > **[Devices]** > **[Inventory]** の順に選択します。

ステップ 10 プロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラ 名の横にあるチェックボックスをオンにします。

ステップ 11 [Actions] ドロップダウンリストから、[Provision] > [Provision] を選択します。 >

ステップ 12 [Assign Site] ウィンドウで、[Next] をクリックします。

[設定（Configuration）] ウィンドウが表示されます。

ステップ 13 Catalyst 9800 シリーズ ワイヤレス コントローラ のワイヤレスコントローラのロールとして [Active Main WLC] または [Guest Anchor] を選択します。

ステップ 14 プライマリ コントローラの管理 AP の場所を設定するには、[Select Primary Managed AP Locations] をクリックします。

ステップ 15 [Select Secondary Managed AP Locations] をクリックして、セカンダリ管理 AP の場所のセカンダリコントローラをプライマリ管理 AP の場所のプライマリコントローラとして設定します。

ステップ 16 親サイトまたは個々のサイトのいずれかを選択できます。親サイトを選択すると、その下にあるすべての子も選択されます。チェックボックスをオフにして、特定のサイトの選択を解除することができます。

（注） 管理 AP の場所を継承することで、サイトおよび特定のサイトのビルディングとフロアを自動的に選択できます。1 つのサイトは 1 つの ワイヤレス コントローラ によってのみ管理されます。

ステップ 17 [Rolling AP Upgrade] エリアで、[Enable] チェックボックスをオンにして、ローリング AP アップグレードステータスを有効にします。

ローリング AP アップグレードの詳細については、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのローリング AP アップグレードを設定するためのワークフロー （62 ページ） を参照してください。

（注） ローリング AP アップグレード操作は、ファブリック対応のゲストアンカーデバイスではサポートされていません。

ステップ 18 [AP Reboot Percentage] ドロップダウンリストから、反復 1 回で再起動される AP の割合を選択します。アップグレードをずらす必要があるため、再起動プロセスを実行する AP のサブセットのみを選択します。そのため、これらの AP に接続されているすべてのクライアントは、リージョン内の他の AP に安全にステアリングされます。

ステップ 19 [Mobility Group] で [Configure] をクリックして、モビリティピアを設定します。

[Configure Mobility Group] サイドパネルが表示されます。

詳細については、「モビリティ設定の概要 （59 ページ）」を参照してください。

ステップ 20 [Mobility Group Name] ドロップダウンリストで、 をクリックして新しいモビリティグループを追加するか、既存のモビリティグループの中から選択することができます。

既存のモビリティピア情報は、 Cisco DNA Center で使用可能なインテントからロードされます。

ステップ 21 [RF Group Name] テキストボックスに RF グループの名前を入力します。

ステップ 22 [Mobility Peers] で [Add] をクリックして、モビリティピアを設定します。

ステップ 23 [Device Name] ドロップダウンリストからコントローラを選択します。

デバイスがプロビジョニングされると、 Cisco DNA Center はデバイスにモビリティグループを作成し、RF グループを割り当て、ピアのすべての終端を設定します。モビリティグループの設定は、選択したすべてのピアデバイスに自動的に展開されます。

ステップ 24 **[Save]** をクリックします。

ステップ 25 モビリティグループ名と RF グループ名をリセットするには、次のいずれかの方法を実行します。

- [Configure Mobility Group] サイドパネルで、[Mobility Group Name] ドロップダウンリストから [default] を選択します。
- **[Provision]** > > **[Configuration]** ページの [Mobiliy Group] で、[Reset] をクリックします。

これにより、[RF Group Name] が自動的に [default] に設定され、すべてのピアが削除されます。プロビジョニングが完了すると、デバイスのモビリティが設定され、そのデバイスは他のすべてのピアから削除されます。

ステップ 26 アクティブなメインのワイヤレスコントローラでは、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 27 [Assign Interface] エリアで、次の操作を実行します。

- [VLAN ID]：VLAN ID の値を入力します。
- [IP Address]：インターフェイス IP アドレスを入力します。
- [Gateway IP Address]：ゲートウェイ IP アドレスを入力します。
- [Subnet Mask (in bits)]：インターフェイスのネットマスクの詳細を入力します。

（注） Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネット マスクを割り当てる必要はありません。

ステップ 28 **[次へ (Next)]** をクリックします。

[Advanced Configuration] ウィンドウが表示されます。ここでは、事前定義されたテンプレート変数の値を入力できます。

ステップ 29 [Devices] パネルでデバイスまたはテンプレートを検索します。

ステップ 30 [wlanid] テキストフィールドに、事前定義されたテンプレート変数の値を入力します。

ステップ 31 **[次へ (Next)]** をクリックします。

ステップ 32 [Summary] ウィンドウで、次の設定を確認します。

- デバイスの詳細
- ネットワークの設定
- SSID
- 管理サイト
- インターフェイス
- 詳細設定

ステップ 33 [Deploy] をクリックして、Catalyst 9800 シリーズ ワイヤレス コントローラ をプロビジョニングします。

- デバイスをすぐに展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻でデバイスの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

ステップ 34 Cisco DNA Center からデバイスにプッシュされる設定を確認するには、Catalyst 9800 シリーズ ワイヤレス コントローラ で次のコマンドを使用します。

- **#show wlan summary**
- **#show run | sec line**
- **#show running-configuration**

ステップ 35 デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 36 [Inventory] ウィンドウで、デバイスの [Provision Status] カラムの [See Details] をクリックし、ネットワークインテントの詳細情報を取得するか、アクションのリストを表示します。

ステップ 37 [Device Provisioning] の下の [See Details] をクリックします。

ステップ 38 [Deployment of network intent] の下の [View Details] をクリックし、デバイス名をクリックします。

ステップ 39 デバイス名をクリックして展開します。

ステップ 40 [Configuration Summary] エリアを展開して、操作の詳細、機能名、および管理機能を表示します。また、[Configuration Summary] には、デバイスのプロビジョニング中に発生したエラーも理由とともに表示されます。

ステップ 41 デバイスに送信される正確な設定の詳細を表示するには、[Provision Summary] エリアを展開します。

ステップ 42 AP をプロビジョニングします。

詳細については、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （37 ページ）を参照してください。

Cisco Embedded Wireless Controller on Catalyst Access Points 対応 Day 0 ワークフロー

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ（EWC AP）は、次世代の Wi-Fi ソリューションであり、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に Cisco Catalyst 9100 シリーズアクセスポイントを統合し、進化および成長し続ける組織にそのクラスで最高のワイヤレスエクスペリエンスをもたらします。

始める前に

- サイト、ビルディング、フロアなどのネットワーク階層を設計します。

  詳細については、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

- CLI、SNMP、HTTP、HTTPS などのデバイスログイン情報をグローバルレベルで定義します。グローバルレベルで定義されたログイン情報は、サイトによって継承されます。

  詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、およびグローバル SNMPv3 クレデンシャルの設定を参照してください。

- SSID、ワイヤレスインターフェイス、および無線周波数プロファイルを作成します。

  詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成、ゲスト ワイヤレス ネットワークの SSID の作成、ワイヤレスインターフェイスの作成、およびワイヤレス無線周波数プロファイルの作成を参照してください。

（注） Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ では、Flex ベースの SSID の作成のみがサポートされています。

- Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が接続されているスイッチでオプション #43 を使用して DHCP サーバを設定します。これは Cisco DNA Center プラグアンドプレイサーバの IP アドレスです。これを使用して、AP は PnP サーバに接続し、設定をダウンロードします。
- インベントリに Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ があることを確認します。ない場合は、ディスカバリ機能を使用して検出します。詳細については、CDP を使用したネットワークの検出、Discover Your Network Using an IP Address Range、および インベントリについてを参照してください。
- AP は、シスコ ワイヤレス コントローラ 設定なしで初期設定へリセットされた状態である必要があります。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ は、次のような複数のフォームファクタで使用できます。

- Catalyst 9115AX アクセスポイント上の Cisco 組み込みワイヤレスコントローラ
- Catalyst 9117AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9120AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ
- Catalyst 9130AX アクセスポイントの Cisco 組み込みワイヤレスコントローラ

ステップ 1 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が DHCP サーバと通信します。

DHCP サーバは、応答で、オプション #43 とともに IP アドレスを提供します。オプション #43 には、Cisco プラグアンドプレイサーバの IP アドレスが含まれています。

ステップ 2 オプション #43 に基づいて、 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ はプラグアンドプレイ エージェントをオンにし、Cisco DNA Center プラグアンドプレイサーバに接続します。

（注） ネットワーク内に Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ のセットがある場合、それらは内部プロトコルを通過します。プロトコルは、PnP サーバに到達するためにシスコ ワイヤレス コントローラ 上でプライマリ AP として設定されている 1 つの Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を選択します。

ステップ 3 [Provision] > [Devices] > [Plug and Play] タブで未要求 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を検索します。 > >

テーブルには、すべての未要求デバイスが一覧表示されます。[State] 列が [Unclaimed] として表示されます。[Filter] または [Find option] を使用して、特定のデバイスを検索することができます。

[Onboarding State] 列の下でオンボーディングステータスが [Initialized] になるまで待つ必要があります。

ステップ 4 Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ を要求するには、AP デバイス名の横にあるチェックボックスをオンにします。

ステップ 5 デバイステーブルの上にあるメニューバーで、[Actions] > [Claim] の順に選択します。 >

[Claim Devices] ウィンドウが表示されます。

ステップ 6 [Site Assignement] ウィンドウで、[Site] ドロップダウンリストからサイトを選択します。

選択された AP のこの特定のサイトに対する要求は、関連付けられている構成にも適用されます。

ステップ 7 **[次へ (Next)]** をクリックします。

ステップ 8 デバイスを設定するには、[Configuratio] ウィンドウのデバイス名をクリックします。

ステップ 9 [Configuration for device name] ページで、デバイスの静的 IP の詳細を割り当てます。

- **[Management IP]**
- **[Subnet Mask]**
- **[Gateway]**

ステップ 10 **[Save]** をクリックします。

ステップ 11 **[次へ (Next)]** をクリックします。

[概要（Summary）] ページが表示されます。

ステップ 12 [Summary] ページで [Claim] をクリックします。

Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ が要求されると、設定された IP アドレスが Cisco Embedded Wireless Controller に割り当てられます。

ステップ 13 要求されたデバイス（内部 AP を備えた Cisco Embedded Wireless Controller）は、[Provision] > [Devices] > [Inventory] ウィンドウの下で使用可能になりました。 > >

ステップ 14 AP をプロビジョニングするには、シスコ製 AP のプロビジョニング：Day 1 AP プロビジョニング （37 ページ） を参照してください。

ステップ 15 追加の Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ をプロビジョニングするには、Cisco AireOS コントローラのプロビジョニング （29 ページ） を参照してください。

ステップ 16 CSV ファイルからデバイスを一括インポートするには、デバイスの一括追加 （12 ページ） を参照してください。

ステップ 17 デバイスを手動で追加するには、「デバイスの追加または編集」を参照してください。

Catalyst 9000 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラの設定とプロビジョニング

サポートされているハードウェア プラットフォーム

デバイス ロール	プラットフォーム
組み込みワイヤレスコントローラ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ

デバイス ロール	プラットフォーム
	Cisco Catalyst 9500-H シリーズ スイッチ
ファブリック エッジ	Cisco Catalyst 9300 シリーズ スイッチ Cisco Catalyst 9400 シリーズ スイッチ Cisco Catalyst 9500-H シリーズ スイッチ Cisco Catalyst 3600 シリーズ スイッチ Cisco Catalyst 3850 シリーズ スイッチ
AP	Cisco 802.11ac Wave 2 AP： • Cisco Aironet 1810 シリーズ OfficeExtend アクセス ポイント • Cisco Aironet 1810W シリーズ アクセス ポイント • Cisco Aironet 1815i Access Point • Cisco Aironet 1815w アクセスポイント • Cisco Aironet 1815m アクセス ポイント • Cisco 1830 Aironet シリーズ アクセスポイント • Cisco Aironet 1850 シリーズ アクセス ポイント • Cisco Aironet 2800 シリーズ アクセス ポイント • Cisco Aironet 3800 シリーズ アクセス ポイント • Cisco Aironet 4800 シリーズ アクセス ポイント Cisco 802.11ac Wave 1 AP • Cisco Aironet 1700 シリーズ アクセス ポイント • Cisco Aironet 2700 シリーズ アクセス ポイント • Cisco Aironet 3700 シリーズ アクセス ポイント

事前設定

Catalyst 9300 シリーズ スイッチ用 Cisco Catalyst 9800 組み込みワイヤレス コントローラ で、スイッチが **aaa new-model** ですでに設定されている場合は、次のコマンドが存在することを確認してください。

