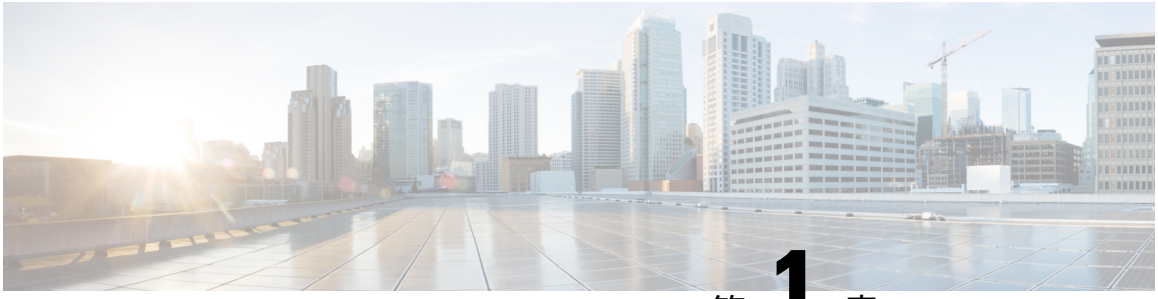
Cisco DNA Center 第 2 世代アプライアンス リリース 1.3 インストールガイド

初版：2019 年 5 月 31 日

最終更新：2019 年 11 月 13 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

Cisco DNA Center アプライアンス機能の確認

アプライアンスのハードウェア仕様

シスコは、ラックマウント可能な物理アプライアンスの形で Cisco Digital Network Architecture（DNA）Center を提供しています。第 2 世代の Cisco DNA Center アプライアンスは、Cisco Unified Computing System（UCS）C220 M5 小型フォームファクタ（SFF）シャーシまたは Cisco UCS C480 M5 シャーシのいずれかで構成されています。両方とも 1 つの INTEL X710-DA2 ネットワーク インターフェイス カード（NIC）と 1 つの INTEL X710-DA4 NIC が追加されています。次に示す第 2 世代アプライアンスの 4 つのバージョンを使用できます。

- 44 コアアプライアンス：シスコ製品番号 DN2-HW-APL
- 44 コア アップグレード アプライアンス：シスコ製品番号 DN2-HW-APL-U

  これは第 1 世代 44 コアアプライアンス（シスコ製品番号 DN1）からアップグレードする場合の関連製品番号です。
- 56 コアアプライアンス：シスコ製品番号 DN2-HW-APL-L
- 112 コアアプライアンス：シスコ製品番号 DN2-HW-APL-XL

Cisco DNA Center ソフトウェアイメージはこれらのアプライアンスに事前にインストールされていますが、使用するには設定する必要があります。

次の表はアプライアンスのハードウェア仕様をまとめたものです。

表 *1 : 44* コア *Cisco DNA Center* アプライアンスのハードウェア仕様

機能	説明
シャーシ	1 ラックユニット（1RU）シャーシ
プロセッサ	22 コア Intel Xeon Gold 6152 2.1 GHz プロセッサ X 2
メモリ	32 GB DDR4 2666 MHz の登録済み DIMM（RDIMM）X 8
ストレージ	• RAID 1 で 480 GB X 2 • RAID 1 で 1.9 TB X 2 • RAID 10 で 1.9 TB X 6
ディスク管理（RAID）	• スロット 1 ～ 4 の RAID 1 • スロット 5 ～ 10 の RAID 10
ネットワークおよび管理 I/O	サポートされるコネクタ： • Intel X710-DA2 NIC 上の 10 Gbps イーサネットポート X 2 • 1 Gbps RJ-45 管理ポート（Marvell 88E6176）X 1 • 10GBase-T LOM ポート（マザーボードに Intel X550 コントローラを搭載）X 2 次のコネクタを使用できますが、通常は Cisco DNA Center の日常業務では使用されません。 • RS-232 シリアル ポート（RJ-45 コネクタ）X 1 • VGA（DB-15）コネクタ X 1 • USB 3.0 コネクタ X 2 • USB 2.0 2 個、VGA（DB-15）1 個、シリアル（RS-232）RJ-45 コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1 10 Gbps イーサネットポート 4 個を提供する Intel X710-DA4 NIC は、今回の Cisco DNA Center リリースでは無効ですが、今後の製品リリースで有効になります。ご注意ください。
電源	770 W AC 電源 X 2。 1+1 の冗長構成。
冷却	ホットスワップ可能なファン モジュール（前面から背面に向かう冷却用）X 7。

機能	説明
ビデオ	最大 1920 X 1200、60 Hz 時 16 bpp、最大 512 MB のビデオメモリを搭載したビデオグラフィックスアレイ（VGA）ビデオ解像度（デフォルトの割り当ては 8 MB）。

表 *2 : 56* コア *Cisco DNA Center* アプライアンスのハードウェア仕様

機能	説明
シャーシ	1 ラックユニット（1RU）シャーシ
プロセッサ	28 コア Intel Xeon Platinum 8180 2.5 GHz プロセッサ X 2
メモリ	32 GB DDR4 2666 MHz RDIMM X 12
ストレージ	• RAID 1 で 480 GB X 2 • RAID 1 で 1.9 TB X 2 • RAID 10 で 1.9 TB X 6
ディスク管理（RAID）	• スロット 1 ～ 4 の RAID 1 • スロット 5 ～ 10 の RAID 10
ネットワークおよび管理 I/O	サポートされるコネクタ： • Intel X710-DA2 NIC 上の 10 Gbps イーサネットポート X 2 • 1 Gbps RJ-45 管理ポート（Marvell 88E6176）X 1 • 10GBase-T LOM ポート（マザーボードに Intel X550 コントローラを搭載）X 2 次のコネクタを使用できますが、通常は Cisco DNA Center の日常業務では使用されません。 • RS-232 シリアル ポート（RJ-45 コネクタ）X 1 • VGA（DB-15）コネクタ X 1 • USB 3.0 コネクタ X 2 • USB 2.0 2 個、VGA（DB-15）1 個、シリアル（RS-232）RJ-45 コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1 10 Gbps イーサネットポート 4 個を提供する Intel X710-DA4 NIC は、今回の Cisco DNA Center リリースでは無効ですが、今後の製品リリースで有効になります。ご注意ください。

機能	説明
電源	770 W AC 電源 X 2。 1+1 の冗長構成。
冷却	ホットスワップ可能なファン モジュール（前面から背面に向かう冷却用）X 7。
ビデオ	最大 1920 X 1200、60 Hz 時 16 bpp、最大 512 MB のビデオメモリを搭載したビデオグラフィックスアレイ（VGA）ビデオ解像度（デフォルトの割り当ては 8 MB）。

表 *3 : 112* コア *Cisco DNA Center* アプライアンスのハードウェア仕様

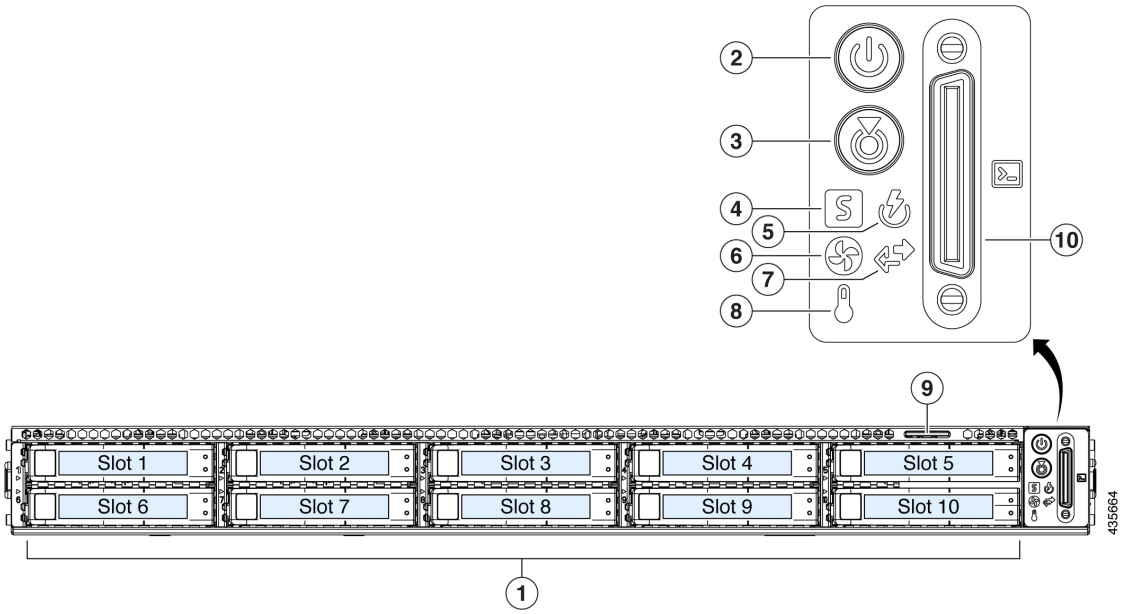
機能	説明
シャーシ	4 ラックユニット（4RU）シャーシ。
プロセッサ	2 個の 28 コア Intel Xeon Platinum 8176 2.1 GHz プロセッサを搭載した CPU モジュール X 2
メモリ	32 GB DDR4 2666 MHz RDIMM X 24
ストレージ	• RAID 1 で 480 GB X 2 • RAID 1 で 3.8 TB X 2 • 1.9 TB（RAID 10）X 16
ディスク管理（RAID）	• ドライブベイ 1 および 2 の RAID 1 • スロット 3 ～ 18 の RAID 10 • ドライブベイ 19 および 20 の RAID 1

機能	説明
ネットワークおよび管理 I/O	サポートされるコネクタ： • Intel X710-DA2 NIC 上の 10 Gbps イーサネットポート X 2 • 10 Base-T Gbps イーサネットポート X 2 • 1 ギガビットイーサネット管理ポート 次のコネクタを使用できますが、通常は Cisco DNA Center の日常業務では使用されません。 • RS-232 シリアル ポート（RJ-45 コネクタ）X 1 • VGA（DB-15）コネクタ X 1 • USB 3.0 コネクタ X 3 • USB 2.0 2 個、VGA（DB-15）1 個、シリアル（RS-232）RJ-45 コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1 10 Gbps イーサネットポート 4 個を提供する Intel X710-DA4 NIC は、今回の Cisco DNA Center リリースでは無効ですが、今後の製品リリースで有効になります。ご注意ください。
電源	1600 W AC 電源装置 X 4。 3+1 の冗長構成（Cisco Integrated Management Controller での設定が必須）。
冷却	前面から背面冷却のそれぞれに 2 個のファンがある 4 個ホットスワップ ファン モジュールです。
ビデオ	60 Hz で最大 1600 X 1200、16 bpp の VGA ビデオ解像度、最大 256 MB のビデオメモリ。

前面パネルと背面パネル

次の図と表では Cisco DNA Center アプライアンスの前面パネルと背面パネルについて説明します。

図 *1 : 44* および *56* コアアプライアンスの前面パネル

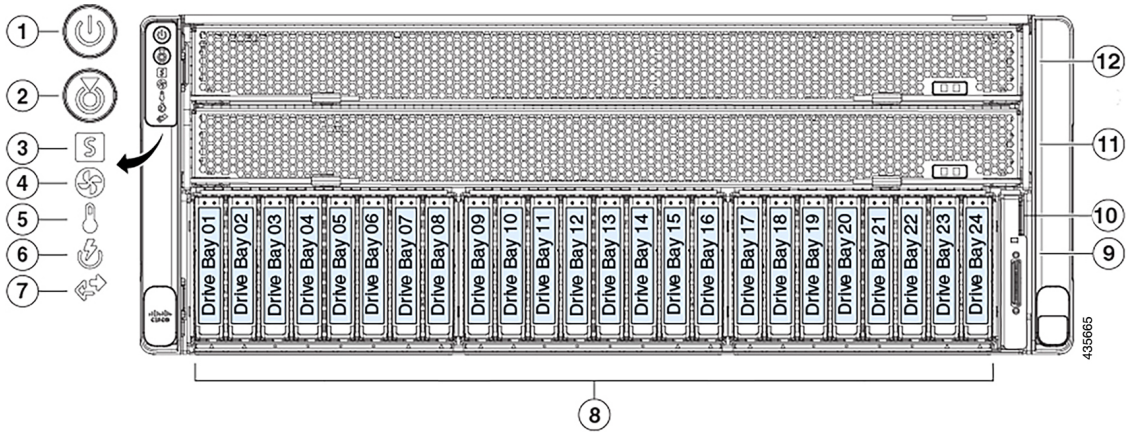


コンポーネント	説明
1	このアプライアンスでは次のとおり合計 10 個のドライブを使用できます。 • 480 GB SAS SSD X 2（スロット 1 および 2）。 • 1.9 TB SATA SSD X 8（スロット 3 ～ 10）。 取り付けられたドライブにはそれぞれ、障害 LED とアクティビティ LED が付いています。 ドライブ障害 LED の状態とその説明： • 消灯：ドライブは正常に動作中です。 • オレンジ：ドライブに障害が発生しています。 • オレンジの点滅：ドライブの再構成中です。 ドライブアクティビティ LED の状態とその説明： • 消灯：スレッドにドライブが存在しません（アクセスなし、障害なし）。 • 緑：ドライブの準備が完了しています。 • 緑の点滅：ドライブはデータの読み取り中または書き込み中です。

コンポーネント	説明
2	電源ボタン/電源ステータス LED LED の状態とその説明： • 消灯：アプライアンスに AC 電力が供給されていません。 • オレンジ：アプライアンスはスタンバイ電源モードです。Cisco Integrated Management Controller（CIMC）と一部のマザーボード機能にだけ電力が供給されています。 • 緑：アプライアンスはメイン電源モードです。すべてのサーバコンポーネントに電力が供給されています。
3	ユニット識別ボタンと LED。LED の状態とその説明： • 消灯：ユニット識別機能は非アクティブです。 • 青：ユニット識別 LED はアクティブです。
4	システムステータス LED。LED の状態とその説明： • 緑：アプライアンスは正常動作状態で稼働しています。 • 緑の点滅：アプライアンスはシステムの初期化とメモリチェックを行っています。 • オレンジの点灯：アプライアンスは縮退運転状態になっています。次の 1 つ以上が原因の可能性があります。 • 電源装置の冗長性が失われている。 • CPU が一致しない。 • 少なくとも 1 つの CPU に障害が発生している。 • 少なくとも 1 つの DIMM に障害が発生している。 • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 • オレンジの点滅（2 回）：システムボードで重度の障害が発生しています。 • オレンジの点滅（3 回）：メモリ（DIMM）で重度の障害が発生しています。 • オレンジの点滅（4 回）：CPU で重度の障害が発生しています。

コンポーネント	説明
5	電源装置ステータス LED。LED の状態とその説明： • 緑：すべての電源装置が正常に動作しています。 • オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。
6	ファンステータス LED。LED の状態とその説明： • 緑：すべてのファンモジュールが正常に動作中です。 • オレンジの点灯：1 つのファンモジュールに障害が発生しています。 • オレンジの点滅：重大な障害。2 つ以上のファンモジュールに障害が発生しています。
7	ネットワーク リンク アクティビティ LED。LED の状態とその説明： • 消灯：イーサネットリンクがアイドル状態です。 • 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。 • 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。
8	温度ステータス LED。LED の状態とその説明： • 緑：アプライアンスは正常温度で稼働中です。 • オレンジの点灯：1 つ以上の温度センサが警告しきい値を超過しています。 • オレンジの点滅：1 つ以上の温度センサが重大しきい値を超過しています。
9	引き抜きアセット タグ
10	KVM コネクタ。USB 2.0 コネクタ X 2、VGA コネクタ X 1、シリアルコネクタ X 1 を装備した KVM ケーブルで使用します。

図 *2 : 112* コアアプライアンスの前面パネル



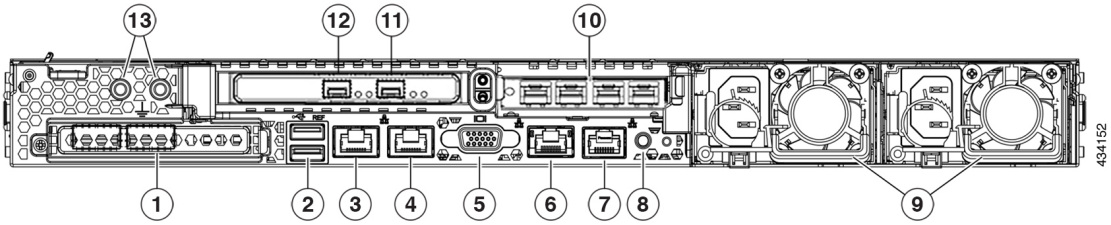
コンポーネント	説明
1	電源ボタン/電源ステータス LED LED の状態とその説明： • 消灯：アプライアンスに AC 電力が供給されていません。 • オレンジ：アプライアンスはスタンバイ電源モードです。CIMC と一部のマザーボード機能にだけ電力が供給されています。 • 緑：アプライアンスはメイン電源モードです。すべてのサーバコンポーネントに電力が供給されています。
2	ユニット識別ボタンと LED。LED の状態とその説明： • 消灯：ユニット識別機能は非アクティブです。 • 青：ユニット識別 LED はアクティブです。

コンポーネント	説明
3	システムステータス LED。LED の状態とその説明： • 緑：アプライアンスは正常動作状態で稼働しています。 • オレンジの点灯：アプライアンスは縮退運転状態になっています。次の 1 つ以上が原因の可能性があります。 • 電源装置の冗長性が失われている。 • CPU が一致しない。 • 少なくとも 1 つの CPU に障害が発生している。 • 少なくとも 1 つの DIMM に障害が発生している。 • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 • オレンジの点滅：アプライアンスは重大な障害が発生している状態であり、次の 1 つ以上が原因の可能性があります。 • ブートの失敗 • 修復不能なプロセッサーまたはバス エラーが検出されました • 過熱状態
4	ファンステータス LED。LED の状態とその説明： • 緑：すべてのファンモジュールが正常に動作中です。 • オレンジの点灯：ファンモジュールが縮退運転状態にあります。1 つのファン モジュールに障害があります。 • オレンジの点滅：2 つ以上のファンモジュールに障害があります。
5	温度ステータス LED。LED の状態とその説明： • 緑：アプライアンスは正常温度で稼働中です。エラーが検出されませんでした。 • オレンジの点灯：1 つ以上の温度センサが警告しきい値を超過しています。 • オレンジの点滅：1 つ以上の温度センサで重要な回復不能なしきい値を超えました。

コンポーネント	説明
6	電源装置ステータス LED。LED の状態とその説明： • 緑：すべての電源装置が正常に動作しています。 • オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 • オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。
7	ネットワーク リンク アクティビティ LED。LED の状態とその説明： • 消灯：イーサネット LOM ポートリンクがアイドル状態です。 • 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。
8	このアプライアンスでは次のとおり合計 20 個のドライブを使用できます。 • 480 GB SATA SSD X 2（ドライブベイ 1 および 2 内）。 • 1.9 TB SATA SSD X 16（スロット 3 ～ 18）。 • 3.8 TB SATA SSD X 2（ドライブベイ 19 および 20）。 （注） ドライブベイ 21 ～ 24 は、このアプライアンスでは使用されません。 取り付けられたドライブにはそれぞれ、障害 LED とアクティビティ LED が付いています。 ドライブ障害 LED の状態とその説明： • 消灯：ドライブは正常に動作中です。 • オレンジ：ドライブに障害が発生しています。 • オレンジの点滅：ドライブの再構成中です。 ドライブアクティビティ LED の状態とその説明： • 消灯：スレッドにドライブが存在しません（アクセスなし、障害なし）。 • 緑：ドライブの準備が完了しています。 • 緑の点滅：ドライブはデータの読み取り中または書き込み中です。
9	KVM コネクタ。USB 2.0 コネクタ X 2、VGA コネクタ X 1、シリアルコネクタ X 1 を装備した KVM ケーブルで使用します。

コンポーネント	説明
10	引き抜きアセットタグ。
11	CPU モジュールベイ 1。
12	CPU モジュールベイ 2。

図 *3 : 44*および *56* コアアプライアンスの背面パネル



コンポーネント	説明
1	モジュラ LAN-on-motherboard（mLOM）カード ベイ（x16 PCIe レーン）
2	USB 3.0 ポート X 2
3	1 Gbps/10 Gbps 管理ポート（1、eno1、ネットワークアダプタ 1）：このイーサネットポートはアプライアンスのマザーボードに搭載されており、リンクパートナーの機能に応じて 1 Gbps、10 Gbps をサポートできます。これは背面パネルでは **1** 、Maglev 設定ウィザードでは eno1 とネットワークアダプタ 1 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 このポートにはリンクステータス LED とリンク速度 LED が付いています。ステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 速度 LED の状態とその説明： • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。

コンポーネント	説明
4	1 Gbps/10 Gbps クラウドポート（2、eno2、ネットワークアダプタ 2）：このイーサネットポートはアプライアンスのマザーボードに搭載されており、リンクパートナーの機能に応じて 1 Gbps、10 Gbps をサポートできます。これは背面パネルでは **2** 、Maglev 設定ウィザードでは eno2 とネットワークアダプタ 2 として識別されます。このポートは、10 Gbps エンタープライズポートではインターネット接続ができない場合に任意で代用します。インターネットに接続しているインターネットサーバまたはプロキシサーバに接続します。 このポートにはリンクステータス LED とリンク速度 LED が付いています。リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックはありません。 速度 LED の状態とその説明： • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。
5	VGA ビデオポート（DB-15）。

コンポーネント	説明
6	1 Gbps CIMC ポート：これは VGA ビデオポートの右側にある組み込みポートで、RJ45 シリアルポートの左側にあります。アプライアンスの CIMC GUI に対するブラウザアクセスを有効にしていると、IP アドレスが割り当てられます（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。このポートは、アプライアンスのシャーシおよびソフトウェアのアウトオブバンド管理用に予約されています。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 このポートにはリンクステータス LED とリンク速度 LED が付いています。リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 速度 LED の状態とその説明： • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。
7	シリアル ポート（RJ-45 コネクタ）
8	ユニット背面の ID ボタンと LED
9	電源装置（最大 2 台、1+1 の冗長構成）各電源装置には、電源障害 LED と AC 電源 LED が付いています。 障害 LED の状態とその説明： • 消灯：電源装置は正常に動作中です。 • オレンジの点滅：イベント警告しきい値に達しましたが、電源装置は動作し続けています。 • オレンジの点灯：重大障害しきい値に達し、電源装置がシャットダウンしています（ファンの障害や過熱状態など）。 AC 電源 LED の状態とその説明： • 消灯：電源に AC 電力が供給されていません。 • 緑の点灯：AC 電力供給も、DC 出力も OK です。 • 緑の点滅：AC 電力供給は OK ですが、DC 出力は使用できません。 詳細については「電力仕様」を参照してください。

コンポーネント	説明
10	アプライアンスの PCIe ライザ 2/スロット 2 に設置されている Intel X710-DA4 ネットワーク インターフェイス カード（NIC）。このカードは、この Cisco DNA Center リリースでは無効になっており、今後のリリースで有効になることに注意してください。 **重要** このカードがアプライアンスで有効になっている場合は、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、ネットワーク インターフェイス カードの無効化 （78 ページ）を参照してください。
11	10 Gbps クラスタポート（enp94s0f1、ネットワークアダプタ 4）：これはアプライアンス PCIe ライザ 1/スロット 1 の Intel X710-DA2 NIC の右側にある 10 Gbps ポートです。これは Maglev 設定ウィザードでは enp94s0f1 とネットワークアダプタ 4 として識別されます。このポートをクラスタ内のほかのノードに接続しているスイッチに接続します。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 リンク速度 LED の状態とその説明： • 消灯：リンク速度は 100 Mbps 以下です。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 （注） 低速でも動作可能ですが、エンタープライズポートとクラスタポートは 10 Gbps でのみ動作するように設計されています。

コンポーネント	説明
12	10 Gbps エンタープライズポート（enp94s0f0、ネットワークアダプタ 3）：これはアプライアンス PCIe ライザ 1/スロット 1 の Intel X710-DA2 NIC の左側にある 10 Gbps ポートです。これは Maglev 設定ウィザードでは enp94s0f0 とネットワークアダプタ 3 として識別されます。このポートを、エンタープライズ ネットワークに接続しているスイッチに接続します。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 速度 LED の状態とその説明： • 消灯：リンク速度は 100 Mbps 以下です。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 （注） 低速でも動作可能ですが、エンタープライズポートとクラスタポートは 10 Gbps でのみ動作するように設計されています。
13	二重孔アース ラグ用ネジ穴。

図 *4 : 112* コアアプライアンスの背面パネル

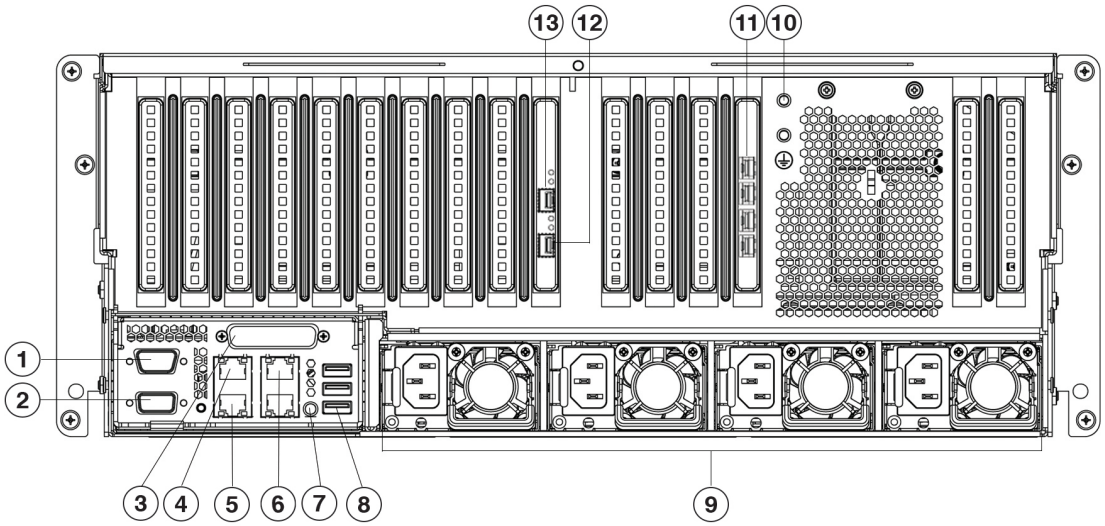
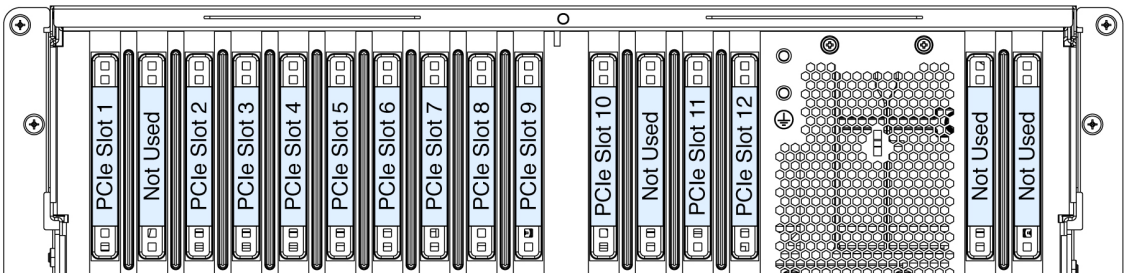


図 *5 : 112* コアアプライアンスの背面パネルのスロット



コンポーネント	説明
1	シリアル ポート COM 1（DB-9 コネクタ）
2	VGA ビデオ ポート（DB-15 コネクタ）
3	現時点ではサポートされていません。
4	1 Gbps/10 Gbps 管理ポート（1、enp53s0f0、ネットワークアダプタ 1）：このイーサネットポートはアプライアンスのマザーボードに組み込まれており、リンクパートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。これは背面パネルでは **1** 、Maglev 設定ウィザードでは enp53s0f0 とネットワークアダプタ 1 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 このポートにはリンクステータス LED とリンク速度 LED が付いています。ステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 速度 LED の状態とその説明： • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。

コンポーネント	説明
5	1 Gbps/10 Gbps クラウドポート（2、enp53s0f1、ネットワークアダプタ 2）：このイーサネットポートはアプライアンスのマザーボードに搭載されており、リンクパートナーの機能に応じて 1 Gbps、10 Gbps をサポートできます。これは背面パネルでは **2** 、Maglev 設定ウィザードでは enp53s0f1 とネットワークアダプタ 2 として識別されます。このポートは、10 Gbps エンタープライズポートではインターネット接続ができない場合に任意で代用します。インターネットに接続しているインターネットサーバまたはプロキシサーバに接続します。 このポートにはリンクステータス LED とリンク速度 LED が付いています。リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックはありません。 速度 LED の状態とその説明： • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。

コンポーネント	説明
6	1 Gbps CIMC ポート：これは管理ポートの右側にある10/100/1000イーサネット専用管理ポート（Base-T）です。背面パネルでは**3**として識別されます。アプライアンスの CIMC GUI に対するブラウザアクセスを有効にしていると、このポートに IP アドレスが割り当てられます（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。アプライアンスのシャーシおよびソフトウェアのアウトオブバンド管理用に予約されています。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 このポートにはリンクステータス LED とリンク速度 LED が付いています。リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 速度 LED の状態とその説明： • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。
7	背面 ID ボタン/LED
8	USB 3.0 ポート× 3
9	電源装置 1 ～ 4：ホットスワップ可能、3+1 の冗長構成（CIMC で設定） 詳細については「電力仕様」を参照してください。
10	二重孔アース ラグ用ネジ穴。
11	アプライアンスの PCIe ライザ 2/スロット 12 に設置されている Intel X710-DA4 ネットワーク インターフェイス カード（NIC）。このカードは、この Cisco DNA Center リリースでは無効になっており、今後のリリースで有効になることに注意してください。 **重要** このカードがアプライアンスで有効になっている場合は、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「ネットワーク インターフェイス カードの無効化 （78 ページ）」を参照してください。

コンポーネント	説明
12	10 Gbps クラスタポート（enp69s0f1、ネットワークアダプタ 4）：これはアプライアンスの PCIe スロット 9 に搭載されている Intel X710-DA2 NIC の下にある 10 Gbps ポートです。これは Maglev 設定ウィザードでは enp69s0f1 とネットワークアダプタ 4 として識別されます。このポートをクラスタ内のほかのノードに接続しているスイッチに接続します。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 リンク速度 LED の状態とその説明： • 消灯：リンク速度は 100 Mbps 以下です。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 （注） 低速でも動作可能ですが、エンタープライズポートとクラスタポートは 10 Gbps でのみ動作するように設計されています。

コンポーネント	説明
13	10 Gbps エンタープライズポート（enp69s0f0、ネットワークアダプタ 3）：これはアプライアンスの PCIe スロット 9 に搭載されている Intel X710 DA2 NIC の下にある 10 Gbps ポートです。これは Maglev 設定ウィザードでは enp69s0f0 とネットワークアダプタ 3 として識別されます。このポートを、エンタープライズ ネットワークに接続しているスイッチに接続します。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態とその説明： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 速度 LED の状態とその説明： • 消灯：リンク速度は 100 Mbps 以下です。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 （注） 低速でも動作可能ですが、エンタープライズポートとクラスタポートは 10 Gbps でのみ動作するように設計されています。

物理仕様

次の表にアプライアンスの物理仕様を示します。別途指定のない限り、44、56、および 112 コアアプライアンスにはこの仕様が適用されます。

表 *4 :* 物理仕様

説明	仕様
高さ	44 および 56 コアアプライアンス：4.32cm（1.7 インチ） 112 コアアプライアンス：17.6cm（6.9 インチ）

説明	仕様
幅	44 および 56 コアアプライアンス： • ハンドルなし：43.0 cm（16.9 インチ） • ハンドルを含む：48.3 cm（19.0 インチ） 112 コアアプライアンス：48.3cm（19.0 インチ）
奥行（長さ）	44 および 56 コアアプライアンス： • ハンドルなし：75.6 cm（29.8 インチ） • ハンドルを含む：78.7 cm（30.98 インチ） 112 コアアプライアンス：83.1cm（32.7 インチ）
前面のスペース	76 mm（3 インチ）
周囲と側面の間に必要な隙間	25 mm（1 インチ）
背面のスペース	152 mm（6 インチ）
最大重量（フル装備シャーシ）	44 および 56 コアアプライアンス：17.0kg（37.5 ポンド） 112 コアアプライアンス：66.2kg（146 ポンド）

環境仕様

次の表に Cisco DNA Center アプライアンスの環境仕様を示します。別途指定のない限り、44、56、および 112 コアアプライアンスにはこの仕様が適用されます。

