Cisco DNA Center リリース 1.2.10 第 2 世代アプライアンス設置ガイド

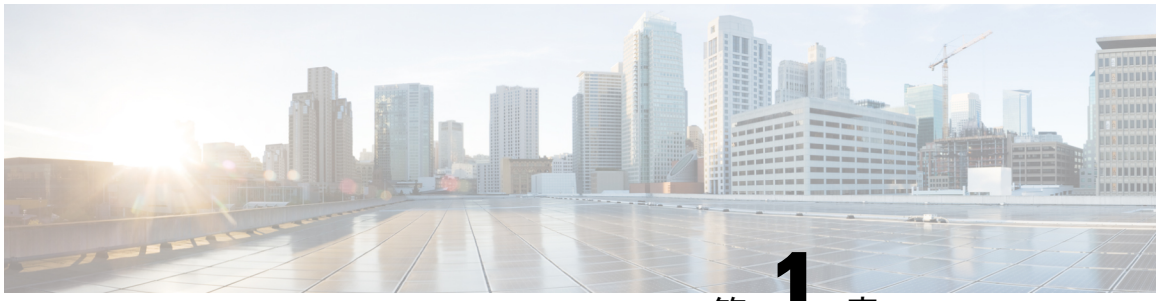
初版：2019 年 2 月 20 日

最終更新：2020 年 2 月 5 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次



第 1 章

アプライアンス機能の確認

機能概要

シスコは、Cisco DNA Center をラックマウント可能なアプライアンスの形式で提供しています。第 2 世代のアプライアンスは、Cisco UCS C220 M5 小型フォームファクタ（SFF）シャーシで構成され、Intel X710-DA2 ネットワーク インターフェイス カード（NIC）が PCIe スロット 1 に追加されています。次に示す第 2 世代アプライアンスの 3 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

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

機能	説明
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。
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

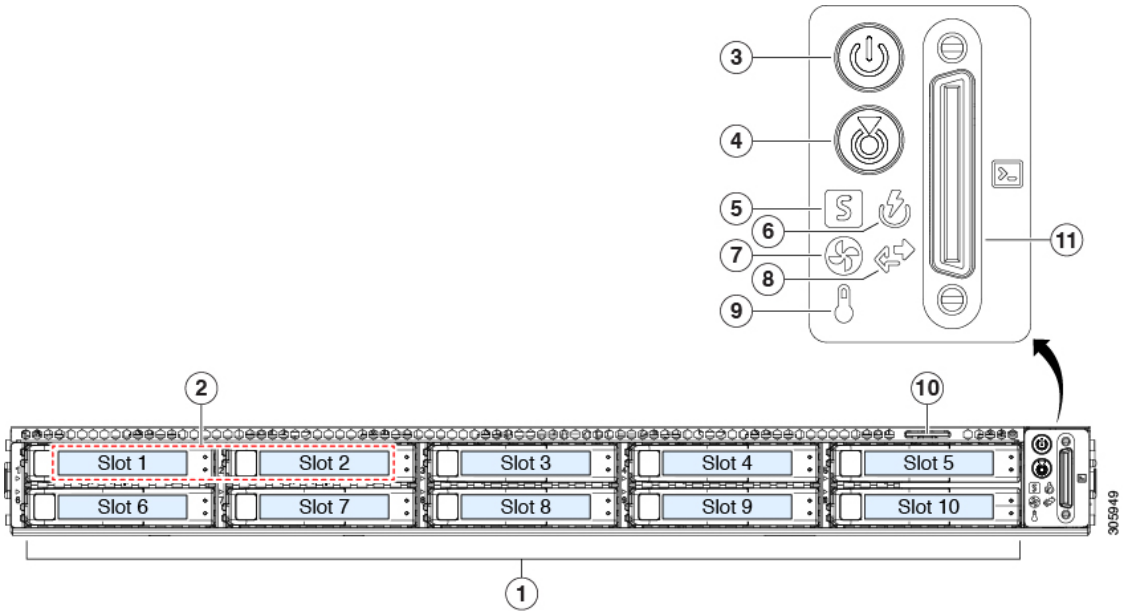
機能	説明
シャーシ	1 ラックユニット（1RU）シャーシ。
プロセッサ	28 コア Intel Xeon Platinum 8180 2.5 GHz プロセッサ X 2
メモリ	32 GB DDR4 2666 MHz RDIMM X 12
ストレージ	• RAID 1 で 480 GB X 2 • RAID 1 で 1.9 TB X 2 • RAID 10 で 1.9 TB X 6
ディスク管理（RAID）	• スロット 1 ～ 4 の RAID 1 • スロット 5 ～ 10 の RAID 10
ネットワークおよび管理 I/O	サポートされるコネクタ： • Intel X710-DA2 NIC 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。
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）。

前面パネルと背面パネル

次の図と表では第 2 世代 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:* アプライアンスの前面パネル

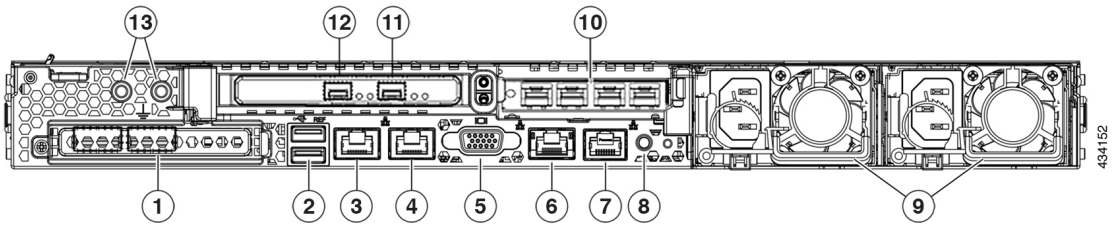


コンポーネント	説明
1	10 台の 2.5 インチ SAS/SATA ハードドライブおよびソリッドステートドライブ（SSD）。取り付けられたドライブにはそれぞれ、障害 LED とアクティビティ LED が付いています。 ドライブ障害 LED の状態とその説明： • 消灯：ドライブは正常に動作中です。 • オレンジ：ドライブに障害が発生しています。 • オレンジの点滅：ドライブの再構成中です。 ドライブアクティビティ LED の状態とその説明： • 消灯：スレッドにドライブが存在しません（アクセスなし、障害なし）。 • 緑：ドライブの準備が完了しています。 • 緑の点滅：ドライブはデータの読み取り中または書き込み中です。
2	ドライブベイ 1 および 2 で SAS/SATA および NVMe PCIe SSD をサポート。これらのドライブでは、障害 LED とアクティビティ LED およびその状態は、取り付けられた 2.5 インチ SAS/SATA ドライブの場合と同様です。
3	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。
4	ユニット識別ボタンと LED。LED の状態とその説明： • 青：ユニット識別機能はアクティブです。 • 消灯：ユニット識別機能は非アクティブです。

コンポーネント	説明
5	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動作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 個の CPU に障害が発生している。 • 少なくとも 1 個の 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。
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	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。

コンポーネント	説明
8	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： • 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。 • 消灯：イーサネットリンクがアイドル状態です。
9	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ー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ーが重大しきい値を超過しています。
10	引き抜きアセットタグ。
11	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:* アプライアンスの背面パネル



コンポーネント	説明
1	モジュール型 LAN on Motherboard（mLOM）カードベイ（x16）
2	USB 3.0 ポート（2 個）

コンポーネント	説明
3	**1Gbps/10Gbps 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。エンタープライズ管理ネットワークへのアクセスを提供す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： • 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。 • 消灯：リンクが確立されていません。 速度 LED の状態とその説明： • 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。 • 消灯：リンク速度は 10 Mbps 以下です。
4	**1Gbps/10Gbps 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、10Gbps 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： • 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。 • 消灯：リンクが確立されていません。 速度 LED の状態とその説明： • 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。 • 消灯：リンク速度は 10 Mbps 以下です。

コンポーネント	説明
5	VGA ビデオポート（DB-15）。
6	**1Gbps 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（「CIMC への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。エンタープライズ管理ネットワークへのアクセスを提供す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： • 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。 • 消灯：リンクが確立されていません。 速度 LED の状態とその説明： • 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。 • 消灯：リンク速度は 10 Mbps 以下です。
7	シリアル ポート（RJ-45 コネクタ）
8	背面ユニット識別ボタン/LED

コンポーネント	説明
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（たとえば、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： • 緑の点灯：AC 電力供給も、DC 出力も OK。 • 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。 • 消灯：電源装置に AC 電力が供給されていません。 詳細については「電力仕様」を参照してください。
10	アプライアンスの PCIe ライザ 2/スロット 2 にある 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（enp216s0f3、enp216s0f2、enp216s0f1、enp216s0f0）が含まれているため、設定に悪影響を及ぼす可能性があります。カードを無効にするには「ネットワーク インターフェイス カードの無効化 （60 ページ）」を参照してください。

コンポーネント	説明
11	**10Gbps 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 10Gbps 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： • 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。 • 消灯：リンクが確立されていません。 リンク速度 LED の状態とその説明： • 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。 • 消灯：リンク速度は 100 Mbps 以下です。 （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 10Gbps 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	**10Gbps 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 10Gbps 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： • 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。 • 消灯：リンクが確立されていません。 速度 LED の状態とその説明： • 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。 • 消灯：リンク速度は 100 Mbps 以下です。 （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 10Gbps 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。

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。

表 *3：*物理仕様

説明	仕様
高さ	4.32 cm（1.7 インチ）
幅	43.0 cm（16.89 インチ） ハンドルを含めた場合： 48.2 cm（18.98 インチ）

説明	仕様
奥行（長さ）	75.6 cm（29.8 インチ） ハンドルを含めた場合： 78.7 cm（30.98 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）	17.0 kg（37.5 ポンド）

環境仕様

次の表に、アプライアンスの環境仕様を示します。

表 *4 :* 環境仕様

説明	仕様
動作時温度	5 ～ 35 °C（41 ～ 95 °F） 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 ～ 65 °C（–40 ～ 149 °F）
湿度（RH）（動作時）	10 ～ 90%（28 °C（82 °F）時、結露なし）
非動作時湿度	5 ～ 93%（28 °C（82 °F）時）
動作時高度	0 ～ 10,000 フィート（0 ～ 3,000 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	5.5
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	40

電力仕様

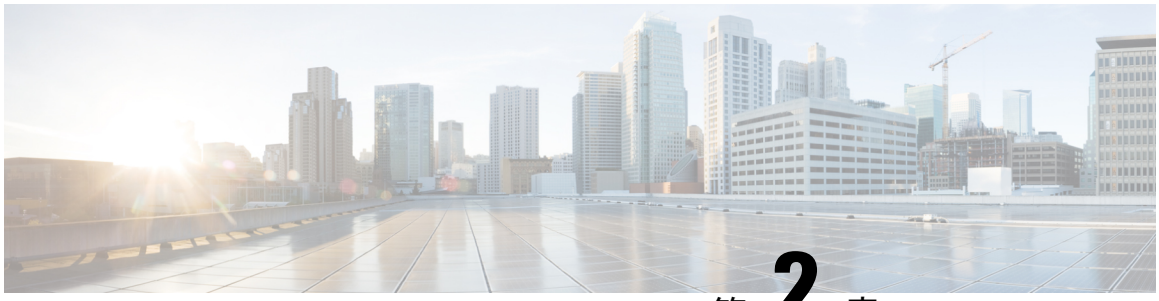
アプライアンスに同梱されているデュアル770 W AC電源（Cisco部品番号UCSC-PSU1-770W）は、下の表に一覧になっています。

注意 アプライアンス内で異なるタイプの電源装置を組み合わせて使用しないでください。両方の電源装置が同じである必要があります。

表 *5 : AC* 電源の仕様

説明	仕様
AC 入力電圧	公称範囲：100 ～ 120 VAC、200 ～ 240 VAC （範囲：90 ～ 132 VAC、180 ～ 264 VAC）
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	100 VAC で 9.5 A 208 VAC で 4.5 A
最大入力電圧	950 VA @ 100 VAC
PSU あたりの最大出力電力	770 W
最大突入電流	15 A（サブサイクル期間）
最大保留時間	12 ms @ 770 W
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（80Plus Platinum 認証済み）
フォームファクタ	RSP2
入力コネクタ	IEC320 C14

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

次の表に、アプライアンスの設置、設定、およびセットアップを試みる前に実行する必要がある計画および情報収集タスクの詳細を示します。この表のタスクが完了したら、データセンターにアプライアンスを物理的に設置することで続行できます。

詳細については「Cisco DNA CenterおよびCisco Software-Defined Access」を参照してください。

表 *6 :* 計画作業

ステップ	説明
1	スタンドアロン設置および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：インターフェイスケーブル接続。
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、およびその他の IP トラフィック情報を収集します：必要な IP アドレスおよびサブネット。
3	Web ベースのリソースへのアクセスに必要なソリューションを準備します：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。

ステップ	説明
4	Cisco DNA Center トラフィックのファイアウォールおよびセキュリティポリシーを再設定します：必要なネットワークポート。Cisco DNA Center を使用して SDA ネットワークを管理している場合は、「必要な SD アクセス ポートおよびプロトコル」も参照してください。
5	アプライアンスの設定時および初回のセットアップ時に使用される追加情報を収集します：必須の設定情報と必要な初期設定情報。

Cisco DNA CenterおよびCisco Software-Defined 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。

- 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、『ソフトウェア定義型アクセス：インテントベースのネットワーキングの実現』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、『SD-Accessアクセスセグメンテーション設計ガイド』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、『ソフトウェア定義型アクセス導入ガイド』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。

インターフェイスケーブル接続

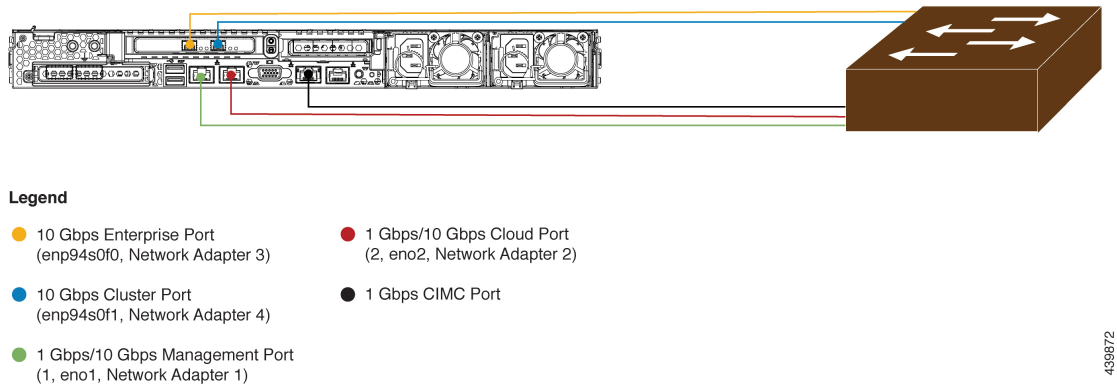
次のタイプのネットワークアクセスを提供するスイッチに、アプライアンスのポートを接続します。Cisco DNA Center の機能に必要なため、最低でも企業およびクラスタのポートインターフェイスを設定する必要があります。

- **（オプション）1Gbps または 10Gbps の管理ポート（1、eno1、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）を使用して Cisco DNA Center のグラフィック ユーザ インターフェイスにアクセスできます。その目的は、ユーザがアプライアンスでソフトウェアを使用できるようにすることです。このポートを、企業管理ネットワークに接続してスイッチにケーブル接続し、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）1Gbps または 10Gbps のクラウドポート（2、eno2、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。10Gbps のエンタープライズポート（enp94s0f0、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ケーブル接続し、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）10Gbps 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 の左側にあるポートです。その目的は、Cisco DNA Center のネットワークとの通信および管理を有効にすることです。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ケーブル接続し、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）10Gbps 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 の右側にあるポートです。その目的は、クラスタ内のプライマリ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ケーブル接続し、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。

  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 をクラスタリンクとして指定することを推奨します。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、再インストールが必要になります。将来的に 3 ノードクラスタへの拡張を可能にするために、IP アドレスを使用してクラスタポートを設定することを推奨します。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いて、稼働状態になっていることを確認します。
- **（オプション、ただし強く推奨）1Gbps CIMC ポート**：このポートは、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グラフィック ユーザ インターフェイスへのブラウザアクセスを提供します。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。このポートを、企業管理ネットワークに接続してスイッチにケーブル接続し、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。

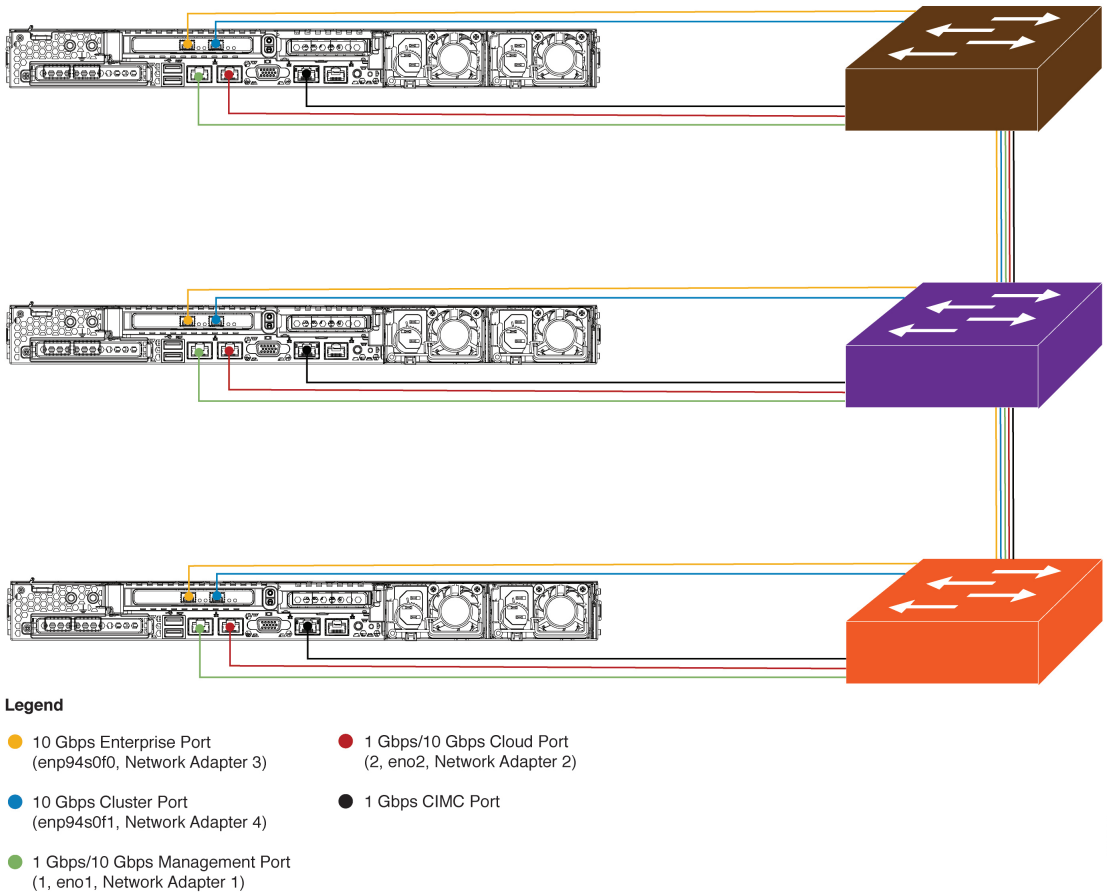
次の図は、単一ノード Cisco DNA Center クラスタの推奨される接続を示しています。

図 *3:* 単一ノードクラスタの推奨される配線



次の図は、3 ノード Cisco DNA Center クラスタの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、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 *4:3* ノードクラスタの推奨される配線



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アプライアンス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。

10Gbps 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-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-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。アプライアンスを単一ノードクラスタとして設置するか、3 ノードクラスタのプライマリまたはアドオンノードとして設置するかによって、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有効な 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。

1. **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、仮想 IP 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仮想 IP 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仮想 IP アドレスもダウンします。このような状況が発生すると、Cisco DNA Center はクラスタ内リンクが復元されるまで使用できなくなります（SWIM と ISE の統合は動作しなくなり、NDP コレクタから情報を収集できないため、アシュアランスデータは表示されません）。

2. **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 DNA Center Security Best Practices Guide』を参照してください。

3. [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。

4. **（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。

5. [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 Network Time Protocol（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 Cisco Identity Services Engine（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。

6. [サービスサブネット（Services Subnet）]：アシュアランス、インベントリ収集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 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。