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
```

これは、NETCONF の設定では必須です。プロビジョニングに自動アンダーレイを使用している場合、これらの設定は必要ありません。

Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー

1. Cisco DNA Center をインストールします。

   詳細については、『CISCO DNA Center インストール ガイド』を参照してください。

2. Cisco DNA Center GUI にログインし、必要なアプリケーションが**実行**状態であることを確認します。

   確認するには、Cisco DNA Center のホームページで、歯車アイコン をクリックし、**[System Settings]** > **[Software Updates]** > **[Installed Apps]** を選択します。

3. Cisco Identity Services Engine と Cisco DNA Center を連動させます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。

4. Cisco Catalyst 9000 シリーズスイッチおよびエッジスイッチを検出します。

   Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラを検出するには、NETCONF を有効にし、ポートを 830 に設定する必要があります。

   エッジスイッチを検出するために NETCONF を有効にする必要はありません。

   詳細については、CDP を使用したネットワークの検出およびDiscover Your Network Using an IP Address Rangeを参照してください。

   [Preferred Management IP] を [Use Loopback] に変更します。

5. デバイスが [Device Inventory] に**管理対象**状態で表示されていることを確認します。

   詳細については、インベントリについておよびインベントリに関する情報の表示を参照してください。

   デバイスが**管理対象**状態になっていることを確認します。

6. ネットワークの地理的な場所を表すネットワーク階層を設計します。サイト、ビルディング、フロアを作成すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

   新しいネットワーク階層を作成します。または Cisco Prime Infrastructure に既存のネットワーク階層がある場合は、それを Cisco DNA Center にインポートできます。

   既存のネットワーク階層をインポートしてアップロードするには、既存のサイト階層をアップロードを参照してください。

   新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

7. 非ファブリックネットワークで設計フェーズ中にヒートマップの可視化を取得するには、フロアマップに AP を追加して配置します。

ファブリックネットワークの場合、設計時にフロアマップに AP を配置することはできません。APは、ファブリックネットワークにデバイスを追加した後にオンボードされます。

詳細については、「AP の追加、配置、および削除」を参照してください。

8. AAA（Cisco ISE がネットワークおよびクライアントエンドポイント用に設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、および SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバが、ネットワーク全体のデフォルトになります。

   詳細については、グローバルネットワーク設定について、グローバルネットワーク サーバの設定、および「AAA サーバの追加」を参照してください。

9. CLI、SNMP、HTTP などのデバイスクレデンシャルを設定します。

   詳細については、グローバル デバイス クレデンシャルについて、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、グローバル HTTPS クレデンシャルの設定を参照してください。

10. IP アドレスプールをグローバルレベルで設定します。

    IP アドレスプールを設定するには、IP アドレス プールを設定するを参照してください。

    プロビジョニングするビルディングの IP アドレスプールを予約するには、「LAN アンダーレイのプロビジョニング」を参照してください。

11. エンタープライズおよびゲストワイヤレス ネットワークを作成します。グローバルワイヤレス設定を 1 回定義すると、Cisco DNA Center はあらゆる場所にあるさまざまなデバイスに設定をプッシュします。

    ワイヤレスネットワークの設計は、2 段階のプロセスです。まず、[Wireless] ページで SSID を作成する必要があります。次に、作成した SSID をワイヤレス ネットワーク プロファイルに関連付けます。このプロファイルは、サイトにデバイスを展開するために使用されるトポロジを構築するのに役に立ちます。

    詳細については、エンタープライズ ワイヤレス ネットワーク用 SSID の作成およびゲスト ワイヤレス ネットワークの SSID の作成を参照してください。

12. バックホールの設定を行います。詳細については、「バックホールの設定の管理」を参照してください。

13. [Policy] ページで、次のように設定します。

    - 仮想ネットワークを作成する。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。詳細については、仮想ネットワークおよび仮想ネットワークの作成を参照してください。
    - グループベースのアクセス コントロール ポリシーを作成し、契約を追加する。詳細については、「グループベースのアクセス コントロール ポリシーの作成」を参照してください。

14. 設計フェーズ中に追加された設定を使用して、Cisco Catalyst 9000 シリーズスイッチとエッジノードスイッチをプロビジョニングします。
    - ファブリックドメインを作成する。
    - CP+ボーダー+エッジまたはCP+ボーダーを作成して、デバイスをファブリックネットワークに追加します。
    - Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラで、組み込みワイヤレス機能を有効にします。
    - ファブリックドメイン内のオンボード AP。

    デバイスが正常に展開されると、展開ステータスが [Configuring] から [Success] に変わります。

Cisco Catalyst 9000 シリーズ スイッチでの組み込みワイヤレスのプロビジョニング

始める前に

Catalyst 9000 シリーズ スイッチの Cisco Catalyst 9800 組み込みワイヤレスコントローラをプロビジョニングする前に、Catalyst 9000 スイッチ用 Cisco Catalyst 9800 組み込みワイヤレスコントローラを設定するためのワークフロー （72 ページ）の手順を完了していることを確認します。

この手順では、Cisco Catalyst 9300 シリーズ スイッチ、Cisco Catalyst 9400 シリーズ スイッチ、および Cisco Catalyst 9500H シリーズ スイッチに組み込みワイヤレスをプロビジョニングする方法について説明します。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devices] > **[Inventory]**ウィンドウに、検出されたデバイスのリストが表示されます。

ステップ 2 Catalyst 9000 シリーズ スイッチデバイスと、サイトに関連付けるエッジスイッチの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Provision] > [Assign Device to Site] を選択します。 >

ステップ 4 [Assign Device to Site] ウィンドウで、[Choose a Site] をクリックします。

ステップ 5 [Choose a site] ウィンドウで、サイトの横にあるチェックボックスをオンにして、デバイスを関連付けます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。
次の手順では、設計フェーズ中に追加された設定を使用して、Catalyst 9000 シリーズ スイッチとエッジノードをプロビジョニングします。

ステップ 8 [Devices] > [Inventory] ウィンドウで、プロビジョニングするデバイス名の横にあるチェックボックスをオンにします。 >

ステップ 9 [Actions] ドロップダウンリストから、[Provision] を選択します。

ステップ 10 **[次へ (Next)]** をクリックします。

ステップ 11 [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

ステップ 12 エッジスイッチをプロビジョニングするには、プロビジョニングするエッジスイッチの横にあるチェックボックスをオンにします。

ステップ 13 [Actions] ドロップダウンリストから、[Provision] を選択します。

ステップ 14 **[次へ (Next)]** をクリックします。

ステップ 15 [Summary] ウィンドウで設定を確認し、[Deploy] をクリックします。

デバイスが正常に展開されると、[Provision Status] が [Configuring] から [Success] に変わります。

ステップ 16 ファブリックドメインにデバイスを追加するには、Cisco DNA Center のホームページで [Provision] > [Fabric] を選択します。 >

ステップ 17 ファブリック LAN を作成します。

ステップ 18 IP トランジットネットワークを追加します。

IP トランジットネットワークは通常の IP ネットワークで使用され、外部に接続したり、2 つ以上のファブリックサイトを接続したりします。

ステップ 19 デバイスを追加して、ファブリックドメインに仮想ネットワークを関連付けます。

ステップ 20 Cisco Catalyst 9000 シリーズ スイッチをコントロールプレーン、ボーダーノード、およびエッジノードか、またはコントロールプレーンとボーダーノードとして追加します。

デバイスをクリックし、[Add as CP+Border+Edge] または [Add as CP+Border] を選択します。

ステップ 21 エッジノードをクリックして、[Add to Fabric] を選択します。

ステップ 22 **[Save]** をクリックします。

ステップ 23 ワイヤレス機能を有効にする前に Cisco Catalyst 9000 シリーズ スイッチにワイヤレスパッケージをインストールしなかった場合は、Cisco DNA Center に「機能を有効にするには、`9800-SW` イメージが必要です`[OK]` をクリックして、`9800-SW` イメージを手動でインポートしてください。（`9800-SW image is necessary for turning on the capability. Click "OK" to import the 9800-SW image manually`）」という警告メッセージが表示されます。

ステップ 24 [OK] をクリックして、イメージを手動でインストールします。

ステップ 25 [Download Image] ウィンドウで、[Choose File] をクリックしてローカルに保存されているソフトウェアイメージに移動するか、または [Enter image URL] でソフトウェアイメージのインポート元となる HTTP または FTP を指定します。

ステップ 26 [Import] をクリックします。

インポートの進捗状況が表示されます。

ステップ 27 [Activate image on device] をクリックします。

「デバイスでイメージが有効化されると、デバイスがリブートします。デバイスをリブートしてもよろしいですか。（`Activate image on device will reboot the device. Are you sure you want to reboot the device?`）」という警告メッセージが表示されます。

ステップ 28 [Yes] をクリックします。

デバイスパッケージのアップグレードが完了すると、デバイスがリブートし、オンラインになります。

ステップ 29 表示されるダイアログボックスに、コントローラで管理されている AP の場所が表示されます。ここからサイトの変更、削除、または再割り当てができます。

ステップ 30 **[次へ (Next)]** をクリックします。

ステップ 31 [Summary] ウィンドウで詳細を確認し、[Save] をクリックします。

ステップ 32 [Modify Fabric Domain] ウィンドウで、[Now] をクリックして変更を確定し、[Apply] をクリックして設定を適用します。
次の手順では、ファブリックドメインで AP をオンボードします。

ステップ 33 Cisco DNA Center ホームページで、[プロビジョニング（Provision）] をクリックします。

ステップ 34 **[ファブリック（Fabric）]** タブをクリックします。

ファブリックドメインのリストが表示されます。

ステップ 35 作成したファブリックドメインを選択し、[Host Onboarding] タブをクリックして、AP の IP プールを有効にします。

ステップ 36 ファブリックドメイン内のデバイスに適用される認証テンプレートを選択します。これらのテンプレートは、Cisco ISE から取得される事前定義済みの設定です。認証テンプレートを選択したら、[保存（Save）] をクリックします。

ステップ 37 [Virtual Networks] の下で、[INFRA_VN] をクリックして、選択した仮想ネットワークに 1 つ以上の IP プールを関連付けます。

ステップ 38 [Virtual Network] の下で、ゲスト仮想ネットワークをクリックして、選択したゲスト仮想ネットワークの IP プールを関連付けます。

ステップ 39 設計フェーズ中に AP 用に作成された [IP Pool Name] チェックボックスをオンにします。

ステップ 40 [Update] をクリックして設定を保存します。

AP は、指定したプールから IP アドレスを取得します。このプールは、AP VLAN に関連付けられていて、いずれかの検出方法を通じてシスコ ワイヤレス コントローラに登録されます。

ステップ 41 ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。[Wireless SSID] セクションで、ゲスト SSID または企業 SSID を選択してアドレスプールを割り当ててから、[Save] をクリックします。

ステップ 42 [Inventory]>[Resync] を実行して手動で再同期をトリガーし、組み込みのワイヤレス用の Cisco DNA Center で AP を確認します。
検出された AP が [Provision] ページの [Inventory] に表示され、[Status] は [Not Provisioned] として表示されます。

ステップ 43 AP をプロビジョニングします。

ステップ 44 アプリケーションポリシーを設定および展開します。

アプリケーションポリシーを展開する前に、Catalyst 9300 シリーズ スイッチおよび Cisco Catalyst 9500H シリーズ スイッチをプロビジョニングします。

2 つの異なる SSID で異なるビジネスとの関連性を持つ 2 つの異なるポリシーは機能しません。関連性を設定するときは、最後に展開したポリシーが常に優先されます。

アプリケーションのデフォルトのビジネスとの関連性を変更しても、FlexConnect モードでは動作しません。

非ファブリック SSID にのみアプリケーションポリシーを適用できます。

Cisco Catalyst 9000 シリーズスイッチに Catalyst 9800 組み込みワイヤレスを搭載したファブリックインアボックス

ファブリックインアボックスに関する情報

Cisco Catalyst 9000 シリーズ スイッチには、Cisco DNA Center を使用して設定できる単一のスイッチで、ファブリックエッジ、コントロールプレーン、ボーダー、および組み込みのワイヤレス機能をホストする機能があります。

この機能を使用すると、小規模サイトの場所での設定が簡素化され、Cisco SD-Access の導入コストが削減されます。

Cisco Catalyst 9000 シリーズスイッチに CP+ ボーダー + エッジノードを追加する方法については、Cisco Catalyst 9800 シリーズ ワイヤレスコントローラのプロビジョニング （65 ページ）を参照してください。

拡張性に関する情報

次の表に、デバイスの拡張性に関する情報を示します。

ファブリックの構造	Cisco Catalyst 9300 シリーズ スイッチ	Cisco Catalyst 9400 シリーズ スイッチ	Cisco Catalyst 9500 シリーズ スイッチ	Cisco Catalyst 9500-H シリーズ スイッチ
仮想ネットワーク	256	256	256	256
ローカルエンドポイント/ホスト	4 K	4 K	4 K	4 K
SGT/DGT テーブル	8 K	8 K	8 K	8 K
SGACL（セキュリティ ACE）	5K	18K	18K	18K

リリース間コントローラモビリティの概要

リリース間コントローラモビリティ（IRCM）は、異なるソフトウェアバージョンのさまざまな シスコ ワイヤレス コントローラ で実行されるシームレスなモビリティとワイヤレスサービスをサポートします。

Cisco DNA Center は、次のデバイスの組み合わせでゲストアンカー機能をサポートしています。

- アンカーコントローラとしての Cisco AireOS コントローラとフォーリンコントローラとしての Cisco AireOS コントローラの設定。
- フォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとゲストアンカーコントローラとしての Cisco AireOS コントローラの設定。
- アンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラとフォーリンコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定。

コントローラデバイスでIRCMを設定する際の、このリリースにおける制限事項を次に示します。

- フォーリンコントローラとしての Cisco AireOS コントローラの設定、およびアンカーコントローラとしての Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定はサポートされていません。
- ファブリックゲストアンカーの設定はサポートされていません。
- 複数のアンカーコントローラの設定、および 1 つのフォーリン コントローラ シナリオの設定はサポートされていません。
- ゲスト SSID のみがサポートされています。
- ゲストアンカーノードでの非ゲストアンカー SSID のブロードキャストはサポートされていません。
- モビリティトンネルは暗号化されません。

ゲスト アンカーの設定とプロビジョニング

（注） Cisco AireOS コントローラを外部コントローラとして、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをゲストアンカーコントローラとして設定することは、リリース間コントローラモビリティ（IRCM）の使用中はサポートされていません。

ゲスト アンカー シスコ ワイヤレス コントローラ を設定するには、次の手順に従います。

ステップ 1 サイト、ビルディング、フロアなどのネットワーク階層を設計します。詳細については、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

ステップ 2 AAA、DHCP、DNS サーバなどのネットワーク サーバを設定します。詳細については、グローバル ネットワーク サーバの設定およびCisco ISE またはその他の AAA サーバの追加を参照してください。

