アプライアンスの設定

アプライアンスの設定ワークフロー

次の 2 つのモードのいずれかを使用して、アプライアンスをネットワークに展開できます。

- スタンドアロン：すべての機能を提供する単一のノードとして。このオプションは通常、初期展開、テスト展開、小規模なネットワーク環境での使用に適しています。
- クラスタ：最大 3 つのノードのクラスタの 1 つとして。このモードでは、すべてのサービスとデータがホスト間で共有されます。これは、大規模な展開で推奨されるオプションです。

初期導入でスタンドアロンモードを選択した場合は、後でクラスタを形成するためにアプライアンスを追加できます。スタンドアロンホストの設定時には、クラスタ内の最初のノードまたはプライマリノードとして設定されていることを確認してください。

初期導入でクラスタモードを選択した場合は、アドオンノードの設定に進む前に、プライマリノードの設定を完了してください。

次の表に、設定タスクとその実行順序を詳しく説明します。この表のタスクが正常に完了したら、初回設定ワークフローで説明されているように、初回設定を完了して続行します。

表 *1:* アプライアンスの設定タスク

ステップ	説明
1	アプライアンスの Cisco Integrated Management Controller（CIMC）グラフィック ユーザ インターフェイスへのブラウザアクセスを有効にします：CIMC へのブラウザアクセスの有効化
2	ハードウェアとスイッチの設定を確認して調整することで、設定に問題がないことを確認します：プリフライトチェックの実行
3	CIMC から Maglev 設定ウィザードを起動し、クラスタ内のプライマリ ノードを設定します：プライマリ ノードの設定
4	3 つのアプライアンスを設置し、クラスタに 2 番目と 3 番目のノードを追加する場合：アドオン ノードの設定

CIMC への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 Cisco Integrated Management Controller（CIMC）ポートに IP アドレスとゲートウェイを割り当てます。この操作により、アプライアンスの設定に使用する CIMC グラフィック ユーザ インターフェイスへのブラウザアクセスが可能になります。

この CIMC 設定が完了したら、CIMC にログインして、正しい設定の確認に役立ついくつかのタスクを実行します（「プリフライトチェックの実行」を参照）。

ヒント　お客様の環境のセキュリティを確保するため、アプライアンスを初めて起動するときに、CIMC 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。CIMC ユーザパスワードを後で変更する場合には、次に示すように、CIMC GUI を使用する方法が最も簡単です。

1. ☰ > **[管理者（Admin）]** > **[ユーザ管理（User Management）]** > **[ローカルユーザ（Local user）][管理（Management）]** を選択します。
2. ID [1] を選択してから、[ユーザの変更（Modify User）] をクリックします。

   新しいパスワードを [パスワードの変更（Change Password）] フィールドに入力してから、[保存（Save）] をクリックします。

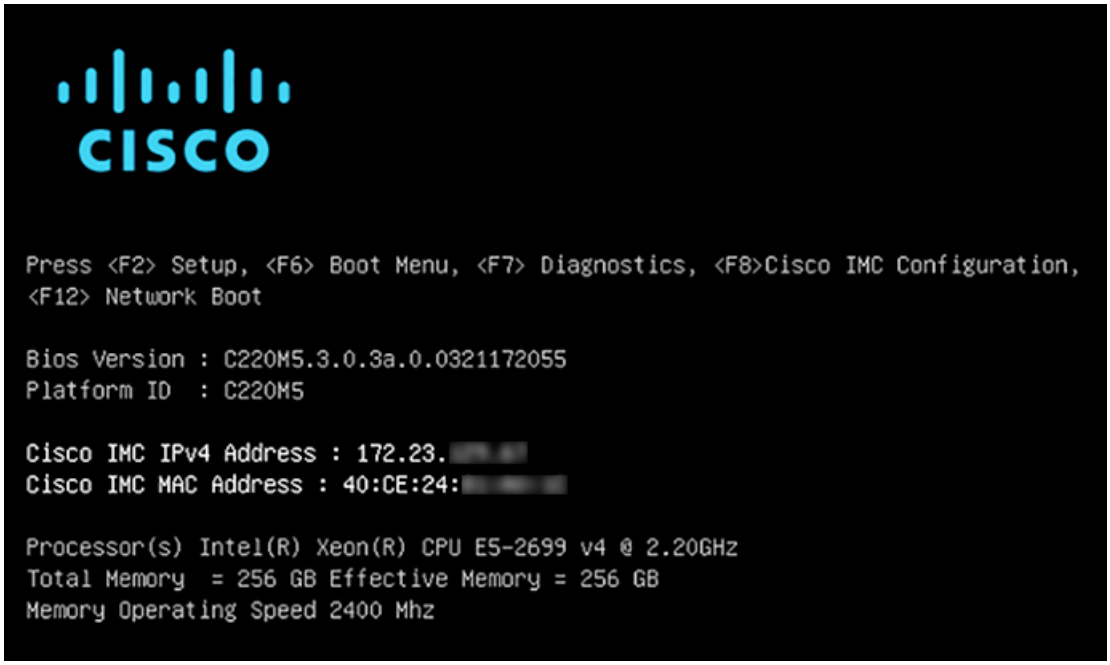
ステップ 1　次のいずれかを接続して、アプライアンスコンソールにアクセスします。

- 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 11）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 2 および 5）に接続するキーボードとモニタ。

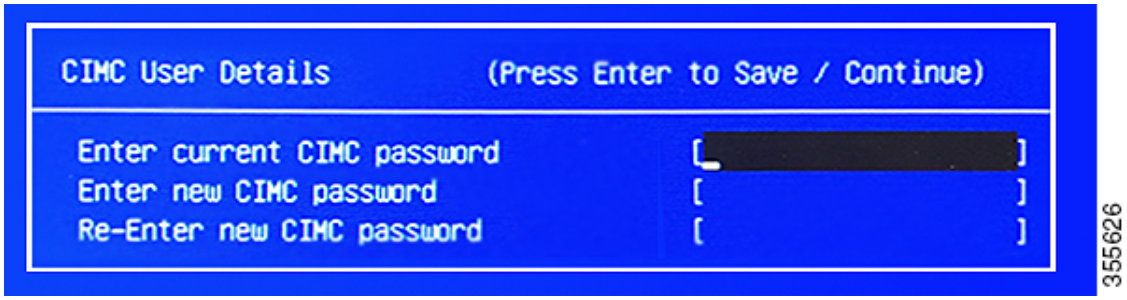
ステップ 2 アプライアンスの電源コードが接続され、電源がオンになっていることを確認します。

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。次に示すように、Cisco IMC 設定ユーティリティのブート画面が表示されるのを確認します。



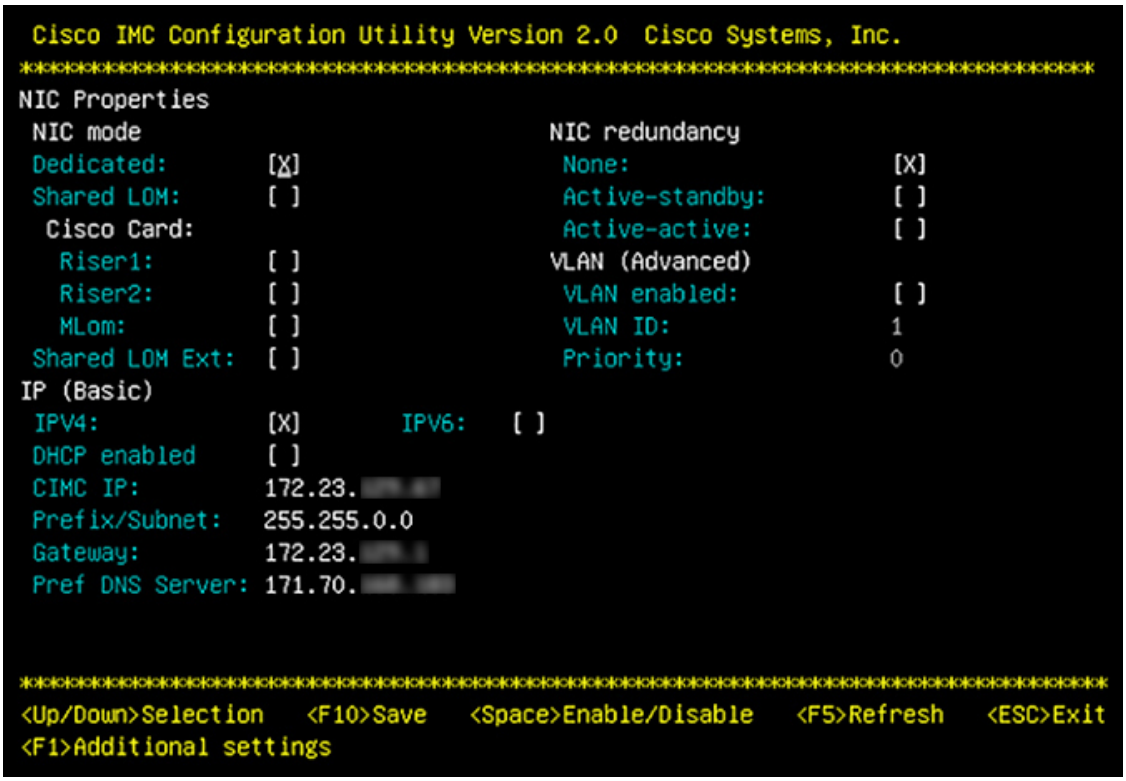
アップ

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ユーザの詳細（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 **[現在の CIMC パスワードを入力（Enter current CIMC Password）]**フィールドに入力します。次に、[新しいCIMCパスワードを入力（Enter New CIMC Password）] フィールドと [新しいCIMCパスワードを再入力（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。

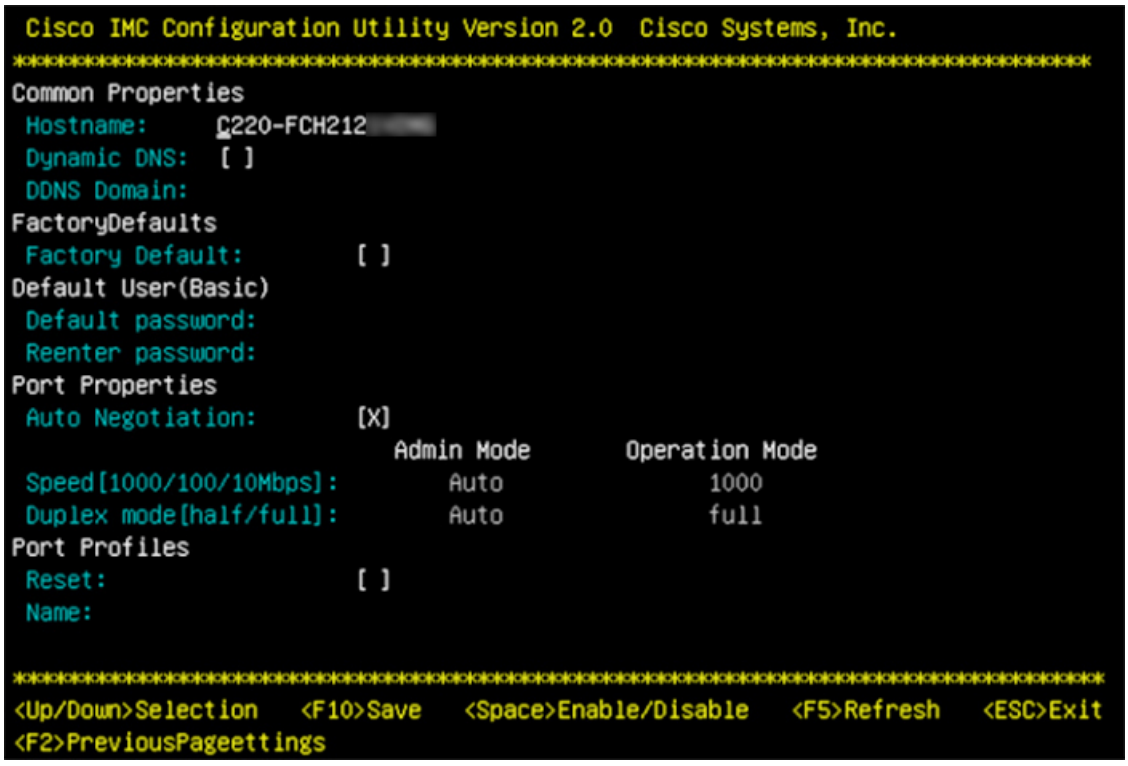
ステップ 6 [新しいCIMCパスワードを再入力（Re-Enter New CIMC Password）] フィールドで **Enter** を押すと、次に示すように、Cisco IMC 設定ユーティリティに [NICプロパティ（NIC Properties）] 画面が表示されます。



ステップ 7 次の変更を加えます。

- [NICモード（NIC mode）]：[専用（Dedicated）] を選択します。
- [IP（基本）（IP (Basic)）]：[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 **[追加設定（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 [共通プロパティ（Common Properties）] 画面が表示されます。



ステップ 9 次の変更を加えます。

- **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。

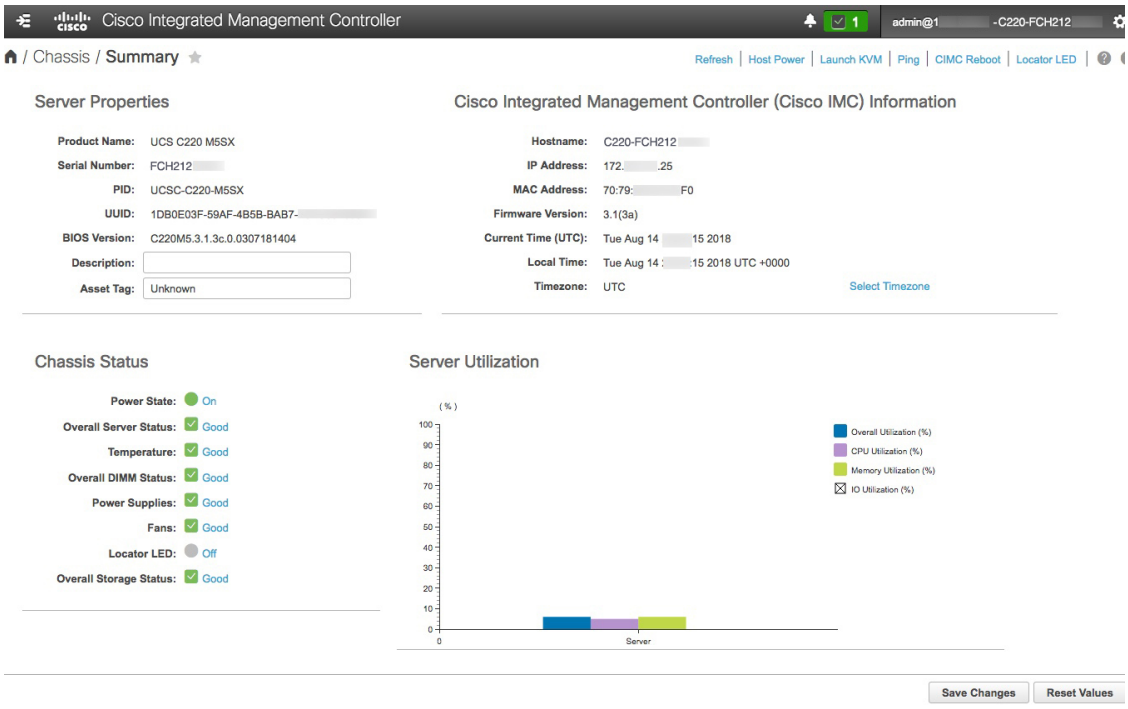
ステップ 11 **Esc** を押して**終了**し、アプライアンスをリブートします。

