



Cisco DNA Center 第2世代アプライアンスリリース 2.3.5 設置ガイド

初版：2022年12月21日

最終更新：2023年12月7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)

© 2022–2023 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 5
	物理仕様 22
	環境仕様 23
	電力仕様 24

第 2 章	導入の計画 27
	プランニング ワークフロー 27
	Cisco DNA CenterおよびCisco Software-Defined Access 28
	インターフェイスクーブル接続 28
	必要な IP アドレスおよびサブネット 33
	必要なインターネット URL と完全修飾ドメイン名 38
	インターネットへのアクセスを保護する 41
	必要なネットワークポート 41
	必要なポートとプロトコル： Cisco Software-Defined Access 44
	必須の設定情報 52
	必要な初期設定情報 53

第 3 章	アプライアンスの設置 57
	アプライアンスのインストール ワークフロー 57
	アプライアンスを開梱して点検 57
	インストール警告とガイドラインの確認 58
	ラック要件の確認 60

アプライアンスの接続および電源投入 61

LED の確認 61

第 4 章

アプライアンスの設定準備 67

アプライアンス設定の準備の概要 67

Cisco Integrated Management Controller に対するブラウザアクセスの有効化 68

事前設定タスクの実行 73

NIC ボンディングの概要 77

アプライアンスサポート 78

アップグレードされたアプライアンスでの NIC の有効化 79

アプライアンスのイメージの再作成 86

Cisco DNA Center イメージの確認 86

ブート可能な USB フラッシュドライブの作成 87

Etcher の使用 88

Linux CLI の使用 89

Mac CLI の使用 89

Cisco DNA Center アプライアンスの仮想ドライブの再初期化 90

Cisco DNA Center ISO イメージのインストール 90

Cisco DNA Center アプライアンスの設定 91

第 5 章

Maglev ウィザードを使用したアプライアンスの設定 93

アプライアンスの設定の概要 93

Maglev ウィザードを使用したプライマリノードの設定 94

FIPS モードのサポート 116

Maglev ウィザードを使用したセカンダリノードの設定 117

最新の Cisco DNA Center リリースへのアップグレード 139

第 6 章

ブラウザベースのウィザードを使用した 44/56 コアアプライアンスの設定 141

アプライアンスの設定の概要 141

ブラウザベースの構成ウィザード 141

ブラウザベースのウィザードの前提条件 142

インストール構成ウィザードを使用したアプライアンスの設定	143
詳細インストール構成ウィザードを使用したプライマリノードの設定	157
詳細インストール構成ウィザードを使用したセカンダリノードの設定	178
最新の Cisco DNA Center リリースへのアップグレード	199

第 7 章

ブラウザベースのウィザードを使用した 112 コアアプライアンスの設定	201
アプライアンスの設定の概要	201
ブラウザベースの構成ウィザード	201
ブラウザベースのウィザードの前提条件	202
インストール構成ウィザードを使用したアプライアンスの設定	203
詳細インストール構成ウィザードを使用したプライマリノードの設定	218
詳細インストール構成ウィザードを使用したセカンダリノードの設定	238
最新の Cisco DNA Center リリースへのアップグレード	258

第 8 章

初期設定の完了	259
初期設定ワークフロー	259
互換性のあるブラウザ	259
クイック スタート ワークフローの完了	260
Cisco ISE と Cisco DNA Center の統合	265
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	270
認証サーバとポリシー サーバの設定	273
SNMP プロパティの設定	277

第 9 章

展開のトラブルシューティング	279
トラブルシューティング タスク	279
ログアウト	279
設定ウィザードを使用したアプライアンスの再設定	280
アプライアンスの電源の再投入	282
Cisco IMC GUI を使用	282
SSH を使用	283

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	285
新しい HA の展開	285
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	286
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	287
HA のアクティブ化	288
HA の展開に関する追加の考慮事項	288
テレメトリ	289
ワイヤレス コントローラ	289



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 \(5 ページ\)](#)
- [物理仕様 \(22 ページ\)](#)
- [環境仕様 \(23 ページ\)](#)
- [電力仕様 \(24 ページ\)](#)

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 2 世代の Cisco DNA Center アプライアンスは、Cisco Unified Computing System (UCS) C220 M5 小型フォームファクタ (SFF) シャーシまたは Cisco UCS C480 M5 シャーシのいずれかで構成されています。両方とも 1 つの INTEL X710-DA2 ネットワーク インターフェイス カード (NIC) と 1 つの INTEL X710-DA4 NIC が追加されています。第 2 世代アプライアンスには、次の 6 つのバージョンがあります。

- 44 コアアプライアンス : シスコ製品番号 DN2-HW-APL
- 44 コア プロモーションアプライアンス : シスコ製品番号 DN2-HW-APL-U
- 56 コアアプライアンス : シスコ製品番号 DN2-HW-APL-L
- 56 コア プロモーションアプライアンス : シスコ製品番号 DN2-HW-APL-L-U
- 112 コアアプライアンス : シスコ製品番号 DN2-HW-APL-XL
- 112 コア プロモーションアプライアンス : シスコ製品番号 DN2-HW-APL-XL-U

次の表はアプライアンスのハードウェア仕様をまとめたものです。

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

機能	説明
シャーシ	1 ラックユニット (1RU) シャーシ
プロセッサ	22 コア Intel 6238 2.1 GHz プロセッサ X 2
メモリ	32 GB DDR4 2933 MHz の登録済み DIMM (RDIMM) X 8
ストレージ	<ul style="list-style-type: none"> • RAID 1 で 480 GB X 2 • RAID 1 で 1.9 TB X 2 • RAID 10 で 1.9 TB X 6
ディスク管理 (RAID)	<ul style="list-style-type: none"> • スロット 1 ~ 4 の RAID 1 • スロット 5 ~ 10 の RAID 10
ネットワークおよび管理 I/O	<p>サポートされるコネクタ：</p> <ul style="list-style-type: none"> • Intel X710-DA2 NIC 上の 10 Gbps イーサネットポート X 2 • 1 Gbps RJ-45 管理ポート (Marvell 88E6176) X 1 • 10GBase-T LOM ポート (マザーボードに Intel X550 コントローラを搭載) X 2 • Intel X710-DA4 NIC 上の 1 Gbps/10 Gbps イーサネットポート X 4 <p>(注) これらのポートは、アプライアンスで NIC ボンディングが有効になっている場合にのみアクティブになります。詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p> <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 • VGA (DB-15) コネクタ X 1 • USB 3.0 コネクタ X 2 • USB 2.0 2 個、VGA (DB-15) 1 個、シリアル (RS-232) RJ-45 コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1
電源	<p>770 W AC 電源 X 2。</p> <p>1+1 の冗長構成。</p>
冷却	ホットスワップ可能なファン モジュール (前面から背面に向かう冷却用) X 7。

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

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

機能	説明
シャーシ	1 ラックユニット (1RU) シャーシ
プロセッサ	28 コア Intel 8280 2.7 GHz プロセッサ X 2
メモリ	32 GB DDR4 2933 MHz RDIMM X 12
ストレージ	<ul style="list-style-type: none"> RAID 1 で 480 GB X 2 RAID 1 で 1.9 TB X 2 RAID 10 で 1.9 TB X 6
ディスク管理 (RAID)	<ul style="list-style-type: none"> スロット 1 ~ 4 の RAID 1 スロット 5 ~ 10 の RAID 10
ネットワークおよび管理 I/O	<p>サポートされるコネクタ：</p> <ul style="list-style-type: none"> Intel X710-DA2 NIC 上の 10 Gbps イーサネットポート X 2 1 Gbps RJ-45 管理ポート (Marvell 88E6176) X 1 10GBase-T LOM ポート (マザーボードに Intel X550 コントローラを搭載) X 2 Intel X710-DA4 NIC 上の 1 Gbps/10 Gbps イーサネットポート X 4 <p>(注) これらのポートは、アプライアンスでNICボンディングが有効になっている場合にのみアクティブになります。詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p> <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 VGA (DB-15) コネクタ X 1 USB 3.0 コネクタ X 2 USB 2.0 2 個、VGA (DB-15) 1 個、シリアル (RS-232) RJ-45 コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1

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

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

機能	説明
シャーシ	4 ラックユニット（4RU）シャーシ。
プロセッサ	2 個の 28 コア Intel 8276 2.2 GHz プロセッサを搭載した CPU モジュール X 2
メモリ	32 GB DDR4 2933 MHz RDIMM X 24
ストレージ	<ul style="list-style-type: none"> • RAID 1 で 480 GB X 2 • RAID 1 で 3.8 TB X 2 • 1.9 TB（RAID 10） X 16
ディスク管理（RAID）	<ul style="list-style-type: none"> • ドライブベイ 1 および 2 の RAID 1 • スロット 3 ~ 18 の RAID 10 • ドライブベイ 19 および 20 の RAID 1

機能	説明
ネットワークおよび管理 I/O	<p>サポートされるコネクタ：</p> <ul style="list-style-type: none"> • Intel X710-DA2 NIC 上の 10 Gbps イーサネットポート X 2 • 10 Base-T Gbps イーサネットポート X 2 • 1 ギガビットイーサネット管理ポート • Intel X710-DA4 NIC 上の 1 Gbps/10 Gbps イーサネットポート X 4 <p>(注) これらのポートは、アプライアンスでNICボンディングが有効になっている場合にのみアクティブになります。詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p> <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 • VGA (DB-15) コネクタ X 1 • USB 3.0 コネクタ X 3 • USB 2.0 2 個、VGA (DB-15) 1 個、シリアル (RS-232) RJ-45 コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1
電源	<p>1600 W AC 電源装置 X 4。</p> <p>3+1 の冗長構成 (Cisco Integrated Management Controller での設定が必須)。</p>
冷却	<p>前面から背面冷却のそれぞれに 2 個のファンがある 4 個ホットスワップファンモジュールです。</p>
ビデオ	<p>60 Hz で最大 1600 X 1200、16 bpp の VGA ビデオ解像度、最大 256 MB のビデオメモリ。</p>

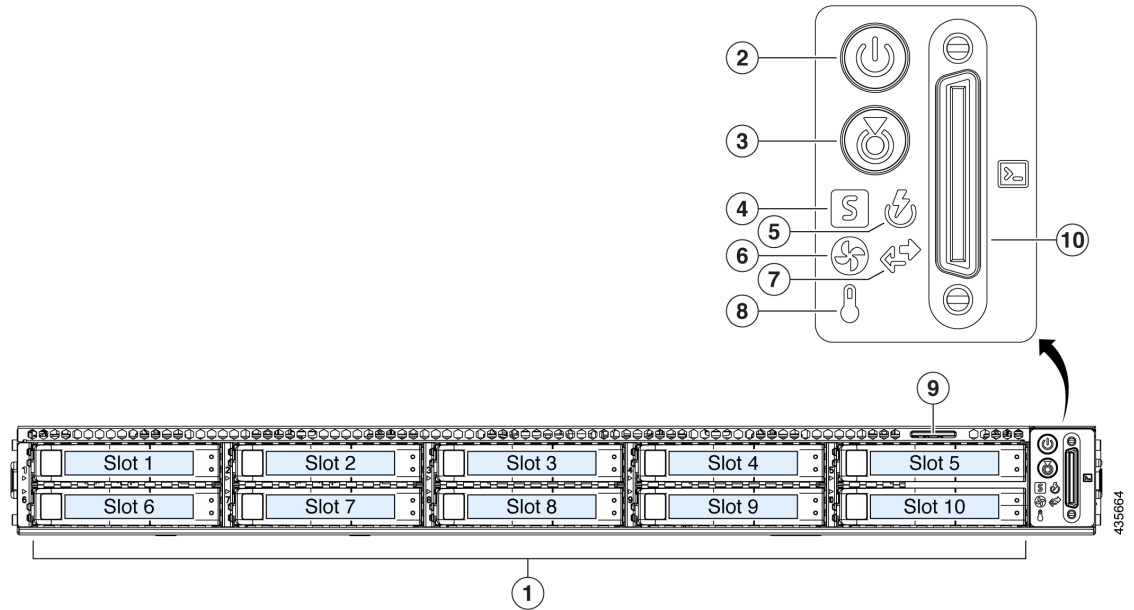
前面パネルと背面パネル

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



(注) [cisco.com](https://www.cisco.com) でこのガイドを表示している場合は、図のいずれかをクリックすると、フルサイズバージョンが表示されます。

図 1: 44 および 56 コアアプライアンスの前面パネル

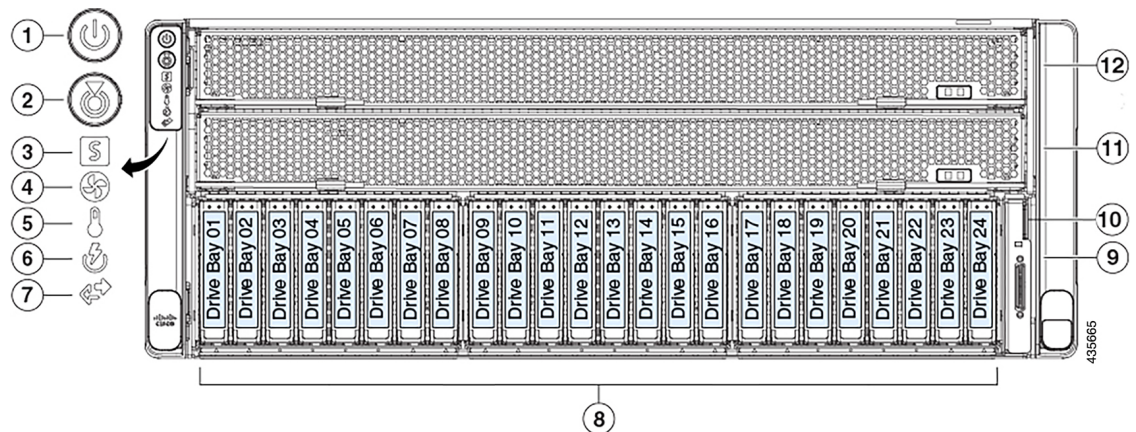


コンポーネント	説明
1	<p>このアプライアンスでは次のとおり合計 10 個のドライブを使用できます。</p> <ul style="list-style-type: none"> • 480 GB SAS SSD X 2 (スロット 1 および 2)。 • 1.9 TB SATA SSD X 8 (スロット 3 ~ 10)。 <p>取り付けられたドライブにはそれぞれ、障害 LED とアクティビティ LED が付いています。</p> <p>ドライブ障害 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：ドライブは正常に動作中です。 • 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。

コンポーネント	説明
2	<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 (Cisco IMC) と一部のマザーボード機能にだけ電力が供給されています。 • 緑：アプライアンスはメイン電源モードです。すべてのサーバコンポーネントに電力が供給されています。
3	<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"> • 消灯：ユニット識別機能は非アクティブです。 • 青：ユニット識別 LED はアクティブです。
4	<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 (2 回)：システムボードで重度の障害が発生しています。 • オレンジの点滅 (3 回)：メモリ (DIMM) で重度の障害が発生しています。 • オレンジの点滅 (4 回)：CPU で重度の障害が発生しています。
5	<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。

コンポーネント	説明
6	<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。
7	<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"> 消灯：イーサネットリンクがアイドル状態です。 緑の点滅：1つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。 緑：1つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。
8	<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	引き抜きアセットタグ。
10	KVM コネクタ。USB 2.0 コネクタ X 2、VGA コネクタ X 1、シリアルコネクタ X 1 を装備した KVM ケーブルで使します。

図 2: 112 コアアプライアンスの前面パネル

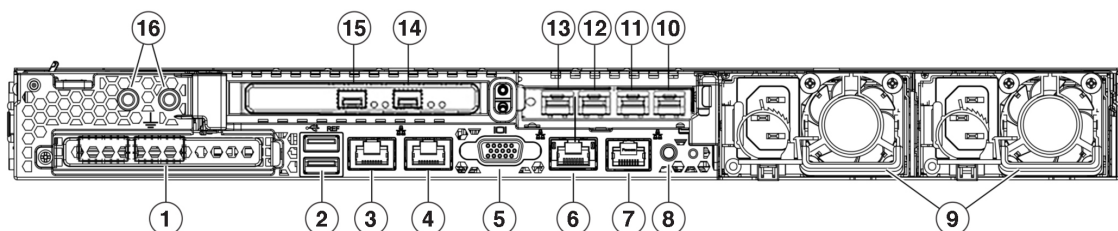


コンポーネント	説明
1	<p>電源ボタン/電源ステータス LED LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：アプライアンスに AC 電力が供給されていません。 • オレンジ：アプライアンスはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機構にだけ電源が投入されています。 • 緑：アプライアンスはメイン電源モードです。すべてのサーバコンポーネントに電力が供給されています。
2	<p>ユニット識別ボタンと LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：ユニット識別機能は非アクティブです。 • 青：ユニット識別 LED はアクティブです。
3	<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。 • 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 つ以上が原因の可能性があります。 <ul style="list-style-type: none"> • ブートの失敗 • 修復不能なプロセッサまたはバスエラーが検出された • 過熱状態
4	<p>ファンスステータス 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：ファンモジュールが縮退運転状態にあります。1 つのファンモジュールに障害があります。 • オレンジの点滅：2 つ以上のファンモジュールに障害があります。

コンポーネント	説明
5	<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。エラーが検出されませんでした。 ・ オレンジの点灯：1 つ以上の温度センサが警告しきい値を超過しています。 ・ オレンジの点滅：1 つ以上の温度センサが重要な回復不能なしきい値を超過しています。
6	<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。
7	<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"> ・ 消灯：イーサネット LOM ポートリンクがアイドル状態です。 ・ 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 ・ 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。
8	<p>このアプライアンスでは次のとおり合計 20 個のドライブを使用できます。</p> <ul style="list-style-type: none"> ・ 480 GB SATA SSD X 2（ドライブベイ 1 および 2 内）。 ・ 1.9 TB SATA SSD X 16（スロット 3～18）。 ・ 3.8 TB SATA SSD X 2（ドライブベイ 19 および 20）。 <p>（注） ドライブベイ 21～24 は、このアプライアンスでは使用されません。</p> <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。

コンポーネント	説明
9	KVM コネクタ。USB 2.0 コネクタ X 2、VGA コネクタ X 1、シリアルコネクタ X 1 を装備した KVM ケーブルで使します。
10	引き抜きアセットタグ。
11	CPU モジュールベイ 1。
12	CPU モジュールベイ 2。

図 3:44 および 56 コアアプライアンスの背面パネル



(注) Cisco DNA Center アプライアンスで NIC ボンディングが有効になっている場合は、エンタープライズ、クラスター内、管理、およびインターネットポートの2つのインスタンスを設定して使用できます。詳細については、「[NIC ボンディングの概要 \(77 ページ\)](#)」を参照してください。

引き出し線	説明
1	モジュラ LAN-on-motherboard (mLOM) カード ベイ (x16 PCIe レーン)
2	USB 3.0 ポート X 2

引き出し線	説明
3、10	<p>1 Gbps/10 Gbps 管理ポート（ネットワークアダプタ 3）：このイーサネットポートは、リンクパートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 3 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。</p> <ul style="list-style-type: none"> • プライマリインスタンス（コールアウト 3）は、背面パネルに 1 というラベルが付いています。 • セカンダリインスタンス（コールアウト 10）は、アプライアンスの PCIe ライザ 2/スロット 2 にある Intel X710-DA4 NIC の 4 番目のポートです。 <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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。

引き出し線	説明
4、11	<p>1 Gbps/10 Gbps インターネットポート（ネットワークアダプタ 4）：このイーサネットポートは、リンクパートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 4 として識別されます。このポートは、10 Gbps エンタープライズポートではインターネット接続ができない場合に任意で使用されます。インターネットに接続しているインターネットサーバまたはプロキシサーバに接続します。</p> <ul style="list-style-type: none"> • プライマリインスタンス（コールアウト 4）は、背面パネルに 2 というラベルが付いています。 • セカンダリインスタンス（コールアウト 11）は、アプライアンスの PCIe ライザ 2/スロット 2 の Intel X710-DA4 NIC の 3 番目のポートです。 <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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックはありません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。
5	VGA ビデオポート（DB-15）。

引き出し線	説明
6	<p>1 Gbps Cisco IMC ポート：これは VGA ビデオポートの右側にある組み込みポートで、RJ45 シリアルポートの左側にあります。アプライアンスの Cisco IMC GUI に対するブラウザアクセスを有効にしていると、IP アドレスが割り当てられます（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。このポートは、アプライアンスのシャーシおよびソフトウェアのアウトオブバンド管理用に予約されています。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。</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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。
7	シリアルポート（RJ-45 コネクタ）
8	ユニット背面の ID ボタンと LED
9	<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"> • 消灯：電源に AC 電力が供給されていません。 • 緑の点灯：AC 電力供給も、DC 出力も OK です。 • 緑の点滅：AC 電力供給は OK ですが、DC 出力は使用できません。 <p>詳細については「電力仕様」を参照してください。</p>

引き出し線	説明
12, 15	<p>10 Gbps エンタープライズポート（ネットワークアダプタ 1）：このポートは、Maglev 構成ウィザードでネットワークアダプタ 1 として識別されます。このポートを、エンタープライズ ネットワークに接続しているスイッチに接続します。</p> <ul style="list-style-type: none"> • プライマリインスタンス（コールアウト 15）は、アプライアンスの PCIe ライザ 1/スロット 1 の Intel X710-DA2 NIC の左側のポートです。 • セカンダリインスタンス（コールアウト 12）は、アプライアンスの PCIe ライザ 2/スロット 2 の Intel X710-DA4 NIC の 2 番目のポートです。 <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。 リンクステータス LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 100 Mbps 以下です。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 <p>(注) 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。</p>

引き出し線	説明
13、14	<p>10 Gbps のクラスタ内ポート（ネットワークアダプタ 2）：このポートは、Maglev 構成ウィザードでネットワークアダプタ 2 として識別されます。このポートをクラスタ内のほかのノードに接続しているスイッチに接続します。</p> <ul style="list-style-type: none"> • プライマリインスタンス（コールアウト 14）は、アプライアンスの PCIe ライザ 1/スロット 1 の Intel X710-DA2 NIC の右側のポートです。 • セカンダリインスタンス（コールアウト 13）は、アプライアンスの PCIe ライザ 2/スロット 2 の Intel X710-DA4 NIC の最初のポートです。 <p>このポートは、アプライアンスの PCIe ライザ 2/スロット 2 にある Intel X710-DA4 NIC にあります。</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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>リンク速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 100 Mbps 以下です。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 <p>(注) 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。</p>
16	二重孔アース ラグ用ネジ穴。

図 4: 112 コアアプライアンスの背面パネル

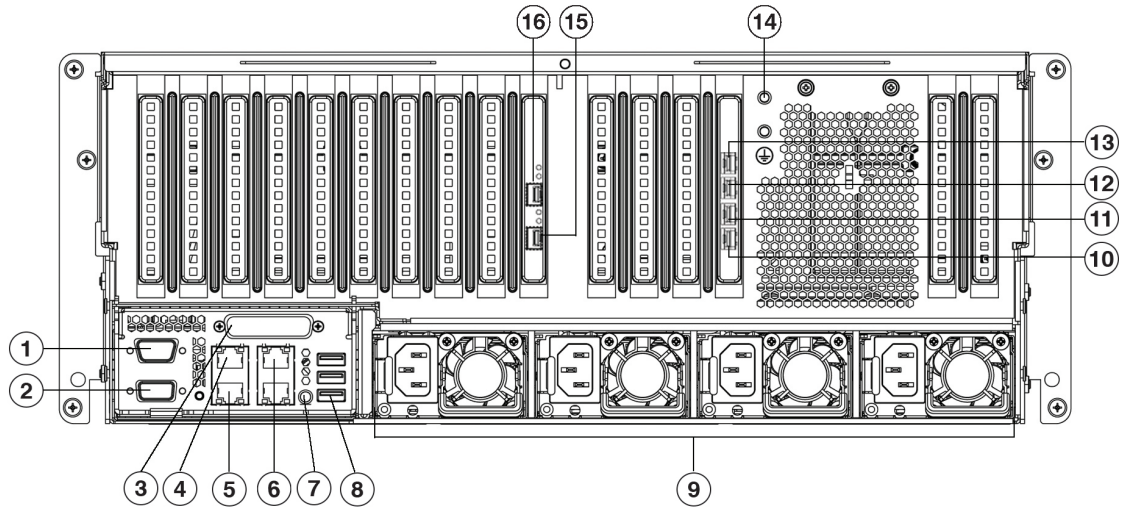
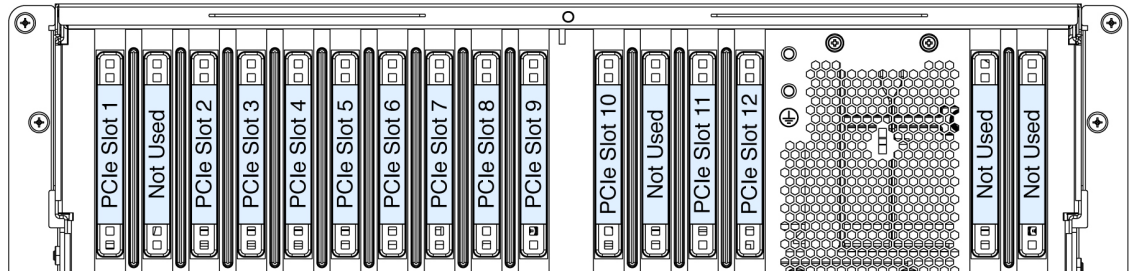


