Cisco Catalyst 9800-CL Cloud ワイヤレスコントローラ 設置ガイド

初版：2018 年 11 月 20 日

最終更新：2021 年 8 月 2 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

ここでは、本ガイドについて説明し、本ガイドで使用されている表記規則に関する情報と関連ドキュメントに関する詳細を示します。内容は次のとおりです。

マニュアルの変更履歴

次の表に、このマニュアルの変更履歴を示します。

日付	変更点
2018 年 11 月	このマニュアルの最初のバージョンです。
2019 年 7 月	Google Cloud Platform（GCP）のサポートに関する情報を追加しました。
2020 年 2 月	Microsoft Hyper-V のサポートに関する情報を追加しました。

本書の目的

このドキュメントでは のインストールについて説明します。

対象読者

このドキュメントは、主に、のインストール、メンテナンス、およびトラブルシューティングの担当者向けに設計されています。このマニュアルを使用するには、次の条件を満たす必要があります。

- 電子回路および配線手順を熟知している。
- 電子または電子機械の技術者として働いた経験がある。
- ハイエンドのネットワーキング機器を導入した経験がある。

（注） このガイドには、認定電気技術者が行う手順も一部含まれています。

表記法

テキストのタイプ	説明
ユーザ入力	表示どおりにユーザが入力するテキストやユーザが押すキーは、このフォント（例：this font）で示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、**courier** フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体（**this font** ）で示しています。 CLI コマンド内の変数は、イタリック体（*this font* ）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。

テキストのタイプ	説明
文字列	引用符を付けない一組の文字。stringの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてstringとみなされます。
<>	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、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

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。

ワンポイント アドバイス：時間の節約に役立つアクションを示します。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 **安全上の重要な注意事項**

この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保存しておいてください。ステートメント 1071

関連資料

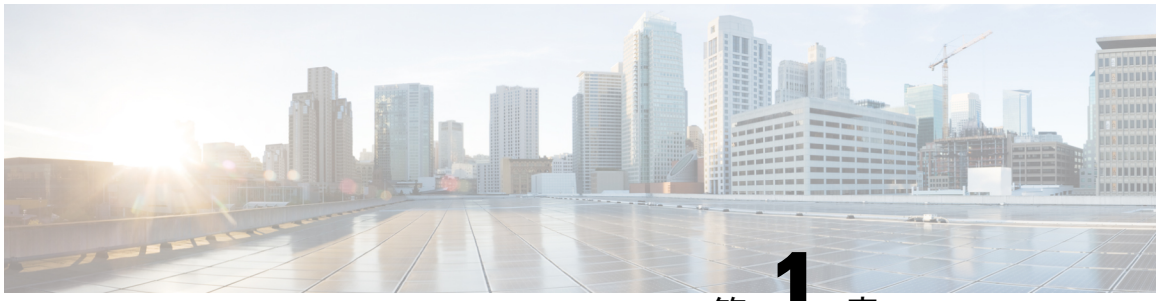
Cisco Catalyst 9800 ワイヤレス コントローラの詳細については、次のドキュメントを参照してください。

- *Release Notes for Cisco Catalyst 9800 Wireless Controller*
- *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*
- *Cisco Catalyst 9800 Series Wireless Controller Command Reference*
- *Cisco Wireless Solutions Software Compatibility Matrix*

マニュアルの入手方法およびテクニカル サポート

ドキュメントの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元で直接受け取るには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。



第 1 章

クラウド向け Cisco Catalyst 9800 ワイヤレス コントローラの概要

はじめに

Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラ（このドキュメントでは「コントローラ」という）は仮想ワイヤレス コントローラで、Linux ベースの 64 ビット ゲスト オペレーティング システムの仮想マシン（VM）インスタンスとして Cisco Unified Computing System（UCS）に導入されます。このコントローラは、Cisco IOS XE ソフトウェアの機能およびテクノロジーのサブセットをサポートし、仮想化プラットフォームに Cisco IOS XE 機能を実装します。

VM としてコントローラを導入すると、Cisco IOS XE ソフトウェアは従来のシスコ ハードウェア プラットフォーム上に導入されているかのように機能します。

仮想化のメリット

コントローラは仮想化のメリットを生かして、次のメリットを実現します。

- ハードウェア独立性：コントローラは VM 上で実行するため、仮想化プラットフォームがサポートしている x86 ハードウェア上でサポートできます。

- リソースの共有：コントローラで使用されるリソースはハイパーバイザによって管理されており、これらのリソースはVM間で共有できます。VMサーバが特定のVMに割り当てるハードウェア リソースの量は、サーバ上の別の VM に再割り当てできます。
- 導入における柔軟性：サーバ間で容易にVMを移動できます。したがって、ある物理的な場所にあるサーバから別の物理的な場所にあるサーバへハードウェア リソースを移動せずにコントローラを移動できます。

ソフトウェアの設定と管理

次の方法を使用して、コントローラのソフトウェア設定と管理を行うことができます。

- Cisco IOS XE CLI コマンドにアクセスするには、仮想ビデオ グラフィック アレイ（VGA）コンソールまたは仮想シリアル ポートのコンソールを使用します。
- Cisco IOS XE CLI コマンドにアクセスするには、リモート SSH または Telnet を使用します。

（注） シリアルコンソールから **show redundancy trace main** コマンドを実行すると、コントローラがリロードすることがあります。

シリアルコンソールは、大規模な展開には推奨されません。この場合は Telnet または SSH を使用することを推奨します。仮想シリアルポートの追加方法に関する詳細については、『Cisco Catalyst C9800-CL Wireless Controller Virtual Deployment Guide』の「Adding Virtual Serial Port」を参照してください。

仮想マシン

コントローラはVMとして実行できます。VMは、オペレーティング システムまたはプログラムをインストールできるコンピューティング環境のソフトウェア実装です。VMは、一般に物理的なコンピューティング環境をエミュレートしますが、CPU、メモリ、ハード ディスク、ネットワーク、およびその他のハードウェア リソースの要求は、基礎となる物理ハードウェアにこの要求を転送する、仮想化レイヤによって管理されます。

ESXi に Open Virtualization Archive（OVA）ファイルを導入できます。OVA ファイルは、新しいVMのパラメータとリソース割り当て要件の詳細定義を提供することにより、VMの展開プロセスを合理化します。

OVA ファイルは記述子（.ovf）ファイル、ストレージ（.vmdk）ファイル、およびマニフェスト（.mf）ファイルで構成されます。

- 記述子または .ovf ファイル：拡張子として .ovf を持つ XML ファイル。パッケージに関するすべてのメタデータで構成されます。これは、製品のすべての詳細情報、仮想ハードウェアの要件、およびライセンスをエンコードします。

- ストレージまたは vmdk ファイル：VM から 1 つの仮想ディスクをエンコードするファイル形式。
- マニフェストまたは .mf ファイル：パッケージング時に生成されるセキュア ハッシュ アルゴリズム（SHA）キーを保存するオプション ファイル。

ハイパーバイザのサポート

ハイパーバイザは、単一のハードウェア ホスト マシンを複数のオペレーティング システムで共有できるようにします。各オペレーティング システムはホスト プロセッサ、メモリ、およびその他のリソースを専有するように見えますが、ハイパーバイザは、オペレーティング システムで必要なリソースのみを制御して割り当て、オペレーティング システム（VM）が相互に干渉しないことを保証します。

⚠

注意 スナップショットを取得中に、コントローラがクラッシュする可能性があります。UCS で RAID0 設定を使用してクラッシュを回避することをお勧めします。

- VMware ESXi バージョン 5.5 以降を使用していることを確認します。

サポートされるハイパーバイザ タイプ

コントローラのインストールは、選択した Type 1（ネイティブ、ベア メタル）ハイパーバイザ上でサポートされます。インストールは VMware Fusion、VMware Player、Virtual Box などの Type 2（ホスト型）ハイパーバイザではサポートされていません。

ハイパーバイザ vNIC の要件

コントローラのバージョン番号に応じて、ハイパーバイザそれぞれが異なるタイプの仮想ネットワーク インターフェイス カード（vNIC）をサポートします。

表 *1 : VMware ESXi* の *vNIC* 要件

VMware ESXi の vNIC 要件	**値**
サポートされる NIC の種類	VMXNET3
vNIC ホット追加のサポート	あり
vNIC ホット削除のサポート	あり

表 *2 :* カーネルベースの仮想マシン（*KVM*）の *vNIC* の要件

KVM の vNIC の要件	**値**
サポートされる NIC の種類	Virtio、ixgbevf、ixgbbe

KVM の vNIC の要件	値
vNIC ホット追加のサポート	あり
vNIC ホット削除のサポート	なし

表 *3 : Amazon Web Services*（*AWS*）の *vNIC* の要件

AWS の vNIC の要件	値
サポートされる NIC の種類	VMXNET3
vNIC ホット追加のサポート	なし
vNIC ホット削除のサポート	なし

サーバ要件

ソフトウェア リリースに応じてサーバとプロセッサの要件が異なります。次の表にサーバの要件を示します。

表 *4 :* サーバ要件

ソフトウェア リリース	Intel	AMD
Cisco IOS XE Gibraltar 16.10.1 以降	仮想化テクノロジーの拡張機能を搭載した 64 ビットの Intel Core2 以降の世代のプロセッサ。	仮想化テクノロジーの拡張機能を搭載した 64 ビットの Intel Core2 以降の世代と同等のプロセッサ。

サポートされるテンプレートとハードウェア要件

17.3 リリース以降では、Cisco Catalyst 9800-CL Cloud ワイヤレスコントローラのプライベート クラウド インスタンスでハイ スループット テンプレートを設定できます。この機能拡張により、スループットを 2 Gbps から 5 Gbps に上げることができます。

表 *5:* サポートされるテンプレートとハードウェア要件

モデル構成	小規模（ロースループット）	中規模（ロースループット）	大規模（ロースループット）	小規模（ハイスループット）	中規模（ハイスループット）	大規模（ハイスループット）
vCPU の最小数（ハイパースレッディングはサポートされない）	4	6	10	7	9	13
最小 CPU 割り当て（MHz）	4,000	6,000	10, 000	4000	6000	10,000
最小メモリ（GB）	8	16	32	8	16	32
必要なストレージ容量（GB）	16	16	16	16	16	16
仮想 NIC（vNIC）（*）サードパーティ製 NIC は高可用性用	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*	2/(3)*

セキュアブート

セキュアブート機能は、コントローラの起動プロセス中に悪意のあるソフトウェアアプリケーションと不正なオペレーティングシステムがコントローラにロードされないようにします。セキュアブート機能が有効な場合、許可されたソフトウェアアプリケーションのみがコントローラから起動します。

この機能により、コントローラ上で起動するソフトウェアアプリケーションがシスコによって認定されていることが保証されます。セキュアなコンピューティングシステムによって、コン

トローラ上の意図したソフトウェアがマルウェアや改ざんされたソフトウェアを伴わずに実行されるようにします。Unified Extensible Firmware Interface（UEFI）仕様は、受け入れ可能なデジタル署名を持たないソフトウェアのロードを防ぐセキュアブート方法を定義しています。

セキュアブートモードとブートローダのバージョンを表示するには、**show platform software system boot** コマンドを使用します。

```
Device# show platform software system boot
Boot mode: EFI or EFI Secure
Bootloader version: 3.3
```

ガイドライン

- 次のセキュアブート環境がサポートされています。
  - ESXi バージョン 6.5
  - オープンスタックライセンスを使用した KVM RHEL 7.5
  - NFVIS リリース 3.11
- EFI ファームウェアモードのみがセキュアブート機能をサポートします。
- この機能は、Cisco IOS XE Bengaluru 17.6 リリースで作成された VM でサポートされます。
- GRUB3 および新しいディスクパーティションレイアウトは、Cisco IOS XE Bengaluru 17.6 リリース以降で使用できます。

（注） Cisco IOS XE Bengaluru 17.6 リリースより前に作成された VM は、BIOS モードのみをサポートします。

（注） VM が1 7.6 ISO または OVA イメージを使用してインストールされている場合、17.3.4 へのダウングレードは起動時に次のエラーメッセージで失敗します。

```
IOSXE image not compatible with installation.Failing boot..
```

（注） 各ハイパーバイザには、ゲスト VM のセキュアブートを可能にする固有のプロセスがあります。セキュアブートを有効にするには、関連するハイパーバイザのマニュアルを参照してください。セキュアブートを有効にするためのハイパーバイザ固有の一連の手順を以下におおまかに示します。

ESXi セキュアブートの設定

1. VM バージョン 13 を使用する ESXi バージョン 6. 5 以降を使用して VM を作成します。
2. 次の手順を実行して、EFI ファームウェアモードを選択します。
    1. **[Actions]** > **[Edit Settings]**の順に移動します。

        [Edit Time Settings] ページが表示されます。
    2. **[VM Options]** > **[Boot Options]** > **[Firmware]**の順に移動します。
    3. [Choose which firmware should be used to boot the virtual machine] ドロップダウンリストから、[EFI] オプションを選択します。
    4. [**保存（Save**）] をクリックします。
3. VM の電源をオンにしてブートを初期化し、IOS プロンプトが完了するまで待ちます。
4. VM の電源をオフにします。
5. 次の手順を実行して、EFI セキュアブートを有効にします。
    1. **[Actions]** > **[Edit Settings]**の順に移動します。

        [Edit Time Settings] ページが表示されます。
    2. **[VM Options]** > **[Boot Options]** > **[Firmware]**の順に移動します。
    3. [Whether or not to enable UEFI secure boot for this VM] チェックボックスをオンにして、EFI セキュアブートを有効にします。
    4. [**保存（Save**）] をクリックします。
6. VM の電源をオンにすると、VNF が安全に起動します。

KVM セキュアブートの設定

1. ユーザが定義した名前で VM を作成します。
2. VM が作成され、VNF IOS プロンプトが完了したら、VM の電源をオフにします。
3. [EFI Firmware] メニューから PK、KEK、および db 証明書をインストールし、リセットします。

    カスタムキーを作成するには、セキュアブートのカスタムキーに関する説明を参照してください。db 証明書については、 MicCorUEFCA2011_2011-06-27.crt および MicWinProPCA2011_2011-10-19.crt を参照してください。
4. VM をセキュアブートします。

NFVIS セキュアブートの設定

1. NFVIS 3.11 リリース以降にアップグレードします。

2. ISRv EFI tarball を NFVIS リポジトリに登録します。
3. 登録された EFI イメージを使用して VM を作成します。
4. VM をセキュアブートします。

（注） セキュアブートはデフォルトで無効になっています。セキュアブートを有効にするには、CIMC からファームウェア設定を変更する必要があります。セキュアブートは、別の UEFI パーティションからブートする必要があります。

セキュアブートを有効にするには、次の手順を実行します。

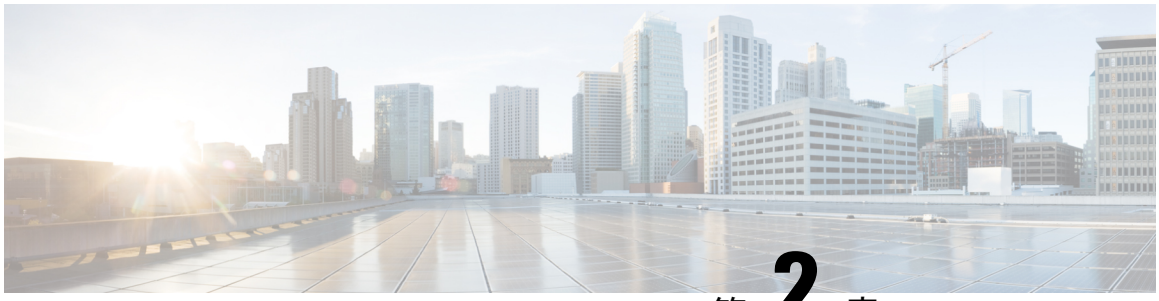
1. CIMC にログインし、**show bios detail** コマンドを使用して BIOS バージョンを表示します。

```
ENCS# scope bios
ENCS/bios # show detail
BIOS:
    BIOS Version: " ENCS54_2.6 (Build Date: 07/12/2018)"
    Boot Order: EFI
    FW Update/Recovery Status: Done, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: disabled
ENCS/bios #
```

2. セキュアブートを有効にします。

```
ENCS/bios # set secure-boot enable
Setting Value : enable
Commit Pending.
ENCS/bios *# commit
ENCS/bios # show detail
BIOS:
    BIOS Version: "ENCS54_2.6 (Build Date: 07/12/2018)"
    Boot Order: EFI
    FW Update/Recovery Status: None, OK
    Active BIOS on next reboot: main
    UEFI Secure Boot: enabled
ENCS/bios #
```

（注） レガシーブート、UEFI ブート、および UEFI セキュアブートの 3 つのブートモードがあります。セキュアブートは、UEFI パーティションがあるディスクでのみ使用できます。



第 2 章

VMware 環境でのコントローラのインストール

VMware 環境の概要

コントローラは、Cisco IOS-XE のオペレーティング システムで実行されます。仮想インストールのイメージには、基盤となっている Cisco IOS-XE オペレーティング システムとワイヤレス コントローラ コードが含まれています。Cisco.com から Cisco IOS XE ソフトウェアをダウンロードし、仮想マシン（VM）環境に直接インストールする必要があります。ただし、初期インストール プロセスの一環として、コントローラ ソフトウェアをインストールしてブートできるように、まず VM 属性をプロビジョニングする必要があります。

コントローラをインストールするために必要な高レベルのタスクを次に示します。

（注） それぞれのインストールオプションは、使用しているハイパーバイザに依存します。

OVA ファイルを使用したコントローラのインストール

1. コントローラ ソフトウェア（.ova ファイル）を Cisco.com からダウンロードします。

2. VM 上にネットワーク インターフェイスを作成します。
3. VMware vSphere クライアントを使用して OVA テンプレートを導入し、コントローラ VM を作成します。
4. VM に電源を投入し、コントローラ ソフトウェアをブートします。

コントローラ VM イメージ（OVA ファイル）の取得

1. クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ 製品ページを開きます。
2. [Download Software] リンクをクリックし、[Download Software] ページを開きます。
3. [Download Software] ページで、モデルを選択します。
4. 該当する Cisco IOS XE ソフトウェアをクリックします。デフォルトでは、推奨される Cisco IOS XE のリリースが選択されます。
5. 使用可能なイメージのリストで [Download Now] または [Add to Cart] をクリックします。
6. 手順に従ってソフトウェアをダウンロードしてください。

インストールオプション

現在、コントローラは次のインストールオプションのみをサポートしています。

- VM 環境での OVA テンプレートの導入。
- ISO のインストールを使用したコントローラの導入。

（注） .ova ファイルは、初回インストールにのみ使用できます。これは、Cisco IOS XE ソフトウェア バージョンのアップグレードには使用できません。

ROMMON とコントローラ

コントローラには、シスコの多くのハードウェア ベースのデバイスに含まれているような ROMMON イメージは含まれていません。最初のブートローダ プロセス中に、インストール スクリプトにより、ゴールデン イメージと呼ばれるコントローラ ソフトウェア イメージのクリーン バージョンが作成され、アクセス不可能なパーティションに配置されます。このクリーン バージョンはソフトウェア イメージが適切に機能していない場合やブートできない場合に使用できます。

VMware ESXi 環境でのインストール

この項では、VMware ツールに関する情報と、最新の Cisco IOS XE ソフトウェアを実行しているコントローラの VM の要件、およびサポート対象の VM 機能のリストを示します。