表 *5:* 環境仕様

説明	仕様
動作時温度	41 ～ 95 °F（5 ～ 35 °C） 海抜 305 m（1000 フィート）ごとに最高温度が 1°C 低下します。
非動作時温度（アプライアンスが倉庫にあるか運送中の場合）	–40 ～ 149 °F（–40 ～ 65 °C）
湿度（RH）（動作時）	10 ～ 90%（28°C（82°F）時、結露なし）

説明	仕様
非動作時湿度（RH）（アプライアンスが倉庫にあるか運送中の場合）	5 ～ 93%（28°C（82°F）時）
動作時高度	0 ～ 10,000 フィート（0 ～ 3,048 m）
非動作時高度（アプライアンスが倉庫にあるか運送中の場合）	0 ～ 40,000 フィート（0 ～ 12,192 m）
音響出力レベル、ISO7779 に基づく A 特性 LWAd（B）を測定、23°C（73°F）での動作時	44 および 56 コアアプライアンス：5.5 112 コアアプライアンス： • 最低設定：7.08 • 標準設定：7.67 • 最大設定：8.24
音圧レベル、ISO 7779 に基づく A 特性 LpAm（dBA）を測定、23°C（73 °F）での動作時	44 および 56 コアアプライアンス：40 112 コアアプライアンス： • 最低設定：57.6 • 標準設定：63.5 • 最大設定：70.5

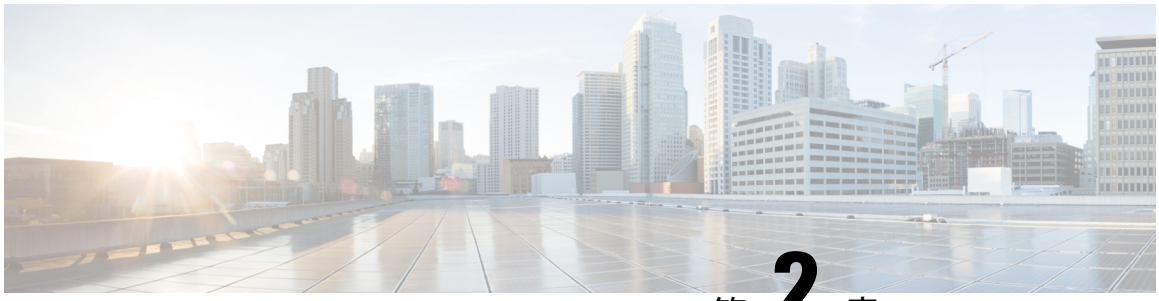
電力仕様

Cisco DNA Center アプライアンスに同梱されている電源の仕様は、下表に一覧表示されています。44 および 56 コアアプライアンスには、770W 電源モジュール（シスコ製品番号 UCSC-PSU1-770W）が 2 個付属しており、112 コアアプライアンスには 1600W AC 電源モジュール（シスコ製品番号 UCSC-PSU1-1600W）が 4 個付属しています。別途指定のない限り、両方の電源装置にこの仕様が適用されます。

表 *6 : AC* 電源の仕様

説明	仕様
AC 入力電圧	770 W： • 公称範囲：100 ～ 120 VAC、200 ～ 240 VAC • 範囲：90 ～ 132 VAC、180 ～ 264 VAC 1600 W： • 公称範囲：AC 200 ～ 240 V • 範囲：AC 180 ～ 264 V
AC 入力周波数	公称範囲：50 ～ 60 Hz （範囲：47 ～ 63 Hz）
最大 AC 入力電流	770 W： • 100 VAC で 9.5 A • 208 VAC で 4.5 A 1600 W：9.5 A @ AC 200 V
最大入力電圧	770 W：950 VA @ AC 100 V 1600 W：1250 VA @ AC 200 V
PSU あたりの最大出力電力	770 W @ AC 100 ～ 120 V 1600 W：AC 200 ～ 240 V
最大突入電流	770 W：15 A @ 35°C 1600 W：15 A @ 35°C
最大保留時間	770 W：12 ms 1600 W：80 ms @
電源装置の出力電圧	12 VDC
電源装置のスタンバイ電圧	12 VDC
効率評価	Climate Savers Platinum Efficiency（80 Plus Platinum 認証済み）
フォーム ファクタ	RSP2
入力コネクタ	IEC320 C14

（注） 次の URL にある Cisco UCS Power Calculator を使用すると、ご使用のアプライアンス設定の電源に関する詳細情報を取得できます。http://ucspowercalc.cisco.com



第 2 章

導入の計画

プランニング ワークフロー

Cisco DNA Center アプライアンスの設置、設定、セットアップを試みる前に、次の計画と情報収集のタスクを実行する必要があります。これらのタスクを完了したあと、データセンターにアプライアンスを物理的に設置すると続行できます。

（注） 詳細については、「Cisco DNA CenterおよびCisco SD-Access」を参照してください。

1. スタンドアロン設置とクラスタ設置で推奨されるケーブル接続とスイッチングの要件を確認します。詳細については「インターフェイスケーブル接続」を参照してください。
2. アプライアンスの設定時に適用するIPアドレッシング、サブネット化などのIPトラフィック情報を収集します。詳細については「必要なIPアドレスおよびサブネット」を参照してください。
3. 必要なWebベースのリソースに対するアクセスのソリューションを準備します。詳細については「必要なインターネット URL と完全修飾ドメイン名」と「インターネットへのアクセスを保護する」を参照してください。

4. Cisco DNA Center トラフィックのファイアウォールとセキュリティポリシーを再設定します。詳細については「必要なネットワーク ポート」を参照してください。Cisco DNA Center を使用して Cisco SD-Access（SD-Access）ネットワークを管理している場合は「必要なポートとプロトコル： Cisco SD-Access」も参照してください。
5. アプライアンスの構成時と初回設定時に使用される追加情報を収集します。詳細については「必須の設定情報」と「必要な初期設定情報」を参照してください。

Cisco DNA CenterおよびCisco SD-Access

Cisco SD-Access ファブリックアーキテクチャを使用するネットワークも含め、すべてのネットワークタイプで Cisco DNA Centerを使用できます。Cisco SD-Accessは、従来のネットワークをインテントベースのネットワークに変換します。これにより、ビジネスロジックがネットワークの物理的な部分になり、構成、プロビジョニング、トラブルシューティングなどの日常的なタスクを簡単に自動化できるようになります。Cisco SD-Access ソリューションは、ネットワークをビジネスニーズに合わせ、問題解決を改善し、セキュリティ侵害の影響を軽減するために必要な時間を短縮します。

Cisco SD-Access ソリューションの詳細については、このガイドの範囲外です。Cisco DNA Center で使用する Cisco SD-Access ファブリックアーキテクチャの実装を計画しているネットワークアーキテクトや管理者は、次のリソースから追加情報とガイダンスを入手できます。

- Cisco SD-Access と Cisco DNA の簡単な説明については、ホワイトペーパー『Cisco Digital Network Architecture – An Overview』を参照してください。
- 通常のネットワークのアプローチと技術では不可能なソリューションを自動化するために、Cisco DNA Center が Cisco SD-Access を活用する方法については、『Software Defined Access: Enabling Intent-Based Networking』を参照してください。
- ネットワークで Cisco SD-Access を実装する方法を示す検証済みデザインについては、最新バージョンの『Cisco Software-Defined Access Design Guide』を参照してください。
- Cisco SD-Access アクセスセグメンテーションを使用したネットワークセキュリティの強化に関するガイダンスについては、『Software-Defined Access Segmentation Design Guide』を参照してください。
- ワイヤレス固有の設計ガイダンスについては、『SD-Access Wireless Design and Deployment Guide』を参照してください。
- Cisco DNA Center での SDA の展開に関するガイダンスは、『Software-Defined Access Deployment Guide』を参照してください。
- Cisco DNA Center と Cisco SD-Access ソリューションの基盤であるデジタル ネットワークアーキテクチャの詳細と、この革新的なアーキテクチャで他のシスコ製品やソリューション、サードパーティの製品やソリューションが果たす役割については、『Cisco DNA Design Zone』を参照してください。

- その他の設計ガイド、導入ガイド、ホワイトペーパーについては、『Cisco Design Zone』を参照してください。

インターフェイスケーブル接続

次のタイプのネットワークアクセスを提供するスイッチに、アプライアンスのポートを接続します。Cisco DNA Center の機能に必要なため、最低でも企業およびクラスタのポートインターフェイスを設定する必要があります。

（注） 44、56、および 112 コアアプライアンスのポートに割り当てられているインターフェイス名が異なります。2 つのインターフェイス名が指定された場合は、1 つ目が 44 および 56 コアアプライアンスに適用され、2 つ目が 112 コアアプライアンスに適用されます。

- **（オプション）1 Gbps または 10 Gbps の管理ポート（1、eno1/enp53s0f0、ネットワークアダプタ 1）**：このポート（背面パネルに **1** というラベル付き）が Cisco DNA Center の GUI にアクセスするため、ユーザはアプライアンス上でソフトウェアを使用できます。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
- **（オプション）1 Gbps または 10 Gbps のクラウドポート（eno2/enp53s0f1、ネットワークアダプタ 2）**：このポートは、背面パネルに **2** というラベルが付いており、オプションです。10 Gbps のエンタープライズポート（enp94s0f0/enp69s0f0、ネットワークアダプタ 3）を使用してアプライアンスをインターネット（インターネット プロキシ サーバを含む）に接続できない場合にのみ使用してください。クラウドポートを使用する必要がある場合は、インターネットプロキシサーバに接続しているスイッチに接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
- **（必須）10 Gbps エンタープライズポート（enp94s0f0/enp69s0f0、ネットワークアダプタ 3）**：このポートの目的は、Cisco DNA Center がネットワークと通信し、ネットワークを管理できるようにすることです。このポートを、エンタープライズネットワークに接続しているスイッチに接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
  - 44 と 56 のコアアプライアンスでは、これはアプライアンスの PCIe スロット 1 に搭載されている Intel X710-DA2 NIC の左側にあるポートです。
  - 112 コアアプライアンスでは、これはアプライアンスの PCIe スロット 12 に搭載されている Intel X710-DA2 NIC の上にある 10 Gbps ポートです。
- **（必須）10 Gbps クラスタポート（enp94s0f1 または enp69s0f1、ネットワークアダプタ 4）**：このポートの目的は、クラスタ内のマスタノードとアドオンノード間の通信を可能にすることです。このポートをクラスタ内の他のノードに接続しているスイッチに接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

- 44 および 56 コアアプライアンスでは、これはアプライアンスの PCIe スロット 1 に搭載されている Intel X710-DA2 NIC の右側にあるポートです。
- 112 コアアプライアンスでは、これはアプライアンスの PCIe スロット 12 に搭載されている Intel X710-DA2 NIC の下にある 10 Gbps ポートです。

アプライアンス設定中、Maglev設定ウィザードは、クラスタリンクオプションをインターフェイスに割り当てるまで続行できません。ポート enp94s0f1 または enp69s0f1 をクラスタリンクとして指定するようお勧めします。ただし、クラスタリンクとしてマークされたインターフェイスは、設定が完了した後は変更できないことに注意してください。後で、クラスタリンクとしてマークされたインターフェイスを変更する必要がある場合は、アプライアンスを再設定する必要があります。将来的に3ノードクラスタに拡張できるようにするため、IPアドレスを使用してクラスタポートを設定するようお勧めします。また、クラスタ リンク インターフェイスがスイッチポートに接続されており、稼働状態になっていることを確認します。

（注） Cisco DNA Center アプライアンスのイメージを作成しなおすために完了する必要があるタスクの説明については「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。

- **（オプション、ただし強く推奨）1 Gbps CIMC ポート**：このポートで、Cisco Integrated Management Controller（CIMC）アウトオブバンド アプライアンス管理インターフェイスとそのGUIにブラウザがアクセスします。その目的は、アプライアンスとそのハードウェアを管理できるようにすることです。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用してIPアドレスを1つ設定します。

次の図は、シングルノード Cisco DNA Center クラスタで推奨される接続を示しています。

図 *6*：シングルノードクラスタで推奨されるケーブル接続：*44* および *56* コアアプライアンス

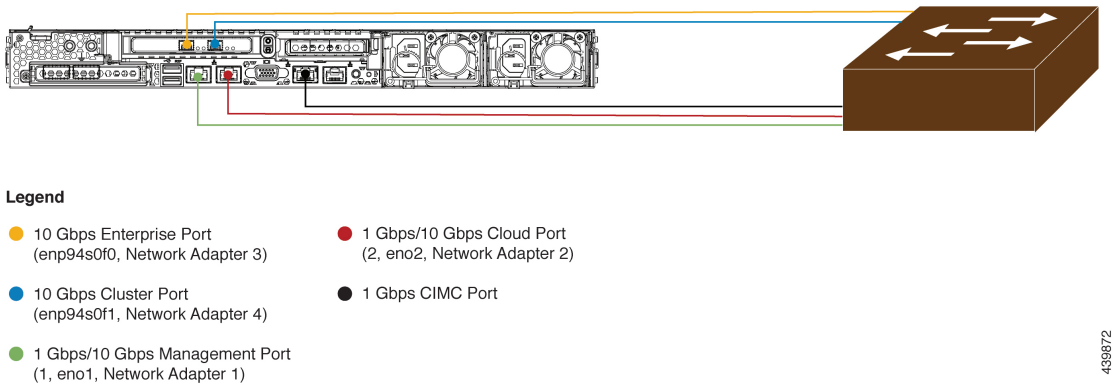
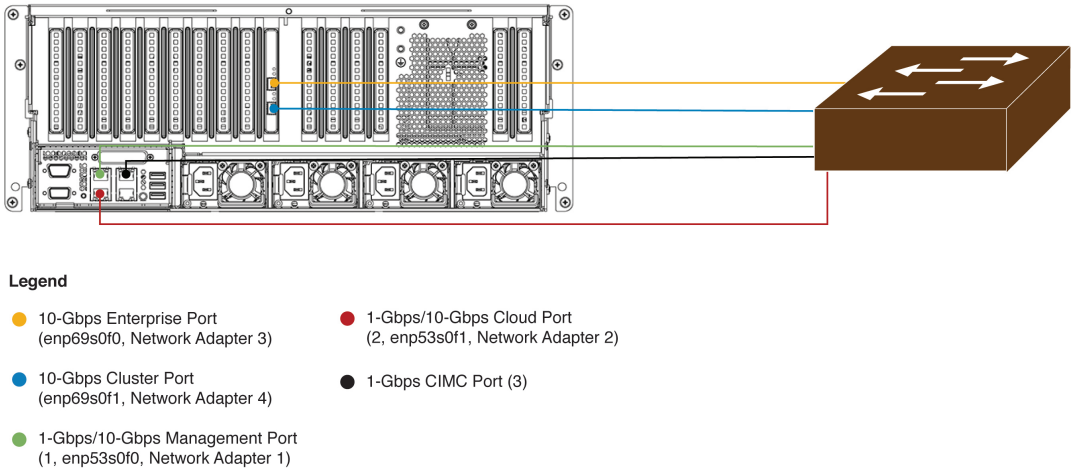
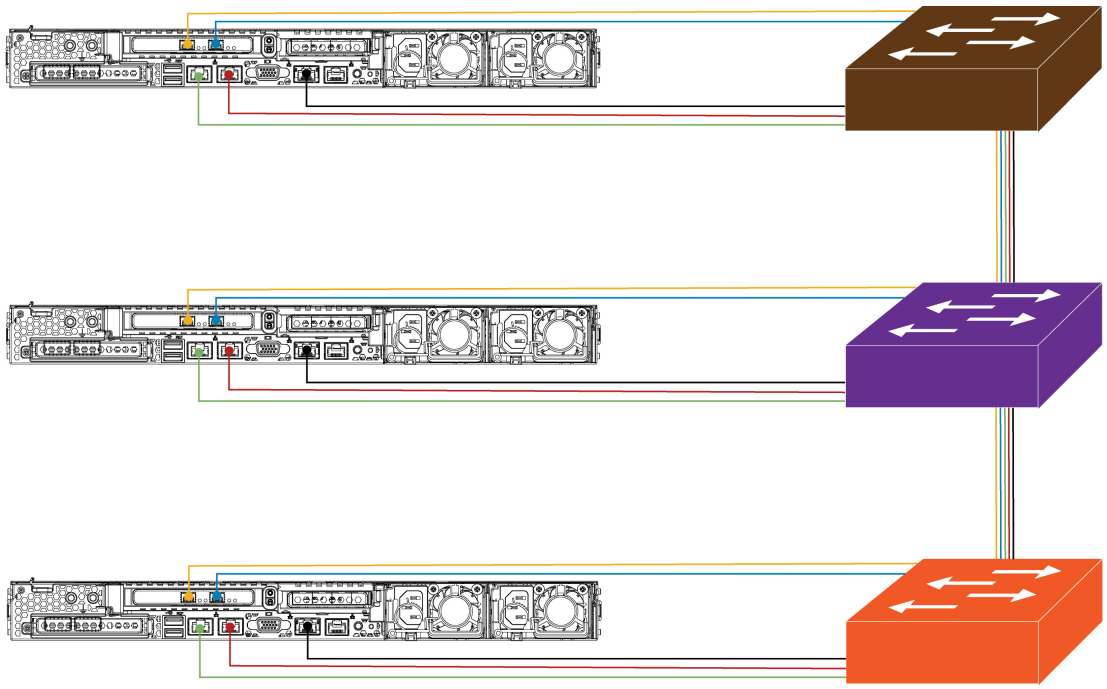


図 *7:* シングルノードクラスタで推奨されるケーブル接続：*112* コアアプライアンス



次の図は、3 ノードの Cisco DNA Center クラスタで推奨される接続を示しています。3 ノードクラスタ内の各ノードの接続は 1 つ以外すべて、シングルノードクラスタの場合と同じであり、同じポートを使用します。例外はクラスタポート（enp94s0f1 または enp69s0f1、ネットワークアダプタ 4）であり、これは 3 ノードクラスタ内の各ホストが他のホストと通信できるようにするために必要です。

図 *8 : 3* ノードクラスタで推奨されるケーブル接続：*44* および *56* コアアプライアンス

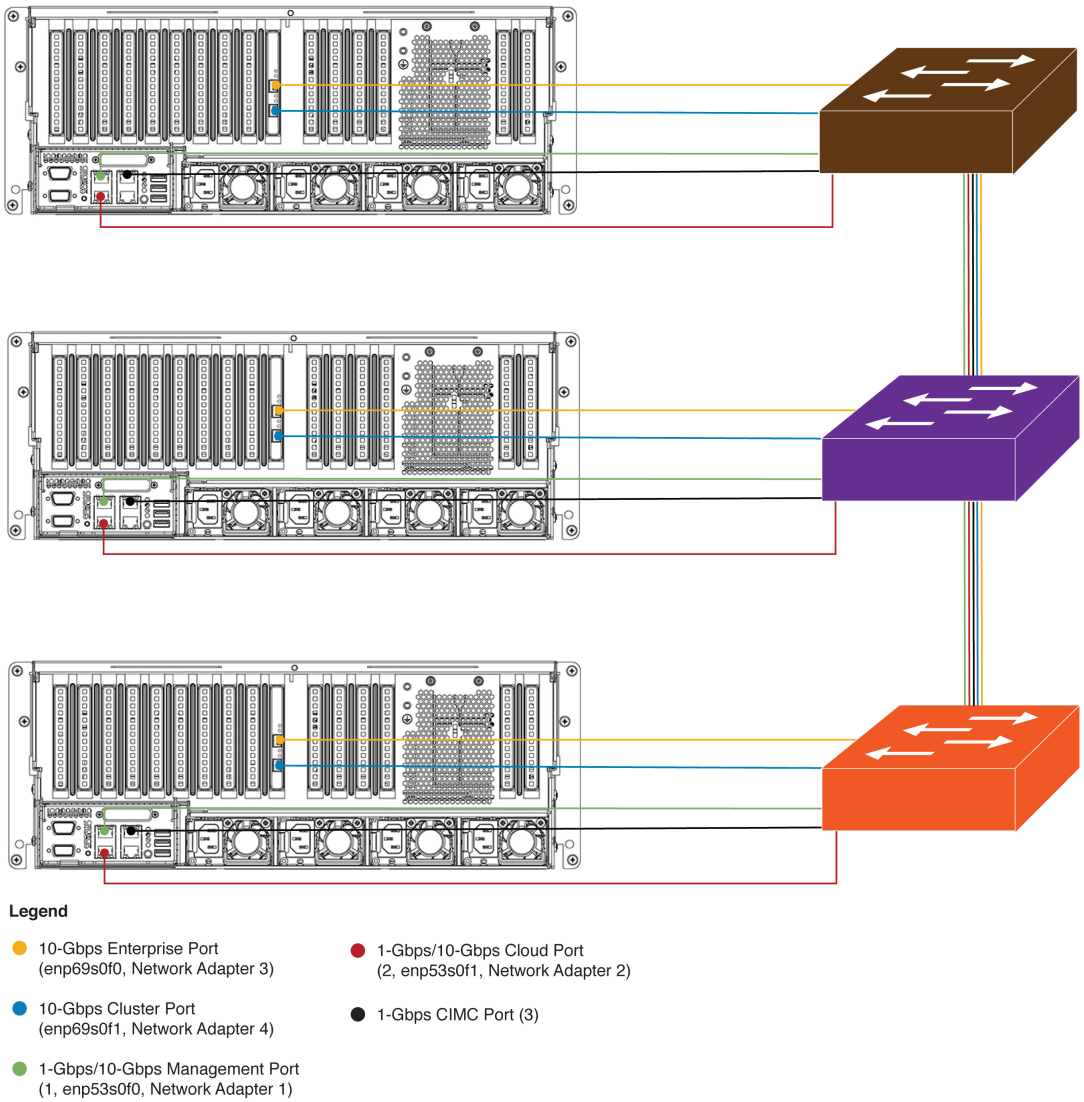


Legend

- 10 Gbps Enterprise Port (enp94s0f0, Network Adapter 3)
- 10 Gbps Cluster Port (enp94s0f1, Network Adapter 4)
- 1 Gbps/10 Gbps Management Port (1, eno1, Network Adapter 1)
- 1 Gbps/10 Gbps Cloud Port (2, eno2, Network Adapter 2)
- 1 Gbps CIMC Port

439813

図 *9 : 3* ノードクラスタで推奨されるケーブル接続：*112* コアアプライアンス



各ポートの詳細については、前面パネルと背面パネルにあるシャーシの背面パネルの図と付属の説明を参照してください。

（注） マルチノードクラスタの導入では、すべてのメンバノードを同じサイトの同じネットワーク内にする必要があります。アプライアンスは、複数のネットワークまたはサイト間でのノードの配布をサポートしていません。

10 Gbps のエンタープライズポートとクラスタポートを接続する場合は、ポートで次のメディアタイプのみがサポートされていることに注意してください。

- SFP-10G-SR（ショートレンジ、MMF）

- SFP-10G-SR-S（ショートレンジ、MMF）
- SFP-10G-LR（ロングレンジ、SMF）
- SFP-H10GB-CU1M（Twinax ケーブル、パッシブ、1 m）
- SFP-H10GB-CU3M（Twinax ケーブル、パッシブ、3 m）
- SFP-H10GB-CU5M（Twinax ケーブル、パッシブ、5 m）
- SFP-H10GB-CU7M（Twinax ケーブル、パッシブ、7 m）
- SFP-H10GB-ACU7M（Twinax ケーブル、アクティブ、7 m）

必要な IP アドレスおよびサブネット

設置を開始する前に、使用する予定の各アプライアンスポートに割り当てるのに十分な IP アドレスがネットワークにあることを確認する必要があります。アプライアンスをシングルノードクラスタとしてインストールするか、3 ノードクラスタのマスタまたはアドオンノードとしてインストールするかによって、次のアプライアンスポート（NIC）アドレスが必要になります。

- **エンタープライズ ポート アドレス（Enterprise Port Address）（必須）**：サブネットマスクを持つ 1 つの IP アドレス。
- **クラスタポートアドレス（Cluster Port Address）（必須）**：サブネットマスクを持つ 1 つの IP アドレス。
- **管理ポートアドレス（Management Port Address）（オプション）**：1 つの IP アドレスとサブネットマスク。
- **クラウドポートアドレス（Cloud Port Address）（オプション）**：サブネットマスクを持つ 1 つの IP アドレス。これはオプションのポートであり、エンタープライズポートを使用してクラウドに接続できない場合にのみ使用されます。この目的で使用する必要がある場合を除き、クラウドポートの IP アドレスは必要ありません。
- **CIMCポートアドレス（CIMC Port Address）（オプション、ただし強く推奨）**：サブネットマスクを持つ 1 つの IP アドレス。

（注） これらの要件で要求されるすべての IP アドレスは、有効な IPv4 ネットマスクを持つ物理 IPv4 アドレスである必要があります。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ます。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。

また、次の追加の IP アドレスと専用 IP サブネットが必要になります。これは、アプライアンスの設定時に入力が求められ、適用されます。

- [クラスタ仮想IPアドレス（Cluster Virtual IP Addresses）]：クラスタごとに設定されたネットワーク インターフェイスごとに 1 つの仮想 IP（VIP）アドレス。この要件は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可能性のある単一ノードクラスタに適用されます。設定するネットワークインターフェイスごとにVIPを指定する必要があります。各 VIP は、対応する設定済みインターフェイスの IP アドレスと同じサブネットからのものである必要があります。各アプライアンスには、エンタープライズ、クラスタ、管理、およびクラウドの 4 つのインターフェイスがあります。Cisco DNA Center の機能に必要なため、最低でも企業およびクラスタのポートインターフェイスを設定する必要があります。サブネットマスクと1つ以上の関連ゲートウェイまたはスタティックルートとともにIPをインターフェイスに指定すると、そのインターフェイスは設定されていると見なされます。設定時にインターフェイスを完全にスキップすると、そのインターフェイスは設定されていないと見なされます。

  次の点に注意してください。

  - 単一ノード設定で、今後 3 ノードクラスタに変換する予定がない場合は、VIP アドレスを指定する必要はありません。ただし、これを行う場合は、設定されているすべてのネットワークインターフェイスに VIP アドレスを指定する必要があります（3 ノードクラスタの場合と同様）。
  - 単一ノードクラスタのクラスタ内リンクがダウンすると、管理インターフェイスとエンタープライズ インターフェイスに関連付けられている VIP アドレスもダウンします。これが発生すると、クラスタ内リンクが復元されるまで Cisco DNA Center を使用できません（ソフトウェアイメージ管理（SWIM）と Cisco Identity Services Engine（ISE）の統合が動作しません。またネットワーク データ プラットフォーム（NDP）コレクタから情報を収集できないため、Cisco DNA アシュアランス データが表示されません）。

- **デフォルトゲートウェイ IP アドレス（Default Gateway IP Address）**：ネットワークの優先デフォルトゲートウェイのIPアドレス。他のルートがトラフィックに一致しない場合、トラフィックはこのIPアドレスを経由してルーティングされます。通常は、インターネットにアクセスするネットワーク設定内のインターフェイスにデフォルトゲートウェイを割り当てる必要があります。Cisco DNA Center の導入時に留意すべきセキュリティ上の考慮事項については、『Cisco Digital Network Architecture Center Security Best Practice Guide』を参照してください。

- **DNSサーバのIPアドレス（DNS Server IP Addresses）**：1 つ以上のネットワークの優先 DNS サーバの IP アドレス。設定時に、複数の DNS サーバの IP アドレスとネットマスクを、スペースで区切ったリストとして入力することによってそれらを指定できます。

- **（オプション）スタティックルートアドレス（Static Route Addresses）**：1 つ以上のスタティックルートの IP アドレス、サブネットマスク、およびゲートウェイ。設定時に、複数のスタティックルートの IP アドレス、ネットマスク、およびゲートウェイを、スペースで区切ったリストとして入力することによってそれらを指定できます。

  アプライアンスの任意のインターフェイスに対して1つ以上のスタティックルートを設定できます。デフォルトゲートウェイ以外の特定の方向でトラフィックをルーティングする場合は、スタティックルートを指定する必要があります。スタティックルートを持つ各イ

ンターフェイスは、IP route コマンドテーブルでトラフィックがルーティングされるデバイスとして設定されます。このため、トラフィックが送信されるインターフェイスとスタティックルートの方向を一致させることが重要です。

スタティックルートは、スイッチやルータで使用されるようなネットワークデバイスのルーティングテーブルでは推奨されません。この場合はダイナミック ルーティング プロトコルの方が適しています。ただし、他の方法では到達できないネットワークの特定の部分にアプライアンスがアクセスできるようにするには、必要に応じてそれらを追加する必要があります。

- [NTPサーバのIPアドレス（NTP Server IP Addresses）]：DNS 解決可能なホスト名、または 1 つ以上の Network Time PROTOCOL（NTP）サーバの IP アドレス。

  設定時に、複数の NTP サーバの IP やマスクまたはホスト名をスペースで区切ったリストとして入力することによって、それらを指定できます。実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定することを推奨します。

  これらのサーバは、事前にハードウェアを同期するときに指定し、クラスタ内の各アプライアンスでソフトウェアを設定する際に再度指定します。時刻の同期は、マルチホストクラスタ全体でのデータの精度と処理の調整にとって重要です。アプライアンスを実稼働環境に展開する前に、アプライアンスのシステムクロックの時刻が現在の時刻であること、および指定した NTP サーバが正確な時刻を維持していることを確認してください。アプライアンスを ISE と統合する予定の場合は、ISE がアプライアンスと同じ NTP サーバと同期していることも確認する必要があります。

- **サービスサブネット（Services Subnet）**：Cisco DNA アシュアランス などの内部アプリケーションサービス間の通信用 IP を管理し、取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。専用 IPv4 サービスサブネットは、Cisco DNA Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりすることはできません。サブネットの最小サイズは21 ビットです。IPv4 サービスサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。

  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 100.64.0.0/10

  詳細については、RFC 1918 では『Address Allocation For Private Internets』を、RFC 6598 では『IANA-Reserved IPv4 Prefix For Shared Address Space』を参照してください。

重要

- 有効なCIDRサブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20および172.17.61.0/20サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了したら、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません（詳細については「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）。

- **クラスタサービスサブネット（Cluster Services Subnet）**：データベースアクセス、メッセージバスなどのインフラストラクチャ サービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。専用 IPv4 クラスタ サービス サブネットは、Cisco DNA Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりすることはできません。サブネットの最小サイズは 21 ビットです。IPv4 クラスタサービスサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
  - 100.64.0.0/10

  詳細については、RFC 1918 では『Address Allocation For Private Internets』を、RFC 6598 では『IANA-Reserved IPv4 Prefix For Shared Address Space』を参照してください。

  サービスサブネットとして 10.10.10.0/21 を指定する場合は、これら 2 つのサブネットは重複しないため、10.0.8.0/21 のクラスタサービスサブネットを指定することもできます。また、設定ウィザードによって、これらのサブネット間の重複（存在する場合）が検出され、重複を修正するように求められることにも注意してください。

重要

- 有効なCIDRサブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20および172.17.61.0/20サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了したら、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません（詳細については「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）。

2つのサービスとクラスタサービスのサブネットで推奨される合計IPアドレス空間には、4096のアドレスが含まれており、それぞれ2048のアドレスの2/21サブネットに分割されています。2/21サブネットを重複させることはできません。Cisco DNA Centerの内部サービスは、専用のIPアドレスセットの動作に必要です（Cisco DNA Centerマイクロサービスアーキテクチャの要件）。この要件に対応するには、Cisco DNA Centerシステムごとに2つの専用サブネットを割り当てる必要があります。

アプライアンスがこのようなアドレス空間を必要とする理由の1つは、システムパフォーマンスを維持するためです。東西（ノード間）通信には内部ルーティングおよびトンネリングテクノロジーが使用されているため、重複するアドレス空間を使用すると、アプライアンスが仮想ルーティングを実行し、内部的にFIBを転送（FIB）するように強制されることがあります。これにより、1つのサービスから別のサービスに送信されるパケットに対して複数のencap/decapが発生し、高いレイヤでのカスケードの影響により、非常に低いレベルの高い内部遅延が発生します。

もう1つの理由はCisco DNA Center Kubernetesベースのサービスコンテナ化アーキテクチャです。各アプライアンスはKubernetes K8ノードごとにこの空間のIPアドレスを使用します。複数のノードが1つのサービスを構成できます。現在、Cisco DNA Centerは、複数のIPアドレスを必要とするサービスを100以上サポートしており、新しい機能と対応するサービスが常に追加されています。IPが不足したり、お客様がシステムをアップグレードするためだけに連続するアドレス空間を再割り当てすることを要求したりすることなく、シスコが新しいサービスや機能を追加できるようにするために、アドレス空間の要件は最初は意図的に大きく維持されています。

これらのサブネットでサポートされているサービスは、レイヤ3でも有効になっています。クラスタサービススペースは、特に、アプリケーションサービスとインフラストラクチャサービスの間でデータを伝送し、頻繁に使用されます。