（注）

- 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、「アプライアンスの設定」章の「アプライアンスの再イメージ化」のトピックを参照してください）。

7. [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。

（注）

- 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、「アプライアンスの設定」章の「アプライアンスの再イメージ化」のトピック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。最初は意図的に大きなアドレス空間を確保するように要求されます。これは、IP が不足することなく、また単にシステムをアップグレードするだけのために連続するアドレス空間の再割り当てをお客様に求めることなく、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です。

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

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：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	**eno1**	**ネットワークアダプタ #1**
クラウド：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	**eno2**	**ネットワークアダプタ #2**
エンタープライズ：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	**enp94s0f0**	**ネットワークアダプタ #3**
クラスタ：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	**enp94s0f1**	**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」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
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

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 Cisco.com およびその他の URL にアクセスして、ソフトウェアアップデート、ライセンス、および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 に必要とするアクセスをアプライアンスに提供するには、HTTPS プロキシサーバを使用することをお勧めします。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プロキシサーバは、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できますが、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。このような理由から、設定時にプロキシを設定する場合は、必ずプロキシのHTTPポートを指定する必要があります。

何らかの理由で設定後にプロキシ設定を変更する必要がある場合は、GUIインターフェイス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SDアクセス ポートおよびプロトコル」を参照してください。

（注） 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 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）
80	HTTP	TCP
111	NFS（アシュアランスのバックアップに使用）	TCPおよびUDP
123	NTP	UDP
162	SNMP	UDP
443	HTTPS	TCP
2049	NFS（アシュアランスのバックアップに使用）	TCPおよびUDP
2222	SSH	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）
20048	NFS（アシュアランスのバックアップに使用）	TCP および UDP
32767	NFS（アシュアランスのバックアップに使用）	TCP および UDP

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と Cisco ISE へ）	TCP
23	Telnet（ネットワーク デバイスへ）	TCP
53	DNS	UDP
80	ポート 80 は出力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。 シスコでサポートされている証明書および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 URL にあるシスコのアドレスへの発信 IP トラフィックを許可するようにネットワークを設定できます。 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

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）
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

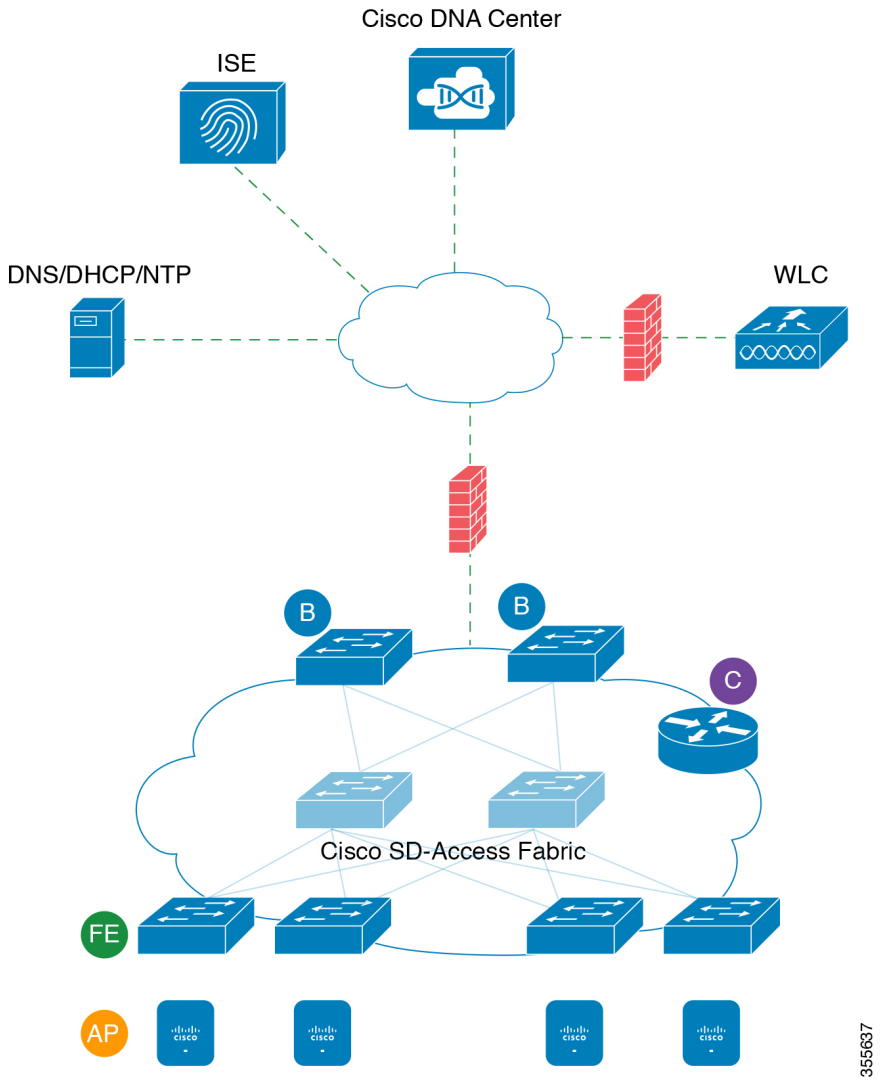
プロトコル（TCP または UDP）	ポート番号	トラフィックのタイプ
TCP	22	SSH
TCP	2222	SSH
TCP	80	HTTP
TCP	443	HTTPS
UDP	67	bootps
UDP	123	NTP
UDP	162	SNMP

さらに、アプライアンスから次の URL にあるシスコのアドレスへの発信 IP トラフィックを許可するようにネットワークを設定できます。https://www.cisco.com/security/pki/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 SD アクセス ポートおよびプロトコル

このトピックでは、次の図に示すように、一般的なSDAファブリック導入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 *5 : SDA* ファブリック インフラストラクチャ



ネットワークに SDA を実装している場合は、次の表の情報を使用して、ネットワーク管理を自動化するために必要なアクセスを Cisco DNA Center に提供しながら、SDA 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	接続先	説明
任意	Cisco DNA Center	UDP 53	DNS Server	Cisco DNA Center から DNS サーバの間で使用

任意	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
任意	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
任意	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
任意	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）
任意	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 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）
任意	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（SDA 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 自動化中の初期に使用
任意	Cisco DNA Center	UDP 123	NTP Server	Cisco DNA Center から NTP サーバの間で使用
任意	Cisco DNA Center	TCP 22、UDP 161	WLC	Cisco DNA Center から WLC へ
ICMP	Cisco DNA Center	ICMP	WLC	Cisco DNA Center から WLC へ
任意	Cisco DNA Center	TCP 80、TCP 443	AP	Cisco DNA Center からセンサー、アクティブセンサー（Cisco Aironet 1800S）の AP の間で使用

任意	Cisco DNA Center	TCP 32626	AP	Cisco DNA Center から AP へ（gRPC 用）

[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	接続先	説明
任意	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
任意	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
任意	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
任意	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
任意	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
任意	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
任意	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
任意	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
任意	Cisco DNA Center	TCP 443	apiconsole.cisco.com	CSSM スマートライセンス API
任意	Cisco DNA Center	TCP 443	sso.cisco.com	CCO とスマートライセンス
任意	Cisco DNA Center	TCP 443	api.cisco.com	CCO とスマートライセンス

任意	Cisco DNA Center	TCP 443	apx.cisco.com	CCO とスマートライセンス
任意	Cisco DNA Center	TCP 443	dashboard.meraki.com	Meraki の統合
任意	Cisco DNA Center	TCP 443	api.meraki.com	Meraki の統合
任意	Cisco DNA Center	TCP 443	n63.meraki.com	Meraki の統合
任意	Cisco DNA Center	TCP 443	dnacenter.uservoice.com	ユーザフィードバックの送信
任意	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/*）
任意	Cisco DNA Center	TCP 443	www.mapbox.com	マップと WLC の国番号の識別

表 *14 : SDA* 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	接続先	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およびルータと 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 リレーパケット用に使用されます。
任意	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およびルータのループバック IP と Cisco DNA Center の間で PnP 用に使用
任意	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
任意	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

任意	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およびルータと Cisco DNA Center の間でアシュアランス用に使用
任意	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
任意	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	任意	Cisco DNA Center	ファブリックスイッチおよびルータのループバックと Cisco DNA Center の間で SNMP デバイス検出のために使用
任意	ファブリックアンダーレイ	UDP 53	DNS Server	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 カプセル化制御メッセージ
TCP および UDP 4342	ファブリックアンダーレイ	任意	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
任意	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）
任意	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およびルータのループバック IP と ISE の間で RADIUS 用に使用
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	任意	ISE	ファブリックスイッチと ISE の間で CoA 用に使用

任意	ファブリックアンダーレイ	UDP 123	NTP Server	ファブリックスイッチおよびルータのループバック IP と NTP サーバの間で使用
任意	control-plane	UDP および TCP 4342/4343	WLC	コントロールプレーンのループバック IP と WLC の間でファブリック対応ワイヤレス用に使用

[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*：ワイヤレス *LAN* コントローラ（*WLC*）トラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 5246/5247/5248	WLC	任意	AP IP プール	WLC と AP サブネットの間で CAPWAP 用に使用
ICMP	WLC	ICMP	AP IP プール	WLC と Ping を許可する AP の間でトラブルシューティングのために使用
任意	WLC	UDP 69/5246/5247 TCP 22	AP IP プール	WLC と AP サブネットの間で CAPWAP 用に使用
任意	WLC	UDP および TCP 4342/4343	コントロールプレーン	WLC とコントロールプレーンループバック IP の間で使用
任意	WLC	TCP 32222	Cisco DNA Center	WLC と Cisco DNA Center の間でデバイス検出のために使用
UDP 161	WLC	任意	Cisco DNA Center	WLC と Cisco DNA Center の間で SNMP 用に使用
任意	WLC	UDP 162	Cisco DNA Center	WLC と Cisco DNA Center の間で SNMP トラップ用に使用
任意	WLC	TCP 16113	MSE および Spectrum Expert	WLC と MSE および Spectrum Expert の間で NMSP 用に使用
ICMP	WLC	ICMP	Cisco DNA Center	WLCから、トラブルシューティングに向けた Ping の許可に使用
任意	HA サーバ	TCP 1315	Cisco DNA Center	データベースサーバ HA（QoS）
任意	HA サーバ	TCP 1316 ～ 1320	Cisco DNA Center	HA データベースポート

任意	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
任意	WLC および各種 Syslog サーバ	UDP 514	WLC	Syslog（オプション）
任意	WLC	UDP 53	DNS Server	WLC と DNS サーバの間で使用
任意	WLC	TCP 443	ISE	WLC と ISE の間でゲスト SSID Web 認証のために使用
任意	WLC	UDP 1645、1812	ISE	WLC と ISE の間で RADIUS 認証のために使用
任意	WLC	UDP 1646、1813	ISE	WLC と ISE の間で RADIUS アカウンティングのために使用
任意	WLC	UDP 1700、3799	ISE	WLC と ISE の間で RADIUS CoA 用に使用
ICMP	WLC	ICMP	ISE	WLC と ISE ICMP の間でトラブルシューティングのために使用
任意	WLC	UDP 123	NTP サーバ	WLC と NTP サーバの間で使用

表 *16 :* ファブリック対応ワイヤレスアクセスポイント（*AP*）の *IP* プールトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 68	AP IP プール	UDP 67	DHCP サーバ	AP IP プールと DHCP サーバの間で使用
ICMP	AP IP プール	ICMP	DHCP サーバ	AP IP プールと ICMP の間でトラブルシューティングのために使用
任意	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
任意	AP IP プール	UDP 69/5246/5247/5248	WLC	AP IP プールと WLC の間で CAPWAP 用に使用
ICMP	AP IP プール	ICMP	WLC	AP IP プールから WLC に送信。トラブルシューティングのために Ping を許可

表 *17 : Identity Services Engine*（*ISE*）トラフィック

送信元ポート[4]	送信元	宛先ポート	接続先	説明

任意	ISE	TCP 64999	Border	ISE とボーダーノードの間で SXP 用に使用
任意	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	任意	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
任意	ISE	UDP 1700/3799	ファブリックアンダーレイ	ISE とファブリックスイッチおよびルータのループバック IP の間で気付アドレス用に使用
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
任意	ISE	UDP 123	NTP Server	ISE と NTP サーバの間で使用
UDP 1812/1645/1813/1646	ISE	任意	WLC	ISE と WLC の間で RADIUS 用に使用
ICMP	ISE	ICMP	WLC	ISE と WLC の間でトラブルシューティングのために使用

[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	接続先	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	接続先	説明
UDP 123	NTP Server	任意	ISE	NTP サーバから ISE の間で使用
UDP 123	NTP Server	任意	Cisco DNA Center	NTP サーバから Cisco DNA Center
UDP 123	NTP Server	任意	ファブリックアンダーレイ	NTP サーバとファブリックスイッチおよびルータのループバックの間で使用
UDP 123	NTP Server	任意	WLC	NTP サーバと WLC の間で使用

表 *20 : DNS* サーバトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 53	DNS Server	任意	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 Server	任意	WLC	DNS サーバと WLC 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。

1. **Linux ユーザ名（Linux User Name）**：これは **maglev** です。このユーザ名はプライマリ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いて、変更できません。

2. **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。選択した場合は、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。

   - 長さが 8 文字以上である。
   - タブまたは改行を含まない。
   - 次の中から少なくとも 3 つのカテゴリの文字を含む。

- 大文字のアルファベット
- 小文字のアルファベット
- 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プライマリノードの Linux パスワードを入力するように求められます。

3. [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）] を押すことができます。Maglev 設定ウィザードは、そのシードフレーズを使用してランダムかつ安全なパスワードを生成します。[自動生成パスワード（Auto Generated Password）] フィールドを使用して、生成されたパスワードをさらに編集できます。

4. **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）。安全であることを確認するため、初回ログイン時にこのパスワードを変更するように求められます。

   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、上記で説明した Linux パスワードと同じ要件を満たす必要があります。

5. [CIMCユーザパスワード（CIMC User Password）]：CIMC グラフィック ユーザ インターフェイス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 ブラウザ経由でアクセスするために CIMC を初回セットアップするときに変更するように求められます（「CIMC への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、上記で説明した 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。

6. **プライマリノード IP アドレス（Primary 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、プライマリ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

アプライアンスの設定が完了したら、Cisco DNA Center に初回ログインし、基本的なセットアップタスクを完了します。この初回設定時には、次の情報が必要になります。

1. **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。

2. **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。
3. **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。
4. **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。現在のリリースでは、InfoBlox または Bluecat がサポートされています。
5. **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。
6. **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。シスコでは、通常の Cisco DNA Center のすべての操作に対して、これらの新しいユーザアカウントのいずれかを常に使用することを推奨しています。Cisco DNA Center の再設定や、スーパーユーザ権限が明示的に必要なその他の操作を除き、管理者スーパーユーザアカウントを使用することは避けてください。

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。

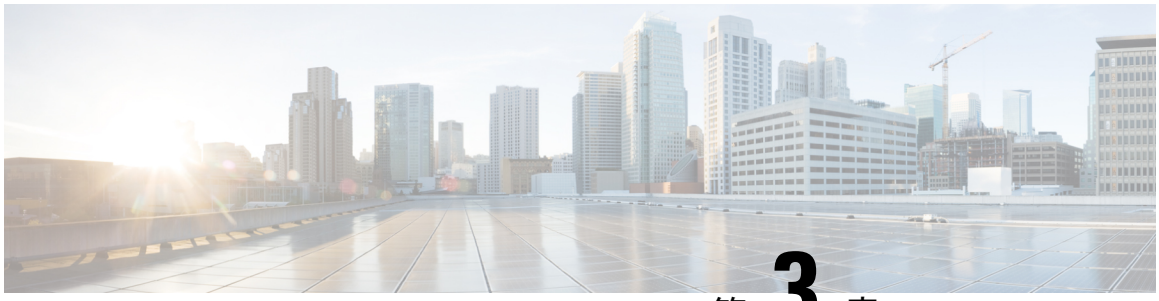
また残りの設定タスクを完了するために次の情報が必要になります。これは初回ログイン後に実行できます。

1. **ISEサーバのIPとログイン情報（ISE Server IP and Credentials）**：Cisco Identify Services Engine（ISE）サーバの IP アドレス、管理ユーザ名、パスワードが必要です。これらは「Cisco ISE と Cisco DNA Center の統合」で説明されているように、組織の ISE サーバにログインして Cisco DNA Center とのデータ共有設定を行うために必要です。
2. **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、上記の 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、および再試行/タイムアウト設定が必要です。

   別の認証およびポリシーサーバを使用している場合は、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、および再試行/タイムアウトの設定が必要になります。

この情報を使用して、選択した認証およびポリシーサーバと Cisco DNA Center を統合します。これについては、「認証サーバとポリシー サーバの設定」で説明しています。

3. **SNMPの再試行とタイムアウト値（SNMP Retry and Timeout Values）**：「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

次の表に、物理的な設置タスクとその実行順序を詳しく説明します。設置する Cisco DNA Center アプライアンスごとに、次の手順を実行します。最初のプライマリ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。

この表内のすべてのタスクが正常に完了したら、「アプライアンスの設定ワークフロー」の手順に従って続行します。

表 *21 : Cisco DNA Center* アプライアンスの設置タスク

ステップ	説明
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。 • Cisco DNA CenterおよびCisco Software-Defined 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 • 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 • 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。 • 機能概要 • 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

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。

ヒント 後でアプライアンスの輸送が必要になったときに備えて、輸送用の箱を保管しておいてください。

（注） シャーシは厳密に検査したうえで出荷されています。輸送中の破損や内容品の不足がある場合には、ただちにカスタマー サービス担当者に連絡してください。

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。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 破損の有無を調べ、内容品の間違いや破損がある場合には、カスタマー サービス担当者に連絡してください。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

この警告マークは「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。装置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

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、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る可能性があります。アプライアンスをラックに取り付けるときは、これらのレールによりアプライアンス間で必要な最小の間隔が提供されるので、レールキットにアプライアンスをマウントすることを推奨します。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 鉄共振技術を使用する無停電電源装置（UPS）タイプは避けてください。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 Site Preparation Guide*』を参照してください。
- アプライアンスの周囲に、保守作業および適切な通気のための十分なスペースがあることを確認します。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、0.38 インチ（9.6 mm）の正方形、0.28 インチ（7.1 mm）の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバあたりの縦方向の最小ラック スペースは、1 RU、つまり 1.75 インチ（44.45 mm）である必要があります。

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。

電源ステータスは、次のように電源ステータス LED で確認できます。

- 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。
- 緑色：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。

次のタスク

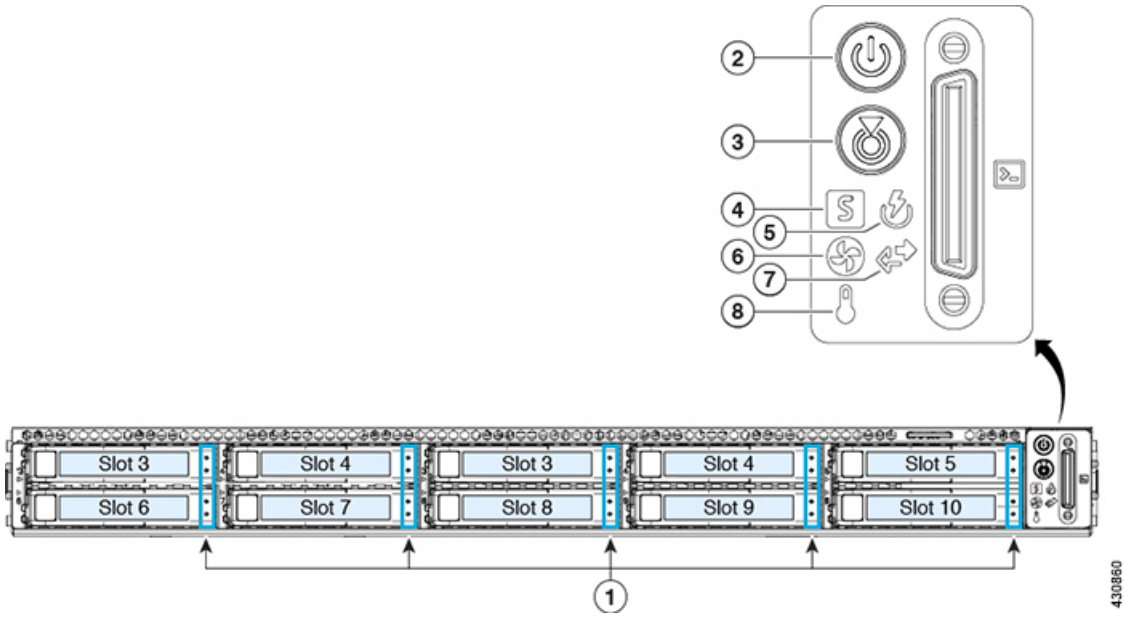
「LED の確認」で説明されている手順に従って続行します。

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。

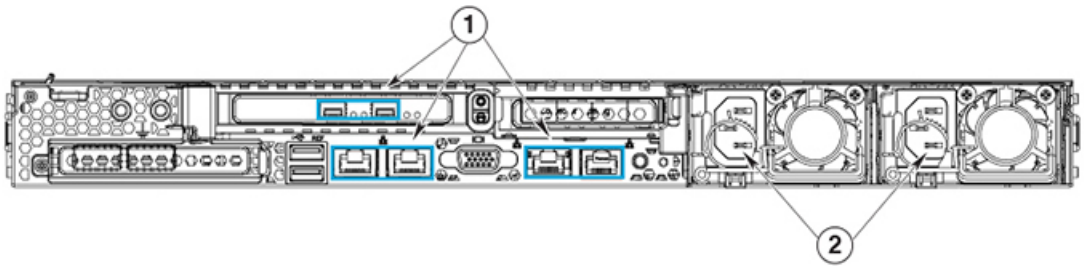
次の図は、物理的な設置と初回の電源投入が終わった後（設定前）動作しているアプライアンスの LED を示しています。