コントローラは、VMware ESXi ハイパーバイザ上で実行できます。同じハイパーバイザを使用して複数の VM を実行できます。

VMware vSphere の Web クライアントは PC 上で実行し、vCenter サーバにアクセスする Web アプリケーションです。VMware vSphere Web クライアント ソフトウェアを使用して VMware vCenter Server 上で VM を作成、設定、管理したり、コントローラを起動または停止できます。

vSphere 製品のインストールの詳細については、対応する VMware 製品のドキュメントを参照してください。

（注） Cisco IOS XE Amsterdam 17.1.1s までは、vSphere クライアントからのインターフェイスのホット削除がサポートされていません。

VMware 要件

次に、コントローラの導入に必要な VMware ツールを示します。

- VMware vSphere Web クライアント次のバージョンがサポートされています。
  - VMware vSphere Web Client 6.0
- VMware vCenter Server。

  サポート対象のバージョンのリストについては、リリースノートを参照してください。
- VMware vSwitch。標準または分散型の vSwitch がサポートされています。
- ハード ドライブ。単一ハードディスク ドライブのみがサポートされています。1 台の VM 上で複数のハード ディスク ドライブはサポートされません。
- vCPU。次の vCPU 設定がサポートされています。
  - [Small Template]：vCPU X 4（最小 4 GB の RAM の割り当てが必要）
  - [Medium Template]：vCPU X 6（最小 16 GB の RAM の割り当てが必要）
  - [Large Template]：vCPU X 10（最小 32 GB の RAM の割り当てが必要）
- 仮想 CPU コア
- 仮想ハード ディスク領域：最小 8 GB が必要です。
- 仮想ネットワーク インターフェイス カード（VNIC）。

サポートされている VMware 機能と操作

VMware では、仮想アプリケーションを管理したり、複製、移行、シャットダウン、復帰などの操作を実行したりするためのさまざまな機能と操作がサポートされています。

これらの操作の一部では、VM の実行時状態が保存され、再起動時に復元されます。実行時状態にトラフィック関連状態が含まれていると、実行時状態を回復または再生するときに、ユーザ コンソールに追加のエラー、統計情報、またはメッセージが表示されます。設定のみに基づいて回復される保存状態の場合は、これらの機能と動作を問題なく使用できます。

注意 vMotion、スナップショット、分散リソーススケジューラ（DRS）、vNIC チーミング、SR-IOV モードなどの VMware 機能がサポートされています。ただし、スナップショットからの複製はサポートされません。

また、SR-IOV モードが有効な場合、vMotion、DRS、スナップショット、および vNIC チーミングはサポートされません。

詳細については、Cisco Catalyst 9800-CL クラウド ワイヤレス コントローラのデータ シートを参照してください。

VMware の機能と動作の詳細については、対応する VMware のドキュメントを参照してください。

VM 上でのネットワーク インターフェイスの作成

VMware vSphere クライアントで次のタスクを実行してネットワーク インターフェイスを作成します。

始める前に

この手順は、コントローラの初回インストールにのみ必要です。

ステップ 1 VMware vSphere Client にログインします。
ステップ 2 vSphere GUI で、[Configuration] タブをクリックします。
ステップ 3 [Networking] 領域で、[Add Networking…] をクリックします。
ステップ 4 [Connection Type] で、デフォルトの設定をそのままにし、[Next] をクリックします。
ステップ 5 [Network Access] で VM の名前のいずれかを選択します。
ステップ 6 [Next] をクリックします。
ステップ 7 [Connection Settings] で、[Network Label] フィールドに名前を入力します。
ステップ 8 [VLAN ID (Optional)] ドロップダウン リストで [All (4095)] を選択します。
ステップ 9 [Next] をクリックします。
ステップ 10 [Summary] で、更新を確認し、[Finish] をクリックします。

新しく追加したネットワーク インターフェイスが [Networking] 領域で使用できるようになります。

仮想スイッチの NIC チーミングの設定

複数の物理NICを1つのチームに含めることで、仮想スイッチのネットワーク容量を増やすことができます。これは、NICチーミングと呼ばれます。仮想スイッチがチーム内の物理NIC間のネットワーク トラフィックを分散させる方法を配布するには、環境のニーズと能力に応じてロード バランシングを選択します。

仮想スイッチで NIC チーミングを設定するには、VMware vSphere クライアントで次のタスクを実行します。

始める前に

この手順は、NIC チーミングを設定する場合にのみ必要です。

（注） VMXNET3 は、コントローラでサポートされている仮想アダプタ タイプです。

ステップ 1 VMware vSphere Client にログインします。

ステップ 2 [仮想スイッチ（Virtual Switches）] に移動します。

ステップ 3 仮想スイッチのプロパティを表示するには、[編集（Edit）] をクリックします。

ステップ 4 [仮想スイッチのプロパティ（Virtual switch properties）] ページの [NIC チーミング] タブに移動します。

ステップ 5 [**ロードバランシング (Load Balancing)**] ドロップダウン メニューから、仮想スイッチがチーム内の物理NIC間の発信トラフィックのロード バランシングを行う方法を指定します。

仮想スイッチでは、次のオプションを設定できます。

- 発信元仮想ポート ID に基づくルート：スイッチの仮想ポート ID に基づいてアップリンクを選択します。
- IP ハッシュに基づくルート：各パケットの送信元および宛先 IP アドレスのハッシュに基づいてアップリンクを選択します。
- 送信元 MAC ハッシュに基づくルート：送信元イーサネットのハッシュに基づいてアップリンクを選択します。
- 明示的なフェールオーバー順序の使用：フェールオーバー検出基準を満たすアクティブなアダプタのリストから最も高い順序のアップリンクを使用します。このオプションでは、実際のロード バランシングは実行されません。

ステップ 6 [ネットワークフェールオーバー検出（Network Failover detection）] ドロップダウン メニューから、フェールオーバー検出の方法を指定します。

仮想スイッチでは、次のオプションを設定できます。

- リンク ステータスのみ：ネットワーク アダプタによって提供されるリンク ステータスに依存します。このオプションは、物理スイッチの電源障害や削除されたケーブルなどの障害を検出します。
- ビーコン プロービング：チーム内のすべての NIC でビーコン プローブを送受信し、リンク ステータスとともにこの詳細を使用してリンク障害を判別します。

ステップ 7 スイッチにフェールオーバーを通知するには、[通知スイッチ（Notify Switches）] ドロップダウン メニューから [はい（Yes）] または [いいえ（No）] を選択します。

ステップ 8 [フェールバック (Failback)] ドロップダウン メニューから、障害から回復した後に物理アダプタをアクティブ ステータスに戻すかどうかを選択します。

フェールバックが [はい (Yes)] に設定されている場合、アダプタはリカバリ後すぐにアクティブに戻ります。デフォルトでは、フェールバック ポリシーは NIC チームで有効になっています。

フェールバックが [**いいえ（No**）] に設定されている場合、障害が発生したアダプタは、別のアクティブなアダプタに障害が発生し、交換が必要になるまで回復後は非アクティブのままになります。

（注） フェールオーバー順序の最初の物理 NIC で断続的な障害が発生した場合、フェールバック ポリシーにより NIC が頻繁に更新される可能性があります。物理スイッチの MAC アドレスが頻繁に変更されるため、アダプタがオンラインになった直後に物理ポートがトラフィックを受け入れない可能性があります。このような遅延を最小限に抑えるために、物理スイッチで次の設定を変更できます。

- ESXi ホストに接続されている物理 NIC でスパニング ツリー プロトコル（STP）を無効にします。
- アクセス インターフェイスとトランク インターフェイスの PortFast モードまたは PortFast トランク モードをそれぞれ有効にします。これにより、物理スイッチ ポートの初期化中に約 30 秒間短縮されます。

ステップ 9 設定を確認して、設定を適用します。

vSphere を使用した VM でのコントローラ OVA の導入に関する情報

提供されたコントローラ OVA ファイル パッケージを使用して、コントローラを VM に導入できます。

VMware vSphere クライアント、VMware OVF ツール、または共通の OVF ツール（COT）を使用して、OVA を導入できます。

制限事項および要件

OVA パッケージを VM に導入する場合は、次の制限事項が適用されます。

- 仮想 CPU 設定を変更した場合は、コントローラをリブートする必要があります。RAM 割り当ての変更では、コントローラをリブートする必要ありません。
- OVA を導入する場合、VM には、OVF 環境ファイル用に 1 台と .iso ファイル用に 1 台の 2 台の仮想 CD/DVD ドライブが必要です。

vSphere を使用した VM でのコントローラ OVA ファイルの導入

VMware vSphere クライアントで次のステップを実行します。

提供されたコントローラ OVA ファイルパッケージを使用して、コントローラを VM に導入できます。

VMware vSphere クライアント、VMware OVF ツール、または共通の OVF ツールを使用して、OVA を導入できます。

始める前に

- 仮想CPU設定を変更した場合は、コントローラをリブートする必要があります。ただし、RAM 割り当ての変更では、コントローラをリブートする必要ありません。
- OVA を導入する場合、VM には、OVF 環境ファイル用に 1 台と .iso ファイル用に 1 台の 2 台の仮想 CD/DVD ドライブが必要です。
- ネットワーク インターフェイスが正しく設定されていることを確認します。

ステップ 1 VMware vSphere Client にログインします。

ステップ 2 vSphere クライアントのメニューから、 [File] > [Deploy OVF Template] を選択します。

ステップ 3 **OVA** ウィザードで、導入するコントローラの OVA の送信元を選択します。

[OVF Template Details] ウィンドウに OVA に関する情報が表示されます。

ステップ 4 [Next] をクリックします。

ステップ 5 [Name and Location] フィールドで、VM の名前を指定し、[Next] をクリックします。

ステップ 6 [Next] をクリックします。

ステップ 7 [Deployment Configuration] で、ドロップダウンリストから必要なプロファイルを選択します。

ステップ 8 [Disk Format] で、デフォルトの設定（[Thick Provision Lazy Zeroed]）をそのままにし、[Next] をクリックします。

ステップ 9 [Network Mapping] ドロップダウン リストで、宛先ネットワークに 1 つ以上の仮想ネットワーク インターフェイス カード（vNIC）を割り当てます。一意のインターフェイスに各ネットワークを接続します。次のマッピングをお勧めします。

- GigabitEthernet 1 からデバイス管理インターフェイス：アウトオブバンド管理ネットワークにマッピングします。
- GigabitEthernet 2 からワイヤレス管理インターフェイス：AP とサービスに到達するネットワークにマッピングします。通常、このインターフェイスは複数の VLAN を伝送するトランクです。
- GigabitEthernet 3 から高可用性インターフェイス：SSO のピアツーピア通信用の別のネットワークにマッピングします。

ステップ 10 [Ready to Complete] で、すべての導入設定を確認します。

ステップ 11 [Finish] をクリックして OVA を展開します。

コントローラ VM が左側のパネルに表示されます。

ステップ 12 VM の電源を自動的に投入するには、[Power On] をクリックします。

VM の基本プロパティの編集

VMware vSphere クライアントで次のタスクを実行します。

ステップ 1 VMware vSphere Client にログインします。

ステップ 2 vSphere GUI で、[Configuration] タブをクリックします。

ステップ 3 [Networking] 領域で、新しく追加したネットワーク インターフェイスの [Properties] をクリックします。

ステップ 4 [Edit] をクリックしてネットワーク インターフェイスのプロパティを表示します。

ステップ 5 [Security] タブをクリックします。

ステップ 6 オンになっている VM 名をオフにします。

ステップ 7 [Promiscuous Mode] で、次のタスクを実行します。

デフォルトでは [Promiscuous Mode] は [Reject] に設定されています。

（注） 無差別モードは、vSphere ESXi の仮想スイッチまたはポートグループ レベルで定義できるセキュリティ ポリシーです。このモードを使用しないと、タグ付けされたトラフィックが適切にフローしません。

- チェックボックスをオンにします。
- ドロップダウン リストで [Accept] を選択し、このスイッチを通じて送受信されるトラフィックを表示します。

（注） [Forged Transmits] も [Accept] に設定されていることを確認します。

ステップ 8 [OK] をクリックした後、[Close] をクリックします。

VMware ESXi 用の SR-IOV の設定

SR-IOV で推奨されるソフトウェアバージョン

表 *6 :* サポートされている *NIC* タイプの一覧

NIC	ファームウェア	ドライバのバージョン	ホスト OS
Intel x710	7.10	I40en 1.10.6 INETCLI プラグイン バージョン 1.4.1	VMware バージョン 6.5 以降

インターフェイスでの SR-IOV モードの設定

ステップ 1 ポートなしでポートグループを作成します。

ステップ 2 ダミーの仮想スイッチを作成し、**手順 1** で作成したポートグループをこのスイッチに接続します。

ステップ 3 [Host] > [Manage] > [Hardware] で、x710 PCI デバイスポートの SR-IOV を有効にします。

（注） 最大のパフォーマンスを得るために、ポートあたり 1 つの VF が作成されます。

ステップ 4 eWLC インスタンスを作成します。ネットワークアダプタを追加するときに、次の手順を実行します。

1. 作成したポートグループに [Network Adapter] を選択します。
2. SR-IOV パススルーとして [Adapter Type] を選択します。
3. SR-IOV が有効になっているポートにマッピングされるように、[Physical Function] を選択します。
4. [Guest OS MTU Change] を [Allow] に設定します。
5. [保存（Save）] をクリックします。

信頼モードの有効化とスプーフィングチェックの無効化

GUI から ESXi への SSH を有効にするには、次の手順を実行します。

ステップ 1 [Host] > [Actions] > [Services] > [Enable SSH] の順に選択して移動します。

ステップ 2 [SSH] を [ESXi] に設定します。

スプーフィングチェックを無効にするには、次の手順を実行します。

コントローラのブート中に、次のコマンドを使用して信頼モードとスプーフィングチェックを設定します。

esxcli intnet sriovnic vf set -t on -s off -v *<vf-id> -n <physical_port_name>*

ここで、各変数は次のように定義されます。

<physical_port_name> は、VM が関連付けられている SR-IOV ポートです。

<vf-id> は、VM インスタンスに割り当てられた VF ID です。

サンプル出力：

```
[root@localhost:~] esxcli intnet sriovnic vf set -t on -s off -v 0 -n vmnic6
```

（注） VF ID がコントローラに割り当てられているかどうかを確認するには、**/var/log** にある **vmkernel.log** ファイルを確認します。

SR-IOV 永続設定の構成

上記の方法で設定された SR-IOV 設定は、リブート後は保持されません。この問題を解決するには、ホストのリブート時に自動的に有効になるサービスとして上記の設定を実行します。

ステップ 1 ファームウェアバージョン 7.0 およびドライババージョン 1.8.6 以前のバージョンのファームウェアとドライバでは、ブート時に VM のロードを停止して信頼モードの有効化とスプーフィングチェックの無効化を実行する必要があります。

ステップ 2 ファームウェアバージョン 7.10 およびドライババージョン 1.10.6 以降のバージョンのファームウェアとドライバでは、信頼モードとスプーフィングチェックの設定が永続化されていることを確認した後で、次のコマンドを入力します。

esxcli system module parameters set -a -p max_vfs=1,1,1,1 -m i40en

esxcli system module parameters set -m i40en -p trust_all_vfs=1,1,1,1

SR-IOV ドライバとファームウェアバージョンの確認

次のコマンドを使用して NIC を確認できます。

esxcli network nic list

```
[root@localhost:~] esxcli network nic list

Name     PCI Device    Driver  Admin Status  Link Status  Speed  Duplex  MAC Address
      MTU  Description

-------  ------------  ------  ------------  -----------  -----  ------  -----------------
  ----  -----------------------------------------------------


vmnic6   0000:87:00.0  i40en   Up           Up          10000  Full    3c:fd:fe:ee:ce:d8
  1500  Intel Corporation Ethernet Controller X710 for 10GbE SFP+
```

```
vmnic7   0000:87:00.1  i40en   Up           Down            0  Half    3c:fd:fe:ee:ce:d9
  1500  Intel Corporation Ethernet Controller X710
```

次のコマンドを使用して、特定のインターフェイスのパラメータを表示できます。

```
esxcli network nic get -n vmnic6
```

```
[root@localhost:~] esxcli network nic get -n vmnic6
Advertised Auto Negotiation: true

   Advertised Link Modes: Auto, 1000BaseSR/Full, 10000BaseSR/Full

   Auto Negotiation: true

   Cable Type: FIBRE

   Current Message Level: 0

   Driver Info:

         Bus Info: 0000:87:00:0

         Driver: i40en

         Firmware Version: 7.10 0x80006471 1.2527.0

         Version: 1.10.6
[root@localhost:~]  esxcli intnet sriovnic vf get -n vmnic6
VF ID           Trusted         Spoof Check
-----           -------         -----------
0               true            false
```

次のコマンドを使用して、プロセッサ、メモリ、vNIC、ハイパーバイザ、およびスループットプロファイルの詳細を確認できます。

```
Device # show platform software system all
```

```
Device # show platform software system all

Controller Details:
==================
VM Template: medium
Throughput Profile: high
AP Scale: 3000
Client Scale: 32000
WNCD instances: 3
Processor Details
==================
Number of Processors : 9
Processor : 1 - 9
vendor_id : GenuineIntel
cpu MHz  : 2593.748
cache size : 4096 KB
Crypto Supported : Yes
model name : Intel Core Processor (Haswell, IBRS)
Memory Details
==============
Physical Memory : 16363364KB

VNIC Details
============
Name              Mac Address     Driver Name       Status  Platform MTU
```

```
GigabitEthernet1  3cfd.fede.ccbc  net_i40e_vf       DOWN    1522
GigabitEthernet2  3cfd.fede.ccbd  net_i40e_vf       DOWN    1522

Hypervisor Details
====================
Hypervisor: VMWARE
Manufacturer: VMware, Inc
Product Name: VMware Virtual Platform
Serial Number: VMware-42 06 f0 d7 62 6a fd 6d-75 0e cc 81 5d ce ac 71
UUID: 0E3546DD-DE6E-400D-9B3D-025215519CB8
image_variant :

Boot Details
====================
Boot mode: BIOS
Bootloader version: 1.1
```

Intel NIC のファームウェアに関する詳細については、以下を参照してください。

https://downloadcenter.intel.com/product/82947/Intel-Ethernet-Controller-X710-Series

Intel および Cisco NIC のドライバに関する詳細については、以下を参照してください。

https://www.vmware.com/resources/compatibility/detail.php%3FdeviceCategory%3Dio%26productid%3D37996

Cisco NIC のファームウェアに関する詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/tsd-products-support-series-home.html

ISO イメージを使用したコントローラ用の VM の作成

次の手順で、VMware vSphere を使用したコントローラの導入方法に関する一般的なガイドラインを示します。ただし、実行する必要がある正確なステップは、VMware 環境と設定の特性に応じて異なる場合があります。

始める前に

vSphere クライアントがマシンにインストールされていることを確認します。

ステップ 1 VMware vSphere Client にログインします。

ステップ 2 vSphere クライアントのメニューで、[File] > [New] > [Virtual Machine] を選択します。

ステップ 3 [Create New Virtual Machine] ウィンドウで、[Custom] を選択し、[Next] をクリックします。

ステップ 4 VM の名前を入力し、[Next] をクリックします。

ステップ 5 VM ファイルに [Datastore] を選択して、[Next] をクリックします。

ステップ 6 [Virtual Machine Version] を選択し、[Next] をクリックします。

ステップ 7 [Guest Operating System] ウィンドウで [Other] を選択し、[Version] ドロップダウン リストから [Other (64-bit)] をバージョンとして選択し、[Next] をクリックします。

ステップ 8 [CPU] の下で、次の設定を選択します。

- 仮想ソケット（仮想 CPU）の数

- ソケットあたりのコア数

ソケットごとのコアの数は、選択されている仮想ソケットの数に関係なく、常に[1]に設定する必要があります。たとえば、4 vCPU 設定のコントローラは、4 つのソケットおよびソケットあたり 1 のコアで設定する必要があります。

