



インストールまたは Cisco APIC イメージの回復

- [設置上の注意事項 \(1 ページ\)](#)
- [使用上のガイドライン \(2 ページ\)](#)
- [Cisco APIC ソフトウェア イメージの回復またはインストールの条件 \(5 ページ\)](#)
- [PXE サーバーを使用して Cisco APIC ソフトウェアを APIC サーバー M1/L1、M2/L2 または、M3/L3にインストールする。 \(6 ページ\)](#)
- [PXE サーバーを使用して Cisco APIC ソフトウェアを APIC サーバー M4/L4 にインストールする。 \(8 ページ\)](#)
- [PXE サーバを使用する Cisco APIC のインストール \(9 ページ\)](#)
- [仮想メディアを使用する Cisco APIC ソフトウェアのインストール \(12 ページ\)](#)
- [ACI ファブリックのクリーン初期化の実行 \(26 ページ\)](#)

設置上の注意事項

- ハードウェアのインストール手順については、「[Cisco ACI ファブリック ハードウェア インストール ガイド](#)」を参照してください。
- このリリースをインストールまたはアップグレードする前に、Cisco APIC 設定をバックアップします。実稼働で実行しない単一の Cisco APIC クラスタは、インストールまたはアップグレード中にデータベースの破損が発生すると設定が失われる可能性があります。
- 初めて Cisco APIC にアクセスする方法については、『[Cisco APIC 入門ガイド](#)』を参照してください。
- Microsoft System Center Virtual Machine Manager (SCVMM) または Microsoft Windows Azure パックを持つ Cisco ACI は ASCII 文字のみをサポートしています。非 ASCII 文字はサポートしていません。Windows のシステム ロケールの設定に [English] が設定されていることを確認します。それ以外の場合、SCVMM および Windows Azure Pack を持つ Cisco ACI はインストールされません。また、システムロケールをインストール後に英語以外のロケールに変更した場合、Cisco APIC や Cisco ACI ファブリックと通信すると統合コンポーネントが失敗する場合があります。

- インストールの指示を含む Cisco APIC Python SDK ドキュメントについては、「[APIC Python SDK ドキュメンテーション](#)」を参照してください。

インストールに必要な SDK egg ファイルがパッケージに含まれます。egg ファイル名の形式は次のとおりです。

```
acicobra-A.B_CD-py2.7.egg
```

- **A** : メジャーリリース番号。
- **B** : マイナーリリース番号。
- **C** : メンテナンスリリース番号。
- **D** : リリースレター (パッチレター) 。文字は小文字です。

たとえば、5.2(4d) リリースの egg ファイル名は次のとおりです。

```
acicobra-5.2_4d-py2.7.egg
```

- UNIX/Linux および Mac OS X で SSL 対応の SDK をインストールするには、コンパイラが必要です。Windows インストールでは、wheel パッケージを使用して SDK の依存関係用のコンパイル済み共有オブジェクトをインストールできます。
- モデルパッケージは SDK のパッケージによって異なります。SDK のパッケージを先にインストールしてください。
- Cisco APIC 6.0 (2) 以降、新しいタイプの SSL 証明書のサポート - ECDSA 証明書が有効になりました。この証明書は、Cisco APIC の以前のバージョンではサポートされていません。ECDSA 証明書を展開してから Cisco APIC の以前のバージョンにダウングレードすると、Cisco APIC Web サーバーは機能しません。Cisco APIC 6.0 (2) より前のバージョンにダウングレードする前に、RSA ベースの証明書を使用するように Cisco APIC Web サーバーを更新する必要があります。

使用上のガイドライン

- Cisco APIC GUI は次のブラウザをサポートします。
 - Mac および Windows 向け Chrome バージョン 59 (最低)
 - Mac、Linux、Windows 向け Firefox バージョン 59 (最低)
 - Internet Explorer バージョン 11 (最低)
 - Safari 10 (最低)



(注) リリース 1.3(1) にアップグレードした後、ブラウザを再起動します。

- Cisco APIC GUI には、ビデオ デモンストレーションを含むクイックスタート ガイドのオンラインバージョンが含まれます。
- インフラストラクチャの IP アドレス範囲は、インバンドおよびアウトオブバンドのネットワーク用の ファブリックで使用する他の IP アドレスと重複してはなりません。
- Cisco APIC はテナントの負荷に IPAM サービスを提供しません。
- GUI から Cisco APIC CLI に到達するには、[システム (System)] > [コントローラ (Controllers)] を選択し、コントローラをハイライトしてから、[SSH の起動 (launch SSH)] を右クリックして選択します。コマンドのリストを取得するには、esc キーを 2 回押します。
- 5 分間の統計データの一部では 10 秒のサンプルの数は 30 ではなく 29 です。
- 次のサービスでは、アウトオブバンド管理接続を持つ DNS ベースのホスト名を使用します。IP アドレスは、インバンドおよびアウトオブバンド管理接続両方で使用できます。
 - Syslog サーバ
 - Call Home SMTP サーバ
 - テクニカル サポート エクスポート サーバ
 - 設定エクスポート サーバ
 - 統計情報エクスポート サーバ
- リーフおよびスパイン スイッチは、IP 接続を持つホストからファブリックへ管理できません。
- 2 個のエンドポイント間でアトミック カウンタを設定する場合、IP は 2 個のエンドポイントのどちらかで学習され、エンドポイントベース ポリシーではなく IP ベース ポリシーを使用することをお勧めします。
- 同じノードで 2 つのレイヤ 3 の外部ネットワークを設定するときに、ループバックはレイヤ 3 ネットワークに別々に設定されます。
- アプリケーション EPG およびレイヤ 3 外部 EPG を含むすべてのエンドポイント グループ (EPG) にはドメインが必要です。インターフェイス ポリシー グループは、接続エンティティ プロファイル (AEP) に関連付けられ、AEP はドメインに関連付けられている必要があります。EPG とドメイン、およびインターフェイス ポリシー グループとドメインの関連付けに基づいて、EPG が使用するポートと VLAN が検証されます。これは、ブリッジ型のレイヤ 2 アウトサイドおよびルーテッド レイヤ 3 アウトサイド EPG を含むすべての EPG に適用されます。詳細については、『Cisco Fundamentals GuideCisco』、および KB の記事、「Creating Domains, Attach Entity Profiles, and VLANs to Deploy an EPG on a Specific Port」を参照してください。



(注) 1.0(4X) 以前のリリースでは、アプリケーション EPG またはレイヤ 2/レイヤ 3 アウトサイド EPG のスタティック パスを作成するとき、物理ドメインは必要ありませんでした。このリリースでは必須です。物理ドメインを使用しないアップグレードは、EPG で「無効なパス設定」という障害が発生します。

- EPG は、それ自体のテナント内でのみコントラクトインターフェイスに関連付けられます。
- ユーザ パスワードは、次の基準を満たす必要があります。
 - 最少文字数は 8 文字
 - 最大文字数は 64 文字
 - 連続して繰り返される文字は 3 文字未満
 - 次の文字タイプのうち 3 個を含む：小文字、大文字、数字、記号
 - 簡単に推測することができない
 - ユーザ名やユーザ名を逆にしたものは使用できません
 - cisco、isco、またはこれらの文字列の並べ替えを変化させたものや、それらの文字の大文字化の変更により取得される変形語であってはなりません
- 電力消費の統計情報がリーフ スイッチ ノード スロット 1 では表示されません。
- API またはアドバンスド GUI で作成され CLI を通して更新されたレイヤ 3 外部ネットワークについては、プロトコルは API またはアドバンスド GUI を通して外部ネットワークでグローバルに有効にする必要があります、CLI を介してさらに更新を行う前に、すべての参加ノードのノードプロファイルは API またはアドバンスド GUI を通して追加される必要があります。
- CLI から作成されたレイヤ 3 外部ネットワークについては、API を使用して更新しないようにする必要があります。これらの外部ネットワークは、「_ui_」で始まる名前でも識別されます。
- NX OS スタイル CLI で発行された「show」コマンドの出力は、今後のソフトウェアリリースで変更されます。Cisco は、自動化に show コマンドの出力の使用を推奨していません。
- このソフトウェアのバージョンで、CLI は管理ログイン権限を持つユーザに対してのみサポートされています。
- 仮想プライベートクラウド (vPC) メンバノードを異なる設定ゾーンに分離しないでください。ノードが異なる設定ゾーンにあるとき、インターフェイス ポリシーが変更され vPC メンバノードの 1 つのみに展開されている場合、vPC のモードが不一致になります。

