アプライアンスの設定準備

アプライアンス設定の準備の概要

Cisco DNA Center アプライアンスを正常に設定するには、まず、次のタスクを実行します。

1. アプライアンスの Cisco IMC に対するアクセスを有効にします（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。
2. Cisco IMC を使用して、ハードウェアとスイッチの重要な設定を確認、調整します（「事前設定チェックの実行」を参照）。
3. Cisco DNA Center ソフトウェアはあらかじめアプライアンスにインストールされていますが、状況によってはソフトウェアを再インストールする必要が生じる場合があります（現在のクラスタリンク設定を変更する前など）。このような場合は、「アプライアンスのイメージの再作成」で説明されているタスクも実行する必要があります。

（注） アプライアンスのイメージを再作成する必要がない場合は、「アプライアンスの設定の概要」に進みます。

Cisco Integrated Management Controller に対するブラウザアクセスの有効化

「アプライアンスのインストールワークフロー」の説明に従ってアプライアンスをインストールした後、Cisco IMC 設定ユーティリティを使用して、アプライアンスの CiIMC ポートに IP

アドレスとゲートウェイを割り当てます。この操作で Cisco IMC GUI にアクセスできるようになります。これはアプライアンスを設定するとき使用する必要があります。

Cisco IMC の設定が完了したら、Cisco IMC にログインし、「事前設定チェックの実行」に記載されているタスクを実行して、設定が正しいことを確認します。

ヒント お客様の環境のセキュリティを確保するため、アプライアンスの初回ブート時は、Cisco IMC ユーザのデフォルトパスワードを変更するように求められます。Cisco IMC ユーザパスワードを後で変更するには、次のように Cisco IMC GUI を使用します。

1. GUI の左上隅から **[Toggle Navigation]** アイコン（  ）をクリックし、**[Admin]** > **[User Management]** を選択します。

   [Local User Management] タブがすでに選択されている必要があります。

2. ユーザ**1**のチェックボックスをオンにして、**[Modify user]** をクリックします。

   [Modify User Details] ダイアログボックスが開きます。

3. [Change Password] チェックボックスをオンにします。

4. 新しいパスワードを入力して確認し、**[Save]** をクリックします。

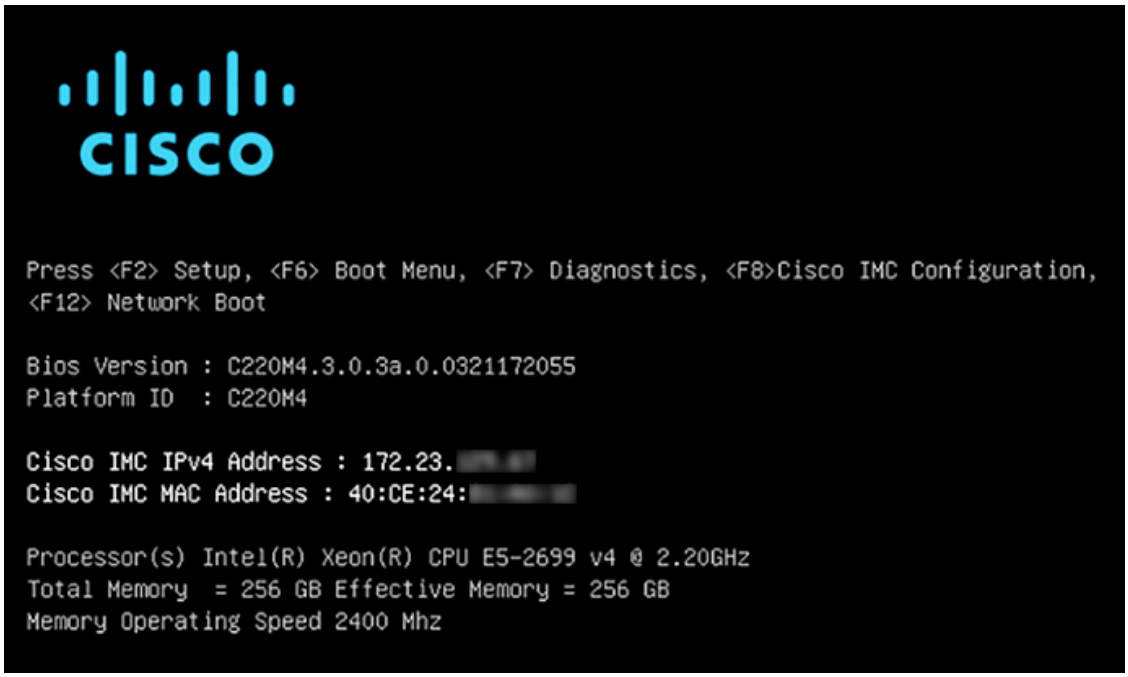
ステップ 1 次のいずれかを接続して、アプライアンスコンソールにアクセスします。

- アプライアンスの前面パネルにある KVM コネクタ（「前面パネルと背面パネル」の前面パネル図のコンポーネント 12）に接続する KVM ケーブルか、
- アプライアンスの背面パネルにある USB ポートと VGA ポート（「前面パネルと背面パネル」の背面パネル図のコンポーネント 7 および 12）に接続するキーボードとモニタ。

ステップ 2 アプライアンスの電源コードが接続され、電源がオンになっていることを確認します。

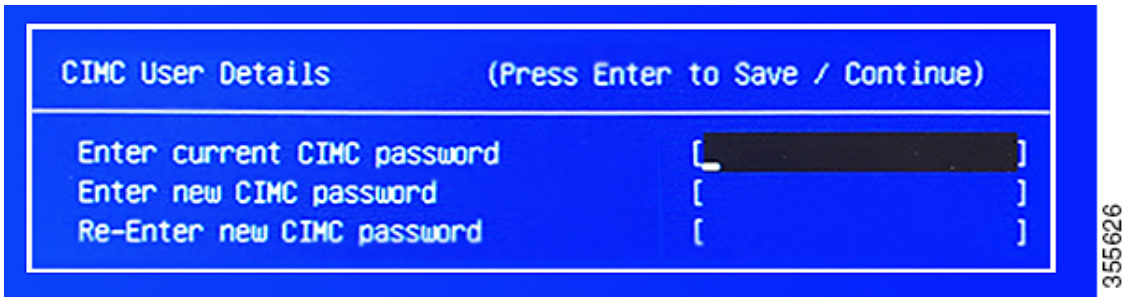
ステップ 3 前面パネルの**電源**ボタンを押して、アプライアンスをブートします。