RFC 1918およびRFC 6598の要件は、クラウドからパッケージとアップデートをダウンロードするためのCisco DNA Centerの要件によるものです。選択したIP範囲がRFC 1918およびRFC 6598に準拠していない場合、すぐにパブリックIPの重複の問題につながる可能性があります。

インターフェイス名とウィザードの設定順序

インターフェイス名と、これらのインターフェイスをMaglev設定ウィザードで設定する順序は、次の表に示すように、Cisco DNA Centerアプライアンスの第1世代と第2世代とで異なります。お使いのアプライアンスが第1世代と第2世代のどちらかを判断するには、次のとおりシスコ製品番号を参照してください。

- 第1世代44コアアプライアンス：DN1-HW-APL
- 第2世代：
  - 44コアアプライアンス：DN2-HW-APL
  - 44コア アップグレード アプライアンス：DN2-HW-APL-U
  - 56コアアプライアンス：DN2-HW-APL-L
  - 112コアアプライアンス：DN2-HW-APL-XL

表 *7:* インターフェイス名とウィザードの設定順序

機能	**Cisco DNA Center** アプライアンスの種類	インターフェイス名	**Maglev** 設定ウィザードでの設定順序
管理（**Management**）：管理ネットワークから Cisco DNA Center GUI にアクセスできます。	第 1 世代	enp1s0f0	ネットワークアダプタ #2
	第 2 世代	• **44** および **56** コアアプライアンス：**eno1** • **112** コアアプライアンス：**enp53s0f0**	**ネットワークアダプタ #1**
クラウド（**Cloud**）：この目的で別のインターフェイスを使用できない場合にインターネットアクセスを提供します。	第 1 世代	enp1s0f1	ネットワークアダプタ #3
	第 2 世代	• **44** および **56** コアアプライアンス：**eno2** • **112** コアアプライアンス：**enp53s0f1**	**ネットワークアダプタ #2**
エンタープライズ（**Enterprise**）：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します。	第 1 世代	enp9s0	ネットワークアダプタ #4
	第 2 世代	• **44** および **56** コアアプライアンス：**enp94s0f0** • **112** コアアプライアンス：**enp69s0f0**	**ネットワークアダプタ #3**
クラスタ（**Cluster**）：アプライアンスをクラスタノードにリンクします。	第 1 世代	enp10s0	ネットワークアダプタ #1
	第 2 世代	• **44** および **56** コアアプライアンス：**enp94s0f1** • **112** コアアプライアンス：**enp69s0f1**	**ネットワークアダプタ #4**

必要なインターネット URL と完全修飾ドメイン名

アプライアンスでは、次の URL と完全修飾ドメイン名（FQDN）の表へのセキュアなアクセスが必要です。

この表では、各 URL と FQDN を使用する機能について説明します。IP トラフィックがアプライアンスとこれらのリソースとの間を移動できるように、ネットワーク ファイアウォールまたはプロキシサーバのいずれかを設定する必要があります。リストされている URL と FQDN にこのアクセスを提供できない場合は、関連付けられている機能が損なわれるか、または動作不能になります。

インターネットへのプロキシアクセスの要件の詳細については、「インターネットへのアクセスを保護する」を参照してください。

表 *8 :* 必要な *URL* と *FQDN* アクセス

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
システムとアプリケーション パッケージ ソフトウェアにアップデートをダウンロードし、製品チームにユーザからのフィードバックを送信します。	推奨：*.ciscoconnectdna.com:443[1] ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • https://www.ciscoconnectdna.com • https://cdn.ciscoconnectdna.com • https://registry.ciscoconnectdna.com • https://registry-cdn.ciscoconnectdna.com
Cisco DNA Center パッケージの更新	https://*.ciscoconnectdna.com/*
スマートアカウントおよび SWIM ソフトウェアのダウンロード	https://apx.cisco.com https://cloudsso.cisco.com/as/token.oauth2 https://*.cisco.com/*
ユーザ フィードバック	https://dnacenter.uservoice.com
Cisco Meraki との統合	推奨：*.meraki.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • dashboard.meraki.com:443 • api.meraki.com:443 • n63.meraki.com:443

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco.com とシスコ スマートライセンスとの統合	*. cisco.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • software.cisco.com • cloudsso.cisco.com • cloudsso1.cisco.com • cloudsso2.cisco.com • apiconsole.cisco.com • api.cisco.com • apx.cisco.com • sso.cisco.com • apmx-prod1-vip.cisco.com • apmx-prod2-vip.cisco.com • tools.cisco.com
サイトとロケーションマップで正確な情報をレンダリング	• www.mapbox.com • *. tiles.mapbox.com/*: 443 プロキシの場合、宛先は *.tiles.mapbox.com/* です。

[1] シスコは ciscoconnectdna.com とそのサブドメインを所有し、維持しています。Cisco Connect DNA インフラストラクチャは、シスコのセキュリティおよび信頼に関するガイドラインを満たし、継続的なセキュリティテストを実施しています。このインフラストラクチャは堅牢であり、組み込みのロードバランシング機能と自動化機能を備えています。24 時間 365 日の可用性を確保するために、クラウド運用チームが監視と保守を行います。

インターネットへのアクセスを保護する

デフォルトでは、アプライアンスは、インターネット経由でアクセスして、ソフトウェアアップデート、ライセンス、デバイスソフトウェアをダウンロードしたり、最新のマップ情報、ユーザフィードバックなどを提供したりするように設定されています。これらの目的でインターネット接続を提供することは必須要件です。

HTTPS プロキシサーバを使用することは、リモート URL に安全にアクセスするための信頼性の高い方法です。「必要なインターネット URL と完全修飾ドメイン名」に記載されている URL にアプライアンスがアクセスするために必要なアクセス権を付与するには、HTTPS プロキシサーバを使用するようお勧めします。アプライアンス設置時に、この目的で使用するプロキシ

サーバの URL とポート番号を、プロキシのログインクレデンシャルとともに入力するように求められます（プロキシが必要な場合）。

このリリースでは、アプライアンスはHTTPを介したプロキシサーバとの通信のみをサポートしています。HTTPS プロキシサーバをネットワーク内の任意の場所に配置できます。プロキシサーバは HTTPS を使用してインターネットと通信しますが、アプライアンスは HTTP 経由でプロキシサーバと通信します。そのためアプライアンスの設定中、プロキシを設定するときにプロキシの HTTP ポートを指定するようお勧めします。

設定後にプロキシ設定を変更する必要が生じた場合は、GUI を使用して行うことができます。

必要なネットワーク ポート

次の2つの表にアプライアンスが使用する既知のネットワークサービスポートを一覧表示します。これらのポートが、ファイアウォール設定またはプロキシゲートウェイのどちらで開くかを問わず、アプライアンスとの間で送受信されるトラフィックフローに対して開いていることを確認する必要があります。

SDAインフラストラクチャを採用するネットワークにアプライアンスを導入する場合は、追加のポート、プロトコル、およびトラフィックタイプに対応している必要があります。詳細については、「必要なポートとプロトコル： Cisco SD-Access」を参照してください。

（注） Cisco DNA Center の展開時に留意すべきセキュリティ上の考慮事項については、『Cisco Digital Network Architecture Center Security Best Practices Guide』を参照してください。

表 *9:* ポート：着信トラフィック

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
2222	SSH	TCP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443	HTTPS	TCP

表 *10:* ポート：発信トラフィック

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
22	SSH（ネットワーク デバイスへ）	TCP

ポート番号	許可されるトラフィック	プロトコル（TCP または UDP）
23	Telnet（ネットワーク デバイスへ）	TCP
53	DNS	UDP
80	ポート 80 は発信プロキシ設定に使用できます。 さらに、プロキシが設定ウィザードによって設定されている場合（プロキシがすでにネットワークに使用されている場合）、8080 などの他の一般的なポートも使用できます。 シスコのサポートする証明書プールとトラストプールにアクセスするには、アプライアンスから次のリストに記載されたシスコのアドレスに対する発信 IP トラフィックを許可するようにネットワークを設定します。 https://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	SNMP エージェント	UDP
443	HTTPS	TCP
5222	PxGrid の ISE XMP	TCP
9060	ISE ERS の API トラフィック	TCP

次の表に、アプライアンスへの着信 IP トラフィックを許可するポートを示します。

表 *11* : ポート : *IP* トラフィック

プロトコル（TCP または UDP）	ポート番号	トラフィック タイプ
TCP	22	SSH
TCP	2222	SSH
TCP	80	HTTP

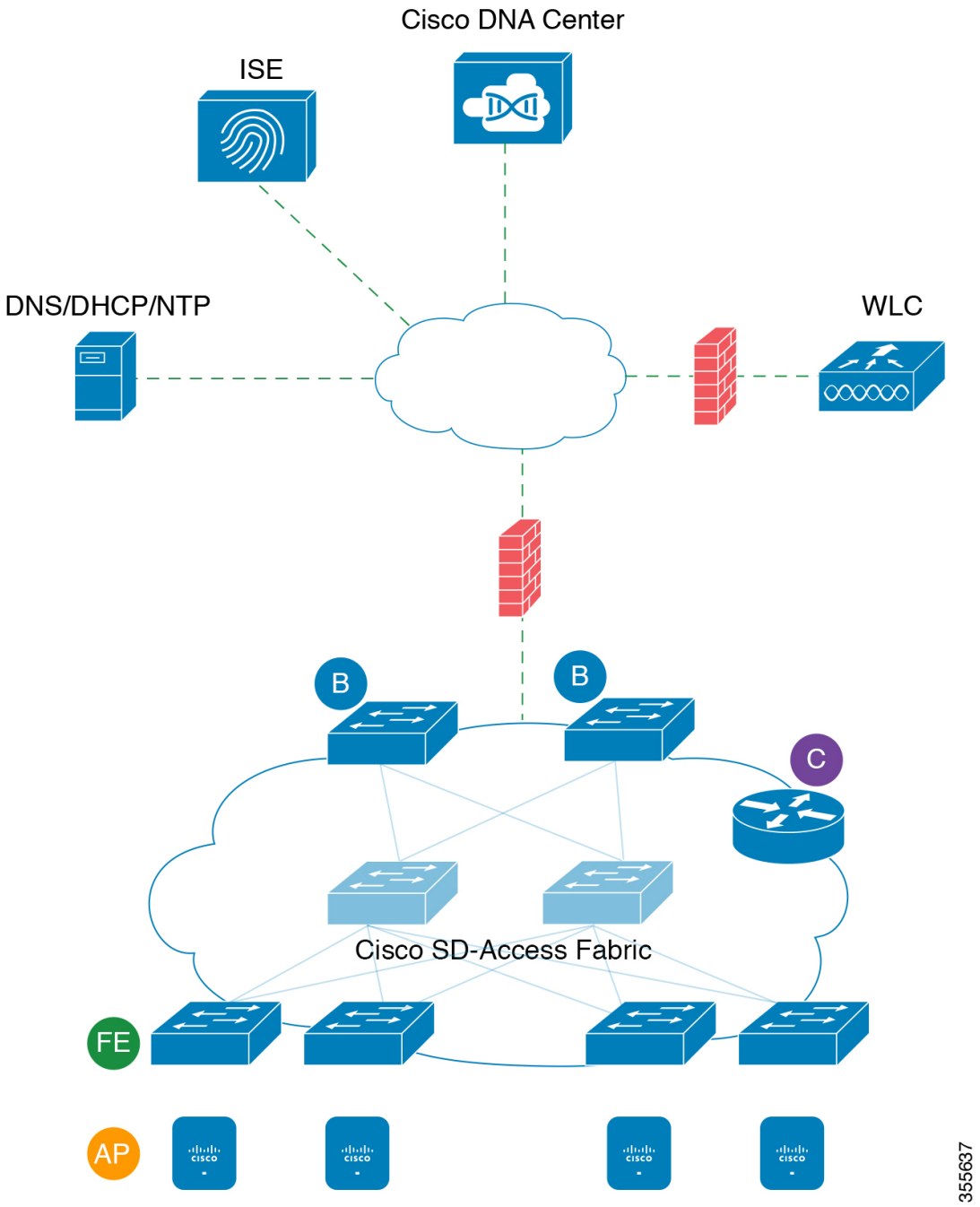
プロトコル（TCP または UDP）	ポート番号	トラフィック タイプ
TCP	443	HTTPS
UDP	67	bootps
UDP	123	NTP
UDP	162	SNMP

（注） ほかにもアプライアンスからシスコのアドレス（https://www.cisco.com/security/pki/）に対する発信 IP トラフィックを許可するようネットワークを設定する方法があります。アプライアンスからシスコがサポートする証明書およびトラストプールにアクセスするには、上述の URL に記載されている IP アドレスを使用します。

必要なポートとプロトコル： Cisco SD-Access

このトピックでは、下の図に示すような一般的な Cisco SD-Access ファブリック展開にネイティブなポート、プロトコル、およびトラフィックのタイプについて詳しく説明します。

図 *10 : Cisco SD-Access* ファブリック インフラストラクチャ



ネットワークにCisco SD-Accessを実装している場合は、次の表の情報を使用して、ネットワーク管理の自動化に必要なアクセス権を Cisco SD-Access に提供しながら、Cisco DNA Center インフラストラクチャを適切に保護するファイアウォールとセキュリティポリシーを計画します。

表 *12 : Cisco DNA Center* トラフィック

送信元ポート[2]	送信元	宛先ポート	宛先	説明
任意（Any）	Cisco DNA Center	UDP 53	DNS サーバ	Cisco DNA Center から DNS サーバの間で使用
いずれか（Any）	Cisco DNA Center	TCP 22	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SSH に使用
いずれか（Any）	Cisco DNA Center	TCP 23	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で Telnet に使用
いずれか（Any）	Cisco DNA Center	UDP 161	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SNMP デバイス検出に使用
ICMP	Cisco DNA Center	ICMP	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間で SNMP デバイス検出に使用
いずれか（Any）	Cisco DNA Center	TCP 443	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間でソフトウェアアップグレードに使用（プロキシがない場合はインターネットへの間でも使用）
いずれか（Any）	Cisco DNA Center	TCP 80	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間でプラグアンドプレイ（PnP）に使用（プロキシがない場合はインターネットへの間でも使用）
いずれか（Any）	Cisco DNA Center	TCP 830	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間で NETCONF に使用（Cisco SD-Access 組み込みワイヤレス）
UDP 123	Cisco DNA Center	UDP 123	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間で LAN 自動化中の初回期間に使用
いずれか（Any）	Cisco DNA Center	UDP 123	NTP サーバ	Cisco DNA Center から NTP サーバの間で使用

いずれか（Any）	Cisco DNA Center	TCP 22、UDP 161	シスコ ワイヤレス コントローラ	Cisco DNA Center からシスコ ワイヤレス コントローラの間で使用
ICMP	Cisco DNA Center	ICMP	シスコ ワイヤレス コントローラ	Cisco DNA Center からシスコ ワイヤレス コントローラの間で使用
いずれか（Any）	Cisco DNA Center	TCP 80、TCP 443	AP	Cisco DNA Center からセンサ、アクティブセンサ（Cisco Aironet 1800S）の AP の間で使用
いずれか（Any）	AP	TCP 32626	Cisco DNA Center	Cisco DNA アシュアランス インテリジェントキャプチャ（gRPC）機能で使用されるトラフィック統計情報とパケットキャプチャデータの受信に使用されます。

[2] のクラスタ、PKI、SFTP サーバ、プロキシポートのトラフィックは、この表には含まれていません。

表 *13*：インターネット接続トラフィック

送信元ポート	送信元	宛先ポート	宛先	説明
任意（Any）	Cisco DNA Center	TCP 443	registry.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	www.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	registry-cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	software.cisco.com	デバイスソフトウェアのダウンロード
いずれか（Any）	Cisco DNA Center	TCP 443	cloudsso.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか（Any）	Cisco DNA Center	TCP 443	cloudsso1.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証

いずれか（Any）	Cisco DNA Center	TCP 443	cloudsso2.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか（Any）	Cisco DNA Center	TCP 443	apiconsole.cisco.com	CSSM スマートライセンスの API
いずれか（Any）	Cisco DNA Center	TCP 443	sso.cisco.com	CCO とスマートライセンス
いずれか（Any）	Cisco DNA Center	TCP 443	api.cisco.com	CCO とスマートライセンス
いずれか（Any）	Cisco DNA Center	TCP 443	apx.cisco.com	CCO とスマートライセンス
いずれか（Any）	Cisco DNA Center	TCP 443	dashboard.meraki.com	Meraki の統合
いずれか（Any）	Cisco DNA Center	TCP 443	api.meraki.com	Meraki の統合
いずれか（Any）	Cisco DNA Center	TCP 443	n63.meraki.com	Meraki の統合
いずれか（Any）	Cisco DNA Center	TCP 443	dnacenter.uservoice.com	ユーザフィードバックの送信
いずれか（Any）	Cisco DNA Center Admin Client	TCP 443	*.tiles.mapbox.com	ブラウザでのマップのレンダリング（プロキシ経由のアクセスの場合、宛先は *.tiles.mapbox.com/*）
いずれか（Any）	Cisco DNA Center	TCP 443	www.mapbox.com	マップとシスコ ワイヤレス コントローラの国番号の識別

表 *14 : Cisco SD-Access* ファブリック アンダーレイ トラフィック

送信元ポート[3]	送信元	宛先ポート	宛先	説明
UDP 68	ファブリックアンダーレイ	UDP 67	DHCP サーバ	ファブリックスイッチ、ルータからDHCPサーバの間で、ファブリックエッジノードによって開始される DHCP リレーパケットに使用。

いずれか（Any）	ファブリックアンダーレイ	TCP 80	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間で PnP に使用
いずれか（Any）	ファブリックアンダーレイ	TCP 443	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間でイメージのアップグレードに使用
いずれか（Any）	ファブリックアンダーレイ	UDP 162	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間で SNMP トラップに使用
いずれか（Any）	ファブリックアンダーレイ	UDP 514	Cisco DNA Center	ファブリックスイッチ、ルータから Cisco DNA アシュアランス
いずれか（Any）	ファブリックアンダーレイ	UDP 6007	Cisco DNA Center	ファブリックルータから Cisco DNA Center の間で NetFlow に使用
いずれか（Any）	ファブリックアンダーレイ	UDP 123	Cisco DNA Center	ファブリックスイッチから Cisco DNA Center の間で LAN 自動化時に使用
ICMP	ファブリックアンダーレイ	ICMP	Cisco DNA Center	ファブリックスイッチ、ルータループバックから Cisco DNA Center の間で SNMP デバイス検出に使用
UDP 161	ファブリックアンダーレイ	いずれか（Any）	Cisco DNA Center	ファブリックスイッチ、ルータループバックから Cisco DNA Center の間で SNMP デバイス検出に使用
いずれか（Any）	ファブリックアンダーレイ	UDP 53	DNS サーバ	ファブリックスイッチ、ルータから DNS サーバの間で名前解決に使用
TCP および UDP 4342	ファブリックアンダーレイ	TCP および UDP 4342	ファブリックルータおよびスイッチ	LISP でカプセル化された制御メッセージ
TCP および UDP 4342	ファブリックアンダーレイ	いずれか（Any）	ファブリックルータおよびスイッチ	LISP コントロールプレーン通信

いずれか（Any）	ファブリックアンダーレイ	UDP 4789	ファブリックルータおよびスイッチ	ファブリックカプセル化データパケット（VXLAN-GPO）
いずれか（Any）	ファブリックアンダーレイ	UDP 1645/1646/1812/1813	ISE	ファブリックスイッチ、ルータループバック IP から ISE の間で RADIUS に使用
ICMP	ファブリックアンダーレイ	ICMP	ISE	ファブリックスイッチ、ルータから ISE の間でトラブルシューティングに使用
UDP 1700/3799	ファブリックアンダーレイ	いずれか（Any）	ISE	ファブリックスイッチから ISE の間で気付アドレス（CoA）に使用
いずれか（Any）	ファブリックアンダーレイ	UDP 123	NTP サーバ	ファブリックスイッチ、ルータループバック IP から NTP サーバの間で使用
いずれか（Any）	control-plane	UDP および TCP 4342/4343	シスコ ワイヤレス コントローラ	コントロールプレーンのループバック IP からシスコ ワイヤレス コントローラの間でファブリック対応ワイヤレスに使用

[3] ボーダー ルーティング プロトコル、SPAN、プロファイリング、およびテレメトリトラフィックは、この表には含まれていません。

表 *15：*シスコ ワイヤレス コントローラ トラフィック

送信元ポート	送信元	宛先ポート	宛先	説明
UDP 5246/5247/5248	シスコ ワイヤレス コントローラ	いずれか（Any）	AP IP プール	シスコ ワイヤレス コントローラから AP サブネットの間で CAPWAP に使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	AP IP プール	シスコ ワイヤレス コントローラから AP の間でトラブルシューティング目的の ping を許可するために使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 69/5246/5247 TCP 22	AP IP プール	シスコ ワイヤレス コントローラから AP サブネットの間で CAPWAP に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP および TCP 4342/4343	コントロールプレーン	シスコ ワイヤレス コントローラからコントロールプレーンのループバック IP の間で使用

いずれか（Any）	シスコ ワイヤレス コントローラ	TCP 32222	Cisco DNA Center	シスコ ワイヤレス コントローラから Cisco DNA Center の間でデバイス検出に使用
UDP 161	シスコ ワイヤレス コントローラ	いずれか（Any）	Cisco DNA Center	シスコ ワイヤレス コントローラから Cisco DNA Center の間で SNMP に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 162	Cisco DNA Center	シスコ ワイヤレス コントローラから Cisco DNA Center トラップの間で SNMP トラップに使用
いずれか（Any）	シスコ ワイヤレス コントローラ	TCP 16113	Cisco Mobility Services Engine（MSE）と Cisco SPECTRUM EXPERT	シスコ ワイヤレス コントローラから Cisco MSE、SPECTRUM EXPERT の間で NMSP に使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	Cisco DNA Center	シスコ ワイヤレス コントローラからトラブルシューティング目的の ping を許可するために使用
いずれか（Any）	HA サーバ	TCP 1315	Cisco DNA Center	データベースサーバ HA（QoS）
いずれか（Any）	HA サーバ	TCP 1316 ～ 1320	Cisco DNA Center	HA データベースポート
いずれか（Any）	HA Web サーバ	TCP 8082	Cisco DNA Center	HA Web サーバのヘルスモニタポート
いずれか（Any）	シスコ ワイヤレス コントローラと各種 Syslog サーバ	UDP 514	シスコ ワイヤレス コントローラ	Syslog（オプション）
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 53	DNS サーバ	シスコ ワイヤレス コントローラから DNS サーバの間で使用
いずれか（Any）	シスコ ワイヤレス コントローラ	TCP 443	ISE	シスコ ワイヤレス コントローラから ISE の間でゲスト SSID Web 認証に使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 1645、1812	ISE	シスコ ワイヤレス コントローラから ISE の間で RADIUS 認証に使用

いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 1646、1813	ISE	シスコ ワイヤレス コントローラから ISE の間で RADIUS アカウンティングに使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 1700、3799	ISE	シスコ ワイヤレス コントローラから ISE の間で RADIUS CoA に使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	ISE	シスコ ワイヤレス コントローラから ISE ICMP の間でトラブルシューティングに使用
いずれか（Any）	シスコ ワイヤレス コントローラ	UDP 123	NTP サーバ	シスコ ワイヤレスコントローラから NTP サーバまで

表 *16 :* ファブリック対応ワイヤレス *AP IP* プールトラフィック

送信元ポート	送信元	宛先ポート	宛先	説明
UDP 68	AP IP プール	UDP 67	DHCP サーバ	AP IP プールから DHCP サーバの間で使用。
ICMP	AP IP プール	ICMP	DHCP サーバ	AP IP プールから ICMP の間でトラブルシューティングに使用。
いずれか（Any）	AP IP プール	514	各種	Syslog：宛先設定可能。デフォルトは 255.255.255.255 です。
いずれか（Any）	AP IP プール	UDP 69/5246/5247/5248	シスコ ワイヤレス コントローラ	AP IP プールからシスコ ワイヤレス コントローラの間で CAPWAP に使用。
ICMP	AP IP プール	ICMP	シスコ ワイヤレス コントローラ	AP IP プールからシスコ ワイヤレス コントローラの間でトラブルシューティング目的の ping を許可するために使用。

表 *17 : ISE* トラフィック

送信元ポート[4]	送信元	宛先ポート	宛先	説明
任意（Any）	ISE	TCP 64999	ボーダー	ISE からボーダーノードの間で SGT Exchange Protocol（SXP）に使用
いずれか（Any）	ISE	UDP 514	Cisco DNA Center	ISE から Syslog サーバ（Cisco DNA Center）の間で使用

UDP 1645/1646/1812/1813	ISE	いずれか（Any）	ファブリックアンダーレイ	ISEからファブリックスイッチ、ルータの間でRADIUSと認証用に使用
いずれか（Any）	ISE	UDP 1700/3799	ファブリックアンダーレイ	ISEからファブリックスイッチ、ルータループバック IP の間でCoA に使用
ICMP	ISE	ICMP	ファブリックアンダーレイ	ISE からファブリックスイッチの間でトラブルシューティングに使用
いずれか（Any）	ISE	UDP 123	NTP サーバ	ISE と NTP サーバの間で使用
UDP 1812/1645/1813/1646	ISE	いずれか（Any）	シスコ ワイヤレスコントローラ	ISE からシスコ ワイヤレス コントローラの間でRADIUS に使用
ICMP	ISE	ICMP	シスコ ワイヤレスコントローラ	ISE からシスコ ワイヤレス コントローラの間でトラブルシューティングに使用

[4] 注：高可用性およびプロファイリング トラフィックは、この表には含まれていません。

表 *18 : DHCP* サーバトラフィック

送信元ポート	送信元	宛先ポート	宛先	説明
UDP 67	DHCP サーバ	UDP 68	AP IP プール	DHCP サーバからファブリック AP の間で使用
ICMP	DHCP サーバ	ICMP	AP IP プール	トラブルシューティング用のICMP：ファブリックから DHCP の間で使用
UDP 67	DHCP サーバ	UDP 68	ファブリックアンダーレイ	DHCPからファブリックスイッチ、ルータの間で使用
ICMP	DHCP サーバ	ICMP	ファブリックアンダーレイ	トラブルシューティング用のICMP：ファブリックから DHCP の間で使用
UDP 67	DHCP サーバ	UDP 68	ユーザ IP プール	DHCP サーバからファブリックスイッチ、ルータの間で使用
ICMP	DHCP サーバ	ICMP	ユーザ IP プール	トラブルシューティング用のICMP：ユーザと DHCP の間で使用

表 *19 : NTP* サーバトラフィック

送信元ポート	送信元	宛先ポート	宛先	説明

UDP 123	NTP サーバ	いずれか（Any）	ISE	NTP サーバから ISE の間で使用
UDP 123	NTP サーバ	いずれか（Any）	Cisco DNA Center	NTP サーバから Cisco DNA Center
UDP 123	NTP サーバ	いずれか（Any）	ファブリックアンダーレイ	NTP サーバからファブリックスイッチ、ルータループバックの間で使用
UDP 123	NTP サーバ	いずれか（Any）	シスコ ワイヤレス コントローラ	NTP サーバからシスコ ワイヤレス コントローラの間で使用

表 *20 : DNS* トラフィック

送信元ポート	送信元	宛先ポート	宛先	説明
UDP 53	DNS サーバ	いずれか（Any）	ファブリックアンダーレイ	DNS サーバからファブリックスイッチの間で使用
UDP 53	DNS サーバ	いずれか（Any）	シスコ ワイヤレス コントローラ	DNS サーバからシスコ ワイヤレス コントローラの間で使用

必須の設定情報

アプライアンスの設定中、必要な IP アドレスおよびサブネットに加えて、次の情報を入力するように求められます。

- **Linux ユーザ名（Linux User Name）**：これは **maglev** です。このユーザ名はマスタノードとアドオンノードの両方を含む、クラスタ内のすべてのアプライアンスで共通しており、変更できません。
- **Linux パスワード（Linux Password）**：Linux ユーザ名 **maglev** のパスワードを指定します。このパスワードは、Linux コマンドラインを使用して各アプライアンスへのセキュアなアクセスを保証します。必要に応じてクラスタ内の各アプライアンスの Linux ユーザ名 **maglev** ごとに異なる Linux パスワードを割り当てることができます。

  デフォルト値はないため、ユーザが Linux パスワードを作成する必要があります。パスワードは次の要件を満たしている必要があります。

  - 長さは 8 文字以上にすること。
  - タブも改行も含まないこと。
  - 次のうち少なくとも 3 つのカテゴリの文字を含むこと。
    - アルファベットの大文字

- アルファベットの小文字
- 数字
- 特殊文字（! や # など）

Linux パスワードは暗号化され、Cisco DNA Center データベースにハッシュされます。マルチノードクラスタを展開している場合は、各アドオンノードにマスタノードの Linux パスワードを入力するように求められます。

- **パスワード生成シード（Password Generation Seed）（オプション）**：Linux パスワードを作成する代わりに、シードフレーズを入力し、**[パスワードの生成（Generate Password）]** を押す方法もあります。**[Maglev 設定（Maglev Configuration）]** ウィザードでは、このシードフレーズを使用してランダムで安全なパスワードが生成されます。**[自動生成パスワード（Auto Generated Password）]**フィールドを使用すると、生成されたパスワードをさらに編集できます。
- **管理者パスフレーズ（Administrator Passphrase）**：クラスタ内の Cisco DNA Center への Web アクセスに使用されるパスワードを指定します。これはスーパーユーザ権限を持つ管理者のアカウント **admin** のパスワードであり、初めて Cisco DNA Center にログインするときに使用します（「初回ログイン」を参照）。初めてログインすると、このパスワードを変更するよう求められます。

  このパスワードにはデフォルトがないため、作成する必要があります。管理者のパスフレーズは、上述の Linux パスワードと同じ要件を満たす必要があります。
- **CIMC ユーザパスワード**：CIMC GUI へのアクセスに使用するパスワードを指定します。工場出荷時のデフォルトは「*password*」ですが、Web ブラウザを使用してアクセスするために CIMC を初めて設定するとき、変更を求められます（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。

  CIMC ユーザパスワードは、上述の Linux パスワードと同じ要件を満たす必要があります。工場出荷時の初期状態にリセットした場合にのみ、*password* に戻すことができます。
- [マスタノードIPアドレス（Master Node IP Address）]：クラスタにアドオンノードをインストールする場合にのみ必要です。これは、マスタノード上のクラスタポートの IP アドレスです（「インターフェイスケーブル接続」を参照）。

必要な初期設定情報

アプライアンスを設定したら、Cisco DNA Center にログインして、必須の設定タスクを完了します。この初回設定では次の情報が必要になります。

- **スーパーユーザ権限を持つ管理者の新しいパスワード（New Admin Superuser Password）**：Cisco DNA Center 管理者の新しいスーパーユーザパスワードを入力するように求められます。スーパーユーザ権限を持つ管理者のパスワードをリセットすると、運用上のセキュリ

ティが向上します。これはたとえばCisco DNA Centerアプライアンスを設置して設定した企業スタッフが Cisco DNA Center のユーザまたは管理者ではない場合に特に重要です。

- **Cisco.com ログイン情報（Cisco.com Credentials）**：ソフトウェアのダウンロードを登録し、電子メールでシステム通信を受信するために組織が使用する Cisco.com ユーザ ID とパスワード。
- **シスコ スマートアカウントのクレデンシャル（Cisco Smart Account Credentials）**：組織がデバイスとソフトウェアライセンスの管理に使用する Cisco.com スマートアカウントのユーザ ID とパスワード。
- **IP アドレスマネージャの URL とクレデンシャル（IP Address Manager URL and Credentials）**：Cisco DNA Center で使用する予定のサードパーティ製 IP アドレスマネージャ（IPAM）サーバのホスト名、URL、管理者ユーザ名、管理者パスワード。このリリースでは InfoBlox と Bluecat がサポートされています。
- **プロキシ URL、ポート、クレデンシャル（Proxy URL, Port and Credentials）**：Cisco DNA Centerソフトウェアのアップデートの取得、デバイスライセンスの管理などのダウンロード可能なコンテンツの取得のために Cisco DNA Center で使用するプロキシサーバの URL（ホスト名または IP アドレス）、ポート番号、ユーザ名、ユーザパスワード。
- **Cisco DNA Centerユーザ（Users）**：作成する新規 Cisco DNA Center ユーザのユーザ名、パスワード、権限の設定。シスコは通常の Cisco DNA Center 操作すべてで、常にこれらの新しいユーザアカウントのいずれかを使用するよう推奨しています。Cisco DNA Center の再設定や、スーパーユーザ権限が明示的に必要となるその他の操作を除き、管理者用スーパーユーザアカウントは使用しないようにしてください。