図 5: 112 コアアプライアンスの背面パネルのスロット



- (注) Cisco DNA Center アプライアンスでNIC ボンディングが有効になっている場合は、エンタープライズ、クラスタ内、管理、およびインターネットポートの2つのインスタンスを設定して使用できます。詳細については、「[NIC ボンディングの概要 \(77 ページ\)](#)」を参照してください。

引き出し線	説明
1	シリアルポート COM 1 (DB-9 コネクタ)
2	VGA ビデオポート (DB-15 コネクタ)
3	現時点ではサポートされていません。

引き出し線	説明
4、13	<p>1 Gbps/10 Gbps 管理ポート（ネットワークアダプタ 3）：このイーサネットポートは、リンクパートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 3 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。</p> <ul style="list-style-type: none"> • プライマリインスタンス（コールアウト 4）は、背面パネルに 1 というラベルが付いています。 • セカンダリインスタンス（コールアウト 13）は、アプライアンスの PCIe ライザ 2/スロット 12 の Intel X710-DA4 NIC の一番上にあるポートです。 <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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。

引き出し線	説明
5、12	<p>1 Gbps/10 Gbps インターネットポート（ネットワークアダプタ 4）：このイーサネットポートは、リンクパートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 4 として識別されます。このポートは、10 Gbps エンタープライズポートではインターネット接続ができない場合に任意で使用されます。インターネットに接続しているインターネットサーバまたはプロキシサーバに接続します。</p> <ul style="list-style-type: none"> • プライマリインスタンス（コールアウト 5）は、背面パネルに 2 というラベルが付いています。 • セカンダリインスタンス（コールアウト 12）は、アプライアンスの PCIe ライザ 2/スロット 12 の Intel X710-DA4 NIC の上から 2 番目のポートです。 <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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックはありません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。

引き出し線	説明
6	<p>1 Gbps Cisco IMC ポート：これは管理ポートの右側にある10/100/1000イーサネット専用管理ポート（Base-T）です。背面パネルでは3として識別されます。アプライアンスのCisco IMC GUIに対するブラウザアクセスを有効にしていると、このポートにIPアドレスが割り当てられます（「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」を参照）。アプライアンスのシャーシおよびソフトウェアのアウトオブバンド管理用に予約されています。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。</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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 10 Mbps 以下です。 • 緑：リンク速度は 1 Gbps です。 • オレンジ：リンク速度は 100 Mbps です。
7	背面 ID ボタン/LED
8	USB 3.0 ポート×3
9	<p>電源装置 1～4：ホットスワップ可能、3+1 の冗長構成（Cisco IMC で設定）。</p> <p>詳細については「電力仕様」を参照してください。</p>

引き出し線	説明
10、15	<p>10 Gbps のクラスタ内ポート（ネットワークアダプタ 2）：このポートは、Maglev 構成ウィザードでネットワークアダプタ 2 として識別されます。このポートをクラスタ内のほかのノードに接続しているスイッチに接続します。</p> <ul style="list-style-type: none"> • プライマリインスタンス（コールアウト 15）は、アプライアンスの PCIe ライザ 1/スロット 9 の Intel X710-DA2 NIC の下部にあるポートです。 • セカンダリインスタンス（コールアウト 10）は、アプライアンスの PCIe ライザ 2/スロット 12 の Intel X710-DA4 NIC の下部にあるポートです。 <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"> • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>リンク速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：リンク速度は 100 Mbps 以下です。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 <p>（注） 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。</p>

引き出し線	説明
11、16	<p>10 Gbps エンタープライズポート（ネットワークアダプタ 1）：このポートは、Maglev 構成ワイザードでネットワークアダプタ 1 として識別されます。アプライアンスで NIC ボンディングが有効になっている場合は、このポートをエンタープライズ ネットワークに接続しているスイッチに接続します。</p> <ul style="list-style-type: none"> プライマリインスタンス（コールアウト 16）は、アプライアンスの PCIe ライザ 1/スロット 9 の Intel X710-DA2 NIC の一番上にあるポートです。 セカンダリインスタンス（コールアウト 11）は、アプライアンスの PCIe ライザ 2/スロット 12 の Intel X710-DA4 NIC の上から 3 番目のポートです。 <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"> 消灯：リンクが確立されていません。 緑の点滅：アクティブなリンクにトラフィックが存在します。 緑：リンクはアクティブですが、トラフィックは存在しません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> 消灯：リンク速度は 100 Mbps 以下です。 緑：リンク速度は 10 Gbps です。 オレンジ：リンク速度は 1 Gbps です。 <p>（注） 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。</p>
14	二重孔アース ラグ用ネジ穴。

物理仕様

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

表 4: 物理仕様

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

説明	仕様
幅	44 および 56 コアアプライアンス : <ul style="list-style-type: none"> • ハンドルなし : 43.0 cm (16.9 インチ) • ハンドルを含む : 48.3 cm (19.0 インチ) 112 コアアプライアンス : 48.3 cm (19.0 インチ)
奥行 (長さ)	44 および 56 コアアプライアンス : <ul style="list-style-type: none"> • ハンドルなし : 75.6 cm (29.8 インチ) • ハンドルを含む : 78.7 cm (30.98 インチ) 112 コアアプライアンス : 83.1 cm (32.7 インチ)
前面のスペース	76 mm (3 インチ)
周囲と側面の間に必要な隙間	25 mm (1 インチ)
背面のスペース	152 mm (6 インチ)
最大重量 (フル装備シャーシ)	44 および 56 コアアプライアンス : 17.0 kg (37.5 ポンド) 112 コアアプライアンス : 66.2 kg (146 ポンド)

環境仕様

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

表 5: 環境仕様

説明	仕様
動作時温度	41 ~ 95 °F (5 ~ 35 °C) 海拔 305 m (1000 フィート) ごとに最高温度が 1°C 低下します。
非動作時温度 (アプライアンスが倉庫にあるか運送中の場合)	-40 ~ 149 °F (-40 ~ 65 °C)
湿度 (RH) (動作時)	10 ~ 90% (28°C (82°F) 時、結露なし)
非動作時湿度 (RH) (アプライアンスが倉庫にあるか運送中の場合)	5 ~ 93% (28°C (82°F) 時)

電力仕様

説明	仕様
動作時高度	0 ～ 10,000 フィート (0 ～ 3,048 m)
非動作時高度 (アプライアンスが倉庫にあるか運送中の場合)	0 ～ 40,000 フィート (0 ～ 12,192 m)
音響出力レベル、ISO7779 に基づく A 特性 LWAd (B) を測定、23°C (73°F) での動作時	44 および 56 コアアプライアンス : 5.5 112 コアアプライアンス : <ul style="list-style-type: none"> • 最低設定 : 7.08 • 標準設定 : 7.67 • 最大設定 : 8.24
音圧レベル、ISO 7779 に基づく A 特性 LpAm (dBA) を測定、23°C (73 °F) での動作時	44 および 56 コアアプライアンス : 40 112 コアアプライアンス : <ul style="list-style-type: none"> • 最低設定 : 57.6 • 標準設定 : 63.5 • 最大設定 : 70.5

電力仕様

Cisco DNA Center アプライアンスに同梱されている電源装置の仕様を次の表に示します。44 コアおよび 56 コアのアプライアンスには、2 つの 770 W 電源装置 (シスコ製品番号 UCSC-PSU1-770W) が付属しています。112 コアアプライアンスには、4 つの 1600 W AC 電源装置 (シスコ製品番号 UCSC-PSU1-1600W) が付属しています。別途指定のない限り、両方の電源装置にこの仕様が適用されます。

表 6: AC 電源の仕様

説明	仕様
AC 入力電圧	770 W : <ul style="list-style-type: none"> • 公称範囲 : 100 ～ 120 VAC、200 ～ 240 VAC • 範囲 : 90 ～ 132 VAC、180 ～ 264 VAC 1600 W : <ul style="list-style-type: none"> • 公称範囲 : AC 200 ～ 240 V • 範囲 : AC 180 ～ 264 V

説明	仕様
AC 入力周波数	公称範囲 : 50 ~ 60 Hz (範囲 : 47 ~ 63 Hz)
最大 AC 入力電流	770 W : <ul style="list-style-type: none"> • 100 VAC で 9.5 A • 208 VAC で 4.5 A 1600 W : 9.5 A @ AC 200 V
最大入力電圧	770 W : 950 VA @ AC 100 V 1600 W : 1250 VA @ AC 200 V
PSU あたりの最大出力電力	770 W @ AC 100 ~ 120 V 1600 W : AC 200 ~ 240 V
最大突入電流	770 W : 15 A @ 35°C 1600 W : 15 A @ 35°C
最大保留時間	770 W : 12 ms 1600 W : 80 ms
電源装置の出力電圧	12 VDC
電源装置のスタンバイ電圧	12 VDC
効率評価	Climate Savers Platinum Efficiency (80 Plus Platinum 認証済み)
フォーム ファクタ	RSP2
入力コネクタ	IEC320 C14



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



第 2 章

導入の計画

- [プランニング ワークフロー](#) (27 ページ)
- [Cisco DNA Center および Cisco Software-Defined Access](#) (28 ページ)
- [インターフェースケーブル接続](#) (28 ページ)
- [必要な IP アドレス および サブネット](#) (33 ページ)
- [必要なインターネット URL と完全修飾ドメイン名](#) (38 ページ)
- [インターネットへのアクセスを保護する](#) (41 ページ)
- [必要なネットワークポート](#) (41 ページ)
- [必要なポートとプロトコル： Cisco Software-Defined Access](#) (44 ページ)
- [必須の設定情報](#) (52 ページ)
- [必要な初期設定情報](#) (53 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。「[インターフェースケーブル接続](#)」を参照してください。
2. アプライアンスの設定時に適用する IP アドレッシング、サブネット化などの IP トラフィック情報を収集します。「[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。「[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。「[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。「[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、少なくともエンタープライズおよびクラスタ内ポートインターフェイスを設定する必要があります。

アプライアンスで NIC ボンディングが有効になっている場合、エンタープライズ、クラスタ内、管理、およびインターネットポートのセカンダリインスタンスは Intel X710-DA4 NIC に存在します。これらのポートを、各ポートのプライマリインスタンスを接続するスイッチとは異なるスイッチに接続します ([NIC ボンディングの概要 \(77 ページ\)](#) を参照してください)。



- (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。実稼働環境の単一ノード展開と3ノード展開の両方で、クラスタ内ポートをクラスタリンクとして割り当てます。
 - 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 \(86 ページ\)](#) 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 エンタープライズポート (ネットワークアダプタ 1) : このポートの目的は、Cisco DNA Center がネットワークと通信し、ネットワークを管理できるようにすることです。このポートを、エンタープライズネットワークに接続しているスイッチに接続し、ポートのサブネットマスクを使用してIPアドレスを1つ設定します。

プライマリインスタンス :

- 44 および 56 コアアプライアンスでは、これはPCIe スロット 1 に搭載されている Intel X710-DA2 NIC の左側にあるポートです。
- 112 コアアプライアンスでは、これはPCIe スロット 9 に搭載されている Intel X710-DA2 NIC の上部にある 10 Gbps ポートです。

セカンダリインスタンス :

- 44 および 56 コアアプライアンスでは、これはPCIe スロット 2 に搭載されている Intel X710-DA4 NIC の 2 番目のポートです。
- 112 コアアプライアンスでは、これはPCIe スロット 12 に搭載されている Intel X710-DA4 NIC の上から 3 番目の 10 Gbps ポートです。

- (必須) 10 Gbps クラスタ内ポート (ネットワークアダプタ 2) : このポートの目的は、クラスタ内のプライマリノードとセカンダリ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。

プライマリインスタンス :

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

- 112 コアアプライアンスでは、これはPCIe スロット 9 に搭載されている Intel X710-DA2 NIC の下部にある 10 Gbps ポートです。

セカンダリインスタンス：

- 44 および 56 コアアプライアンスでは、これはPCIe スロット 2 に搭載されている Intel X710-DA4 NIC の最初のポートです。
- 112 コアアプライアンスでは、これはPCIe スロット 12 に搭載されている Intel X710-DA4 NIC の下部にある 10 Gbps ポートです。
- (オプション) 1 Gbps または 10 Gbps の管理ポート (ネットワークアダプタ 3) : このポートから Cisco DNA Center GUI にアクセスできるため、ユーザーはアプライアンス上でソフトウェアを使用できます。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

プライマリインスタンス：アプライアンスの背面パネルに 1 というラベルが付いています。

セカンダリインスタンス：

- 44 および 56 コアアプライアンスでは、これはPCIe スロット 2 に搭載されている Intel X710-DA4 NIC の 4 番目のポートです。
- 112 コアアプライアンスでは、これはPCIe スロット 12 に搭載されている Intel X710-DA4 NIC の上部にある 10 Gbps ポートです。
- (オプション) 1 Gbps または 10 Gbps のインターネットポート (ネットワークアダプタ 4) : このポートは、背面パネルに 2 というラベルが付いており、オプションです。10 Gbps のエンタープライズポート (ネットワークアダプタ 1) 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ーを含む) に接続できない場合にのみ使用してください。この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ー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。

プライマリインスタンス：アプライアンスの背面パネルに 2 というラベルが付いています。

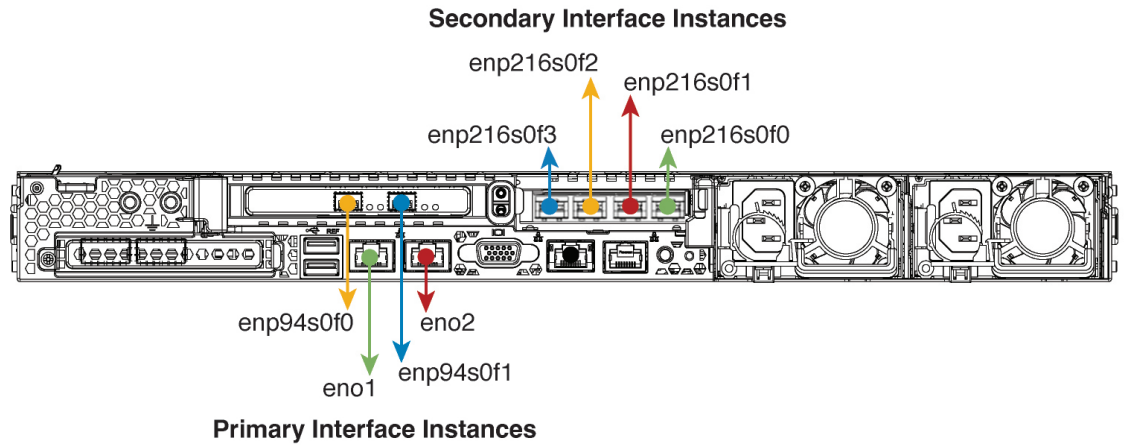
セカンダリインスタンス：

- 44 および 56 コアアプライアンスでは、これはPCIe スロット 2 に搭載されている Intel X710-DA4 NIC の 3 番目のポートです。
- 112 コアアプライアンスでは、これはPCIe スロット 12 に搭載されている Intel X710-DA4 NIC の上から 2 番目の 10 Gbps ポートです。
- (オプション、ただし強く推奨) 1 Gbps Cisco IMC ポート：このポートで、Cisco Integrated Management Controller (CIMC) アウトオブバンドアプライアンス管理インターフェイスとその GUI にブラウザがアクセスします。その目的は、アプライアンスとそのハードウェア

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

次の図は、シングルノード Cisco DNA Center クラスタで推奨される接続と、各インターフェイスに割り当てられているラベルを示しています。

図 6:44 および 56 コアアプライアンスに推奨されるケーブル接続



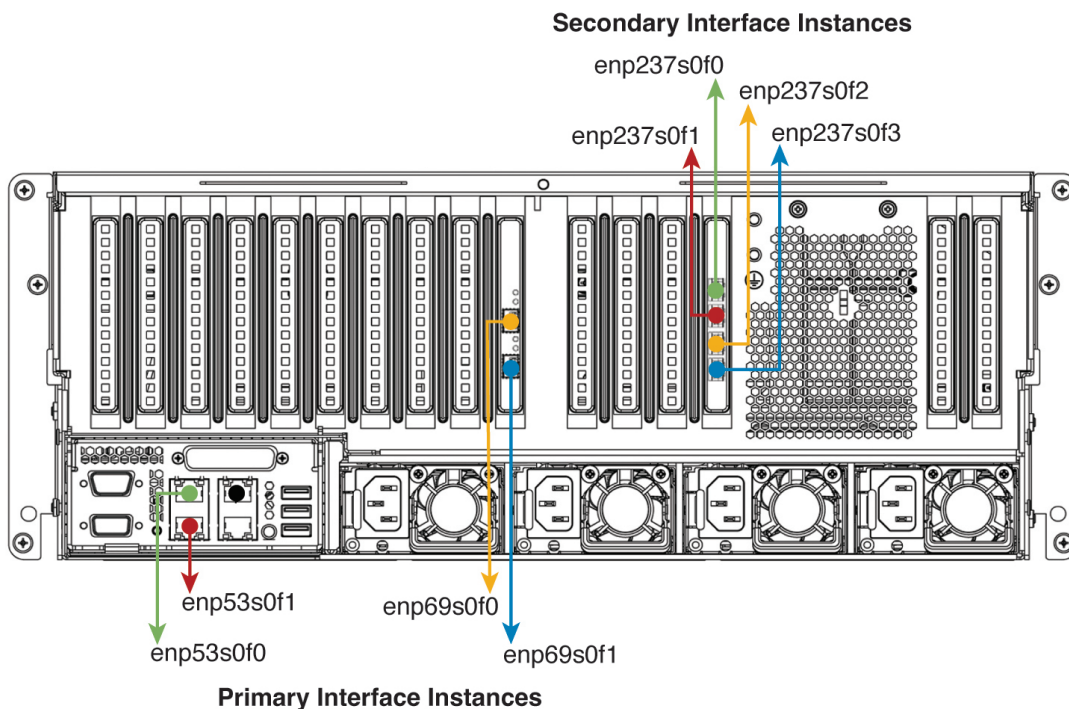
Legend

- 10-Gbps Enterprise Port (Network Adapter 1)
- 10-Gbps Intracluster Port (Network Adapter 2)
- 1-Gbps/10-Gbps Management Port (Network Adapter 3)
- 1-Gbps/10-Gbps Internet Port (Network Adapter 4)
- 1-Gbps Cisco IMC Port



(注) 管理インターフェイスとインターネットインターフェイスの両方とも、プライマリインスタンスの帯域幅は 1 Gbps で、セカンダリインスタンスの帯域幅は 10 Gbps です。

図 7: 112 コアアプライアンスに推奨されるケーブル接続



Legend

- 10-Gbps Enterprise Port (Network Adapter 1)
- 10-Gbps Intracluster Port (Network Adapter 2)
- 1-Gbps/10-Gbps Management Port (Network Adapter 3)
- 1-Gbps/10-Gbps Internet Port (Network Adapter 4)
- 1-Gbps Cisco IMC Port



(注) 管理インターフェイスとインターネットインターフェイスの両方とも、プライマリインスタンスの帯域幅は 1 Gbps で、セカンダリインスタンスの帯域幅は 10 Gbps です。

3 ノード Cisco DNA Center クラスタ内の各ノードの接続は、シングルノードクラスタの場合と同じであり、同じポートが使用されます。3 ノードクラスタをケーブル接続する場合は、次の手順を実行します。

- 各ノードのエンタープライズ、クラスタ内、管理、およびインターネットポートのプライマリインスタンスと Cisco IMC ポートをプライマリスイッチに接続します。
- 各ノードのエンタープライズ、クラスタ内、管理、およびインターネットポートのセカンダリインスタンスをセカンダリスイッチに接続します。

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



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

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

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

必要な IP アドレスおよびサブネット

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

- [Enterprise Port Address] (必須) : サブネットマスクを持つ 1 つの IP 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。
- [Management 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。
- [Internet 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、インターネットポートの IP アドレスは必要ありません。
- [CIMC Port Address] (オプション、ただし強く推奨) : サブネットマスクを持つ 1 つの IP アドレス。



- (注) これらの要件で要求されるすべての IP アドレスは、有効な IPv4 ネットマスクを持つ有効な IPv4 アドレスである必要があります。アドレスと対応するサブネットが重複していないことを確認します。重複している場合、サービスの通信の問題が発生する可能性があります。

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

- **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、およびインターネットの 4 つのインターフェイスがあります。Cisco DNA Center の機能に必要なため、最低でも企業およびクラスタのポートインターフェイスを設定する必要があります。サブネットマスクと 1 つ以上の関連ゲートウェイまたはスタティックルートとともに IP をインターフェイスに指定すると、そのインターフェイスは設定されていると見なされます。設定時にインターフェイスを完全にスキップすると、そのインターフェイスは設定されていないと見なされます。

次の点に注意してください。

- 単一ノード設定で、今後 3 ノードクラスタに変換する予定がない場合は、VIP アドレスを指定する必要はありません。ただし、これを行う場合は、設定されているすべてのネットワークインターフェイスに VIP アドレスを指定する必要があります (3 ノードクラスタの場合と同様)。
 - 単一ノードクラスタのクラスタ内リンクがダウンすると、管理インターフェイスとエンタープライズ インターフェイスに関連付けられている VIP アドレスもダウンします。これが発生すると、クラスタ内リンクが復元されるまで Cisco DNA Center を使用できません (ソフトウェアイメージ管理 [SWIM] と Cisco Identity Services Engine [ISE] の統合が動作しません。またネットワーク データ プラットフォーム [NDP] コレクタから情報を収集できないため、Cisco DNA アシユアランスデータが表示されません)。
 - エンタープライズインターフェイスまたは管理インターフェイスには、リンクローカルまたはルーティング不可能な IP アドレスを使用しないでください。
-
- **デフォルトゲートウェイ IP アドレス (Default Gateway IP Address)** : ネットワークの優先デフォルトゲートウェイの IP アドレス。他のルートがトラフィックに一致しない場合、トラフィックはこの IP アドレスを経由してルーティングされます。通常は、インターネットにアクセスするネットワーク設定内のインターフェイスにデフォルトゲートウェイを割り当てる必要があります。Cisco DNA Center の導入時に留意すべきセキュリティ上の考慮事項については、『[Cisco Digital Network Architecture Center 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。
-
- **DNS サーバの IP アドレス (DNS Server IP Addresses)** : 1 つ以上のネットワークの優先 DNS サーバの IP アドレス。設定時に、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。
 - **(オプション) スタティックルートアドレス (Static Route Addresses)** : 1 つ以上のスタティックルートの IP アドレス、サブネットマスク、およびゲートウェイ。設定時に、複

数のスタティックルートの IP アドレス、ネットマスク、およびゲートウェイを、スペースで区切ったリストとして入力することによってそれらを指定できます。

アプライアンスの任意のインターフェイスに対して1つ以上のスタティックルートを設定できます。デフォルトゲートウェイ以外の特定の方向でトラフィックをルーティングする場合は、スタティックルートを指定する必要があります。スタティックルートを持つ各インターフェイスは、IP route コマンドテーブルでトラフィックがルーティングされるデバイスとして設定されます。このため、トラフィックが送信されるインターフェイスとスタティックルートの方向を一致させることが重要です。

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

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

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

- **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後、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（「[アプライアンスのイメージの再作成](#)」を参照してください）。

- **クラスタサブネット (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後、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てはできません（「[アプライアンスのイメージの再作成](#)」を参照してください）。
- クラスタポート、コンテナサブネット、またはクラスタサブネットの IP アドレスを入力する場合は、169.254.0.0/23 サブネット内のアドレスを指定しないでください。

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

アプライアンスがこのようなアドレス空間を必要とする理由の1つは、システムパフォーマンスを維持するためです。東西（ノード間）通信には内部ルーティングおよびトンネリングテクノロジーが使用されているため、重複するアドレス空間を使用すると、アプライアンスが仮想ルーティングを実行し、内部的に FIB を転送（FIB）するように強制されることがあります。これにより、1つのサービスから別のサービスに送信されるパケットに対して複数の 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。IP アドレスが不足したり、お客様がシステムをアップグレードするためだけに連続するアドレス空間を再割り当てすることを要求したりすることなく、シスコが新しいサービスや機能を追加できるようにするために、アドレス空間の要件は最初は意図的に大きく維持されています。

これらのサブネットでサポートされているサービスは、レイヤ3でも有効になっています。クラスタスペースは、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。

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 7: 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します。	<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/ • https://download-ssc.cisco.com/
クラウドドメインで認証します。	https://dnaservices.cisco.com
ThousandEyes と統合します。	<ul style="list-style-type: none"> • *.awsglobalaccelerator.com • api.thousandeyes.com