Cisco IMC 設定ユーティリティの次のようなブート画面が表示されます。



ステップ 4 ブート画面が表示されたら、すぐに **F8** キーを押して Cisco IMC 設定を実行してください。

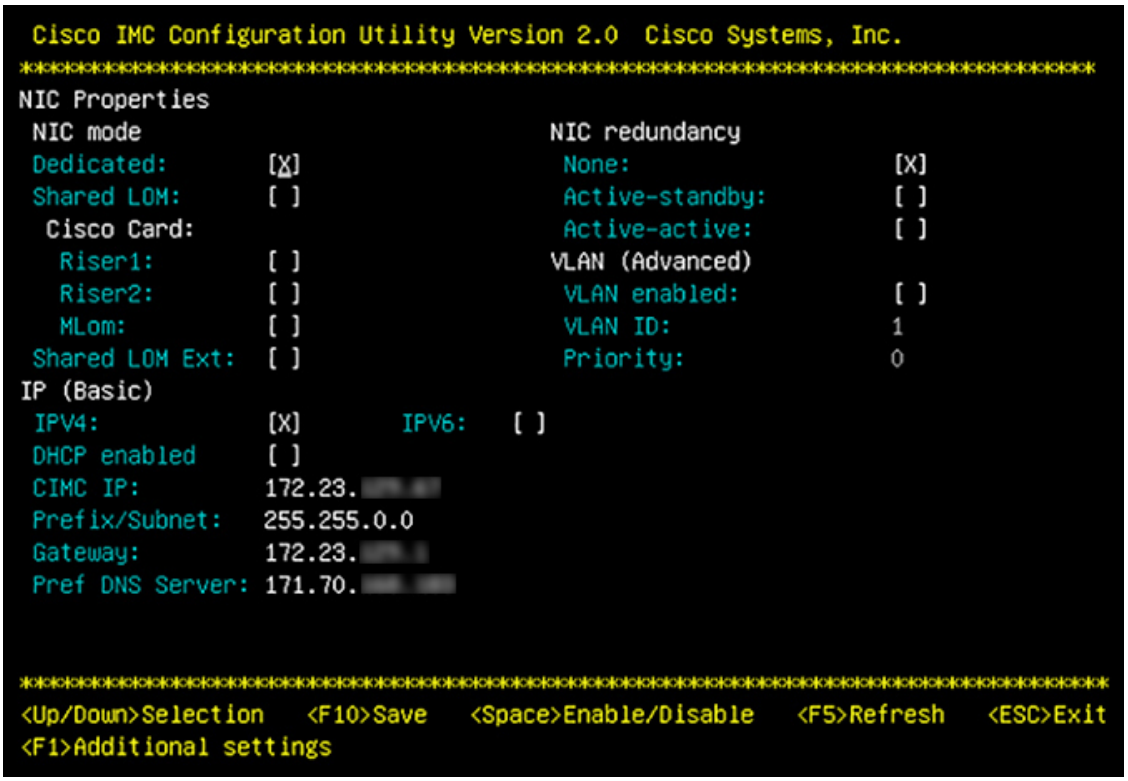
次に示すように、Cisco IMC 設定ユーティリティに **[CIMC User Details]** 画面が表示されます。



ステップ 5 デフォルトの CIMC ユーザパスワード（新規アプライアンスで付与されるデフォルトのパスワードは「*password*」）を **[Enter current CIMC Password]**フィールドに入力します。

ステップ 6 次に **[Enter New CIMC Password]** フィールドと **[Re-Enter New CIMC Password]** フィールドに新しい CIMC ユーザパスワードを入力して確認します。

[Re-Enter New CIMC Password] フィールドで **Enter** を押すと、次に示すように、Cisco IMC 設定ユーティリティに **[NIC Properties]** 画面が表示されます。

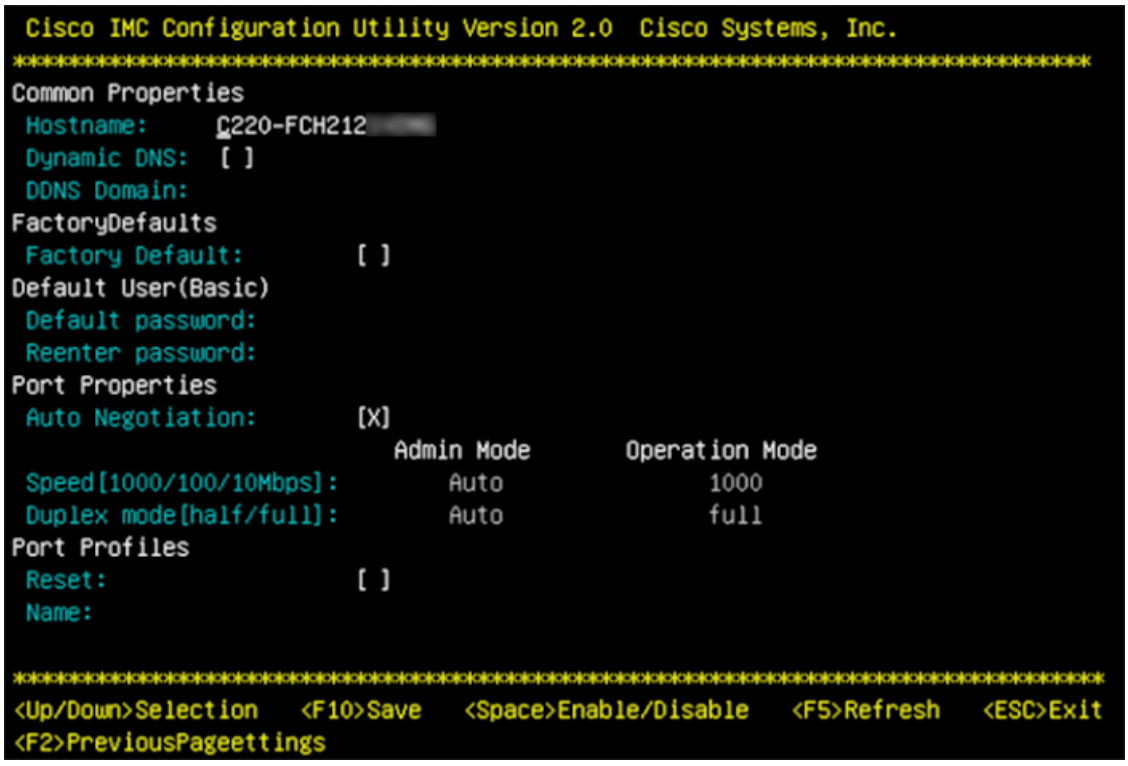


ステップ 7 次のアクションを実行します。

- **NIC モード（NIC mode）**：**[Dedicated]** を選択します。
- **IP（基本）**：**[IPV4]** を選択します。
- **CIMC IP**：CIMC ポートの IP アドレスを入力します。
- **プレフィックス/サブネット（Prefix/Subnet）**：CIMC ポート IP アドレスのサブネットマスクを入力します。
- **ゲートウェイ（Gateway）**：優先するデフォルトゲートウェイの IP アドレスを入力します。
- **優先DNSサーバ（Pref DNS Server）**：優先 DNS サーバの IP アドレスを入力します。
- **NIC 冗長性（NIC Redundancy）**：**[なし（None）]** を選択します。

ステップ 8 **F1** を押して **[Additional Settings]** を指定します。

次に示すように、Cisco IMC 設定ユーティリティに **[Common Properties]** 画面が表示されます。



ステップ 9 次のアクションを実行します。

- **ホスト名（Hostname）**：このアプライアンスで使用する CIMC のホスト名を入力します。
- **ダイナミックDNS（Dynamic DNS）**：チェックボックスをオフにすると、この機能が無効になります。
- **出荷時の初期状態（Factory Defaults）**：チェックボックスをオフにして、この機能を無効にします。
- **デフォルトのユーザ（基本設定）（Default User（Basic））**：フィールドを空白のままにします。
- **ポートのプロパティ（Port Properties）**：新しい設定を入力するか、フィールドに表示されるデフォルト値を受け入れます。
- **ポートプロファイル（Port Profiles）**：チェックボックスをオフにすると、この機能が無効になります。

