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 （1 ページ）
- Cisco Integrated Management Controller に対するブラウザアクセスの有効化 （2 ページ）
- 事前設定タスクの実行 （7 ページ）
- NIC ボンディングの概要 （11 ページ）
- アプライアンスのイメージの再作成 （13 ページ）
- Catalyst Center アプライアンスの設定 （19 ページ）

アプライアンス設定の準備の概要

Catalyst 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 へのブラウザ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 （2 ページ）」を参照）。
2. Cisco IMC 事前設定タスクの実行 （7 ページ） 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。
3. 特定の状況において、事前インストール済みの Catalyst Center ソフトウェアを再インストールします。たとえば、現在のクラスターリンク設定を変更する前に再インストールします。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 （13 ページ） のタスクを完了してください。

（注） アプライアンスのイメージを作成しなおす必要がない場合は、使用する設定ウィザードに固有の「アプライアンスの設定の概要」のトピックに進みます。

- Maglev 設定ウィザード
- ブラウザベースの構成ウィザード（32 コアおよび 56 コアアプライアンス）
- ブラウザベースの構成ウィザード（80 コアアプライアンス）

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 CIMC ポートに IP アドレスとゲートウェイを割り当てます。Cisco IMC GUI にアクセスして、アプライアンスを設定できます。

Cisco IMC の設定が完了したら、Cisco IMC にログインし、「事前設定タスクの実行 （7 ページ）」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 デフォルトユーザー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 ユーザー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。
3. [**Modify User Details**] ダイアログボックスで、[**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。

手順

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。

- KVM ケーブルをアプライアンスの前面パネルの KVM コネクタに接続します。
- キーボードとモニターをアプライアンスの背面パネルにある USB および VGA ポートに接続します。

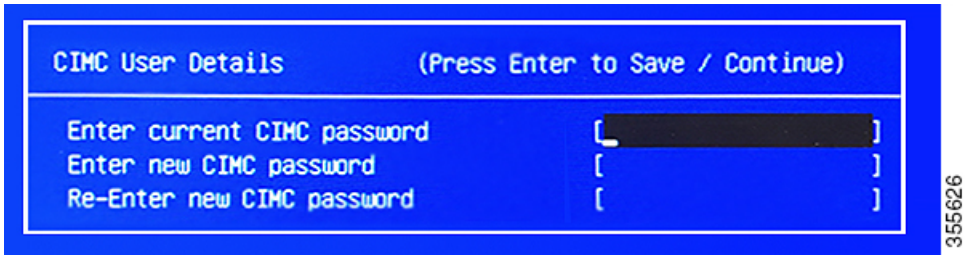
ステップ 2　アプライアンスの電源コードが接続され、電源がオンになっていることを確認します。

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ブート画面が開きます。

ステップ 4 [**F8**] を押して、Cisco IMC の設定を実行します。

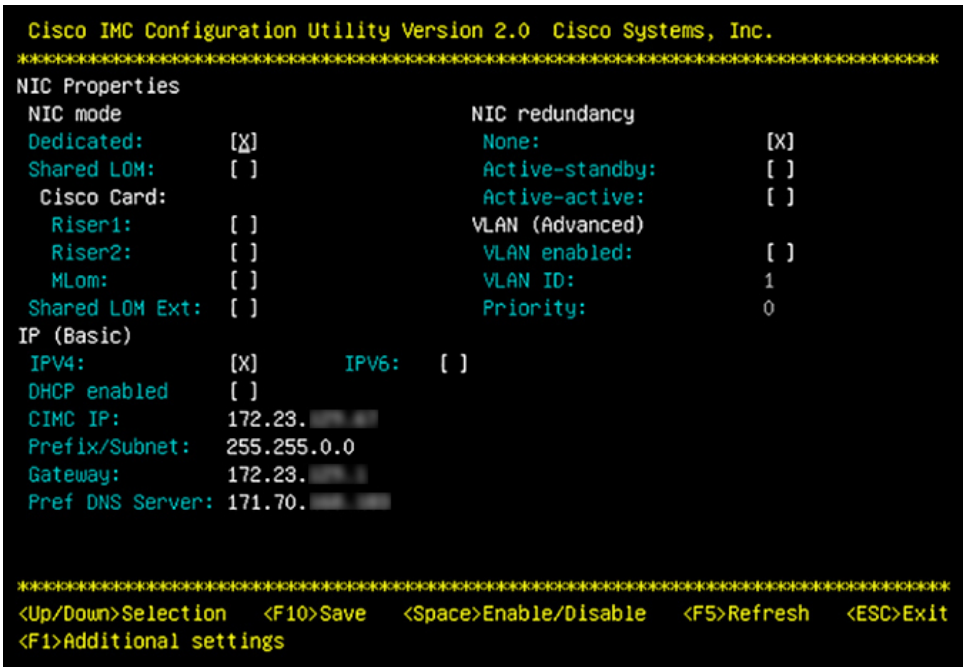
次に示すように、Cisco IMC 設定ユーティリティに [**CIMC User Details**] 画面が表示されます。