ステップ 3 Cisco Identity Services Engine を設定し、外部 Web 認証と中央 Web 認証を使用してゲスト ワイヤレス ネットワークの SSID を作成します。詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成」を参照してください。

ステップ 4 Cisco Discovery Protocol（CDP）または IP アドレス範囲を使用して ワイヤレス コントローラ を検出します。デバイスは [Inventory] ウィンドウに示され、[Managed] 状態になっています。詳細については、「ディスカバリについて」を参照してください。

ステップ 5 アクティブなメイン ワイヤレス コントローラ として外部 ワイヤレス コントローラ をプロビジョニングします。Cisco AireOS コントローラのプロビジョニング （29 ページ） を参照してください。

ステップ 6 ゲスト アンカーとして ワイヤレス コントローラ のロールを選択し、ゲスト アンカー コントローラをプロビジョニングします。詳細については、「Cisco AireOS コントローラのプロビジョニング （29 ページ）」を参照してください。

ステップ 7 CLI、SNMP、HTTP、HTTPS などのデバイス クレデンシャルを設定します。詳細については、グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、およびグローバル HTTPS クレデンシャルの設定を参照してください。

IRCM：Cisco AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco AireOS コントローラを検出します。

  Catalyst 9800 シリーズ ワイヤレス コントローラを検出するには、NETCONF を有効にしてポートを 830 に設定する必要があります。NETCONF は、ネットワークデバイスの設定をインストール、操作、削除するメカニズムです。

  詳細については、CDP を使用したネットワークの検出またはDiscover Your Network Using an IP Address Rangeを参照してください。

- サイト、ビルディング、フロアを追加してネットワーク階層を設計すると、後で設計の設定や構成を適用する場所を簡単に特定できるようになります。

  新しいネットワーク階層を作成するには、ネットワーク階層のサイトの作成、ビルディングの追加、およびビルディングへのフロアの追加を参照してください。

- AP の位置情報を追加し、フロアマップに配置して、ヒートマップカバレッジを可視化します。

  詳細については、「AP の追加、配置、および削除」を参照してください。

- AAA（Cisco ISE がネットワークとクライアントエンドポイント向けに設定されている）、NetFlow コレクタ、NTP、DHCP、DNS、syslog、SNMP トラップなどのネットワーク設定を定義します。これらのネットワークサーバが、ネットワーク全体のデフォルトになります。AAA サーバを追加するときに、TACACS サーバを追加できます。

  詳細については、グローバル ネットワーク設定について、グローバル ネットワーク サーバの設定、および「AAA サーバの追加」を参照してください。

- ゲスト ワイヤレス ネットワークの SSID を作成します。

  詳細については、「ゲスト ワイヤレス ネットワークの SSID の作成」を参照してください。

- フォーリンコントローラとアンカーコントローラの WLAN プロファイル名は、モビリティに対して同じにする必要があります。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devices] > [Inventory] > ウィンドウに、検出されたデバイスのリストが表示されます。

ステップ 2 フォーリンコントローラとしてプロビジョニングする Catalyst 9800 シリーズ ワイヤレス コントローラの横にあるチェックボックスをオンにします。

ステップ 3 [Actions] ドロップダウンリストから、[Provision] > [Provision] を選択します。 >

ステップ 4 [Assign Site] ウィンドウで、[Choose a Site] をクリックして Catalyst 9800 シリーズ ワイヤレス コントローラ デバイスにサイトを割り当てます。

ステップ 5 [Add Sites] ウィンドウで、サイト名の横にあるチェックボックスをオンにして Catalyst 9800 シリーズ ワイヤレス コントローラ を関連付けます。

ステップ 6 **[Save]** をクリックします。

ステップ 7 [Apply] をクリックします。

ステップ 8 [Next] をクリックします。

ステップ 9 Catalyst 9800 シリーズ ワイヤレス コントローラ のロールを [Active Main WLC] として選択します。

ステップ 10 アクティブなメイン ワイヤレス コントローラ では、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 11 [Assign Interface] エリアで、次の操作を実行します。

- [VLAN ID]：VLAN ID の値を入力します。
- [IP Address]：インターフェイス IP アドレスを入力します。
- [Gateway IP Address]：ゲートウェイ IP アドレスを入力します。
- [Subnet Mask (in bits)]：インターフェイスのネットマスクの詳細を入力します。

（注） Catalyst 9800 シリーズ ワイヤレス コントローラ では、IP アドレス、ゲートウェイ IP アドレス、およびサブネット マスクを割り当てる必要はありません。

ステップ 12 **[次へ (Next)]** をクリックします。

ステップ 13 [Summary] ウィンドウで、設定の詳細を確認します。

ステップ 14 [Deploy] をクリックし、Catalyst 9800 シリーズ ワイヤレス コントローラ をフォーリンコントローラとしてプロビジョニングします。

ステップ 15 [Devices] > [Inventory] > ウィンドウで、ゲストアンカーコントローラとしてプロビジョニングする Cisco AireOS コントローラの横にあるチェックボックスをオンにします。

ステップ 16 手順 3 ～ 8 を繰り返します。

ステップ 17 Cisco AireOS コントローラのロールを [Guest Anchor] として選択します。

ステップ 18 ゲストアンカー ワイヤレス コントローラ の場合は、インターフェイスと VLAN の詳細を設定する必要があります。

ステップ 19 手順 11 ～ 14 を繰り返します。

Meraki デバイスのプロビジョニング

この手順では、Meraki ダッシュボードによって管理されている Cisco Meraki デバイスに SSID をプロビジョニングする方法について説明します。

始める前に

- Meraki ダッシュボードを Cisco DNA Center と統合します。Meraki ダッシュボードの統合を参照してください。
- SSID を作成します。エンタープライズ ワイヤレス ネットワーク用 SSID の作成を参照してください。

（注） Meraki ダッシュボードは、次の種類の SSID をサポートしています。

- [Open]：この SSID は、Meraki ダッシュボードの [Open] に対応しています。
- [WPA2 Personal]：この SSID は、Meraki ダッシュボードの [preshared key with WAP2] に対応しています。
- [WPA2 Enterprise]：この SSID は、Meraki ダッシュボードの [WAP-2 encryption with Meraki authentication] または [WAP-2 encryption with My Radius server] に対応しています。Cisco DNA Center におけるビルディングレベルのクライアントおよびエンドポイントの認証用に AAA サーバまたは Cisco ISE サーバを定義している場合は、その設定が Meraki ダッシュボードの [my Radius server] にプロビジョニングされます。それ以外の場合は、Merakiデバイスによる認証に [Meraki Radius] が使用されます。

- ネットワークプロファイルを作成し、SSID がプロビジョニングされるサイトに割り当てます。ワイヤレス用のネットワークプロファイルの作成を参照してください。

（注） Cisco DNA Center のネットワーク階層 [Sites] > [Buildings] は、Meraki ダッシュボードの [Organization] > [Network] に対応しています。ワイヤレス用のネットワークプロファイルの作成 ワークフローの [Add Sites to Profile] ウィンドウで、[Buildings] を選択することをお勧めします。

（注） Cisco DNA Center Meraki ネットワークを作成して、SSID をネットワークにプロビジョニングします。Meraki ダッシュボードは、Meraki ネットワーク構成を Meraki デバイスにプロビジョニングします。

ステップ 1 Cisco DNA Center のホームページで、[Provision] を選択します。

[Devices] > **[Inventory]**ウィンドウが表示され、検出されたすべてのデバイスが示されます。

ステップ 2 Meraki ダッシュボードを表示するには、左側のペインで [Global] サイトを展開し、ビルディングを選択します。

選択したビルディングで使用可能なすべての Meraki ダッシュボードが表示されます。

ステップ 3 プロビジョニングする Meraki ダッシュボードの横にあるチェックボックスをオンにします。

ステップ 4 [Actions] ドロップダウンリストから、[Provision] > [Provision Device] を選択します。

[Assign Site] ウィンドウが表示され、Meraki ダッシュボードと関連付けられたビルディングを確認できます。

ステップ 5 関連付けられたビルディングを変更する場合は、[Choose a site] をクリックします。

ステップ 6 [Choose a site] ウィンドウで、ビルディングを選択して [Save] をクリックします。

ステップ 7 [Next] をクリックします。

[設定（Configuration）] ウィンドウが表示されます。管理ビルディングは、プライマリロケーションで表示できます。

ステップ 8 Meraki ダッシュボードのセカンダリ管理ロケーションを選択するには、[Select Secondary Managed AP Locations] をクリックします。

ステップ 9 [Managed AP Location] ウィンドウで、ビルディング名の横にあるチェックボックスをオンにします。

ステップ 10 **[Save]** をクリックします。

ステップ 11 **[次へ (Next)]** をクリックします。
[Summary（サマリ）] ウィンドウには、次の情報が表示されます。

- デバイスの詳細

- **ネットワーク設定（Network Settings）**
- **SSID**

  （注） Meraki 展開では、各ネットワークで最大 15 の SSID がサポートされています。

- **管理サイト**

ステップ 12 [展開（Deploy）] をクリックします。

- 即座に Meraki ダッシュボードを展開するには、[Now] オプションボタンをクリックし、[Apply] をクリックします。
- 将来の日付と時刻で Meraki ダッシュボードの展開をスケジュールするには、[Later] オプションボタンをクリックし、展開する日時を定義します。

プロビジョニング後のデバイスの削除

- 既にファブリック ドメインに追加されているデバイスを削除する場合、ファブリック ドメインからそのデバイスを削除し、次に**[プロビジョニング（Provision）]** メニューから削除します。
- **[インベントリ（Inventory）]** ウィンドウからデバイスを削除することはできません。代わりに、**[プロビジョニング（Provision）]** メニューからプロビジョニングしたデバイスを削除する必要があります。

ステップ 1 Cisco DNA Center のホームページから、**[プロビジョニング（Provision）]** > **[デバイス（Devices）]** を選択します。

[デバイス インベントリ（Device Inventory）] ウィンドウが表示されます。

ステップ 2 検出され、プロビジョニングされたすべてのデバイスが表示される **[インベントリ（Inventory）]** タブをクリックします。

ステップ 3 削除するデバイスの横にあるチェックボックスをオンにします。

（注） APは、接続していたコントローラが削除された場合にのみ削除されます。

ステップ 4 **[アクション（Actions）]** ドロップダウン リストから、**[デバイスの削除（Delete Device）]** を選択します。

ステップ 5 確認プロンプトで、[OK（OK）] をクリックします。

LAN アンダーレイのプロビジョニング

LAN 自動化を使用して、LAN アンダーレイをプロビジョニングします。

始める前に

- ネットワーク階層を設定します。（デバイスをサイトに追加する（26ページ）を参照）。
- 以下のグローバル ネットワーク設定が定義済みであることを確認します。
  - AAA、DHCP、DNS サーバなどのネットワーク サーバ。（グローバル ネットワーク サーバの設定 を参照）。
  - CLI、SNMP、HTTP、HTTPS などのデバイスのクレデンシャル。(グローバル CLI クレデンシャルの設定、グローバル SNMPv2c クレデンシャルの設定、グローバル SNMPv3 クレデンシャルの設定、グローバル HTTPS クレデンシャルの設定を参照。)
  - IP アドレス プール。（IP アドレス プールを設定する を参照）。
- インベントリに少なくとも 1 つのデバイスがあることを確認してください。デバイスがない場合は、ディスカバリ機能を使用して検出します。

  （注） 検出されたサイトがユーザ名「cisco」の CLI ログイン情報を使用して設定されている場合、LAN 自動化はブロックされます。

- ネットワークに Cisco Catalyst 9400 スイッチが設定されている場合は、LAN 自動化で 40G ポートが自動的に有効になるように設定されたスイッチで次の操作が実行されていることを確認します。
  - Day-0 設定はスイッチで実行されます。
  - 40G Quad Small Form-Factor Pluggable（QSFP）トランシーバはスーパーバイザのポート 9 またはポート 10 のいずれかに挿入されます。スーパーバイザ上の 1 ~ 8 のポートには、10G または 1G Small Form-Factor Pluggable（SFP）トランシーバは挿入されません。デュアル スーパーバイザ エンジンがある場合は、40G QSFP がポート 9 に挿入されていることを確認します。

    Catalyst 9400 シリーズ スーパーバイザの詳細については、『Cisco Catalyst 9400 Series Supervisor Installation Note』を参照してください。

ステップ 1 プロビジョニングするサイト用に IP アドレス プールを予約します。

（注） LAN 自動化 IP アドレス プールのサイズは、最小 25 ビット以上のサイズのネットマスクでなければなりません。

a) Cisco DNA Center のホームページで、**[Design]** > **[Network Settings]** > **[IP Address Pools]** の順に選択します。
b) [ネットワーク階層（Network Hierarchy）] ペインで、サイトを選択します。
c) [IP プールの予約（Reserve IP Pool）] をクリックして以下のフィールドに入力し、使用可能なグローバル IP アドレス プールのすべてまたは一部を特定のサイト用に予約します。

- [IP プール名（IP Pool Name）]：予約済み IP アドレスのプールの一意の名前。
- [タイプ（Type）]：IP アドレス プールのタイプ。LAN 自動化のバイアは、**LAN** を選択します。
- [Global IP Pool]：IP アドレスのすべてまたは一部を予約する IPv4 アドレスプール。

  （注） LAN 自動化では、IPv4 サブネットのみが使用されます。

- [CIDR Prefix/No. of IP Addresses]：グローバル IP アドレスプールのすべてまたは一部を予約するための IP サブネットとマスク、または予約する IP アドレス数。
- ゲートウェイ IP アドレス（Gateway IP Address）：ゲートウェイ IP アドレス。
- **DHCP Servers**: DHCP サーバの IP アドレス。

d) [予約（Reserve）] をクリックします。

ステップ 2 デバイスを検出してプロビジョニングします。

a) Cisco DNA Center のホームページから、**[プロビジョニング（Provision）]** > **[デバイス（Devices）]** > **[インベントリ（Inventory）]** を選択します。

すべての検出されたデバイスが表示されます。

b) **[** LAN 自動化（LAN Automation） **]** ドロップダウン リストから、[LAN 自動化（LAN Automation）] を選択します。
c) スライドして表示される [LAN 自動化（LAN Automation）] ダイアログ ボックスで、以下のフィールドに入力します。

- [Primary Site]：このサイトからプライマリデバイスを選択します。
- [Peer Site]：このサイトがピアデバイスの選択に使用されます。このサイトは、プライマリサイトとは異なる場合がありますので注意してください。
- [Primary Device]：Cisco DNA Center が新しいデバイスを検出しプロビジョニングする起点として使用するプライマリデバイスを選択します。
- [Peer Device]：ピアデバイスを選択します。
- プライマリ検出ポート（Primary Discover Ports）：新規デバイスの検出とプロビジョニングに使用するポート。
- [Discovered Device Site]：新たに検出されたすべてのデバイスがこのサイトに割り当てられます。このサイトは、プライマリサイトおよびピアサイトとは異なる場合があります。
- IP プール（LAN Pool）：LAN 自動化用に予約された IP アドレス プール。（ステップ 1 を参照）。

- **[** ISIS ドメイン パスポート（ISIS Domain Password） **]** : LAN 自動化が開始するときにユーザが指定する IS-IS パスワード。パスワードがすでにシードデバイスに存在する場合は、再使用され、上書きされることはありません。ユーザが指定するパスワードが入力され、既存の IS-IS パスワードがデバイスにない場合、ドメイン パスワードがしっ用されます。プライマリとセコンダリ シードの両方がドメイン パスワードをもつ場合、それらが一致することを確認してください。
- **[** マルチキャストの有効化（Enable Multicast） **]** : LAN 自動化は RP としてシード デバイスから、サブスクライバとして検出されたデバイスからマルチキャスト ツリーを作成します。
- [Device Name Prefix]：プロビジョンしているデバイスの名前プレフィックス。Cisco DNA Center で各デバイスをプロビジョニングするときに、ここで指定されたテキストでデバイスにプレフィックスを付与し、末尾に一意の番号を追加します。たとえば、名前プレフィックスとして **Access** を入力した場合、各デバイスがプロビジョニングされると、Access-1、Access-2、Access-3 のように名前が付けられます。
- [Hostname Map File]：シリアル番号とホスト名のマッピングを含む CSV ファイルを使用して、検出されたデバイスのユーザー指定の名前を設定します。検出されたデバイスがスタックの場合、スタックのすべてのシリアル番号が CSV ファイルで指定されます。

  CSV ファイルの例を次に示します。