この情報を入力する初回セットアップウィザードを起動して対応する方法の詳細については、「初回ログイン」を参照してください。

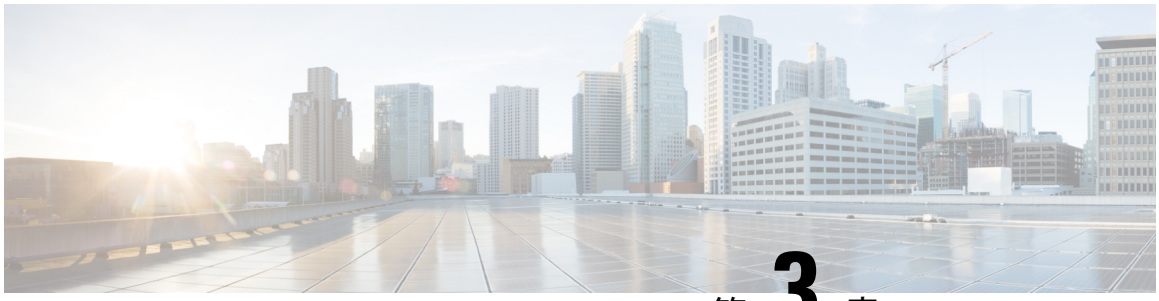
また残りの設定タスクを完了するために次の情報が必要になります。これは初回ログイン後に実行できます。

- **認証およびポリシーサーバ情報（Authorization and Policy Server Information）**：認証サーバまたはポリシーサーバとして Cisco ISE を使用している場合、前項目と同じ情報が必要になるほか、ISE CLI ユーザ名、CLI パスワード、サーバ FQDN、サブスクライバ名（*cdnac* など）、ISE SSH キー（オプション）、プロトコル選択（RADIUS または TACACS）、認証ポート、アカウンティングポート、再試行、タイムアウトの設定が必要となります。
- **[認証およびポリシーサーバ情報（Authorization and Policy Server Information）]**：認証およびポリシーサーバとして Cisco ISE を使用している場合は、上述の ISE の統合と同じ情報に加えて、ISE CLI ユーザ名、CLI パスワード、サーバ FQDN、サブスクライバ名（*cdnac* など）、ISE SSH キー（オプション）、プロトコル選択（RADIUS または TACACS）、認証ポート、アカウンティングポート、再試行とタイムアウトの設定が必要です。

  Cisco ISE 以外の認証サーバ、ポリシーサーバを使用している場合、サーバの IP アドレス、プロトコルの選択（RADIUS または TACACS）、認証ポート、アカウンティングポート、再試行、タイムアウトの設定が必要になります。

この情報は、選択した認証サーバ、ポリシーサーバと Cisco DNA Center を統合するために必要です。詳細については「認証サーバとポリシー サーバの設定」で説明しています。

- **SNMP の再試行とタイムアウト値（SNMP Retry and Timeout Values）**：これは「SNMP プロパティの設定」で説明されているように、デバイスのポーリングとモニタリングをセットアップするために必要です。



第 3 章

アプライアンスの設置

アプライアンスのインストール ワークフロー

Cisco DNA Centerアプライアンスを物理的に設置するには、次のタスクを完了します。インストールする各アプライアンスに対して、次のタスクを実行します。最初のマスターノードを設定する前に、必ずすべてのアプライアンスを設置してください。

1. 設定およびセットアップ時に提供する必要がある情報の収集など、導入計画の要件を確認して対処します（次のトピックで説明します）。
   - Cisco DNA CenterおよびCisco SD-Access
   - インターフェイスケーブル接続
   - 必要な IP アドレスおよびサブネット （34 ページ）
   - 必要なインターネット URL と完全修飾ドメイン名
   - インターネットへのアクセスを保護する
   - 必要なネットワーク ポート
   - 必須の設定情報
   - 必要な初期設定情報
2. アプライアンスの機能と仕様を確認します。
   - アプライアンスのハードウェア仕様

- 前面パネルと背面パネル
- 物理仕様
- 環境仕様
- 電力仕様

3. アプライアンスを開梱します：アプライアンスを開梱して点検
4. アプライアンスに関する操作上の警告とガイドラインを確認します：インストール警告とガイドラインの確認
5. ラックにアプライアンスを設置します：ラック要件の確認
6. アプライアンスに電源を接続し、電源をオンにします：アプライアンスの接続および電源投入
7. 前面パネルおよび背面パネルのLEDをチェックして、アプライアンスが機能していることを確認します：LED の確認

これらのタスクがすべて完了したら、「アプライアンス設定の準備の概要」で説明されている手順に進みます。

アプライアンスを開梱して点検

⚠

注意 内部アプライアンスのコンポーネントを取り扱うときは、静電気防止用ストラップを着用し、モジュールのフレームの端のみを持つようにしてください。

ステップ 1 段ボール箱からアプライアンスを取り出します。（将来、アプライアンスの輸送が必要になったときに備え）梱包材はすべて保管しておいてください。

ステップ 2 カスタマーサービス担当者から提供された機器リストおよび以下の一覧と、梱包品の内容を照合します。すべての品目が揃っていることを確認してください。

ステップ 3 破損や不一致がないことを確認し、万一不備があった場合は、シスコカスタマーサービス担当者にご連絡ください。次の情報を用意しておきます。

- 発送元の請求書番号（梱包明細を参照）
- 破損している装置のモデルとシリアル番号
- 破損状態の説明
- 破損による設置への影響

インストール警告とガイドラインの確認

（注） サーバの設置、操作、または保守を行う前に、『Regulatory Compliance and Safety Information for Cisco UCS C-Series Servers』を参照して重要な安全情報を確認してください。

警告 **安全上の重要な注意事項**

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

ステートメント 1071

警告 **システムの過熱を防ぐため、最大推奨周囲温度の 35°C （95°F）を超えるエリアで操作しないでください。**

ステートメント 1047

警告 **いつでも装置の電源を切断できるように、プラグおよびソケットにすぐ手が届く状態にしておいてください。**

ステートメント 1019

警告 **この製品は、設置する建物に短絡（過電流）保護機構が備わっていることを前提に設計されています。保護デバイスの定格 250 V、15 A を超えないようにしてください。**ステートメント 1005

警告 **装置は地域および国の電気規則に従って設置する必要があります。**

ステートメント 1074

警告 この装置は、立ち入りが制限された場所への設置を前提としています。立ち入りが制限された場所とは、特殊な器具、錠と鍵、またはその他の保安手段を使用しないと入れない場所を意味します。

ステートメント 1017

次の 4 つは 112 コアアプライアンスに固有の警告です。

警告 この装置は、アースさせる必要があります。絶対にアース導体を破損させたり、アース線が正しく取り付けられていない装置を稼働させたりしないでください。アースが適切かどうかはっきりしない場合には、電気検査機関または電気技術者に確認してください。

ステートメント 1024

警告 北欧諸国（ノルウェー、フィンランド、スウェーデン、デンマーク）では、このシステムは、すべての機器のメインアース接続の電圧が同じ（等電位接地）であり、システムが接地された電源コンセントに接続されている、アクセス制限区域に設置する必要があります。

ステートメント 328

警告 システムの電源接続の前に高リーク電流アース接続を行う必要があります。

ステートメント 342

警告 本機器は、電力を供給する前に、お客様が準備した地線を使用して外部接地する必要があります。アースが適切かどうかはっきりしない場合には、電気検査機関または電気技術者に確認してください。

ステートメント 366

注意 アプライアンスを取り付ける際は、適切なエアーフローを確保するために、レールキットを使用する必要があります。レールキットを使用せずに、ユニットを別のユニットの上に物理的に置く（つまり積み重ねる）と、アプライアンスの上部にある通気口がふさがれます。これは、過熱したり、ファンの回転が速くなったり、電力消費が高くなったりする原因となります。アプライアンスをラックに取り付けるときは、アプライアンス間で必要な最小の間隔を確保できるレール キットのマウントを推奨します。レール キットを使用してユニットをマウントする場合は、アプライアンス間の間隔を余分にとる必要はありません。

⚠

注意 鉄共振テクノロジーを使用する UPS モデルは使用しないでください。このタイプの UPS は、Cisco UCS などのシステムに使用すると、データ トラフィック パターンの変化によって入力電流が大きく変動し、動作が不安定になるおそれがあります。

アプライアンスを設置する際には、次のガイドラインに従ってください。

- アプライアンスを設置する前に、設置場所を検討して準備します。設置場所を計画する際に推奨される作業については、『*Cisco UCS サイト計画および準備作業（Cisco UCS Site Preparation Guide）*』を参照してください。
- アプライアンスの作業に支障がないように、また適切なエアーフローが確保されるように、アプライアンス周辺に十分なスペースを確保できることを確認してください。このアプライアンスでのエアーフローは、前面から背面に流れます。
- 設置場所の空調が「環境仕様」に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、「ラック要件の確認」に記載された要件に適合していることを確認します。
- 設置場所の電源が、「電力仕様」に記載された要件に適合していることを確認します。使用可能な場合は、電源障害に備えて UPS を使用してください。

ラック要件の確認

適切な操作を行うため、アプライアンスを設置するラックは次の要件を満たす必要があります。

- 標準的な 19 インチ（48.3 cm）幅 4 支柱 EIA ラック（ANSI/EIA-310-D-1992 のセクション 1 に準拠した英国ユニバーサル ピッチに適合するマウント支柱付き）。
- 付属のスライドレールを使用する場合、ラック支柱の穴は、9.6mm（0.38インチ）の正方形、7.1 mm（0.28 インチ）の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバごとのラックの垂直方向のスペースは次を満たす必要があります。
  - 44 および 56 コアアプライアンスの場合、1 RU は 44.45 mm（1.75 インチ）に相当します。
  - 112 コアアプライアンスの場合、177.8 mm（7.0 インチ）に相当する RU が 4 つあります。

アプライアンスの接続および電源投入

この項では、アプライアンスの電源をオンにして、それが機能していることを確認する方法について説明します。

ステップ 1 付属の電源コードをアプライアンスの各電源装置に接続してから、接地付き AC 電源出力に接続します。詳細については「電力仕様」を参照してください。

初回のブートアップ時には、アプライアンスがブートしてスタンバイ電源モードになるまでに約 2 分かかります。

電源ステータス LED は、次のとおりアプライアンスの電源ステータスを示します。

- 消灯：アプライアンスには AC 電力が供給されていません。
- オレンジ：アプライアンスはスタンバイ電源モードです。CIMC と一部のマザーボード機能にだけ電力が供給されています。
- 緑：アプライアンスはメイン電源モードです。電力は、すべてのアプライアンス コンポーネントに供給されています。

電源ステータス LED などのアプライアンス LED の詳細については、「前面パネルと背面パネル」を参照してください。

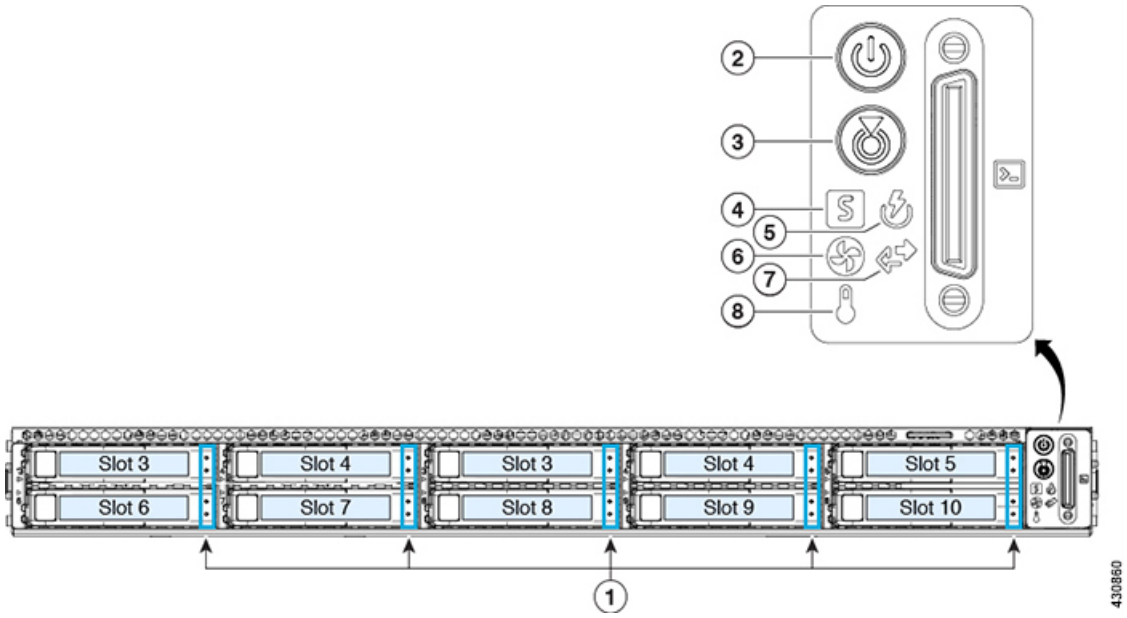
ステップ 2 前面パネルの KVM コネクタに接続されている付属の KVM ケーブルを使用して、USB キーボードと VGA モニタをサーバに接続します。または、背面パネルの VGA および USB ポートを使用することもできます。一度に接続できる VGA インターフェイスは 1 つのみです。

LED の確認

アプライアンスの電源を投入したら、前面パネルと背面パネルの LED とボタンの状態をチェックし、機能していることを確認します。

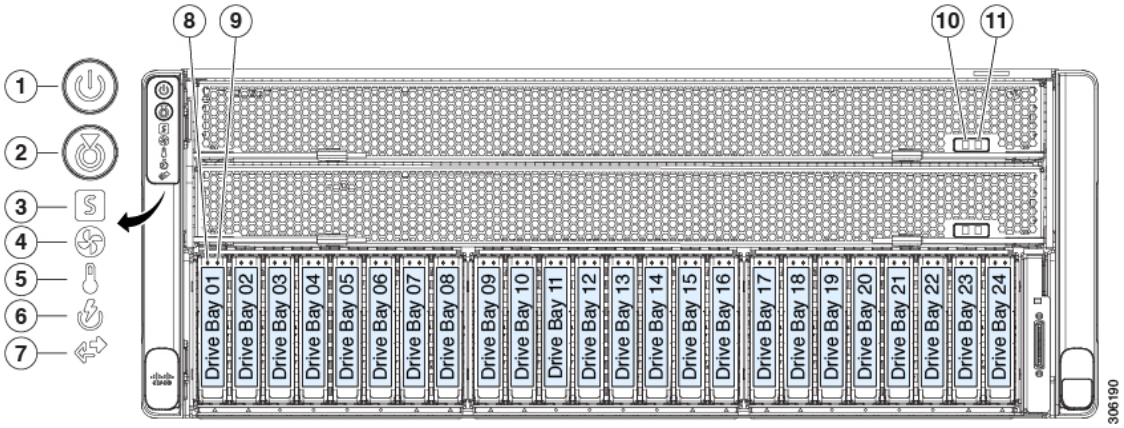
次の図は、物理的な設置と初回の電源投入が終わった後（設定前）動作しているアプライアンスの LED を示しています。

図 *11 : 44* および *56* コアアプライアンスの前面パネル *LED*



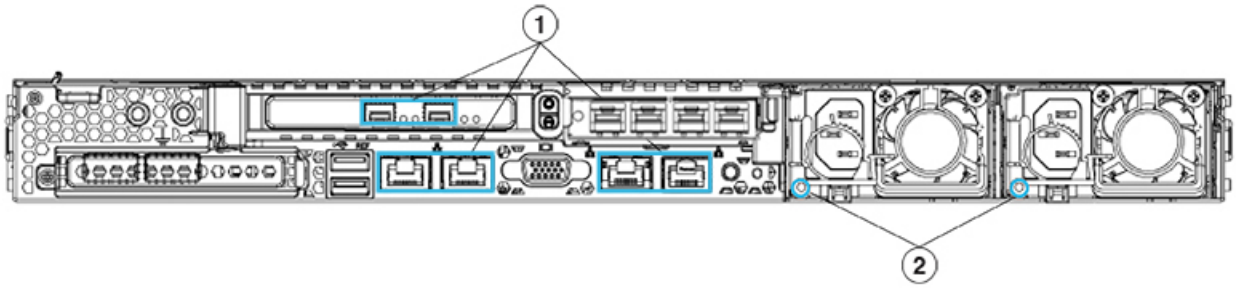
LED	望ましいステータスインジケータ
1	• ドライブ障害 LED：消灯 • ドライブアクティビティ LED：緑
2	電源ステータス：緑
3	ユニット識別：消灯
4	システムステータス：緑
5	電源装置ステータス：緑
6	ファンステータス：緑
7	ネットワーク リンク アクティビティ：消灯
8	温度ステータス：緑

図 *12 : 112* コアアプライアンスの前面パネル *LED*



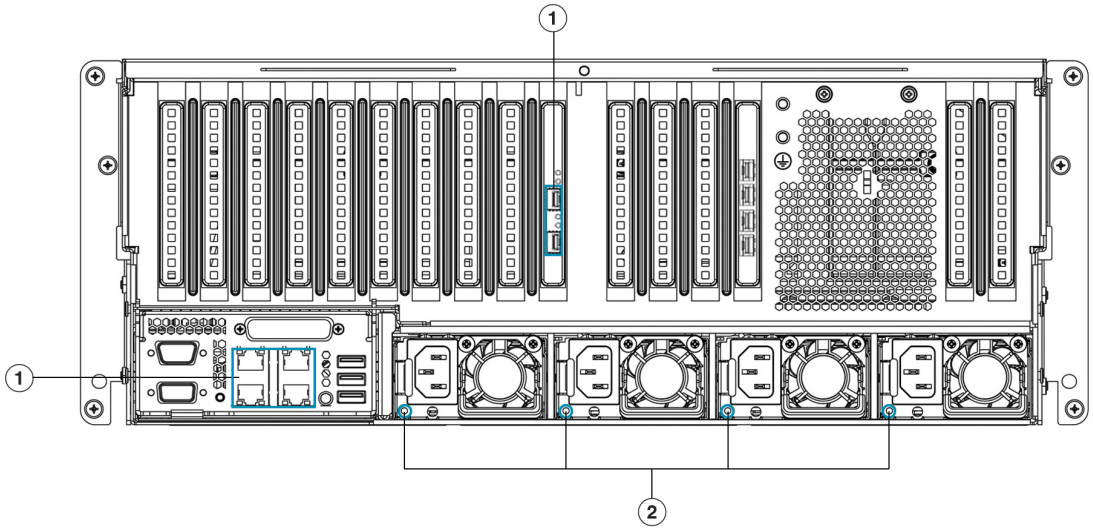
LED	望ましいステータスインジケータ
1	電源ステータス：緑
2	ユニット識別：消灯
3	システムステータス：緑
4	ファンステータス：緑
5	温度ステータス：緑
6	電源装置ステータス：緑
7	ネットワーク リンク アクティビティ：消灯
8	ドライブ障害 LED：消灯
9	ドライブアクティビティ LED：緑
10	CPU モジュール電源のステータス：緑
11	CPU モジュール障害：消灯

図 *13 : 44* および *56* コアアプライアンスの背面パネル *LED*



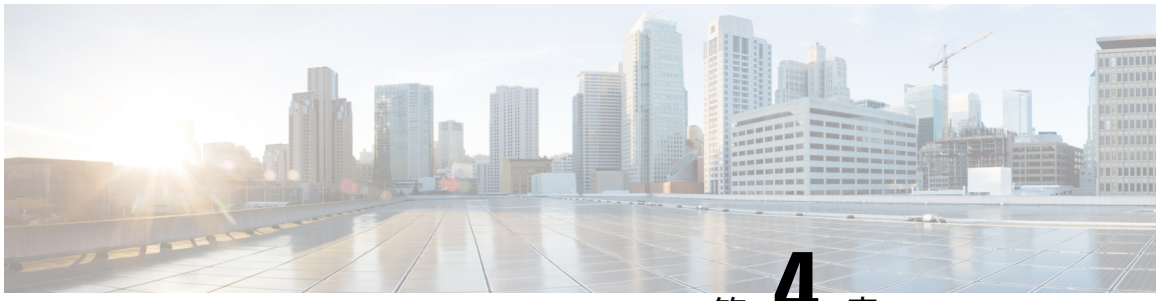
LED	望ましいステータスインジケータ
1	正常であれば、最初の電源投入時にはすべてのポートのリンクステータスとリンク速度 LED がオフになります。 Maglev 設定ウィザードを使用してネットワーク設定を構成およびテストした後（「Maglev ウィザードを使用したマスタノードの設定」と「Maglev ウィザードを使用したアドオンノードの設定」を参照）、すべての**ケーブル接続**ポートのリンクステータス、リンク速度、電源ステータス LED がグリーンになります。すべての**ケーブル接続されていない**ポートの LED は変化しません。
2	AC 電源ステータス LED：緑

図 *14 : 112* コアアプライアンスの背面パネルの *Led*



LED	望ましいステータスインジケータ
1	正常であれば、最初の電源投入時にはすべてのポートのリンクステータスとリンク速度 LED がオフになります。 Maglev 設定ウィザードを使用してネットワーク設定を構成およびテストした後（「Maglev ウィザードを使用したマスタノードの設定」および「Maglev ウィザードを使用したアドオンノードの設定」を参照）、すべての**ケーブル接続**ポートのリンクステータス、リンク速度、および電源ステータス LED がグリーンになります。すべての**ケーブル接続されていない**ポートの LED は変化しません。
2	AC 電源ステータス LED：緑

以上に示されていない色の LED が表示される場合は、問題の状態が発生している可能性があります。そのステータスの考えられる原因については、前面パネルと背面パネルを参照してください。アプライアンスの設定に進む前に、問題の状態を修正してください。



第 4 章

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. アプライアンスに付属する Intel X710-DA4 ネットワーク インターフェイス カード（NIC）が現在有効になっている場合は、これを無効にする必要があります（「ネットワーク インターフェイス カードの無効化 （78 ページ）」を参照）。
4. 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. > **[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] をクリックしてから、[**ユーザの変更**] をクリックします。
3. 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。

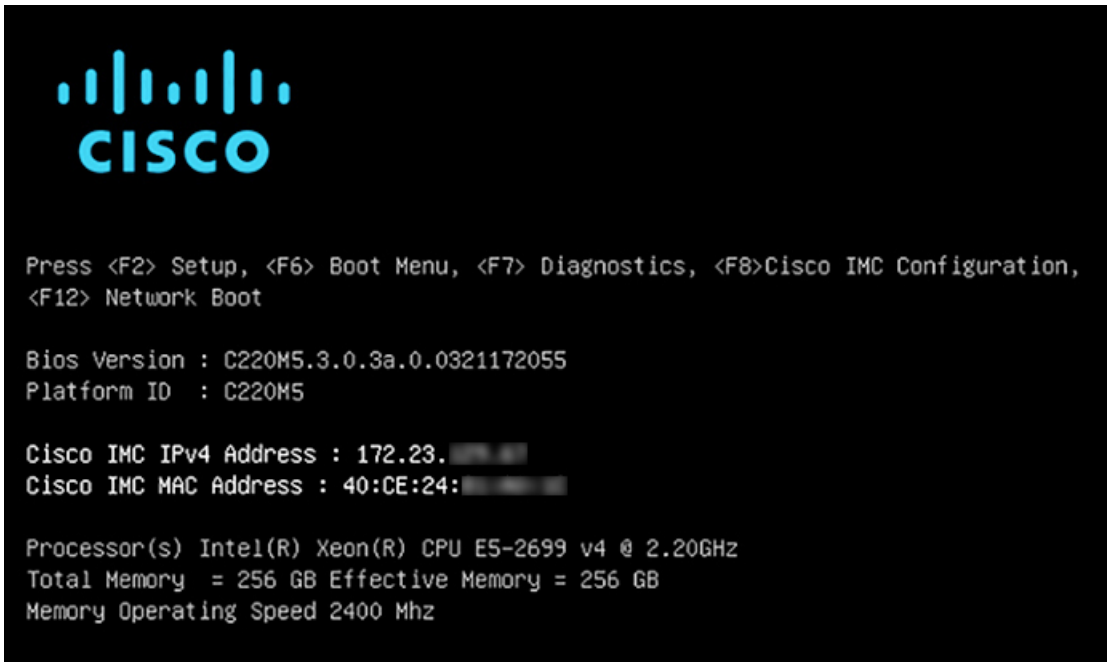
ステップ 1 次のいずれかを接続して、アプライアンスコンソールにアクセスします。

- 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。

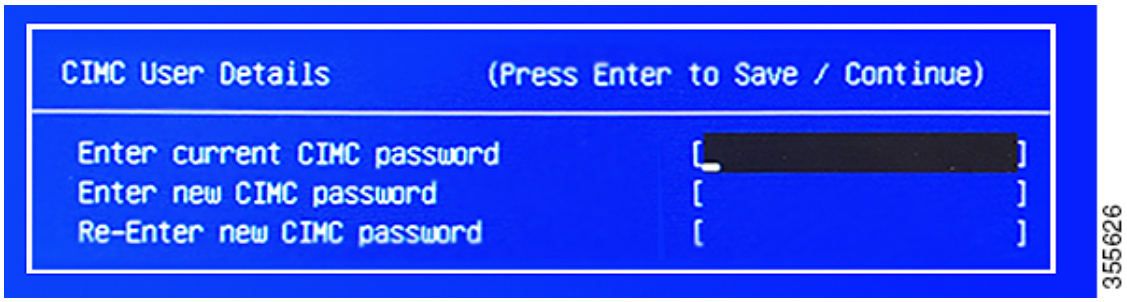
ステップ 3 前面パネルの**電源**ボタンを押して、アプライアンスをブートします。

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。

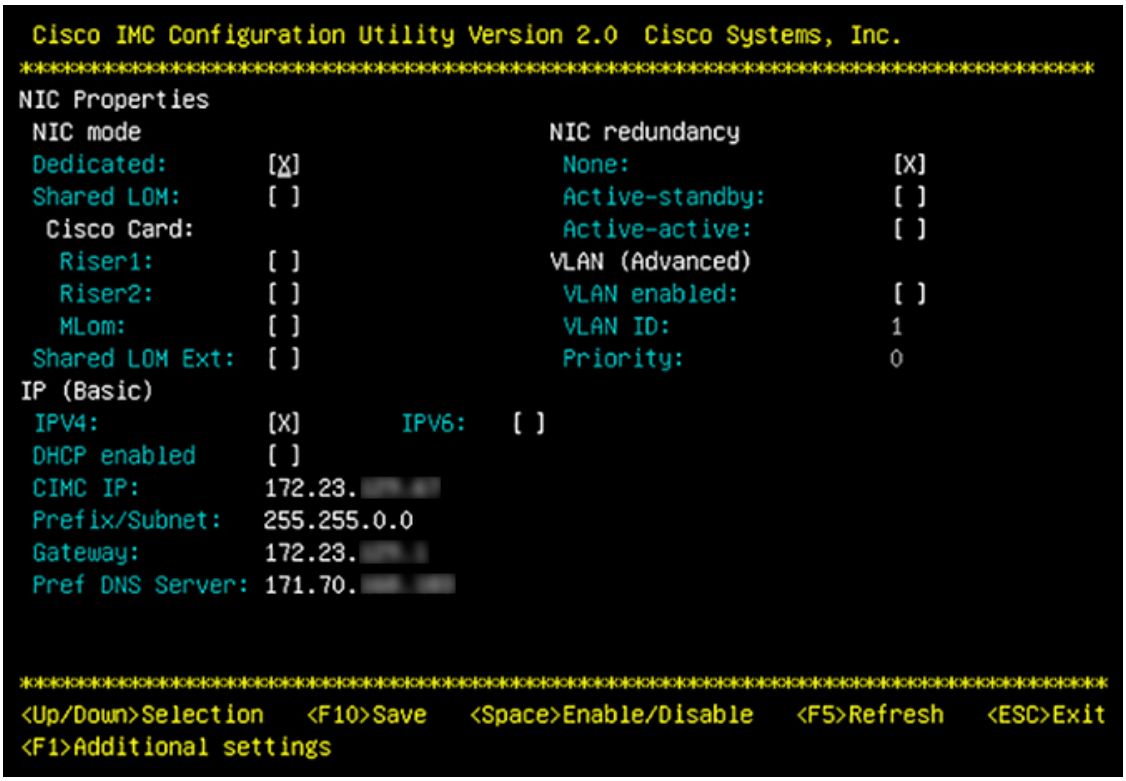
次に示すように、Cisco IMC 設定ユーティリティに **[CIMC ユーザの詳細（CIMC User Details）]** 画面が表示されます。



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。

ステップ 6 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。

[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。

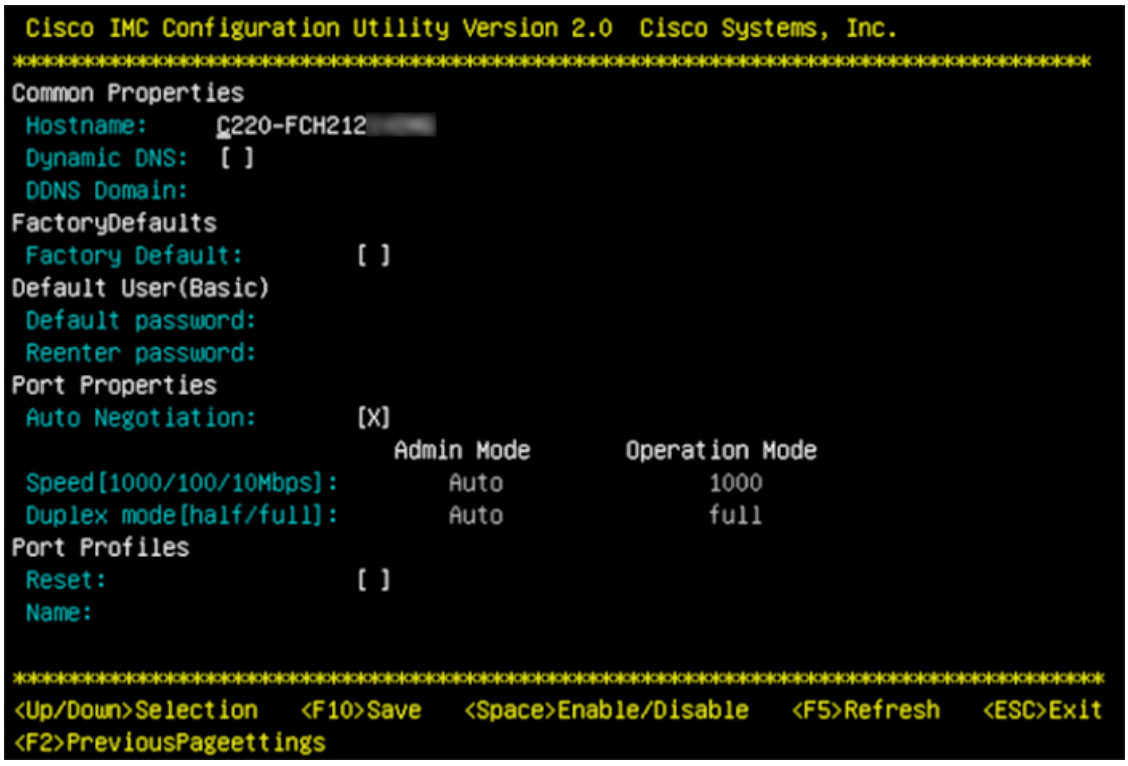


ステップ 7 次のアクションを実行します。

- **NIC モード（NIC mode）**：**[専用（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 **[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。

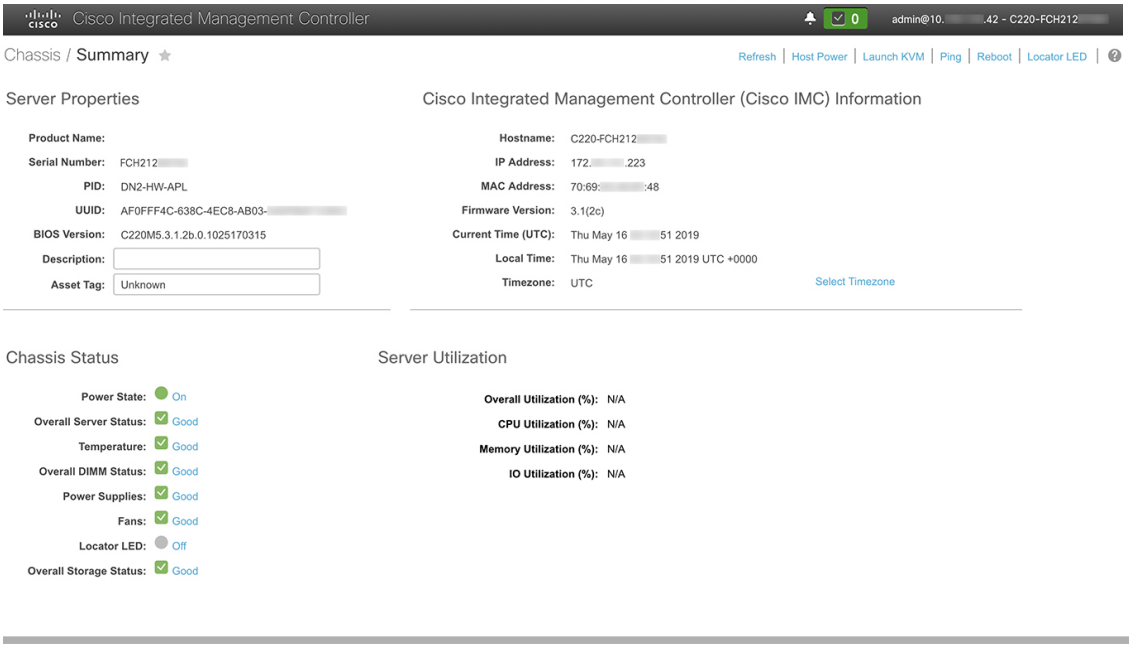
ステップ 11 **Esc** キーを押して終了し、アプライアンスをリブートします。