図 *6 :* 前面パネル *LED*



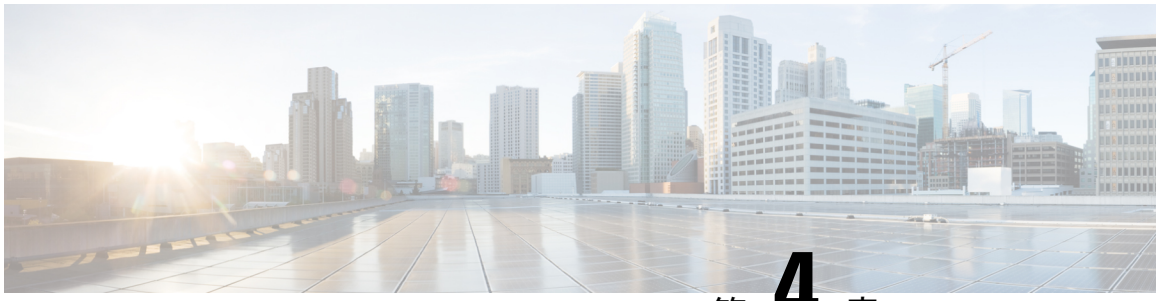
LED	望ましいステータスインジケータ
1	ドライブ障害 LED：消灯。 ドライブアクティビティ LED：緑
2	電源ステータス：緑
3	ユニット識別：消灯
4	システムステータス：緑
5	電源装置ステータス：緑
6	ファンステータス：緑
7	ネットワーク リンク アクティビティ：消灯
8	温度ステータス：緑

図 *7 :* 背面パネル *LED*



LED	望ましいステータスインジケータ
1	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 がオフであり、電源ステータス LED がグリーンになっているはずです。 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（「プライマリノードの設定」および「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	電源装置障害 LED：オフ AC 電源 LED：緑色

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

アプライアンスの設定ワークフロー

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

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

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

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

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

表 *22*：アプライアンスの設定タスク

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

CIMC へのブラウザアクセスの有効化

「アプライアンスのインストール ワークフロー」の説明に従ってアプライアンスをインストールした後、Cisco IMC 設定ユーティリティを使用して、アプライアンスの Cisco Integrated Management Controller（CIMC）ポートに IP アドレスとゲートウェイを割り当てます。この操作により、アプライアンスの設定に使用する CIMC グラフィック ユーザ インターフェイスへのブラウザアクセスが可能になります。

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

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

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

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

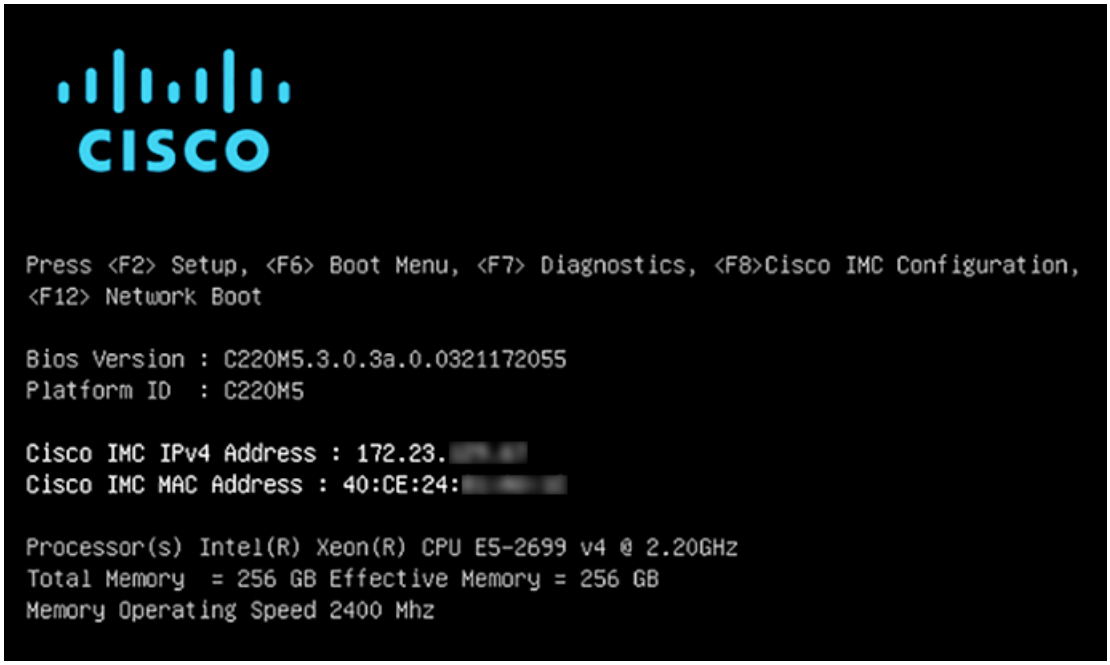
ステップ 1　次のいずれかを接続して、アプライアンスコンソールにアクセスします。

- アプライアンスの前面パネルにある KVM コネクタ（「前面パネルと背面パネル」の前面パネル図のコンポーネント 11）に接続する KVM ケーブルか、

- アプライアンスの背面パネルにある USB ポートと VGA ポート（「前面パネルと背面パネル」の背面パネル図のコンポーネント 2 および 5）に接続するキーボードとモニタ。

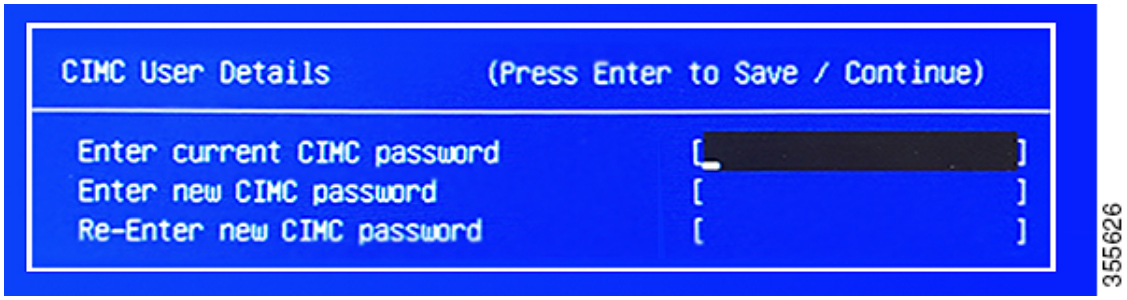
ステップ 2 アプライアンスの電源コードが接続され、電源がオンになっていることを確認します。

ステップ 3 前面パネルの**電源**ボタンを押して、アプライアンスをブートします。次に示すように、Cisco IMC 設定ユーティリティのブート画面が表示されるのを確認します。



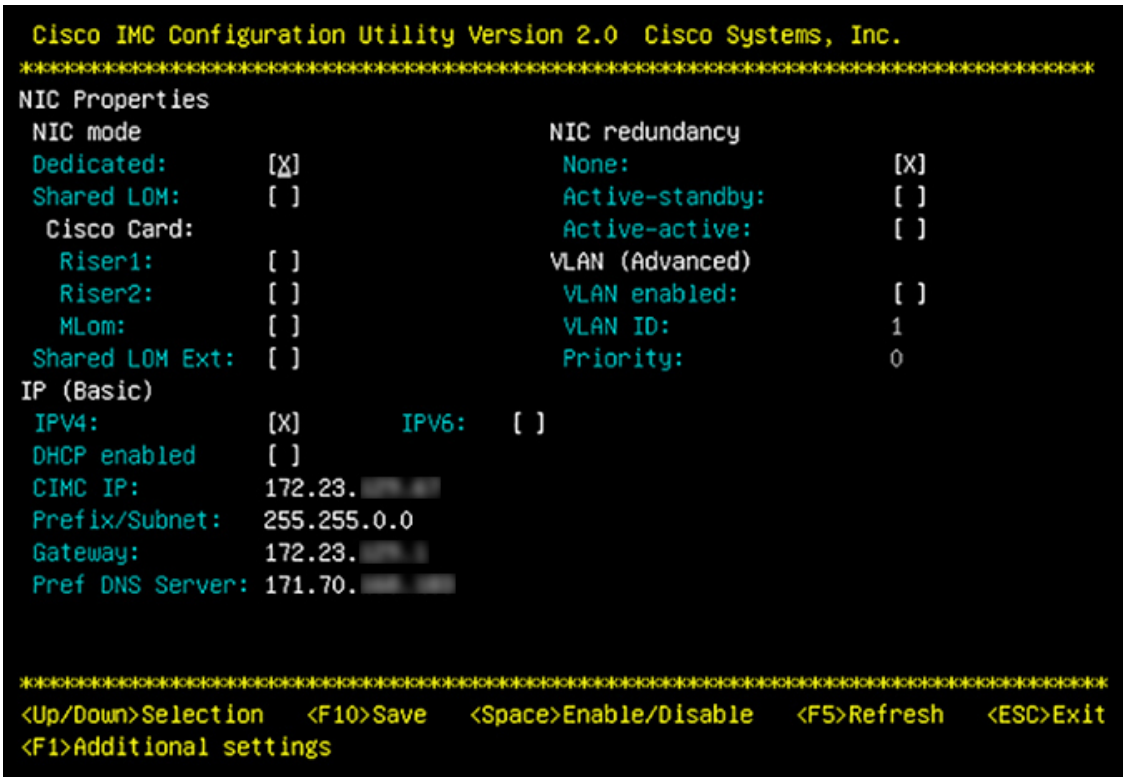
アップ

ステップ 4 ブート画面が表示されたら、すぐに **F8** キーを押して Cisco IMC 設定を実行してください。次に示すように、Cisco IMC 設定ユーティリティに [CIMCユーザの詳細（CIMC User Details）] 画面が表示されます。



ステップ 5 デフォルトの CIMC ユーザパスワード（新規アプライアンスで付与されるデフォルトのパスワードは「**password**」）を **[現在の CIMC パスワードを入力（Enter current CIMC Password）]**フィールドに入力します。次に、[新しいCIMCパスワードを入力（Enter New CIMC Password）] フィールドと [新しいCIMCパスワードを再入力（Re-Enter New CIMC Password）] フィールドに新しい CIMC ユーザパスワードを入力して確認します。

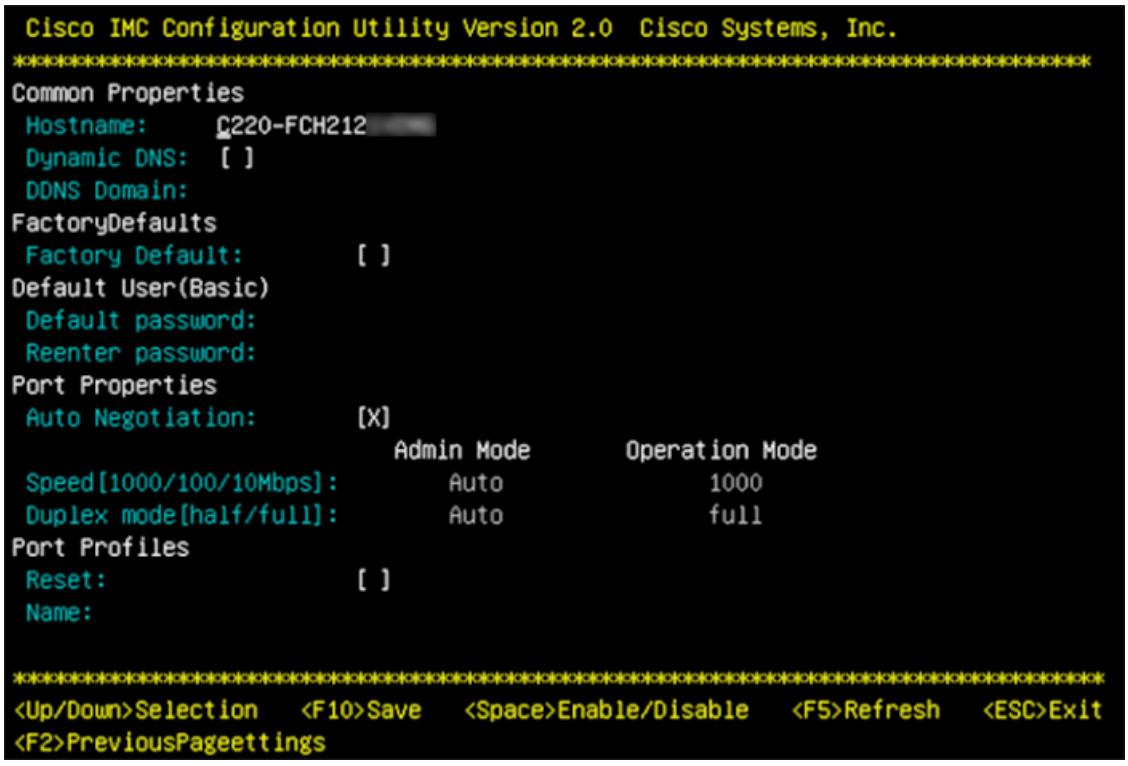
ステップ 6 [新しいCIMCパスワードを再入力（Re-Enter New CIMC Password）] フィールドで **Enter** を押すと、次に示すように、Cisco IMC 設定ユーティリティに [NICプロパティ（NIC Properties）] 画面が表示されます。



ステップ 7 次の変更を加えます。

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

ステップ 8 **F1** を押して **[追加設定（Additional Settings）]** を指定します。次に示すように、Cisco IMC 設定ユーティリティに [共通プロパティ（Common Properties）] 画面が表示されます。



ステップ 9 次の変更を加えます。

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

ステップ 10 **F10** を押して、設定を**保存**します。

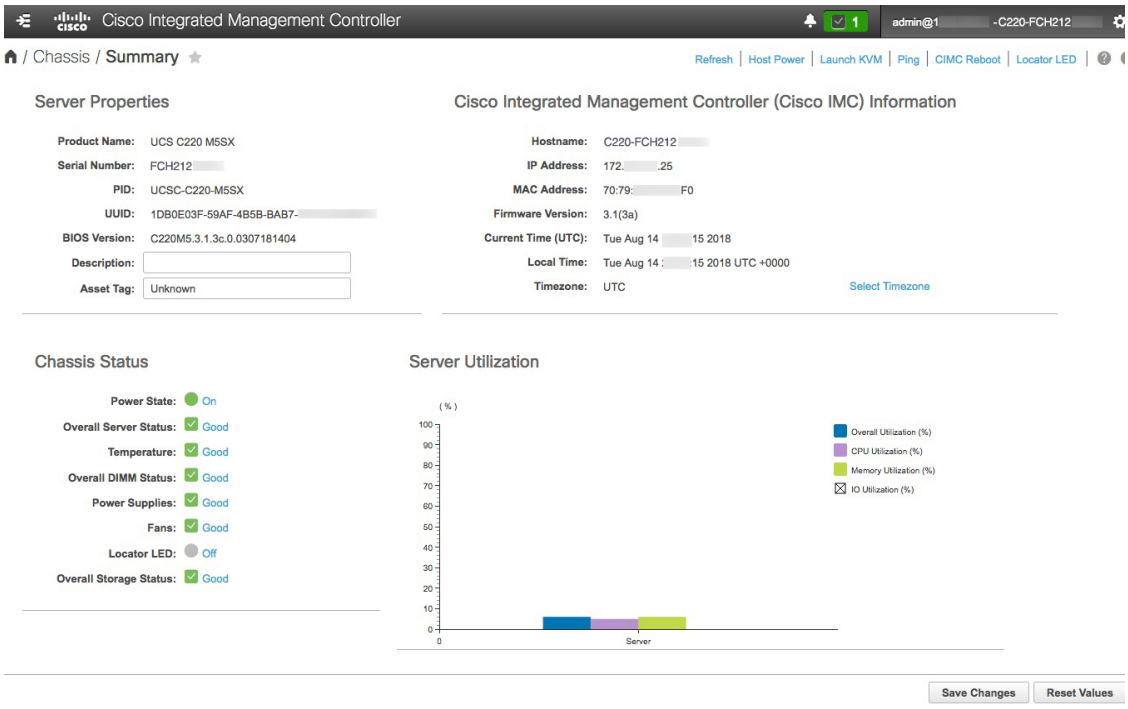
ステップ 11 **Esc** を押して**終了**し、アプライアンスをリブートします。

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

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

ブラウザに、次に示すような Cisco Integrated Management Controller GUI のメインログインウィンドウが表示されます。

ステップ 13 ステップ 5 で設定した CIMC ユーザ ID とパスワードを使用してログインします。ログインに成功すると、次に示すような [Cisco Integrated Management Controllerシャーシの概要（Cisco Integrated Management Controller Chassis Summary）] ウィンドウがブラウザに表示されます。



次のタスク

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

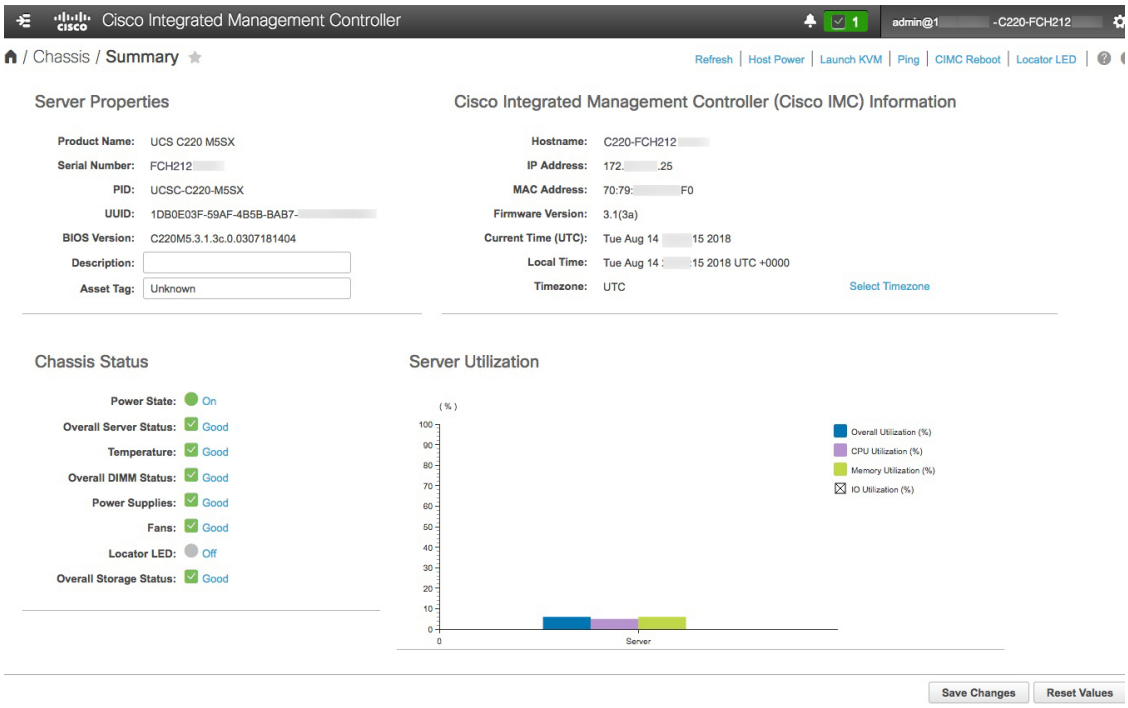
プリフライトチェックの実行

「アプライアンスのインストールワークフロー」の説明に従ってアプライアンスをインストールし、「CIMC へのブラウザアクセスの有効化」の説明に従って CIMC GUI へのアクセスを設定した後、CIMC を使用して次の事前設定タスクを実行します。この操作は、正しい設定と展開の確実な実行に役立ちます。