```
standalone-switch,FCW2212L0NF
stack-switch,"FCW2212E00Y,FCW2212L0GV"
```

d) **[開始（Start）]** をクリックします。

Cisco DNA Center は、新規デバイスの検出とプロビジョニングを開始します。

LAN 自動化では、VLAN 1 のシードデバイスで IP アドレスを設定します。シードデバイスのこの VLAN 1 IP アドレスが Cisco DNA Center から到達できない場合は、[LAN Automation Status] ウィンドウにエラーメッセージが表示されます。エラーの詳細および可能な修復アクションを表示するには、このウィンドウの [See Details] リンクにマウスカーソルを合わせます。

ステップ 3 プロビジョニングしているデバイスの進行状況をモニタして確認します。

a) **[プロビジョニング（Provisioning）]** > **[デバイス（Device）]** > **[インベントリ（Inventory）]** タブから、**[LAN 自動化（LAN Automation）]** > **[LAN 自動化スのテータス（LAN Status）]** をクリックします。

[LAN 自動化のステータス（LAN Automation Status）] ダイアログボックスに、プロビジョニングしているデバイスの進捗状況が表示されます。

（注） 新規デバイスをプロビジョニングするプロセスは、数分かかる場合があります。

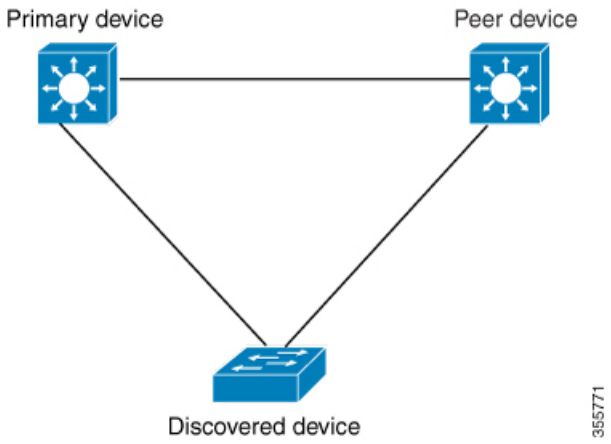
b) すべてのデバイスが検出され、管理状態にある場合、[LAN 自動化ステータス（LAN Automation Status）] ダイアログボックスの **[** LAN 自動化ステータス（LAN Automation Status） **]** ダイアログボックスをクリックします。

LAN 自動化プロセスが完了し、新規デバイスがインベントリに追加されます。

LAN 自動化のピアデバイスの使用事例

デュアル ホームのスイッチのプロビジョニング

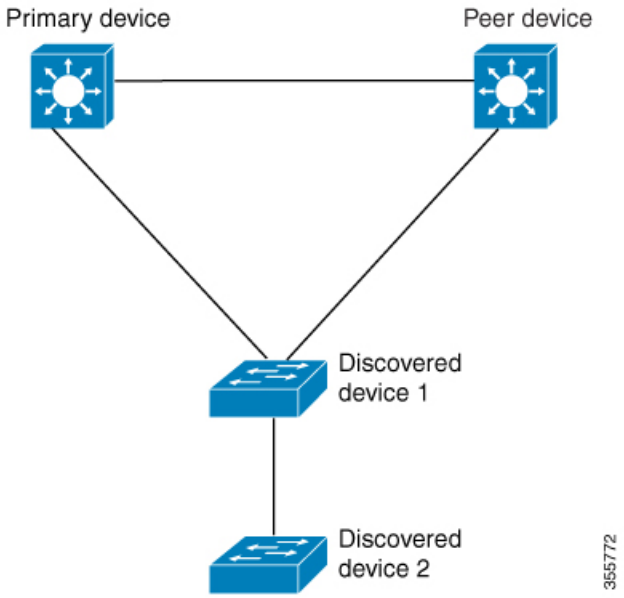
デュアル ホームのスイッチのプロビジョニングのために、常にピア デバイスを選択する必要があります。



Cisco DNA Center プライマリ デバイスで DHCP サーバを設定します。Cisco DNA Center が検出されたデバイスがプライマリ デバイスとピア デバイスの両方に接続されていることを理解しているため、LAN 自動化タスクが停止されると、2 つのレイヤー 3 ポイントツーポイント接続を設定します。1 つの接続は、検出されたデバイスとプライマリ デバイスの間で確立されます。もう 1 つの接続は検出されたデバイスとピア デバイスの間で確立されます。

（注） LAN 自動化ジョブが実行される前に、プライマリ デバイスとピア デバイスの間のリンクが設定される場合、ピア デバイスを Cisco DNA Center のLAN 自動化設定の一部としてピア デバイスに接続するプライマリ デバイスのインターフェイスを選択する必要があります。

LAN 自動化の 2 段階制限



前述のトポロジの場合、Cisco DNA Center は次のリンクを設定します。

- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から プライマリ デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から ピア デバイス に接続するためにルートする
- ポイントツーポイントのレイヤ 3 は 検出されたデバイス *1* から 検出されたデバイス *2* に接続するためにルートする

検出されたデバイス *3*という名前のデバイスが以下の検出されたデバイス *2*に直接接続されるシナリオを考えてください。検出されたデバイス *2* と 検出されたデバイス *3*の間の接続は、LAN 自動化ジョブの一部として設定されません。プライマリ デバイスから 2 段階以上離れているためです。

LAN 自動化の状態を確認

実行中の LAN 自動化ジョブのステータスを確認できます。

始める前に

LAN 自動化ジョブを作成し、開始する必要があります。

ステップ 1 Cisco DNA Center のホームページから、**[プロビジョニング（Provision）]** > **[デバイス（Devices）]** を選択します。

ステップ 2 [Inventory] タブをクリックします。
すべての検出されたデバイスが表示されます。

ステップ 3 **[LAN 自動ステータス（LAN Auto Status）]** をクリックします。

LAN 自動化ジョブ実行中または完了のステータスが表示されます。

ファブリックの概要

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

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

ファブリック サイトとファブリック ドメイン

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

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

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

ファブリックドメインは、1 つ以上のファブリックサイトとトランジットサイトで構成できます。複数のファブリック サイトは、トランジット サイトを使用して互いに接続されます。 ¥

トランジット サイトには 2 つのタイプがあります。

- SD-Access トランジット: サイト間通信のためのドメイン全体のコントロールプレーン ノードでネイティブ SD-Access (LISP、VXLAN、CTS) ファブリックを有効にします。
- IP ベース トランジット: 従来型の IP ベース (VRF-LITE、MPLS) ネットワークを利用します。これは、サイト間で VRF と SGT のりマッピングを必要とします。

マルチサイト ファブリック ドメイン

マルチサイトファブリックドメインは、トランジットサイト経由で相互接続されたファブリックサイトの集合体です。ファブリック サイトは、コントロール プレーン ノード、ボーダー ノード、およびエッジノードの独自のセットを持つファブリックの一部です。指定されたファブリック サイトもまた、ファブリック WLC と AP、および関連するサイト指定の ISE PSN も含みます。単一のファブリックドメインに含まれる複数のファブリックサイトは、トランジット サイトを使用して相互接続されます。

Software-Defined Access（SDA）ファブリックは、複数のサイトで構成されることがあります。各サイトは、優れた拡張性、復元力、生存性、およびモビリティを備えます。サイトの全体的な集約（すなわち、ファブリックドメイン）には、非常に多くのエンドポイントに対応できることや、各サイト内に含まれるサイトを集約することによってモジュール方式で（または水平方向に）拡張できることも要求されます。

トランジット サイト

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

- IP トランジット：通常の IP ネットワークを使用して、外部ネットワークに接続するか 2 つ以上のファブリックサイトを接続します。
- SDA トランジット：LISP/VxLAN のカプセル化を使用して 2 つのファブリックサイトを接続します。SDA トランジットエリアは、独自のコントロールプレーンノードを持つがエッジノードやボーダーノードはないファブリックの一部として定義できます。ただし、外部ボーダーを持つファブリックを使用することもできます。SDA トランジットを使用すると、エンドツーエンドポリシープレーンは SGT グループ タグを使用して維持されます。

IP のトランジット ネットワークの作成

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

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。

ステップ 2 **[ファブリック（Fabric）]** タブをクリックします。

ステップ 3 **[ファブリック ドメインまたはトランジットを追加（Add Fabric Domain or Transit）]** タブをクリックします。

ステップ 4 ポップアップから、**[トランジットを追加（Add Transit）]** を選択します。

ステップ 5 ネットワークのトランジットの名前を入力します。

ステップ 6 トランジット タイプとして、**IP ベース** を選択します。
ルーティング プロトコルが BGP にデフォルトとして設定されます。

ステップ 7 次の 3 つのラジオボタンから選択した正しい ASN フォーマットで、トランジットネットワークの自律システム番号（ASN）を入力してください：[ASPLAIN]、[ASDOT]、[ASDOT+]。

ステップ 8 **[Save]** をクリックします。

SDA トランジット ネットワークの作成

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

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。

ステップ 2 **[ファブリック（Fabric）]** タブをクリックします。

ステップ 3 **[ファブリック ドメインまたはトランジットを追加（Add Fabric Domain or Transit）]** タブをクリックします。

ステップ 4 ポップアップから、**[トランジットを追加（Add Transit）]** を選択します。

ステップ 5 ネットワークのトランジットの名前を入力します。

ステップ 6 トランジット タイプとして [SD-Access] を選択します。

ステップ 7 このトランジット ネットワークの**トランジット コントロール プレーンのサイト**を入力します。少なくとも 1 つのトランジット マップ サーバを選択します。

ステップ 8 このトランジット ネットワークの**トランジット コントロール プレーン**を入力します。

ステップ 9 追加するすべてのマップ サーバに対し、手順 7 および 8 を繰り返します。

ステップ 10 **[Save]** をクリックします。

次のタスク

SDA トランジットの作成後、ファブリック サイトに移動し、SDA トランジットを接続するサイトに接続します。[プロビジョニング（Provision）]>[ファブリック（Fabric）]>[ファブリック サイト（Fabric Site）] の順に移動します。作成したファブリック サイトを選択します。[ファブリックサイト（Fabric Site）]>[ボーダー（Border）]>[ボーダーの編集（Edit Border）]>[トランジット（Transit）] の順にクリックします。ドロップダウン リストで SDA トランジット サイトをポイントし、[追加（Add）] をクリックします。

ファブリック ドメインの作成

Cisco DNA Center では、デフォルト *LAN* ファブリックと呼ばれるデフォルトのファブリック ドメインが作成されます。

始める前に

ネットワークが設計されていること、ポリシーが Cisco Integrated Services Engine（ISE）から取得されているか Cisco DNA Center で作成されていること、デバイスがインベントリに登録され、サイトに追加されていることを確認してください。

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** をクリックします。

ステップ 2 **[ファブリック（Fabric）]** タブをクリックします。

ステップ 3 **[ファブリック ドメインまたはトランジットを追加（Add Fabric Domain or Transit）]** タブをクリックします。

ステップ 4 ポップアップから、**[トランジットを追加（Add Transit）]** を選択します。

ステップ 5 ファブリック名を入力します。

ステップ 6 ファブリック サイトの 1 つを選択します。

ステップ 7 [Add] をクリックします。

ファブリックの準備状況とコンプライアンスのチェック

ファブリックの準備状況チェック

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

ファブリックの準備状況チェックには、次の項目が含まれます。

- ソフトウェアバージョン：デバイスが適切なソフトウェアイメージを使用して実行されているかどうかを確認します。
- ソフトウェアライセンス：デバイスが適切なソフトウェアライセンスを使用して実行されているかどうかを確認します。
- ハードウェアバージョン：デバイスのハードウェアバージョンがサポートされているかどうかを確認します。
- イメージタイプ：デバイスがサポートされているイメージタイプ（IOS XE、IOS、NXOS、Cisco コントローラ）を使用して実行されているかどうかを確認します。
- ループバック インターフェイス：デバイス上のループバック インターフェイスの設定を確認します。SDA アプリケーションを使用するには、デバイスにループバック インターフェイスが設定されている必要があります。
- 接続チェック：エッジノードからマップサーバへの接続、エッジノードからボーダーへの接続など、デバイス間で必要な接続を確認します。
- 既存の設定チェック（ブラウンフィールドチェック）：SD-Access を介してプッシュされ、後でエラーになる可能性がある設定と競合するデバイス上の設定を確認します。

サポートされているソフトウェアバージョンの詳細については、Cisco SD-Access ハードウェアおよびソフトウェアの互換性マトリックス [英語] を参照してください。

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

ファブリック コンプライアンス チェック

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

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

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

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

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

ファブリック ドメインの設定

デバイスをサイトに追加し、それらのデバイス（ボーダー、コントロールプレーン、またはエッジ）にロールを割り当てることができます。また、IPアドレスプールを設定してホスト間の通信を有効にできます。

ファブリックへのデバイスの追加

ファブリック ドメインを作成した後にファブリック サイトを追加してから、このファブリック サイトにデバイスを追加できます。また、デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかを指定することもできます。

（注） ファブリック ドメイン内のデバイスをコントロール プレーン ノードまたはボーダー ノードとして指定する手順はオプションです。デバイスによってはこれらのロールを実行しない場合があります。ただし、各ファブリック ドメインには、少なくとも 1 つのコントロール プレーン ノードデバイスと 1 つのボーダー ノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大 6 つのコントロール プレーン ノードを追加できます。

（注） 現在、シスコ ワイヤレス コントローラ は 2 つのコントロールプレーンノードとのみ通信します。

始める前に

デバイスをプロビジョニングします。デバイスをプロビジョニングするには、[プロビジョニング（Provision）] タブをクリックし、[デバイス（Devices）] を選択します。ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジにデバイスがグレー色で表示されます。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。問題解決の一環としてデバイスの設定を更新する場合は、デバイスで [Inventory] > [Resync] > を実行して、デバイス情報を再同期してください。

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

ステップ 1 Cisco DNA Center のホームページから、[Provision] > [Devices] > の順に選択します。
すべてのプロビジョニングされたファブリック ドメインがウィンドウに表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。
結果の画面に、そのファブリック ドメイン内のすべてのサイトが表示されます。

ステップ 3 サイトを選択します。

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

ステップ 4 デバイスをクリックします。[デバイスの詳細（device details）] ウィンドウに、次のオプションが表示されます。

オプション	説明
エッジ ノード	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。
ボーダー ノード	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。詳細については、「**ボーダーノードとしてのデバイスの追加**」セクションを参照してください。
コントロール プレーン	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。