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。

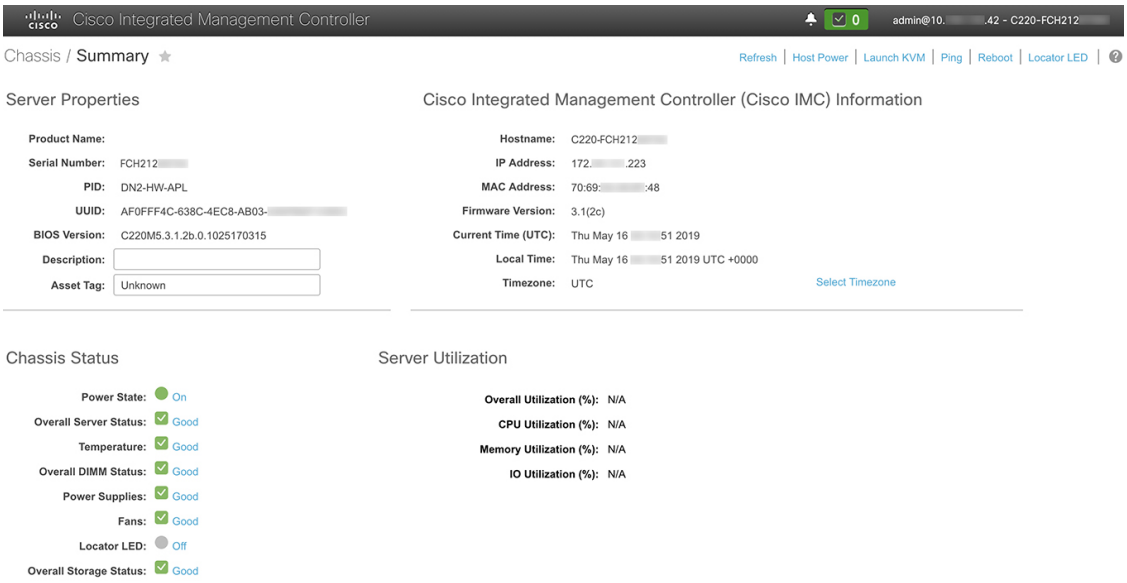


事前設定チェックの実行

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。このタスクは、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にする上で不可欠です。
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。

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 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。

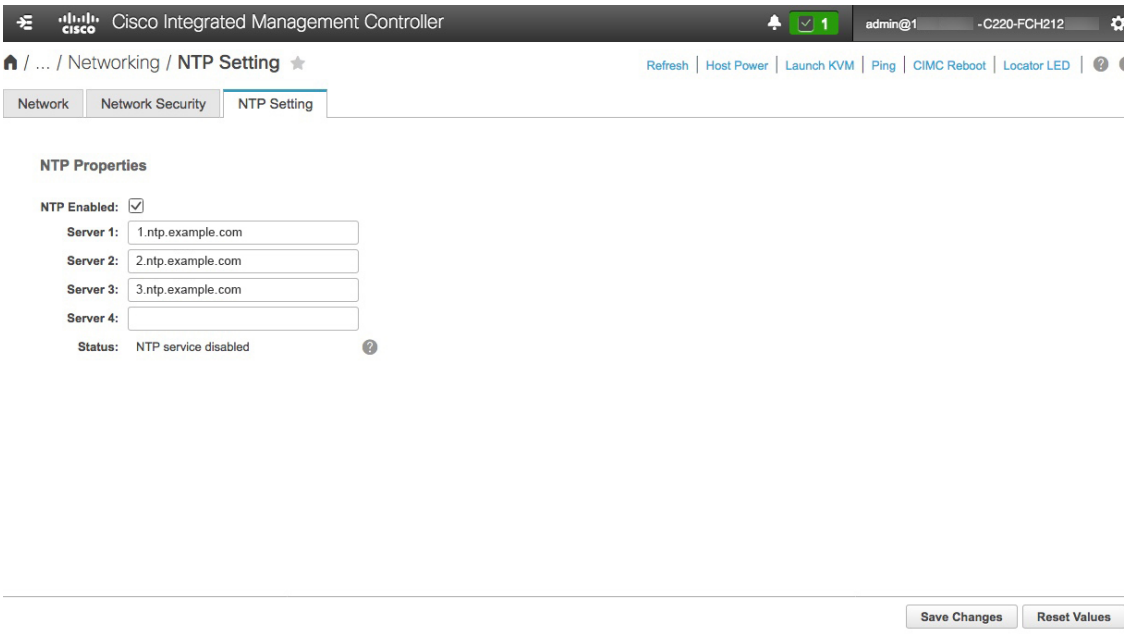


ステップ 2 次に示すように、アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol（NTP）サーバと同期します。

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。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） 第 1 世代の Cisco DNA Center アプライアンスとは異なり、第 2 世代の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。Cisco IMC で高スループットをサポートするために、第2世代アプライアンスにインストールされているネットワーク インターフェイス カード（NIC）を設定する必要はありません。すでにデフォルトで有効になっているためです。

