Cisco DNA Spaces：コネクタ コンフィギュレーション ガイド

初版：2019 年 8 月 1 日

最終更新：2021 年 10 月 13 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

対象読者

このドキュメントは、組織内の資産の使用状況を監視、管理、および最適化するために Cisco DNA Spaces を展開する Cisco Digital Network Architecture（DNA）Spaces ネットワーク管理者および IT 管理者を対象としています。

表記法

このマニュアルでは、次の表記法を使用しています。

表 *1* : 表記法

表記法	説明
太字	コマンド、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザーが値を指定する関数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。文字列を引用符で囲まないでください。引用符で囲むと、文字列に引用符が含まれます。

表記法	説明
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco Marketplace にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

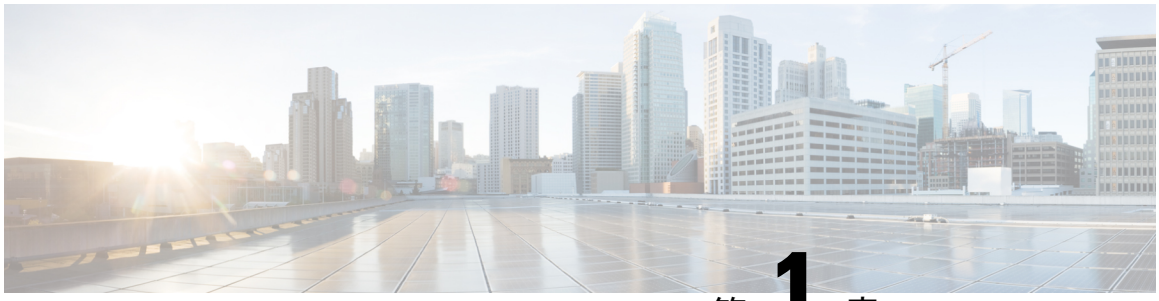
Cisco バグ検索ツール

Cisco バグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

はじめに

第 I 部

概要



第 1 章

概要

Cisco DNA Spaces：コネクタ の概要

Cisco DNA Spaces：コネクタ（このドキュメントでは以降すべての参照箇所でコネクタ と呼びます）は、各 コントローラ がクライアント情報を失わずにクライアントデータを送信できるようにすることで、Cisco DNA Spaces が複数の コントローラ およびスイッチと効率的に通信できるようにします。

コネクタ は、コントローラ、アクセスポイント（AP）、およびスイッチから効率的にデータを収集して集約し、集約したデータを Cisco DNA Spaces に送信します。コネクタ アーキテクチャでは、複数の コントローラ、AP、およびスイッチが単一のポイント（コネクタ）を介して Cisco DNA Spaces に接続できます。単一の コネクタ は、シスコ ワイヤレス コントローラ、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、および Cisco Catalyst 9300/9400 シリーズ スイッチ に同時に接続できます。

（注） このドキュメントでは、コントローラ という用語を、次を指すものとして使用しています。詳細については、「互換性マトリクス」を参照してください。

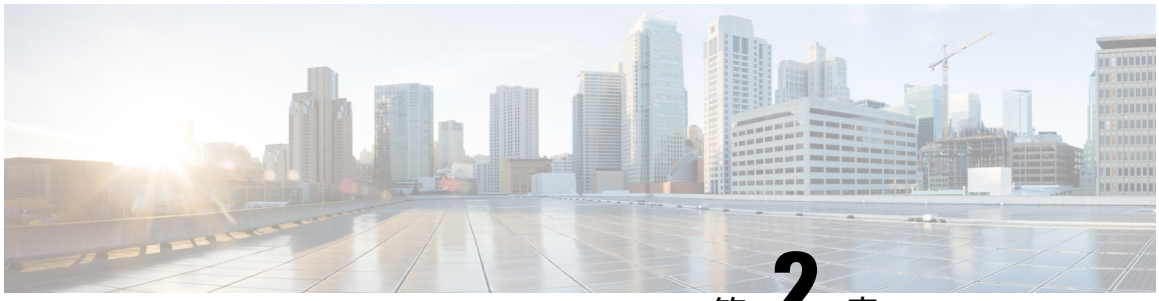
- シスコ ワイヤレス コントローラ（Cisco DNA Spaces ダッシュボードに WLC AireOS として表示）
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（Cisco DNA Spaces ダッシュボードに Catalyst WLC として表示）
- Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ（Cisco EWC-AP）

コネクタ はデータを HTTPS 経由で Cisco DNA Spaces に送信します。データはプロキシを介してルーティングすることもできます。

（注） コネクタ の最新バージョンへのアップグレードを推奨します。

第 II 部

使用する前に



第 2 章

互換性マトリクス

Cisco DNA Spaces の互換性マトリクス

ハードウェアまたはアプリケーション名	Cisco DNA Spaces：コネクタ のサポート
シスコ ワイヤレス コントローラ	• 8.5 • 8.8 • 8.9 • 8.10 （注） リストに表示されている各リリースの最新のソフトウェアまたはメンテナンスリリースバージョンを使用します。

ハードウェアまたはアプリケーション名	Cisco DNA Spaces：コネクタ のサポート
Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	• 16.12.4 • 16.12.4a • 16.12.5 • 17.3.1 • 17.3.2 • 17.3.3 • 17.3.4 • 17.4.x • 17.5.x • 17.6.1 （注） リストに表示されている各リリースの最新のソフトウェアバージョンまたはメンテナンスリリースを使用します。

ハードウェアまたはアプリケーション名	Cisco DNA Spaces：コネクタ のサポート
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（Cisco EWC-AP）	次のバージョンがサポートされます。 • 16.12.5 • 17.3.1 • 17.3.2a、 • 17.3.3 • 17.3.4 • 17.4.1 • 17.5.1 • 17.6.1 （注） リストに表示されている各リリースの最新のソフトウェアバージョンまたはメンテナンスリリースを使用します。 次のアクセスポイントがサポートされます。 • Cisco Aironet 9115 シリーズ アクセスポイント • Cisco Aironet 9117 シリーズ アクセスポイント • Cisco Aironet 9120 シリーズ アクセスポイント • Cisco Aironet 9130 シリーズ アクセスポイント
Cisco Catalyst 9300/9400 シリーズ スイッチ	サポートされるバージョンは17.3.3以降です。
Cisco Prime Infrastructure	—
Cisco DNA Center	—

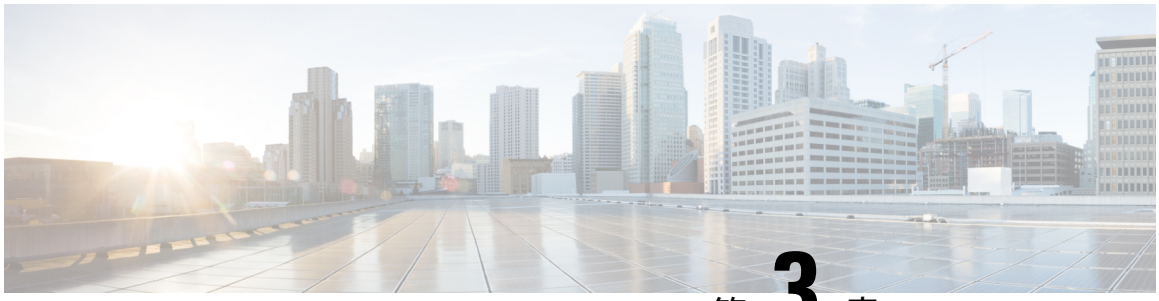
ハードウェアまたはアプリケーション名	Cisco DNA Spaces：コネクタ のサポート
Cisco DNA Spaces：IoT サービス	• Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 17.3.1 以降でサポート • シスコ ワイヤレス コントローラ ではサポート対象外 • Catalyst アクセスポイント上のシスコ組み込みワイヤレスコントローラ（Cisco EWC-AP） ではサポート対象外
OpenRoaming	• Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 16.12 以降でサポート • シスコ ワイヤレス コントローラ 8.3 以降でサポート
Cisco FastLocate の コントローラ でサポート	• シスコ ワイヤレス コントローラ リリース 8.1.123.0 でサポート • Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のすべてのリリースでサポート
Cisco HyperLocation の コントローラ でサポート	• シスコ ワイヤレス コントローラ でサポート • Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポート
コネクタのアクティブ/アクティブ	• 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（Cisco EWC-AP） ではサポート対象外 • Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポート • シスコ ワイヤレス コントローラ でサポート

ハードウェアまたはアプリケーション名	Cisco DNA Spaces：コネクタ のサポート
テスト済みの VMware 環境	• VMware ESXi：6.5.0 Update 2（ビルド 13004031）、6.7.0 Update 2（ビルド 13006603）、6.7.0 Update 3（ビルド 16316930） • VMware vSphere クライアントバージョン 6.7.0 • VMware vCenter サーバアプライアンス 6.7.0
テスト済みの Hyper-V 環境	Hyper-V バージョン 10.0.17763.1

テスト済みプロキシ	• Squid プロキシ
	  • 転送専用モード（SSL トンネリング）
	  • Squid-in-the-Middle モード（傍受機能を使用した SSL トンネリング）
	• McAfee
	• Cisco Web セキュリティアプライアンス

Cisco FastLocate のテスト済みアクセスポイント	• 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 FastLocate のテスト済みアクセスポイント（Wi-Fi 6）	• Cisco Aironet 9120 シリーズ アクセスポイント • Cisco Aironet 9130 シリーズ アクセスポイント
Cisco Hyperlocation のテスト済みアクセスポイント	• Cisco Aironet 3700 シリーズ アクセスポイント（HyperLocation アンテナが必要） • Cisco Aironet 4800 シリーズ アクセス ポイント

ハードウェアまたはアプリケーション名	Cisco DNA Spaces：コネクタ のサポート
コネクタの最小要件およびサイジング	• 2 vCPU • 4 GB RAM • 60 GB ハードディスク



第 3 章

前提条件

Cisco DNA Spaces：コネクタ の設定の前提条件

- 必要なポートが開いていることを確認します。「オープンポートに関する情報（ワイヤレス） （13 ページ）」を参照してください。
- https://www.cisco.com および cisco.com ドメインを明示的に許可して、Cisco DNA Spaces：コネクタ がこれらの Web サイトまたはドメインとの接続を確立できるようにします。
- OpenRoaming を展開する必要がある場合は、https://cisco.openroaming.org. を明示的に許可します。
- 簡易ネットワーク管理プロトコル（SNMP） v2C および v3 の場合、シスコ ワイヤレス コントローラ に Cisco DNA Spaces：コネクタ 証明書を登録するための読み取り/書き込み権限が必要です。
- **config cloud-services cmx disable** コマンドを使用して、Cisco DNA Spaces：コネクタ を有効にする前に、シスコ ワイヤレス コントローラ の Cisco DNA Spaces 接続サービスを無効にします。
- 次のコマンドを実行して、Cisco DNA Spaces：コネクタ を有効にする前に、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の Cisco DNA Spaces 接続サービスを無効にします。
  - **no nmsp cloud-services server url**
  - **no nmsp cloud-services server token**
  - **no nmsp cloud-services enable**
- Cisco DNA Spaces ダッシュボードで設定する コントローラ IP は、Cisco DNA Spaces：コネクタ に到達できる必要があります。

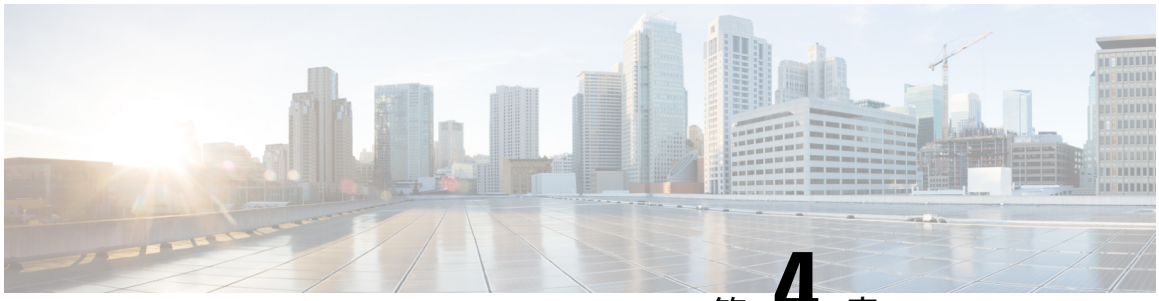
- Cisco DNA Spaces：コネクタ には、ドメインネームシステム（DNS）サーバへのアクセスが必要です。明示的なプロキシを設定する場合、Cisco DNA Spaces：コネクタ はプロキシを使用して通信できる必要があります。
- VMware ESXi 6.5 以降。
- 仮想マシンのサイズ：標準オプション
- 必要な最小帯域幅：4 Mbps（5,000 AP、60,000 クライアント）。

注 キャプティブポータルを使用している場合は、バッファに加えて 30 Mbps 以上の帯域幅を推奨します。この帯域幅により、キャプティブポータルを Cisco DNA Spaces からロードする際のエンドユーザ エクスペリエンスが向上します。

Cisco DNA Spaces：コネクタ の前提条件（有線）

- 必要なポートが開いていることを確認します。「オープンポート（有線） （15ページ）」を参照してください。
- https://www.cisco.com および cisco.com ドメインを明示的に許可して、Cisco DNA Spaces：コネクタ がこれらの Web サイトまたはドメインとの接続を確立できるようにします。
- Cisco DNA Spaces ダッシュボードで設定する Cisco Catalyst 9300/9400 シリーズ スイッチ IP は、Cisco DNA Spaces：コネクタ に到達できる必要があります。
- Cisco DNA Spaces：コネクタ には、許可済みのドメインネームシステム（DNS）サーバが必要です。明示的なプロキシを設定する場合、Cisco DNA Spaces：コネクタ はプロキシを使用して通信できる必要があります。
- VMware ESXi 6.5 以降。
- 仮想マシンのサイズ：標準オプション
- 必要な最小帯域幅：4 Mbps（5,000 AP、60,000 クライアント）。

注 キャプティブポータルを使用している場合は、バッファに加えて 30 Mbps 以上の帯域幅を推奨します。この帯域幅により、キャプティブポータルを Cisco DNA Spaces からロードする際のエンドユーザ エクスペリエンスが向上します。

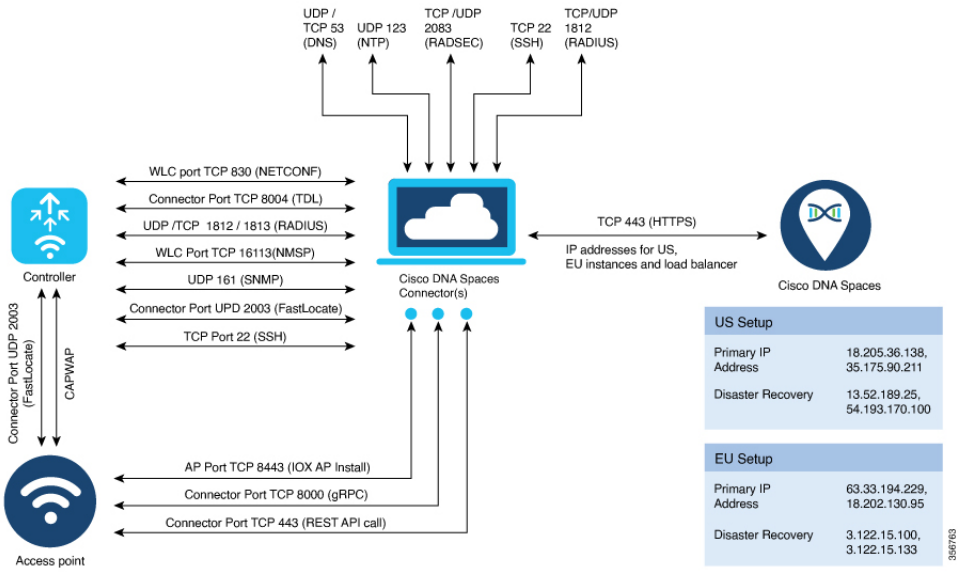


第 4 章

オープンポート（ワイヤレス）

オープンポートに関する情報（ワイヤレス）

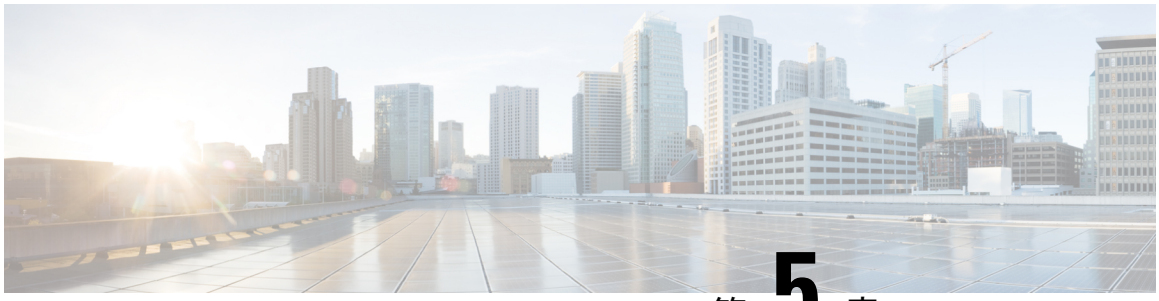
このセクションでは、さまざまなサービスまたはプロトコルを適切に機能させるために開く必要のある コネクタ ポートを示します。



OpenRoaming ファイアウォールルール

表 *2 : OpenRoaming* ファイアウォールルール

送信元 IP アドレス	宛先IP アドレス	方向	トランスポート	送信元ポート	宛先ポート	プロトコル	詳細情報
シスコワイヤレス コントローラの IP アドレス	コネクタ	単一方向（Unidirectional）	UDP および TCP	いずれか（Any）	1812、1813	『Remote Authentication Dial In User Service (RADIUS)』	OpenRoaming クライアントの RADIUS メッセージに関する コネクタ と シスコ ワイヤレス コントローラ 間の通信。
コネクタ	いずれか（Any）	単一方向（Unidirectional）	TCP	いずれか（Any）	2083	RADIUS over TLS (RADSEC)	コネクタ と OpenRoaming ID プロバイダー間の通信
コネクタ	いずれか（Any）	単一方向（Unidirectional）	TCP	いずれか（Any）	443		CSR 署名用の HTTPS : OpenRoaming メンバーシップ

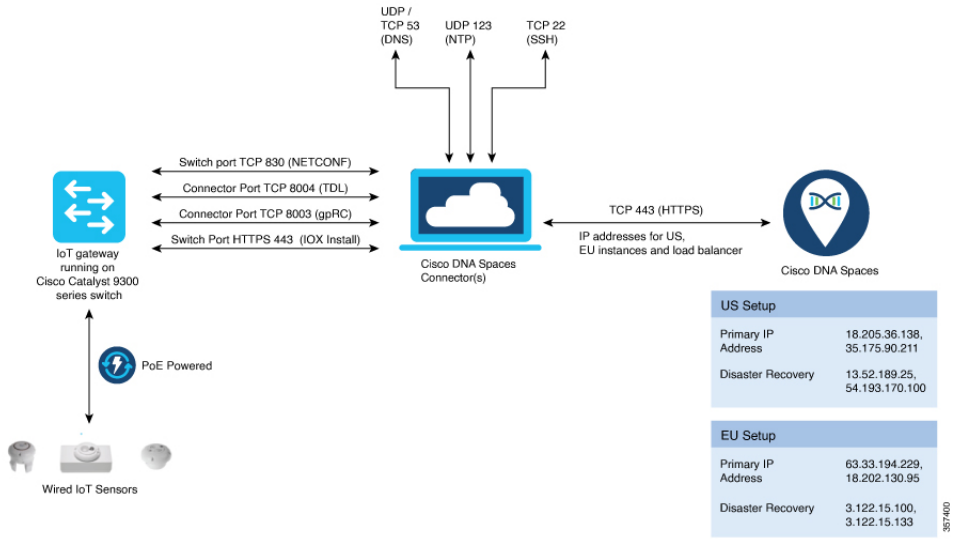


第 5 章

オープンポート（有線）

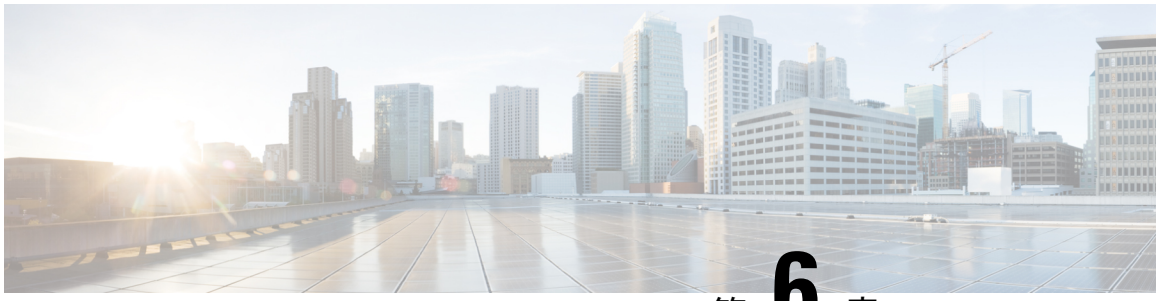
オープンポート（有線）

このセクションでは、各サービスまたはプロトコルを適切に機能させるために開く必要のあるコネクタ ポートを示します。



第 III 部

初期設定



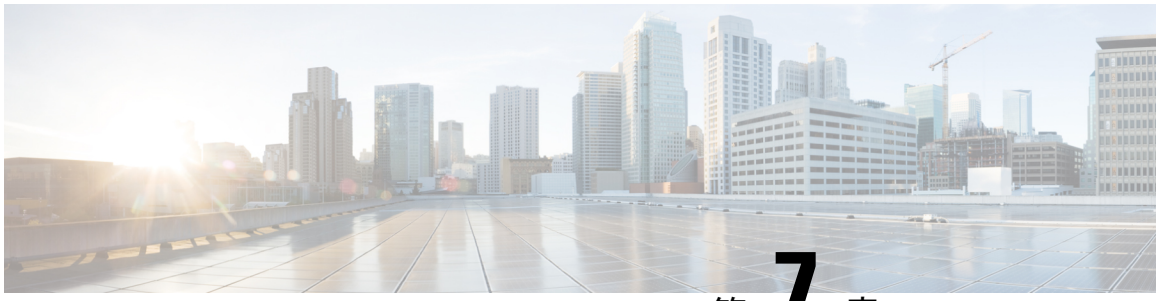
第 6 章

初期設定

Cisco DNA Spaces：コネクタ の初期設定

Cisco DNA Spaces：コネクタ を稼働させるには、次の手順を実行します。

1. ローカル展開ネットワークに Cisco DNA Spaces：コネクタ をインストールします。「Cisco DNA Spaces：コネクタ OVA のダウンロードと展開（単一インターフェイス） （31 ページ）」を参照してください
2. Cisco DNA Spacesダッシュボードで、Cisco DNA Spaces：コネクタ を作成して コネクタ のトークンを生成します。Cisco DNA Spaces からの コネクタ のトークンの取得（ワイヤレス） （69 ページ） または コネクタ インスタンスの作成と Cisco DNA Spaces からのトークンの取得（有線） （67 ページ） を参照してください。
3. 展開された Cisco DNA Spaces：コネクタ で、このトークンを設定します。この設定により、Cisco DNA Spaces と 展開された Cisco DNA Spaces：コネクタ の間に接続が確立されます。Cisco DNA Spaces で同等の コネクタ（トークンに基づく）がアクティブになります。「Cisco DNA Spaces：コネクタ のアクティブ化 （72 ページ）」を参照してください
4. Cisco DNA Spaces ダッシュボードで シスコ ワイヤレス コントローラ または Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ または Cisco Catalyst 9300/9400 シリーズ スイッチ を設定します。コネクタ から シスコ ワイヤレス コントローラ へ （83 ページ） または Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ への コネクタ の接続 （89 ページ） または Cisco Catalyst 9300/9400 シリーズ スイッチ への コネクタ の接続 （95 ページ） を参照してください。コネクタ と コントローラ またはスイッチの間の接続をテストします。



第 7 章

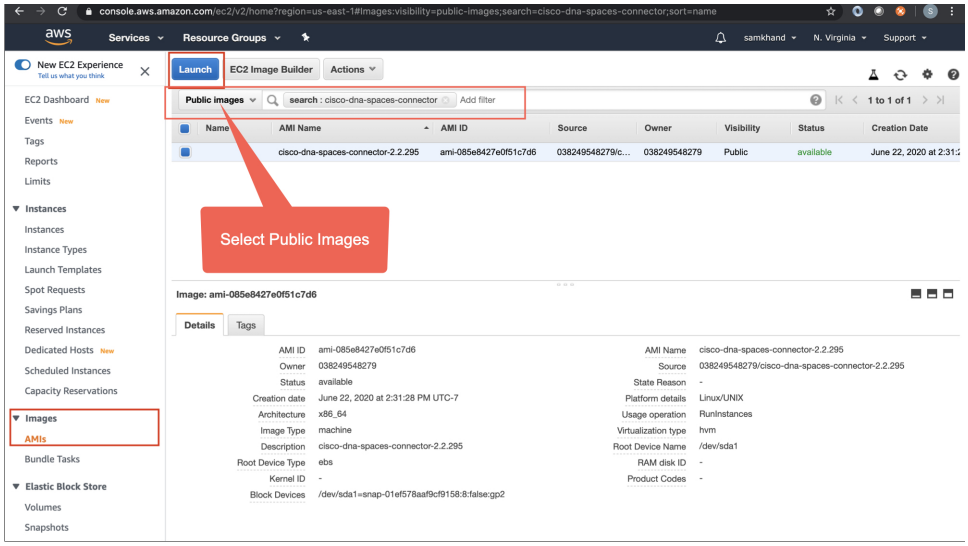
Cisco DNA Spaces：コネクタ AMI

Cisco DNA Spaces：コネクタ AMI のダウンロードと展開

この章では、Cisco DNA Spaces：コネクタ をダウンロードして展開し、コネクタ GUI の URL を取得する方法について説明します。

ステップ 1 Amazon Web Services アカウントにログインし、[EC2 Dashboard] に移動します。左側のナビゲーションペインで、[Images] > [AMI] の順に選択します。

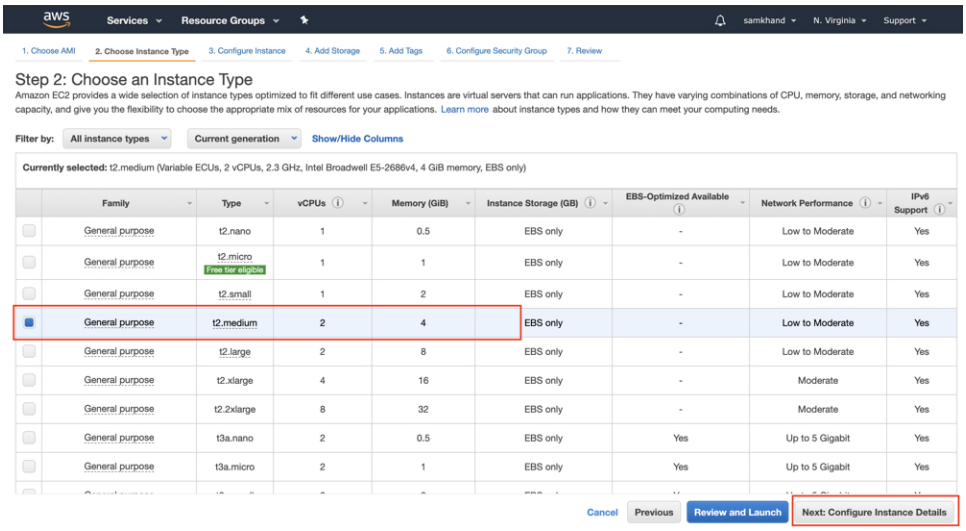
ステップ 2 検索バーで [Public Images] をクリックし、AMI ID *ami-085e8427e0f51c7d6* を検索するか、「*cisco-dna-spaces-connector*」と入力します。



ステップ 3 表示されたイメージをクリックし、[Launch] をクリックします。

ステップ 4 対応する [Type] が [t2.medium]、[vCPU] の値が [2]、[Memory (GB)] が [4] のインスタンスを選択します。

[t2.medium] は、2 vCPU と 4 GB のメモリを備えた標準の Cisco DNA Spaces：コネクタ に対応しており、推奨される設定です。次に [Next: Configure Instance Details] をクリックします。

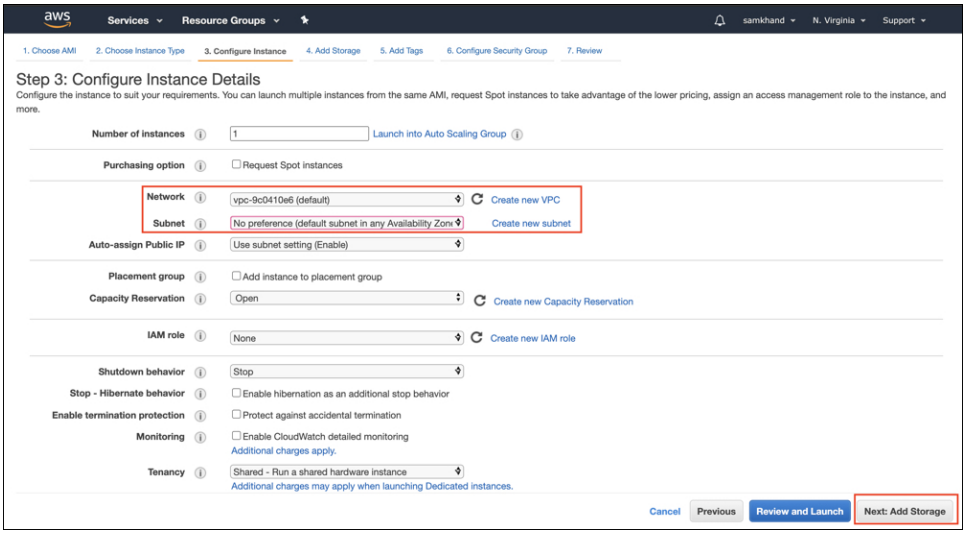


（注） より高性能な vCPU およびメモリ構成のオプションを選択して、さらに高度な構成を選択することも可能です。次の構成のインスタンスタイプを選択できます。完全一致が使用できない場合は、次に使用可能な vCPU またはメモリの構成を選択できます。

- 4 vCPU および 8 GB メモリ（このドキュメントでの呼称は Advanced1）
- 8 vCPU および 16 GB メモリ（このドキュメントでの呼称は Advanced2）

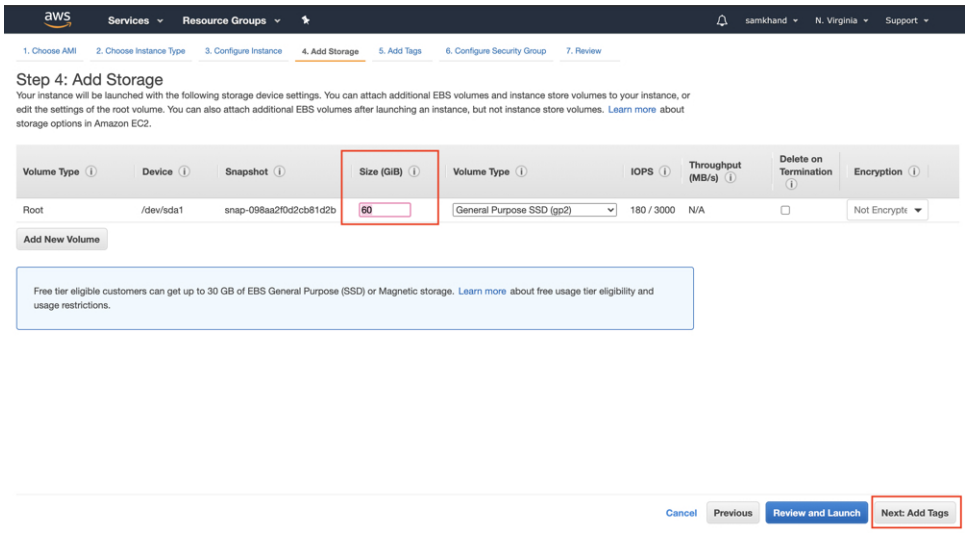
ステップ 5 [Network] と [Subnet] を選択します。[Next: Add Storage] をクリックします。

図 *1*：インスタンスの詳細設定



ステップ 6 [Size (GB)] の値に「60」と入力します。[Next: Add Tags] をクリックします。

図 *2*：ストレージの追加



ステップ 7 [click to add a Name tag] をクリックします。名前を入力してから、[Next: Configure Security Group] をクリックします。

図 *3*：タグの追加

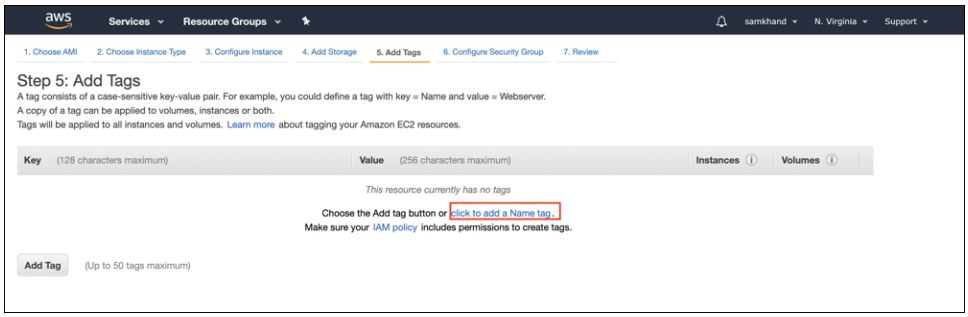
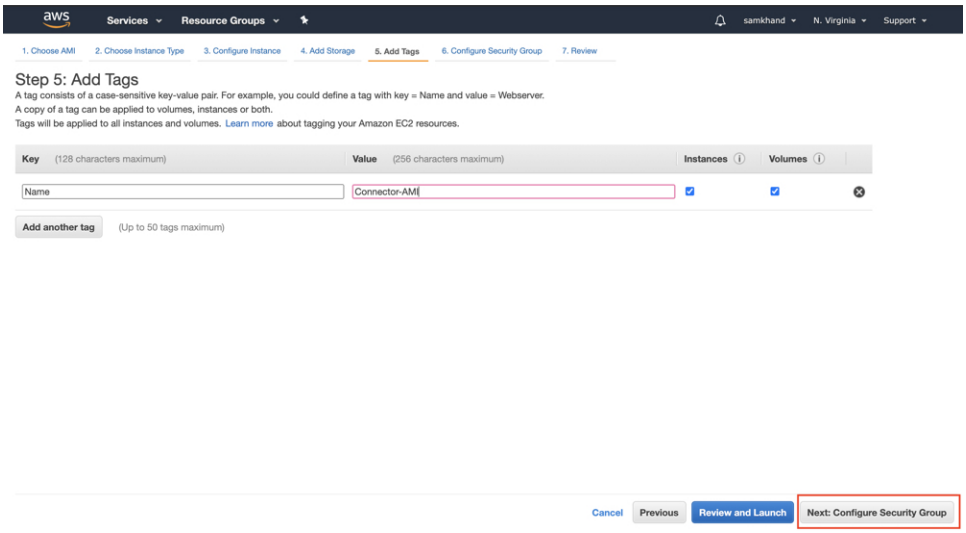


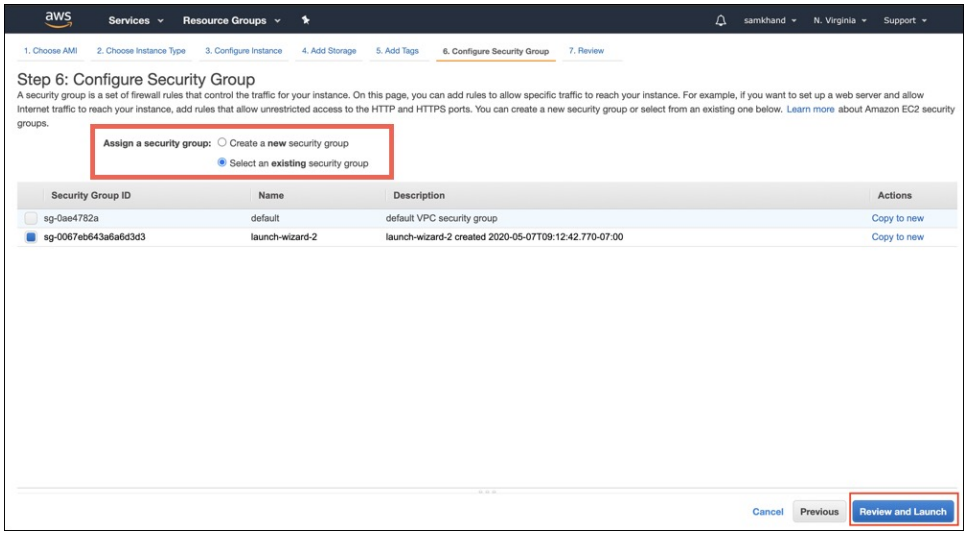
図 *4*：タグ名の入力



ステップ 8　次の手順に従って、セキュリティグループを設定します。

a) 該当するオプションボタンをクリックして、新しいセキュリティグループを作成するか、既存のセキュリティグループを変更します。

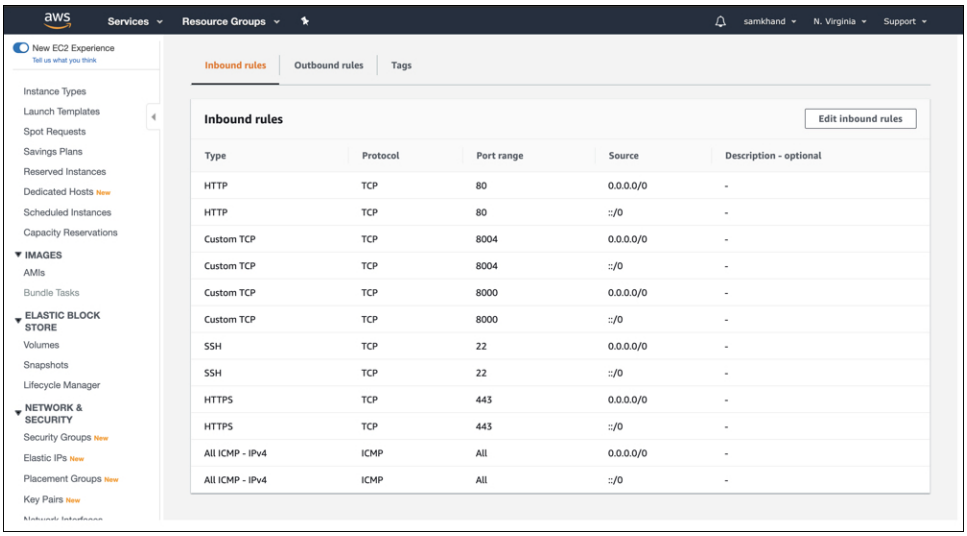
図 *5*：セキュリティグループの設定



b) インバウンドトラフィックのルールを使用してポートを設定します。特定の IP アドレスに対して制限するか、あるいはすべての IP アドレスに対して開いたままにするかを選択できます。