ゲスト境界/コントロールプレーン	次のオプションを使用できます。 • コントロールプレーン：デバイスをコントロールプレーンとして使用する場合はこのチェックボックスをオンにします。 • [Border]：デバイスをボーダーノードとして動作させる場合は、このチェックボックスをオンにします。 • [Select One Guest Virtual Network]：作成されたすべてのゲスト仮想ネットワークが一覧表示されます。ゲスト仮想ネットワークのチェックボックスをオンにして、[有効化（Enable）] をクリックします。 （注） [ポリシー（Policy）]アプリケーションでゲスト仮想ネットワークを作成したことを確認してください。仮想ネットワークの作成を参照してください。
ランデブー ポイント	デバイスでランデブーポイントを設定するには、このトグルボタンをクリックします。 詳細については、「**ランデブーポイントとしてのデバイスの追加**」セクションを参照してください。

デバイスをファブリックインアボックスとして設定するには、**[コントロールプレーン（Control Plane）]**、**[ボーダーノード（Border Node）]**、および **[エッジノード（Edge Node）]** オプションを選択します。

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

ステップ 5 **[Save]** をクリックします。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付

いた状態で表示されます。エラー通知の [詳細の表示（See more details）] をクリックして問題領域を特定し、修正します。

ボーダーノードとしてのデバイスの追加

ファブリックにデバイスを追加する場合、ファブリックへのデバイスの追加 （93 ページ）で説明したように、コントロールプレーン、ボーダーノード、またはエッジノードとして動作するようにさまざまな組み合わせで追加できます。

ボーダー ノードとしてデバイスを追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Fabric] をクリックします。
プロビジョニングされたすべてのファブリック ドメインのリストが表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。
すべてのファブリック対応サイトのリストが表示されます。

ステップ 3 ファブリックサイトのリストから、サイトを選択します。インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

ステップ 4 デバイスをクリックして、[Border Node] を選択します。

ステップ 5 追加するデバイスの名前が記載されたスライディングウィンドウが表示されます。

a) [Layer 3 Handoff] を展開します。

b) 次のいずれかのオプションボタンをクリックします。

- [ASPLAIN]：自律システム番号（ASN）を ASPLAIN 形式で受け入れます。
- [ASDOT]：ASN を ASDOT 形式で受け入れます。
- [ASDOT+]：ASN を ASDOT+ 形式で受け入れます。

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

d) [Select] ドロップダウンリストから、1 つの IP アドレスプールを選択します。

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

- ボーダーで SDA トランジットを有効にするには、[トランジットを選択（Select Transit）] ドロップダウン リストからユーザが作成した SDA トランジット ドメインを選択します。[Add] をクリックします。
- ボーダーで IP トランジットを有効にするには、[トランジットを選択（Select Transit）] ドロップダウン リストからユーザが作成した IP トランジット ドメイン を選択します。[Add] をクリックします。

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

  ドロップダウン リストから [外部インターフェイス（External Interface）] を選択します。[リモートAS番号（Remote AS Number）] を入力します。リストで [仮想ネットワーク（Virtual Network）]

をチェックします。この仮想ネットワークは、ボーダーによってリモート ピアにアドバタイズされなければなりません。1つ、複数、またはすべての仮想ネットワークを選択できます。**[Save]** をクリックします。

f) デフォルトでは、ボーダーノードは内部ボーダーとして指定され、既知のトラフィックへのゲートウェイとして機能し、特定の外部ルートをインポートします。ボーダーノードは、外部ルートをインポートせずに、すべての不明なトラフィックへのゲートウェイとして機能する外部ボーダーとして設定できます。ボーダーノードには、内部ボーダーおよび外部ボーダーを組み合わせたロールを設定することもできます。

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

ステップ 6 （任意）ファブリックネットワークに非ファブリックネットワークを接続している場合、または従来のネットワークからSoftware-Defined Accessネットワークに移行する場合にのみ、この手順を実行します。[Layer 2 Handoff] をクリックします。仮想ネットワークの 1 つをクリックします。

すべての仮想ネットワークと、各仮想ネットワークのプールの数が表示されます。

仮想ネットワーク リストのチェックボックスをクリックできない場合、仮想ネットワークの下にあるセグメントが外部 VLAN にハンドオフされたことを示します。

仮想ネットワークを選択すると、仮想ネットワークに存在する IP アドレス プールのリストが表示されます。非ファブリックデバイスを接続できるインターフェイスのリストが表示されます。

ファブリックを拡張する必要がある [External VLAN] 番号を入力します。仮想ネットワークは、1 つのインターフェイスでのみハンドオフできます。複数のインターフェイス経由で同じ仮想ネットワークを処理することはできません。

[Save] をクリックします。

ステップ 7 [Add] をクリックします。

ホスト オンボーディングの設定

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

このタブでは次の操作を実行できます。

- ファブリックに適用する認証テンプレートを選択します。これらのテンプレートは、Cisco ISEから取得される定義済みの設定です。認証テンプレートを選択したら、[保存（Save）] をクリックします。
- IP アドレス プールを仮想ネットワーク（デフォルト、ゲスト、またはユーザ定義）に関連付け、[更新（Update）] をクリックします。表示される IP アドレス プールは、サイト固有のプールのみです。
- ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。ゲスト SSID またはエンタープライズ SSID を選択してアドレス プールを割り当て、[保存（Save）] をクリックできます。
- ファブリックドメインに接続している特定のタイプのデバイスについて、各ポート固有の設定を適用します。これを行うには、固有の割り当てが必要なポートを選択し、[Assign] をクリックして、ドロップダウンリストからポートタイプを選択します。

  次の制約事項に注意してください。

  - Cisco SD-Access 展開環境では、AP、拡張ノード、ユーザデバイス（単一のコンピュータまたは単一のコンピュータと電話機など）、および単一サーバのみがサポートされます。
  - 各ポートは最大 10 個の MAC アドレスを学習できます。
  - 内部スイッチまたは仮想スイッチを備えたサーバはサポートされていません。
  - その他のネットワーキング機器（ハブ、ルータ、スイッチなど）はサポートされていません。

認証テンプレートを選択

ファブリック ドメイン内のすべてのデバイスに適用される認証テンプレートを選択できます。

ステップ 1 [Authentication Template] セクションからサイト用の認証テンプレートを選択します。

- **クローズ認証（Closed Authentication）**：認証前のすべてのトラフィック（DHCP、DNS、ARP を含む）は廃棄されます。
- [Low Impact]：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワーク アクセスが許可されます。
- **認証なし**
- **オープン認証（Open Authentication）**：ホストには、802.1X 認証を受ける必要なくネットワーク アクセスが許可されます。

Cisco DNA Center リリース 1.3.3.0 以降では、選択した認証テンプレートの設定を編集して、サイト固有の認証要件に対応することができます。

ステップ 2 （オプション）選択した認証方式の設定を編集するには、[Edit] をクリックします。

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

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

必要な変更を行って、[Save] をクリックします。

編集ウィンドウが閉じます。

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

ステップ 3 [Set as Default] をクリックします。

（注） Cisco DNA Center リリース 1.3.3.0 以降では、ヒットレス認証変更機能を使用すると、ファブリックからデバイスを削除することなく、1 つの認証方式から別の認証方式に切り替えることができます。

ファブリック ドメインへの仮想ネットワークの関連付け

IP アドレス プールにより、ホスト デバイスはファブリック ドメイン内で通信できるようになります。

IP アドレス プールを設定すると、Cisco DNA Center はすぐに各ノードに接続し、ホストが通信できるように適切なスイッチ仮想インターフェイス（SVI）を作成します。

IP アドレス プールを追加することはできませんが、リストされているものからプールを設定できます。ここにリストされている IP アドレスプールは、ネットワークの設計時に作成されたものです。

ステップ 1 From the **Virtual Networks** section on the **Host Onboarding** tab, click a virtual network（VN）.

ステップ 2 [Edit Virtual Network] ウィンドウの次のフィールドを確認します。

フィールド	説明
IPプール名（IP Pool Name）	IP アドレスプールが表示されます。 IP アドレスプールのリストから、仮想ネットワークの一部にする必要があるものを選択します。
認証ポリシー（Authentication policy）	仮想ネットワークの認証ポリシーが表示されます。

フィールド	説明
トラフィック タイプ	仮想ネットワーク上で有効になっているトラフィックのタイプを表示します。 仮想ネットワークを介した音声トラフィックまたはデータ トラフィックの送信を選択します。
グループ	IP プールが属しているグループを表示します。
ワイヤレスプール	選択した IP プールを**ワイヤレスプール**として有効または無効にします。 有効にすると、ファブリックのワイヤレス SSID を設定するときに、定義済みのワイヤレスプールから選択できます。
レイヤー2拡張機能（Layer-2 Extension）	レイヤ2フラッディングが有効になっているか、無効になっているかを表示します。 IP プールおよびレイヤ 2 VNI のレイヤ 2 MAC アドレス登録を有効にします。レイヤ2拡張機能はデフォルトで有効になっており、無効にすることはできません。
レイヤ2フラッディング（Layer-2 Flooding）	レイヤ2フラッディングが有効になっているか、無効になっているかを表示します。 レイヤ 2 フラッディングはデフォルトで無効になっています。

ステップ 3 [Add] をクリックして、選択した仮想ネットワークに 1 つ以上の IP アドレスプールを関連付けます。

結果のウィンドウの必須フィールドに入力します。

- 対応するドロップダウンリストから、**IP** プール、**トラフィック**タイプ、および**グループ**を選択します。
- レイヤ 2 フラッディングを有効にするには、[Layer-2 Flooding] チェックボックスをオンにします。
- [Critical pool] チェックボックスをオンにして、この IP プールをクリティカル IP アドレスプールに含めます。
- [Common Pool]**I** チェックボックスをオンにして、この IP プールがファブリック内の複数のサイト間で共有されるようにします。

  Cisco DNA Center リリース 1.3.3.0 では、ファブリック内の複数のサイト間での IP プールの共有をサポートする、サイト間レイヤ 2 のハンドオフ機能が導入されています。

ステップ 4 [更新（Update）] をクリックして設定を保存します。ここで指定した設定は、仮想ネットワーク上のすべてのデバイスに展開されます。

ステップ 5 すべての仮想ネットワークに IP プールを関連付けた後、[Save] をクリックします。

ファブリック ドメインのワイヤレス SSID の設定

ステップ 1 [Wireless SSID] セクションで、ホストがアクセス可能なネットワーク内のワイヤレス SSID を指定します。

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

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

ステップ 4 SSID でワイヤレスマルチキャストを有効にするには、[Enable Wireless Multicast] チェックボックスをオンにします。

ファブリック ドメイン内のポートの設定

[ポート割り当ての選択（Select Port Assignment）] セクションでは、ファブリック ドメイン上の各アクセスデバイスを設定できます。各デバイスでは、各ポートのネットワークの動作設定を指定できます。

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

ステップ 1 **[ファブリック デバイスの選択（Select Fabric Device）]** セクションで、設定するアクセス デバイスを選択します。
デバイスで利用可能なポートが表示されます。

ステップ 2 デバイス上のポートを選択し、許可された IP アドレス プール、プロビジョニングされているグループ、音声またはデータ プール、およびポートの認証タイプを指定します。

ステップ 3 **[Save]** をクリックします。

拡張ノードデバイスの設定

拡張ノードはレイヤ 2 スイッチモードで動作するデバイスで、ファブリックテクノロジーをネイティブにはサポートしていません。拡張ノードは、自動化されたワークフローによって設定されます。設定後、拡張ノードデバイスがファブリックトポロジビューに表示されます。拡張ノードでの [Port Assignment] は、[Host Onboarding] ウィンドウで実行できます。

拡張ノードデバイスは、マルチキャストトラフィックをサポートします。

Cisco DNA Center 1.3.3.0 以降では、ポリシー拡張ノードがサポートされています。ポリシー拡張ノードのポート割り当て時に、[Group] を選択できます。

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

Cisco デジタル ビルディング シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ、および Cisco 産業用イーサネット 4000、4010、5000 シリーズスイッチは、ポリシー拡張ノードデバイスではありません。ポート割り当て時の [Cisco TrustSec] と [Group] の選択はサポートされていません。

拡張ノードの設定手順

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

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

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

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

- Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチ：15.2(7)E0s
- Cisco Catalyst IE 3400、3400 Heavy Duty（X-coded および D-coded）シリーズスイッチ：IOS XE 17.1.1s
- Cisco Catalyst IE 3300 シリーズスイッチ：IOS XE 16.12.1s
- Cisco Digital Building シリーズスイッチ、Cisco Catalyst 3560-CX スイッチ：15.2(7)E0s

ポリシー拡張ノードを設定する前に、次のことを確認してください。

- ポリシー拡張ノードデバイス、およびポリシー拡張ノードをサポートするエッジデバイスで必要な最小ソフトウェアバージョンは Cisco IOS XE 17.1.1 s です。
- ポリシー拡張ノードとそれをサポートするエッジノードの両方で、Network Advantage と DNA Advantage のライセンスレベルが有効になっている必要があります。

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

ステップ 2 拡張 IP アドレス プールを、[Fabric] > [Host Onboarding] タブの下にある INFRA_VN に割り当てます。プールタイプとして**拡張ノード**を選択します。

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

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