ステップ 10 F10 を押して、設定を保存します。

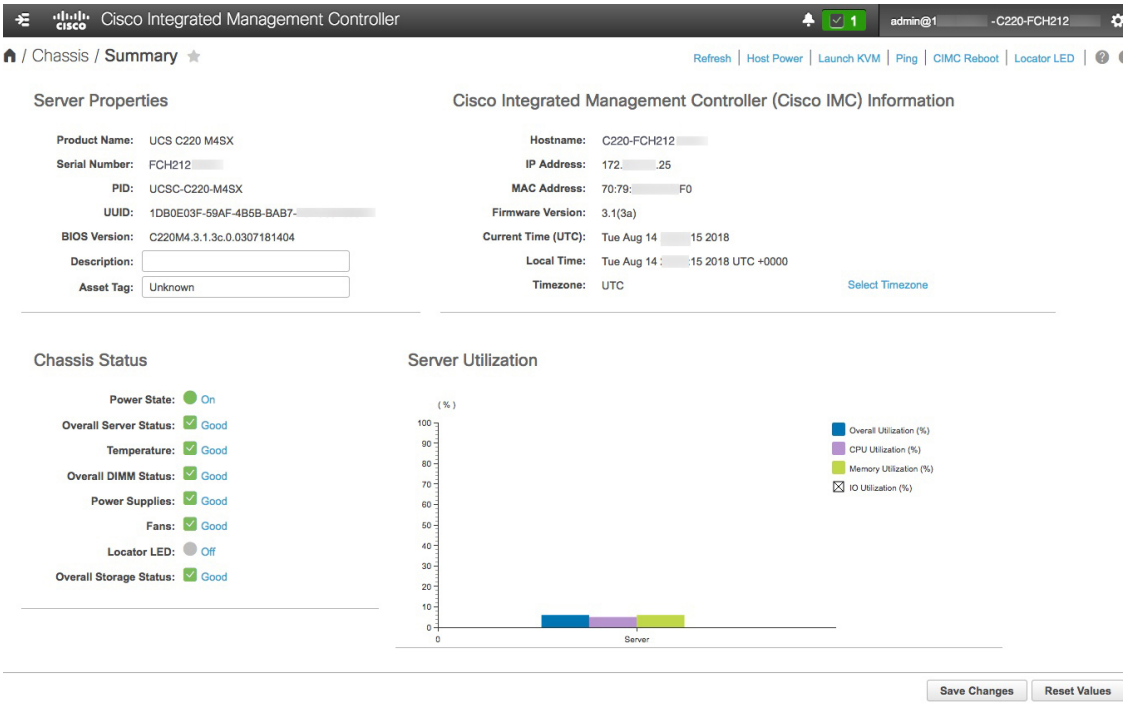
ステップ 11 **Esc** キーを押して終了し、アプライアンスをリブートします。

ステップ 12 設定が保存され、アプライアンスのリブートが完了したら、アプライアンスがインストールされているサブネットへのアクセスが可能なクライアントマシンで互換性のあるブラウザを開き、次の URL を入力します。

https://*CIMC_ip_address*（この ***CIMC_ip_address*** は先ほどステップ 7 で入力した Cisco IMC ポート IP アドレスです。

次に示すような Cisco IMC GUI のメインログインウィンドウがブラウザに表示されます。

ステップ 13 ステップ 5 で設定した Cisco IMC ユーザのユーザ ID とパスワードを使用してログインします。ログインに成功すると、以下と同じような **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウがブラウザに表示されます。



ステップ 14 このバージョンの Cisco IMC が、インストールする Cisco DNA Center リリースでサポートされていることを確認します。

a) [Firmware Version] フィールドにリストされているバージョンをメモします。

b) インストールする Cisco DNA Center リリースのリリースノートを参照してください。「Supported Firmware」セクションには、ご使用の Cisco DNA Center リリースでサポートされている Cisco IMC のバージョンが示されています。

c) 次のいずれかを実行します。

- 適切な Cisco IMC バージョンがインストールされている場合は、ここで終了できます。
- Cisco IMC のバージョンを更新する必要がある場合は、『*Cisco Host Upgrade Utility User Guide*』を参照してください。

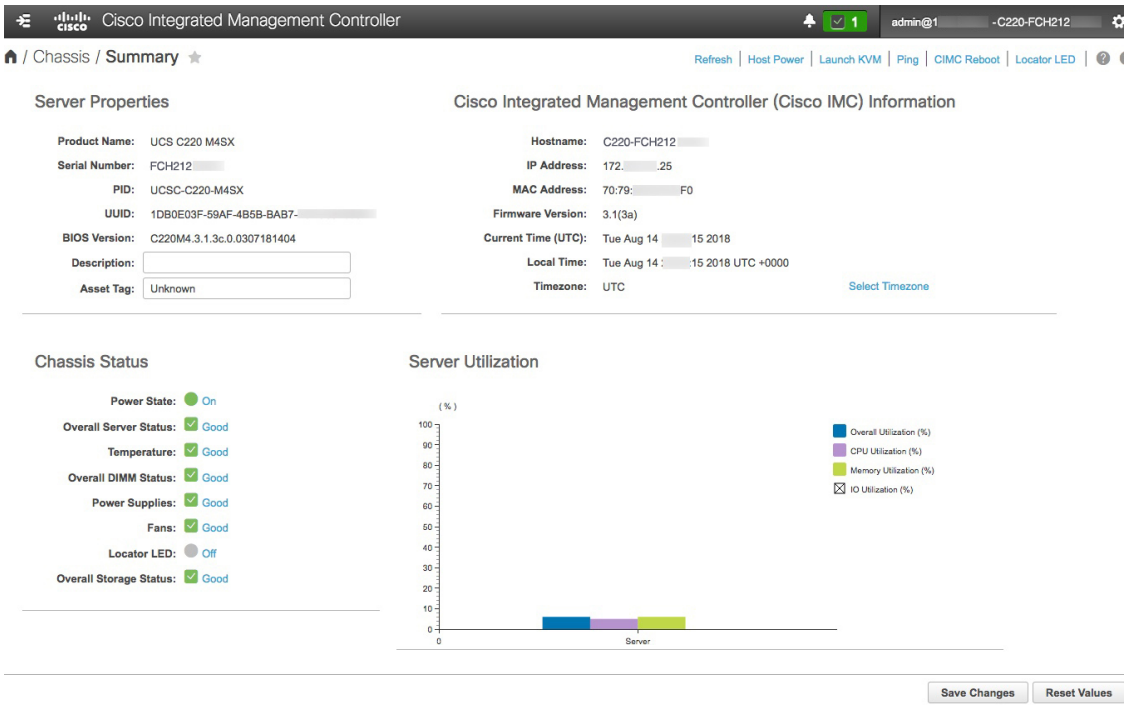
事前設定チェックの実行

アプライアンスをインストール（「アプライアンスのインストールワークフロー」の説明どおり）し、Cisco IMC の GUI へのアクセスを設定（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」の説明どおり）した後、Cisco IMC を使用して次の事前設定タスクを実行します。この操作は、正しい設定と展開の確実な実行に役立ちます。

1. アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol（NTP）サーバと同期します。同期する NTP サーバは、「必要な IP アドレスおよびサブネット」で説明されているように、実装の計画時に収集したホスト名または IP を持つ NTP サーバである必要があります。Cisco DNA Center データがネットワーク全体で正しく同期されるよう徹底するには、このタスクが不可欠です。
2. アプライアンスの 10 Gbps ポートが有効で、高スループットに適した設定になっていることを確認します。
3. 10 Gbps アプライアンスポートに接続されているスイッチを再設定して、高スループット設定がサポートされるようにします。
4. オーバーサイズの 802.1p フレームがサポートされるように、10 Gbps アプライアンスポートに接続されているスイッチを再設定します。

ステップ 1 「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」で設定した CISCO imc IP アドレス、ユーザ ID、パスワードを使用して、アプライアンスの Cisco IMC にログインします。

ログインに成功すると、次に示すような **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウがブラウザに表示されます。