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco Enterprise Network Function Virtualization Infrastructure Software (NFVIS) デバイスを管理します。	*.amazonaws.com
顧客動向テレメトリを収集します。	https://data.pendo.io
API 呼び出しを許可して、Cisco CX Cloud Success Tracks へのアクセスを有効にします。そうしないと、Machine Reasoning Engine (MRE) がサポートする Security Advisories、Bug Identifier、および EOX 機能の拡張構成ベースのスキャンに追加された拡張機能が期待どおりに動作しません。	https://api-cx.cisco.com
Webex と統合します。	<ul style="list-style-type: none"> • http://analytics.webexapis.com • https://webexapis.com
ユーザフィードバック	https://dnacenter.uservoice.com
Cisco Meraki と統合します。	推奨 : *.meraki.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 <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を確認します。	<ul style="list-style-type: none"> • http://validation.identrust.com • http://commercial.ocsp.identrust.com (注) 上記の URL は、直接でも Cisco DNA Center で構成されているプロキシサーバー経由でも到達できるようにする必要があります。
Cisco DNA Center リモートサポート機能が有効になっている場合、シスコの認定スペシャリストがトラブルシューティングデータを収集できるようにします。	wss://prod.radkit-cloud.cisco.com:443

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
cisco.com とシスコスマートライセンスと統合します。	<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 • cloudssso.cisco.com • cloudssso1.cisco.com • cloudssso2.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
Network-Based Application Recognition (NBAR) に接続します。	prod.sdavc-cloud-api.com:443
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します。	<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 プロキシを設定します。	<ul style="list-style-type: none"> • https://api.use1.prd.kairos.ciscolabs.com (米国東部リージョン) • https://api.eucl.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します。	https://ec.walkme.com
ライセンスサービスにアクセスします。	https://swapi.cisco.com

目的	...Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco Spaces と統合します。	<ul style="list-style-type: none"> • https://dnaspaces.io • https://dnaspaces.eu • https://ciscospaces.sg

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かで開くかを問わず、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する必要があります。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 DNA Center セキュリティのベストプラクティスガイド](#)』を参照してください。

表 8: 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
2068	HTTPS	TCP (注) このポートは、リモート KVM コンソールのリダイレクトポートとして機能します。アプライアンスの構成中に Cisco IMC を使用する場合は、アプライアンスの構成が完了するまでポートを開いておく必要があります。
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
21730	アプリケーション可視性サービス (CBAR デバイス通信に使用)	UDP

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)
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 9: ポート : 発信トラフィック

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

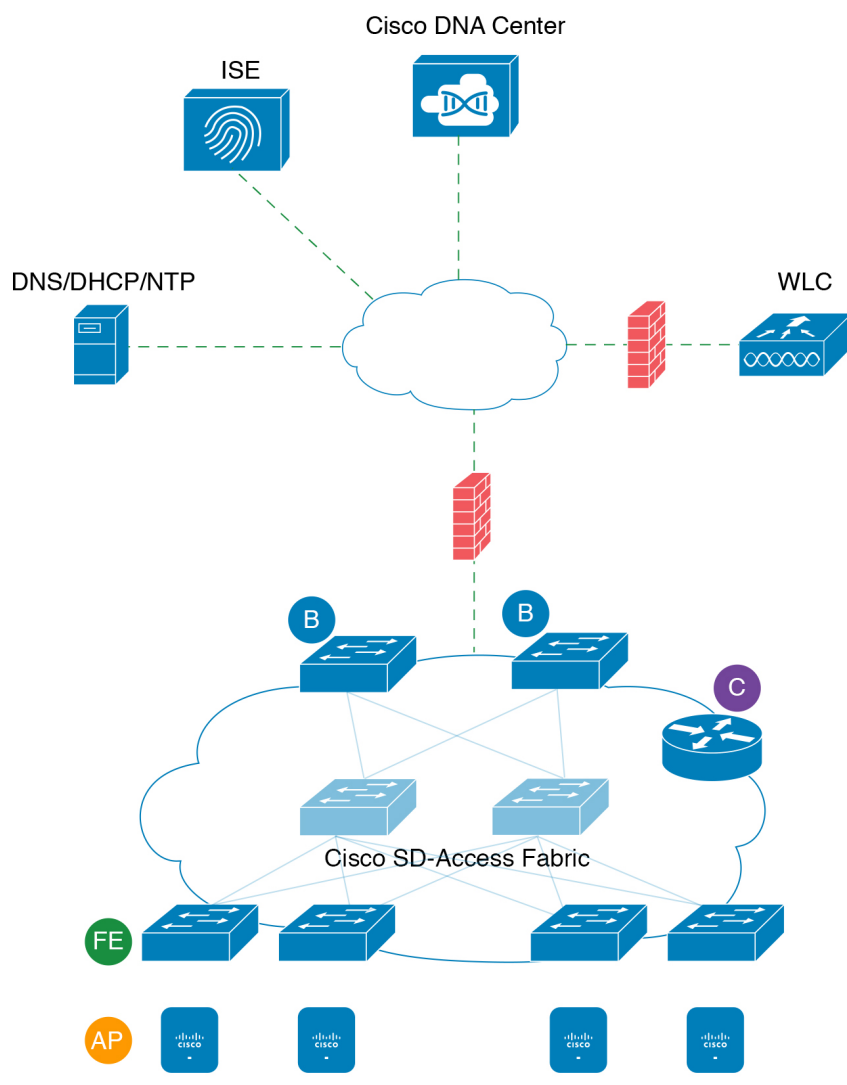


- (注) ほかにアプライアンスからシスコのアドレス (<https://www.cisco.com/security/pki/>) に対する発信 IP トラフィックを許可するようネットワークを設定する方法があります。アプライアンスからシスコがサポートする証明書およびトラストプールにアクセスするには、上述の URL に記載されている IP アドレスを使用します。

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 8 : 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 10: 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	スイッチと NFVIS のアプリケーション ホスティング
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 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 11: 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 12: 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、ルータループバック IP から Cisco DNA Center の間で SNMP トラップに使用
いずれか (Any)	ファブリックアンダーレイ	UDP 514	Cisco DNA Center	ファブリックスイッチ、ルータから Cisco DNA アシユアランス
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から Cisco DNA Center の間で NetFlow に使用
いずれか (Any)	ファブリックアンダーレイ	UDP 123	Cisco DNA Center	ファブリックスイッチから Cisco DNA Center の間で LAN 自動化時に使用
ICMP	ファブリックアンダーレイ	ICMP	Cisco DNA Center	ファブリックスイッチ、ルータループバックから Cisco DNA Center の間で SNMP デバイス検出に使用
UDP 161	ファブリックアンダーレイ	いずれか (Any)	Cisco DNA Center	ファブリックスイッチ、ルータループバックから Cisco DNA Center の間で SNMP デバイス検出に使用
いずれか (Any)	ファブリックアンダーレイ	UDP 53	DNS Server	ファブリックスイッチ、ルータから DNS サーバの間で名前解決に使用

TCPおよびUDP 4342	ファブリックアン ダーレイ	TCP および UDP 4342	ファブリック ルータおよびス イッチ	LISP でカプセル化された制御メッセー ジ
TCP および UDP 4342	ファブリックアン ダーレイ	いずれか (Any)	ファブリック ルータおよびス イッチ	LISP コントロールプレーン通信
いずれか (Any)	ファブリックアン ダーレイ	UDP 4789	ファブリック ルータおよびス イッチ	ファブリックカプセル化データパケッ ト (VXLAN-GPO)
いずれか (Any)	ファブリックアン ダーレイ	UDP 1645/1646/1812/1813	ISE	ファブリックスイッチ、ルータルー 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 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 13: 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	<ul style="list-style-type: none"> • TCP 443 (Cisco AireOS ワイヤレスコントローラ) • TCP 25103 (Cisco 9800 ワイヤレスコントローラ) 	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アカウントティングに使用
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 14: 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 15: Cisco 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 16: DHCP サーバトラフィック

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 67	DHCP サーバ	UDP 68	AP IP 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	AP IP 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 17: 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 18: 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。このユーザー名はプライマリノードとセカンダリ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。
- タブや改行を含まない。

- 次のうち少なくとも3つのカテゴリの文字を含むこと。
 - 大文字の英字 (A ~ Z)
 - 小文字の英字 (a ~ z)
 - 数字 (0 ~ 9)
 - 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、各セカンダリノードにプライマリノードの Linux パスワードを入力することも求められます。

- **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ーアカウント 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 ([クイック スタート ワークフローの完了 \(260 ページ\)](#) 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。

- **CISCO IMC ユーザパスワード** : Cisco IMC 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)。

Cisco IMC 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。

- [Primary Node IP Address] : クラスタにセカンダリ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、[クイック スタート ワークフローの完了 \(260 ページ\)](#) 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 \(273 ページ\)](#) 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](#) (57 ページ)
- [アプライアンスを開梱して点検](#) (57 ページ)
- [インストール警告とガイドラインの確認](#) (58 ページ)
- [ラック要件の確認](#) (60 ページ)
- [アプライアンスの接続および電源投入](#) (61 ページ)
- [LEDの確認](#) (61 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。

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

アプライアンスを開梱して点検



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

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

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

インストール警告とガイドラインの確認



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



警告 安全上の重要な注意事項

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

ステートメント 1071



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

ステートメント 1047



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

ステートメント 1019



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



警告 装置は地域および国の電気規則に従って設置する必要があります。

ステートメント 1074



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

ステートメント 1017

次の4つは 112 コアアプライアンスに固有の警告です。



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

ステートメント 1024



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

ステートメント 328



警告 システムの電源接続の前に高リーク電流アース接続を行う必要があります。

ステートメント 342



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

ステートメント 366



注意 アプライアンスを取り付ける際は、適切なエア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。
- サーバごとのラックの垂直方向のスペースは次を満たす必要があります。

- 44 および 56 コアアプライアンスの場合、1 RU は 44.45 mm (1.75 インチ) に相当します。
- 112 コアアプライアンスの場合、4 RU は 177.8 mm (7.0 インチ) に相当します。

アプライアンスの接続および電源投入

アプライアンスの電源をオンにして、アプライアンス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、次に、接地された 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。

(注) 44 および 56 コアアプライアンスの場合、アプライアンスに付属の電源のいずれかまたは両方を使用できます。112 コアアプライアンスの場合は、4 台の電源装置のうち少なくとも 3 台を使用します。

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

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

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

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

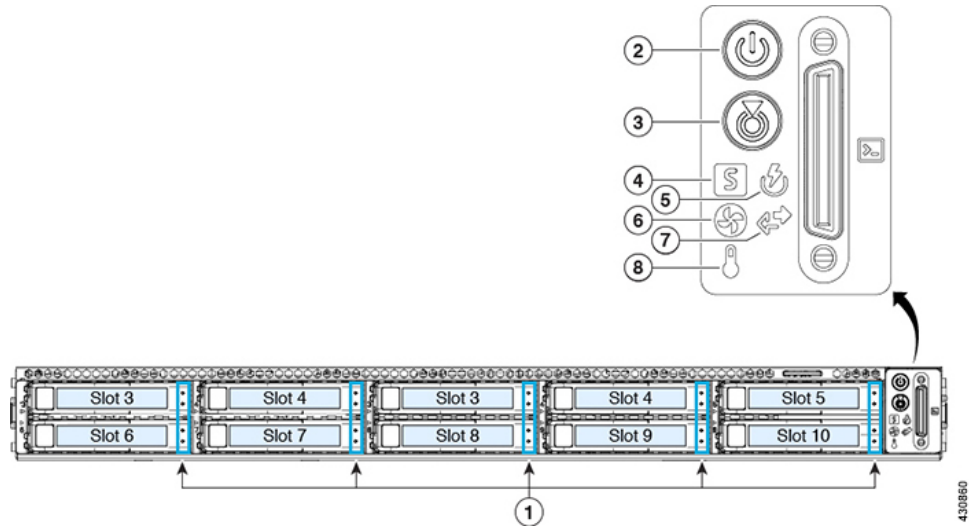
ステップ 2 前面パネルの KVM コネクタに接続されている付属の KVM ケーブルを使用して、USB キーボードと VGA モニタをサーバに接続します。または、背面パネルの VGA および USB ポートを使用することもできます。一度に接続できる VGA インターフェイスは 1 つのみです。

LED の確認

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

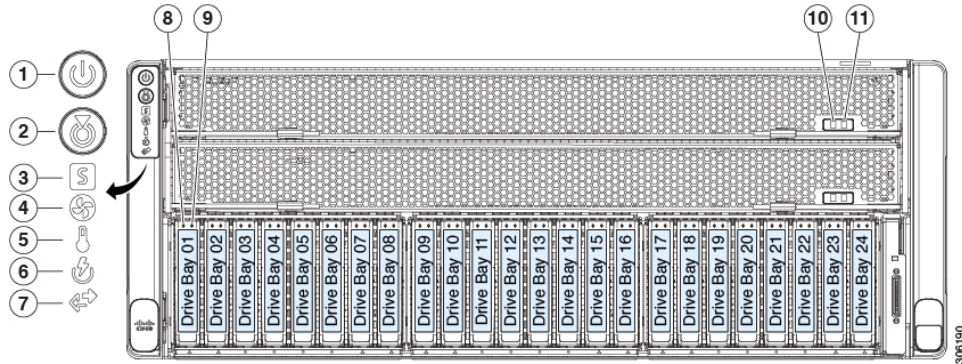
次の図は、物理的な設置と初回の電源投入が終わった後（設定前）動作しているアプライアンスの LED を示しています。

図 9:44 および 56 コアアプライアンスの前面パネル LED



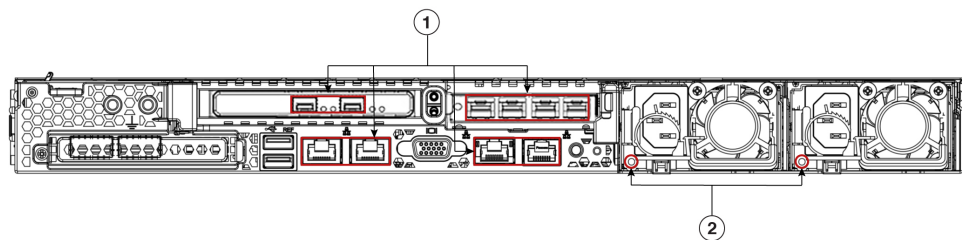
LED	望ましいステータスインジケータ
1	<ul style="list-style-type: none"> ドライブ障害 LED : 消灯 ドライブアクティビティ LED : 緑
2	電源ステータス : 緑
3	ユニット識別 : 消灯
4	システムステータス : 緑
5	電源装置ステータス : 緑
6	ファンスステータス : 緑
7	ネットワーク リンク アクティビティ : 消灯
8	温度ステータス : 緑

図 10: 112 コアアプライアンスの前面パネル LED



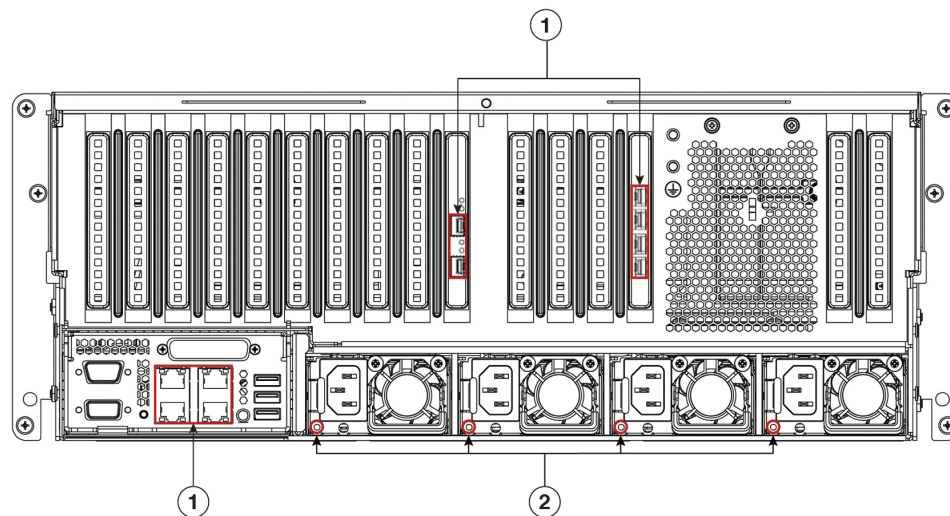
LED	望ましいステータスインジケータ
1	電源ステータス：緑
2	ユニット識別：消灯
3	システムステータス：緑
4	ファンステータス：緑
5	温度ステータス：緑
6	電源装置ステータス：緑
7	ネットワーク リンク アクティビティ：消灯
8	ドライブ障害 LED：消灯
9	ドライブアクティビティ LED：緑
10	CPU モジュール電源のステータス：緑
11	CPU モジュール障害：消灯

図 11: 44 および 56 コアアプライアンスの背面パネル LED



LED	望ましいステータスインジケータ
1	<p>正常であれば、最初の電源投入時にはすべてのポートのリンクステータスとリンク速度 LED がオフになります。</p> <p>Maglev 設定ウィザード（「Maglev ウィザードを使用したプライマリノードの設定」と「Maglev ウィザードを使用したセカンダリノードの設定」を参照）またはブラウザベースの設定ウィザード（詳細インストール構成ウィザードを使用したプライマリノードの設定（157ページ））と詳細インストール構成ウィザードを使用したセカンダリノードの設定（178ページ）を参照）を使用して、ネットワーク設定が設定され、テストされた後、ケーブル接続済みポートのリンクステータスとリンク速度を表す LED は、すべて緑になる必要があります。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。</p>
2	AC 電源ステータス LED : 緑

図 12: 112 コアアプライアンスの背面パネル LED



LED	望ましいステータスインジケータ
1	<p>正常であれば、最初の電源投入時にはすべてのポートのリンクステータスとリンク速度 LED がオフになります。</p> <p>Maglev 構成ウィザード（「Maglev ウィザードを使用したプライマリノードの設定」と「Maglev ウィザードを使用したセカンダリノードの設定」を参照）またはブラウザベースの構成ウィザード（詳細インストール構成ウィザードを使用したプライマリノードの設定（218ページ））と詳細インストール構成ウィザードを使用したセカンダリノードの設定（238ページ）を参照）を使用して、ネットワーク設定を設定し、テストした後は、すべてのケーブル接続済みポートのリンクステータスとリンク速度を表す LED が緑になる必要があります。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。</p>
2	AC 電源ステータス LED : 緑

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



第 4 章

アプライアンスの設定準備

- [アプライアンス設定の準備の概要 \(67 ページ\)](#)
- [Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(68 ページ\)](#)
- [事前設定タスクの実行 \(73 ページ\)](#)
- [NIC ボンディングの概要 \(77 ページ\)](#)
- [アプライアンスのイメージの再作成 \(86 ページ\)](#)
- [Cisco DNA Centerアプライアンスの設定 \(91 ページ\)](#)

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（「[事前設定タスクの実行](#)」を参照）。
3. アプライアンスに付属する Intel X710-DA4 ネットワーク インターフェイス カード (NIC) が現在無効になっている場合は、NIC ボンディングを使用するために、有効にする必要があります（[アップグレードされたアプライアンスでの NIC の有効化 \(79 ページ\)](#) を参照）。
4. Cisco DNA Center ソフトウェアはあらかじめアプライアンスにインストールされていますが、状況によってはソフトウェアを再インストールする必要が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作成しなおす必要がない場合は、使用する設定ウィザードに固有の「アプライアンスの設定の概要」のトピックに進みます。

- [アプライアンスの設定の概要](#)
- [アプライアンスの設定の概要](#)
- [アプライアンスの設定の概要](#)


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、「[事前設定タスクの実行](#)」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。

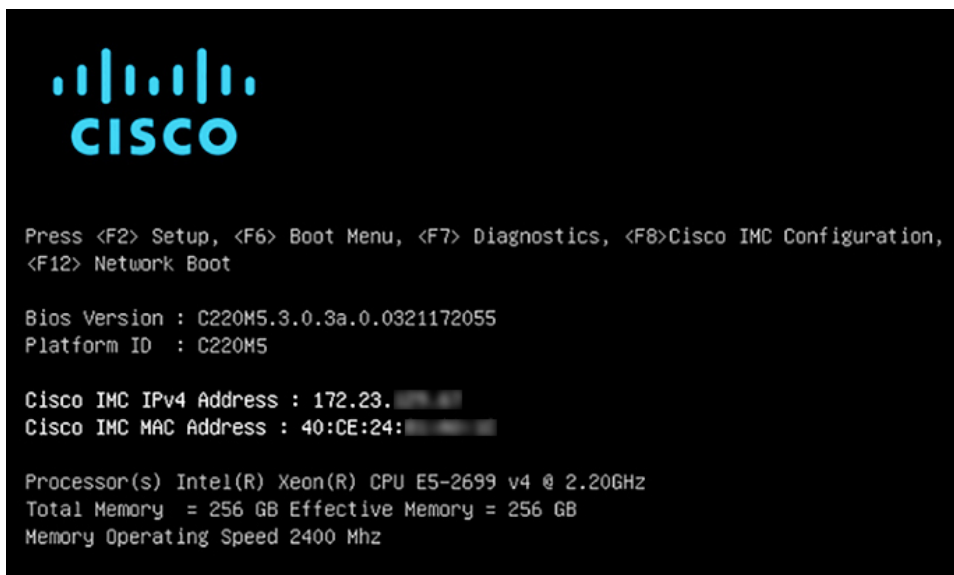
ステップ 1 次のいずれかを接続して、アプライアンスコンソールにアクセスします。

- 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 11）に接続する KVM ケーブルか、

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

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。

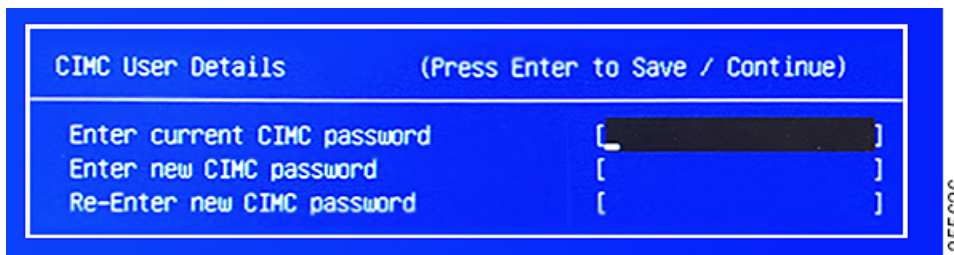
ステップ 3 前面パネルの電源ボタンを押して、アプライアンスをブートします。



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。

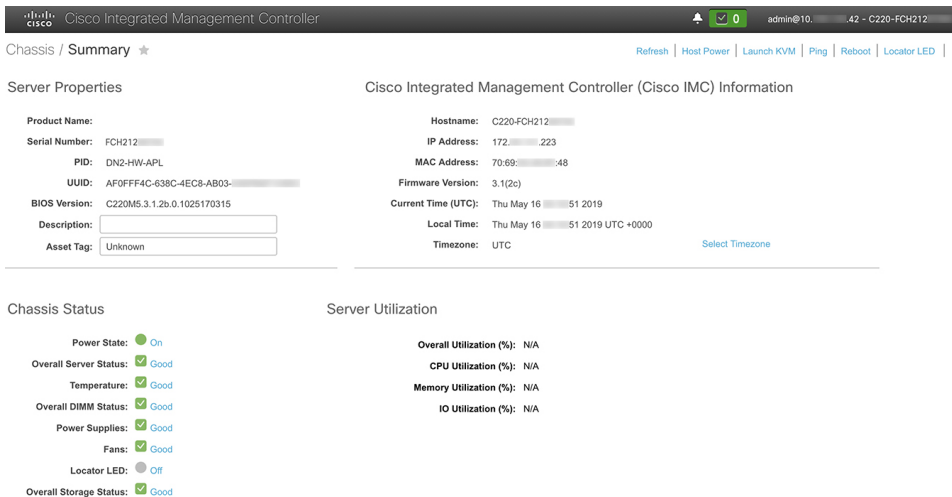
ステップ 12 設定が保存され、アプライアンスのリブートが完了したら、アプライアンスがインストールされているサブネットへのアクセスが可能なクライアントマシンで互換性のあるブラウザを開き、次の URL を入力します。

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。



- ステップ 14** このバージョンの Cisco IMC が、インストールする Cisco DNA Center リリースでサポートされていることを確認します。
- [Firmware Version] フィールドにリストされているバージョンをメモします。
 - インストールする Cisco DNA Center リリースの [リリースノート](#) を参照してください。「Supported Firmware」セクションには、ご使用の Cisco DNA Center リリースでサポートされている Cisco IMC のバージョンが示されています。
 - 次のいずれかを実行します。
 - 適切な Cisco IMC バージョンがインストールされている場合は、ここで終了できます。

- Cisco IMC のバージョンを更新する必要がある場合は、『Cisco Host Upgrade Utility User Guide』を参照してください。

事前設定タスクの実行

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. 10 Gbps アプライアンスポートに接続されているスイッチを再設定して、高スループット設定がサポートされるようにします。

ステップ 1 「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」で設定した CISCO imc IP アドレス、ユーザ ID、パスワードを使用して、アプライアンスの Cisco IMC にログインします。

ログインに成功すると、次に示すような [Cisco Integrated Management Controller Chassis Summary] ウィンドウがブラウザに表示されます。