仮想 CPU のサポート対象数と、それに対応するRAM の必要な割り当ては導入するプロファイルによって異なります。

ステップ 9 [Memory] で、プロファイルのサポート対象のメモリ サイズを設定し、[Next] をクリックします。

ステップ 10 [Network] で、導入するプロファイルに基づいて 2 つ（HA が必要な場合は 3 つ）の vNIC を割り当てます。

a) [How many NICs do yo want to connect?] ドロップダウン リストで、接続する vNIC の数を選択します。
b) [Network] ドロップダウン リストで、vNIC を選択します。

（vNIC ごとに異なるネットワークを選択します）

（注） 2 または 3 つのインターフェイスを追加することをお勧めします（デバイス管理 に 1 つ、ワイヤレス管理 に 1 つ、HA を設定する場合は HA に 1 つ）。

c) [Adapter] ドロップダウン リストからアダプタ タイプとして [VMXNET3] を選択します。
d) すべての vNIC を選択して電源投入時に接続します。
e) [Next] をクリックします。

ステップ 11 [SCSI Controller] ウィンドウで、[SCSI Controller] に [VMware Paravirtual] を選択し、[Next] をクリックします。

ステップ 12 [Create a Disk] ウィンドウで、次の値を選択します。

- [Capacity]：ディスク サイズ。8 GB のディスクをお勧めします。
- [Disk Provisioning]：[Thick Provision Lazy Zeroed] または [Thick Provision Eager Zeroed] のいずれかを選択します。
- [Location]：仮想マシンを持つストア。

ステップ 13 [Next] をクリックします。

ステップ 14 [Advanced Options] ウィンドウで、[Virtual Device Node] を選択し、[Next] をクリックします。

ステップ 15 [Finish] をクリックします。

ステップ 16 新たに作成したインスタンスに移動して右クリックし、[Edit Settings] を選択します。

ステップ 17 [Hardware] タブで、[CD/DVD Drive] をクリックします。

a) [Datastore ISO File] オプションとして、VM のブート元の**デバイス タイプ**を選択します。データ ストア上の .iso ファイルの場所を参照します。コントローラ ISO ファイルが選択されていることを確認します。
b) [Device Status] 領域で、[Connect at power on] チェックボックスをオンにします。

ステップ 18 [OK] をクリックします。

これで、VMが設定され、ブートする準備が整います。VMの電源投入時にコントローラがブートされます。

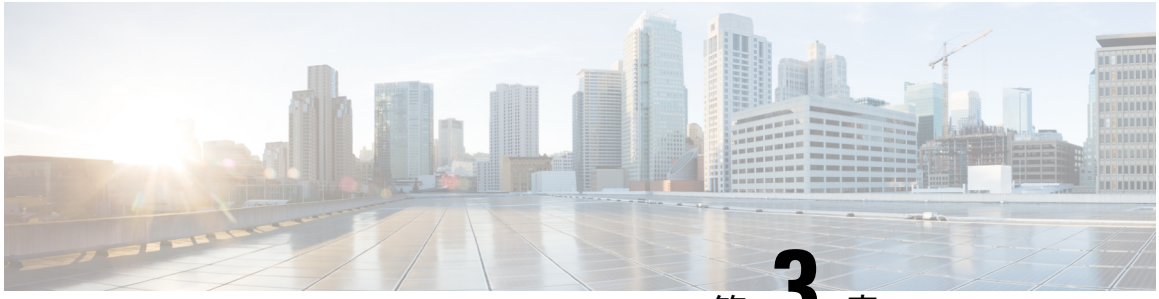
コントローラの電源投入

コントローラを起動するには、次のステップを実行します。

ステップ 1 vSphere クライアントから仮想スイッチを選択します。

ステップ 2 VM を選択し、[Power On] をクリックします。

VM が起動プロセスを開始します。VM が起動すると、コントローラはブート プロセスを開始します。



第 3 章

KVM 環境でのコントローラのインストール

カーネルベースの仮想マシン環境の概要

クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ は、カーネルベースの仮想マシン（KVM）を使用して Ubuntu、Red Hat Enterprise Linux（RHEL）7.2、および Red Hat Enterprise Virtualization（RHEV）の上部でサポートされます。KVM でのインストールでは仮想マシン（VM）の作成と、.iso ファイルまたは .qcow2 ファイルを使用したインストールが必要です。VM は、KVM コマンド ラインまたは Virsh を使用して起動できます。

- .qcow2：KVM 環境でソフトウェア イメージをブートするために使用します。
- .iso：Virsh ツールを使用して手動で クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ をインストールするために使用します。また、KVM 環境で virsh コマンドを使用してコントローラを起動するには、サンプル XML 設定の virsh.xml ファイルも必要です。

サポートされているプロファイルの設定

次のプロファイル設定がサポートされています。

表 7: サポートされているプロファイルの設定

テンプレート	CPU	RAM	AP	クライアント
Small	4 vCPU	8 GB	1000	10000
Medium	6 vCPU	16 GB	3000	320000
Large	10 vCPU	32 GB	6000	640000

サポートされているネットワー キング オプション

次のネットワーキング オプションがサポートされています。

- Linux ブリッジ
- Open vSwitch（OVS）

KVM のインストールに必要なパッケージ

KVM をインストールするには、次のパッケージが必要です。

- Qemu-kvm
- Qemu-utils
- Uml-utilities
- Socat
- KVM
- Libvirt-bin
- Virtinst

KVM 環境でのインストール手順

一連のインストール ステップを説明する自動インストール パッケージを使用するか、または virt-manager、virt install、virsh など、KVM でサポートされている管理ソフトウェアのいずれかを使用して KVM 環境に クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ をインストールできます。

KVM インストーラ パッケージは KVM 用の自動インストール パッケージです。このパッケージを実行すると、次のモードを提供します。

- [Default]：バンドルされているイメージ ファイルとデフォルトの VM 設定オプション（[Small]、[Medium]、または [Large]）のいずれかを使用してコントローラをインストールします。
- [Interactive]：VM設定のカスタマイズを許可し、バンドルされたイメージファイルか、または別の .qcow2 イメージをインストールするオプションを提供します。

（注） サポートされていない VM 操作のリストについては、VMware ESXi 環境でのインストール （11 ページ）の章の「サポートされている VMware 機能と操作」セクションを参照してください。

始める前に

クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ ソフトウェア インストール イメージ パッケージから .run 実行可能ファイルをダウンロードし、ホスト マシンのローカル ドライブにコピーします。

.qcow2 イメージを使用した Linux ブリッジ ネットワーキングでのコントローラのインストール

この手順は、コントローラ用の VM を手動で作成するための一般的なガイドラインです。実行する必要がある正確なステップは、KVM 環境とセットアップの特性によって異なることがあります。詳細については、Red Hat Linux、Ubuntu、および Virsh のドキュメントを参照してください。

virt-install コマンドを使用してインスタンスを作成し、次の構文を使用してブートします。

```
--connect=qemu:///system \
--os-type=linux \
--os-variant=rhel4 \
--arch=x86_64 \
--cpu host \
--console pty,target_type=virtio \
--hvm \
--import \
--name=my_c9k_vm \
--disk path=<path_to_c9800-c_qcow2>,bus=ide,format=qcow2 \
--vcpus=1,sockets=1,cores=1,threads=1 \
--ram=4096 \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio  \
--noreboot \
```

（注） インストールが完了すると、コントローラ VM はシャットダウンされます。**virsh start** コマンドを使用してコントローラ VM を起動します。

ISO イメージを使用した Vrish でのコントローラのインストール

この手順は、コントローラ用の VM を手動で作成するための一般的なガイドラインです。実行する必要がある正確なステップは、KVM 環境とセットアップの特性によって異なることがあります。詳細については、Red Hat Linux、Ubuntu、および Virsh のドキュメントを参照してください。

ステップ 1 **qemu-img** コマンドを使用し、**.qcow2** 形式で 8 GB のディスク イメージを作成します。

```
qemu-img create -f qcow2 c9000-c_disk.qcow2 8G
```

ステップ 2 **virt-install** コマンドを使用してコントローラをインストールします。これには、新しい VM を作成するための適切な権限が必要です。次に、4 GB の RAM を持つ 1 つの vCPU VM と 3 つのネットワーク インターフェイスを作成する例を示します。

```
virt-install \
--connect=qemu:///system \
--os-type=linux \
--os-variant=rhel4 \
--arch=x86_64 \
--cpu host \
--hvm \
--import \
--name=my_c9k_vm \
--cdrom=<path_to_c9800-c_iso> \
--disk path=c9000-c_disk.qcow2,bus=virtio,size=8,sparse=false,cache=none,format=qcow2 \
--ram=4096 \
--vcpus=1,sockets=1,cores=1,threads=1 \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio \
--noreboot \
```

（注） **virt-install** コマンドで新しい VM インスタンスを作成し、コントローラは指定したディスク ファイルにイメージをインストールします。インストールが完了すると、コントローラ VM はシャットダウンされます。**virsh start** コマンドを使用してコントローラ VM を起動します。

.qcow2イメージを使用したOVSネットワークでのコントローラのインストール

この手順は、コントローラ用のVMを手動で作成するための一般的なガイドラインです。実行する必要がある正確なステップは、KVM 環境とセットアップの特性によって異なることがあります。詳細については、Red Hat Linux、Ubuntu、および Virsh のドキュメントを参照してください。

virt-install コマンドを使用してインスタンスを作成し、次の構文を使用してブートします。

```
--connect=qemu:///system \
--os-type=linux \
--os-variant=rhel4 \
--arch=x86_64 \
--cpu host \
--console pty,target_type=virtio \
--hvm \
--import \
--name=my_c9k_vm \
--cdrom=<path_to_c9800-c_iso> \
--disk path=c9000-c_disk.qcow2,bus=virtio,size=8,sparse=false,cache=none,format=qcow2 \
--ram=4096 \
--vcpus=1,sockets=1,cores=1,threads=1 \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio \
--noreboot \
```

（注） インストールが完了すると、コントローラ VM はシャットダウンされます。**virsh start** コマンドを使用してコントローラ VM を起動します。

ブートストラップ設定を使用したVrishでのコントローラのインストール

この手順は、コントローラ用のVMを手動で作成するための一般的なガイドラインです。実行する必要がある正確なステップは、KVM 環境とセットアップの特性によって異なることがあります。詳細については、Red Hat Linux、Ubuntu、および Virsh のドキュメントを参照してください。

始める前に

必要な設定で *iosxe_config.txt* というテキスト ファイルを作成し、**mkisofs -l -o** *iso-file-name.iso iosxe_config.txt* コマンドを使用し、iosxe_config.txt ファイルを入力として指定して .iso イメージを作成します。

```
mkisofs -l -o test.iso iosxe_config.txt
```

次にサンプルの設定ファイルを示します。

```
hostname C9800-CL
license smart enable
username lab privilege 15 password lab
ip domain-name cisco.com
interface GigabitEthernet1
 ip address 10.0.0.5 255.255.255.0
 no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
line vty 0 4
  login local
exit
```

virt-install コマンドを使用してコントローラをインストールします。このコマンドを使用するには、新しい VM を作成するための適切な権限が必要です。次に、4 GB の RAM を持つ 1 つの vCPU VM と 3 つのネットワーク インターフェイスを作成する例を示します。

```
virt-install \
--connect=qemu:///system \
--os-type=linux \
--os-variant=rhel4 \
--arch=x86_64 \
--cpu host \
--console pty,target_type=virtio \
--hvm \
--import \
--name=my_c9k_vm \
--disk path=<path_to_c9800-c_qcow2>,bus=ide,format=qcow2 \
--vcpus=1,sockets=1,cores=1,threads=1 \
--ram=4096 \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio \
--network=network:<network name>,model=virtio \
--noreboot \
```

ISO イメージを使用した VMM でのコントローラ インスタンスの作成

ステップ 1 [Applications] > [System Tools] > [Virtual Machine Manager] を使用して virt-manager を起動します。

ハイパーバイザの選択およびルート パスワードの入力を求められる可能性があります。

ステップ 2 上部にある [File] オプションを選択し、[New Virtual Machine] オプションを選択します。

ステップ 3 仮想マシンの詳細を入力します。

a) VM の名前を入力します。
b) オペレーティング システム オプションで、[Local install media] を選択します。
c) [Forward] をクリックします。

ステップ 4 ディスクから **ISO イメージ**を選択します。

ステップ 5 [Automatically Detect operating system based on install media] を選択します。

ステップ 6 メモリおよび CPU オプションを設定します。

a) [Memory (RAM)] を設定します。
b) [CPUs] を設定します。
c) [Forward] をクリックして続行します。

ステップ 7 ディスク イメージ サイズを 8 GB に設定し、[Forward] をクリックします。

ステップ 8 インスタンス名を入力します。

ステップ 9 最初に [Customize configuration before install] ボックスをオンにしてから、[Finish] をクリックします。

これにより、他の NIC を追加することができます。

ステップ 10 [Network] タブを選択して他の NIC を追加します。

ステップ 11 [Network source] ドロップダウンで [Network] を選択します。

（注） virtio ネットワーク ドライバのみがサポートされています。

ステップ 12 ドロップダウンを使用して、[Portgroup] を選択します。

ステップ 13 [完了（Finish）] をクリックします。

KVM VMM（virt-manager）でのブートストラップ設定

仮想マシン マネージャとも呼ばれる virt-manager は、libvirt を通じて仮想マシンを管理するためのデスクトップ アプリケーションです。実行中のドメインの概要（ライブ パフォーマンスやリソース使用率の統計情報）が表示されます。ウィザードを使用して、新しいドメインを作成したり、ドメインのリソース割り当てを設定/調整したり、仮想ハードウェアをイネーブルにすることができます。組み込みの VNC および SPICE クライアント ビューアは、ゲスト ドメイン用のフル機能のグラフィカルなコンソールとして使用できます。

ステップ 1 [Applications] > [System Tools] > [Virtual Machine Manager] を使用して virt-manager を起動します。

ハイパーバイザの選択、およびルート パスワードの入力を求められる可能性があります。

ステップ 2 上部にある [File] オプションを選択し、[New Virtual Machine] オプションをクリックします。

ステップ 3 仮想マシンの詳細を入力します。

a) [Name] を指定します。
b) オペレーティング システムの場合、[Import existing disk image] を選択します。

この方法でディスクイメージ（qcow2イメージを選択した場合は、事前にインストールされた、ブート可能なオペレーティング システムを含んでいるもの）をインポートできます。

c) [Forward] をクリックして続行します。

ステップ 4 コントローラ qcow2 イメージ パスを選択します。

ステップ 5 メモリおよび CPU オプションを設定します。

a) [Memory (RAM)] を *8192* に設定します。
b) [CPUs] を *4* に設定します。
c) [Forward] をクリックして続行します。

ステップ 6 インスタンス名を入力します。

ステップ 7 [Finish] をクリックする前に [Customize configuration before install] ボックスをオンにします。

これにより、複数の NIC を追加することができます。

ステップ 8 [Network] を選択します。

ブリッジまたはネットワークのいずれかを選択します。

ステップ 9 [Finish] をクリックします。

ステップ 10 編集する**インスタンス名**をダブルクリックします。

ステップ 11 [i] を選択してインスタンス情報を取得します。

ステップ 12 [Begin Installation] を選択してインスタンスを起動します。

ステップ 13 [Monitor] 記号をクリックして仮想コンソールに移動します。

KVM での SR-IOV の設定

SR-IOV で推奨されるソフトウェアバージョン

表 *8 :* サポートされている *NIC* タイプの一覧

NIC	ファームウェア	ドライバのバージョン	ホスト OS
Intel x710	7.10	I40e 2.10.19.82	KVM RedHat バージョン 7.5 以降
Ciscoized x710	7.0	I40e 2.10.19.82	KVM RedHat バージョン 7.5 以降

Intel VT-D の有効化

（注） 後続のタスクを実行するには、ルート権限が必要です。

Intel VT-D を有効にするには、次の手順を実行します。

ステップ 1 **/etc/sysconfig/grub** ファイルの **GRUB_CMDLINX_LINUX** 行で、末尾に **intel_iommu = on** および **iommu = pt** パラメータを追加します。

ステップ 2 次のコマンドを実行して、**/etc/grub2.cfg** ファイルを再生成します。

grub2-mkconfig -o /etc/grub2.cfg

（注） EFI の場合は、次のコマンドを実行します。

grub2-mkconfig -o /etc/grub2-efi.cfg

ステップ 3 変更を有効にするには、システムをリブートします。

これで、システムで PCI デバイスを割り当てることができるようになりました。

インターフェイスでの SR-IOV モード仮想機能（VF）の設定

VF が使用できない場合は、次のコマンドを使用して SR-IOV VF を設定します。

ステップ 1 インターフェイスで VF を設定します。

echo “no_of_vfs” > /sys/class/net/<interface_name>/device/sriov_numvfs

サンプル出力：

```
echo 1 > /sys/class/net/enp129s0f0/device/sriov_numvfs
```

ここでは、最大のパフォーマンスを得るために、ポートあたり 1 つの VF が作成されます。

ステップ 2 次のコマンドを使用して、VF でスプーフィングチェック、信頼モード、および MAC を設定します。

```
ip link set dev enp129s0f0 vf 0 trust on
ip link set enp129s0f0 vf 0 spoofchk off
ip link set enp129s0f0 vf 0 mac 3c:fd:fe:de:cc:bc
```

（注） MAC アドレスは一意にする必要があります。

ステップ 3 次のコマンドを使用して設定を確認します。

ip link show *interface_name*

サンプル出力：

```
ip link show enp129s0f0
6: enp129s0f0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen
 1000
link/ether 3c:fd:fe:de:01:bc brd ff:ff:ff:ff:ff:ff
vf 0 MAC 3c:fd:fe:de:cc:bc, spoof checking off, link-state auto, trust on
```

SR-IOV 永続設定の構成

上記の方法で設定された SR-IOV 設定は、リブート後は保持されません。この問題を解決するには、ホストのリブート時に自動的に有効になるサービスとして上記の設定を実行します。

ステップ 1 永続化するコマンドを使用して bash スクリプトを作成します。次のように、**/usr/bin/sriov-config** ファイルにスクリプトを記述する必要があります。

```
#!/bin/sh
echo "no_of_vfs" > /sys/class/net/<interface_name>/device/sriov_numvfs
ip link set dev <interface_name> vf 0 trust on
ip link set <interface_name> vf 0 spoofchk off
ip link set <interface_name> vf 0 mac 3c:fd:fe:de:cc:bc
```

サンプル出力：

```
#!/bin/sh
echo 1 > /sys/class/net/enp129s0f0/device/sriov_numvfs
ip link set dev enp129s0f0 vf 0 trust on
ip link set enp129s0f0 vf 0 spoofchk off
ip link set enp129s0f0 vf 0 mac 3c:fd:fe:de:cc:bc
```

（注） すべての VF に対して同じ手順を繰り返す必要があります。

ステップ 2 スクリプトの実行権限を指定します。

chmod 777 /usr/bin/sriov-config

ステップ 3 システムサービスを作成します。ブートの最後に実行する新しいシステムサービスを定義します。このサービスでは、**手順 1** で説明したように、必須の sriov コマンドを含む bash スクリプトを実行します。

（注） **/usr/lib/systemd/system** に **sriov.service** という名前の新しいファイルを作成し、次の内容を追加します。

```
[Unit]
Description=SR-IOV configuration
After=rc-local.service
Before=getty.target
[Service]
Type=oneshot
ExecStart=/usr/bin/sriov-config
[Install]
WantedBy=multi-user.target
```