（注） オプション 43 の詳細については、DHCP コントローラ ディスカバリ （4 ページ）を参照してください。

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

ステップ 5 （任意）ポートチャネルを作成します。

この手順は、ファブリックのグローバル認証モードが [No Authentication] ではない場合にのみ実行します。認証モードは **Open**、**Low Impact**、または **Closed** のいずれかです。

拡張ノードに接続されているファブリックエッジノードでポートチャネルを作成します。ポートチャネルを作成するには、次の手順を実行します。

a) [Provision] > [Fabric] > [Fabric Infrastructure] に移動し、ファブリックエッジノードを選択します。タイトルにデバイス名の付いたウィンドウがスライド表示されます。

b) [ポートチャネルの作成（Create Port Channel）] をクリックします。

c) ウィンドウのすべてのフィールドに入力します。拡張ノードのオンボーディングでは LACP は機能しないことに注意してください。

- [LACP] は選択しないでください。
- すべてのデバイスに対して [PAGP] を選択します。

  Cisco IOS XE リリース 17.1.1s 以降、IE 3300 および IE 3400 デバイスは PAGP をサポートしています。

- Cisco IOS XE 17.1.1s よりも前のバージョンを実行している場合は、IE 3300 および IE 3400 デバイスの [Static mode] を選択します。

d) [Provision] > [Fabric] > [Host Onboarding] に移動して、作成したポートチャネルを選択します。結果のウィンドウで、[Connected Device] タイプとして [Extended Node] を選択します。

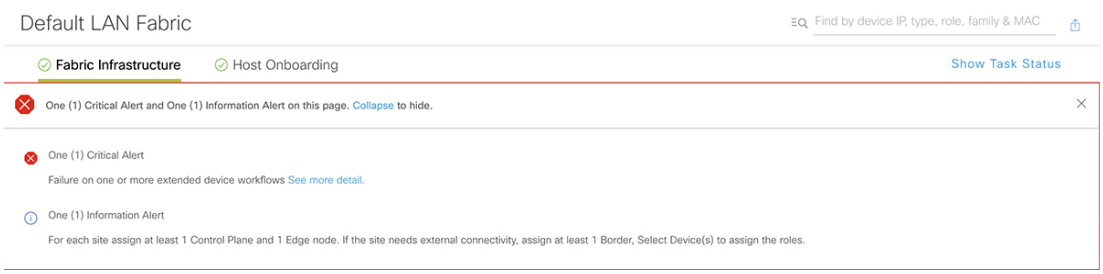
これにより、ファブリックエッジノードにポートチャネルを作成して拡張デバイスをオンボードします。

ステップ 6 以前の設定がない場合は、拡張ノードデバイスの電源をオンにします。拡張ノードデバイスに設定がある場合は、以前の設定の書き込み消去を実行して、拡張ノードデバイスをリロードします。

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

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

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



[See more details] をクリックしてエラーを確認します。

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

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

ポートチャネルの設定

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

ポート チャネルの作成

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

ステップ 1 [Provision] > [Fabric] > [Fabric Infrastructure] タブに移動し、ファブリックエッジノードを選択します。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ 2 [Port Channel] タブを選択し、[Create Port Channel] をクリックします。

ステップ 3 表示されたポートの一覧から、バンドルするポートと適切なプロトコルを選択します。

IE 3300 または IE 3400 拡張ノードの場合は、プロトコルとして [On] を選択します。

他の拡張ノードの場合は、プロトコルとして [PAGP] を選択します。

ステップ 4 [完了（Done）] をクリックします。

新しいポートチャネルが作成され、ウィンドウに表示されます。

ステップ 5 [Provision] > [Fabric] > [Host Onboarding] ページに移動します。作成されたポートチャネルを選択します。

結果のウィンドウで、ファブリックエッジノードと拡張ノードの間にポートチャネルを作成する場合は、[Connected Device] タイプとして [Extended Node] を選択します。

ファブリックエッジノードとサーバの間にポートチャネルを作成する場合は、[Connected Device] タイプとして [Server] を選択します。

ステップ 6 [Update] をクリックします。

ポートチャネルの更新

始める前に

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

ステップ 1 [Provision] > [Fabric] > [Fabric Infrastructure] タブに移動し、ファブリックエッジノードを選択します。

タイトルにデバイス名の付いたウィンドウがスライド表示されます。

ステップ 2 [Port Channel] タブを選択します。

ステップ 3 表示されるポートチャネルのリストから、更新するポートチャネルを選択します。

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

ステップ 4 ポートチャネルでインターフェイスを追加したり、既存のインターフェイスを削除したりすることができます。ポートチャネルで必要な更新を実行します。

ステップ 5 [Done] をクリックします。

ポートチャネルの削除

ステップ 1 ホームページから、[Provision] > [Fabric] > [Fabric Infrastructure] トポロジビューに移動します。

ステップ 2 ポートチャネルを削除するデバイスをクリックします。

デバイス名の付いたウィンドウがスライド表示されます。

ステップ 3 [Port Channel] タブを選択します。

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

ステップ 4 削除するポートチャネルを選択して、[Delete] をクリックします。

ステップ 5 表示された削除の確認メッセージで [Yes] をクリックします。

これにより、ポートチャネルが削除されます。

マルチキャスト概要

マルチキャスト トラフィックは、次のような異なる方法で転送されます。

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

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

マルチキャストの設定

リリース 1.3.3.0 以降、Cisco DNA Center は仮想ネットワークでグループ通信またはマルチキャストトラフィックを有効にするためのワークフローを提供しています。このワークフローでは、ネットワークでのマルチキャスト実装（ネイティブマルチキャストまたはヘッドエンドレプリケーション）を選択することもできます。

ステップ 1 Cisco DNA Center の [Home] ページで、[Provision] をクリックします。すべてのプロビジョニングされたファブリック ドメインがウィンドウに表示されます。

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

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

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

結果のウィンドウは、マルチキャスト設定のワークフローを開始します。

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

ステップ 6 使用可能な仮想ネットワークのリストから、マルチキャストを設定する仮想ネットワークを選択します。**[次へ (Next)]** をクリックします。

ステップ 7 [IP Pools] ドロップダウンリストから、1 つの IP アドレスプールを選択します。選択した IP アドレスプールは、選択した仮想ネットワークに関連付けられます。**[次へ (Next)]** をクリックします。

ステップ 8 実装するマルチキャストのタイプを選択します。

- **SSM**（ 送信元特定マルチキャスト）
- **ASM**（任意の固有のマルチキャスト）

[次へ (Next)] をクリックします。

ステップ 9 a) [SSM] を選択時、仮想ネットワークごとに IP グループの範囲を追加して、SSM リストを設定します。仮想ネットワークに複数の IP グループ範囲を追加できます。

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

[次へ (Next)] をクリックします。

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

- **内部 RP**
- **外部 RP**

[次へ (Next)] をクリックします。

[Internal RP] を選択した場合は、次の手順を実行します。

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

[External RP] を選択した場合は、次の手順を実行します。

1. 外部ランデブーポイントの IP アドレスを入力します。
2. **[次へ (Next)]** をクリックします。

ステップ 10 設定を送信する前に、[Summary] ページに表示されているマルチキャスト設定を確認し、必要に応じて変更します。

[Finish] をクリックして、マルチキャストの設定を完了します。

サイト間レイヤ 2 のハンドオフ

サイト間のレイヤ2ハンドオフ機能を使用すると、ファブリック内の複数のサイトにわたってIPサブネットを拡張できます。同じIPサブネットがファブリック内のサイト間で共存します。

次の制約事項に注意してください。

- 一体型ファブリックまたはボーダーとエッジとして設定されたデバイスは、サイト間のレイヤ 2 ハンドオフには使用できません。
- サイト間のレイヤ 2 ハンドオフと SDA トランジットはサポートされていません。

始める前に

- すべてのデバイスが検出され、プロビジョニングされており、IPプールが共有されるサイトでその IP プールが予約されていることを確認します。
- IPプールを共有するサイトがアンダーレイ接続されていることを確認します。ボーダー間でこの接続がないと、共通サブネット上のIPアドレスを取得しようとするホストでDHCPが機能しない可能性があります。

- アンダーレイマルチキャストが設定されていることを確認します。これは、レイヤ2のフラッディングが機能するために必要です。アンダーレイマルチキャストは、LAN 自動化ワークフロー中に設定されます。

ステップ 1 ファブリック ドメインへの仮想ネットワークの関連付け. [Layer-2 Flooding] チェックボックスと [Common Pool] チェックボックスがオンになっていることを確認します。

[Layer-2 Flooding] と [Common Pool] が有効になっている場合、IP プールは他のサイトへ拡張できるようになります。

ステップ 2 ボーダーにレイヤ 2 ハンドオフを設定します。

[Provision] > [Fabric] > [Fabric Infrastructure] タブで、サイト間レイヤ 2 ハンドオフを設定するボーダーデバイスを選択します。

[L2 Handoff] セクションで、共通 IP プールが関連付けられている仮想ネットワークを選択します。

サイト間で他のボーダーに接続するボーダーの外部インターフェイスを設定します。

[Extend the subnet to other site] チェックボックスをオンにして、外部 VLAN 番号を共通 IP プールに割り当てます。

ステップ 3 IP プールを共有する他のサイトに対して、上記の手順を繰り返します。

すべての相互接続されたボーダーで同じ外部 VLAN 番号を指定していることを確認します。

Applications

アプリケーションおよびアプリケーション セット

アプリケーションは、ネットワーク内で使用されているソフトウェアプログラムまたはネットワーク シグナリング プロトコルです。Cisco DNA Center は、約 1400 の異なるアプリケーションから成る Cisco Next Generation Network-Based Application Recognition（NBAR2）ライブラリの全アプリケーションをサポートしています。

アプリケーションは、アプリケーションセットと呼ばれる論理グループに分類されています。アプリケーションセットには、ポリシー内でのビジネスとの関連性を割り当てることができます。

アプリケーションは、同様のトラフィック処理要件が規定されている RFC 4594 の定義に従い、業界標準ベースのトラフィック クラスにもマッピングされています。トラフィッククラスでは、割り当てられているビジネスとの関連性グループに基づいて、アプリケーショントラフィックに適用される処理（Differentiated Services Code Point（DSCP）マーキング、キューイング、破棄など）を定義します。

Cisco DNA Center に含まれていない追加のアプリケーションがある場合は、カスタム アプリケーションとして追加して、アプリケーションセットに割り当てることができます。詳細については、カスタムアプリケーション（109ページ）を参照してください。必要なすべてのアプリケーションを含むカスタム アプリケーション セットを作成することもできます。

NBAR2 の詳細については、https://www.cisco.com/c/en/us/products/ios-nx-os-software/network-based-application-recognition-nbar/index.htmlを参照してください。

単方向と双方向のアプリケーション トラフィック

一部のアプリケーションは、完全な左右対称であり、接続の両端に同一の帯域幅プロビジョニングを必要とします。このようなアプリケーションのトラフィックを、双方向のトラフィックと呼びます。たとえば、100 kbps の低遅延キューイング（LLQ）が一方向の音声トラフィックに割り当てられている場合、逆方向の音声トラフィックにも 100 kbps の LLQ をプロビジョニングする必要があります。このシナリオは、同じ Voice over IP（VoIP）コーダ/デコーダ（コーデック）が両方の方向で使用されており、マルチキャスト保留音（MOH）のプロビジョニングが考慮されていないことが前提となっています。しかし、Streaming-Video やマルチキャスト MoH などの特定のアプリケーションは、ほとんどの場合単方向です。したがって、ブランチからキャンパスに向かう方向のトラフィックフローでは、ブランチルータでこのようなトラフィック向けの帯域幅保証をプロビジョニングするのは、不要であるばかりか非効率的となる可能性があります。

Cisco DNA Center では、アプリケーションが特定のポリシーに関して単方向か双方向かを指定できます。

スイッチおよびワイヤレス コントローラでは、NBAR2 やカスタム アプリケーションがデフォルトで単方向となっています。ただし、ルータでは、NBAR2 アプリケーションはデフォルトで双方向です。

カスタム アプリケーション

カスタム アプリケーションは、Cisco DNA Center に追加するアプリケーションです。カスタム アプリケーションの横にはオレンジ色のバーが表示され、標準 NBAR2 アプリケーションおよびアプリケーション セットと区別されます。有線デバイスについては、サーバ名、IP アドレスとポート、または URL に基づいてアプリケーションを定義できます。ワイヤレス デバイスについてはカスタム アプリケーションを定義できません。

IP アドレスとポートに従ってアプリケーションを定義する場合は、DSCP 値とポート分類を定義することもできます。

設定プロセスを簡素化するために、類似のトラフィックおよびサービスレベル要件を持つ別のアプリケーションに基づいてアプリケーションを定義できます。Cisco DNA Center は、他のアプリケーションのトラフィック クラス設定を、定義しているアプリケーションにコピーします。

Cisco DNA Center カスタム アプリケーションの一部として定義される場合でも、ポート番号 80、443、および 8080 の ACL を設定しません。カスタム アプリケーションでトランスポート IP が定義されている場合、Cisco DNA Center はデバイス上のアプリケーションを設定します。

（注） ポリシーが展開されているときにデバイス上のカスタムアプリケーションをプログラムする場合は、そのカスタム アプリケーションを、ポリシーで定義されているいずれかのアプリケーション セットに割り当てる必要があります。

お気に入りのアプリケーション

Cisco DNA Center では、他のすべてのアプリケーションの前に設定したいアプリケーションにフラグを付けることができます（カスタムアプリケーションを除く）。お気に入りとしてアプリケーションにフラグを付けることで、デバイス上のお気に入りのアプリケーションに対してQoSポリシーが設定されていることを確認できるようにします。詳細については、リソースが制限されているデバイスの処理順を参照してください。

お気に入りとしてマークできるアプリケーションの数に制限はありませんが、少数のお気に入りのアプリケーション（たとえば、25 未満）だけを指定すると、TCAM（Ternary Content Addressable Memory）が限られているネットワークデバイスでの展開において、それらのアプリケーションがビジネス関連の観点から正しく処理されるようにするうえで役立ちます。

お気に入りのアプリケーションは、ビジネス関連のグループまたはトラフィック クラスに属させることが可能で、ポリシー単位ではなくシステム全体で設定されます。たとえば、お気に入りとしてcisco-jabber-videoアプリケーションにフラグを付けた場合、そのアプリケーションはすべてのポリシーでお気に入りのフラグが付きます。