The screenshot displays the Cisco Integrated Management Controller (IMC) Chassis Summary page. The page is divided into several sections:

- Server Properties:**
 - Product Name: FCH212
 - Serial Number: FCH212
 - PID: DN2-HW-APL
 - UUID: AF0FFF4C-638C-4EC8-AB03-
 - BIOS Version: C220M5.3.1.2b.0.1025170315
 - Description: [Empty text box]
 - Asset Tag: Unknown
- Cisco Integrated Management Controller (Cisco IMC) Information:**
 - Hostname: C220-FCH212
 - IP Address: 172. .223
 - MAC Address: 70:69: .48
 - Firmware Version: 3.1(2c)
 - Current Time (UTC): Thu May 16 51 2019
 - Local Time: Thu May 16 51 2019 UTC +0000
 - Timezone: UTC
- 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
- Server Utilization:**
 - Overall Utilization (%): N/A
 - CPU Utilization (%): N/A
 - Memory Utilization (%): N/A
 - IO Utilization (%): N/A

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。

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

(注)

- 第 1 世代の Cisco DNA Center アプライアンスとは異なり、第 2 世代のアプライアンスでは仮想インターフェイスカード (VIC) が使用されません。Cisco IMC で高スループットをサポートするために、第 2 世代アプライアンスに標準搭載のネットワークインターフェイスカード (NIC) を設定する必要はありません。すでにデフォルトで有効になっているためです。

- Cisco IMC で NTP 認証はサポートされていません。

ステップ 3 アプライアンスの高スループット設定と一致するようにスイッチを再設定します。

- 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。
- 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 mode access
MySwitch(config-if)#switchport access vlan 99
MySwitch(config-if)#speed auto
```



```
MySwitch(config-if)#duplex full
MySwitch(config-if)#mtu 1500
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#copy running-config startup-config
```

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

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

次の点に注意してください。

- これらのコマンドは単なる例です。
 - 正常に機能させるには、第 2 世代 Cisco DNA Center アプライアンスのスイッチポートをアクセスモードに設定する必要があります。トランクモードは、VLAN モードを除きサポートされません。
- c) `show interface tengigabitethernet` という *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、正しい MTU、デュプレックス、リンクタイプが設定されていることをコマンド出力で確認します。次に例を示します。

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

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

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

MySwitch#

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

```
MySwitch#show mac address-table interface tengigabitethernet 1/1/3
Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
99      XXXe.3161.1000   DYNAMIC Tel1/1/3
Total Mac Addresses for this criterion: 1
```

MySwitch#

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

The screenshot displays the Cisco IMC GUI for BIOS configuration. The breadcrumb path is **Home / Compute / BIOS**. The main navigation tabs include BIOS, Remote Management, Troubleshooting, Power Policies, and PID Catalog. Below these are links for [Enter BIOS Setup](#), [Clear BIOS CMOS](#), [Restore Manufacturing Custom Settings](#), and [Restore Defaults](#). The sub-navigation tabs are **Configure BIOS**, **Configure Boot Order**, and **Configure BIOS Profile**. The **BIOS Properties** section contains the following settings:

- Running Version:** C220M5.4.1.3m.0.0708220050
- UEFI Secure Boot:**
- Actual Boot Mode:** Legacy
- Configured Boot Mode:** Legacy (selected in a dropdown menu)
- Last Configured Boot Order Source:** CIMC
- Configured One time boot device:** (empty dropdown menu)

A blue **Save Changes** button is located at the bottom of the configuration area.

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

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

ブートモードを [UEFI] に変更しないでください。このモードが設定されている場合、Cisco DNA Center アプライアンスのインターフェイスは ping できない可能性があります。

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。
- アプライアンスを設定する準備ができている場合は、使用する設定ウィザードに固有の「[アプライアンス設定の概要](#)」のトピックに進みます。
 - [アプライアンスの設定の概要](#)

- [アプライアンスの設定の概要](#)
- [アプライアンスの設定の概要](#)

NIC ボンディングの概要

任意の Cisco DNA Center アプライアンスで、エンタープライズ インターフェイス、クラスタ内 インターフェイス、管理 インターフェイス、および インターネット インターフェイスを設定できます。アプライアンスでネットワーク インターフェイス コントローラ (NIC) ボンディングを有効にすると、各インターフェイスに次の2つのインスタンスが設定されます。プライマリ インスタンス (アプライアンスのマザーボードまたは Intel X710-DA2 NIC に配置) は1つのスイッチに接続され、セカンダリ インスタンス (アプライアンスの Intel X710-DA4 NIC に配置) が別のスイッチに接続されます。NIC ボンディングを使用すると、各インターフェイスの2つのインスタンスが単一の論理インターフェイスに統合され、1つの MAC アドレスを持つ単一のデバイスとして表示されます。この機能が有効になっている場合、アプライアンスでインターフェイスを設定するときに選択するボンディングモードに応じて、次の利点を得られます。



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

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



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

- LACP モード：このモードを選択すると、Cisco DNA Center によりグループ化された2つのインターフェイスで同じ速度とデュプレックス設定が共有されます。このモードでは、インターフェイスにロードバランシングとより高い帯域幅が提供されます。このモードを有効にするには、最初に次の点を確認する必要があります。
 - Linux ユーティリティ `ethtool` は、各インターフェイスの速度とデュプレックスモードを取得するために使用されるベースドライバをサポートしている必要があります。
 - エンタープライズポートに接続されているスイッチは、ダイナミックインターフェイス集約をサポートしている必要があります。

- スイッチで LACP を有効にした後、LACP モードが **active**（アプライアンスに接続されたスイッチポートがアクティブ ネゴシエーションステートになり、ポートが LACP パケットを送信してリモートポートとのネゴシエーションを開始する）に設定されていることを確認します。次に、LACP レートを **fast** に変更します（LACP がサポートするインターフェイスに LACP 制御パケットが送信されるレートをデフォルトから 30 秒ごとに変更します）。



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

実稼働環境で NIC ボンディングを使用する前に、次の作業を行う必要があります。

- アプライアンスでこの機能がサポートされていることを確認します。「[アプライアンスサポート \(78 ページ\)](#)」を参照してください。
- アプライアンスに付属する Intel X710-DA4 NIC が現在無効になっている場合は、NIC ボンディングを使用するために、有効にする必要があります（[アップグレードされたアプライアンスでの NIC の有効化 \(79 ページ\)](#) を参照）。
- アプライアンスの背面パネルにあるセカンダリポートの位置を確認します。「[前面パネルと背面パネル \(5 ページ\)](#)」を参照してください。
- 推奨されるアプライアンス（スイッチのケーブル接続）を確認します。[インターフェイスケーブル接続 \(28 ページ\)](#) を参照してください。

アプライアンスサポート

すべての第 2 世代 Cisco DNA Center アプライアンスは NIC ボンディングをサポートします。

- 44 コアアプライアンス：シスコ製品番号 DN2-HW-APL
- 44 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-U
- 56 コアアプライアンス：シスコ製品番号 DN2-HW-APL-L
- 56 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-L-U
- 112 コアアプライアンス：シスコ製品番号 DN2-HW-APL-XL
- 112 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-XL-U

アップグレードされたアプライアンスでの NIC の有効化

以前のバージョンから Cisco DNA Center 2.3.4 にアップグレードする予定のアプライアンスで Intel X710-DA4 NIC を有効にするには、次の手順を実行します。

ステップ 1 アプライアンスに Intel X710-DA4 NIC がインストールされていることを確認します。

- a) アプライアンスの Cisco IMC にログインします。
- b) [概要 (Summary)] ウィンドウの [サーバプロパティ (Server Properties)] エリアに次の値が設定されていることを確認します。
 - PID : 44 コアアプライアンスの DN2-HW-APL、56 コアアプライアンスの DN2-HW-APL-L、または 112 コアアプライアンスの DN2-HW-APL-XL (次の例を参照)。
 - BIOS バージョン : この値は 44 および 56 コアアプライアンスの C220M5、または 112 コアアプライアンスの C480M5 のいずれかで開始する必要があります (次の例を参照)。

Server Properties

Product Name:

Serial Number: FCH224-

PID: **DN2-HW-APL-XL**

UUID: 6FF202AA-EEF9-4DF4-9FE4-

BIOS Version: **C480M5** 4.0.1c.0.0706181854

Description:

Asset Tag:

Cisco Integrated Management Controller

Hostname: C480-FCH224-

IP Address: 10.195.


MAC Address: A8:B4:56:

Firmware Version: 4.0(1a)

Current Time (UTC): Wed Nov 6 18:51:54 2019

Local Time: Wed Nov 6 10:51:54 2019 PST -08

Timezone: America/Los_Angeles

- c)  > [Chassis] > [Inventory] > [Network Adapters] を選択します。
- d) [ネットワークアダプタ (Network Adapters)] 表で、次のスロットのいずれかに INTEL X710-DA4 Quad Port ネットワークアダプタが表示されていることを確認します。
 - 44 または 56 コアアプライアンスの場合は、PCIe スロット 2。
 - 112 コアアプライアンスの場合は、PCIe スロット 12 (次の例を参照)。

Cisco Integrated Management Controller

/ ... / Inventory / Network Adapters ★

CPU Memory PCI Adapters Power Supplies Cisco VIC Adapters Network Adapters Storage SAS Expan

Network Adapters Total 3 ⚙️

Slot	Product Name	Number Of Interfaces	External Ethernet Interfaces	
			ID	MAC Address
9	Intel X710-DA2 Dual Port 10Gb SFP+ conver...	2	1	3c:fd:fe:...
			2	3c:fd:fe:...
			4	3c:fd:fe:...
			3	3c:fd:fe:...
12	Intel X710-DA4 Quad Port 10Gb SFP+ conver...	4	1	3c:fd:fe:...
			2	3c:fd:fe:...
			1	2c:f8:9b:...
			2	2c:f8:9b:...
L	Cisco(R) LOM X550-T2	2	1	2c:f8:9b:...
			2	2c:f8:9b:...

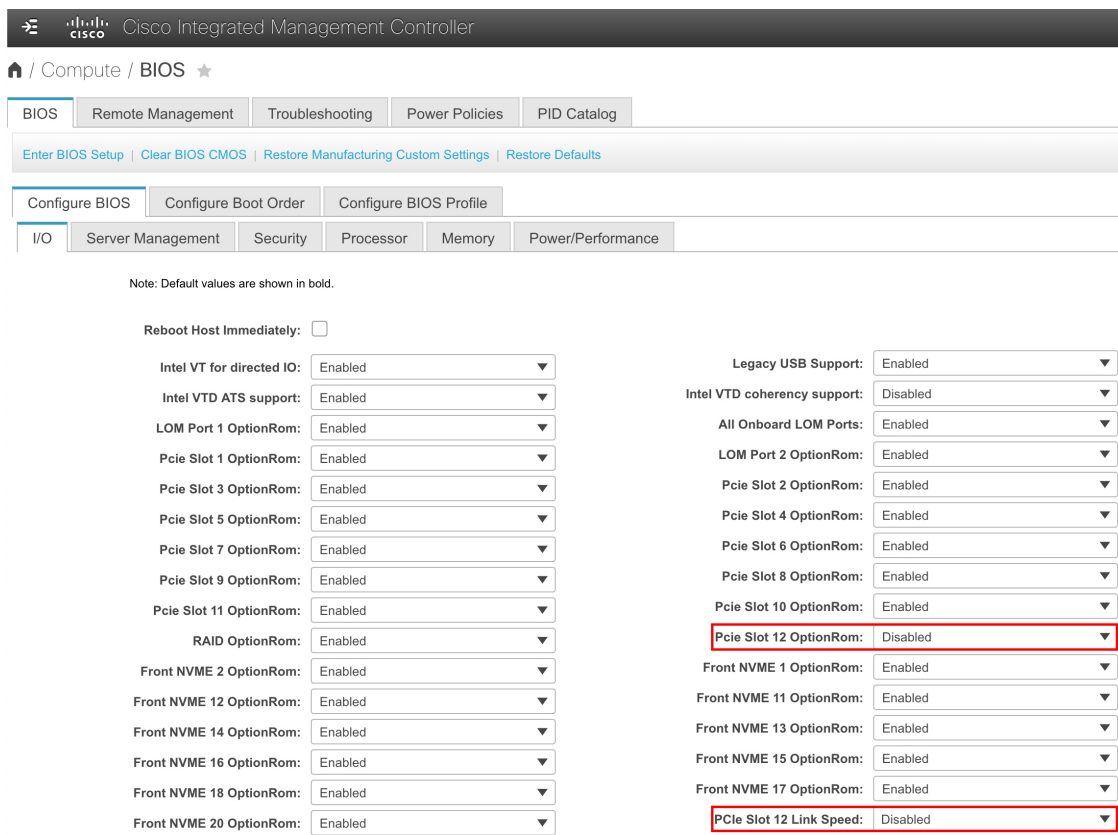
ステップ 2 アプライアンスの PCIe カードが有効になっていることを確認します。

a) > **[Compute]** を選択します。

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

b) 必要に応じて、次のパラメータを設定してから **[Save]** をクリックします。

- 44 または 56 コアアプライアンスの場合、**[PCIe Slot 2 OptionROM]** パラメータを **[Enabled]** に、**[PCIe Slot 2 Link Speed]** パラメータを **[Auto]** に設定。
- 112 コアの アプライアンスの場合、**[PCIe Slot 12 OptionROM]** パラメータを **[Enabled]** に、**[PCIe Slot 12 Link Speed]** パラメータを **[Auto]** に設定（次の例を参照）。

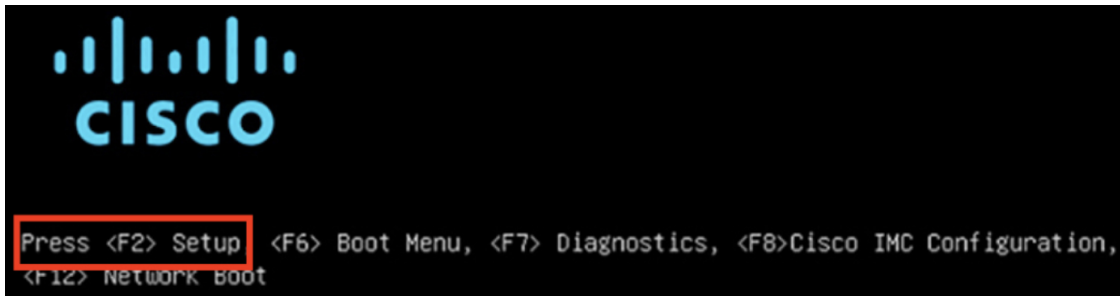


c) 次のいずれかを実行します。

- アプライアンスでこれらの2つのパラメータを設定する必要がある場合は、アプライアンスをリブートして、設定を続行します。この手順の残りを実行する必要はありません。
- 112コアアプライアンスの[I/O]タブにいずれか1つパラメータのみ表示されている場合は、ステップ3に進み、残りの手順を実行します。

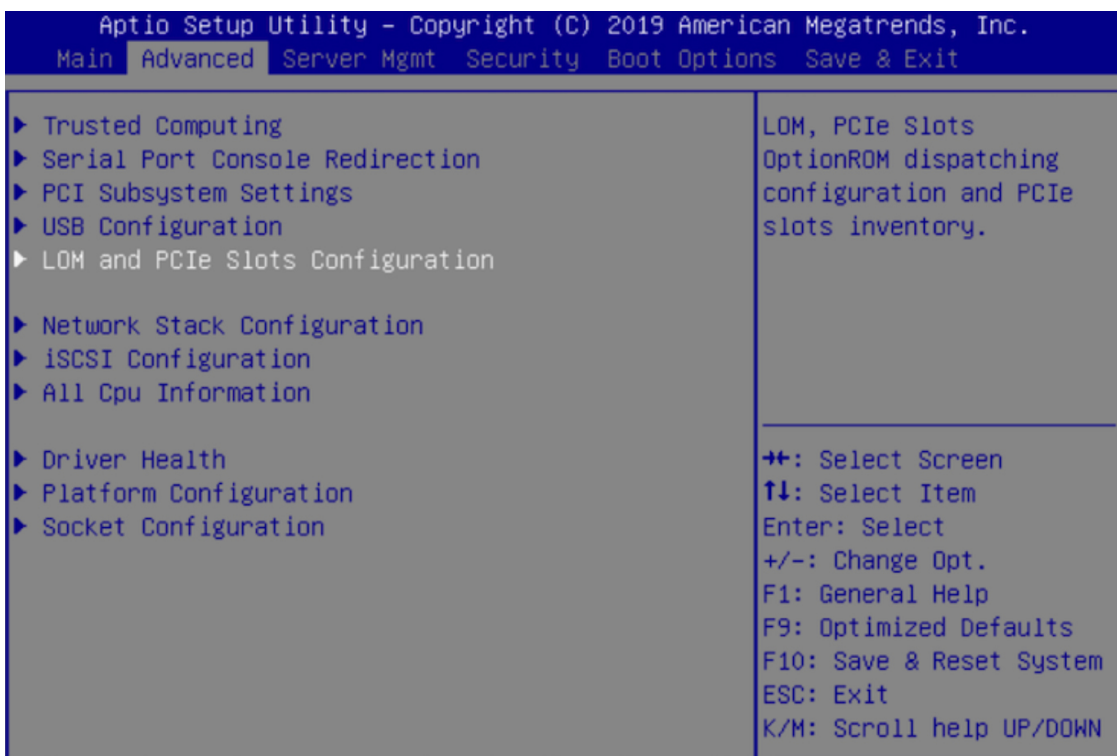
ステップ3 アプライアンスの BIOS を起動します。

- Cisco IMC から KVM セッションを開始します。
- [ホスト電源 (Host Power)] リンクをクリックしてから [電源の再投入 (Power Cycle)] を選択し、アプライアンスの電源を再投入します。
- 起動時に、次の画面が表示されたらすぐに **F2** キーを押してアプライアンスの BIOS を起動し、Aptio セットアップユーティリティを開きます。

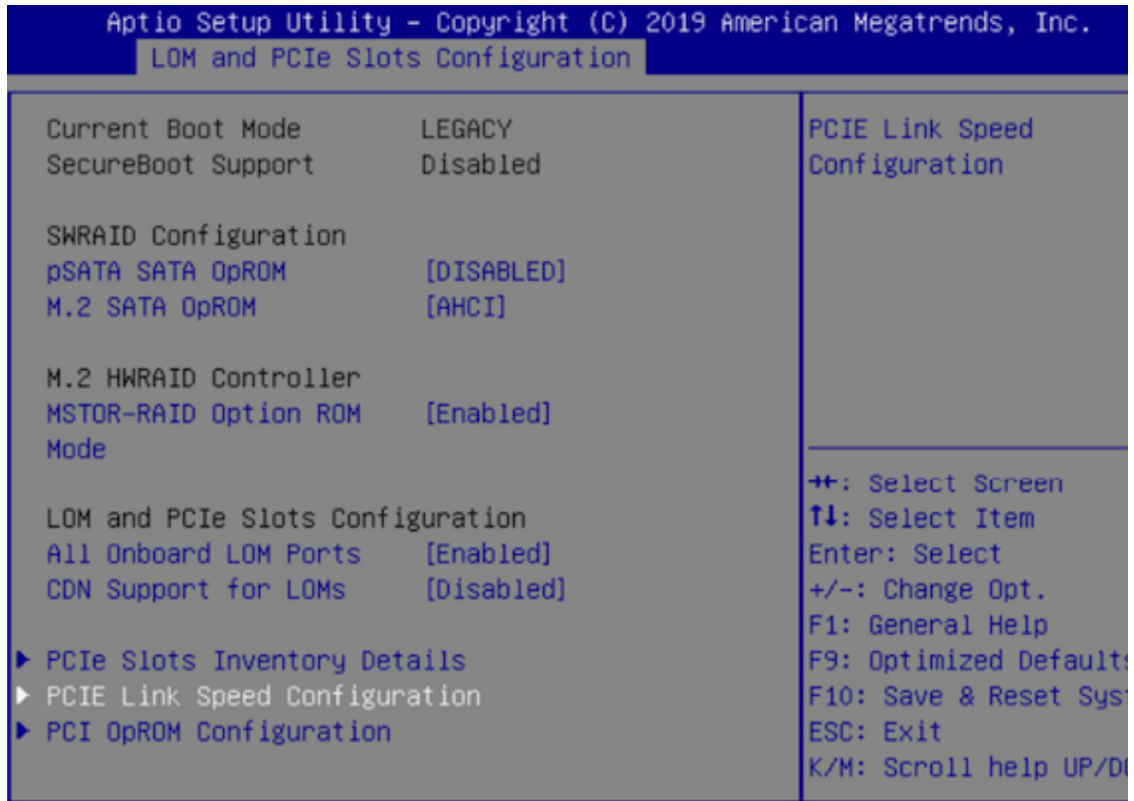


ステップ 4 PCIe カードを有効にします。

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

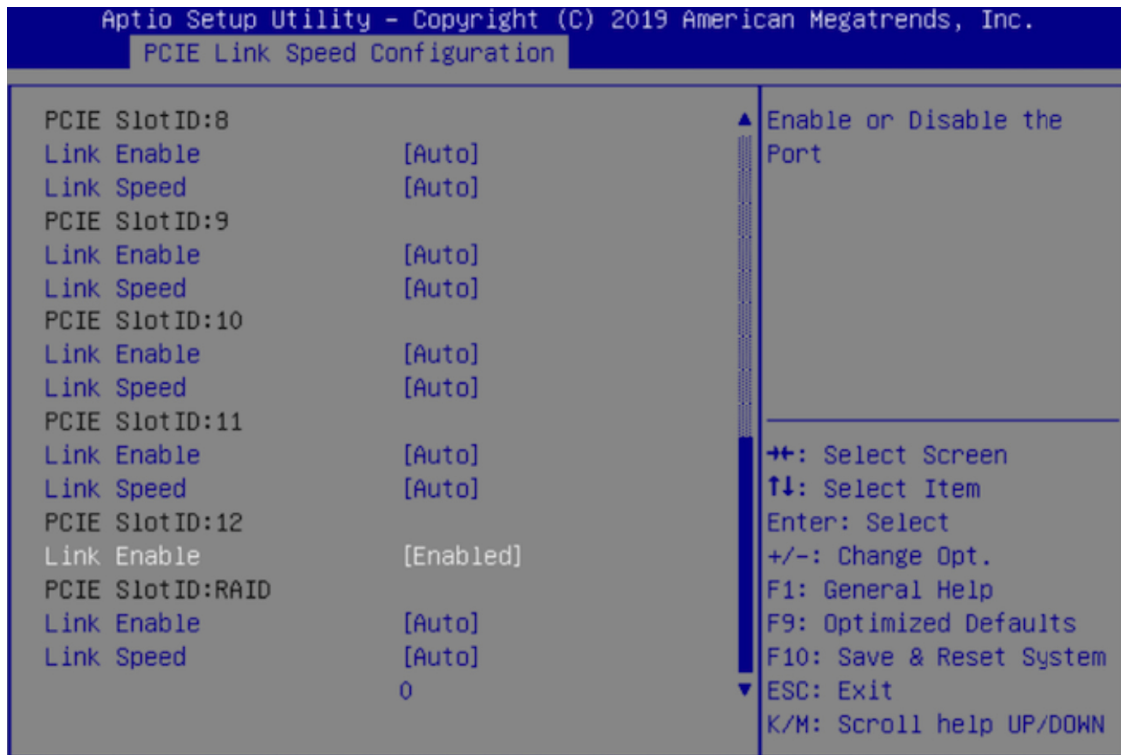


- b) [LOM および PCIe スロットの設定 (LOM and PCIe Slots Configuration)] タブで [PCIe リンク速度の設定 (PCIe Link Speed Configuration)] を選択します。

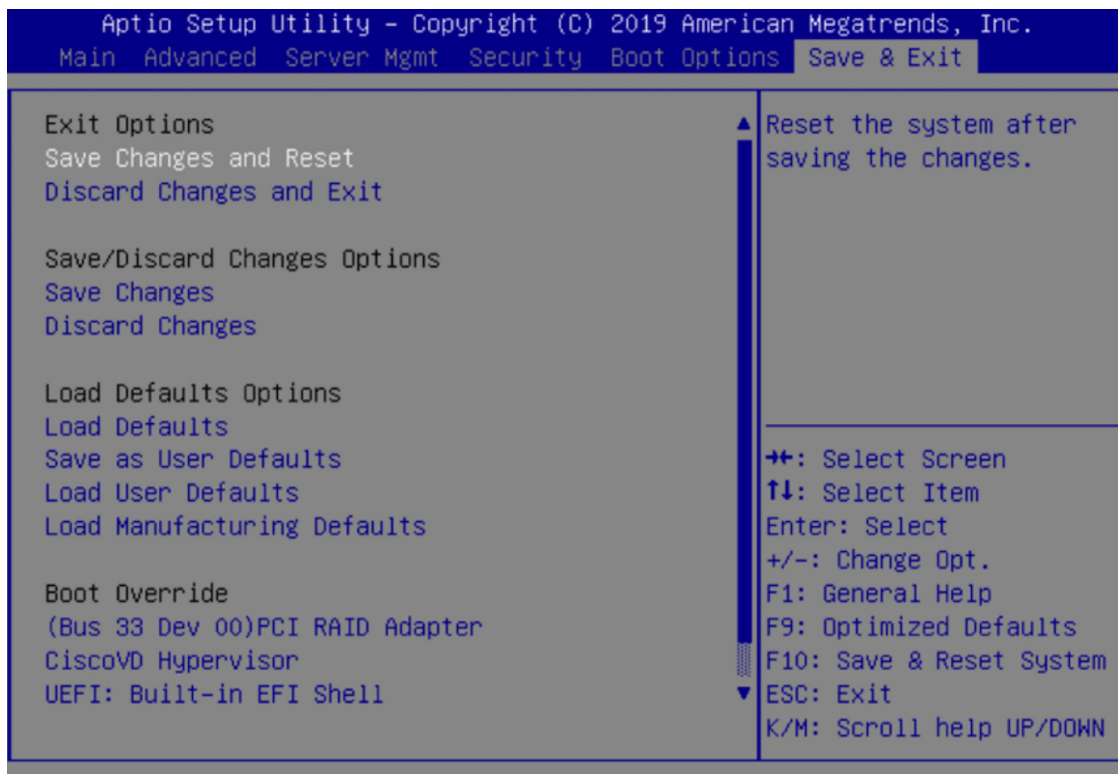


- c) [PCIe リンク速度の設定 (PCIe Link Speed Configuration)]タブを下向きにスクロールしてPCIe SlotID : 12 の [リンク有効化 (Link Enable)] オプションを見つけ、**Enter** を押します。
- d) [Enable] を選択し、Enter を押します。


次の例のような画面が表示されます。



- e) **ESC**キーを2回押してメインの BIOS メニューに戻り、[保存して終了 (Save & Exit)] タブを開きます。
- f) [変更を保存してリセット (Save Changes And Reset)] オプションを選択し、**Enter** を押します。



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

重要 アプライアンスの NIC を有効にした後、アプライアンスを Cisco IMC のデフォルト設定にリセットした場合 ( > [Admin] > [Utilities] > [Reset to factory Default])、この手順をもう一度実行する必要があります。

ステップ 5 Cisco DNA Center 2.3.5 にアップグレードします。

『Cisco DNA Center アップグレードガイド』で、現在のバージョンに固有のアップグレード手順を実行します。

アップグレード中に、Cisco DNA Center によって Intel X710-DA4 NIC を使用するようにアプライアンスが設定されます。アップグレードが完了し、アプライアンスがリブートすると、Cisco IMCはこのNICとNICにある4つのインターフェイスを認識します。Intel X710-DA2 NIC およびアプライアンスのマザーボードにある4つのインターフェイスを合わせると、アプライアンスのインターフェイスは合計で8つになります。

ステップ 6 [設定ウィザードを使用したアプライアンスの再設定 \(280 ページ\)](#) の説明に従って、構成ウィザードを完了し、アプライアンスで Intel X710-DA4 NIC を使用できるようにします。

アプライアンスのイメージの再作成

バックアップからの回復やクラスタリンク設定の変更など、Cisco DNA Center アプライアンス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 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 フラッシュドライブの作成](#)」を参照してください。
- ステップ 3** アプライアンスの RAID コントローラ：[Cisco DNA Center アプライアンスの仮想ドライブの再初期化](#) (90 ページ) によって管理されている仮想ドライブを再初期化します。
- ステップ 4** アプライアンスに 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 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 イメージの場所を把握します（電子メールを使用するか、シスコサポートチームと連絡を取ります）。

-
- ステップ 1** シスコが指定した場所から Cisco DNA Center イメージ (.iso、.bin、.zip) をダウンロードします。
- ステップ 2** シスコの指定した場所から署名検証用のシスコ公開キー (cisco_image_verification_key.pub) をダウンロードします。
- ステップ 3** シスコが指定した場所からイメージのセキュア ハッシュ アルゴリズム (SHA512) チェックサムファイルをダウンロードします。
- ステップ 4** シスコサポートから電子メールで、またはセキュアなシスコの Web サイト（利用可能な場合）からダウンロードして、イメージのシグニチャファイル (.sig) を入手します。
- ステップ 5** (オプション) SHA 検証を実行して、不完全なダウンロードによってイメージが破損していないかどうかを判定します。

オペレーティングシステムに応じて、次のコマンドのいずれかを実行します。

- Linux システムの場合：`sha512sum image-filename`

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

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

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

次に例を示します。

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

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

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

コマンドの出力とダウンロードした **SHA512** チェックサムファイルを比較します。コマンド出力が一致しない場合は、イメージを再度ダウンロードし、もう一度適切なコマンドを実行します。それでも出力が一致しない場合は、シスコサポートにお問い合わせください。

ステップ 6 署名を確認し、イメージが正規のものでシスコ製であることを確認します。

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

- (注) このコマンドは Mac と Linux の両方の環境で動作します。まだ **OpenSSL** をインストールしていない場合、Windows ではダウンロードしてインストールする必要があります ([こちらから入手可能](#))。

イメージが正規であれば、このコマンドを実行すると、「verified OK」というメッセージが表示されます。このメッセージが表示されない場合は、イメージをインストールせず、シスコサポートにお問い合わせください。

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

ブート可能な USB フラッシュドライブの作成

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

始める前に

- 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 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。



(注) Rufus ユーティリティを使用して Cisco DNA Center ISO イメージを書き込まないでください。Etcher、Linux CLI、または Mac CLI のみを使用してください。

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 アプライアンスの仮想ドライブの再初期化

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

- 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。
- ステップ 2** Cisco IMC GUI の左上隅から、**[Toggle Navigation]** アイコン (☰) をクリックします。
- ステップ 3** Cisco IMC メニューから、**[Storage] > [Cisco 12G Modular Raid Controller]** を選択します。
- ステップ 4** **[Virtual Drive Info]** タブをクリックします。
- ステップ 5** リストされている最初の仮想ドライブ (ドライブ番号 0) のチェックボックスをオンにして、**[Initialize]** をクリックします。
- ステップ 6** **[Initialize Type]** ドロップダウンリストから **[Full initialize]** を選択します。
- ステップ 7** **[Initialize VD]** をクリックします。
- ステップ 8** アプライアンスの残りの仮想ドライブにそれぞれステップ 5～7 を繰り返しますが、**[Fast Initialize]** を選択します (完全な初期化が必要なのは最初の仮想ドライブのみです。2 番目と 3 番目の仮想ドライブには、完全な初期化は必要ありません)。

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 フラッシュドライブの作成](#)」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、**[Cisco DNA Center 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、ブートローダーが自動的に Cisco DNA Center インストーラを起動します。

インストーラが再起動し、ウィザードのウェルカム画面が表示されます。プライマリクラスタノードを設定するのか、セカンダリクラスタノードを設定するのかに応じて、[Maglev ウィザードを使用したプライマリノードの設定 \(94 ページ\)](#) または [Maglev ウィザードを使用したセカンダリノードの設定 \(117 ページ\)](#) のステップ 4 に進みます。

Cisco DNA Center アプライアンスの設定

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。アプライアンスの再イメージ化を完了するには、[Maglev ウィザードを使用したアプライアンスの設定 \(93 ページ\)](#) の手順を実行します。



第 5 章

Maglev ウィザードを使用したアプライアンスの設定

- [アプライアンスの設定の概要 \(93 ページ\)](#)
- [Maglev ウィザードを使用したプライマリノードの設定 \(94 ページ\)](#)
- [Maglev ウィザードを使用したセカンダリノードの設定 \(117 ページ\)](#)
- [最新の Cisco DNA Center リリースへのアップグレード \(139 ページ\)](#)

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。初期展開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。
- **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。初期展開でクラスタモードを選択した場合は、セカンダリ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. クラスタのプライマリノードを設定します。 [Maglev ウィザードを使用したプライマリノードの設定 \(94 ページ\)](#) を参照してください。
2. 3 つのアプライアンスを設置し、クラスタに 2 番目と 3 番目のノードを追加する場合、「[Maglev ウィザードを使用したセカンダリノードの設定 \(117 ページ\)](#)」を参照してください。

Maglev ウィザードを使用した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セカンダリノードとしてインストールされたアプライアンスを設定する場合には、代わりに[Maglev ウィザードを使用したセカンダリノードの設定 \(117 ページ\)](#)に記載されている手順を実行します。



重要

- 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。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、(ネットワークのデバイスを検出してテレメトリを有効にするために完了する) クイック スタート ワークフローが開始されません。

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。
- 「[事前設定タスクの実行](#)」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 のリリースに対応する [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]** または **[HTML-based KVM]** 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 コンソールが別の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 **[Static IP Configuration]** 画面が表示されます。

Maglev ウィザードを使用したプライマリノードの設定