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
```

（注） これらのコマンドは単なる例です。

重要 正常に機能させるには、第 2 世代 Cisco DNA 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、第1世代のアプライアンスのモードであるため、サポートされていません。

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

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。

ネットワーク インターフェイス カードの無効化

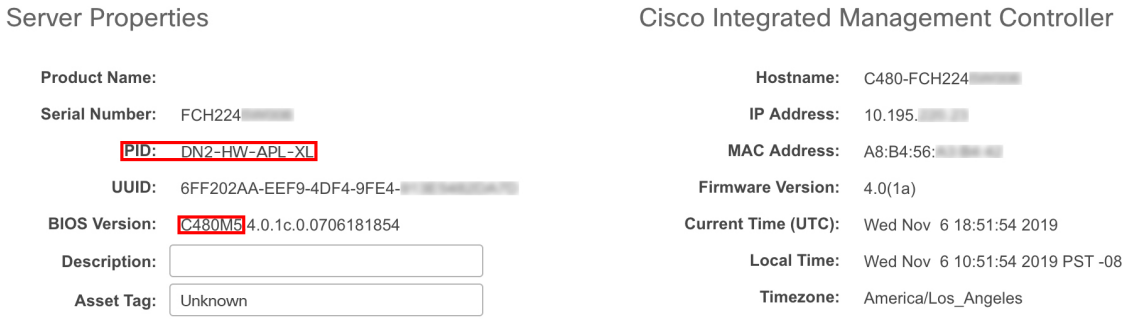
アプライアンスが Intel X710-DA4 ネットワーク インターフェイス カード（NIC）を有効にした状態で出荷されている場合は、次の手順を実行して無効にする必要があります。カードを無効にしない場合、アプライアンスには4つの追加インターフェイスが含まれているため、設定に悪影響を及ぼす可能性があります。

ステップ 1 Cisco DNA Center アプライアンスがあること、INTEL X710-DA4 NIC がインストールされていることを確認します。

a) アプライアンスの Cisco IMC にログインします。

b) **[概要（Summary）]** ウィンドウの **[サーバプロパティ（Server Properties）]** エリアに次の値が設定されていることを確認します。

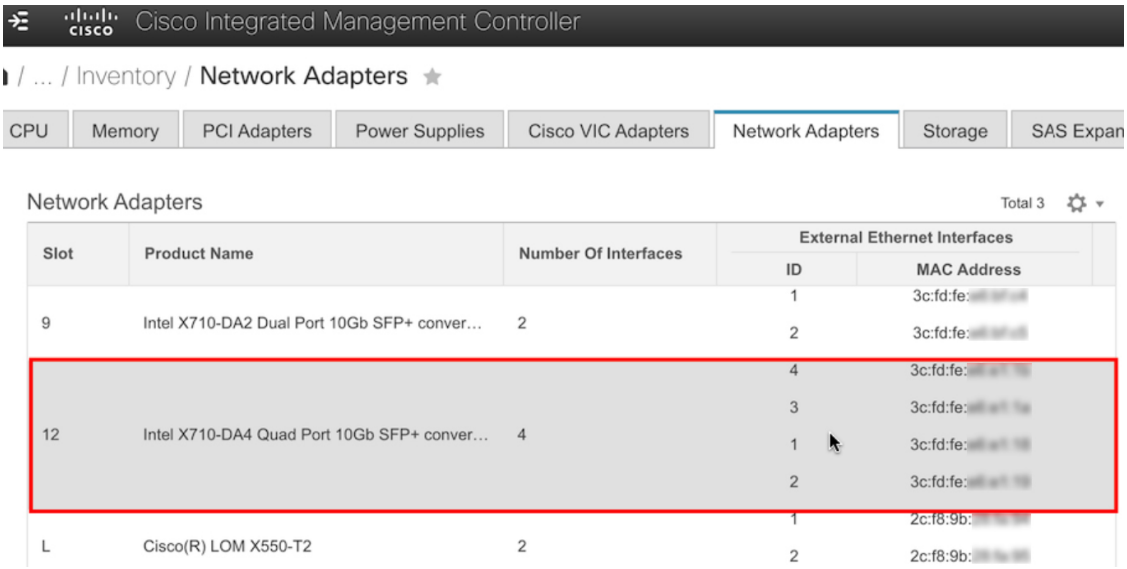
- PID：44 コアアプライアンスの場合は **DN2-HW-APL** 、56 コアアプライアンスの場合は **DN2-HW-APL-L**、112 コアアプライアンスの場合は **DN2-X-HW-APL-XL** です（次の例を参照）。
- BIOS バージョン：この値は 44 および 56 コアアプライアンスの **C220M5** 、または 112 コアアプライアンスの **C480M5** のいずれかで開始する必要があります（次の例を参照）。



c) > **[シャーシ（Chassis）]** > **[インベントリ（Inventory）]** > **[ネットワークアダプタ（Network Adaptor）]** を選択します。

d) **[ネットワークアダプタ（Network Adapters）]** 表で、次のスロットのいずれかに INTEL X710-DA4 Quad Port ネットワークアダプタが表示されていることを確認します。

- 44 または 56 コアアプライアンスの場合は**スロット 2**。
- 112 コアアプライアンスの場合は**スロット 12**（次の例を参照）。



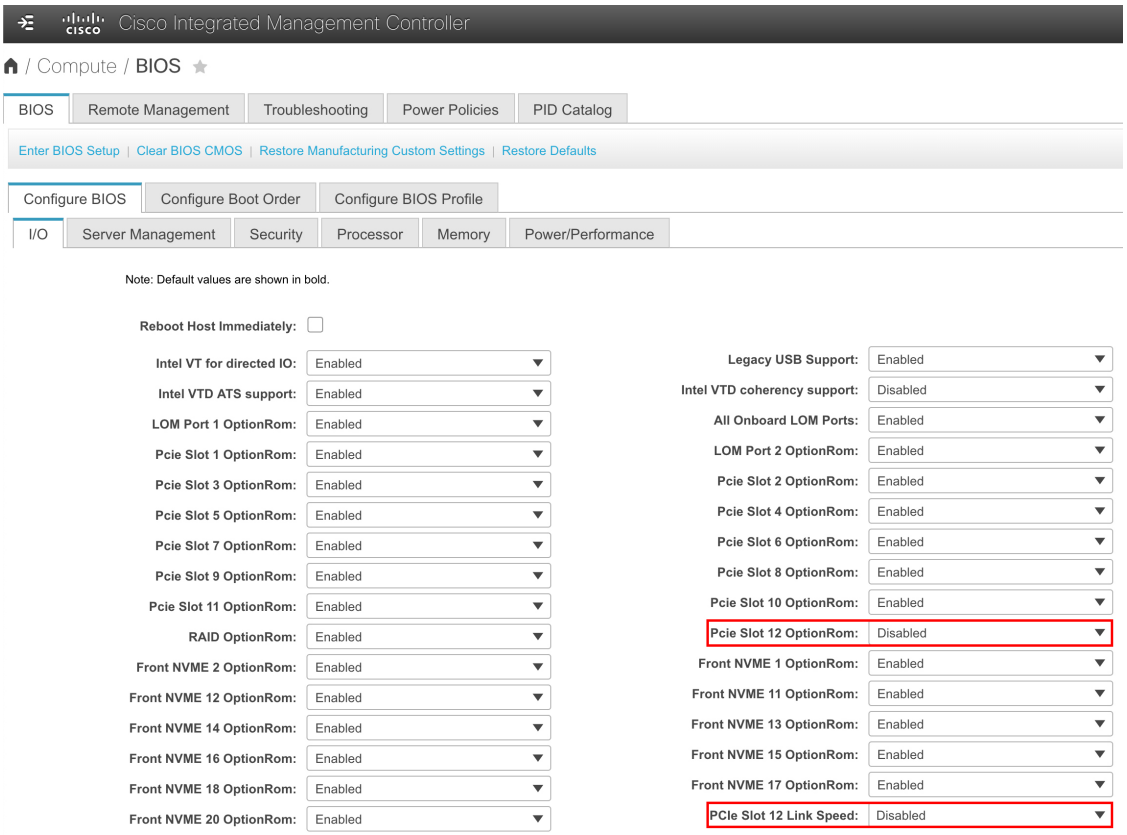
ステップ 2 次の要領でアプライアンスの PCIe カードが無効になっていることを確認します。

a) > **[コンピューティング（Compute）]** を選択します。

[BIOS] > **[BIOS の設定（Configure BIOS）]** > **[I/O]** タブが開きます。

b) 次のパラメータを**[Disabled（無効）]** に設定してから、**[保存（Save）]** をクリックします。

- 44 または 56 コアアプライアンスの場合、**PCIe スロット 2 OptionROM** と **PCIe スロット 2 リンク速度**。
- 112 コアアプライアンスの場合は **PCIe スロット 12 OptionROM** および **PCIe スロット 12 リンク速度**（次の例を参照）。



c) 次のいずれかを実行します。

- アプライアンスでこれら 2 つのパラメータを **[無効（Disabled）]** に設定できる場合は、アプライアンスをリブートして、設定を続行します。この手順の残りを実行する必要はありません。
- お使いの 112 コアアプライアンスで **[I/O]** タブにこれらのパラメータのいずれか 1 つのみ表示される場合は、ステップ 3 に進み、残りの手順を実行します。

ステップ 3 アプライアンスの BIOS を起動します。

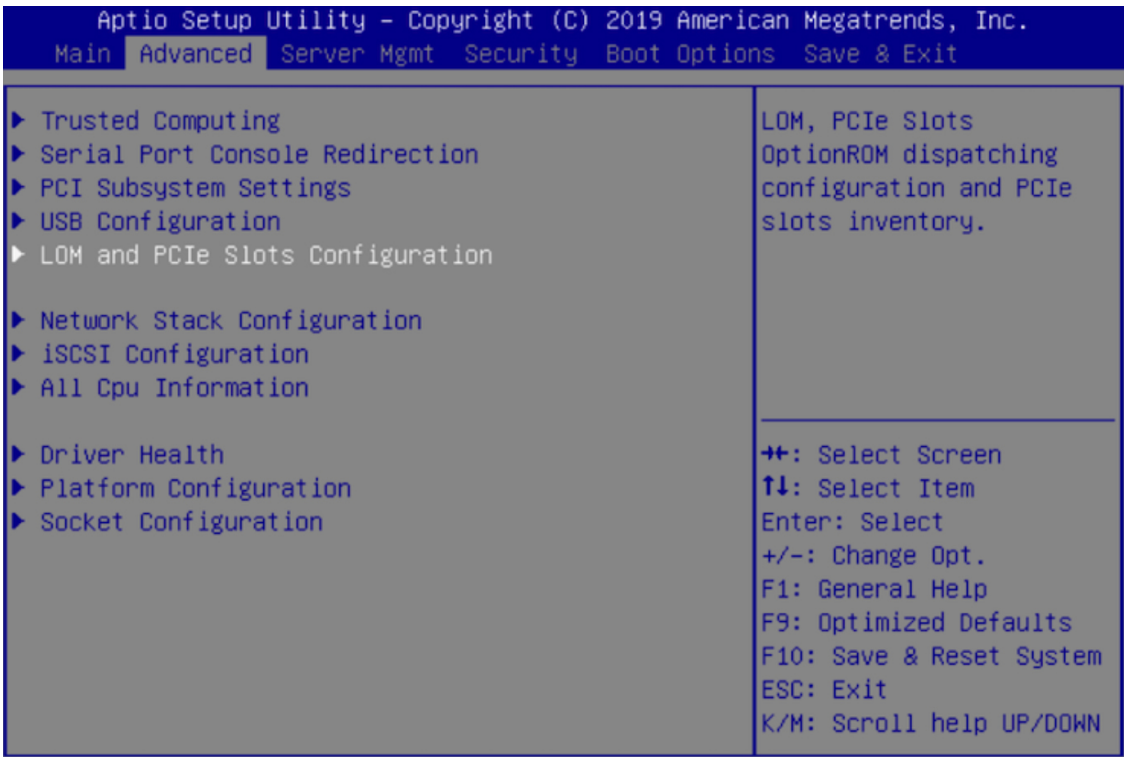
a) Cisco IMC から KVM セッションを開始します。

b) **[ホスト電源（Host Power）]** リンクをクリックしてから **[電源の再投入（Power Cycle）]** を選択し、アプライアンスの電源を再投入します。

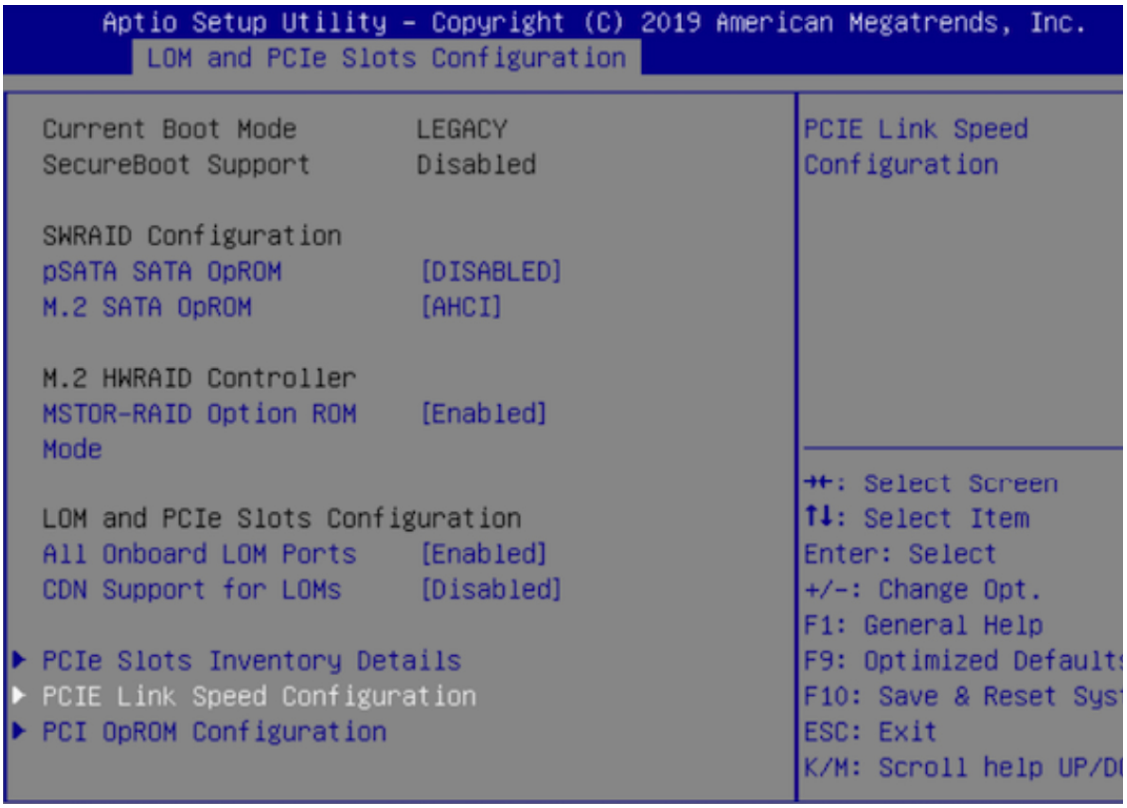
c) 起動時に、次の画面が表示されたらすぐに **F2** キーを押してアプライアンスの BIOS を起動し、Aptio セットアップ ユーティリティを開きます。

ステップ 4 次の要領で PCIe カードを無効にします。

a) Aptio セットアップユーティリティの **[メイン（Main）]** タブで **[詳細（Advanced）]** タブを選択し、**[LOMとPCIeスロットの設定（LOM and PCIe Slots Configuration）]** を選択します。



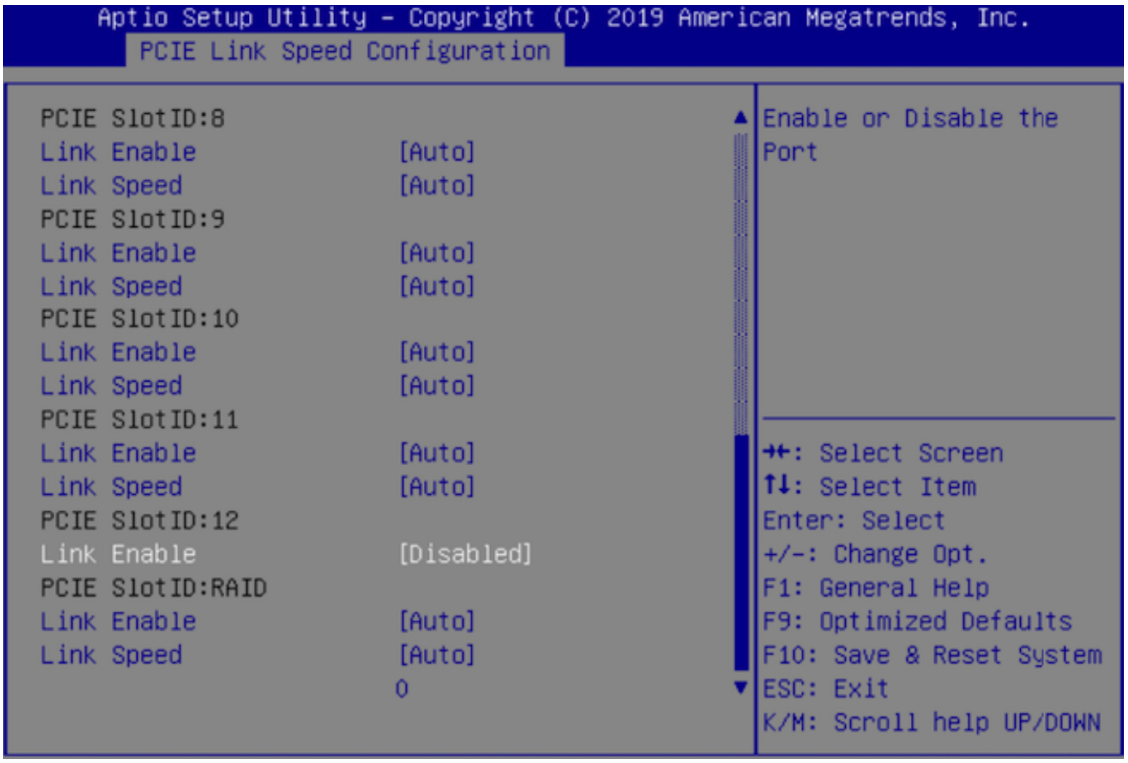
b) **[LOMおよびPCIeスロットの設定（LOM and PCIe Slots Configuration）]** タブで **[PCIeリンク速度の設定（PCIe Link Speed Configuration）]** を選択します。



c) **[PCIe リンク速度の設定（PCIe Link Speed Configuration）]** タブを下向きにスクロールして PCIe SlotID：12 の **[リンク有効化（Link Enable）]** オプションを見つけ、**Enter** を押します。

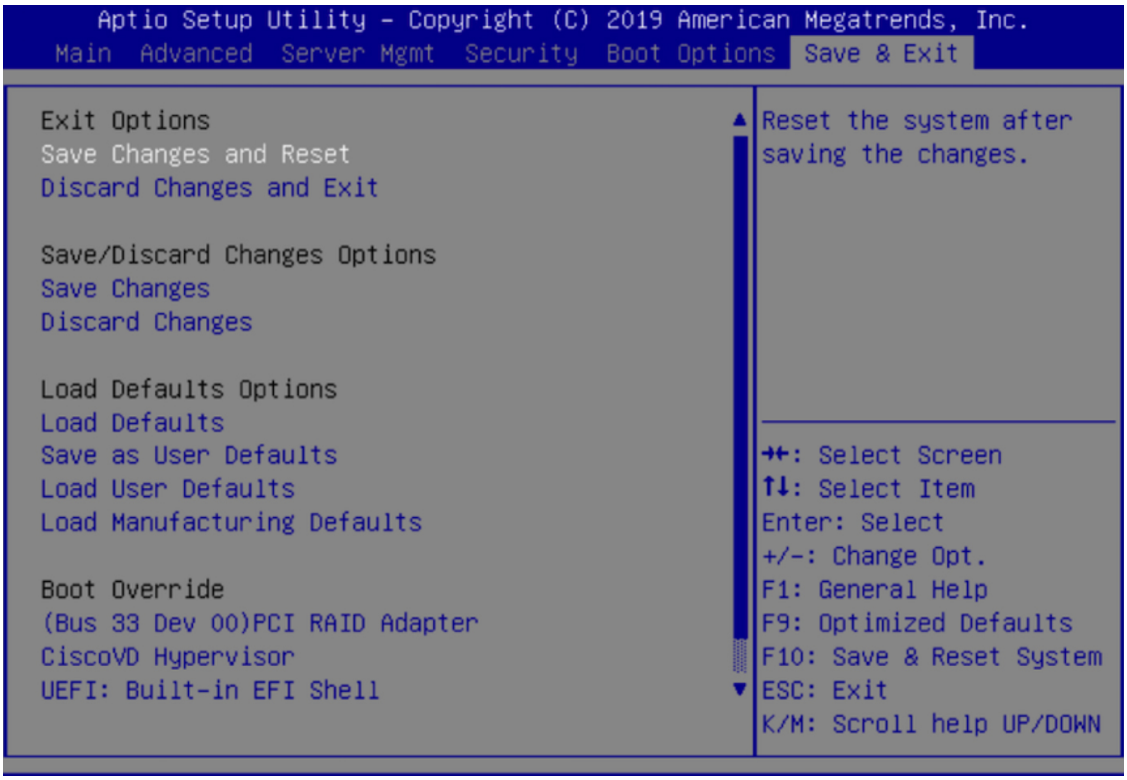
d) **[無効化（Disable）]** を選択し、**Enter** を押します。

次の例のような画面が表示されます。



e) **ESC**キーを 2 回押してメインの BIOS メニューに戻り、**[保存して終了（Save & Exit）]** タブを開きます。

f) **[変更を保存してリセット（Save Changes And Reset）]** オプションを選択し、**Enter** を押します。



アプライアンスがリブートし、設定ウィザードが開きます。アプライアンスの設定を続けます。

重要 アプライアンスの NIC を無効にした後、 > **[管理者（Admin）]** > **[ユーティリティ（Utilities）]** > **[工場出荷時のデフォルトにリセット（Reset to factory Default）]** でアプライアンスを Cisco IMC のデフォルト設定にリセットした場合は、この手順をもう一度実行する必要があります。

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。

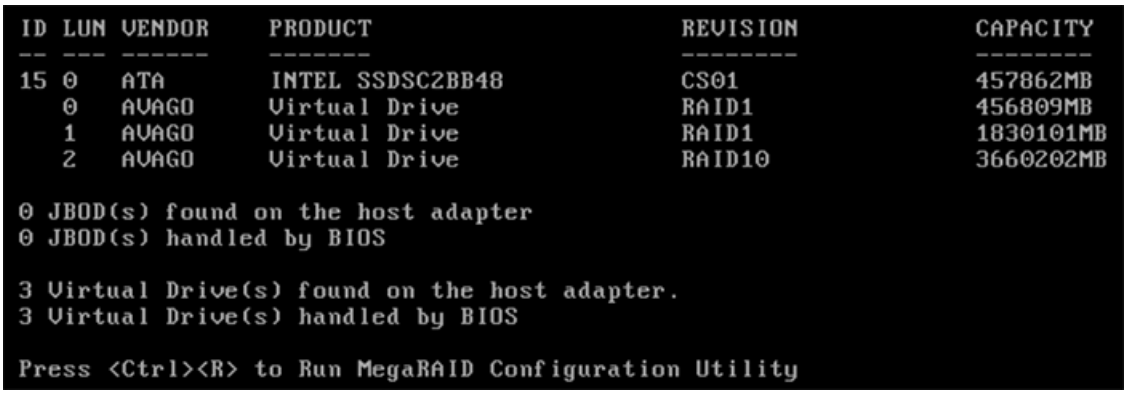
ステップ 3 アプライアンスの RAID コントローラによって管理されている 3 つの仮想ドライブを再初期化します。

a) CIMC 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。

- **[電源（Power）] > [システムの電源オン（Power On System）]**
- **[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））]**

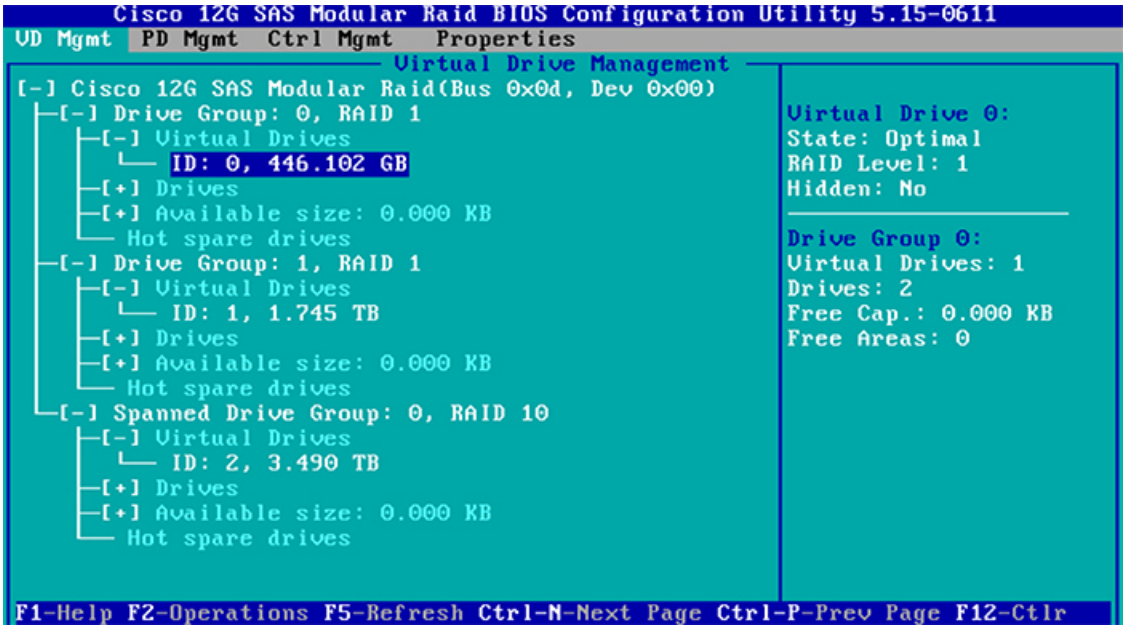
アプライアンスがリブートされると、アプライアンス上のすべてのドライブ（物理と仮想の両方）を一覧表示する画面が表示されます。



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 **[電源（Power）] > [システムのリセット（ウォームブート）（Reset System（warm boot））]** を選択して、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 **[初期化（Initialization）] > [高速初期化（Fast 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。

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」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 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。

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。

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**

たとえば cdnac-sw-1.3 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-1.3.iso of=/dev/sdd bs=4M && sync**

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-1.3.iso という Cisco DNA Center 1.3 の 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-1.3.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-1.3 CDNAC-SW-1.3.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**

この例を続け、次のコマンドを実行します。 **sudo dd if=CDNAC-1.3.dmg of=/dev/disk2 bs=1m**

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 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 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。

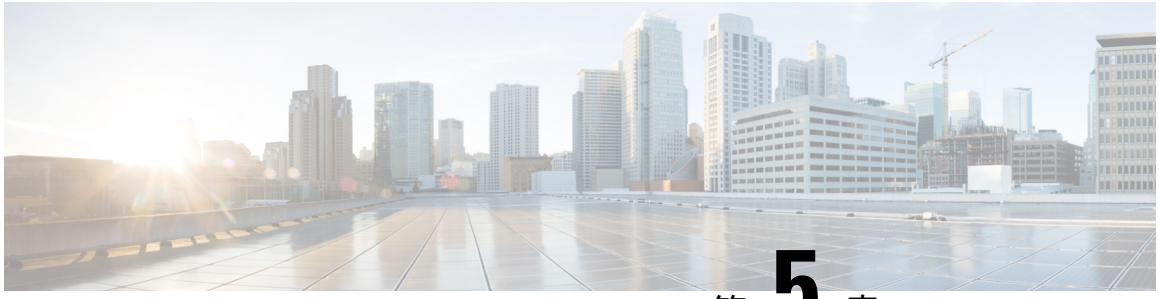
ブートデバイス選択メニューが表示されます。

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 設定ウィザードの初期画面が開きます。マスタまたはセカンダリクラスタノードを設定するかどうかに応じて、ステップ 4の「Maglev ウィザードを使用したマスタノードの設定」または、「Maglev ウィザードを使用したアドオンノードの設定」のいずれかに進みます。



第 5 章

アプライアンスの設定

アプライアンスの設定の概要

次の2つのモードのいずれかを使用すると、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：3 ノードクラスタに属するノードとして。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マスタ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、マスタノードの設定を完了してください。

続行するには、次のタスクを実行します。

1. Cisco IMC から Maglev 設定ウィザードを起動し、クラスタ内のマスタノードを設定します。「Maglev ウィザードを使用したマスタノードの設定」を参照してください。
2. 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、「Maglev ウィザードを使用したアドオンノードの設定」を参照してください。

Maglev ウィザードを使用したマスタノードの設定

最初にインストールされたアプライアンスをマスタ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、常にマスタノードとして設定する必要があります。

すでにマスタノードがある既存のクラスタのアドオンノードとしてインストールされたアプライアンスを設定する場合には、代わりに「Maglev ウィザードを使用したアドオンノードの設定」の手順を実行します。

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「必須の設定情報」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。
- 「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」の説明に従って、マスタノードで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「事前設定チェックの実行」の説明に従って、マスタ 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。
- Cisco IMC、Cisco DNA Center との互換性があるブラウザを使用しています。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 お使いのブラウザで、実行した Cisco IMC GUI 設定で設定した Cisco IMC の IP アドレスをポイントし、Cisco IMC ユーザとして Cisco IMC GUI にログインします（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。

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 Cisco IMC 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 マスタノードの設定を開始するには、[Cisco DNA Centerクラスタを開始する（Start a DNA-C Cluster）] を選択します。

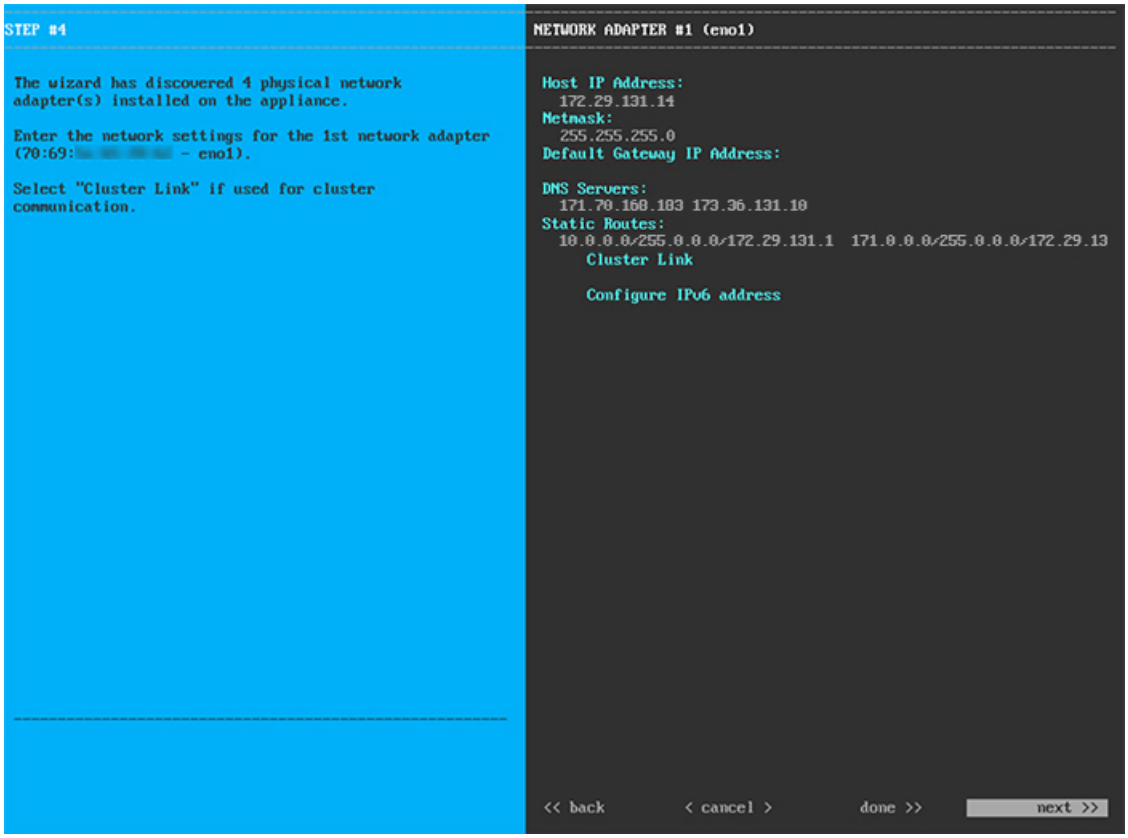
ウィザードでは、アプライアンス上のすべてのポートが検出され、次の順序で 1 つずつ別の画面に表示されます。

1. 1Gbps/10Gbps 管理ポート（1、eno1/enp53s0f0、ネットワークアダプタ #1）
2. 1Gbps/10Gbps クラウドポート（eno2/enp53s0f1、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/enp69s0f0、ネットワークアダプタ #3）
4. 10Gbps クラスタポート（enp94s0f1/enp69s0f1、ネットワークアダプタ #4）

（注） 44、56、および 112 コアアプライアンスのポートに割り当てられているインターフェイス名が異なります。この手順で 2 つのインターフェイス名が指定された場合は、1 つ目が 44 および 56 コアアプライアンスに適用され、2 つ目が 112 コアアプライアンスに適用されます。

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「事前設定チェックの実行」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/enp53s0f0）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「必須の設定情報」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。

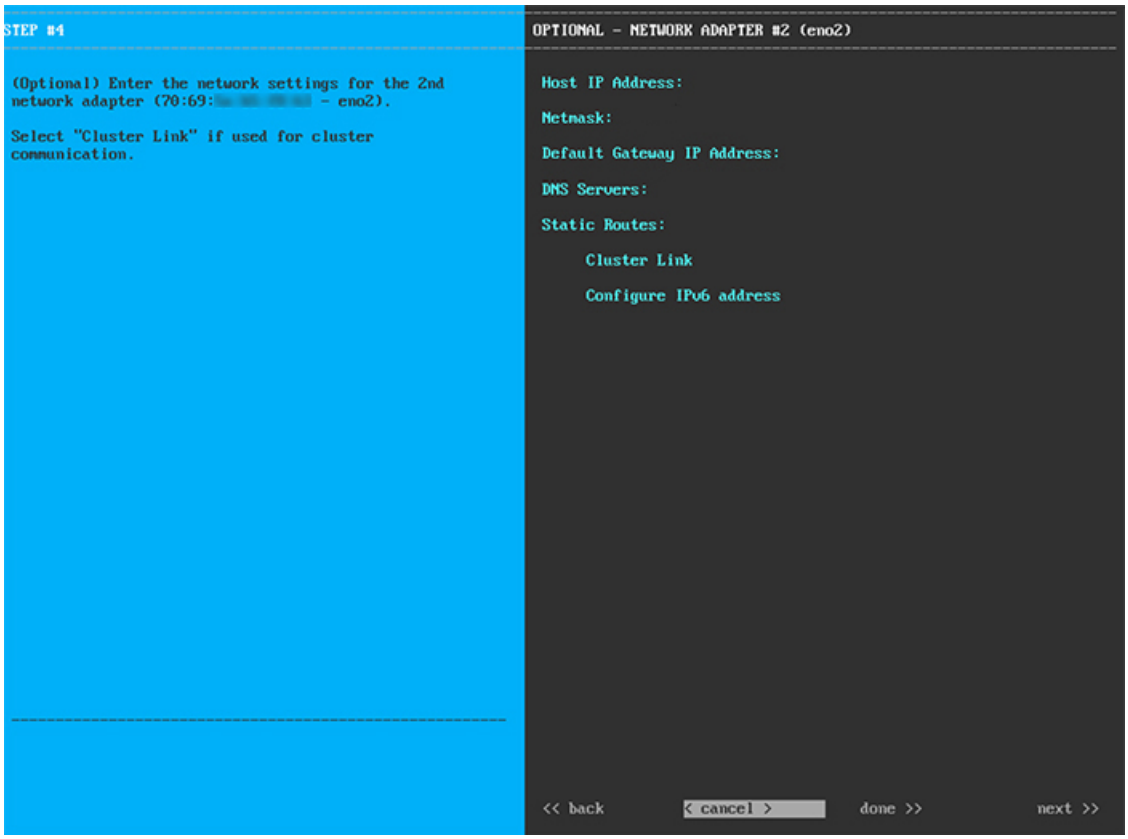
表 *21 :* ネットワークアダプタ *#1* のマスタノードエントリ：*1Gbps/10Gbps* 管理ポート（*eno1/enp53s0f0*）

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。これは必須です。
ネットマスク（Netmask）	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。この IP アドレスは、通常、エンタープライズポートのみで必要になります。

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 121（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 1 Gbps /10 Gbps クラウドポート（2、eno2/enp53s0f1）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、10 Gbps エンタープライズポート（enp94s0f0/enp69s0f0）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「必須の設定情報」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。

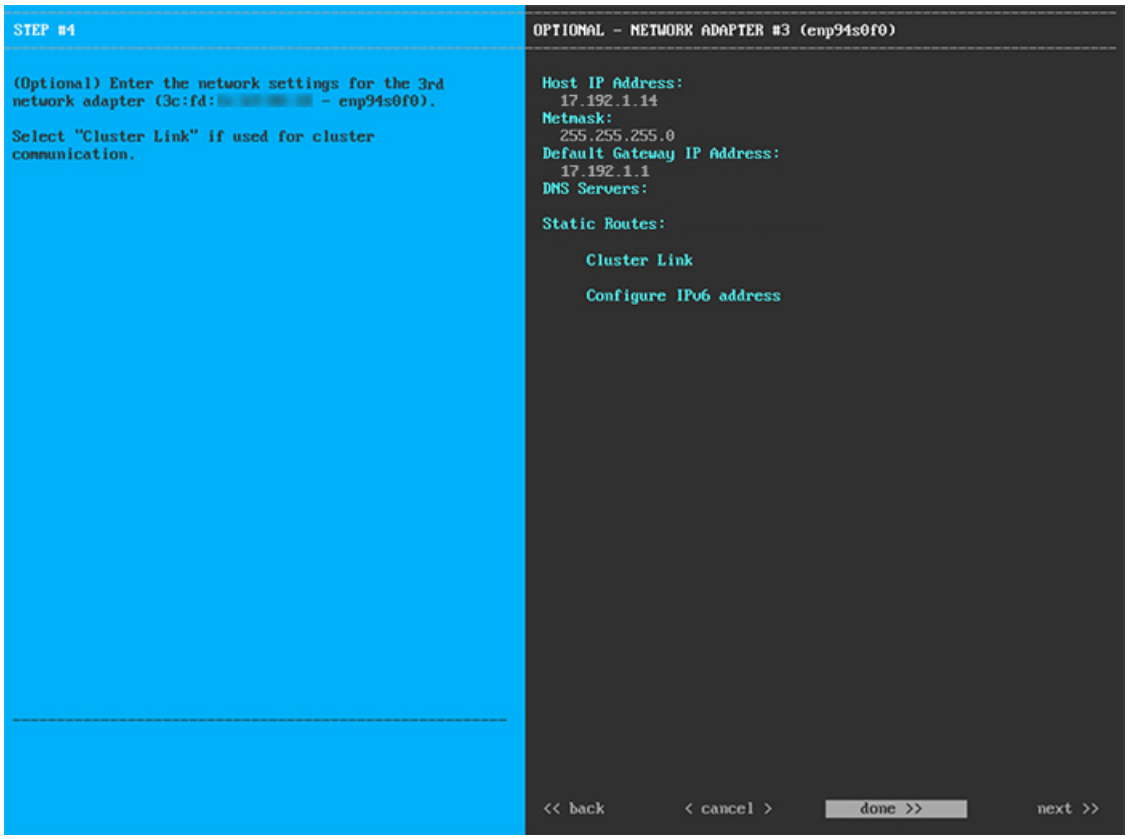
表 *22 :* ネットワークアダプタ *#2* のマスタノードエントリ：*1 Gbps/10 Gbps* クラウドポート（*eno2/enp53s0f1*）

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（Netmask）	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 アドレスを入力してください。この IP アドレスは、通常、エンタープライズポートのみで必要になります。

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のみで必要になります。
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10 Gbps エンタープライズポート（enp94s0f0/enp69s0f0）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「必須の設定情報」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。

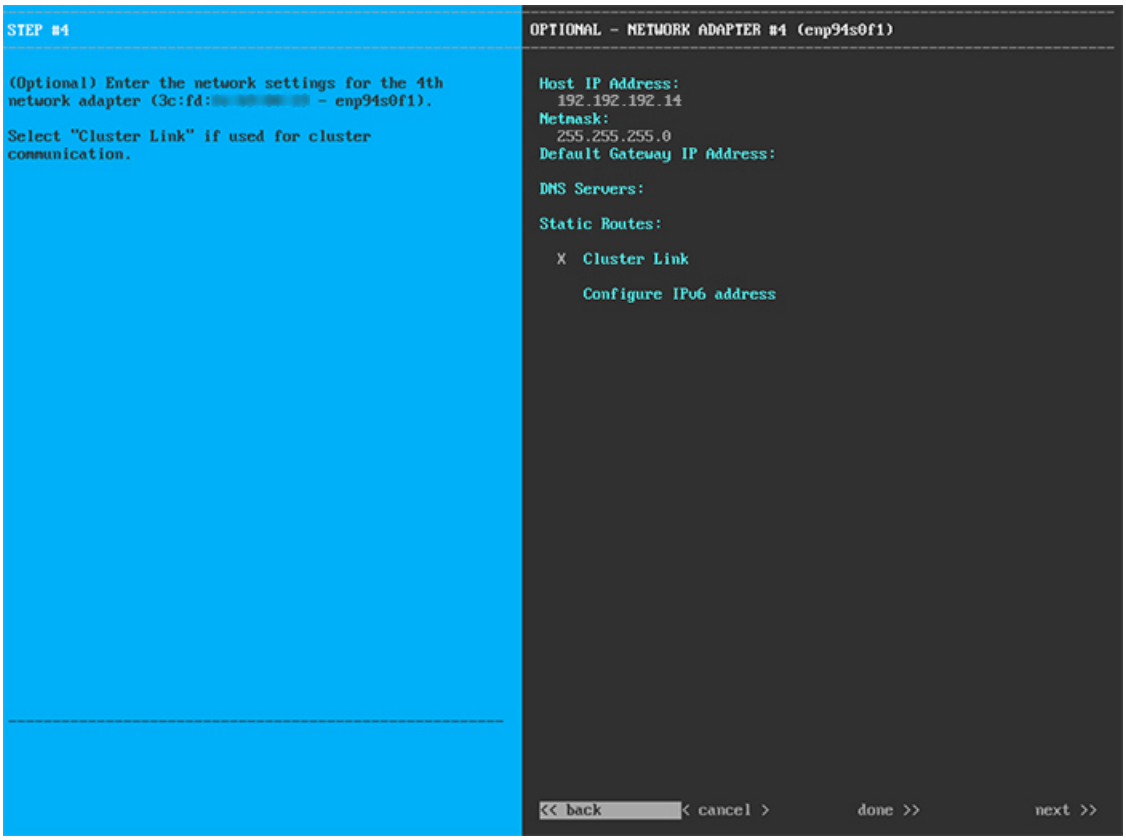
表 *23 :* ネットワークアダプタ *#3* のマスタノードエントリ：*10Gbps* エンタープライズポート（*enp94s0f0/enp69s0f0*）

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（Netmask）	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のみで必要になります。
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10 Gbps クラスタポート（enp94s0f1/enp69s0f1）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「必須の設定情報」を参照してください）。



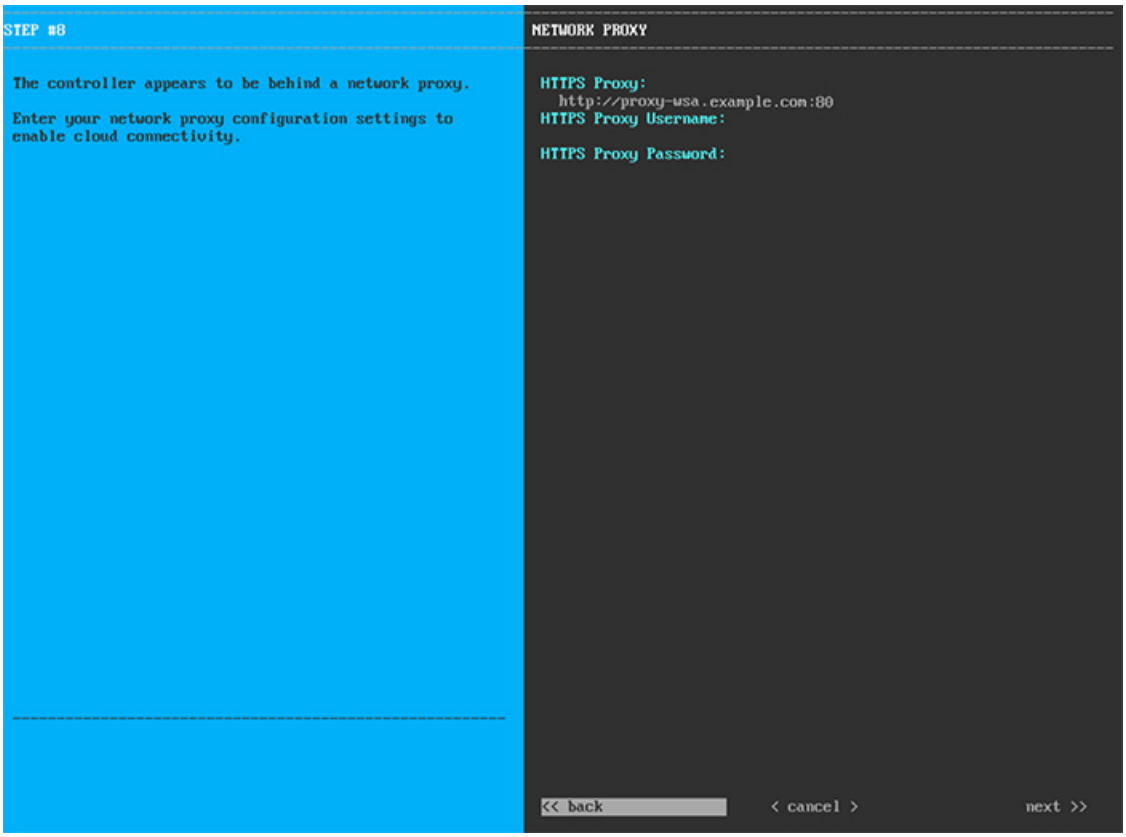
次の表に示すように、[ネットワークアダプタ#4（NETWORK ADAPTER #4）] の設定値を入力します。

表 *24 :* ネットワークアダプタ *#4* のマスタノードエントリ：*10 Gbps* クラスタポート（*enp94s0f1/enp69s0f1*）

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。
[Netmask]	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。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
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 *25*：ネットワークプロキシのマスタノードエントリ

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、マスタノードの仮想 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。

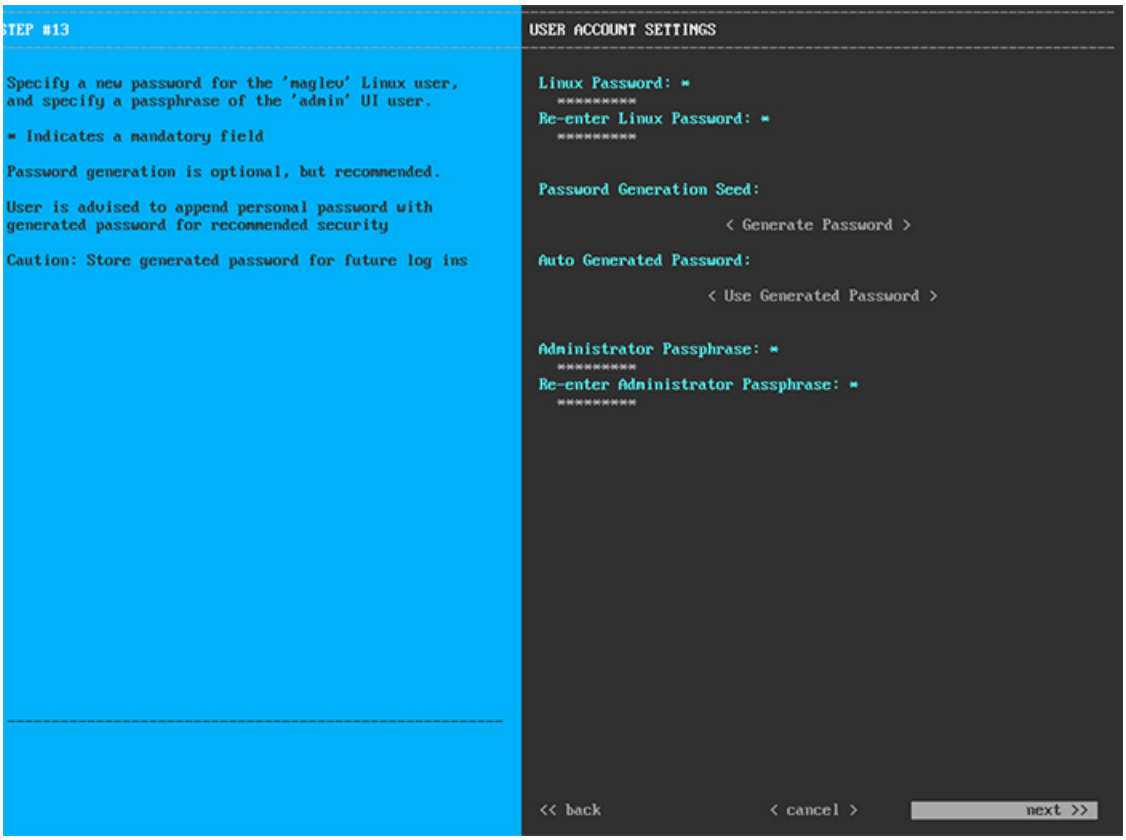
重要　設定済みのネットワークインターフェイスごとに 1 つずつ仮想 IP アドレスを入力する必要があります。この操作を行わない限り、ウィザードを完了することはできません。これらのアドレスは、クラスタリンクのステータスに関連付けられており、ステータスは **[アップ（UP）]** の状態となっている必要があります。

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 ではこのドメイン名を使用して次の操作が実行されます。

- 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。

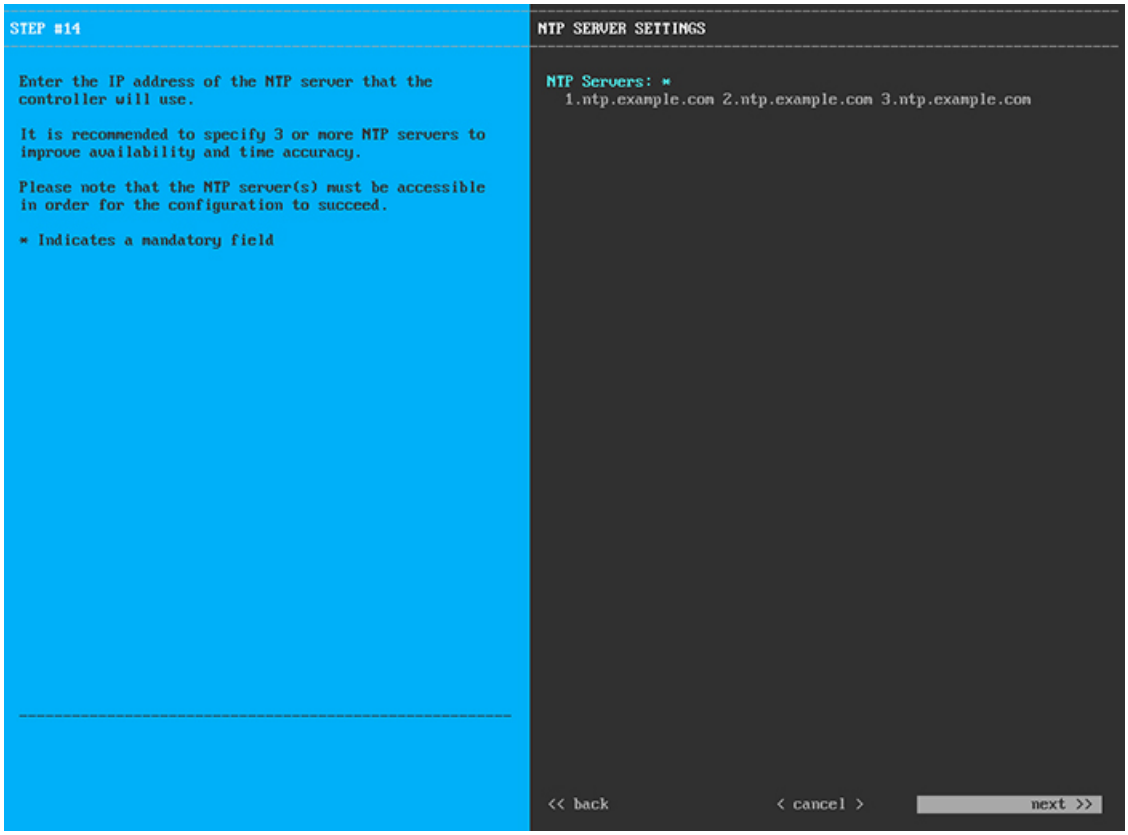
表 *26* : ユーザアカウント設定のマスタノードエントリ

Linux パスワード	maglev ユーザに対して設定されている 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（Administrator Passphrase）	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。

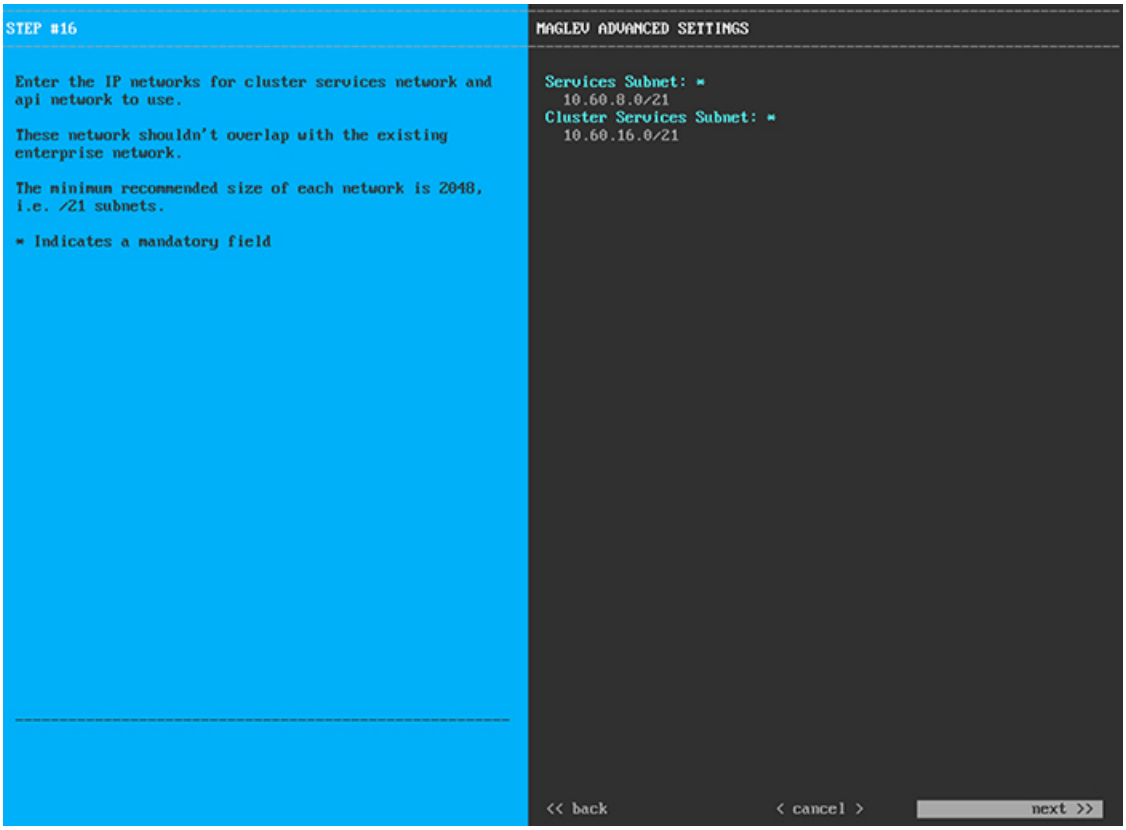
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように、[NTPサーバの設定（NTP SERVER SETTINGS）] の値を入力するようウィザードに求められます。



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 サーバを設定することを推奨します。

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。



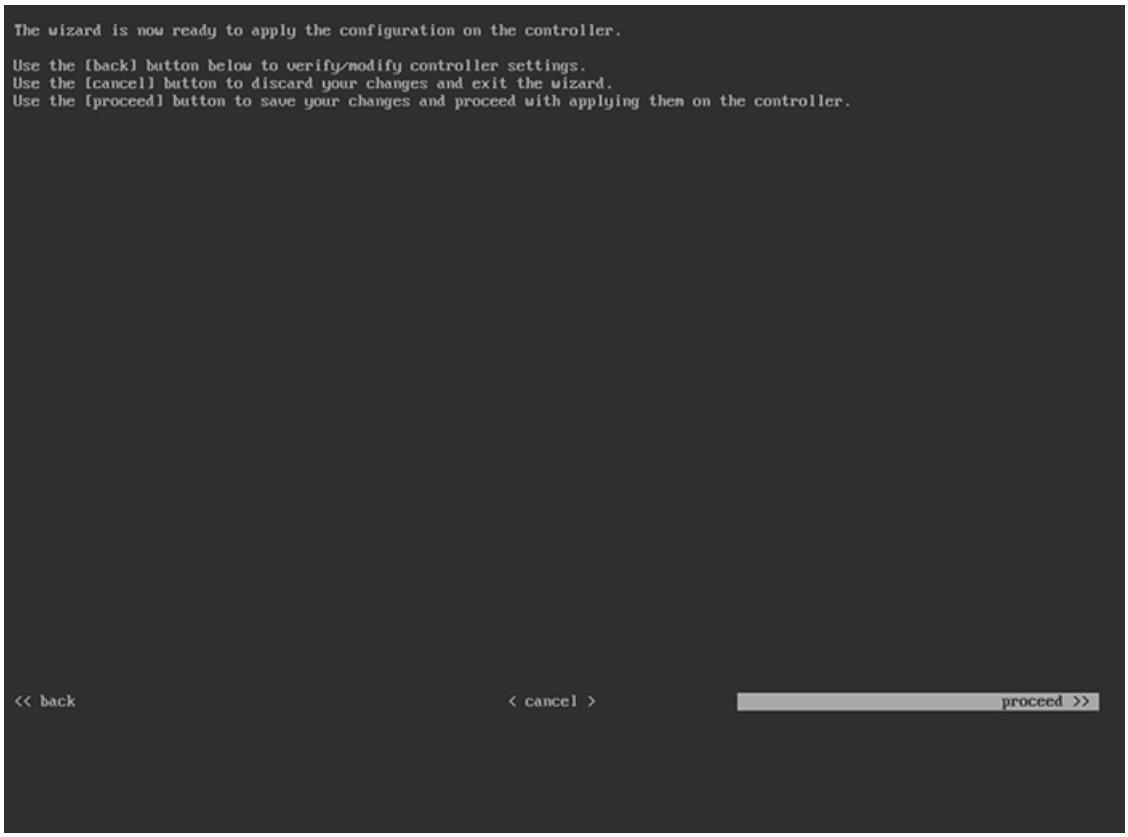
次の表に示すように、[MAGLEV 詳細設定（MAGLEV ADVANCED SETTINGS）] の設定値を入力します。

表 *27 : Maglev* 詳細設定のマスタノードエントリ

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マスタ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 番目のインストール済みアプライアンスを設定します（「Maglev ウィザードを使用したアドオンノードの設定」）。

Maglev ウィザードを使用した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。

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マスタ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マスタ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、マスタノードの 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-master-1) ~
$ 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。

- 「Maglev ウィザードを使用したマスタノードの設定」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「必須の設定情報」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。
- 「Cisco Integrated Management Controller に対する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 Cisco Integrated Management Controller に対するブラウザのアクセス権が設定されたこと。

- 「事前設定チェックの実行」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を確認しました。
- 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 設定ウィザードでは 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 お使いのブラウザで、実行した cisco imc GUI 設定で設定した Cisco IMC の IP アドレスをポイントし、cisco imc ユーザとして Cisco IMC GUI にログインします（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。

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 設定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 Cisco IMC 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 設定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。