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。

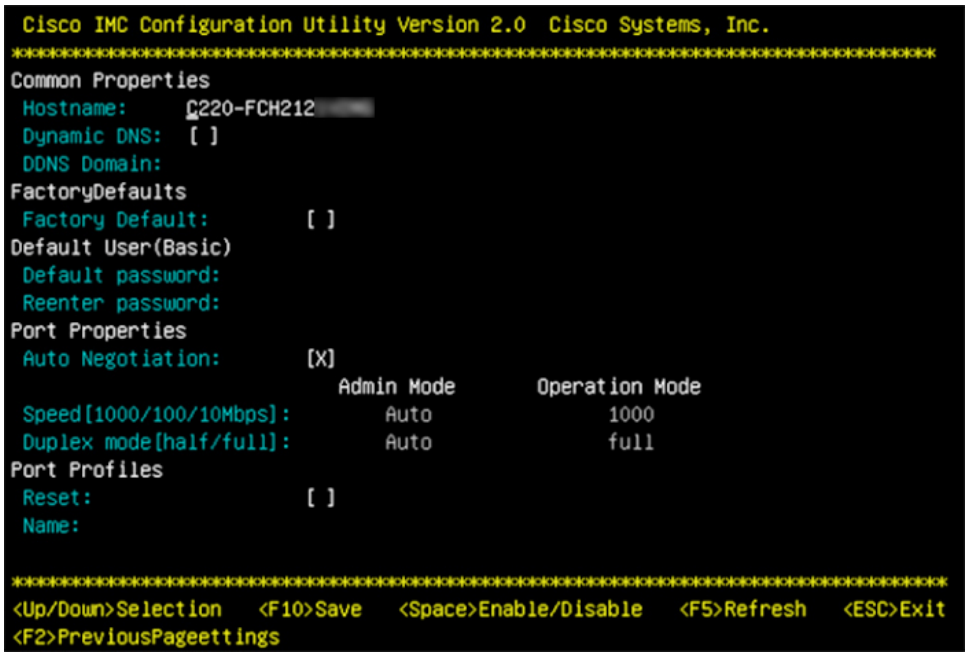


ステップ 7 次のアクションを実行します。

- **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。

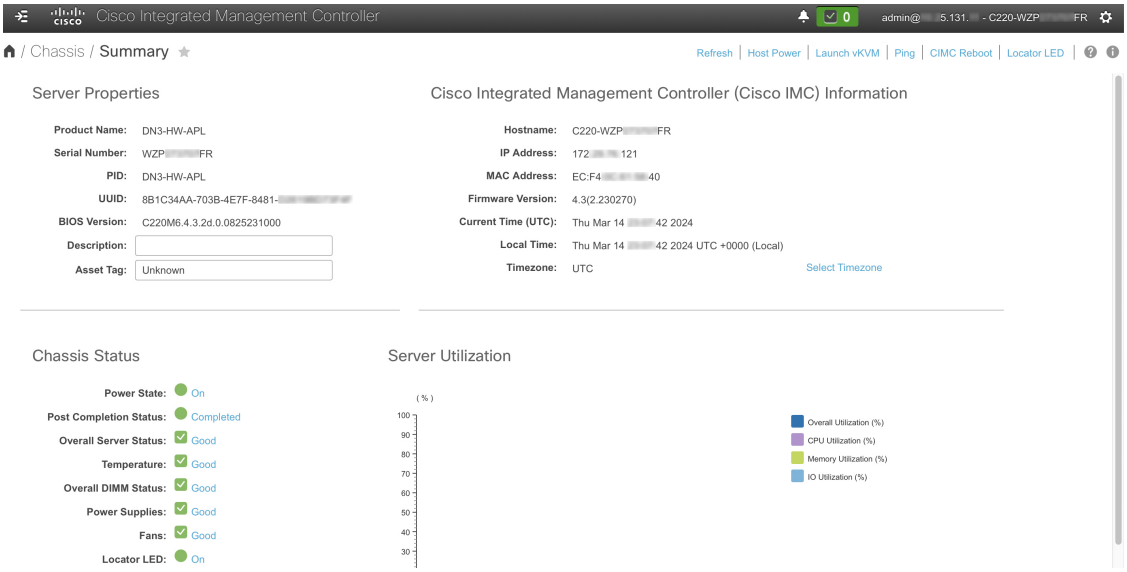
ステップ 12 設定が保存され、アプライアンスのリブートが完了したら、アプライアンスサブネットにアクセスできるクライアントマシンでブラウザを開き、次の URL を入力します。