- 複数のログイン ドメインを定義する場合は、Cisco APIC にログインするときに使用するログイン ドメインを選択できます。デフォルトでは、ドメイン ドロップダウンリストは空であり、ドメインを選択しない場合 DefaultAuth ドメインが認証に使用されます。この場合、DefaultAuth のログイン ドメインにユーザ名がないとログインに失敗する可能性があります。その結果、選択したログイン ドメインに基づくクレデンシャルを入力する必要があります。
- ファームウェア メンテナンス グループに含まれるのは、最大 80 ノードです。
- コントラクトがエンドポイントグループに関連付けられていない場合、DSCP マーキングは vzAny コントラクトを持つ VRF ではサポートされていません。DSCP は actrl ルールとともにリーフ スイッチに送信されますが、vzAny コントラクトに actrl ルールはありません。したがって、DSCP 値が送信されることはありません。
- Cisco ACI ファブリックの NTP サーバとしては、リーフ スイッチを使用することをお勧めします。

Cisco APIC ソフトウェア イメージの回復またはインストールの条件

このクラスターは Cisco APIC をインストールまたは回復する方法を説明します。既存のサーバが完全に応答していない Cisco APIC イメージを所有し、新しい Cisco APIC イメージをインストールする場合、Cisco APIC イメージを回復します。



- (注) 既存の UCSサーバが存在する場合、Cisco APIC ソフトウェア セクションのインストールをスキップします。

Cisco APIC イメージをインストールすることで、次のタスクを完了します。

- ディスク上にある既存のデータが消去されます。
- ディスクが再フォーマットされます。
- 新しいソフトウェア イメージがインストールされます。

次のいずれかの方法を使用して、サーバに Cisco APIC ソフトウェアをインストールすることができます。

- PXE サーバの使用
- 仮想メディアの使用



(注) 他の仮想メディアのインストールを実行するときと同じように、Cisco APIC ISO イメージファイルを使用してインストールを行うことができます。手順の詳細については、このマニュアルでは説明していません。

PXE サーバーを使用して Cisco APIC ソフトウェアを APIC サーバー M1/L1、M2/L2 または、M3/L3 にインストールする。

この手順では、ブート前実行環境 (PXE) サーバーを使用して Cisco Application Policy Infrastructure Controller (APIC) ソフトウェアを APIC サーバー M1/L1、M2/L2、または M3/L3 にインストールします。

手順

ステップ 1 Linux の標準構成で PXE サーバを設定します。

ステップ 2 リリース 4.0 以降の Cisco APIC ソフトウェア イメージをインストールするために、PXE 設定ファイルに次のようなエントリがあることを確認します。

```
label 25
    kernel vmlinuz dd blacklist=iscsi blacklist=ahci nodmraid noprobe=ata1 noprobe=ata2
    noprobe=ata3 noprobe=ata4
    append initrd=initrd root=live:squashfs.img_URL rd.live.img rd.live.debug=1
    rd.live.ram=1 rd.debug atomix.isourl=iso_URL
```

例 :

```
label 25
    kernel ifcimages/vmlinuz dd blacklist=iscsi blacklist=ahci nodmraid noprobe=ata1
    noprobe=ata2 noprobe=ata3 noprobe=ata4
    append initrd=ifcimages/initrd.img
    root=live:http://192.0.2.10/myisomount/LiveOS/squashfs.img rd.live.img rd.live.debug=1
    rd.live.ram=1 rd.debug atomix.isourl=http://192.0.2.10/aci-apic-dk9.4.0.0.iso
```

ステップ 3 Cisco.com から Cisco APIC.iso イメージをダウンロードします。

ステップ 4 マウント フォルダを作成し、Cisco APIC.iso イメージをマウントします。

```
$ mkdir -p mount_folder
$ mount -t iso9660 -o loop iso_image mount_folder
```

例 :

```
$ cd /home/user
$ mkdir -p myisomount
$ mount -t iso9660 -o loop /local/aci-apic-dk9.4.0.0.iso myisomount
```

ステップ 5 Initrd. img および vmlinuz ファイルがマウントフォルダの場所にあることを確認します。

例：

```
$ ls /home/user/myisomount/images/pxeboot/
initrd.img vmlinuz
```

ステップ 6 マウントされた Cisco APIC.iso イメージから、vmlinuz および initrd を tftpboot パスにコピーします。

例：

```
$ mkdir -p /var/lib/tftpboot/ifcimages
$ cp -f /home/user/myisomount/images/pxeboot/vmlinuz /var/lib/tftpboot/ifcimages/
$ cp -f /home/user/myisomount/images/pxeboot/initrd.img /var/lib/tftpboot/ifcimages/
```

ステップ 7 Cisco APIC.iso イメージとマウントフォルダを HTTP ルートディレクトリにコピーします。

例：

```
$ cp -R /local/aci-apic-dk9.4.0.0.iso /var/www/html
$ cp -R /home/user/myisomount /var/www/html
```

ステップ 8 PXE の構成 (/var/lib/tftpboot/pxelinux.cfg/default) にエントリを追加して、Cisco APIC.iso イメージのためのキックスタート ファイルを参照するようにします。

例：

```
[root@pxeserver ~]# cat /var/lib/tftpboot/pxelinux.cfg/default
label 25
    kernel ifcimages/vmlinuz dd blacklist=iscsi blacklist=ahci nodmraid noprobe=ata1
    noprobe=ata2 noprobe=ata3 noprobe=ata4
    append initrd=ifcimages/initrd.img
    root=live:http://192.0.2.10/myisomount/LiveOS/squashfs.img rd.live.img rd.live.debug=1
    rd.live.ram=1 rd.debug atomix.isourl=http://192.0.2.10/aci-apic-dk9.4.0.0.iso
```

この情報を使用して、PXE メニュー エントリ イメージが正しく設定されていることを確認します。

ステップ 9 PXE サーバを再起動します。

ステップ 10 Cisco APIC を再起動し、F12 キーを押してネットワーク ブートを開始します。

ステップ 11 PXE サーバで設定されたオプションを選択して、Cisco APIC イメージを起動します。

PXE サーバーを使用して Cisco APIC ソフトウェアを APIC サーバー M4/L4 にインストールする。

この手順では、Preboot Execution Environment (PXE) サーバーを使用して Cisco Application Policy Infrastructure Controller (APIC) ソフトウェアを APIC サーバー M4/L4 にインストールします。

手順

- ステップ 1 PXE サーバーに DNSMasq パッケージと HTTP サーバー パッケージをインストールします。
- ステップ 2 インストールする ISO を、PXE サーバーがファイルをホストするパス（/var/www/html など）にダウンロードします。
- ステップ 3 必要に応じて ISO を解凍またはマウントします。

例：

```
$ sudo mkdir /mnt/iso /mnt/efi
$ sudo mount -o loop /var/www/html/aci-apic-dk9.6.0.2b.iso /mnt/iso
$ sudo mount -t vfat /mnt/iso/images/efiboot.img /mnt/efi
```

