



Cisco DNA Center リリース 2.1.2 第1世代アプライアンス設置ガイド

初版：2020年8月31日

最終更新：2020年3月25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。

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	Cisco DNA Center アプライアンス機能の確認 1
	アプライアンスのハードウェア仕様 1
	前面パネルと背面パネル 2
	物理仕様 11
	環境仕様 11
	電力仕様 12
	10 ギガビット イーサネット スイッチ 13

第 2 章	導入の計画 15
	プランニング ワークフロー 15
	Cisco DNA CenterおよびCisco Software-Defined Access 16
	インターフェイスクーブル接続 16
	必要な IP アドレスおよびサブネット 20
	インターフェイス名とウィザードの設定順序 24
	必要なインターネット URL と完全修飾ドメイン名 26
	インターネットへのアクセスを保護する 28
	必要なネットワークポート 29
	必要なポートとプロトコル： Cisco Software-Defined Access 30
	必須の設定情報 40
	必要な初期設定情報 41

第 3 章	アプライアンスの設置 45
	アプライアンスのインストール ワークフロー 45
	アプライアンスを開梱して点検 45

インストール警告とガイドラインの確認 46

ラック要件の確認 47

アプライアンスの接続および電源投入 47

LED の確認 48

第 4 章

アプライアンスの設定準備 51

アプライアンス設定の準備の概要 51

Cisco Integrated Management Controller に対するブラウザアクセスの有効化 51

事前設定チェックの実行 57

アプライアンスのイメージの再作成 64

 Cisco DNA Center ISO イメージの確認 65

 ブート可能な USB ドライブの作成 66

 Etcher の使用 66

 Linux CLI の使用 67

 Mac CLI の使用 68

 Cisco DNA Center ISO イメージのインストール 68

第 5 章

アプライアンスの設定 71

アプライアンスの設定の概要 71

プライマリノードの設定 72

アドオンノードの設定 89

最新の Cisco DNA Center リリースへのアップグレード 107

第 6 章

初期設定の完了 109

初期設定ワークフロー 109

互換性のあるブラウザ 109

初回ログイン 110

Cisco ISE と Cisco DNA Center の統合 112

 グループベースのアクセスコントロール：ポリシーデータの移行と同期 116

認証サーバとポリシーサーバの設定 119

SNMP プロパティの設定 121

第 7 章**展開のトラブルシューティング 123**

トラブルシューティング タスク 123

ログアウト 123

設定ウィザードを使用したアプライアンスの再設定 124

アプライアンスの電源の入れ直し 126

Cisco IMC GUI を使用 126

SSH を使用 127

付録 A :**ハイ アベイラビリティ クラスターの展開シナリオの確認 129**

新しい HA の展開 129

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 130

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 130

高可用性のアクティブ化 131

HA の展開に関する追加の考慮事項 131

テレメトリ 132

ワイヤレス コントローラ 132



第 1 章

Cisco DNA Center アプライアンス機能の確認

- [アプライアンスのハードウェア仕様 \(1 ページ\)](#)
- [前面パネルと背面パネル \(2 ページ\)](#)
- [物理仕様 \(11 ページ\)](#)
- [環境仕様 \(11 ページ\)](#)
- [電力仕様 \(12 ページ\)](#)
- [10 ギガビットイーサネットスイッチ \(13 ページ\)](#)

アプライアンスのハードウェア仕様

シスコは、ラックマウント可能な物理アプライアンスの形で Cisco Digital Network Architecture (DNA) Center を提供しています。第1世代 Cisco DNA Center アプライアンス (シスコ製品番号 DN1-HW-APL) は、Cisco Unified Computing System (UCS) C220 M4 小型フォームファクタ (SFF) シャーシで構成され、さらに mLOM スロットに仮想インターフェイスカード (VIC) 1227 が追加されています。Cisco DNA Center ソフトウェアイメージは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。

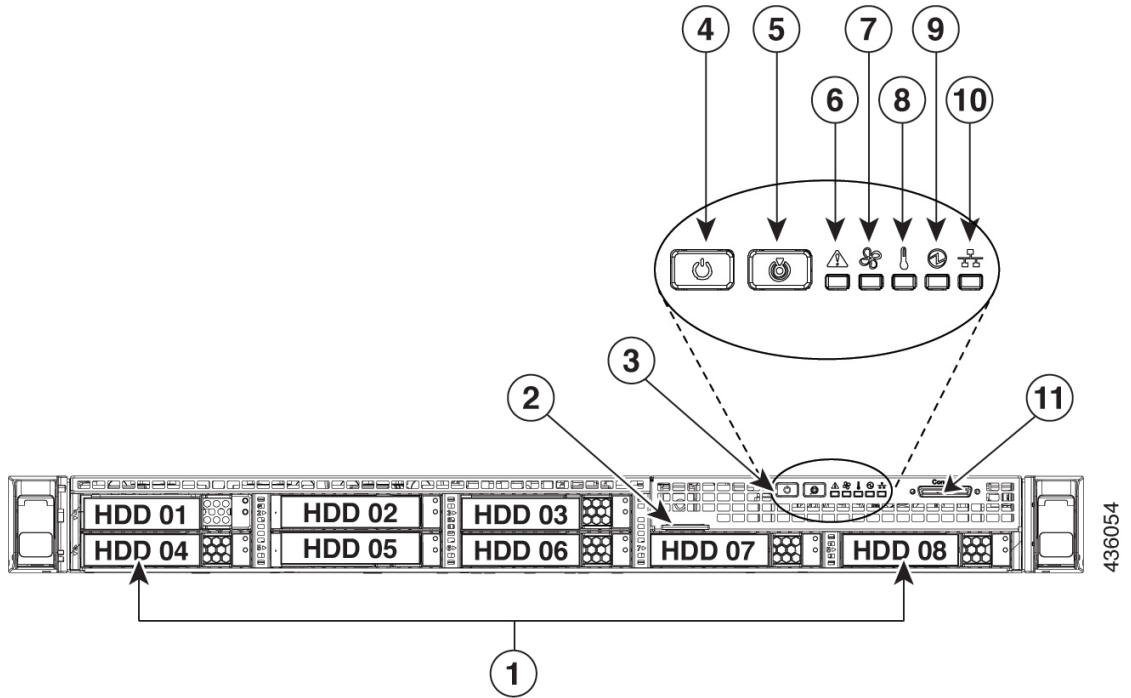
機能	説明
シャーシ	1 ラックユニット (1RU) シャーシ
プロセッサ	22 コア Intel Xeon E5-2699 v4 2.20 GHz プロセッサ X 2
メモリ	32 GB DDR4 2400 MHz の登録済み DIMM (RDIMM) X 8
ストレージ	<ul style="list-style-type: none">• 1.9 TB、2.5 インチ Enterprise Value 6G SATA ソリッドステートドライブ (SSD) X 6• 480 GB、2.5 インチ Enterprise Value 12G SATA SSD X 2

機能	説明
ディスク管理 (RAID)	<ul style="list-style-type: none"> • スロット 1 ~ 4 の RAID 1 • スロット 5 ~ 8 の RAID 10
ネットワークおよび管理 I/O	<p>サポートされるコネクタ：</p> <ul style="list-style-type: none"> • Cisco UCS VIC 1227 上の 10 Gbps イーサネットポート X 2 • 1 Gbps イーサネット専用管理ポート X 1 • 1 Gbps BASE-T イーサネット LAN ポート X 2 <p>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。</p> <ul style="list-style-type: none"> • RS-232 シリアルポート (RJ-45 コネクタ) X 1 • 15 ピン VGA2 コネクタ X 1 • USB 3.0 コネクタ X 2 • USB 2.0 2 個、VGA 1 個、シリアル (DB-9) 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
電源	<ul style="list-style-type: none"> • 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 6
ビデオ	60 Hz で最大 1920 X 1200、16 bpp のビデオグラフィックアレイ (VGA) ビデオ解像度、最大 256 MB のビデオメモリ

前面パネルと背面パネル

次の図と表では、44 コアの 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

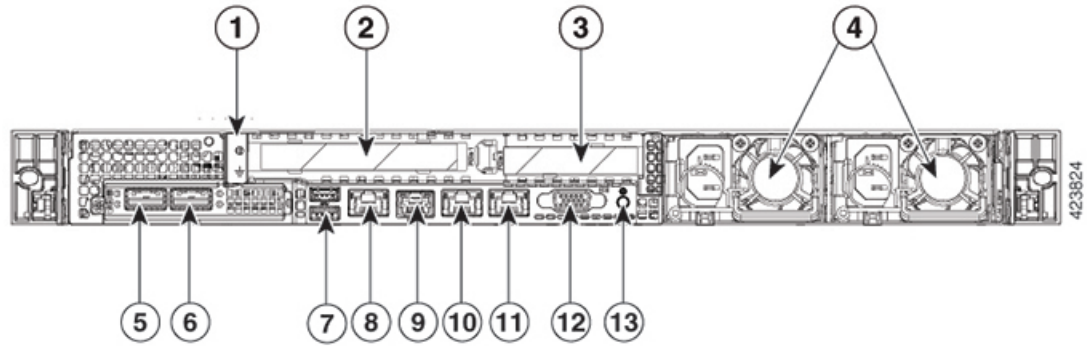


コンポーネント	説明
1	<p>このアプライアンスでは、次のように合計 8 個のドライブを使用できます。</p> <ul style="list-style-type: none"> • 1.9 TB SATA SSD X 6 • 480 GB SAS SSD X 2 <p>取り付けられたドライブにはそれぞれ、障害 LED とアクティビティ LED が付いています。</p> <p>ドライブ障害 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：ドライブは正常に動作中です。 • オレンジ：ドライブに障害が発生しています。 • オレンジの点滅：ドライブの再構成中です。 <p>ドライブアクティビティ LED の状態とその説明：</p> <ul style="list-style-type: none"> • 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	引き抜きアセットタグ

コンポーネント	説明
3	操作サブパネルのボタンおよび LED これらのボタンの LED の状態と、示されている条件については、次のエントリで説明します。
4	<p>電源ボタン/電源ステータス LED LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：アプライアンスに AC 電力が供給されていません。 • オレンジ：アプライアンスはスタンバイ電源モードです。Cisco Integrated Management Controller (CIMC) と一部のマザーボード機能にだけ電力が供給されています。 • 緑：アプライアンスはメイン電源モードです。すべてのサーバコンポーネントに電力が供給されています。
5	<p>ユニット識別ボタンと LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 青：ユニット識別 LED 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。
6	<p>システムステータス LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 緑：アプライアンスは正常動作状態で稼働しています。 • 緑の点滅：アプライアンスはシステムの初期化とメモリチェックを行っています。 • オレンジの点灯：アプライアンスは縮退運転状態になっています。次の 1 つ以上が原因の可能性があります。 <ul style="list-style-type: none"> • 電源装置の冗長性が失われている。 • CPU が一致しない。 • 少なくとも 1 つの CPU に障害が発生している。 • 少なくとも 1 つの DIMM に障害が発生している。 • RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 • オレンジの点滅：アプライアンスは重大な障害が発生している状態であり、次の 1 つ以上が原因である可能性があります。 <ul style="list-style-type: none"> • ブートに失敗した。 • 修復不能な CPU またはバスエラーが検出された。 • サーバが過熱状態にある。

コンポーネント	説明
7	<p>ファンステータス LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 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。
8	<p>温度ステータス LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 緑：アプライアンスは正常温度で稼働中です。 • オレンジの点灯：1つ以上の温度センサが警告しきい値を超過しています。 • オレンジの点滅：1つ以上の温度センサが重大しきい値を超過しています。
9	<p>電源装置ステータス LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 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。
10	<p>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：</p> <ul style="list-style-type: none"> • 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。
11	<p>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。</p>

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	アース ラグの穴 (DC 電源装置の場合)
2	PCIe ライザー 1/スロット 1
3	PCIe ライザー 2/スロット 2
4	<p>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。</p> <p>障害 LED の状態とその説明：</p> <ul style="list-style-type: none"> 消灯：電源装置は正常に動作中です。 オレンジの点滅：イベント警告しきい値に達しましたが、電源装置は動作し続けています。 オレンジの点灯：重大障害しきい値に達し、電源装置がシャットダウンしています (ファンの障害や過熱状態など)。 <p>AC 電源 LED の状態とその説明：</p> <ul style="list-style-type: none"> 緑の点灯：AC 電力供給も、DC 出力も OK です。 緑の点滅：AC 電力供給は OK ですが、DC 出力は使用できません。 消灯：電源に AC 電力が供給されていません。 <p>詳細については「電力仕様」を参照してください。</p>

コンポーネント	説明
5	<p>10 Gbps クラスタポート（ポート 2、enp10s0、ネットワークアダプタ 1）：これは、アプライアンスの mLOM スロットの Cisco Virtual Interface Card (VIC) 1227 の 2 番目の 10 Gbps ポートです。背面パネルにはポート 2 というラベルが付いていて、Maglev 設定ウィザードはそれを enp10s0 およびネットワークアダプタ 1 として識別します。このポートを Cisco DNA Center クラスタ内の他のノードに接続しているスイッチに接続します。</p> <p>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。</p> <p>リンクステータス LED の状態とその説明：</p> <ul style="list-style-type: none">• 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。 <p>リンク速度 LED の状態とその説明：</p> <ul style="list-style-type: none">• 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。 <p>(注) エンタープライズポートとクラスタポートは、10 Gbps でのみ動作する必要があります。</p>

コンポーネント	説明
6	<p>10 Gbps エンタープライズポート（ポート 1、enp9s0、ネットワークアダプタ 1）：これは、アプライアンスの mLOM スロットの Cisco Virtual Interface Card (VIC) 1227 の最初の 10 Gbps ポートです。背面パネルにはポート 1 とラベルが付いていて、Maglev 設定ウィザードはそれを enp9s0 およびネットワークアダプタ 4 として識別します。このポートを、Cisco DNA Center の管理対象のネットワーク機器への IP 到達可能性があるスイッチに接続します。</p> <p>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。</p> <p>リンクステータス LED の状態とその説明：</p> <ul style="list-style-type: none"> • 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。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 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。 <p>(注) Cisco DNA Center アプライアンスのエンタープライズポートとクラスタポートは、10 Gbps でのみ動作する必要があります。</p>
7	USB 3.0 ポート X 2

コンポーネント	説明
8	<p>1 Gbps CIMC ポート (M) : これは、2つの USB 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。背面パネルには M というラベルが付いていて、アプライアンスの CIMC GUI へのブラウザアクセスを有効にすると、IP アドレスが割り当てられます (「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照)。このポートは、Cisco DNA Center 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 (OOB) 管理用に予約されています。このポートは、専用の OOB エンタープライズ管理ネットワークにアクセスできるスイッチに接続します。</p> <p>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 :</p> <ul style="list-style-type: none"> • 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。 <p>速度 LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 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。
9	シリアル ポート (RJ-45 コネクタ)

コンポーネント	説明
10	<p>1 Gbps Cisco DNA Center GUI ポート (1、enp1s0f0、ネットワークアダプタ 2) : これは、最初の Intel i350 1g GB イーサネット コントローラ ポートです。アプライアンスのマザーボードに組み込まれています。背面パネルには 1 というラベルが付いていて、Maglev 設定ウィザードはそれを enp1s0f0 とネットワークアダプタ 2 として識別します。このポートは、専用のエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。</p> <p>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 :</p> <ul style="list-style-type: none"> • 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。 <p>速度 LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 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。
11	<p>1 Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ 3) : これは 2 番目の組み込み 1 Gbps イーサネット コントローラ ポートです。背面パネルには 2 というラベルが付いていて、Maglev 設定ウィザードはそれを enp1s0f1 とネットワークアダプタ 3 として識別します。このポートはオプションです。インターネット接続が 10 Gbps エンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ 4) 経由では実行できない場合に使用されます。</p> <p>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 :</p> <ul style="list-style-type: none"> • 緑の点滅 : アクティブなリンクにトラフィックが存在します。 • 緑 : リンクはアクティブですが、トラフィックはありません。 • 消灯 : リンクが確立されていません。 <p>速度 LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 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。
12	VGA ビデオポート (DB-15) 。このポートの周囲のパネル領域は青色です。

コンポーネント	説明
13	青色 LED ロケータボタン

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 1: 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)
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)	37.9 ポンド (17.2 キロ)

環境仕様

次の表に Cisco DNA Center アプライアンスの環境仕様を示します。

表 2: 環境仕様

説明	仕様
動作時温度	41 ~ 95 °F (5 ~ 35 °C) 海拔 305 m (1000 フィート) ごとに最高温度 が 1°C 低下します。

説明	仕様
非動作時温度（アプライアンスが倉庫にあるか運送中の場合）	-40 ~ 149 °F (-40 ~ 65 °C)
湿度（RH）（動作時）	10 ~ 90%（28°C（82°F）時、結露なし）
湿度、非動作時	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	5.4
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	37

電力仕様

次の表に、Cisco DNA Center アプライアンスに同梱されている 2 つの 770 W AC 電源（シスコ部品番号 UCSC-PSU1-770W）の仕様を示します。

表 3: 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 @ 100 ~ 120 VAC
最大突入電流	35°C で 15 A
最大保留時間	12 ms @ 770 W
電源装置の出力電圧	12 VDC

説明	仕様
電源装置のスタンバイ電圧	12 VDC
効率評価	Climate Savers Platinum Efficiency (80 Plus Platinum 認証済み)
フォームファクタ	RSP2
入力コネクタ	IEC320 C14



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

10 ギガビットイーサネットスイッチ

次の表に、現時点で第 1 世代 Cisco DNA Center アプライアンスから起動できる 10 ギガビットイーサネット Cisco スイッチを一覧表示します。この表は、テスト対象のスイッチが増えると更新されます。

Cisco スイッチ	シスコの部品番号	コメント
Cisco Nexus 5672UP	N5K-C5672UP	—
Cisco Catalyst 6880-X	C6880-X-LE	—
Cisco Nexus 7700 (6 スロット)	N77-C7706	Cisco Nexus 7700 スイッチ Supervisor2 拡張モジュール (シスコ製品番号 N77-SUP2E) を設置してテスト済み。
<p>この表の残りのスイッチが正しく機能するためには、スイッチと Cisco DNA Center アプライアンスの両方で次の設定を構成します。</p> <ul style="list-style-type: none"> • [Default VLAN] : アプライアンスとスイッチに同じポート番号を指定します。 • [VLAN Mode] : [Trunk] モードを設定します。 <p>事前設定チェックの実行 (57 ページ) のステップ 3 と 4 を参照してください。</p>		
Cisco Catalyst 3850-48XS-S	WS-C3850-48XS-S	—
Cisco Catalyst 4500X-32 SFP+	WS-C4500X-32SFP+	—
Cisco Catalyst C9500-40X-E	C9500-40X	—

10 ギガビットイーサネットスイッチ

Cisco スイッチ	シスコの部品番号	コメント
Cisco Catalyst 3650-48PQ-E	WS-C3650-48PQ-E	—



第 2 章

導入の計画

- [プランニング ワークフロー](#) (15 ページ)
- [Cisco DNA Center および Cisco Software-Defined Access](#) (16 ページ)
- [インターフェイスクーブル接続](#) (16 ページ)
- [必要な IP アドレス および サブネット](#) (20 ページ)
- [必要なインターネット URL と完全修飾ドメイン名](#) (26 ページ)
- [インターネットへのアクセスを保護する](#) (28 ページ)
- [必要なネットワークポート](#) (29 ページ)
- [必要なポートとプロトコル： Cisco Software-Defined Access](#) (30 ページ)
- [必須の設定情報](#) (40 ページ)
- [必要な初期設定情報](#) (41 ページ)

プランニング ワークフロー

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

1. スタンドアロン設置とクラスタ設置で推奨されるケーブル接続とスイッチングの要件を確認します。詳細については「[インターフェイスクーブル接続](#)」を参照してください。
2. アプライアンスの設定時に適用する IP アドレッシング、サブネット化などの IP トラフィック情報を収集します。詳細については「[必要な IP アドレス および サブネット](#)」を参照してください。
3. 必要な Web ベースのリソースに対するアクセスのソリューションを準備します。詳細については「[必要なインターネット URL と完全修飾ドメイン名](#)」と「[インターネットへのアクセスを保護する](#)」を参照してください。
4. Cisco DNA Center トラフィックのファイアウォールとセキュリティポリシーを再設定します。詳細については「[必要なネットワークポート](#)」を参照してください。Cisco DNA Center を使用して Cisco Software-Defined Access (SD-Access) ネットワークを管理している場合は「[必要なポートとプロトコル： Cisco Software-Defined Access](#)」も参照してください。

5. アプライアンスの構成時と初回設定時に使用される追加情報を収集します。詳細については「[必須の設定情報](#)」と「[必要な初期設定情報](#)」を参照してください。

Cisco DNA CenterおよびCisco 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。

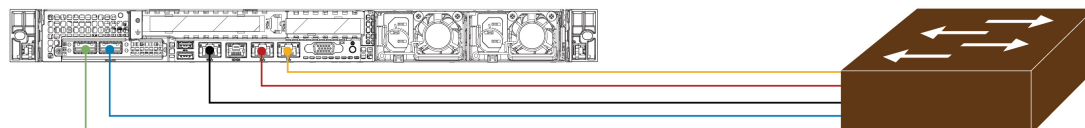


- (注)
- アプライアンス設定中、Maglev設定ウィザードは、**クラスタリンク**オプションをインターフェイスに割り当てるまで続行できません。実稼働環境で単一ノードを展開する場合も3ノードを展開する場合も、ポート **enp10so** を第1世代 Cisco DNA Center アプライアンス (シスコ製品番号 DN1-HW-APL) のクラスタリンクとして指定します。
 - クラスタリンクとしてマークされたインターフェイスは、設定が完了した後は変更できないことに注意してください。後で、クラスタリンクとしてマークされたインターフェイスを変更する必要がある場合は、アプライアンスのイメージを作成しなおす必要があります。Cisco DNA Center アプライアンスのイメージを作成し直すために完了する必要があるタスクの説明については、[アプライアンスのイメージの再作成 \(64 ページ\)](#) を参照してください。将来的に3ノードクラスタに拡張できるようにするため、IPアドレスを使用してクラスタポートを設定するようお勧めします。また、クラスタリンクインターフェイスがスイッチポートに接続されており、稼働状態になっていることを確認します。
 - 複数のクラスタを構築する場合は、クラスタ間の相互作用 (クラスタが破損する可能性がある) を防ぐために、クラスタごとに個別の IP スキームを使用する必要があります。
-
- **(必須) 10 Gbps クラスタポート (ポート 2、enp10so、ネットワークアダプタ 1)** : これは、アプライアンスの mLOM スロットの VIC 1227 カードの左側のポートです。その目的は、Cisco DNA Center 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接続し、ポートのサブネットマスクを使用して IP アドレスを1つ設定します。
 - **(オプション) 1 Gbps Cisco DNA Center GUI ポート (1、enp1s0f0、ネットワークアダプタ 2)** : このポートは、Cisco DNA Center GUI へのアクセスを提供します。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。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用して IP アドレスを1つ設定します。
 - **(オプション) 1 Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ 3)** : このポートはオプションです。10 Gbps のエンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ 4) 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のみ使用してください。クラウドポートを使用する必要がある場合は、インターネットプロキシサーバに接続しているスイッチに接続し、ポートのサブネットマスクを使用して IP アドレスを設定します。
 - **(必須) 10 Gbps エンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ 4)** : これは、アプライアンス mLOM スロットの VIC 1227 カードの右側のポートです。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、ただし強く推奨) 1 Gbps CIMC ポート (M)** : このポートで、Cisco Integrated Management Controller (CIMC) アウトオブバンドアプライアンス管理インターフェイスとその GUI にブラウザがアクセスします。その目的は、アプライアンスとその