`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。

ブラウザに次のような Cisco IMC GUI のメインログインウィンドウが表示されます。

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、[**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 Catalyst 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確認します。

b) インストールする Catalyst 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 Catalyst 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 1 つのタスクを実行します。

- 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。

事前設定タスクの実行

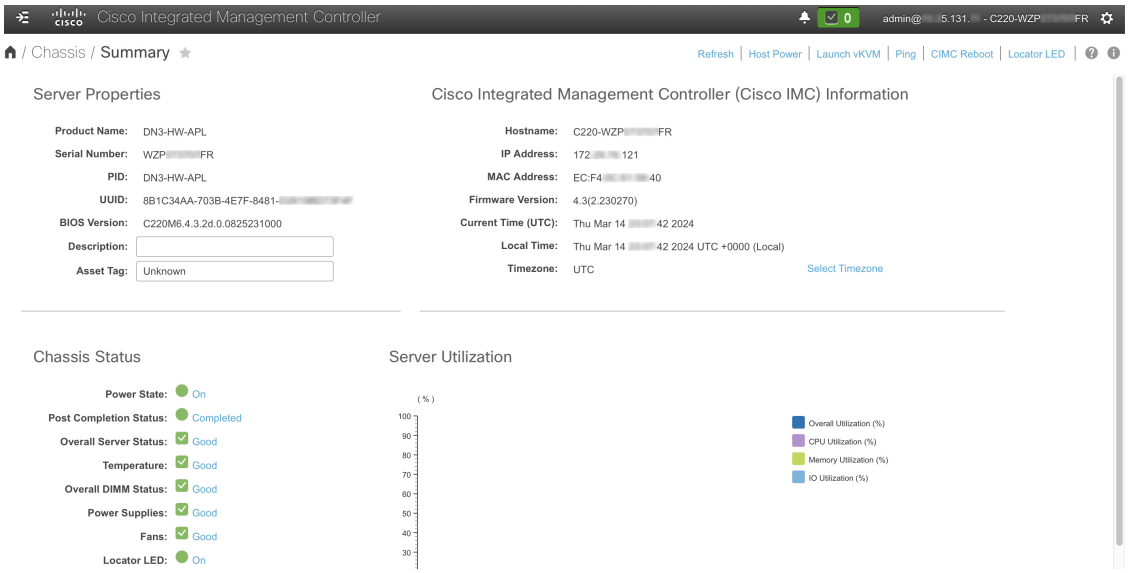
最初に、アプライアンスをインストールし、Cisco IMC GUI へのアクセスを設定します。アプライアンスのインストール ワークフローおよびCisco Integrated Management Controller に対するブラウザアクセスの有効化 （2 ページ）を参照してください。その後、Cisco IMC を使用して事前設定タスクを完了し、正しい設定と展開を確保します。

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）サーバーと同期します。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 サーバーを使用します。この同期は、Catalyst Center データをネットワーク全体で適切に同期しておくために重要です。
2. 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。

手順

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 （2 ページ）」で設定した Cisco IMC IP アドレス、ユーザー 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。

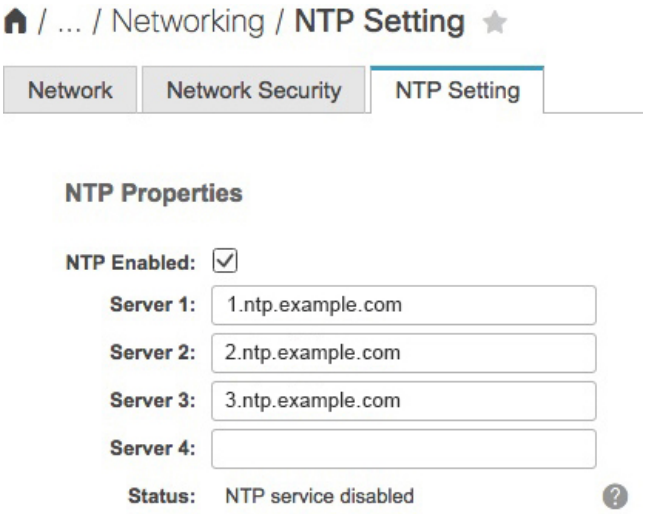


ステップ 2 次に示すように、アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol（NTP）サーバーと同期します。