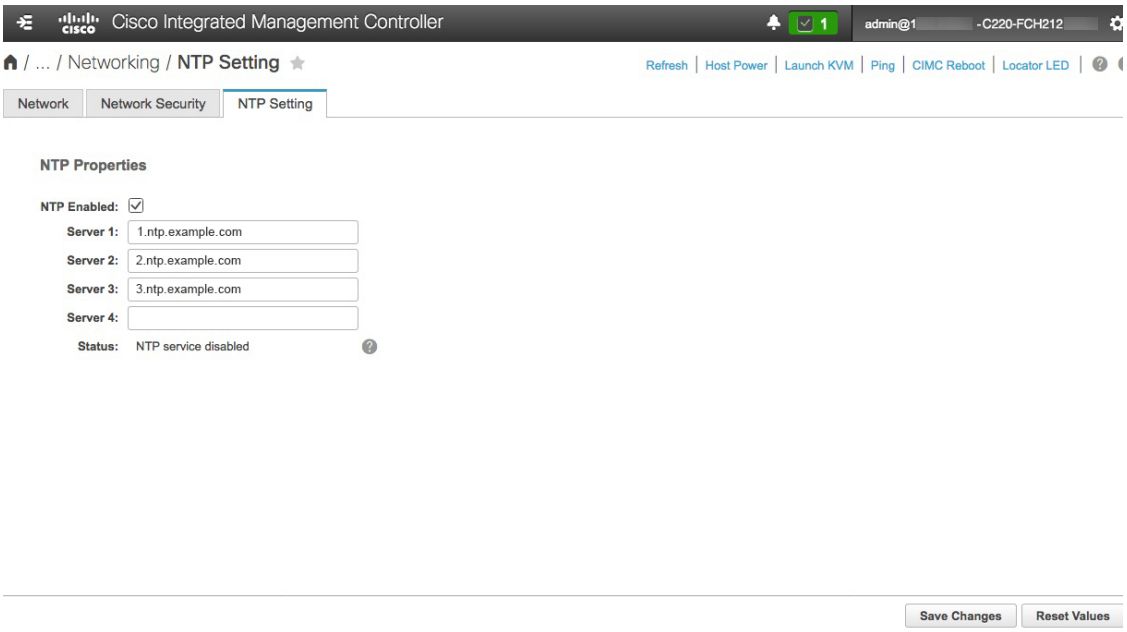


ステップ 2 次に示すように、アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol（NTP）サーバと同期します。

a) Cisco IMC GUI の左上隅から、**[Toggle Navigation]** アイコン（ ）をクリックします。

b) Cisco IMC メニューから **[Admin]** > **[Networking]** を選択し、**[NTP Setting]** タブを選択します。

c) **[NTP Enabled]** チェックボックスがオンになっていることを確認してから、次に示す例のように、4 つの番号付き**サーバ**フィールドに最大 4 つの NTP サーバホスト名またはアドレスを入力します。



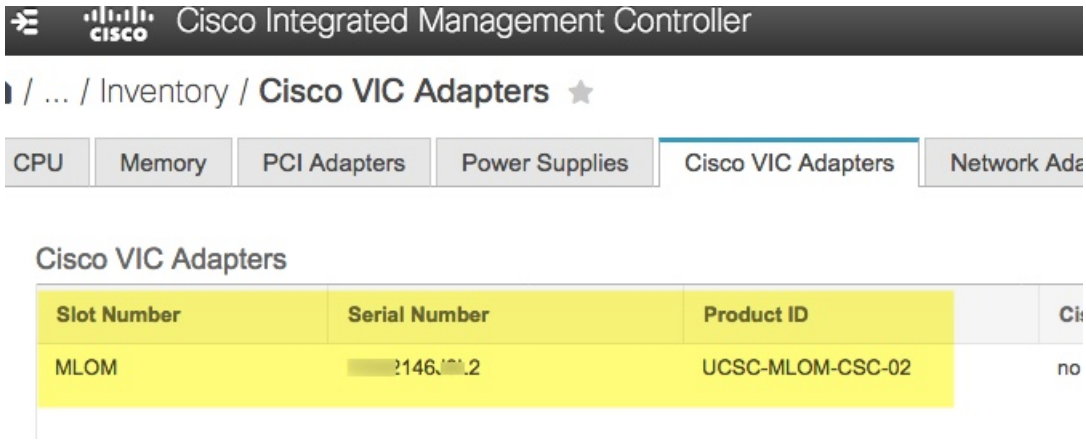
d) [Save Changes] をクリックします。Cisco IMC はエントリを検証した後、アプライアンスハードウェアの時刻と NTP サーバの時刻の同期を開始します。

（注） Cisco IMC で NTP 認証はサポートされていません。

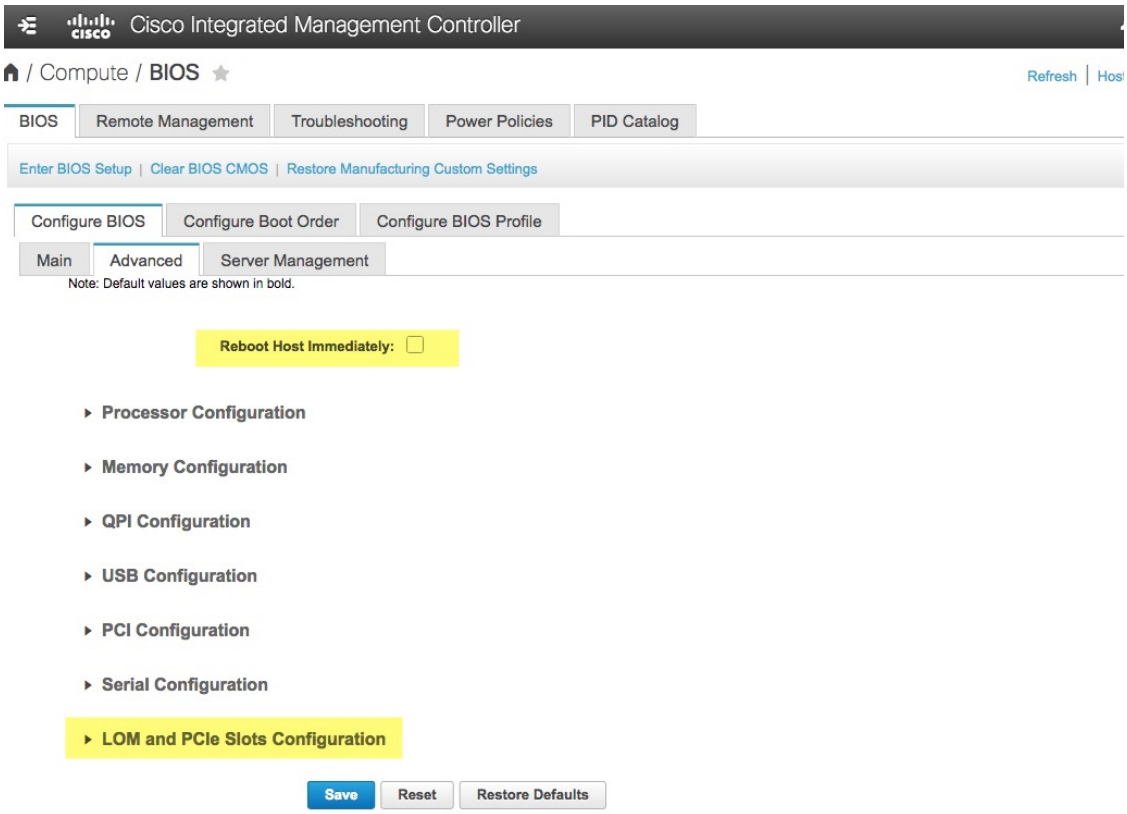
ステップ 3 次に、以下の手順を実行して、アプライアンス NIC が高スループットをサポートするように設定されていることを確認します。