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

ステップ 1 「CIMC へのブラウザアクセスの有効化」で設定した CIMC IP アドレス、ユーザ ID およびパスワードを使用して、アプライアンスの CIMC にログインします。ログインに成功すると、次に示すような [Cisco

Integrated Management Controller シャーシの概要（Cisco Integrated Management Controller Chassis Summary）] ウィンドウがブラウザに表示されます。

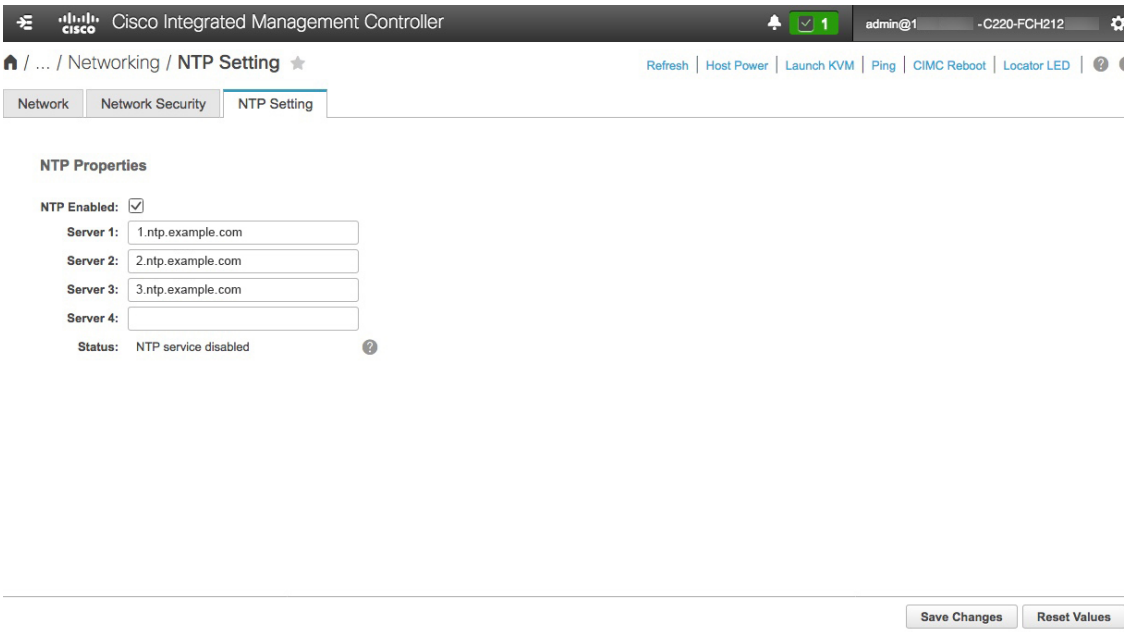


ステップ 2 次に示すように、アプライアンスハードウェアを、ネットワークの管理に使用する Network Time Protocol（NTP）サーバと同期します。

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

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

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



d) 完了したら、[変更の保存（Save Changes）] をクリックします。CIMC は、エントリを検証した後、アプライアンスハードウェアの時刻と NTP サーバの時刻の同期を開始します。

ステップ 3 次に、以下の手順に従って、アプライアンスの高スループット設定と一致するようにスイッチを再設定します。

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

b) 次の一連のコマンドを入力して、スイッチポートを設定します。

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

これらのコマンドは単なる例であることに注意してください。アプライアンス NIC を設定する際に入力したものと同じ VLAN ID と MTU の値を使用します。スイッチの例では、リンク速度、デュプレックス、およびMTUのコマンド値がデフォルトになっているので、デフォルト値を変更した場合にのみ入力する必要が生じます。アプライアンス NIC と同様に、スループットが向上するように MTU を設定することもできます（上限は 9000）。

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

```
MySwitch#show interface tengigabitethernet 1/1/3
TenGigabitEthernet1/1/3 is up, line protocol is up (connected)
  Hardware is Ten Gigabit Ethernet, address is XXXe.310.8000 (bia XXX.310.8000)
```

```
MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not set
Full-duplex, 10GB/s, link type is auto, media type is SFP-10Gbase-SR
```

d) `show run interface tengigabitethernet portID` というコマンドを実行して、X710-DA2 NIC ポートからのケーブルが接続されているスイッチポートを設定します。次に例を示します。

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

MySwitch#
```

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

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

MySwitch#
```

次のタスク

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

ネットワーク インターフェイス カードの無効化

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

カードを無効にするには、以下の手順を実行します。

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

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

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

ステップ 3 Cisco IMC の変更を保存します。

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

アプライアンスのイメージの再作成

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

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

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

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

「ブート可能な USB ドライブの作成」を参照してください。

ステップ 3 アプライアンスに Cisco DNA Center を再インストールします。

「Cisco DNA Center ISO イメージのインストール」を参照してください。

Cisco DNA Center ISO イメージの確認

Cisco DNA Center を展開する前に、ダウンロードした ISO イメージが正規の Cisco イメージかどうか確認することを強く推奨します。

始める前に

Cisco DNA Center ISO イメージの場所を把握します（電子メールを使用するか、シスコサポートチームと連絡を取るかのいずれかの方法で）。

ステップ 1 シスコによって指定された場所から Cisco DNA Center ISO イメージ（.iso）をダウンロードします。

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

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

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

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

（オペレーティングシステムに応じて）次のコマンドのいずれかを実行します。

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

Microsoft Windows にはチェックサムユーティリティが組み込まれていませんが、http://www.microsoft.com/en-us/download/details.aspx?id=11533 で Microsoft のユーティリティをインストールできます。上述のコマンド（または Microsoft Windows ユーティリティ）の出力を、ステップ 3 でダウンロードした SHA512 チェックサムファイルと比較します。コマンド出力が一致しない場合は、ISO イメージを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコ サポートにお問い合わせください。

ステップ 6 署名を確認し、ISO イメージが正規の製品でありシスコ製であることを確認します。

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

（注） このコマンドは、MAC と Linux の両方の環境で動作します。Windows の場合、まだ OpenSSL をインストールしていないなら、ダウンロードしてインストールする必要があります（ここで入手可能）。

ISO イメージが純正であれば、このコマンドを実行すると、「Verified OK」というメッセージが表示されます。このメッセージが表示されない場合は、ISO イメージをインストールせず、シスコ サポートに連絡してください。

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

ブート可能な USB ドライブの作成

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

始める前に

- Cisco DNA Center ISO イメージのコピーをダウンロードして確認します。「Cisco DNA Center ISO イメージの確認」を参照してください。
- 使用している USB フラッシュドライブの容量が少なくとも 32 GB であることを確認します。

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

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

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

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

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

- 成功時に自動マウント解除する
- 成功時に書き込みを検証する

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

ステップ 5 **[イメージの選択（Select Image）]** をクリックします。

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

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

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

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

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

Cisco DNA Center ISO イメージのインストール

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

始める前に

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

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

ステップ 2 CIMC にログインし、KVM セッションを開始します。

ステップ 3 アプライアンスの電源を投入または再投入します。

- アプライアンスが実行されていない場合には、**[電源（Power）]** > **[システムの電源オン（Power On System）]** を選択します。
- アプライアンスがすでに実行されている場合には、**[電源（Power）]**>**[システムの電源の再投入（コールドブート）（Power Cycle System（cold boot））]** を選択します。

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

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

ブートデバイス選択メニューが表示されます。

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

ステップ 7 [GNU GRUB] ブートローダウィンドウで、[Cisco DNA アプライアンスの作成（Manufacture Cisco DNA appliance）] を選択してから、**Enter** を押します。

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

Cisco DNA Center ISO イメージのインストールが完了すると、インストーラがリブートし、Maglev 設定ウィザードが開きます。

プライマリノードの設定

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

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

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

始める前に

次のことを確認します。

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

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

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

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

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

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

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

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

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

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

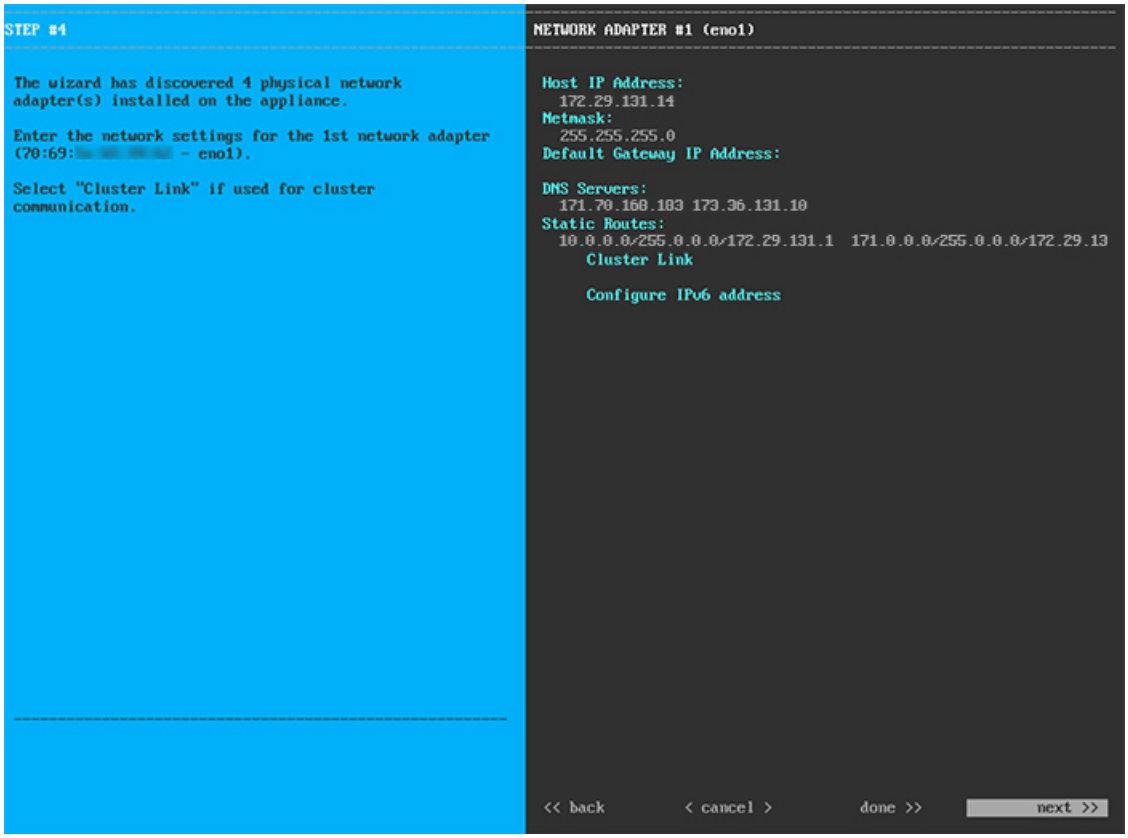
ステップ4 最初のクラスタオプションを選択して、プライマリノードの設定を開始します。

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

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

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

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

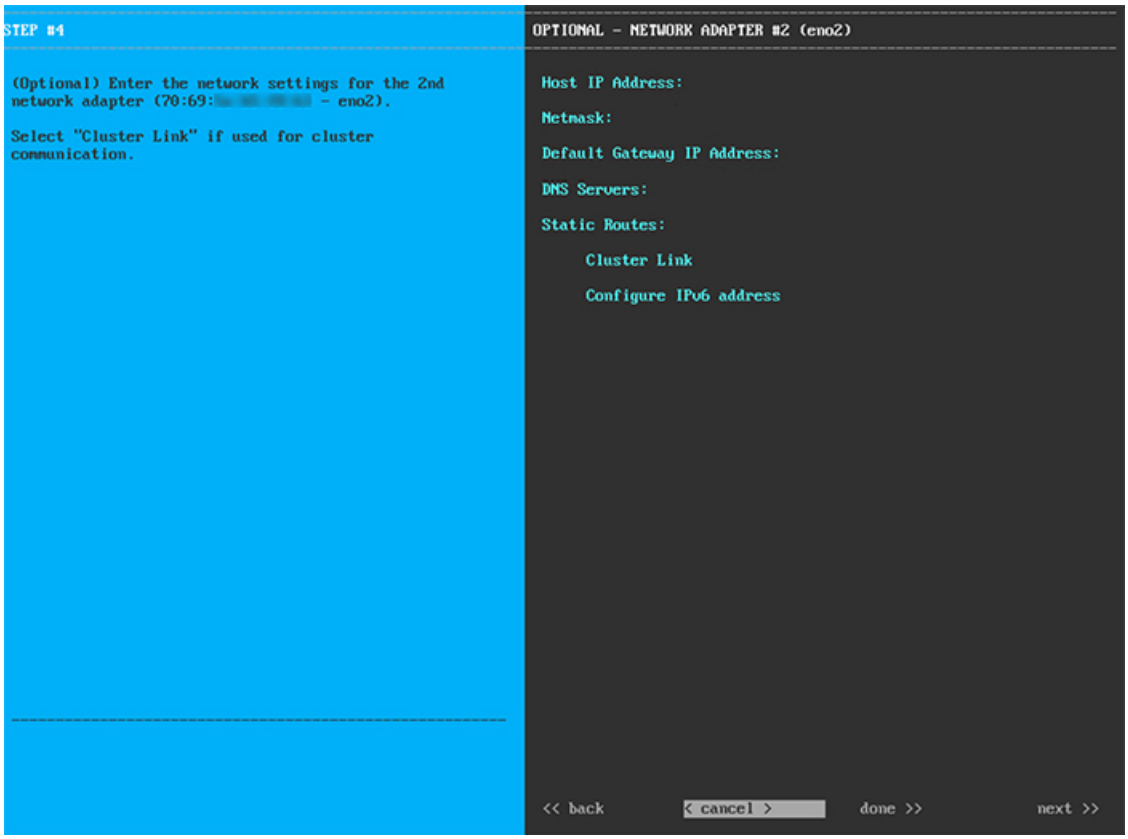
表 *23 :* ネットワークアダプタ *#1* のプライマリノードエントリ：*1Gbps/10Gbps* 管理ポート（*eno1*）

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

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

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

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

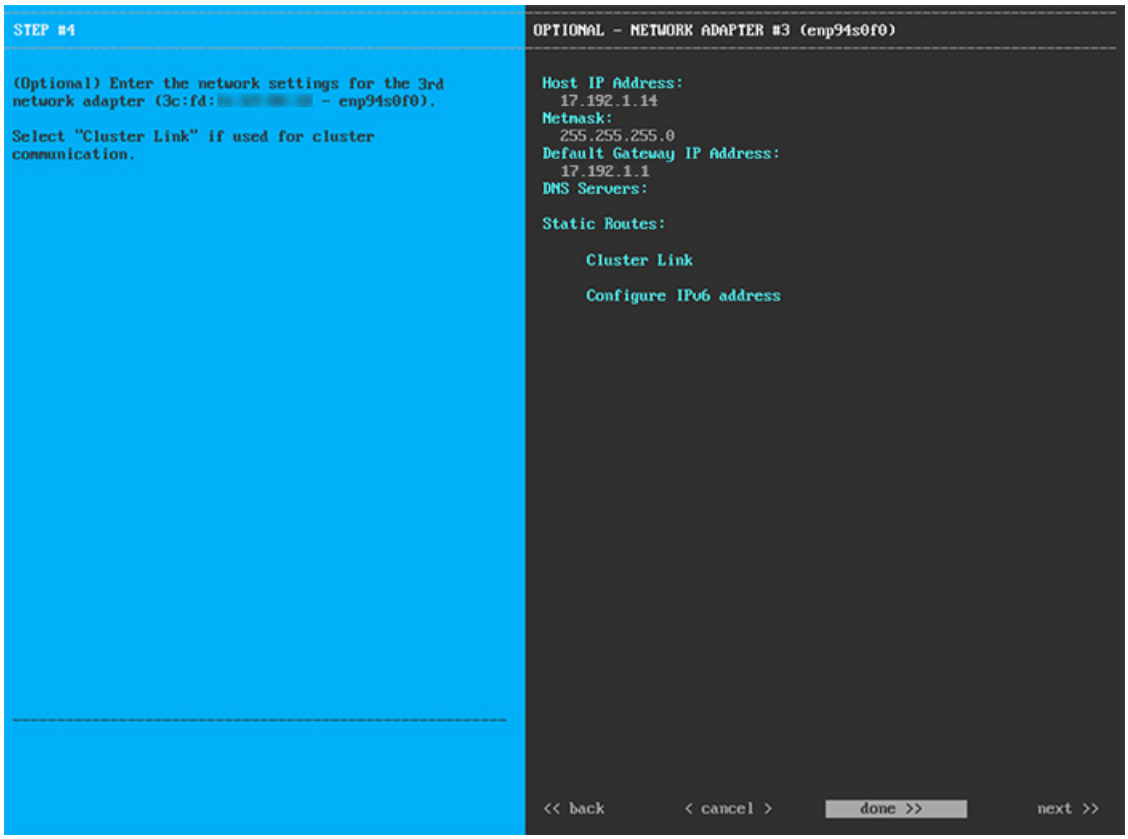
表 *24 :* ネットワークアダプタ *#2* のプライマリノードエントリ：*1Gbps/10Gbps* クラウドポート（*eno2*）

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

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

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

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

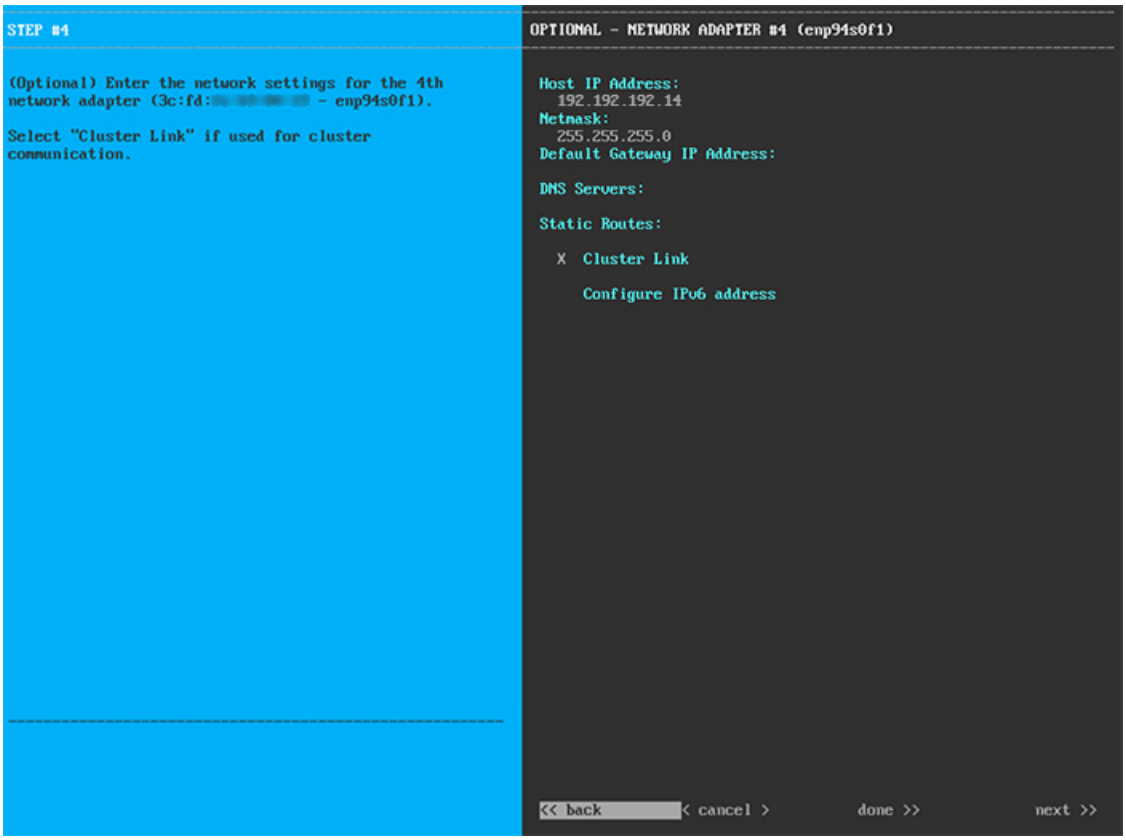
表 *25 :* ネットワークアダプタ *#3* のプライマリノードエントリ：*10Gbps* エンタープライズポート（*enp94s0f0*）