```

STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for
Enterprise Interface Configuration,
Static IP is configured as an alternative
to DHCP for web UI Configuration.
- Click Configure after entering
Information for configuring IP which will
be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4,
Please select IPV6 mode for Ipv6
Configuration

-----

STATIC IP CONFIGURATION

IPv6 mode

IP Address:
Netmask:
Default Gateway Address:
Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>

```

ステップ 4 [Skip] をクリックします。

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。

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

-----
Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

-----

< exit >

```

(注) DHCP サーバーによってアプライアンスのエンタープライズ インターフェイスに割り当てられた IP アドレス、サブネットマスク、およびデフォルトゲートウェイを使用せずに、ブラウザベースのウィザードのいずれかを使用してアプライアンスを構成するユーザーのみ、この画面を完了する必要があります。

ステップ 5 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。画面が更新されます。

```
Welcome to Maglev Configuration Wizard!

This wizard will walk you through the steps to configure this host. Select one of the options below to specify how would you like to configure this host:

Start using DNAC pre manufactured cluster
Start configuration of DNAC in advanced mode

< back >                                < exit >

This mode will enable you to stand up the DNAC Node in it's default manufactured state. This mode supports bringing up DNAC only in IPv4 mode. Use Advanced mode for deploying DNAC in IPv6 mode.
```

ステップ 6 次のいずれかのオプションを選択します。

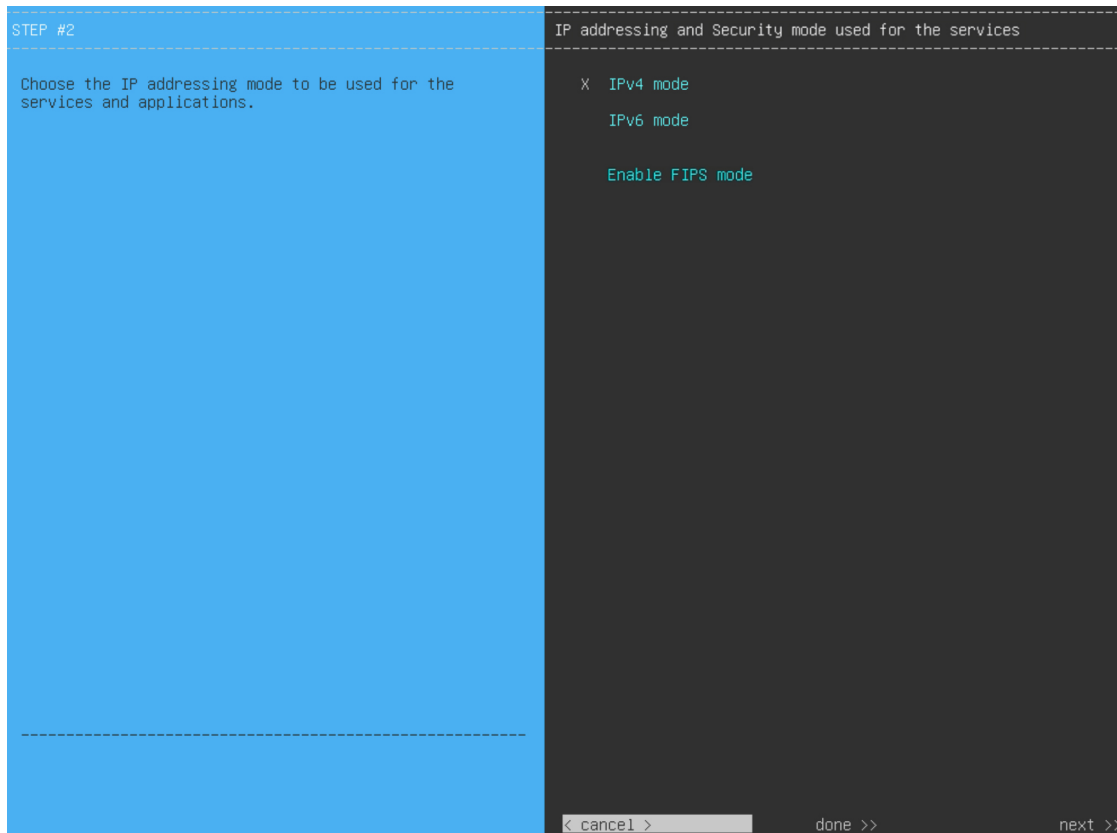
- [Start using DNAC pre manufactured cluster] : デフォルトの設定でアプライアンスを設定するには、このオプションを選択します。
 - クラスタ内インターフェイスの IP アドレス : 169.254.6.66
 - クラスタ内インターフェイスのサブネットマスク : 255.255.255.128
 - コンテナサブネット : 169.254.32.0/20
 - クラスタサブネット : 169.254.48.0/20
 - IPv4 アドレス指定
 - 管理スーパーユーザーのパスワード : maglev1@3

これらの設定はいずれも変更できないため、使用する場合にのみこのオプションを選択します。

重要 このオプションは、新しい Cisco DNA Center アプライアンスを設定する場合にのみ使用できます。アプライアンスのイメージを再作成する場合、[Start configuration of DNAC in advanced mode] オプションを選択してウィザードの操作を続行します。

- [Start configuration of DNAC in advanced mode] : 前述の箇条書きにリストされている1つ以上のデフォルト設定を使用しないアプライアンスを設定するには、このオプションを選択します。アプライアンスで IPv6 アドレッシングを使用する場合も、このオプションを選択します。

画面が更新されます。



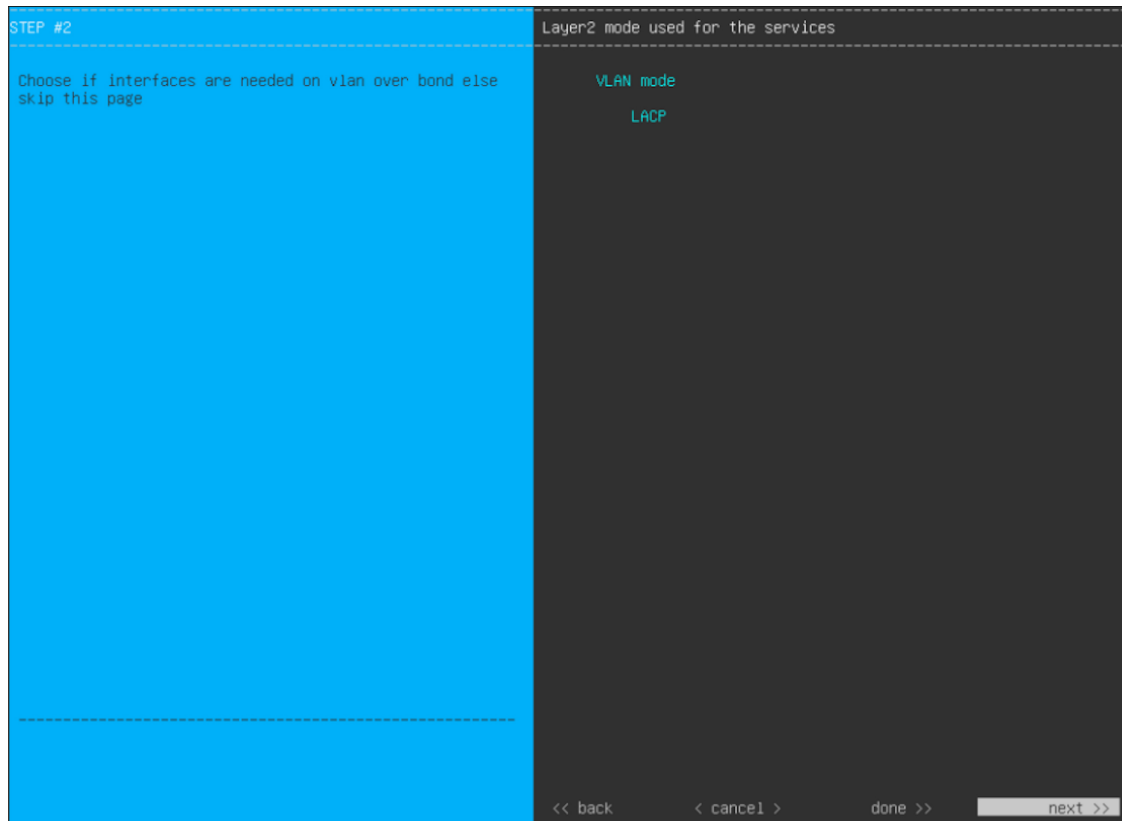
ステップ 7 次の手順を実行し、[next>>] をクリックして続行します。

- Cisco DNA Center アプライアンスで実行されているアプリケーションとサービスが IPv4 または IPv6 アドレッシングを使用するかどうかを指定します。
- (任意) Cisco DNA Center アプライアンスで FIPS モードを有効にするには、[Enable FIPS Mode] チェックボックスをオンにします。

アプライアンスで FIPS モードを有効にする際の注意事項については、[FIPS モードのサポート \(116 ページ\)](#) を参照してください。

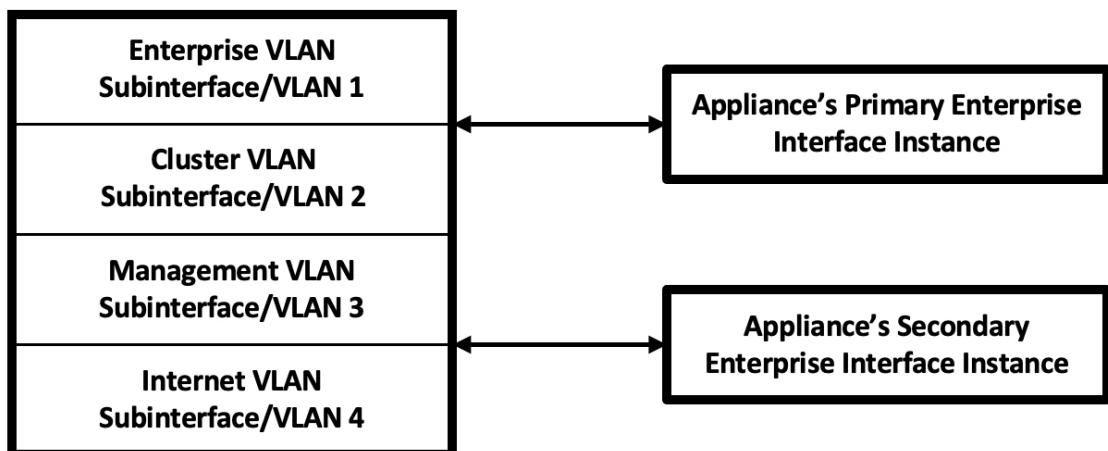
ステップ 8 (オプション) 次の手順を実行して、アプライアンスのレイヤ 2 ポートチャネルモード (VLAN タグ付き) を有効にします。このモードが有効になると、アプライアンスのエンタープライズインターフェイス

スのプライマリインスタンスとセカンダリインスタンスの両方を使用してネットワークに接続する、単一の結合インターフェイスが作成されます。選択したら、[next>>] をクリックして続行します。



- a) [VLAN mode] オプションを選択して dot1q/VLAN トランッキングを有効にし、アプライアンスのエンタープライズ、クラスター、管理、およびインターネットインターフェイスを、結合されたインターフェイス上にある VLAN サブインターフェイスに変換します（次の図を参照）。デフォルトでは、このインターフェイスはアクティブ バックアップ モード（HA を有効にする）で動作します。

Bonded Interface



- b) 代わりにこのインターフェイスを LACP モード（ロードバランシングとより高い帯域幅を有効にする）で動作させる場合は、[LACP] オプションも選択する必要があります。
- c) アプライアンスのエンタープライズインターフェイスの設定を入力するときは、[VLAN ID of Interface] フィールドに結合インターフェイスの一意の VLAN ID を入力してください。

重要

- 結合インターフェイス機能は、一般的には使用されません。Cisco DNA Center 展開で必要な場合にのみ有効にしてください。NIC ボンディングを有効にするだけの場合は、次の 2 つのウィザード画面で有効化できます。
- この機能は、次の展開タイプのいずれかが使用されていることを前提としています。
 - アプライアンスのエンタープライズ インターフェイスとクラスタインターフェイスが構成されている展開。
 - アプライアンスのエンタープライズ、クラスタ、および管理インターフェイスが構成されている展開。

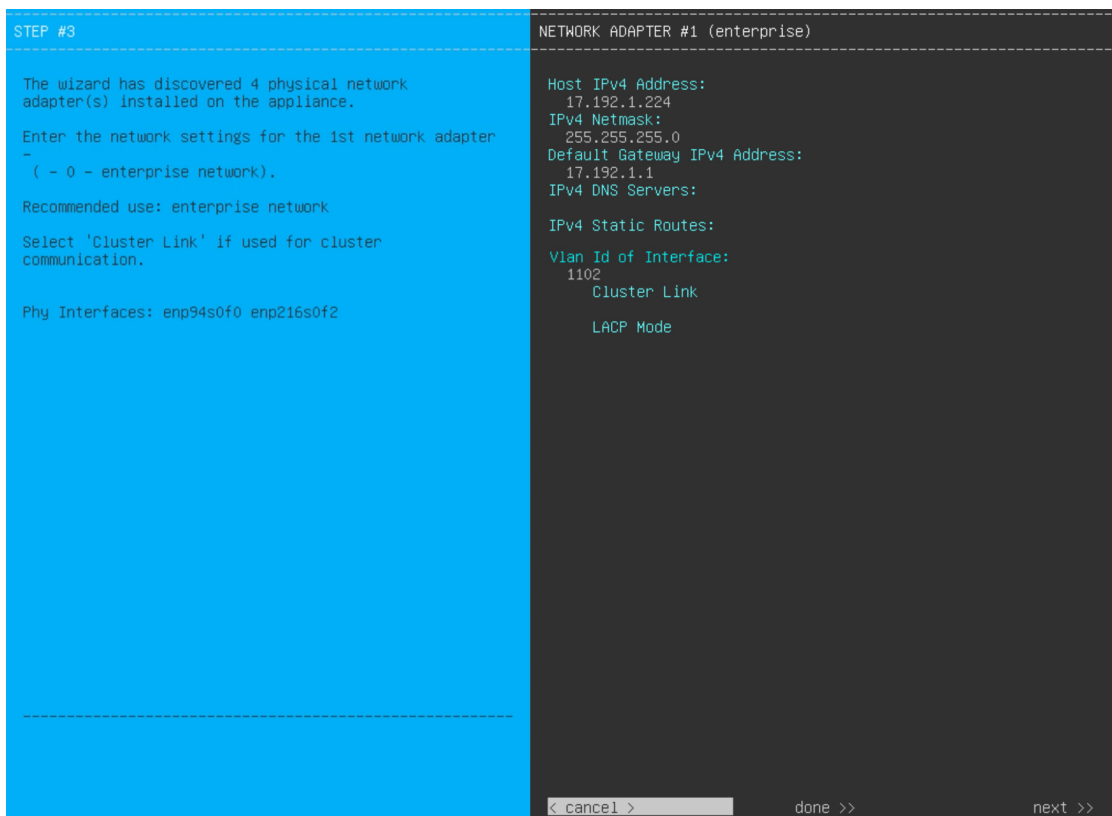
ウィザードでは、アプライアンス上のすべてのポートが検出され、次の順序で 1 つずつ別の画面に表示されます。

1. (必須) 10 Gbps エンタープライズポート—ネットワークアダプタ #1
2. (必須) 10 Gbps クラスタポート—ネットワークアダプタ #2
3. (任意) 1 Gbps/10 Gbps 管理ポート—ネットワークアダプタ #3
4. (任意) 1 Gbps/10 Gbps インターネットポート—ネットワークアダプタ #4

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、[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 に連絡したりする前に「事前設定タスクの実行」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「Get Assistance from the Cisco TAC」を参照してください）。

ステップ 9

ウィザードにより、最初に 10 Gbps エンタープライズポートが 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、アプライアンスをエンタープライズネットワークにリンクするために必要なポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「必要な IP アドレスおよびサブネット」と「必須の設定情報」を参照してください）。