a) 必要に応じて、アイコンをクリックして Cisco IMC のメニューを表示します。

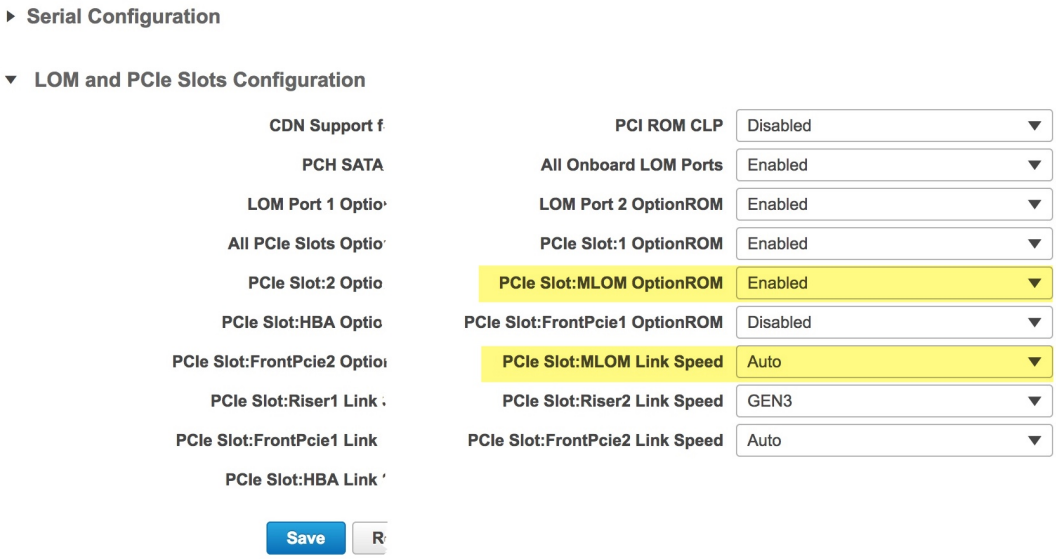
b) Cisco IMC のメニューから、**[Chassis]** > **[Inventory]** > **[Cisco VIC Adapters]** の順に選択します。次に示すように、製品 ID「UCSC-MLOM-CSC-02」が MLOM スロット用に一覧表示されていることを確認します。



c) > **[Compute]** > **[BIOS]** > **[Configure BIOS]** > **[Advanced]** の順に選択します。[Reboot Host Immediately] チェックボックスがオフになっていることを確認し、[LOM and PCIe Slots Configuration] ドロップダウンの場所を確認します。

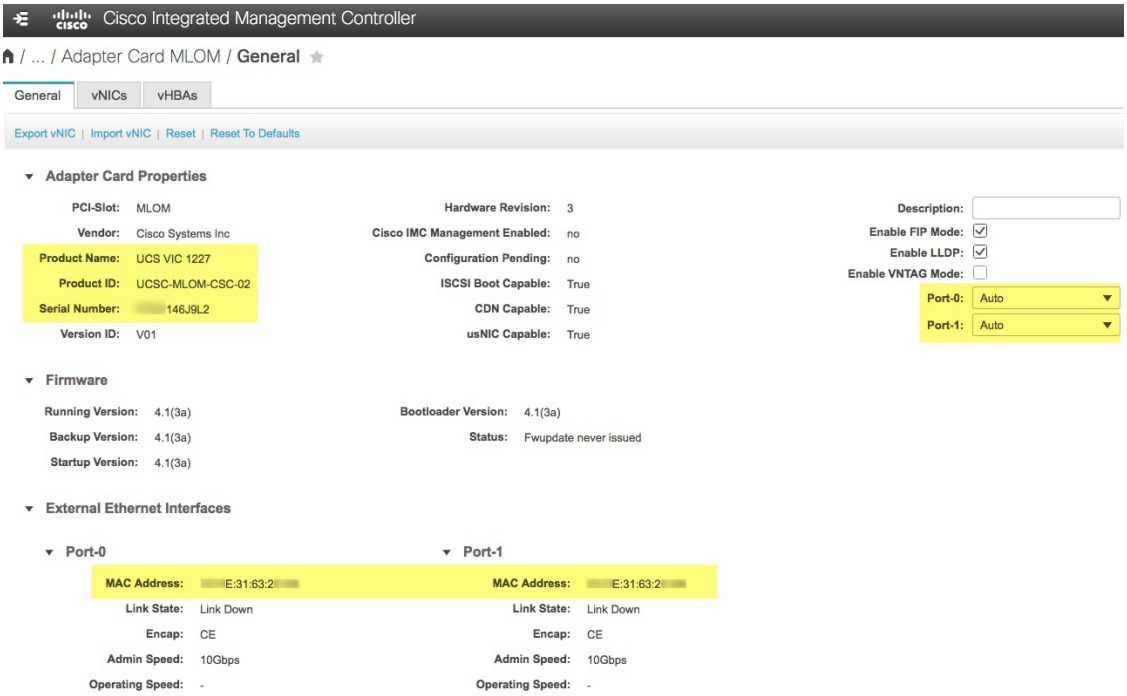


d) [LOM and PCIe Slots Configuration] を選択します。次に、ドロップダウンセレクタを使用して、[PCIe Slot MLOM OptionROM] を [Enabled] に、[PCIe Slot: MLOM Link Speed] を [Auto] に設定します。



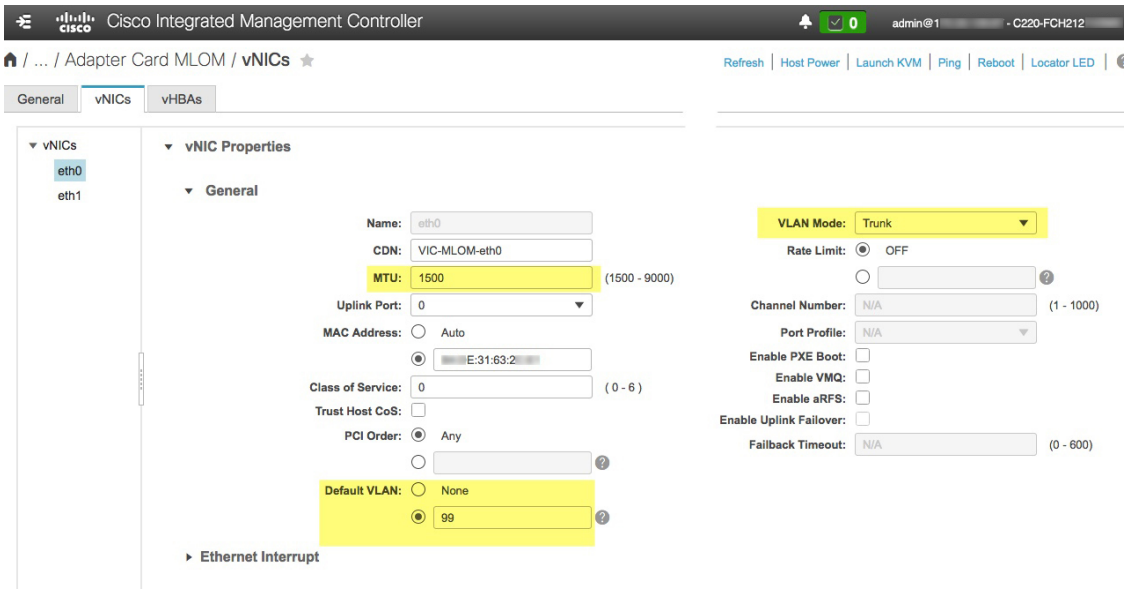
e) **[保存（Save）]** をクリックします。ホストをリブートするように求められます。[OK] をクリックして、リブートせずに続行します。

f) > **[Networking]** > **[Adapter Card MLOM]** > **[General]** の順に選択します。[Port-0] と [Port-1] の MAC アドレスを確認します（ページ下部にある [External Ethernet Interfaces] セクションに表示されます）。次に示すように、[Adapter Card Properties] セクションで、[Port-0] と [Port-1] の横にあるドロップダウンセレクタを使用して、両方のポートの速度を [Auto] に設定します。[Save Changes] をクリックします。



g) [vNICs] タブをクリックし、[vNICs] ドロップダウンで [eth0] を選択します。セレクタとフィールドを使用して、次の値を [eth0] に設定します。