インバウンドトラフィックのルールを使用して、イメージに表示される特定のポートを設定します。

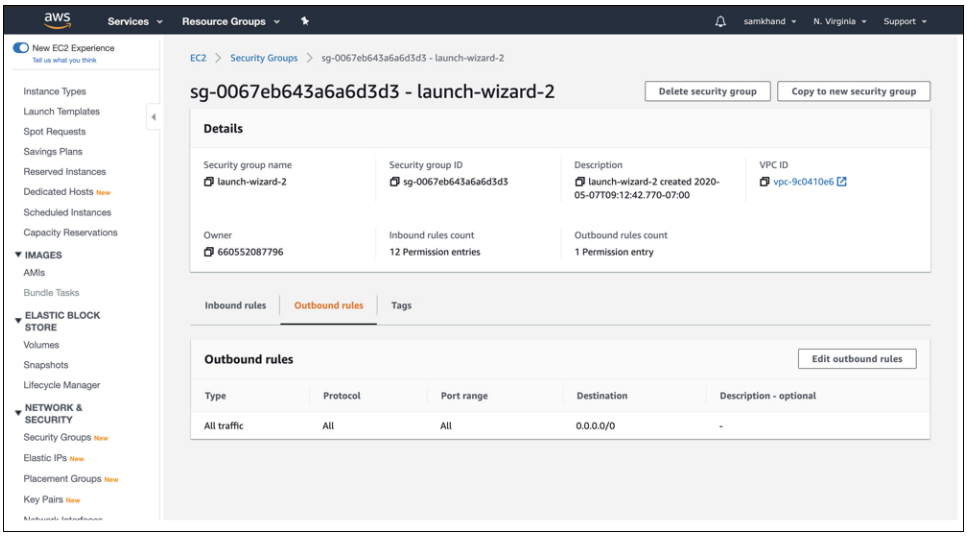
図 *6*：インバウンドトラフィックのルールによるポートの設定



c) アウトバウンドトラフィックのルールを使用してポートを設定します。

次の図に示すアウトバウンドルールを設定します。

図 *7*：アウトバウンドトラフィックのルールを使用したポートの設定

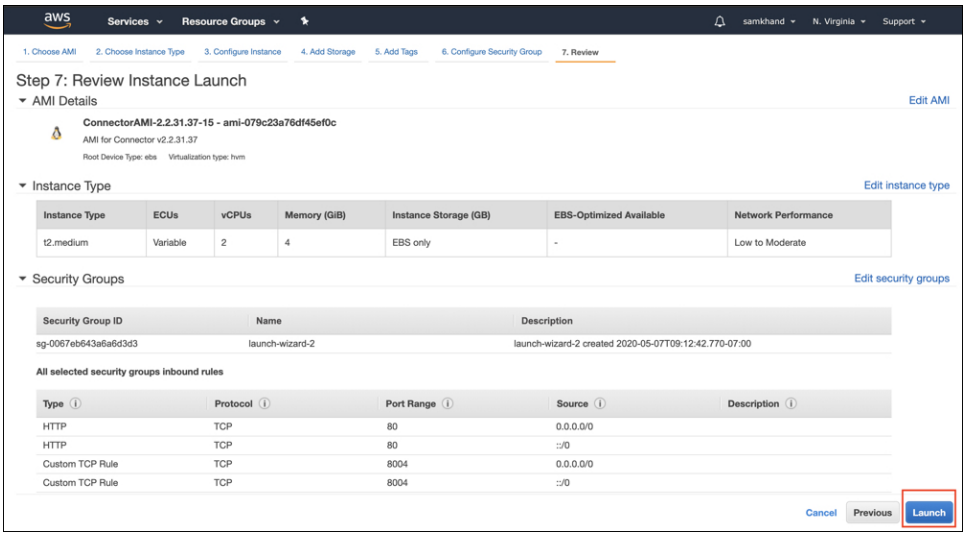


（注） さまざまなサービスを機能させるために開く必要があるポートの詳細については、オープンポートに関する情報（ワイヤレス） （13 ページ）を参照してください。

d) [Review and Launch] をクリックします。

ステップ 9 インスタンスを確認して、[Launch] をクリックします。

図 *8*：インスタンスの確認と起動



ステップ 10 表示される [Select an existing key pair or create a new key pair] ダイアログボックスで、次のいずれかを実行できます。

- ドロップダウンリストから [Create a new key pair] を選択します。[Key pair name] を入力し、[Download Key Pair] をクリックしてダウンロードします。[Launch Instance] をクリックしてインスタンスを起動します。
- ドロップダウンリストから [Choose an existing key pair] を選択します。[Select a key Pair] ドロップダウンリストから、以前にダウンロードしたキーペアを選択します。[Launch Instance] をクリックしてインスタンスを起動します。

図 *9*：新しいキーペアの作成

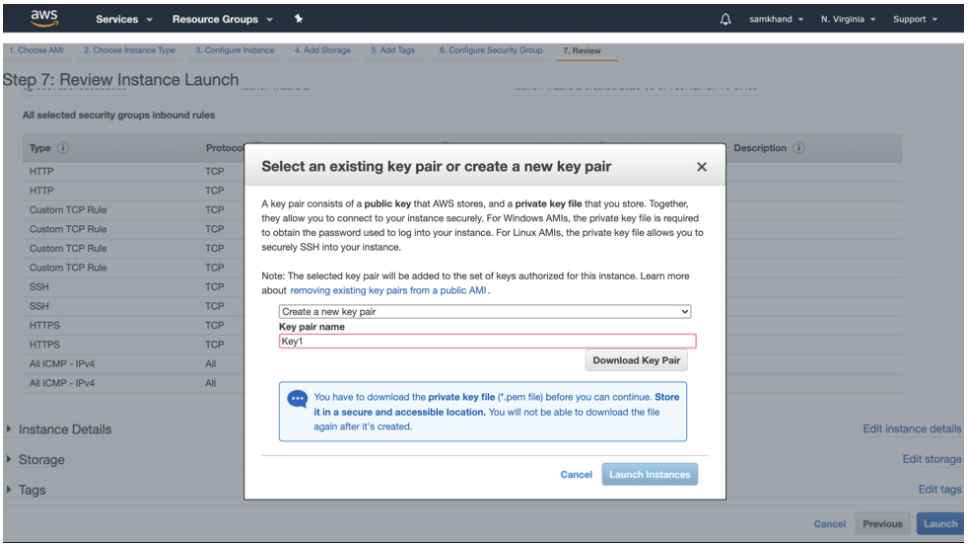
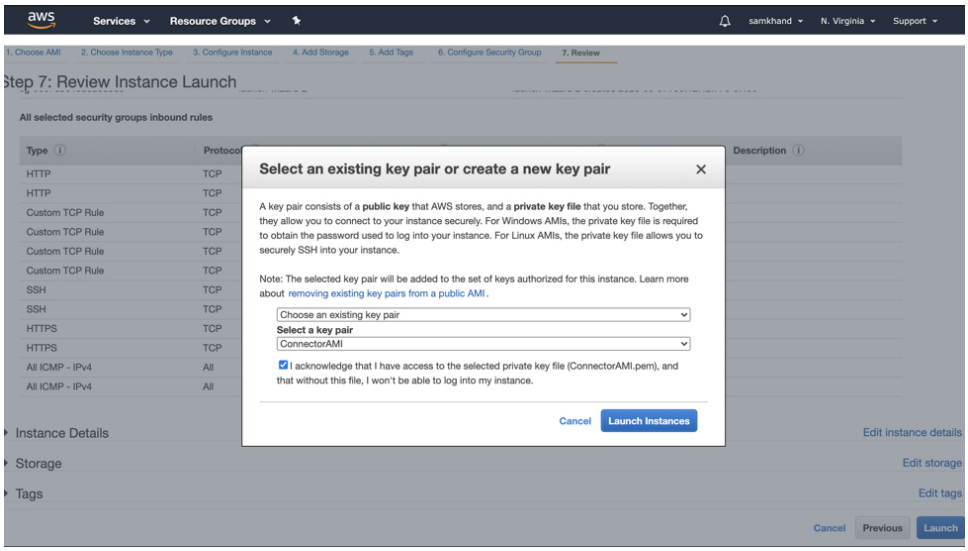
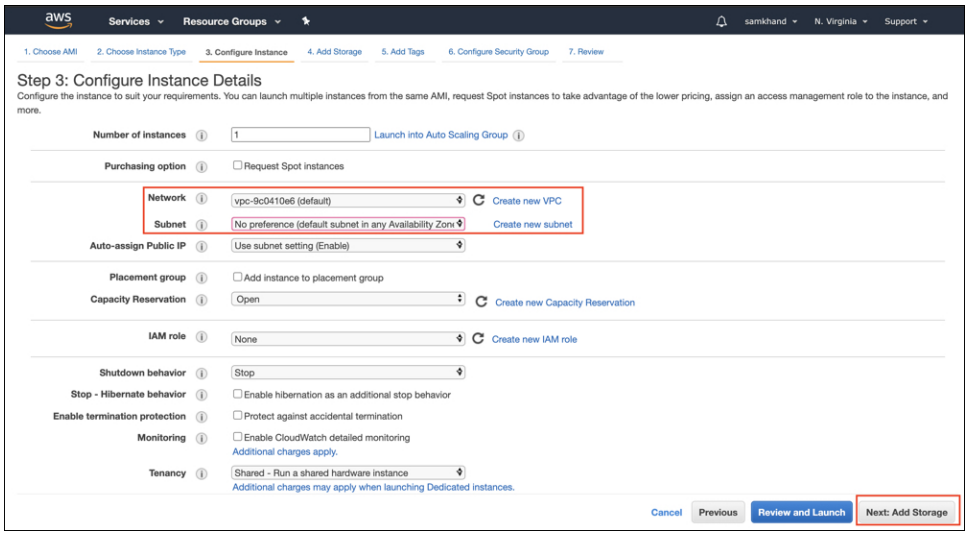


図 *10*：既存のキーペアの選択



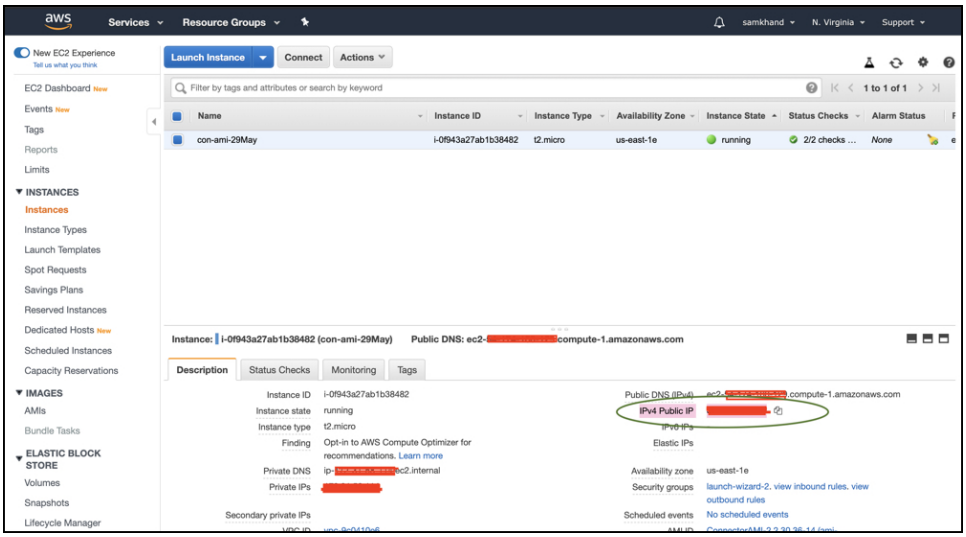


ステップ 11 キーペア（.pem）ファイルをシステムにダウンロードしたら、ファイルの場所に移動します。**chmod** コマンドを使用して、.pem ファイルに対する適切な権限を設定します。

```
chmod 400 /path/to/MyAccessKey1.pem
```

ステップ 12 EC2 ダッシュボードで、インスタンスの起動が完了し、ステータスが [Running] に変わるまで待ちます。または、[Instances] ページで実行中のインスタンスを確認できます。インスタンスをクリックして、CLI の起動に使用する IPv4 アドレスを取得します。取得した時点で設定を完了できます。

図 *11 : [Instances]* ページと *IPv4* アドレス



ステップ 13 初期設定を実行してホスト名を設定し、**dnasadmin** ユーザと **root** ユーザのパスワードを変更します。

a) **SSH** コマンド、**手順 12** で取得した IPv4 アドレス、および**手順 10** でダウンロードしたキーペアを使用して、コネクタ にログインします。

```
ssh -i /path/to/key/MyAccessKey1.pem dnasadmin@IPv4 address
```

b) **root** ユーザと **dnasadmin** ユーザのユーザ名とパスワードを変更します。最初のログインユーザ名 **dnasadmin** とログインパスワード **dnasadmin123!** を使用します。

次のパスワード要件に従うことで、「不適切なパスワード」プロンプトを回避できます。

- パスワードは 14 文字を超える長さにする必要があります。
- パスワードには少なくとも 1 つの大文字を含める必要があります。
- パスワードには少なくとも 1 つの小文字を含める必要があります。
- パスワードには少なくとも 1 つの特殊文字を含める必要があります。

次に、SSH コマンドの出力例を示します。

```
ssh -i /path/to/key/MyAccessKey1.pem dnasadmin@10.1.1.1
Password:
WELCOME to DNA SPACES CONNECTOR SETUP
Please enter hostname: my-connector-ami
Change passwords for root and dnasadmin
Changing password for user root.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
passwd: all authentication tokens updated successfully.
Changing password for user dnasadmin.
New password:
BAD PASSWORD: The password is shorter than 14 characters
Retype new password:
passwd: all authentication tokens updated successfully.
Generating self-signed certificates ...
Setup is complete
```

```
System will reboot in 10 seconds ...
Connection to 10.1.1.1 closed by remote host.
Connection to 10.1.1.1 closed.
```

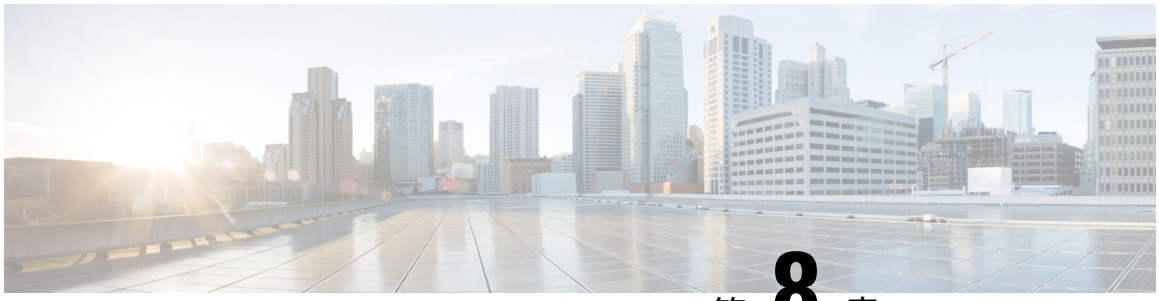
ステップ 14 ブラウザウィンドウとアドレス https://*IPv4* アドレスを使用して Cisco DNA Spaces：コネクタ GUI にログインします。

ステップ 15 SSH ユーザ名 **dnasadmin** と**手順 13** で設定したこのユーザのパスワードを使用して、Cisco DNA Spaces：コネクタ CLI にログインします。

```
ssh dnasadmin@10.1.1.1
```

次のタスク

Cisco DNA Spaces からの コネクタ のトークンの取得（ワイヤレス）



第 8 章

Cisco DNA Spaces：コネクタ OVA

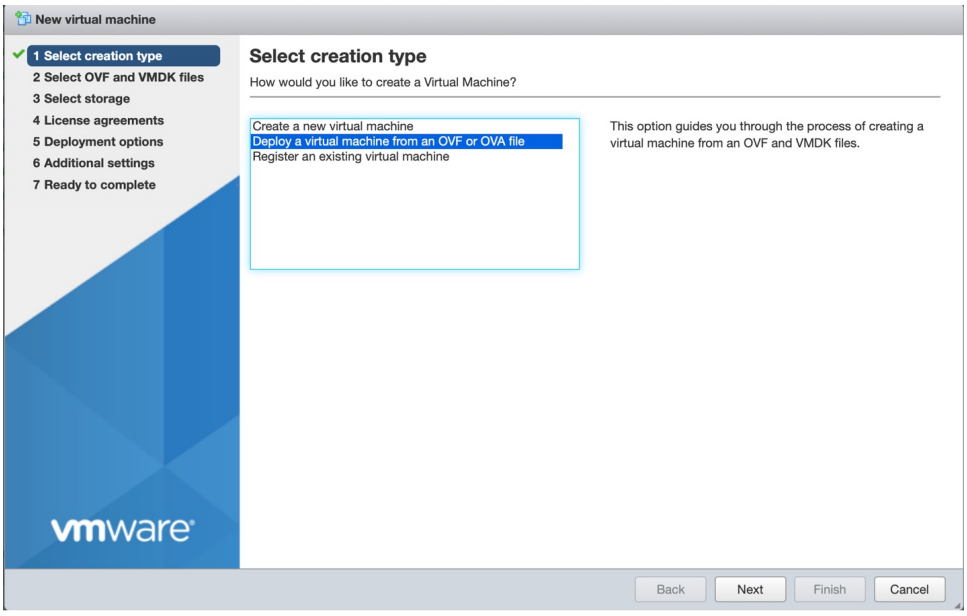
Cisco DNA Spaces：コネクタ OVA のダウンロードと展開（単一インターフェイス）

この章では、Cisco DNA Spaces：コネクタ をダウンロードして展開し、コネクタ GUI の URL を取得する方法について説明します。

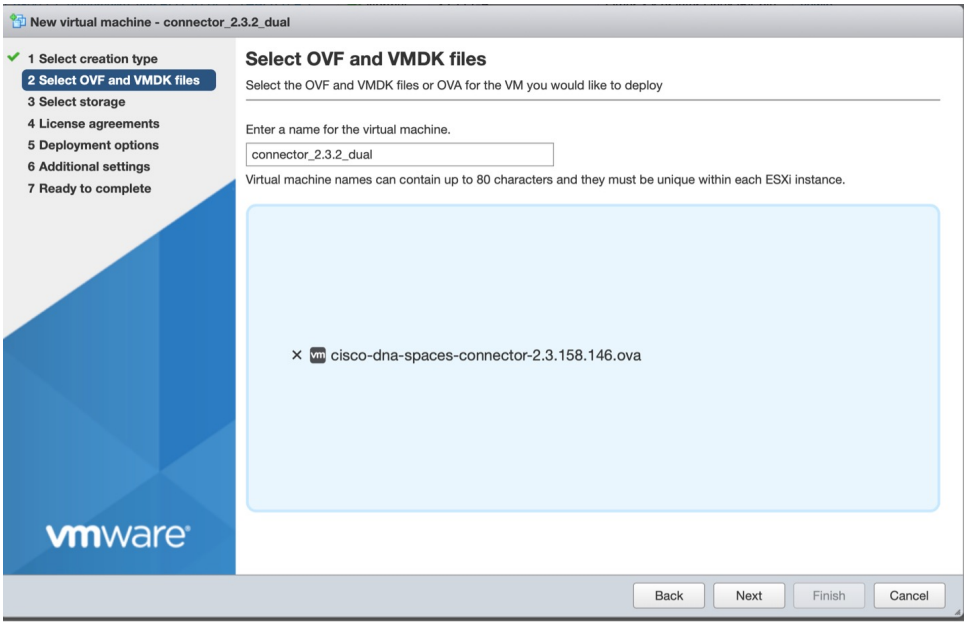
ステップ 1 Cisco.com から コネクタ 2.3 をダウンロードします。

ステップ 2 ESXi サーバで仮想マシンを作成し、ダウンロードした Cisco DNA Spaces：コネクタ OVA を展開します。

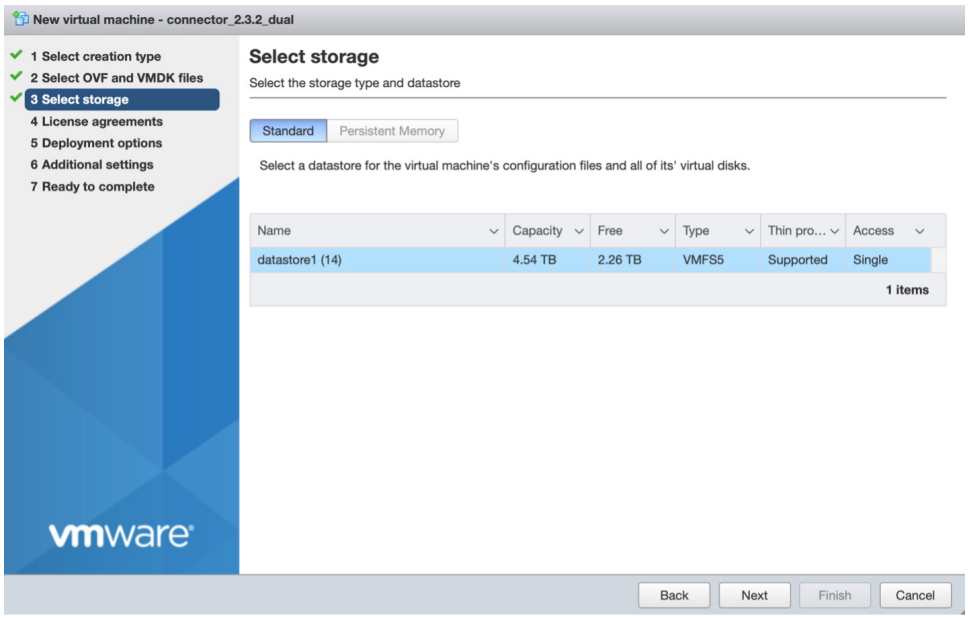
ステップ 3 [Select creation type] ウィンドウで、[Deploy a virtual machine from an OVF or OVA] ファイルを選択し、[Next] をクリックします。



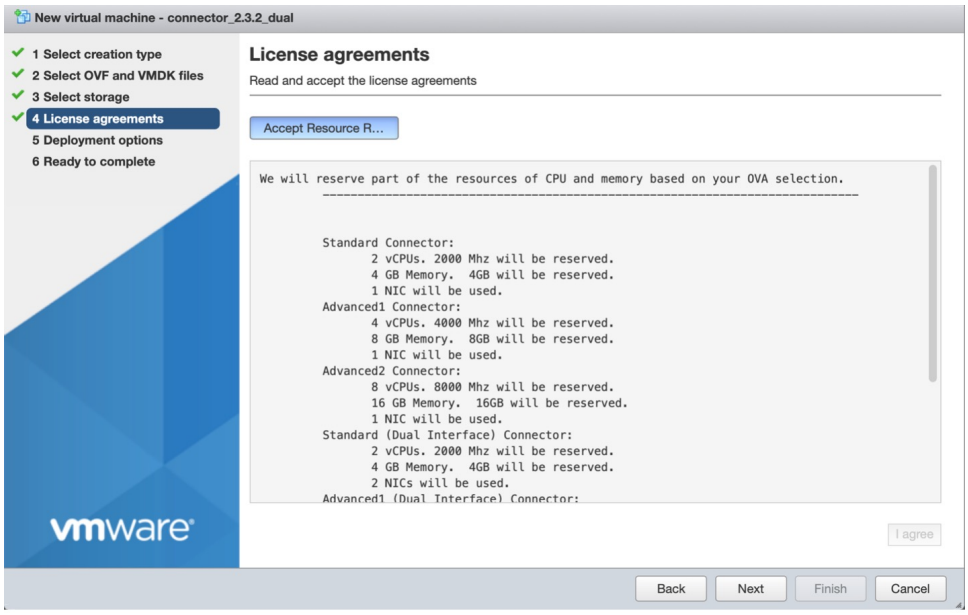
ステップ 4 [Select OVF and VMDK files] ウィンドウで、仮想マシンの名前を入力します。青色のエリアをクリックして、コンピュータからファイルを選択するか、ファイルをドラッグアンドドロップします。[Next] をクリックします。



ステップ 5 [Select storage] ウィンドウに、[Standard] ストレージ設定が表示されます。[Next] をクリックします。



ステップ 6 [License agreements] ウィンドウで、表示されるライセンス契約を読み、最後までスクロールします。[I Agree] をクリックしてから、[Next] をクリックします。



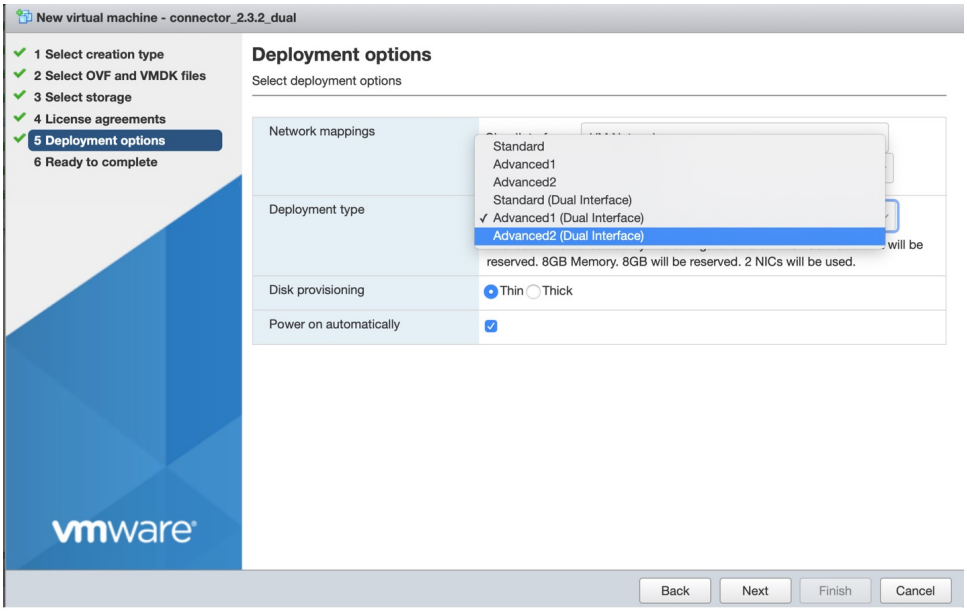
ステップ 7 [Deployment Options] ウィンドウで、次の手順を実行します。

a) [Network-mapping] フィールドに、ネットワークの名前を入力します。

b) [Deployment type] ドロップダウンリストから、次のいずれかのオプションを選択して、[Next] をクリックします。

- **規格**
- **Advanced1**

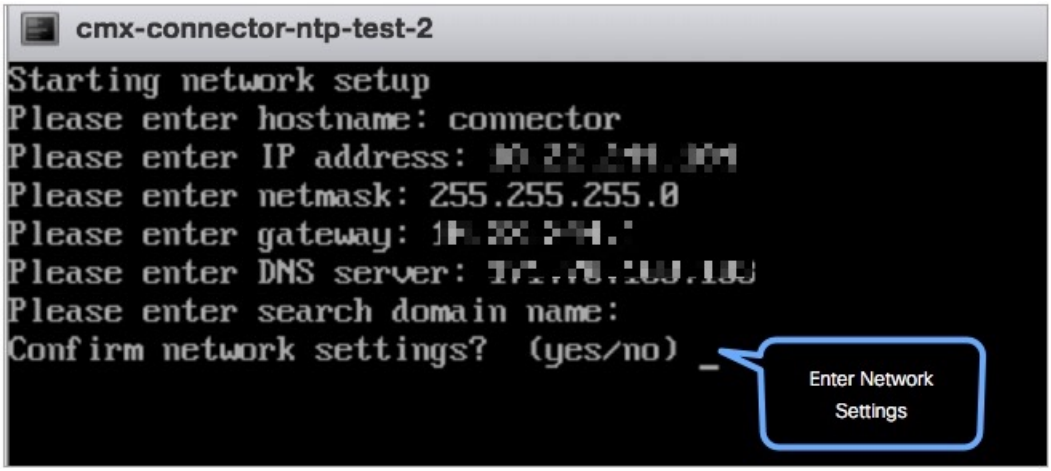
- **Advanced2**



ステップ 8 ネットワーク設定を確認し、[Finish] をクリックします。

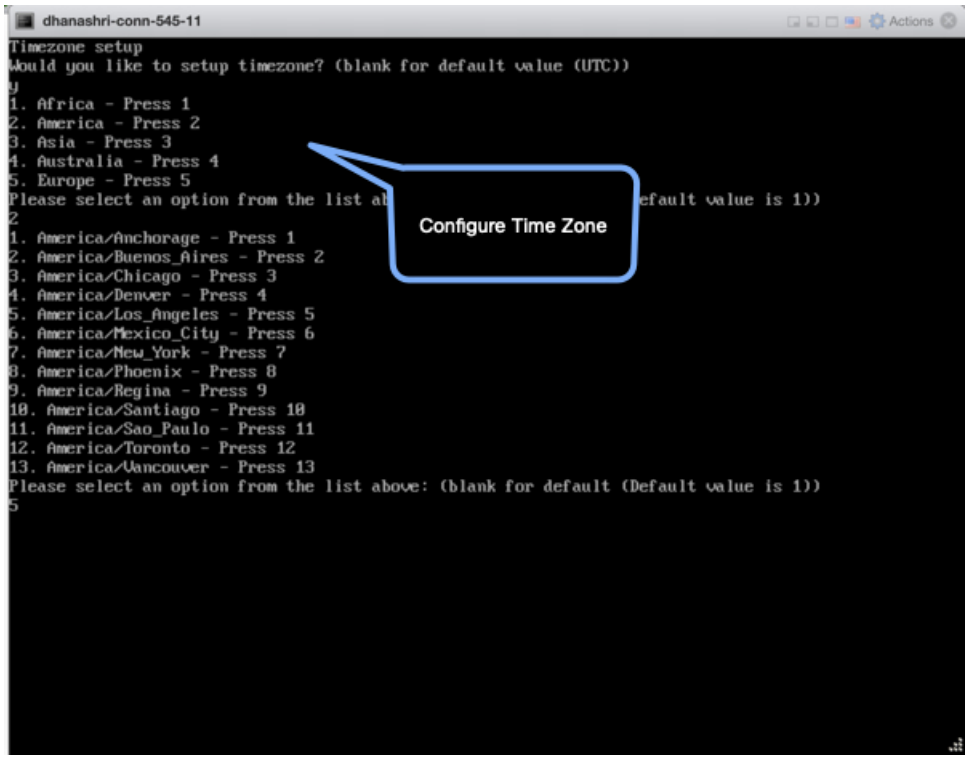
ステップ 9 端末にログインし、デフォルトのユーザ名「**root**」とデフォルトのパスワード「**cisco**」を入力します。

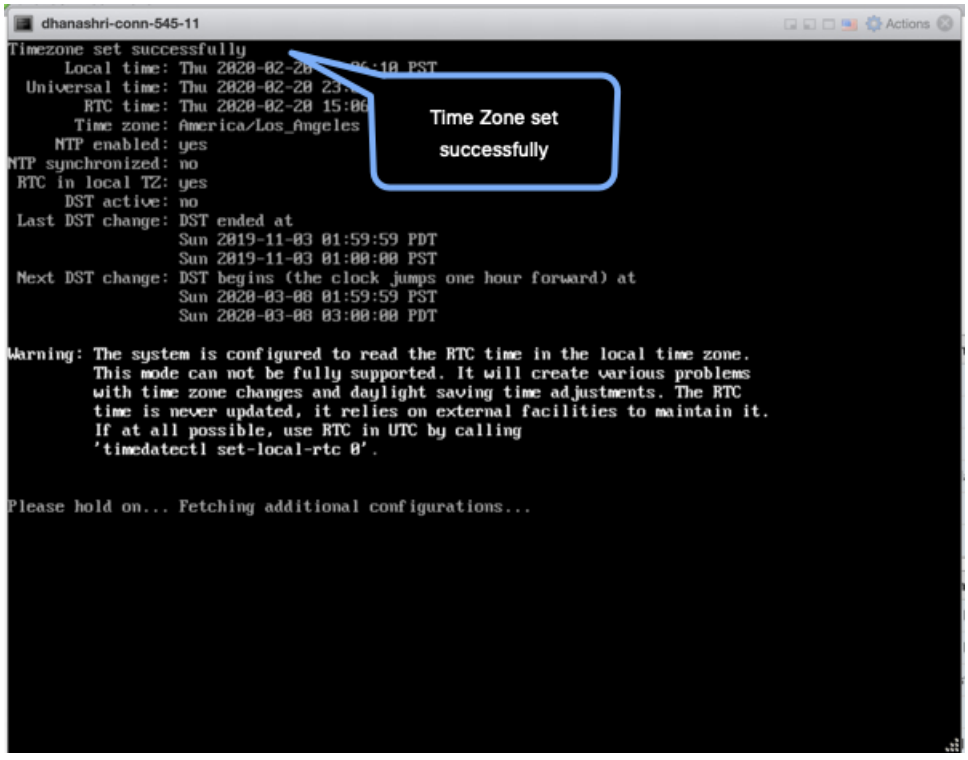
ステップ 10 Cisco DNA Spaces：コネクタ で設定する IP アドレス、ホスト名などのパラメータを指定して、ネットワーク設定を入力します。



（注） この設定画面は60秒でタイムアウトするので、再設定を避けるために時間内に入力してください。

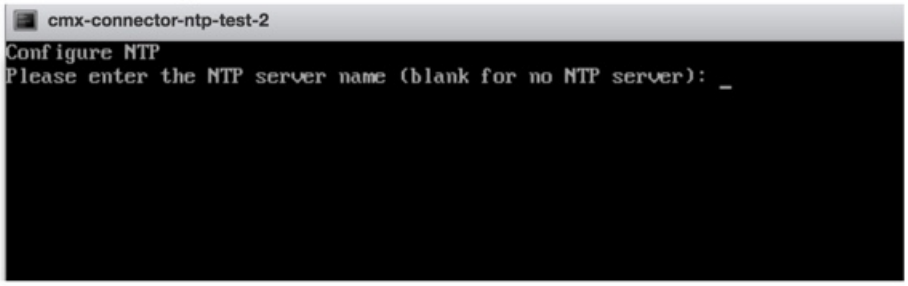
ステップ 11 タイムゾーンを入力します。



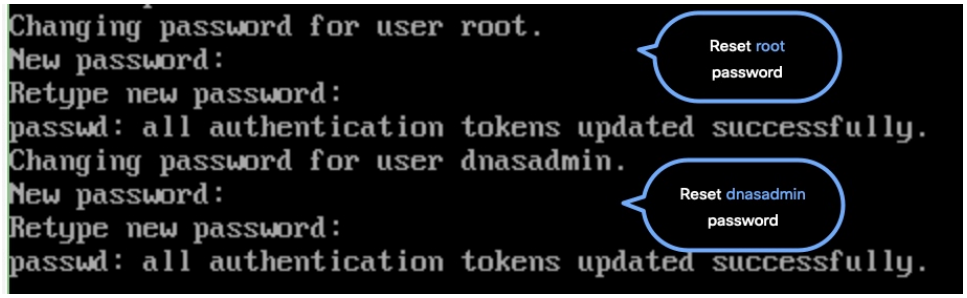


ステップ 12 Network Time Protocol（NTP）サーバ名を入力して、システム時刻を NTP サーバと同期します。NTP サーバを設定しない場合は、空白のままにします。