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

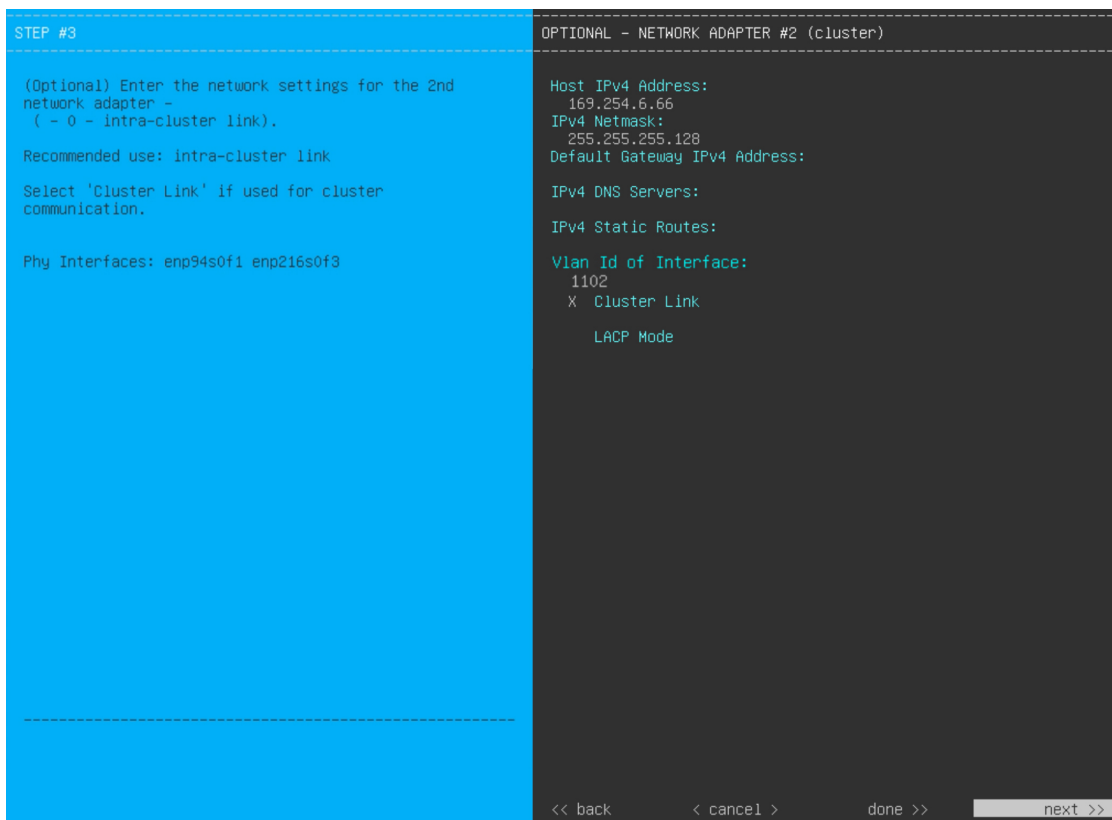
表 19: ネットワークアダプタ #1 のプライマリノードエントリ: 10 Gbps エンタープライズポート

[Host IPv4/IPv6 Address] フィールド	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。
[IPv4 Netmask/IPv6 Prefix Length] フィールド	次のいずれかを実行します。 <ul style="list-style-type: none"> • IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 • IPv6 アドレッシングを選択した場合は、プレフィックス長 (ビット単位) を入力します。有効な値の範囲は 10 ~ 127 です。
[Default Gateway IPv4/IPv6 Address] フィールド	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。 <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>

[IPv4/IPv6 DNS Servers] フィールド	<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>
[IPv4/IPv6 Static Routes] フィールド	<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><ネットワークマスク><ゲートウェイ>の形式で入力します。これは通常、Cisco DNA Center 管理ポートでのみ必要です。</p>
[Vlan Id of Interface] フィールド	<p>前の手順で有効にした結合インターフェイスの VLAN ID を入力します。有効にしていない場合、このフィールドは表示されません。</p>
[Cluster Link] フィールド	<p>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。</p>
[LACP Mode] フィールド	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2 つのイーサネットインターフェイスを 1 つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 このポートの [LACP] モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する 2 つのイーサネットインターフェイスが 1 つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p> <p>(注) このフィールドは、前の手順でオプションを選択しなかった場合に表示されます。</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 10 入力したエンタープライズポート値の検証が成功すると、ウィザードに 10 Gbps クラスタポートが [NETWORK ADAPTER #2] 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、ネットワークマスク、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 [NETWORK ADAPTER #2] の設定値を入力します。

表 20: ネットワークアダプタ #2 のプライマリノードエントリ: 10 Gbps クラスポート

[Host IPv4/IPv6 address] フィールド	<p>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。</p> <p>(注) 以前に [Start using DNAC pre manufactured cluster] オプションを選択した場合、[169.254.6.66] がこのフィールドにすでに設定されているため、別のアドレスを入力することはできません。</p>
[IPv4 Netmask/IPv6 Prefix Length] フィールド	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 <p>(注) 以前に [Start using DNAC pre manufactured cluster] オプションを選択した場合、[255.255.255.128] がこのフィールドにすでに設定されているため、別のネットマスクを入力することはできません。</p> <ul style="list-style-type: none"> IPv6 アドレッシングを選択した場合は、プレフィックス長 (ビット単位) を入力します。有効な値の範囲は 10 ~ 127 です。

[Default Gateway IPv4/IPv6 address] フィールド	<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>
[IPv4/IPv6 DNS Servers] フィールド	<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>
[IPv4/IPv6 Static Routes] フィールド	<p>1 つ以上のスタティックルートスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。</p>
[Cluster Link] フィールド	<p>このポートが Cisco DNA Center クラスタへのリンクであるとして設定するには、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>
[LACP Mode] フィールド	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2 つのイーサネットインターフェイスを 1 つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 このポートの [LACP] モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する 2 つのイーサネットインターフェイスが 1 つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p> <p>(注) このフィールドは、ステップ 8 でオプションを選択しなかった場合に表示されます。</p>

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 11 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/10 Gbps 管理ポートが [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）。

```

STEP #3
-----
(Optional) Enter the network settings for the 3rd
network adapter -
(- 0 - management network).

Recommended use: management network

Select 'Cluster Link' if used for cluster
communication.

Phy Interfaces: eno1 enp216s0f0

-----
OPTIONAL - NETWORK ADAPTER #3 (management)
-----
Host IPv4 Address:
172.29.131.224
IPv4 Netmask:
255.255.255.0
Default Gateway IPv4 Address:

IPv4 DNS Servers:
171.70.168.183 173.96.131.10
IPv4 Static Routes:
10.0.0.0/255.0.0.0/172.29.131.1 171.0.0.0/255.0.0.0/172.29.13
Cluster Link

<< back      < cancel >      done >>      next >>

```

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

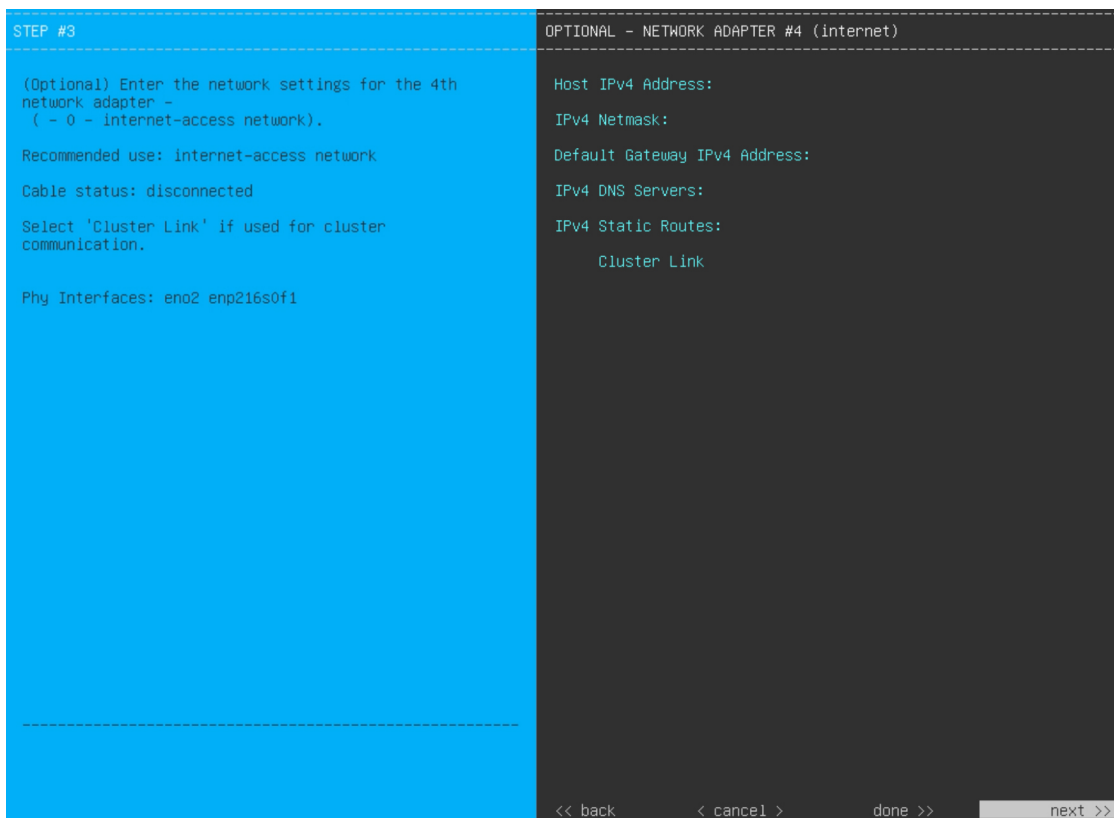
表 21: ネットワークアダプタ #3 のプライマリノードエントリ: 1 Gbps/10 Gbps 管理ポート

[Host IPv4/IPv6 address] フィールド	管理ポートの IP アドレスを入力します。これは、このポートを使用して管理ネットワークから Cisco DNA Center GUI にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。
[IPv4 Netmask/IPv6 Prefix Length] フィールド	IP アドレスを入力した場合は、次のいずれかを実行します。 <ul style="list-style-type: none"> IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。

[Default Gateway IPv4/IPv6 address] フィールド	<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>
[IPv4/IPv6 DNS Servers] フィールド	<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。
[IPv4/IPv6 Static Routes] フィールド	<p>1 つ以上のスタティックルートスペースで区切り、<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。</p>
[Cluster Link] フィールド	<p>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。</p>

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 12** 入力した管理ポート値の検証が成功すると、ウィザードに 1 Gbps/10 Gbps インターネットポートが [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](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、10 Gbps エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「[必要な IP アドレスおよびサブネット](#)」と「[必須の設定情報](#)」を参照してください）。



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

表 22: ネットワークアダプタ #4 のプライマリノードエントリ: 1 Gbps/10 Gbps インターネットポート

[Host IPv4/IPv6 address] フィールド	インターネットポートの 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インターネット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、空白のままにできます。
[IPv4 Netmask/IPv6 Prefix Length] フィールド	IP アドレスを入力した場合は、次のいずれかを実行します。 <ul style="list-style-type: none"> • IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 • IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。
[Default Gateway IPv4/IPv6 address] フィールド	インターネット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。 <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>

[IPv4/IPv6 DNS Servers] フィールド	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。
[IPv4/IPv6 Static Routes] フィールド	1 つ以上のスタティックルートスペースで区切り、<ネットワーク><ネットマスク><ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。
[Cluster Link] フィールド	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 13 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、ユーザーの使用する **[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。

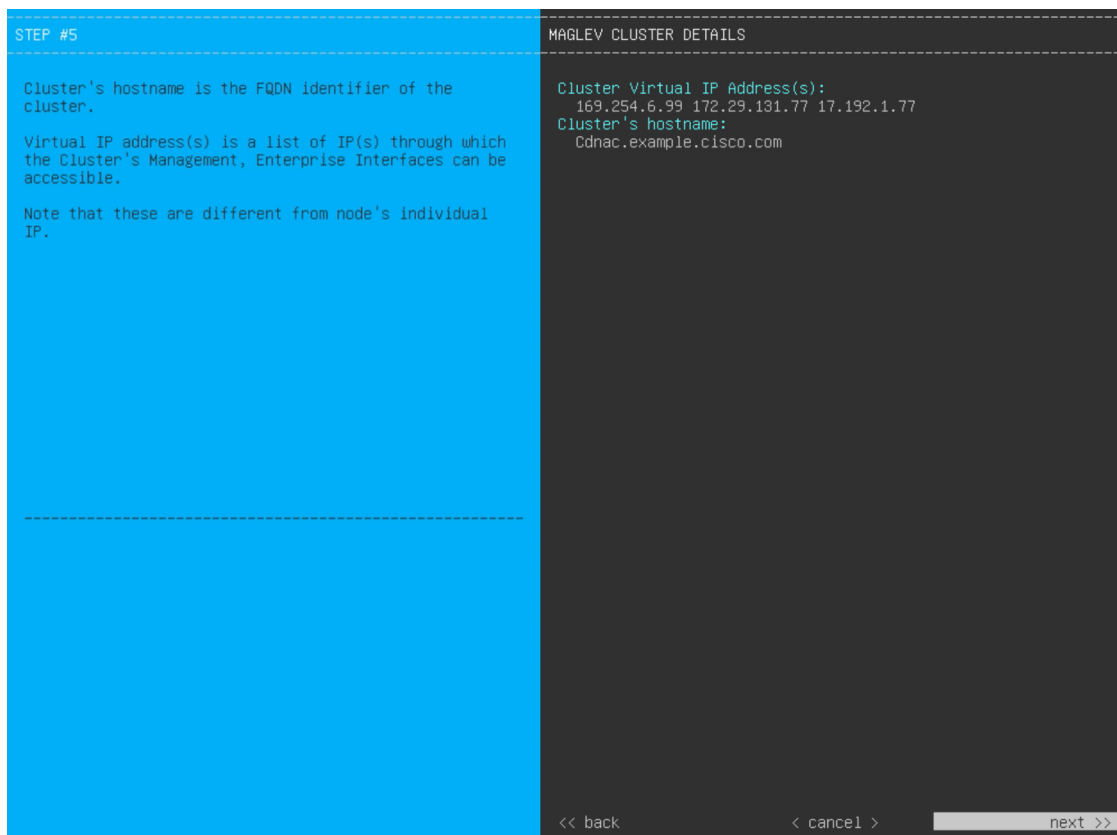
次の表に示すように **[NETWORK PROXY]** の設定値を入力します。

表 23: 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 (HTTPS Proxy)] フィールド	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> • 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。 • ポート番号を含む IPv6 URL を入力する場合は、URL の IP アドレス部分を角カッコで囲みます。次の例では、443 がポート番号です。 http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/
[HTTPS Proxy Username] フィールド	<p>ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。</p>
[HTTPS Proxy Password] フィールド	<p>ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。</p>

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 14 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次のステップに進みます。

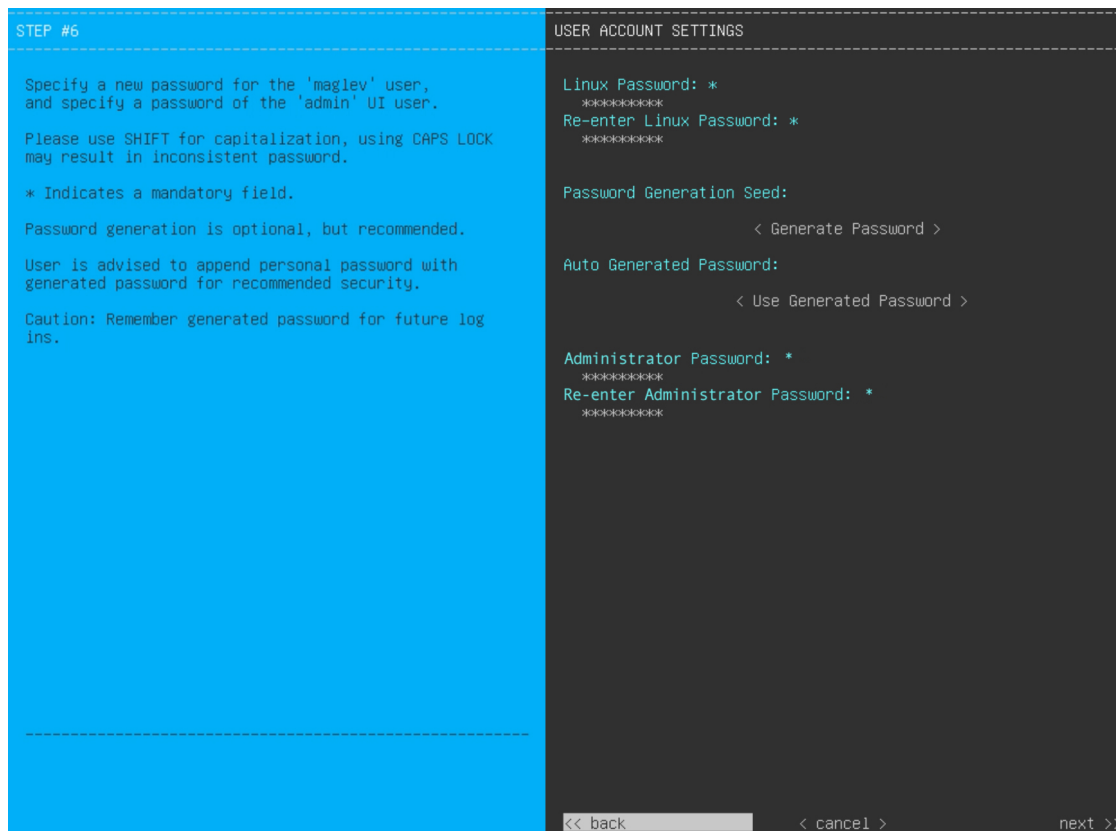
重要 設定済みのネットワークインターフェイスごとに1つずつ仮想 IP アドレスを入力する必要があります。この操作を行わない限り、ウィザードを完了することはできません。これらのアドレスは、クラスタリンクのステータスに関連付けられており、ステータスは[UP]の状態となっている必要があります。

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 15 クラスタの詳細を入力すると、次に示すように [USER ACCOUNT SETTINGS] の値を入力するためのウィザードのプロンプトが表示されます。



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

表 24: ユーザアカウント設定のプライマリノードエントリ

[Linux Password] フィールド	8 文字以上の長さの maglev ユーザーの Linux パスワードを入力します。
[Re-enter Linux Password] フィールド	Linux パスワードをもう一度入力して確認します。
[Password Generation Seed] フィールド	Linux パスワードを自分で作成しない場合には、このフィールドにシードフレーズを入力してから、[パスワードの生成 (Generate password)] を押してパスワードを生成します。
[Auto Generated Password] フィールド	(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。

[Administrator Password] フィールド	<p>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。</p> <p>次の点に注意してください。</p> <ul style="list-style-type: none"> • ウィザードの早い段階で FIPS モードを有効にした場合は、このパスワードが 8 文字以上であることを確認してください。 • 以前の手順で [Start using DNAC pre manufactured cluster] オプションを選択した場合、アプライアンスにはデフォルトのパスワード (maglev1@3) がすでに設定されているため、構成ウィザードで変更することはできません。その結果、このフィールドと次のフィールドはこの画面に表示されません。
[Re-enter Administrator Password] フィールド	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 16 ユーザーアカウントの詳細を入力すると、[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。

<p>STEP #7</p> <p>Enter the IP address of the NTP server that the controller will use.</p> <p>It is recommended to specify 3 or more NTP servers to improve availability and time accuracy.</p> <p>Please note that the NTP server(s) must be accessible in order for the configuration to succeed.</p> <p>* Indicates a mandatory field</p>	<p>NTP SERVER SETTINGS</p> <p>NTP Servers: *</p> <p>ntp.es1.example.com ntp1.es1.example.com ntp2.es1.example.com</p> <p>NTP Authentication</p> <p><< back < cancel > next >></p>
--	---

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

[NTP Server (NTP サーバ)] フィールド	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。
[NTP Authentication] チェックボックス	<p>Cisco DNA Center と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> • NTP サーバーのキー ID。有効な値の範囲は $1 \sim 4294967295$ ($2^{32}-1$) です。 この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。 • NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。 <p>(注) 前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。</p>

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 17 適切な NTP サーバーを指定した後、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。

(注) 以前の手順で [Start using DNAC pre manufactured cluster] オプションを選択した場合、アプライアンスにはデフォルトのコンテナおよびクラスタサブネットがすでに設定されているため、構成ウィザードで変更することはできません。その結果、次のウィザード画面は表示されません。ステップ 17 に進みます。

STEP #8	MAGLEV ADVANCED SETTINGS
<p>Enter the IP networks for cluster services network and api network to use.</p> <p>These networks shouldn't overlap with the existing enterprise network.</p> <p>The maximum and minimum recommended size for each networks are /12 and /21 subnets respectively.</p> <p>* Indicates a mandatory field.</p>	<pre> Container subnet: * 169.254.32.0/20 Cluster subnet: * 169.254.48.0/20 Enable Intracluster IPSec </pre> <p style="text-align: right;"> << back cancel > next >> </p>

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

表 25: Maglev 詳細設定のプライマリノードエントリ

[Container Subnet] フィールド	<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 (33 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>
--------------------------	---

[Cluster Subnet] フィールド	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 (33 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。
[Enable Intracluster IPsec] チェックボックス	3 ノードの高可用性 (HA) クラスタ内のノード間の IPsec 接続を有効にする場合にオンにします。

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 18 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)。

```
The wizard is now ready to apply the configuration on the controller.
Use the [back] button below to verify/modify controller settings.
Use the [cancel] button to discard your changes and exit the wizard.
Use the [proceed] button to save your changes and proceed with applying them on the controller.
```

<< back < cancel > proceed >>

[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。

構成プロセスの最後に、アプライアンスの電源を再投入すると、「CONFIGURATION SUCCEEDED!」というメッセージが表示されます。

```
CONFIGURATION SUCCEEDED
The configuration wizard has completed successfully!
To access the Maglev Web UI, please point your browser to one of the following URLs:

To access the Maglev Web Console, please point your browser to one of the following URLs:
https://17.192.1.224
https://169.254.6.66
https://172.29.131.224

The wizard will automatically close in 30 seconds
```

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。
- 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 番目のインストール済みアプライアンスを設定します（[Maglev ウィザードを使用したセカンダリノードの設定](#)（117 ページ））。

FIPS モードのサポート

Cisco DNA Center は連邦情報処理標準（FIPS）をサポートしています。これは、暗号化アルゴリズムの導入、キー情報とデータバッファの処理、およびオペレーティングシステムの操作に関するベストプラクティスを指定する政府認証標準です。アプライアンスで FIPS モードを有効にする場合は、次の点に注意してください。

- 以前の Cisco DNA Center バージョンからアップグレードされたアプライアンスでは FIPS モードを有効化できません。最新バージョンがすでにインストールされているアプライアンスでのみ有効化できます。
- FIPS モードが有効になっている場合、URL からイメージをインポートすることはできません。コンピュータまたは cisco.com からのみイメージをインポートできます。
- [USER ACCOUNT SETTINGS] 画面で、デフォルトの管理スーパーユーザー用に 8 文字以上のパスワードを入力する必要があります。
- アプライアンスで FIPS モードが有効になっている場合、外部認証を有効にすることはできません。
- Maglev 設定ウィザードの完了時に [Start using DNAC pre manufactured cluster] オプションを選択した場合、[IP addressing and Security mode used for the services] 画面は表示されません。その結果、FIPS モードを有効化できません。
- Cisco DNA Center は、FIPS モードが有効になっている場合、SNMPv2c デバイスクレデンシャルをサポートしません。代わりに、SNMPv3 クレデンシャルを指定する必要があります。

- アプライアンスで FIPS モードを有効化した後で、無効化できる唯一の方法は、アプライアンスのイメージを再作成することです（既存のデータをすべて消去するため）。その後、FIPS モードを無効化してアプライアンスを再構成できます。詳細については、「[アプライアンスのイメージの再作成（86 ページ）](#)」を参照してください。
- FIPS モードが有効になっている場合、KeyWrap を有効化できるのは、Cisco DNA Center と Cisco ISE がまだ統合されていない場合のみです。詳細については、「[認証サーバとポリシー サーバの設定（273 ページ）](#)」を参照してください。
- アプライアンスを構成した後、次の操作を実行して、FIPS モードが有効になっているかどうかを確認できます。
 1. アプライアンスの SSH コンソールを開き、`ssh -p 2222 maglev@appliance's-IP-address` コマンドを実行します。
 2. デフォルトの管理スーパーユーザーのパスワードを入力して、アプライアンスにログインします。
 3. `magctl fips status` コマンドを実行します。
- Cisco Wide Area Bonjour アプリケーションは FIPS モードをサポートしていません。そのため、このアプリケーションを Cisco DNA Center GUI または CLI からインストールすることはできません。
- FIPS モードが有効になっている場合、エンドポイント分析に関連する一部の機能は Cisco DNA Center GUI で使用できません。
- FIPS モードは、マップアーカイブのエクスポートとインポートに影響します。

FIPS モードが有効の場合：

 - エクスポートされるマップアーカイブは暗号化されません。
 - 暗号化されていないマップアーカイブのみをインポートできます。

FIPS モードが無効の場合：

 - エクスポートされるマップアーカイブは暗号化されます。
 - 暗号化されたマップアーカイブと暗号化されていないマップアーカイブの両方をインポートできます。

Maglev ウィザードを使用したセカンダリノードの設定

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。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、（ネットワークのデバイスを検出してテレメトリを有効にするために完了する）クイック スタート ワークフローが開始されません。
- 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。