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

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

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

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



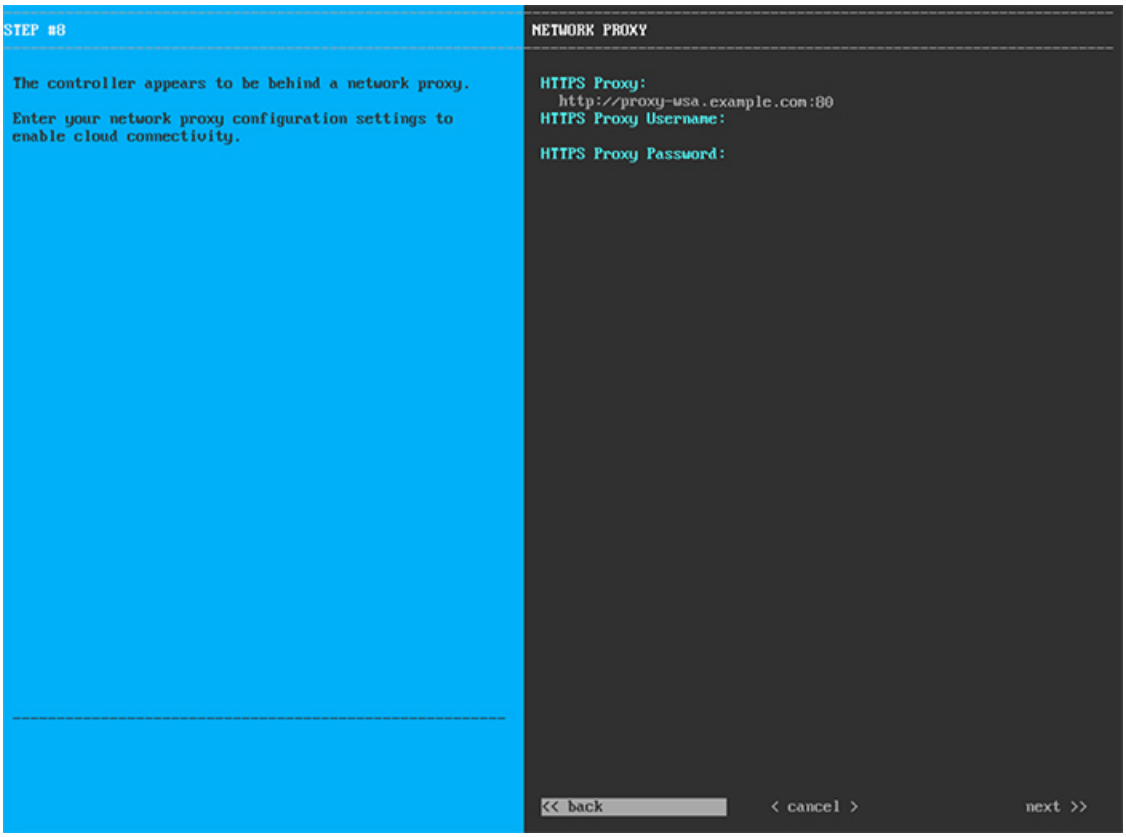
次の表に示すように、[ネットワークアダプタ#4（NETWORK ADAPTER #4）] の設定値を入力します。

表 *26 :* ネットワークアダプタ *#4* のプライマリノードエントリ：*10Gbps* クラスタポート（*enp94s0f1*）

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

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

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



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

表 *27*：ネットワークプロキシのプライマリノードエントリ

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

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

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

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

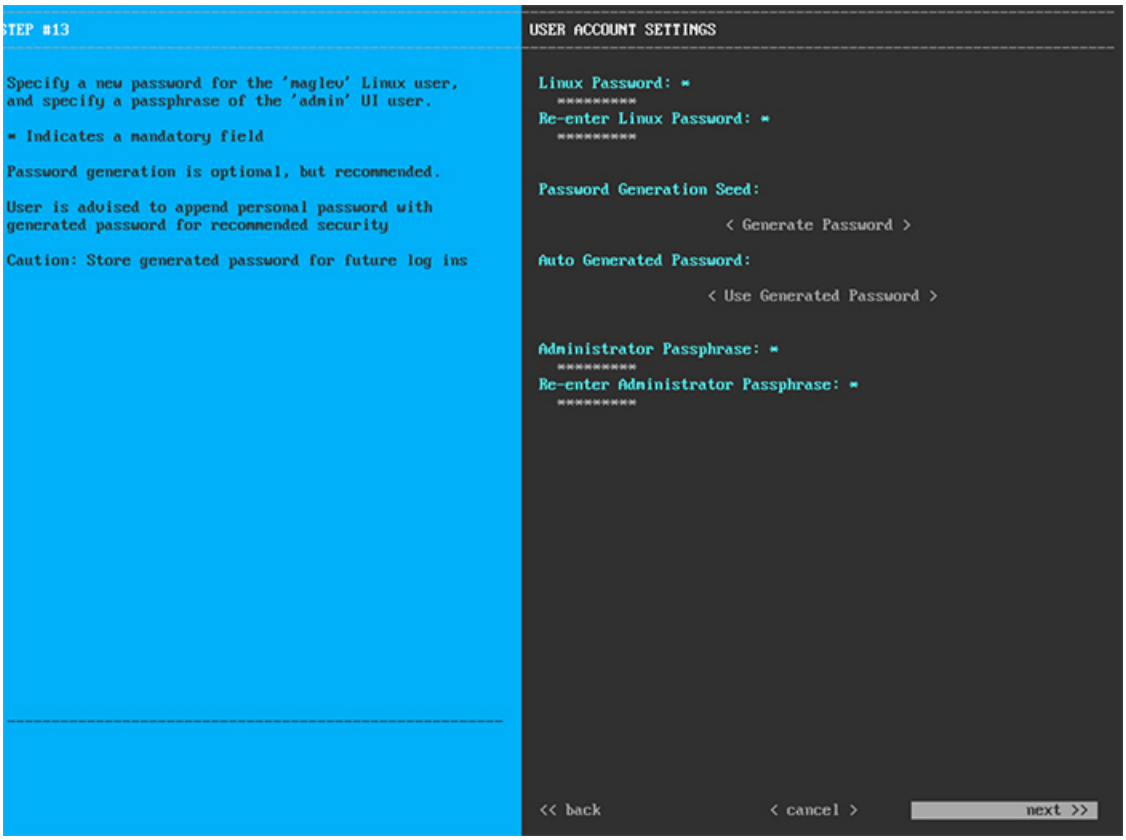
重要 設定済みのネットワークインターフェイスごとに 1 つずつ仮想 IP アドレスを入力する必要があります。この操作を行わない限り、ウィザードを完了することはできません。これらのアドレスは、クラスタリンクのステータスに関連付けられており、ステータスは**[アップ（UP）]**の状態となっている必要があります。

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

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

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

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



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

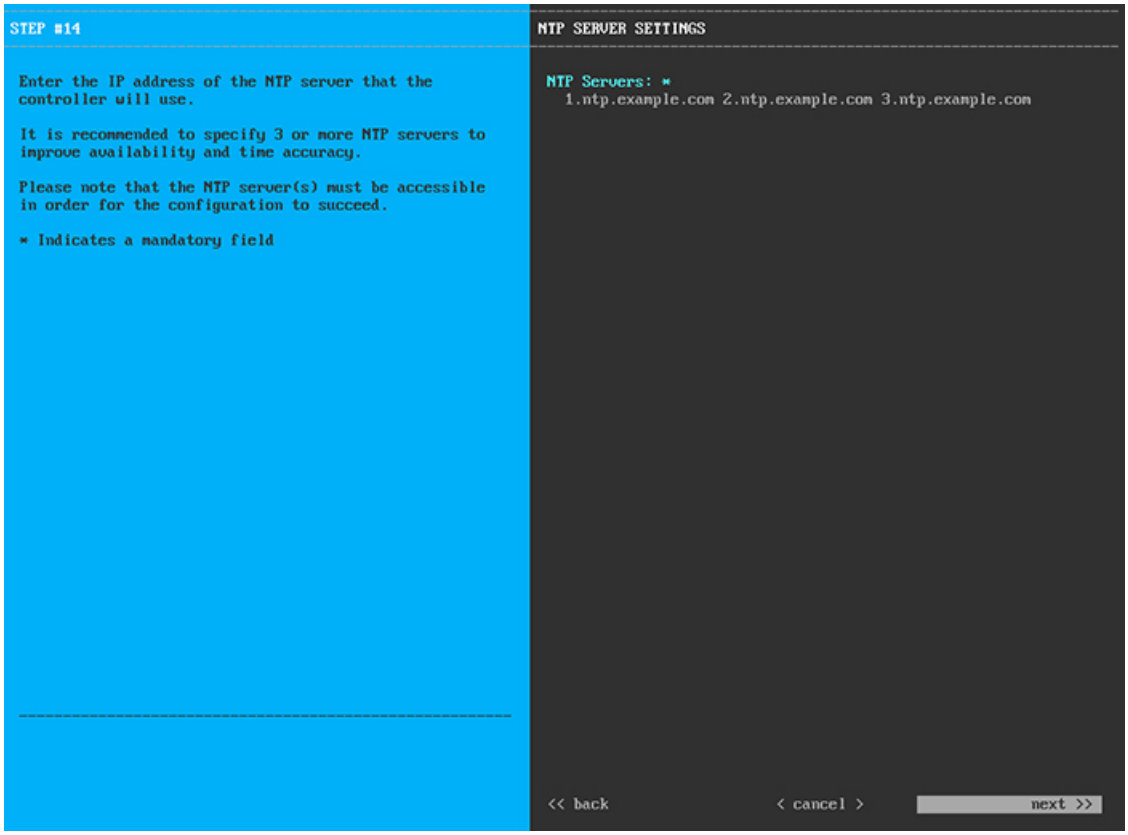
表 *28* : ユーザアカウント設定のプライマリノードエントリ

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

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

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

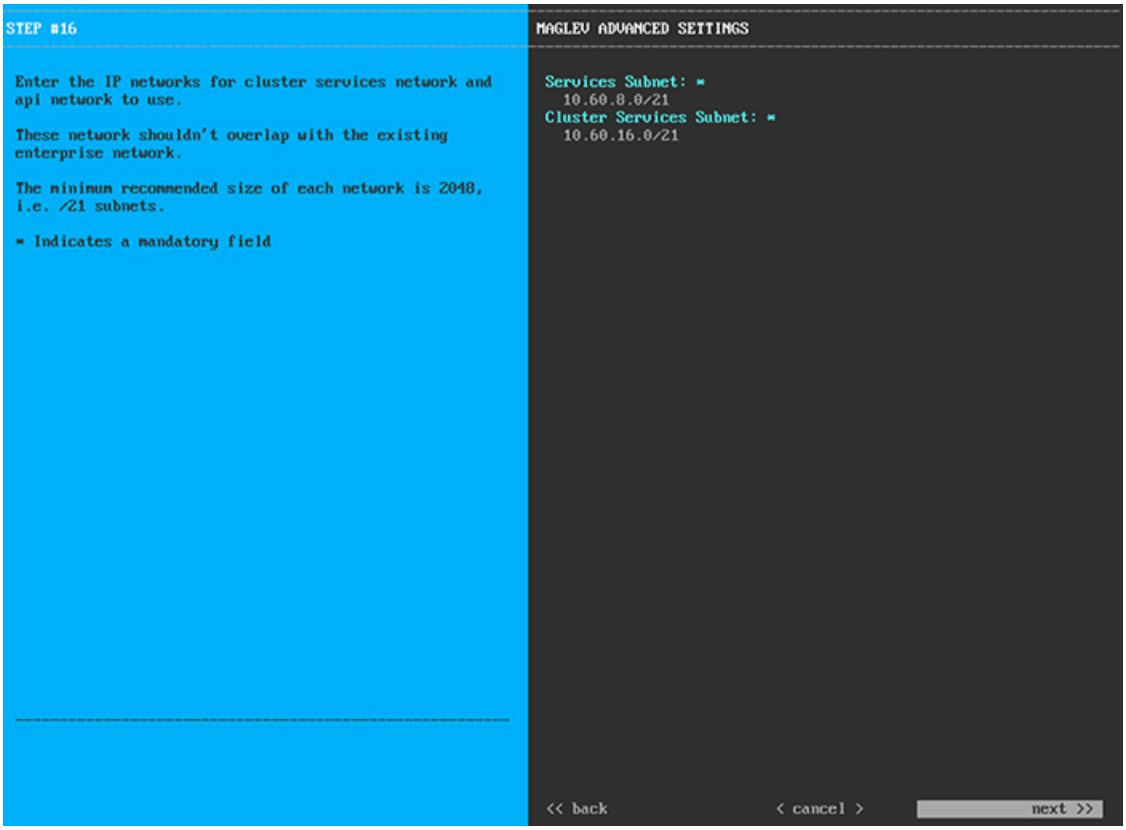
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように、[NTPサーバの設定（NTP SERVER SETTINGS）] の値を入力するようウィザードに求められます。



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

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

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



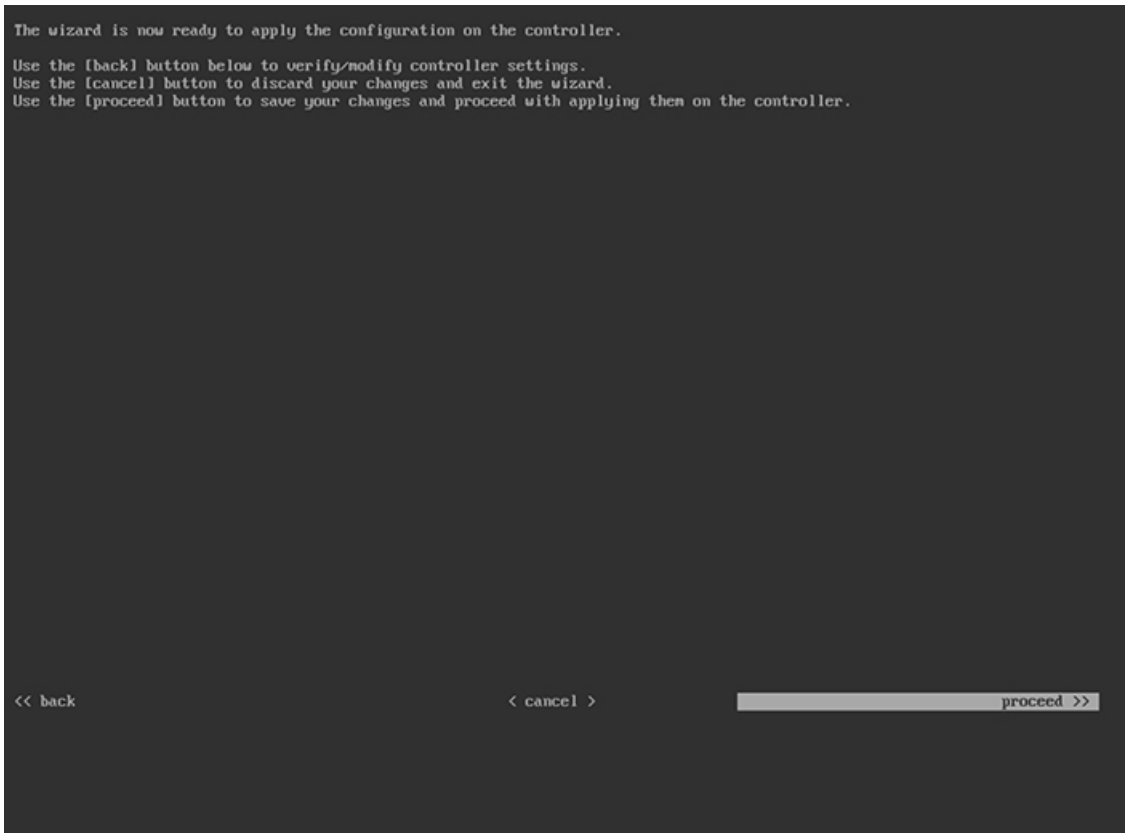
次の表に示すように、[MAGLEV 詳細設定（MAGLEV ADVANCED SETTINGS）] の設定値を入力します。

表 *29 : Maglev* 詳細設定のプライマリノードエントリ

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

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

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



[続行>>（proceed>>）] を選択して設定を完了します。

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

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

次のタスク

タスクが完了した後：

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

アドオンノードの設定

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

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

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

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

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

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

Welcome to the Maglev Appliance

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

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

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

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

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

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

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

始める前に

次のことを確認します。

- 「プライマリノードの設定」の手順に従って、クラスタ内の最初のアプライアンスが設定されたこと。
- 「必要なIPアドレスおよびサブネット」と「必須の設定情報」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。

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

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

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

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

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

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

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

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

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

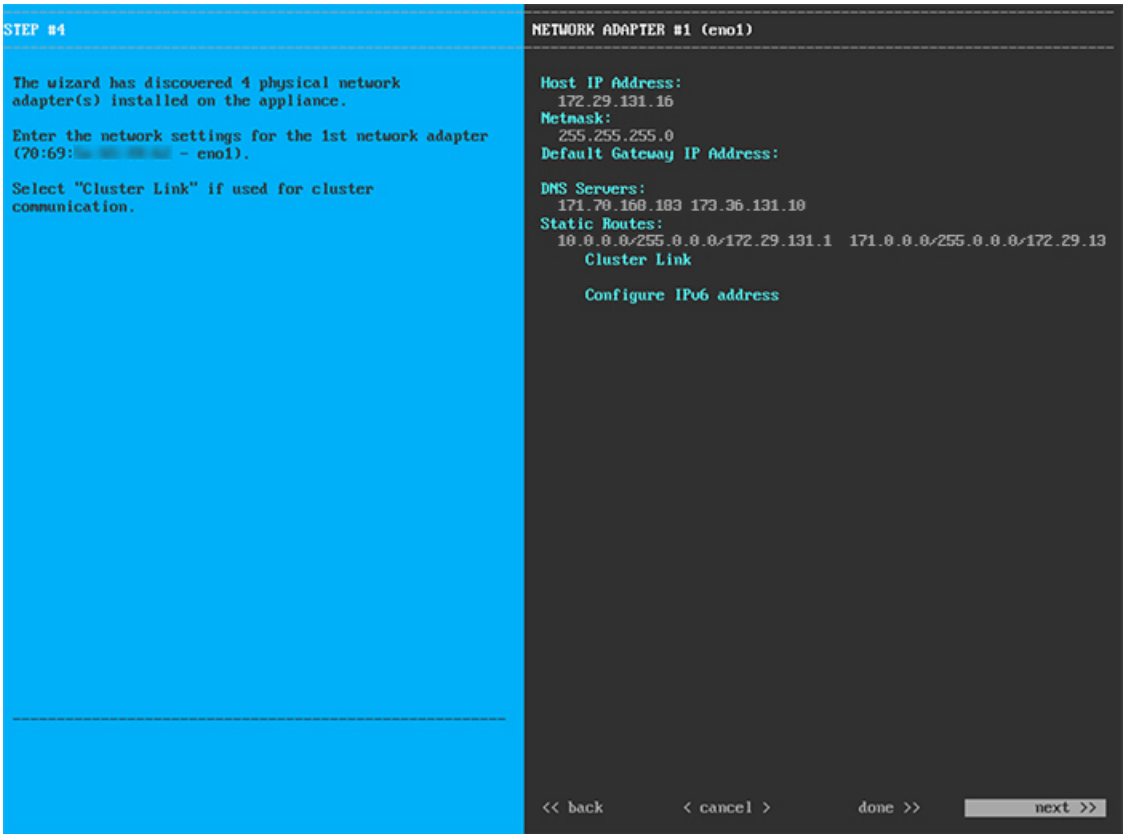
ステップ 4 **[Cisco DNA Centerクラスタに追加（Join a DNA-C cluster）]** を選択して、アドオンノードの設定を開始します。