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*。***CIMC_ip_address*** は、ステップ 5 で入力した CIMC ポート IP アドレスです。

ブラウザに、次に示すような Cisco Integrated Management Controller 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 CIMC 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、次に示すような [Cisco Integrated Management Controllerシャーシの概要（Cisco Integrated Management Controller Chassis Summary）] ウィンドウがブラウザに表示されます。



次のタスク

問題の発生しない設定に役立つタスクを実行します（「プリフライトチェックの実行」）。

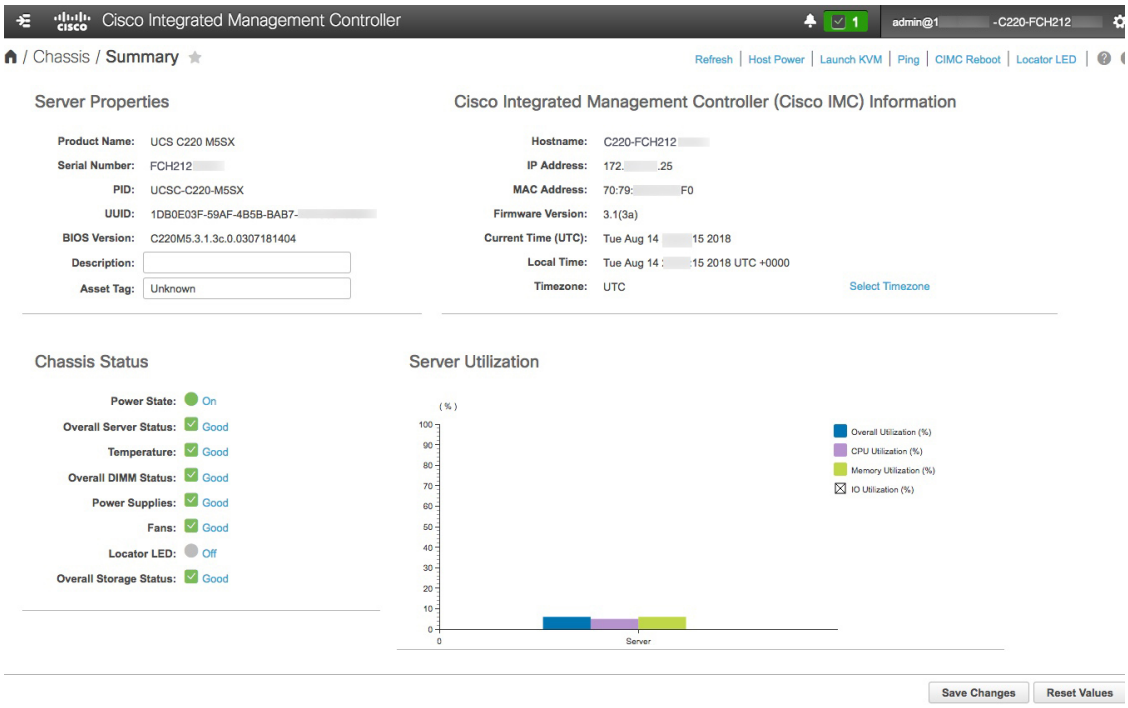
プリフライトチェックの実行

「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、「CIMC へのブラウザアクセスの有効化」の説明に従って CIMC GUI へのアクセスを設定した後、CIMC 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. 10Gbps 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。

ステップ 1 「CIMC へのブラウザアクセスの有効化」で設定した CIMC IP アドレス、ユーザ ID およびパスワードを使用して、アプライアンスの CIMC 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 シャーシの概要（Cisco Integrated Management Controller Chassis Summary）] ウィンドウがブラウザに表示されます。

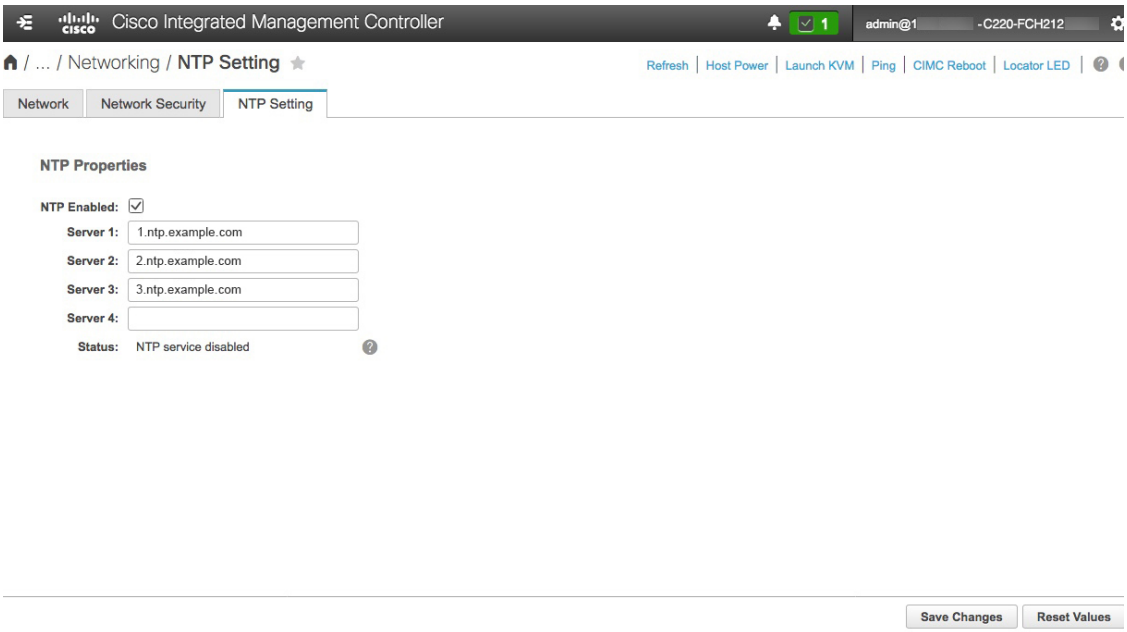


ステップ 2 次に示すように、アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol（NTP）サーバと同期します。

a) [シャーシの概要（Device Summary）] ウィンドウが表示されたら、アイコンをクリックして [CIMC] メニューを表示します。

b) [CIMC] メニューで、**[管理者（Admin）]** > **[ネットワーキング（Networking）]** > **[NTP 設定（NTP Setting）]** を選択します。CIMC に **[NTP 設定（NTP Setting）]** タブが表示されます。

c) [NTP 有効化（NTP Enabled）] 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（Server）] 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) 完了したら、[変更の保存（Save Changes）] をクリックします。CIMC 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。

ステップ 3 次に、以下の手順に従って、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) 次の一連のコマンドを入力して、スイッチポートを設定します。

```
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
```

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 NIC を設定する際に入力したものと同じ VLAN ID と MTU の値を使用します。スイッチの例では、リンク速度、デュプレックス、およびMTUのコマンド値がデフォルトになっているので、デフォルト値を変更した場合にのみ入力する必要が生じます。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、および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` という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 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

最初にインストールしたアプライアンスをクラスタのプライマリノードとして設定して、続行します。「プライマリノードの設定」を参照してください。

ネットワーク インターフェイス カードの無効化

アプライアンスが PCIe ライザ 2/スロット 2 の Intel X710-DA4 ネットワーク インターフェイス カード（NIC）を有効にした状態で出荷されている場合は、無効にする必要があります。カードを無効にしない場合、アプライアンスには 4 つの追加インターフェイス（enp216s0f3、enp216s0f2、enp216s0f1、enp216s0f0）が含まれているため、設定に悪影響を及ぼす可能性があります。

カードを無効にするには、以下の手順を実行します。

ステップ 1 Cisco IMC にログインし、**[コンピューティング（Compute）]** > **[BIOS]** > **[BIOSの設定（Configure BIOS）]** > **[I/O]** を選択します。

ステップ 2 次のフィールドで、[有効（Enabled）] を [無効（Disabled）] に変更します。

- **PCIeスロット2オプションROM（PCIe Slot 2 Option ROM）**
- **PCIe Slot 2 Link Speed**

ステップ 3 Cisco IMC の変更を保存します。

ステップ 4 Cisco DNA Center アプライアンスを再起動します。

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 ISO イメージの確認」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 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」を参照してください。

Cisco DNA Center ISO 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 ISO イメージが正規の Cisco イメージかどうか確認することを強く推奨します。

始める前に

Cisco DNA Center ISO 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るかのいずれかの方法で）。

ステップ 1 シスコによって指定された場所から Cisco DNA Center ISO イメージ（.iso）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 ISO 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、ISO 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 （任意）SHA 検証を実行して、不完全なダウンロードによって ISO 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** *ISO-image-filename*
- Mac システムの場合：**shasum -a 512** *ISO-image-filename*

Microsoft Windows にはチェックサムユーティリティが組み込まれていませんが、http://www.microsoft.com/en-us/download/details.aspx?id=11533 で Microsoft のユーティリティをインストールできます。上述のコマンド（または Microsoft Windows ユーティリティ）の出力を、ステップ 3 でダウンロードした SHA512 チェックサムファイルと比較します。コマンド出力が一致しない場合は、ISO 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、ISO イメージが正規の製品であり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 ISO-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。Windows の場合、まだ OpenSSL をインストールしていないなら、ダウンロードしてインストールする必要があります（ここで入手可能）。

ISO イメージが純正であれば、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、ISO イメージをインストールせず、シスコ サポートに連絡してください。

ステップ 7 Cisco ISO 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 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 ドライブの作成」を参照してください。

ブート可能な USB 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 ドライブを作成するには、次の手順を実行します。

始める前に

- Cisco DNA Center ISO イメージのコピーをダウンロードして確認します。「Cisco DNA 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の容量が少なくとも 32 GB であることを確認します。

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歯車アイコンをクリックし、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 [戻る（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 **[イメージの選択（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 **[開く（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. **[ドライブの選択（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、[続行（Continue）]をクリックします。

ステップ 7 **[フラッシュ（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。

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 USB ドライブの作成」を参照してください。
- アプライアンスに別のバージョンの Cisco DNA Center がすでにインストールされている場合には、「アプライアンスのイメージの再作成」で説明されている手順を実行します。

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 CIMC 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、**[電源（Power）]** > **[システムの電源オン（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、**[電源（Power）]**>**[システムの電源の再投入（コールドブート）（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 **[はい（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 **[マクロ（Macros）]** > **[ユーザ定義マクロ（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] ブートローダウィンドウで、[Cisco DNA アプライアンスの作成（Manufacture Cisco DNA appliance）] を選択してから、**Enter** を押します。

（注） 30 秒以内に選択しなかった場合、ブートローダが自動的に Maglev インストーラを起動します。その前に選択を実行する必要があります。

Cisco DNA 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 設定ウィザードが開きます。

プライマリノードの設定

最初にインストールされたアプライアンスをプライマリノードとして設定するには、次の手順を実行します。最初のアプライアンスは、スタンドアロンとして運用するか、またはクラスタの一部として運用するかにかかわらず、常にプライマリノードとして設定する必要があります。

すでにプライマリノードがある既存のクラスタのアドオンノードとして設置されたアプライアンスを設定する場合には、代わりに「アドオンノードの設定」の手順を実行します。

（注） この手順の実行中に入力するすべての IP アドレスが有効な IPv4 ネットマスクを持つ有効な IPv4 アドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

始める前に

次のことを確認します。

- 「必要な IP アドレスおよびサブネット」と「必要な設定情報」で必要とされているすべての情報が収集されたこと。
- 「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、最初のアプライアンスがインストールされたこと。
- 「CIMC へのブラウザアクセスの有効化」の説明に従って、プライマリノードで CIMC ブラウザアクセスが設定されたこと。
- 「プリフライトチェックの実行」の説明に従って、プライマリ ノード アプライアンスのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- CIMC および Cisco DNA Center と互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応するリリースノートを参照してください。
- 次の手順のステップ 7 で指定する DNS サーバと Cisco DNA Center の間のファイアウォールで ICMP が許容されること。Maglev 構成ウィザードでは ping を使用して、ユーザの指定した DNS サーバを確認します。Cisco DNA Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

ステップ 1 CIMC GUI の設定時に設定した CIMC IP アドレスにブラウザでアクセスし、CIMC ユーザとして CIMC GUI にログインします（「CIMC へのブラウザアクセスの有効化」を参照）。

ログインが成功すると、次に示すように、アプライアンスに **[Cisco Integrated Management Controller Chassisの概要（Cisco Integrated Management Controller Chassis Summary）]** ウィンドウが右上の青いリンクメニューとともに表示されます。

ステップ 2 青いリンクメニューで **[KVM の起動（Launch KVM）]** を選択してから **[Java ベースの KVM（Java based KVM）]** と **[HTML ベースの KVM（HTML based KVM）]** のいずれかを選択します。Java ベースの KVM を選択した場合、KVM コンソールを独自のウィンドウで表示するために、ブラウザまたはファイルマネージャから Java スタートアップファイルを起動する必要があります。HMTL ベースの KVM を選択すると、KVM コンソールが別個のブラウザウィンドウまたはタブで自動的に起動します。

選択したKVMのタイプに関係なく、KVMコンソールを使用して、設定の進行状況をモニタし、Maglev構成ウィザードのプロンプトに応答します。

ステップ3 KVMが表示されたら、次のいずれかを選択してアプライアンスをリブートします。

a) メインのCIMC GUIブラウザウィンドウで、**[ホストの電源（Host Power）]**>**[電源の再投入（Power Cycle）]**を選択します。その後、KVMコンソールに切り替えて続行します。

b) KVMコンソールで、**[電源（Power）]**>**[システムの電源の再投入（コールドブート）（Power Cycle System（cold boot））]**を選択します。