- **[VLAN Mode]**：**[Trunk]**
- **MTU**：**1500**
- [Default VLAN]：99（「99」は一例にすぎないことに注意してください。アプライアンスとそれに接続されているアップリンクスイッチで使用するデフォルト VLAN 値を入力する必要があります）



ヒント　1500は、最大伝送単位（MTU）の最小サイズです。さらに大きな値を入力して、10 Gbpsポートのスループットを向上させることができます（上限は9000）。

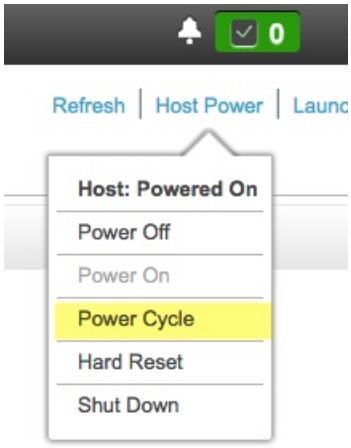
h) [Save Changes] をクリックします。ホストをもう一度リブートするように求められます。[Cancel] をクリックして、リブートせずに続行します。

i) [vNICS] ドロップダウンから [eth1] を選択し、アプライアンスとそれに接続されているアップリンクスイッチで使用する値を設定します。

j) 完了したら、[変更の保存（Save Changes）] をクリックします。ホストをリブートするように求められます。今回は、[OK] をクリックしてアプライアンスをリブートします。

k) アプライアンスのリブートが完了したら、Cisco IMC GUI に再度ログインします。> **[Networking]** > **[Adapter Card MLOM]** > **[General]** > **[vNICs]** の順に選択します。vNIC MAC アドレスと、以前に設定した [MTU]、[VLAN]、[VLAN Mode] の各パラメータが正確かどうかを確認します。

l) 終了したら、右上の [Host Power] メニューをクリックして、[Power Cycle] を選択します。次に [OK] をクリックします。



ステップ 4 アプライアンスの高スループット設定と一致するようにスイッチを再設定します。

a) セキュアシェル（SSH）クライアントを使用して、設定するスイッチにログインし、スイッチプロンプトで EXEC モードを開始します。

b) スイッチポートを設定します。

Cisco Catalyst スイッチで、次のコマンドを入力します。次に例を示します。

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitethernet 1/1/3
MySwitch(config-if)#switchport
MySwitch(config-if)#switchport mode trunk
MySwitch(config-if)#switchport trunk allowed vlan 99
MySwitch(config-if)#switchport voice vlan dot1p
MySwitch(config-if)#speed auto
MySwitch(config-if)#duplex full
MySwitch(config-if)#mtu 1500
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#do copy running-config startup-config
```

Cisco Nexus スイッチで、次のコマンドを入力して、Link Layer Discovery Protocol（LLDP）およびプライオリティフロー制御（PFC）を無効にします。次に例を示します。

```
N7K2# configure terminal
N7K2(config)# interface eth 3/4
N7K2(config-if)# no priority-flow-control mode auto
N7K2(config-if)# no lldp transmit
N7K2(config-if)# no lldp receive
```

これらのコマンドは単なる例であることに注意してください。アプライアンスの NIC を設定する場合は、この手順のステップ 3 で入力したものと同じ VLAN ID と MTU 値を使用してください。リンク速度、デュプレックス、MTU の各パラメータに表示される値が、スイッチのデフォルトです。このデフォルトを変更した場合にのみ、これらのパラメータの新しい値を入力します。アプライアンス NIC と同様に、スループットが向上するように MTU を設定することもできます（上限は 9000）。

c) `show interface tengigabitethernet` *`portID`* コマンドを実行して、ポートが接続されて動作していることと、正しいMTU、デュプレックス、リンクタイプが設定されていることをコマンド出力で確認します。次に例を示します。

```
MySwitch#show interface tengigabitethernet 1/1/3
TenGigabitEthernet1/1/3 is up, line protocol is up (connected)
  Hardware is Ten Gigabit Ethernet, address is XXXe.310.8000 (bia XXX.310.8000)
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 10GB/s, link type is auto, media type is SFP-10Gbase-SR
```

d) `show run interface tengigabitethernet` *`portID`* コマンドを実行して、VIC 1227 ポートからのケーブルが接続されているスイッチポートを設定します。次に例を示します。

```
MySwitch#show run interface tengigabitethernet 1/1/3
Building configuration...
Current configuration : 129 bytes
!
interface TenGigabitEthernet1/1/3
 switchport trunk allowed vlan 99
 switchport mode trunk
end
```

```
MySwitch#
```

e) `show run interface tengigabitethernet portID` コマンドを実行して、ポートに `voice vlan dot1p` が正しく設定されていることをコマンド出力で確認します。次に例を示します。

```
MySwitch#show run interface tengigabitEthernet 1/1/3
Building configuration...
Current configuration : 129 bytes
!
interface TenGigabitEthernet1/1/3
 switchport trunk allowed vlan 99
 switchport mode trunk
 switchport voice vlan dot1p
end

MySwitch#
```

f) `show mac address-table interface tengigabitethernet portID` コマンドを実行して、コマンド出力で MAC アドレスを確認します。次に例を示します。

```
MySwitch#show mac address-table interface tengigabitethernet 1/1/3
          Mac Address Table
-------------------------------------------
Vlan     Mac Address       Type      Ports
----     -----------       ----      -----
99       XXXe.3161.1000    DYNAMIC   Te1/1/3
Total Mac Addresses for this criterion: 1