新しいセカンダリ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。クラスタにセカンダリ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、セキュアシェルを使用して、プライマリノードの Cisco DNA Center 管理ポートに Linux ユーザ（maglev）としてログインしてから、`maglev package status` コマンドを実行します。インストールされているすべてのパッケージは、コマンド出力で「展開済み (DEPLOYED)」と表示されます。

```

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]
NAME                               DISPLAY_NAME                               DEPLOYED    AVAILABLE    STATUS    PROGRESS
-----
access-control-application         Access Control Application                 -           2.1.369.60050 NOT_DEPLOYED
ai-network-analytics               AI Network Analytics                      -           2.6.10.494   NOT_DEPLOYED
app-hosting                        Application Hosting                       -           1.6.6.2201241723 NOT_DEPLOYED
application-policy                 Application Policy                         -           2.1.369.170033 NOT_DEPLOYED
application-registry               Application Registry                       -           2.1.369.170033 NOT_DEPLOYED
application-visibility-service     Application Visibility Service            -           2.1.369.170033 NOT_DEPLOYED
assurance                           Assurance - Base                          2.2.2.485   -           DEPLOYED
automation-core                   NCP - Services                           2.1.368.60015 2.1.369.60050 DEPLOYED
base-provision-core                Automation - Base                         2.1.368.60015 2.1.369.60050 DEPLOYED
cloud-connectivity-contextual-content Cloud Connectivity - Contextual Content 1.3.1.364   -           DEPLOYED
cloud-connectivity-data-hub        Cloud Connectivity - Data Hub             1.6.0.380   -           DEPLOYED
cloud-connectivity-tethering        Cloud Connectivity - Tethering            2.12.1.2    -           DEPLOYED
cloud-provision-core               Cloud Device Provisioning Application     2.1.368.60015 2.1.369.60050 NOT_DEPLOYED
command-runner                     Command Runner                            2.1.368.60015 2.1.369.60050 DEPLOYED
device-onboarding                  Device Onboarding                         2.1.368.60015 2.1.369.60050 DEPLOYED
disaster-recovery                  Disaster Recovery                          -           2.1.367.360196 NOT_DEPLOYED
dna-core-apps                      Network Experience Platform - Core       2.1.368.60015 2.1.369.60050 DEPLOYED
dnac-platform                     Cisco DNA Center Platform                 1.5.1.180   1.5.1.182   DEPLOYED
dnac-search                        Cisco DNA Center Global Search           1.5.0.466   -           DEPLOYED
endpoint-analytics                 AI Endpoint Analytics                     -           1.4.375     NOT_DEPLOYED
group-based-policy-analytics        Group-Based Policy Analytics              -           2.2.1.401   NOT_DEPLOYED
icap-automation                    Automation - Intelligent Capture          -           2.1.369.60050 NOT_DEPLOYED
image-management                   Image Management                          2.1.368.60015 2.1.369.60050 DEPLOYED
machine-reasoning                  Machine Reasoning                         2.1.368.210017 2.1.369.210024 DEPLOYED
ncp-system                         NCP - Base                               2.1.368.60015 2.1.369.60050 DEPLOYED
ndp-base-analytics                 Network Data Platform - Base Analytics    1.6.1028    1.6.1031    DEPLOYED
ndp-platform                       Network Data Platform - Core              1.6.596     -           DEPLOYED
ndp-ui                             Network Data Platform - Manager          1.6.543     -           DEPLOYED
network-visibility                  Network Controller Platform              2.1.368.60015 2.1.369.60050 DEPLOYED
path-trace                          Path Trace                                2.1.368.60015 2.1.369.60050 DEPLOYED
platform-ui                         Cisco DNA Center UI                       1.6.2.448   1.6.2.448   DEPLOYED
rbac-extensions                     RBAC Extensions                          2.1.368.1910001 2.1.369.1910003 DEPLOYED
rogue-management                   Rogue and aWIPS                           -           2.2.0.51    NOT_DEPLOYED
sd-access                           SD Access                                 -           2.1.369.60050 NOT_DEPLOYED
sensor-assurance                   Assurance - Sensor                         -           2.2.2.484   NOT_DEPLOYED
sensor-automation                  Automation - Sensor                       -           2.1.369.60050 NOT_DEPLOYED
ssa                                Stealthwatch Security Analytics           2.1.368.1091226 2.1.369.1091317 DEPLOYED
system                             System                                     1.6.594     -           DEPLOYED
system-commons                     System Commons                            2.1.368.60015 2.1.369.60050 DEPLOYED
umbrella                           Cisco Umbrella                            -           2.1.368.592066 NOT_DEPLOYED
wide-area-bonjour                   Wide Area Bonjour                         -           2.4.368.75006 NOT_DEPLOYED

```

[Wed Nov 30 15:45:08 UTC] maglev@192.0.2.1 (maglev-master-192.0.2.1) ~

- 各セカンダリノードのクラスタ接続プロセス中に、一部のサービスのダウンタイムが発生することが予想されます。サービスはすべてのノードに再配布される必要があり、そのプロセスの間、クラスタはダウンします。

始める前に

次のことを確認します。

- Maglev ウィザードを使用したプライマリノードの設定 (94 ページ) 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。
 - 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。
 - 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、両方のセカンダリアプライアンスで Cisco IMC に対するブラウザのアクセス権が設定されたこと。

- 「事前設定タスクの実行」の説明に従って、セカンダリアプライアンスのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- 互換性のあるブラウザを使用していること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]** または **[HTML-based KVM]** 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 コンソールが別の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。

リポートメッセージが表示された後、KVM コンソールに [Static IP Configuration] 画面が表示されます。

```
STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration,
Static IP is configured as an alternative to DHCP for web UI Configuration.
- Click Configure after entering Information for configuring IP which will
be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4,
Please select IPv6 mode for Ipv6 Configuration

-----

STATIC IP CONFIGURATION

IPv6 mode
IP Address:
Netmask:
Default Gateway Address:
Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>
```

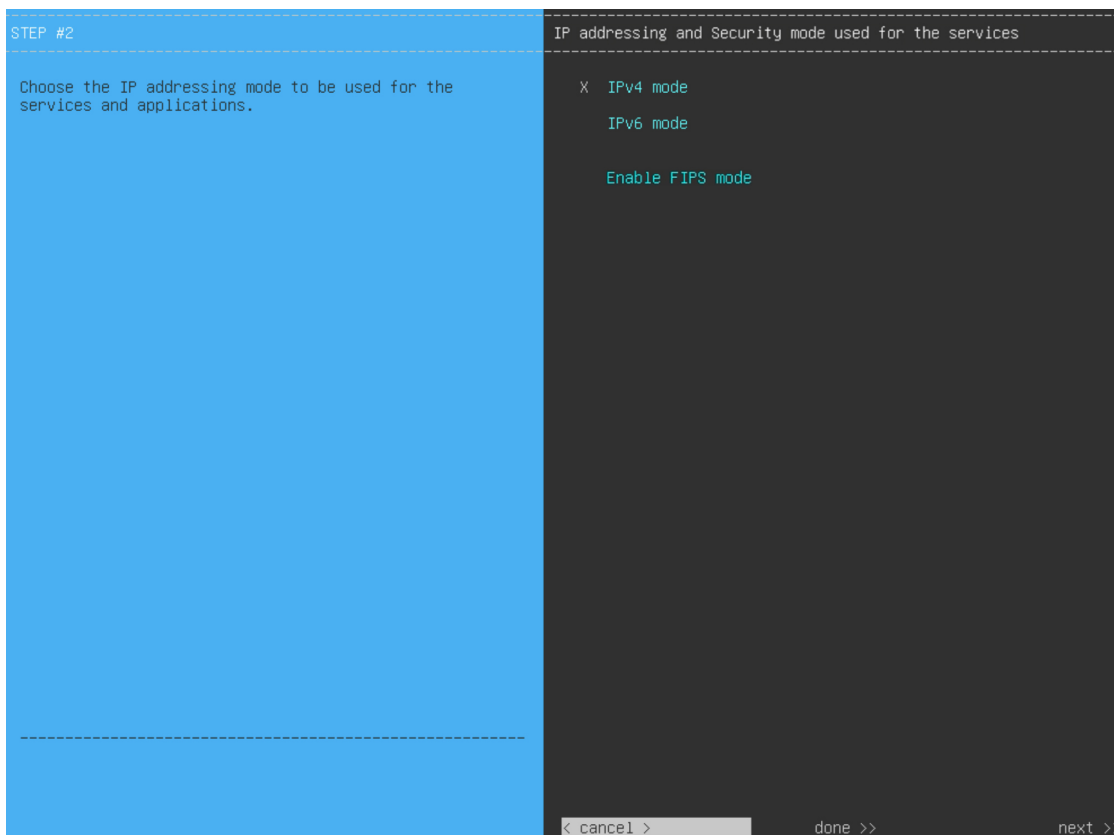
ステップ 4 [Skip] をクリックします。

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。

```
Welcome to the Maglev Configuration Wizard!  
The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you  
would like to configure this host:  
  
Start a Cisco DNA Center Cluster  
Join a Cisco DNA Center Cluster  
  
< exit >
```

(注) DHCP サーバーによってアプライアンスのエンタープライズ インターフェイスに割り当てられた IP アドレス、サブネットマスク、およびデフォルトゲートウェイを使用せずに、ブラウザベースのウィザードのいずれかを使用してアプライアンスを構成するユーザーのみ、この画面を完了する必要があります。

ステップ 5 [Join a Cisco DNA Center Cluster] を選択して、セカンダリノードの設定を開始します。
画面が更新されます。



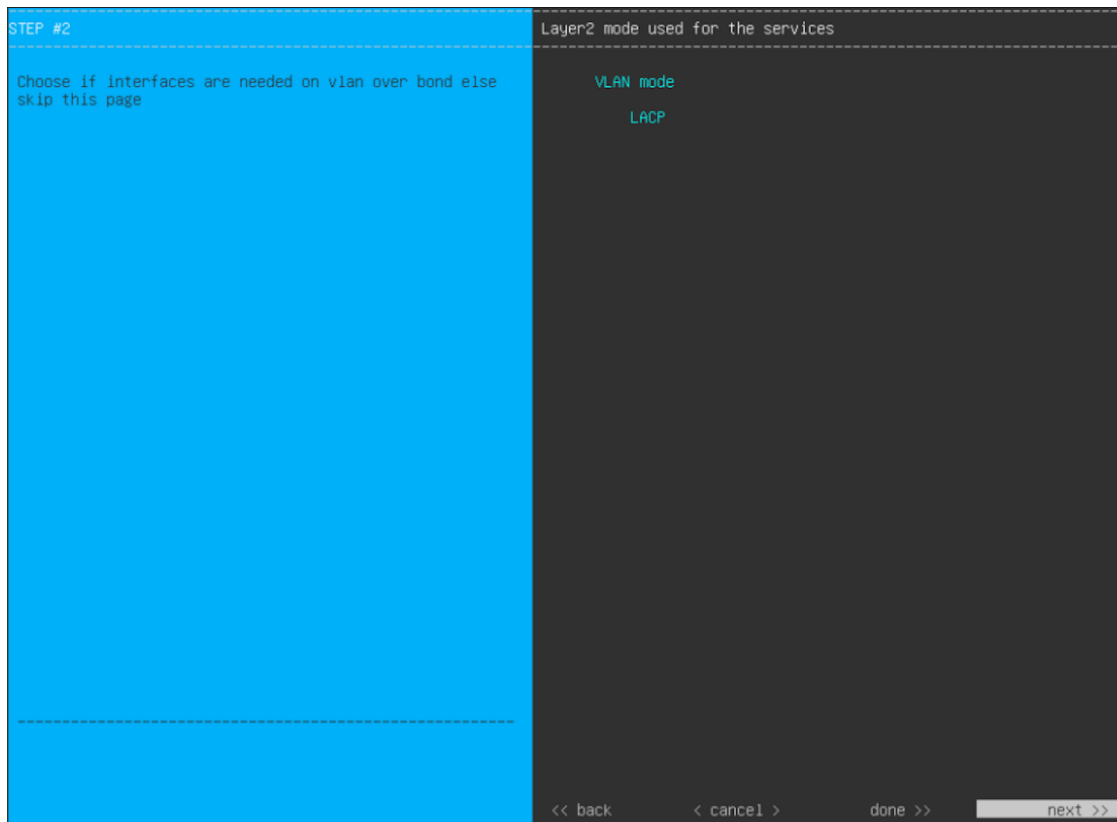
ステップ 6 次の手順を実行し、[next>>] をクリックして続行します。

- Cisco DNA Center アプライアンスで実行されているアプリケーションとサービスが IPv4 または IPv6 アドレッシングを使用するかどうかを指定します。
- (任意) Cisco DNA Center アプライアンスで FIPS モードを有効にするには、[Enable FIPS Mode] チェックボックスをオンにします。

アプライアンスで FIPS モードを有効にする際の注意事項については、[FIPS モードのサポート \(116 ページ\)](#) を参照してください。

ステップ 7 (オプション) アプライアンスのレイヤ 2 LACP ポートチャンネルモード (VLAN タギングあり) を設定するには、[VLAN mode] オプションと [LACP] オプションの両方を選択します。選択したら、[next>>] をクリックして続行します。

重要 [VLAN mode] オプションは dot1q/VLAN トランッキングを有効にし、[LACP] オプションは NIC ボンディングモードを有効にして、アプライアンスのエンタープライズ インターフェイスおよびクラスタ内インターフェイスにロードバランシングとより高い帯域幅を提供します。このオプションの組み合わせは一般的には使用されないため、Cisco DNA Center の展開で必要な場合にのみ両方を選択してください。NIC ボンディングのみを有効にする場合は、次の 2 つのウィザード画面で有効にできます。

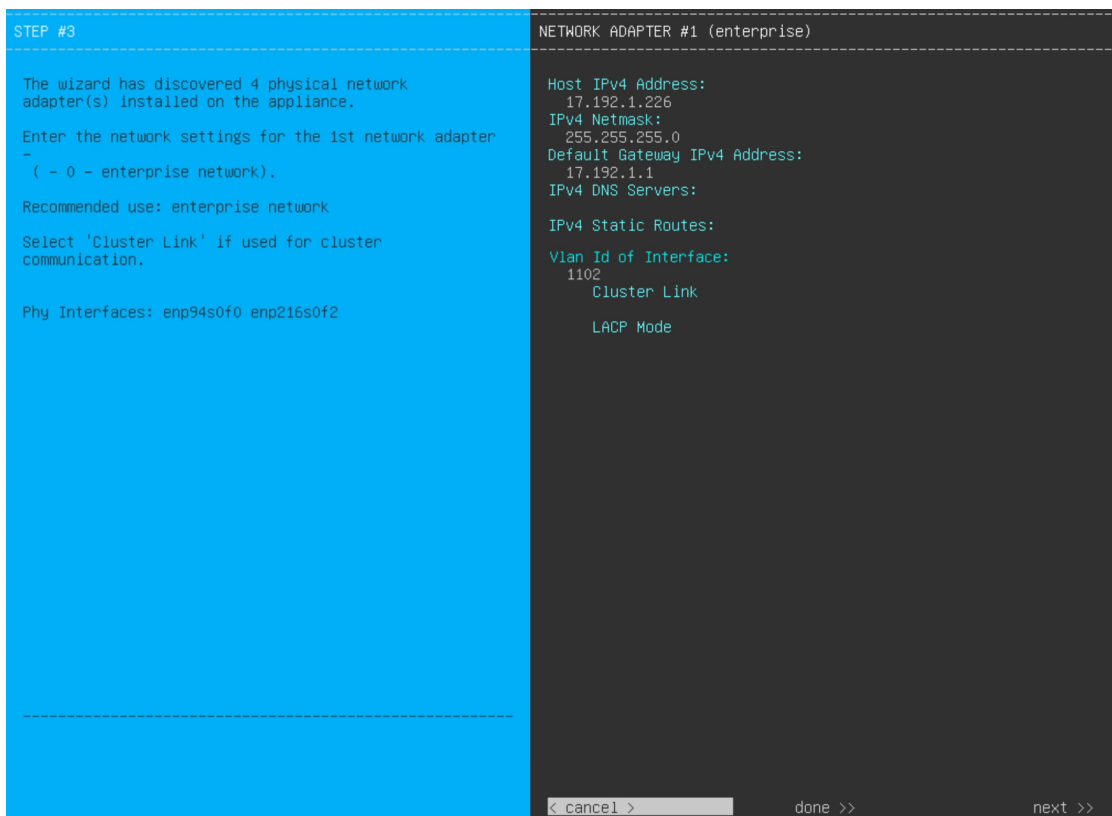


ウィザードでは、アプライアンス上のすべてのポートが検出され、次の順序で1つずつ別の画面に表示されます。

1. (必須) 10 Gbps エンタープライズポート—ネットワークアダプタ #1
2. (必須) 10 Gbps クラスタポート—ネットワークアダプタ #2
3. (任意) 1 Gbps/10 Gbps 管理ポート—ネットワークアダプタ #3
4. (任意) 1 Gbps/10 Gbps インターネットポート—ネットワークアダプタ #4

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、**[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 に連絡したりする前に「[事前設定タスクの実行](#)」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「[Get Assistance from the Cisco TAC](#)」を参照してください）。

ステップ 8 ウィザードにより、最初に 10 Gbps エンタープライズポートが 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、アプライアンスをエンタープライズネットワークにリンクするために必要なポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「[必要な IP アドレスおよびサブネット](#)」と「[必須の設定情報](#)」を参照してください）。



次の表のとおり [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 26: ネットワークアダプタ #1 のセカンダリノードエントリ: 10 Gbps エンタープライズポート

[Host IPv4/IPv6 Address] フィールド	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。
[IPv4 Netmask/IPv6 Prefix Length] フィールド	IP アドレスを入力した場合は、次のいずれかを実行します。 <ul style="list-style-type: none"> • IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 • IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。
[Default Gateway IPv4/IPv6 address] フィールド	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。 <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>

[IPv4/IPv6 DNS Servers] フィールド	<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>
[IPv4/IPv6 Static Routes] フィールド	<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><ネットワークマスク><ゲートウェイ>の形式で入力します。これは通常、Cisco DNA Center 管理ポートでのみ必要です。</p>
[Vlan Id of Interface] フィールド	<p>設定するアプライアンス用に作成される LACP リンク上でタグ付けされる VLAN ID を入力します。</p> <p>(注) このフィールドは、前の手順で両方のオプションを選択してアプライアンスのレイヤ 2 LACP ポートチャネルモードを設定した場合にのみ表示されます。</p>
[Cluster Link] フィールド	<p>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。</p>
[LACP Mode] フィールド	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2 つのイーサネットインターフェイスを 1 つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 このポートの [LACP] モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する 2 つのイーサネットインターフェイスが 1 つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p> <p>(注) このフィールドは、前の手順でオプションを選択しなかった場合に表示されます。</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 9 入力したエンタープライズポート値の検証が成功すると、ウィザードに 10 Gbps クラスポートが [NETWORK ADAPTER #2] として表示されます。「[インターフェイスクラス接続](#)」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 #3
(Optional) Enter the network settings for the 2nd
network adapter -
(- 0 - intra-cluster link).

Recommended use: intra-cluster link

Select 'Cluster Link' if used for cluster
communication.

Phy Interfaces: enp94s0f1 enp216s0f3

-----
OPTIONAL - NETWORK ADAPTER #2 (cluster)

Host IPv4 Address:
169.254.6.64
IPv4 Netmask:
255.255.255.128
Default Gateway IPv4 Address:

IPv4 DNS Servers:

IPv4 Static Routes:

Vlan Id of Interface:
1102
X Cluster Link

LACP Mode

<< back      < cancel >      done >>      next >>

```

次の表のとおり [NETWORK ADAPTER #2] の設定値を入力します。

表 27: ネットワークアダプタ #2 のセカンダリノードエントリ: 10 Gbps クラスポート

[Host IPv4/IPv6 address] フィールド	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。
[IPv4 Netmask/IPv6 Prefix Length] フィールド	IP アドレスを入力した場合は、次のいずれかを実行します。 <ul style="list-style-type: none"> • IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 • IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。

[Default Gateway IPv4/IPv6 address] フィールド	<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>
[IPv4/IPv6 DNS Servers] フィールド	<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>
[IPv4/IPv6 Static Routes] フィールド	<p>1 つ以上のスタティックルートスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。</p>
[Vlan Id of Interface] フィールド	<p>設定するアプライアンス用に作成される LACP リンク上でタグ付けされる VLAN ID を入力します。</p> <p>(注) このフィールドは、ステップ 7 で両方のオプションを選択してアプライアンスのレイヤ 2 LACP ポートチャネルモードを設定した場合にのみ表示されます。</p>
[Cluster Link] フィールド	<p>このポートが Cisco DNA Center クラスタへのリンクであるとして設定するには、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>

[LACP Mode] フィールド	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2つのイーサネットインターフェイスを1つの論理チャンネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 このポートの [LACP] モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネットインターフェイスが1つの論理チャンネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p> <p>(注) このフィールドは、ステップ7でオプションを選択しなかった場合に表示されます。</p>
-------------------	---

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 10** 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/10 Gbps 管理ポートが [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）。

```

STEP #3
(Optional) Enter the network settings for the 3rd
network adapter -
(- 0 - management network).

Recommended use: management network

Select 'Cluster Link' if used for cluster
communication.

Phy Interfaces: eno1 enp216s0f0

OPTIONAL - NETWORK ADAPTER #3 (management)

Host IPv4 Address:
172.29.131.226
IPv4 Netmask:
255.255.255.0
Default Gateway IPv4 Address:

IPv4 DNS Servers:
171.70.168.183 173.36.131.10
IPv4 Static Routes:
10.0.0.0/255.0.0.0/172.29.131.1 171.0.0.0/255.0.0.0/172.29.13
Cluster Link