ハードウェアを管理できるようにすることです。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

次の図は、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



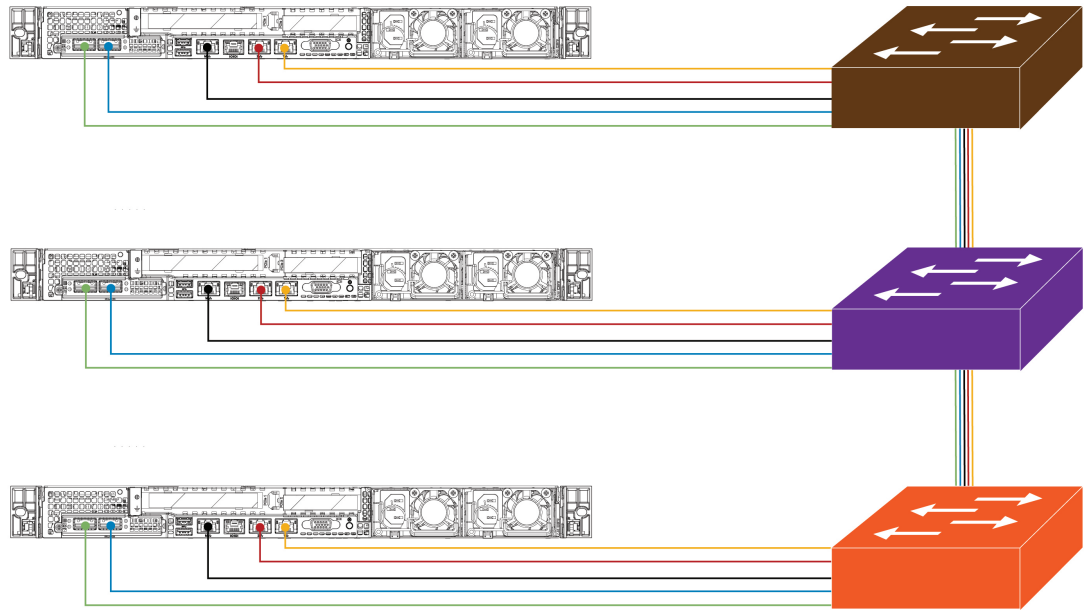
Legend

- 10 Gbps Cluster Port
(Port 2, enp10s0, Network Adapter 1)
- 10 Gbps Enterprise Port
(Port 1, enp9s0, Network Adapter 4)
- 1 Gbps CIMC Port (M)
- 1 Gbps Cisco DNA Center GUI Port
(1, enp1s0f0, Network Adapter 2)
- 1 Gbps Cloud Port
(2, enp1s0f1, Network Adapter 3)

439871

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（ポート 2、enp10so、ネットワークアダプタ 1）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 ノードクラスターの推奨される配線



Legend

- 10 Gbps Cluster Port
(Port 2, enp10s0, Network Adapter 1)
- 10 Gbps Enterprise Port
(Port 1, enp9s0, Network Adapter 4)
- 1 Gbps CIMC Port (M)
- 1 Gbps Cisco DNA Center GUI Port
(1, enp1s0f0, Network Adapter 2)
- 1 Gbps Cloud Port
(2, enp1s0f1, Network Adapter 3)

439812

背面パネルのポートとその使用方法についての短いビデオプレゼンテーションは、「[アシュアランスと SD-Access のための Cisco DNA Center アプライアンスの開梱](#)」の最初の 5 分間（「はじめに」の項）を参照してください。

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

10 Gbps のエンタープライズポートとクラスターポートを接続する場合は、両方の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-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必要とされ、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VIPアドレスもダウンします。これが発生すると、クラスタ内リンクが復元されるまで Cisco DNA Center を使用できません (ソフトウェアイメージ管理 [SWIM] と Cisco Identity Services Engine [ISE] の統合が動作しません。またネットワーク データ プラットフォーム [NDP] コレクタから情報を収集できないため、Cisco DNA アシユアランスデータが表示されません)。
 - リンクローカルIPアドレスをホストインターフェイスに使用することはできません。
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る必要があります。Cisco DNA Center の展開時に留意すべきセキュリティ上の考慮事項については、『[Cisco Digital Network Architecture Center Security Best Practices Guide](#)』を参照してください。
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、DNSサーバのIPアドレス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、複数の値を指定できます。
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、IProute 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、NTP サーバの IP アドレス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、複数の値を指定できます。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. **コンテナサブネット (Container Subnet)** : アシユアランス、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。デフォルトでは、Cisco DNA Center によりリンクローカルサブネット (**169.254.32.0/20**) がこのパラメータに設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、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、重複したりしていないことを確認してください。また、サブネットの最小サイズが 21 ビットであることを確認してください。指定するサブネットは、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『[プライベートインターネット用のアドレス割り当て](#)』を、RFC 6598 では『[IANA-Reserved IPv4 Prefix For Shared Address Space](#)』を参照してください。

**重要**

- 有効な CIDR サブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20 および 172.17.61.0/20 サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了したら、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません (詳細については、「アプライアンスの設定」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. **クラスタサブネット (Cluster 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。デフォルトでは、Cisco DNA Center によりリンクローカルサブネット (**169.254.48.0/20**) がこのパラメータに設定されています。

このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、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、重複したりしていないことを確認してください。また、サブネットの最小サイズが 21 ビットであることを確認してください。指定するサブネットは、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『[プライベートインターネット用のアドレス割り当て](#)』を、RFC 6598 では『[IANA-Reserved IPv4 Prefix For Shared Address Space](#)』を参照してください。

コンテナサブネットとして 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 のクラスタサブネットを指定することもできます。また、設定ウィザードによって、これらのサブネット間の重複（存在する場合）が検出され、重複を修正するように求められることにも注意してください。

**重要**

- 有効な CIDR サブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20 および 172.17.61.0/20 サブネットに誤ったビットが表示されます。
- Cisco DNA Center アプライアンスの設定が完了したら、最初にアプライアンスを再イメージ化せず、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）。

コンテナとクラスタの 2 つのサブネットが推奨される合計 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 encaps/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 余りサポートしており、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ため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。クラウドスペースは、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 アドレス範囲が 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 アドレス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 プロモーションアプライアンス : DN2-HW-APL-U
 - 56 コアアプライアンス : DN2-HW-APL-L
 - 56 コア プロモーションアプライアンス : DN2-HW-APL-L-U
 - 112 コアアプライアンス : DN2-HW-APL-XL
 - 112 コア プロモーションアプライアンス : DN2-HW-APL-XL-U

表 4: 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
クラスタ (Cluster) : アプライアンスをクラスタノードにリンクします。	第 1 世代	enp10s0	ネットワークアダプタ #1
	第 2 世代	<ul style="list-style-type: none"> • 44 および 56 コアアプライアンス : enp94s0f1 • 112 コアアプライアンス : enp69s0f1 	ネットワークアダプタ #4
管理 (Management) : 管理ネットワークから Cisco DNA Center GUI にアクセスできます。	第 1 世代	enp1s0f0	ネットワークアダプタ #2
	第 2 世代	<ul style="list-style-type: none"> • 44 および 56 コアアプライアンス : eno1 • 112 コアアプライアンス : enp53s0f0 	ネットワークアダプタ #1
クラウド (Cloud) : この目的で別のインターフェイスを使用できない場合にインターネットアクセスを提供します。	第 1 世代	enp1s0f1	ネットワークアダプタ #3
	第 2 世代	<ul style="list-style-type: none"> • 44 および 56 コアアプライアンス : eno2 • 112 コアアプライアンス : enp53s0f1 	ネットワークアダプタ #2
エンタープライズ (Enterprise) : アプライアンスをエンタープライズネットワークにリンクします。	第 1 世代	enp9s0	ネットワークアダプタ #4
	第 2 世代	<ul style="list-style-type: none"> • 44 および 56 コアアプライアンス : enp94s0f0 • 112 コアアプライアンス : enp69s0f0 	ネットワークアダプタ #3

必要なインターネット URL と完全修飾ドメイン名

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

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

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

表 5: 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フィードバックを送信	<p>推奨 : *.ciscoconnectdna.com:443¹</p> <p>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。</p> <ul style="list-style-type: none"> • https://www.ciscoconnectdna.com • https://cdn.ciscoconnectdna.com • https://registry.ciscoconnectdna.com • https://registry-cdn.ciscoconnectdna.com
Cisco DNA Center アップデートパッケージ	<ul style="list-style-type: none"> • https://*.ciscoconnectdna.com/ • *.cloudfront.net • *.tesseractcloud.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	<ul style="list-style-type: none"> • https://apx.cisco.com • https://cloudsso.cisco.com/as/token.oauth2 • https://*.cisco.com/
クラウドドメインでの認証	https://dnaservices.cisco.com
ユーザフィードバック	https://dnacenter.uservoice.com

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco Meraki との統合	<p>推奨 : *.meraki.com:443</p> <p>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。</p> <ul style="list-style-type: none"> • dashboard.meraki.com:443 • api.meraki.com:443 • n63.meraki.com : 443
OCSP/CRL を使用した SSL/TLS 証明書の失効ステータスの確認	<ul style="list-style-type: none"> • http://ocsp.quovadisglobal.com • http://crl.quovadisglobal.com/* • http://*.identrust.com <p>(注) これらの URL では、Cisco DNA Center に設定されているプロキシサーバーは使用されません。Cisco DNA Center が各 URL に直接アクセスできることを確認します。</p>
cisco.com とシスコ スマート ライセンスとの統合	<p>*.cisco.com : 443</p> <p>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。</p> <ul style="list-style-type: none"> • software.cisco.com • cloudsso.cisco.com • cloudsso1.cisco.com • cloudsso2.cisco.com • apiconsole.cisco.com • api.cisco.com • apx.cisco.com • sso.cisco.com • apmx-prod1-vip.cisco.com • apmx-prod2-vip.cisco.com • tools.cisco.com • tools1.cisco.com • tools2.cisco.com • smartreceiver.cisco.com

目的	..Cisco DNA Center がアクセスする必要がある URL と FQDN
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	<ul style="list-style-type: none"> • www.mapbox.com • *.tiles.mapbox.com/*: 443 プロキシの場合、宛先は *.tiles.mapbox.com/* です。
Cisco AI Network Analytics のデータ収集では、クラウドホストへのアウトバウンド HTTPS (TCP 443) アクセスを許可するようにネットワークまたは HTTP プロキシを設定	<ul style="list-style-type: none"> • https://api.use1.prd.kairos.ciscolabs.com (米国東部リージョン) • https://api.eu1.prd.kairos.ciscolabs.com (欧州中央リージョン)
GUI から特定のタスクを完了できる対話型ヘルプフローのメニューにアクセス	https://ec.walkme.com

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

インターネットへのアクセスを保護する

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

HTTPS プロキシサーバを使用することは、リモート URL に安全にアクセスするための信頼性の高い方法です。「[必要なインターネット URL と完全修飾ドメイン名](#)」に記載されている URL にアプライアンスがアクセスするために必要なアクセス権を付与するには、HTTPS プロキシサーバを使用するようお勧めします。アプライアンス設置時に、この目的で使用するプロキシサーバの URL とポート番号を、プロキシのログインクレデンシャルとともに入力するように求められます (プロキシが必要な場合)。

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

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

必要なネットワークポート

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

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



- (注) Cisco DNA Center の展開時に留意すべきセキュリティ上の考慮事項については、『[Cisco Digital Network Architecture Center セキュリティ ベスト プラクティス ガイド](#)』を参照してください。

表 6: 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)
22	SSH	[TCP]
67	BOOTP	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
514	Syslog	UDP
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]
9991	マルチキャストドメインネームシステム (mDNS)	TCP
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 7: 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	<p>ポート 80 は発信プロキシ設定に使用できます。</p> <p>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)、ほかの一般的なポート (8080 など) も使用できます。</p> <p>シスコのサポートする証明書プールとトラストプールにアクセスするには、アプライアンスから次のリストに記載されたシスコのアドレスに対する発信 IP トラフィックを許可するようにネットワークを設定します。</p> <p>https://www.cisco.com/security/pki/</p>	TCP
123	NTP	UDP
161	SNMP エージェント	UDP
443	HTTPS	TCP
5222、8910	Cisco ISE XMP (PxGrid 用)	TCP
9060	Cisco ISE ERS API トラフィック	TCP

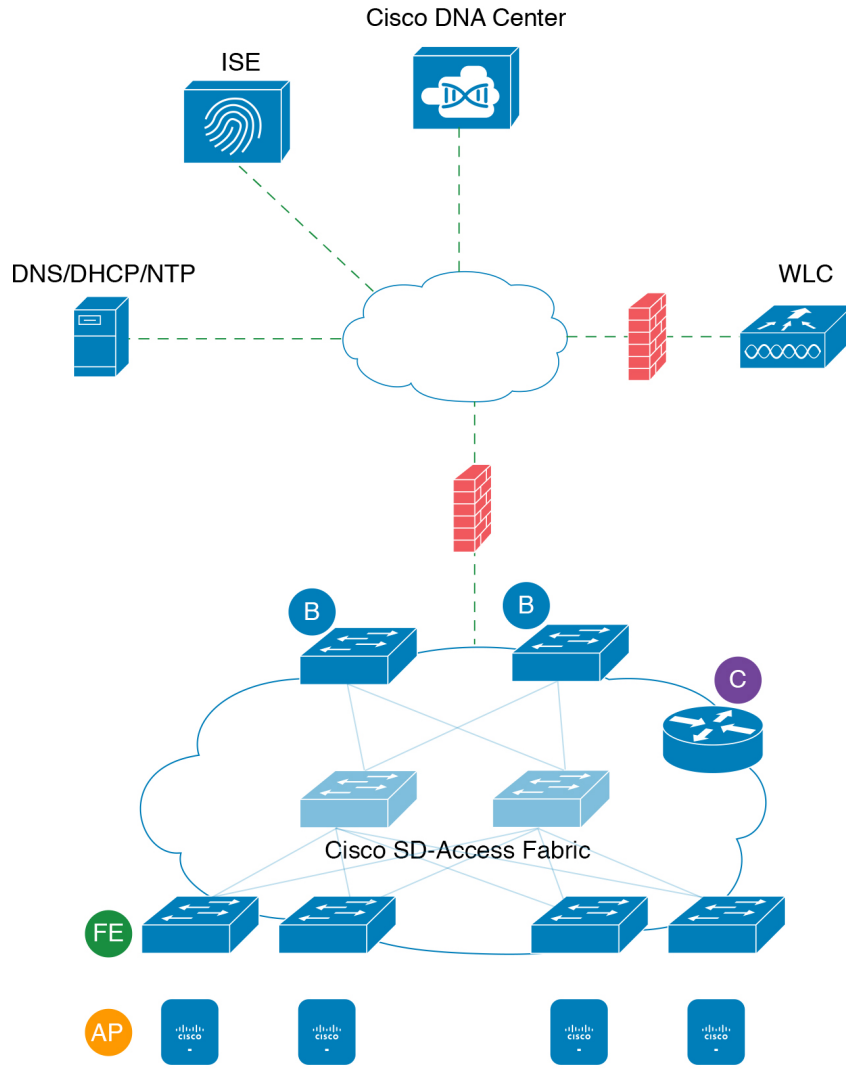


- (注) ほかにアプライアンスからシスコのアドレス (<https://www.cisco.com/security/pki/>) に対する発信 IP トラフィックを許可するようネットワークを設定する方法があります。アプライアンスからシスコがサポートする証明書およびトラストプールにアクセスするには、上述の URL に記載されている IP アドレスを使用します。

必要なポートとプロトコル : Cisco Software-Defined Access

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

図 5 : Cisco SD-Access ファブリック インフラストラクチャ



355637

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

表 8 : 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
いずれか (Any)	Cisco DNA Center	UDP 53	DNS Server	Cisco DNA Center から DNS サーバの間で使用

いずれか (Any)	Cisco DNA Center	TCP 22	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間でSSH に使用
いずれか (Any)	Cisco DNA Center	TCP 23	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間でTelnet に使用
いずれか (Any)	Cisco DNA Center	UDP 161	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間でSNMP デバイス検出に使用
ICMP	Cisco DNA Center	ICMP	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチのループバックの間でSNMP デバイス検出に使用
いずれか (Any)	Cisco DNA Center	TCP 443	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間でソフトウェアアップグレードに使用 (プロキシがない場合はインターネットの間でも使用)
いずれか (Any)	Cisco DNA Center	UDP 6007	スイッチとルータ	Cisco DNA Center からスイッチおよびルータの間でNetFlow に使用
いずれか (Any)	Cisco DNA Center	TCP 830	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間でNETCONF に使用 (Cisco SD-Access 組み込みワイヤレス)
UDP 123	Cisco DNA Center	UDP 123	ファブリックアンダーレイ	Cisco DNA Center からファブリックスイッチの間でLAN 自動化中の初回期間に使用
いずれか (Any)	Cisco DNA Center	UDP 123	NTP Server	Cisco DNA Center から NTP サーバの間で使用
いずれか (Any)	Cisco DNA Center	TCP 22、 UDP 161	シスコ ワイヤレス コントローラ	Cisco DNA Center からシスコ ワイヤレス コントローラの間で使用
ICMP	Cisco DNA Center	ICMP	シスコ ワイヤレス コントローラ	Cisco DNA Center からシスコ ワイヤレス コントローラの間で使用
いずれか (Any)	AP	TCP 32626	Cisco DNA Center	Cisco DNA アシユアランス インテリジェントキャプチャ (gRPC) 機能で使用されるトラフィック統計情報とパケットキャプチャデータの受信に使用されます。

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

表 9: 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
いずれか (Any)	Cisco DNA Center	TCP 443	registry.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか (Any)	Cisco DNA Center	TCP 443	www.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか (Any)	Cisco DNA Center	TCP 443	registry-cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか (Any)	Cisco DNA Center	TCP 443	cdn.ciscoconnectdna.com	Cisco DNA Center パッケージ更新のダウンロード
いずれか (Any)	Cisco DNA Center	TCP 443	software.cisco.com	デバイスソフトウェアのダウンロード
いずれか (Any)	Cisco DNA Center	TCP 443	cloudsso.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか (Any)	Cisco DNA Center	TCP 443	cloudsso1.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか (Any)	Cisco DNA Center	TCP 443	cloudsso2.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
いずれか (Any)	Cisco DNA Center	TCP 443	apiconsole.cisco.com	CSSM スマートライセンス API
いずれか (Any)	Cisco DNA Center	TCP 443	sso.cisco.com	Cisco.com クレデンシャルとスマートライセンス
いずれか (Any)	Cisco DNA Center	TCP 443	api.cisco.com	Cisco.com クレデンシャルとスマートライセンス

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

表 10 : Cisco Software-Defined Access ファブリック アンダーレイ トラフィック

送信元ポート ³	送信元	宛先ポート	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、ルータから DHCP サーバの間で、ファブリックエッジノードによって開始される DHCP リレーパケットに使用。
いずれか (Any)	ファブリックアンダーレイ	TCP 80	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間で PnP に使用
いずれか (Any)	ファブリックアンダーレイ	TCP 443	Cisco DNA Center	ファブリックスイッチ、ルータループバック IP から Cisco DNA Center の間でイメージのアップグレードに使用

いずれか (Any)	ファブリックア ンダーレイ	UDP 162	Cisco DNA Center	ファブリックスイッチ、ルー ターバック IP から Cisco DNA Center の間で SNMP ト ラップに使用
いずれか (Any)	ファブリックア ンダーレイ	UDP 514	Cisco DNA Center	ファブリックスイッチ、ルー ターから Cisco DNA アシユアラ ンス
いずれか (Any)	ファブリックア ンダーレイ	UDP 6007	Cisco DNA Center	ファブリックスイッチおよび ルーターから Cisco DNA Center の間で NetFlow に使用
いずれか (Any)	ファブリックア ンダーレイ	UDP 123	Cisco DNA Center	ファブリックスイッチから Cisco DNA Center の間で LAN 自動化時に使用
ICMP	ファブリックア ンダーレイ	ICMP	Cisco DNA Center	ファブリックスイッチ、ルー ターバックから Cisco DNA Center の間で SNMP デ バイス検出に使用
UDP 161	ファブリックア ンダーレイ	いずれか (Any)	Cisco DNA Center	ファブリックスイッチ、ルー ターバックから Cisco DNA Center の間で SNMP デ バイス検出に使用
いずれか (Any)	ファブリックア ンダーレイ	UDP 53	DNS Server	ファブリックスイッチ、ルー ターから 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 クルーターお よびスイッ チ	LISP でカプセル化された制 御メッセージ
TCP および UDP 4342	ファブリックア ンダーレイ	いずれか (Any)	ファブリッ クルーターお よびスイッ チ	LISP コントロールプレーン 通信
いずれか (Any)	ファブリックア ンダーレイ	UDP 4789	ファブリッ クルーターお よびスイッ チ	ファブリックカプセル化デー タパケット (VXLAN-GPO)
いずれか (Any)	ファブリックア ンダーレイ	UDP 1645/1646/1812/1813	ISE	ファブリックスイッチ、ルー ターバック IP から ISE の間で RADIUS に使用