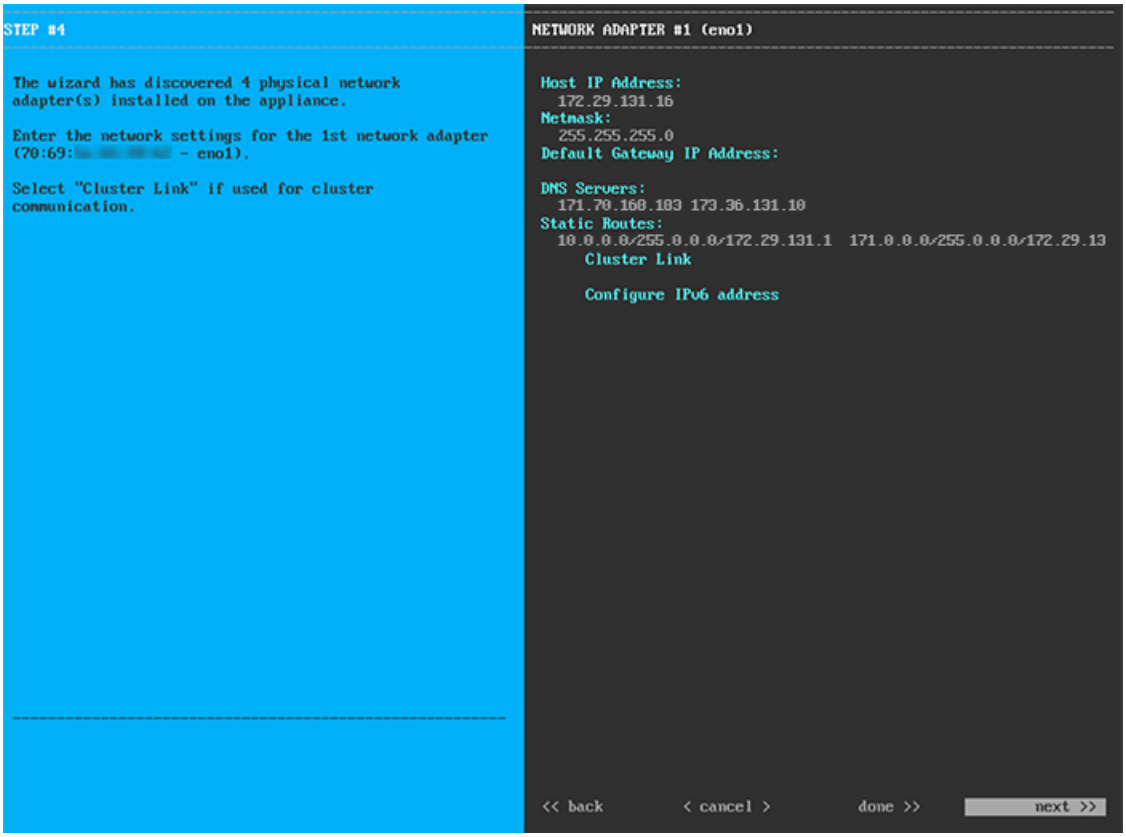
1. 1Gbps/10Gbps 管理ポート（1、eno1/enp53s0f0、ネットワークアダプタ #1）
2. 1Gbps/10Gbps クラウドポート（eno2/enp53s0f1、ネットワークアダプタ #2）
3. 10Gbps エンタープライズポート（enp94s0f0/enp69s0f0、ネットワークアダプタ #3）
4. 10Gbps クラスタポート（enp94s0f1/enp69s0f1、ネットワークアダプタ #4）

（注） 44、56、および 112 コアアプライアンスのポートに割り当てられているインターフェイス名が異なります。この手順で 2 つのインターフェイス名が指定された場合は、1 つ目が 44 および 56 コアアプライアンスに適用され、2 つ目が 112 コアアプライアンスに適用されます。

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。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「事前設定チェックの実行」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/enp53s0f0）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「必須の設定情報」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。

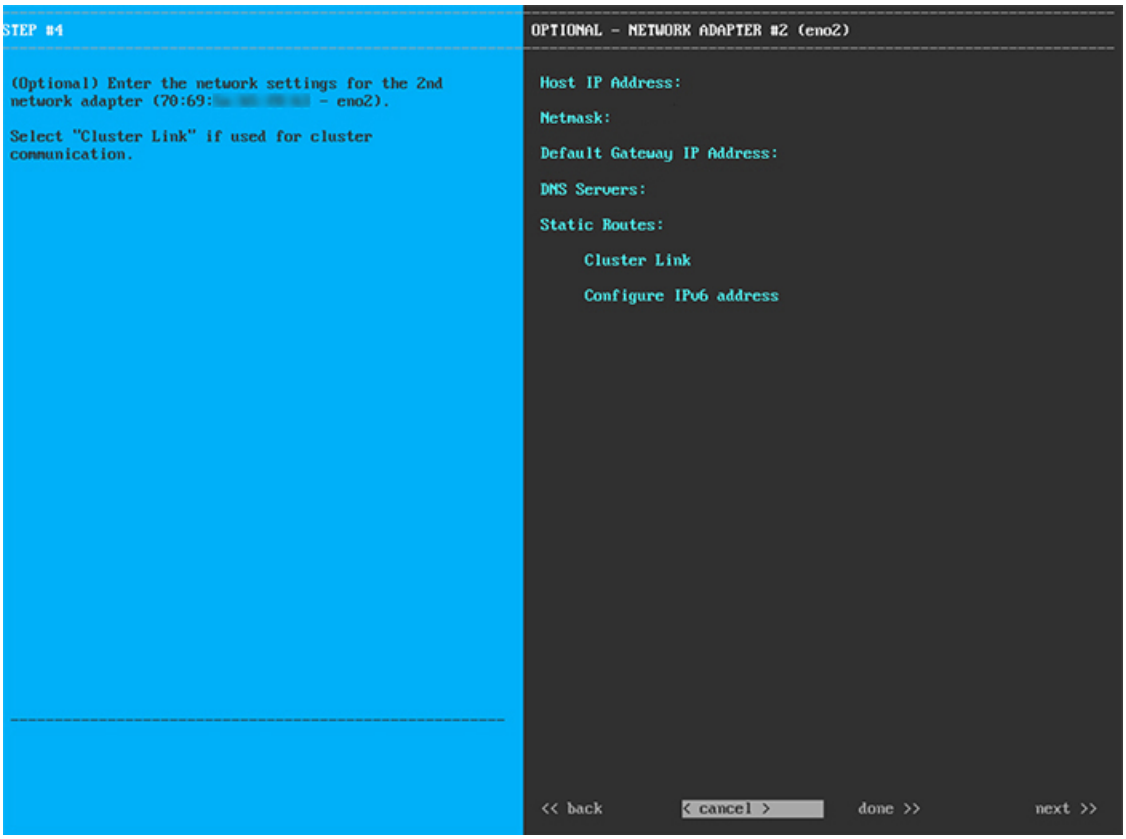
表 *28* : ネットワークアダプタ *#1* のアドオンノードエントリ：*1Gbps/10Gbps* 管理ポート（*eno1/enp53s0f0*）

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。これは必須です。
[Netmask]	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。この IP アドレスは、通常、エンタープライズポートのみで必要になります。

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 121（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、<ネットワーク>/<ネットマスク>/<ゲートウェイ> 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 1 Gbps /10 Gbps クラウドポート（2、eno2/enp53s0f1）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、10 Gbps エンタープライズポート（enp94s0f0/enp69s0f0）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「必須の設定情報」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。

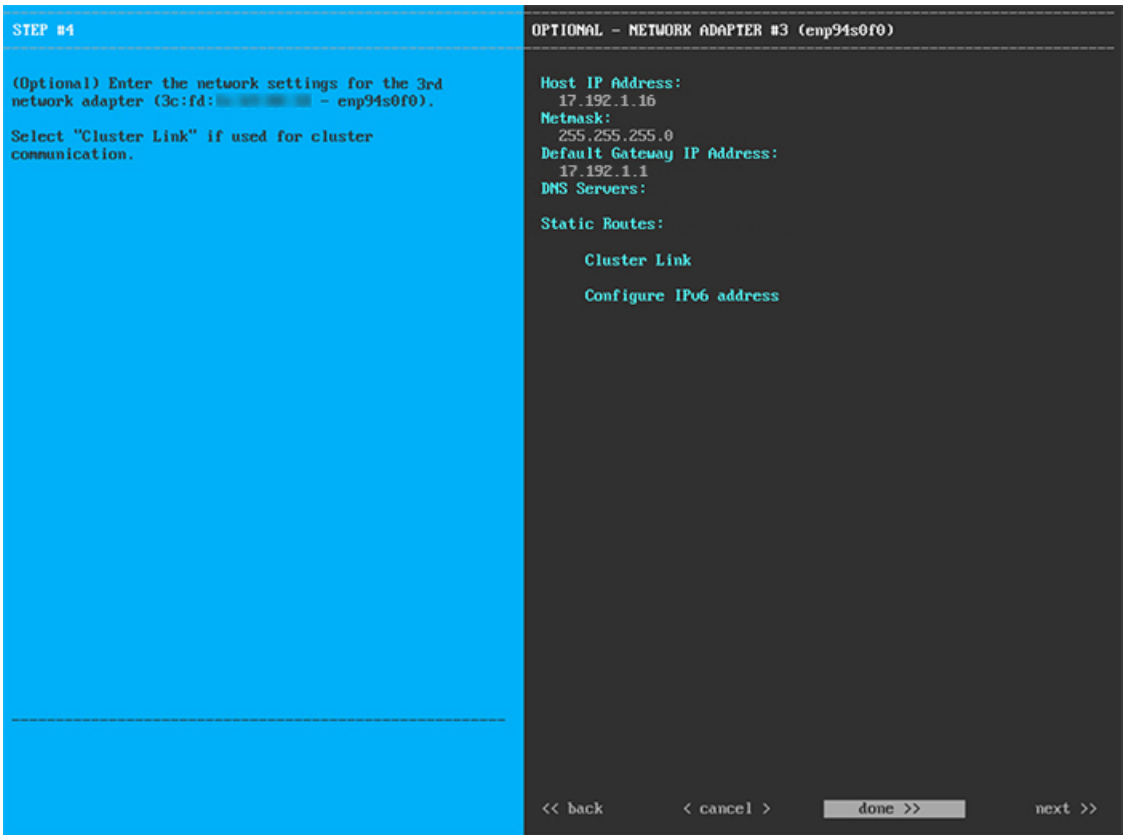
表 *29* : ネットワークアダプタ *#2* のアドオンノードエントリ：*1Gbps/10Gbps* クラウドポート（*eno2/enp53s0f1*）

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。
[Netmask]	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。この IP アドレスは、通常、エンタープライズポートのみで必要になります。

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、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。これは通常、 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10 Gbps エンタープライズポート（enp94s0f0/enp69s0f0）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「必須の設定情報」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。

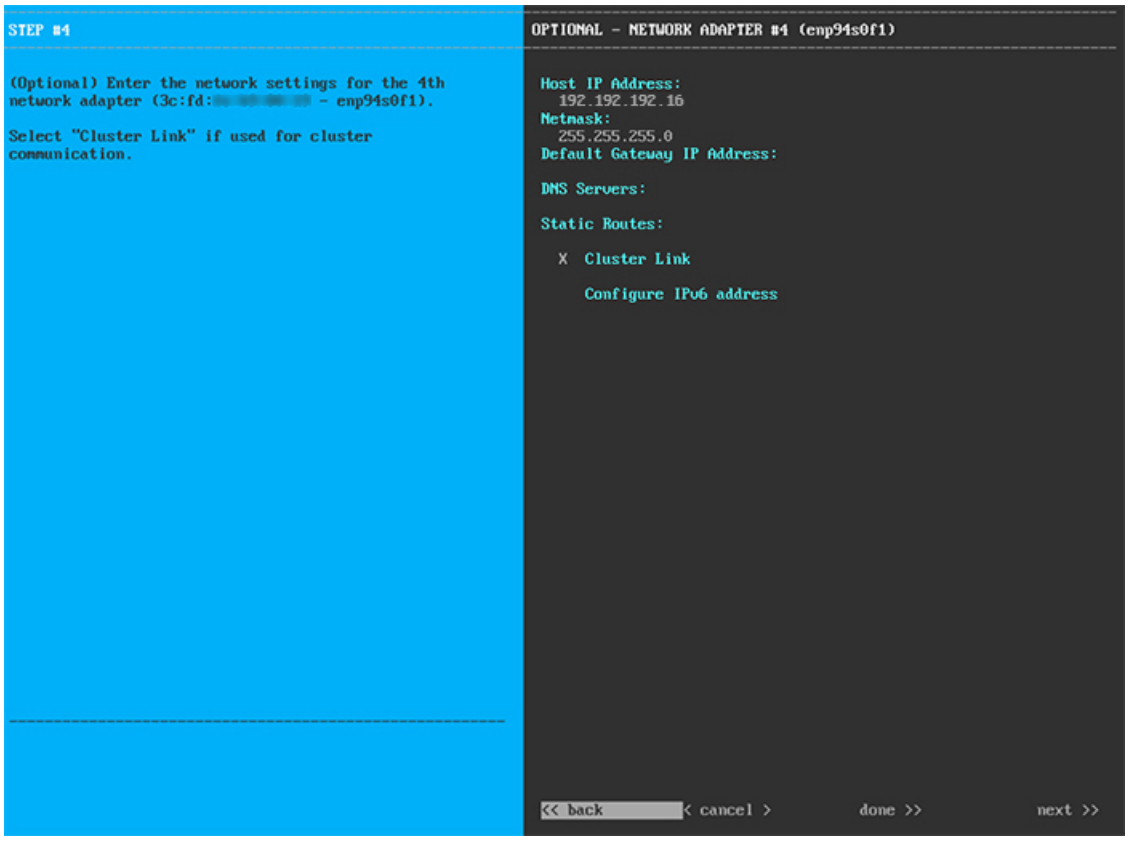
表 *30* : ネットワークアダプタ *#3* のアドオンノードエントリ：*10 Gbps* エンタープライズポート（*enp94s0f0/enp69s0f0*）

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。
[Netmask]	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、<ネットワーク>/<ネットマスク>/<ゲートウェイ> 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10 Gbps クラスタポート（enp94s0f1/enp69s0f1）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「必須の設定情報」を参照してください）。



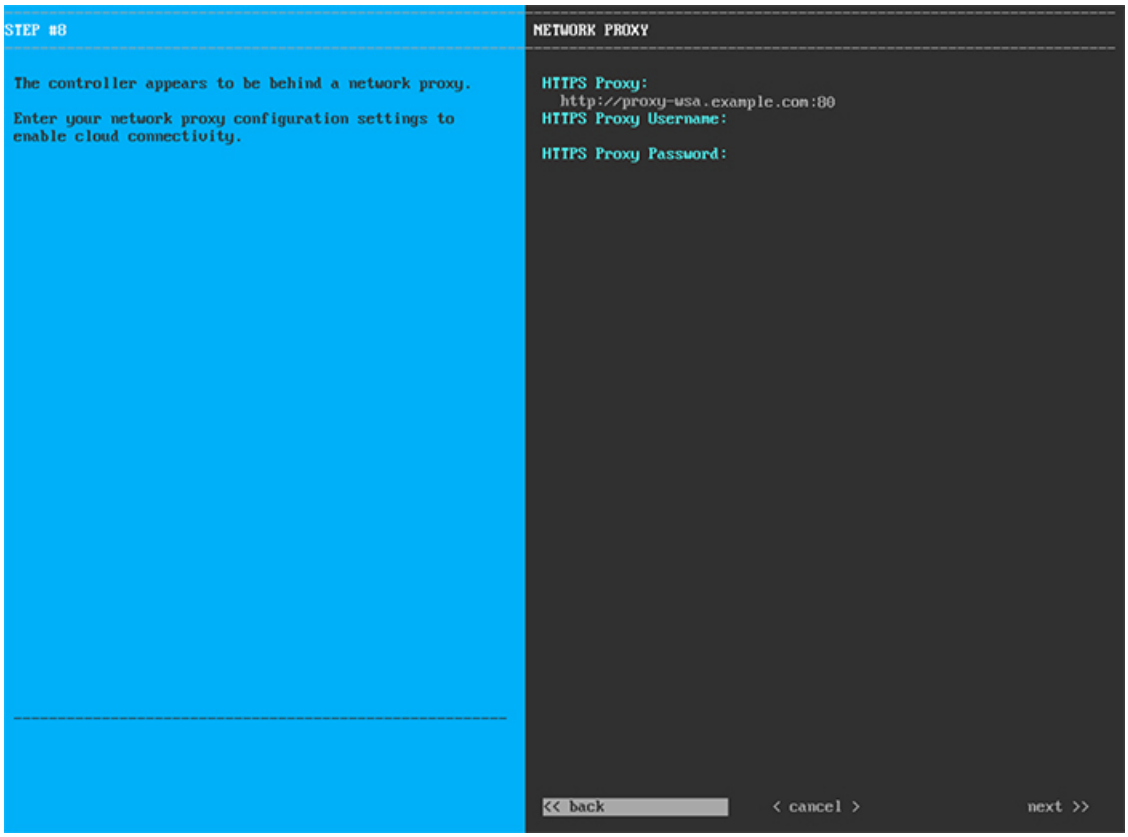
次の表に示すように、[ネットワークアダプタ#4（NETWORK ADAPTER #4）] の設定値を入力します。

表 *31* : ネットワークアダプタ *#4* のアドオンノードエントリ：*10 Gbps* クラスタポート（*enp94s0f1/enp69s0f1*）

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。
[Netmask]	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。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
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。



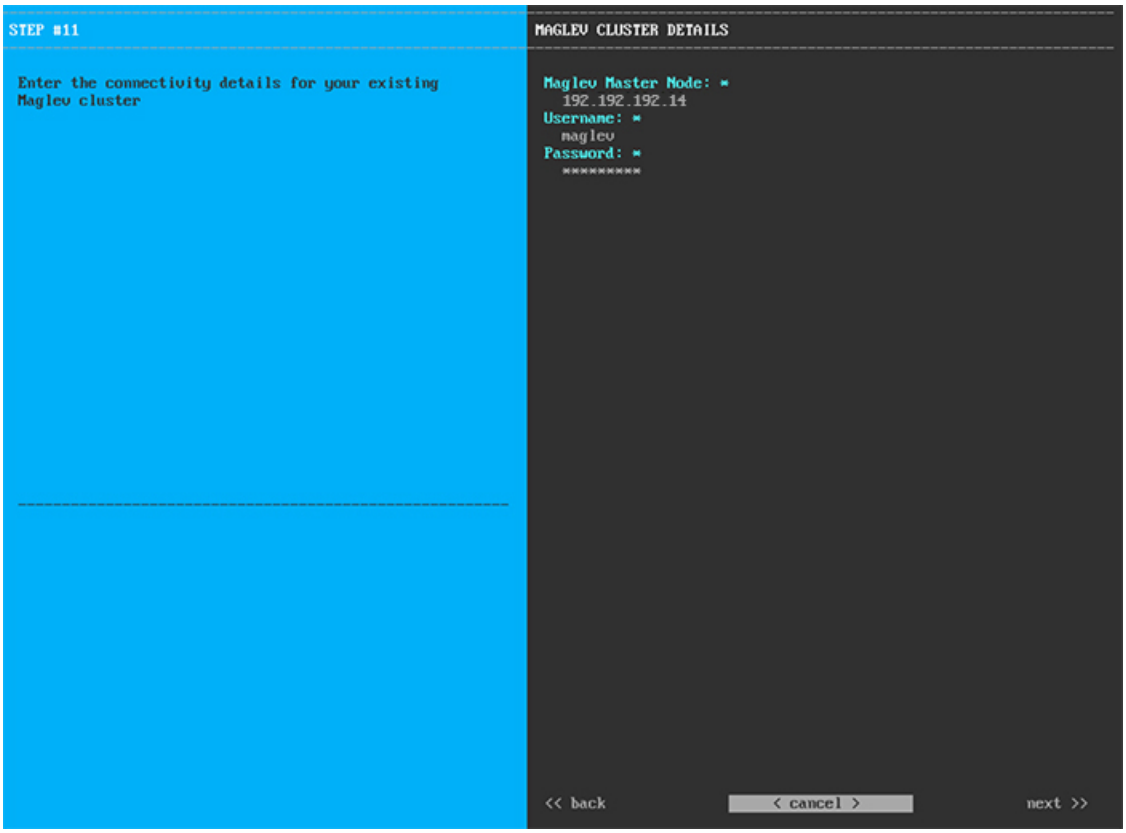
次の表に示すように、[ネットワークアダプタ（NETWORK ADAPTER）] の設定値を入力します。

表 *32* : 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、マスタノードのクラスタポートとマスタノードのログインの詳細を確認するプロンプトがウィザードに表示されます。



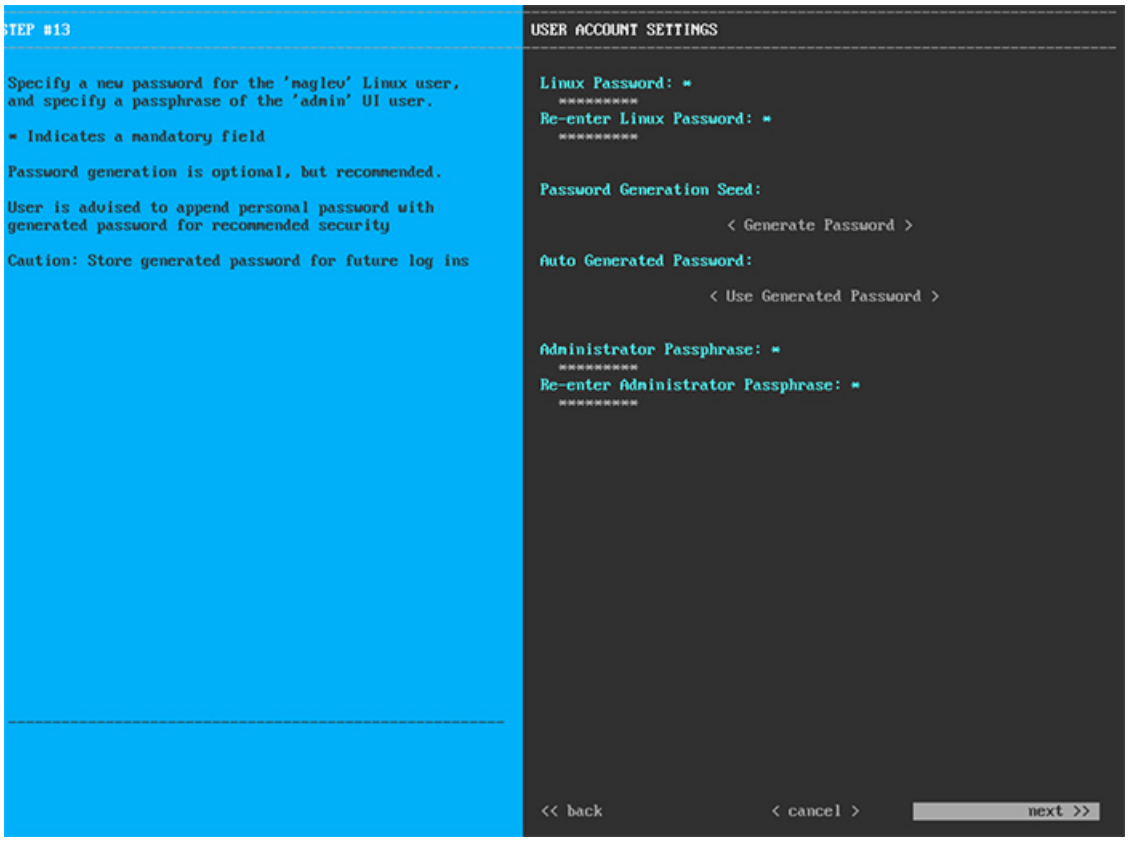
次の表の説明に従って、[MAGLEV クラスタの詳細（MAGLEV CLUSTER DETAILS）] に値を入力します。

表 *33 : Maglev* クラスタの詳細へのアドオンノードエントリ

Maglev マスタノード	クラスタ内のマスタノードでクラスタポートの 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、これはマスタノードの IP アドレス enp94s0f1、ネットワークアダプタ #4 です。
ユーザ名	**maglev** と入力します。
パスワード	マスタノードで設定した 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。

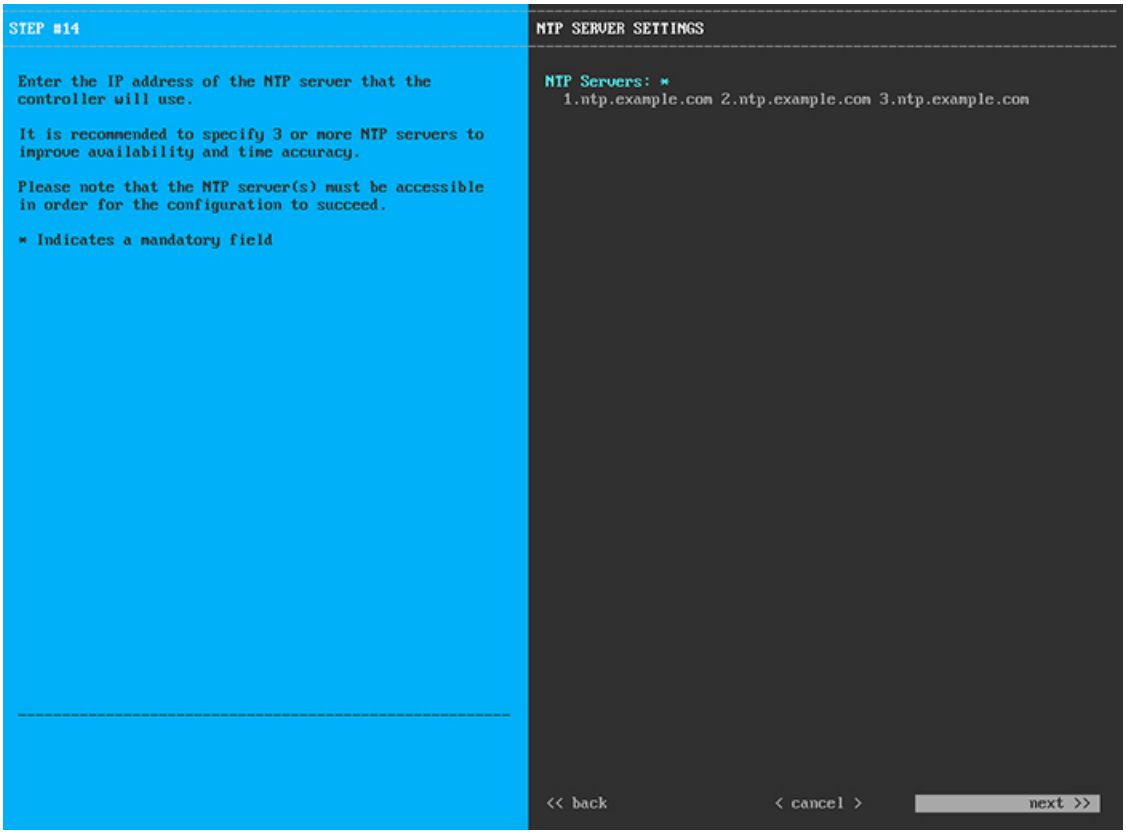
表 *34* : ユーザアカウント設定のアドオンノードエントリ

Linux パスワード	maglev ユーザに対して設定されている 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（Administrator Passphrase）	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。

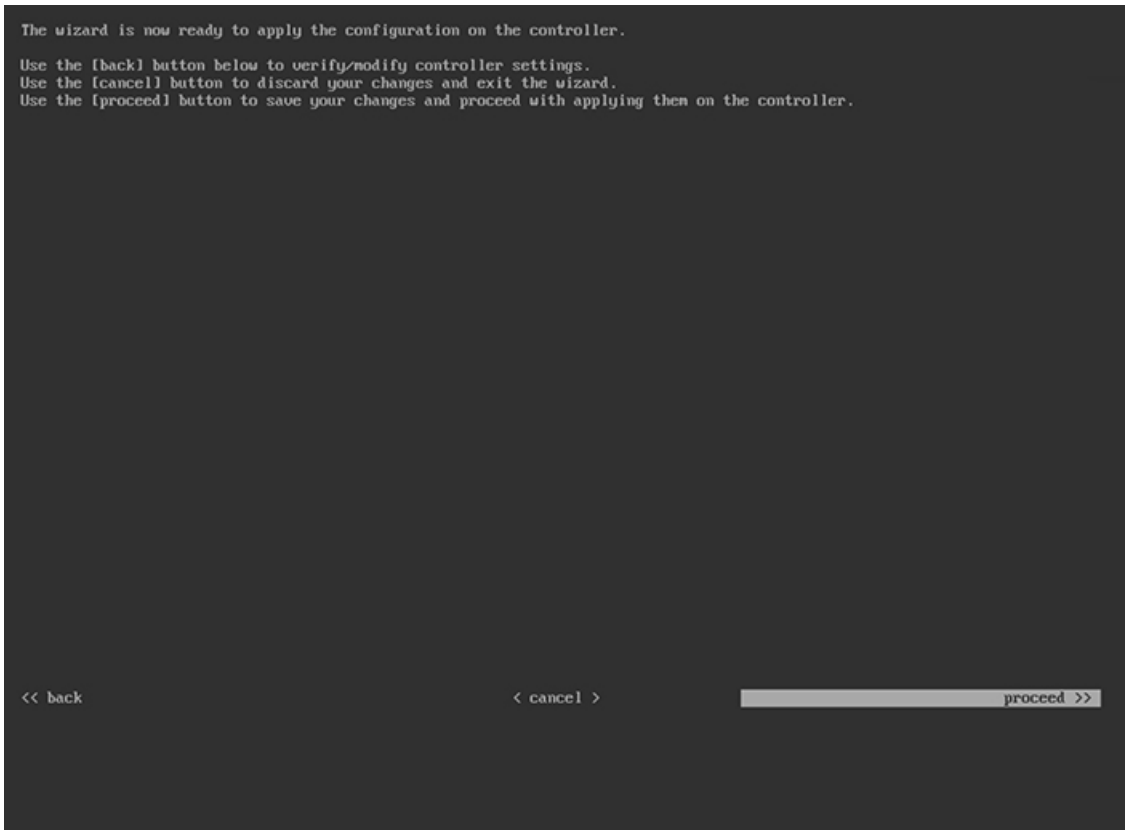
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように、[NTPサーバの設定（NTP SERVER SETTINGS）] の値を入力するようウィザードに求められます。



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。このサーバは、マスタノードに対して指定したものと同じ NTP サーバ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。

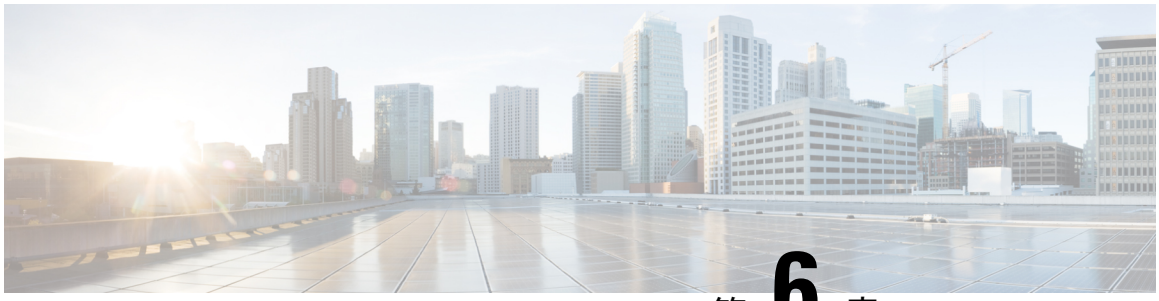
次のタスク

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。

最新の Cisco DNA Center 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。



第 6 章

初期設定の完了

初期設定ワークフロー

インストールしたすべての Cisco DNA Center アプライアンスの設定が完了したら、次のタスクを実行して、Cisco DNA Center を実稼働に使用する準備をします。

（注） この作業を完了するために必要なパラメータ情報については「必要な初期設定情報」を参照してください。

1. 互換性のあるブラウザを使用して、Cisco DNA Center にアクセスしていることを確認してください。

   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ドキュメントを参照してください。

2. 最初に管理者として Cisco DNA Center GUI にログインします。最初の管理ログイン中、次のプロンプトが表示されます。

   1. 管理スーパーユーザーの新規パスワードを提供します。
   2. ソフトウェアイメージをダウンロードし、シスコから電子メール通信を受信するために組織が使用する cisco.com ユーザ名とパスワードを入力します。
   3. 組織がスマート アカウント ライセンスを管理するために使用する cisco.com ユーザ名とパスワードを入力します。

4. Cisco DNA Center で使用する予定の IP アドレスマネージャ（IPAM）サーバを設定します。

これらのタスクの詳細については、「初回ログイン」を参照してください。

3. Cisco DNA Center を Cisco Identity Services Engine（ISE）と一緒に使用する予定の場合は、2 つが適切に統合されていることを確認してください：Cisco ISE との統合 Cisco DNA Center の統合
4. Cisco DNA Center にポリシーおよび AAA サーバ（ISE を含む）を接続します：認証サーバとポリシー サーバの設定
5. 基本的な SNMP の再試行およびポーリングパラメータを設定します：SNMP プロパティの設定
6. HA 動作を最適化するために、クラスタノード間でサービスを再配布します：サービスの再配布
7. 初回設定を完了したら：ログアウト

互換性のあるブラウザ

Cisco DNA Center の GUI は次の HTTPS 対応ブラウザと互換性があります。

- Google Chrome：バージョン 62.0 以降。
- Mozilla Firefox：バージョン 54.0 以降。

Cisco DNA Center へのログインに使用するクライアント システムは、64 ビット オペレーティング システムとブラウザを装備していることが推奨されます。

初回ログイン

Cisco DNA Center アプライアンスをインストールして設定した後、Web ベースの GUI にログインできます。Cisco DNA Center にアクセスする際には、互換性のある HTTPS 対応ブラウザを使用してください。

スーパーユーザ権限を持つ管理者（`admin` というユーザ名、スーパー管理者ロール（SUPER-ADMIN-ROLE）が割り当てられている）として初めてログインする場合、システムセキュリティを強化し、基本的なセットアップタスクを完了するのに役立つ、初回セットアップウィザードを完了するように求められます。ウィザードの各ステップを省略することは可能ですが、システムをできるだけ早く使用できるようにするため、指示どおりにすべてのステップを完了することをお勧めします。

また、新しいCisco DNA Centerユーザを作成する必要があります。毎日の操作で使用する追加のユーザアカウントを少なくとも 1 つ作成し、このユーザアカウントにネットワーク管理者ロール（NETWORK-ADMIN-ROLE）を割り当てることをお勧めします。

始める前に

Cisco DNA Center にログインして初回セットアップウィザードを完了するには、次の情報が必要です。

- Maglev ウィザードを使用したマスタノードの設定の手順に従って指定した「管理者」スーパーユーザのユーザ名とパスワード。
- 必要な初期設定情報 に記載されている必要な情報。

ステップ 1 Cisco DNA Center アプライアンスのリブートが完了したら、ブラウザを起動します。

ステップ 2 **HTTPS://** と設定プロセスの最後に表示された Cisco DNA Center GUI の IP アドレスを使用して、Cisco DNA Center GUI にアクセスするホスト IP アドレスを入力します。

IP アドレスを入力すると、次のいずれかのメッセージが表示されます（使用しているブラウザによって異なります）。

- Google Chrome：接続のプライバシーは保護されません
- Mozilla Firefox：警告：今後セキュリティリスクが見つかる潜在的可能性があります

ステップ 3 メッセージを無視して **[詳細設定（Advanced）]** をクリックします。

サイトのセキュリティ証明書が信頼されていないことを示すメッセージが表示されます。このメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Cisco DNA Center での証明書の使用方法については、『Cisco Digital Network Architecture Center 管理者ガイド』の「証明書と秘密キーのサポート」の項を参照してください。

ステップ 4 メッセージを無視して、ウィンドウの下部にあるリンクをクリックします。

[ログイン（Login）]Cisco DNA Center ウィンドウが表示されます。

ステップ 5 **[ログイン（Login）]** ウィンドウで Cisco DNA Center の設定時に設定した管理ユーザ名（admin）とパスワードを入力し、**[ログイン（Log In）]** をクリックします。

[ログインのリセット（Reset Login）] ウィンドウが表示されます。

ステップ 6 古いパスワードを入力してから、スーパーユーザ権限を持つ管理者の新しいパスワードを入力して確認し、**[保存（Save）]** をクリックします。

[Cisco.com IDの入力（Enter Cisco.com ID）] ウィンドウが表示されます。

ステップ 7 Cisco.com ユーザのユーザ名とパスワードを入力してから **[次へ（Next）]** をクリックします。

cisco.com ユーザログインが既知のどの Cisco Smart Account ユーザログインとも一致しない場合は、**[Smart Account]** ウィンドウが表示されます。

ステップ 8 **[スマートアカウント（Smart Account）]** ウィンドウが表示された場合には、組織のスマートアカウントのユーザ名とパスワードを入力するか、対応するリンクをクリックして新しいスマートアカウントを開きます。完了したら **[次へ（Next）]** をクリックします。

[IPアドレスマネージャ（IP Address Manager）] ウィンドウが表示されます。

ステップ 9 組織が外部 IP アドレスマネージャ（IPAM）を使用している場合には、次の手順を実行してから **[次へ（Next）]** をクリックします。

- IPAM サーバの名前と URL を入力します。
- サーバへのアクセスに必要なユーザ名とパスワードを入力します。
- 使用中の IPAM プロバイダー（Infoblox など）を選択します。
- Cisco DNA Center で使用する利用可能な IP アドレスの特定のビューを IPAM サーバデータベースで選択します。

[プロキシサーバの入力（Enter Proxy Server）] ウィンドウが表示されます。

ステップ 10 組織が使用するプロキシサーバ情報を入力し、**[次へ（Next）]**をクリックします。

- プロキシサーバに対するログインが必要な場合には、サーバのユーザ名とパスワードを含めます。
- 続行する前にこの情報を検証する（推奨）場合には、**[設定の検証（Validate Settings）]** チェックボックスがオンになっていることを確認します。

ソフトウェアの **[EULA]** ウィンドウが表示されます。

ステップ 11 **[次へ（Next）]** をクリックして、ソフトウェアのエンドユーザライセンス契約書に同意します。

[準備完了（Ready to go!）] ウィンドウが表示されます。

ステップ 12 このウィンドウでいずれかのリンクをクリックするか、[システム360に移動（Go To System 360）] をクリックして [システム360（System 360）] ダッシュボードを表示することにより、Cisco DNA Center の使用を開始できます。

シスコでは、[ユーザ管理（User Management）] リンクをクリックして、[ユーザ管理（User Management）] ウィンドウを表示することを推奨しています。**[追加（Add）]** をクリックして、新しい Cisco DNA Center ユーザの追加を開始します。新しいユーザの名前とパスワードを入力し、ユーザのロールを選択したら、**[保存（Save）]** をクリックして新しいユーザを作成します。初期展開の新しいユーザすべてが追加されるまで、必要に応じてこの手順を繰り返します。ネットワーク管理者ロール（NETWORK-ADMIN-ROLE）を持つユーザを少なくとも 1 人作成してください。

次のタスク

残りの管理設定タスクを任意の順序で実行します。

- Cisco ISE との統合 Cisco DNA Center
- 認証サーバとポリシー サーバの設定
- SNMP プロパティの設定

Cisco ISE との統合 Cisco DNA Center

このリリースの Cisco DNA Center は、Cisco ISE と信頼された通信リンクを作成するメカニズムを備えており、Cisco DNA Center は安全な方法で Cisco ISE とデータを共有できます。Cisco ISE が Cisco DNA Center に登録されると、Cisco DNA Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。ユーザは Cisco DNA Center を使用してデバイスを検出し、Cisco DNA Center と Cisco ISE の両方の機能を検出したデバイスに適用できます。この理由はこれらのデバイスが両方のアプリケーションに公開されるためです。 また Cisco DNA Center デバイスと Cisco ISE デバイスはすべてデバイス名で一意に識別されます。

Cisco DNA Center デバイスは Cisco DNA Center サイト階層内の特定のサイトにプロビジョニングされて所属すると、即座に Cisco ISE にプッシュされます。Cisco DNA Center デバイスのアップデート（IP アドレス、SNMP または CLI のクレデンシャル、Cisco ISE 共有秘密情報など）はすべて、自動的に ISE 上の対応するデバイスインスタンスに使用されます。Cisco DNA Center デバイスが削除されるときは、Cisco ISE からも削除されます。Cisco DNA Center デバイスが Cisco ISE にプッシュされるのは、Cisco ISE が AAA サーバとして設定されている特定のサイトにそれらのデバイスが関連付けられている場合に限ることに注意してください。

始める前に

Cisco ISE を Cisco DNA Center と統合する前に、次の前提条件を満たしていることを確認します。

- ネットワークに 1 つ以上の Cisco ISE バージョン 2.3（以降）のホストを展開済みであること。Cisco ISE のインストールについては、Cisco Identity Services Engine のインストールガイド、アップグレードガイド（バージョン 2.3 以降用）を参照してください。
- スタンドアロン ISE 導入環境がある場合は、Cisco ISE ノード上で pxGrid サービスおよび ERS と統合し、これらを有効化する必要があります。
- 分散型 Cisco ISE 展開がある場合：
  - Cisco DNA Center を Cisco ISE 管理ノード、プライマリポリシー管理ノード（PAN）と統合し、ERS を有効にする必要があります。

  （注） PAN を介した ERS 使用がベストプラクティスです。ただしバックアップの場合は、PSN で発信をイネーブルにします。

  - 単一ノードの導入環境と同様に、分散型の導入環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型の導入環境では、他の任意の Cisco ISE ノード上で pxGrid を有効化できます。

- ポート 22、443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信が有効になっています。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Cisco DNA Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できます。
- Cisco ISE ノードでは SSH が有効化されます。
- Cisco ISE 管理ノード証明書のサブジェクト名または SAN のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれます。
- Cisco DNA Center システム証明書の [サブジェクト代替名（SAN）（Subject Alternative Name（SAN））] フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

Cisco DNA Center に対応した Cisco ISE の設定の詳細については、『Cisco ISE Administrators Guide』の「*Integration with Cisco DNA Center*」を参照してください。

ステップ 1 次のように Cisco ISE の pxGrid サービスと ERS を有効化します。

a) Cisco ISE のプライマリ管理ノードにログインします。

b) **[管理（Administration）]** > **[システム（System）]** > **[展開（Deployment）]** を選択します。

[展開設定（Deployment Configuration）] ウィンドウが開きます。

c) pxGrid サービスを有効化する Cisco ISE ノードのホスト名をクリックします。

分散型展開の場合、これは展開環境内の任意の Cisco ISE ノードです。

[ノードの編集（Edit Node）] ウィンドウが開き、**[General Settings（一般設定）]** タブがデフォルトで選択されています。

d) **[PxGrid]** 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、**[保存（Save）]** をクリックします。

e) **[管理（Administration）]** > **[システム（System）]** > **[設定（Settings）]** の順に選択します。

f) 左側のナビゲーションウィンドウで **[設定（Settings）]** をクリックして、**[設定（Settings）]** ウィンドウを開きます。

g) **[読み取り/書き込み用にERSを有効化（Enable ERS for Read/Write）]** オプションボタンをクリックし、通知プロンプトで **[OK]** をクリックします。

h) **[保存（Save）]** をクリックします。

ステップ 2 次のように Cisco ISE ノードを AAA サーバとして Cisco DNA Center に追加します。

a) Cisco DNA Center GUI にログインします。

b) **メニュー**アイコン（☰）をクリックし、**[システム（System）]** > **[システム360（System 360）]** を選択します

c) [Identity Services Engine（ISE）] ペインで、**[設定（Configure）]** リンクをクリックします。

d) **[認証サーバとポリシーサーバ（Authentication And Policy Servers）]** ウィンドウで [] をクリックします。

e) **[AAA/ISEサーバの追加（Add AAA/ISE server）]** スライドインペインで、次のタスクを実行します。