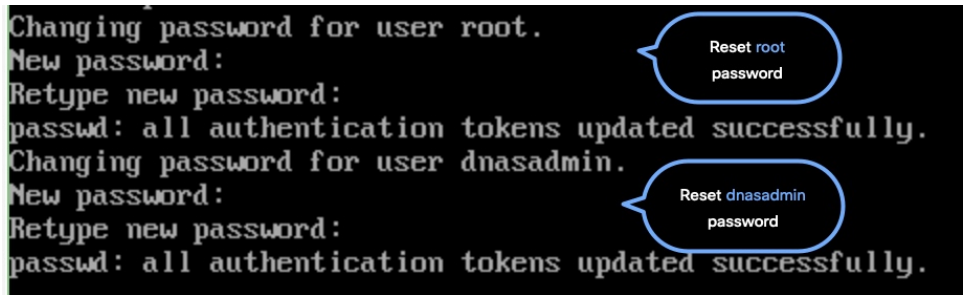
図 *12 : NTP* 設定の入力



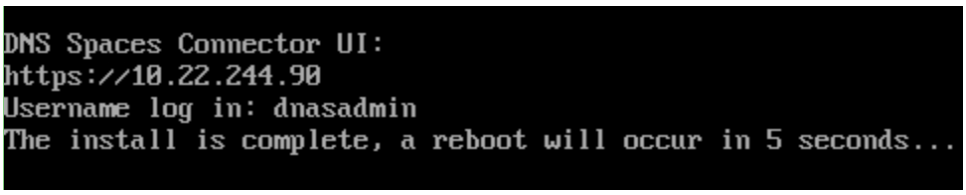
ステップ 13 **root** ユーザの新しいパスワードを設定します。



ステップ 14 管理者権限を持つユーザである **dnasadmin** ユーザの新しいパスワードを設定します。



ステップ 15 自動リブートの前に URL をコピーして保存します。後でこの URL を使用して Cisco DNA Spaces：コネクタ GUI を開くことができます。



次のタスク

Cisco DNA Spaces からの コネクタ のトークンの取得（ワイヤレス）

Cisco DNA Spaces：コネクタ OVA のダウンロードと展開（デュアルインターフェイス）

コネクタ 2.3.2 以降、コネクタ が 2 つの別々のネットワークに接続する必要があるネットワーク展開で コネクタ のデュアルインターフェイス展開を使用できます。

これらのネットワークの 1 つは、通常、ほとんどのデバイスが接続されているプライベートネットワークです。もう一方のネットワークは外部向けであるため、クラウドホスト型の Cisco DNA Spaces に接続できます。

この展開は、コネクタによって管理されるほとんどのデバイスがプライベートネットワークまたは内部ネットワーク上にある場合に推奨されます。

（注） コントローラ をプライベートネットワークに接続することをお勧めします。この設定によって、コネクタ が SSH 接続を使用して コントローラ に接続できるようになるためです。

始める前に

オープン仮想アプライアンス（OVA） をインストールする Cisco Unified Computing System（Cisco UCS） デバイスが 2 つの別個のネットワークに接続されていることを確認します。このネットワーク構成では、Cisco UCS デバイスに 2 つの物理ネットワーク インターフェイス カード（NIC）が設定されています。各 NIC はスイッチに接続されます。このようにして、Cisco UCS デバイスは 2 つのネットワークに接続されます。

図 *13 : 2* つの物理インターフェイス

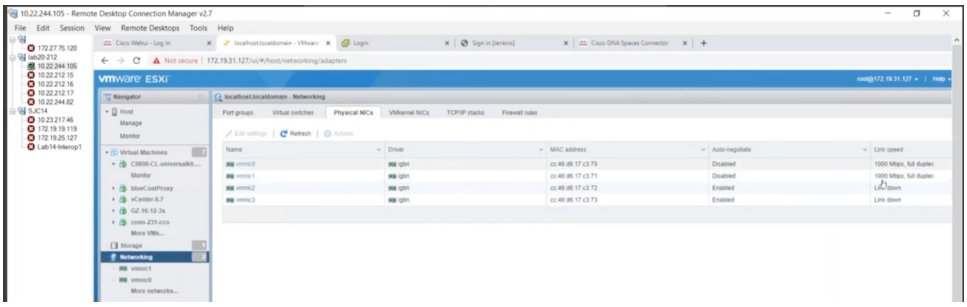
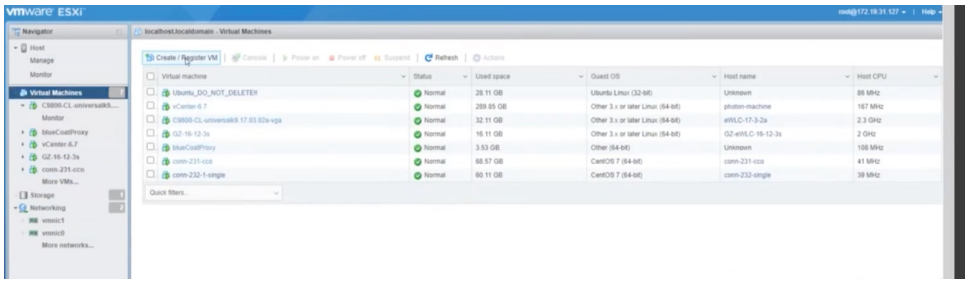


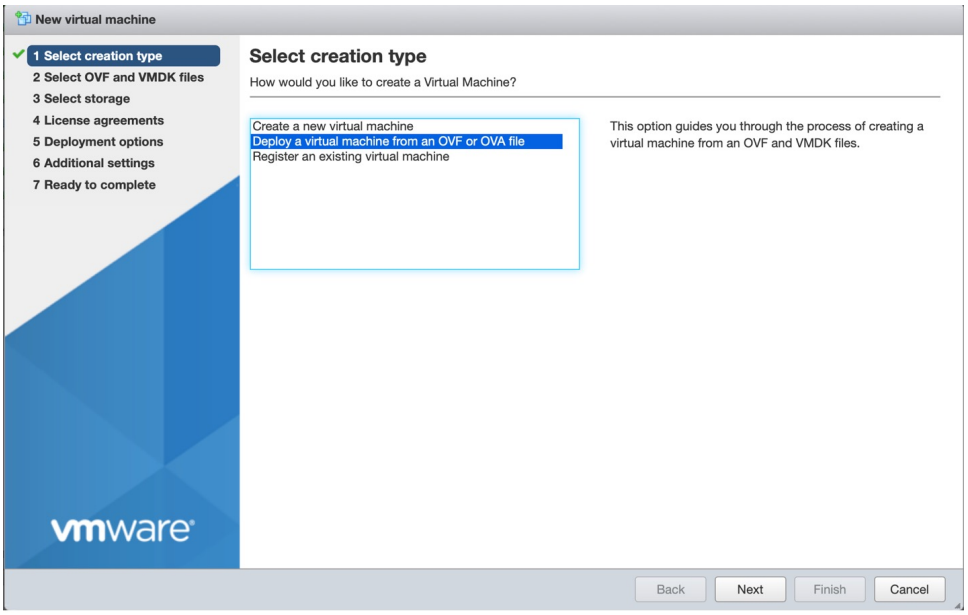
図 *14 : 2* つの別個のネットワーク



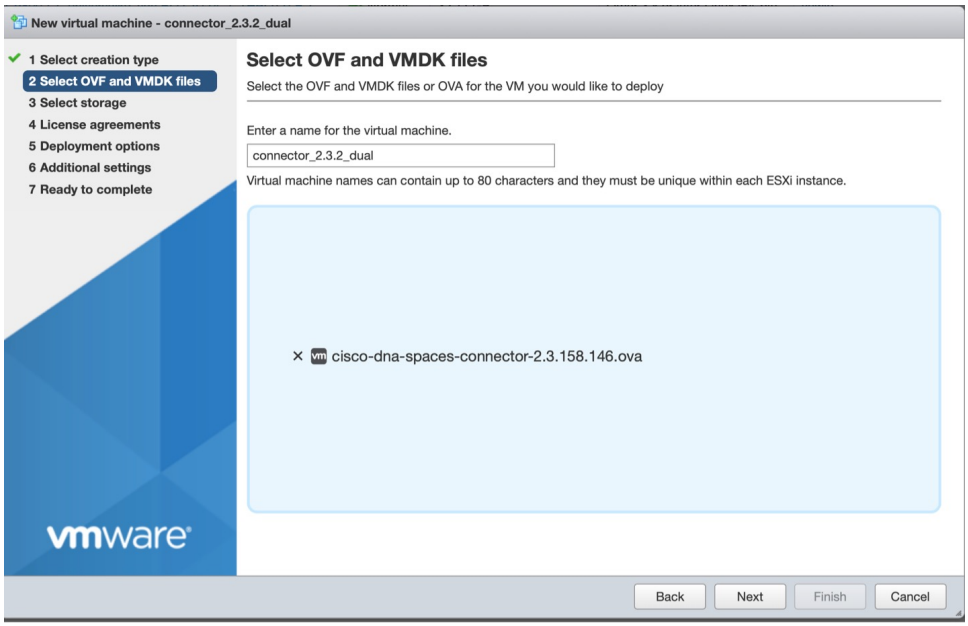
ステップ 1 Cisco.com から コネクタ 2.3 をダウンロードします。

ステップ 2 ESXi サーバで仮想マシンを作成し、ダウンロードした Cisco DNA Spaces：コネクタ OVA を展開します。

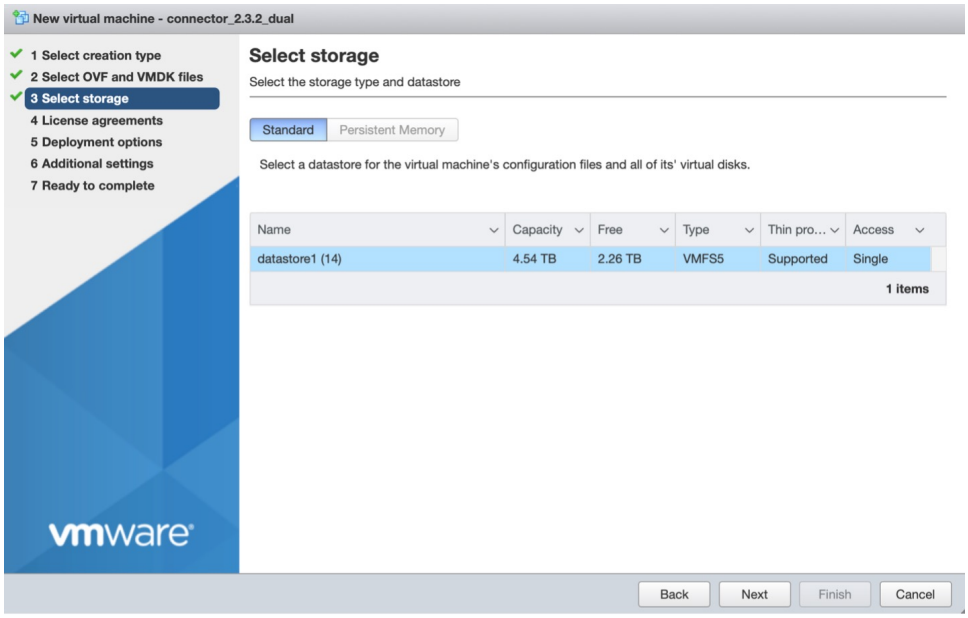
ステップ 3 [Select creation type] ウィンドウで、[Deploy a virtual machine from an OVF or OVA] ファイルを選択し、[Next] をクリックします。



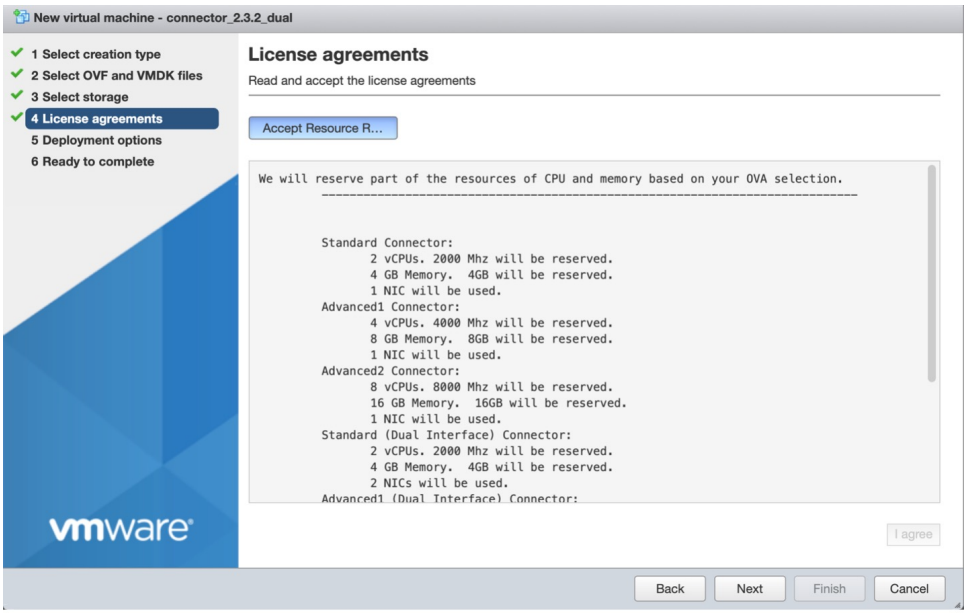
ステップ 4 [Select OVF and VMDK files] ウィンドウで、仮想マシンの名前を入力します。青色のエリアをクリックして、コンピュータからファイルを選択するか、ファイルをドラッグアンドドロップします。[Next] をクリックします。



ステップ 5 [Select storage] ウィンドウに、[Standard] ストレージ設定が表示されます。[Next] をクリックします。



ステップ 6 [License agreements] ウィンドウで、表示されるライセンス契約を読み、最後までスクロールします。[I Agree] をクリックしてから、[Next] をクリックします。



ステップ 7 [Deployment options] ウィンドウで、次の手順を実行します。

a) [CloudInterface] フィールドに、外部向けネットワークの名前を入力します。

b) [CloudInterface] フィールドに、プライベートネットワークの名前を入力します。

c) [Deployment type] ドロップダウンリストから、次のいずれかの展開タイプを選択して、[Next] をクリックします。

- [Standard (Dual Interface)]
- [Advanced1 (Dual Interface)]
- [Advanced2 (Dual Interface)]

図 *15*：外部向けネットワークとプライベートネットワークの名前の入力

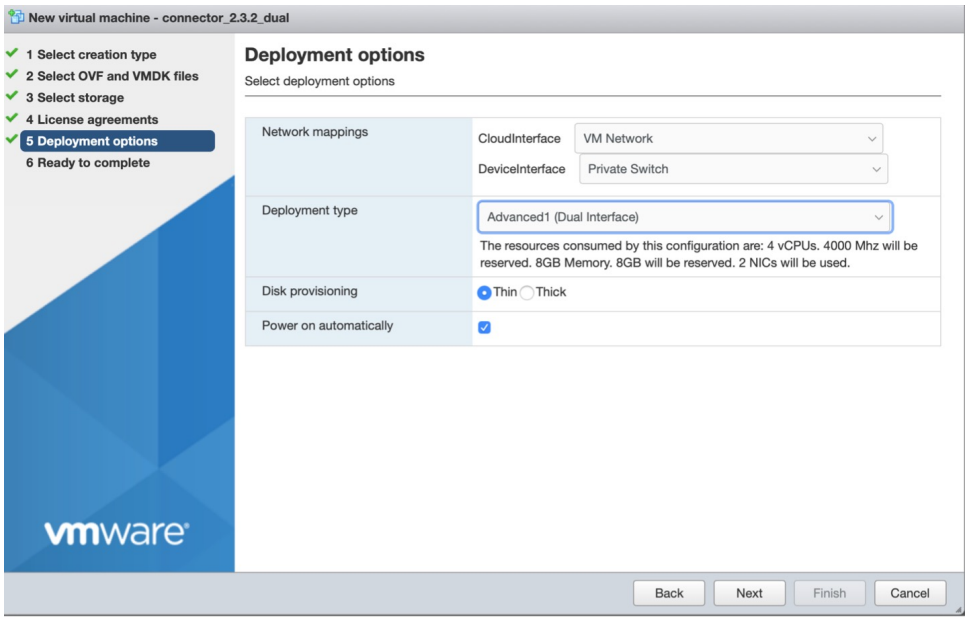
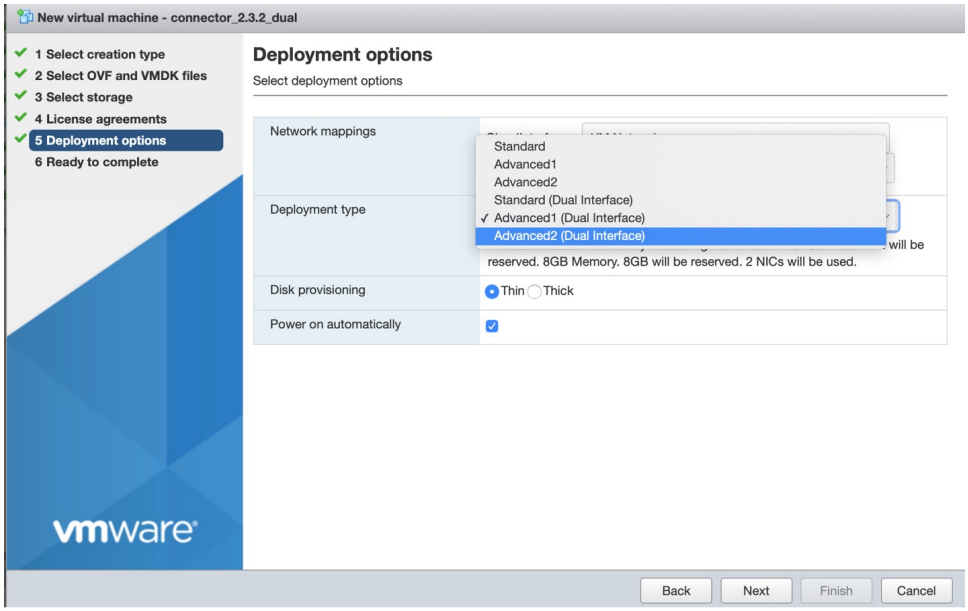


図 *16*：展開タイプの選択

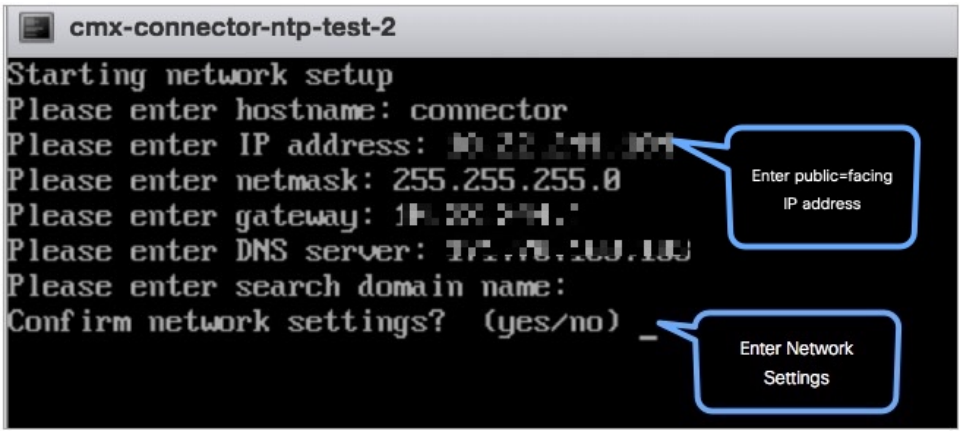


ステップ 8 ネットワーク設定を確認し、[Finish] をクリックします。

ステップ 9 端末にログインし、デフォルトのユーザ名「**root**」とデフォルトのパスワード「**cisco**」を入力します。

ステップ 10 IP アドレス、ホスト名などのパラメータを指定して、外部向けネットワークのネットワーク設定を最初に設定します。

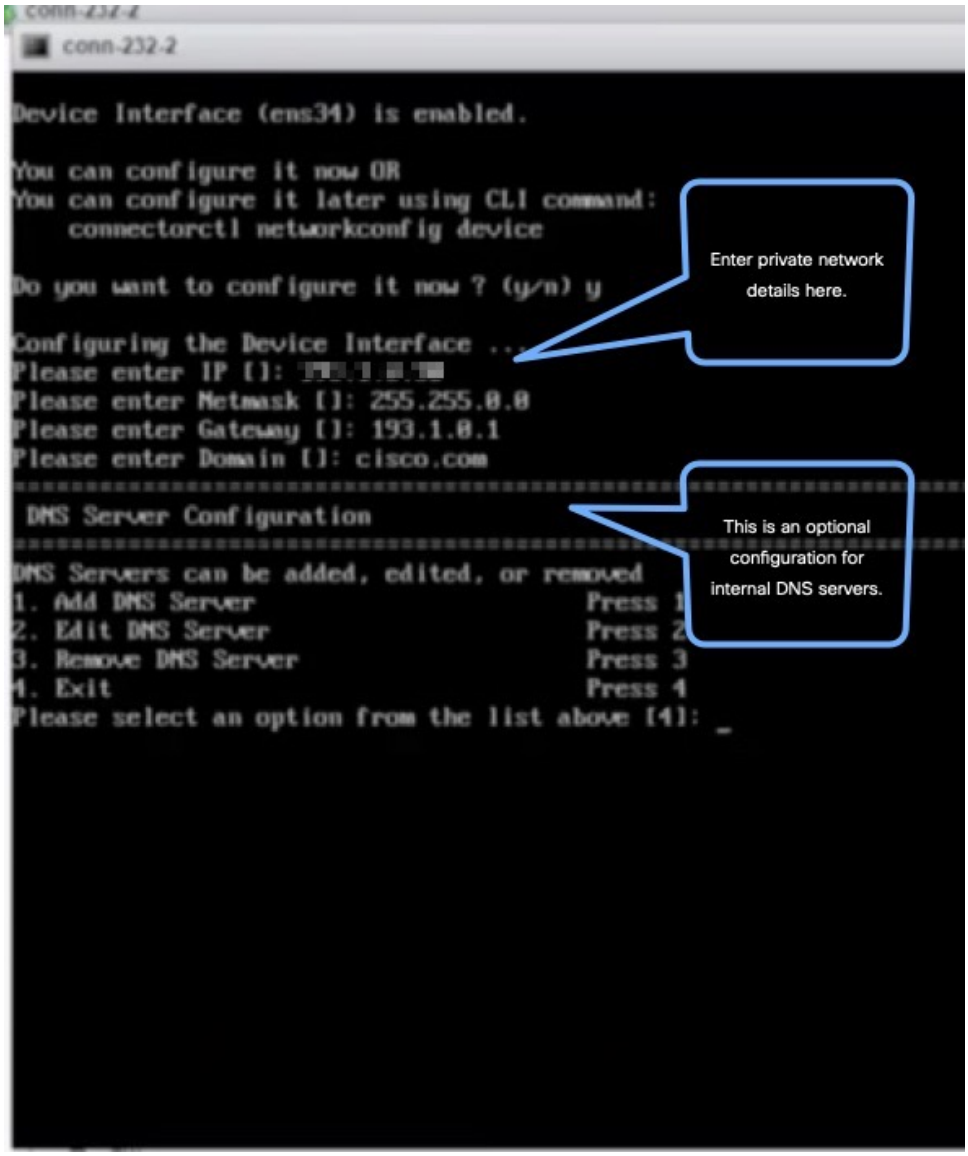
図 *17 :* 外部向けネットワークのネットワーク設定の入力



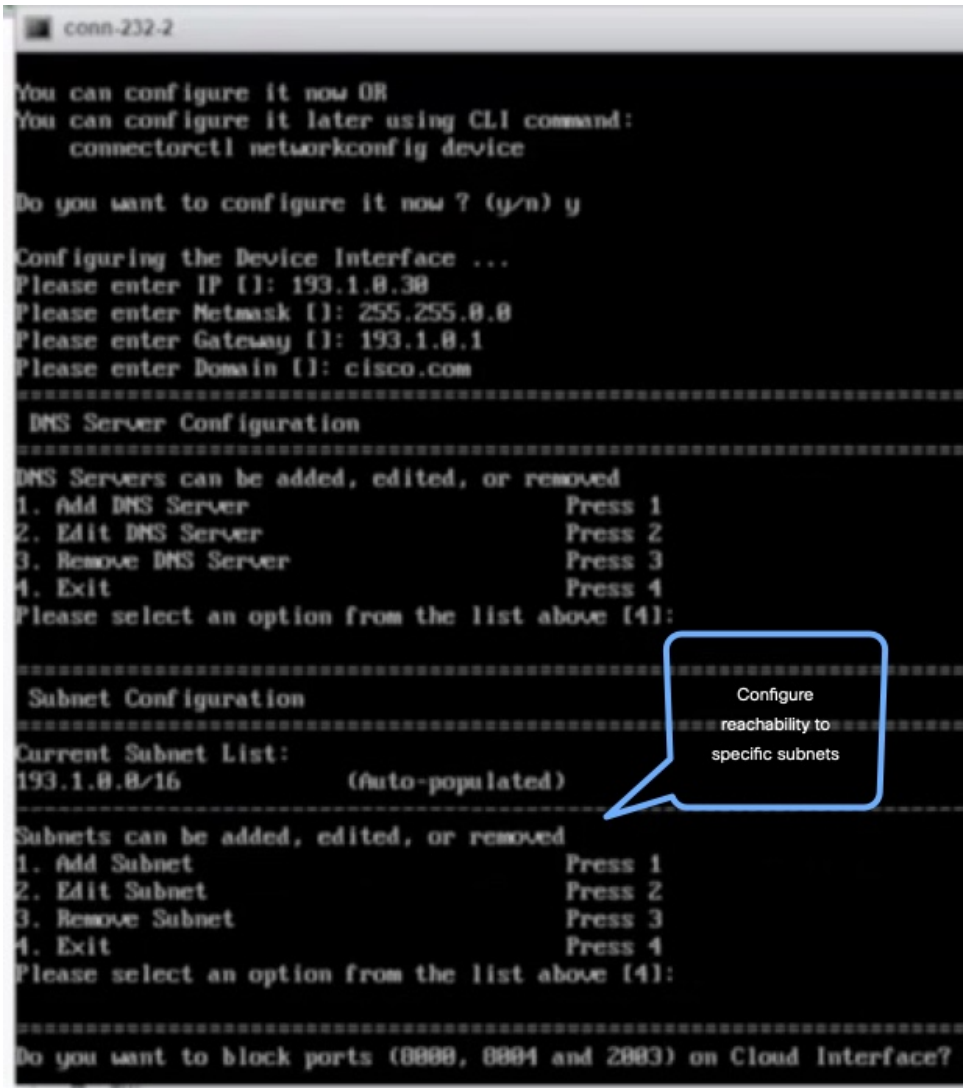
（注） この設定画面は60秒でタイムアウトするので、再設定を避けるために時間内に入力してください。

ステップ 11 IP アドレス、ホスト名などのパラメータを指定して、プライベートネットワークのネットワーク設定を実行します。

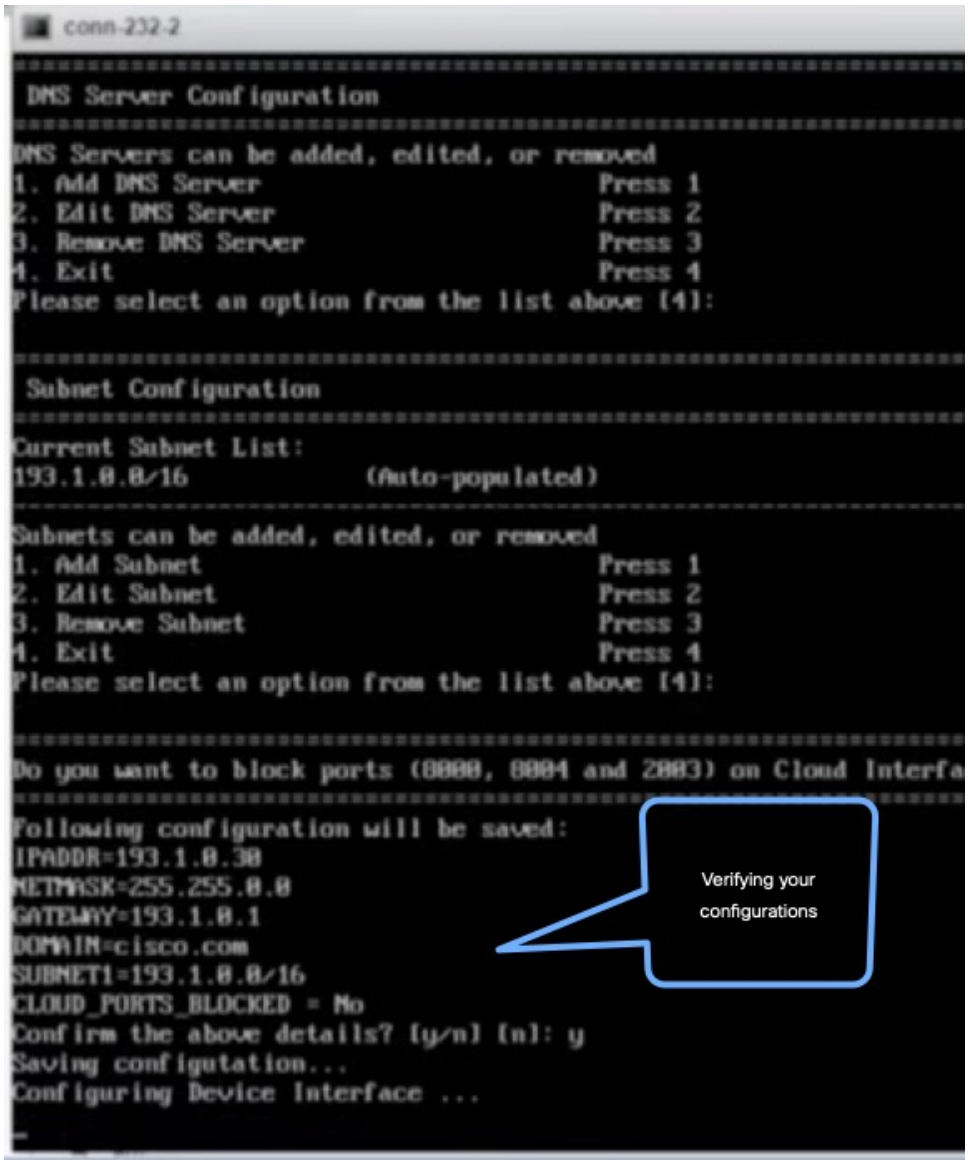
図 *18 :* プライベートネットワークのネットワーク設定の入力



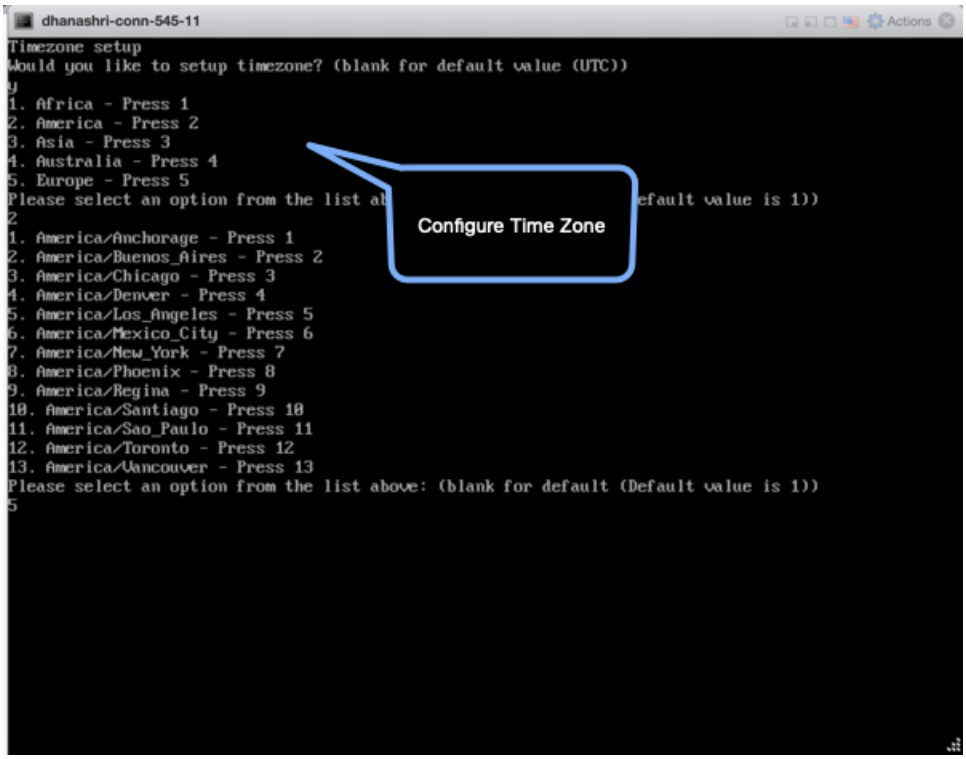
ステップ 12 コネクタ が到達可能なサブネットを設定します。

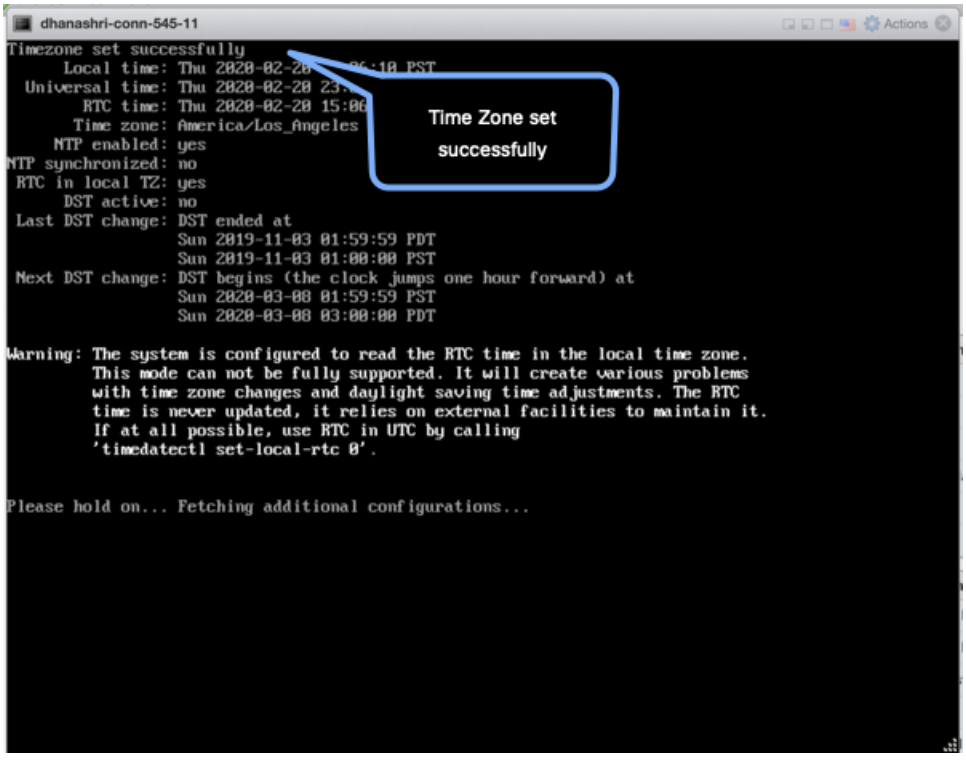


設定とネットワークの到達可能性が検証済みであることを確認できます。



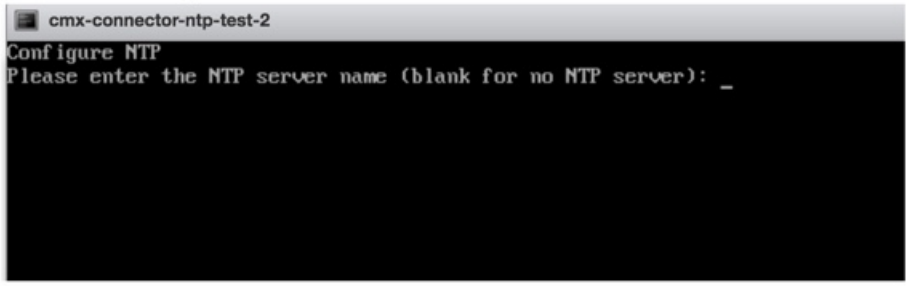
ステップ 13　タイムゾーンを入力します。



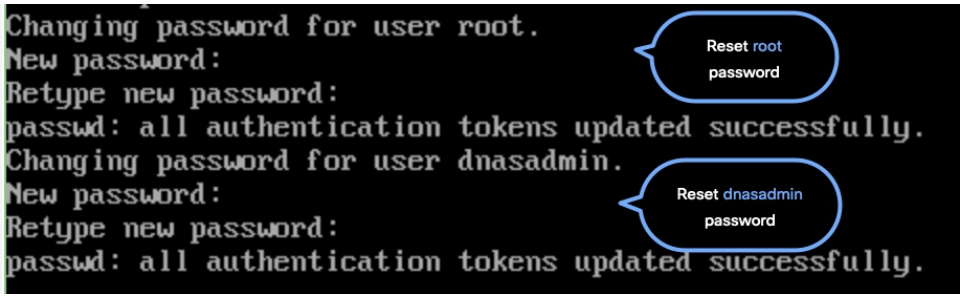


ステップ 14 Network Time Protocol（NTP）サーバ名を入力して、システム時刻を NTP サーバと同期します。NTP サーバを設定しない場合は、空白のままにします。