ICMP	ファブリックア ンダーレイ	ICMP	ISE	ファブリックスイッチ、ルー タから ISE の間でトラブル シューティングに使用
UDP 1700/3799	ファブリックア ンダーレイ	いずれか (Any)	ISE	ファブリックスイッチから ISE の間で気付アドレス (CoA) に使用
いずれか (Any)	ファブリックア ンダーレイ	UDP 123	NTP Server	ファブリックスイッチ、ルー タループバック IP から NTP サーバの間で使用
いずれか (Any)	control-plane	UDP および TCP 4342/4343	シスコワイ ヤレスコン トローラ	コントロールプレーンのルー プバック IP からシスコワイ ヤレス コントローラの間で ファブリック対応ワイヤレス に使用

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

表 11: シスコワイヤレスコントローラトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 5246/5247/5248	シスコワイヤレス コントローラ	いずれか (Any)	AP IP アドレ スプール	シスコワイヤレスコントロー ラから AP サブネットの間で CAPWAP に使用
ICMP	シスコワイヤレス コントローラ	ICMP	AP IP アドレ スプール	シスコワイヤレスコントロー ラから AP の間でトラブル シューティング目的の ping を 許可するために使用
いずれか (Any)	シスコワイヤレス コントローラ	TCP 25103	Cisco DNA Center	シスコワイヤレスコントロー ラから Cisco DNA Center の間 でアシュアランスに使用
いずれか (Any)	シスコワイヤレス コントローラ	UDP 69/5246/5247 TCP 22	AP IP アドレ スプール	シスコワイヤレスコントロー ラから AP サブネットの間で CAPWAP に使用
いずれか (Any)	シスコワイヤレス コントローラ	UDP およ び TCP 4342/4343	コントロール プレーン	シスコワイヤレスコントロー ラからコントロールプレーン のループバック IP アドレスの 間で使用
いずれか (Any)	シスコワイヤレス コントローラ	TCP 22	Cisco DNA Center	シスコワイヤレスコントロー ラから Cisco DNA Center の間 でデバイス検出に使用

UDP 161	シスコワイヤレスコントローラ	いずれか (Any)	Cisco DNA Center	シスコワイヤレスコントローラから Cisco DNA Center の間で SNMP に使用
いずれか (Any)	シスコワイヤレスコントローラ	UDP 162	Cisco DNA Center	シスコワイヤレスコントローラから Cisco DNA Center トラップの間で SNMP トラップに使用
いずれか (Any)	シスコワイヤレスコントローラ	TCP 16113	Cisco Mobility Services Engine (MSE) と Cisco SPECTRUM EXPERT	シスコワイヤレスコントローラから Cisco MSE、SPECTRUM EXPERT の間で NMSP に使用
いずれか (Any)	シスコワイヤレスコントローラ	UDP 6007	Cisco DNA Center	ワイヤレスコントローラから Cisco DNA Center の間で NetFlow ネットワークテレメトリに使用
ICMP	シスコワイヤレスコントローラ	ICMP	Cisco DNA Center	シスコワイヤレスコントローラからトラブルシューティング目的の ping を許可するために使用
いずれか (Any)	シスコワイヤレスコントローラと各種 Syslog サーバ	UDP 514	シスコワイヤレスコントローラ	Syslog (オプション)
いずれか (Any)	シスコワイヤレスコントローラ	UDP 53	DNS Server	シスコワイヤレスコントローラから DNS サーバの間で使用
いずれか (Any)	シスコワイヤレスコントローラ	TCP 443	ISE	シスコワイヤレスコントローラから ISE の間でゲスト SSID Web 認証に使用
いずれか (Any)	シスコワイヤレスコントローラ	UDP 1645、1812	ISE	シスコワイヤレスコントローラから ISE の間で RADIUS 認証に使用
いずれか (Any)	シスコワイヤレスコントローラ	UDP 1646、1813	ISE	シスコワイヤレスコントローラから ISE の間で RADIUS アカウンティングに使用
いずれか (Any)	シスコワイヤレスコントローラ	UDP 1700、3799	ISE	シスコワイヤレスコントローラから ISE の間で RADIUS CoA に使用

ICMP	シスコワイヤレスコントローラ	ICMP	ISE	シスコワイヤレスコントローラから ISE ICMP の間でトラブルシューティングに使用
いずれか (Any)	シスコワイヤレスコントローラ	UDP 123	NTP サーバ	シスコワイヤレスコントローラから NTP サーバの間で使用

表 12: ファブリック対応ワイヤレス AP IP アドレス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 アドレスプール	UDP 67	DHCP サーバ	AP IP アドレスプールから DHCP サーバの間で使用
ICMP	AP IP アドレスプール	ICMP	DHCP サーバ	AP IP アドレスプールから ICMP の間でトラブルシューティングに使用
いずれか (Any)	AP IP アドレスプール	514	各種	Syslog : 宛先設定可能。Default is 255.255.255.255.
いずれか (Any)	AP IP アドレスプール	UDP 69/5246/5247/5248	シスコワイヤレスコントローラ	AP IP アドレスプールからシスコワイヤレスコントローラの間で CAPWAP に使用
ICMP	AP IP アドレスプール	ICMP	シスコワイヤレスコントローラ	AP IP アドレスプールからシスコワイヤレスコントローラの間でトラブルシューティング目的の ping を許可するために使用

表 13: 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
いずれか (Any)	ISE	TCP 64999	Border	ISE からボーダーノードの間で SGT Exchange Protocol (SXP) に使用
いずれか (Any)	ISE	UDP 514	Cisco DNA Center	ISE から Syslog サーバ (Cisco DNA Center) の間で使用
UDP 1645/1646/1812/1813	ISE	いずれか (Any)	ファブリックアンダーレイ	ISE からファブリックスイッチ、ルータの間で RADIUS と認証用に使用

いずれか (Any)	ISE	UDP 1700/3799	ファブリックアン ダーレイ、シスコ ワイヤレスコント ローラ	ISEからファブリックスイッチ、 ルータループバック IP アドレス の間でRADIUS認可変更 (CoA) に使用 ISEからワイヤレスコントローラ の間で CoA に使用する場合、 UDP ポート 3799 も開いている必 要があります。
ICMP	ISE	ICMP	ファブリックアン ダーレイ	ISEからファブリックスイッチの 間でトラブルシューティングに使用
いずれか (Any)	ISE	UDP 123	NTP Server	ISE と NTP サーバの間で使用
UDP 1812/1645/1813/1646	ISE	いずれか (Any)	シスコワイヤレス コントローラ	ISEからシスコワイヤレスコン トローラの間で RADIUS に使用
ICMP	ISE	ICMP	シスコワイヤレス コントローラ	ISEからシスコワイヤレスコン トローラの間でトラブルシュー ティングに使用

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

表 14: 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	APIPアドレスプール	DHCP サーバからファブリック AP の間で使用
ICMP	DHCP サー バ	ICMP	APIPアドレスプール	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 アドレス 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 アドレス 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 15: 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	いずれか (Any)	ISE	NTP サーバから ISE の間で使用
UDP 123	NTP Server	いずれか (Any)	Cisco DNA Center	NTP サーバから Cisco DNA Center
UDP 123	NTP Server	いずれか (Any)	ファブリックアンダーレイ	NTP サーバからファブリックスイッチ、ルータループバックの間で使用
UDP 123	NTP Server	いずれか (Any)	シスコワイヤレスコントローラ	NTP サーバからシスコワイヤレスコントローラの間で使用

表 16: DNS 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	いずれか (Any)	ファブリックアンダーレイ	DNS サーバからファブリックスイッチの間で使用
UDP 53	DNS Server	いずれか (Any)	シスコワイヤレスコントローラ	DNS サーバからシスコワイヤレスコントローラの間で使用

必須の設定情報

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

- **Linux ユーザ名 (Linux User Name)** : これは **maglev** です。このユーザ名は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おり、変更できません。
- **Linux パスワード (Linux Password)** : Linux ユーザ名 **maglev** のパスワードを指定します。このパスワードは、Linux コマンドラインを使用して各アプライアンスへのセキュアなアクセスを保証します。必要に応じてクラスタ内の各アプライアンスの Linux ユーザ名 **maglev** ごとに異なる Linux パスワードを割り当てることができます。

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

- 長さは 8 文字以上にする。
- タブも改行も含まない。

- 次のうち少なくとも3つのカテゴリの文字を含むこと。
 - アルファベットの大文字
 - アルファベットの小文字
 - 数字
 - 特殊文字 (!や#など)

Linux パスワードは暗号化され、Cisco DNA Center データベースにハッシュされます。マルチノードクラスタを展開している場合は、各アドオンノードに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。

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

このパスワードにはデフォルトがないため、作成する必要があります。管理者のパスフレーズは、上述の Linux パスワードと同じ要件を満たす必要があります。

- **CIMC ユーザパスワード (CIMC User Password)** : CIMC GUI へのアクセスに使用するパスワードを指定します。工場出荷時のデフォルトは「`password`」ですが、Web ブラウザを使用してアクセスするために CIMC を初めて設定するとき、変更を求められます (「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」を参照)。

CIMC ユーザパスワードは、上述の Linux パスワードと同じ要件を満たす必要があります。工場出荷時の初期状態にリセットした場合にのみ、`password` に戻すことができます。

- **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 (「[インターフェースケーブル接続](#)」を参照)。

必要な初期設定情報

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

- **スーパーユーザ権限を持つ管理者の新しいパスワード (New Admin Superuser Password)** : Cisco DNA Center 管理者の新しいスーパーユーザパスワードを入力するように求められま

す。スーパーユーザ権限を持つ管理者のパスワードをリセットすると、運用上のセキュリティが向上します。これはたとえば Cisco DNA Center アプライアンスを設置して設定した企業スタッフが Cisco DNA Center のユーザまたは管理者ではない場合に特に重要です。

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

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

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

- **ISE サーバの IP とログイン情報 (ISE Server IP and Credentials)** : Cisco ISE サーバの IP アドレスとログイン情報、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。

新規またはアップグレードのインストールでは Cisco DNA Center が設定され、Cisco ISE が認証およびポリシー (AAA) サーバとして設定されているかどうかを確認します。正しいバージョンの Cisco ISE がすでに設定されている場合、Cisco ISE から Cisco DNA Center へのグループポリシーデータの移行を開始できます。

Cisco ISE が設定されていない場合、または必要なバージョンの Cisco ISE が存在しない場合は、Cisco DNA Center がインストールされますが、グループベースのポリシーは無効になります。Cisco ISE をインストールまたはアップグレードして、Cisco DNA Center に接続する必要があります。その後はデータ移行を開始できます。

Cisco DNA Center 以前のバージョンに存在するデータは、アップグレード時に保持されません。データ移行操作では Cisco DNA Center と Cisco ISE のデータがマージされます。移行で競合が発生した場合は Cisco ISE のデータが優先されます。

Cisco DNA Center が使用できなくなった場合、さらに Cisco DNA Center より前のポリシーを管理する必要がある場合、Cisco ISE には読み取り専用設定を上書きするオプションがあります。これで Cisco ISE のポリシーを直接変更できます。Cisco DNA Center が再び使用可能になったら、Cisco ISE の読み取り専用設定を無効にして、Cisco DNA Center の [グループベースのアクセスコントロール設定 (Group Based Access Control Settings)] ページを同期しなおす必要があります。Cisco ISE で直接行われた変更は Cisco DNA Center に反映されないため、絶対に必要な場合にのみこのオプションを使用してください。

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

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

この情報は、選択した認証サーバ、ポリシーサーバと Cisco DNA Center を統合するために必要です。詳細については、[認証サーバとポリシーサーバの設定 \(119 ページ\)](#) を参照してください。

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



第 3 章

アプライアンスの設置

- アプライアンスのインストールワークフロー (45 ページ)
- アプライアンスを開梱して点検 (45 ページ)
- インストール警告とガイドラインの確認 (46 ページ)
- ラック要件の確認 (47 ページ)
- アプライアンスの接続および電源投入 (47 ページ)
- LED の確認 (48 ページ)

アプライアンスのインストールワークフロー

Cisco DNA Center アプライアンスを物理的に設置するには、この章で説明されているタスクを実行します。設置するアプライアンスごとにこれらのタスクを実行します。なおプライマリノードを設定する前に、すべてのアプライアンスを設置してください。

アプライアンスを開梱して点検



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

- ステップ 1** 段ボール箱からアプライアンスを取り出します。（将来、アプライアンスの輸送が必要になったときに備え）梱包材はすべて保管しておいてください。
- ステップ 2** カスタマーサービス担当者から提供された機器リストと梱包品の内容を照合します。すべての品目が揃っていることを確認してください。
- ステップ 3** 破損や不一致がないことを確認し、万一不備があった場合は、シスコカスタマーサービス担当者にご連絡ください。次の情報を用意しておきます。
 - 発送元の請求書番号（梱包明細を参照）
 - 破損している装置のモデルとシリアル番号

- 破損状態の説明
- 破損による設置への影響

インストール警告とガイドラインの確認



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



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



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

アプライアンスを設置する際には、次のガイドラインに従ってください。

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

ラック要件の確認

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

- 標準的な 19 インチ (48.3 cm) 幅 4 支柱 EIA ラック (ANSI/EIA-310-D-1992 のセクション 1 に準拠した英国ユニバーサル ピッチに適合するマウント支柱付き)。
- 付属のスライドレールを使用する場合、ラック支柱の穴は、9.6 mm (0.38 インチ) の正方形、7.1 mm (0.28 インチ) の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバ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 LED は、次のとおりアプライアンスの電源ステータスを示します。

- 消灯：アプライアンスには AC 電力が供給されていません。

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

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

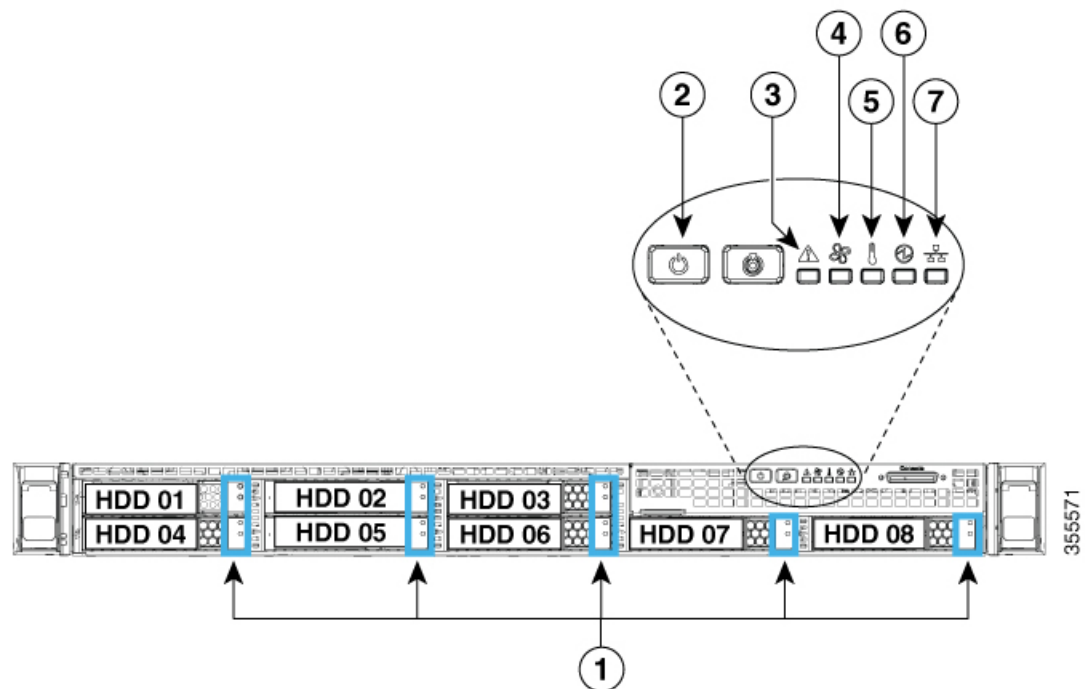
ステップ 2 前面パネルの KVM コネクタに接続されている付属の KVM ケーブルを使用して、USB キーボードと VGA モニタをサーバに接続します。または、背面パネルの VGA および USB ポートを使用することもできます。一度に接続できる VGA インターフェイスは 1 つのみです。

LED の確認

Cisco DNA Center 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。

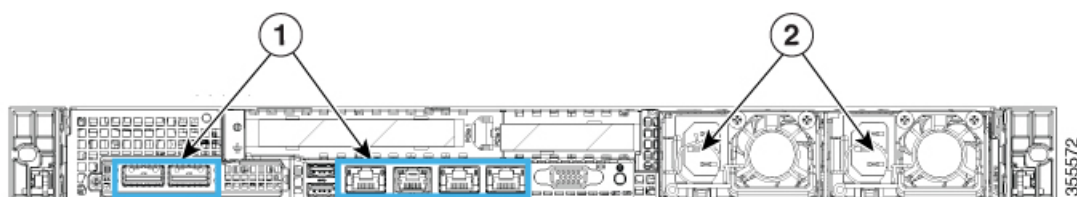
次の図は、物理的な設置と初回の電源投入が終わった後（設定前）動作しているアプライアンスの LED を示しています。

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	システムステータス : 緑
4	ファンステータス : 緑
5	温度ステータス : 緑
6	電源装置ステータス : 緑
7	ネットワーク リンク アクティビティ : 消灯

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	初めて電源を投入すると、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、電源ステータス LED が緑色になります。 Maglev 設定ウィザードを使用してネットワーク設定を構成およびテストした後（「 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 が緑色になります。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準備

- [アプライアンス設定の準備の概要](#) (51 ページ)
- [Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#) (51 ページ)
- [事前設定チェックの実行](#) (57 ページ)
- [アプライアンスのイメージの再作成](#) (64 ページ)

アプライアンス設定の準備の概要

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

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



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

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


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

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

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



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

1. GUI の左上隅から **[Toggle Navigation]** アイコン () をクリックし、**[Admin] > [User Management]** を選択します。
[Local User Management] タブがすでに選択されている必要があります。
2. ユーザ**1**のチェックボックスをオンにして、**[Modify user]** をクリックします。
[Modify User Details] ダイアログボックスが開きます。
3. **[Change Password]** チェックボックスをオンにします。
4. 新しいパスワードを入力して確認し、**[Save]** をクリックします。

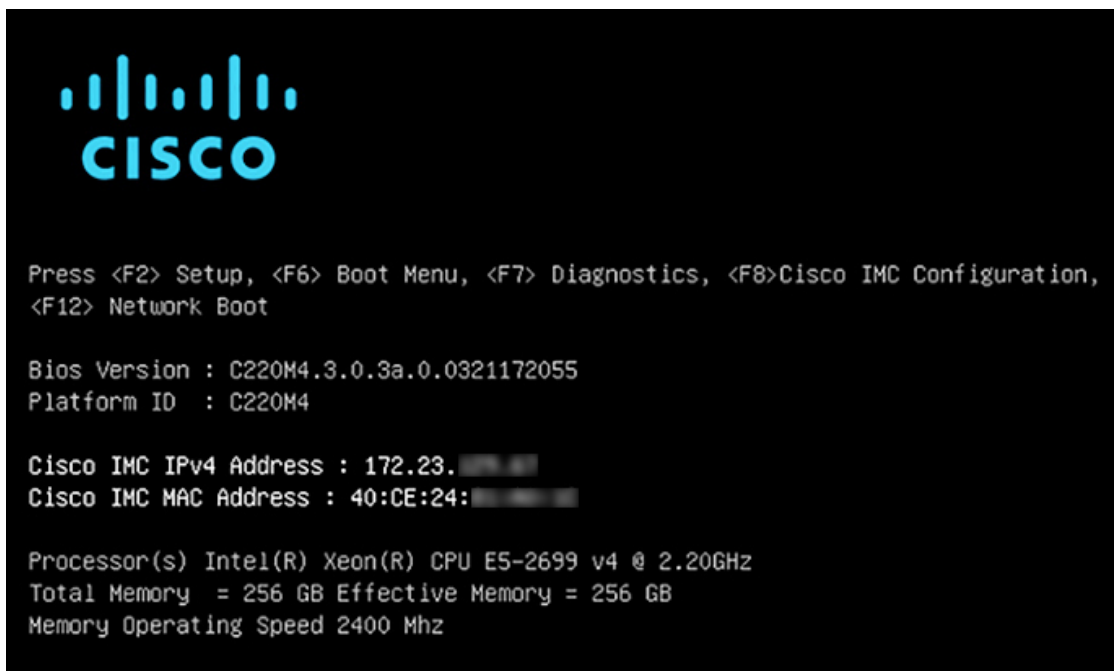
ステップ 1 次のいずれかを接続して、アプライアンスコンソールにアクセスします。

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

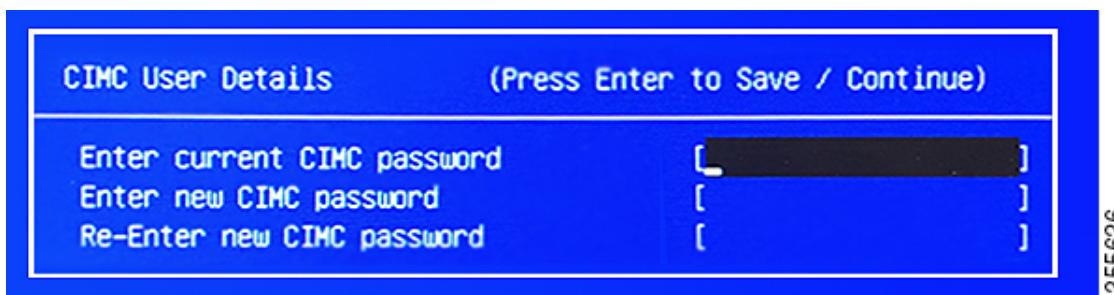
ステップ 2 アプライアンスの電源コードが接続され、電源がオンになっていることを確認します。