（注） **ExecStart=/usr/bin/sriov-config** コマンドラインでスクリプトを実行します。

ステップ 4 次のコマンドを使用して、**sriov.service** を有効にし、開始します。

systemctl --now enable sriov.service

（注） このコマンドによってサービスが即座に開始され、ホストがリブートするたびにサービスが実行されるようにします。

KVM の SR-IOV 設定の詳細については、以下を参照してください。

https://www.intel.com/content/www/us/en/embedded/products/networking/xl710-sr-iov-config-guide-gbe-linux-brief.html

コントローラへの SR-IOV の接続

コマンドラインを使用した新しい仮想マシンへの接続

PCI VF デバイスを追加するには、**virt-install** の**ホストデバイス**オプションを使用します。**手順 1**（インターフェイスでの SR-IOV モード仮想機能（VF）の設定 （31 ページ））の情報と PCI BDF 番号を使用して、デバイスを接続します。

10GbE SFP+ 用 Intel Corporation Ethernet Controller X710 の仮想機能。（enp129s0f0）：

```
PCI BDF                                          Interface
=========                                        ==========
0000:18:06.0                           enp129s0f0
0000:18:06.1                                     enp129s0f1
```

VM の作成と起動

VM を作成して起動するには、次のコマンドを使用します。

```
sudo virt-install --virt-type=kvm --name ewlc_sriov_3-18 --ram 16384 --vcpus=9 --hvm
--cdrom=/home/C9800-CL-universalk9.BLD_POLARIS_DEV_LATEST_20200318_062819-serial.iso
--network none --host-device=pci_0000_18_06_0 --host-device=pci_0000_18_06_1 --graphics
 vnc --disk
path=/var/lib/libvirt/images/ewlc_sriov_3-18.qcow2,size=8,bus=virtio,format=qcow2
```

次のコマンドを使用して VM コンソールを表示します。

```
virsh console ewlc_sriov_3-18
Connected to domain ewlc_sriov_3-18
Escape character is ^]
```

次のコマンドを入力して、インターフェイスの SR-IOV ドライバを確認できます。

Device > enable

Device #show platform software vnic-if interface-mapping

```
Device # show platform software vnic-if interface-mapping
------------------------------------------------------------
Interface Name      Driver Name     Mac Addr
------------------------------------------------------------
```

```
GigabitEthernet2    net_i40e_vf     3cfd.fede.ccbd
GigabitEthernet1    net_i40e_vf     3cfd.fede.ccbc
------------------------------------------------------------
```

（注） 上記の MAC アドレスは、VF に設定されているアドレスと同じです。

次のコマンドを使用して、プロセッサ、メモリ、vNIC、ハイパーバイザ、およびスループットプロファイルの詳細を確認できます。

Device # show platform software system all

```
Device# show platform software system all
Controller Details:
==================
VM Template: medium
Throughput Profile: high
AP Scale: 3000
Client Scale: 32000
WNCD instances: 3

Processor Details
==================
Number of Processors : 9
Processor : 1 - 9
vendor_id : GenuineIntel
cpu MHz  : 2593.748
cache size : 4096 KB
Crypto Supported : Yes
model name : Intel Core Processor (Haswell, IBRS)
Memory Details
===============
Physical Memory : 16363364KB

VNIC Details
============
Name                      Mac Address     Driver Name       Status  Platform MTU
GigabitEthernet1   3cfd.fede.ccbc   net_i40e_vf        DOWN    1522
GigabitEthernet2   3cfd.fede.ccbd   net_i40e_vf        DOWN    1522

Hypervisor Details
====================
Hypervisor: KVM
Manufacturer: Red Hat
Product Name: KVM
Serial Number: Not Specified
UUID: 0E3546DD-DE6E-400D-9B3D-025215519CB8
image_variant :

Boot Details
====================
Boot mode: BIOS
Bootloader version: 1.1
```

KVM VMM を使用したコントローラへのインターフェイスの接続（virt-manager）

virt-manager で [Hardware] > [Add Hardware] を選択し、PCI ホストデバイスを VM に追加します。NIC カードに移動し、VM に接続する必要がある VF を選択します。

PCI が VM に追加されたら、VM を起動できます。

SR-IOV ドライバとファームウェアバージョンの確認

次のコマンドを使用して、イーサネットとドライバのバージョンを確認できます。

```
ethtool -i <interface_name>
```

（注） このコマンドは、ホストマシンで実行する必要があります。

```
[root@cpp-rhel-perf ~]# ethtool -i enp129s0f0
driver: i40e
version: 2.10.19.82
firmware-version: 7.10 0x8000646c 1.2527.0
expansion-rom-version:
bus-info: 0000:81:00.0
```

次のコマンドを使用して、イーサネット情報、ドライバのバージョン、および SR-IOV VF の名前を出力できます。

```
lspci | grep -i eth
```

```
[root@cpp-rhel-perf ~]# lspci | grep -i eth
81:00.0 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+
(rev 02)
81:00.1 Ethernet controller: Intel Corporation Ethernet Controller X710 for 10GbE SFP+
(rev 02)
81:02.0 Ethernet controller: Intel Corporation Ethernet Virtual Function 700 Series (rev
 02)
81:0a.0 Ethernet controller: Intel Corporation Ethernet Virtual Function 700 Series (rev
 02)
```

Intel NIC のファームウェアに関する詳細については、以下を参照してください。

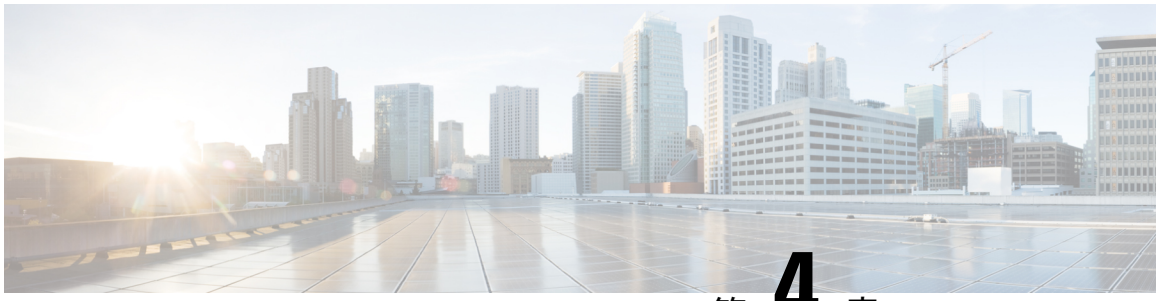
https://downloadcenter.intel.com/product/82947/Intel-Ethernet-Controller-X710-Series

Intel および Cisco NIC のドライバに関する詳細については、以下を参照してください。

https://downloadcenter.intel.com/download/24411/Intel-Network-Adapter-Driver-for-PCIe-40-Gigabit-Ethernet-Network-Connections-Under-Linux-?product=82947

Cisco NIC のファームウェアに関する詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/tsd-products-support-series-home.html



第 4 章

NFVIS 環境でのコントローラのインストール

Cisco Enterprise Network Function Virtualization Infrastructure ソフトウェアの概要

Cisco Enterprise Network Function Virtualization Infrastructure ソフトウェア（Cisco Enterprise NFVIS）は、サービス プロバイダーやエンタープライズが仮想ルータ、ファイアウォール、WAN 加速化などの仮想化ネットワーク機能をサポート対象のシスコのデバイス上へ容易に動的に導入できるようにする Linux ベースのインフラストラクチャ ソフトウェアす。ネットワーク機能それぞれのための物理デバイスの他に必要なものはありません。自動化されたプロビジョニングと一元化された管理を使用できます。

Cisco Enterprise NFVIS ソリューションは、重要なネットワーク機能をソフトウェアに容易に変換できるようにし、ネットワーク サービスを分散された場所に数分で導入できるようにします。仮想および物理の両方のデバイスから構成される多様なネットワークの上部で実行できる、完全に統合されたプラットフォームを実現します。

Cisco 5400 シリーズのエンタープライズ ネットワーク コンピューティング システムは、ルーティング、スイッチング、ストレージ、処理、ならびにその他のコンピューティングおよびネットワーキング アクティビティのホストを小型の 1-RU ボックス内で実現します。この高性能ユニットは、仮想化されたネットワーク機能を導入するためのインフラストラクチャを提供

し、処理、ワークロード、およびストレージに関する課題に対処するサーバとして機能することで、この目標を実現します。

インストール手順

VM ライフサイクルの管理とは、要件に応じて VM を登録し、導入し、更新し、監視して、それらの VM のサービスをチェーン化するプロセス全体を指しています。Cisco Enterprise NFVIS ポータルを使用して次のタスクを実行できます。

VM イメージの登録

VM イメージを登録するには、関連する VM イメージを最初に NFVIS サーバにコピーまたはダウンロードするか、あるいは HTTP または HTTPS サーバ上でイメージをホストする必要があります。ファイルをダウンロードしたら、登録 API を使用してイメージを登録できます。この API を使用すると、tar.gz ファイルをホストする場所（HTTP または HTTPS サーバ上）へのファイルパスを指定することができます。イメージの登録は 1 回限りのアクティビティです。イメージを HTTP または HTTPS サーバ上に登録し、アクティブな状態になると、登録されたイメージを使用して複数の VM 導入を実行できます。

セットアップのカスタマイズ

イメージファイルに定義されているプロファイルが要件に一致しない場合は、VM イメージを登録した後に、VM イメージのカスタムプロファイルまたはフレーバを必要に応じて作成できます。フレーバ作成オプションでは、VM が実行する仮想 CPU など、VM イメージの特定のプロファイリングの詳細や、VM が使用する仮想メモリの量を指定することができます。

トポロジ要件に応じて、導入時に VM に接続する追加のネットワークやブリッジを作成できます。

VM の導入

VM は導入 API を使用して導入できます。この API では、導入時にシステムに渡すパラメータに値を指定できます。導入する VM に応じて、必須のパラメータとオプションのパラメータがあります。

VM の管理とモニタリング

VM ステータスを取得したり、ログをデバッグできるようにするコマンドを使用して VM を監視できます。VM 管理 API を使用すると、VM を起動、停止、またはリブートでき、CPU 使用率などの VM の統計情報を表示できます。

また、VM はプロファイルを変更または更新することで管理することもできます。イメージファイル内の既存のプロファイルのいずれかに VM のプロファイルを変更できます。または、新しいカスタム プロファイルを VM に作成できます。VM 上の vNIC は追加または更新することもできます。

NFVIS でのイメージのアップロード

次に示す手順に従ってイメージを NFVIS にアップロードします。

ステップ 1 [VM Life Cycle] > [Image Repository] を選択します。

ステップ 2 [Image Registration] タブを選択し、[Images] の横にあるアップロード矢印をクリックします。

ステップ 3 [Drop Files or Click] オプションからファイルを選択します。

ステップ 4 [Start] をクリックしてイメージをアップロードします。

イメージをアップロードすると、NFVISはそれぞれのプロファイルを作成し、イメージを登録します。ファイルは同じページのイメージのセクションの下に表示されています。

Web インターフェイスを使用した VM パッケージの作成

次の示す手順に従い、Web インターフェイスを使用して VM イメージを作成します。

ステップ 1 ECNS から、[Image Packaging] タブを選択し、[VM Packages] の横にある [create] アイコンをクリックします。

ステップ 2 [Image Packaging] タブに詳細を入力します。

ステップ 3 [Submit] をクリックします。

ブートストラップ ファイルがアップロードされます。

イメージを作成したら、そのイメージを登録し、プロファイルが ENCS に適切に入力されるようにする必要があります。

ステップ 4 作成したイメージを選択し、[Register] をクリックします。

ネットワークの作成

次の手順に従ってネットワークを作成します。

ステップ 1 ECNS から、[VM Life Cycle] > [Networking] を選択します。

これにより、[Networks & Bridges] ウィンドウを開きます。

ステップ 2 [Networks & Bridges] の横にある [create] アイコンをクリックします。

ステップ 3 [Network]、[Mode]、[Vlan]、[Bridge]、および [Interface] に値を入力します。

（注） Single Root Input/Output Virtualization（SRIOV）はサポートされていません。

ステップ 4 [Submit] をクリックします。

これにより、ネットワークが作成されます。

NFVIS でのコントローラの導入

次の手順に従って、NFVIS にコントローラを導入します。

ステップ 1 ENCS から [VM Life Cycle] > [Deploy] を選択します。

これにより [VM Deployment] ウィンドウが開きます。

ステップ 2 [VM Deployment] ウィンドウで、[controller] **アイコン**を下のペインにドラッグ アンド ドロップし、必要に応じて適切なネットワークにマッピングします。

（注） サポートしている AP は 1,000、クライアントは 10,000 のみです。

ステップ 3 [VM Details] 領域で、**VM 名**を入力します。

ステップ 4 ドロップダウンで**イメージ** の名前を選択します。

ステップ 5 ドロップダウン リストで**プロファイル**の名前を選択します。

ステップ 6 VM を導入する前にブートストラップ設定ファイルを提供するため、[Bootstrap Config] オプションを選択します。

ブートストラップ設定ファイルに「iosxe_config.txt」というファイル名が使用されていることを確認します。

ステップ 7 [Deploy] をクリックします。

次のタスク

VM インスタンスを導入した後は、VM インスタンスの概要が示されている [Manage] タブでインスタンスの詳細を確認できます。

VM の横にある [Console] 記号をクリックし、コンソールへのアクセス権を取得します。

VM リソースの割り当ての表示

次の手順に従って、VM リソースの割り当てを表示します。

ステップ 1 ECNS から、[VM Life Cycle] > [Resource Allocation] を選択します。

これにより、CPU の割り当て全体が示された [VM CPU Allocation] タブが開きます。

ステップ 2 [VM Memory Allocation] タブをクリックします。

このタブにはメモリの割り当て全体が示されます。

ステップ 3 [VM Disk Allocation] タブをクリックします。

このタブにはディスクの割り当て全体が示されます。

VM 統計情報の表示

次の手順に従って、VM リソースの使用率を表示します。

ステップ 1 ECNS から [VM Life Cycle] > [VM Monitoring] を選択します。

これにより、VM ごとの CPU 使用率全体が表示された [VM CPU Utilization] タブが開きます。

ステップ 2 [Memory Allocation] タブをクリックします。

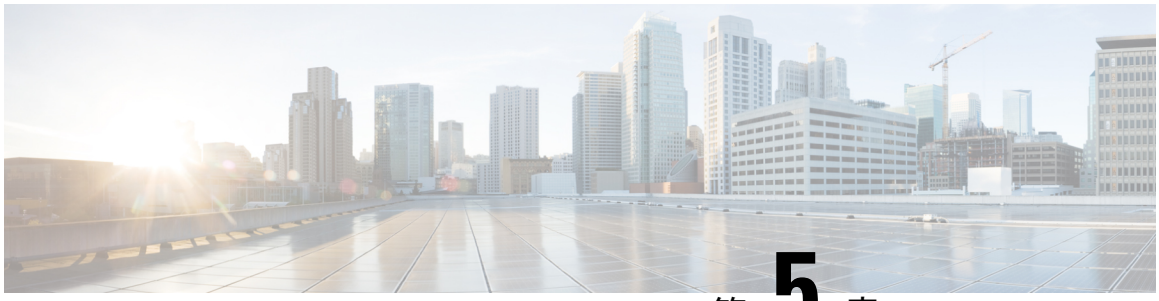
このタブには、VM あたりのメモリ使用率が表示されます。

ステップ 3 [VNIC Utilization] タブをクリックします。

このタブには、VM あたりの VNIC 使用率が表示されます。

ステップ 4 [Disk Utilization] タブをクリックします。

このタブには、VM あたりのディスク使用率が表示されます。



第 5 章

AWS 環境でのコントローラのインストール

Amazon Web Services の概要

コントローラは、パブリック クラウド ソリューション用に Amazon Web Service（AWS）に導入できます。

前提条件

AWS でコントローラの起動を試みる前に、次の前提条件を満たす必要があります。

- AWS アカウントを作成します。
- コントローラ コンソールにアクセスするには、SSH クライアント（Windows 場合の Putty、Macintosh の場合はターミナルなど）が必要です。
- 導入するインスタンス タイプを決定します。
- IAM ユーザを作成します。
- キー ペアを作成します。
- VPC を作成します。

- セキュリティ グループを作成します。
- VPN ゲートウェイを作成します。
- サブネットを作成します。
- リモート サイトごとに次を作成します。
  - カスタマ ゲートウェイを作成します。
  - VPN 接続を作成します。

一般情報

- パブリック クラウド内のすべてのインターフェイスがレイヤ 3 です。トランク インターフェイスはありません。
- パブリック クラウドのすべての IP 割り当てはパブリック クラウドの DHCP を使用して実行されます。コントローラに割り当てる IP を決めることができます。
- インターフェイスは 1 つのみがサポートされます。このインターフェイスはデバイス管理とワイヤレス管理で共有されます。

仮想プライベート クラウドの作成

次の手順に従って AWS で VPC を設定します。

始める前に

- VPC は AWS アカウント専用の仮想ネットワークで、AWS クラウド内の他の仮想ネットワークからは論理的に分離されています。
- VPC の IP アドレス範囲の指定、サブネットの追加、セキュリティ グループの関連付け、およびルート テーブルの設定を行えます。
- 必要に応じて、IPsec AWS 管理対象の VPN 接続を使用して VPC を会社のデータセンターに接続し、AWS クラウドをデータセンターとして拡張します。

（注） VPN 接続は、VPC に接続されている仮想プライベート ゲートウェイと、データセンターにあるカスタマ ゲートウェイで構成されます。仮想プライベート ゲートウェイは VPN 接続の Amazon 側の VPN コンセントレータです。カスタマ ゲートウェイは VPN 接続のユーザ側の物理デバイスまたはソフトウェア アプライアンスです。

ステップ 1 ナビゲーション パス（[AWS Console] > [VPC Dashboard] > [Launch VPC Wizard] > [VPC with a Private Subnet Only and Hardware VPN Access] ）を使用して VPN 設定を選択します。

ステップ 2 [VPC with a Private Subnet Only and Hardware VPN Access] ウィンドウで詳細を入力します。

ステップ 3 ナビゲーション パス（[VPC Console] > [Subnets] > [Create Subnet]）を使用してサブネットを作成します。

ステップ 4 ナビゲーション パス（[VPC Console] > [Security Groups] > [Create Security Group]）を使用してセキュリティ グループを作成します。

セキュリティ グループは、1 つ以上のインスタンスで発着信するトラフィックを制御する仮想ファイアウォールです。インスタンスが起動すると、1 つ以上のセキュリティ グループをそのインスタンスに関連付けることができます。インスタンスに対してデフォルトのセキュリティ グループを使用できますが、インスタンスのロールを反映するセキュリティ グループを作成することをお勧めします。

ステップ 5 [Create] をクリックします。

これにより VPC が作成されます。

仮想プライベート ゲートウェイの作成

次の手順に従って、AWS 仮想プライベート ゲートウェイを作成します。

始める前に

ステップ 1 [VPN Connections] > [Virtual Private Gateway] をクリックします。

[Create Virtual Private Gateway] ウィンドウが表示されます。次の詳細を入力します。

a) 名前タグを入力します。

AWS VPN ルータ名を使用します。

b) ASN を選択します。

カスタム ASN を使用するか、または Amazon ゲートウェイによって選択されたデフォルトの ASN のいずれかを使用します。

（注） AWS VPN ゲートウェイを作成した後は切断と表示されるため、VPC に接続する必要があります。

ステップ 2 [Actions] ボタンをクリックし、[Attach to VPC] を選択します。

ステップ 3 ポップアップ ウィンドウで、以前作成した VPC を選択します。

VPC に AWS VPN を接続します。

カスタマ ゲートウェイの作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 AWS コンソールから [VPC] ダッシュ ボードに移動します。