- ステップ 4 インストーラの EFI ファイルを、/srv/tftp などの PXE サーバーの TFTP パスにコピーします。

例：

```
$ cp -av /mnt/efi/EFI/BOOT/*.EFI /srv/tftp/
```

- ステップ 5 ISO のマウント解除。

例：

```
$ sudo umount /mnt/efi
$ sudo umount /mnt/iso
```

- ステップ 6 DNSMasq を構成します。

例：

次のテキストは構成例です。必要に応じて設定を変更してください。これを /etc/dnsmasq.conf 構成ファイルに保存して、デフォルトの構成を上書きします。

```
interface=*
bind-interfaces
enable-tftp
tftp-root=/srv/tftp
port=0
log-dhcp
dhcp-no-override

# UEFI PXE clients only.
dhcp-vendorclass=BIOS,PXEClient:Arch:00000

# Boot directly into shim.
dhcp-boot="BOOTX64.EFI"
```



```
# Use this option to pass parameters to the installer. Currently only
# atxi.wipe= and atomix.isourl are supported.
dhcp-option-force=129,"atomix.isourl=http://ipaddress-of-PXE-server/path/to/install/iso"

# Create a DHCP range and set the gateway.
dhcp-range=rack-rack1-data0,192.168.41.0,static,255.255.255.0,infinite
dhcp-option=rack-rack1-data0,3,192.168.41.1

# Static mapping for clients.
dhcp-host=52:54:00:a2:34:c0,,192.168.41.2,brick2-data2,infinite
dhcp-host=52:54:00:a2:34:02,,192.168.41.3,brick2-data3,infinite
dhcp-host=52:54:00:a2:34:03,,192.168.41.4,brick2-data4,infinite
```

ステップ 7 PXE サーバを再起動します。

ステップ 8 Cisco APIC を再起動し、F12 キーを押してネットワーク ブートを開始します。

PXE サーバを使用する Cisco APIC のインストール

PXE サーバを使用して、UEFI、UEFI セキュアブート、およびレガシー BIOS システムの Cisco Application Policy Infrastructure Controller (APIC) ISO をインストールできます。

次のソフトウェアがシステムにインストールされていることを確認します。

```
sudo apt install -y dnsmasq lighttpd syslinux-common pxelinux
```

DNSMasq の構成

新しい **dnsmasq** 構成を作成するには、以下のコマンドを実行します。

```
$ sudo systemctl stop dnsmasq
$ sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
$ sudo mkdir -p /srv/tftp
```

次のコードスニペットでは、ISO をホストしている HTTP サーバの IP の詳細を入力し、HTTP サーバの IP に到達できる必要があるクライアントの DHCP サブネット範囲を構成する必要があります。変更を含む構成ファイルを保存した後、次のコマンドを実行します。

```
sudo systemctl restart dnsmasq

interface=*
bind-interfaces
enable-tftp
tftp-root=/srv/tftp
port=0
log-dhcp
dhcp-no-override

dhcp-match=x86PC, option:client-arch, 0 # matches legacy BIOS x86
dhcp-match=BC_EFI, option:client-arch, 7 # matches UEFI x86-64

# Load different PXE boot image depending on client architecture
pxe-service=tag:x86PC,X86PC, "Install Linux on x86 BIOS", pxelinux.0
pxe-service=tag:BC_EFI,BC_EFI, "Install Linux on x86-64 UEFI", bootx64.efi

# Set bootfile name only when tag is "bios" or "uefi"
dhcp-boot=tag:x86PC,pxelinux.0 # for Legacy BIOS detected by dhcp-match above
```

```

dhcp-boot=tag:BC_EFI,bootx64.efi    # for UEFI arch detected by dhcp-match above

# Enable PXELinux client options
dhcp-option=tag:x86PC,208,fl:00:74:7e # pxelinux.magic string

# set boot params, note the ip/network is tied to the netplan config in this layer
dhcp-option-force=129,"atxi.wipe=true atomix.isourl=http://<IP of your HTTP
server>/atomix.iso"

# an example IPV4 subnet range
dhcp-range=192.168.41.3,192.168.41.50,12h
dhcp-lease-max=25

```

HTTP設定

デフォルトの **lighttpd** 構成ファイルは、ポート 80 のすべてのインターフェイスでリッスンするため、変更する必要はありません。



- (注) ファイルの名前は、`dhcp-option-force=129` 設定の `/etc/dnsmasq.conf` 値と一致する必要があります。この値は DHCP 設定を介してマシンに渡され、URL を使用して **iso** ファイルをダウンロードします。

インストーラ **ISO** ファイルを次のパスにコピーします。

```
/var/www/html/<ISONAME.iso>
```

PXELINUX の構成

BIOS/レガシーを介して再起動するシステムは、**pxelinux** を使用してインストーラを取得します。上記の **DNSMasq** 構成ファイルの **tftp** の場所が、これらのファイルと構成をコピーするか、必要に応じてコマンドを調整するために使用されていることを確認します。

```

sudo mkdir -p /srv/tftp
sudo cp -av /usr/lib/PXELINUX/* /srv/tftp/
sudo cp /usr/lib/syslinux/modules/bios/* /srv/tftp/
sudo mkdir -p /srv/tftp/pxelinux.cfg

```

次の設定を `/srv/tftp/pxelinux.cfg/default` の場所にコピーし、HTTP サーバーの IP と ISO へのパスに一致するように HTTP URL を変更します。

```

DEFAULT atomix-install

label atomix-install
    kernel vmlinuz
    append initrd=initrd.img ro verbose debug console=tty0 console=ttyS0,115200n8
    atomix.isourl=http://<HTTP_IP>/<ISO NAME>
    sysappend 3

```

ISO からのコンテンツの抽出

ISO を取得したら、次に示すように、ISO からいくつかのファイルを抽出し、特定のディレクトリに配置する必要があります。

```

$ sudo mkdir /mnt/iso /mnt/efi
$ sudo mount -o loop /var/www/html/<ISO filename> /mnt/iso
$ sudo mount -t vfat /mnt/iso/images/efiboot.img /mnt/efi
$ cp -av /mnt/efi/EFI/BOOT/BOOTX64.efi /srv/tftp/bootx64.efi
$ cp -av /mnt/efi/EFI/BOOT/GRUBX64.efi /srv/tftp/grubx64.efi
$ cp -av /mnt/iso/isolinux/vmlinuz /srv/tftp/vmlinuz

```

```
$ cp -av /mnt/iso/isolinux/initrd.img /srv/tftp/initrd.img
$ sudo umount /mnt/efi
$ sudo umount /mnt/iso
```

テスト

構成を適用したら、テスト システムをインストーラで起動し、ネットワーク設定を構成し、HTTP を介して ISO をシステムにダウンロードして、インストールを続行する必要があります。

PXE サーバーでは、次の **dnsmasq** サービスを使用できます。

```
sudo journalctl --follow -u dnsmasq
```



(注) 一部の **dnsmasq** ログエントリには、次のようなエラーが表示される場合があります。ただし、これらのエラーは致命的ではなく、ファームウェアの UEFI PXE クライアントは再試行します。

```
Feb 17 01:01:25 ubuntu dnsmasq-dhcp[1201]: 1836224829 sent size: 10 option: 43 vendor-encap
06:01:08:0a:04:00:50:58:45:ff
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: error 8 User aborted the transfer received
from 192.168.41.3
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: failed sending /srv/tftp/bootx64.efi to
192.168.41.3
Feb 17 01:01:25 ubuntu dnsmasq-tftp[1201]: sent /srv/tftp/bootx64.efi to 192.168.41.3
Feb 17 01:01:47 ubuntu dnsmasq-tftp[1201]: error 3 User provided memory block is too
small received from 192.168.41.3
Feb 17 01:01:47 ubuntu dnsmasq-tftp[1201]: failed sending /srv/tftp/grubx64.efi to
192.168.41.3
Feb 17 01:02:09 ubuntu dnsmasq-tftp[1201]: sent /srv/tftp/grubx64.efi to 192.168.41.3
```