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

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



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



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

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

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

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                               NIC redundancy
Dedicated:      [X]                   None:           [X]
Shared LOM:     [ ]                   Active-standby: [ ]
Cisco Card:
  Riser1:       [ ]                   Active-active:  [ ]
  Riser2:       [ ]                   VLAN (Advanced)
  MLOm:         [ ]                   VLAN enabled:   [ ]
  Shared LOM Ext: [ ]                   VLAN ID:        1
                                           Priority:        0
IP (Basic)
IPV4:           [X]                   IPV6:           [ ]
DHCP enabled    [ ]
CIMC IP:        172.23.
Prefix/Subnet:  255.255.0.0
Gateway:        172.23.
Pref DNS Server: 171.70.
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F1>Additional settings
    
```

ステップ7 次のアクションを実行します。

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

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

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


```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
Common Properties
Hostname:      C220-FCH212
Dynamic DNS:   [ ]
DDNS Domain:
FactoryDefaults
Factory Default: [ ]
Default User(Basic)
Default password:
Reenter password:
Port Properties
Auto Negotiation: [X]
                Admin Mode      Operation Mode
Speed [1000/100/10Mbps]:      Auto          1000
Duplex mode[half/full]:      Auto          full
Port Profiles
Reset:         [ ]
Name:
*****
<Up/Down>Selection  <F10>Save  <Space>Enable/Disable  <F5>Refresh  <ESC>Exit
<F2>PreviousPageettings
    
```

ステップ 9 次のアクションを実行します。

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

ステップ 10 F10 を押して、設定を保存します。

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

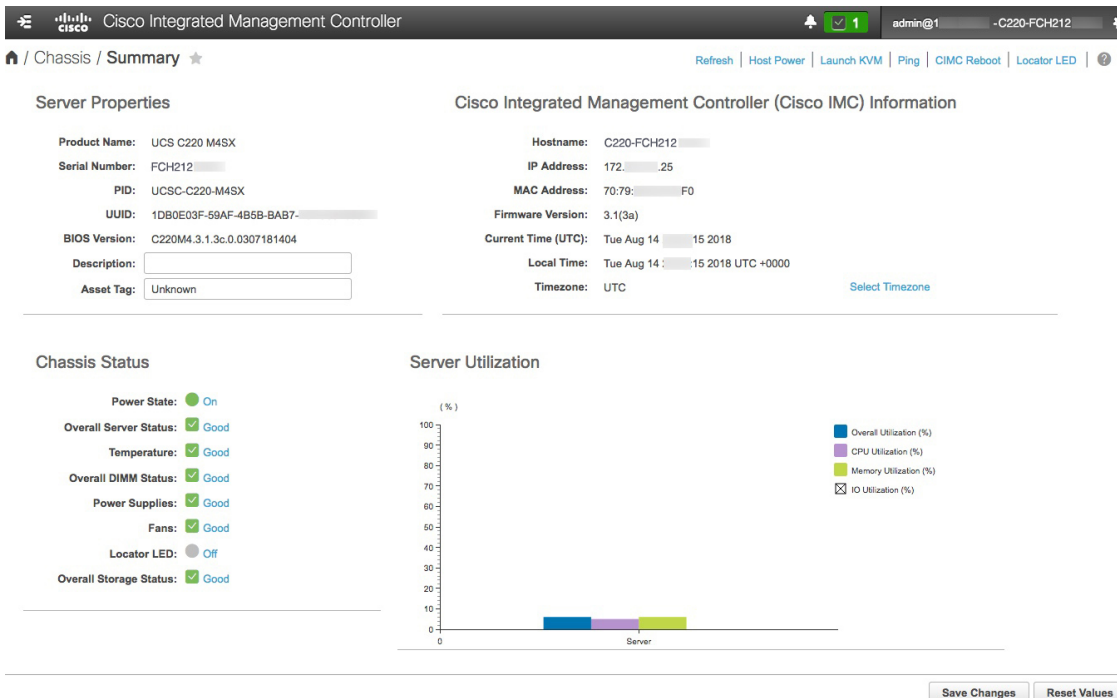
ステップ 12 設定が保存され、アプライアンスのリブートが完了したら、アプライアンスがインストールされているサブネットへのアクセスが可能なクライアントマシンで互換性のあるブラウザを開き、次の URL を入力します。

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

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



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



事前設定チェックの実行

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

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

ステップ 1 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」で設定した CISCO imc IP アドレス、ユーザ ID、パスワードを使用して、アプライアンスの Cisco IMC にログインします。ログインに成功すると、次に示すような **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウがブラウザに表示されます。

The screenshot shows the Cisco IMC GUI for a UCS C220 M4SX server. The 'Server Properties' section includes fields for Product Name, Serial Number, PID, UUID, BIOS Version, Description, and Asset Tag. The 'Cisco Integrated Management Controller (Cisco IMC) Information' section displays Hostname, IP Address, MAC Address, Firmware Version, Current Time (UTC), Local Time, and Timezone. Below these are 'Chassis Status' (Power State: On, Overall Server Status: Good, Temperature: Good, Overall DIMM Status: Good, Power Supplies: Good, Fans: Good, Locator LED: Off, Overall Storage Status: Good) and a 'Server Utilization' bar chart showing Overall, CPU, Memory, and IO Utilization percentages.

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。


- Cisco IMC GUI の左上隅から、[Toggle Navigation] アイコン (☰) をクリックします。
- Cisco IMC メニューから [Admin] > [Networking] を選択し、[NTP Setting] タブを選択します。
- [NTP Enabled] チェックボックスがオンになっていることを確認してから、次に示す例のように、4 つの番号付きサーバフィールドに最大 4 つの NTP サーバホスト名またはアドレスを入力します。

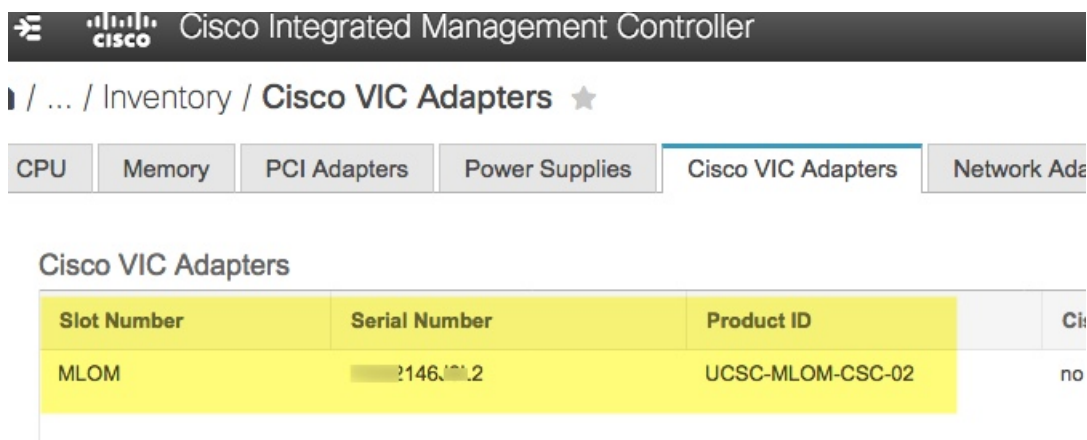
The screenshot shows the 'NTP Setting' page in the Cisco IMC GUI. Under 'NTP Properties', the 'NTP Enabled' checkbox is checked. There are four input fields for 'Server 1' through 'Server 4', each containing '1.ntp.example.com'. The 'Status' is 'NTP service disabled'. The page includes 'Save Changes' and 'Reset Values' buttons at the bottom right.


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

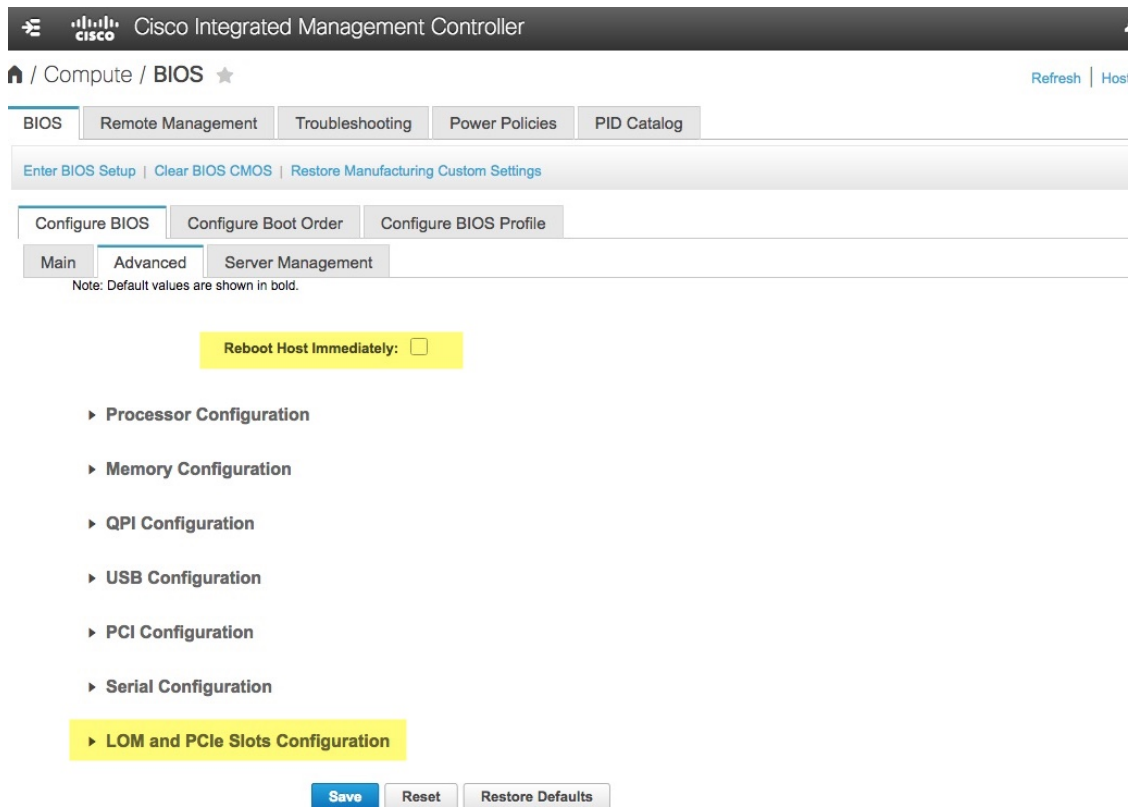
(注) Cisco IMC で NTP 認証はサポートされていません。

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

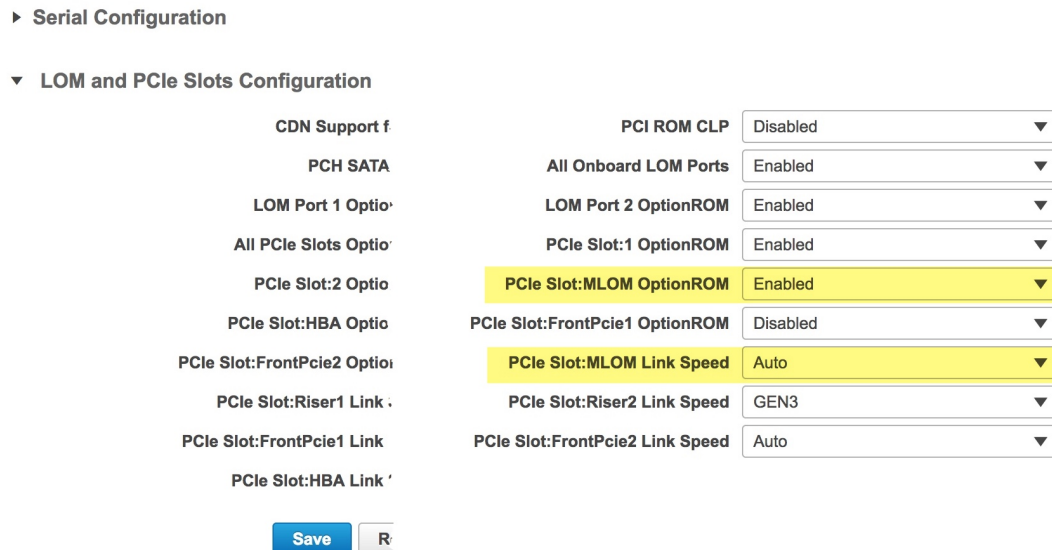
- a) 必要に応じて、 アイコンをクリックして Cisco IMC のメニューを表示します。
- b) Cisco IMC のメニューから、[Chassis] > [Inventory] > [Cisco VIC Adapters] の順に選択します。次に示すように、製品 ID 「UCSC-MLOM-CSC-02」が MLOM スロット用に一覧表示されていることを確認します。



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

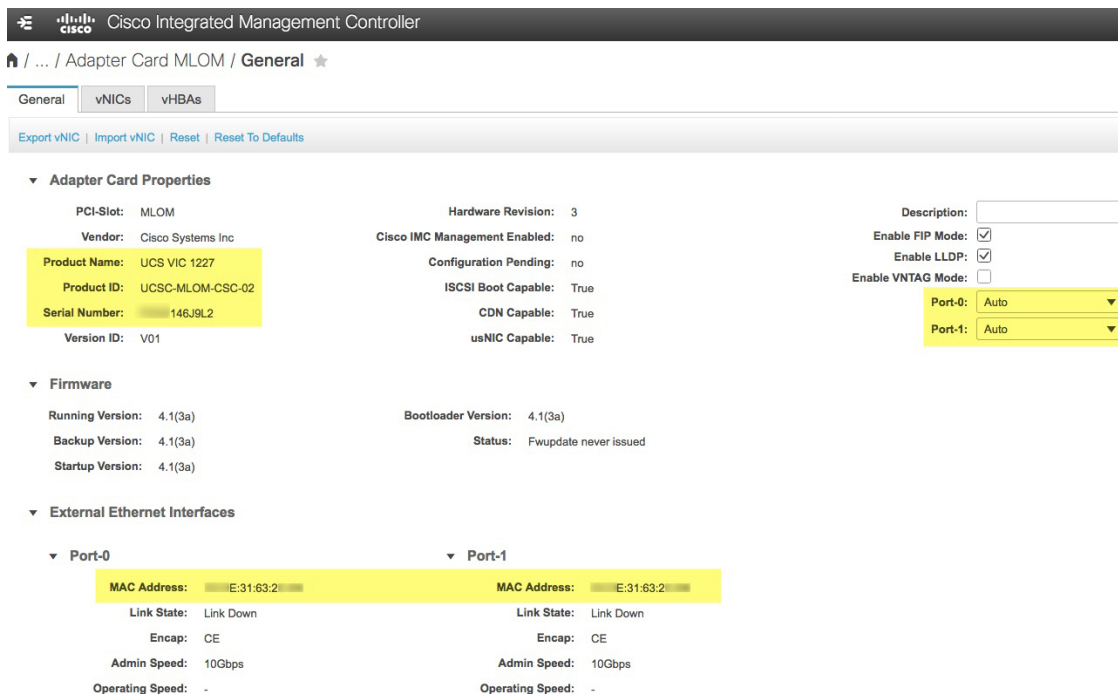


d) [LOM and PCIe Slots Configuration] を選択します。次に、ドロップダウンセレクトを使用して、[PCIe Slot MLOM OptionROM] を [Enabled] に、[PCIe Slot: MLOM Link Speed] を [Auto] に設定します。



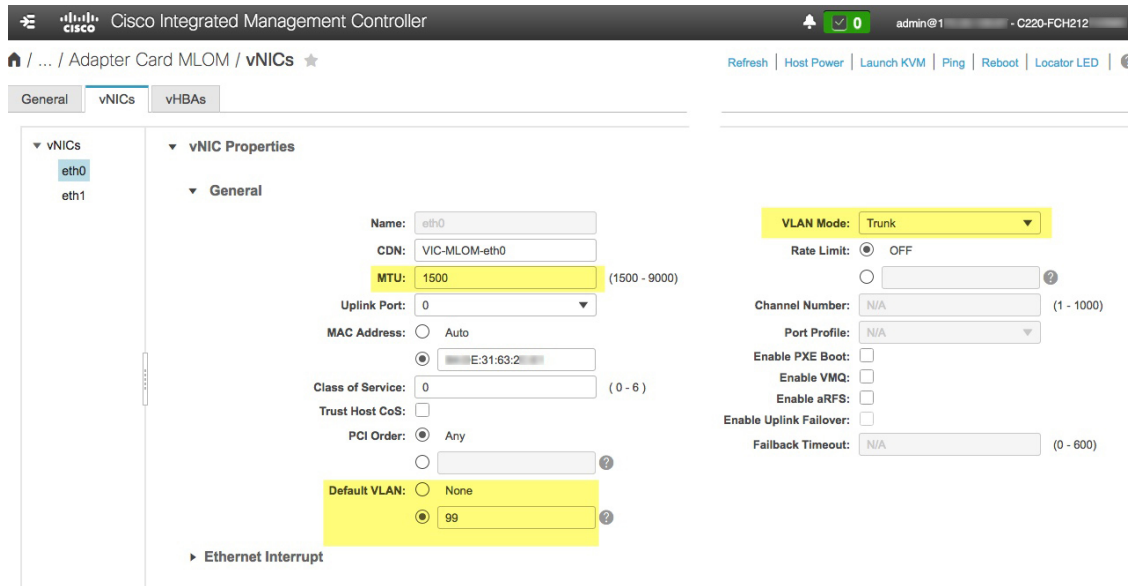
e) [保存 (Save)] をクリックします。ホストをリブートするように求められます。[OK] をクリックして、リブートせずに続行します。

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



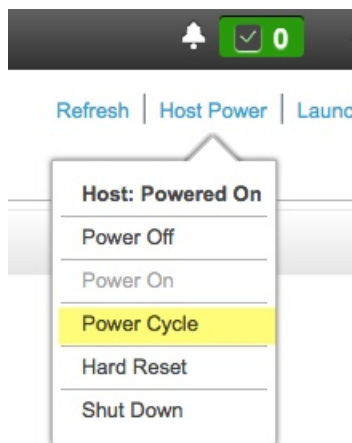
- g) [vNICs] タブをクリックし、[vNICs] ドロップダウンで [eth0] を選択します。セクタとフィールドを使用して、次の値を [eth0] に設定します。

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



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

- h) [Save Changes] をクリックします。ホストをもう一度リブートするように求められます。[Cancel] をクリックして、リブートせずに続行します。
- i) [vNICs] ドロップダウンから [eth1] を選択し、アプライアンスとそれに接続されているアップリンクスイッチで使用する値を設定します。
- j) 完了したら、[変更の保存 (Save Changes)] をクリックします。ホストをリブートするように求められます。今回は、[OK] をクリックしてアプライアンスをリブートします。
- k) アプライアンスのリブートが完了したら、Cisco IMC GUI に再度ログインします。☰ > [Networking] > [Adapter Card MLOM] > [General] > [vNICs] の順に選択します。vNIC MAC アドレスと、以前に設定した [MTU]、[VLAN]、[VLAN Mode] の各パラメータが正確かどうかを確認します。
- l) 終了したら、右上の [Host Power] メニューをクリックして、[Power Cycle] を選択します。次に [OK] をクリックします。



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

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

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

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

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

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

これらのコマンドは単なる例であることに注意してください。アプライアンスの NIC を設定する場合は、この手順のステップ 3 で入力したものと同一 VLAN ID と MTU 値を使用してください。リンク速度、デュプレックス、MTU の各パラメータに表示される値が、スイッチのデフォルトです。このデフォルトを変更した場合にのみ、これらのパラメータの新しい値を入力します。アプライアンス NIC と同様に、スループットが向上するように MTU を設定することもできます (上限は 9000)。

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

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

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

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

MySwitch#

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

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

MySwitch#

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

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

MySwitch#
```

次のタスク

このタスクが完了したら、次のいずれかを実行します。

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

アプライアンスのイメージの再作成

バックアップからの回復やクラスタリンク設定の変更など、Cisco DNA Center アプライアンスイメージの再作成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 イメージであることを確認するよう強くお勧めします。

始める前に

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

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

次に例を示します。

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

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

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

実行したコマンドの出力とダウンロードした SHA512 チェックサムファイルを比較します。コマンド出力が一致しない場合は、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。まだ OpenSSL をインストールしていない場合、Windows ではダウンロードしてインストールする必要があります ([こちらから](#)入手可能)。

ISO イメージが純正であれば、このコマンドを実行すると、「問題がないことを確認 (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、シスコサポートにお問い合わせください。

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

ブート可能な USB ドライブの作成

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

始める前に

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

Etcher の使用

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

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

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

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

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

- 成功時に自動マウント解除する
- 成功時に書き込みを検証する

ステップ4 [Back] をクリックして、メインウィンドウに戻ります。

ステップ5 [Select Image] をクリックします。

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

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

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

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

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

Linux CLI の使用

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

- a) フラッシュドライブをマシンの USB ポートに挿入します。
- b) Linux シェルを開き、次のコマンドを実行します。 **lsblk**

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

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

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

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

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

Mac CLI の使用

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

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

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

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

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

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

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

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

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

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

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

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

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

Cisco DNA Center ISO イメージのインストール

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

始める前に

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

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

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

ステップ 3 アプライアンスの電源を投入または再投入します。

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

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

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

ブートデバイス選択メニューが表示されます。

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

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

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

Cisco DNA Center ISO イメージのインストールが完了すると、インストーラがリブートし、Maglev 設定ウィザードの初期画面が開きます。プライマリクラスタノードを設定するのか、アドオンクラスタノードを設定するのかに応じて、「[プライマリノードの設定](#)」または「[アドオンノードの設定](#)」のステップ 4 に進みます。



第 5 章

アプライアンスの設定

- [アプライアンスの設定の概要 \(71 ページ\)](#)
- [プライマリノードの設定 \(72 ページ\)](#)
- [アドオンノードの設定 \(89 ページ\)](#)
- [最新の Cisco DNA Center リリースへのアップグレード \(107 ページ\)](#)

アプライアンスの設定の概要

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

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

初期導入でスタンドアロンモードを選択した場合は、後でクラスタを形成するためにアプライアンスを追加できます。スタンドアロンホストの設定時には、クラスタ内の最初のノード、つまり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。

初期展開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。

続行するには、次のタスクを実行します。

1. Cisco IMC から Maglev 設定ウィザードを起動し、クラスタ内の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](#)」を参照してください。
2. 3 つのアプライアンスを設置し、クラスタに 2 番目と 3 番目のノードを追加する場合は、「[アドオンノードの設定](#)」を参照してください。