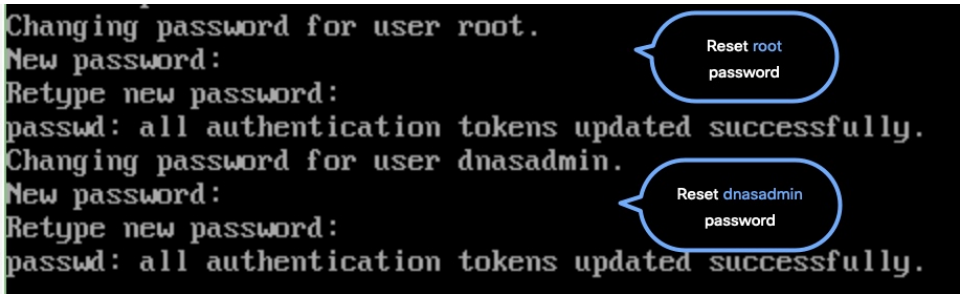
図 *19 : NTP* 設定の入力



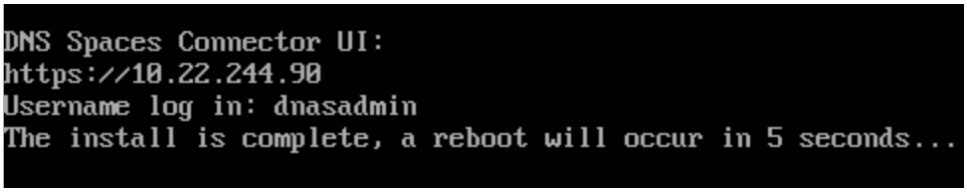
ステップ 15 **root** ユーザの新しいパスワードを設定します。



ステップ 16 管理者権限を持つユーザである **dnasadmin** ユーザの新しいパスワードを設定します。

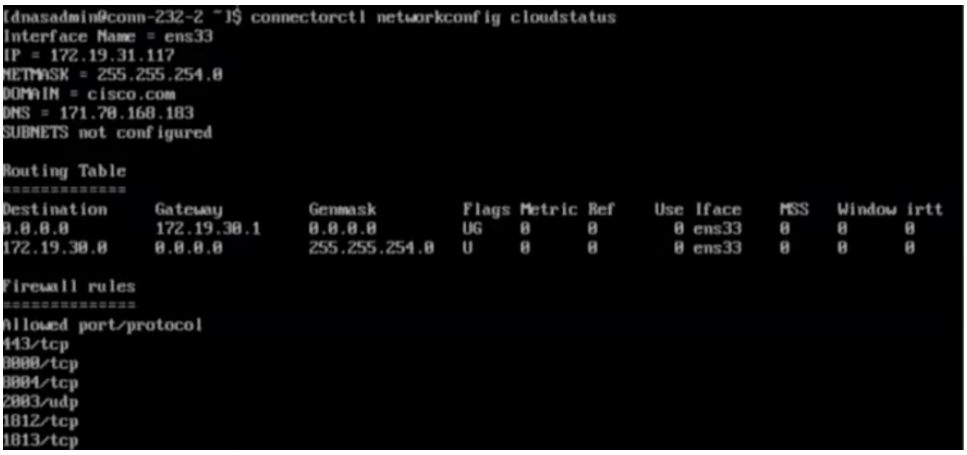


ステップ 17 自動リブートの前に URL をコピーして保存します。後でこの URL を使用して Cisco DNA Spaces：コネクタ GUI を開くことができます。



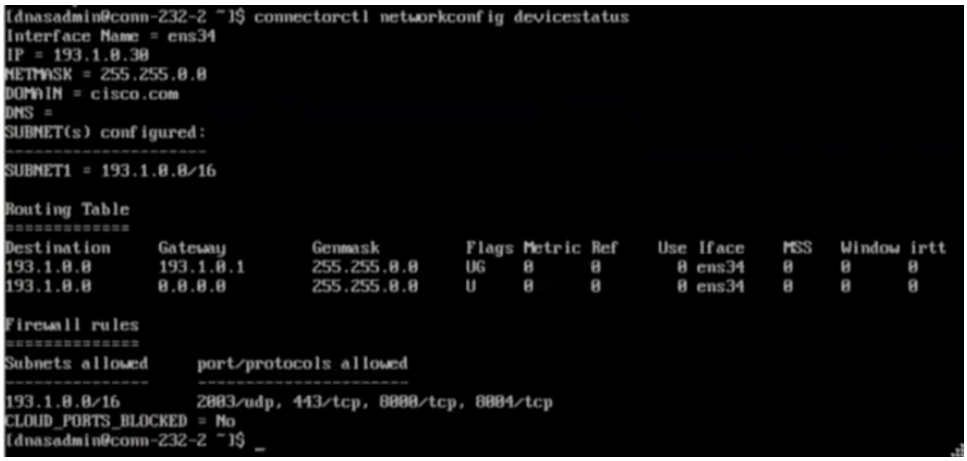
ステップ 18 **connectorctl networkconfig cloudstatus** コマンドを使用して、外部向けネットワークのネットワーク設定を確認します。

図 *20 :* プライベートネットワークのネットワーク設定の入力



ステップ 19 **connectorctl networkconfig devicestatus** コマンドを使用して、プライベートネットワークのネットワーク設定を確認します。

図 *21 :* プライベートネットワークのネットワーク設定の入力



次のタスク

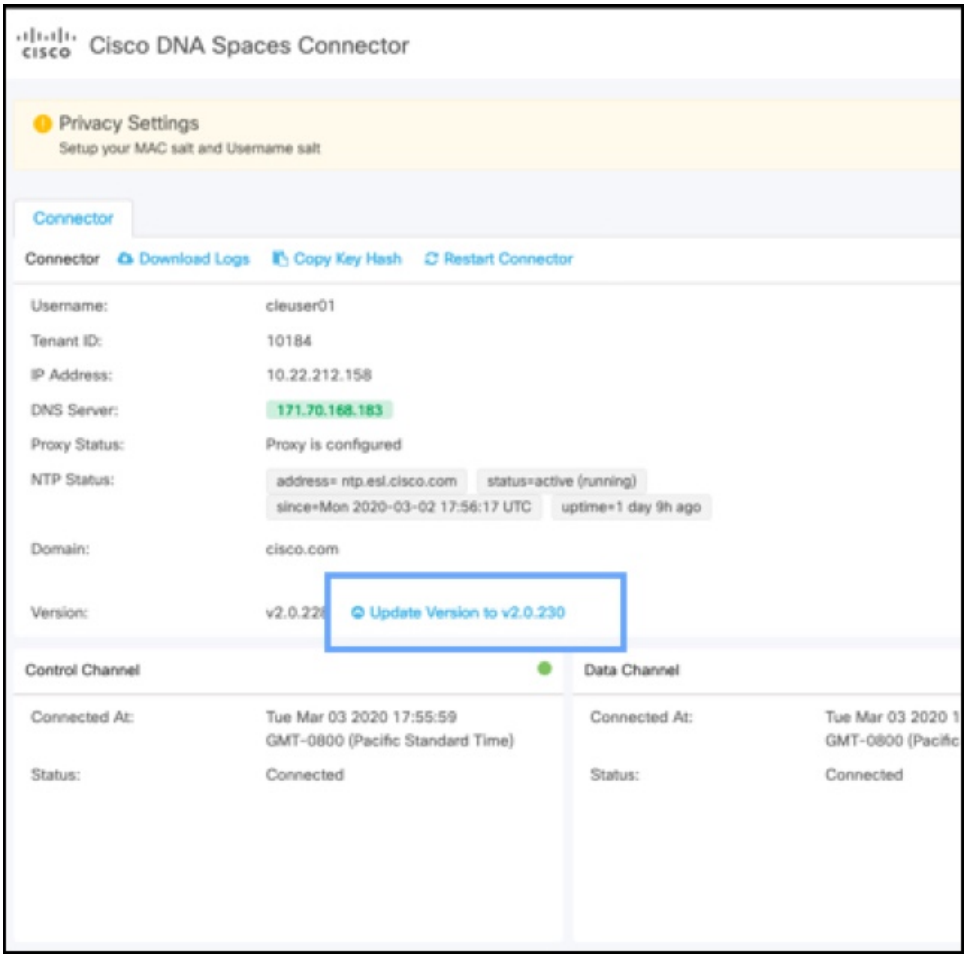
Cisco DNA Spaces からの コネクタ のトークンの取得（ワイヤレス）

Cisco DNA Spaces：コネクタ Docker のアップグレード

コネクタ GUI から コネクタ Docker を最新バージョンにアップグレードできます。アップグレードリンクは、新しいアップグレードイメージが使用可能な場合にのみ表示されることにご注意ください。

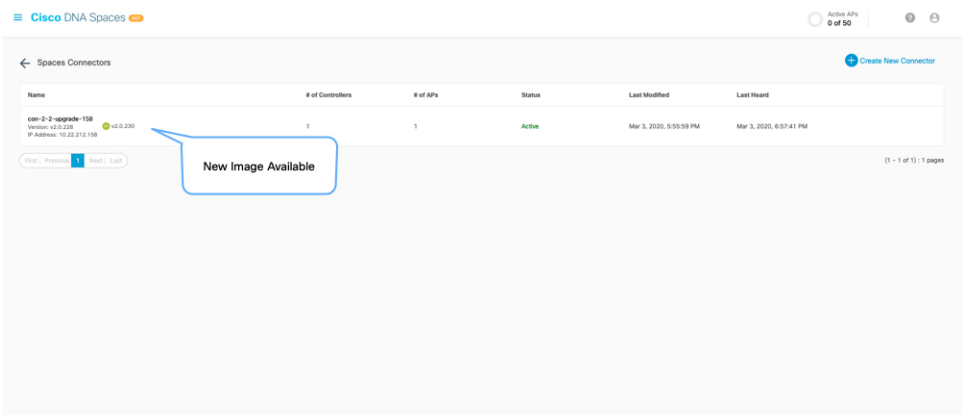
（注） この手順では、コネクタ OVA はアップグレードされません。

図 *22 :* コネクタ 上の *Docker* アップグレードリンク



Cisco DNA Spaces ダッシュボードから コネクタ Docker を最新バージョンにアップグレードすることもできます。アップグレードリンクは、新しいアップグレードイメージが使用可能な場合にのみ表示されます。

図 *23 : Docker* アップグレードリンクは、新しいイメージが使用可能な場合にのみ表示される



アップグレードパス

次の表は HTML 形式で表示するのが最適です。

表 *3 :* アップグレードパス

リリース番号	リリース名	このリリースへのアップグレード	推奨事項
リリース 2.3.2	cisco-dna-spaces-connector-2.3.495.connector	cisco-dna-spaces-connector-2.3.495.connector	—
	cisco-dna-spaces-connector-2.3.478.ova	cisco-dna-spaces-connector-2.3.495.ova	—
	—	cisco-dna-spaces-connector-2.3.496.vhdx	—
リリース 2.3.1	cisco-dna-spaces-connector-2.3.478.ova	cisco-dna-spaces-connector-2.3.495.ova	—
	cisco-dna-spaces-connector-2.3.478.connector	cisco-dna-spaces-connector-2.3.495.connector	OS レベルでセキュリティパッチを取得するには、OVA アップグレードが必要です。

リリース番号	リリース名	このリリースへのアップグレード	推奨事項
リリース 2.3	cisco-dna-spaces-connector-2.3.462.ova	cisco-dna-spaces-connector-2.3.478.ova	—
	cisco-dna-spaces-connector-2.2.462.connector	cisco-dna-spaces-connector-2.3.478.connector	OS レベルでセキュリティパッチを取得するには、OVA アップグレードが必要です。
リリース 2.2	cisco-dna-spaces-connector-2.2.295.connector	cisco-dna-spaces-connector-2.3.478.connector	OS レベルでセキュリティパッチを取得するには、OVA アップグレードが必要です。
	cisco-dna-spaces-connector-2.2.295.ova	cisco-dna-spaces-connector-2.3.478.ova	OS レベルでセキュリティパッチを取得するには、OVA アップグレードが必要です。
延期中のリリース 2.1.1	cisco-dna-spaces-connector-2.1.1.connector	cisco-dna-spaces-connector-2.3.478.connector	OS セキュリティ修正により、2.1.1 から 2.3 へのアップグレードが可能
	cisco-dna-spaces-connector-2.1.1.ova		
延期中のリリース 2.0	cisco-dna-spaces-connector-2.0.connector	アップグレードはサポートされていません。新しいコネクタを展開して、同じトークンを使用することはできます。	
	cisco-dna-spaces-connector-2.0.ova		
延期中のリリース 1.0	cisco-dna-spaces-connector-1.0.188.connector		
	cisco-dna-spaces-connector1.0.188.ova		

コネクタ OVA のアップグレード

次に、Cisco DNA Spaces：コネクタ OVA のアップグレード手順を示します。

ステップ 1 Cisco.com から コネクタ 2.3 をダウンロードします。

ステップ 2 コネクタ をホストしているマシンに、ダウンロードしたファイルをコピーします。

ステップ 3 コネクタ コマンドラインにログインします。

ステップ 4 **connectorctl upgrade** <<*upgrade_file_name*>> コマンドを使用して、OVA アップグレードプロセスを開始します。

```
(cmxadminPcon-2-3-upg-87 -]S connectorctl upgrade cisco-dna-spaces-connector-2.3.494.connector
Machine will restart automatically after upgrade. Do you still want to continue? [yes / noj [yesj:
 yes
Before upgrade, OVA version:2.2.295
New image exists.
Backing up current version of the image and db ...
Preparing for upgrade ...
umount: /mnt/cmx: not mounted
mount: /dev/loop0 is write-protected, mounting read-only
Starting pip repo
Starting upgrade ...
Warning: RPMDB altered outside of yum.
Error: No matching Packages to list
0000000000000000000000000000 IMPORTANT 000000*0000000000000000000*0000a«000
We are changing username from 'cmxadmin' to 'dnasadmin*
We will be performing following tasks now.
1. Create new user 'dnasadmin'
2. You will need to set up password for 'dnasadmin'
3. We will move over all files/folders from /home/cmxadmin to /ho®e/dnasadmin
4. Delete 'cmxadnin* user.

After the reboot, REMEMBER to login using dnasadmin credentials.
0000000000000000000000000000000000000000000000000000000000000000000000000000000800


Please press ENTER to continue...
```

dnasadmin ユーザが作成されました。

ステップ 5 プロンプトが表示されたら、新しく作成された **dnasadmin** ユーザのパスワードを設定します。

```
Please press ENTER to continue...
New user dnasadmin created.
Set password for user dnasadmin
Changing password for user dnasadmin.
New password:

Retype new password:

passwd: all authentication tokens updated successfully.
Start cleanup ...
Error response from daemon: No such container:
c9408eelb68f2acdel436622c4eeddf742dcd53a2619faa30c01aadcld8bd88e
```

ステップ 6 アップグレードが完了するまで数分間待ちます。

```
Error response from daemon: No such container: c9408eelb68f2acdel436622c4eeddf742dcd53a2

Upgrade successful.
After upgrade, OVA version : 2.3.494

System will reboot in 5 seconds...
```

ステップ 7 アップグレードが完了したら、**dnasadmin** ユーザとしてコネクタにログインします。

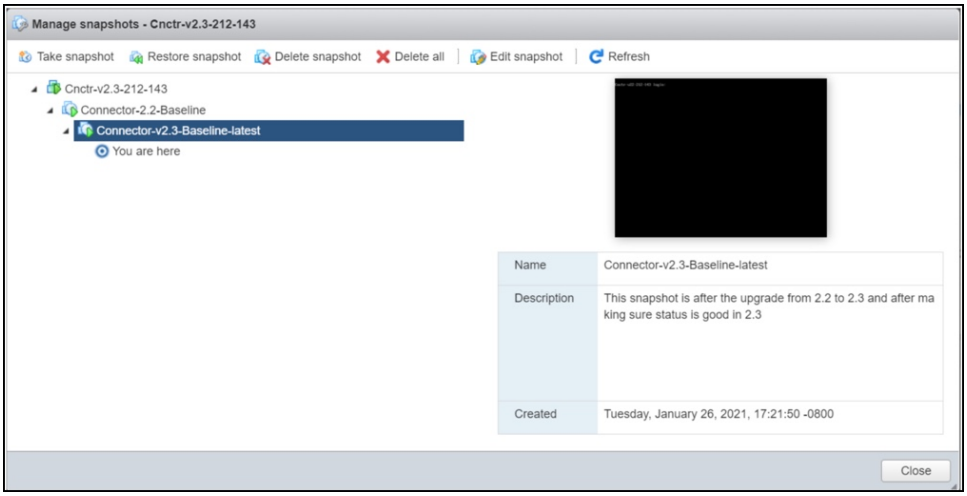
- コネクタ がアップグレード前と同じ状態で実行されていることを確認します。
- CSCvr74830 では、アップグレード中に表示される 2 つの既知のエラーを無視できます。

バックアップの代わりにスナップショットを使用

コネクタ をバックアップする代わりに、展開された Cisco DNA Spaces：コネクタ OVA のスナップショットを使用できます。次の前提条件を満たしていることを確認してください。

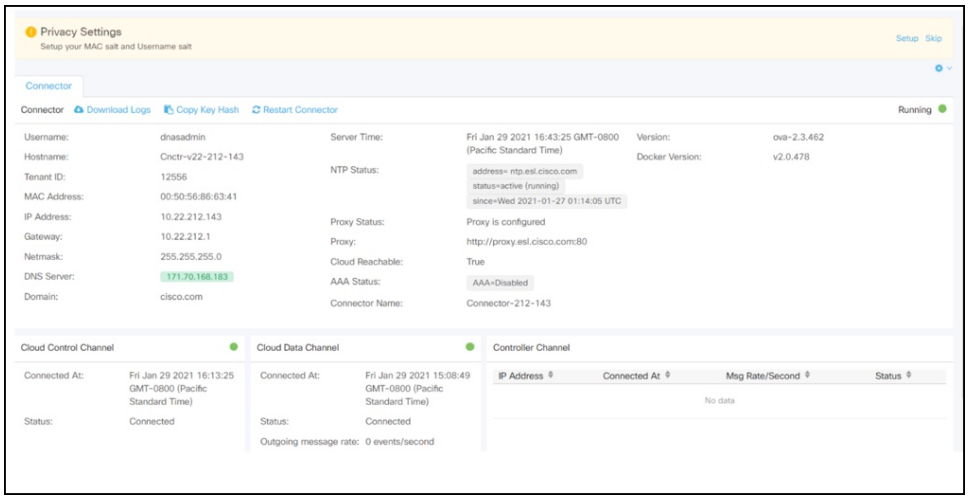
- コネクタ が展開されます。
- すべてのサービスが開始されます。
- コネクタ が Cisco DNA Spaces に追加されます。

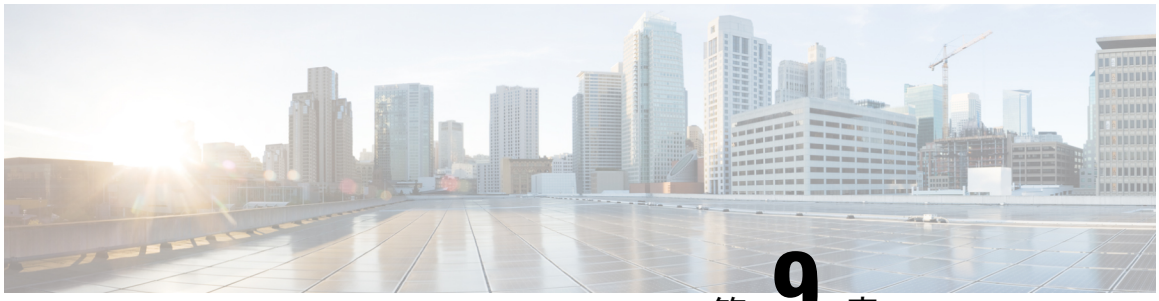
図 *24 :* スナップショットを使用したバックアップ



（注） スナップショットの復元の際、プロキシは引き継がれません。プロキシを再設定する必要があります。

図 *25 :* プロキシが再設定された後の コネクタ





第 9 章

Cisco DNA Spaces：コネクタ Hyper-V

Hyper-V のダウンロードと展開

この章では、Cisco DNA Spaces：コネクタ をダウンロードして展開し、コネクタ GUI の URL を取得する方法について説明します。

（注） **dnasadmin** は、以前は **cmxadmin** でした。

始める前に

Hyper-V で vSwitch を作成します。コネクタ はこの vSwitch に接続します。

手順の概要

1. Cisco.com からコネクタの VHDX イメージをダウンロードし、Hyper-V インスタンスを作成するフォルダの場所に VHDX を保存します。
2. 作成された vSwitch を右クリックし、[New] > [Virtual machine] の順に選択します。
3. [Next] をクリックして、Hyper-V の展開を開始します。
4. コネクタ の [Name] を入力し、仮想マシンを作成する場所を選択します。
5. [Sepecify Generation] ページで [Generation 1 VM] を選択します。
6. [Assign Memory] ページで、仮想マシンインスタンスに 4096 MB（4GB）のメモリを指定します。
7. [Configure Networking] ページで、前提条件として作成した vSwitch を選択します。
8. [Connect Virtual Hard Disk] ページで、[Use an existing hard disk] オプションを選択し、VHDX ファイルが保存されているフォルダの場所を選択します（前提条件）。
9. [Completing the New Machine Wizard] ページに、最終的な要約が表示されます。この要約を確認して、[Finish] をクリックします。
10. 作成された Hyper-V インスタンスを選択し、[Start] をクリックします。

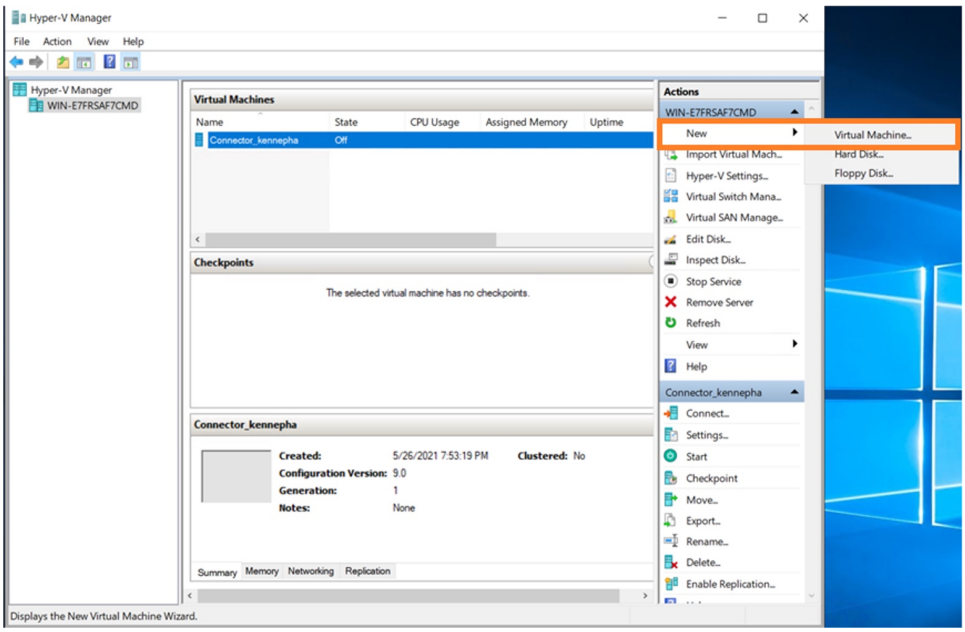
11. 端末にログインし、デフォルトのユーザ名「**root**」とデフォルトのパスワード「**cisco**」を入力します。
12. Cisco DNA Spaces：コネクタ で設定する IP アドレス、ホスト名などのパラメータを指定して、ネットワーク設定を入力します。
13. タイムゾーンを入力します。
14. Network Time Protocol（NTP）サーバ名を入力して、システム時刻を NTP サーバと同期します。NTP サーバを設定しない場合は、空白のままにします。
15. **root** ユーザの新しいパスワードを設定します。
16. 管理者権限を持つユーザである **dnasadmin** ユーザの新しいパスワードを設定します。
17. 自動リブートの前に URL をコピーして保存します。後でこの URL を使用して Cisco DNA Spaces：コネクタ GUI を開くことができます。

手順の詳細

ステップ 1 Cisco.com からコネクタの VHDX イメージをダウンロードし、Hyper-V インスタンスを作成するフォルダの場所に VHDX を保存します。

ステップ 2 作成された vSwitch を右クリックし、[New] > [Virtual machine] の順に選択します。

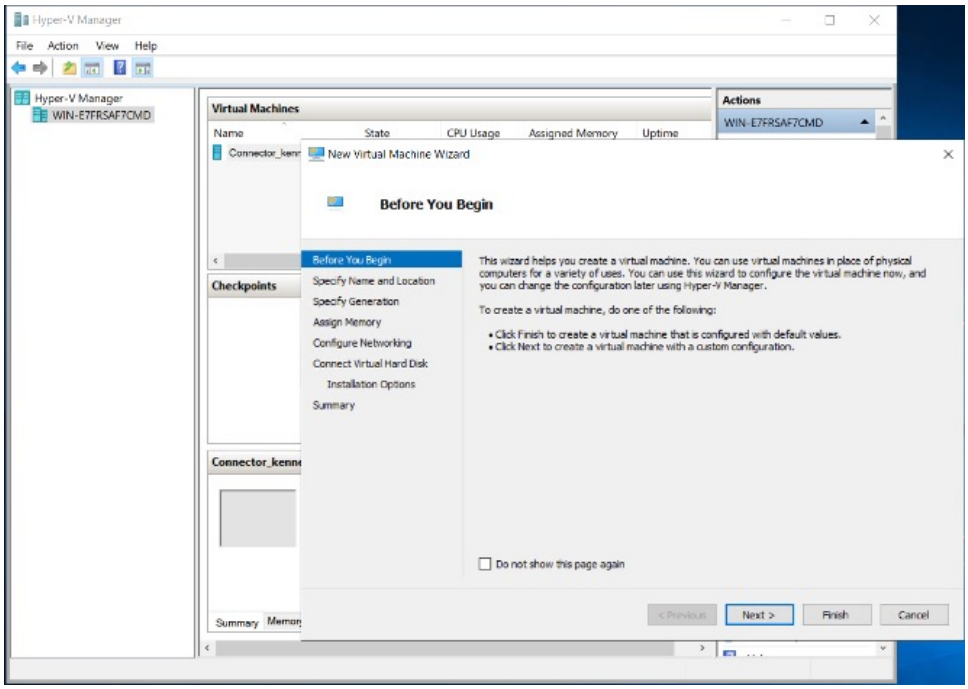
図 *26 : Hyper-V* 展開の開始



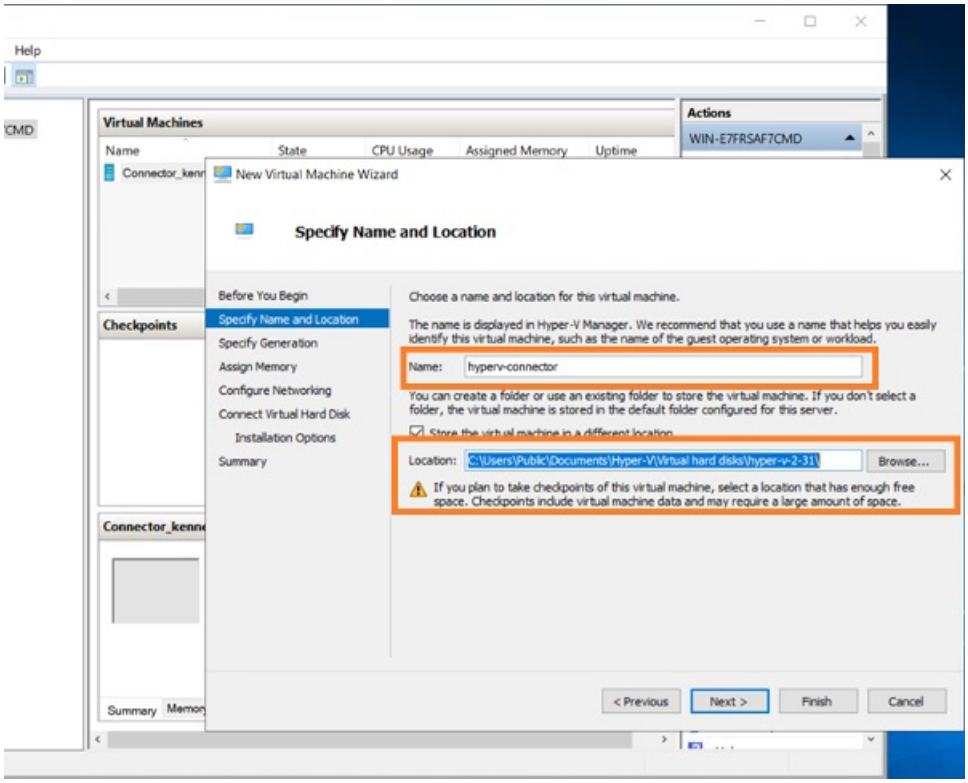
（注） [Import Virtual Machine] オプションや [New] > [Hard Disk] オプションは使用しないでください。

ステップ 3 [Next] をクリックして、Hyper-V の展開を開始します。

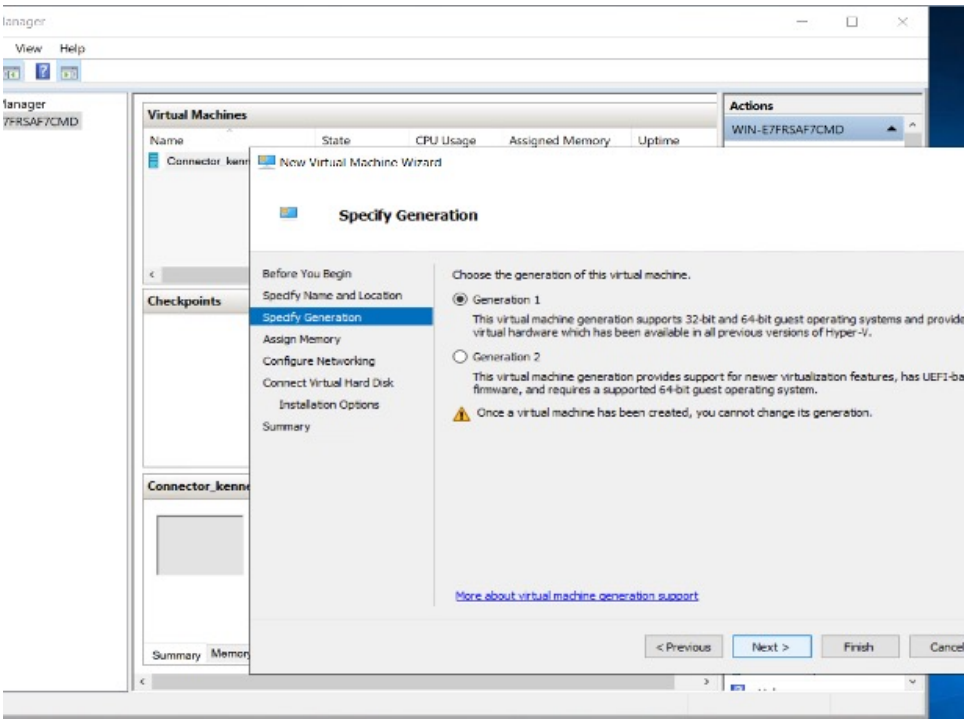
図 *27 : Hyper-V* 展開の開始



ステップ 4 コネクタ の [Name] を入力し、仮想マシンを作成する場所を選択します。



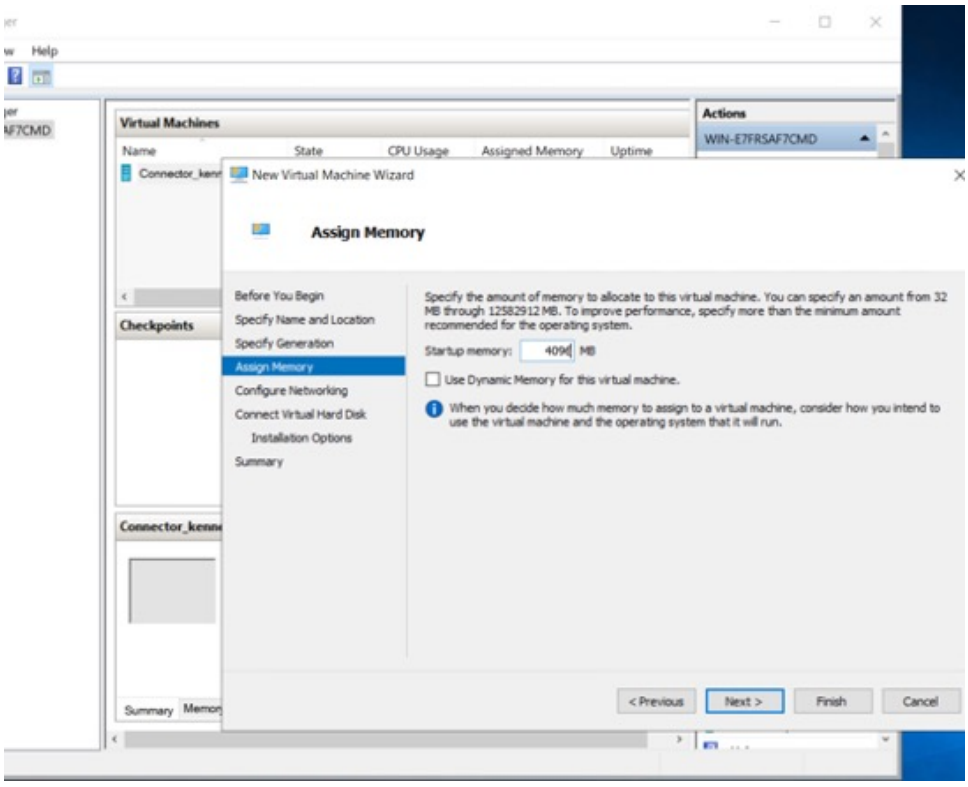
ステップ 5 [Sepecify Generation] ページで [Generation 1 VM] を選択します。



（注） [Generation 2 VM] はサポートされていません。

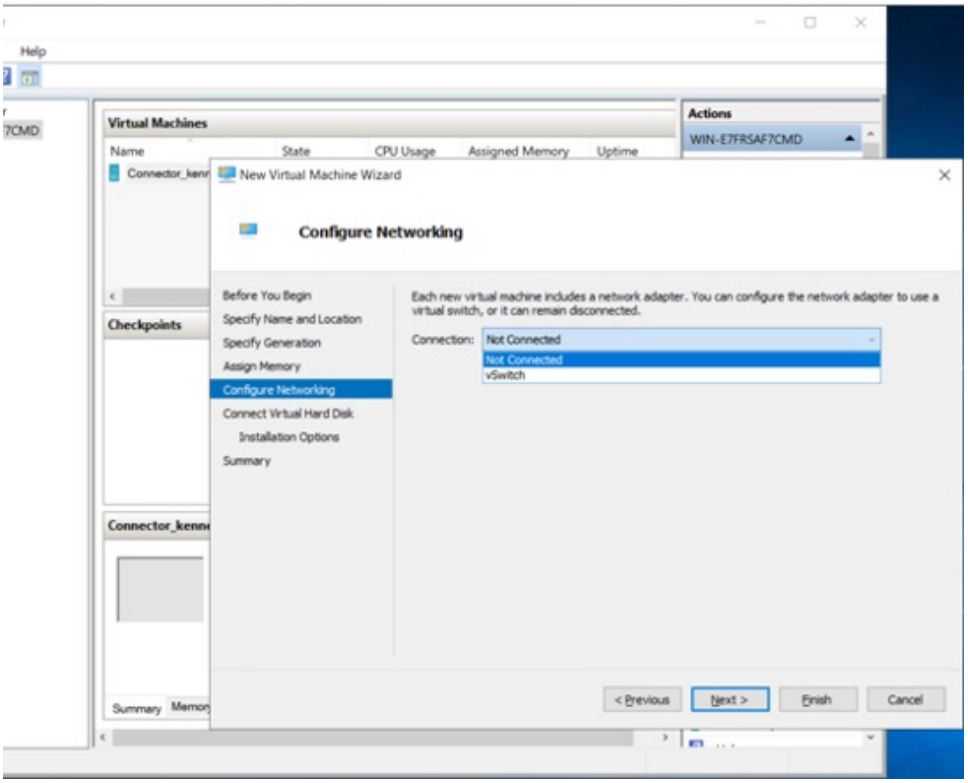
ステップ 6 [Assign Memory] ページで、仮想マシンインスタンスに 4096 MB（4GB）のメモリを指定します。

（注） 4096 MB（4GB）のメモリは、OVA の標準設定に相当します。



ステップ 7　[Configure Networking] ページで、前提条件として作成した vSwitch を選択します。

図 *28 : vSwitch* の選択



ステップ 8 [Connect Virtual Hard Disk] ページで、[Use an existing hard disk] オプションを選択し、VHDX ファイルが保存されているフォルダの場所を選択します（前提条件）。