PXE クライアントでは、シリアル コンソール出力にインストールが表示され、特に ISO を取得する方法が表示されます。

これは、インストーラ **iso** ファイルを取得する方法を示すインストーラ出力の一部です。

```
++ cmdline=' BOOT_IMAGE=vmlinuz initrd=initrd.img ro verbose debug console=tty0
console=ttyS0,115200n8 atomix.isourl=http://192.168.41.2/atomix.iso ip=192.168.41.41:192.'
++ case "$cmdline" in
++ val='http://192.168.41.2/atomix.iso
ip=192.168.41.41:192.168.41.2:192.168.41.2:255.255.255.0 BOOTIF=01-52-54-00-12-34-56 '
++ val=http://192.168.41.2/atomix.iso
++ echo http://192.168.41.2/atomix.iso
+ kcurl=http://192.168.41.2/atomix.iso
+ '[' -z http://192.168.41.2/atomix.iso ']'
+ '[' -n http://192.168.41.2/atomix.iso ']'
+ '[' -z '' ']'
+ dhclient
[ 3.573160] 8021q: adding VLAN 0 to HW filter on device ens4
+ tmpiso=/tmp/atomix.iso
++ seq 1 3
+ for count in $(seq 1 3)
+ '[' http: = https ']'
+ busybox wget --output-document=/tmp/atomix.iso http://192.168.41.2/atomix.iso
Connecting to 192.168.41.2 (192.168.41.2:80)
atomix.iso 100% |*****| 842M 0:00:00 ETA
+ break
+ mkdir -p /cdrom
+ mount -o loop,ro /tmp/atomix.iso /cdrom
```

```
[ 4.896038] ISO 9660 Extensions: RRIP_1991A
+ echo 'Found install image through PXE'
Found install image through PXE
...
```

仮想メディアを使用する Cisco APIC ソフトウェアのインストール

仮想メディア（vMedia）を使用した Cisco APIC ソフトウェアのインストールまたはアップグレードは、次の高度なプロセスが必要です：

- 必要に応じて、Cisco Integrated Management Controller（CIMC）ソフトウェアをアップグレードします。
- [Cisco.com](https://www.cisco.com) から、関連する Cisco APIC .iso イメージを入手します。
- コントローラの CIMC Web インターフェイスにアクセスします。



(注) CIMC へのアクセスと、仮想メディアを管理の詳細については、CIMC ソフトウェア (1.5 または 2.0) のコントローラのバージョンに対応する「[CIMC 設定ガイド](#)」を参照してください。

- CIMC vMedia 機能を使用して、.iso イメージをマウントします。
- コントローラを起動し電源を再投入します。
- 起動プロセス中に **[F6]** を押し、ワンタイム起動デバイスとして **[Cisco vCIMC-Mapped vDVD]** を選択します。BIOS パスワードを入力する必要があります。デフォルトパスワードは **password** です。
- インストールする画面の指示に従って、Cisco APIC ソフトウェア。



- (注)
- Cisco APIC リリース 6.0 (2) 以降、ネットワーク経由でのみイメージをインストールできます。画像の場所の URL を指定する必要があります。指定しないと、インストールが無期限に一時停止します。該当するホスト IP アドレス、サブネット、ゲートウェイ、および **[image path]** などの構成の詳細情報ネットワーク キングを入力して、プロンプトに応答します。
 - CIMC 仮想メディアを使用して Cisco APIC ソフトウェアをインストールする前に、Cisco UCS 220 M5 および Cisco UCS 220 M6 サーバーの CIMC コンソールリダイレクションを有効にします。次の CIMC 仮想メディアのインストールで変更を有効にするには、Cisco APIC を再起動する必要があります。

CIMC ソフトウェアのアップグレード

Cisco ACI ファブリック内の Cisco APIC ソフトウェアをアップグレードする場合は、ファブリックで実行されている CIMC のバージョンもアップグレードする必要があります。したがって、各 Cisco APIC リリースでサポートされている CIMC ソフトウェアバージョンのリストについては、該当する Cisco APIC リリースノートを確認することをお勧めします。Cisco APIC リリース ノートは、[APIC のドキュメンテーション ページ](#)で入手できます。

CIMC ソフトウェアをアップグレードするには、まず、ファブリック内の Cisco APIC について、使用している UCS C シリーズ サーバのタイプを決定する必要があります。

Cisco APIC は、次の UCS C シリーズ サーバを使用します。

- Cisco UCS 220 M5 (第 3 世代アプライアンス APIC-SERVER-M3 および APIC-SERVER-L3)
- Cisco UCS 220 M4 (第 2 世代アプライアンス APIC-SERVER-M2 および APIC-SERVER-L2)
- Cisco UCS 220 M3 (第 1 世代アプライアンス APIC-SERVER-M1 および APIC-SERVER-L1)

これら Cisco APIC のサーバのバージョンは、信頼されたプラットフォームモジュール (TPM) 証明書および APIC 製品 ID (PID) を使用してセキュリティ保護されたイメージを使用して製造されている Cisco APIC バージョンの標準バージョンとは異なります。

次の表に、これら Cisco APIC サーバごとの詳細について説明します。

APIC プラットフォーム	対応する UCS プラットフォーム	説明
APIC-SERVER-M1	UCS-C220-M3	中規模の CPU、ハードドライブ、および最大 1000 個のエッジポート用のメモリ構成を備えた 3 台の Cisco APIC 第 1 世代コントローラで構成されるクラスター。
APIC-SERVER-M2	UCS-C220-M4	中規模の CPU、ハードドライブ、および最大 1000 個のエッジポート用のメモリ構成を備えた 3 台の Cisco APIC 第 2 世代コントローラで構成されるクラスター。
APIC-SERVER-M3	UCS-C220-M5	中規模の CPU、ハードドライブ、および最大 1000 個のエッジポート用のメモリ構成を備えた 3 台の Cisco APIC 第 2 世代コントローラで構成されるクラスター。

APIC プラットフォーム	対応する UCS プラットフォーム	説明
APIC-SERVER-L1	UCS-C220-M3	大規模の CPU、ハードドライブ、および 1000 個を超えるエッジポート用のメモリ構成を備えた 3 台の Cisco APIC 第 1 世代コントローラで構成されるクラスター。
APIC-SERVER-L2	UCS-C220-M4	大規模の CPU、ハードドライブ、および 1000 個を超えるエッジポート用のメモリ構成を備えた 3 台の Cisco APIC 第 2 世代コントローラで構成されるクラスター。
APIC-SERVER-L3	UCS-C220-M5	大規模の CPU、ハードドライブ、および 1000 個を超えるエッジポート用のメモリ構成を備えた 3 台の Cisco APIC 第 2 世代コントローラで構成されるクラスター。

次の手順では、Cisco ホストアップグレードユーティリティ (HUU) を使用して Cisco APIC CIMC をアップグレードする方法について説明します。HUU を使用してソフトウェアをアップグレードする方法の詳細については、[Upgrading the Firmware on a Cisco UCS C-Series Server Using the HUU](#) で説明されています。

始める前に

- Cisco APIC リリースノートに記載されている情報を確認し、アップグレードに使用する CIMC ソフトウェアイメージを確認します。Cisco APIC リリースノートは、[APIC のドキュメンテーションページ](#)で入手できます。
- [ソフトウェアダウンロードサイト](#)からソフトウェアイメージを取得します。
- イメージの MD5 チェックサムが、Cisco.com で公開されているものと一致することを確認します。
- アップグレードに十分な時間を確保します。

CIMC バージョンのアップグレードプロセスに必要な時間は、ローカルマシンと UCS-C シャーシ間のリンクの速度と、送信元/ターゲットソフトウェアイメージ、およびその他の内部コンポーネントバージョンによって異なります。

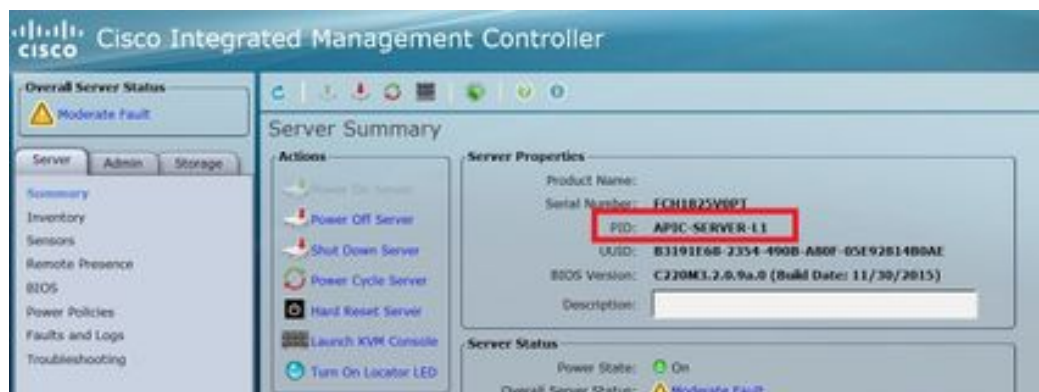
- CIMC バージョンを変更する場合、vKVM を実行するためにインターネットブラウザと Java ソフトウェアのバージョンの変更が必要になることがあります。