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](#)」に記載された手順を実行します。



-
- (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](#)」で指定されているすべての情報を収集したこと。
- 「[アプライアンスのインストールワークフロー](#)」の説明に従って、最初のアプライアンスがインストールされたこと。
- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」の説明に従って、プライマリノードで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「[事前設定チェックの実行](#)」の説明に従って、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。
- 互換性のあるブラウザを使用していることを確認済みであること。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](#) ドキュメントを参照してください。
- 次の手順で指定するデフォルトゲートウェイおよび DNS サーバと Cisco DNA Center の間のファイアウォールで ICMP が許容されること。Maglev 設定ウィザードでは ping を使用して、ユーザが指定したゲートウェイおよび DNS サーバを確認します。ファイアウォールが配置されており、そのファイアウォールで ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

ステップ 1 お使いのブラウザで、実行した cisco imc GUI 設定で設定した Cisco IMC の IP アドレスをポイントし、cisco imc ユーザとして Cisco IMC GUI にログインします（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」を参照）。

ログインが成功すると、次に示すように、アプライアンスに **[Cisco Integrated Management Controller Chassis 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 ハイパーリンクメニューで **[Launch KVM]** を選択してから **[Java based KVM]** と **[HTML based KVM]** のいずれかを選択します。**[Java-based 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。**[HTML-based 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。

- メインの Cisco IMC GUI ブラウザウィンドウで、**[Host Power]** > **[Power Cycle]** を選択し、KVM コンソールに切り替えて続行します。
- KVM コンソールで、**[Power]** > **[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、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。

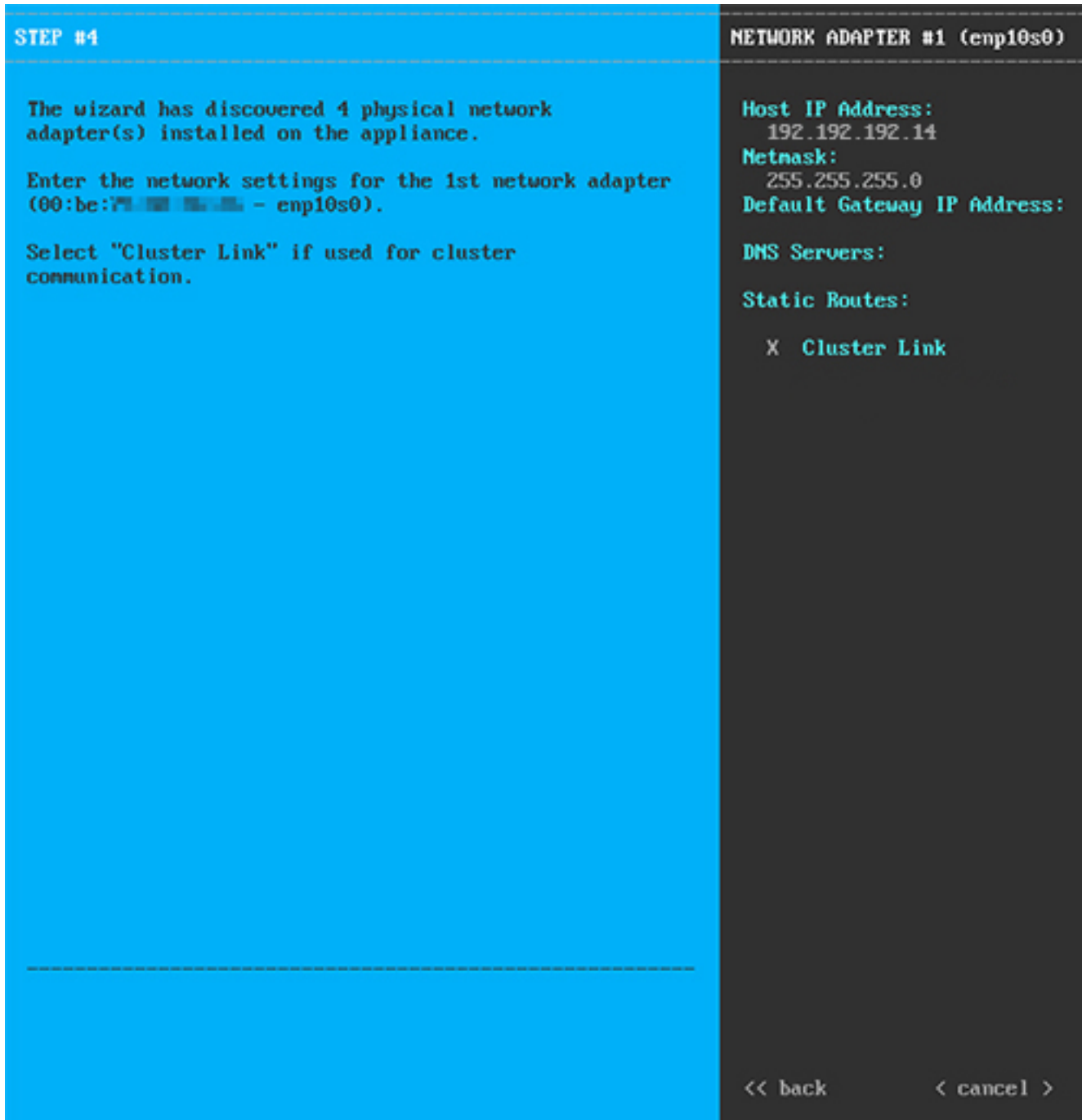


ステップ 4 プライマリノードの設定を開始するには、[Start a Cisco DNA Center Cluster] を選択します。
 ウィザードでは、アプライアンス上のすべてのポートが検出され、次の順序で1つずつ別の画面に表示されます。

1. 10 Gbps クラスタポート (ポート 2、enp10s0、ネットワークアダプタ #1)
2. 1 Gbps Cisco DNA Center GUI ポート (1、enp1s0f0、ネットワークアダプタ #2)
3. 1 Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ #3)
4. 10 Gbps エンタープライズポート (ポート 1、enp9s0、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。Cisco DNA Center 機能にはこの2つのポートが必要です。機能していないことが判明した場合には、[キャンセル (Cancel)] を選択して、設定をすぐに終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に「[事前設定チェックの実行](#)」に記載されているすべての手順が完了していることを確認してください。

ステップ 5 ウィザードでは、まず10Gbps クラスタポート (ポート 2、enp10s0) が検出され、[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)。



次の表のとおり [ネットワークアダプタ #1 (NETWORK ADAPTER #1)] の設定値を入力します。

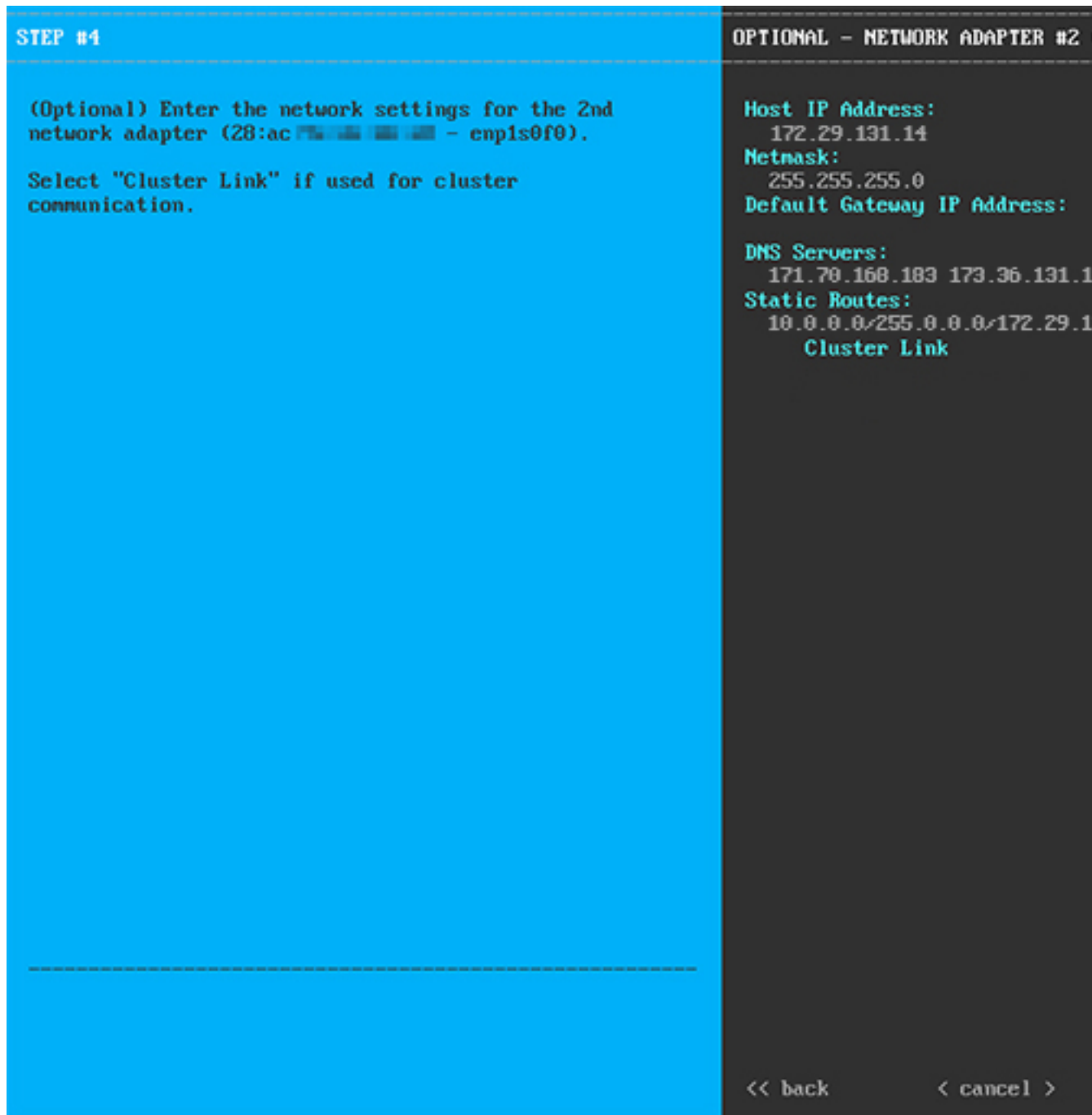
表 17: ネットワークアダプタ #1 のプライマリノードエントリ: 10 Gbps クラスタポート (enp10s0)

<p>ホスト IP アドレス</p>	<p>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。</p>
--------------------	---

<p>Netmask</p>	<p>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。</p>
<p>デフォルトゲートウェイ IP アドレス</p>	<p>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。</p> <p>重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。</p>
<p>DNS Servers</p>	<p>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。</p> <p>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。</p>
<p>スタティック ルート</p>	<p>1 つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク><ゲートウェイ>の形式で入力します。このスタティックルートは、通常、GUI ポートでのみ必要になります。</p>
<p>クラスタリンク</p>	<p>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。</p>

設定値の入力が完了したら、[next >>] をクリックして続行します。入力した値がウィザードによって検証され、正しくない値が含まれていた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 [<< back] をクリックして再入力します。

ステップ 6 入力したクラスタポート値の検証が成功すると、ウィザードに 1 Gbps Cisco DNA Center GUI ポート (1、enp1s0f0) が [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)。



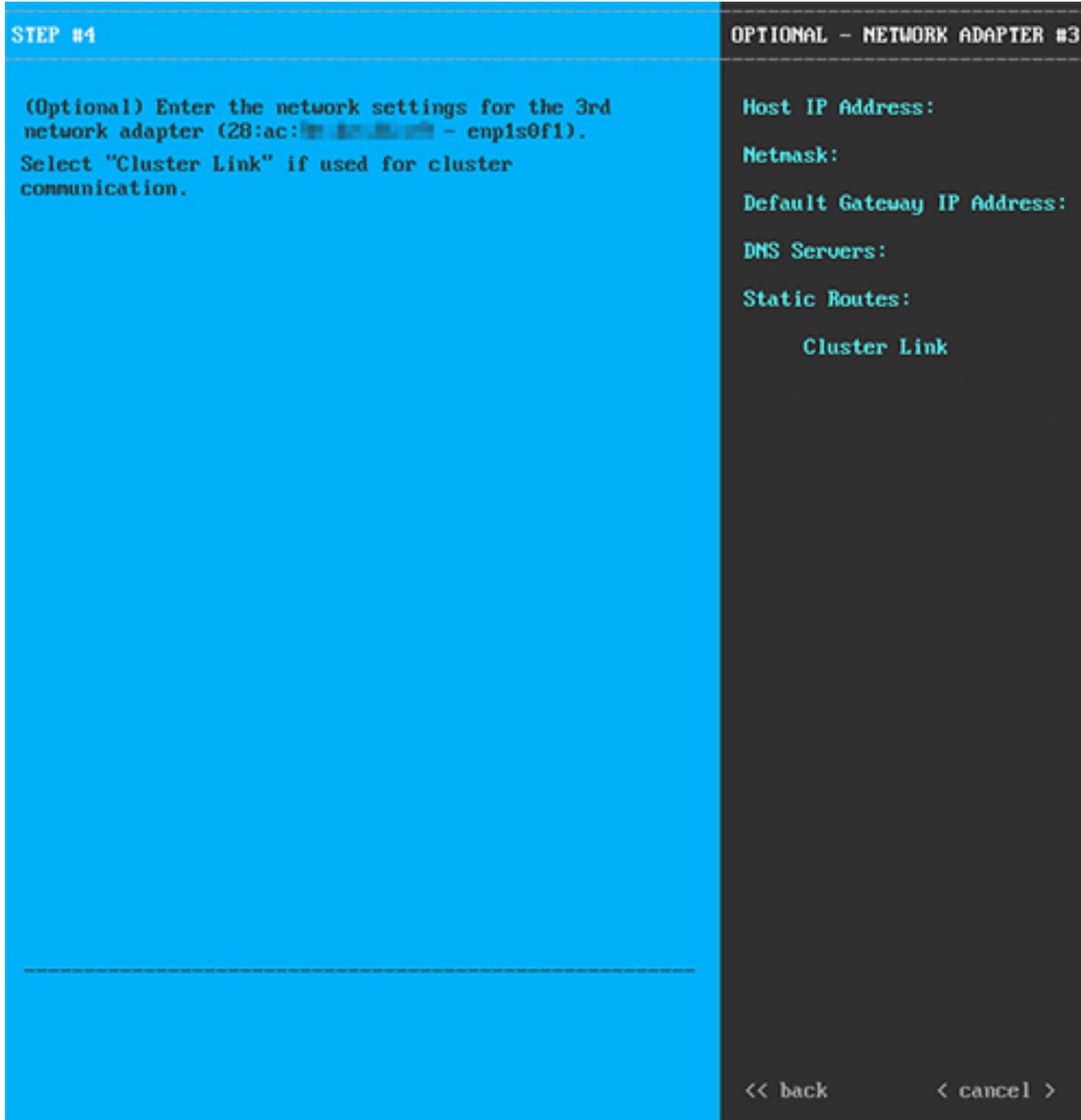
次の表のとおり [ネットワークアダプタ #2 (NETWORK ADAPTER #2)] の設定値を入力します。

表 18: ネットワークアダプタ #2のプライマリノードエントリ: 1 Gbps GUI ポート (enp1s0f0)

ホスト IP アドレス	1 Gbps GUI ポートの IP アドレスを入力します。これは、GUI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。
Netmask	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	<p>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。</p> <p>重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。</p>
DNS Servers	<p>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。</p> <p>重要</p> <ul style="list-style-type: none"> • 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、<ネットワーク><ネットマスク><ゲートウェイ> の形式で入力します。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

必要な情報を入力したら [Next >>] をクリックして続行します。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 Cisco DNA Center GUI ポート値が正常に検証されると、ウィザードに 1 Gbps クラウドポート (2、enp1s0f1) が [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 (ポート1、enp9s0) 経由でリンクを実行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)。



次の表のとおり [NETWORK ADAPTER #3]の設定値を入力します。

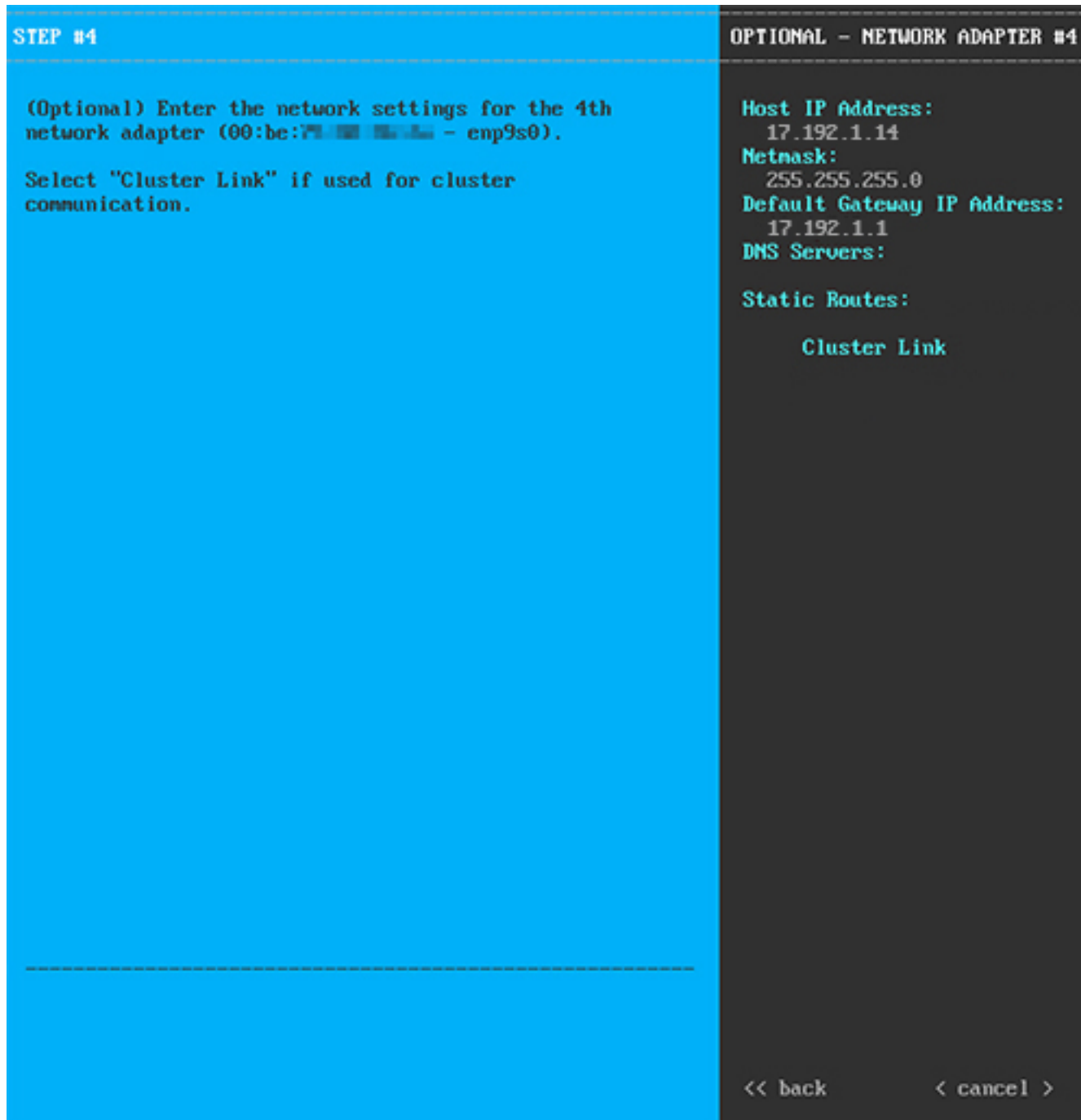
表 19: ネットワークアダプタ #3のプライマリノードエントリ: 1 Gbps クラウドポート (enp1s0f1)

ホスト IP アドレス	クラウドポートの IP アドレスを入力します。この操作はインターネット接続にクラウドポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにしておくことができます。
Netmask	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	クラウドポートに使用するデフォルトゲートウェイの IP アドレスを入力します。 重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。
DNS Servers	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 重要 クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ>の形式で入力します。このスタティックルートは、通常、Cisco DNA Center GUI ポートでのみ必要になります。
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。

必要な情報を入力したら [Next >>] をクリックして続行します。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 入力したクラウドポート値が正常に検証されると、ウィザードに 10 Gbps エンタープライズポート (ポート 1、enp9s0) が [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

まず（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）。



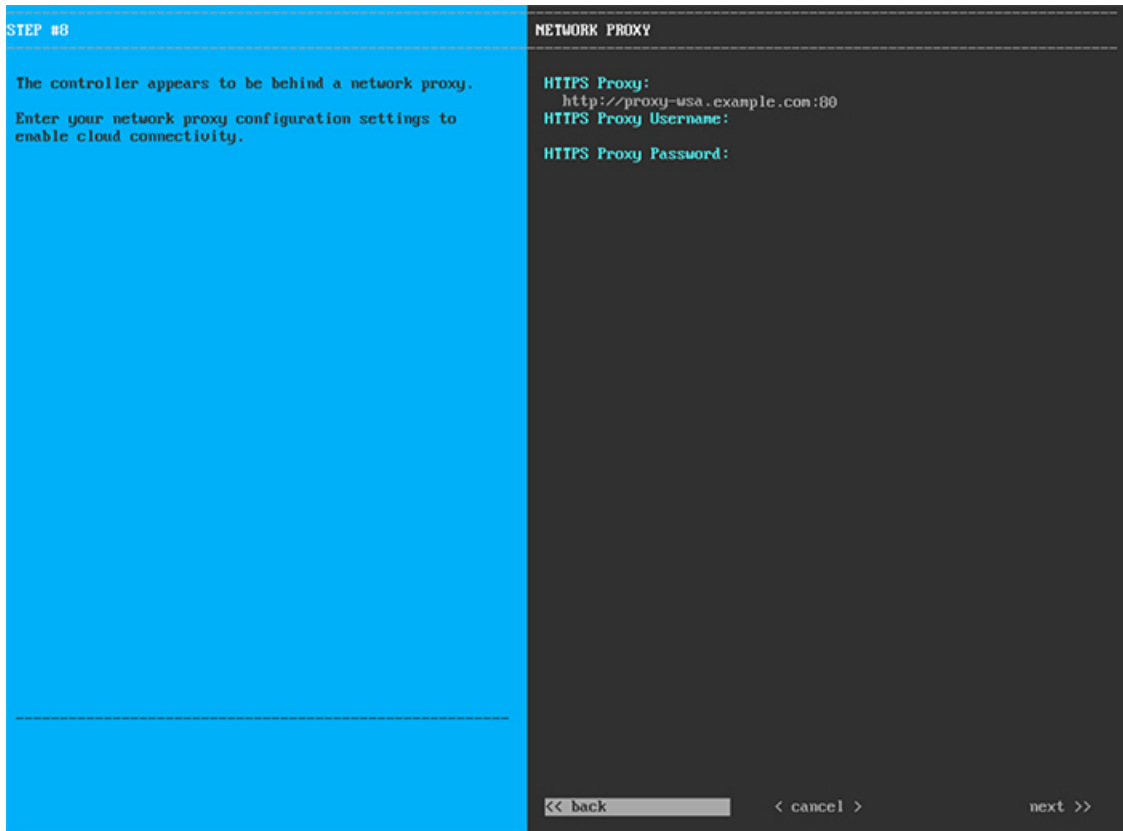
次の表のとおり [NETWORK ADAPTER #4] の設定値を入力します。