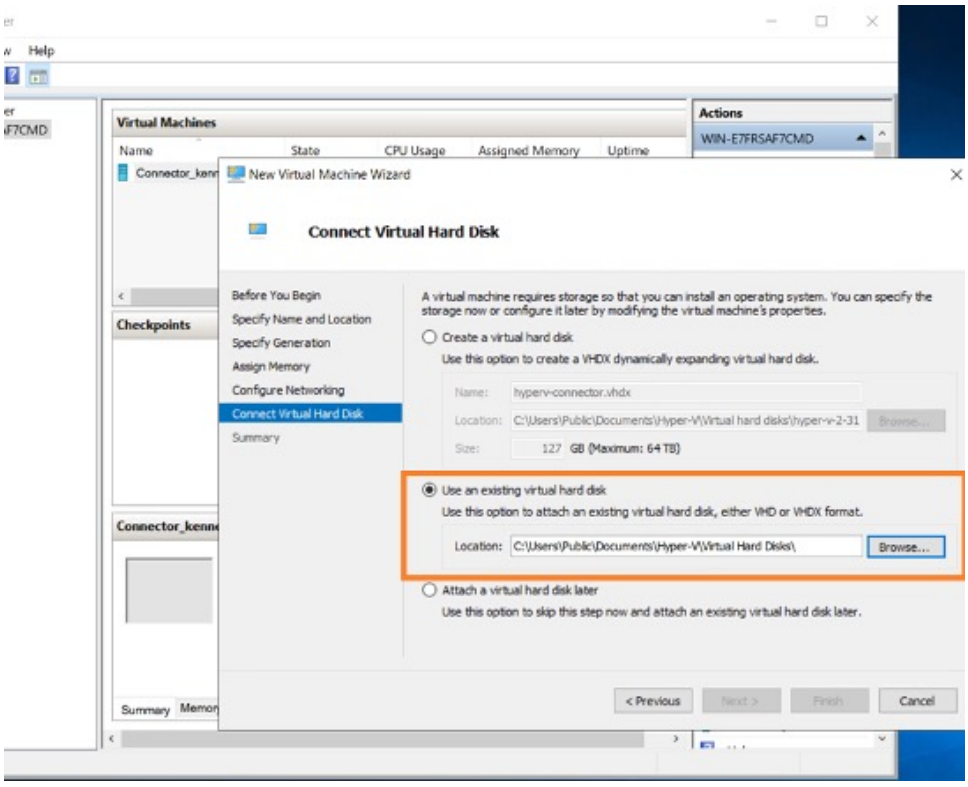
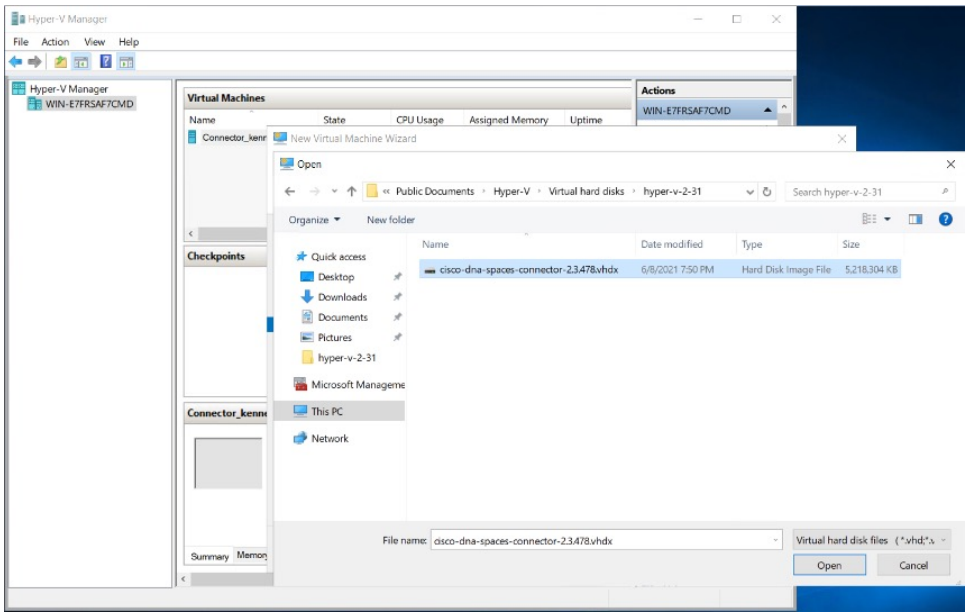
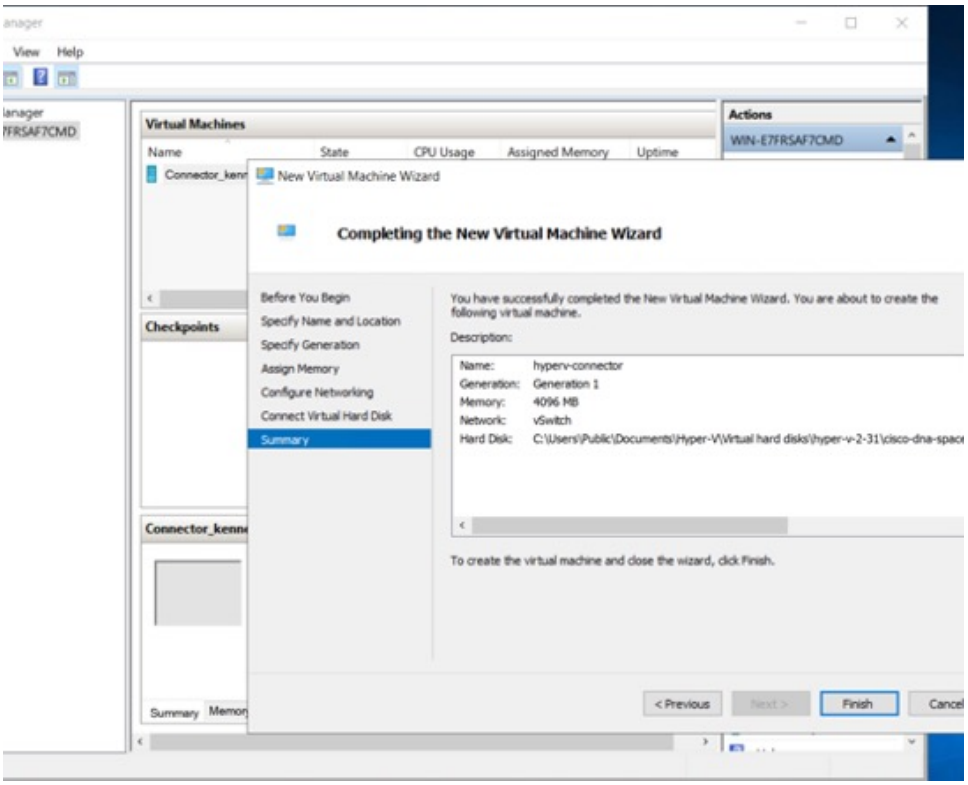


図 *29 : VHDX* ファイルが保存されているフォルダの場所

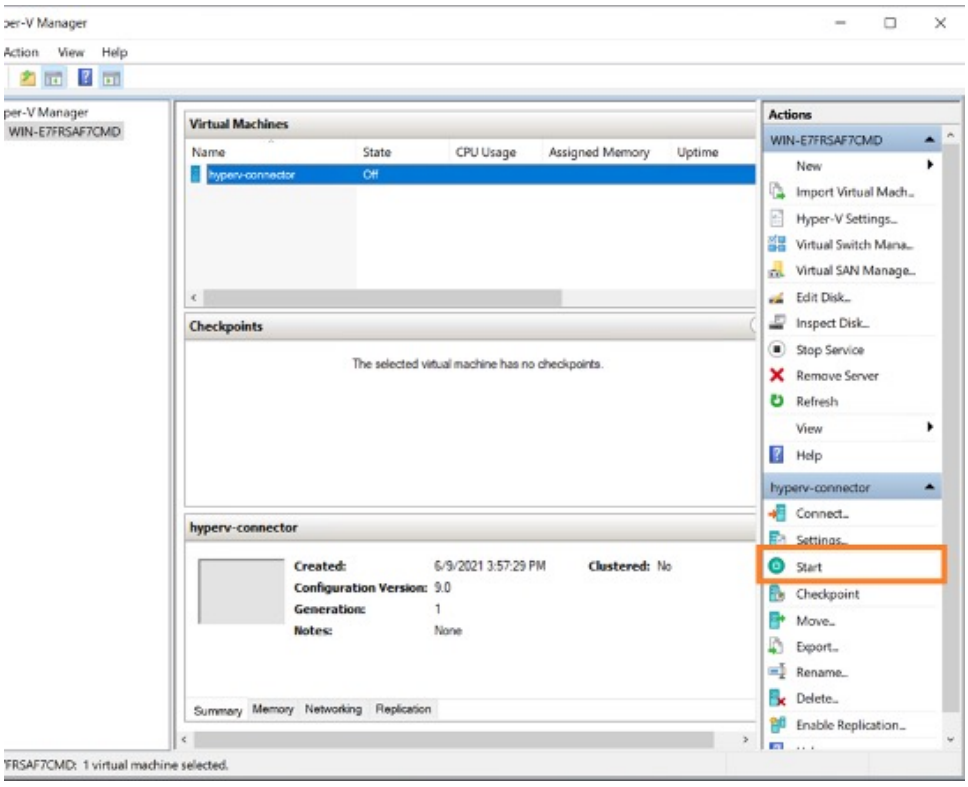


ステップ 9 [Completing the New Machine Wizard] ページに、最終的な要約が表示されます。この要約を確認して、[Finish] をクリックします。



Hyper-V インスタンスが作成されます。

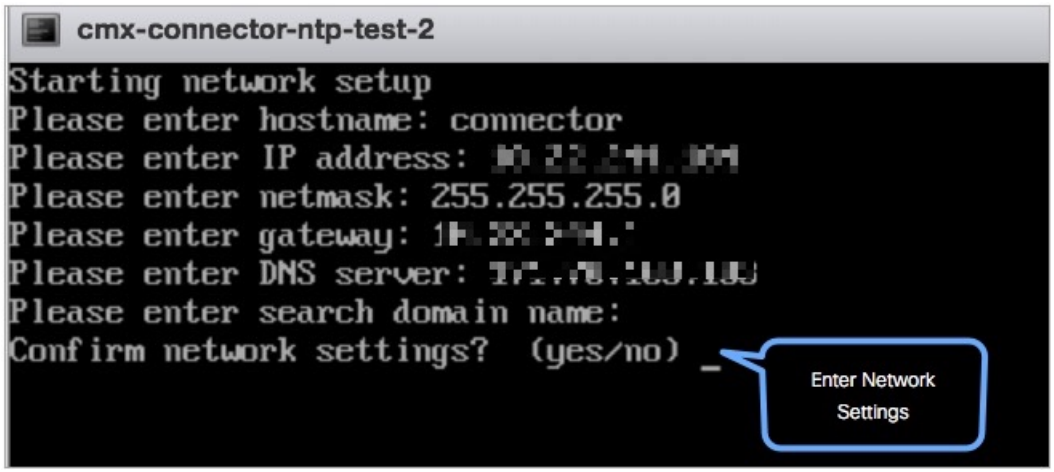
ステップ 10 作成された Hyper-V インスタンスを選択し、[Start] をクリックします。



仮想マシンコンソールが開きます。

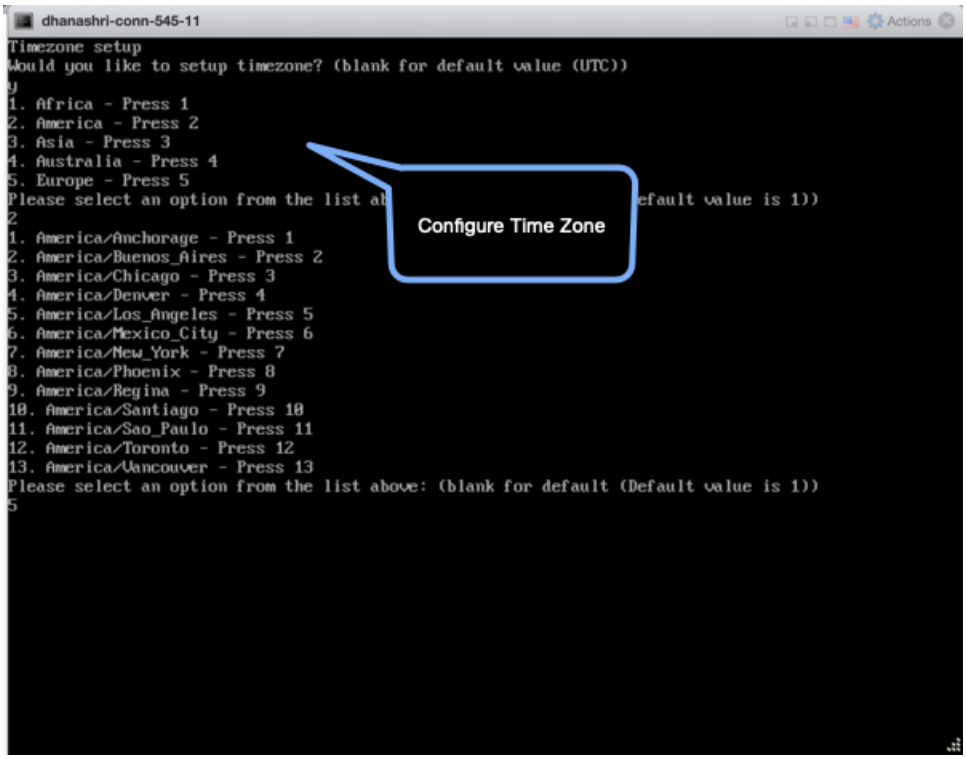
ステップ 11 端末にログインし、デフォルトのユーザ名「**root**」とデフォルトのパスワード「**cisco**」を入力します。

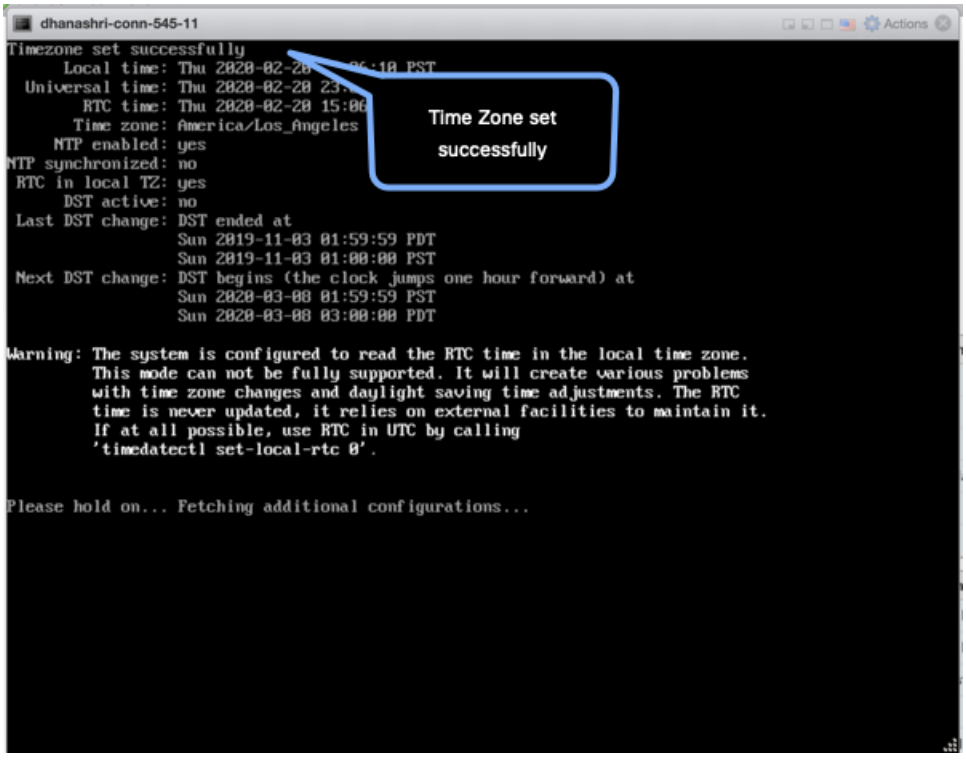
ステップ 12 Cisco DNA Spaces：コネクタ で設定する IP アドレス、ホスト名などのパラメータを指定して、ネットワーク設定を入力します。



（注） この設定画面は60秒でタイムアウトするので、再設定を避けるために時間内に入力してください。

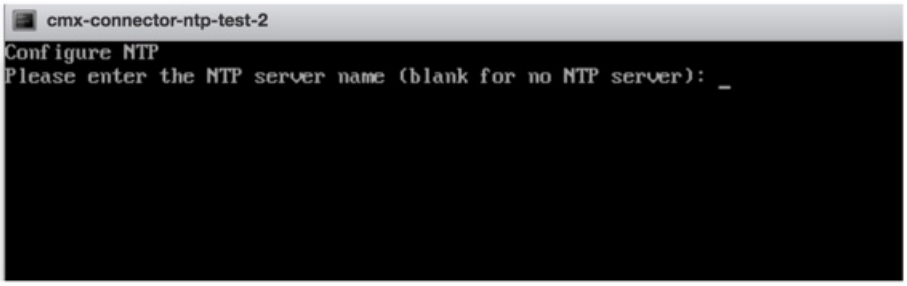
ステップ 13 タイムゾーンを入力します。



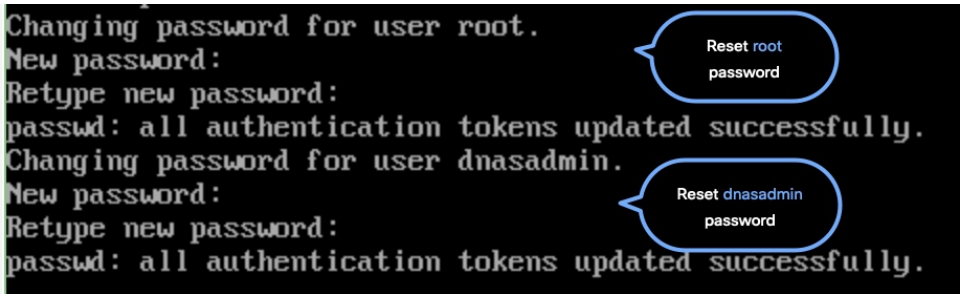


ステップ 14 Network Time Protocol（NTP）サーバ名を入力して、システム時刻を NTP サーバと同期します。NTP サーバを設定しない場合は、空白のままにします。

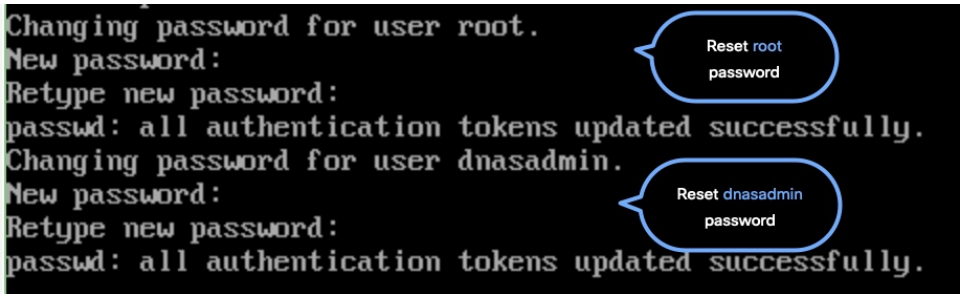
図 *30* : *NTP* 設定の入力



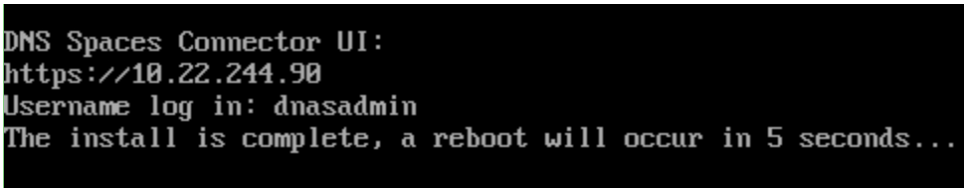
ステップ 15 **root** ユーザの新しいパスワードを設定します。



ステップ 16 管理者権限を持つユーザである **dnasadmin** ユーザの新しいパスワードを設定します。

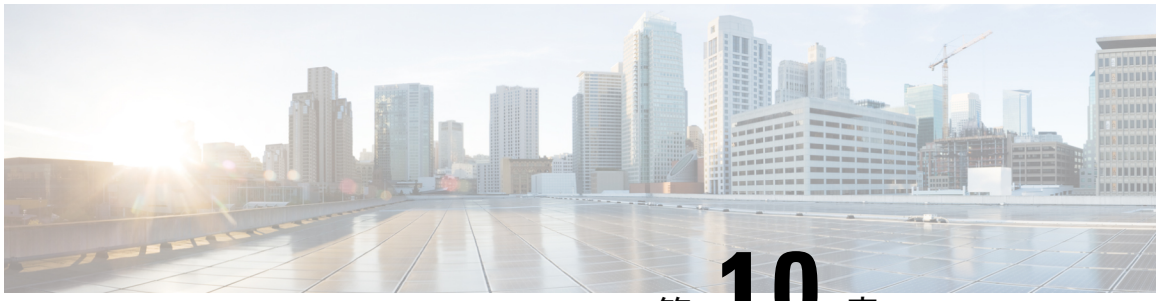


ステップ 17 自動リブートの前に URL をコピーして保存します。後でこの URL を使用して Cisco DNA Spaces：コネクタ GUI を開くことができます。



次のタスク

Cisco DNA Spaces からの コネクタ のトークンの取得（ワイヤレス）



第 10 章

コネクタ on Cisco DNA Spaces

コネクタ インスタンスの作成と Cisco DNA Spaces からのトークンの取得（有線）

この手順では、コネクタ を Cisco DNA Spaces アカウントに接続する方法を示します。

次の手順では、Cisco DNA Spaces アカウントに追加する コネクタ ごとにトークンを生成します。各トークンは コネクタ に固有のものです。トークンによって Cisco DNA Spaces が有効になり、コネクタ を識別して接続できるようになります。

Cisco DNA Spaces は複数の コネクタ をサポートしており、それぞれの コネクタ を 1 つまたは複数の コントローラ に関連付けることができます。

（注） Cisco DNA Spaces：コネクタ インスタンスは、一度に 1 つの Cisco DNA Spaces アカウントのみと通信できます。

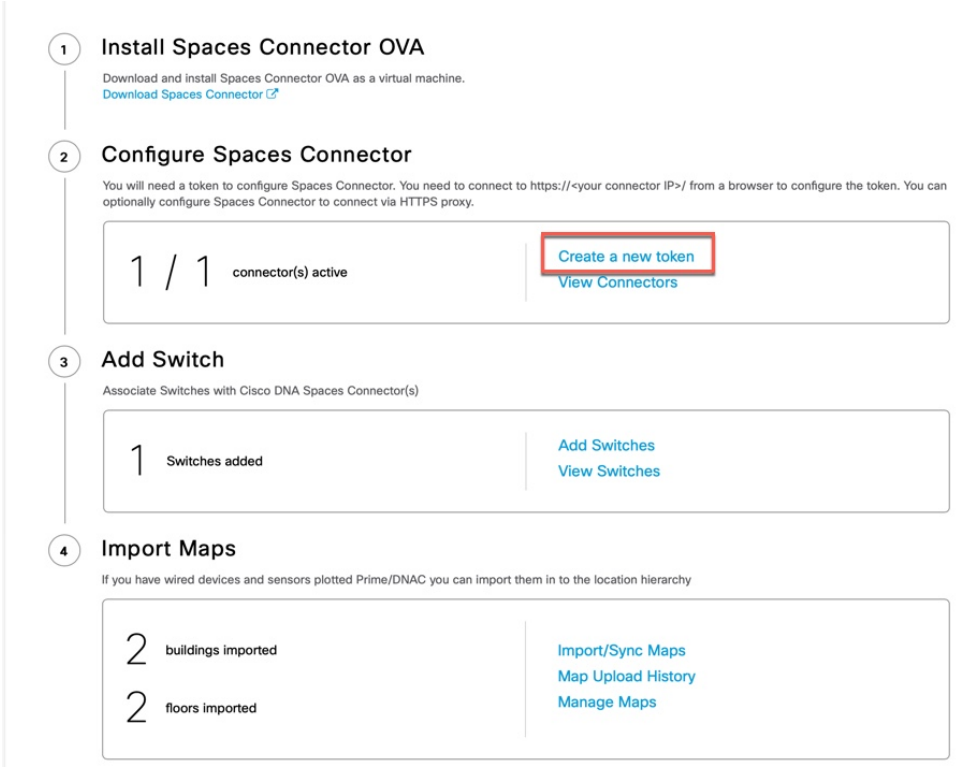
始める前に

Cisco DNA Spaces：コネクタ OVA をダウンロードして展開します。

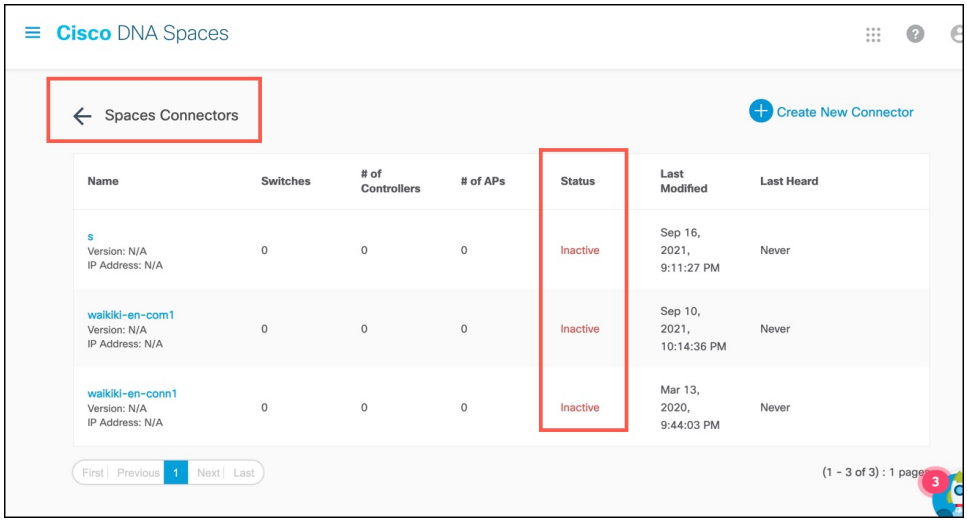
ステップ 1 [Cisco DNA Spaces] > [Setup] > [Wired Networks] にログインします。

（注） Cisco DNA Spaces の URL は地域によって異なります。

ステップ 2 [Step 2: Configure Spaces Connector] エリアで、[Create a new token] をクリックします。



ステップ 3 [Create a new token] ページで、コネクタ の名前を入力します。[Generate Token] をクリックします。トークンが生成されます。コピーボタンを使用してこのトークンをコピーします。新しいコネクタ が追加されました。



ステップ 4 表示された [Spaces コネクタ] ページで、追加した コネクタ の 3 つのドットボタンをクリックします。[Enable IoT Services] をクリックします。

ステップ 5 [Manage IoT Service] ページで、スイッチの 3 つのドットボタンをクリックします。[Enable Service] を選択して、IoT ストリームを有効にします。

Cisco DNA Spaces からの コネクタ のトークンの取得（ワイヤレス）

この手順では、コネクタ を Cisco DNA Spaces アカウントに接続する方法を示します。

次の手順では、Cisco DNA Spaces アカウントに追加する コネクタ ごとにトークンを生成します。各トークンは コネクタ に固有のものです。トークンによって Cisco DNA Spaces が有効になり、コネクタ を識別して接続できるようになります。

Cisco DNA Spaces は複数の コネクタ をサポートしており、それぞれの コネクタ を 1 つまたは複数の コントローラ に関連付けることができます。

（注） Cisco DNA Spaces：コネクタ インスタンスは、一度に 1 つの Cisco DNA Spaces アカウントのみと通信できます。

始める前に

Cisco DNA Spaces：コネクタ OVA をダウンロードして展開します。

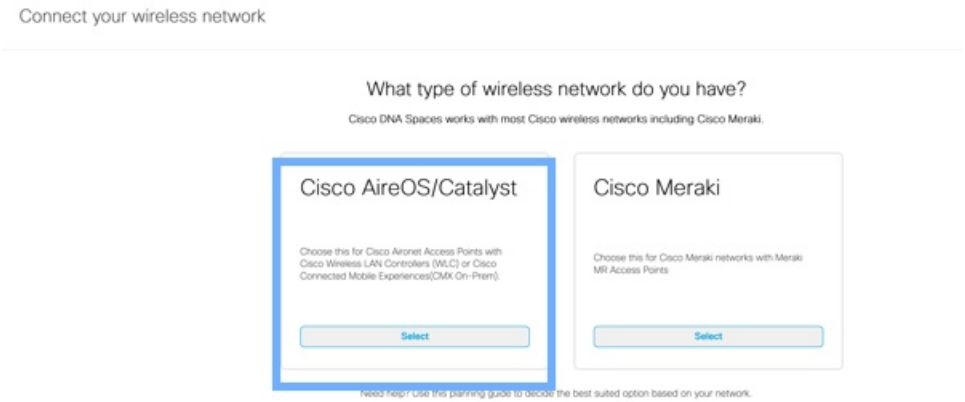
ステップ 1 **Cisco DNA Spaces** にログインします。

（注） Cisco DNA Spaces の URL は地域によって異なります。

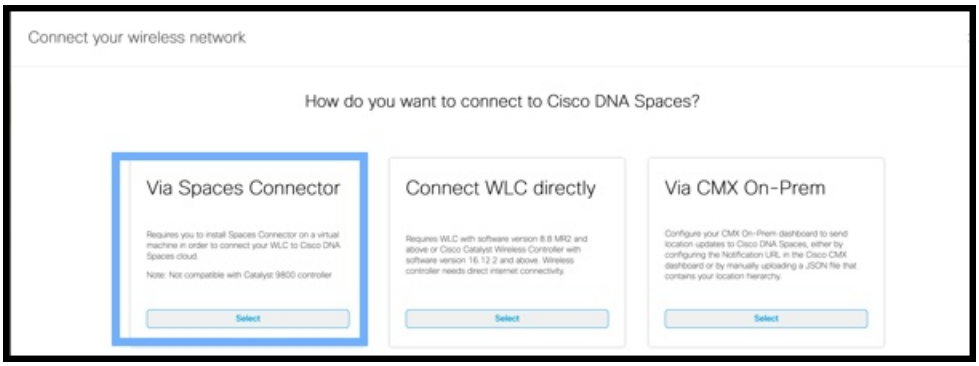
ステップ 2 左側のナビゲーションペインから、[Setup] > [Wireless Networks] の順に選択します。

ステップ 3 [Get your wireless network connected with Cisco DNA Spaces] エリアで、[Add New] をクリックします。

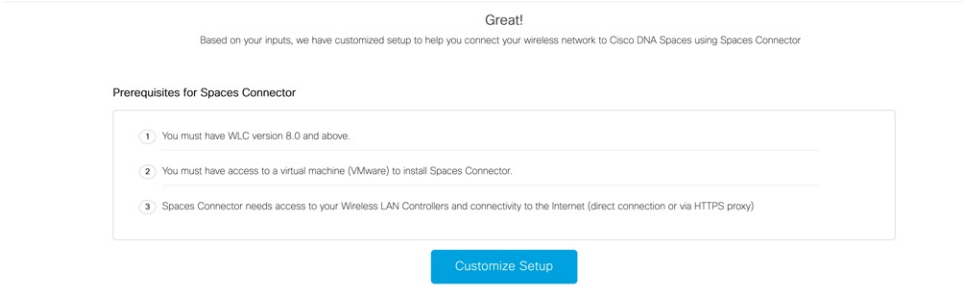
ステップ 4 [Cisco AireOS/Catalyst] エリアで、[Select] をクリックします。



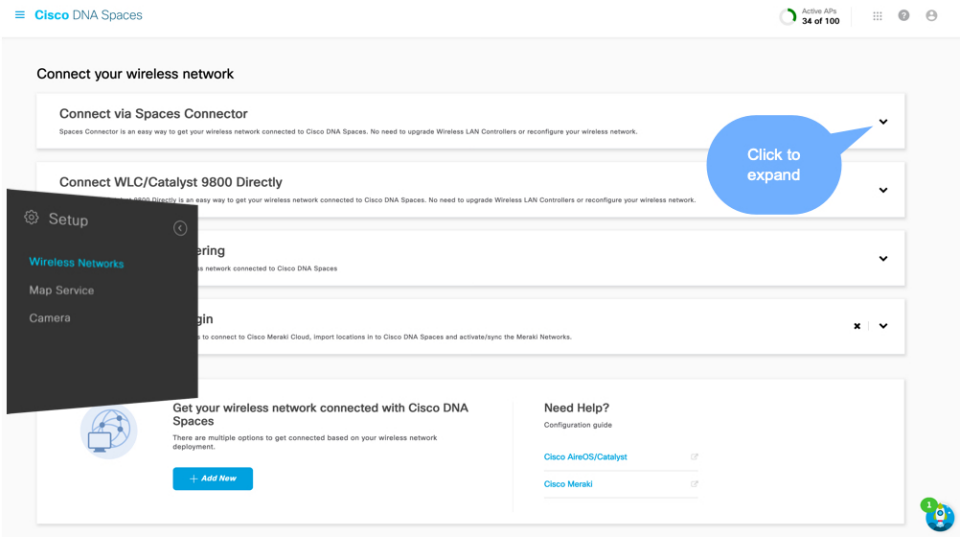
ステップ 5 [Via Spaces Connector] エリアで、[Select] をクリックします。



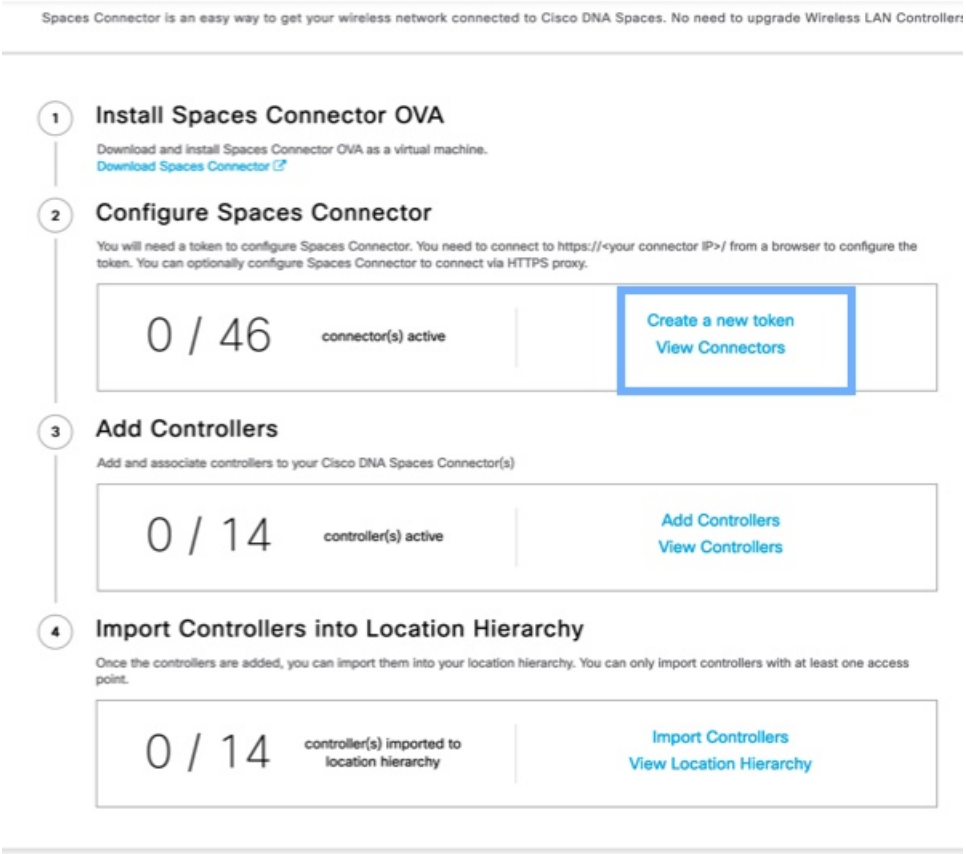
ステップ 6 [Prerequisites for Spaces Connector] ダイアログボックスで、[Continue Setup] をクリックします。



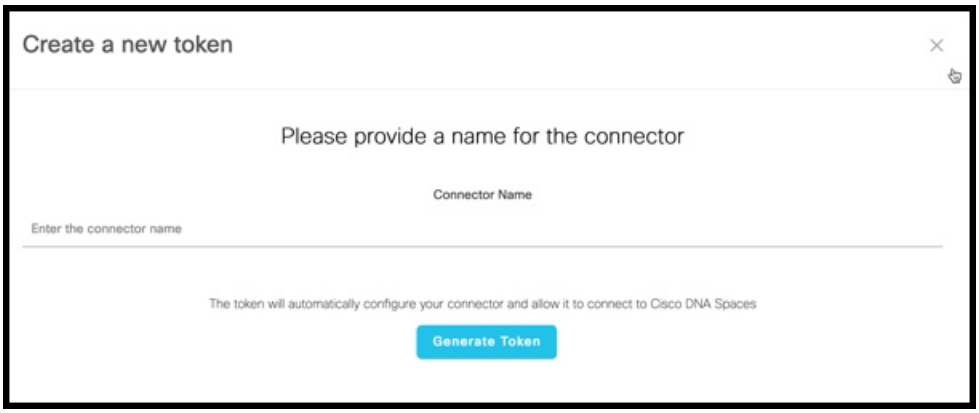
ステップ 7 それぞれのドロップダウン矢印を使用して、[Connects by Spaces Connector] エリアを展開します。



ステップ 8　表示された手順のリストで、[Configure Spaces Connector] エリアの [Create New Token] をクリックします。