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**] を選択します。[**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、4 つの番号付き [**Server**] フィールドに最大 4 つの NTP サーバー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 サーバーの時刻の同期を開始します。

（注）

- 第 3 世代 Catalyst Center アプライアンスでは、仮想インターフェイス カード（VIC）が使用されません。第 3 世代アプライアンスに標準搭載のネットワーク インターフェイス カード（NIC）では、高スループットがすでにデフォルトで有効になっているため、Cisco IMC で NIC を設定する必要はありません。

- Cisco IMC で NTP 認証を使用することはできません。

ステップ 3 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 スイッチでは、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 mode access
MySwitch(config-if)#switchport access vlan 99
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)#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
```

（注）

- これらのコマンドは単なる例です。
- 正常に機能させるには、第 3 世代 Catalyst Center アプライアンスのスイッチポートをアクセスモードに設定する必要があります。トランクモードはサポートされていません。

c) show interface tengigabitethernet *portID* コマンドを実行します。ポートが接続されて動作していること、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 という *portID* コマンドを実行して、X710-DA2 NIC 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。

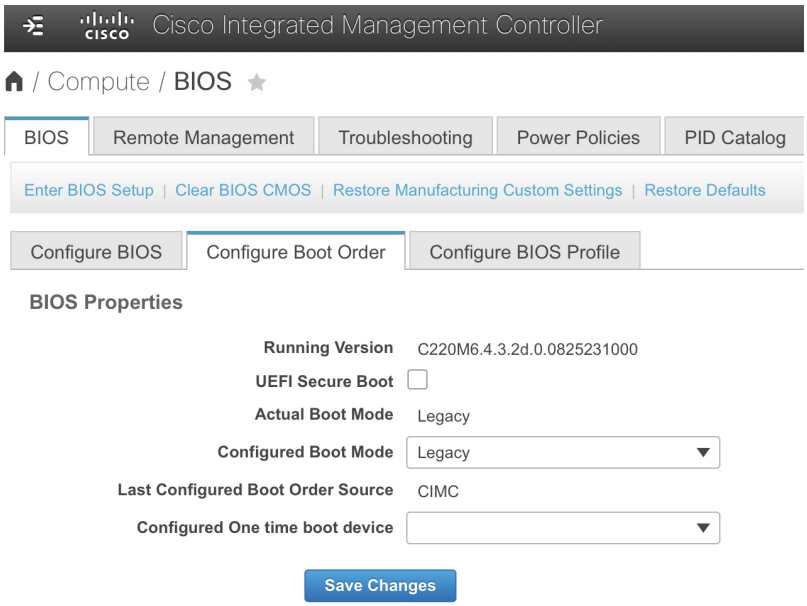
```
MySwitch#show run interface tengigabitethernet 1/1/3
Building configuration...
Current configuration : 129 bytes
! interface TenGigabitEthernet1/1/3
 switchport access vlan 99
 ip device tracking maximum 10
```

```
end

MySwitch#
```

e) show mac address-table interface tengigabitethernet という 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#
```

ステップ 4 [Configured Boot Mode] ドロップダウンリストで、[Legacy]（デフォルトモード）が設定されていることを確認します。



[**Configure Boot Order**] タブにアクセスするには、次の手順を実行します。

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、**[Compute]** > **[BIOS]** > **[Configure Boot Order]** を選択します。

注意

[**Legacy**] ブートモード設定を維持します。[**UEFI**] ブートモード設定が原因で、Catalyst Center アプライアンスインターフェイスが ping に応答しない場合があります。

次のタスク

このタスクを完了した後、次のいずれかのタスクを実行します。

- アプライアンスを設定する前に Catalyst 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（13ページ）」を参照してください。
- アプライアンスを設定する準備ができている場合は、使用する設定ウィザードに一致する「アプライアンス設定の概要」のトピックに進みます。
  - Maglev 設定ウィザード
  - ブラウザベースの構成ウィザード（32 コアおよび 56 コアアプライアンス）
  - ブラウザベースの構成ウィザード（80 コアアプライアンス）