- (注) CIMC バージョンをアップグレードしても、Cisco APIC がトラフィックのデータパスに含まれていないため、実稼働ネットワークには影響しません。また、CIMC ソフトウェアをアップグレードするときに Cisco APIC を停止する必要はありません。

手順

- ステップ 1** CIMC クレデンシャルを使用して CIMC にログインします。
- CIMC クレデンシャルは、Cisco APIC クレデンシャルとは異なる場合があることに注意してください。
- ステップ 2** CIMC GUI を使用して、Cisco APIC の UCS プラットフォームのモデルを決定します。
- a) [サーバ (Server)] > [サマリ (Summary)] の下に表示される PID エントリを見つけます。



- b) この手順の最初に記載されている表を使用して、PID エントリに表示される APIC プラットフォームに対応する UCS プラットフォームを検索します。
- たとえば、上記の例に示されている **APIC-SERVER-L1** エントリは、この手順の最初に示されている情報に基づいて、UCS-C220-M3 プラットフォームにマッピングされていることがわかります。

- ステップ 3** <https://software.cisco.com/download> で適切な HUU.iso イメージを見つけます。
- a) <https://software.cisco.com/download> の検索ウィンドウに、前の手順で見つけた Cisco APIC の UCS プラットフォームモデルを、ダッシュを使用せずに入力します。
- 前の手順の例では、検索ウィンドウに **UCS C220 M3** と入力します。
- b) 検索結果のリンクをクリックすると、UCS プラットフォームで使用可能なソフトウェアが表示されます。
- c) お使いのサーバで使用可能なソフトウェアのリストで、ファームウェアエントリを見つけます。これは、**Unified Computing System (UCS) Server Firmware** のように表示されています。ファームウェアのリンクをクリックします。

- d) **CISCO UCS Host Upgrade Utility**.iso イメージのリンクを見つけて、このイメージのリリース情報をメモしておきます。



- ステップ 4** 推奨される [CISCO APIC および Cisco Nexus 9000 シリーズ ACI モード スイッチ リリース \(Recommended Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches Releases\)](#) ドキュメントに移動し、ご使用の UCS プラットフォームおよび APIC ソフトウェア リリースの適切なエントリが含まれている行を見つけます。

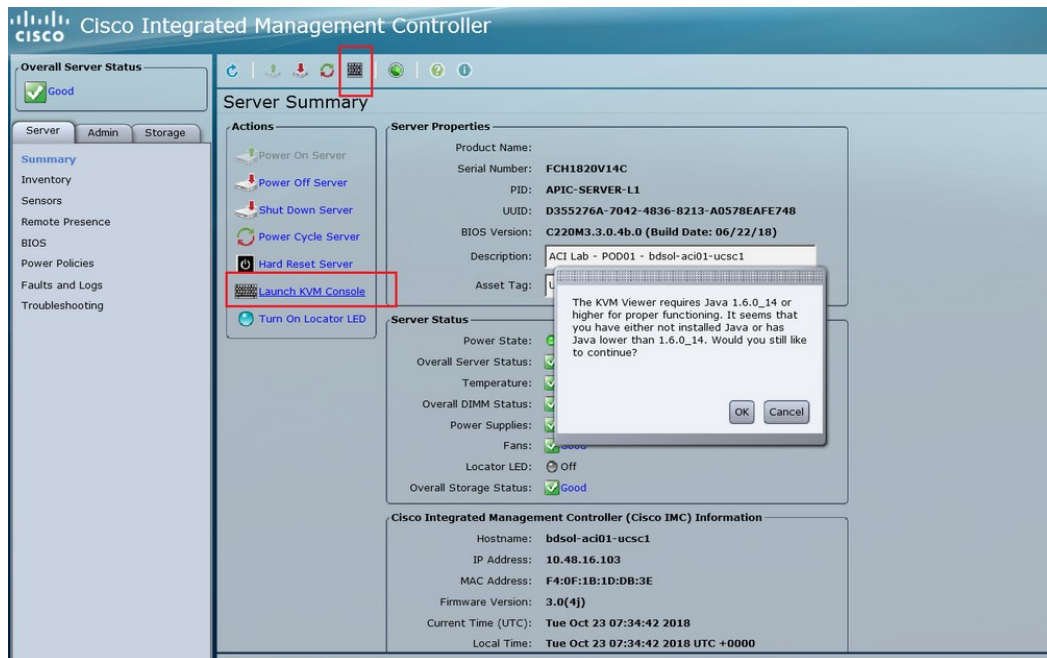
表に示されている UCS バージョンは、対応する APIC リリースに基づく、最新バージョンの CIMC ソフトウェアではない可能性があることに注意してください。たとえば、APIC リリースの 3.0 ブランチの場合、対応する CIMC ソフトウェアリリースは 3.0(3e) である可能性があります。これは必ずしも CIMC ソフトウェアの最新リリースではありませんが、APIC リリースの 3.0 ブランチ CIMC ソフトウェアの正しいバージョンです。

- ステップ 5** 2 つのソースからの情報を比較して、正しいバージョンのイメージをダウンロードしていることを確認します。

2 つのソースの間で矛盾する情報が見つかった場合は、[推奨される CISCO APIC および Cisco Nexus 9000 シリーズ ACI モード スイッチ リリース \(Recommended Cisco APIC and Cisco Nexus 9000 Series ACI-Mode Switches Releases\)](#) のマニュアルに記載されている情報を、ご使用の UCS プラットフォームおよび APIC ソフトウェア リリースの正しいバージョンの HUU.iso イメージを示すものとして使用してください。

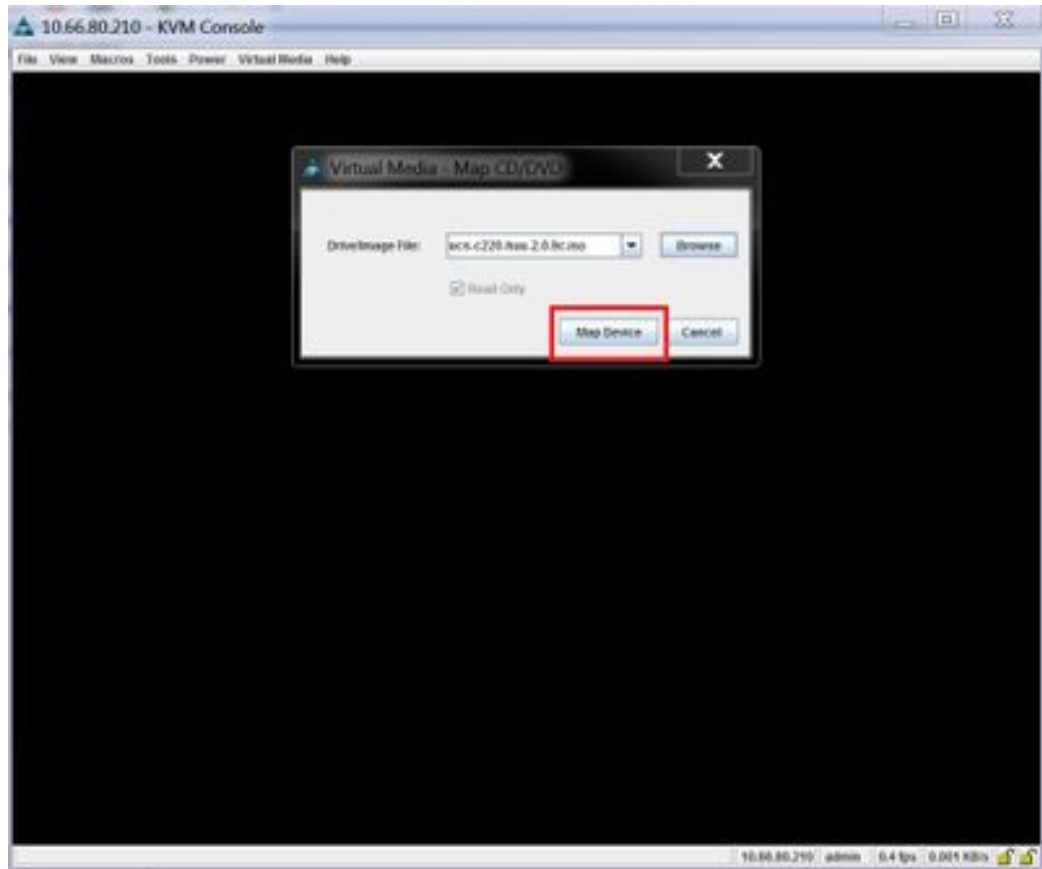
- ステップ 6** <https://software.cisco.com/download> サイトから適切な、.iso イメージをダウンロードします。