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

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

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

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

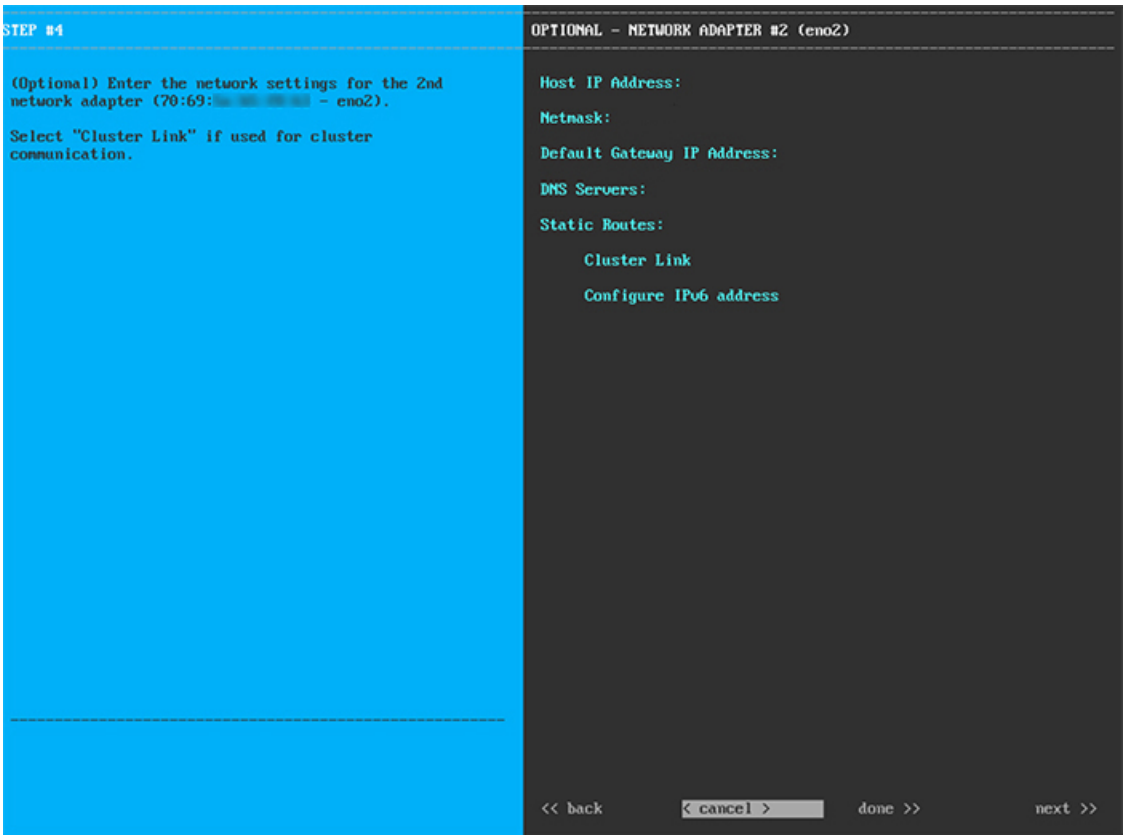
表 *30*：ネットワークアダプタ *#1* のアドオンノードエントリ：*1Gbps/10Gbps* 管理ポート（*eno1*）

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

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

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

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

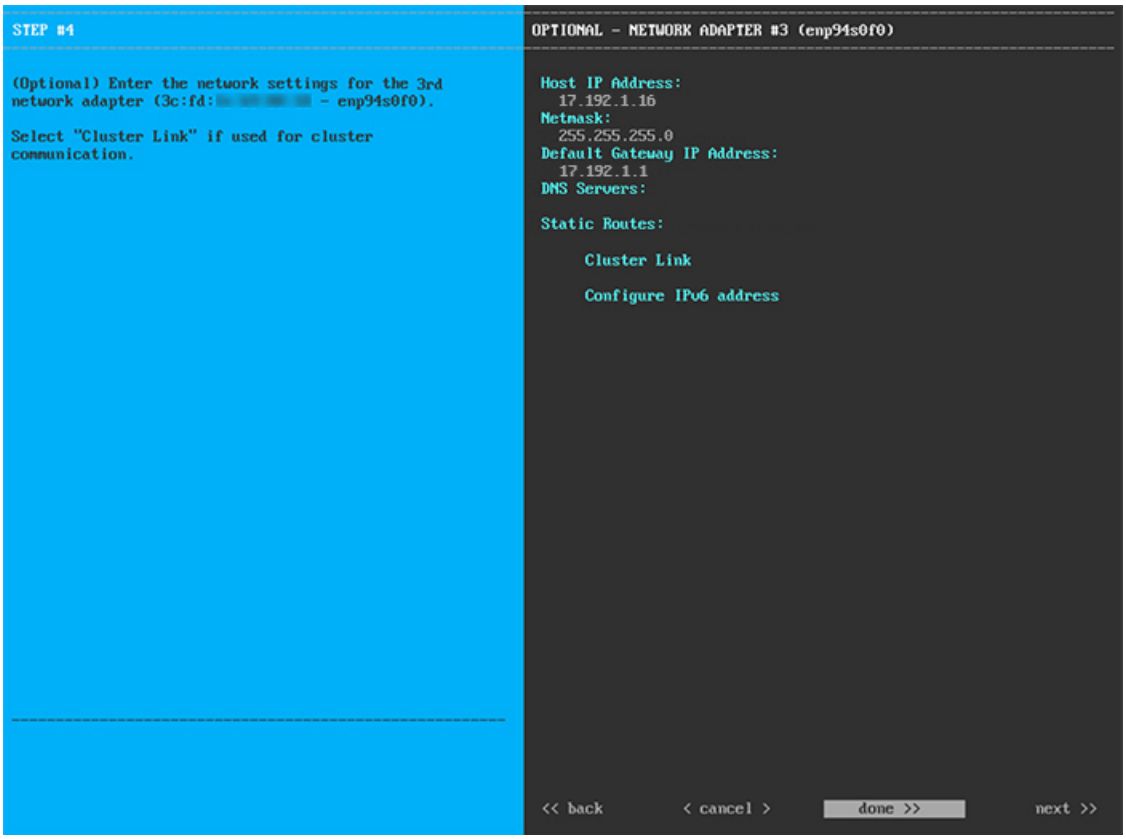
表 *31* : ネットワークアダプタ *#2* のアドオンノードエントリ：*1Gbps/10Gbps* クラウドポート（*eno2*）

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

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

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

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

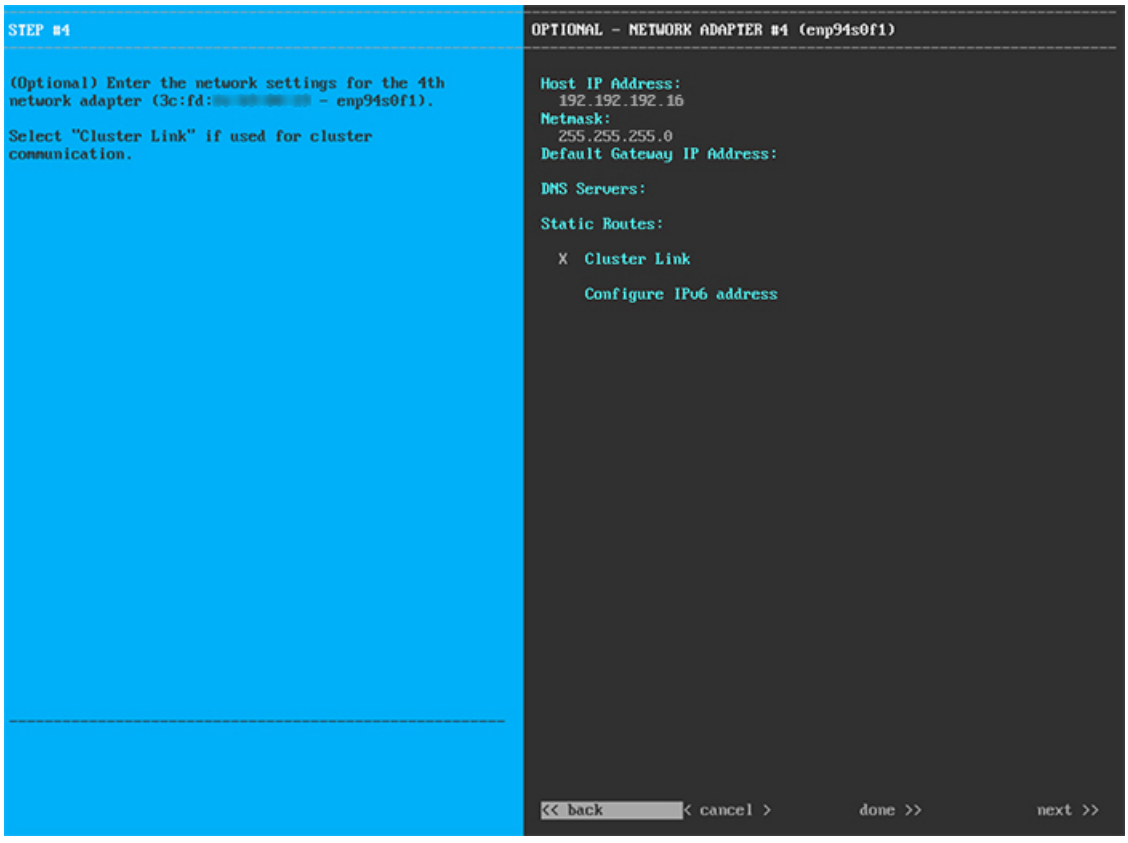
表 *32*：ネットワークアダプタ *#3* のアドオンノードエントリ：*10Gbps* エンタープライズポート（*enp94s0f0*）

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

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

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

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



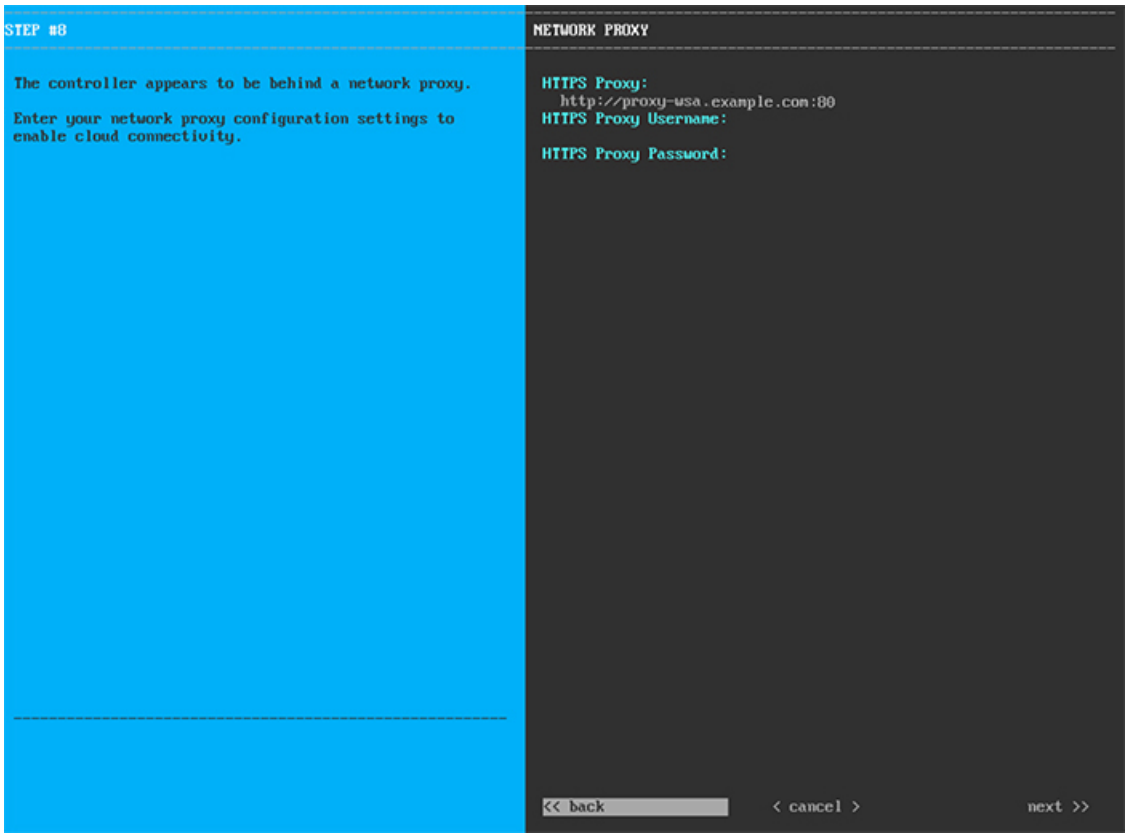
次の表に示すように、[ネットワークアダプタ#4（NETWORK ADAPTER #4）] の設定値を入力します。

表 *33 :* ネットワークアダプタ *#4* のアドオンノードエントリ：*10Gbps* クラスタポート（*enp94s0f1*）

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

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

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



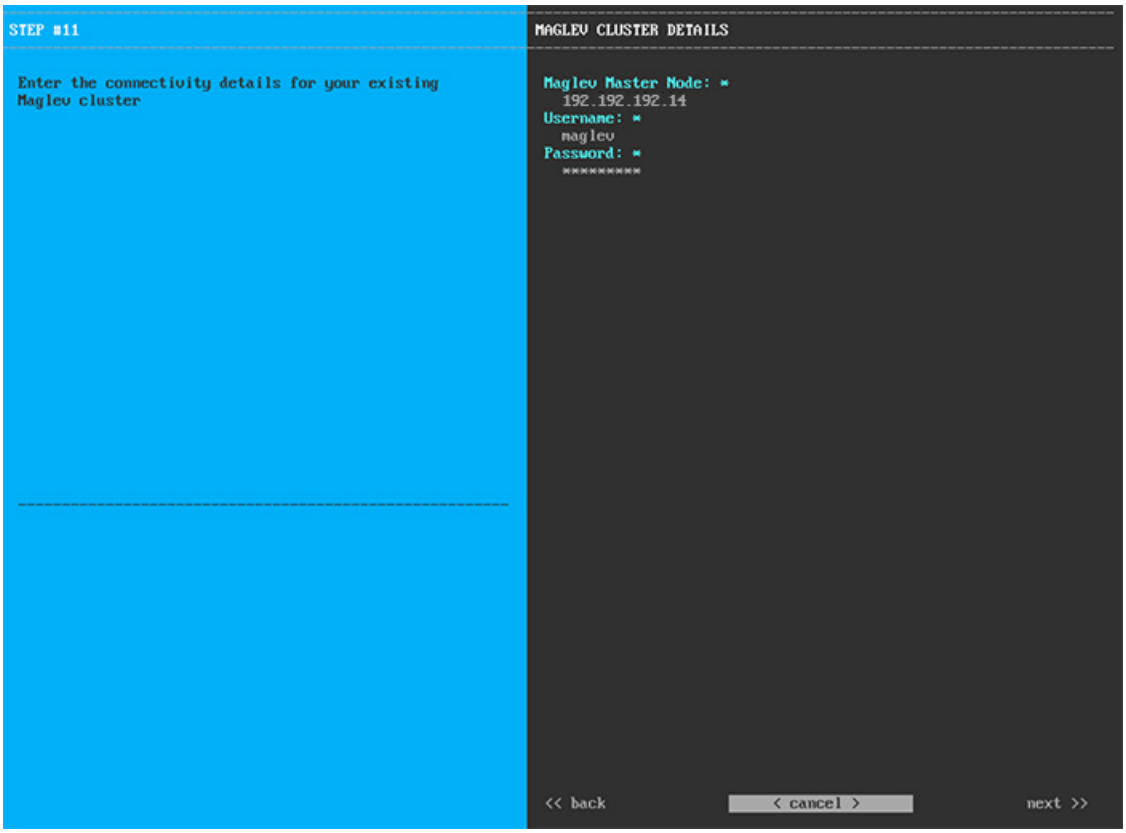
次の表に示すように、[ネットワークアダプタ（NETWORK ADAPTER）] の設定値を入力します。

表 *34* : ネットワークプロキシのアドオンノードエントリ

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

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

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



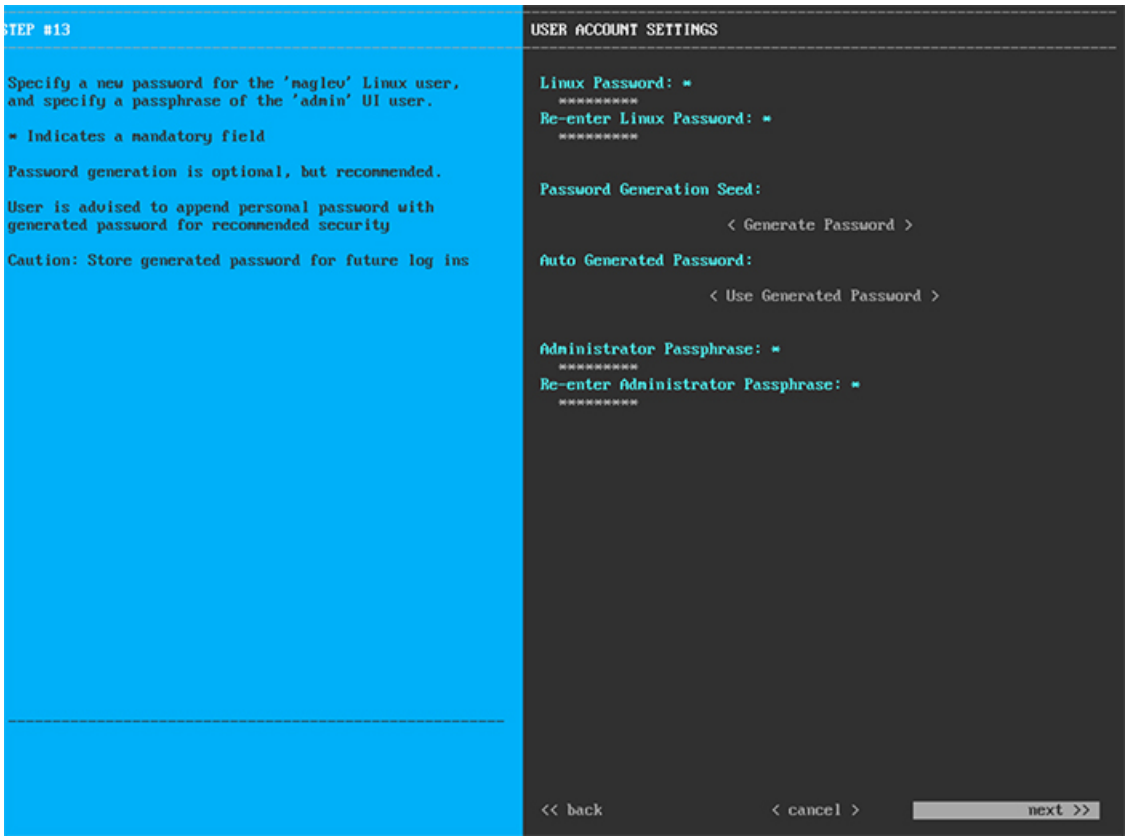
次の表の説明に従って、[MAGLEV クラスタの詳細（MAGLEV CLUSTER DETAILS）] に値を入力します。