NIC ボンディングの概要

任意の Catalyst Center アプライアンスで、エンタープライズ インターフェイス、クラスター内インターフェイス、管理インターフェイス、およびインターネット インターフェイスを設定できます。アプライアンスでネットワーク インターフェイス コントローラ（NIC）のボンディングを有効にすると、各インターフェイスには2つのインスタンスがあります。プライマリインスタンス（アプライアンスのマザーボードまたはIntel E810-XXVDA2 ネットワークアダプタのいずれかにある）が1台のスイッチに接続されています。セカンダリインスタンス（アプライアンスの Intel E810-XXVDA4 ネットワークアダプタにある）が別のスイッチに接続されています。NIC ボンディングを使用すると、各インターフェイスの 2 つのインスタンスが単一の論理インターフェイスに統合されます。単一の MAC アドレスを持つ単一のデバイスとして表示されます。この機能を有効にすると、アプライアンスのインターフェイスの設定時に選択したボンディングモードに応じて、利点を得られます。利点を次に示します。

（注） シングルノードクラスタと 3 ノード Catalyst Center クラスタの両方で NIC ボンディングがサポートされます。

- アクティブ/バックアップモード：この機能がアプライアンスで有効になっている場合、デフォルトでは、これがアプライアンスのインターフェイスに設定されているボンディングモードです。このモードでは、Catalyst Center によりグループ化された 2 つのインターフェイスの高可用性（HA）が可能になります。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。

（注） 1 Gbps と 10 Gbps の両方のスループットをサポートするインターフェイスでこのモードを有効にすると、Catalyst Center によりスループットが自動的に 1 Gbps に設定されます。

- LACP モード：このモードを選択すると、Catalyst Center によりグループ化された 2 つのインターフェイスで同じ速度とデュプレックス設定が共有されます。このモードでは、イン

ターフェイスにロードバランシングとより高い帯域幅が提供されます。このモードを有効にするには、最初に次の点を確認する必要があります。

- Linux ユーティリティ ethtool は、各インターフェイスの速度とデュプレックスモードを取得するために使用されるベースドライバをサポートしている必要があります。
- エンタープライズポートに接続されているスイッチは、ダイナミックインターフェイス集約をサポートしている必要があります。
- スイッチ上で LACP を有効にした後、次のことを確認します。
  - LACP モードは [**active**] に設定されています。この設定により、アプライアンスに接続されているスイッチポートをアクティブ ネゴシエーション ステートにします。これによりポートはLACPパケットを送信し、リモートポートとのネゴシエーションを開始します。
- LACP レートが [**fast**] に設定されています。この設定により、LACP サポート対象インターフェイスに LACP 制御パケットが送信されるレートが、デフォルトの 30 秒から 1 秒に変更されます。

（注）

- LACP モードは、アプライアンスのエンタープライズおよびクラスタ内インターフェイスでのみ有効にできます。管理およびインターネットアクセスインターフェイスは、アクティブ/バックアップモードのみをサポートします。
- アプライアンスの初期設定時に、アプライアンスのインタークラスターインターフェイスでのみ LACP モードを有効にできます。

実稼働環境で NIC ボンディングを使用する前に、以下の作業を実施してください。

- アプライアンスでこの機能がサポートされていることを確認します。「アプライアンスサポート （12 ページ）」を参照してください。
- アプライアンスの背面パネルにあるセカンダリポートの位置を確認します。「前面パネルと背面パネル」を参照してください。
- 推奨されるアプライアンス（スイッチのケーブル接続）を確認します。インターフェイスケーブル接続を参照してください。

アプライアンスサポート

すべての第 3 世代 Catalyst Center アプライアンスは NIC ボンディングをサポートします。

- 32 コアアプライアンス：シスコ部品番号 DN3-HW-APL

- 56 コアアプライアンス：シスコ部品番号 DN3-HW-APL-L
- 80 コアアプライアンス：シスコ部品番号 DN3-HW-APL-XL

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ーリンク設定の変更など、Catalyst Center アプライアンスを再イメージ化する必要がある場合があります。アプライアンスを再イメージ化するには、次の手順を実行します。