表 20: ネットワークアダプタ #4 のプライマリノードエントリ: 10 Gbps エンタープライズポート (enp9s0)

ホスト IP アドレス	10 Gbps エンタープライズポートの IP アドレスを入力します。これは必須です。
Netmask	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルトゲートウェイ IP アドレス	<p>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。</p> <p>重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。</p>
DNS Servers	<p>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。</p> <p>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。</p>
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ>の形式で入力します。このスタティックルートは、通常、Cisco DNA Center GUI ポートでのみ必要になります。
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。

必要な情報を入力したら [Next>>] をクリックして続行します。以前の画面でしたように、検証エラーを修正します。ネットワークアダプタの設定がウィザードによって検証され、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、ユーザの使用する [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から求められます。



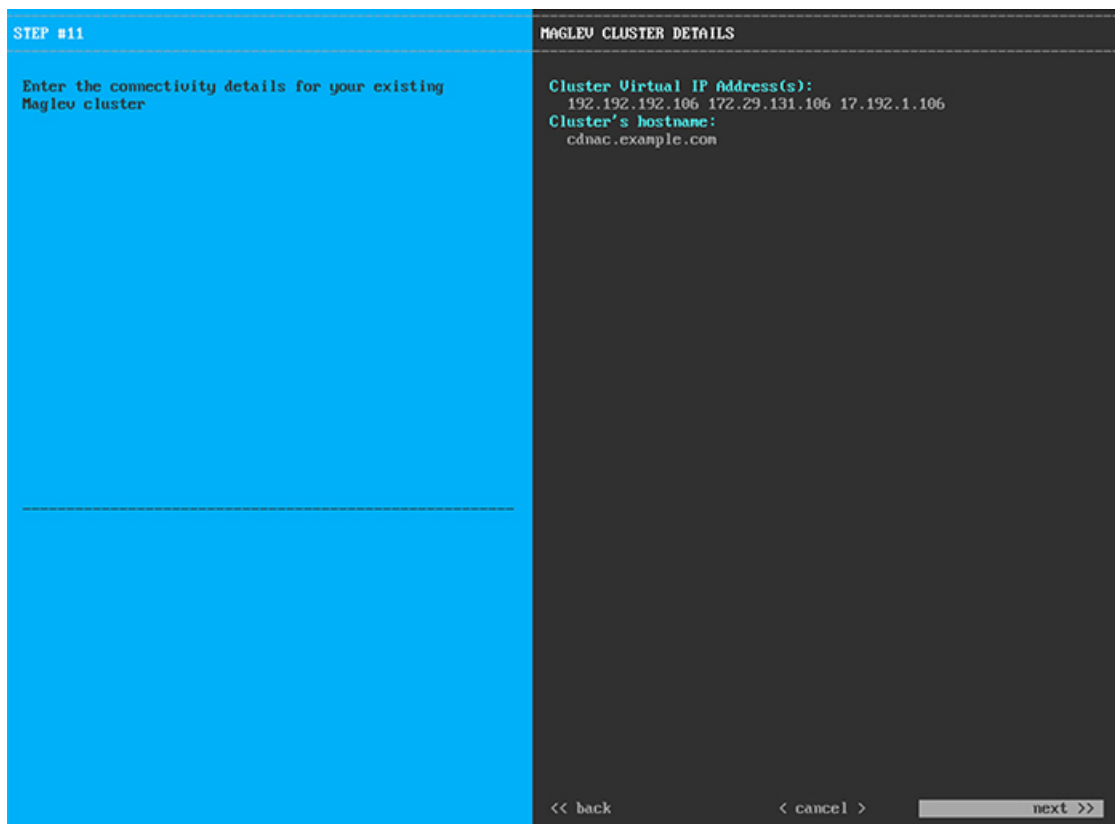
次の表に示すように [NETWORK PROXY] の設定値を入力します。

表 21: 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不要な場合には、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不要な場合には、このフィールドを空白のままにします。

必要な情報を入力したら [Next >>] をクリックして続行します。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 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。

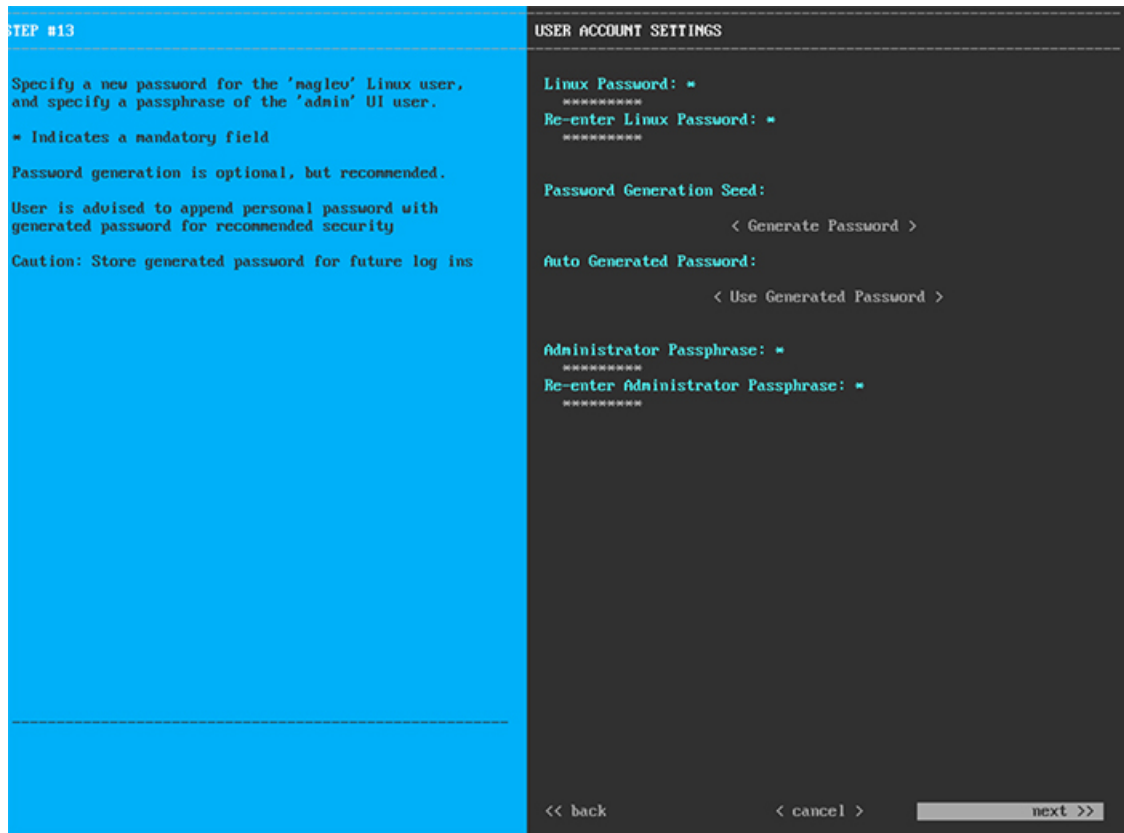
重要 設定済みのネットワークインターフェイスごとに1つずつ仮想 IP アドレスを入力する必要があります。この操作を行わない限り、ウィザードを完了することはできません。これらのアドレスは、クラスタリンクのステータスに関連付けられており、ステータスは[UP]の状態となっている必要があります。

クラスタの完全修飾ドメイン名 (FQDN) を指定するオプションもあります。Cisco DNA Center ではこのドメイン名を使用して次の操作が実行されます。

- このホスト名を使用して、クラスタの Web インターフェイスと、Cisco DNA Center が管理するエンタープライズネットワーク内のデバイスによって使用される Representational State Transfer (REST) API にアクセスします。
- Cisco DNA Center 証明書の [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。

必要な情報を入力したら [Next>>] をクリックして続行します。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 ユーザアカウントの詳細を入力すると、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からメッセージが表示されます。



次の表のとおり [USER ACCOUNT SETTINGS] の値を入力します。

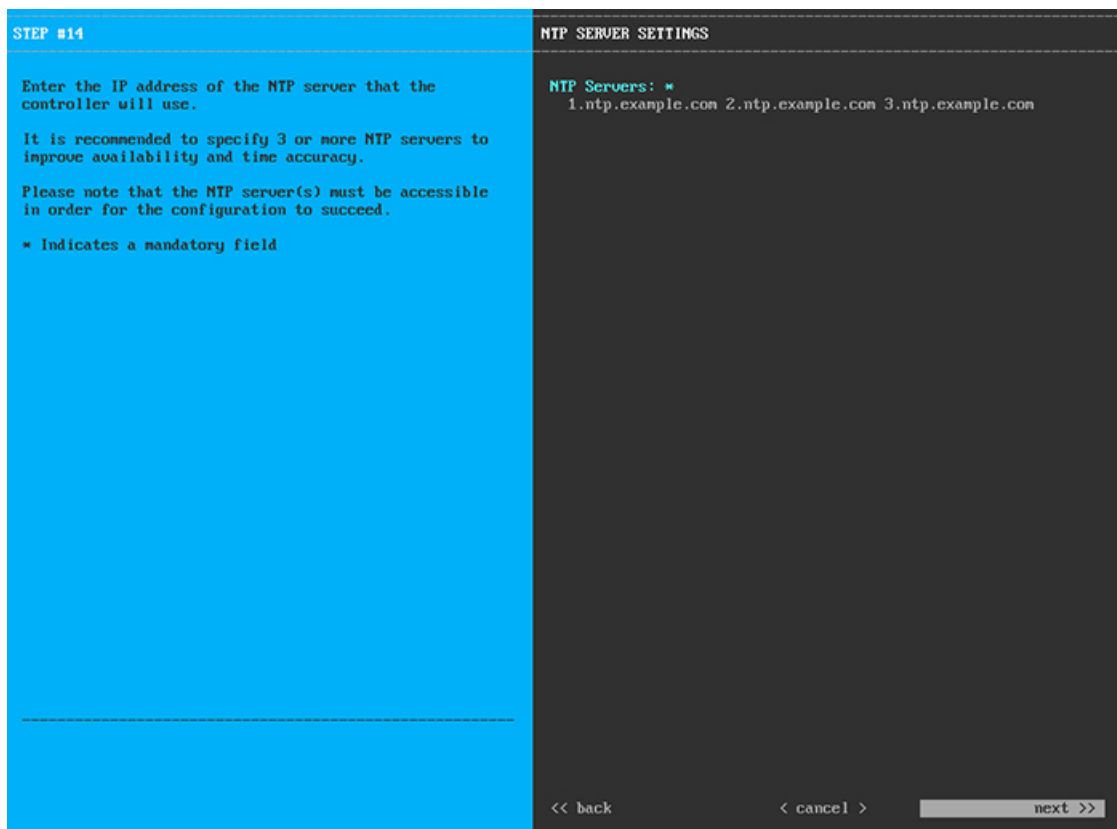
表 22: ユーザアカウント設定のプライマリノードエントリ

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、 [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。

必要な情報を入力したら **[Next>>]** をクリックして続行します。以前の画面でしたように、検証エラーを修正します。

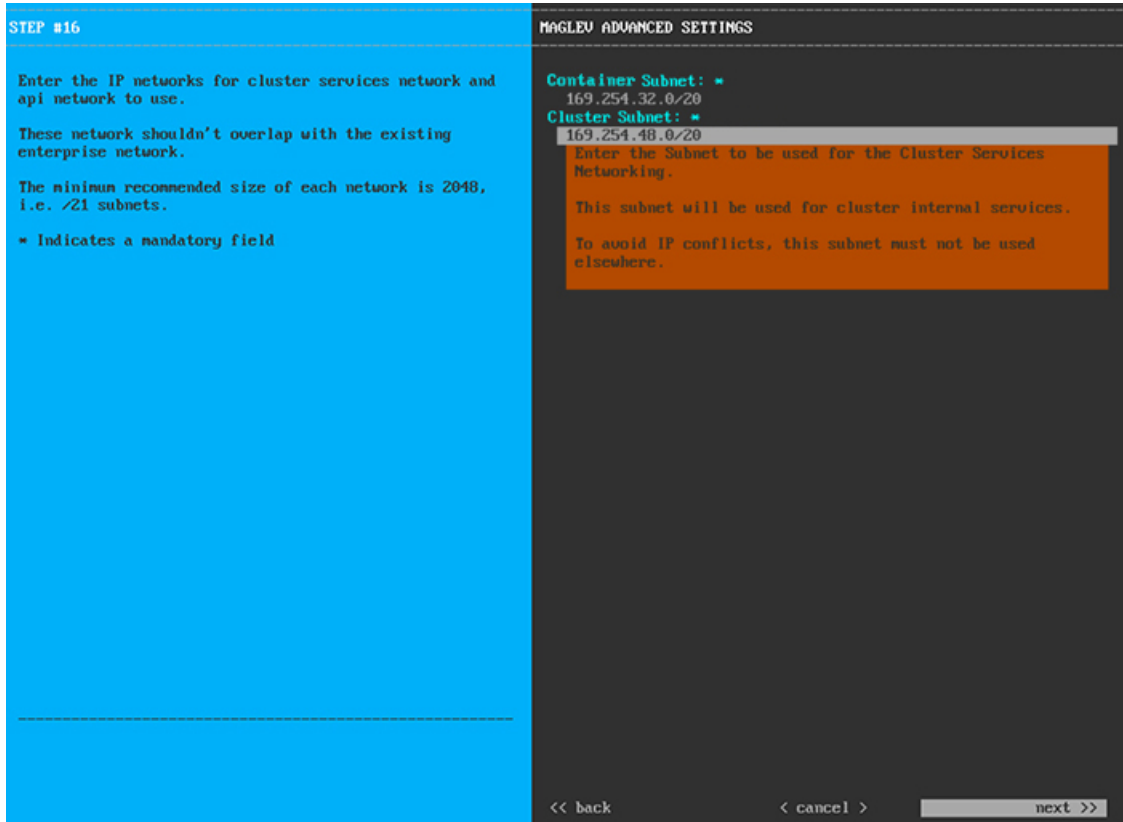
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように **[NTP SERVER SETTINGS]** の値を入力するようウィザードからメッセージが表示されます。



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

必要な情報を入力したら **[Next>>]** をクリックして続行します。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 適切なNTPサーバを指定すると、次に示すように、**[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 ADVANCED SETTINGS] の設定値を入力します。

表 23: Maglev 詳細設定のプライマリノードエントリ

<p>コンテナサブネット</p>	<p>内部サービスを管理するために Cisco DNA Center で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは 169.254.32.0/20 にあらかじめ設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、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、重複したりしていないことを確認してください。詳細については、必要な IP アドレスおよびサブネット (20 ページ) のコンテナサブネット (Container Subnet) に関する説明を参照してください。</p>
------------------	---

<p>クラスタサブネット</p>	<p>内部クラスタサービスを管理するために Cisco DNA Center で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは 169.254.48.0/20 にあらかじめ設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、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、重複したりしていないことを確認してください。詳細については、必要な IP アドレスおよびサブネット (20 ページ) のクラスタサブネット (Cluster Subnet) に関する説明を参照してください。</p>
------------------	---

終了したら、[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、ウィザードで設定を適用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 (以下参照)。



[Proceed >>] をクリックして、設定ウィザードを完了します。

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

- このアプライアンスをスタンドアロンモードでのみ展開する場合には、所定の初期設定（「[初期設定ワークフロー](#)」）を実行します。
- 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。

