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。