表 *35 : Maglev* クラスタの詳細へのアドオンノードエントリ

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

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

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



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

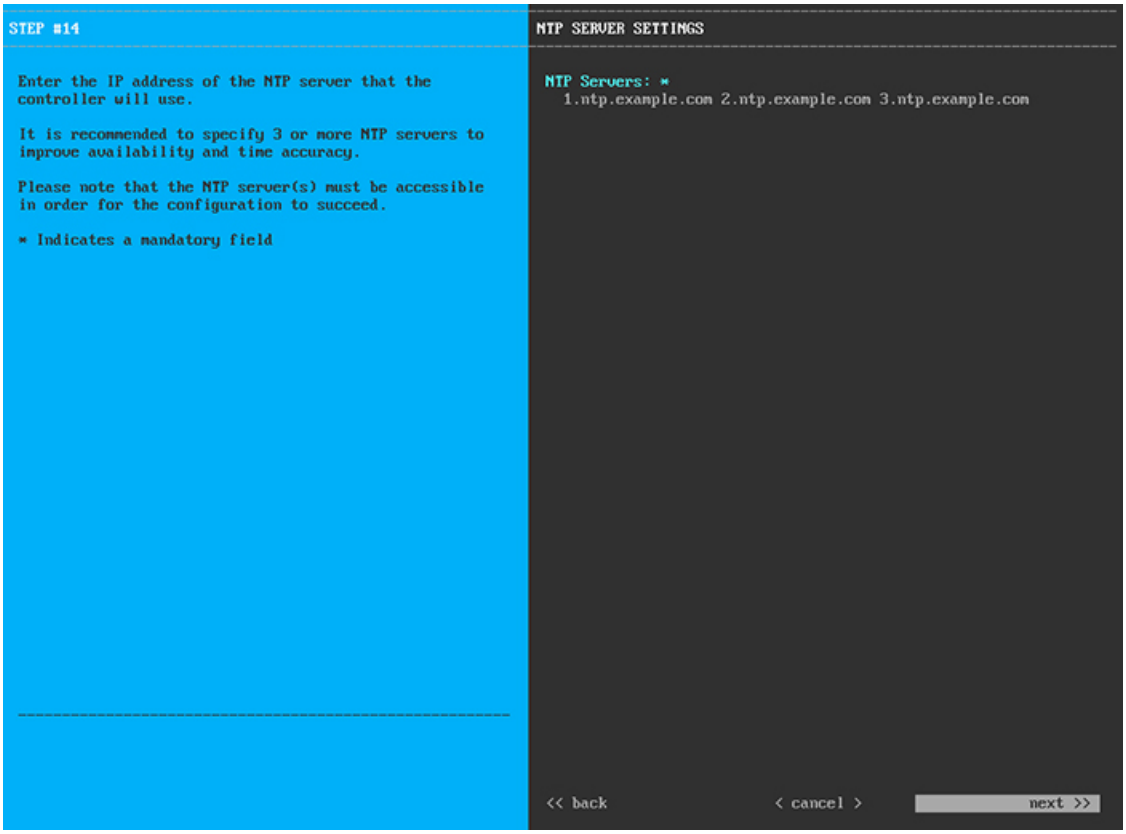
表 *36* : ユーザアカウント設定のアドオンノードエントリ

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

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

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

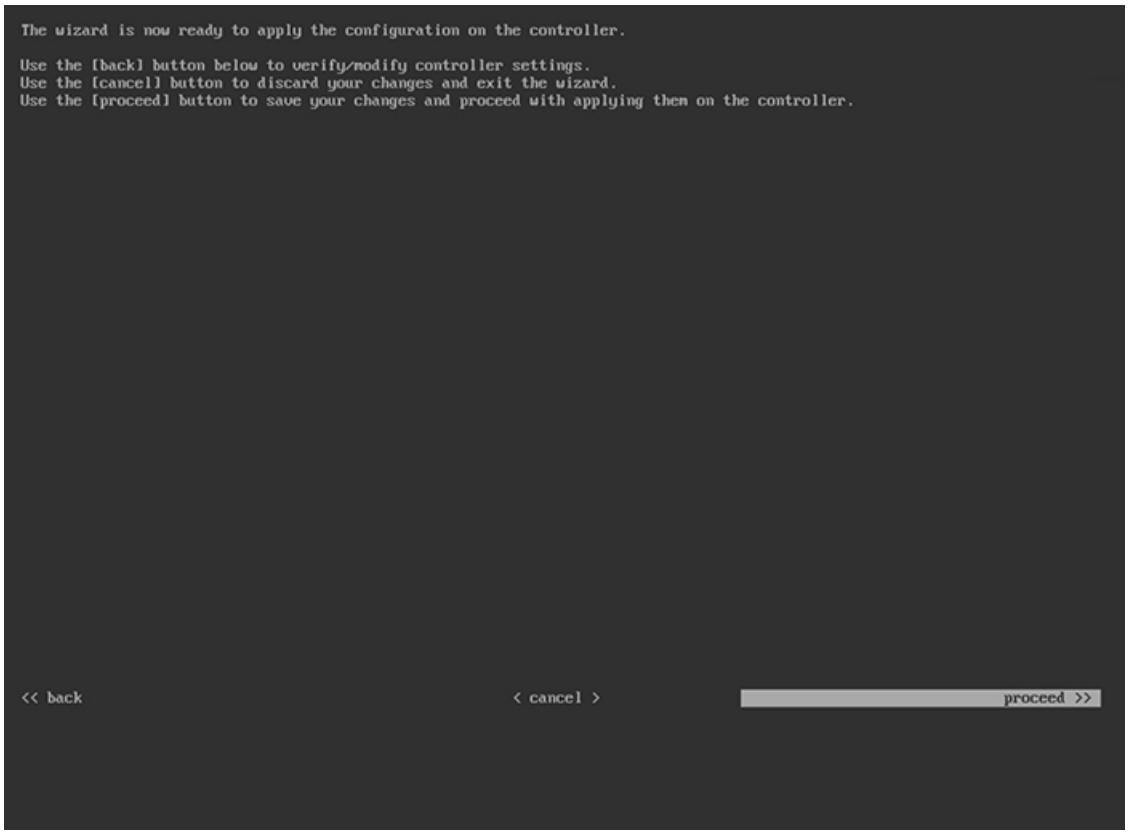
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように、[NTPサーバの設定（NTP SERVER SETTINGS）] の値を入力するようウィザードに求められます。



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

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

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



[続行>>（proceed>>）] を選択して設定を完了します。

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

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

次のタスク

タスクが完了した後：

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

ハイ アベイラビリティ クラスタの展開シナリオ

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

クラスタに導入する場合は、ネットワークに適した導入シナリオを選択します。

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

次の項では、各シナリオについて説明します。

新しい HA の展開

最新の HA クラスタをインストールするには、次の手順を実行します。

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

「プライマリノードの設定」を参照してください。

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

「アドオンノードの設定」を参照してください。

標準インターフェイス設定を使用したプライマリノードの既存 HA の展開

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

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

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

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

「インターフェイスケーブル接続」を参照してください。

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

「設定ウィザードを使用したアプライアンスの再設定」を参照してください。

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

「アドオンノードの設定」を参照してください。

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

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

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

非標準インターフェイス設定を使用したプライマリノードの既存 HA の展開

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

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

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

ステップ 2 リモートリポジトリのバックアップを作成します。

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

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

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

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

ステップ 5 ステップ 2 で作成したバックアップファイルを復元します。

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

「アドオンノードの設定」を参照してください。

HA の展開に関する追加の考慮事項

既存の HA の導入では、次の追加設定を行う必要があります。

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

テレメトリ

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

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

ステップ 2 デバイスでテレメトリを無効にします。

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

   [テレメトリ（Telemetry）] ウィンドウが表示されます。

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

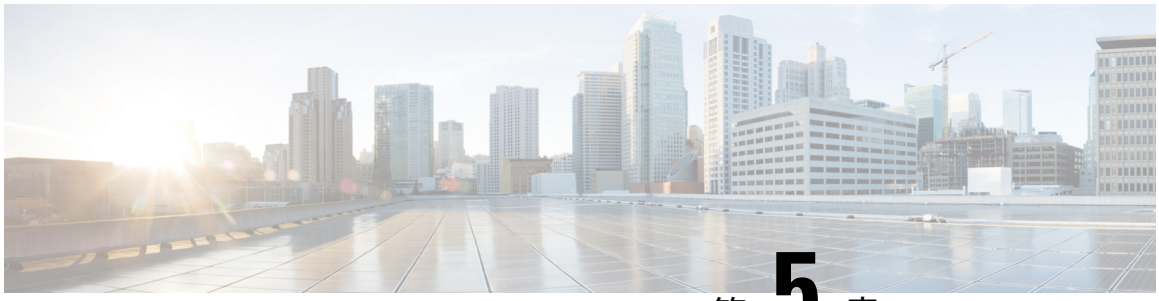
ステップ 3 以前のテレメトリプロファイルとデバイスの関連付けを使用して、テレメトリを再度有効にします。

ワイヤレス コントローラ

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

Cisco DNA Center の最新リリースへのアップグレード

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



第 5 章

初期設定の完了

初期設定ワークフロー

設置したすべての Cisco DNA Center アプライアンスの設定が完了したら、次の表に一覧になっているタスクを実行し、本番環境での使用向けに Cisco DNA Center を準備する必要があります。

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。

表 *37 : Cisco DNA Center* アプライアンスの初期設定タスク

ステップ	説明
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を参照してください。

ステップ	説明
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 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 Web インターフェイスは、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する必要があります。

初めて管理者スーパーユーザ（ユーザ名は「admin」で、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。

新しい Cisco DNA Center ユーザを作成する必要もあります。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。

- 「プライマリノードの設定」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」で必要とされている情報。

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 Cisco DNA Center GUI へのアクセスに使用するホスト IP アドレスを入力します。

HTTPS と、設定プロセスの最後に表示された Cisco DNA Center GUI の IP アドレスを使用します。

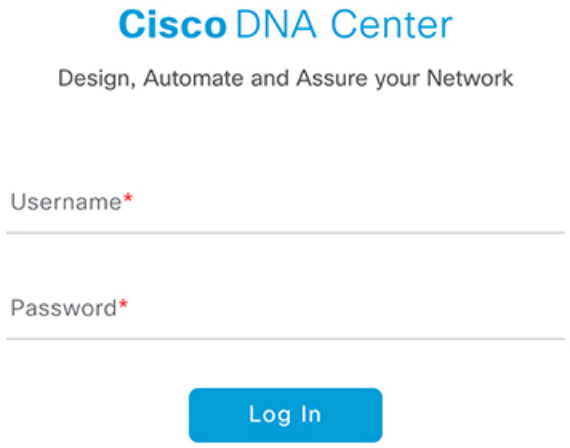
ステップ 3 ブラウザに IP アドレスを入力すると、「接続はプライベートではない」ことを示すメッセージが表示されます。

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

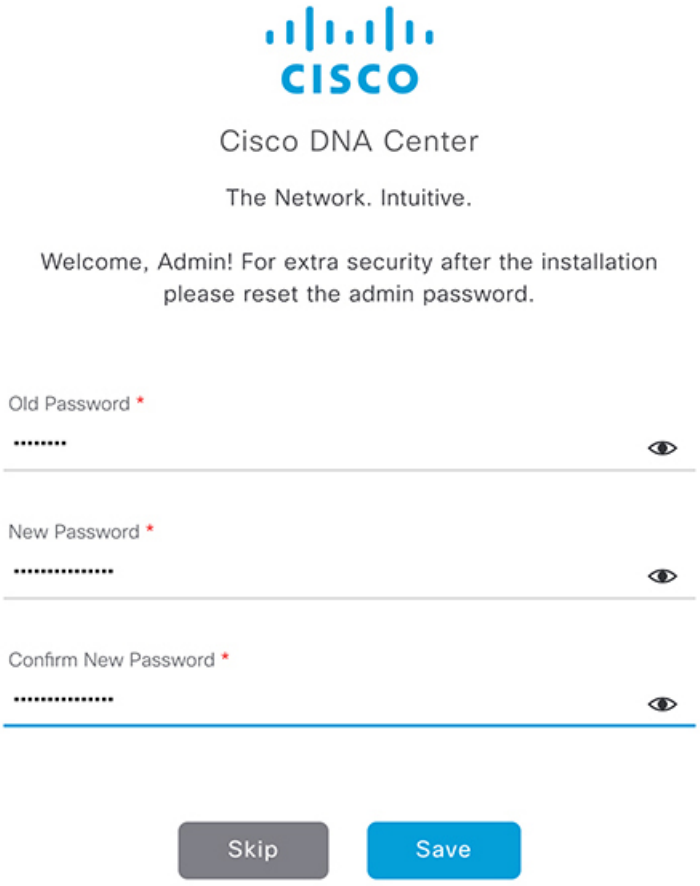
ステップ 4 サイトのセキュリティ証明書が信頼されていないことを示すメッセージが表示されます。

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。後ほど、Cisco DNA Center GUI を使用して信頼できる証明書をアップロードするオプションが表示されます。

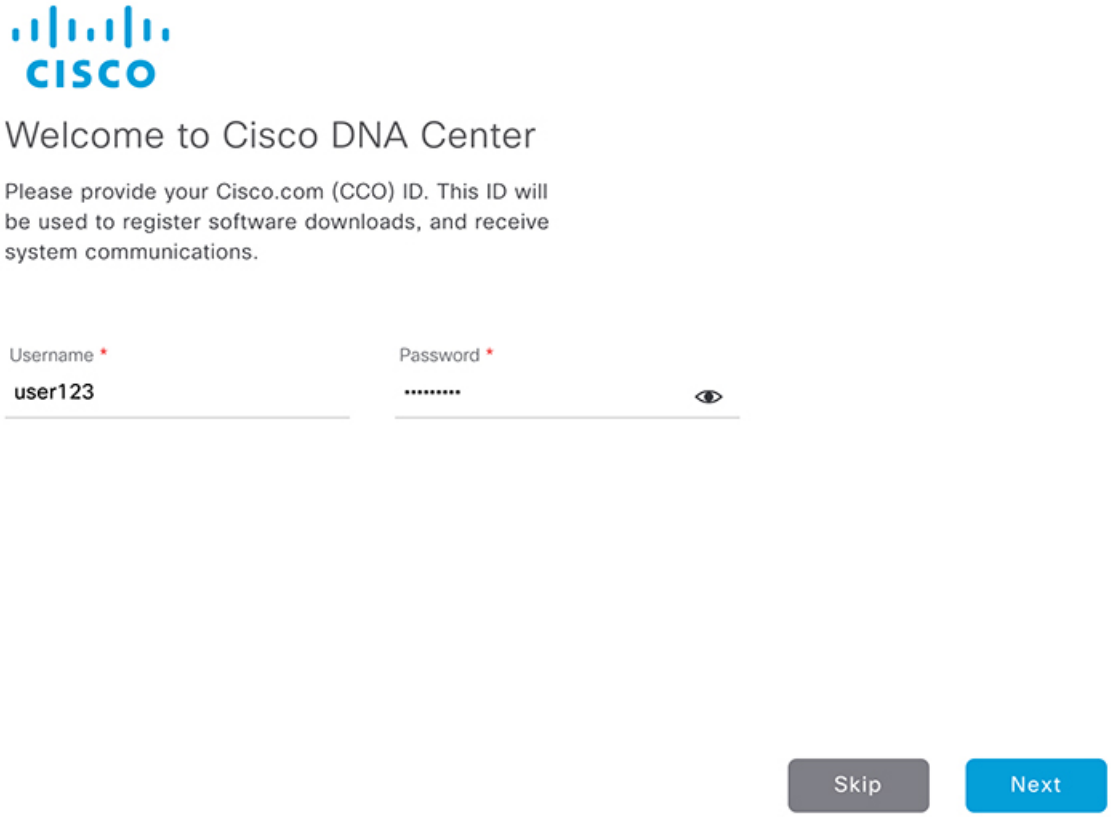
メッセージを無視して、ページの下部にあるリンクをクリックします。[ログイン（Login）]Cisco DNA Center ウィンドウが表示されます。



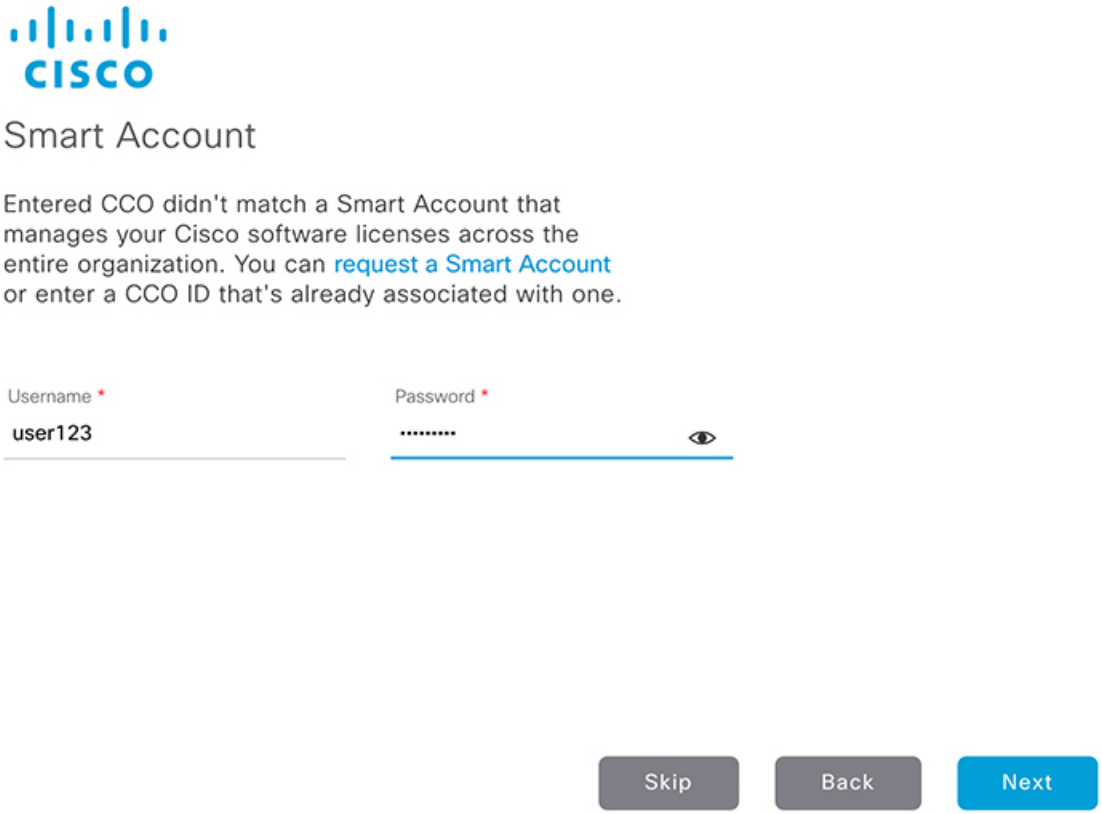
ステップ 5 [ログイン（Login）] ウィンドウで、Cisco DNA Center の設定時に設定した管理者ユーザ名（admin）とパスワードを入力します。入力後、[ログイン（Login）] をクリックします。**[ログインのリセット（Reset Login）]** ウィンドウが表示されます。



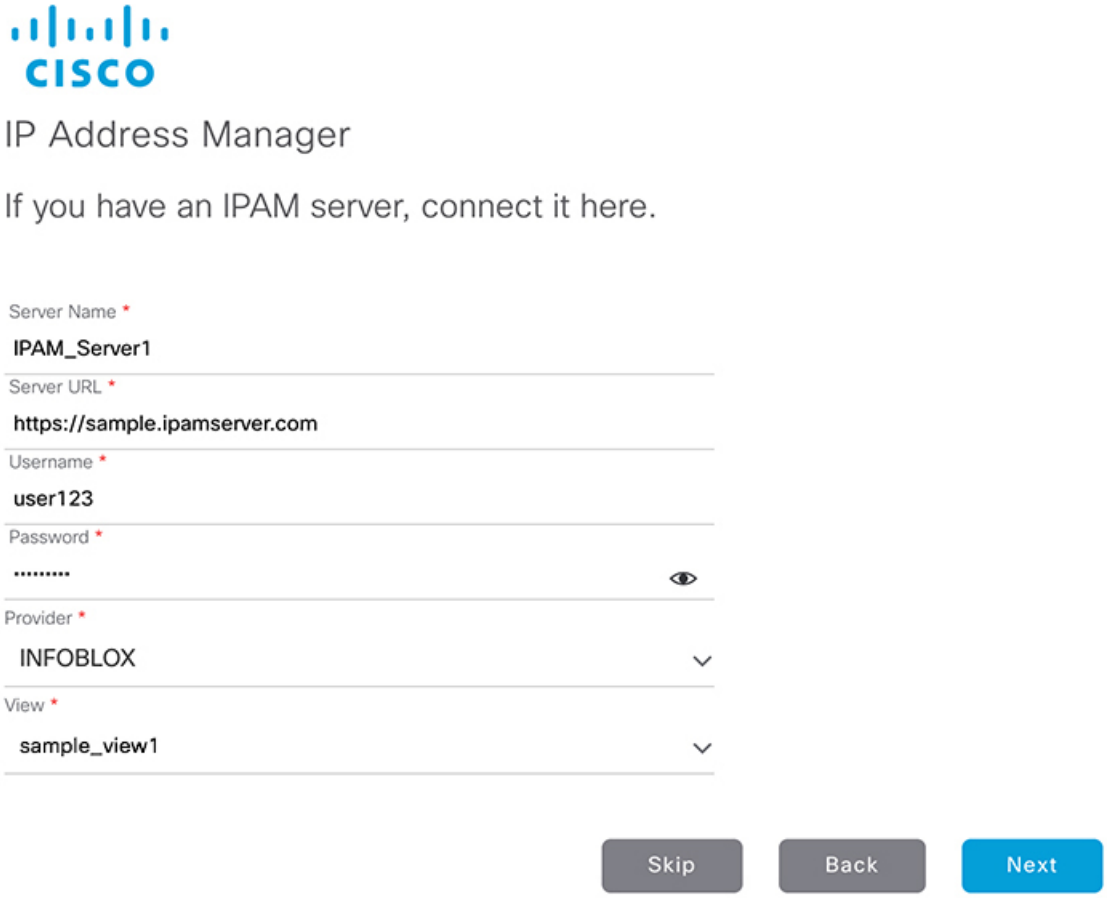
ステップ 6 古いパスワードを入力してから、管理者スーパーユーザの新しいパスワードを入力して確認します。次に、[保存（Save）] をクリックします。**[Cisco.com ID の入力（Enter Cisco.com ID）]** ウィンドウが表示されます。