- 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。
- 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、SSH を使用してプライマリノードの Cisco DNA Center GUI 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ません。このため、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+21l6NFHAKOZDs0cNLHBR75j1KV3ZXIKuUaiadk.
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 enp9s0: 17.192.1.14
Usage of /: 59.8% of 28.03GB     IP address for enp10s0: 192.192.192.14
Memory usage: 21%              IP address for enp1s0f0: 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-1) ~
$ maglev package status
[administration] password for 'admin':
```

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

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

- 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ます、そのプロセスの間、クラスタはダウンします。

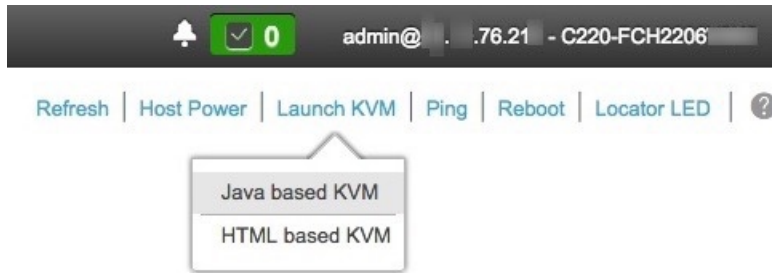
始める前に

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](#)」で指定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。

Cisco DNA Center GUI からこの情報にアクセスできます。[Help] アイコン (🔗) をクリックし、[About] > [Packages] の順に選択してください。
 2. Cisco TAC に連絡し、このコマンドの出力を提供して 2 番目と 3 番目のアプライアンスにインストールする必要がある ISO をポイントするよう依頼したこと。
- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」の説明に従って、両方のアドオンアプライアンスで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「[事前設定チェックの実行](#)」の説明に従って、アドオン ノードアプライアンスのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていることを確認しました。
- 互換性のあるブラウザを使用していることを確認済みであること。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 [リリースノートドキュメント](#)を参照してください。
- 次の手順で指定するデフォルトゲートウェイおよび DNS サーバと Cisco DNA Center の間のファイアウォールで ICMP が許容されること。Maglev 設定ウィザードでは ping を使用して、ユーザが指定したゲートウェイおよび DNS サーバを確認します。ファイアウォールが配置されており、そのファイアウォールで ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

- ステップ 1** お使いのブラウザで、実行した `cisco imc` GUI 設定で設定した Cisco IMC の IP アドレスをポイントし、`cisco imc` ユーザとして Cisco IMC GUI にログインします（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」を参照）。
- ログインが成功すると、次に示すように、アプライアンスに **[Cisco Integrated Management Controller Chassis 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 ハイパーリンクメニューで **[Launch KVM]** を選択してから **[Java based KVM]** と **[HTML based KVM]** のいずれかを選択します。 **[Java-based 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。 **[HTML-basedKVM]** 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。

- メインの Cisco IMC GUI ブラウザウィンドウで、 **[Host Power]** > **[Power Cycle]** を選択し、KVM コンソールに切り替えて続行します。
- KVM コンソールで、 **[Power]** > **[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、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 Data Center クラスタに追加 (Join a Cisco DNA Center 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. 10 Gbps クラスタポート (ポート 2、enp10s0、ネットワークアダプタ #1)
2. 1 Gbps Cisco DNA Center GUI ポート (1、enp1s0f0、ネットワークアダプタ #2)
3. 1 Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ #3)
4. 10 Gbps エンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ #4)

(注) 設定の過程でウィザードに 10 Gbps ポートのうちの 1 つまたは両方が表示されない場合、これらのポートは機能しないか無効になっている可能性があります。これらの 10 Gbps ポートは Cisco DNA Center 機能に必要です。機能していないことが判明した場合には、[キャンセル (Cancel)] を選択し、すぐに設定を終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に「[事前設定チェックの実行](#)」に記載されているすべての手順が完了していることを確認してください (詳細については『[リリースノート](#)』の「Cisco TAC 空サポートを受ける」の項を参照してください)。

ステップ 5 ウィザードでは、まず 10 Gbps クラスタポート (ポート 2、enp10s0) が検出され、[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）。

STEP #4	NETWORK ADAPTER #1 (enp10s0)
<p>The wizard has discovered 4 physical network adapter(s) installed on the appliance.</p> <p>Enter the network settings for the 1st network adapter (00:be:27:00:00:00 - enp10s0).</p> <p>Select "Cluster Link" if used for cluster communication.</p> <hr/>	<p>Host IP Address: 192.192.192.16</p> <p>Netmask: 255.255.255.0</p> <p>Default Gateway IP Address:</p> <p>DNS Servers:</p> <p>Static Routes:</p> <p><input checked="" type="checkbox"/> Cluster Link</p> <p><< back < cancel ></p>

次の表に示すように、[NETWORK ADAPTER #1]の設定値を入力します。

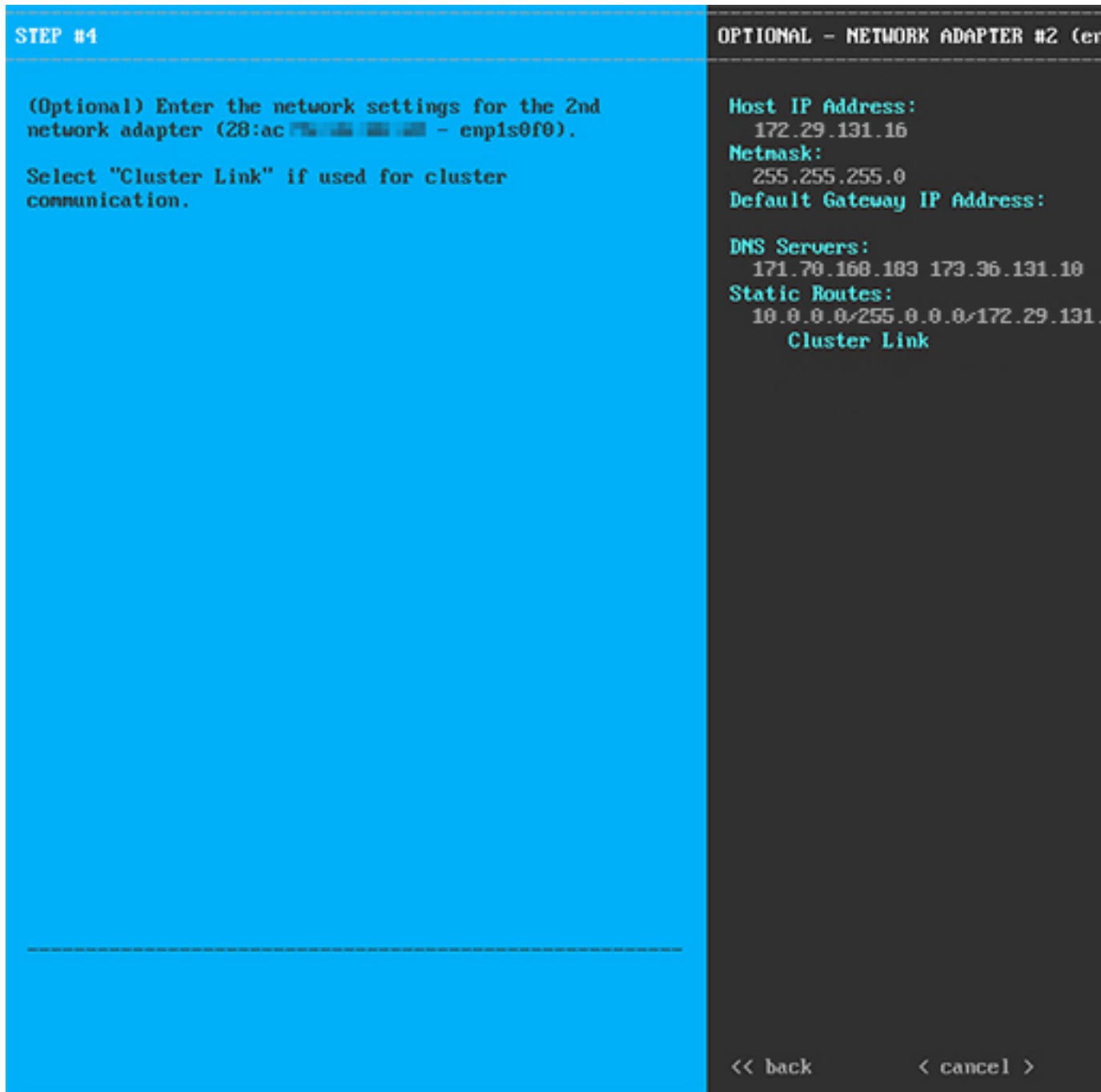
表 24: ネットワークアダプタ #1 のアドオンノードエントリ: 10 Gbps クラスポート (enp10s0)

ホスト IP アドレス	クラスポートの IP アドレスを入力します。これは必須です。クラスポートのアドレスは後で変更できないことに注意してください。
Netmask	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルトゲートウェイ IP アドレス	<p>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。</p> <p>重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。</p>
DNS Servers	<p>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。</p> <p>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。</p>
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク><ゲートウェイ>の形式で入力します。このスタティックルートは、通常、Cisco DNA Center GUI ポートでのみ必要になります。
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。この操作はクラスポートでのみ必要になります。

設定値の入力が完了したら、[next >>] をクリックして続行します。入力した値がウィザードによって検証され、正しくない値が含まれていた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 [<< back] をクリックして再入力します。

ステップ 6 入力したクラスポート値の検証が成功すると、ウィザードに 1 Gbps Cisco DNA Center GUI ポート (1、enp1s0f0) が [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）。



次の表のとおり [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 25: ネットワークアダプタ #2のアドオンノードエントリ: 1 Gbps GUI ポート (enp1s0f0)

ホスト IP アドレス	1 Gbps GUI ポートの IP アドレスを入力します。これは、GUI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。
Netmask	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	<p>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。</p> <p>重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。</p>
DNS Servers	<p>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。</p> <p>重要</p> <ul style="list-style-type: none"> • 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、<ネットワーク><ネットマスク><ゲートウェイ> の形式で入力します。
クラスタリンク	このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

必要な情報を入力したら [Next >>] をクリックして続行します。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 Cisco DNA Center GUI ポート値が正常に検証されると、ウィザードに 1 Gbps クラウドポート (2、enp1s0f1) が [NETWORK ADAPTER #3] として表示されます。「**インターフェイスクーブル接続**」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 (ポート1、enp9s0) 経由でリンクを実行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)。

STEP #4	OPTIONAL - NETWORK ADAPTER #3 (en
<p>(Optional) Enter the network settings for the 3rd network adapter (28:ac:80:00:00:00 - enp1s0f1). Select "Cluster Link" if used for cluster communication.</p> <hr/>	<p>Host IP Address: Netmask: Default Gateway IP Address: DNS Servers: Static Routes: Cluster Link</p> <p><< back < cancel ></p>

次の表のとおり [NETWORK ADAPTER #3]の設定値を入力します。

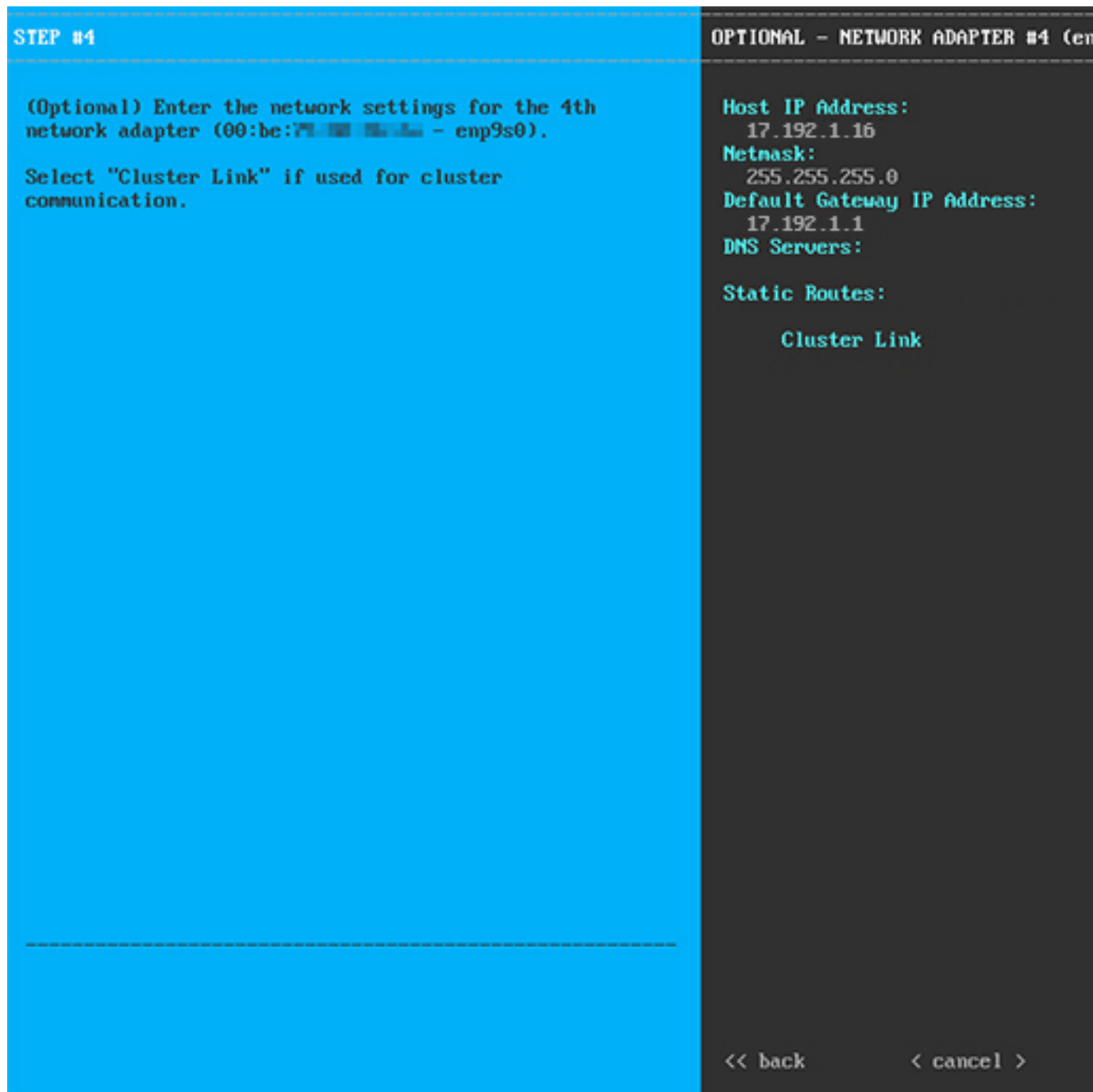
表 26: ネットワークアダプタ #3のアドオンノードエントリ: 1 Gbps クラウドポート (enp1s0f1)

ホスト IP アドレス	クラウドポートの IP アドレスを入力します。この操作はインターネット接続にクラウドポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにしておくことができます。
Netmask	ポートの IP アドレスに対応するネットマスクを入力します。この操作は IP アドレスを入力する場合に必要になります。
デフォルトゲートウェイ IP アドレス	クラウドポートに使用するデフォルトゲートウェイの IP アドレスを入力します。 重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。
DNS Servers	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 重要 クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク><ゲートウェイ>の形式で入力します。このスタティックルートは、通常、GUI ポートでのみ必要になります。
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。

必要な情報を入力したら [Next >>] をクリックして続行します。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** 入力したクラウドポート値が正常に検証されると、ウィザードに 10 Gbps エンタープライズポート (ポート 1、enp9s0) が [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

まず（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）。



次の表のとおり [NETWORK ADAPTER #4] の設定値を入力します。

表 27: ネットワークアダプタ #4 のアドオンノードエントリ: 10 Gbps エンタープライズポート (enp9s0)

ホスト IP アドレス	10 Gbps エンタープライズポートの IP アドレスを入力します。これは必須です。
Netmask	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルトゲートウェイ IP アドレス	<p>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。</p> <p>重要 アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。</p>
DNS Servers	<p>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。</p> <p>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。</p>
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ>の形式で入力します。このスタティックルートは、通常、GUI ポートでのみ必要になります。
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。

必要な情報を入力したら [Next >>] をクリックして続行します。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、ユーザの使用する [NETWORK PROXY] の設定値を入力するようウィザードから求められます。



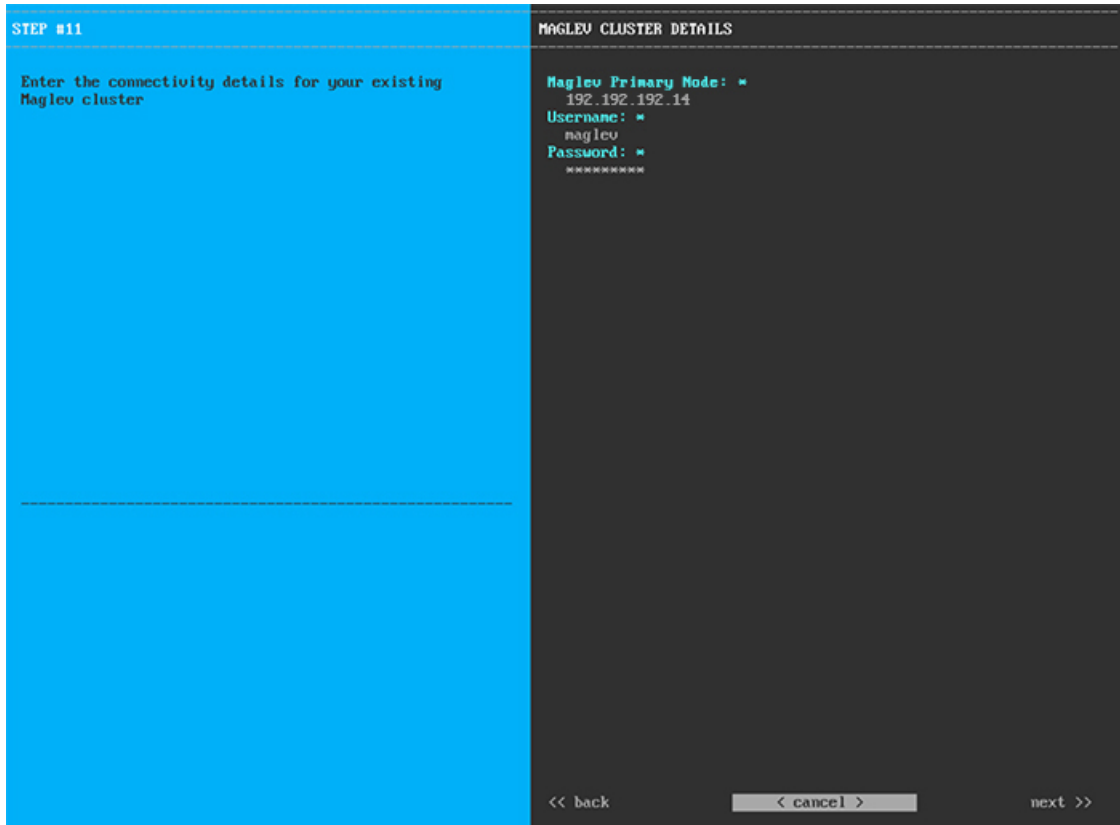
次の表に示すように [NETWORK PROXY] の設定値を入力します。

表 28: 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不要な場合には、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不要な場合には、このフィールドを空白のままにします。

必要な情報を入力したら [Next>>] をクリックして続行します。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 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。



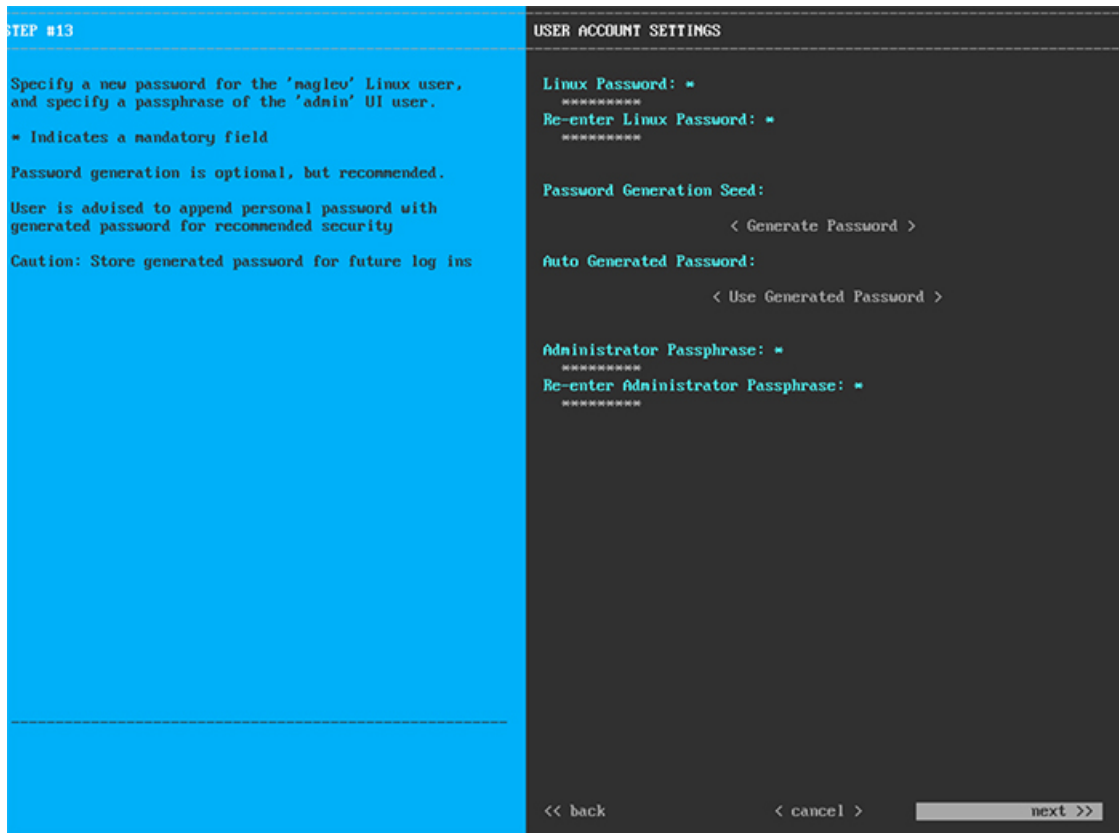
次の表の説明に従って、[MAGLEV クラスタの詳細 (MAGLEV CLUSTER DETAILS)] に値を入力します。

表 29: Maglev クラスタの詳細へのアドオンノードエントリ

[Maglev Primary Node]	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、この IP アドレスはプライマリノード上のポート 2、enp10s0、ネットワークアダプタ #1 の IP アドレスです。
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。

必要な情報を入力したら [Next>>] をクリックして続行します。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。



次の表のとおり [ユーザアカウント設定 (USER ACCOUNT SETTINGS)] の値を入力します。

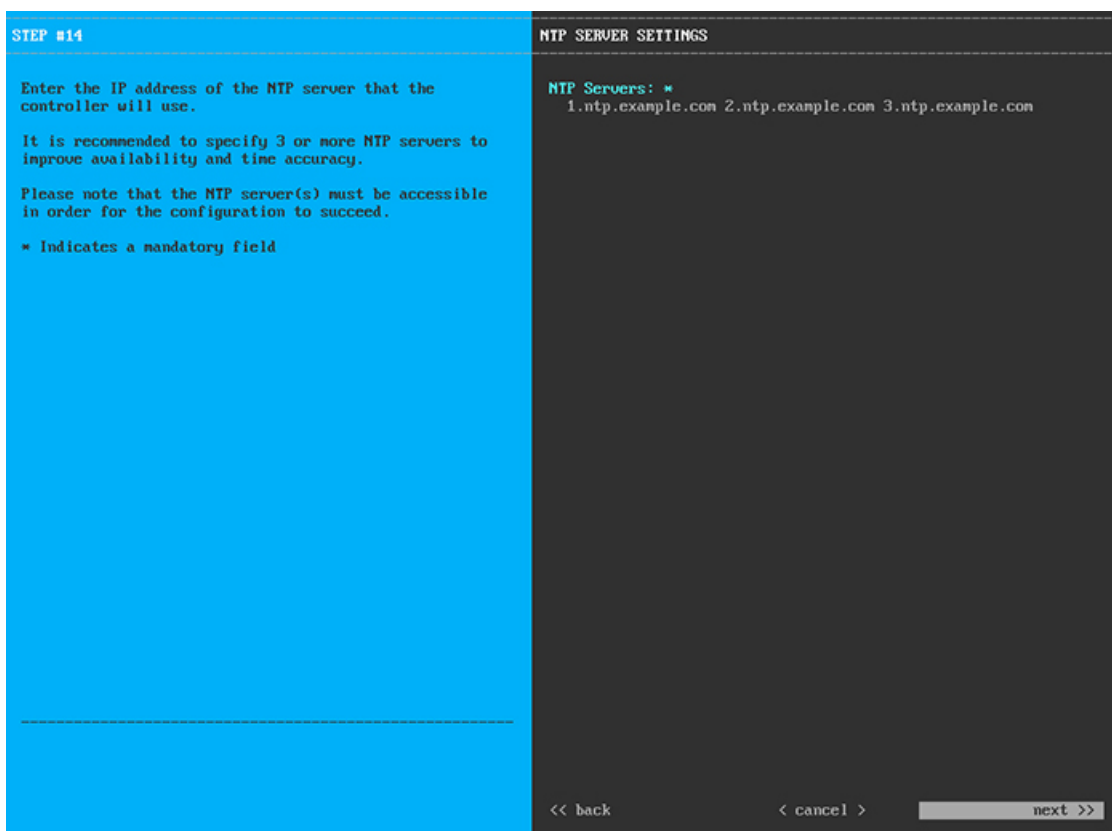
表 30: ユーザアカウント設定のアドオンノードエントリ

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、 [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>] をクリックしてパスワードを保存します。

管理者パスワード	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。
管理者パスワードの再入力	管理者パスワードをもう一度入力して確認します。

必要な情報を入力したら **[Next>>]** をクリックして続行します。以前の画面でしたように、検証エラーを修正します。

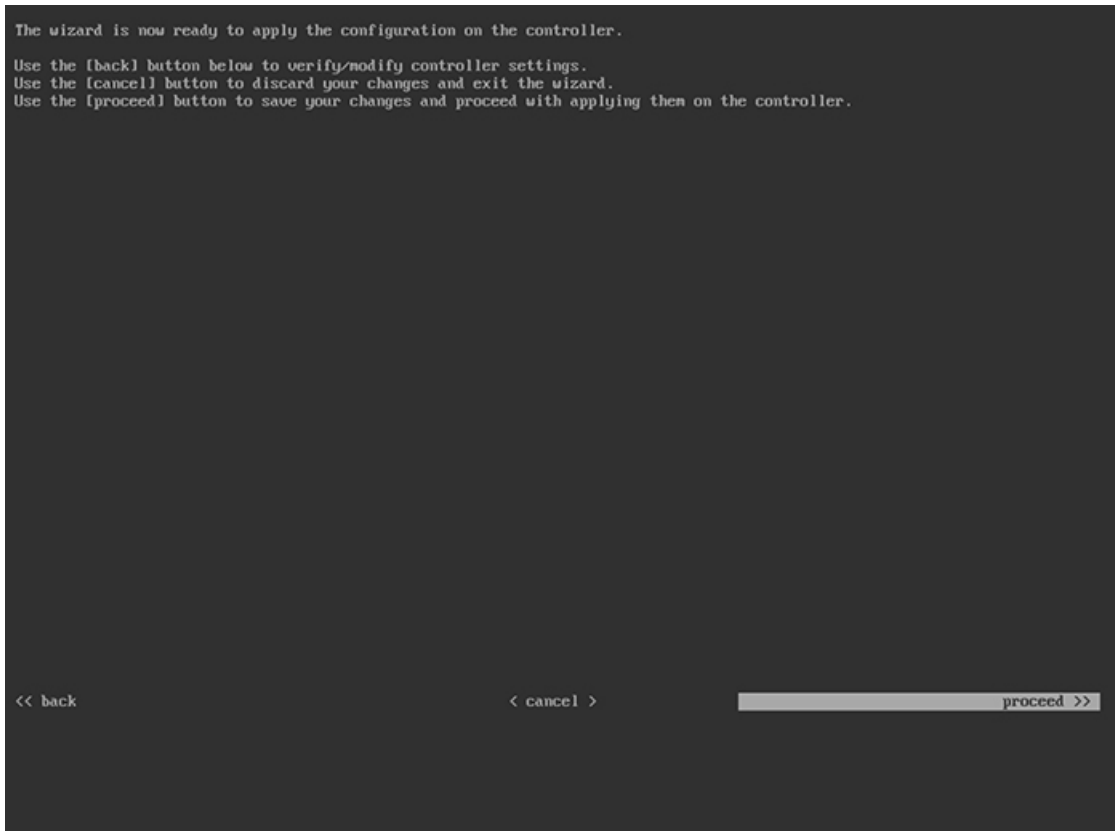
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように **[NTP SERVER SETTINGS]** の値を入力するようウィザードからメッセージが表示されます。



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。

必要な情報を入力したら **[Next>>]** をクリックして続行します。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、ウィザードで設定を適用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（以下参照）。



[Proceed >>] をクリックして、設定ウィザードを完了します。

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

- 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](#)」）を実行します。

最新の Cisco DNA Center リリースへのアップグレード

Cisco DNA Center の現在のリリースへのアップグレードの詳細については、『[Cisco DNA Center Upgrade Guide](#)』 [英語] を参照してください。



第 6 章

初期設定の完了

- [初期設定ワークフロー](#) (109 ページ)
- [互換性のあるブラウザ](#) (109 ページ)
- [初回ログイン](#) (110 ページ)
- [Cisco ISE と Cisco DNA Center の統合](#) (112 ページ)
- [認証サーバとポリシーサーバの設定](#) (119 ページ)
- [SNMP プロパティの設定](#) (121 ページ)

初期設定ワークフロー

インストールしたすべての Cisco DNA Center アプライアンスの設定が完了したら、この章で説明するタスクを実行して、Cisco DNA Center を実稼働に使用する準備をします。次の点に注意してください。

- 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。
- 実稼働環境に高可用性 (HA) を展開している場合、HA の動作を最適化するためにクラスターノード間でサービスを再配布する必要があります ([高可用性のアクティブ化 \(131 ページ\)](#) を参照)。アプライアンスの SNMP 設定を行った後、この手順を完了します。

互換性のあるブラウザ

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

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

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

初回ログイン

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

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

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

始める前に

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

- 「[プライマリノードの設定](#)」の手順に従って指定した *admin* スーパーユーザのユーザ名とパスワード。
- [必要な初期設定情報](#) に記載されている必要な情報。

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

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

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

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

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

次のメッセージが表示されます。

- Google Chrome :