- ステップ 7** CIMC GUI から KVM コンソールを起動します。

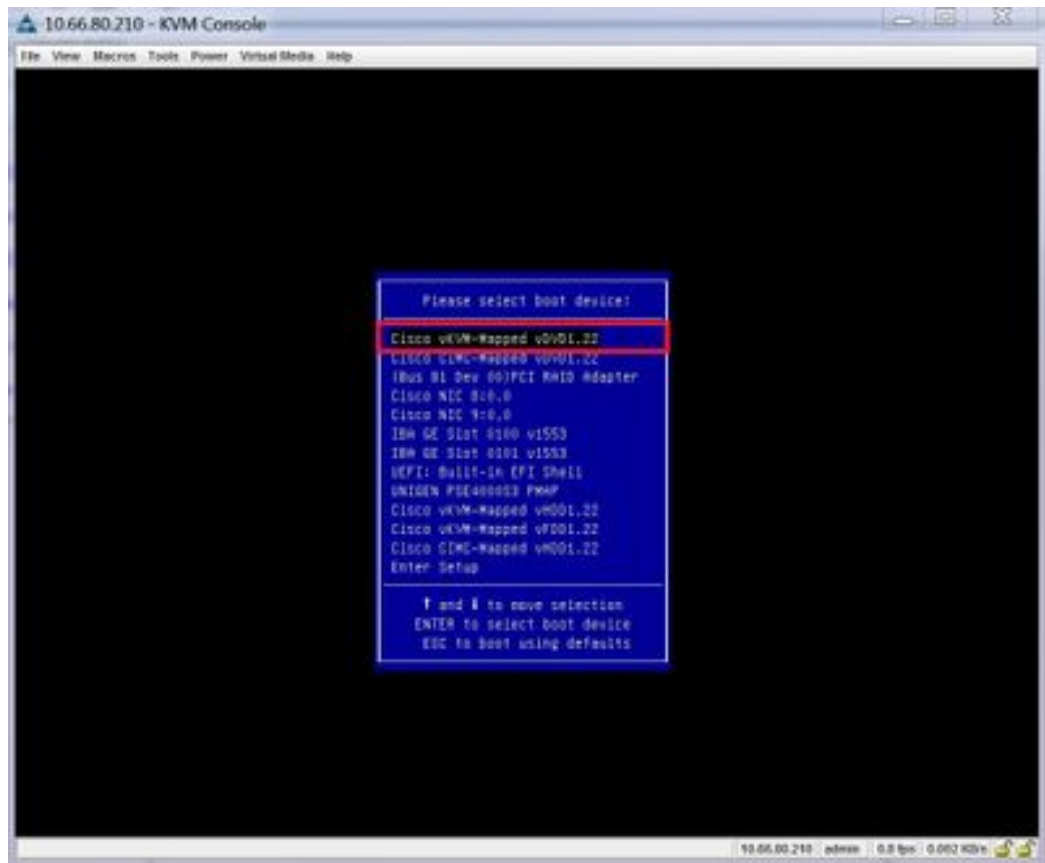


(注) KVM コンソールを開く際に問題が発生した場合は、通常、Java のバージョンで問題が発生しています。お使いの CIMC バージョンで使用可能なさまざまな回避策については、Cisco APIC リリース ノートを参照してください。これは [APIC のドキュメンテーション ページ](#) で確認できます。

- ステップ 8** KVM コンソールで、[仮想メディア (Virtual Media)] > [仮想手パイスのアクティブ化 (Activate virtual Devices)] をクリックし、セッションを受け入れます。
- ステップ 9** [仮想メディア (Virtual Media)] > [CD/DVD のマッピング (Map CD/DVD)] をクリックし、PC でダウンロードしたイメージに移動します。
- ステップ 10** ダウンロードした HUU.iso イメージを選択し、[デバイスのマッピング (Map Device)] をクリックして、ダウンロードした ISO を PC にマッピングします。



- ステップ 11** [マクロ (Macros)] > [静的マクロ (Static Macros)] > [Ctrl-Alt-Del] をクリックして、サーバを再起動します。
- このオプションを使用してサーバを再起動できない場合は、[電源 (Power)] > [システムの電源 サイクル (Power Cycle System)] をクリックして、コールドリブートを実行します。
- ステップ 12** [F6] を押してブートメニューを表示し、マップされた DVD を選択してブートできるようにします。
- また、ユーザ定義マクロを作成して、リモートデスクトップアプリケーションを使用している場合は、[マクロ (Macros)] > ユーザ定義マクロ (User Defined Macros)] > [F6] を選択して、このアクションを実行することもできます。
- ステップ 13** プロンプトが表示されたら、パスワードを入力します。
- デフォルトのパスワードは password です。
- ステップ 14** ブートデバイスを選択するように求められたら、次の図に示すように、[Cisco vKVM にマッピングされた vDVD (Cisco vKVM-Mapped vDVD)] オプションを選択します。