ステップ 2 [VPN Connections] > [Customer Gateways] をクリックします。

ステップ 3 [Create Customer Gateway] をクリックします。

[Create Customer Gateway] ウィンドウが表示されます。次の詳細を入力します。

a) VPN ルータの名前。
b) [dynamic] または [static] としてルーティングを選択します。
c) ルータまたはファイアウォールの外部のインターネットのルーティング可能なアドレスを入力します。

ステップ 4 [Create Customer Gateway] をクリックします。

VPN 接続の作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 AWS コンソールから [VPC] ダッシュ ボードに移動します。

ステップ 2 [VPN Connections] > [VPN Connections] をクリックします。

ステップ 3 [Create VPN Connection] をクリックします。

[Create VPN Connection] ウィンドウが表示されます。次の詳細を入力します。

a) VPN 接続の名前。
b) AWS VPN ゲートウェイとカスタム ゲートウェイを選択します。
c) [dynamic] または [static] としてルーティングを選択します。
d) VPN を通じて到達可能なリモート サブネットを入力します。

リモート サブネットは、AP がオンプレミスとなるリモート ネットワークです。

ステップ 4 （オプション）IPSEC VPN のトンネル インターフェイスにサブネットとキーを割り当てます。

AWS は冗長性を確保するために 2 つのインターフェイスを作成します。詳細を指定しなかった場合は、AWS はランダムにトンネル オブジェクトを生成します。

ステップ 5 [Create VPN Connection] をクリックします。

これにより、VPN 接続が作成されます。接続をセットアップし、ステータスを [pending] から [available] に変化させるまでに数分かかります。

ステップ 6 VPN を作成している間に、設定をダウンロードして、カスタマ VPN ルータに導入できます。[Download Configuration] をクリックします。

ステップ 7 ポップアップ ウィンドウで、カスタマ VPN ルータのブランドとタイプを選択します。

ステップ 8 [Download] をクリックします。

キー ペアの作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 AWS コンソールから **EC2** ダッシュ ボードに移動します。

ステップ 2 [Network & Security] > [Key pairs] をクリックします。

ステップ 3 [Create Key Pair] をクリックします。

Cloud Formation テンプレートを使用した AWS でのコントローラのインストール

始める前に

- VPC はコントローラ管理インターフェイスに適切なサブネットで作成します。
- エンタープライズ サイトから VPC に管理対象の VPN 接続が作成されます。
- AWS マーケットプレイスから CloudFormation テンプレートをダウンロードし、コンピュータに保存します。

ステップ 1 AWS コンソールから [CloudFormation] ページに移動します。

ステップ 2 [Create Stack] をクリックします。

ステップ 3 [Choose a template] セクションで、[upload template to Amazon S3] オプションを選択します。

これにより、*json* ファイルを AWS を直接ロードします。

ステップ 4 [Next] をクリックします。

これにより、[Specify Details] ページが表示されます。

ステップ 5 [Stack] と [Instance Details] に入力します。

必要なスタックの名前を入力します。ホスト名はコントローラの名前です。インスタンスのキー ペアはキー ペアの名前です。AMI ID は EC2 インスタンスの AMI です。

ステップ 6 [Next] をクリックします。

これにより、[Network Details] ページが開きます。

ステップ 7 [Network] と [User] に詳細を入力します。

管理ネットワークと管理セキュリティについては、ドロップダウンを使用してサブネットとセキュリティグループを選択します。ユーザ名とパスワードを入力し、インスタンスをリモートから接続します。

ステップ 8 [Next] をクリックします。

ステータスが「CREATE_IN_PROGRESS」から「CREATE_COMPLETE」に移行するまで待機します。

ステップ 9 [Instance Type] を選択します。

ステップ 10 **EC2** ダッシュボードに移動して [Running Instances] をクリックします。

新しいインスタンスは、[Status Checks]（システム ステータス チェックおよびインスタンス ステータス チェック）が [Initializing] と表示されます。緑色に変わるまで数分待ちます。

ステータスが緑色に変わったら、クラウドのコントローラを使用する準備が整います。定義されたクレデンシャルを使用するか、.pem ファイルを使用し、SSH で接続できます。

AWSコンソールを使用したコントローラのインストール

次の手順を従い、AWS コンソールでコントローラをインストールします。

ステップ 1 AWS コンソールから [EC2 Management] ページに移動します。

ステップ 2 [Launch Instance] をクリックします。

ステップ 3 [My AMIs] をクリックし、クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ の AMI を選択します。

ステップ 4 [Instance Type] を選択します。

要件に従ってインスタンスを選択することをお勧めします。

ステップ 5 [Instance Details] を設定します。

a) [Availability Zone] を選択します。
b) [Network] を選択します。
c) [Subnet] を選択します。
d) 他のユーザに、インスタンスの使用を制限または許可する IAM を関連付けます。

（注） 起動中にパブリック IP を無効にする必要があります。

ステップ 6 [Add Storage] ページに移動します。

このオプションのステップを使用して、インスタンスに接続する追加のボリュームを指定します。

ステップ 7 [Add Tags] ページに移動します。

a) [Tag Volumes] に入力します。

b) [Interfaces] を選択します。

c) [Instance] を選択します。

ステップ 8 [Configure Security Group] に移動します。セキュリティ グループを選択します。関連するセキュリティ グループがない場合は、新しいものを作成します。

ステップ 9 [Review and Launch] をクリックします。インスタンスの設定を確認します。

ステップ 10 [Launch Instances] をクリックします。

インスタンスを起動する前に、インスタンスにアクセスするキー ペアが必要です。キー ペアは、AWS が保存する公開キーとユーザが保存するプライベート キーで構成されます。キーがない場合は、[Create a new keypair] をクリックして新しいキーを作成するか、または既存のキーペアを選択します。

次のタスク

インスタンスが起動したら、次の unix コマンドを端末上で使用して クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ インスタンスに接続することができます。

```
ssh -i path_to_pem_file ec2-user@[public-ip|DNS name]
```

EC2 インスタンス コンソールのインスタンスの説明から IP と DNS 名を取得できます。

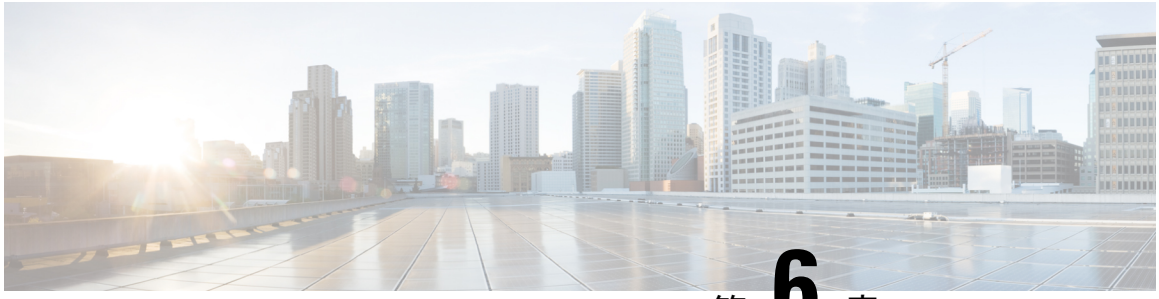
AWS のブートストラップのプロパティ

表 *9 : AWS* のブートストラップのプロパティ

プロパティ	説明
hostname	次の例に示すように、ルータのホスト名を設定します。 `hostname="c9800-aws-instance"`
domain-name	次の例に示すように、ネットワーク ドメイン名を設定します。 `domain-name="cisco.com"`
mgmt-ipv4-gateway	次の例に示すように、IPv4 管理用のデフォルトのゲートウェイ アドレスを設定します。 `mgmt-ipv4-gateway="dhcp"`

プロパティ	説明

ios-config	Cisco IOS コマンドの実行を有効にします。複数のコマンドを実行するには、複数の ios-config のインスタンスと各インスタンスに付加されている番号（ios-config-1、ios-config-2 など）を使用します。
	
	Cisco IOS コマンドを指定すると、エスケープ文字を使用してコマンド内にある特殊文字（アンパサンド（&）、二重引用符（”）、一重引用符（'）、よりも小さい（<）、またはよりも大きい（>））を渡します。次の例の「ios-config-5」を参照してください。
	
	`ios-config-1="username cisco priv 15 pass ciscoxyz"`
	`ios-config-2="ip scp server enable"`
	`ios-config-3="ip domain lookup"`
	`ios-config-4="ip domain name cisco.com”`
	`ios-config-5="event syslog pattern "\(Tunnel1\) is down: BFD peer down notified""`



第 6 章

GCP へのコントローラのインストール

GCP への クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ のインストール

クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ は Cisco IOS XE を実行している仮想コントローラです。Cisco IOS XE 機能のほとんどはクラウド コントローラで使用でき、Google Cloud Platform（GCP）にコントローラ ソフトウェアを導入することを選択できます。

GCP に クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ を展開するには、仮想マシン、インターフェイス、仮想プライベート クラウド （VPC）ネットワーク、ルート、パブリック IP アドレス、ファイアウォール ルール、およびストレージのリソースを使用してプロジェクトを作成する必要があります。異なるプロジェクトに存在するリソースは、外部ネットワークを介してのみ接続できます。

Google Compute Engine インスタンスは、Google 提供する Linux および Windows サーバのパブリック イメージと、既存のシステムから作成またはインポートできるプライベート カスタム イメージを実行できます。コンピューティング インスタンスは、SSH 公開キー認証を使用します。特定の Compute Engine リソースは、リージョンまたはゾーンに存在します。たとえば、インスタンスや永続ディスクなどのゾーン内に存在するリソースは、ゾーン リソースと呼ばれます。

静的な外部 IP アドレスなどの他のリソースはリージョナルです。リージョナル リソースは、ゾーンに関係なく、そのリージョン内のリソースで使用できますが、ゾーン リソースは同じゾーン内の他のリソースでしか使用できません。ファイアウォールを使用すると、セキュリ

ティ グループを使用して、インスタンスに到達できるプロトコル、ポート、および送信元 IP 範囲を指定できます。スタティック IPv4 アドレスは、ダイナミック クラウド コンピューティングに使用されます。メタデータ（タグとも呼ばれる）を使用すると、GCP コンピューティング リソースを作成して割り当てることができます。

GPC VPC の概念

- VPC ネットワークは、単にネットワークと呼ばれることもあり、データセンター ネットワークのような物理ネットワークの仮想バージョンです。
- GCP コンピューティング インスタンスなどの GCP クラウド リソースを VPC に起動できます。
- VPC の IP アドレス範囲の指定、サブネットの追加、セキュリティ グループの関連付け、およびルート テーブルの設定を行えます。
- 必要に応じて、IPsec GCP 管理対象の VPN 接続を使用して VPC を会社のデータセンターに接続し、GCP クラウドをデータセンターとして拡張します。

GCP での VPCの作成

次の手順に従って GCP で VPC ネットワークを設定します。

ステップ 1 GCP コンソールのナビゲーション メニューから、[VPCネットワーク（VPC network）] までスクロール ダウンし、[VPCネットワーク（VPC network）] を選択します。

ステップ 2 [CREATE VPC NETWORK] をクリックします。

ステップ 3 ネットワークの [名前（Name）] を入力します。

たとえば、 "custom-network1" を使用します。

ステップ 4 ネットワークの [説明（Description）] を入力します。

ステップ 5 [サブネット（Subnets）] セクションで [サブネットの追加（Add Subnet）] をクリックします。

[新規のサブネット（New subnet）] ダイアロ グボックスが開きます。サブネットの名前を入力します（例：*subnet-europe-west-192*）。

ステップ 6 [リージョン（Region）] を選択します。

たとえば、"europe-west1" を使用します。

ステップ 7 [IPアドレスの範囲（IP address range）] を入力します。

たとえば、"192.168.5.0/24" を使用します。

ステップ 8 [Done] をクリックします。

これにより、サブネットが作成されます。

ステップ 5 ー ステップ 9 を実行して、VPC ネットワークのサブネットを作成します。複数のサブネットをネットワークに追加できます。

ステップ 9 [作成（Create）] をクリックします。

これにより VPC ネットワークが作成されます。

ダイナミック ルーティングを使用した VPN 接続の作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 GCP コンソールから、[VPN] ページに移動します。

ステップ 2 [Create VPN Connection] をクリックします。

[Create VPN Connection] ウィンドウが表示されます。次の詳細を入力します。

a) **VPN ゲートウェイ**の名前。

b) **VPC** ネットワークを選択します。

VPN ゲートウェイがサービスを提供するインスタンスを含むネットワーク。

c) [リージョン（Region）] を選択します。

VPN ゲートウェイを検索するリージョン。通常、これは、到達する必要があるインスタンスを含むリージョンです。

d) **IP アドレス**を入力します。

既存のスタティック外部 IP アドレスを選択します。スタティック外部 IP アドレスを持っていない場合は、ドロップダウン メニューから [新しいスタティック IP アドレス（New static IP address）] をクリックして 1 つ作成します。

e) **Peer IP アドレス**を入力します。

ピア ゲートウェイのパブリック IP アドレス。

f) **IKE** バージョンを入力します。

IKEv2 は優先されますが、すべてのピア ゲートウェイで管理できる場合は IKEv1 がサポートされます。

g) [共有秘密（Shared Secret）] を入力します。

そのトンネルの暗号化の確立に使用される文字列。両方の VPN ゲートウェイに同じ共有秘密を入力する必要があります。トンネルのピア側の VPN ゲートウェイ デバイスが自動的に生成しない場合は、[生成（Generate）] オプションを使用して 1 つ作成できます。

h) [ルーティングオプション（Routing Option）] を選択します。

i) 詳細を入力して、**クラウド ルータ**を作成します。[保存して続行（Save and Continue）] をクリックします。

ステップ 3 クラウド ルータを作成します。

a) **GOOGLE ASN** を入力します。

設定しているルータのプライベート ASN (64512-65534、42億-4294967294)。これは、まだ使用していないプライベート ASN である可能性があります。たとえば、65002 とします。

AWS は冗長性を確保するために 2 つのインターフェイスを作成します。詳細を指定しなかった場合は、AWS はランダムにトンネル オブジェクトを生成します。

ステップ 4 **BGP** セッションの詳細を入力します。

a) BGP の名前を入力します。

b) **Peer ASN** を入力します。

設定しているルータのプライベート ASN (64512-65534、42億-4294967294)。これは、まだ使用していないプライベート ASN である可能性があります。たとえば、65001 とします。

c) **GOOGLE BGP IP アドレス** を入力します。

BGP インターフェイスの IP アドレスは、169.254.0.0/16 にある同じ /30 サブネットに属するリンク ローカル IP アドレスである必要があります。たとえば、169.254.1.1 です。

d) **Peer BGP IP アドレス**を入力します

AWS は冗長性を確保するために 2 つのインターフェイスを作成します。詳細を指定しなかった場合は、AWS はランダムにトンネル オブジェクトを生成します。

ステップ 5 [作成（Create）] をクリックします。

これにより、ゲートウェイ、クラウドルータ、およびすべてのトンネルが作成されます。ピア ルータが設定されるまで、トンネルは接続されないことに注意してください。

次のタスク

ピア ネットワーク サブネットからの着信トラフィックが許可されるように VPN のファイアウォール ルールを設定します。

スタティック ルーティングを使用した VPN 接続の作成

次の手順に従ってカスタマ ゲートウェイを作成します。

ステップ 1 GCP コンソールから、[VPN] ページに移動します。

ステップ 2 [Create VPN Connection] をクリックします。

[Create VPN Connection] ウィンドウが表示されます。次の詳細を入力します。

a) **VPN ゲートウェイ**の名前。

b) **VPC** ネットワークを選択します。

VPN ゲートウェイがサービスを提供するインスタンスを含むネットワーク。このネットワークがオンプレミス ネットワークと競合していないことを確認します。

c) [リージョン（Region）] を選択します。

VPN ゲートウェイを検索するリージョン。通常、これは、到達する必要があるインスタンスを含むリージョンです。

d) **IP アドレス**を入力します。

既存のスタティック外部 IP アドレスを選択します。スタティック外部 IP アドレスを持っていない場合は、ドロップダウン メニューから [新しいスタティックIPアドレス（New static IP address）] をクリックして 1 つ作成します。

e) **Peer IP アドレス**を入力します。

ピア ゲートウェイのパブリック IP アドレス。

f) **IKE** バージョンを入力します。

IKEv2 は優先されますが、すべてのピア ゲートウェイで管理できる場合は IKEv1 がサポートされます。

g) [共有秘密（Shared Secret）] を入力します。

そのトンネルの暗号化の確立に使用される文字列。両方の VPN ゲートウェイに同じ共有秘密を入力する必要があります。トンネルのピア側の VPN ゲートウェイ デバイスが自動的に生成しない場合は、[生成（Generate）] オプションを使用して 1 つ作成できます。

h) **リモート ネットワークの IP** の範囲を入力します。

例：10.0.0.0/8. 現在設定している Cloud VPN ゲートウェイからのトンネルの反対側のネットワークのピア ネットワークの範囲です。

i) **ローカル サブネット**を指定します。

トンネルを介してルーティングされる IP 範囲を指定します。この値は、IKE ハンドシェイクで使用されるため、トンネルの作成後に変更することはできません。

j) **ゲートウェイ サブネット**を指定します。

ローカルサブネットがデフォルトのオプションであるため、空白のままにしておくことができます。

k) **ローカル IP** の範囲を入力します。

ゲートウェイのサブネットを除き、空白のままにしておくことができます。

ステップ 3 [作成（Create）] をクリックします。

これにより、ゲートウェイが作成され、すべてのトンネルが開始されます。ピア ルータが設定されるまで、トンネルは接続されないことに注意してください。

次のタスク

ピア ネットワーク サブネットからの着信トラフィックが許可されるように VPN のファイアウォール ルールを設定します。

ファイアウォール ルールの作成

ファイアウォール ルールにより、ピア ネットワーク サブネットからの着信トラフィックが許可されます。また、コンピューティング エンジンプ レフィックスからの着信トラフィックが許可されるように、ピア ネットワーク ファイアウォールを設定する必要があります。

トラフィックが VM インスタンスに渡されるようにするには、ファイアウォール ルールを作成します。

ステップ 1 Google Cloud Platform コンソールのナビゲーション メニューから、[VPCネットワーク（VPC network）] までスクロール ダウンし、[ファイアウォールルール（Firewall Rules）] を選択します。

ステップ 2 [CREATE FIREWALL RULE] をクリックし、詳細を入力します。

a) ファイアウォール ポリシーの**名前**を入力します。

b) **VPC ネットワーク**を入力します。

c) **送信元フィルタ**を入力します。

最大 4 つの異なる送信元フィルタ タイプを使用してトラフィックをフィルタリングすることを選択します。

たとえば、送信元 IP 範囲を指定する場合は、0.0.0.0/0 を入力して任意の IP アドレスを選択できます。

d) **送信元 IP の範囲**を入力します

0.0.0.0/0（ネットワーク内のすべての IP 範囲を選択します）。

e) 許可されたプロトコルとポートを入力します。

プロトコルとポートの範囲。

複数のプロトコルとポート範囲が組み合わされています。例：「icmp」、「udp：4789-4790」、「tcp：0-6553」。

ステップ 3 [作成（Create）] をクリックします。

ファイアウォール ルールを作成します。別のファイアウォール ルールを追加するには、上記の手順を繰り返します。

GCP へのコントローラのインストール

GCP にコントローラ インスタンスを展開するには、次の手順を使用します。

始める前に

GCP にコントローラを導入する場合は、次の前提条件が適用されます。

- GCP を使用したユーザ アカウントまたはサブスクリプション。
- クラウド アイデンティティとアクセス管理（IAM）ユーザ
- VPC。
- サブネット。
- セキュリティ グループ。
- VPN 接続。
- リモート サイトごとに次を作成します。
  - カスタマ ゲートウェイ
  - VPN 接続