手順

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

「Catalyst Center ISO イメージの確認」を参照してください。

ステップ 2 Catalyst 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 USB ドライブの作成」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：Catalyst Center アプライアンスの仮想ドライブの再初期化 （17 ページ）によって管理されている仮想ドライブを再初期化します。

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

Catalyst Center ISO イメージのインストール （18 ページ）を参照してください。

Catalyst Center イメージの確認

Catalyst 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

Catalyst 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）。

手順

ステップ 1 シスコが指定した場所から Catalyst 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、Catalyst 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 USB 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

Catalyst 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

- Catalyst Center ISO イメージのコピーをダウンロードして確認します。「Catalyst Center ISO 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が次の要件を満たしていることを確認します。
  - USB 3.0 以降
  - 64 GB
  - 非暗号化

（注） Etcher、Linux CLI、または Mac CLI のみを使用して Catalyst Center ISO イメージを書き込みます。

Etcher の使用

手順

ステップ 1 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。無料のオープンソースユーティリティを使用して、ラップトップまたはデスクトップにブート可能な USB ドライブを作成できます。

Linux、macOS、または Windows 用の Etcher は、https://www.balena.io/etcher/ でダウンロードできます。

（注）
互換性の問題を回避するため、Windows 10 以降でのみ Etcher を使用してください。

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 Catalyst Center ISO イメージに移動します。それを選択し、[**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 Catalyst 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

手順

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` パーティションが表示されていることを確認します。このパーティションは、USB フラッシュ ドライブの存在を示します。

ステップ 2 以前にダウンロードした Catalyst 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 status=progress && sync**

たとえば、`CC-SW-1.330.iso` 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/CC-SW-1.330.iso of=/dev/sdd bs=4M status=progress && sync**

Mac CLI の使用

手順

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 以前ユーザーがダウンロードした Catalyst 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** *Catalyst-Center-version ISO-image-filename*

この例を続け、`CC-SW-1.330.iso` という Catalyst 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、`CC-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 CC-1.330 CC-SW-1.330.iso**

重要
ISO イメージを Box パーティションに配置しないでください。

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=CC-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。

Catalyst Center アプライアンスの仮想ドライブの再初期化

Catalyst Center アプライアンスの仮想ドライブを再初期化するには、次の手順を実行します。

手順

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 （2 ページ）」で設定した Cisco IMC IP アドレス、ユーザー 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。

ステップ 2 Cisco IMC GUI の左上隅から、**[Toggle Navigation]** アイコン（）をクリックします。

ステップ 3 Cisco IMC メニューから、**[Storage]** > **[Cisco 12G Modular Raid Controller]** を選択します。

ステップ 4 [Virtual Drive Info] タブをクリックします。

ステップ 5 リストされている最初の仮想ドライブ（ドライブ番号 237）のチェックボックスをオンにします。[初期化（Initialize）] をクリックします。

ステップ 6 [**Initialize Type**] ドロップダウンリストから [**Full Initialize**] を選択します。

ステップ 7 [Initialize VD] をクリックします。

ステップ 8 アプライアンスの残りの仮想ドライブにそれぞれステップ 5 ～ 7 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。

ステップ 9 ドライブで実行しているタスクのステータスを表示するには、[**Operations**] エリアで [**Refresh**] をクリックします。

次の詳細が表示されます。

フィールド	説明
動作	ドライブで実行中の操作の名前。
[Progress in %]	操作の進行状況（完了した割合）。
[Elapsed Time in secs]	操作開始から経過した時間（秒数）。

Catalyst Center ISO イメージのインストール

アプライアンスに Catalyst 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

Catalyst 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 USB ドライブの作成」を参照してください。

手順

ステップ 1 Catalyst 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 表示されたウィンドウで [**Yes**] をクリックして、サーバー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。

重要
ドライブを取り外し可能ディスクとしてマウントします。

ステップ 7 [**GNU GRUB**] ブートローダーウィンドウで、**Catalyst Center インストーラー** 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 Catalyst 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ーノードとセカンダリクラスターノードのどちらを設定するかに応じて、適切な手順を使用してステップ 4 に進みます。

- Maglev ウィザードを使用したプライマリノードの設定
- Maglev ウィザードを使用したセカンダリノードの設定

Catalyst Center アプライアンスの設定

Catalyst Center ISO イメージのインストールが完了すると、インストーラがリブートし、Maglev 設定ウィザードの初期画面が開きます。アプライアンスの再イメージ化を完了するには、Maglev ウィザードを使用したアプライアンスの設定の手順を実行します。

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。