ステップ 9　[Create a new token] ダイアログボックスで、コネクタ の名前を入力します。



ステップ 10 [Generate Token] をクリックします。

ステップ 11 表示されるダイアログボックスで、[Copy] をクリックしてトークンの文字列をコピーします。

Cisco DNA Spaces：コネクタ のアクティブ化

この手順では、Cisco DNA Spaces から取得した コネクタ のトークンを使用して コネクタ をアクティブにする方法を示します。

始める前に

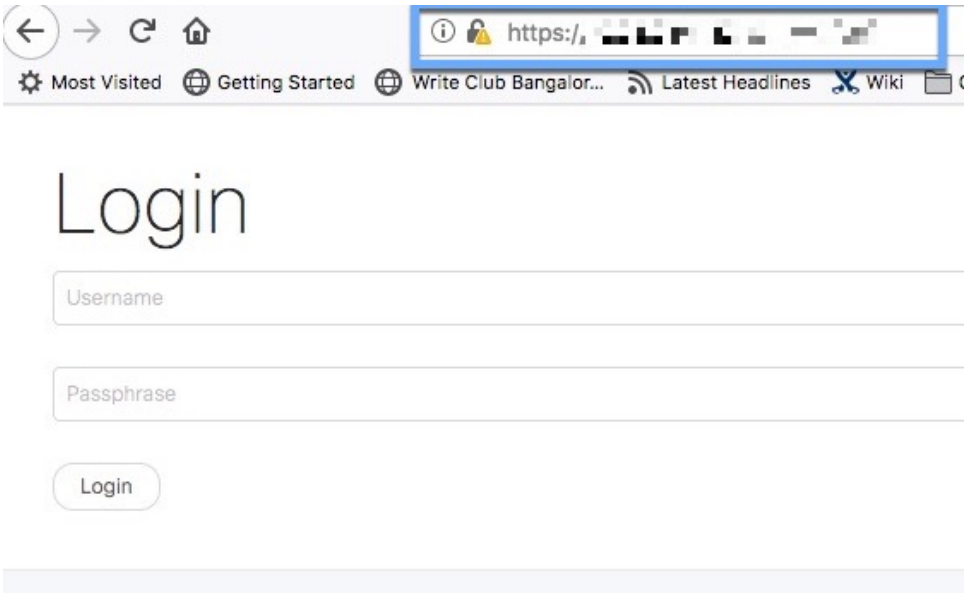
Cisco DNA Spaces：コネクタ OVAを展開し、IP アドレスを設定します。コネクタ から Cisco DNA Spaces のトークンを取得します。

手順の概要

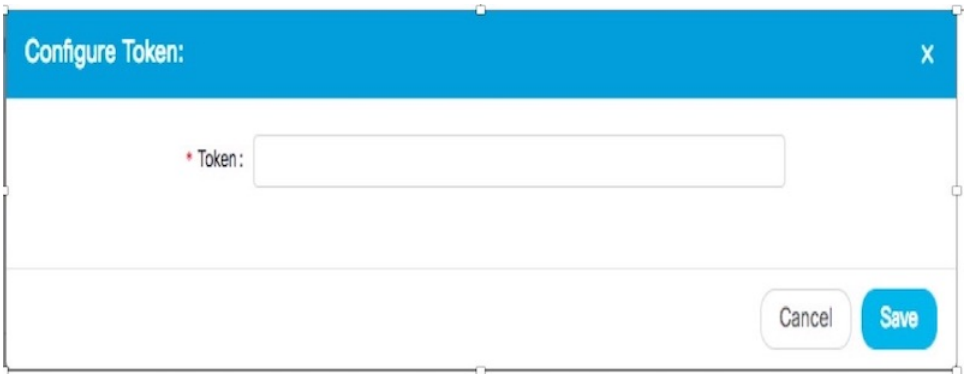
1. Cisco DNA Spaces：コネクタ GUI を起動し、ユーザ名「**dnasadmin**」と、このユーザに対して以前に設定したパスワードを入力します。
2. ウィンドウの右上隅にある設定（歯車）アイコンをクリックし、[Configure Token] を選択し、Cisco DNA Spaces から受信したトークンを追加して、[Save] をクリックします。
3. ダッシュボードでさまざまな接続の正常性を確認します。

手順の詳細

ステップ 1 Cisco DNA Spaces：コネクタ GUI を起動し、ユーザ名「**dnasadmin**」と、このユーザに対して以前に設定したパスワードを入力します。



ステップ 2 ウィンドウの右上隅にある設定（歯車）アイコンをクリックし、[Configure Token] を選択し、Cisco DNA Spaces から受信したトークンを追加して、[Save] をクリックします。



（注）
- トークンを入力した後、Cisco DNA Spaces：コネクタ が Cisco DNA Spaces から最新の Docker イメージを初期化してダウンロードするまで数分かかる場合があります。実際の所要時間は、ネットワーク接続の速度によって異なります。ステータスが [Configure Token] から [Retrieving Connector Status] に変わります。[Configure Token] 通知オプションが Cisco DNA Spaces：コネクタ Web UI から消えます。

ステップ 3 ダッシュボードでさまざまな接続の正常性を確認します。

次のタスク

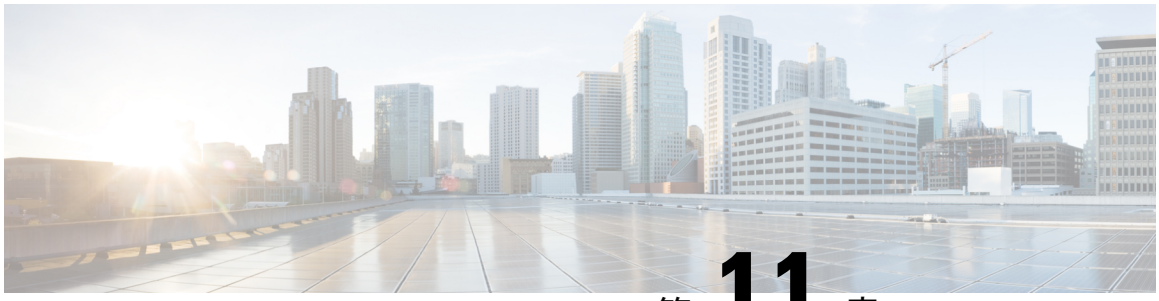
このダッシュボードの要素の詳細については、ダッシュボード （75 ページ） を参照してください。

（注）

- CSCvx02620 の場合、クレデンシャルの入力後に Cisco DNA Spaces：コネクタ GUI がハングします。クレデンシャルを入力するページが表示された後、エラーが発生していないのにコネクタ WebUI がハングします。引き続きコネクタに SSH 接続することは可能です。

  このエラーは、コネクタ と Cisco DNA Spaces GUI の間の接続に問題があるときに、Cisco DNA Spaces から コネクタ にトークンを追加した場合に発生します。この場合、後に続くログインの試行中に コネクタ が動作を停止する可能性があります。

  コネクタ GUI へのアクセスを回復するには、データベースからトークンを削除する必要があります。



第 11 章

ダッシュボード

ダッシュボード

• [Status]：右上隅の Cisco DNA Spaces：コネクタ のステータス。

• [Cloud Control Channel]：コネクタ と Cisco DNA Spaces の間における制御チャネルの接続の正常性。

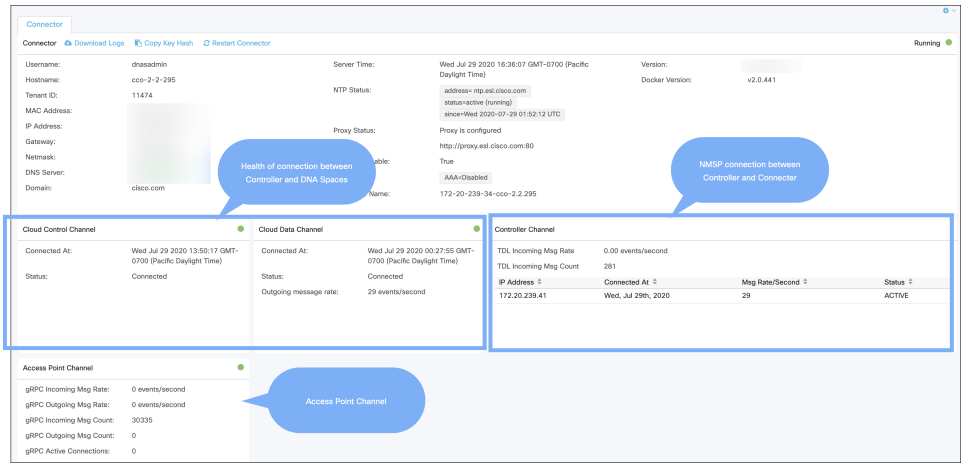
• [Cloud Data Channel]：コネクタ と Cisco DNA Spaces の間におけるデータチャネルの接続の正常性。

• [Controller Channel]：コネクタ と シスコ ワイヤレス コントローラ または Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ 間の NMSP 接続。

TDL メッセージレートとメッセージ数は、テレメトリ サブスクリプションの詳細を示します。TDL メッセージは、テレメトリ サブスクリプションを介したモデル駆動型テレメトリデータのコレクタとして コネクタ が使用される場合に生成されます。

(注) テレメトリ サブスクリプションは、NETCONF などのプログラマブルインターフェイスを介して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ および Cisco Catalyst 9300/9400 シリーズ スイッチ のみで作成できます。

図 *31* : コネクタの詳細

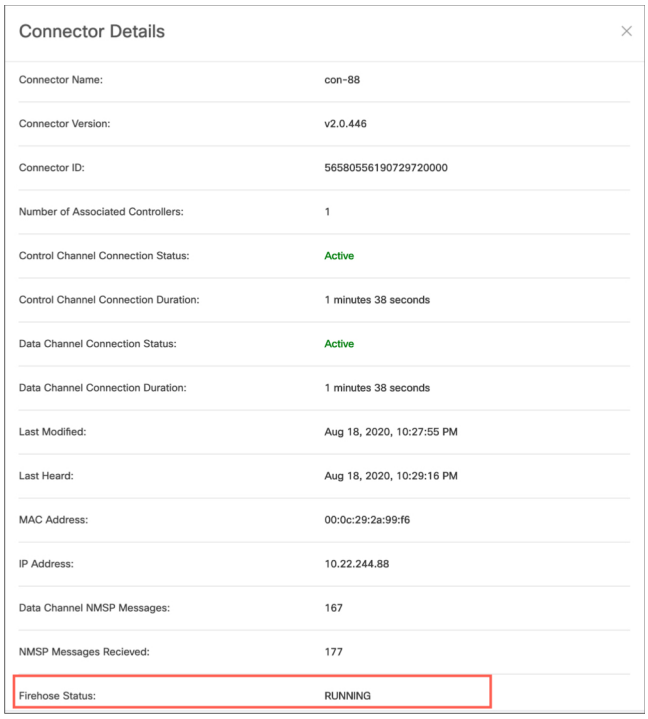


- [Local Firehose Channel Details]：提携アプリケーションとしての Cisco DNA Spaces と Cisco DNA Spaces の間で未加工の Firehose API データのストリームを交換するために使用される双方向チャネルのステータス。

図 *32* : ローカル *Firehose* チャネルのステータス（コネクタ の表示）

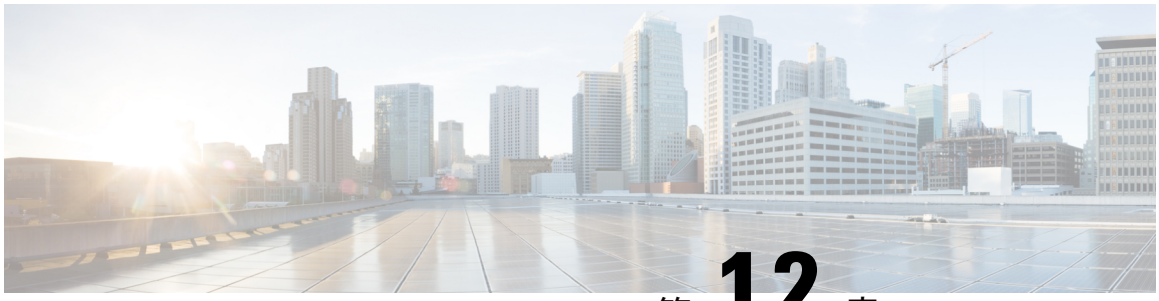
Cisco DNA Spaces ダッシュボードでローカル Firehose チャネルのステータスを確認することもできます。

図 *33* : ローカル *Firehose* チャネルのステータス（*Cisco DNA Spaces* ダッシュボードの表示）



- [Access Point Channel Details]：コネクタ と、IoT ゲートウェイが有効になっているアクセスポイント間の gRPC チャネルのステータス。IoT サービスからのデータは、こうした種類のデータの一例です。

図 *34* : *gRPC* の詳細



第 12 章

プロキシの設定

プロキシの設定

コネクタ GUIでは、プロキシや他のプライバシー設定も実行できます。コネクタ をホストしている Cisco UCS がプロキシの背後にある場合、コネクタ を Cisco DNA Spaces に接続するプロキシを設定できます。このプロキシ設定がないと、コネクタ は Cisco DNA Spaces と通信できません。

手順の概要

1. コネクタ CLI インターフェイスに SSH 接続します。**dnasadmin** ユーザがアクセスできる場所にプロキシ証明書ファイルをコピーします。
2. （任意） CLI から **setproxycert** コマンドを実行します。
3. コネクタ GUIに戻り、[set up HTTP Proxy] をクリックします。表示されるダイアログボックスにプロキシアドレスを入力します。

手順の詳細

ステップ 1 コネクタ CLI インターフェイスに SSH 接続します。**dnasadmin** ユーザがアクセスできる場所にプロキシ証明書ファイルをコピーします。

```
Username:~ username$ scp ~/Downloads/cert.pem dnasadmin@x.x.x.x
Username:~ username$ ssh dnasadmin@x.x.x.x
dnasadmin@x.x.x.x's password:
Last failed login: Mon Oct 22 23:54:08 UTC 2018 from x.x.x.x on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Mon Oct 22 22:43:17 2018 from x.x.x.x
```

ステップ 2 （任意） CLI から **setproxycert** コマンドを実行します。

```
[dnasadmin@connector ~]$ connectorctl setproxycert cert.pem
New cert exists.
Restarting connector container ...
Connector container was restarted.
setProxyCert successful.
```

ステップ 3 コネクタ GUIに戻り、[set up HTTP Proxy] をクリックします。表示されるダイアログボックスにプロキシアドレスを入力します。

図 *35 :* プロキシの設定

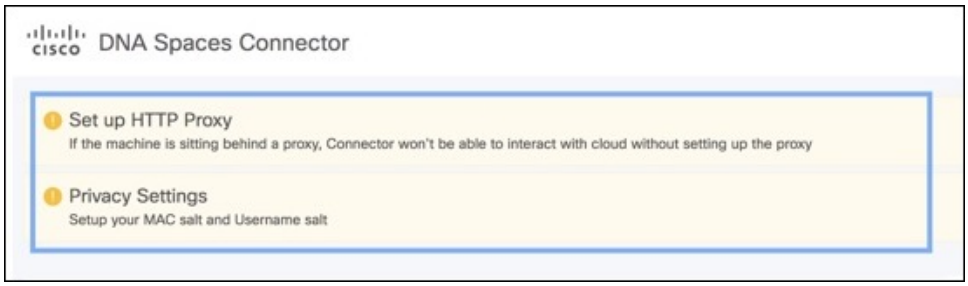
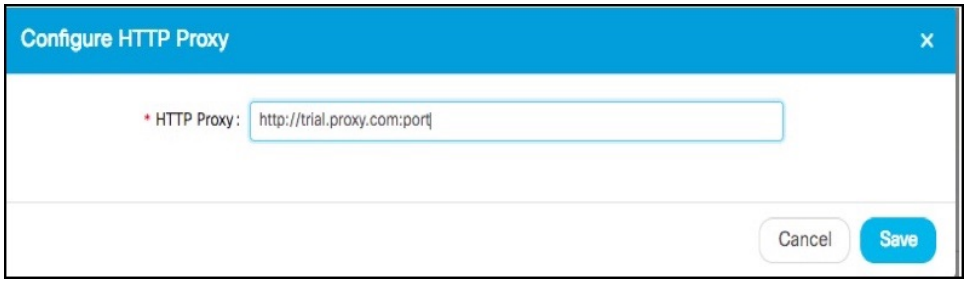


図 *36 :* プロキシの設定



基本認証クレデンシャルを含むプロキシを設定することもできます。

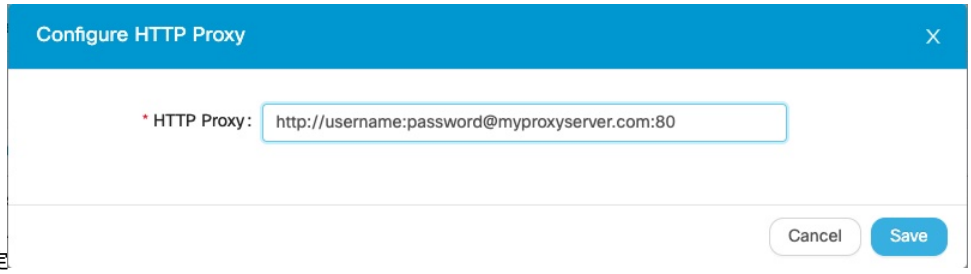
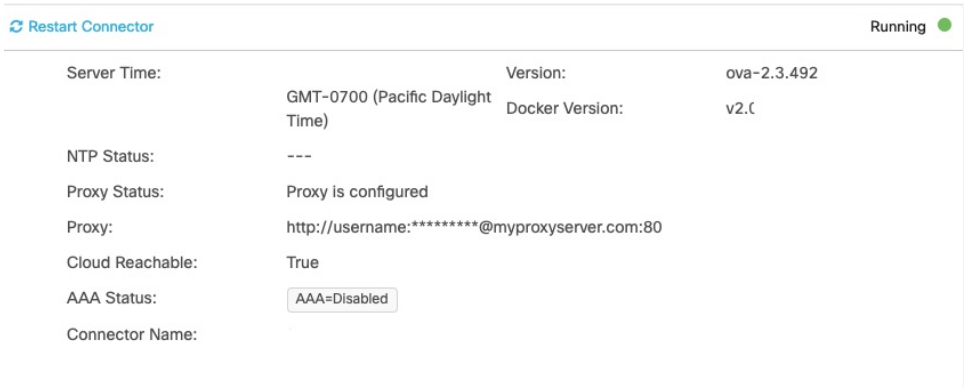


図 *37 :* 基本認証によるプロキシの設定

図 *38 :* 基本認証によって設定されたプロキシ



プロキシ設定のトラブルシューティング

手順の概要

1. コネクタ CLI インターフェイスに SSH 接続し、プロキシサーバの IP アドレスを ping します。
2. *curl*：（*60*）ピアの証明書発行者がユーザによって信頼できないとマークされているなどの証明書エラーが発生した場合は、次の手順を実行してプロキシサーバ証明書をコネクタに追加します。
3. 前の手順で問題が解決しない場合は、プロキシの許可リストに **dnaspaces.io** ドメインを含めて、HTTPS 復号から除外する必要があります（プロキシで有効になっている場合）。

手順の詳細

ステップ 1 コネクタ CLI インターフェイスに SSH 接続し、プロキシサーバの IP アドレスを ping します。

ステップ 2 *curl*：（*60*）ピアの証明書発行者がユーザによって信頼できないとマークされているなどの証明書エラーが発生した場合は、次の手順を実行してプロキシサーバ証明書を コネクタ に追加します。

a) プロキシで使用される証明書を取得し、Cisco DNA Spaces：コネクタ にコピーします。

b) **connectorctl setproxycert** コマンドを実行し、出力を確認します。

```
[dnasadmin@dnasadmin ~]$ connectorctl setproxycert squid.pem

New cert exists.
Starting connector container ...
Current version in database: latest
Container: [<Container: adlbledc71>]
Running connector version: latest
setproxycert successful.
```

（注） 透過的プロキシを使用している場合や、GUI を使用してプロキシを設定していない場合、このコマンドは失敗する可能性があります。このコマンドによって、証明書が正しく設定されているかどうかを確認できます。

c) コネクタ でトークンを再設定します。

ステップ 3 前の手順で問題が解決しない場合は、プロキシの許可リストに **dnaspaces.io** ドメインを含めて、HTTPS 復号から除外する必要があります（プロキシで有効になっている場合）。

（注） dnaspaces.io ドメインで HTTPS 復号を実行しようとすると、Websocket 接続が干渉を受けたり、完全に阻害されたりする可能性があります。

第 13 章

シスコ ワイヤレス コントローラへのコネクタの接続

コネクタ から シスコ ワイヤレス コントローラ へ

始める前に

- コネクタ OVA を展開し、Cisco DNA Spaces のトークンを使用してアクティブにします。
- Cisco DNA Spaces：コネクタ から到達可能な シスコ ワイヤレス コントローラ の IP アドレス。
- CSCvk38081 では、コントローラ のダイナミック インターフェイスと同じサブネットにコネクタを追加しないことを推奨します。ただし、この推奨事項に従わない場合は、コントローラ を コネクタ に追加し、すべての SNMP クエリをコントローラのダイナミック インターフェイスの IP アドレスに設定できます。

  また、コントローラ のサービスポートと同じサブネット上に コネクタ を追加しないことを推奨します。ただし、この推奨事項に従わない場合は、コントローラ を コネクタ に追加し、すべての SNMP クエリをコントローラのサービスポートの IP アドレスに設定できます。

  この制限は、コントローラ の制限の結果です。SNMP クエリは通常管理 IP アドレスに対して行われますが、SNMP応答パケットは、動的インターフェイスまたは送信元ポートの IP アドレスで設定された送信元 IP アドレスフィールドとともに返されます。

ステップ 1 Cisco DNA Spaces にログインします。

ステップ 2 Cisco DNA Spaces ダッシュボードで、[Setup] > [Wireless Networks] の順に選択します。

ステップ 3 ステップのリストを表示するには、それぞれのドロップダウン矢印を使用して、[Connector via Spaces Connector] エリアを展開します。

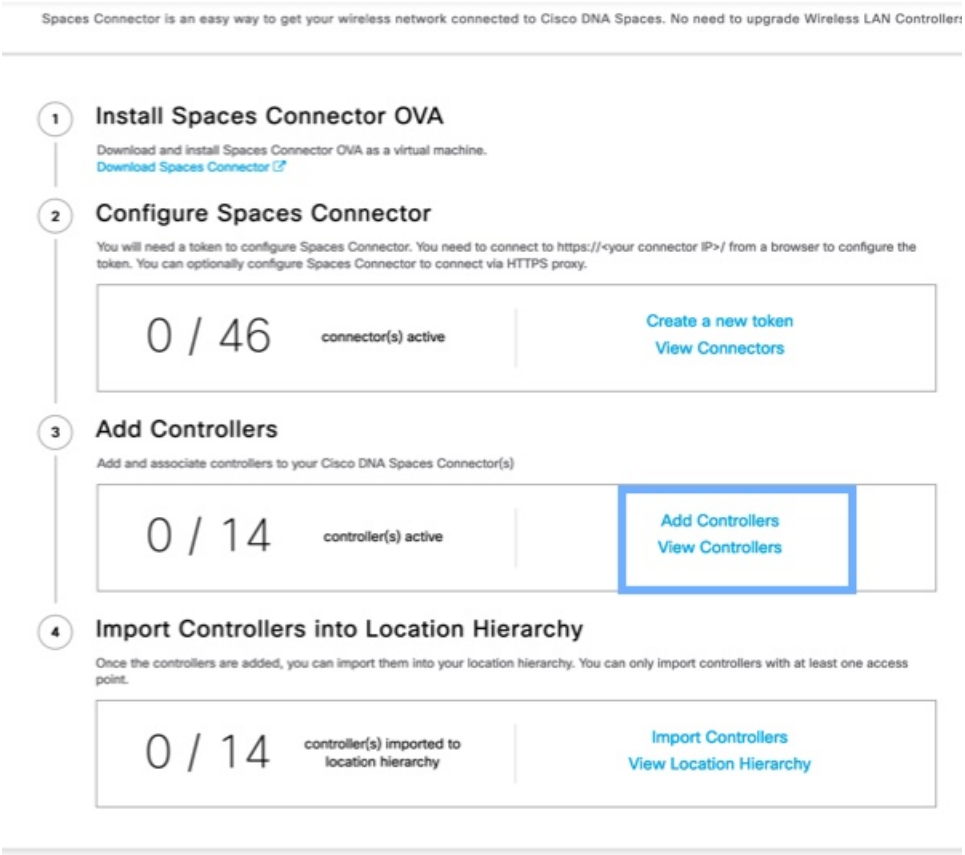
ステップ 4 コネクタ から既存の コントローラ への接続をテストするには、[Step 3] エリアの [View Controllers] をクリックします。

a) コントローラ を編集するには、鉛筆アイコンをクリックします。

b) [Connector] ドロップダウンリストからアクティブな コネクタ を選択して、[Test Connectivity] ボタンを有効にします。

c) ステップ 9 に進んでください。

ステップ 5 新しい コントローラ を追加するには、[Step 3] エリアの [Add Controllers] をクリックします。



ステップ 6 [Connector] ドロップダウンリストから、コネクタ を選択します。

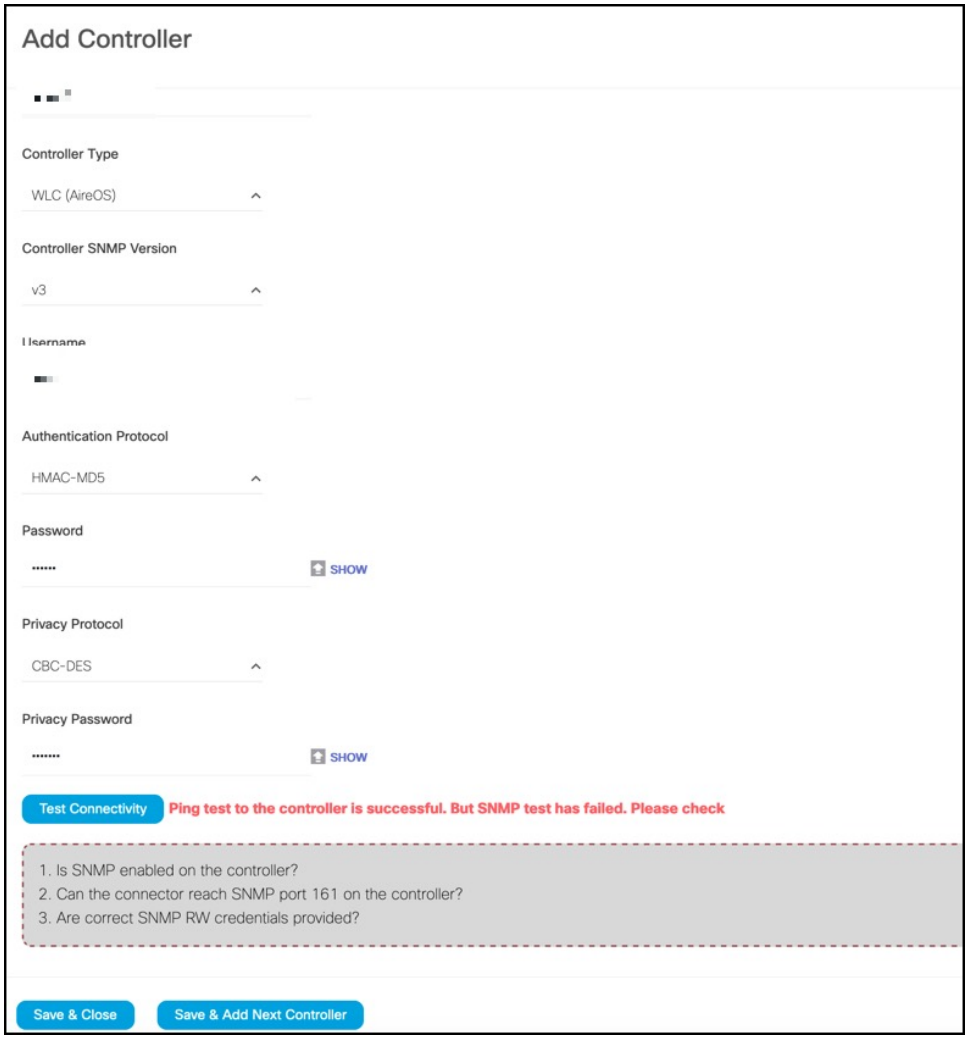
ステップ 7 [Controller IP] アドレスと [Controller Name] を入力し、[Controller Type] ドロップダウンリストから [WLC (AireOS)] を選択して シスコ ワイヤレス コントローラ に接続します。

ステップ 8 [Controller SNMP Version] ドロップダウンリストから、コントローラ の SNMP バージョンを選択します。

- **SNMP** バージョンを **v2C** として選択する場合は、SNMP 読み取り/書き込みコミュニティを指定します。
- **SNMP** バージョンを **v3** として選択する場合は、SNMP v3 バージョンのユーザ名、パスワード、および認証プロトコルのクレデンシャルを指定します。SNMP v3 に コントローラ での読み取り/書き込み権限があることを確認します。

（注） コントローラ に コネクタ 証明書を登録するには、SNMP v2c と SNMP v3 の両方に コントローラ での読み取り/書き込み権限が必要です。コネクタ は SNMP v1 をサポートしていません。

図 *39* : シスコ ワイヤレス コントローラ（コントローラ）の追加



ステップ 9 [Test Connectivity] をクリックして、Cisco DNA Spaces から コネクタ に対してテスト PING および SNMP 機能を実行します。このテストでは、到達可能性と入力されたクレデンシャルをチェックします。

[Test Connectivity] は、アクティブな コネクタ が選択されている場合にのみ有効になります。

図 *40* : コネクタ のリストとその状態

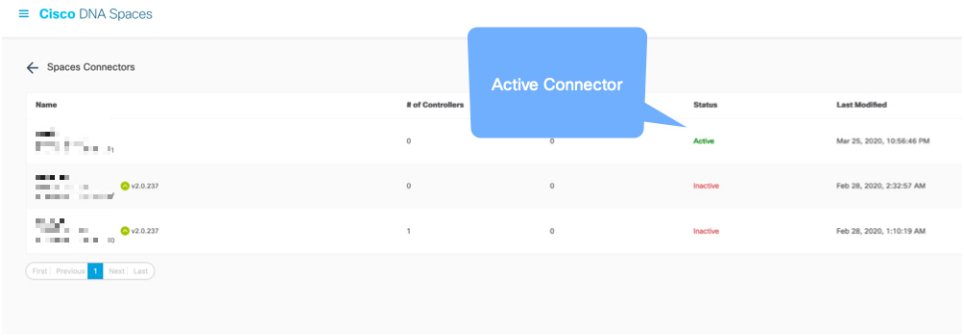


表 *4* : エラーの説明

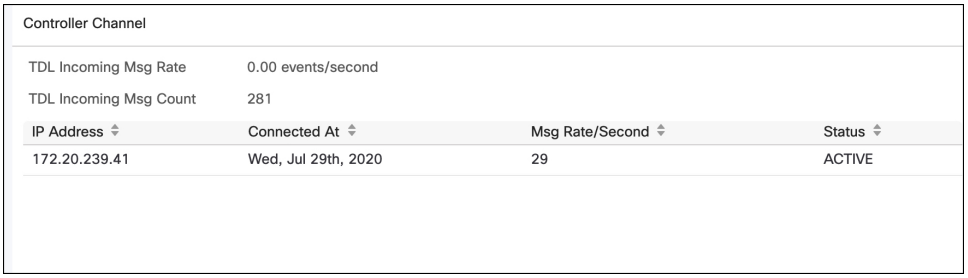
PING のステータス	SSH クレデンシャルテストのステータス	表示されるテスト接続メッセージ
SUCCESSFUL	SUCCESSFUL	接続テストに成功しました
SUCCESSFUL	FAILED	コントローラ に対する PING テストに成功しました。しかしながら、SSH テストには失敗しました。次の点をチェックします。 1. コントローラで SSH が有効になっていますか。 2. コントローラ の SSH ポート 22 は コネクタ から到達可能ですか。 3. 正しい SSH 読み取り/書き込みクレデンシャルを入力しましたか。
FAILED	SUCCESSFUL	接続テストに成功しました

PING のステータス	SSH クレデンシャルテストのステータス	表示されるテスト接続メッセージ
FAILED	FAILED	コントローラ に対する PING テストと SSH テストの両方に失敗しました。次の点をチェックします。 **1.** コネクタ とドメインコントローラの間で IP 接続が確立されていますか。 **2.** コントローラ で SNMP が有効になっていますか。 **3.** コントローラ の SNMP ポート 161 は コネクタ から到達可能ですか。 **4.** 正しい SNMP 読み取り/書き込みクレデンシャルを入力しましたか。

ステップ 10 [Save] をクリックし、[Close] をクリックします。

コネクタ Web UIの [Controller Channel] 領域に新しい コントローラ が表示されます。コネクタ に正常に接続された コントローラ がアクティブとして表示されます。コントローラ が [Active] になるまでに約 5 分かかります。ウィンドウを更新して、ステータスの変更を表示します。

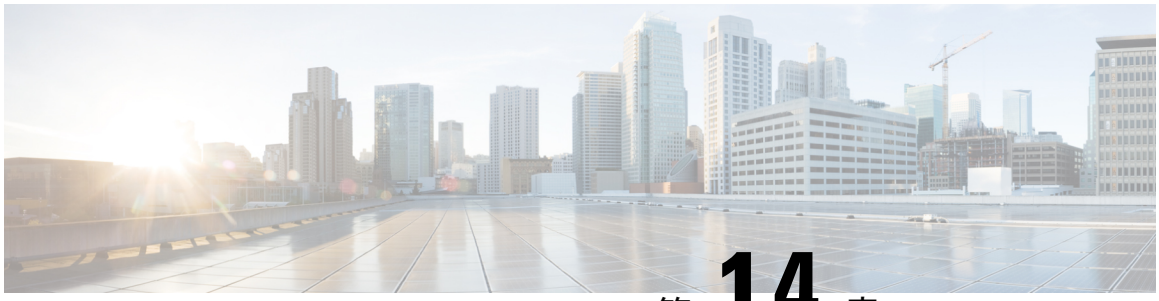
追加された コントローラ は、コネクタ の [Controller Channel] エリアにも表示されます。



1 つの コネクタ に複数の コントローラ を追加できます。

次のタスク

Cisco DNA Spaces ロケーション階層に追加された コントローラ をインポートできます。



第 14 章

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへのコネクタの接続

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ への コネクタ の接続

始める前に

- コネクタ OVA を展開し、Cisco DNA Spaces のトークンを使用してアクティブにします。
- Cisco DNA Spaces：コネクタ から到達可能な Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ の IP アドレス。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ CLIで、コンフィギュレーション モードを開始し、**aaa authorization exec default local** コマンドと **aaa authentication login default local** コマンドを使用して、ローカル認証で AAA を有効にします。

  IoT サービス を実行する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ CLIで **イネーブル**モードを開始し、次のコマンドを実行します。

  ```
  show run | sec  aaa
  ```

  表示された出力に含まれる **aaa authorization exec default** の設定を保存します。**設定**モードを開始して、ローカル認証の設定を既存の設定に追加します。

  たとえば、表示された出力が **aaa authorization exec default group dnac-network-tacacs-group** の場合、追加する設定は **aaa authorization exec default group dnac-network-tacacs-group local** です。この手順により、既存の設定が上書きされないようにすることができます。

.