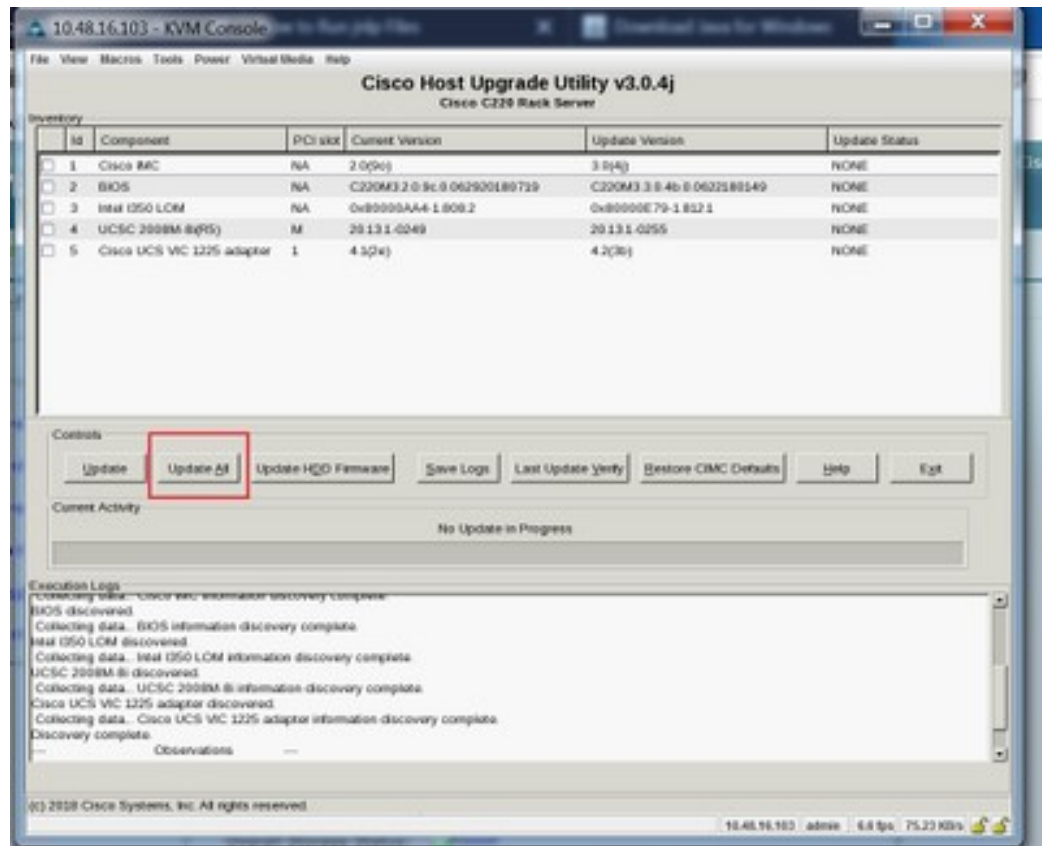


ステップ 15 プロセスが完了するのを待ち、プロンプトが表示されたら、利用規約に同意します。

HUU が ISO から抽出を行うには、10～15 分かかります。その後、ファームウェアやその他のツールがコピーするには、さらに 10～15 分かかります。

ステップ 16 HUU 画面が表示されたら、適切な選択を行います。

すべてのコンポーネントのすべてのファームウェアを更新するには、[すべて更新 (Update all)] オプションを選択することをお勧めします。



ステップ 17 Cisco IMC セキュアブートを有効にするかどうかを確認するポップアップが表示された場合は、そのオプションに対して **[いいえ (No)]** を選択します。

[Cisco UCS C-シリーズ サーバ統合管理コントローラ CLI 設定ガイド、リリース 4.0 \(Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 2.0\(1\)\)](#) の「Cisco IMC セキュアブートの紹介 (Introduction to Cisco IMC Secure Boot)」のセクションを参照してください。

ステップ 18 HUU の **[更新ステータス (Update Status)]** 列に表示されている情報を使用して、更新の進行状況をモニタします。

ステップ 19 各コンポーネントのステータスが **[パス (PASS)]** になったら、**[終了 (Exit)]** をクリックして、サーバを再起動します。

サーバがリブートすると、CIMC GUI は終了します。CIMC に再度ログインし、アップグレードが正常に完了したことを確認する必要があります。

アップグレードが正常に完了したことを確認するには、GUI を使用するか、または CIMC HUU を起動し、**[最後の更新の確認 (Last Update Verify)]** を選択して、すべてのコンポーネントがアップグレードをパスしたことを確かめます。

CIMC 仮想メディアを使用した Cisco APIC ソフトウェアのインストール

Cisco Integrated Management Controller (CIMC) 仮想メディアを使用して Cisco APIC ソフトウェアをインストールするには、この手順に従ってください。



(注) 次の手順では、2つのコンソール ウィンドウを開きます。

- vKVM コンソール
- Serial over LAN (/sol)

この手順のほとんどの手順で、1つまたは他のコンソールウィンドウに特定のコマンドを入力して、2つのコンソール ウィンドウの間を逆方向に反転させることができます。

始める前に

[CIMC ソフトウェアのアップグレード \(13 ページ\)](#) の情報を確認して、このセクションの手順を開始する前に、Cisco Integrated Management Controller (CIMC) ソフトウェアをアップグレードする必要があるかどうかを判断してください。

- APIC-M4/L4 サーバは CIMC 接続で構成する必要があります。
- Cisco APIC ISO は、APIC-M4/L4 CIMC および管理インターフェイスから到達可能な HTTP、HTTPS、または NFS サーバで使用可能である必要があります。
- Cisco.com から関連する Cisco APIC.iso イメージを取得し、.iso イメージを HTTP サーバにコピーします。

手順

ステップ 1 vKVM コンソールにアクセスします。

- コントローラの Cisco Integrated Management Controller (CIMC) GUI を開きます。
- CIMC GUI からの APIC-M1、M2、M3、L1、L2、または L3 サーバの場合、[サーバ (Server)] > [サマリ (Summary)] > [KVM の起動 (Launch KVM)] を選択し、[JAVA ベース KVM (JAVA based KVM)] または [HTML ベース KVM (HTML based KVM)] のいずれかを選択して KVM コンソールにアクセスします。

大規模なファイルにはより信頼性の高いオプションであるため、可能な限り Java ベースの KVM オプションを使用することを推奨します。

- APIC-M4/L4 サーバの場合、CIMC GUI から [サーバ (Server)] > [サマリ (Summary)] > [KVM の起動 (Launch vKVM)] を選択し、HTTP ベース vKVM コンソールにアクセスします。

ステップ 2 Serial on LAN (SOL) コンソールにアクセスします。

- ターミナル ウィンドウから、CIMC コンソールにログインします。

```
# ssh admin@cimc_ip
```

ここで、*cimc_ip*は CIMC IP アドレスです。次に例を示します。

```
# ssh admin@192.0.2.1
admin@192.0.2.1's password:
system#
```

- b) 範囲を仮想メディアに変更します。

```
system# scope vmedia
system /vmedia #
```

- c) .iso イメージを HTTP サーバにマップします。

```
system /vmedia # map-www volume_name http://http_server_ip_and_path iso_file_name
```

それぞれの説明は次のとおりです。

- *volume_name* は、ボリュームの名前です。
- *http_server_ip_and_path*は、HTTP サーバの IP アドレスと .iso ファイルの場所へのパスです。
- *iso_filename* は、.iso ファイルの名前です。

*http_server_ip_and_path*と *iso_filename*の間にスペースがあることに注意してください。

次に例を示します。

```
system /vmedia # map-www apic http://198.51.100.1/home/images/ aci-apic-dk9.4.0.3d.iso
Server username:
```

- d) マッピングのステータスを確認します。

```
system /vmedia # show mappings detail
```

マップステータスは [OK] と表示されます。

- e) SOL (Serial over LAN) に接続し、インストールプロセスを監視します。

```
system /vmedia # connect host
```

ステップ 3 KVM コンソールで、[電源]>[パワー サイクル システム (コールド起動)][システムのリセット (Reset System)] を選択してコントローラの電源を再投入します。

ステップ 4 SOL コンソールから: ブートプロセス中に画面を観察し、適切な時点で **F6** を押してブート選択メニューを開始するように準備します。

起動プロセスが開始されると、最初に次のメッセージが表示されます。

```
Cisco Systems, Inc.
Configuring and testing memory..
Configuring platform hardware...
...
```

システム起動メッセージは、次の画面が表示されるまで表示され続けます。

```
...
Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> Cisco IMC COnfiguration, <F12>
Network Boot
```

ステップ 5 SOL コンソールから: 上記のメッセージが表示されたら、**F6** キーを押して [起動選択 (boot selection)] メニューを表示します。

適切な時点で **F6** を押すことができる場合は、「**起動選択メニューの入力..**」と表示されます。お客様の機会がなく、適切な時点で **F6** を押すことができなかった場合は、[ステップ 3 \(22 ページ\)](#) に戻ってコントローラの電源を再投入し、**F6** キーを押してブート選択メニューを表示できるようになるまで、このプロセスを繰り返します。

ステップ 6 SOL コンソールから: 起動選択メニューで、ワнтаイム起動デバイスとして **Cisco CIMC-Mapped vDVD 1.22** オプションを選択します。

```
/-----\
| Please select boot device: |
|-----|
| (Bus 05 Dev 00)PCI RAID Adapter |
| UNIGEN PHF16H0CM1-DTE PMAP |
| Cisco vKVM-Mapped vHDD1.22 |
| Cisco CIMC-Mapped vHDD1.22 |
| Cisco vKVM-Mapped vDVD1.22 |
| Cisco CIMC-Mapped vDVD1.22 |
| Cisco vKVM-Mapped vFDD1.22 |
| UEFI: Built-in EFI Shell |
| IBA GE Slot 0100 v1585 |
| IBA GE Slot 0101 v1585 |
| Enter Setup |
|-----|
| ^ and v to move selection |
| ENTER to select boot device |
| ESC to boot using defaults |
|-----|
```