アプライアンスをリブートするかどうかの確認を求められたら、**[OK]**をクリックします。

リブートメッセージが表示された後、次に示すように、KVMコンソールにMaglev構成ウィザードのウェルカム画面が表示されます。

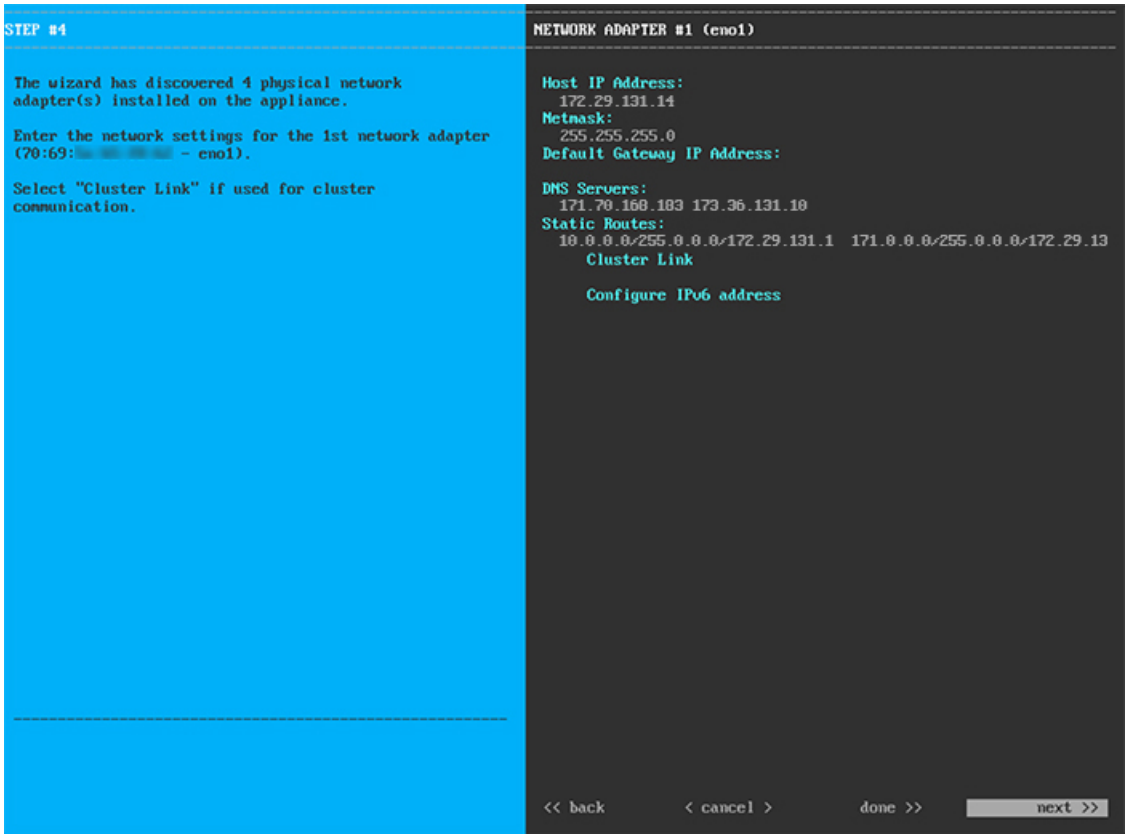
ステップ4 最初のクラスタオプションを選択して、プライマリノードの設定を開始します。

ウィザードでは、アプライアンス上のすべてのポートが検出され、次の順序で1つずつ別の画面に表示されます。

1. 1Gbps/10Gbps管理ポート（1、eno1、ネットワークアダプタ#1）
2. 1Gbps/10Gbpsクラウドポート（2、eno2、ネットワークアダプタ#2）
3. 10Gbpsエンタープライズポート（enp94s0f0、ネットワークアダプタ#3）
4. 10Gbpsクラスタポート（enp94s0f1、ネットワークアダプタ#4）

（注） 設定の過程でウィザードがエンタープライズポートとクラスタポートのいずれかまたは両方を表示できない場合は、これらのポートが機能していないか、または無効になっている可能性があります。これらの 10 Gbps ポートは Cisco DNA Center 機能に必要です。10 Gbps ポートが機能していないことが判明した場合には、[キャンセル（Cancel）]を選択して、設定をすぐに終了します。設定を再開したり、Cisco Technical Assistance Center（TAC）に連絡したりする前に「プリフライトチェックの実行」に記載されているすべての手順が完了していることを確認してください。

ステップ 5 このウィザードでは 1Gbps/10Gbps 管理ポート（1、eno1）がまず検出され、**[ネットワークアダプタ#1（NETWORK ADAPTER #1）]** として表示されます。「インターフェイスケーブル接続」で説明したように、このポートは管理ネットワークから Cisco DNA Center GUI にアクセスするために使用されます。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



次の表に示すように、**[ネットワークアダプタ#1（NETWORK ADAPTER #1）]**の設定値を入力します。

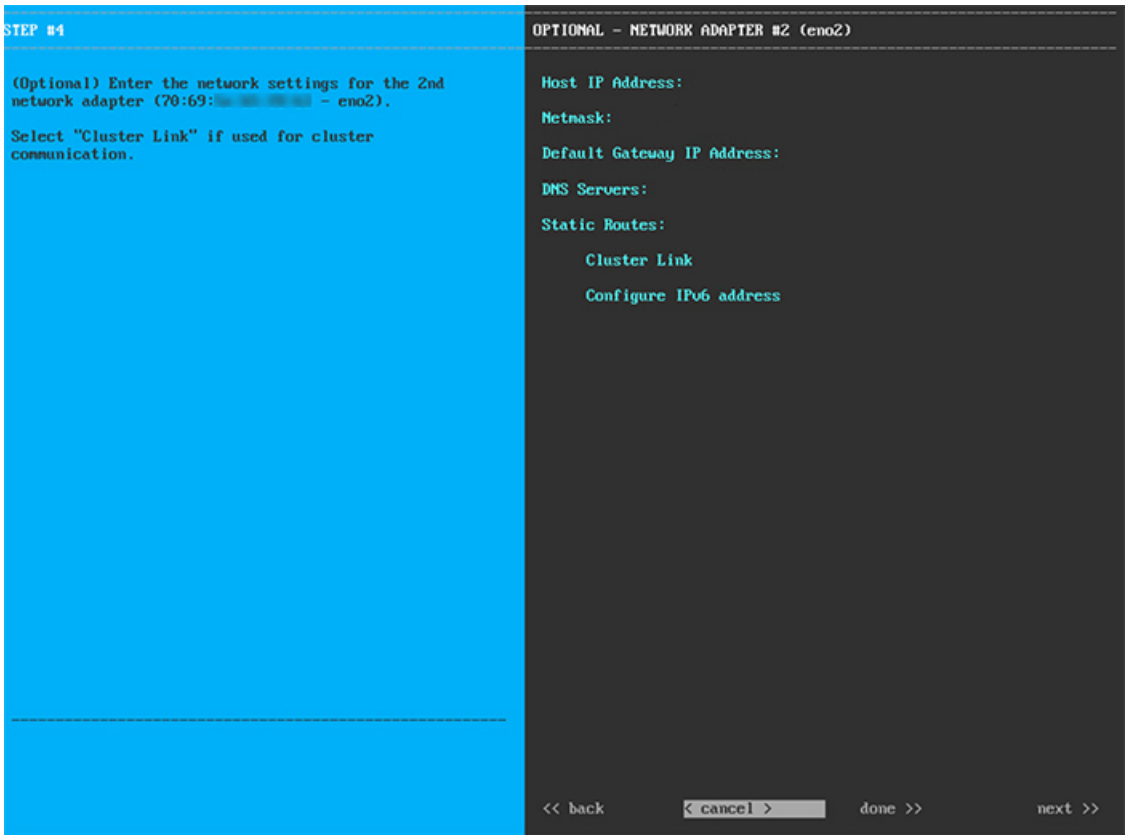
表 *2*：ネットワークアダプタ *#1* のプライマリノードエントリ：*1Gbps/10Gbps* 管理ポート（*eno1*）

ホスト IP アドレス（Host IP address）	管理ポートの IP アドレスを入力します。これは、このポートを使用して管理ネットワークから Cisco DNA Center GUI にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。

ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは通常、エンタープライズポートでのみ必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** • NTP の場合、Cisco DNA Center と NTP サーバの間のポート 123（UDP）が開いていることを確認します。 • クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

設定値の入力が完了したら、[次へ>>（next>>）] を選択して続行します。[次へ>>（next>>）] を選択すると、入力した値がウィザードによって検証され、正しくない場合にはエラーメッセージが表示されます。エラーメッセージが表示された場合には、入力した値が正しいことを確認してから、再入力します。必要に応じて、[戻る<<（<<back）] を選択して再入力します。

ステップ 6 入力した管理ポート値の検証が成功すると、ウィザードに 1Gbps /10Gbps クラウドポート（2、eno2）が **[ネットワークアダプタ #2（NETWORK ADAPTER #2）]** として表示されます。「インターフェイスケーブル接続」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、10Gbps エンタープライズポート（enp94s0f0）経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



次の表に示すように、[ネットワークアダプタ#2（NETWORK ADAPTER #2）] の設定値を入力します。

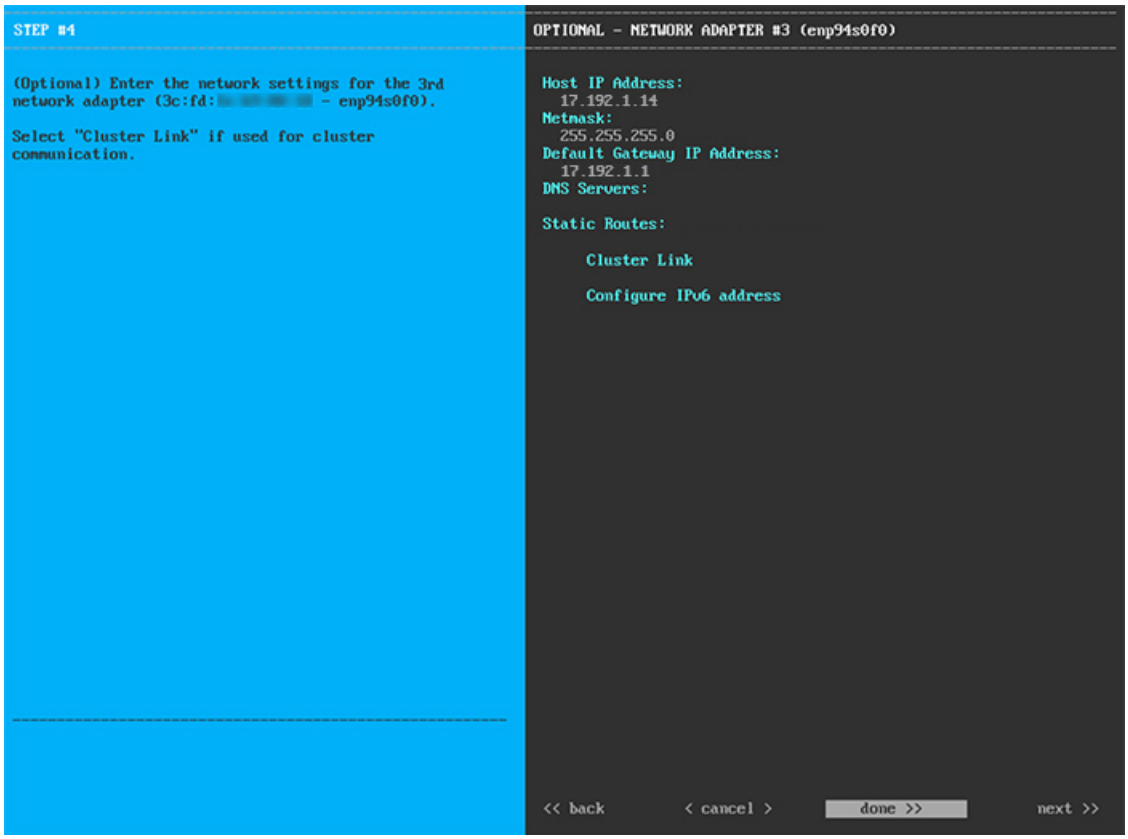
表 *3*：ネットワークアダプタ *#2* のプライマリノードエントリ：*1Gbps/10Gbps* クラウドポート（*eno2*）

ホスト IP アドレス（Host IP address）	クラウドポートの IP アドレスを入力します。この操作はインターネット接続にクラウドポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにしておくことができます。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	クラウドポートに使用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。これは通常、エンタープライズポートでのみ必要になります。

DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。通常、これは管理ポートでのみ必要です。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 7 入力したクラウドポート値の検証が成功すると、ウィザードに 10Gbps エンタープライズポート（enp94s0f0）が **[ネットワークアダプタ#3（NETWORK ADAPTER #3）]** として表示されます。「インターフェイスケーブル接続」で説明したように、このポートは、アプライアンスをエンタープライズネットワークにリンクするために必要なポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