手順の概要

1. Cisco DNA Spaces にログインします。
2. Cisco DNA Spaces ダッシュボードで、[Setup] > [Wireless Networks] の順に選択します。
3. ステップのリストを表示するには、それぞれのドロップダウン矢印を使用して、[Connector via Spaces Connector] エリアを展開します。
4. コネクタ から既存の コントローラ への接続をテストするには、[Step 3] エリアの [View Controllers] をクリックします。
5. 新しい コントローラ を追加するには、[Step 3] エリアの [Add Controllers] をクリックします。
6. [Connector] ドロップダウンリストから、コネクタ を選択します。
7. [Controller IP] アドレスと [Controller Name] を入力し、[Controller Type] ドロップダウンリストから [Catalyst WLC] を選択して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に接続します。
8. 次のいずれかを実行します。
   - [Netconf username]、[Netconf password]、および [Enable password] を入力します。この選択により、コネクタがNMSP ドロップから正常に回復し、必要に応じて新しい設定を コントローラ にプッシュできるようになります。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で**イネーブル**パスワードをまだ設定していない場合は、この手順での [Enable password] の設定をスキップできます。
   - [Catalyst WLC CLI commands] セクションの設定コマンドをコピーし、コントローラ コマンドライン インターフェイスで手動で実行します。
9. （任意） PING 機能と SSH 機能を実行して到達可能性とクレデンシャルをテストしてから、[Test Connectivity] をクリックします。[Test Connectivity] は、アクティブな コネクタ に対してのみ使用できます。
10. [Save] をクリックし、[Close] をクリックします。

手順の詳細

ステップ 1 Cisco DNA Spaces にログインします。

ステップ 2 Cisco DNA Spaces ダッシュボードで、[Setup] > [Wireless Networks] の順に選択します。

ステップ 3 ステップのリストを表示するには、それぞれのドロップダウン矢印を使用して、[Connector via Spaces Connector] エリアを展開します。

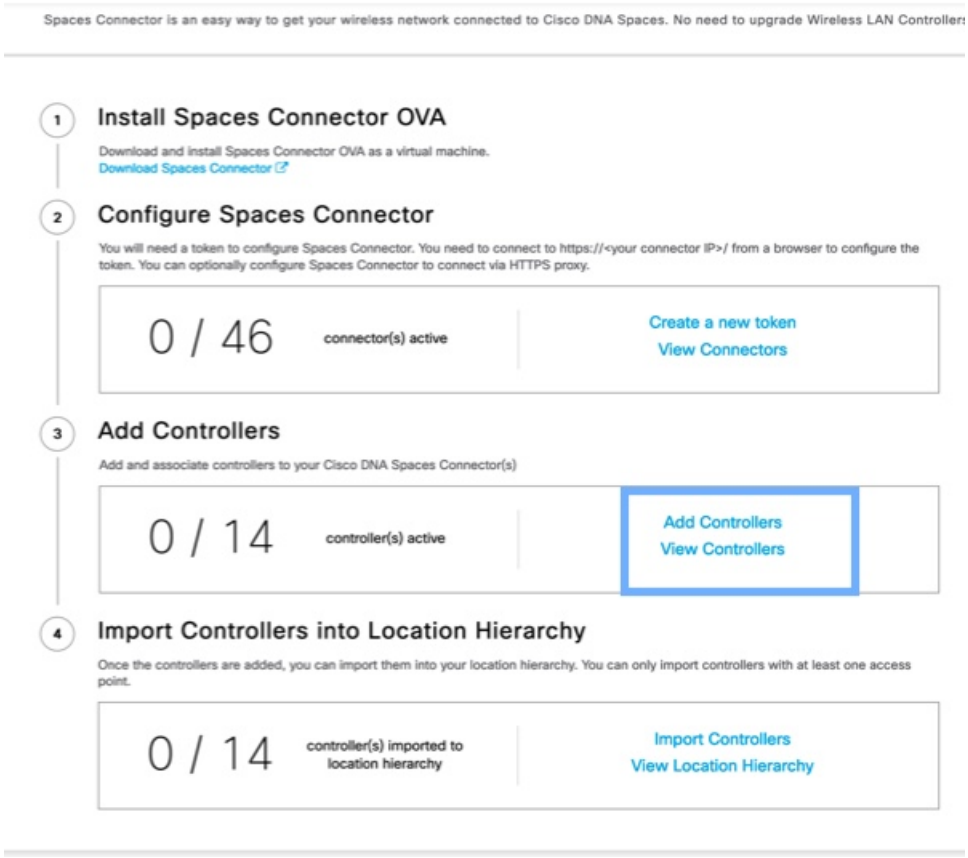
ステップ 4 コネクタ から既存の コントローラ への接続をテストするには、[Step 3] エリアの [View Controllers] をクリックします。

a) コントローラ を編集するには、鉛筆アイコンをクリックします。

b) [Connector] ドロップダウンリストからアクティブな コネクタ を選択して、[Test Connectivity] ボタンを有効にします。

c) ステップ 8 に進みます。

ステップ 5 新しい コントローラ を追加するには、[Step 3] エリアの [Add Controllers] をクリックします。



ステップ 6 [Connector] ドロップダウンリストから、コネクタ を選択します。

ステップ 7 [Controller IP] アドレスと [Controller Name] を入力し、[Controller Type] ドロップダウンリストから [Catalyst WLC] を選択して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ に接続します。

ステップ 8 次のいずれかを実行します。

- [Netconf username]、[Netconf password]、および [Enable password] を入力します。この選択により、コネクタ が NMSP ドロップから正常に回復し、必要に応じて新しい設定を コントローラにプッシュできるようになります。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ で**イネーブル**パスワードをまだ設定していない場合は、この手順での [Enable password] の設定をスキップできます。
- [Catalyst WLC CLI commands] セクションの設定コマンドをコピーし、コントローラ コマンドライン インターフェイスで手動で実行します。

ステップ 9 （任意） PING 機能と SSH 機能を実行して到達可能性とクレデンシャルをテストしてから、[Test Connectivity] をクリックします。[Test Connectivity] は、アクティブな コネクタ に対してのみ使用できます。

図 *41 : Catalyst WLC* コントローラの追加

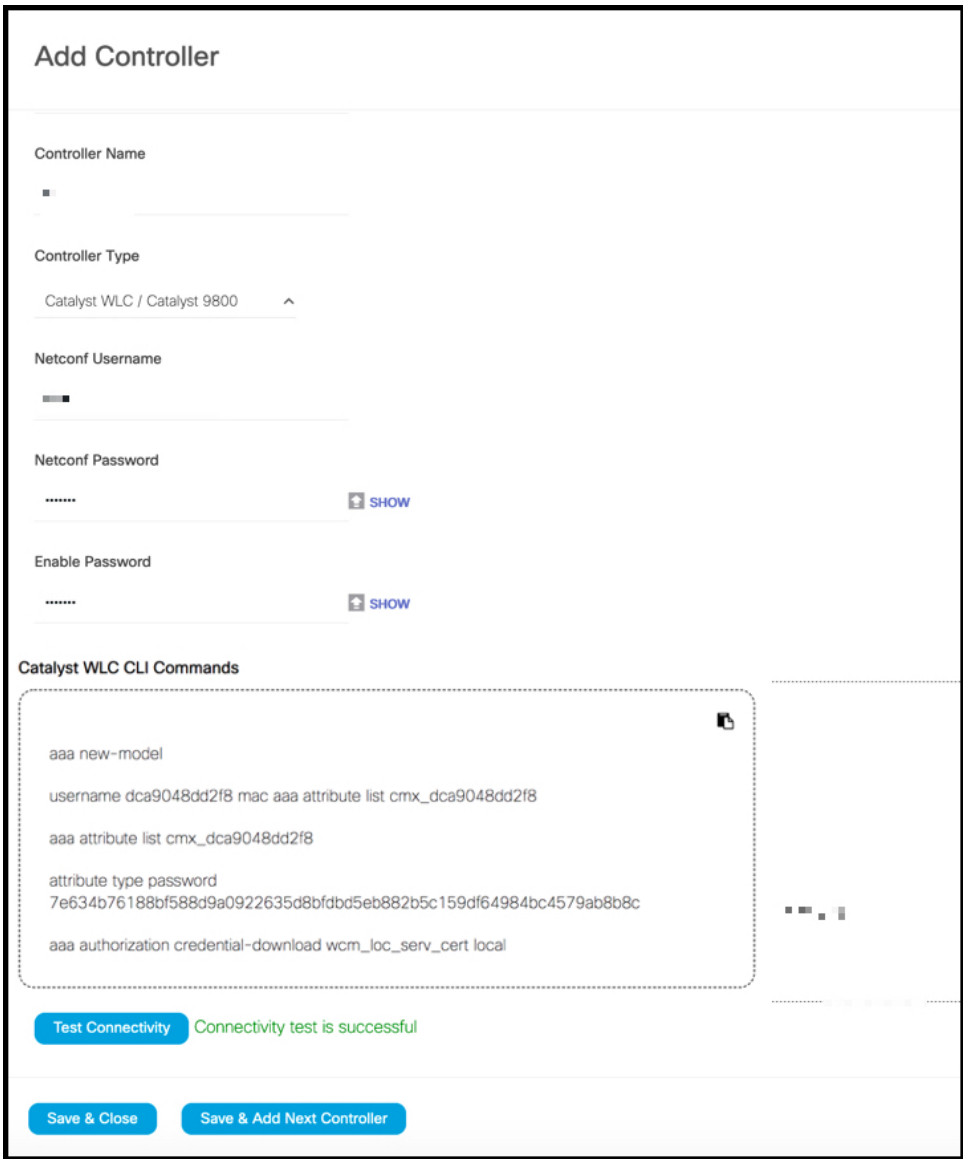


表 *5 :* エラーの説明

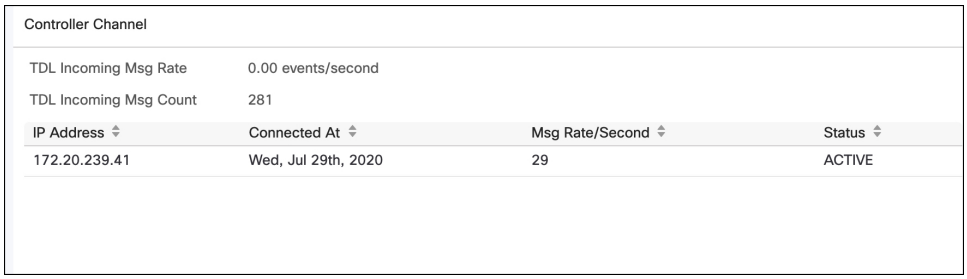
PING のステータス	**SSH** クレデンシャルテストのステータス	表示されるテスト接続メッセージ
SUCCESSFUL	SUCCESSFUL	接続テストに成功しました

PING のステータス	SSH クレデンシャルテストのステータス	表示されるテスト接続メッセージ
SUCCESSFUL	FAILED	コントローラ に対する PING テストに成功しました。しかしながら、SSH テストには失敗しました。次の点をチェックします。 **1.** コントローラで SSH が有効になっていますか。 **2.** コントローラ の SSH ポート 22 は コネクタ から到達可能ですか。 **3.** 正しい SSH 読み取り/書き込みクレデンシャルを入力しましたか。
FAILED	SUCCESSFUL	接続テストに成功しました
FAILED	FAILED	コントローラ に対する PING テストと SSH テストの両方に失敗しました。次の点をチェックします。 **1.** コネクタ とドメインコントローラの間で IP 接続が確立されていますか。 **2.** コントローラ で SSH が有効になっていますか。 **3.** コントローラ の SSH ポート 22 は コネクタ から到達可能ですか。 **4.** 正しい SSH クレデンシャルを入力しましたか。 **5.** AAA はローカル認証で有効になっていますか。 **6.** NMSP および SSH 接続用のワイヤレス管理インターフェイスではないインターフェイスを使用していますか。

ステップ 10 [Save] をクリックし、[Close] をクリックします。

コネクタ Web UIの [Controller Channel] 領域に新しい コントローラ が表示されます。コネクタに正常に接続されたコントローラがアクティブとして表示されます。コントローラが [Active] になるまでに約 5 分かかります。ウィンドウを更新して、ステータスの変更を表示します。

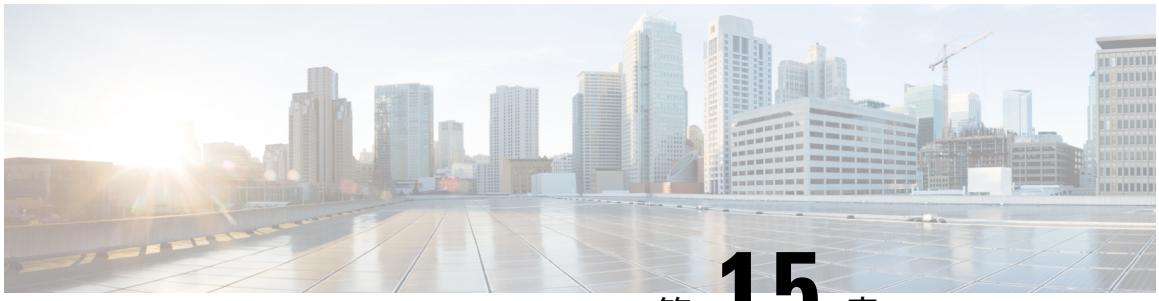
追加された コントローラ は、コネクタ の [Controller Channel] エリアにも表示されます。



1 つの コネクタ に複数の コントローラ を追加できます。

次のタスク

Cisco DNA Spaces ロケーション階層に追加された コントローラ をインポートできます。



第 15 章

Cisco Catalyst 9300/9400 シリーズ スイッチ シリーズへのコネクタの接続

Cisco Catalyst 9300/9400 シリーズ スイッチ への コネクタ の接続

始める前に

- コネクタ OVA を展開し、Cisco DNA Spaces のトークンを使用してアクティブにします。
- Cisco DNA Spaces：コネクタ から到達可能な Cisco Catalyst 9300/9400 シリーズ スイッチ の IP アドレス。
- Cisco Catalyst 9300/9400 シリーズ スイッチ で Netconf コマンドをテストします。

手順の概要

1. Cisco DNA Spaces にログインします。
2. Cisco DNA Spaces ダッシュボードで、[Setup] > [Wired Networks] の順に選択します。
3. [Step 3: Add Switches] エリアで、[Add Switch] をクリックします。
4. [Add Switches] ページで、コネクタ を選択し、スイッチを識別するための名前とスイッチ の IP アドレスを入力します。[Netconf username]、[Netconf password] を入力してから、チェックボックスをクリックして、スイッチでこれらのコマンドをテストしたことを確認します。
5. [Test] をクリックして、スイッチへの接続をテストします。
6. 次のいずれかを実行します。
   - [Save ＆ Add Next Switch] をクリックします。
   - [Save & Close] をクリックします。

手順の詳細

ステップ 1 Cisco DNA Spaces にログインします。

ステップ 2 Cisco DNA Spaces ダッシュボードで、[Setup] > [Wired Networks] の順に選択します。

ステップ 3 [Step 3: Add Switches] エリアで、[Add Switch] をクリックします。

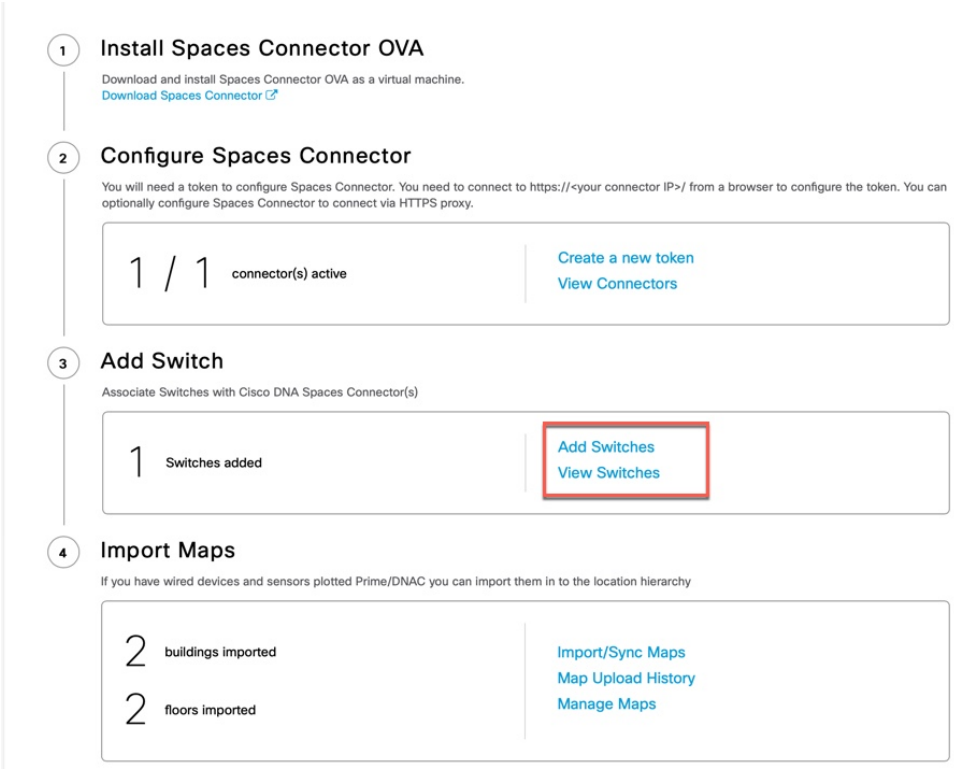


図 *42 :*

ステップ 4 [Add Switches] ページで、コネクタ を選択し、スイッチを識別するための名前とスイッチの IP アドレスを入力します。[Netconf username]、[Netconf password] を入力してから、チェックボックスをクリックして、スイッチでこれらのコマンドをテストしたことを確認します。

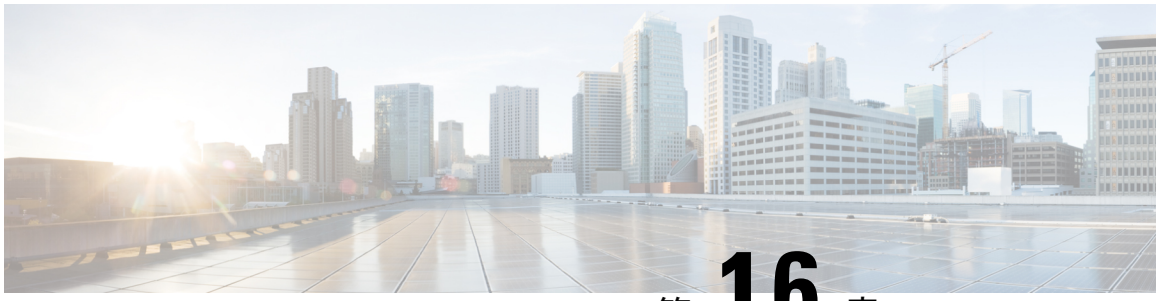
ステップ 5 [Test] をクリックして、スイッチへの接続をテストします。

ステップ 6 次のいずれかを実行します。

- [Save & Add Next Switch] をクリックします。
- [Save & Close] をクリックします。

第 IV 部

ロケーション階層



第 16 章

ロケーション階層

Cisco DNA Spaces ロケーション階層への シスコ ワイヤレス コントローラ のインポート

このタスクは、Cisco DNA Spaces へのロケーションのインポートにマップサービスを使用する場合は適用されません。『*Cisco DNA Spaces Configuration Guide*』の「Importing Locations to the Location Hierarchy Using Map Services」を参照してください。X/Y ロケーションの計算では、マップサービスを使用してマップをダウンロードする必要があります。

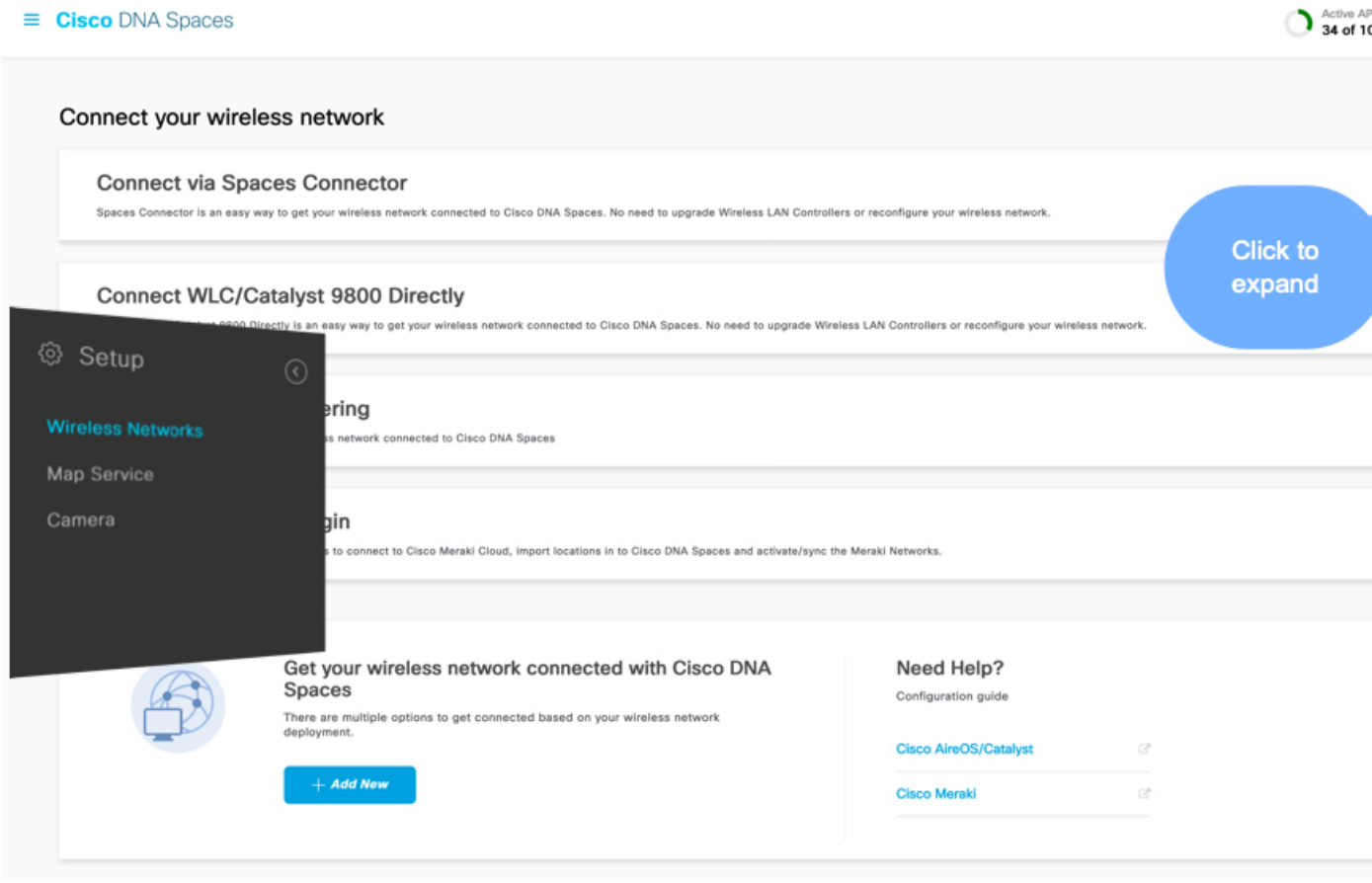
始める前に

- シスコ ワイヤレス コントローラ を Cisco DNA Spaces：コネクタ に接続します。「コネクタ から シスコ ワイヤレス コントローラ へ （83 ページ）」を参照してください
- 少なくとも 1 つのアクセスポイントが シスコ ワイヤレス コントローラ に接続されていることを確認します。

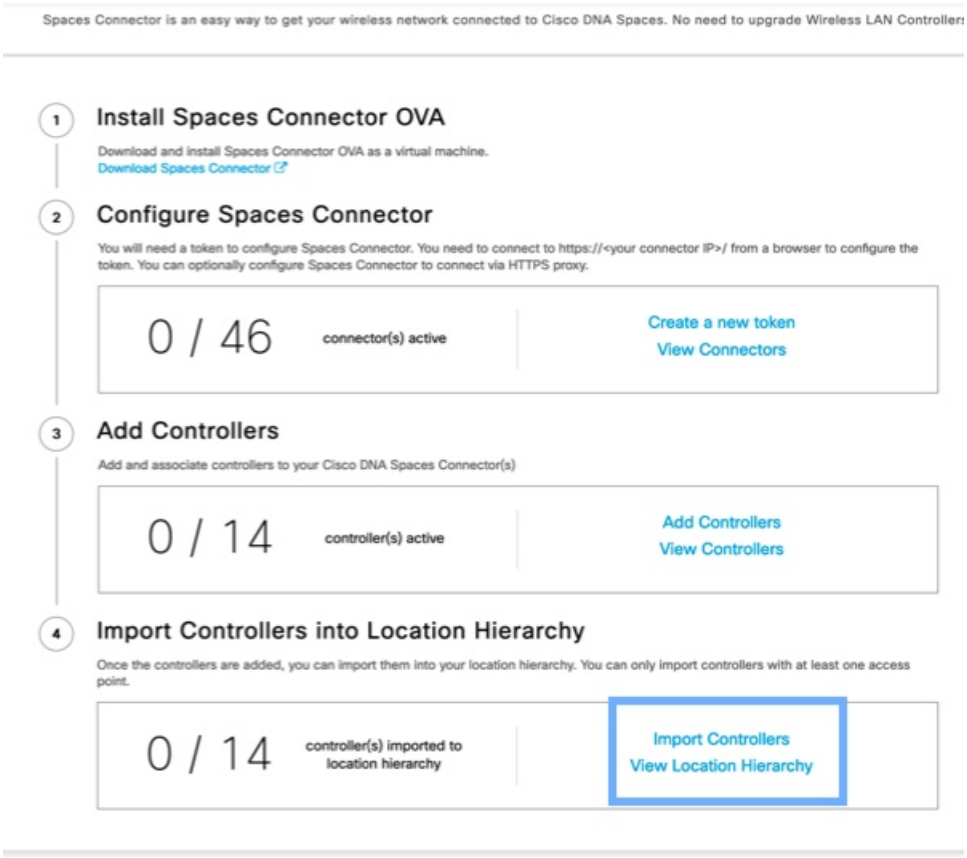
ステップ 1 Cisco DNA Spaces にログインします。

ステップ 2 左側のナビゲーションペインから、[Setup] > [Wireless Networks] の順に選択します。

ステップ 3 それぞれのドロップダウン矢印を使用して、[Connects by Spaces Connector] エリアを展開します。

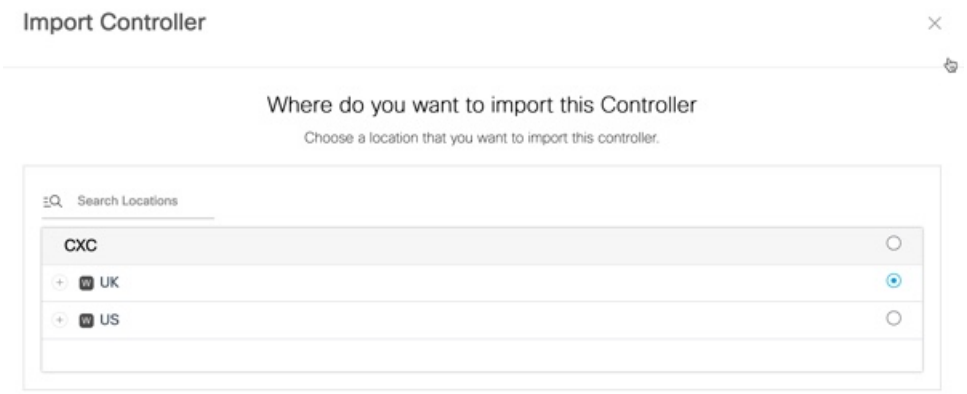


ステップ 4 表示される手順のリストで、4 番目の手順として記載されている [Import Controller] をクリックします。

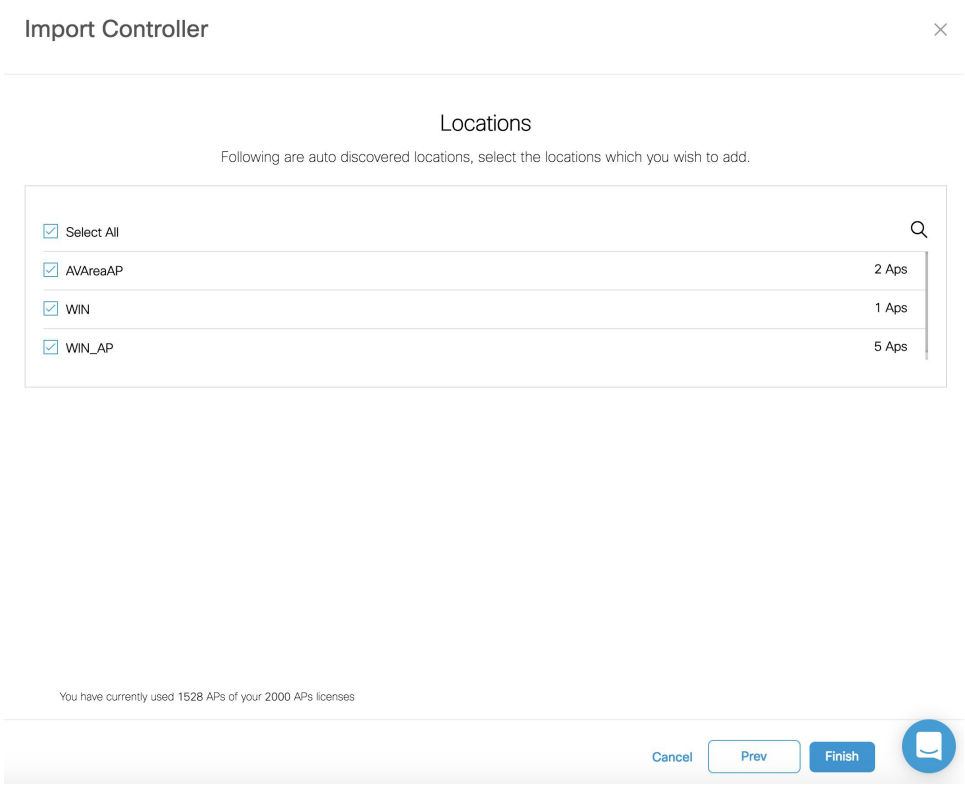


ロケーションおよび以前に追加されたコントローラのリストを表示できます。

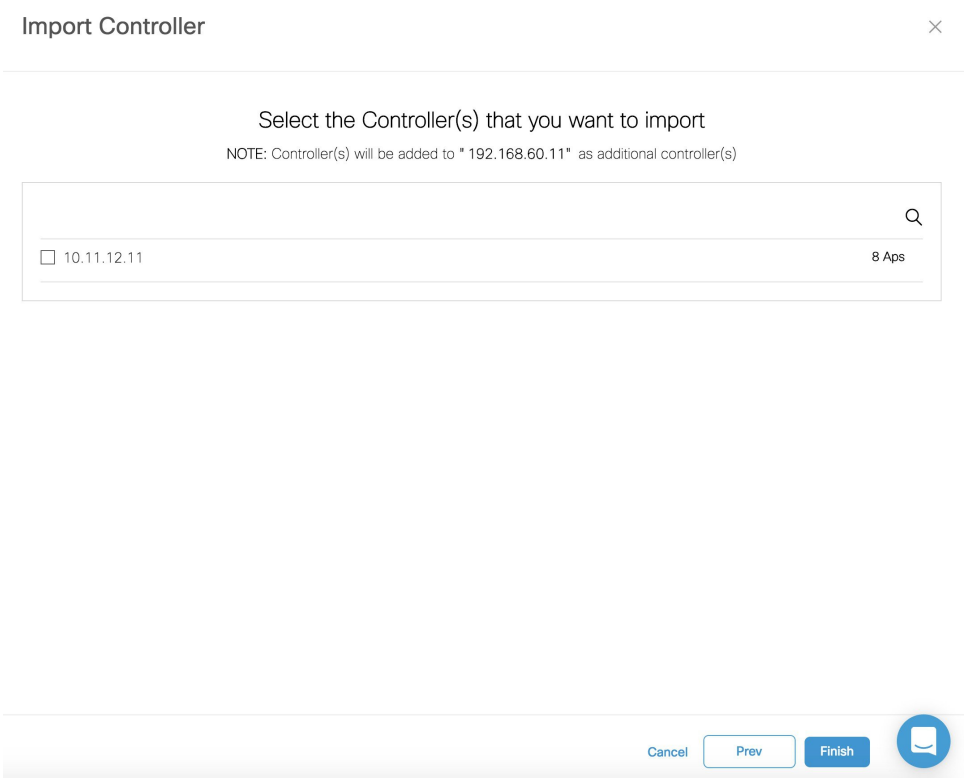
ステップ 5 コントローラをインポートするロケーションを選択します。



コントローラの AP が命名規則に基づいてネットワークとしてグループ化されている場合、それらのネットワーク名が表示されます。同じグループ構成を維持する場合は、ネットワークを選択します。AP がグループ化されていない場合、ネットワーク名は表示されません。



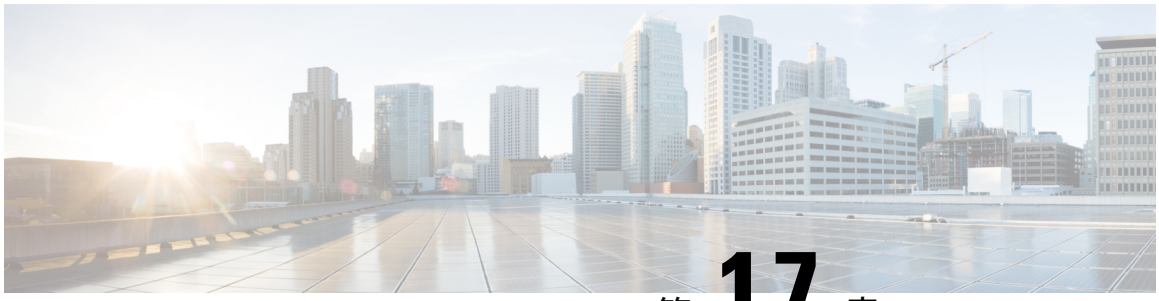
ステップ 6 インポートするコントローラを選択します。



ステップ 7 [Next] と [Finish] をクリックします。

第 V 部

プライバシー設定



第 17 章

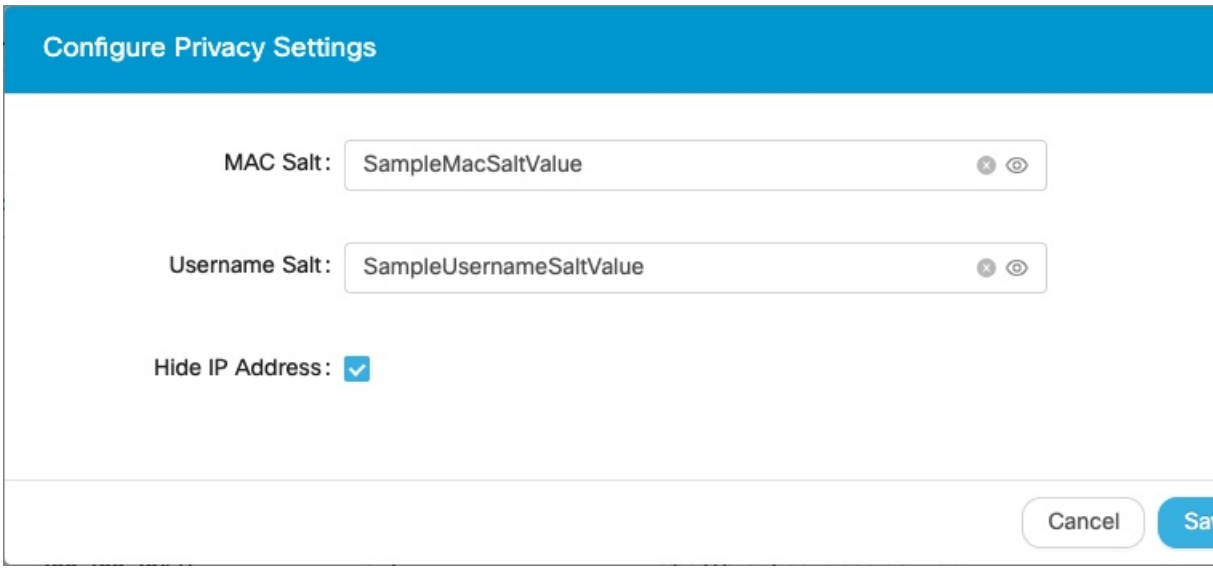
プライバシー設定の構成

プライバシー設定の構成：MAC およびユーザ名ソルト

Cisco DNA Spaces：コネクタ は、ユーザの個人 ID 情報（PII）を保護し、プライバシーを維持する方法を提供します。ハッシュアルゴリズムはユーザ入力（ソルトと呼ばれる）を取り込み、PII フィールドをマスクします。Cisco DNA Spaces がデータを受信すると、MAC アドレス、IP アドレス、またはユーザ名がマスクされ、実際のユーザ情報が保護されます。Cisco DNA Spaces：コネクタ リリース 2.3.2 以降、IP アドレスをマスクできます。

（注） このタスクはオプションです。

Cisco DNA Spaces：コネクタ GUI の [Privacy settings] を使用して、MAC ソルトとユーザ名ソルトを設定できます。



第 VI 部

HotSpot（OpenRoaming）

第 18 章

HotSpot（OpenRoaming）

HotSpot（OpenRoaming）

Cisco DNA Spaces：コネクタ が OpenRoaming プロトコルをサポートするようになりました。

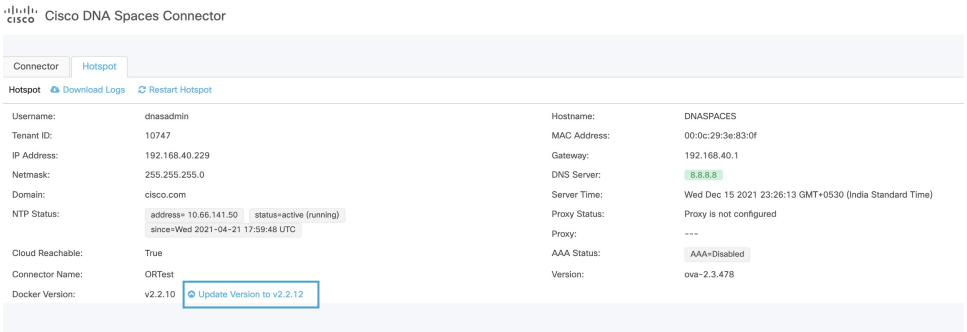
OpenRoaming は、アクセスプロバイダー（公共施設、小売業者、空港、大企業など）と ID プロバイダー（サービス プロバイダー キャリア、デバイス、クラウドプロバイダーなど）を関連付けることで、手間のかからないスムーズなゲスト Wi-Fi オンボーディング エクスペリエンスをモバイルユーザに提供します。

OpenRoaming により、ユーザは、信頼できる ID プロバイダーを使用して一度サインインするだけで、自動的かつシームレスにオンライン接続できます。このサービスは十分にセキュアで高速です。

OpenRoaming 設定の詳細な手順については、『Cisco Wireless Controller and Cisco DNA Spaces Setup Guide』の「Open Roaming configuration」を参照してください。