- **[サーバIPアドレス（Server IP address）]** フィールドに、Cisco ISE 管理 IP アドレスを入力します。
- ネットワークデバイスと Cisco ISE の通信を保護するために使用する **[共有秘密（Shared Secret）]** を入力します。
- **[Cisco ISEサーバ（Cisco ISE Server）]** スライダをクリックして、すべての Cisco ISE 関連フィールドが表示されていることを確認します。
- 該当する Cisco ISE 管理者の CLI クレデンシャルを **[ユーザ名（Username）]** と **[パスワード（Password）]** フィールドに入力します。
- Cisco ISE ノードの **FQDN** を入力します。
- **[サブスクライバ名（Subscriber Name）]** を入力します（例：cdnacenter）。
- （任意）Cisco ISE への接続に使用する Group14-SHA1 **SSH キー**を入力します。
- （任意）**仮想 IP アドレス（Virtual IP Address）**：Cisco ISE ポリシーサービスノードが背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数のポリシーサービス ノード ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

f) [**保存（Save）**] をクリックし、サーバのステータスが **[アクティブ（Active）]** になるまで待ちます。

ステップ 3 次のように Cisco ISE が Cisco DNA Centerに接続され、接続にサブスクライバがあることを確認します。

a) Cisco DNA Center を統合した Cisco ISE ノードにログインします。

b) **[管理（Administration）]** > **[pxGrid サービス（pxGrid Services）]** を選択します。

現在のステータスが **[オフライン（Offline）]** のpxGrid サービスサブスクライバが、ユーザの入力した名前（cdnacenter など）で表示されます。デフォルトでは、サブスクライバのステータスは**オフライン**のままであることに注意してください。

ステップ 4 Cisco DNA Center が Cisco ISE に接続していること、Cisco ISE SGT グループとデバイスが Cisco DNA Center にプッシュされることを次の手順で確認します。

a) Cisco DNA Center GUI にログインします。

b) **メニュー**アイコン（☰）をクリックし、**[システム（System）]** > **[システム360（System 360）]** を選択します。

c) [Identity Services Engine（ISE）] ペインで、**[Update（更新）]** リンクをクリックします。

d) **[認証サーバとポリシーサーバ（Authentication And Policy Servers）]** ウィンドウで、 Cisco ISE AAA サーバのステータスがまだ **[アクティブ（Active）]** であることを確認します。

e) **メニュー**アイコン（☰）をクリックし、**[ポリシー（Policy）]** > **[グループベースアクセスコントロール（Group Based Access Control）]** を選択します。

ISE SGT グループは **[スケーラブルグループ]** 表に表示されます。

認証サーバとポリシー サーバの設定

Cisco DNA Center は AAA サーバをユーザ認証に使用し、Cisco ISE をユーザ認証とアクセス制御の両方に使用します。この手順を使って Cisco ISE を含む AAA サーバを設定します。

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Cisco DNA Center と Cisco ISE が「Cisco ISE との統合 Cisco DNA Centerの統合」の説明に従って統合されたことを確認します。
- 他の製品（Cisco ISE 以外）で AAA 機能を使用している場合、以下に注意してください。
  - AAA サーバで Cisco DNA Center を登録します。これには、AAA サーバと Cisco DNA Center の共有秘密を定義することが含まれます。
  - AAA サーバで Cisco DNA Center の属性名を定義します。
  - Cisco DNA Center マルチホストクラスタの設定の場合は、AAA サーバのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。

ステップ 1 Cisco DNA Center のホームページで、⚙ > **[System Settings]** > **[Settings]** > **[Authentication and Policy Servers]** の順に選択します。

ステップ 2 ⊕ Add をクリックします。

ステップ 3 次の情報を入力して、プライマリ AAA サーバを設定します。

- **サーバの IP アドレス（Server IP Address）**：AAA サーバの IP アドレス。
- **共有秘密（Shared Secret）**：デバイス認証キー。共有秘密情報の長さは、最大 128 文字です。

ステップ 4 AAA サーバ（Cisco ISE 以外）を設定するには、**[Cisco ISE サーバ（Cisco ISE Server）]** ボタンを **[オフ（Off）]** 位置のままにして、次の手順に進みます。

Cisco ISE サーバを設定するには、**[Cisco ISE サーバ（Cisco ISE server）]** ボタンをクリックして **[オン（On）]** の位置に合わせ、次のフィールドに情報を入力します。

- **ユーザ名（Username）**：Cisco ISE CLI へのログインに使用する名前です。

  （注） このユーザにはスーパーユーザの管理権限が必要です。

- **パスワード（Password）**：Cisco ISE CLI ユーザ名のパスワード。
- **FQDN** - Cisco ISE サーバの FQDN。

（注）
- Cisco ISE（**[管理（Administration）] > [展開（Deployment）] > [展開ノード（Deployment Nodes）] > [リスト（List）]**）で定義されている FQDN をコピーして、このフィールドに直接貼り付けすることをお勧めます。
- 入力した FQDN は、Cisco ISE証明書で定義されている FQDN、共通名（CN）または Subject Alternative Name（SAN）と一致する必要があります。

FQDN は次の形式で、ホスト名とドメイン名の 2 つのパートで構成されています。

hostname.domainname.com。

たとえば Cisco ISE サーバの FQDN は、ise.cisco.com である可能性があります。

- **サブスクライバ名（Subscriber Name）**：Cisco ISE pxGrid サービスに登録するとき pxGrid クライアントを識別する一意のテキスト文字列（acme など）。サブスクライバ名は Cisco DNA Center を Cisco ISE に統合するとき使用されます。
- （任意）**SSH キー**：Cisco ISE への接続に使用される Diffie-Hellman-Group14-SHA1 SSH キー。
- （任意）**仮想IPアドレス**：Cisco ISE ポリシーサービスノードが背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数のポリシー サービス ノード ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

（注） 設定された ISE サーバのステータスがパスワードの変更により [失敗（FAILED）] になっている場合は、**[再試行（Retry）]** をクリックし、パスワードを更新して ISE 接続を再同期します。

ステップ 5 [詳細設定の表示（View Advanced Settings）] をクリックして、設定を構成します。

（注） 必要な設定は、サーバのプロトコル設定によって異なります。

- **プロトコル（Protocol）**：**[RADIUS]** はデフォルトで設定されていますが、代わりに **[TACACS]** を選択するか、両方のプロトコルを選択することもできます。

  注目 Cisco ISE サーバに **[TACAS]** を選択しない場合、Cisco ISE ノードの設定には使用できません。

- **認証ポート（Authentication Port）**：**RADIUS** が AAA サーバに認証メッセージを中継するために使用されるポート。デフォルト値は UDP ポート 1812 です。
- **アカウンティングポート（Accounting Port）**：**RADIUS** が AAA サーバに重要なイベントを中継するために使用するポート。これらのイベントの情報は、セキュリティおよび請求目的で使用されます。デフォルトの UDP ポートは 1813 です。
- **ポート（Port）**：**TACACS** が AAA サーバとの通信に使用するポート。デフォルト ポートは 49 です。
- **再試行（Retries）**：接続の試行が中止される前に、Cisco DNA Centerが AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- **タイムアウト（Timeout）**：接続の試行が中止される前に、デバイスが AAA サーバの応答を待機する時間。デフォルトのタイムアウトは 4 秒です。

ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 セカンダリサーバを追加するには、ステップ 2 ～ 6 を繰り返します。

SNMP プロパティの設定

SNMP の再試行とタイムアウトの値を設定できます。

始める前に

SUPER-ADMIN-ROLE 権限を持つユーザのみがこの手順を実行することができます。詳細については、*Cisco Digital Network Architecture Center* 管理者ガイドを参照してください。

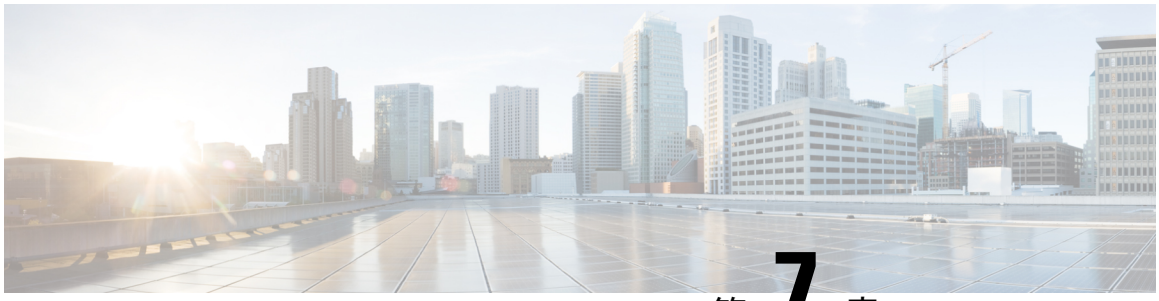
ステップ 1 Cisco DNA Center のホームページで、歯車のアイコン（⚙）をクリックし、[システムの設定（System Settings）] > [設定（Settings）] > [SNMP プロパティ（SNMP Properties）] の順に選択します。

ステップ 2 次のフィールドを設定します。

- **再試行回数（Retries）**：許容されるデバイス接続の最大試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
- **タイムアウト（秒数）（Timeout（in Seconds））**：タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は 5 秒間隔で 1 ～ 300 秒の範囲内です。デフォルトは 5 秒です。

ステップ 3 [適用（Apply）] をクリックします。

（注） デフォルト設定に戻すには、**[デフォルトに戻す（Revert to Defaults）]** をクリックします。



第 7 章

展開のトラブルシューティング

トラブルシューティング タスク

アプライアンスの設定に関する問題をトラブルシューティングする場合は、通常、次のタスクを実行します。

1. 現在、Cisco DNA Center GUI を使用している場合は、ログアウト。
2. アプライアンスのハードウェアを再設定するには、「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」のステップ 12 および 13 の説明に従って、CIMC GUI にログインして使用します。
3. アプライアンスの設定を変更する必要がある場合は、「設定ウィザードを使用したアプライアンスの再設定」の説明に従って、Maglev 設定ウィザードを起動して使用します。
4. アプライアンスの電源を再投入して、変更がアクティブになるようにします：アプライアンスの電源の入れ直し。

アプライアンスのネットワークアダプタの詳細については、『*Cisco UCS C シリーズ サーバ Integrated Management Controller GUI リリース 3.1 コンフィギュレーションガイド*』の「アダプタの管理」の項を参照してください。別の場所に記載されているように、Linux CLI を使用してアプライアンスハードウェアを管理することは避けてください。アプライアンスの設定を変更するには、CIMC GUI または Maglev 設定ウィザードのみを使用します。

ログアウト

次の手順を実行し、Cisco DNA Center GUI からログアウトします。

セキュリティ上の理由から、作業セッションが完了したらログアウトすることをお勧めします。ユーザーがログアウトしない場合、非アクティブ状態になってから 30 分後に自動的にログアウトされます。

ステップ 1 ⚙ をクリックします。

ステップ 2 [Sign out] をクリックします。

これにより、セッションが終了してログアウトされます。

設定ウィザードを使用したアプライアンスの再設定

アプライアンスを再設定する場合は、設定ウィザードを使用してアプライアンス設定を更新する必要があります。Linux CLI では実行できません。標準的な Linux サーバーの設定を更新するために使用する通常の Linux 管理手順は動作しないため、試行しないでください。

アプライアンスが設定されたら、設定ウィザードを使用してすべてのアプライアンス設定を変更できません。変更は次の設定のみに制限されます。

- アプライアンスのホスト IP アドレス
- DNS サーバの IP アドレス
- デフォルトゲートウェイ IP アドレス
- NTP サーバの IP アドレス
- クラスタ仮想 IP アドレス（Cluster Virtual IP address）
- スタティック ルート
- プロキシサーバの IP アドレス
- Maglev ユーザのパスワード
- 管理ユーザのパスワード。

始める前に

次のものが必要です。

- Secure Shell (SSH) クライアント ソフトウェア。
- 再設定が必要なアプライアンス上のエンタープライズポートに設定された IP アドレス。このポートを特定するには、「前面パネルと背面パネル」で背面パネルの図を参照してください。ポート 2222 でこのアドレスのアプライアンスにログインします。
- 現在ターゲットアプライアンスに設定されている Linux ユーザ名（*maglev*）とパスワード。

ステップ 1 セキュアシェル（SSH）クライアントを使用して、ポート 2222 上で再設定する必要のあるアプライアンスのエンタープライズポートの IP アドレスにログインします。

ssh maglev@*Enterprise-port's-IP-address* **-p 2222**

ステップ 2 プロンプトが表示されたら、Linux パスワードを入力します。

ステップ 3 次のコマンドを入力して設定ウィザードにアクセスします。

sudo maglev-config update

Linux パスワードを入力するようプロンプトが表示されたら、再度入力します。

ステップ 4 設定ウィザードには、「Maglev ウィザードを使用したアドオンノードの設定」の場合に表示される画面と同じ一連の画面の短縮バージョンが表示されます。表示された設定を適宜変更します。各画面で変更を終えたら、**[次へ（Next）]** を選択して設定ウィザードを続行します。

ステップ 5 設定プロセスの最後に、設定ウィザードが変更の適用を実行できる状態になったことを示すメッセージが表示されます。次のオプションを使用できます。

- **[戻る（back）]**：変更を確認して検証します。
- **[キャンセル（cancel）]**：変更を破棄して設定ウィザードを終了します。
- **[続行（proceed）]**：変更を保存して、それらの適用を開始します。

[続行（proceed>>）] を選択してインストールを完了します。設定ウィザードで変更が適用されます。

設定プロセスの最後に、「CONFIGURATION SUCCEEDED」というメッセージが表示されます。

次のタスク

アプライアンスの電源を切ってから再度電源を入れて、変更が適用され、アクティブになっていることを確認します。「アプライアンスの電源の入れ直し」を参照してください。

（注） DNS サーバー IP アドレスを更新した場合、アプライアンスの電源を切ってから再度電源を入れて、冷却ブートを実行することを推奨します。これで DNS の変更が確実に反映されます。

アプライアンスの電源の入れ直し

Cisco DNA Center アプライアンスで次の手順を実行して、アプライアンスを停止するか、ウォームリスタートを実行します。ハードウェアを修復する前にアプライアンスを停止することも、ソフトウェアの問題を修正した後にウォームリスタートを開始することもできます。Cisco IMC を使用して行ったハードウェアの変更は、アプライアンスのリブート後に適用されます。

CICM GUI と、CIMC GUI からアクセス可能な KVM コンソールを使用して、アプライアンスの電源を再投入することも可能であることに注意してください。詳細については、「Maglev ウィザードを使用したマスタノードの設定」または「Maglev ウィザードを使用したアドオンノードの設定」の手順 1 ～ 3 を参照してください。

⚠

注意 Cisco IMC GUI からアプライアンスの電源を再投入すると、データの破損または喪失が発生する可能性があります。アプライアンスが SSH、Cisco IMC コンソール、または物理コンソールに完全に応答しない場合にのみ実行してください。

始める前に

次のものが必要です。

- Secure Shell (SSH) クライアント ソフトウェア。
- 再設定が必要なアプライアンス上の 10Gbps エンタープライズポートに設定された IP アドレス。このポートを特定するには、「前面パネルと背面パネル」で背面パネルの図を参照してください。ポート 2222 でこのアドレスのアプライアンスにログインします。
- 現在ターゲットアプライアンスに設定されている Linux ユーザ名（*maglev*）およびパスワード。

ステップ 1 セキュアシェル（SSH）クライアントを使用して、ポート 2222 上で再設定する必要のあるアプライアンスのエンタープライズポートの IP アドレスにログインします。

ssh maglev@*Enterprise-port's-IP-address* **-p 2222**

ステップ 2 プロンプトが表示されたら、Linux パスワードを入力します。

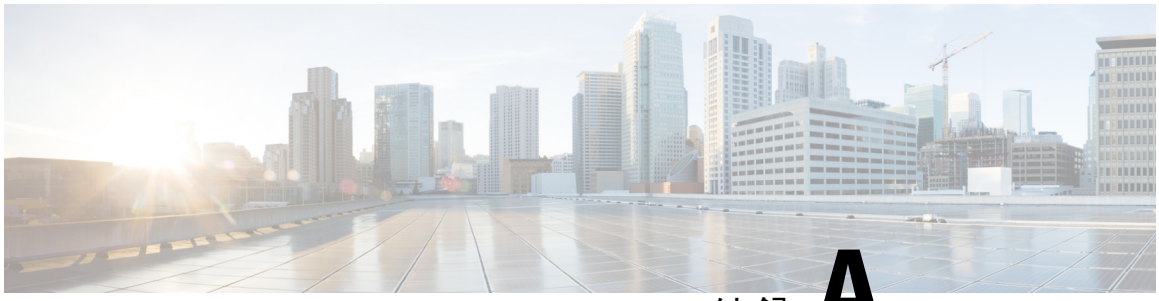
ステップ 3 実行するタスクに適したコマンドを入力します。

- アプライアンスを停止するには、次のように入力します。 **sudo shutdown -h now**
- ウォームリスタートを開始するには、次のように入力します。 **sudo shutdown -r now**

  Linux パスワードを入力するようプロンプトが表示されたら、再度入力します。

ステップ 4 ホストがシャットダウンされたときに表示されるコマンド出力を確認します。

ステップ 5 アプライアンスを停止した場合には、前面パネルの電源ボタンを使用して、アプライアンスを再びオンにすることにより、Maglev ルートプロセスの電源を入れます。



付録 A

ハイ アベイラビリティ クラスタの展開シナリオの確認

Cisco DNA Center のハイアベイラビリティ（HA）の実装については『*Cisco Digital Network Architecture Center* 管理者ガイド』を参照してください。最初にこの情報を確認してから、実稼働環境に HA を展開するかどうかを決定するようお勧めします。これを選択する場合は、次のタスクを実行します。

1. ネットワークに適した導入手順を実行します。
   - 新しい HA の展開
   - 標準インターフェイス設定を使用したマスタノードの既存 HA の展開
   - 非標準インターフェイス設定を使用したマスタノードの既存 HA の展開
2. クラスタノード間でサービスを再サービスの再配布します。
3. HA の展開に関する追加の考慮事項を参照し、必要な追加の設定を行います。

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 次のとおり、最初にインストールされたアプライアンスをマスタノードとして設定します。

「Maglev ウィザードを使用したマスタノードの設定」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。

「Maglev ウィザードを使用した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マスタノードの既存 HA の展開

マスタ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 マスタノードを Cisco DNA Center 1.3 にアップグレードします。

Cisco DNA Center の現在のリリースへの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。

ステップ 2 マスタ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（仮想 IP アドレス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。

「Maglev ウィザードを使用した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マスタノードの既存 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マスタノードの既存 HA の展開

マスタ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 マスタノードを Cisco DNA Center 1.3 にアップグレードします。

Cisco DNA Center の現在のリリースへの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。

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 Digital Network Architecture Center 管理者ガイド』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、マスタ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 がマスタ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 マスタノードで、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使用して、リモートリポジトリのデータを復元します。

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。

「Maglev ウィザードを使用したアドオンノードの設定」を参照してください。

サービスの再配布

Cisco DNA Center の HA の実装については『*Cisco Digital Network Architecture Center* 管理者ガイド』を参照してください。最初にこの情報を確認してから、実稼働環境に HA を展開するかどうかを決定するようお勧めします。展開を選択する場合は、次のとおりクラスタノード間でサービスを再配布することによって HA の動作を最適化します。

1. ⚙ をクリックして、[システム設定（System Settings）] を選択します。

   [システム360（System 360）] タブは、デフォルトで表示されます。

2. [ホスト（Hosts）] 領域で、[サービス配布の有効化（Enable Service Distribution）] をクリックします。

[サービス配布の有効化（Enable Service Distribution）]をクリックすると、Cisco DNA Center がメンテナンスモードになります。このモードではサービスの再配布が完了するまで Cisco DNA Center を使用できません。HA 展開のスケジュールを設定する場合は、このことを考慮する必要があります。

（注） Cisco DNA Center は、データベースの復元、システムアップグレード（パッケージアップグレードではない）の実行、HA のサービス再配布の有効化を実行するたび、（前述のとおり）メンテナンスモードになります。

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 **[ネットワークテレメトリ（Netwotk 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. [サイトの表示（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 以前デバイスに関連付けたプロファイルを使用して、テレメトリをもう一度有効にします。

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。