ステップ 1 [コンピューティングエンジン（Compute Engine）] および [VMインスタンス（VM Instances）] をクリックします。

ステップ 2 [CREATE INSTANCE] をクリックします。

ブートディスクを選択して、新しいコントローラ VM インスタンス（「OS イメージ」またはカスタム イメージから）を作成し、次のフィールドに値を入力します。

a) **名前**を指定します。

小文字のみを使用して VM の名前を指定します。

b) **リージョン**を指定します。

c) **ゾーン**を指定します。

ゾーンは、多くの場合、リージョン内のデータ センターです。

d) **マシン タイプ**を選択します。

Small（4 CPU、8 GB RAM)、Medium（8 CPU、16 GB RAM）、および Large（10 CPU、32 GB RAM）プロファイルをサポートします。

e) （オプショナル）[カスタマイズ（Customize）] をクリックして、コア（vcpus）、メモリ サイズ、および GPU の数を選択します。

ステップ 3 コンテナは選択しないでください。

ステップ 4 ブート ディスクの [変更（Change）] をクリックします。

ステップ 5 [OSイメージ（OS Images）] タブに移動し、オプション ボタンを使用して必要なイメージを選択します。

（注）
- カスタム イメージは、初期インスタンスでのみ必要です。
- ブート ディスクは変更しないでください。

GCP へのコントローラのインストール

ステップ 6 [Select] をクリックします。

ステップ 7 [ファイアウォール（Firewall）] セクションで、[HTTP（allow HTTP traffic）] または [HTTPSトラフィックの許可（Allow HTTPS traffic）] のいずれかを選択し、 Web UI にアクセスします。

ステップ 8 [削除の保護（Deletion protection）] セクションで、インスタンスが削除されないようにするには、[削除保護の有効化（Enable deleted protection)] チェックボックスをオンにします。

ステップ 9 [自動化（Automation）] セクションで、**スタートアップ** スクリプトを指定します。

これにより、インスタンスがブートアップまたは再起動されたときにスクリプトを実行することができます。

このセクションを使用して、インスタンスにアクセスするためのユーザ名とパスワードを追加します。

Cisco IOS コマンドを指定すると、エスケープ文字を使用してコマンド内にある特殊文字（アンパサンド（&）、二重引用符（”）、一重引用符（'）、よりも小さい（<）、またはよりも大きい（>））を渡します。次に例を示します。

```
Section: IOS configuration
hostname ewlc
username cisco priv 15 pass 0 cisco
!if you want to add more IOS commands, you can add here
Section: Scripts
Section: Python Package
```

ステップ 10 [管理、セキュリティ、ディスク、ネットワーキング、単独のテナント（Management, Security, Disks, Networking, Sole Tenancy）] セクションから、[ネットワーキング（Networking）] タブをクリックします。

ステップ 11 **ネットワーク タグ**に SSH キー情報を追加します。

ステップ 12 [ネットワークインターフェイスの追加（Add network interface）] をクリックします。

ステップ 13 [ネットワークインターフェイス（Networking Interface）] ダイアログ ボックスで、デフォルトのインターフェイスを選択します。

たとえば、デフォルトのセキュリティ グループは 10.142.0.0.0/20 です。

ステップ 14 [ネットワークインターフェイス（Networking Interface）] ダイアログ ボックスで、デフォルトのインターフェイスを選択します。

ステップ 15 **IP フォワーディング**を **On** に設定します。

これにより、トラフィックがブロックされなくなります。

ステップ 16 **プライマリ内部 IP**を一時的（自動）として設定します。

このプライベート IP アドレスは、選択したサブネットから自動的に取得されます。

ステップ 17 **外部 IP** を一時的（自動）として設定します。

ターミナルサーバから SSH セッションを開始するときに、このパブリック IP アドレスを使用できます。この外部 IP アドレスをスタティックとして指定することもできます。各インターフェイスの外部 IP アドレスは、一時的または静的のいずれかです。

ステップ 18 [Done] をクリックします。

最初のインターフェイスを作成します。

ステップ 19 [作成（Create）] をクリックします。

新しく作成されたコントローラ VM インスタンスが起動します。起動プロセスが完了するまで数分かかる場合があります。

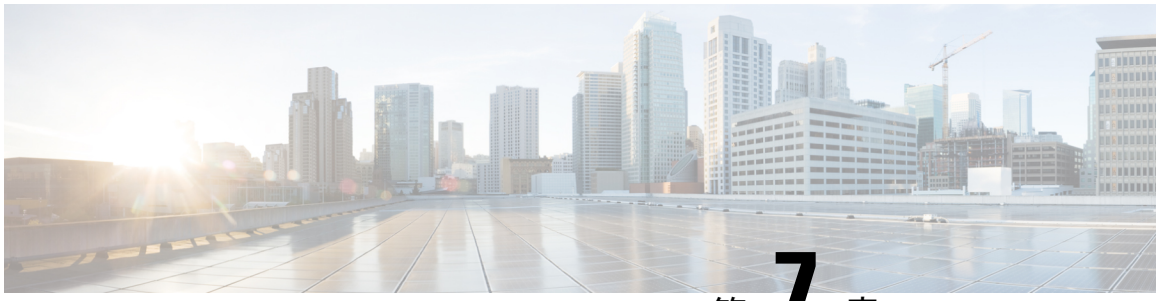
GCP 上のコントローラ インスタンスへのアクセス

設定が完了すると、SSH を使用してコントローラに接続できます。そのためには、SSH の秘密キーが必要です。

以下の手順に従って、SSH を使用して GCP のコントローラにアクセスします。

- コマンド、**ssh -i** *private-key-file-path sername-in-key@ip-address-of-eth1* を入力します。
- または、ブート時に IOS コマンドを使用して作成されたユーザ名とパスワードを使用してログインします。**ssh** *username@ ip-address-of-eth1*

```
ssh -i user1.key user1@35.100.100.50
or
ssh user1@35.100.100.50
```



第 7 章

Microsoft Hyper-V ハイパーバイザへのコントローラのインストール

Microsoft Hyper-V のサポート情報

Microsoft Hyper-V に Catalyst 9800-CL Cloud ワイヤレスコントローラをインストールするには、.iso ファイルを使用して VM を手動で作成し、インストールする必要があります。

次の Microsoft Hyper-V 機能がサポートされています。

- Snapshot
- エクスポート
- Hyper-V レプリカ

Microsoft Hyper-V の詳細については、Microsoft のマニュアルを参照してください。

（注） Microsoft Hyper-V VM の実行中に、次のトレースバックログがコンソールで継続的に取得されることがあります。

```
"PLATFORM_INFRA-5-IOS_INTR_OVER_LIMIT_HIGH_STIME: IOS thread blocked due to SYSTEM LEVEL
ISSUE"
```

この問題を回避するには、次の手順を実行します。

1. 以下で指定したコマンドを使用して、シリアルモードでコントローラを設定します。

```
Device# configure terminal
Device(config)# platform console serial
Device(config)# end
Device# reload
```

2. 次のコマンドを実行します。

```
PS C:\> Set-VMComPort TestVM 1 \\.\pipe\TestPipe
```

3. コンソールにアクセスするには、Putty を管理モードで使用します。

Microsoft Hyper-V のインストール要件

Microsoft Hyper-V VM にコントローラをインストールする前に、次をホストにインストールする必要があります。

- Hyper-V マネージャ
- Failover Cluster Manager
- 仮想スイッチ

（注） VM を作成する前に仮想スイッチを作成しておくことを推奨します。

ハードウェアプロファイルと推奨されるリソースを以下の表に示します。

表 *10* : ハードウェア要件

設定	小規模	中規模	大規模
vCPU の最小数	4	6	10
最小メモリ	8 GB	16 GB	32 GB
ストレージが必要	16 GB	16 GB	16 GB
vNIC の最小数	2	2	2

設定	小規模	中規模	大規模
最大のアクセスポイント	1000	3000	6000
最大のクライアントサポート	10,000	32,000	64,000

VM の作成

VM を作成するには、次の手順を実行します。

（注） Microsoft Hyper-V Manager または Microsoft System Center VMM を使用して、Microsoft Hyper-V にコントローラをインストールできます。

ステップ 1 Hyper-V Manager で、ホストをクリックします。

ステップ 2 [New] > [Virtual Machine] を選択します。

ステップ 3 [Specify Name and Location] をクリックします。

- VM の名前を入力します。
- （オプション）VM を別の場所に保存するには、チェックボックスをオンにします。

ステップ 4 [Next] をクリックします。

ステップ 5 [Specify Generation] 画面で、ロードするマシンの世代を指定します。

（注） 第 1 世代か第 2 世代かの選択は、要件によって異なります。第 2 世代は、Small Computer System Interface（SCSI）からのブート、セキュアブート、より高いハードウェア制限、Unified Extensible Firmware Interface（UEFI）BIOS、GUID パーティションテーブル（GPT）によるパーティション分割などの高度な機能をサポートしています。第2世代が選択されている場合は、コントローラがセキュアブートをサポートしていないため、展開後に [Enable Secure Boot] チェックボックスをオフにしてください。

ステップ 6 [Assign Memory] 画面で、[Startup Memory] の値を入力します。

コントローラの起動メモリ用として、8196 MB が必要です。

ステップ 7 [Next] をクリックします。

ステップ 8 [Configure Networking] 画面で、以前に作成した仮想スイッチへのネットワーク接続を選択します。

この手順で選択したネットワークアダプタは、VM を起動してルータをブートしたときに、コントローラの最初のインターフェイスになります。VM の他の vNIC は、次の手順で作成します。

ステップ 9 [Next] をクリックします。

ステップ 10 [Connect Virtual Hard Disk Screen] で、次のオプションを選択します。

- 仮想ハードディスクは後で接続します。

（注） 新規仮想マシンウィザードでは、.vhdx 形式を使用した仮想ハードディスクの作成のみがサポートされています。コントローラのハードディスクでは、.vhd 形式を使用する必要があります。VM が作成されたら、仮想ハードディスクを作成します。

ステップ 11 [Next] をクリックします。[Summary] 画面が表示されます。

ステップ 12 VM の設定を確認し、問題ないようであれば [Finish] をクリックします。

これで、新しい VM が作成されます。

VM 設定の構成

VM を起動する前に構成を設定するには、次の手順を実行します。

始める前に

インスタンスを起動する前に、ネットワークアダプタ（適宜）とディスクを追加して、.iso イメージをディスクドライブにロードします。

管理、ワイヤレス管理、および高可用性用に個別のネットワークインターフェイスを作成して使用することを推奨します。HA 展開の場合は、ネットワーク インターフェイスを 3 つ作成し、VM を適切なネットワークに接続します。HA 以外の展開では、ネットワーク インターフェイスを 2 つ作成します。

管理、ワイヤレス管理、および HA ネットワークの作成は、VM を起動する前に行う必要があります。これらのインターフェイスの IP アドレスは、静的または DHCP のいずれかであり、ブートストラップ設定の一部として設定する必要があります。

最初に接続されたネットワークが管理に使用され、2 番目がワイヤレス管理（明示的に設定されている場合を除く）、3 番目が HA に使用されるため、ネットワークがインターフェイスに接続される順序が重要となります。

ステップ 1 Hyper-V Manager でホストを選択し、前の手順で作成した VM を右クリックします。

ステップ 2 [設定（Settings）] を選択します。

ステップ 3 VM の仮想 CPU（vCPU）とも呼ばれる仮想プロセッサの数を指定します。

ステップ 4 [IDE Controller 0] で、[Hard Drive] を選択します。

[Virtual Hard Disk] チェックボックスをオンにして [New] をクリックし、新しい仮想ハードディスクを作成します。

新規仮想ハードディスクウィザードが開きます。[Next] をクリックします。

a) [Choose Disk Format] 画面で、[VHD] チェックボックスをオンにして、.vhd 形式で仮想ハードディスクを作成します。[Next] をクリックします。
b) [Choose Disk Type] 画面で、[Fixed Size] オプションをクリックします。[Next] をクリックします。
c) 仮想ハードディスクの名前と場所を指定します。[Next] をクリックします。
d) [Configure Disk] 画面で、空の仮想ハードディスクを新規作成するオプションをクリックします。サイズには 16 GB を指定します。
e) [Next] をクリックして、仮想ハードディスク設定の概要を表示します。
f) [Finish] をクリックすると、新しい仮想ハードディスクが作成されます。

新しいハードディスクが作成されたら、次の手順で VM の設定を続行します。

ステップ 5 [IDE Controller1] で [DVD Drive] を選択します。

[DVD Drive] 画面が表示されます。

[Media] 設定で、[Image File] チェックボックスをオンにし、Cisco.com からダウンロードした .iso ファイルを参照します。

ステップ 6 [OK] をクリックします。

ステップ 7 [Network Adapter] を選択して、仮想スイッチへのネットワーク接続が設定されていることを確認します。

ステップ 8 [Com 1] を選択して、シリアルポートを設定します。

このポートによって、コントローラコンソールへアクセスできます。

ステップ 9 [Hardware] > [Add Hardware] を選択して、ネットワーク インターフェイス（vNIC）を VM に追加します。

a) [Network Adapter] を選択して、[Add] をクリックします。

Microsoft Hyper-V によってネットワークアダプタが追加され、仮想スイッチのステータスが [Not Connected] のハードウェアが強調表示されます。

b) ドロップダウンメニューで仮想スイッチを選択し、その上にネットワークアダプタを配置します。

vNIC ごとに上記手順を繰り返します。コントローラは、HV NETVSC vNIC タイプのみをサポートします。サポートされる vNIC の最大数は 8 です。

（注） vNIC のホットアドは Microsoft Hyper-V ではサポートされていないため、VM を起動する前にネットワーク インターフェイスを追加しておく必要があります。

コントローラのブート後、**show platform software vnic-if interface-mapping** コマンドを使用して、vNIC と vNIC をインターフェイスへマッピングする方法を確認できます。

ステップ 10 [BIOS] をクリックして、VM のブートシーケンスを確認します。

VM は CD からブートするように設定する必要があります。

コントローラをブートするための VM の起動

VM を起動するには、次の手順を実行します。

ステップ 1 仮想スイッチを選択します。

ステップ 2 VM を選択し、[Start] をクリックします。

Hyper-V Manager が VM に接続され、起動プロセスが開始されます。VM が起動すると、コントローラはブートプロセスを開始します。

タグ付きポートの設定

タグ付きポートの設定は、ホスト OS で実行されます。デフォルトでは、VLAN のタグ付きパケットが vNIC のホスト OS でドロップされます。これらのパケットがコントローラを経由するようにするには、コントローラに特定の vNIC をタグ付きとして設定します。

（注） GUI を使用してネットワーク インターフェイスを作成する場合、インターフェイス名を指定することはできず、すべてのインターフェイスの名前が「ネットワークアダプタ」となります。したがって、これらのコマンドを使用すると、コントローラ内のすべてのネットワークアダプタをタグ付きに変換できます。

これらのコマンドは、Power Shell で入力します。

ステップ 1 アダプタと割り当てのリストを表示するには、次のスクリプトを使用します。

```
Get-VMNetworkAdapter -VMName <C9800-name>
```

（注） アダプタ名を変更するには、次のコマンドを使用します。

```
Rename-VMNetworkAdapter -VMName <C9800-name> -Name '<C9800-adapter-name>' -NewName 'Eth1'
```

ここでは、**Eth1** がアダプタ名です。

ステップ 2 Ethernet1（データポート/管理）をトランクとして設定し、ネイティブ VLAN ID を 0 に設定するには、次のスクリプトを使用します。

```
Set-VMNetworkAdapterVlan -VMName “C9800” -VMNetworkAdapterName Eth1 -Trunk -AllowedVlanIdList “1-4000”
 -NativeVlanId 0
```

ステップ 3 Ethernet0（シリアルポート）をアクセスまたはタグなしとして設定するには、次のスクリプトを使用します。

```
Set-VMNetworkAdapterVlan -VMName “C9800” -VMNetworkAdapterName Eth0 -Untagged
```

ステップ 4 トランクポートがタグ付きトラフィックを通過できるようにするには、MACアドレススプーフィングを有効にします。

MAC アドレススプーフィングを有効にするには、次の手順を実行します。

1. 仮想マシンを選択し、[Actions] > [Settings] を選択します。
2. [Network Adapter] を展開し、[Advanced Features] を選択します。
3. [Enable MAC Address spoofing] を選択します。

ブートストラップのデイゼロ設定の作成

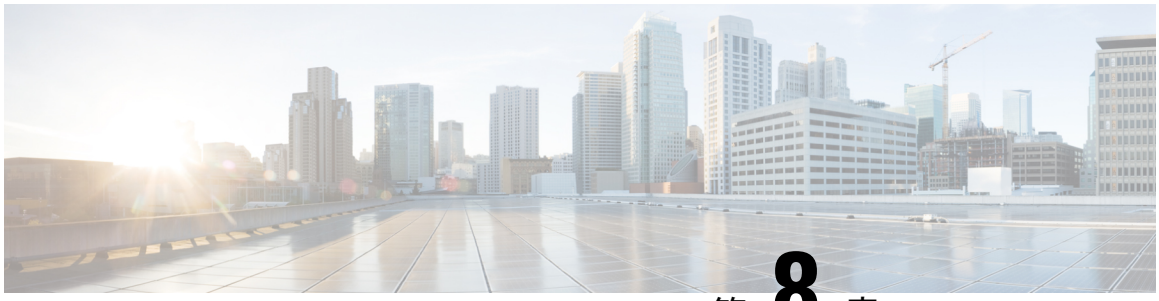
Linux サーバで次の手順を実行します。

ステップ 1 **iosxe_config.txt** ファイルまたは **ovf-env.xml** ファイルを作成します。

ステップ 2 次のコマンドを使用して、このファイルからディスクイメージを作成します。

```
mkisofs -l -o ./c9800_config.iso <configuration_filename>
```

ステップ 3 仮想マシンの作成中に c9800_config.iso を追加ディスクとしてマウントし、VM の電源をオンにします。



第 8 章

コントローラのブートとコンソールへのアクセス

パブリック クラウドのデイ ゼロ Web UI ウィザード

次の手順に従って、デイ ゼロ設定を作成し、コントローラにプッシュします。

ステップ 1 Web ブラウザのアドレス バーで、コントローラの **IP アドレス**を入力します。

ステップ 2 [Username] と [Password] を入力します。

これにより [Configuration Setup Wizard] ウィンドウが表示されます。

次のように [General Settings] ウィンドウに詳細を入力します。

a) [Deployment Mode] を選択します。
b) [Country] を選択します。
c) [Date] を選択します。
d) [Time] に入力するか、またはドロップダウン リストを使用して [Timezone] を選択します。
e) [NTP Servers] に名前を入力します。
f) [AAA Servers] に名前を入力します。

ステップ 3 次のように [Wireless Management Settings] に入力します。

a) [Port Number] を選択します。
b) [IP Address] を選択します。

ステップ 4 [Next] をクリックします。

ステップ 5 次のように [Wireless Network Settings] に入力します。

a) **ネットワーク名**を入力します。

b) [Network Type] を選択します。
c) ドロップダウンを使用して [Security] オプションを選択します。
d) **事前共有キー**を入力します。
e) [Add] をクリックします。