また、BIOS パスワードを入力する必要があります。デフォルトパスワードは **password** です。

ステップ 7 SOL コンソールから: 次のように入力します。

a) インストールプロセスを高速化するために ISO URL を入力するかどうかを決定します。

起動プロセス中は次のメッセージが表示される場合があります。

```
To speed up the install, enter iso url in next ten minutes:
```

ここでは2つのオプションを選択できます。

- **ISO URL の入力:** このオプションを選択することをお勧めします。これによりインストールプロセスが高速化されます。次に、ここに入力する HTTP URL の例を示します。

```
http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
```

次の例に示すように、このオプションを選択するとプロトコルの種類を指定するように求められます。

```
? http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
++ awk -F '\/|:' '{print $4}'
+ urlip=10.75.61.1
+ '[' -z http://10.75.61.1/aci-apic-dk9.4.2.1j.iso ']'
+ '[' -z 10.75.61.1 ']'
+ break
+ '[' -n http://10.75.61.1/aci-apic-dk9.4.2.1j.iso ']'
+ set +e
+ configured=0
+ '[' 0 -eq 0 ']'
+ echo 'Configuring network interface'
Configuring network interface
+ echo 'type static, dhcp, bash for a shell to configure networking, or url to
re-enter the url: '
```

適切な SSH プロトコルタイプを選択します。

- **[static]** : このオプションを選択した場合は、インターフェイス名、管理 IP アドレス、およびゲートウェイを入力するよう求められます。次に、正しい管理インターフェイスを見つける方法の例を示します。

```
? static
+ case $ntype in
+ configure_static
+ echo 'Available interfaces'
Available interfaces
+ ls -l /sys/class/net
total 0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp11s0 ->
../devices/pci0000:00/0000:00:03.0/0000:06:00.0/0000:07:01.0/0000:09:00.0/0000:0a:00.0/0000:0b:00.0/net/enp11s0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp12s0 ->
../devices/pci0000:00/0000:00:03.0/0000:06:00.0/0000:07:01.0/0000:09:00.0/0000:0a:01.0/0000:0c:00.0/net/enp12s0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp1s0f0 ->
../devices/pci0000:00/0000:00:01.0/0000:01:00.0/net/enp1s0f0
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 enp1s0f1 ->
../devices/pci0000:00/0000:00:01.0/0000:01:00.1/net/enp1s0f1
lrwxrwxrwx. 1 root root 0 Sep 26 16:04 lo -> ../devices/virtual/net/lo
+ read -p 'Interface to configure: ' interface
Interface to configure:
[anaconda] 1:main* 2:shell 3:log 4:storage-lo> Switch tab: Alt+Tab | Help:
F1
```

上記の出力では、pci 番号が短いネットワーク インターフェイスが 2 つのアウトオブバンド管理インターフェイス（enp1s0f0 (**eth1-1**) および enp1s0f1）に対応しています。両方のインターフェイスが正しく接続されている場合は、どちらかを選択できます。ただし、1 つのインターフェイスにのみケーブルが接続されている場合は、ケーブル接続されたポートに対応するインターフェイスを選択する必要があります。

- **[dhcp]**

また、この ISO URL の `http_server_ip_and_path` と `iso_filename` の間にスペースがないことにも注意してください (たとえば、`http://198.51.100.1/home/images/aci-apic-dk9.4.0.3d.iso`)。

- [Do not enter the ISO URL] : ISO の URL を入力しない場合は、10 分後にインストールプロセスが開始されます。このオプションは、Cisco APIC バージョン 5.3(x)、6.0(2)以降ではサポートされていません。

この時点で ISO の取得が開始されます。

```
+ read -p 'Interface to configure: ' interface
Interface to configure: enpls0f0
+ read -p 'address: ' addr
address: 10.75.39.72/24
+ read -p 'gateway: ' gw
gateway: 10.75.39.254
+ ip addr add 10.75.39.72/24 dev enpls0f0
+ ip link set enpls0f0 up
+ ip route add default via 10.75.39.254
++ seq 1 2
+ for count in '$(seq 1 2) '
+ ping -c 1 10.75.61.1
PING 10.75.61.1 (10.75.61.1) 56(84) bytes of data.
64 bytes from 10.75.61.1: icmp_seq=1 ttl=125 time=0.875 ms

--- 10.75.61.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.875/0.875/0.875/0.000 ms
+ configured=1
+ break
+ '[' 1 -eq 0 ']'
+ echo 'Fetching http://10.75.61.1/aci-apic-dk9.4.2.1j.iso'
Fetching http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
+ wget -o /dev/null -O /tmp/cdrom.iso http://10.75.61.1/aci-apic-dk9.4.2.1j.iso
```

KVM コンソールで [ツール (Tools)] > [統計情報 (Stats)] に移行することによって、プロセスのステータスを追跡できます。

- SOL コンソールにメッセージ **poweroff** が表示されるまで待機してから、**Ctrl + x (Ctrl + x)** を押して SOL を終了します。
- 範囲を仮想メディアに変更します。

```
system# scope vmedia
system /vmedia #
```

- [2.c \(22 ページ\)](#) にマッピングした .iso イメージのマッピングを解除します。

```
system /vmedia # unmap volume_name
```

マッピングを保存する場合は、[マッピングの保存 (save mapping)] プロンプトで **yes** と入力します。マッピングを保存しない場合は **no** を選択します。次に例を示します。

```
system /vmedia # unmap apic
Save mapping? Enter 'yes' or 'no' to confirm (CTRL-C to cancel) → yes
system /vmedia #
```

- 再度 SOL に接続します。

```
system /vmedia # connect host
```

ステップ 8 KVM コンソールで、[電源]>[システムの電源をオンにする]を選択してコントローラの電源を投入します。

ステップ 9 SOL コンソールから: 次のように入力します。

- a) ファブリック名、コントローラ数、トンネルエンドポイントアドレスプール、インフラ VLAN ID などの初期セットアップのオプションを入力し、インストールプロセスを完了します。

ACI ファブリックのクリーン初期化の実行

最初にファブリックを起動する際にファブリックのクリーン再起動を実行し、ファブリックが正常に動作しない場合、クリーン再起動がファブリックを再度起動する唯一のオプションとなります。これにより、Cisco APIC およびスイッチノードからすべての設定が削除されます。その後、最初から設定を開始するか、設定バックアップから再インポートする必要があります。

手順

ステップ 1 アウトオブバンド管理で各 Cisco APIC にログインし Cisco APIC DME アプリケーションを停止します。

例:

```
acidiag stop mgmt
```

ステップ 2 アウトオブバンド管理を使用して各スイッチにログインします。アウトオブバンド管理が使用できない場合は、コンソールを使用してログインします。次のコマンドセットのいずれかを使用して、スイッチをクリーン再起動します。

例:

```
leaf101# setup-clean-config.sh
In progress
In progress
Done
leaf101# reload
This command will reload the chassis, Proceed (y/n)? [n]: y
```

または

```
leaf101# acidiag touch clean
This command will wipe out this device, Proceed? [y/N] y
leaf101# reload
This command will reload the chassis, Proceed (y/n)? [n]: y
```

ステップ 3 次の通りに各 Cisco APIC にログインし、Cisco APIC を再起動します。

例:

```
acidiag touch clean  
acidiag reboot
```

また、初期設定パラメータを再設定する場合は、以下に示すように `acidiag touch setup` コマンドも含める必要があります。

```
acidiag touch clean  
acidiag touch setup  
acidiag reboot
```

(注) このエラーを無視する：「`acidiag: error: curl: (52) Empty reply from server`」

ファブリックがクリーン再起動されると、ノードは検出されません。ノードポリシーをポストする、UIを使用してスイッチを登録する、または設定のバックアップをインポートできます。

翻訳について

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