ビジネス関連のアプリケーションだけでなく、ビジネスに関係のないアプリケーションにもお気に入りのフラグを付けられることに注意してください。たとえば、管理者がネットワーク上に大量の望ましくない Netflix トラフィックがあることに気づいた場合、Netflix にお気に入りのアプリケーションとしてフラグを付けることができます（Netflixがビジネスに関係ないアプリケーションとして割り当てられている場合でも可能）。この場合、Netflixは、その他のビジネスに関係のないアプリケーションより先にデバイスポリシーに組み込まれるようになり、このアプリケーションを制御するビジネス上の目的が確実に実現されます。

アプリケーションおよびアプリケーション セットの設定

次のサブセクションでは、アプリケーションとアプリケーションセットのコンテキストで実行できるさまざまなタスクについて説明します。

アプリケーション設定の変更

アプリケーションの設定、あるいは既存のNBARアプリケーションまたはカスタムアプリケーションのトラフィッククラスを変更できます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] > [Application] を選択します。

ステップ 2 [Search]、[Show]、または [View By] フィールドを使用して、変更するアプリケーションを見つけます。

ステップ 3 [アプリケーション名（Application Name）] をクリックします。

ステップ 4 ダイアログボックスで、1 つまたは両方の設定を変更します。

- [Traffic Class]：ドロップダウンリストからトラフィック クラスを選択します。有効なトラフィック クラスは、BROADCAST_VIDEO、BULK_DATA、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、NETWORK_CONTROL、OPS_ADMIN_MGMT、REAL_TIME_INTERACTIVE、SIGNALING、TRANSACTIONAL_DATA、VOIP_TELEPHONY です。
- [Application Set]：ドロップダウンリストからアプリケーションの設定を選択します。有効なアプリケーションセットは、認証サービス、バックアップおよびストレージ、コラボレーション アプリケーション、コンシューマ ブラウジング、コンシューマ ファイル シェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、データベース アプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 **[Save]** をクリックします。

サーバ名に基づくカスタム アプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

ステップ 4 ダイアログボックスで、次のフィールドに必要な情報を入力します。

フィールド	説明
アプリケーション名	カスタム アプリケーションの名前。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。
Type	ユーザがアプリケーションにアクセスする方法。サーバ経由でアクセス可能なアプリケーションの [サーバ名（Server Name）] を選択します。
サーバ名	アプリケーションをホストするサーバの名前。
Similar to	類似するトラフィック処理要件を持つアプリケーション。オプションボタンをクリックしてこのオプションを選択し、ドロップダウンリストからアプリケーションを選択します。Cisco DNA Centerは、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。

フィールド	説明
トラフィッククラス	アプリケーションが属するトラフィック クラス。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。
アプリケーションセット	アプリケーションを配置するアプリケーションセット。有効なアプリケーションの設定は、認証サービス、バックアップおよびストレージ、コラボレーション アプリケーション、コンシューマブラウジング、コンシューマ ファイル シェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業 ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカル サービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 5 [OK] をクリックします。

IP アドレスおよびポート ベースのカスタム アプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

ステップ 4 [Application Name] フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。

ステップ 5 [種類（Type）] エリアで、[サーバ IP/ポート（Server IP/Port）] ラジオボタンをクリックして、アプリケーションが IP アドレスとポートを通じてアクセスできます。

ステップ 6 [DSCP] チェック ボックスをオンにして、DSCP 値を定義します。値を定義しない場合のデフォルト値は [Best Effort] です。ベストエフォート サービスとは原則的に、いずれの QoS も適用されないネットワーク デバイスのデフォルト動作です。

ステップ 7 [IP/Port Classifiers] チェックボックスをオンにして、アプリケーションの IP アドレスおよびサブネット、プロトコル、ポートまたはポート範囲を選択します。有効なプロトコルは、[IP]、[TCP]、[UDP]、[TCP/UDP] です。[IP] プロトコルを選択した場合は、ポート番号または範囲は定義しません。 をクリックして、さらに分類子を追加します。

ステップ 8 次のいずれかの方法を使用して、アプリケーショントラフィック処理要件を定義します。

- [Similar To]：お使いのアプリケーションに既存のアプリケーションと同様のトラフィック処理要件がある場合は、[Similar To] オプションボタンをクリックし、ドロップダウンリストからアプリケーションを選択します。Cisco DNA Center は、他のアプリケーションのトラフィッククラスを、定義しているアプリケーションにコピーします。
- [Traffic Class]：アプリケーションに定義するトラフィッククラスがわかっている場合は、[Traffic Class] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ 9 [Application Set] ドロップダウンリストから、アプリケーションが属するアプリケーションセットを選択します。有効なアプリケーションの設定は、認証サービス、バックアップおよびストレージ、コラボレーションアプリケーション、コンシューマブラウジング、コンシューマファイルシェアリング、コンシューマゲーミング、コンシューマメディア、コンシューマ misc、コンシューマ ソーシャル ネットワーキング、データベースアプリケーション、デスクトップ仮想化、電子メール、企業ipc、ファイル共有、一般的なブラウジング、一般的なメディア、一般的な misc、トンネリング、ローカルサービス、ネーミングサービス、ネットワーク制御、ネットワーク管理、リモートアクセス、saas アプリケーション、シグナリング、ソフトウェア開発ツール、ソフトウェアアップデート、ストリーミングメディアです。

ステップ 10 [OK] をクリックします。

URL に基づくカスタム アプリケーションの作成

Cisco DNA Centerに存在しないアプリケーションがある場合、カスタム アプリケーションとして追加することができます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [アプリケーションの追加（Add Application）] をクリックします。

[アプリケーションの追加（Add Application） **]** ダイアログボックスが表示されます。

ステップ 4 **[** アプリケーション名（Application Name） **]** フィールドに、アプリケーションの名前を入力します。名前には、下線とハイフンも含めて最大 24 文字の英数字を指定できます。アプリケーション名で使用できる特殊文字は、下線とハイフンのみです。

ステップ 5 **タイプ**については、[**URL**] オプションボタンをクリックします。

ステップ 6 [**Url**] フィールドに、アプリケーションに到達するために使用する url を入力します。

ステップ 7 トラフィック クラスの設定:

- 同様のトラフィック処理要件を持つ別のアプリケーションと同じトラフィッククラスを使用するには、オプションボタンをクリックして、ドロップダウンリストからアプリケーションを選択します。

- トラフィッククラスを指定するには、[**トラフィッククラス (Traffic class)**] オプションボタンをクリックし、ドロップダウンリストからトラフィッククラスを選択します。有効な値は BULK_DATA、TRANSACTIONAL_DATA、OPS_ADMIN_MGMT、NETWORK_CONTROL、VOIP_TELEPHONY、MULTIMEDIA_CONFERENCING、MULTIMEDIA_STREAMING、BROADCAST_VIDEO、REAL_TIME_INTERACTIVE、および SIGNALING です。

ステップ 8 [**アプリケーションセット (Application set)**] ドロップダウンリストから、アプリケーションを配置するアプリケーションセットを選択します。

ステップ 9 [OK] をクリックします。

カスタム アプリケーションの編集または削除

必要な場合は、カスタム アプリケーションを変更または削除できます。

（注） アプリケーション ポリシーによって直接参照されているカスタム アプリケーションを削除することはできません。通常、アプリケーションポリシーはアプリケーションセットを参照し、個々のアプリケーションを参照しません。ただし、ポリシーにアプリケーションの特別な定義（コンシューマまたはプロデューサの割り当てや双方向の帯域幅プロビジョニングなど）が設定されている場合、ポリシーはそのアプリケーションを直接参照します。そのため、アプリケーションを削除する前に、特別な定義を削除するか、またはアプリケーションへの参照を削除する必要があります。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ 2 [Application] タブをクリックします。

ステップ 3 [Search]、[Show]、または [View By] フィールドを使用して、変更するアプリケーションを見つけます。

ステップ 4 アプリケーションを編集するには、次の手順を実行します。

a) アプリケーション名をクリックして、必要な変更を行います。フィールドの詳細については、サーバ名に基づくカスタム アプリケーションの作成（111 ページ）、IP アドレスおよびポート ベースのカスタム アプリケーションの作成（112 ページ）、またはURL に基づくカスタム アプリケーションの作成（113 ページ）を参照してください。

b) [OK] をクリックします。

ステップ 5 アプリケーションを削除するには：アプリケーションボックスで をクリックし、[OK] をクリックして確定します。

アプリケーションをお気に入りにする

アプリケーションをお気に入りとしてマークして、アプリケーションの QoS 設定を、他のアプリケーションの QoS 設定の前にデバイスに展開する必要あることを指定できます。お気に入りとしてマークされたアプリケーションには、その横に黄色の星が付いています。

ポリシーを追加または編集すると、お気に入りとしてマークされたアプリケーションがアプリケーション セットの上部に表示されます。

アプリケーションは、個々のポリシーベースではなくシステム全体で設定されます。詳細については、「お気に入りのアプリケーション （110 ページ）」を参照してください。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ 2 [Application] タブをクリックします。

ステップ 3 お気に入りとしてマークするアプリケーションを特定します。

ステップ 4 ☆ をクリックします。

カスタム アプリケーション設定の作成

使用したいアプリケーションセットがない場合、カスタム アプリケーション セットを作成できます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [Application Visibility] の順にクリックします。

ステップ 2 [Application Sets] タブをクリックします。

ステップ 3 [Add Application Set] をクリックします。

ステップ 4 ダイアログ ボックスに、新しいアプリケーション設定の名前を入力します。

Cisco DNA Center で新しいアプリケーション設定が作成されますが、その中にアプリケーションは存在しません。

ステップ 5 [OK] をクリックします。

ステップ 6 [Search] を使用して [Show] または [View By] フィールドを使用して、アプリケーション設定を見つけます。

ステップ 7 新しいアプリケーション設定に移動させるアプリケーションを見つけます。

ステップ 8 移動させるアプリケーションの横にあるチェック ボックスをオンにします。

ステップ 9 新しいアプリケーション設定にアプリケーションをドラッグ アンド ドロップします。

カスタム アプリケーション セットの編集または削除

必要な場合は、カスタム アプリケーションを変更または削除できます。

（注） アプリケーション ポリシーによって参照されているカスタム アプリケーション セットを削除することはできません。アプリケーション セットを削除する前に、ポリシーからアプリケーション セットを削除する必要があります。

ステップ 1 From the Cisco DNA Center **Home** page, click **Provision > Services > APplication Visibility**.

ステップ 2 Click the **APplication Sets** tab.

ステップ 3 [検索（Search）]、[表示（Show）]、または [表示方法（View By）] フィールドを使用して、変更するアプリケーション セットを見つけます。

ステップ 4 次のいずれかを実行します。

- アプリケーション設定するには、アプリケーション設定に、またはアプリケーション設定からアプリケーションをドラッグアンドドロップします。[OK] をクリックして、それぞれの変更を確定します。
- アプリケーション設定を削除するには、アプリケーション設定ボックスにある をクリックし、次に [OK] をクリックして確定します。

アプリケーション ホスティング

アプリケーション ホスティングについて

アプリケーション ホスティングを使用すると、Cisco DNA Center によって管理されているデバイス上のサードパーティ製アプリケーションのライフサイクルを管理できます。このリリースでは、お客様は Cisco IOS XE ソフトウェアバージョン 16.12.1s を搭載した Catalyst 9300 シリーズスイッチのサードパーティ製 docker アプリケーションを利用できます。

アプリケーション ホスティングの前提条件

デバイスでアプリケーション ホスティングを有効にするには、次の前提条件を満たしている必要があります。

- デバイスの HTTPS ログイン情報を設定します。デバイスを手動で Cisco DNA Center に追加するときに HTTPS ログイン情報を設定するか、デバイスのログイン情報を編集できます。詳細については、「ネットワーク デバイス クレデンシャルの更新」を参照してください。
- ユーザ認証用にローカルの認証サーバまたは AAA サーバを設定します。ユーザ名およびパスワードは特権 EXEC モード（レベル 15）で設定する必要があります。詳細については、『Cisco Digital Network Architecture Center Administrator Guide』の「Configure Authentication and Policy Servers」を参照してください。

- デバイスで、着脱可能な USB SSD 外部ストレージがサポートされていることを確認します。

（注） 3 ノード Cisco DNA Center クラスタは、アプリケーション ホスティングの高可用性（HA）をサポートしていません。この機能をスタンドアロン アプライアンスのみがサポートします。

アプリケーションをホストするデバイスの準備状況の表示

スイッチにアプリケーションをインストールする前に、Cisco Catalyst 9300 シリーズ スイッチのアプリケーションをホスティングするための準備状況を確認する必要があります。

ステップ 1 From the Cisco DNA Center home page, choose **Provision** > **Services** > **APp Hosting**.

ステップ 2 [All Devices] をクリックします。

ステップ 3 アプリケーションをホストできるデバイスのリストが表示されます。[App Hosting Status] は、デバイスがアプリケーションをホストするための準備状況を示します。ステータスに [Not Ready] と表示されている場合は、ステータスをクリックして理由を確認できます。

アプリケーションの追加

シスコパッケージまたは Docker アプリケーションを追加できます。

始める前に

- [Cisco Package] アプリケーション：IOS SDK ツールを使用してアプリケーションをパッケージ化し、アプリケーションが IOS XE オペレーティングシステムと互換性を持つようにする必要があります。
- [Docker] アプリケーション：Docker イメージを tar ファイルとして保存する必要があります。Docker イメージを tar ファイルとして保存するには、次のコマンドを使用します。