次の表に示すように、[ネットワークアダプタ#3（NETWORK ADAPTER #3）] の設定値を入力します。

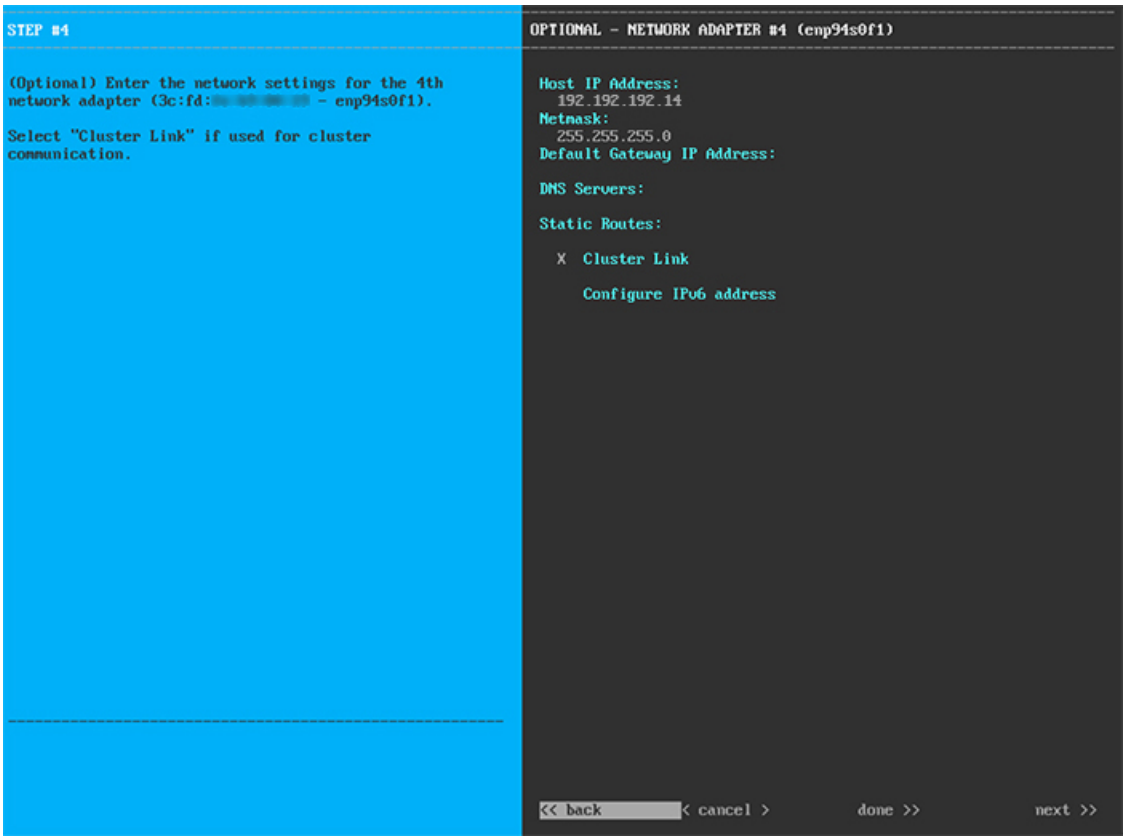
表 *4*：ネットワークアダプタ *#3* のプライマリノードエントリ：*10Gbps* エンタープライズポート（*enp94s0f0*）

ホスト IP アドレス（Host IP address）	エンタープライズポートの IP アドレスを入力します。これは必須です。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルトゲートウェイ IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは必須です。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。通常、Cisco DNA Centerこれは管理ポートでのみ必要です。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 8 入力したエンタープライズポート値の検証が成功すると、ウィザードに 10Gbps クラスタポート（enp94s0f1）が **[ネットワークアダプタ#4（NETWORK ADAPTER #4）]** として表示されます。「インターフェイスケーブル接続」で説明したように、このポートはアプライアンスをクラスタにリンクするために使用されるため、ホスト IP アドレス、ネットマスク、およびこの目的に適した他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



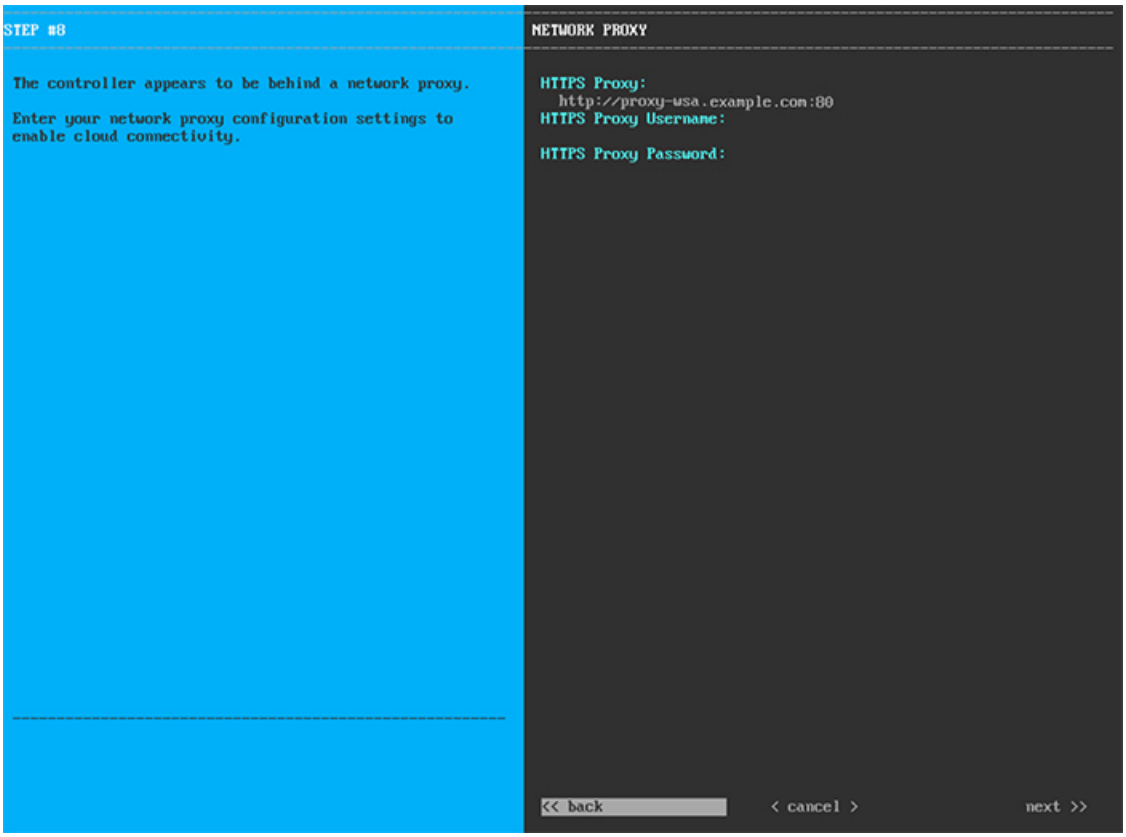
次の表に示すように、[ネットワークアダプタ#4（NETWORK ADAPTER #4）] の設定値を入力します。

表 *5:* ネットワークアダプタ *#4* のプライマリノードエントリ：*10Gbps* クラスタポート（*enp94s0f1*）

ホスト IP アドレス（Host IP address）	クラスタポートの IP アドレスを入力します。これは必須です。クラスタポートのアドレスは後で変更できないことに注意してください。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルトゲートウェイ IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは通常、エンタープライズポートでのみ必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。通常、これは管理ポートでのみ必要です。
クラスタリンク	このポートがCisco DNA Centerクラスタへのリンクであることを示すには、このチェックボックスをオンにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。ウィザードによって、ネットワークアダプタの設定が検証され、適用されます。

ステップ 9 ネットワークアダプタの設定が完了すると、次に示すように、使用している [ネットワークプロキシ（NETWORK PROXY）] の設定値を入力するようウィザードに求められます。



次の表に示すように、[ネットワークアダプタ（NETWORK ADAPTER）] の設定値を入力します。

表 *6*:ネットワークプロキシのプライマリノードエントリ

HTTPS プロキシ	インターネットにアクセスする HTTPS ネットワークプロキシの URL またはホスト名を入力します。 （注） Cisco DNA Center から HTTPS プロキシへの接続は、このリリースの HTTP 経由のみでサポートされます。
HTTPS プロキシ ユーザ名	ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
HTTPS プロキシ パスワード	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 10 ネットワークプロキシの設定が完了すると、次に示すように、[MAGLEVクラスタの詳細（MAGLEV CLUSTER DETAILS）] で、プライマリノードの仮想 IP アドレスを入力するようウィザードに求められます。

クラスタとネットワークの間のトラフィックに使用される仮想 IP アドレスのスペース区切りリストを入力します。この操作は、3 ノードクラスタと、将来 3 ノードクラスタに変換されるシングルノードクラスタの両方の場合に必要です。単一ノードクラスタをセットアップした後、単一ノードクラスタのまま使用し続ける予定の場合には、このステップをスキップしてステップ 11 に進みます。

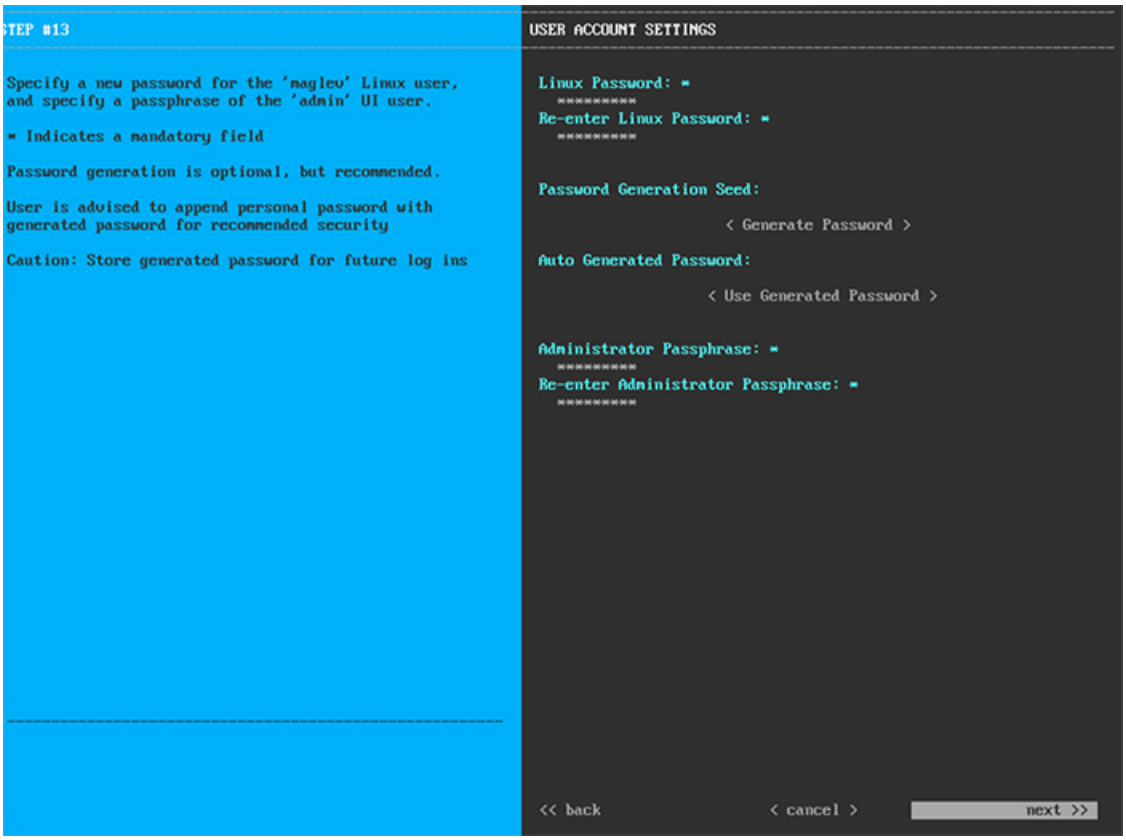
重要 設定済みのネットワークインターフェイスごとに 1 つずつ仮想 IP アドレスを入力する必要があります。この操作を行わない限り、ウィザードを完了することはできません。これらのアドレスは、クラスタリンクのステータスに関連付けられており、ステータスは**[アップ（UP）]**の状態となっている必要があります。

クラスタの完全修飾ドメイン名（FQDN）を指定するオプションもあります。Cisco DNA Center は、このホスト名を使用して次の操作を実行します。

- このホスト名を使用して、クラスタの Web インターフェイスと、Cisco DNA Center が管理するエンタープライズ ネットワーク内のデバイスによって使用される Representational State Transfer（REST）API にアクセスします。
- Cisco DNA Center 証明書の [サブジェクト代替名（SAN）（Subject Alternative Name（SAN））] フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイ サーバが定義されます。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 11 仮想 IP アドレスを入力すると、次に示すように、[ユーザアカウント設定（USER ACCOUNT SETTINGS）] の値を入力するようウィザードに求められます。



次の表の説明に従って、[ユーザアカウント設定（USER ACCOUNT SETTINGS）] の値を入力します。

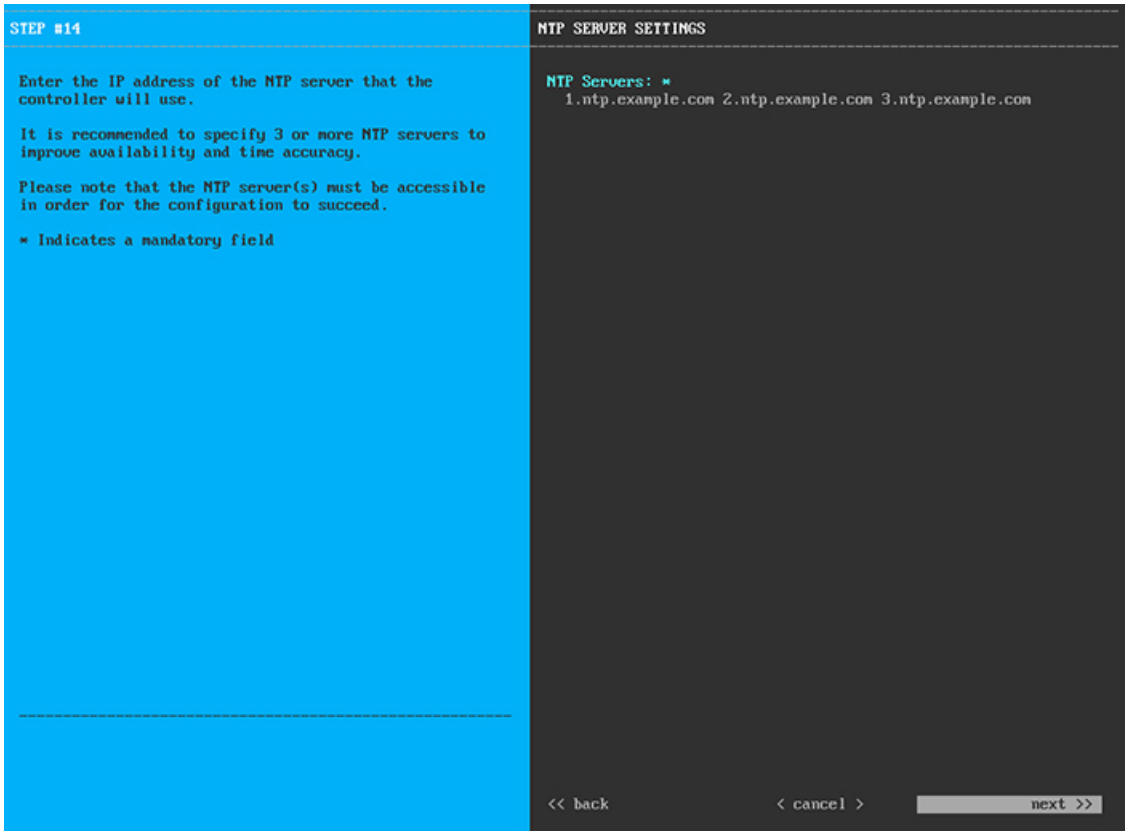
表 7:ユーザアカウント設定のプライマリノードエントリ

Linux パスワード	maglev ユーザの Linux パスワードを入力します。
Linux パスワードの再入力	Linux パスワードをもう一度入力して確認します。
パスワード生成シード	Linux パスワードを自分で作成しない場合には、このフィールドにシードフレーズを入力してから、**[パスワードの生成（Generate password）]** を押してパスワードを生成します。