MySwitch#
```

次のタスク

このタスクが完了したら、次のいずれかを実行します。

- アプライアンスを設定する前に Cisco DNA Center ソフトウェアを再インストールする必要がある場合は、「アプライアンスのイメージの再作成」を参照してください。
- アプライアンスの設定を行う準備ができたら、「アプライアンスの設定の概要」に進みます。

アプライアンスのイメージの再作成

バックアップからの回復やクラスタリンク設定の変更など、Cisco DNA Center アプライアンスの再イメージ化が必要な状況が発生する場合があります。これを行うには、次の手順を実行します。

ステップ 1 Cisco DNA Center ISO イメージをダウンロードし、それが正規の Cisco イメージであることを確認します。

「Cisco DNA Center イメージの確認 （16 ページ）」を参照してください。

ステップ 2 Cisco DNA Center ISO イメージを含むブート可能 USB ドライブを作成します。

「ブート可能な USB フラッシュドライブの作成 （17 ページ）」を参照してください。

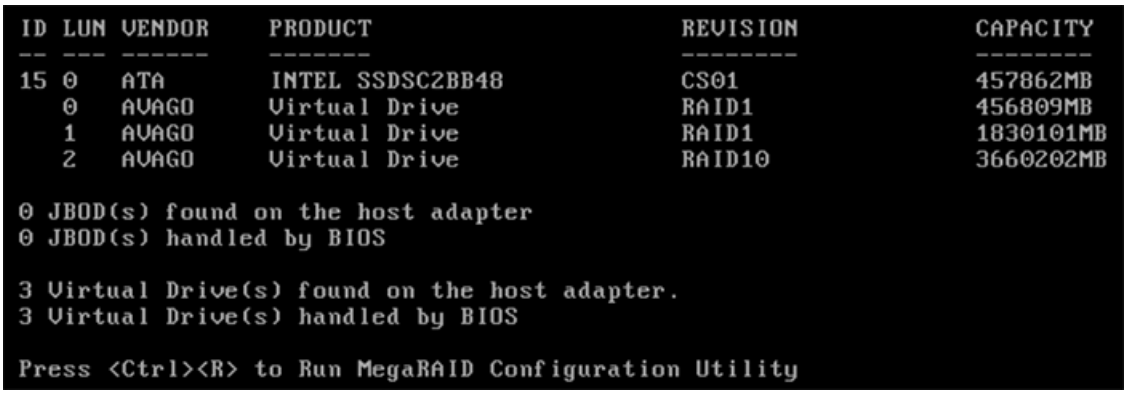
ステップ 3 アプライアンスの RAID コントローラによって管理されている 3 つの仮想ドライブを再初期化します。

a) Cisco IMC にログインし、KVM セッションを開始します。

b) 次のメニューオプションのいずれかを選択して、アプライアンスの電源をオンにするか、電源を再投入します。

- **[Power]** > **[Power On System]** の順に選択します。
- **[Power]** > **[Power Cycle System (cold boot)]** の順に選択します。

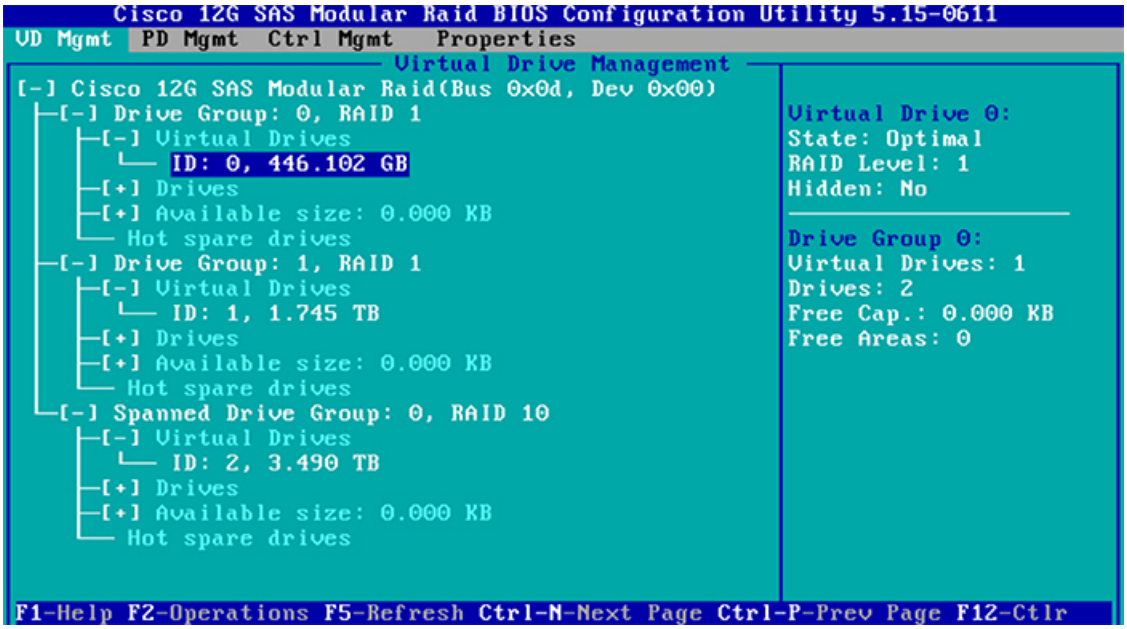
アプライアンスがリブートされると、アプライアンス上のすべてのドライブ（物理と仮想の両方）を一覧表示する画面が表示されます。



c) この画面が表示されたらすぐに、**Ctrl+R** を押して、MegaRAID 設定ユーティリティを実行します。

操作するまでの時間が長すぎると、この画面は消えてしまいます。この画面に戻るには、KVM メニューから **[Power]** > **[Reset System (warm boot)]** の順に選択して、アプライアンスをリブートします。

d) ドライブのエントリ（`ID : 0、446.102 GB` など）を選択してから、**F2** を押します。



この操作により、ドライブの **[詳細プロパティ（Advanced Properties）]** 画面が開きます。

e) 表示されるメニューで、最初の仮想ドライブに **[Initialization]** > **[Full Initialization]** を選択します。

f) アプライアンスの他の仮想ドライブごとに、ステップ 3b ～ 3e を繰り返しますが、[Fast Initialize] を選択します。（完全な初期化が必要なのは最初の仮想ドライブのみです。2番目と3番目の仮想ドライブには、完全な初期化は必要ありません）。

ステップ 4 アプライアンスに Cisco DNA Center を再インストールします。

Cisco DNA Center ISO イメージのインストール （20 ページ）を参照してください。

Cisco DNA Center イメージの確認

Cisco DNA Center を展開する前に、ダウンロードしたイメージが正規の Cisco イメージであることを確認するよう強くお勧めします。

始める前に

Cisco DNA Center イメージの場所を把握します（電子メールを使用するか、シスコサポートチームと連絡を取ります）。

ステップ 1 シスコが指定した場所から Cisco DNA Center イメージ（.iso、.bin、.zip）をダウンロードします。

ステップ 2 シスコの指定した場所から署名検証用のシスコ公開キー（cisco_image_verification_key.pub）をダウンロードします。

ステップ 3 シスコが指定した場所からイメージのセキュア ハッシュ アルゴリズム（SHA512）チェックサムファイルをダウンロードします。

ステップ 4 シスコサポートから電子メールで、またはセキュアなシスコの Web サイト（利用可能な場合）からダウンロードして、イメージのシグニチャファイル（.sig）を入手します。

ステップ 5 （オプション）SHA 検証を実行して、不完全なダウンロードによってイメージが破損していないかどうかを判定します。

オペレーティングシステムに応じて、次のコマンドのいずれかを実行します。

- Linux システムの場合：**sha512sum** *image-filename*
- Mac システムの場合：**shasum -a 512** *image-filename*

Microsoft Windows には組み込みのチェックサムユーティリティはありませんが、certutil ツールを使用できます。

```
certutil -hashfile <filename> sha256 | md5
```

次に例を示します。

```
certutil -hashfile D:\Customers\FINALIZE.BIN sha256
```

Windowsでは、Windows PowerShell を使用してダイジェストを生成することもできます。次に例を示します。