（注） 3 つのワイヤレス ネットワーク設定を入力します。ワイヤレス管理用に 1 つ、デバイス管理用に 1 つ、ゲスト管理用に 1 つ以上が必要です。

ステップ 6 [Next] をクリックします。

これにより [Advanced Settings] ページが開きます。

ステップ 7 [Advanced Settings] ページに詳細情報を入力します。

a) スライダを使用して [Client Density] を選択します。
b) **RF グループ名**を入力します。
c) ドロップダウン リストを使用して、[Traffic Type] を選択します。
d) **仮想 IP アドレス**を入力します。
e) [Generate Certificate] スライダを使用して AP の証明書を生成します。

この証明書は AP がコントローラに参加するために必要です。

f) ドロップダウン リストを使用して [RSA Key-Size] を選択します。
g) [Signature Algorithm] に入力します。
h) [Password] を入力します。
i) [Summary] ページで詳細を確認します。

ステップ 8 [Finish] をクリックします。

ステップ 9 [Yes] をクリックします。

これにより設定が作成され、コントローラにプッシュされます。

プライベート クラウドのデイ ゼロ Web UI ウィザード

次の手順に従って、デイ ゼロ設定を作成し、コントローラにプッシュします。

ステップ 1 Web ブラウザのアドレス バーで、コントローラの **IP address** を入力します。

ステップ 2 [Username] と [Password] を入力します。

これにより [Configuration Setup Wizard] ウィンドウが表示されます。[General Settings] ウィンドウに詳細を入力します。

a) [Deployment Mode] を選択します。
b) [Country] を選択します。
c) [Date] を選択します。

d) [Time] に入力するか、またはドロップダウン リストを使用して [Timezone] を選択します。
e) [NTP Servers] に名前を入力します。
f) [AAA Servers] に名前を入力します。

ステップ 3 次のように [Service Port Settings] に入力します。

a) [DHCP] を選択します。
b) **スタティック IP** アドレスを入力します。
c) **サブネット マスク**を入力します。

ステップ 4 次のように [Static Route Settings] に入力します。（オプション）

a) **IP アドレス**を入力します。
b) **サブネット マスク**を入力します。
c) **ゲートウェイ** アドレスを入力します。

ステップ 5 次のように [Wireless Management Settings] に入力します。

a) [Port Number] を選択します。
b) **VLAN** を入力します。
c) [IPv4] または [IPv6] を選択します。
d) **ワイヤレス管理 IP** アドレスを入力します。
e) **サブネット マスク**を入力します。
f) **管理 VLAN の DHCP サーバ**を入力します。

ステップ 6 [Next] をクリックします。

これにより、[Wireless Network Settings] ページが開きます。

ステップ 7 次のように [Wireless Network Settings] に入力します。

a) **ネットワーク名**を入力します。
b) [Network Type] を選択します。
c) ドロップダウンを使用して [Security] オプションを選択します。
d) **事前共有キー**を入力します。
e) [Add] をクリックします。

（注） 3 つのワイヤレス ネットワーク設定を入力します。ワイヤレス管理用に 1 つ、デバイス管理用に 1 つ、ゲスト管理用に 1 つ以上が必要です。

ステップ 8 [Next] をクリックします。

これにより [Advanced Settings] ページが開きます。

ステップ 9 [Advanced Settings] ページに詳細情報を入力します。

a) スライダを使用して [Client Density] を選択します。
b) **RF グループ名**を入力します。
c) ドロップダウン リストを使用して、[Traffic Type] を選択します。
d) **仮想 IP アドレス**を入力します。
e) 高可用性の**ローカル IP**、**サブネット マスク**、**リモート IP**を入力します。

（注） 導入モードが [ACTIVE] に設定されている場合にだけ使用できます。

f) [Generate Certificate] スライダを使用して AP の証明書を生成します。

この証明書は AP がコントローラに参加するために必要です。

g) ドロップダウン リストを使用して [RSA Key-Size] を選択します。

h) [Signature Algorithm] に入力します。

i) **AP パスワード**を入力します。

j) [Summary] ページで詳細を確認します。

ステップ 10 [Finish] をクリックします。

ステップ 11 [Yes] をクリックします。

これにより設定が作成され、コントローラにプッシュされます。

コントローラのブート

VM に電源が投入されるとコントローラがブートします。設定によっては、仮想 VGA コンソールでのインストール プロセスを監視できます。

次の手順に従ってコントローラをブートします。

1. VM の電源をオンにします。VM の電源投入後 5 秒以内にステップ 2 からステップ 4 で説明したコンソールを選択し、デバイスのブートアップを表示してコントローラ CLI にアクセスします。
2. （オプション）[Auto Console] をクリックして自動コンソール検出を使用します。これがデフォルトの設定であり、5 秒以内に別のオプションが選択されていなかった場合は、自動コンソール検出を使用してコントローラがブートします。
3. （オプション）[Virtual Console] をクリックし、仮想 VGA コンソールを使用します。仮想コンソールを選択した場合は、この手順の残りのステップは適用されません。コントローラがブート プロセスを開始します。
4. 次のコマンドのいずれかを使用して、VM に Telnet で通信します。
   - **telnet://***host-ipaddress:portnumber*
   - **telnet***host-ipaddress portnumber*（UNIX xTerm 端末から）
5. ブート後、メインのソフトウェア イメージおよびゴールデン イメージと、強調表示されたエントリを 3 秒以内に自動的にブートする手順が表示されます。ゴールデン イメージのオプションを選択せず、メインのソフトウェア イメージをブートさせます。

（注） 設定のバックアップを復元している間は、**platform console serial** を追加しないでください。コントローラが grub モードで起動し、復元できなくなる可能性があります。

仮想VGAコンソールを通じたコントローラへのアクセス

デイゼロバナーの後にワイヤレス設定のプロンプトが表示されます。

作成後に設定を変更する方法については、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide』および『Cisco Catalyst 9800 Series Wireless Controller Command Reference Guide』を参照してください。

ここでは、次のトピックについて取り上げます。

- デバイス管理インターフェイスの設定。
- デバイス管理 IP の設定。
- （オプション）静的ルートの設定。
- 管理クレデンシャルの設定。
- ワイヤレス管理インターフェイスの設定。
- 展開モードの選択。
- システム名またはホスト名の設定。
- アクセスポイントでの管理アクセスのログイン情報の設定。
- 国コードの設定。
- NTP サーバを使用するか手動での時刻の設定。
- （オプション）タイムゾーンの設定。
- （オプション）ワイヤレスクライアント密度の設定。
- （オプション）AAA サーバの設定。
- （オプション）ワイヤレスネットワーク設定の構成。
- （オプション）ネットワーク名または SSID の設定。
- （オプション）仮想 IP の設定。
- （オプション）RF ネットワーク名の設定。
- （オプション）自己署名証明書の設定。
- （オプション）高可用性の設定。

（注） 現在、以前の設定に戻す直接的な方法はありません。**Ctrl+C** を押して設定を再起動し、保存せずにセットアップに戻ります。

コントローラのデイゼロ CLI ウィザード

ステップ 1 **write erase** コマンドを使用するか、デイゼロデバイスで直接、デイゼロ セットアップ ウィザードを開始できます。

ステップ 2 デバイス管理インターフェイスのセットアップでは、デバイス管理またはサービスポートを設定します。このインターフェイスにより、GUI を使用してデバイスにアクセスするための基本設定が可能になります。これはオプションの設定で、デバイス管理ではなくワイヤレス管理インターフェイスのみを設定できます。

```
Configure device management interface?[yes]:
```

（注） Cisco Catalyst 9800-CL Cloud ワイヤレスコントローラには、専用のデバイス管理ポートがありません。したがって、指定された範囲からいずれかのオプションを選択するように求められます。

```
Select interface to be used for device management
1. GigabitEthernet1 [Up]
2. GigabitEthernet2 [Up]
3. GigabitEthernet3 [Up]
Choose the interface to config [1]:
```

ステップ 3 デバイス管理 IP は、GUI を使用したデバイスへのアクセスに役立ちます。

```
 Configure static IP address? [yes]:
    Enter the interface IP [GigabitEthernet1]: 192.168.1.10
    Enter the subnet mask [GigabitEthernet1] [255.0.0.0]: 255.255.255.0
```

ステップ 4 （オプション）GUI を使用してデバイスにアクセスするための静的ルートを設定します。

```
Configure static route? [yes]:
Enter the destination prefix: 192.168.1.0
Enter the destination mask: 255.255.255.0
Enter the forwarding router IP: 192.168.1.1
```

ステップ 5 管理ユーザ名とパスワードを入力します。この手順は必須です。

```
Enter the management username: cisco
  Enter the password: ********
  Reenter the password: ********
```

ステップ 6 デバイス管理インターフェイスを設定していない場合は、ワイヤレス管理を設定します。

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the webUI (for this, choose 'no' below)
```

```
Would you like to continue with the wireless setup? [yes]: yes
```

（注） このプロンプトは、17.4 リリースには適用されません。

（注） デバイス管理を設定していない場合は、上記バナーが表示される前の**手順 7** に進みます。

17.3 リリースでは、少なくとも 1 つのインターフェイス（デバイスまたはワイヤレス管理）を設定した後、ウィザードを終了できます。

このバナーは、17.4 では使用できなくなりました。設定を完了する前にウィザードを終了することはできません。

[**Yes**] を選択した場合は、以降の手順に従う必要があります。また、**手順 4** で設定した IP を使用してデバイスにアクセスできます。

ステップ 7 ワイヤレス管理インターフェイスの設定は必須です。

```
Configuring wireless management interface
  Select interface to be used for wireless management
   1. GigabitEthernet2 [Up]
   2. GigabitEthernet3 [Up]
  Choose the interface to config [1]:
```

（注） GigabitEthernet1 がデバイス管理インターフェイスに使用されている場合は、残りの GigabitEthernet インターフェイスが表示されます。

ステップ 8 VLAN ID を入力します。

```
Enter the vlan ID (1-4094): 112
```

ステップ 9 IPv4 または IPv6 アドレスを設定します。

```
  Configure IPv4 address? [yes]:
    Enter the interface IP [GigabitEthernet1]: 9.11.112.40
    Enter the subnet mask [GigabitEthernet1] [255.0.0.0]: 255.255.255.0
  Configure IPv6 address? [yes]: no
```

ステップ 10 VLAN DHCP サーバと IP アドレスを設定します。

```
 Do you want to configure a VLAN DHCP Server? [yes]: yes
   Enter the VLAN DHCP Server IP [GigabitEthernet1]: 9.11.112.45
```

ステップ 11 （オプション）AP クライアントをコントローラに接続するための静的ルートの設定。静的ルートのデフォルトのオプションで、デフォルトルートを設定するように求められます。ただし、別のルートを指定することもできます。

```
 Configure static route? [yes/no]: yes
  Enter the destination prefix [0.0.0.0]:
  Enter the destination mask [0.0.0.0]:
  Enter the forwarding router IP: 9.11.112.1
```

（注） デバイスを HA RMI として設定し、デフォルトルート（つまり、送信元と宛先を 0.0.0.0 に設定）を設定していない場合、ウィザードからデフォルトルート情報が要求されます。

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the webUI(for this, choose 'no' below)

Would you like to continue with the wireless setup? [yes]
```

ステップ 12 展開モードを選択します。

```
 Choose the deployment mode
    1. Standalone
    2. Active
    3. Standby
 Enter your selection [1]:
```

（注） 次のいずれかの展開モードから 1 つ選択できます。

- **スタンドアロン**：このモードでは、高可用性のペアリング情報は表示されません。
- **アクティブ**：このモードでは、デイゼロ情報をすべて使用してコントローラを設定する必要があります。
- **スタンバイ**：このモードでは、[High Availability] 設定に進みます。

ステップ 13 システム名またはホスト名を設定します。

```
Enter the hostname [WLC]: ciscowlc
```

（注） この手順は必須です。ホスト名は、RFC 標準に準拠している必要があります。

ステップ 14 （オプション）AP のログインクレデンシャルを設定します。

```
Configure credentials for management access on Access Points? [yes]:
  Enter the management username: cisco
  Enter the management password: ****
    Reenter the password: ****
  Enter the privileged mode access password: ****
    Reenter the password: ****
```

ステップ 15 国コードを設定します。複数の国コードをカンマで区切って指定できます。

```
Configure country code for wireless operation in ISO format ? [US]:
```

ステップ 16 アクセスポイントがコントローラに接続できるように、日付と NTP を設定します。NTP サーバを使用するか手動で時刻を設定できます。

（注） 次の形式で日付を入力します。

MM/DD/YYYY

```
Configure a NTP server now ? [yes]: no

Configure the system time now? [yes]: yes

Enter the date in MM/DD/YYYY format: 10/05/2021
Enter the time in HH:MM:SS format: 10:22:13
```

ステップ 17 （オプション）タイムゾーンを設定します。

```
Configure timezone? [yes]:
 Enter name of timezone: ind
 Enter hours offset from UTC (-23,23): 5
 Enter mins offset from UTC (0,59) [0]: 30
```

ステップ 18 （オプション）予想されるクライアント密度を設定します。

```
Configure Wireless client density? [yes]:
 Choose the client density
   1. Low
   2. Typical
   3. High
 Enter your selection [2]: 3
```

ステップ 19 （オプション）AAA サーバを設定します。

（注） デイゼロ設定では、最大 6 台のサーバを設定できます。

```
Configure AAA servers? [yes]:
 Enter the AAA server address: 9.11.112.46
 Enter the AAA key: ***
Do you want to add more AAA servers? [yes]:
 Enter the AAA server address: 9.11.112.47
 Enter the AAA key: ***
Do you want to add more AAA servers? [yes]: no
```

（注） WPA2 エンタープライズには AAA サーバが必要です。17.4 リリースでは、AAA を 1 か所でのみ設定する必要があります。**手順 21** を実行すると、WPA2 エンタープライズは**手順 22** で AAA サーバを要求しません。

ステップ 20 （オプション）ワイヤレスネットワークの設定を行い、AP とクライアントを接続するための WLAN 情報を設定します。

```
Configure Wireless network settings? [yes]:
```

ステップ 21 （オプション）クライアントを接続するための SSID を設定します。

```
Enter the network name or service set identifier (SSID):
Choose the network type
    1. Employee
    2. Guest
```

[**Employee**] をネットワークタイプとして選択すると、次のオプションが表示されます。

```
Choose the security type
    1. WPA Personal
    2. WPA Enterprise
   Enter your selection [2]:
```

[**WPA2 Personal**] を選択する場合は、事前共有キー（ASCII）を入力する必要があります。

```
Enter the pre-shared key (ASCII):
```

[**WPA2 Enterprise**] を選択すると、複数の AAA サーバを追加できます。

```
Enter the AAA server address:
```

```
Enter the AAA key:
Enter more AAA server details? [yes]
```

[**Guest**] を選択すると、次のオプションが表示されます。

```
Please choose the security type:
1. Webauth
2. Authbypass
3. Consent
4. Webconsent
Enter the security type:
```

ステップ 22 （オプション）仮想 IP アドレスを設定します。デフォルトの仮想 IP アドレスは 192.0.6.1 です。

```
Configure virtual IP? [yes]:
 Enter the virtual IP [192.0.6.1]:
```

ステップ 23 （オプション）RF ネットワーク名を設定します。

```
Configure RF-Network Name? [yes]:
 Enter the RF-Network Name: ciscorf
```

ステップ 24 （オプション）自己署名証明書を設定します。

```
Auto generate certificate for AP join? [yes]:
Choose key size
1.2048
2.3072
3.4096
Enter your selection [1]:
Choose the signature algorithm
1.SHA256
2.SHA384
Enter your selection [1]:
Enter secret key(minimum 8 characters): ********
Self Signed Certificate generation will be done after system boots up.
```

ステップ 25 （オプション）高可用性を設定します。

展開モードをアクティブまたはスタンバイに選択する場合は、次の HA ペアリングタイプのいずれかを選択する必要があります。

1. RMI
2. RP-RP

（注） HA ペアリングタイプの詳細については、『Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.4.x』の「**Part: High Availability (High Availability > Information About Redundancy Management Interface)**」を参照してください。

```
High Availability configuration
 Please choose the HA pairing type
   1. RMI
   2. RP-RP
 Enter your selection [1]:
```

RMI+RP を選択した場合は、冗長ポートとして使用するインターフェイスを選択する必要があります。

```
Select interface to be used as redundancy port
  1. GigabitEthernet3 [Up]
 Choose the interface to config [1]: 2
 Enter the RMI IP for local chassis: 9.11.112.50
 Enter the RMI IP for remote chassis: 9.11.112.51
 Enter the gateway IP of the last resort: 9.11.112.1
```

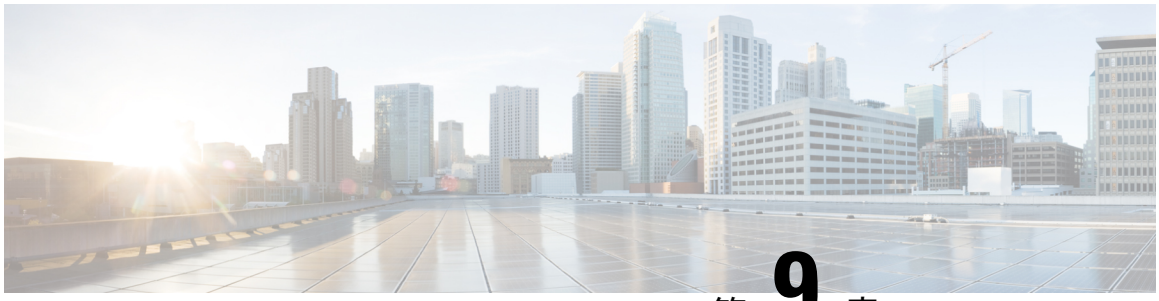
展開モードにスタンバイを選択した場合は、ペアリングを完了するために VLAN ID を指定する必要があります。

```
 Enter the RMI IP for local chassis: 9.11.112.51
 Enter the RMI IP for remote chassis: 9.11.112.50
 Enter the wireless management VLAN: 112
```

RP を選択した場合は、冗長ポートとして使用するインターフェイスを選択する必要があります。

```
Select interface to be used as redundancy port
  1. GigabitEthernet3 [Up]
 Choose the interface to config [1]: 2
 Enter the local IP:
Enter the subnet mask:
Enter the remote IP:
```

（注） デバイス管理インターフェイスには GigabitEthernet1、ワイヤレス管理インターフェイスには GigabitEthernet2、HA には GigabitEthernet3 を使用することを推奨します。



第 9 章

ソフトウェアのアップグレード

ソフトウェア アップグレード プロセスの前提条件

この項では、VM 上の既存のコントローラのインストールの場合の Cisco IOS XE ソフトウェアのアップグレード方法について説明します。

（注）

- この手順では、同じ VM 上での新しいソフトウェア バージョンのコントローラへのアップグレードの詳細を示します。
- アップグレードプロセスを高速化するには、Web UI 方式を使用することをお勧めします。

コントローラのソフトウェアイメージの Cisco IOS XE バージョンをアップグレードする前に、次の前提条件が満たされていることを確認します。

- 使用しているハイパーバイザベンダーおよびバージョンとの互換性現在のバージョンのコントローラでサポートされていない新しいハイパーバイザバージョンにアップグレードする場合は、新しいハイパーバージョンにアップグレードする前にコントローラのバージョンをアップグレードする必要があります。
- コントローラ ソフトウェア イメージの VM のメモリ要件
  - 新しいコントローラ バージョンには以前のバージョンよりも多いメモリが必要な場合は、アップグレード プロセスを開始する前に VM 上でメモリの割り当てを引き上げる必要があります。
  - ソフトウェアをアップグレードまたはダウングレードするには、**.bin** ファイルを使用する必要があります。初回インストールにのみ、**.iso** ファイルと **.ova** ファイルを使用します。