自動生成パスワード	（オプション）シード フレーズは、ランダムで安全なパスワードの一部として表示されます。必要に応じて、このパスワードを「そのまま」使用することも、この自動生成パスワードをさらに編集することもできます。 [<Use Generated Password>] を押してパスワードを保存します。
管理者パスフレーズ	スーパーユーザ権限を持つ管理者のデフォルトのパスワードを入力します。このパスワードは Cisco DNA Center に初めてログインするときに使用します。
管理者パスフレーズの再入力	管理者パスフレーズをもう一度入力して確認します。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

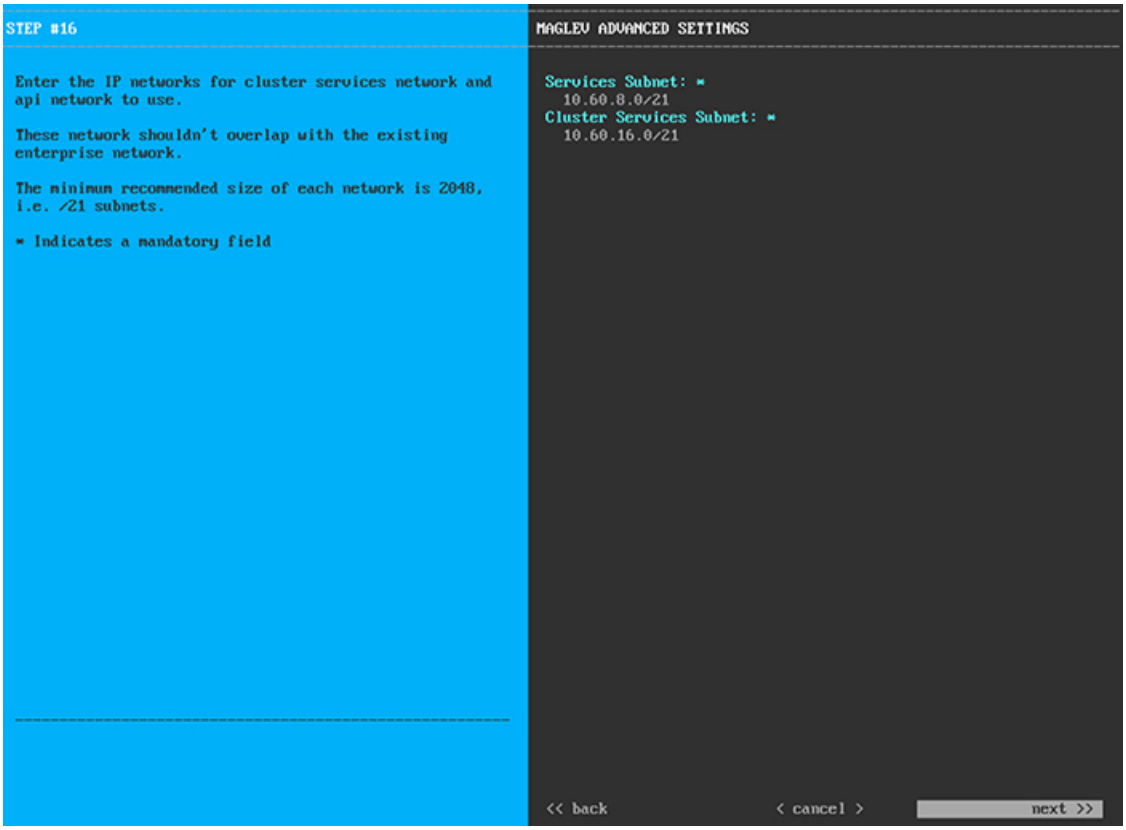
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように、[NTPサーバの設定（NTP SERVER SETTINGS）] の値を入力するようウィザードに求められます。



1つまたは複数のNTPサーバアドレスまたはホスト名をスペースで区切って入力します。1つ以上のNTPアドレスまたはホスト名が必要です。実稼働環境への展開では、少なくとも3台のNTPサーバを設定するようお勧めします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。ウィザードによって、NTPサーバの設定が検証され、適用されます。

ステップ13 NTPサーバを指定すると、次に示すように、[MAGLEV詳細設定（MAGLEV ADVANCED SETTINGS）] の値を入力するようウィザードに求められます。



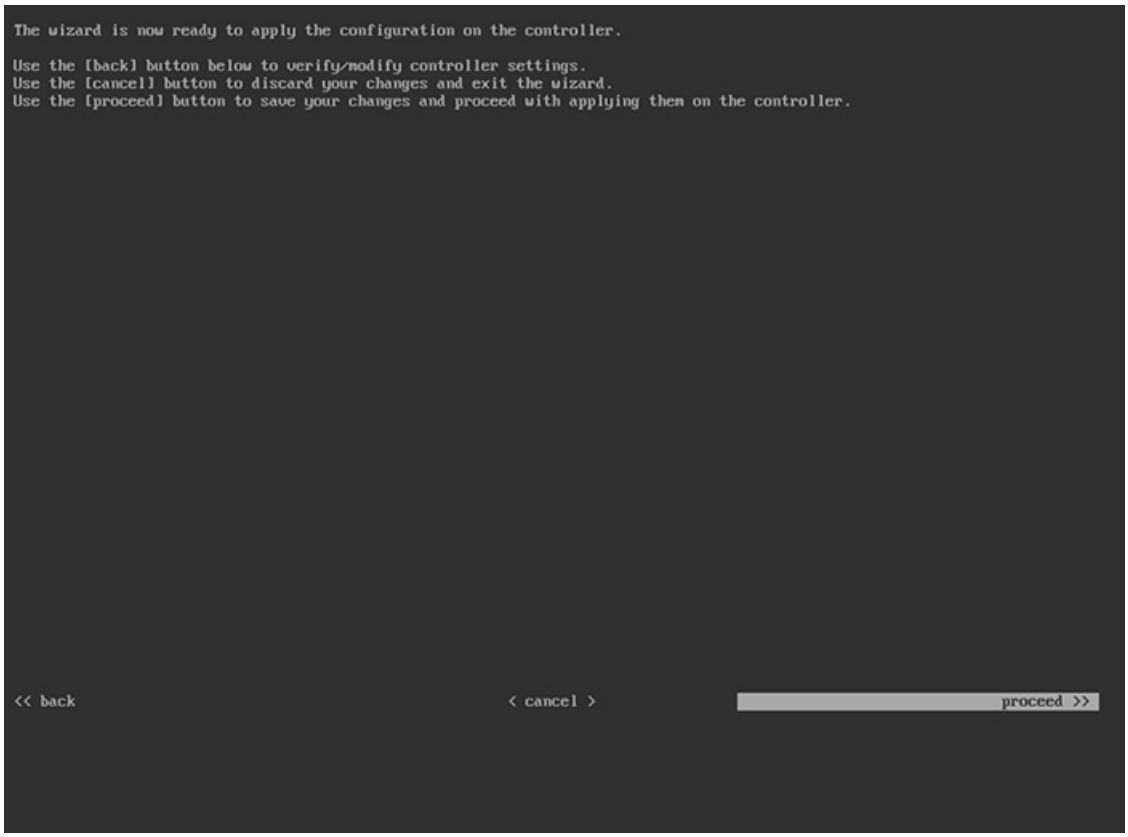
次の表に示すように、[MAGLEV 詳細設定（MAGLEV ADVANCED SETTINGS）] の設定値を入力します。

表 *8 : Maglev* 詳細設定のプライマリノードエントリ

サービスサブネット	独自のサービスの管理に使用する、Cisco DNA Center専用のIPサブネットを入力します。
クラスタサービスサブネット	Cisco DNA Centerが独自のクラスタリングサービスの管理に使用する、専用のIPサブネットを入力します。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 14 Maglev 詳細設定の入力が完了すると、次に示すように、ウィザードが設定の適用を続行する準備ができたことを示す最終メッセージが表示されます。



[続行>>（proceed>>）] を選択して設定を完了します。

ホストが自動的にリブートし、設定を適用してサービスを起動したとのメッセージが KVM コンソールに表示されます。このプロセスには数時間かかることがあります。KVM コンソールでプロセスの進行状況をモニタすることができます。

設定プロセスの最後に、アプライアンスの電源を再投入すると、「**設定に成功しました（CONFIGURATION SUCCEEDED!）**」というメッセージが表示されます。

次のタスク

タスクが完了した後：

- このアプライアンスをスタンドアロンモードのみで展開する場合には、初回セットアップ（「初期設定ワークフロー」）を実行して続行します。
- このアプライアンスをクラスタ内のプライマリノードとして展開する場合には、クラスタ内の 2 番目と 3 番目の設置済みアプライアンスを設定します（「アドオンノードの設定」）。

アドオンノードの設定

クラスタ内の 2 番目と 3 番目のアプライアンスを設定するには、次の手順を実行します。

重要 3 ノードクラスタを構築するには、同じバージョンの**システム**パッケージが 3 つの Cisco DNA Center アプライアンスにインストールされている必要があります。この条件が整わない場合、予期しない動作とダウンタイムの可能性が生じることがあります。

（注） この手順の実行中に入力するすべての IP アドレスが有効な IPv4 ネットマスクを持つ有効な IPv4 アドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

新しいアドオンノードをクラスタに結合する場合には、クラスタ内の最初のホストをプライマリノードとして指定する必要があります。クラスタにアドオンノードを結合する際、次の点に注意してください。

- クラスタに新しいノードを追加する前に、インストールされているすべてのパッケージがプライマリノードに展開されていることを確認してください。展開されているかどうかを確認するには、セキュアシェルを使用して、プライマリノードの Cisco DNA Center 管理ポートに Linux ユーザ（maglev）としてログインしてから、`maglev package status` コマンドを実行します。インストールされているすべてのパッケージは、コマンド出力で「展開済み（DEPLOYED）」と表示されます。次の例では、アプリケーションポリシー、SD アクセス、センサアシュアランス、センサ自動化のパッケージがインストールされていないため、これらのパッケージのステータスのみが [未展開（NOT_DEPLOYED）] になります。アドオンノードを設定する前に、パッケージのステータスが前述のように表示されている必要があります。

```
$ ssh maglev@172.29.131.14 -p 2222
The authenticity of host '[172.29.131.14]:2222 ([172.29.131.14]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:scye+2ll6NFHAkOZDs0cNLHBR75j1KV3ZXIKuUaiadk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.29.131.14]:2222' (ECDSA) to the list of known hosts.
Welcome to the Maglev Appliance
maglev@172.29.131.14's password:

Welcome to the Maglev Appliance

System information as of Thu Dec 20 03:07:13 UTC 2018

System load: 4.08                   IP address for enp94s0f0: 17.192.1.14
Usage of /: 59.8% of 28.03GB        IP address for enp94s0f1: 192.192.192.14
Memory usage: 21%                   IP address for eno1: 172.29.131.14
Swap usage: 0%                      IP address for docker0: 169.254.0.1
Processes: 831                      IP address for tun10: 10.60.3.0
Users logged in: 0
```

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

[Thu Dec 20 03:07:13 UTC] maglev@192.192.192.14
$ maglev package status
[administration] password for 'admin':