```
This server could not prove that it is GUI-IP-address; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.
```
- Mozilla Firefox :

Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust *GUI-IP-address* because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。Cisco DNA Center での証明書の使用方法については、『[Cisco Digital Network Architecture Center 管理者ガイド](#)』の「証明書と秘密キーのサポート」の項を参照してください。

ステップ 4 メッセージを無視し、次のいずれかを実行します。

- Google Chrome : *GUI-IP-address* (安全でない) リンクをクリックして開きます。
- Mozilla Firefox : [リスクを理解して続行する (Accept the Risk and Continue)] をクリックします。

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

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

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

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

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

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

Cisco.com ユーザログインが既知の 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、対応するリンクをクリックして新しいスマートアカウントを開きます。完了したら [次へ (Next)] をクリックします。

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

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

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

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

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

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

ソフトウェアの **[EULA]** ウィンドウが表示されます。

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

[準備完了 (Ready to go!)] ウィンドウが表示されます。

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

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

次のタスク

残りの管理設定タスクを任意の順序で実行します。

- [Cisco ISE と Cisco DNA Center の統合](#)
- [認証サーバとポリシー サーバの設定 \(119 ページ\)](#)
- [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。

- Cisco ISE のプライマリ管理ノードにログインします。
- [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。
- 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。
- [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。
- [Administration] > [System] > [Settings]** の順に選択します。
- 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 空調 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、接続にサブスクリ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。

グループベースのアクセスコントロール：ポリシーデータの移行と同期

Cisco DNA Center の使用を開始するとき

Cisco DNA Center の以前のリリースでは、グループベースのアクセス コントロール ポリシー機能でポリシーのアクセス契約とポリシーを Cisco DNA Center ローカルに保存していました。Cisco DNA Center では同じデータを Cisco ISE にも反映します。Cisco ISE ではネットワークにランタイムポリシーサービスも提供します。その一環でグループベースのアクセスコントロールポリシーのファイルがネットワークデバイスにダウンロードされます。通常、Cisco DNA Center のポリシー情報は Cisco ISE のポリシー情報と一致します。ただし、データが同期されていない可能性があり、その場合はデータが一致していない可能性があります。このため、新規であれアップグレードであれ Cisco DNA Center をインストールした後は、グループベースのアクセスコントロール機能を使用する前に、次の手順が必要になります。

- Cisco ISE と Cisco DNA Center を統合する（未統合の場合）
- Cisco ISE をアップグレードする（必須バージョンさえない場合）。Cisco ISE の必須バージョンについては「Cisco DNA Center リリースノート」を参照してください。
- ポリシーの移行と同期の実行

「移行と同期」とは何ですか。

Cisco DNA Center は統合された Cisco ISE に含まれるグループベースのアクセス コントロールポリシー データをすべて読み取り、そのデータを Cisco DNA Center のポリシーデータと比較します。以前のバージョンからアップグレードした場合は、既存のポリシーデータが保持されます。Cisco DNA Center のグループベースのアクセスコントロールポリシーを管理するには、先にポリシーを同期しておく必要があります。

移行と同期はどのように機能しますか。

通常、Cisco ISE と Cisco DNA Center のポリシーデータは一貫しているため、データの処理や変換は特に必要ありません。ささいな不一致や不整合がある場合、移行中に一部のデータのみが変換されることがあります。競合がある場合は、ネットワーク内でポリシーの挙動が変わらないように Cisco ISE のデータが優先されます。次のリストは、移行中に実行されるアクションを示しています。

- スケーラブルグループ (Scalable Groups) : スケーラブルグループタグ (SGT) (数値) は、スケーラブルグループを一意に特定します。Cisco ISEセキュリティグループが Cisco DNA Center のスケーラブルグループと比較されます。
 - 名前と SGT の値が同じであれば、何も変更されません。Cisco DNA Center の情報は Cisco ISE と一貫性があり、変更する必要はありません。
 - Cisco ISE セキュリティグループの SGT 値が Cisco DNA Center に存在しない場合は、Cisco DNA Center に新しいスケーラブルグループが作成されます。新しいスケーラブルグループには「Default_VN」のデフォルトの関連付けが施されます。
 - Cisco ISE セキュリティグループの SGT 値が Cisco DNA Center に存在しているが、名前が一致しない場合は、Cisco ISE セキュリティグループの名前が Cisco DNA Center のスケーラブルグループの名前に置き換えられます。
 - Cisco ISE セキュリティグループの名前が同じであるが、SGT 値が異なる場合は、Cisco ISE からセキュリティグループが移行されます。この処理では名前とタグの値は保持されますが、Cisco DNA Center スケーラブルグループの名前は変更されます。「_DNA」というサフィックスが追加されます。

契約

ポリシーの参照する Cisco ISE の SGACL はすべて、Cisco DNA Center の契約と比較されます。

- SGACL と契約の名前と内容が同一の場合、それ以上のアクションは必要ありません。Cisco DNA Center の情報は Cisco ISE と一貫性があり、変更する必要はありません。
 - SGACL と契約の名前が同一で、内容が異なっている場合は、Cisco ISE から SGACL の内容が移行されます。Cisco DNA Center の以前の契約内容は破棄されます。

SGACL が Cisco DNA Center に存在しない場合、その名前で作成された新しい契約が作成され、Cisco ISE から SGACL の内容が移行されます。



- (注) Cisco ISE SGACL の内容に沿って新しいアクセス契約を作成する場合は、Cisco DNA Center がテキストコマンドラインが解析され、これらの SGACL コマンドが可能な限りアクセス契約モデルとしてレンダリングされます。ACE行がそれぞれ「高度な」アプリケーション行としてレンダリングされます。Cisco ISE SGACL に正常に解析できないテキストが含まれている場合、SGACL テキストの内容はモデル化された形式に変換されません。これは raw コマンドラインテキストとして保存されます。この SGACL 契約文は編集できますが、移行中、テキストの内容の解析または構文チェックは実行されません。

ポリシー

ポリシーは、送信元グループと宛先グループのペアで一意に識別されます。すべての Cisco ISE TrustSec イーグレス ポリシー マトリックス ポリシーが、Cisco DNA Center のポリシーと比較されます。

- 送信元グループと宛先グループのポリシーで Cisco ISE の同じ SGACL または契約名を参照している場合、変更は行われません。
- 送信元グループと宛先グループのポリシーで Cisco ISE の別の SGACL または契約名を参照している場合、ポリシーでは Cisco ISE の契約名が参照されます。この結果、Cisco DNA Center で以前の契約参照が上書きされます。
- Cisco ISE のデフォルトポリシーがチェックされ、Cisco DNA Center に移行されます。



- (注) Cisco DNA Center はアクセスポリシー内のいずれか 1つの契約をサポートします。Cisco ISE にはアクセスポリシーで複数の SGACL を使用するオプションがありますが、ISE ではこのオプションがデフォルトでは無効であり、広く一般的には使用されていません。以前のリリースの Cisco DNA Center を使用してグループベースのアクセス コントロール ポリシーを管理していた既存の SDA のお客様は、このオプションを使用しないでください。

Cisco ISE で複数の Sgacl を許可するオプションを有効にしてポリシー作成時に使用した場合、これらのポリシーはこのリリースでは Cisco DNA Center に移行できません。移行できない [multiple SGACL] オプションを利用する特定のポリシー機能は次のとおりです。

- ポリシー内で複数の SGACL
- ポリシーレベルの catch-all ルールは [Permit] または [Deny] に設定されています現在の移行では [None] の値のみ Cisco DNA Center サポートされています。
- 顧客が作成した SGACL を使用するよう設定されたデフォルトポリシー。ただし現在、Cisco DNA Center への移行では、[Permit IP]、[Permit_IP_Log]、[Deny IP]、[Deny_IP_Log] の標準値のみサポートされています。

ポリシー移行と同期の操作中に先行する SGACL が何か検出された場合は、通知が生成されます。続行するには、次のオプションの中から選択する必要があります。

- **Cisco DNA Center** でのグループベースアクセスコントロールポリシーを管理：このオプションが選択されている場合は、Cisco DNA Center でグループベースのアクセスコントロールポリシーの管理がすべて実行されます。Cisco ISE セキュリティグループ、SGCAL、イーグレスポリシーを管理する Cisco ISE のユーザインターフェイス画面は、読み取り専用モードで使用できます。（Cisco ISE で複数の SGACL を使用しているために）ポリシーの移行中に問題が生じた場合、これらのポリシーには Cisco DNA Center で選択した契約が含まれなくなります。このポリシーではデフォルトポリシーが使用され、移行が完了したら、そのポリシーに対応する契約を新しく選択できます。デフォルトポリシーの移行中に問題が発生した場合は、デフォルトポリシーが [許可 (Permit)] に設定されます。
- **Cisco ISE** でのグループベースアクセスコントロールポリシーを管理 (Manage Group-Based Access Control Policy)：このオプションが選択されている場合は、Cisco DNA Center グループベースのアクセスコントロールポリシーの管理がすべて非アクティブになります。Cisco ISE は変更されず、ネットワーク内のポリシーの適用には影響しません。グループベースのアクセスコントロールポリシーは、TrustSec ワークセンターの Cisco ISE で管理されます。
- **Cisco DNA Center** と **Cisco ISE** の両方でグループベースのアクセスコントロールポリシーを管理するにはこのオプションは Cisco ISE で加えられたポリシー変更が Cisco DNA Center と同期されないため、一般的な使用には推奨されません。2つのシステムを常に同期しておくことはできません。このオプションは短期または暫定オプションとして意図されており、Cisco ISE で [Allow Multiple SQUAD] オプションを有効にした場合にのみ考慮する必要があります。Cisco ISE の更新でより多くの時間と一段と優れた柔軟性が必要になった場合に使用できます。

認証サーバとポリシーサーバの設定

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

始める前に

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

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして システム > 設定 > 外部サービスの > 認証およびポリシーサーバ。

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 100 文字です。

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

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

- **ユーザ名 (Username)** : Cisco ISE CLI へのログインに使用する名前です。
(注) このユーザにはスーパーユーザの管理権限が必要です。
- **パスワード (Password)** : Cisco ISE CLI ユーザ名のパスワード。
- **FQDN - Cisco ISE サーバの FQDN**。
(注)
 - Cisco ISE ([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、ホスト名とドメイン名の 2 つのパートで構成されています。

hostname.domainname.com。

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

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

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

ステップ5 [Advanced Settings] スライダをクリックして [On] の位置に移動し、次のように設定します。

(注) 必要な設定は、サーバのプロトコル設定によって異なります。

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

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

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

ステップ 6 [Apply] をクリックします。

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

SNMP プロパティの設定

SNMP の再試行とタイムアウトの値を設定できます。

始める前に

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

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **システム (System) > 設定 (Settings) > デバイス設定 (Device Settings) > SNMP**

ステップ 2 次のフィールドを設定します。

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

ステップ3 [保存 (Save)]をクリックします。

(注) デフォルトの設定に戻すには、[リセットして保存 (Reset and Save)]をクリックします。



第 7 章

展開のトラブルシューティング

- [トラブルシューティング タスク \(123 ページ\)](#)
- [ログアウト \(123 ページ\)](#)
- [設定ウィザードを使用したアプライアンスの再設定 \(124 ページ\)](#)
- [アプライアンスの電源の入れ直し \(126 ページ\)](#)

トラブルシューティング タスク

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

1. 現在、Cisco DNA Center GUI を使用している場合は、[ログアウト](#)。
2. アプライアンスのハードウェアを再設定するには、「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」のステップ 12 および 13 の説明に従って、Cisco IMC 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 \(126 ページ\)](#))。

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 シリーズ サーバ Integrated Management Controller GUI コンフィギュレーション ガイド リリース 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、Cisco IMC GUI または Maglev 設定ウィザードのみを使用します。

ログアウト

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

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

ステップ 1 メニューアイコン (☰) 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には、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。

アプライアンスの設定が終わると、設定ウィザードではすべてのアプライアンス設定を変更できなくなります。変更は次の設定のみに制限されます。

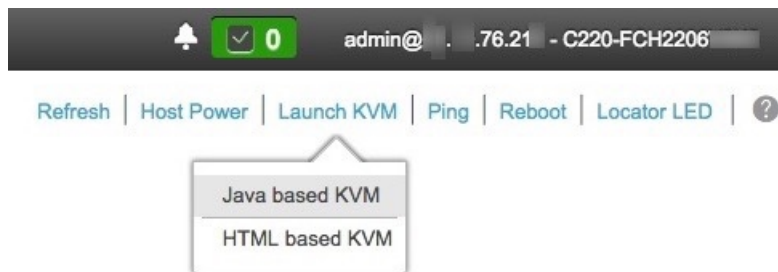
- アプライアンスのホスト IP アドレス
- DNS サーバの IP アドレス
- デフォルトゲートウェイ IP アドレス
- NTP サーバの IP アドレス
- クラスタ仮想 IP アドレス (Cluster Virtual IP address)
- クラスタホスト名 (FQDN)
- スタティック ルート
- プロキシサーバの IP アドレス
- Maglev ユーザのパスワード
- 管理ユーザのパスワード。

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 お使いのブラウザで、実行した `cisco imc` GUI 設定で設定した Cisco IMC の IP アドレスをポイントし、`cisco imc` ユーザとして Cisco IMC GUI にログインします (「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」を参照)。

ログインが成功すると、次に示すように、アプライアンスに **[Cisco Integrated Management Controller Chassis 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 ハイパーリンクメニューで **[Launch KVM]** を選択してから **[Java based KVM]** と **[HTML based KVM]** のいずれかを選択します。**[Java-based 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。**[HTML-based 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 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。表示された設定を適宜変更します。画面ごとに変更を終えたら **[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、「**CONFIGURATION SUCCEEDED**」というメッセージが表示されます。

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

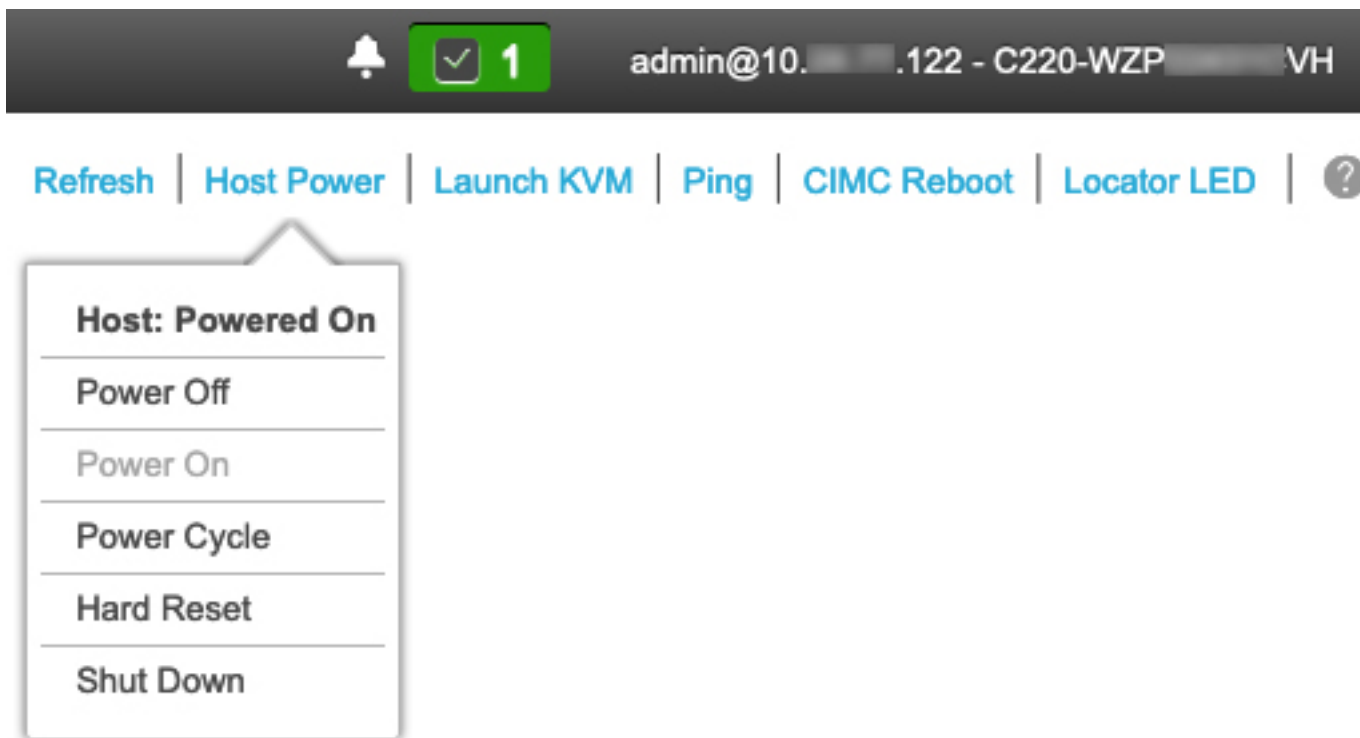
Cisco IMC GUI を使用して行ったハードウェアの変更は、アプライアンスのリブート後に適用されることに注意してください。



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 ([Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(51 ページ\)](#) 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 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 \(2 ページ\)](#) の背面パネル図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があるアプライアンスのエンタープライズポートの IP アドレスにログインします。

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

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

ステップ 3 実行するタスクに適したコマンドを入力します。

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

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

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

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



付録 **A**

ハイアベイラビリティクラスタの展開シナリオの確認

Cisco DNA Center の高可用性 (HA) の実装については、『[Cisco DNA Center High Availability 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。これを選択する場合は、次のタスクを実行します。

1. 次のとおりネットワークに適した導入手順を実行します。
 - [新しい HA の展開](#)
 - [標準インターフェイス設定を使用した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](#)
2. Cisco DNA Center クラスタで[高可用性のアクティブ化](#)を行います。
3. [HA の展開に関する追加の考慮事項](#)を参照し、必要な追加の設定を行います。
 - [新しい HA の展開 \(129 ページ\)](#)
 - [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 \(130 ページ\)](#)
 - [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 \(130 ページ\)](#)
 - [高可用性のアクティブ化 \(131 ページ\)](#)
 - [HA の展開に関する追加の考慮事項 \(131 ページ\)](#)

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 2.1.2 にアップグレードします。

Cisco DNA Center の現在のリリースへのアップグレードの詳細については、『[Cisco DNA Center Upgrade Guide](#)』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（仮想 IP アドレスがまだ追加されていない場合）。

「[設定ウィザードを使用したアプライアンスの再設定](#)」を参照してください。

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

「[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 2.1.2 にアップグレードします。

Cisco DNA Center の現在のリリースへのアップグレードの詳細については、『[Cisco DNA Center Upgrade Guide](#)』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ー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。

「[インターフェースケーブル接続](#)」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使用して、リモートリポジトリのデータを復元します。

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

「[アドオンノードの設定](#)」を参照してください。

高可用性のアクティブ化

Cisco DNA Center の HA の実装については、『[Cisco DNA Center High Availability 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。展開する場合は、次の手順を実行します。

1. Cisco DNA Center GUI で、**[Menu]** アイコン (☰) をクリックし、**[System] > [Settings] > [System Configuration] > [High Availability]** の順に選択します。
2. **[Activate High Availability]** をクリックします。

[Activate High Availability] をクリックすると、Cisco DNA Center は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 のアクティブ化を実行するたび、(前述のとおり) メンテナンスモードになります。

HA の展開に関する追加の考慮事項

既存の HA の導入では、次の追加設定を行う必要があります。



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

テレメトリ

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

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

ステップ 2 デバイスでテレメトリを無効にします。

1. Cisco DNA Center ホームページで **[Tools]** エリアの **[Network Telemetry]** を選択します。
[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、**[Actions]** > **[Disable Telemetry]** を選択します。

ステップ 3 以前デバイスに関連付けたプロファイルを使用して、テレメトリをもう一度有効にします。

ワイヤレスコントローラ

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

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。