OpenRoaming を設定すると、コネクタ に [Hotspot] タブが表示されます。

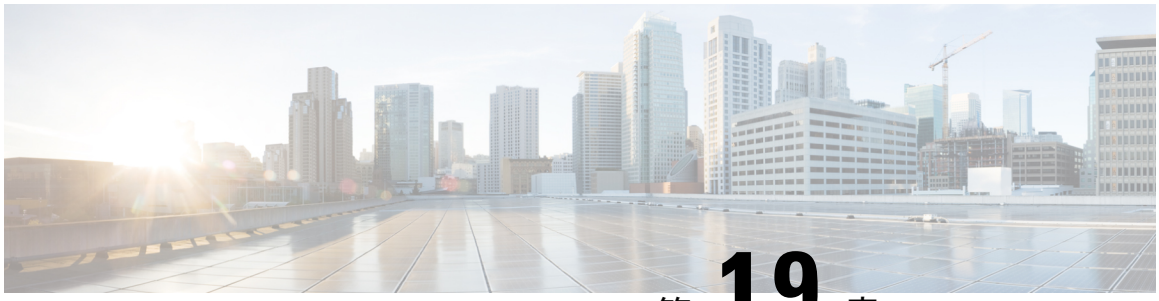
図 *43 : [Hotspot]* タブ



HotSpot（OpenRoaming）

第 VII 部

AAA



第 19 章

AAA の設定

AAA の概要

Cisco DNA Spaces：コネクタ 認証をリモートの認証、許可、アカウンティング（AAA）サーバに転送できるようになりました（ローカル認証をバイパスできます）。コマンドラインを使用して AAA を設定できます。AAA 認証ユーザは、**dnasadmin** ユーザと同じアクセス権で コネクタ Web UI にアクセスできます。コネクタ で AAA をアクティブにすると、**dnasadmin** ユーザを使用して コネクタ にログインできなくなります。

（注） 次のシナリオでは、**dnasadmin** ユーザを使用して Web UI にアクセスできます。

- AAA を誤って設定した場合。
- AAA サーバに到達できない場合。

（注） CSCvt29826 の場合、IPSec を使用する AAA は、**connectorctl generatecert** コマンドを使用して生成される、キータイプが楕円曲線デジタル署名アルゴリズム（ECDSA）の コネクタ で生成される証明書と互換性がありません。

コネクタ と AAA サーバ間の通信は、『Remote Authentication Dial In User Service (RADIUS)』を経由します。

IPSec プロトコルを使用した UDP トラフィックの暗号化を選択できます。サポートされている IPSec 認証タイプは、**Pubkey** と **PSK** です。

Pubkey 認証タイプの場合は、AAA サーバの CA 証明書ファイルを指定します（PEM 形式）。

PSK 認証タイプの場合は、PSK を自動生成するか、AAA サーバで設定された PSK を提供するかを選択します。

AAA の設定

始める前に

- Pubkey 認証タイプを使用して IP セキュリティを有効にするには、AAA サーバの CA 証明書を `/home/dnasadmin` ディレクトリにコピーし、証明書の名前を **radiusca.pem** に変更します。

手順の概要

1. **connectorctl aaa enable**
2. **connectorctl aaa edit**
3. コネクタ Web UI で、[AAA Status] フィールドの AAA ステータスを確認します。

手順の詳細

ステップ 1 **connectorctl aaa enable**

例：

```
[cmxadmin@cmxnew-01 ~]$ connectorctl aaa enable
Do you want to configure AAA Server? [yes/no] [yes]:
Enter AAA Server Host IP : 10.22.244.114
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [n]:

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
[cmxadmin@cmxnew-01 ~]$
```

AAA をイネーブルにします。

ステップ 2 **connectorctl aaa edit**

例：

この例では、Pubkey 認証タイプを使用して AAA を設定します。

例：

```
[cmxadmin@cmxnew-01 ~]$ connectorctl aaa edit
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [n]: y
Enter AAA Server's DNS name : aaa-srv-01
Select IPSec Auth Type: (pubkey/psk) [pubkey]:
```

```
AAA Server's CA Certificate file : radiusca.pem

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[1]: ESTABLISHED 0 seconds ago, 10.22.244.100[cmxnew-01]...10.22.244.114[aaa-srv-01]
         aaa{1}:  INSTALLED, TUNNEL, reqid 1, ESP SPIs: c6c620cb_i c06dcc78_o
         aaa{1}:   10.22.244.100/32 === 10.22.244.114/32
```

例：

この例では、RADIUS サーバから PSK 値を提供する PSK 認証タイプの IP セキュリティを使用して、AAA を設定します。

```
[cmxadmin@cmxnew-01 ~]$ connectorctl aaa edit
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [y]:
Enter AAA Server's DNS name  [aaa-srv-01]:
Select IPSec Auth Type: (pubkey/psk) [pubkey]: psk
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ? [a]: p
Enter PSK from Radius Server : 7dBoZXAkhadFMsyJ8e9HsBxdajnUPcxS

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (1 up, 0 connecting):
         aaa[1]: ESTABLISHED 1 second ago, 10.22.244.100[cmxnew-01]...10.22.244.114[aaa-srv-01]
         aaa{1}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c59d3960_i cf338432_o
         aaa{1}:   10.22.244.100/32 === 10.22.244.114/32
         aaa{2}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: c75d414b_i c7e495e2_o
         aaa{2}:   10.22.244.100/32 === 10.22.244.114/32
```

例：

この例では、PSA 認証タイプによる IP セキュリティを使用して AAA を設定し、新しい PSK 値を自動生成します。

```
[cmxadmin@connector-01 ~]$ connectorctl aaa edit
[cmxadmin@connector-01 ~]$ connectorctl aaa edit
Do you want to CHANGE AAA Server settings? [yes/no] [yes]:
Enter AAA Server Host IP  [10.22.244.114]:
Enter AAA Server Port  [1812]:
Enter AAA Server's shared secret key :
Repeat for confirmation:
Do you want to enable IPSec? (y/n) [y]:
Enter AAA Server's DNS name  [aaa-srv-01]:
Select IPSec Auth Type: (pubkey/psk) [psk]:
Do you want to auto-generate ('a') OR provide ('p') PSK from Radius Server ? [a]: a
Generated PSK value = 3AhBgueQQ6YBkKMwqIr6jyxIuG9ekw8g

AAA Server configured successfully
Connection to AAA Server Successful. AAA Settings are correct.
IPSec is Enabled
IPSec Status:
Security Associations (0 up, 0 connecting):
  no match
```

IP セキュリティステータスは、IP セキュリティトンネルがまだ正常に確立されていないことを示唆するゼロ セキュリティ アソシエーションを示します。数秒後に **connectorctl aaa show** コマンドを使用して PSK 値を比較し、同じ点を確認することができます。

```
[cmxadmin@connector-01 ~]$ connectorctl aaa show
AAA Server is Enabled
AAA Server IP: 10.22.244.114
AAA Server Port: 1812
Shared Secret: **<<masked>>**

IPSec is Enabled
AAA Server DNS: aaa-srv-01
IPSec Auth type: psk
IPSec PSK: 3AhBgueQQ6YBkKMwqIr6jyxIuG9ekw8g
IPSec Status:
Security Associations (1 up, 0 connecting):
        aaa[3]: ESTABLISHED 20 seconds ago, 10.22.244.100[connector-01]...10.22.244.114[aaa-srv-01]

         aaa{3}:  INSTALLED, TRANSPORT, reqid 1, ESP SPIs: ca4688d1_i c24be7d9_o
         aaa{3}:   10.22.244.100/32 === 10.22.244.114/32
Connection to AAA Server Successful. AAA Settings are correct.
```

既存の AAA 設定を編集します。

ステップ 3 コネクタ Web UI で、[AAA Status] フィールドの AAA ステータスを確認します。

図 *44 : IP* セキュリティと *PubKey* を使用した *AAA* の有効化

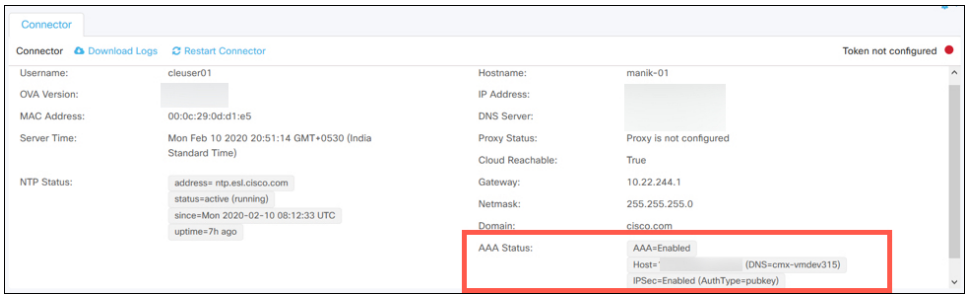
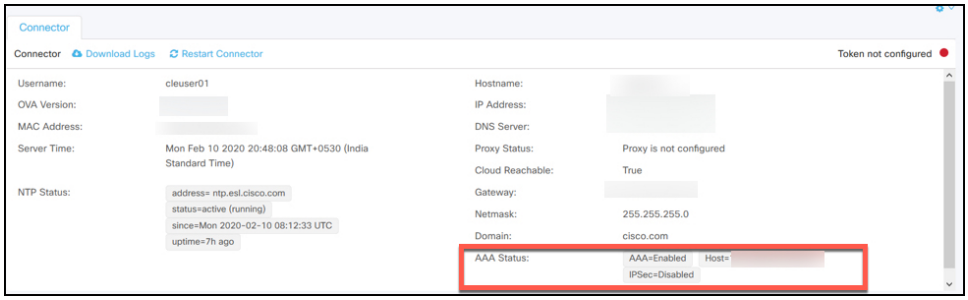


図 *45 : IP* セキュリティなしでの *AAA* の有効化



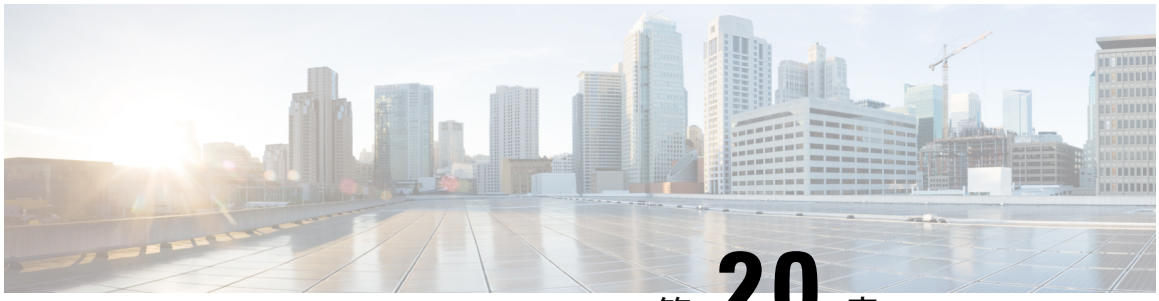
AAA が有効になっています。

次のタスク

connectorctl aaa disable コマンドを使用して、AAA を無効にすることができます。IPSec が有効になっている場合は、**connectorctl aaa restart** コマンドを使用して、必要に応じて IPSec トンネルを再起動することを選択できます。

第 VIII 部

アクティブ/アクティブでのコネクタ



第 20 章

アクティブ/アクティブでのコネクタ

コネクタのアクティブ/アクティブ

アクティブ/アクティブモードで 2 つの Cisco DNA Spaces：コネクタ をペアにして、Cisco DNA Spaces へのデータ中断のないフローを有効にすることができます。

1. Cisco DNA Spaces からトークンを取得し、2 つの異なる コネクタ でトークンを設定します。それぞれの コネクタ に一意の IP アドレスが必要です。
2. 両方の コネクタ が Cisco DNA Spaces から設定を受信します。
3. その後 コネクタ は、デバイスに接続して Cisco DNA Spaces にデータを送り返すことができます。
4. Cisco DNA Spaces が冗長データを管理します。
5. 一方の コネクタ がダウンした場合、もう一方の コネクタ が引き続きデータを送信します。

機能制限

- Cisco DNA Spaces ダッシュボードでは、2 つの コネクタ をアクティブ/アクティブペアにするための設定は必要ありません。
- 両方の コネクタ がすべての コントローラ に接続し、Cisco DNA Spaces にトラフィックを送信します。そのため、コントローラ から Cisco DNA Spaces へのトラフィックが増加します。

- アクティブ/アクティブ コネクタ ペアにするには、2 つの コネクタ で OVA バージョン 2.3 以降を実行する必要があります。
- FastLocate、HyperLocation、および IoT サービス のフェールオーバーサポートはありません。フェールオーバー後にこれらのサービスを再プロビジョニングします。
- CSCvv38762 の場合、IoT サービス のフェールオーバーサポートはありません。フェールオーバー後にこれらのサービスを再プロビジョニングします。
- コネクタ アクティブ/アクティブ機能のモニタリングはサポートされていません。
- CSCvv34216 の場合、コネクタ アクティブ/アクティブペアの一方の コネクタ のみが [Controller Channel] を管理し、他方の コネクタ が [AP Channel] を管理します。

図 *46 :* コネクタ は *[Controller Channel]* のみを管理します。*[AP Channel]* の統計情報はゼロになります。

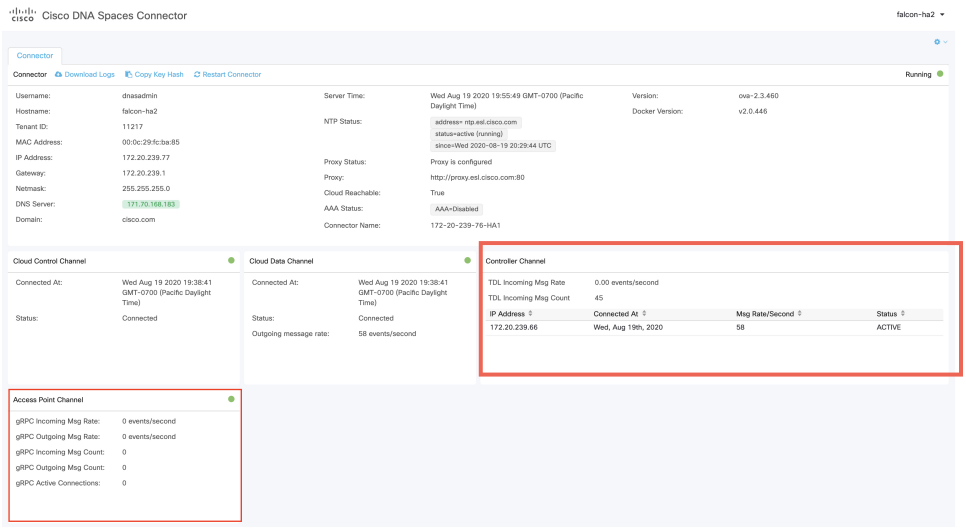
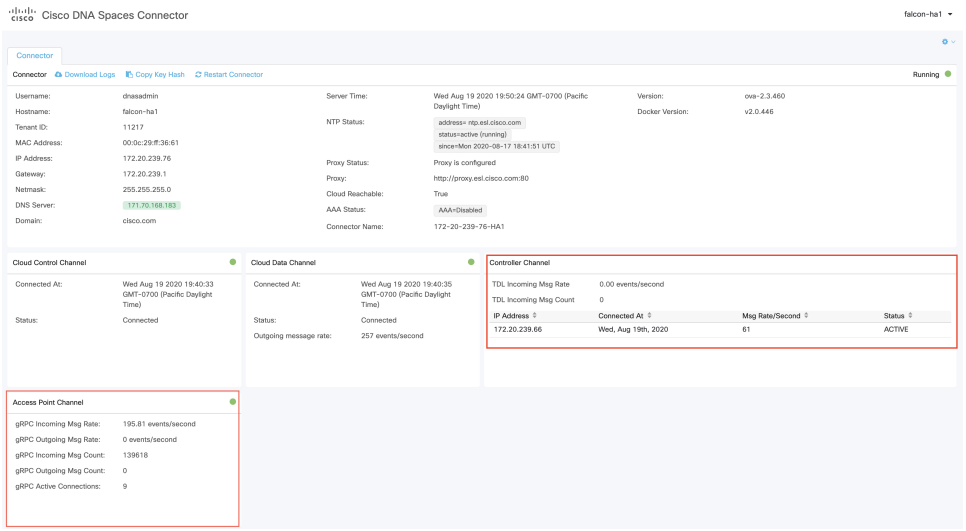


図 *47 :* コネクタ は *[AP Channel]* のみを管理します。*[Controller Channel]* の統計情報はゼロになります。



コネクタアクティブ/アクティブと Cisco CMX 高可用性の比較

コネクタアクティブ/アクティブ機能は、従来の高可用性に類似しています。ただし、仮想 IP アドレス、プライマリ、セカンダリなどの高可用性の概念は、この機能には実装されていません。次に、コネクタアクティブ/アクティブ機能と Cisco CMX の高可用性機能の比較を示します。

表 *6 :* コネクタアクティブ/アクティブ（高可用性）モデル

	コネクタ アクティブ/アクティブ **IoT サービスアプリケーション、アプリケーションの検出と位置特定**	**Cisco CMX レイヤ 2 VIP 高可用性**
IP アドレッシング	両方の コネクタ に一意の IP アドレスが設定されます。	2 つの Cisco CMX デバイスが単一の IP アドレスで設定されます。
動作状態	両方の コネクタ がアクティブ状態に設定されます。	1 つの Cisco CMX はホットプライマリで、もう 1 つはコールドスタンバイです。
フェールオーバー前のデータ	両方の コネクタ に同じデータセットがあり、Cisco DNA Spaces がデータ冗長性の管理を担当します。	ホットプライマリとコールドスタンバイの両方が同じデータセットを保持します。
フェールオーバーのサポート	障害が発生した場合は、FastLocate、HyperLocation、および IoT サービスを再プロビジョニングする必要があります。	ホットプライマリに障害が発生すると、コールドスタンバイがシームレスに引き継ぎます。
バージョン制限	コネクタ アクティブ/アクティブペアには、2.3 以降の同じ OVA バージョンが必要です。	高可用性を実現するため、Cisco CMX と同じバージョンを推奨します。

アクティブ/アクティブでのコネクタの設定

このタスクでは、2 つの コネクタ をアクティブ/アクティブとして設定する方法を示します。

始める前に

OVA バージョン 2.3 以降の 2 つの異なる Cisco DNA Spaces：コネクタ をインストールします。それぞれの コネクタ に一意の IP アドレスを設定します。

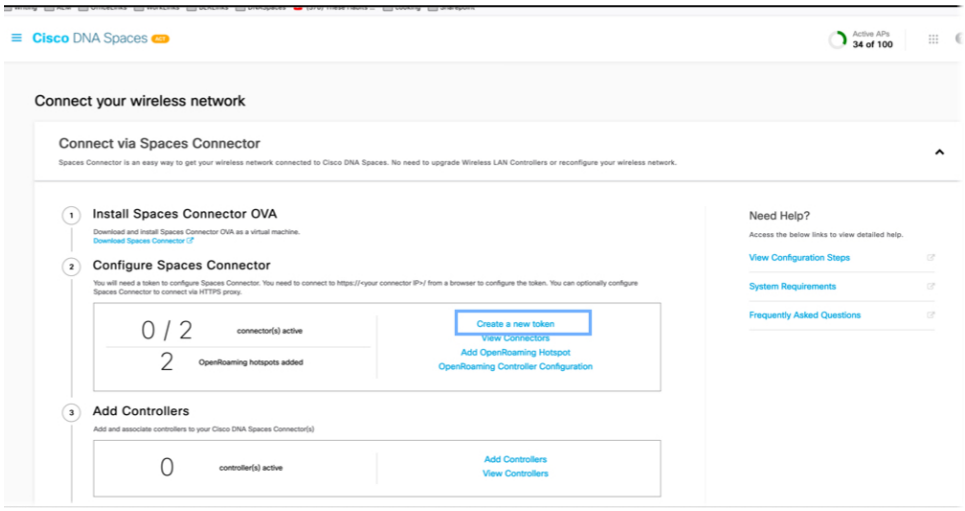
手順の概要

1. [Cisco DNA Spaces] > [Setup] > [Wireless Networks] にログインし、[Configure Spaces Connector] エリアで [Create a new token] をクリックします。
2. コネクタ の名前を入力し、[Generate Token] をクリックします。表示されたトークンをコピーし、後で参照できるように保存します。
3. 最初の コネクタ にログインし、保存されたトークンを設定します。
4. 2 番目の コネクタ にログインし、保存されたトークンを設定します。
5. それぞれの コネクタ で、テナント ID の値が同じであることを確認します。
6. Cisco DNA Spaces ダッシュボードで、両方の コネクタ IPアドレスを確認します。
7. それぞれの コネクタ で、追加されたすべての コントローラ が存在することを確認します。
8. コントローラ CLI で、すべての コネクタ が NMSP 状態であることを確認します。

手順の詳細

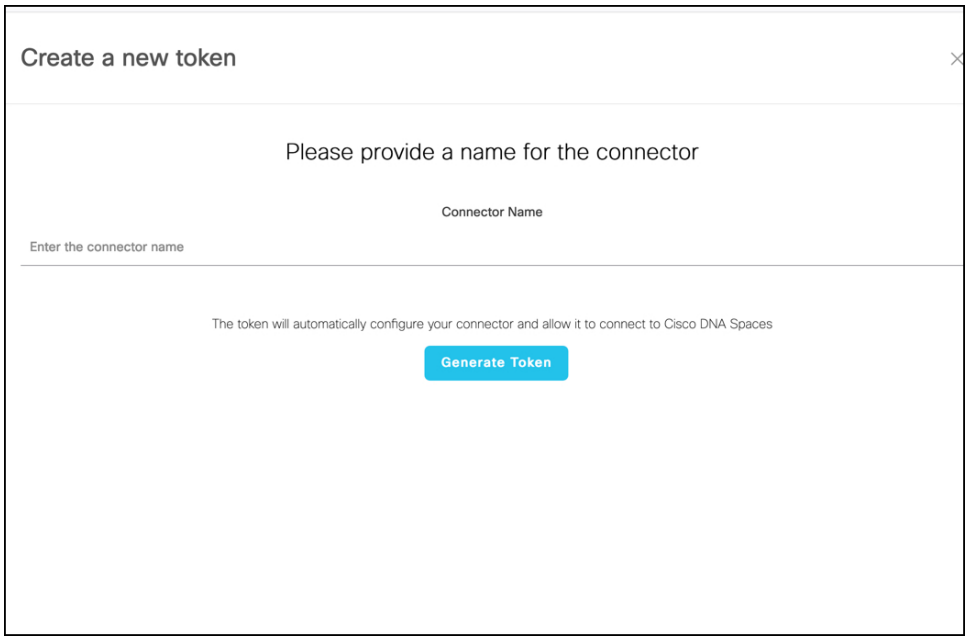
ステップ 1 [Cisco DNA Spaces] > [Setup] > [Wireless Networks] にログインし、[Configure Spaces Connector] エリアで [Create a new token] をクリックします。

図 *48 :* 新しいトークンの作成



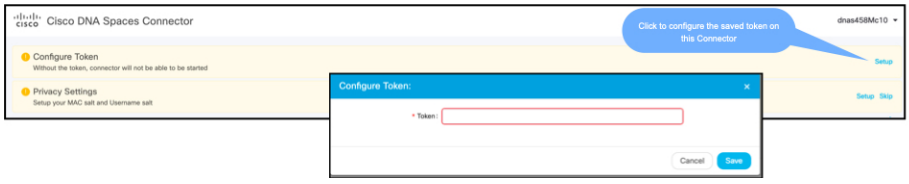
ステップ 2 コネクタ の名前を入力し、[Generate Token] をクリックします。表示されたトークンをコピーし、後で参照できるように保存します。

図 *49 : Connector Name*



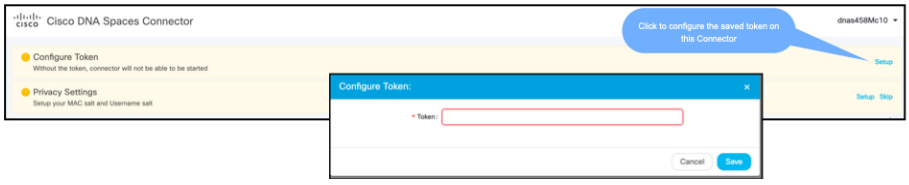
ステップ 3 最初の コネクタ にログインし、保存されたトークンを設定します。

図 *50 : Connector Name*



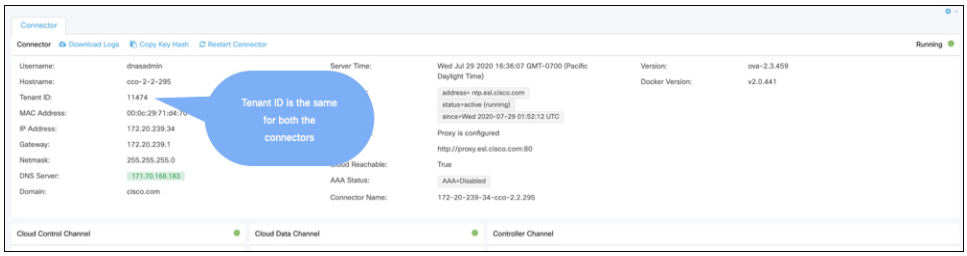
ステップ 4 2 番目の コネクタ にログインし、保存されたトークンを設定します。

図 *51 :* コネクタ *Name*



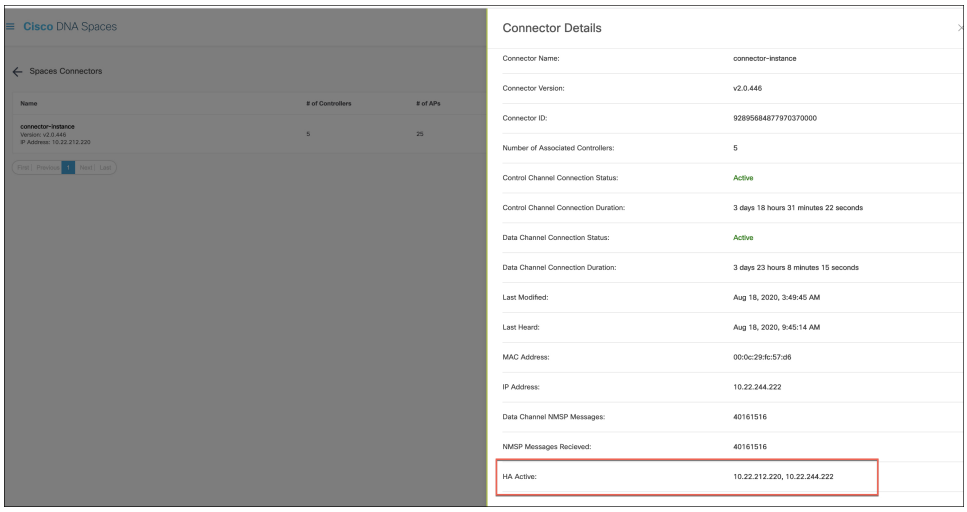
ステップ 5 それぞれの コネクタ で、テナント ID の値が同じであることを確認します。

図 *52 :* コネクタ



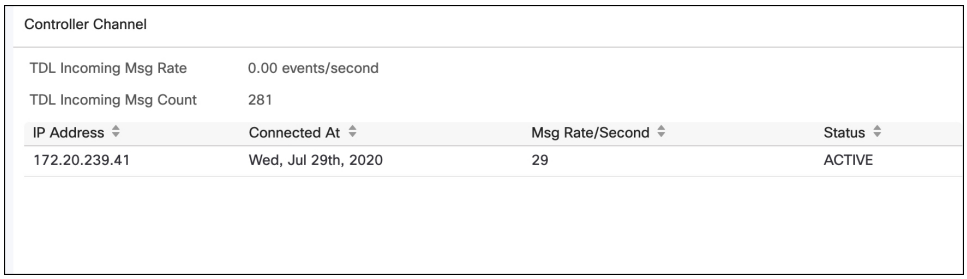
ステップ 6 Cisco DNA Spaces ダッシュボードで、両方の コネクタ IPアドレスを確認します。

図 *53 : Cisco DNA Spaces* ダッシュボード



ステップ 7 それぞれの コネクタ で、追加されたすべての コントローラ が存在することを確認します。

図 *54 :* コネクタ：*[Controller Channel]* エリア



ステップ 8 コントローラ CLI で、すべての コネクタ が NMSP 状態であることを確認します。

図 *55 :* コントローラ コマンドの出力

```
show nmsp status

NMSP Status
-----------
```

```
DNA Spaces/CMX IP Address                          Active    Tx Echo Resp  Rx Echo Req   Tx Data
   Rx Data     Transport
-------------------------------------------------------------------------------------------------------------
10.x.212.xxx                          Inactive  13            13            161         6
   TLS
10.x.212.xxx                          Inactive  0             0             17          6
   TLS
10.x.212.xxx                          Active    45070         45070         1378446     574
   TLS
10.x.244.xx                           Inactive  7             7             79          6
   TLS
10.x.244.xx                           Active    56111         56111         1714241     286
   TLS
10.x.244.xx                           Inactive  7             7             104         6
   TLS
10.x.244.xxx                          Active    23056         23056         683908      298
   TLS
```

アクティブ/アクティブでのコネクタの設定（有線）

このタスクでは、2 つの コネクタ をアクティブ/アクティブとして設定する方法を示します。

始める前に

OVA バージョン 2.3 以降の 2 つの異なる Cisco DNA Spaces：コネクタ をインストールします。それぞれの コネクタ に一意の IP アドレスを設定します。

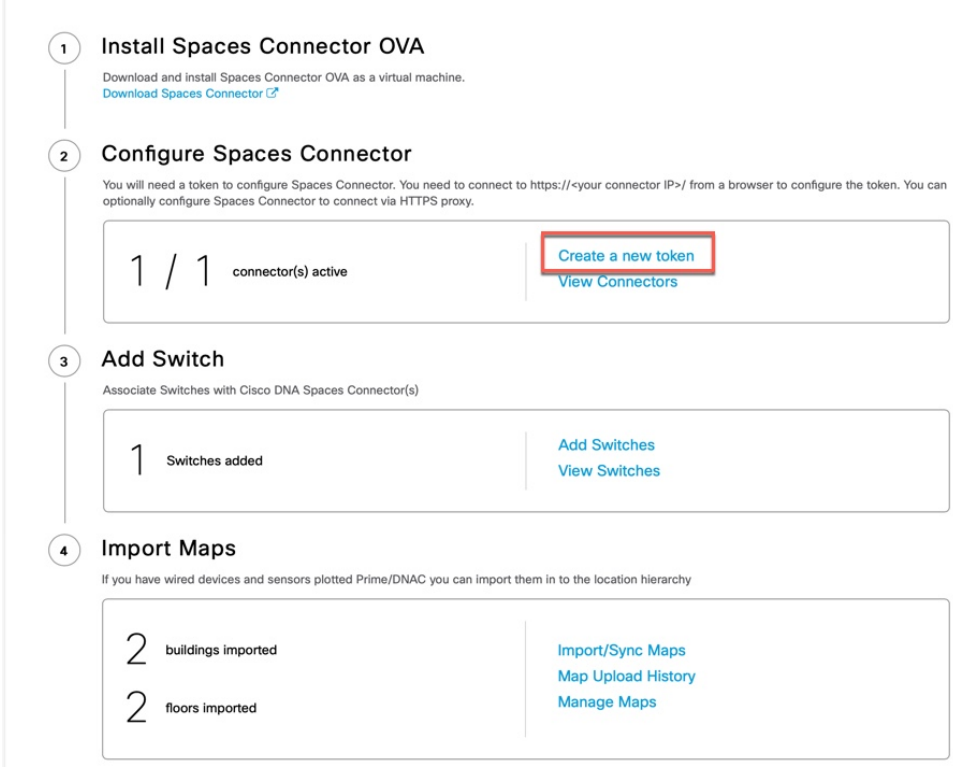
手順の概要

1. [Cisco DNA Spaces] > [Setup] > [Wired Networks] にログインし、[Configure Spaces Connector] エリアで [Create a new token] をクリックします。
2. コネクタ の名前を入力し、[Generate Token] をクリックします。表示されたトークンをコピーし、後で参照できるように保存します。
3. 最初の コネクタ にログインし、保存されたトークンを設定します。
4. 2 番目の コネクタ にログインし、保存されたトークンを設定します。
5. それぞれの コネクタ で、テナント ID の値が同じであることを確認します。
6. Cisco DNA Spaces ダッシュボードで、両方の コネクタ IPアドレスを確認します。
7. それぞれの コネクタ で、追加されたすべての コネクタ が存在することを確認します。

手順の詳細

ステップ 1 [Cisco DNA Spaces] > [Setup] > [Wired Networks] にログインし、[Configure Spaces Connector] エリアで [Create a new token] をクリックします。

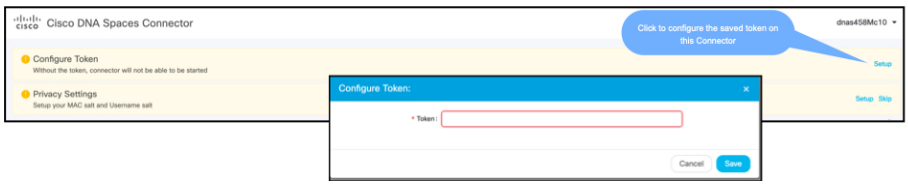
図 *56* : 新しいトークンの作成



ステップ 2 コネクタの名前を入力し、[Generate Token] をクリックします。表示されたトークンをコピーし、後で参照できるように保存します。

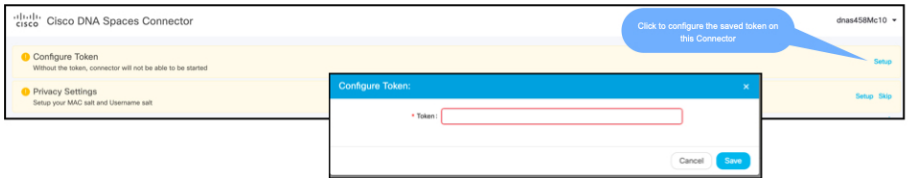
ステップ 3 最初の コネクタ にログインし、保存されたトークンを設定します。

図 *57 : Connector Name*



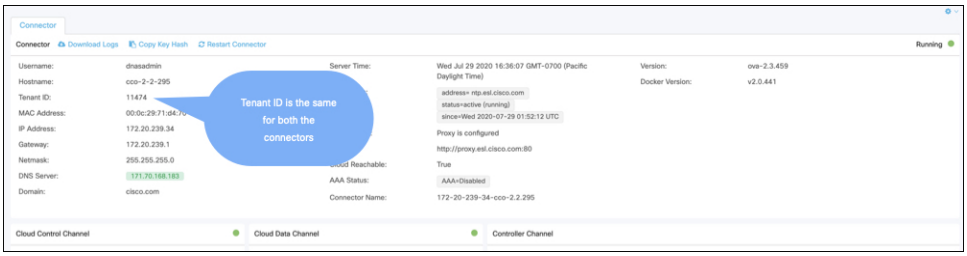
ステップ 4 2 番目の コネクタ にログインし、保存されたトークンを設定します。

図 *58 :* コネクタ *Name*



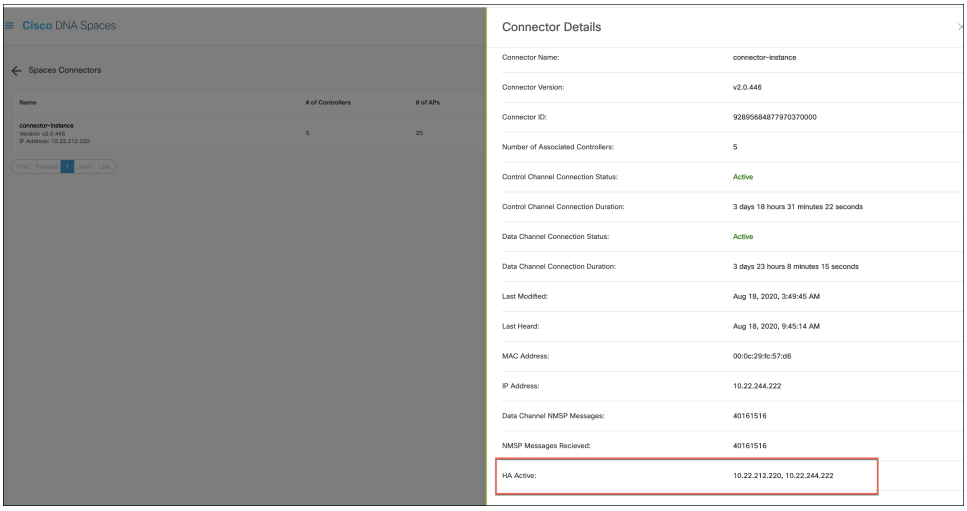
ステップ 5 それぞれの コネクタ で、テナント ID の値が同じであることを確認します。

図 *59* : コネクタ



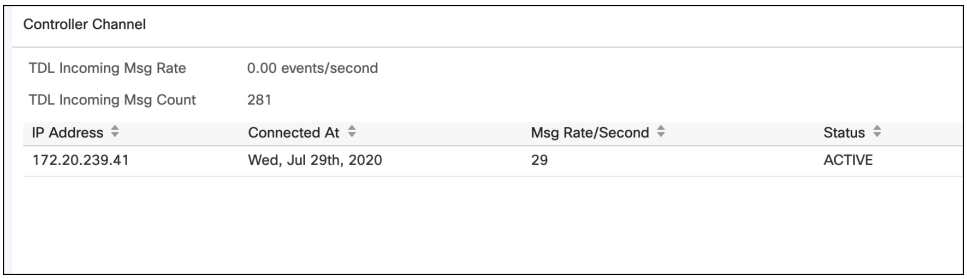
ステップ 6 Cisco DNA Spaces ダッシュボードで、両方の コネクタ IPアドレスを確認します。

図 *60* : *Cisco DNA Spaces* ダッシュボード



ステップ 7 それぞれの コネクタ で、追加されたすべての コネクタ が存在することを確認します。

図 *61* : コネクタ：*[Controller Channel]* エリア



第 IX 部

通信、サービス、およびその他の情報

第 21 章

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、シスコ サービスにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

Cisco バグ検索ツール

シスコバグ検索ツール（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

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