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

NAME                              DEPLOYED        AVAILABLE       STATUS
-------------------------------------------------------------------------------------
application-policy                -               2.1.10.170000   NOT_DEPLOYED
assurance                         1.0.5.686       1.1.8.1440      DEPLOYED
automation-core                   2.1.8.60044     2.1.12.60011    DEPLOYED
base-provision-core               2.1.8.60044     2.1.12.60016    DEPLOYED
command-runner                    2.1.8.60044     2.1.9.60029     DEPLOYED
device-onboarding                 2.1.8.60044     2.1.12.60016    DEPLOYED
image-management                  2.1.8.60044     2.1.12.60011    DEPLOYED
ncp-system                        2.1.8.60044     2.1.9.60029     DEPLOYED
ndp-base-analytics                1.0.7.878       1.0.7.908       DEPLOYED
ndp-platform                      1.0.7.829       1.0.7.866       DEPLOYED
ndp-ui                            1.0.7.956       1.0.7.975       DEPLOYED
network-visibility                2.1.8.60044     2.1.12.60016    DEPLOYED
path-trace                        2.1.8.60044     2.1.12.60016    DEPLOYED
sd-access                         -               2.1.12.60016    NOT_DEPLOYED
sensor-assurance                  -               1.1.5.40        NOT_DEPLOYED
sensor-automation                 -               2.1.9.60029     NOT_DEPLOYED
system                            1.0.4.807       1.0.4.855       DEPLOYED
```

- 一度に1つのノードのみをクラスタに結合してください。複数のノードを同時に追加しないでください。同時に追加しようとすると予期しない動作が発生します。
- 各アドオンノードのクラスタ接続プロセス中に、サービスのダウンタイムが発生することが予想されます。サービスはすべてのノードに再配布される必要があり、そのプロセスの間、クラスタはダウンします。

始める前に

次のことを確認します。

- 「プライマリノードの設定」の手順に従って、クラスタ内の最初のアプライアンスが設定されたこと。
- 「必要なIPアドレスおよびサブネット」と「必要な設定情報」で必要とされているすべての情報が収集されたこと。
- 「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、2番目と3番目のアプライアンスがインストールされたこと。
- 以下を完了していること。

1. 最初のアプライアンスで **maglev package status** コマンドを実行したこと。

   この情報にはCisco DNA Centerホームページからもアクセスできます。**[ヘルプ（Help）]** アイコン（⚙）をクリックし、**[概要（About）]**>**[パッケージを表示（Show Packages）]** の順に選択してください。

2. Cisco TAC に連絡し、このコマンドの出力を提供して 2 番目と 3 番目のアプライアンスにインストールする必要がある ISO をポイントするよう依頼したこと。

- 「CIMC へのブラウザアクセスの有効化」の説明に従って、両方のアドオンアプライアンスで CIMC ブラウザアクセスが設定されたこと。
- 「プリフライトチェックの実行」の説明に従って、アドオン ノードアプライアンスのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- 互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応するリリースノートを参照してください。
- 次の手順のステップ 7 で指定する DNS サーバと Cisco DNA Center の間のファイアウォールで ICMP が許容されること。Maglev 構成ウィザードでは ping を使用して、ユーザの指定した DNS サーバを確認します。Cisco DNA Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

ステップ 1 CIMC GUI の設定時に設定した CIMC IP アドレスにブラウザでアクセスし、CIMC ユーザとして CIMC GUI にログインします（「CIMC へのブラウザアクセスの有効化」を参照）。

ログインが成功すると、次に示すように、アプライアンスに **[Cisco Integrated Management Controller Chassisの概要（Cisco Integrated Management Controller Chassis Summary）]** ウィンドウが右上の青いリンクメニューとともに表示されます。

ステップ 2 青いリンクメニューで **[KVM の起動（Launch KVM）]** を選択してから **[Java ベースの KVM（Java based KVM）]** と **[HTML ベースの KVM（HTML based KVM）]** のいずれかを選択します。Java ベースの KVM を選択した場合、KVM コンソールを独自のウィンドウで表示するために、ブラウザまたはファイルマネージャから Java スタートアップファイルを起動する必要があります。HMTL ベースの KVM を選択すると、KVM コンソールが別個のブラウザウィンドウまたはタブで自動的に起動します。

選択した KVM のタイプに関係なく、KVM コンソールを使用して、設定の進行状況をモニタし、Maglev 構成ウィザードのプロンプトに応答します。

ステップ 3 KVM が表示されたら、次のいずれかを選択してアプライアンスをリブートします。

a) メインの CIMC GUI ブラウザウィンドウで、**[ホストの電源（Host Power）]** > **[電源の再投入（Power Cycle）]** を選択します。その後、KVM コンソールに切り替えて続行します。
b) KVM コンソールで、**[電源（Power）]** > **[システムの電源の再投入（コールドブート）（Power Cycle System（cold boot））]** を選択します。

アプライアンスをリブートするかどうかの確認を求められたら、**[OK]** をクリックします。

リブートメッセージが表示された後、次に示すように、KVM コンソールに Maglev 構成ウィザードのウェルカム画面が表示されます。

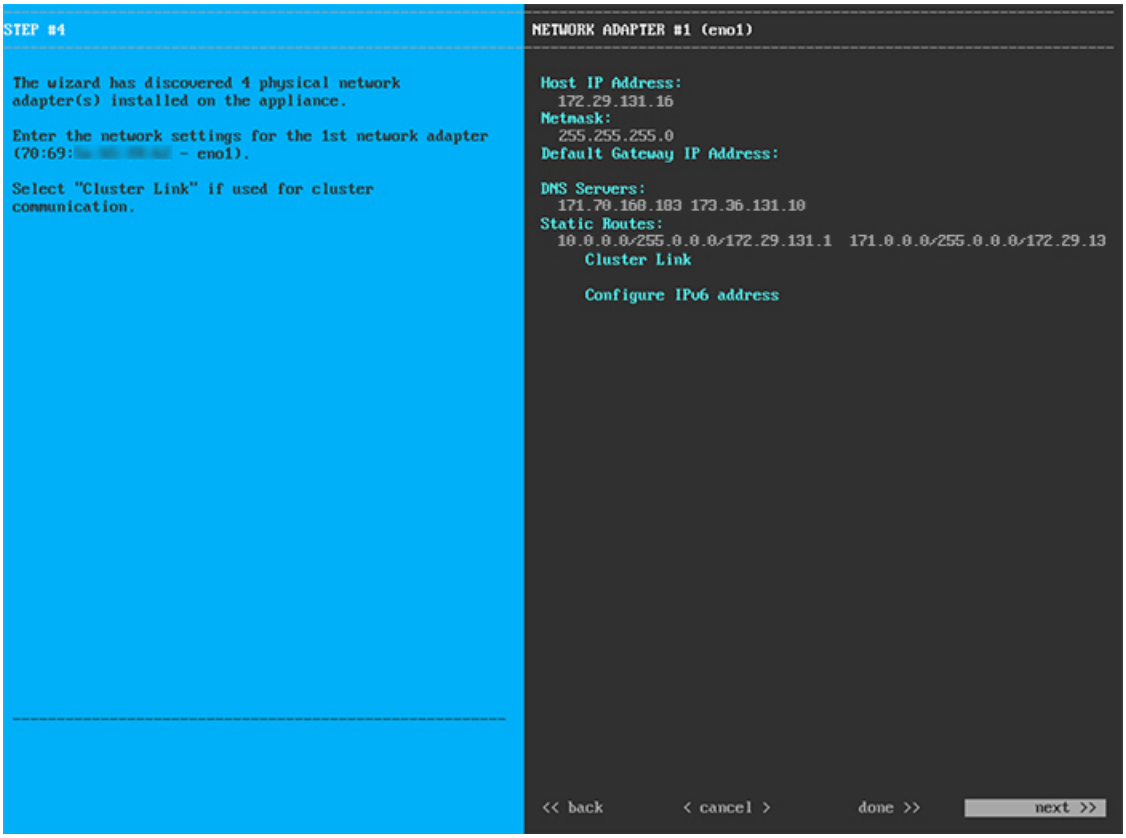
ステップ 4 **[Cisco DNA Centerクラスタに追加（Join a DNA-C cluster）]** を選択して、アドオンノードの設定を開始します。

ウィザードでは、アプライアンス上のすべてのポートが検出され、次の順序で 1 つずつ別の画面に表示されます。

1. 1Gbps/10Gbps 管理ポート（1、eno1、ネットワークアダプタ #1）
2. 1Gbps/10Gbps クラウドポート（2、eno2、ネットワークアダプタ #2）
3. 10Gbps エンタープライズポート（enp94s0f0、ネットワークアダプタ #3）
4. 10Gbps クラスタポート（enp94s0f1、ネットワークアダプタ #4）

（注） 設定の過程でウィザードがエンタープライズポートとクラスタポートのいずれかまたは両方を表示できない場合は、これらのポートが機能していないか、または無効になっている可能性があります。これらの 10 Gbps ポートは Cisco DNA Center 機能に必要です。10 Gbps ポートが機能していないことが判明した場合には、[キャンセル（Cancel）] を選択して、設定をすぐに終了します。設定を再開したり、Cisco Technical Assistance Center（TAC）に連絡したりする前に「プリフライトチェックの実行」に記載されているすべての手順が完了していることを確認してください。