```
docker save -o <path for generated tar file> <image name:tag>
Example: docker save -o alpine-tcpdump.tar itsthenetwork/alpine-tcpdump:latest
```

ステップ 1 Cisco DNA Center ホームページで、**[Provision]** > **[Services]** > **[App Hosting]** の順に選択します。

ステップ 2 [New Application] をクリックします。

ステップ 3 ドロップダウンリストからアプリケーションの [Type] と [Category] を選択します。

ステップ 4 [Select] をクリックして、アップロードするアプリケーションを選択します。

ステップ 5 [Upload] をクリックします。

新しく追加されたアプリケーションは、[App Hosting] ページで確認できます。

Cisco Catalyst 9300 デバイスへのアプリケーションのインストール

Cisco DNA Center Cisco Catalyst 9300 シリーズ スイッチにアプリケーションをインストールできます。

始める前に

- 前提条件を満たします。詳細については、「アプリケーション ホスティングの前提条件（116 ページ）」を参照してください。
- アプリケーションを Cisco DNA Center に追加します。詳細については、「アプリケーションの追加 （117 ページ）」を参照してください。
- アプリケーションをホストするためのスイッチの準備状況を確認します。詳細については、「アプリケーションをホストするデバイスの準備状況の表示 （117ページ）」を参照してください。

ステップ 1 Cisco DNA Center のホームページから、[Provision] > [Services] > [App Hosting] > > の順に選択します。

ステップ 2 アプリケーションを選択し、[Install] をクリックします。

ステップ 3 アプリケーションのインストール先デバイスを選択し、[Next] をクリックします。

ステップ 4 [Configuration App] タブで次の設定を入力します。

- **App Networking**
  - [Device Network]：[Select Network] ドロップダウンリストをクリックして、アプリケーションを設定する VLAN を選択します。
  - [App IP address]：[Address Type] ドロップダウンリストから、[Static] または [Dynamic] を選択します。[Static] を選択した場合は、サムネイルアイコンをクリックして、アプリケーションの [IP Address]、[Gateway]、[Prefix/Mask]、および [DNS] を入力します。
- [Resource Allocation]：[Allocate all resources available on a device] または [Customize resource allocation] チェックボックスをクリックします。[Customize resource allocation] チェックボックスをオンにすると、[CPU]、[Memory]、および [Persistent Storage] の最大値を低い値に変更できます。
- （オプション）[Custom Settings]：Cisco パッケージアプリケーションにのみ適用可能です。アプリケーションによって指定された属性の設定の詳細を入力します。
- （オプション）[App Data]：アプリケーション固有のファイルを参照し、アップロードします。必要なアプリケーション固有のファイルを特定するには、関連するアプリケーションのドキュメントを参照してください。
- [Docker Runtime Options]：アプリケーションに必要な Docker ランタイムオプションを入力します。

ステップ 5 [Next] をクリックして、[Confirm] 画面でアプリケーション設定を確認します。

ステップ 6 [完了（Finish）] をクリックします。

ステップ 7 インストールの [Confirmation] ウィンドウで [Yes] をクリックして、選択した Cisco Catalyst 9300 デバイスでのアプリケーションのインストールを完了します。

次のタスク

アプリケーションをインストールすると、デバイスの IOS XE 設定も変更されます。実行コンフィギュレーションのこの変更は、ルータのリロード後にアプリケーションが予期したとおりに機能するように、スタートアップ コンフィギュレーションにコピーする必要があります。アプリケーションのインストールが正常に完了したら、[Template Editor] を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

アプリケーションの更新

Cisco DNA Center で追加されたアプリケーションを更新できます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [App Hosting] > > の順に選択します。

[App Hosting] ページに使用可能なアプリケーションを表示できます。

ステップ 2 更新するアプリケーションを選択します。

ステップ 3 [Update APplication] をクリックします。

ステップ 4 ドロップダウンリストからアプリケーションの [Type] と [Category] を選択します。

ステップ 5 [Select] をクリックして、アップロードする新しいバージョンのアプリケーションを選択します。

ステップ 6 [Upload] をクリックします。

Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール

Cisco Catalyst 9300 シリーズ スイッチからアプリケーションをアンインストールできます。

ステップ 1 Cisco DNA Center のホームページで、[Provision] > [Services] > [App Hosting] > > の順に選択します。

ステップ 2 アプリケーションを選択し、[Manage] をクリックして、アプリケーションを使用するデバイスを表示します。

ステップ 3 アプリケーションをアンインストールするデバイスを選択します。

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

アプリケーションの削除

Cisco DNA Center からアプリケーションを削除できます。

始める前に

アプリケーションを使用しているすべてのデバイスからアプリケーションをアンインストールする必要があります。詳細については、Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール （119 ページ）を参照してください。

ステップ 1 Cisco DNA Center のホームページから、[Provision] > [Services] > [App Hosting] > > の順に選択します。

[App Hosting] ページで使用可能なホストされたアプリケーションを表示できます。

ステップ 2 削除するアプリケーションを選択します。

ステップ 3 [Delete Applicaiton] をクリックします。

ステップ 4 確認ダイアログボックスで [OK] をクリックします。

アプリケーションは、Cisco DNA Center によって管理されているいずれのデバイスでも使用されていない場合にのみ削除されます。それ以外の場合、エラーメッセージに、アプリケーションを使用しているデバイスの数が表示されます。

確認ダイアログボックスで [Cancel] をクリックし、アプリケーションをアンインストールします。詳細については、Cisco Catalyst 9300 デバイスからのアプリケーションのアンインストール （119 ページ）を参照してください。

アプリケーションログのダウンロード

Cisco DNA Center からアプリケーションログをダウンロードできます。

ステップ 1 From the Cisco DNA Center home page, choose **Provision** > **Services** > **APp Hosting**.

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [APp logs] をクリックして、Cisco DNA Center からアプリケーションログをダウンロードします。

ステップ 4 [APp Logs] ポップアップウィンドウで、ダウンロードするアプリケーションログファイルをドロップダウンリストから選択し、[Download] をクリックします。

デバイス テクニカル サポート ログのダウンロード

トラブルシューティングを行うために、Cisco DNA Center からデバイスのテクニカルサポートのログをダウンロードできます。

ステップ 1 From the Cisco DNA Center home page, choose **Provision** > **Services** > **APp Hosting**.

ステップ 2 [All Devices] をクリックします。

アプリケーションをホストできるデバイスのリストが表示されます。

ステップ 3 [Tech Support logs] をクリックして、デバイスのテクニカルサポートログを Cisco DNA Center からダウンロードします。