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 Cisco スマート アカウント ユーザログインと一致しない場合には、**[スマートアカウント（Smart Account）]** ウィンドウが表示されます。



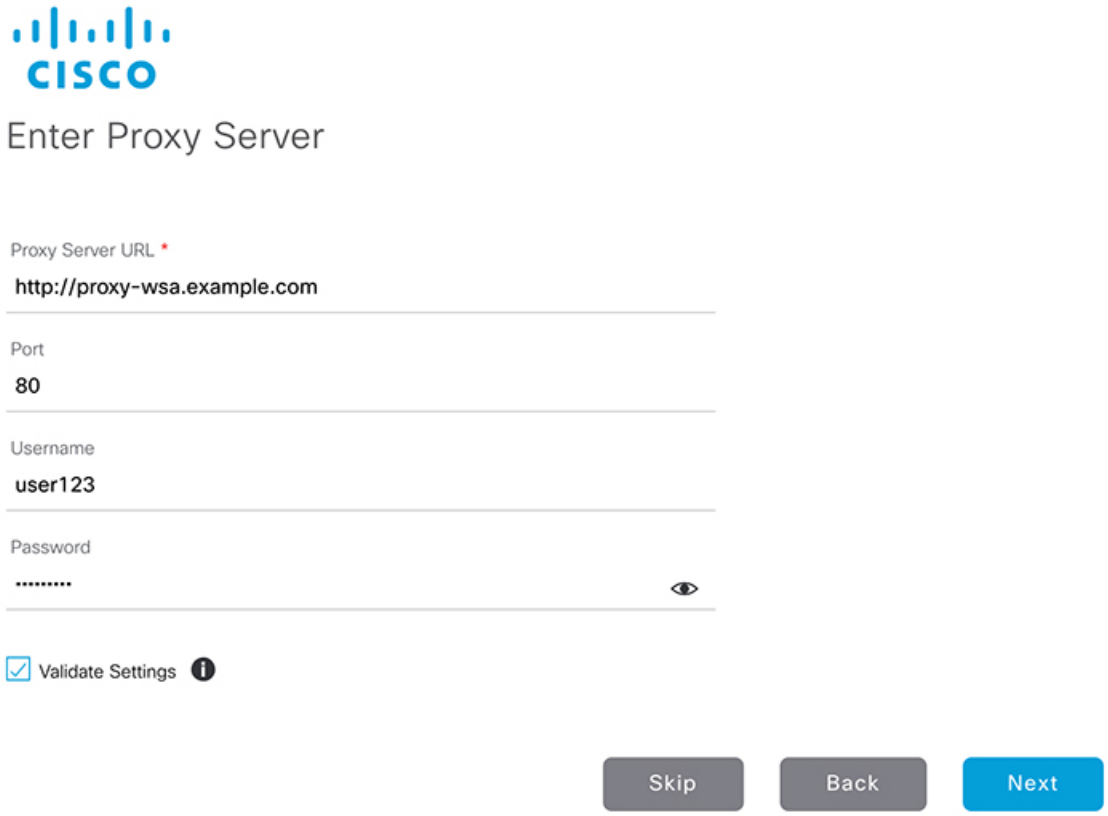
ステップ 8 [スマートアカウント（Smart Account）] ウィンドウが表示された場合には、組織のスマートアカウントのユーザ名とパスワードを入力するか、リンクをクリックして新しいスマートアカウントを開きます。確認したら、[次へ（Next）] をクリックします。**[IP アドレスマネージャ（IP Address Manager）]** ウィンドウが表示されます。



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。

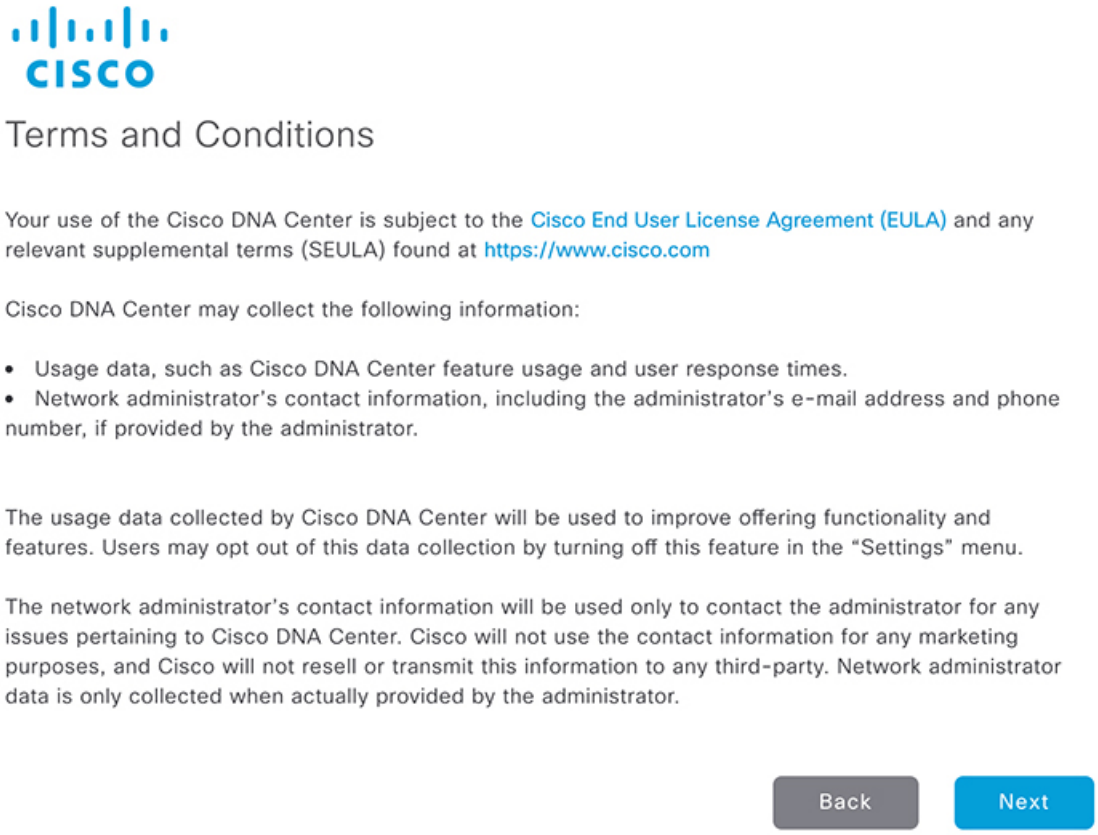
[プロキシサーバの入力（Enter Proxy Server）] ウィンドウが表示されます。



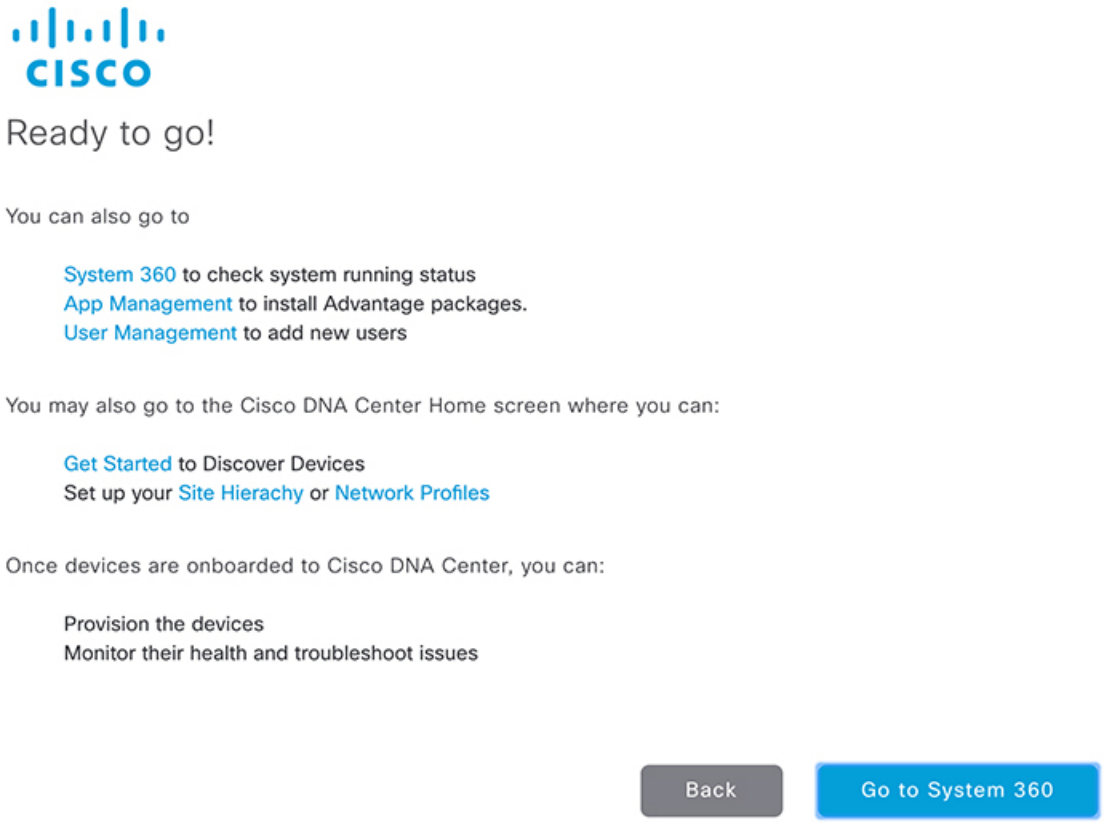
ステップ 10 組織が使用するプロキシサーバ情報を入力します。プロキシサーバに対するログインが必要な場合には、サーバのユーザ名とパスワードを含めます。

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。

確認したら、[次へ （Next）] をクリックします。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後、[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 Cisco DNA Center の統合
- 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 Cisco DNA Center の統合

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 の両方の機能をそれらに適用できます。これは、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。Cisco DNA Center および 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 のログイン情報、Cisco ISE 共有秘密情報など）はすべて、自動的に Cisco 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 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 インストールおよび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 Cisco ISE 展開環境がある場合は、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。

（注） Cisco ISE 2.4 以降では、pxGrid 2.0 および pxGrid 1.0 がサポートされています。pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Cisco DNA Center 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 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、プライマリ PAN で ERS を有効にする必要があります。また、セカンダリ PAN でも ERS を有効にする必要があります。Cisco ISE でプライマリ PAN のフェールオーバーが発生した場合に、セカンダリ PAN で ERS が有効になっていないと、Cisco DNA Center でセカンダリ PAN を使用できません。その結果、Cisco DNA Center と Cisco ISE の間の接続が影響を受けます。

（注） ベストプラクティスは、PAN を介して ERS を使用することです。ただしバックアップの場合は、ポリシーサービスノード（PSN）で ERS を有効化してください。

- 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。
- TrustSec/SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers]** > **[Trustsec]** > **[Trustsec Servers]** > **[Trustsec AAA Servers]** でも定義する必要があります。詳細については、Cisco ISE のご使用のリリースに対応する管理者ワークフローのセグメンテーション ドキュメントを参照してください。

- 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 管理ノード証明書のサブジェクト名またはサブジェクト代替名（SAN）のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Cisco DNA Center システム証明書の 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。

（注） Cisco ISE 2.4 パッチ 13、2.6 パッチ 7、および 2.7 パッチ 3 では、pxGrid 証明書に Cisco ISE のデフォルトの自己署名証明書を使用している場合、証明書が Cisco ISE によって拒否されることがあります。これは、その証明書の古いバージョンに、SSL サーバとして指定された Netscape Cert Type 拡張があるためです。これは、クライアント証明書が必要なため失敗します。

この問題は Cisco ISE 3.0 以降では発生しません。詳細および推奨される回避策については、『Cisco ISE Release Notes』を参照してください。

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 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) **[Administration]** > **[System]** > **[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) [**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 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) [Menu] アイコン（☰）をクリックし、**[System]** > **[System 360]** の順に選択します。

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

d) [Authentication and Policy Servers] ウィンドウで、[Add] をクリックし、ドロップダウンリストから [ISE] を選択します。

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。
- 該当する Cisco ISE 管理ログイン情報を [Username] と [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。
- （任意）Cisco ISE PSN 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**を入力します。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) [追加（Add）] をクリックします。

Cisco ISE との統合を初めて開始したときは、Cisco ISE からの証明書がまだ信頼されていないという通知が表示されます。

- 証明書を表示して詳細を確認できます。
- [Accept] を選択して証明書を信頼し、統合プロセスを続行します。証明書を信頼せずに統合プロセスを終了する場合は、[Decline] を選択します。

統合が正常に完了すると、確認メッセージが表示されます。

統合プロセスで問題が発生した場合は、問題の詳細を示すメッセージが表示されます。編集または再試行が可能な場合はそのオプションが表示されます。

- Cisco ISE 管理ログイン情報が無効であるというエラーメッセージが表示された場合は、[Edit] をクリックし、正しい情報を再入力します。
- 統合プロセスで証明書にエラーが見つかった場合は、Cisco ISE サーバエントリを削除し、証明書の問題が解決した後に統合を最初からやり直す必要があります。

ステップ 3 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確認します。

a) Cisco DNA Center GUI にログインします。
b) [Menu] アイコン（☰）をクリックし、**[System]** > **[System 360]** の順に選択します。
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。

ステップ 4 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 Identity Services Engine (ISE) Deployment] ウィンドウで pxGrid サーバとして表示されている Cisco ISE ノードにログインします。
b) **[Administration]** > **[pxGrid Services]** の順に選択し、[Web Clients] タブをクリックします。

Cisco DNA Center サーバの IP アドレスとともに 2 つの pxGrid クライアントがリストに表示されます。

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 および Cisco ISE が「Cisco ISE と 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 の共有秘密キーを定義することを含まれます。

- 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。

- [Server IP Address]：AAA サーバの IP アドレス。
- [Shared Secret]：デバイス認証のキー。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）] の位置のままにして、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。

- [Cisco ISE]：サーバが Cisco ISE サーバかどうかを示す設定。[Cisco ISE] 設定をクリックして Cisco ISE を有効化します。
- [ユーザ名（Username）]：Cisco ISE コマンドライン インターフェイス（CLI）にログインするために使用する名前。

  （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 サーバの完全修飾ドメイン名（FQDN）。

  （注）
  - Cisco ISE（**[Administration]** > **[Deployment]** > **[Deployment Nodes]** > **[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ることをお勧めします。
  - 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、ホスト名およびドメイン名の 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 サービス登録時の pxGrid クライアントを識別する一意のテキスト文字列（例：`acme`）。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。

- [SSHキー（SSH Key）]：Cisco ISE と接続し、認証するために使用される Diffie-Hellman-Group14-SHA1 SSH キー。
- [仮想IPアドレス（Virtual IP address (es)）]：Cisco ISE ポリシーサービスノード（PSN）の前面にあ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 PSN 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。

ステップ 5 [View Advanced Settings] をクリックして、設定を構成します。

- [プロトコル（Protocol）]：TACACS または RADIUS。

  （注） グレー表示されるオプションは、選択したオプションです（デフォルトでは RADIUS）。TACACS オプションを選択するには、TACACS オプションを選択してから、RADIUS オプションの選択を手動で解除する必要があります。

- [Authentication Port]：AAA サーバへの認証メッセージのリレーに使用されるポート。デフォルト値は UDP ポート 1812 です。
- [Accounting Port]：AAA サーバへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティと請求の目的で使用されます。デフォルトの UDP ポートは 1813 です。
- [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 1 回です。
- [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。

ステップ 6 [Add] 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することができます。

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。

表 *38 : SNMP* のプロパティ

フィールド	説明
Retries	デバイスへ接続可能な試行回数。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）	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。

サービスの再配布

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 Administrator Guide*』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。

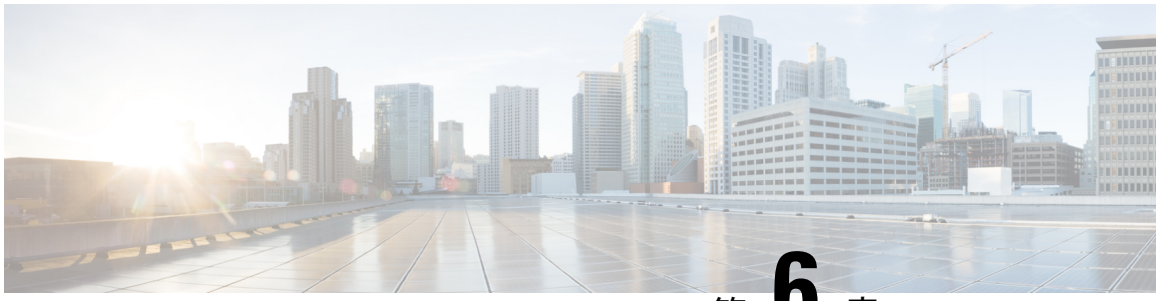
1. ⚙ をクリックして、[システム設定（System Settings）] を選択します。

   [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。



第 6 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。

表 *39* : 基本的なトラブルシューティング タスク

ステップ	説明
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必要がある場合は、「CIMC への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 （120 ページ））。

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-Series Servers Integrated Management Controller CLI Configuration Guide, Release 3.1*』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 Web ベース GUI インターフェイスからログアウトします。

セキュリティ上の理由から、作業セッションの完了時には毎回ログアウトすることを推奨します。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必要がある場合は、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
- 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

ターゲットアプライアンスに現在設定されている Linux ユーザ名（**maglev**）とパスワードが必要になります。

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

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

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

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

ステップ 3 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 4 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 パスワードのプロンプトが表示されたら、再度入力します。

ステップ 5 設定ウィザードには、「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。必要に応じて、表示されている設定を変更します。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 6 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、「設定は成功しました（CONFIGURATION SUCCEEDED）」というメッセージが表示されます。

次のタスク

トピックアプライアンスの電源の入れ直し（120ページ）で説明されているように、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。

（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 の変更が適用されます。

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いずれかの手順を実行して、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 GUI を使用

Cisco IMC GUI からアクセス可能な KVM コンソールを使用して、アプライアンスを停止するか、ウォームリスタートを実行する場合は、この手順で説明するタスクを実行します。

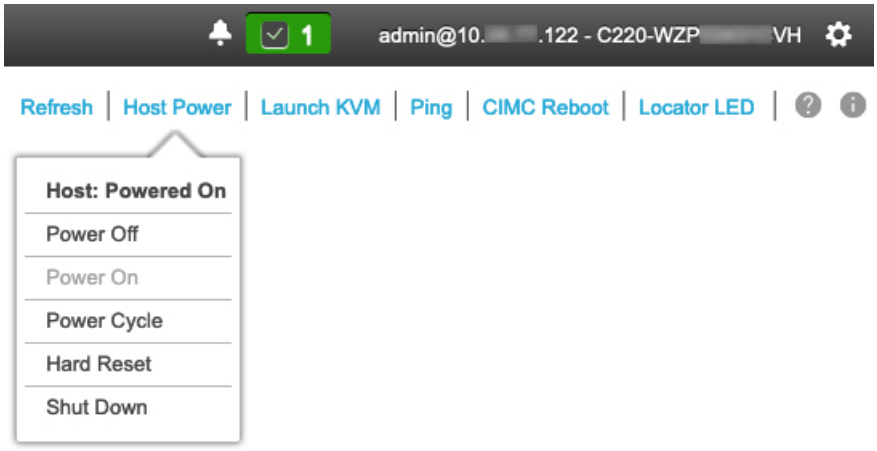
始める前に

Cisco IMC GUI 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ることに注意してください。

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。

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（CIMC へのブラウザアクセスの有効化 （52 ページ）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、ウィンドウ上部のハイパーリンクメニューとともに表示されます。



ステップ 2 KVM が表示されたら、**[Host Power]** > **[Power Cycle]** の順に選択してアプライアンスをリブートします。

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。

SSH を使用

SSH を使用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する場合は、次のタスクを実行します。

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。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。

  エンタープライズポートを特定するには、前面パネルと背面パネル （4 ページ） の背面パネルを参照してください。
- 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 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。