ステップ 5 このウィザードでは 1Gbps/10Gbps 管理ポート（1、eno1）がまず検出され、**[ネットワークアダプタ#1（NETWORK ADAPTER #1）]** として表示されます。「インターフェイスケーブル接続」で説明したように、このポートは管理ネットワークから Cisco DNA Center GUI にアクセスするために使用されます。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



次の表に示すように、**[ネットワークアダプタ#1（NETWORK ADAPTER #1）]**の設定値を入力します。

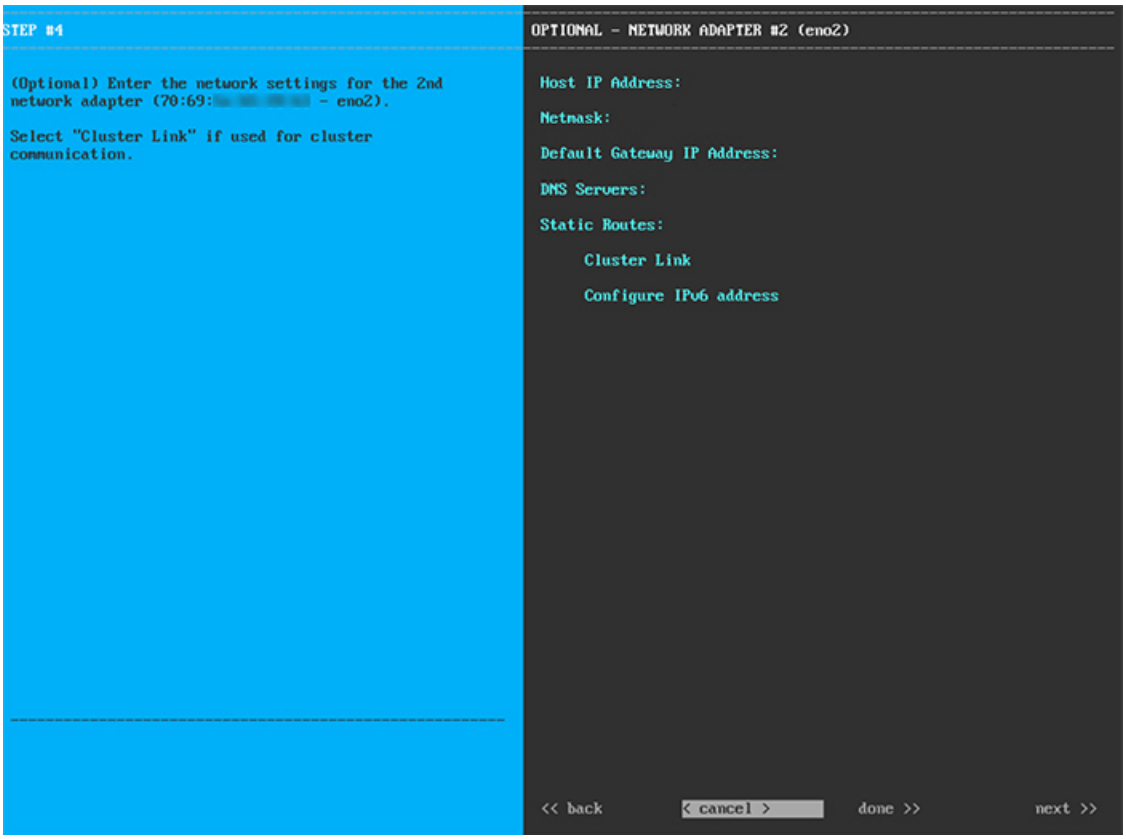
表 *9*：ネットワークアダプタ *#1* のアドオンノードエントリ：*1Gbps/10Gbps* 管理ポート（*eno1*）

ホスト IP アドレス（Host IP address）	管理ポートの IP アドレスを入力します。これは、このポートを使用して管理ネットワークから Cisco DNA Center GUI にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。

ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは通常、エンタープライズポートでのみ必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** • NTP の場合、Cisco DNA Center と NTP サーバの間のポート 123（UDP）が開いていることを確認します。 • クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

設定値の入力が完了したら、[次へ>>（next>>）] を選択して続行します。[次へ>>（next>>）] を選択すると、入力した値がウィザードによって検証され、正しくない場合にはエラーメッセージが表示されます。エラーメッセージが表示された場合には、入力した値が正しいことを確認してから、再入力します。必要に応じて、[戻る<<（<<back）] を選択して再入力します。

ステップ 6 入力した管理ポート値の検証が成功すると、ウィザードに 1Gbps /10Gbps クラウドポート（2、eno2）が **[ネットワークアダプタ#2（NETWORK ADAPTER #2）]** として表示されます。「インターフェイスケーブル接続」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、10Gbps エンタープライズポート（enp94s0f0）経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



次の表に示すように、[ネットワークアダプタ#2（NETWORK ADAPTER #2）] の設定値を入力します。

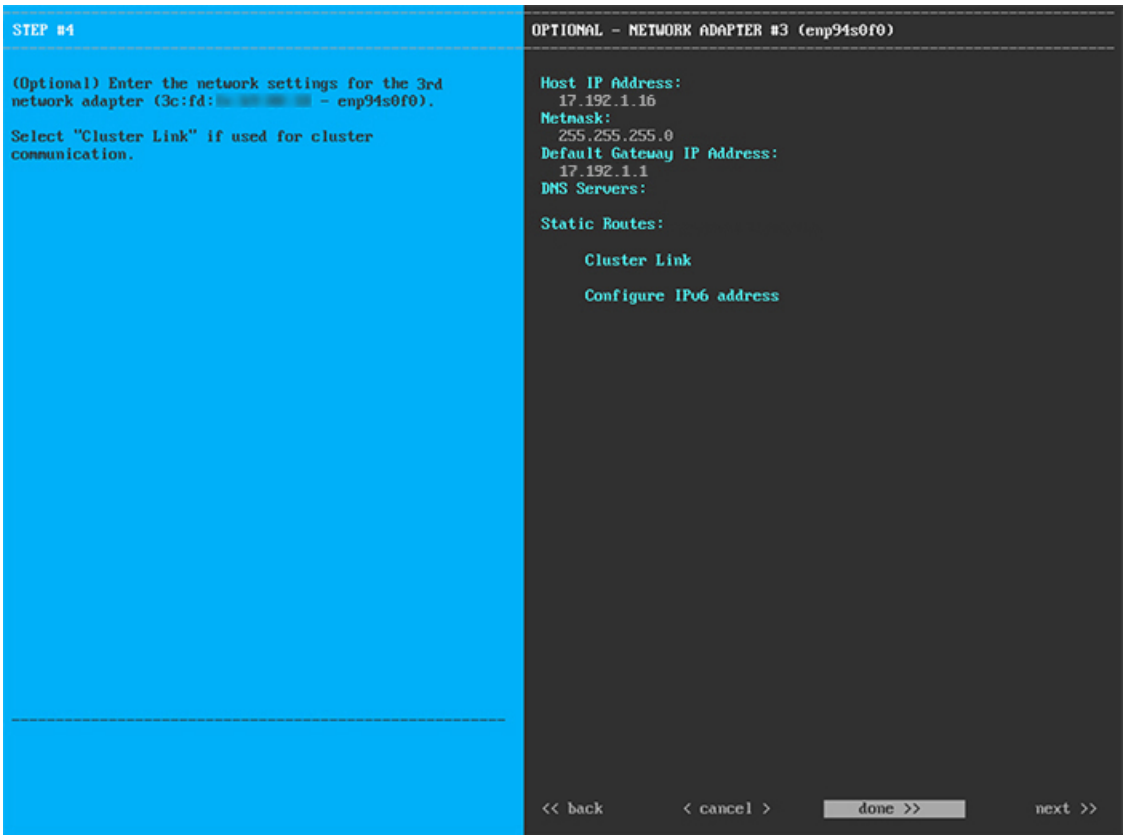
表 *10*：ネットワークアダプタ *#2* のアドオンノードエントリ：*1Gbps/10Gbps* クラウドポート（*eno2*）

ホスト IP アドレス（Host IP address）	クラウドポートの IP アドレスを入力します。この操作はインターネット接続にクラウドポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにしておくことができます。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	クラウドポートに使用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。これは通常、エンタープライズポートでのみ必要になります。

DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。通常、これは管理ポートでのみ必要です。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 7 入力したクラウドポート値の検証が成功すると、ウィザードに 10Gbps エンタープライズポート（enp94s0f0）が **[ネットワークアダプタ#3（NETWORK ADAPTER #3）]** として表示されます。「インターフェイスケーブル接続」で説明したように、このポートは、アプライアンスをエンタープライズネットワークにリンクするために必要なポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



次の表に示すように、[ネットワークアダプタ#3（NETWORK ADAPTER #3）] の設定値を入力します。

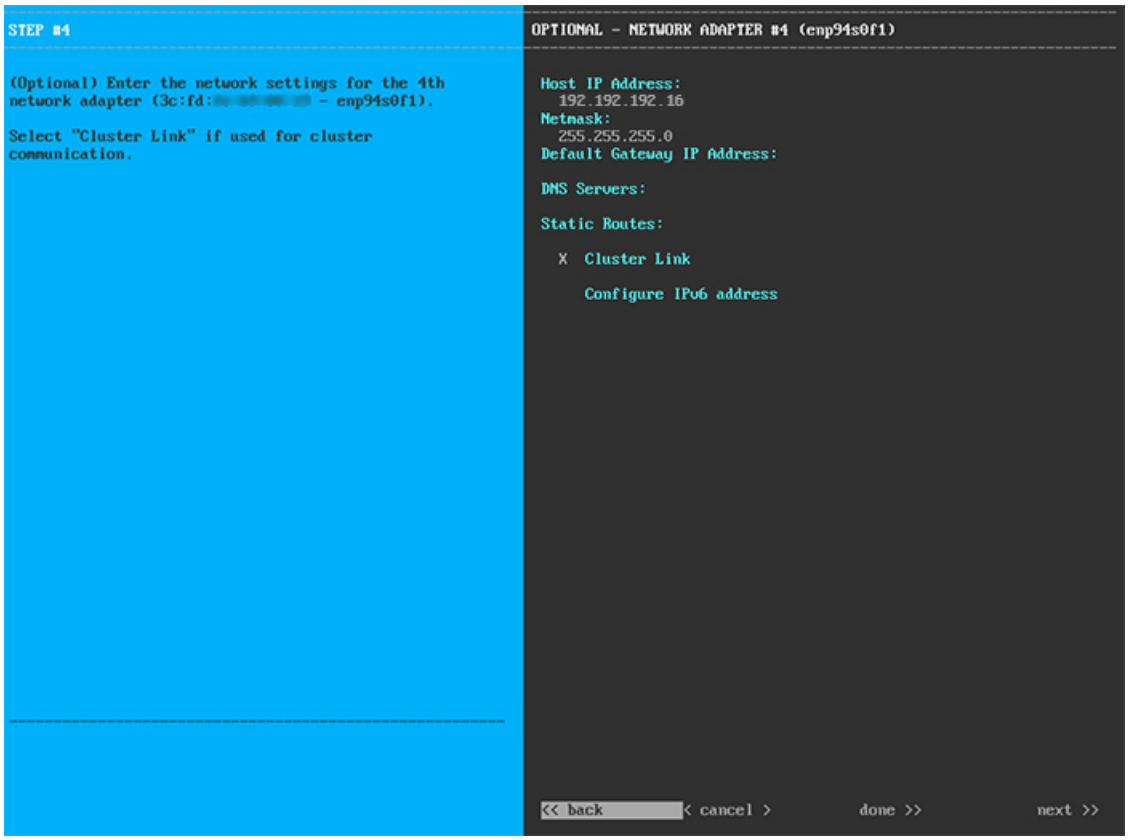
表 *11*：ネットワークアダプタ *#3* のアドオンノードエントリ：*10Gbps* エンタープライズポート（*enp94s0f0*）

ホスト IP アドレス（Host IP address）	エンタープライズポートの IP アドレスを入力します。これは必須です。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルトゲートウェイ IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは必須です。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。通常、 Cisco DNA Centerこれは管理ポートでのみ必要です。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 8 入力したエンタープライズポート値の検証が成功すると、ウィザードに 10Gbps クラスタポート（enp94s0f1）が **[ネットワークアダプタ#4（NETWORK ADAPTER #4）]** として表示されます。「インターフェイスケーブル接続」で説明したように、このポートはアプライアンスをクラスタにリンクするために使用されるため、ホスト IP アドレス、ネットマスク、およびこの目的に適した他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必要な設定情報」を参照してください）。



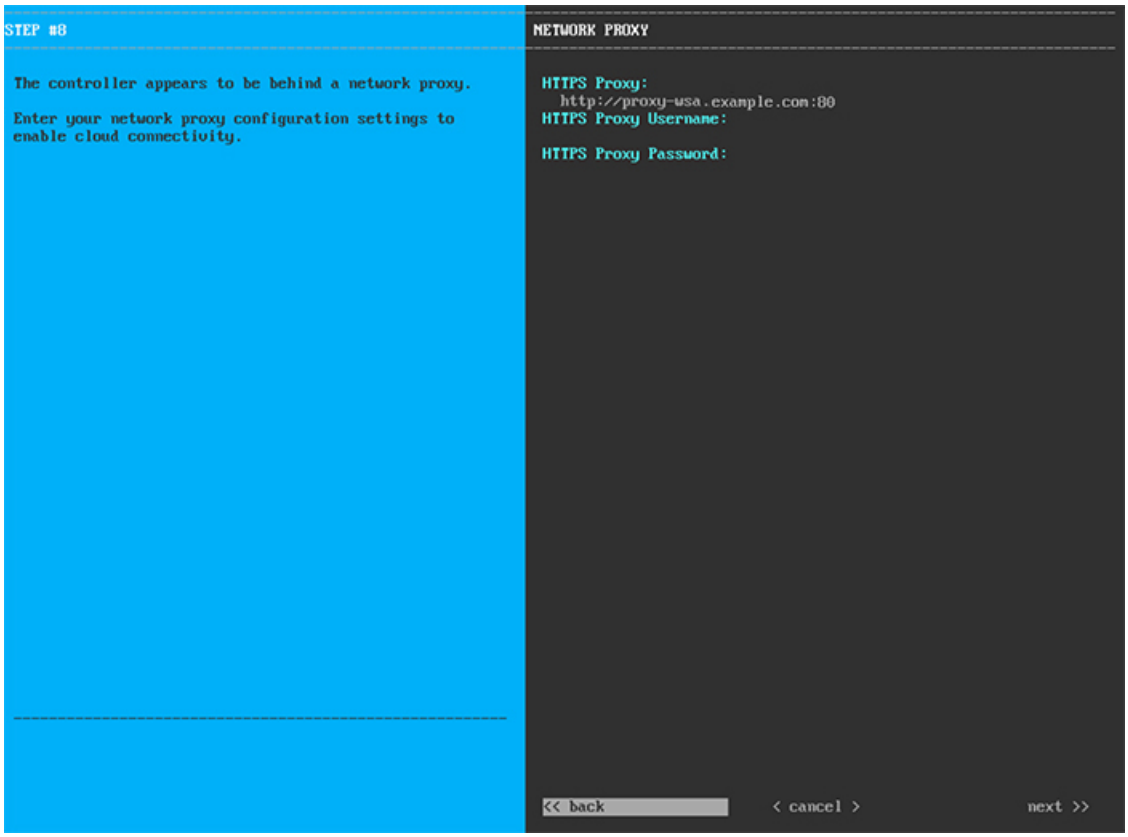
次の表に示すように、[ネットワークアダプタ#4（NETWORK ADAPTER #4）] の設定値を入力します。

表 *12 :* ネットワークアダプタ *#4* のアドオンノードエントリ：*10Gbps* クラスタポート（*enp94s0f1*）

ホスト IP アドレス（Host IP address）	クラスタポートの IP アドレスを入力します。これは必須です。クラスタポートのアドレスは後で変更できないことに注意してください。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルトゲートウェイ IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは通常、エンタープライズポートでのみ必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 **重要** クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。通常、これは管理ポートでのみ必要です。
クラスタリンク	このポートがクラスタへのリンクであることを示すには、このチェックボックスをオンにします。この操作はクラスタポートでのみ必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 9 ネットワークアダプタの設定が完了すると、次に示すように、使用している [ネットワークプロキシ（NETWORK PROXY）] の設定値を入力するようウィザードに求められます。



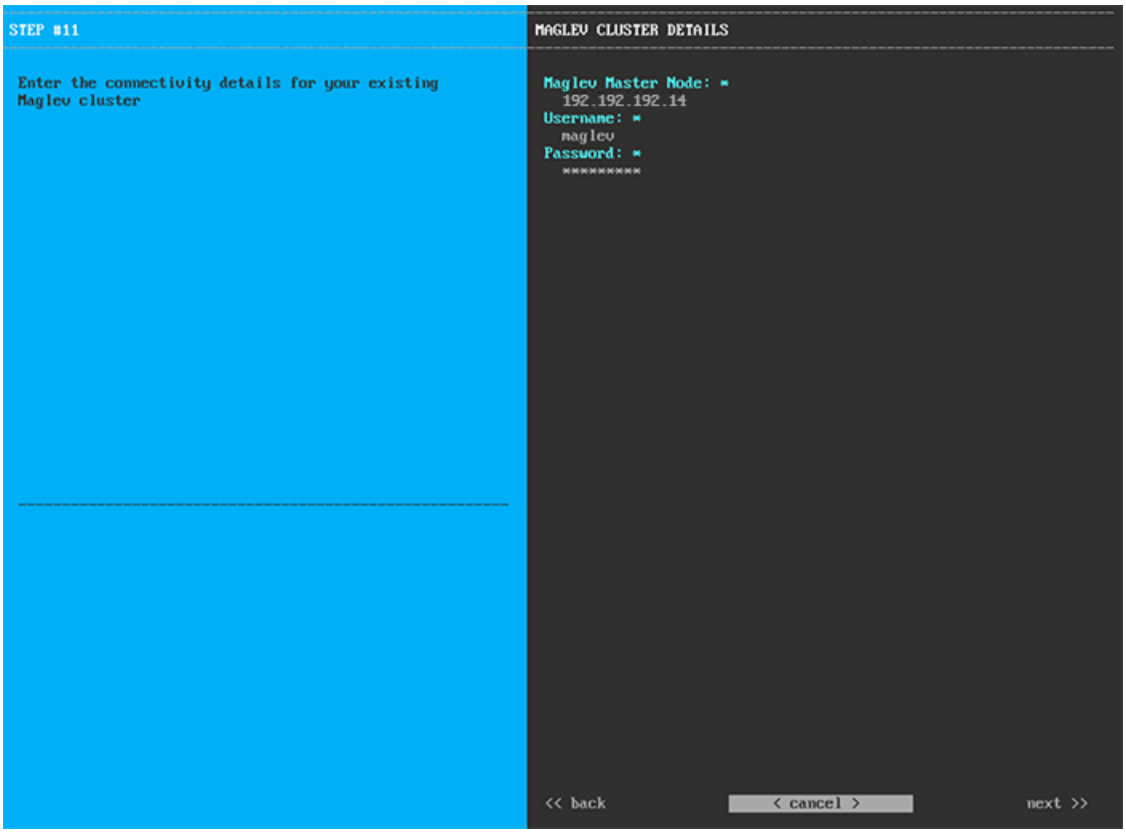
次の表に示すように、[ネットワークアダプタ（NETWORK ADAPTER）] の設定値を入力します。

表 *13*：ネットワークプロキシのアドオンノードエントリ

HTTPS プロキシ	インターネットにアクセスする HTTPS ネットワークプロキシの URL またはホスト名を入力します。 （注） Cisco DNA Center から HTTPS プロキシへの接続は、このリリースの HTTP 経由のみでサポートされます。
HTTPS プロキシ ユーザ名	ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
HTTPS プロキシ パスワード	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

終了したら、[次へ>>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 10 ネットワークプロキシの設定が完了すると、次に示すように、[MAGLEVクラスタの詳細（MAGLEV CLUSTER DETAILS）] で、プライマリノードのクラスタポートとプライマリノードのログイン情報を指定するよう促すウィザードのメッセージが表示されます。



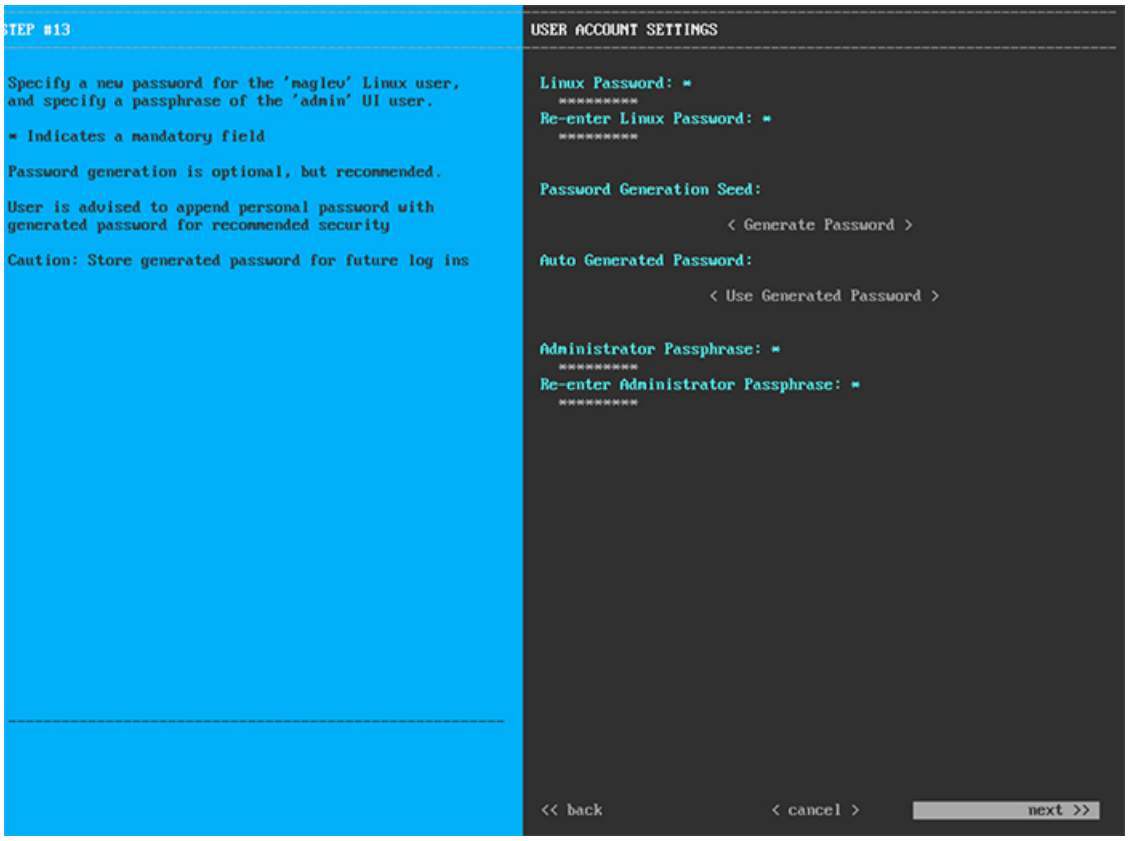
次の表の説明に従って、[MAGLEV クラスタの詳細（MAGLEV CLUSTER DETAILS）] に値を入力します。

表 *14 : Maglev* クラスタの詳細へのアドオンノードエントリ

Maglev ノード	クラスタ内のプライマリノードのクラスタポートの IP アドレスを入力します。ポート割り当ての推奨事項に従っている場合、これはプライマリノードの IP アドレス enp94s0f1、ネットワークアダプタ #4 です。