コントローラソフトウェアのアップグレード（CLI）

次の手順に従い、インストールモードで、あるリリースから別のリリースにアップグレードします。

始める前に

- **install remove inactive** コマンドを使用して、古いインストールファイルをクリーンアップします。
- CLI を使用してソフトウェアをアップグレードする場合は、インストールモードを使用することを推奨します。**show version** コマンドを使用してブート モードを検証します。
- ソフトウェアイメージのアップグレードを実行するには、**boot flash:packages.conf** を使用して IOS をブートする必要があります。
- *flash:packages.conf* からのみブートされるようにブートパラメータを設定していることを確認します。

ステップ 1 ソフトウェアのダウンロードページに移動します。 https://software.cisco.com/download/home/286316412/type

a) IOS XE ソフトウェアのリンクをクリックします。

b) インストールするリリース番号を選択します。

> （注） デフォルトでは、推奨されるリリース番号が選択されます。リリース番号の指定については、次のリンクを参照してください。 https://software.cisco.com/download/static/assets/i18n/reldesignation.html?context=sds

c) [download] をクリックします。

ステップ 2 **copy tftp:***image***flash:** コマンドを実行して、新しいイメージをフラッシュにコピーします。

> （注） TFTP を介して大きなファイルを転送するプロセスは、時間がかかります

```
Device# copy tftp://10.8.0.6//C9800-universalk9_wlc.xx.xx.xx.SPA.bin flash:

Destination filename [C9800-universalk9_wlc..xx.xx.xx..SPA.bin]?
Accessing tftp://10.8.0.6//C9800-universalk9_wlc.xx.xx.xx.SPA.bin...
Loading /C9800-universalk9_wlc.xx.xx.xx.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 601216545 bytes]

601216545 bytes copied in 50.649 secs (11870255 bytes/sec)
```

ステップ 3 次のコマンドを実行して、イメージがフラッシュに正常にコピーされていることを確認します。 **dir flash:**

```
Device# dir flash:*.bin
```

ステップ 4 **install add file bootflash:***image***activate commit** コマンドを実行して、ソフトウェア イメージをフラッシュにインストールします。

（注） 複数手順によるソフトウェアのインストールも可能です。複数手順によるインストールを実行するには、手順 5 に進みます。

```
Device# install add file bootflash:C9800-universalk9_wlc.xx.xx.xx.SPA.bin activate commit

install_add_activate_commit: START Thu Dec  6 15:43:57 UTC 2018
Dec  6 15:43:58.669 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install one-shot
bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
install_add_activate_commit: Adding PACKAGE

--- Starting initial file syncing ---
Info: Finished copying bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin to the selected chassis
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
  [1] Add package(s) on chassis 1
  [1] Finished Add on chassis 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

Image added. Version: xx.xx.xx.216
install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/bootflash/C9800-xx-rpboot.xx.xx.xx.SPA.pkg
/bootflash/C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y
--- Starting Activate ---
Performing Activate on all members
  [1] Activate package(s) on chassis 1
    --- Starting list of software package changes ---
    Old files list:
      Removed C9800-xx-mono-universalk9.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
      Removed C9800-xx-rpboot.BLD_Vxxxx_THROTTLE_LATEST_20181022_153332.SSA.pkg
    New files list:
      Added C9800-xx-mono-universalk9.xx.xx.xx.SPA.pkg
      Added C9800-xx-rpboot.xx.xx.xx.SPA.pkg
    Finished list of software package changes
  [1] Finished Activate on chassis 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members
  [1] Commit package(s) on chassis 1
  [1] Finished Commit on chassis 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit  Thu Dec  6 15:49:21 UTC 2018
Dec  6 15:49:21.294 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed install
one-shot PACKAGE bootflash:C9800-xx-universalk9.xx.xx.xx.SPA.bin
```

（注） **install add file activate commit** コマンドを実行した後に、システムは自動的にリロードします。システムを手動でリロードする必要はありません。

ステップ 5 （オプション）複数手順によるソフトウェアのインストールも可能です。

（注） *flash:packages.conf* からのみブートされるようにブートパラメータを設定していることを確認します。

a) **install add file** コマンドを使用して、コントローラソフトウェアのイメージをフラッシュに追加し、展開します。

```
Device# install add file bootflash:C9800-universalk9_wlc.xx.xx.xx.SPA.bin
```

b) **ap image predownload** コマンドを使用して、AP イメージの事前ダウンロードを実行します。

```
Device# ap image predownload
```

c) **show ap image** コマンドを使用して、AP の事前ダウンロードステータスを確認します。

```
Device# show ap image
```

d) **install activate** コマンドを使用して、パッケージをアクティブ化します。

```
Device# install activate
```

e) リロードが繰り返されても持続するように、**install commit** コマンドを使用してアクティブ化の変更をコミットします。

```
Device# install commit
```

ステップ 6 次のコマンドを実行して、インストールを確認します。 **show version**

（注） 新しいイメージをブートするとブート ローダはが自動的に更新されますが、次にリロードされるまでは新しいブートローダ バージョンは出力に表示されません。

ステップ 7 システム内のアクティブなパッケージの概要を表示するには、次のコマンドを実行します。 **show install summary**

```
Device# show install summary

[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   I    <v1>
IMG   C    <v2>
```

コントローラソフトウェアのアップグレード（GUI）

始める前に

[Remove Inactive Files] リンクを使用して、古いインストールファイルをクリーンアップします。

（注） [Software Maintenance Upgrade]、[AP Service Package]、および [AP Device Package] などの GUI オプションについては、それぞれの機能のセクションを参照してください。

ステップ 1 [Administration] > [Software Management] を選択します。

ステップ 2 [Upgrade Mode] ドロップダウンリストから、次のオプションを選択します。

- [INSTALL]：インストールモードでは、デバイスをブートするために *packages.conf* という名前のパッケージプロビジョニング ファイルを使用します。
- [BUNDLE]：バンドルモードでは、デバイスをブートするために、モノリシック Cisco IOS イメージが使用されます。パッケージがバンドルから抽出され、RAM にコピーされるため、バンドルモードはインストールモードよりも多くのメモリを消費します。

（注） [Destination] フィールドは、[BUNDLE] アップグレードモードでのみ表示されます。

ステップ 3 [Transport Type] ドロップダウンリストで転送タイプを選択し、[TFTP]、[SFTP]、[FTP]、[Device]、または [Desktop (HTTP)] としてデバイスにソフトウェアイメージを転送します。

- [Transport Type] で [TFTP] を選択した場合は、使用する TFTP サーバの**サーバ IP アドレス**を入力します。また、完全な**ファイルパス**も入力します。

  コントローラでは、デフォルトでは IP TFTP の送信元が送信元ポートにマッピングされます。
- [Transport Type] で [SFTP] を選択した場合は、使用する SFTP サーバの**サーバ IP アドレス**を入力します。また、**SFTP のユーザ名**、**SFTP のパスワード**、および完全な**ファイルパス**も入力します。
- [Transport Type] で [FTP] を選択した場合は、使用する FTP サーバの**サーバ IP アドレス**を入力します。また、**FTP のユーザ名**、**FTP のパスワード**、および完全な**ファイルパス**も入力します。
- [Transport Type] で [Device] を選択した場合は、ドロップダウンリストから [File System] を選択します。[File Path] フィールドでデバイスから使用可能なイメージまたはパッケージを参照し、オプションのいずれかを選択して [Select] をクリックします。
- [Transport Type] で [Desktop（HTTPS）] を選択した場合は、ドロップダウンリストから [File System] を選択します。[Source File Path] フィールドで、[Select File] をクリックしてファイルを選択し、[Open] をクリックします。

ステップ 4 [Download & Install] をクリックします。

ステップ 5 新しいソフトウェア イメージでデバイスをブートするには、[Save Configuration & Reload] をクリックします。

コントローラのリブート

新しいシステム イメージをブートフラッシュ メモリにコピーし、新しいシステム イメージをロードし、新しいイメージと設定のバックアップ コピーを保存したら、**reload** コマンドを使用して VM をリブートします。

（注） アクティブなデバイスをリロードすると、スタック全体がリロードされます。

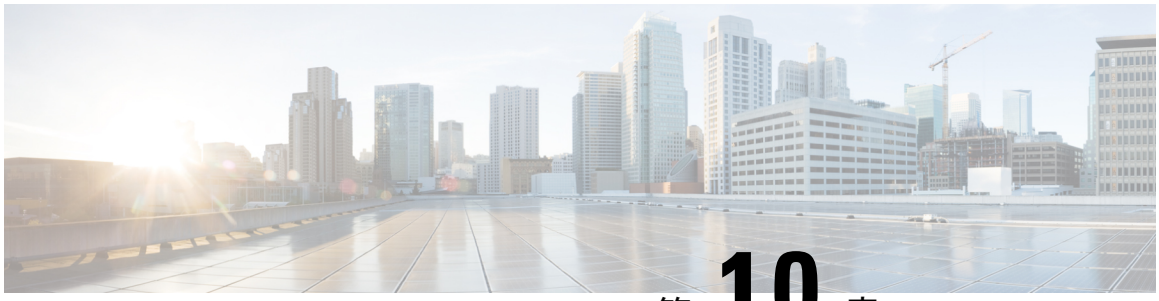
VM のリブートの詳細については、VMware のドキュメントを参照してください。

リブート後、コントローラ VM には、新たにインストールした Cisco IOS XE ソフトウェア バージョンとともに新しいシステム イメージを含める必要があります。

（注） 16.11 から以降のリリースにアップグレードした後、新しいログイン ページを表示できるようになります。

表示されていない場合は、次のいずれかを実行してログイン ページにリダイレクトします。

- GUI を更新します。
- キャッシュをクリアします。



第 10 章

ライセンス情報

評価ライセンス

デバイスが登録されていない場合、ワイヤレスコントローラは評価モードで動作します。評価モードの期間は 90 日間です。評価期間が終了してもワイヤレスコントローラがスマートアカウントに登録されない場合、ワイヤレスコントローラでsyslog評価期限切れメッセージが表示されるようになります。これらのエラーメッセージは情報提供のみを目的としており、ワイヤレスコントローラの機能には影響しません。

ワイヤレスコントローラが EVAL モードのときに、このコントローラでサポートされる AP の数は、ワイヤレスコントローラの容量と等しくなり、完全に動作可能になります。評価モードでワイヤレスコントローラを使用するために他のライセンスは必要ありません。

ライセンス情報の表示

show license udi コマンドを使用して、シャーシのユニバーサルデバイス識別子（UDI）情報を特定します。これは、新しいライセンスを購入する場合に必要になることがあります。

次に、**show license udi** コマンドの出力例を示します。

```
Device# show license udi
SlotID        PID            SN                UDI
-------------------------------------------------------------------------------
*        C9800-CL              xxxxxxxxxxx     C9800-CL:xxxxxxxxxxx
```

Cisco IOS ライセンス レベルの表示

show version コマンドを使用して、コントローラ内の Cisco IOS ライセンスレベルを特定します。

例：

```
WLC# show version | section License

licensed under the GNU General Public License ("GPL") Version 2.0.  The
documentation or "License Notice" file accompanying the IOS-XE software,
License Type: Smart License is permanent
License Level: adventerprise
AIR License Level: AIR DNA Advantage
```

表 *11 : show version* コマンド出力の説明

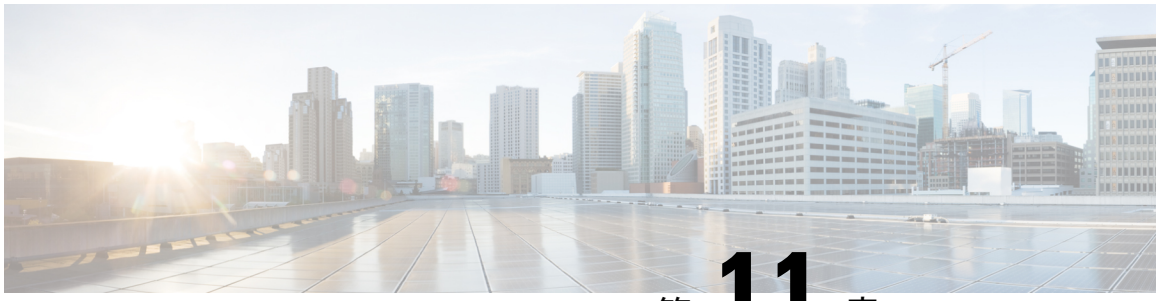
フィールド名	説明
License Level: adventerprise	現在の Cisco IOS ライセンス コード レベルを示します。
License Type: Smart License is permanent	使用するライセンスのタイプを示します。 この例は、シスコのスマートライセンスを使用してユーザアカウントにフローティングライセンスを指定していることを示しています。 そのほかのライセンスのタイプには、永久（購入）ライセンスまたは 60 日間の評価ライセンスがあります。
AIR License Level: AIR DNA Advantage	AIR Network Advantage ライセンスレベルを示します。

show running-config コマンドまたは **show startup-config** コマンドを使用して、ライセンスレベル情報を表示します。次に、**show running-config** コマンドの出力例を示します。

```
WLC# show running-config
.
.
.
license boot level adventerprise
```

表 *12 : show running-config* コマンド出力の説明

フィールド名	説明
license boot level adventerprise	ブートに必要な Cisco lOS ライセンス レベルを示します。



第 11 章

トラブルシューティング

ハードウェアと VM の要件の確認

コントローラの問題をトラブルシューティングしやすくするために、サポートされているハードウェアにデバイスがインストールされ、次の VM の要件が満たされていることを確認します。

- サーバハードウェアがハイパーバイザベンダーでサポートされていることを確認します。VMware を使用している場合、サーバが VMware ハードウェア互換性リストに含まれていることを確認します。詳細については、VMware のドキュメントセットを参照してください。
- VM ベンダーが I/O デバイス（ファイバ チャネル（FC）、Internet Small Computer System Interface（iSCSI）など）や使用中の SAS をサポートしていることを確認します。
- 十分な RAM が VM とハイパーバイザ ホスト用のサーバに割り当てられていることを確認します。
- VMware を使用している場合、サーバに VM と VMware ESXi の両方をサポートするのに十分な RAM があることを確認します。
- コントローラがハイパーバイザバージョンでサポートされているかどうかを確認します。
- メモリの量、CPU の数、およびディスク サイズに基づいて適切に VM が設定されていることを確認します。
- サポートされているネットワーク ドライバを使用して vNIC が設定されていることを確認します。

ネットワーク接続の問題

コントローラのネットワーク接続の問題をトラブルシューティングするには、次の要件を満たしていることを確認します。

- vSwitch を通じて送受信されたトラフィックを表示できるように無差別モードが設定されている必要があります。このモードを使用しないと、タグ付けされたトラフィックが適切にフローしません。
- アクティブで期限内のライセンスが VM にインストールされていることを確認します。**show license** コマンドを入力します。[License State] に [Active]、[In Use] と表示されている必要があります。
- VM の vNIC が正しい物理 NIC か、または適切な vSwitch に接続されていることを確認します。
- 仮想 LAN（VLAN）を使用している場合は、vSwitch が適切な VLAN で設定されていることを確認します。
- 複製されたスタティック MAC アドレスまたは VM を使用している場合は、重複する MAC アドレスがないことを確認します。

注意 重複した MAC アドレスがあるとコントローラの機能ライセンスが無効化され、デバイスのインターフェイスが無効になることがあります。

VM パフォーマンスの問題

コントローラは、一連のサポートされている VM のパラメータおよび設定内で動作して、シスコがテストした一定のパフォーマンス レベルを実現します。

vSphere クライアントを使用してデータを表示し、VM のパフォーマンスをトラブルシューティングします。vCenter を使用している場合は、履歴データを表示できます。vCenter を使用してない場合は、ホストからのライブ データを表示できます。

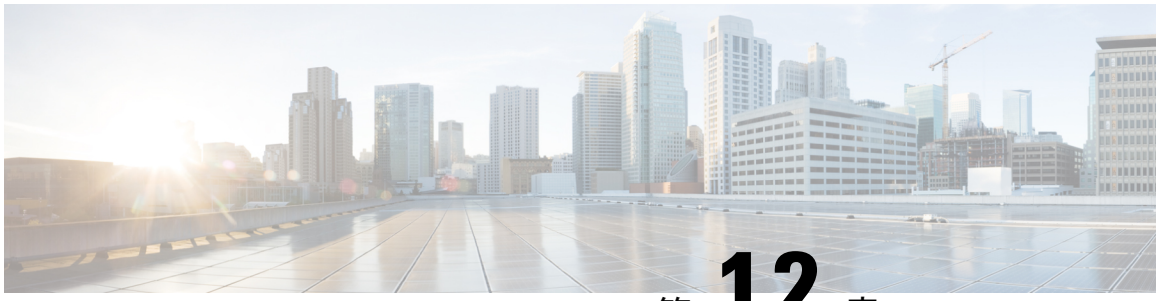
パフォーマンスの問題をトラブルシューティングするためには次の要件が満たされていることを確認します。

- 適切な MTU 設定に合わせてデバイスが設定されていることを確認します。
- デフォルトでは、デバイスの最大 MTU の設定値が 1500 に設定されます。ジャンボ フレームをサポートするには、デフォルトの VMware vSwitch 設定を編集する必要があります。詳細については、VMware vSwitch のドキュメントを参照してください。
- コントローラは VM 間のメモリ共有をサポートしていません。ESXi ホストで、メモリ カウンタを確認し、VM 上で使用され、共有されているメモリを特定します。バルーンとスワップで使用されているカウンタがゼロであることを確認します。
- 対象の VM にコントローラをサポートするのに十分なメモリがない場合は VM のメモリのサイズを増やします。VM またはホストのメモリが不足していると、コントローラ コンソールが停止して、応答しなくなることがあります。

⚠

注意 パフォーマンスの問題をトラブルシューティングするときは、コントローラと同じホスト上の他の VM がコントローラ VM のパフォーマンスに影響する場合があることに注意してください。ホスト上の他の VM がコントローラ VM に影響するようなメモリの問題を引き起こしていないことを確認します。

- ネットワーク パケットがドロップされていないことを確認します。ESXi ホストで、ネットワーク パフォーマンスを確認し、カウンタを表示して、ドロップされたパケットの送受信数を測定します。



第 12 章

プラットフォームおよびシスコ ソフトウェア イメージのサポート情報の検索

プラットフォームおよびシスコソフトウェアイメージのサポート情報

シスコのソフトウェアには、特定のプラットフォームに対応したソフトウェアイメージで構成されるフィーチャセットが含まれています。特定のプラットフォームで使用できるフィーチャセットは、リリースに含まれるシスコ ソフトウェア イメージによって異なります。特定のリリースで使用可能なソフトウェアイメージのセットを識別するか、または所定のCisco IOS XE ソフトウェアイメージに機能が使用できるかどうかを確認するには、Cisco Feature Navigator、Software Advisor、または対応するリリース ノートのドキュメントを参照してください。

Cisco ワイヤレス コントローラ ソフトウェア関連のすべてのドキュメントについては、次を参照してください。

https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/tsd-products-support-series-home.html

Cisco Feature Navigator の使用

プラットフォームのサポートおよびソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートする Cisco IOS XE のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

このツールにアクセスするには、Cisco.com の登録ユーザである必要はありません。

Software Advisor の使用

ある機能がCisco IOS XE リリースでサポートされているかどうかを特定する、その機能のソフトウェア ドキュメントを見つける、またはデバイスでの Cisco IOS XE ソフトウェアの最小要

件を確認するため、次の Cisco.com に Software Advisor ツールが用意されています。
http://tools.cisco.com/Support/Fusion/FusionHome.do

このツールにアクセスするには、Cisco.com の登録ユーザである必要があります。