```
PS C:\Users\Administrator> Get-FileHash -Path D:\Customers\FINALIZE.BIN
Algorithm Hash Path
SHA256 B84B6FFD898A370A605476AC7EC94429B445312A5EEDB96166370E99F2838CB5 D:\Customers\FINALIZE.BIN
```

コマンドの出力とダウンロードした SHA512 チェックサムファイルを比較します。コマンド出力が一致しない場合は、イメージを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコサポートにお問い合わせください。

ステップ 6 署名を確認し、イメージが正規のものでシスコ製であることを確認します。

openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature *signature-filename image-filename*

（注） このコマンドは Mac と Linux の両方の環境で動作します。まだ OpenSSL をインストールしていない場合、Windows ではダウンロードしてインストールする必要があります（こちらから入手可能）。

イメージが正規であれば、このコマンドを実行すると、「`Verified OK`」というメッセージが表示されます。このメッセージが表示されない場合は、イメージをインストールせず、シスコサポートにお問い合わせください。

ステップ 7 Cisco イメージをダウンロードしたことを確認してから、Cisco DNA Center イメージを含むブート可能 USB ドライブを作成します。「ブート可能な USB フラッシュドライブの作成」を参照してください。

ブート可能な USB フラッシュドライブの作成

Cisco DNA Center ISO イメージをインストールできるブート可能 USB フラッシュドライブを作成するには、次のいずれかの手順を実行します。

始める前に

- Cisco DNA Center ISO イメージのコピーをダウンロードして確認します。「Cisco DNA Center イメージの確認」を参照してください。
- 使用している USB フラッシュドライブについて次の事項を確認します。
  - USB 3.0 以降である。
  - 64 GB 以上の容量がある。
  - 暗号化されていない。

（注） Rufus ユーティリティを使用して Cisco DNA Center ISO イメージを書き込まないでください。Etcher、Linux CLI、または Mac CLI のみを使用してください。

Etcher の使用

ステップ 1 ラップトップまたはデスクトップでのブート可能USB ドライブの作成を可能にする、オープンソースのフリーウェアユーティリティ Etcher（バージョン 1.3.1 以降）をダウンロードしてインストールします。

現在、Linux、macOS、Windows バージョンの Etcher を使用できます。https://www.balena.io/etcher/ からダウンロードできます。

（注） Windows 10 を実行しているマシンでは Etcher の Windows バージョンのみを使用してください。古いバージョンの Windows との互換性に関する既知の問題があるためです。

ステップ 2 Etcher をインストールしたマシンに USB ドライブを接続し、Etcher を起動します。

ステップ 3 ウィンドウの右上隅にある ⚙ をクリックし、Etcher が次のように設定されていることを確認します。

- 成功時に自動マウント解除する
- 成功時に書き込みを検証する

ステップ 4 **[Back]** をクリックして、メインウィンドウに戻ります。

ステップ 5 **[Select Image]** をクリックします。

ステップ 6 以前にダウンロードした Cisco DNA Center ISO イメージに移動し、そのイメージを選択して **[Open]** をクリックします。

接続した USB ドライブの名前がドライブアイコン（）の下に表示されます。表示されない場合には、次の操作を実行します。

1. **[Select drive]** をクリックします。
2. 正しい USB ドライブのオプションボタンをクリックしてから、**[Continue]** をクリックします。

ステップ 7 **[Flash!]** をクリックして、ISO イメージを USB ドライブにコピーします。

Etcher では、インストールされた Cisco DNA Center ISO イメージを使用して、ブート可能ドライブとして USB ドライブが設定されます。

Linux CLI の使用

ステップ 1 次のとおり、ご使用のマシンで USB フラッシュドライブが認識されていることを確認します。

a) フラッシュドライブをマシンの USB ポートに挿入します。

b) Linux シェルを開き、次のコマンドを実行します。 **lsblk**

次の例に示すように、このコマンドでは、マシンに現在設定されているディスクパーティションが一覧表示されます。

```
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
sda 8:0 0 446.1G 0 disk
├─sda1 8:1 0 1M 0 part
├─sda2 8:2 0 28.6G 0 part /
├─sda3 8:3 0 28.6G 0 part /install2
├─sda4 8:4 0 9.5G 0 part /var
├─sda5 8:5 0 30.5G 0 part [SWAP]
└─sda6 8:6 0 348.8G 0 part /data
sdb 8:16 0 1.8T 0 disk
├─sdb1 8:17 0 426.1G 0 part /data/maglev/srv/fusion
└─sdb2 8:18 0 1.3T 0 part /data/maglev/srv/maglev-system
sdc 8:32 0 3.5T 0 disk
└─sdc1 8:33 0 3.5T 0 part /data/maglev/srv/ndp
sdd 8:48 1 28.7G 0 disk
└─sdd1 8:49 1 12G 0 part
```

c) SDDパーティション（USB フラッシュドライブの存在を示す）が表示されていることを確認します。

ステップ 2 以前にダウンロードした Cisco DNA Center ISO イメージを USB フラッシュドライブに書き込みます。**time sudo dd if=/data/tmp/***ISO-image-filename* **of=/dev/***flash-drive-partition* **bs=4M && sync status=progress**

たとえば cdnac-sw-1.330という名前の ISO イメージを使用してブート可能な USB ドライブを作成するには、次のコマンドを実行します。**time sudo dd if=/data/tmp/CDNAC-SW-1.330.iso of=/dev/sdd bs=4M && sync status=progress**

Mac CLI の使用

ステップ 1 USB フラッシュドライブに関連付けられているディスクパーティションを確認します。

a) ターミナルウィンドウを開き、次のコマンドを実行します。 **diskutil list**

このコマンドでは、マシンに現在設定されているディスクパーティションが一覧表示されます。

b) フラッシュドライブをマシンの USB ポートに挿入し、 **diskutil list**コマンドをもう一度実行します。

このコマンドを最初に実行したときリストの表示されなかったパーティションは、フラッシュドライブです。たとえば `/dev/disk2` がフラッシュドライブのパーティションだと仮定します。

ステップ 2 このコマンドでフラッシュドライブのパーティションをマウント解除します。**diskutil unmountDisk** *flash-drive-partition*

この例ではこの先、次のように入力します **diskutil unmountDisk /dev/disk2**

ステップ 3 以前ユーザがダウンロードした Cisco DNA Center ISO イメージを使用してディスクイメージを作成します。**hdiutil convert -format UDRW -o** *Cisco-DNA-Center-version ISO-image-filename*

この例を続け、`CDNAC-SW-1.330.iso` という Cisco DNA Center ISO イメージを使用して作業しているとしましょう。次のコマンドを実行すると、`CDNAC-1.330.dmg` という名前の macOS ディスクイメージが作成されます。**hdiutil convert -format UDRW -o CDNAC-1.330 CDNAC-SW-1.330.iso**

重要 ISO イメージがボックスパーティションに存在しないことを確認します。

ステップ 4 ブート可能な USB ドライブを作成します。**sudo dd if=***macOS-disk-image-filename* **of=***flash-drive-partition* **bs=1m status=progress**

この例を続け、次のコマンドを実行します。 **sudo dd if=CDNAC-1.330.dmg of=/dev/disk2 bs=1m status=progress**

ISO イメージのサイズは約 18 GB であるため、完了までに時間がかかることがあります。

Cisco DNA Center ISO イメージのインストール

アプライアンスに Cisco DNA Center ISO イメージをインストールするには、次の手順を実行します。

始める前に

Cisco DNA Center ISO イメージのインストール元となるブート可能 USB ドライブを作成します。「ブート可能な USB フラッシュドライブの作成」を参照してください。

ステップ 1 Cisco DNA Center ISO イメージを含むブート可能 USB ドライブをアプライアンスに接続します。

ステップ 2 Cisco IMC にログインし、KVM セッションを開始します。

ステップ 3 アプライアンスの電源を投入または再投入します。

- アプライアンスが実行されていない場合には、**[Power]** > **[Power On System]** を選択します。
- アプライアンスがすでに実行されている場合には、**[Power]** > **[Power Cycle System（cold boot）]** を選択します。

ステップ 4 表示されたポップアップウィンドウで **[Yes]** をクリックして、サーバ制御アクションを実行しようとしていることを確認します。

ステップ 5 シスコのロゴが表示されたら、**F6** キーを押すか、[KVM] メニューから **[Macros]** > **[User Defined Macros]** > **[F6]** を選択します。

ブートデバイス選択メニューが表示されます。

ステップ 6 USB ドライブを選択してから、**Enter** を押します。

ステップ 7 [GNU GRUB] ブートローダーウィンドウで、[Cisco DNA Center Installer] を選択し、Enter を押します。

（注） 30 秒以内に選択しなかった場合、ブートローダーが自動的に Cisco DNA Center インストーラを起動します。

インストーラが再起動し、ウィザードのウェルカム画面が表示されます。プライマリクラスタノードを設定するのか、セカンダリクラスタノードを設定するのかに応じて、「プライマリマスタノードの設定」または「セカンダリノードの設定」のステップ 4 に進みます。

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。