Username	**maglev** と入力します。
Password	プライマリノードで設定した Linux パスワードを入力します。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 11 Maglev クラスタの詳細を入力すると、次に示すように、このアドオンノードの [ユーザアカウント設定（USER ACCOUNT SETTINGS）] の値を入力するように求められます。



次の表の説明に従って、[ユーザアカウント設定（USER ACCOUNT SETTINGS）] の値を入力します。

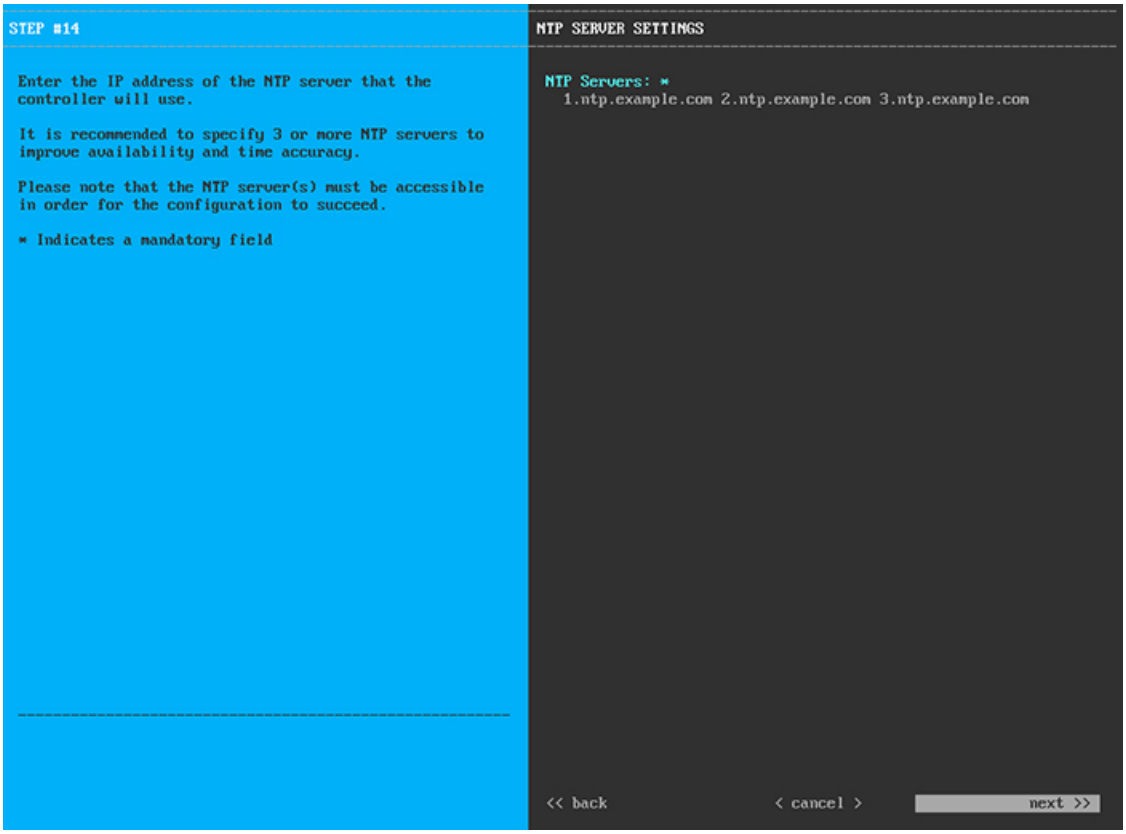
表 *15*：ユーザアカウント設定のアドオンノードエントリ

Linux パスワード	maglev ユーザの Linux パスワードを入力します。
Linux パスワードの再入力	Linux パスワードをもう一度入力して確認します。
パスワード生成シード	Linux パスワードを自分で作成しない場合には、このフィールドにシードフレーズを入力してから、**[パスワードの生成（Generate password）]** を押してパスワードを生成します。
自動生成パスワード	（オプション）シード フレーズは、ランダムで安全なパスワードの一部として表示されます。必要に応じて、このパスワードを「そのまま」使用することも、この自動生成パスワードをさらに編集することもできます。 [<Use Generated Password>] を押してパスワードを保存します。

管理者パスフレーズ	スーパーユーザ権限を持つ管理者のデフォルトのパスワードを入力します。このパスワードは Cisco DNA Center に初めてログインするときに使用します。
管理者パスフレーズの再入力	管理者パスフレーズをもう一度入力して確認します。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

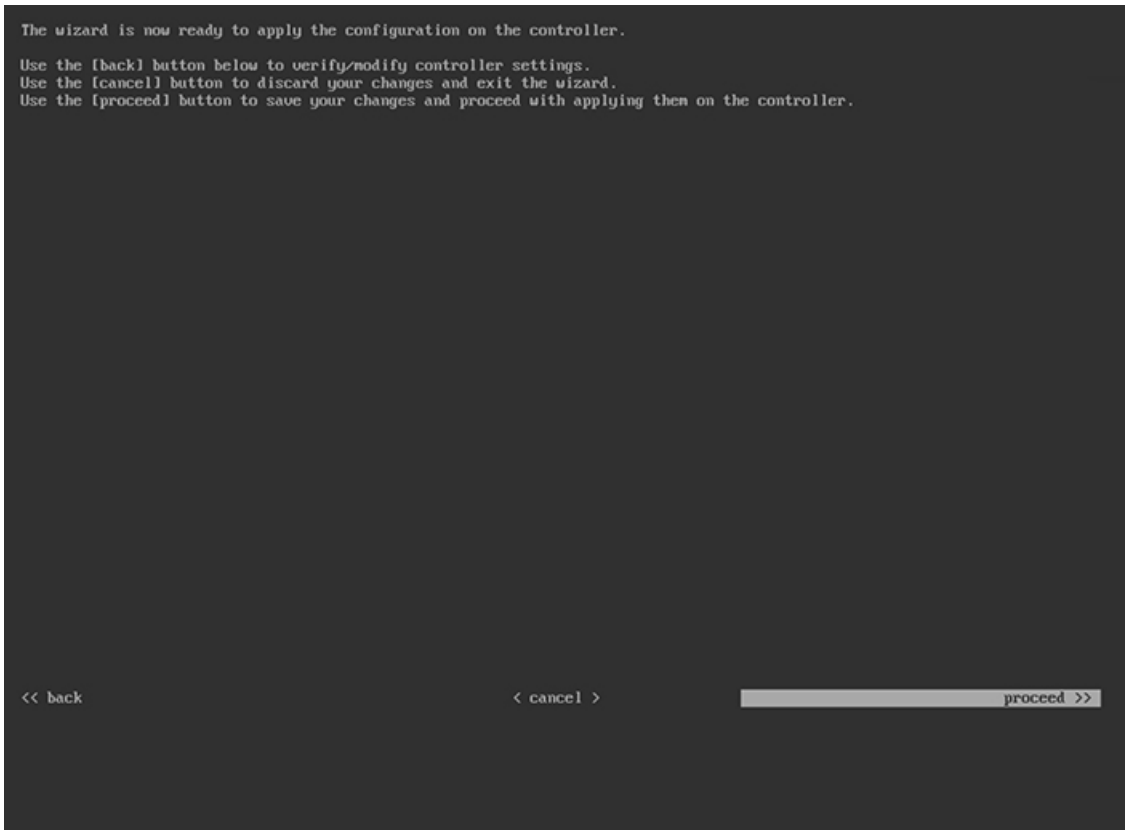
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように、[NTPサーバの設定（NTP SERVER SETTINGS）] の値を入力するようウィザードに求められます。



1つまたは複数のNTPサーバアドレスまたはホスト名をスペースで区切って入力します。1つ以上のNTPアドレスまたはホスト名が必要です。プライマリノードに指定したNTPサーバと同じである必要があります。

終了したら、[次へ>>（next>>）] を選択して続行します。以前の画面でしたように、検証エラーを修正します。

ステップ 13 NTP サーバ設定の入力が完了すると、次に示すように、ウィザードが設定の適用を続行する準備ができたことを示す最終メッセージが表示されます。



[続行>>（proceed>>）] を選択して設定を完了します。

ホストが自動的にリブートし、設定を適用してサービスを起動したとのメッセージが KVM コンソールに表示されます。このプロセスには数時間かかることがあります。KVM コンソールでプロセスの進行状況をモニタすることができます。

設定プロセスの最後に、アプライアンスの電源を再投入すると、「**設定に成功しました（CONFIGURATION SUCCEEDED!）**」というメッセージが表示されます。

次のタスク

タスクが完了した後：

- クラスタ内の 3 番目および最後のノードとして展開する追加のアプライアンスがある場合には、この手順を繰り返します。
- クラスタへのホストの追加が終了したら、初回セットアップ（「初期設定ワークフロー」）を実行して続行します。

ハイ アベイラビリティ クラスタの展開シナリオ

ネットワーク内のアプライアンスは、最大3つのノードのクラスタのうちの1つとして導入できます。このモードでは、すべてのサービスとデータがホスト間で共有されます。

クラスタに導入する場合は、ネットワークに適した導入シナリオを選択します。

- 新しい HA の展開
- 標準インターフェイス設定を使用したプライマリノードの既存 HA の展開
- 非標準インターフェイス設定を使用したプライマリノードの既存 HA の展開

次の項では、各シナリオについて説明します。

新しい HA の展開

最新の HA クラスタをインストールするには、次の手順を実行します。

ステップ 1 最初に設置したアプライアンスをプライマリノードとして設定します。

「プライマリノードの設定」を参照してください。

ステップ 2 次のとおりクラスタ内の 2 番目と 3 番目のアプライアンスを設定します。

「アドオンノードの設定」を参照してください。

標準インターフェイス設定を使用したプライマリノードの既存 HA の展開

プライマリノードが必要なインターフェイスケーブル設定を使用する既存の HA クラスタを展開するには、次の手順を実行します。

ステップ 1 プライマリノードを Cisco DNA Center 1.2.10 にアップグレードします。

Cisco DNA Center の現在のリリースをアップグレードする方法の詳細については、『Release Notes for Cisco DNA Center』を参照してください。

ステップ 2 プライマリノードで必要なインターフェイスケーブル設定を使用していることを確認します。

「インターフェイスケーブル接続」を参照してください。

ステップ 3 仮想 IP アドレスを更新します（VIP がまだ追加されていない場合）。

「設定ウィザードを使用したアプライアンスの再設定」を参照してください。

ステップ 4 次のとおりクラスタ内の 2 番目と 3 番目のアプライアンスを設定します。

「アドオンノードの設定」を参照してください。

ステップ 5 次のコマンドを入力して、glusterfs のサイズを確認します。

sudo du -h /data/maglev/srv/maglev-system/glusterfs/mnt/bricks/default_brick/ | tail -1 | awk '{print $1}'

glusterfs ファイルシステムのサイズが 150 GB を超える場合には、「非標準インターフェイス設定を使用したプライマリノードの既存 HA の展開」の手順を実行します。

非標準インターフェイス設定を使用したプライマリノードの既存 HA の展開

プライマリノードが標準以外のインターフェイス設定を使用する既存の HA クラスタを展開するには、次の手順を実行します。

ステップ 1 プライマリノードを Cisco DNA Center 1.2.10 にアップグレードします。

Cisco DNA Center の現在のリリースをアップグレードする方法の詳細については、『Release Notes for Cisco DNA Center』を参照してください。

ステップ 2 リモートリポジトリのバックアップを作成します。

『Cisco DNA Center Administrator Guide』の「Backup and Restore」の章を参照してください。

ステップ 3 必要なインターフェイスケーブル設定を使用して、プライマリノードイメージを作成し直します。

「インターフェイスケーブル接続」と「Cisco DNA Center ISO イメージのインストール」を参照してください。VIP がプライマリノードで正しく設定されていることを確認します。

ステップ 4 プライマリノードで、バックアップ中に選択したパッケージと同じ一連のパッケージをインストールします。

ステップ 5 ステップ 2 で作成したバックアップファイルを復元します。

ステップ 6 次のとおりクラスタ内の 2 番目と 3 番目のアプライアンスを設定します。

「アドオンノードの設定」を参照してください。

HA の展開に関する追加の考慮事項

既存の HA の導入では、次の追加設定を行う必要があります。

（注） 既知の HA のバグと回避策については、『Cisco Digital Network Architecture Center リリースノート』の「未解決のバグ - HA」を参照してください。

テレメトリ

（VIP を有効にせずに）デバイスのテレメトリを有効にした場合には、次の手順を実行します。

ステップ 1 **maglev-config update** コマンドを使用して、クラスタ VIP を更新します。

ステップ 2 デバイスでテレメトリを無効にします。

1. Cisco DNA Center ホームページで **[** ツール（Tools） **]** エリアの **[** テレメトリ（Telemetry） **]** を選択します。

   [テレメトリ（Telemetry）] ウィンドウが表示されます。

2. [Site View] タブをクリックします。
3. テレメトリを無効にするデバイスのチェックボックスをオンにします。次に、**[アクション（Actions）]**> **[テレメトリの無効化（Disable_Telemetry）]** を選択します。

ステップ 3 以前のテレメトリプロファイルとデバイスの関連付けを使用して、テレメトリを再度有効にします。

ワイヤレス コントローラ

ネットワーク内のワイヤレスコントローラを Cisco DNA Center の新しい VIP で更新する必要があります。

Cisco DNA Center の最新リリースへのアップグレード

Cisco DNA Center の最新リリースに向けたアップグレードの詳細については、『Cisco Digital Network Architecture Center アップグレードガイド』を参照してください。