<< back      < cancel >      done >>      next >>

```

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

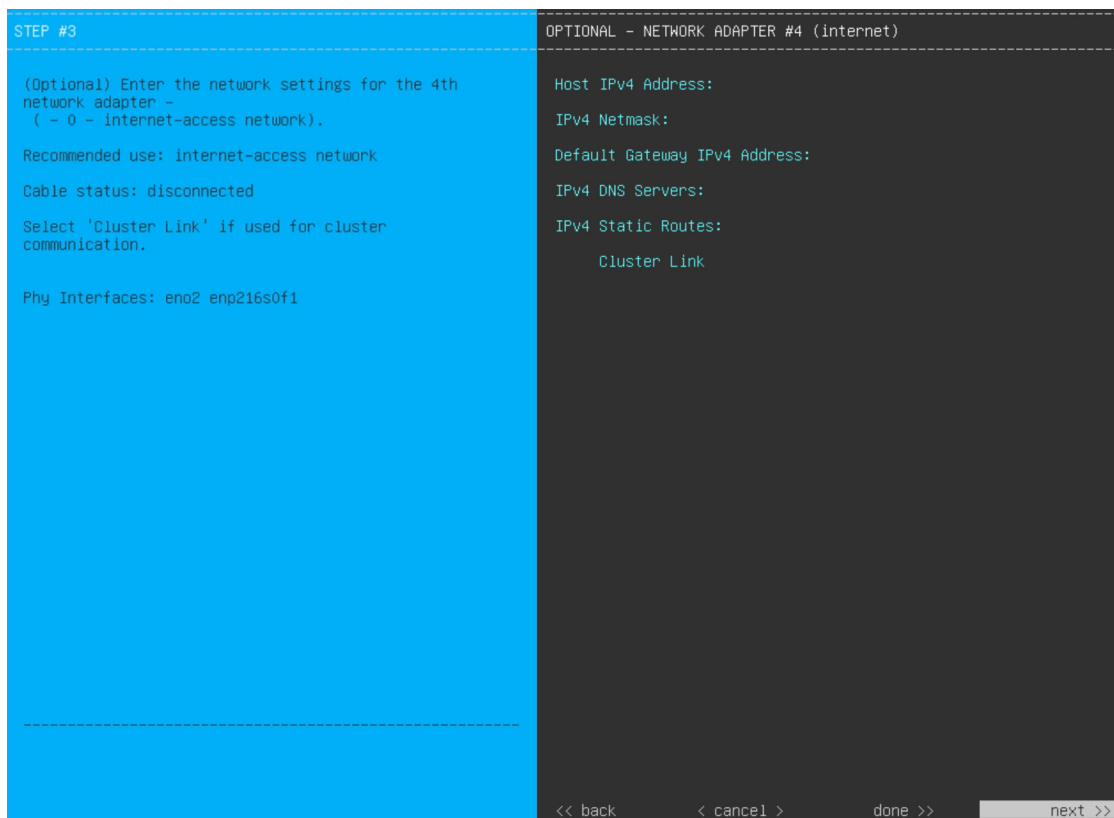
表 28: ネットワークアダプタ #3のセカンダリノードエントリ: 1 Gbps/10 Gbps 管理ポート

[Host IPv4/IPv6 address] フィールド	管理ポートの IP アドレスを入力します。これは、このポートを使用して管理ネットワークから Cisco DNA Center GUI にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。
[IPv4 Netmask/IPv6 Prefix Length] フィールド	次のいずれかを実行します。 <ul style="list-style-type: none"> • IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 • IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。
[Default Gateway IPv4/IPv6 address] フィールド	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。 <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>

[IPv4/IPv6 DNS Servers] フィールド	<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。
[IPv4/IPv6 Static Routes] フィールド	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。
[Cluster Link] フィールド	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 11** 入力した管理ポート値の検証が成功すると、ウィザードに 1 Gbps/10 Gbps インターネットポートが [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](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、10 Gbps エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「[必要な IP アドレスおよびサブネット](#)」と「[必須の設定情報](#)」を参照してください）。



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

表 29: ネットワークアダプタ #4 のセカンダリノードエントリ: 1 Gbps/10 Gbps インターネットポート

[Host IPv4/IPv6 address] フィールド	インターネットポートの 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インターネット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、空白のままにできます。
[IPv4 Netmask/IPv6 Prefix Length] フィールド	次のいずれかを実行します。 <ul style="list-style-type: none"> • IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。 • IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。
[Default Gateway IPv4/IPv6 address] フィールド	インターネット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。

[IPv4/IPv6 DNS Servers] フィールド	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。
[IPv4/IPv6 Static Routes] フィールド	1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。
[Cluster Link] フィールド	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 12 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。

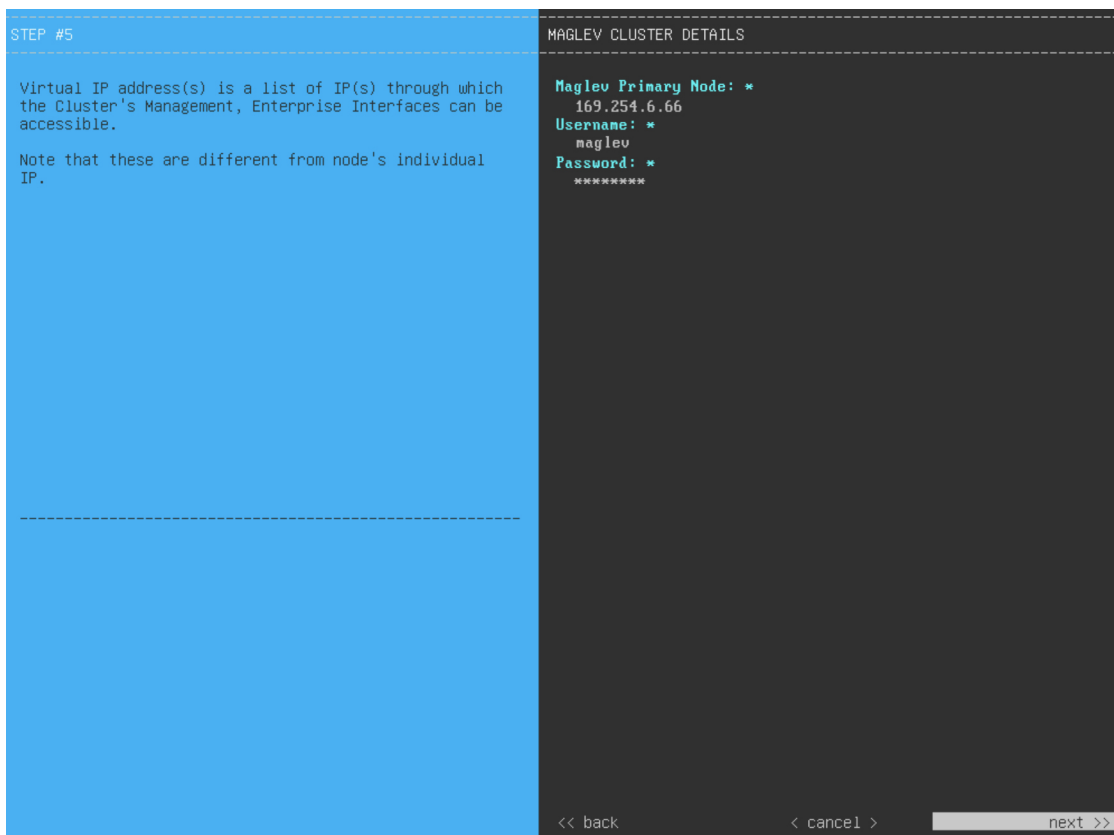
次の表に示すように **[NETWORK PROXY]** の設定値を入力します。

表 30: ネットワークプロキシのセカンダリノードエントリ

[HTTPS プロキシ (HTTPS Proxy)] フィールド	<p>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。</p> <p>(注)</p> <ul style="list-style-type: none"> • 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。 • ポート番号を含む IPv6 URL を入力する場合は、URL の IP アドレス部分を角カッコで囲みます。次の例では、443 がポート番号です。 http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/
[HTTPS Proxy Username] フィールド	<p>ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。</p>
[HTTPS Proxy Password] フィールド	<p>ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。</p>

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 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]** に、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に関する詳細を特定するためのウィザードのプロンプトが表示されます。



次の表の説明に従って、[MAGLEV CLUSTER DETAILS] に値を入力します。

表 31: [MAGLEV CLUSTER DETAILS] のセカンダリノードエントリ

[Maglev Primary Node] フィールド	クラスタ内のプライマリノードのクラスタポートの IP アドレスを入力します。ポート割り当ての推奨事項に従っている場合、これはプライマリノードのネットワークアダプタ #2 の IP アドレスです。
[Username] フィールド	maglev と入力します。
Password フィールド	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 14 クラスタの詳細を入力すると、次に示すとおり、ウィザードに [USER ACCOUNT SETTINGS] の値を入力するよう促すプロンプトが表示されます。

STEP #6	USER ACCOUNT SETTINGS
<p>Specify a new password for the 'maglev' user, and specify a password of the 'admin' UI user.</p> <p>Please use SHIFT for capitalization, using CAPS LOCK may result in inconsistent password.</p> <p>* Indicates a mandatory field.</p> <p>Password generation is optional, but recommended.</p> <p>User is advised to append personal password with generated password for recommended security.</p> <p>Caution: Remember generated password for future log ins.</p>	<pre> Linux Password: * ***** Re-enter Linux Password: * ***** Password Generation Seed: < Generate Password > Auto Generated Password: < Use Generated Password > Administrator Password: * ***** Re-enter Administrator Password: * ***** </pre> <p><< back < cancel > next >></p>

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

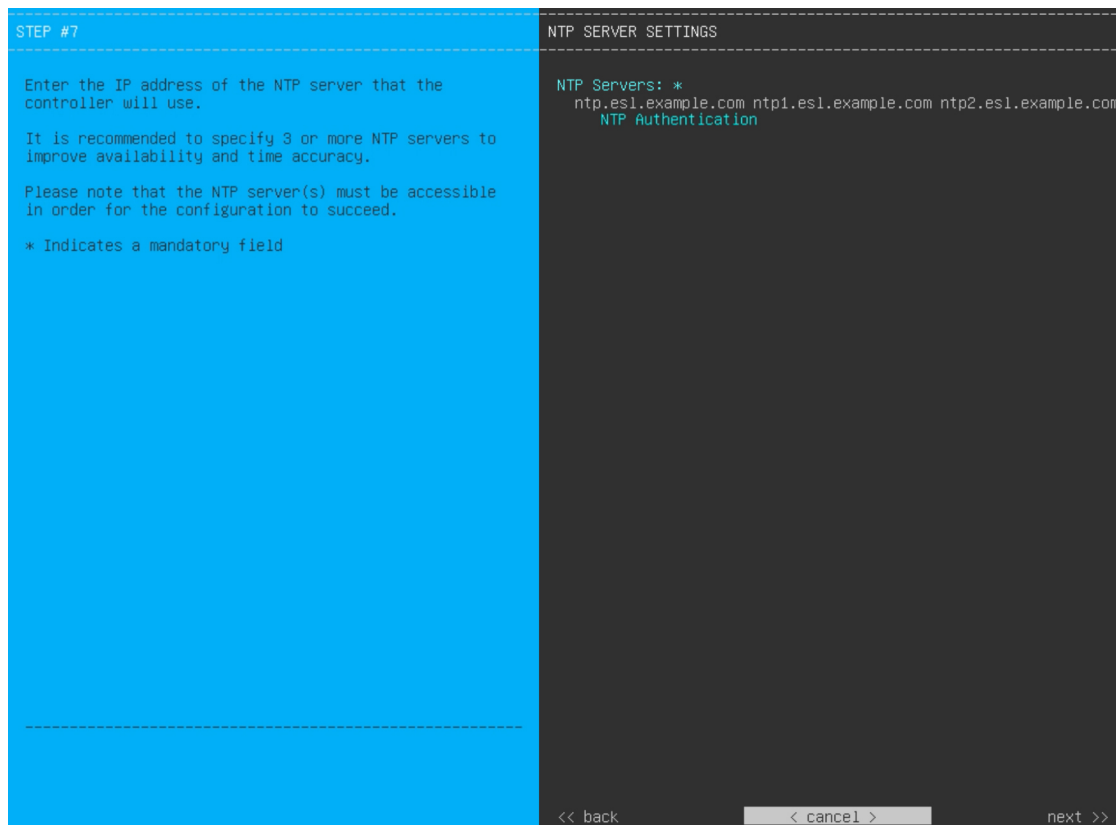
表 32: [USER ACCOUNT SETTINGS] のセカンダリノードエントリ

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

[Re-enter Administrator Password] フィールド	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 15 ユーザーアカウントの詳細を入力すると、[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。



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

[NTP Server (NTP サーバ)] フィールド	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。
------------------------------	--

[NTP Authentication] チェックボックス	<p>Cisco DNA Center と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> • NTP サーバーのキー ID。有効な値の範囲は $1 \sim 4294967295$ ($2^{32}-1$) です。 <p>この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。</p> <ul style="list-style-type: none"> • NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。 <p>(注) 前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。</p>
-------------------------------	--

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 16 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）。

```
The wizard is now ready to apply the configuration on the controller.
Use the [back] button below to verify/modify controller settings.
Use the [cancel] button to discard your changes and exit the wizard.
Use the [proceed] button to save your changes and proceed with applying them on the controller.
```

<< back < cancel > proceed >>

[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。

構成プロセスの最後に、アプライアンスの電源を再投入すると、「CONFIGURATION SUCCEEDED!」というメッセージが表示されます。

```
CONFIGURATION SUCCEEDED

The configuration wizard has completed successfully!

To access the Maglev Web UI, please point your browser to one of the following URLs:

To access the Maglev Web Console, please point your browser to one of the following URLs:

https://17.192.1.226
https://169.254.6.64
https://172.29.131.226

The wizard will automatically close in 30 seconds
```

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

ブラウザベースのウィザードを使用した 44/56 コアアプライアンスの設定

- [アプライアンスの設定の概要 \(141 ページ\)](#)
- [インストール構成ウィザードを使用したアプライアンスの設定 \(143 ページ\)](#)
- [詳細インストール構成ウィザードを使用したプライマリノードの設定 \(157 ページ\)](#)
- [詳細インストール構成ウィザードを使用したセカンダリノードの設定 \(178 ページ\)](#)
- [最新の Cisco DNA Center リリースへのアップグレード \(199 ページ\)](#)

アプライアンスの設定の概要

次のいずれかのモードを使用して、44 または 56 コア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。初期展開でスタンドアロンモードを選択した場合は、これが最初のノード、つまりプライマリノードになります。後でさらにアプライアンスを追加してクラスタを形成できます。
- **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。初期展開でクラスタモードを選択した場合は、セカンダリ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、最初にクラスタのプライマリノードを設定します。3 つのアプライアンスを設置済みで、クラスタに 2 番目と 3 番目のノードを追加する場合は、次に、セカンダリノードを設定します。

ブラウザベースの構成ウィザード

Cisco DNA Center は、アプライアンスの設定に使用できる 2 種類のブラウザベースのウィザードを提供します。説明を読んで、どのウィザードを完了する必要があるかを判断してください。



重要 これらのウィザードは、Cisco DNA Center 2.3.5 がすでにインストールされている新しいアプライアンスを設定している場合に使用できます。以前のバージョンからアップグレードし、これらのウィザードを使用する場合は、Cisco TAC に連絡して支援を受けてください。

インストール構成ウィザード

このウィザードは、クラスタ内のインターフェイスだけでなく、企業インターフェイス、管理インターフェイス、およびインターネット アクセス インターフェイス（すべてアプライアンスのエンタープライズポートに存在）にもデフォルト値を設定し、アプライアンスの設定プロセスを合理化します。デフォルトのインターフェイス設定を使用しても問題がなく、アプライアンスを可能な限り早く稼働させたい場合は、このウィザードを使用します。このウィザードを使用して次のことはできませんので注意してください。

- クラスタのセカンダリノードの設定。
- 第 1 世代 44 コア Cisco DNA Center アプライアンスの設定。

高度なインストール構成ウィザード

このウィザードは、すべての利用可能なアプライアンスの設定（ユーザーによる変更が可能）へのアクセスを提供します。デフォルト設定とは異なるインターフェイス設定を指定する場合は、このウィザードを使用します。クラスタ内の 2 番目または 3 番目のノードを設定する場合にも、このウィザードを使用します。

ブラウザベースのウィザードの前提条件

ブラウザベースのウィザードのいずれかを使用して、アプライアンスの設定が正しいことを確認するには、次の手順を実行します。

- DHCP サーバーが割り当てる IP アドレス、サブネットマスク、デフォルトゲートウェイを使用するために、アプライアンス上のエンタープライズインターフェイスを指定します。ウィザードでこのインターフェイスを設定する場合、割り当てられている IP アドレスまたはサブネットマスクは変更できません。デフォルトゲートウェイのみ変更できます。この章で扱うトピックでは、エンタープライズインターフェイスがこの目的で選択されていることが前提となっています。
- DHCP サーバの割り当てた IP アドレスが、ウィザードを完了するマシンから到達できることを確認します。
- エンタープライズおよびクラスタ内インターフェイスの場合、両方のインターフェイスが接続されていて、[UP] 状態であることを確認します。

アプライアンスのエンタープライズインターフェイスに独自の IP アドレス、サブネットマスク、およびデフォルトゲートウェイを指定する場合（および DHCP サーバーによって割り当てられた値を使用しない場合）は、静的 IP アドレス設定画面が完了していることを確認します。

インストール構成ウィザードを使用したアプライアンスの設定

インストール構成ウィザードを使用して3ノードクラスタのプライマリノードまたはスタンダアロンノードを設定するには、次の手順を実行します。ウィザードでは、デフォルト設定を使用して同じポートでエンタープライズ、管理、およびインターネットインターフェイスを設定することで、設定プロセスが簡素化されます。次の第2世代 Cisco DNA Center アプライアンスは、このウィザードを使用した設定をサポートしています。

- 44 コアアプライアンス：シスコ製品番号 DN2-HW-APL
- 44 コア プロモーションアプライアンス：シスコ製品番号 DN2-HW-APL-U
- 56 コアアプライアンス：シスコ製品番号 DN2-HW-APL-L
- 56 コア プロモーションアプライアンス：シスコ製品番号 DN2-HW-APL-L-U

第1世代 44 コア Cisco DNA Center アプライアンス（シスコ製品番号 DN1-HW-APL）は、このウィザードを使用しても設定することはできません。



重要

- このウィザードは、新しい Cisco DNA Center アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、[Maglev 設定ウィザード](#)を使用する必要があります（[Maglev ウィザードを使用したアプライアンスの設定（93 ページ）](#)を参照）。
- このウィザードを使用して、3ノードクラスタの2番目または3番目のアプライアンスを設定することはできません。これを実行するには、[詳細インストール構成ウィザードを使用したセカンダリノードの設定（178 ページ）](#)で説明されている手順を完了します。また、このウィザードを使用して、アプライアンスのエンタープライズおよびクラスタ内インターフェイスで LACP モードを有効にすることはできません。
- 3ノードクラスタのいずれかのアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、（ネットワークのデバイスを検出してテレメトリを有効にするために完了する）クイック スタート ワークフローが開始されません。
- 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。

- 「[アプライアンスのイメージの再作成 \(86 ページ\)](#)」の説明どおりに Cisco DNA Center ソフトウェアイメージがアプライアンスにインストールされたこと。



重要 次のアプライアンスには Cisco DNA Center ソフトウェアイメージがあらかじめインストールされていないため、これはプロモーションアプライアンスを設定する場合にのみ当てはまります。

- 44 コア プロモーションアプライアンス：シスコ製品番号 DN2-HW-APL-U
 - 56 コア プロモーションアプライアンス：シスコ製品番号 DN2-HW-APL-L-U
-
- [必要な IP アドレスおよびサブネット \(33 ページ\)](#) と [必須の設定情報](#) で必要な情報がすべて収集されたこと。
 - 「[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、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、このアプライアンスで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
 - 「[事前設定タスクの実行](#)」の説明に従って、アプライアンスのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
 - Cisco IMC、Cisco DNA Center との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノート](#) を参照してください。
 - 次の手順で指定する DNS サーバと Cisco DNA Center の間のファイアウォールで ICMP が許容されること。このウィザードでは、ユーザの指定する DNS サーバを ping で確認します。Cisco DNA Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

ステップ 1 インストール構成ウィザードを起動します。

- お使いのブラウザで、実行した `cisco imc` GUI 設定で設定した Cisco IMC の IP アドレスをポイントし、`cisco imc` ユーザとして Cisco IMC GUI にログインします（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」を参照）。
- ログインが成功すると、次に示すように、アプライアンスに **[Cisco Integrated Management Controller Chassis の概要 (Cisco Integrated Management Controller Chassis Summary)]** ウィンドウが右上の青いリンクメニューとともに表示されます。



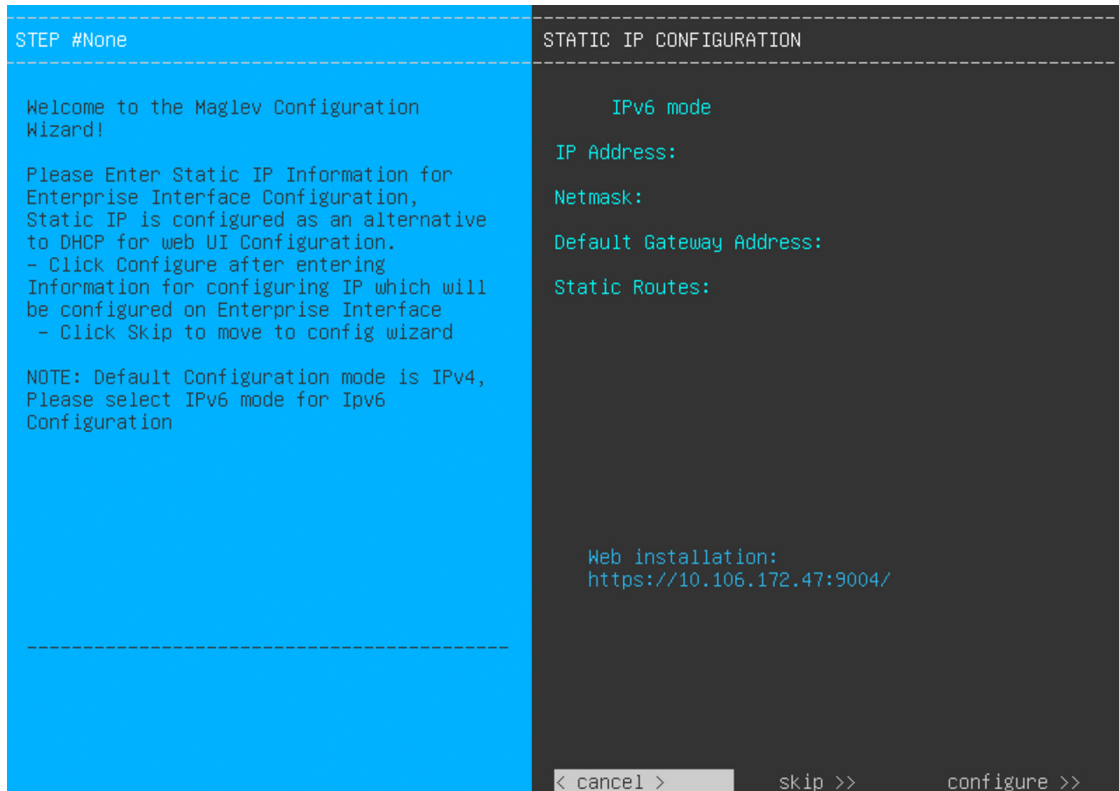
- b) 青いリンクメニューで [Launch KVM] を選択してから、[Java based KVM] と [HTML based KVM] のいずれかを選択します。[Java based KVM] を選択した場合、KVM コンソールを独自のウィンドウで表示するために、ブラウザまたはファイルマネージャから Java スタートアップファイルを起動する必要があります。[HTML based KVM] を選択すると、KVM コンソールが別個のブラウザウィンドウまたはタブで自動的に起動します。

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。

- c) 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] を選択します。その後、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 [Static IP Configuration] 画面が表示されます。



[Web インストール (Web Installation)] フィールドにリストされている URL に注意してください。

d) 次のいずれかを実行します。

- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てるようにするには、[Skip] をクリックします。
- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、[Configure] をクリックします。

(注) 指定する必要があるのは、アプライアンスのエンタープライズインターフェイスの IP アドレス、サブネットマスク、およびデフォルトゲートウェイのみです。

[IPv6 Mode] チェックボックス	IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。
[IP Address] フィールド	使用する静的 IP アドレスを入力します。
[ネットマスク (Netmask)] field	<p>前のフィールドに指定した IP アドレスのネットマスクを入力します。</p> <ul style="list-style-type: none"> • IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。 • IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。

[Default Gateway Address] フィールド	トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
[Static Routes] フィールド	1つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク><ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。

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。

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

-----
Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >
    
```

- e) [Appliance Configuration] 画面を表示するには、[Static IP Configuration] 画面に表示された URL を開きます。


Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA Center Cluster
This appliance will be the primary node of a cluster.

Join A Cisco DNA Center Cluster
This appliance will be added as a node to the primary node of a cluster.



Next

- f) [Start a Cisco DNA Center Cluster] オプションボタンをクリックし、[Next] をクリックします。

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.
Which workflow matches your needs?

<p>Install <input checked="" type="radio"/></p> <p>Configure a standalone node or cluster's primary node.</p> <p>Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.</p>	<p>Advanced Install <input type="radio"/></p> <p>Configure a standalone node or any node in a cluster.</p> <p>Use this wizard to access all of the available appliance configuration options.</p>
---	---



Back

Start

g) [Install] オプションボタンをクリックし、[Start] をクリックします。

[Overview] スライドが開きます。[>] をクリックして、ウィザードで実行するタスクの概要を表示します。

×

Overview

Complete the basic tasks required to configure your appliance for use with Cisco DNA Center.



Start Workflow

h) [Start Workflow] をクリックしてウィザードを起動します。

[Appliance Interface Overview] 画面が開き、Cisco DNA Center アプライアンスで使用可能な 4 つのインターフェイスの説明が表示されます。

Cisco DNA Center Install

Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracluster Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the internet.

In this workflow, the Intracluster Link Interface is predefined. The other 3 interfaces will be configured together on the Enterprise port.

Exit Next

このウィザードは、Cisco DNA Center 機能に必要なエンタープライズポートとクラスタ内ポートの設定に役立ちます。ウィザードの次の画面にこれらのポートのいずれかまたは両方が表示されない場合、表示されないポートは機能していないか、無効になっている可能性があります。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザード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「[事前設定タスクの実行](#)」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 2 インストール構成ウィザードを完了します。

- a) [Next] をクリックします。

[Configure The Enterprise Port] 画面が開きます。

Cisco DNA Center Install

Configure the Enterprise Port

In this workflow, the Management Network and Internet Access Interfaces are on the same port as the Enterprise Network Interface. You can enter up to three DNS addresses. If your network resides behind a firewall, you must [allow access to these URLs](#) and [open these ports](#). If you are setting up a multinode cluster, the cluster's second and third nodes must reside in the same subnet as the primary node. [Download the Intracluster Link interface's information](#)

Enterprise & Management Network & Internet Access Interface

LACP Mode Disabled

IP Address 10.106.172.47

Netmask 255.255.255.128

Default Gateway 10.106.172.1

Intracluster Link Interface

Interface Name cluster

LACP Mode Disabled

IP Address 169.254.6.66

Subnet Mask 255.255.255.128

Exit Next

構成ウィザードにより、エンタープライズポートにエンタープライズ、管理、およびインターネットアクセスインターフェイスが設定されます。リストされているほぼすべてのパラメータの値も事前入力されます。

ネットワークがファイアウォールの背後にある場合は、次の手順を実行します。

- [\[allow access to these URLs\]](#) リンクをクリックすると、Cisco DNA Center がアクセスできる必要がある URL を一覧表示するポップアップウィンドウが表示されます。
- [\[open these ports\]](#) リンクをクリックすると、Cisco DNA Center が使用できる必要があるネットワークサービスポートを一覧表示するポップアップウィンドウが表示されます。

b) **[Next]** をクリックします。

[DNS Configuration] 画面が開きます。

Cisco DNA Center Install

DNS Configuration

Enter the IP address of the preferred DNS server. To enter additional DNS servers, click the Add (+) configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS appliances.

DNS* +

Exit Review Back Next

- c) [DNS] フィールドに、優先 DNS サーバーの IP アドレスを入力します。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要 最大 3 つの DNS サーバーを設定できます。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。

- d) [Next] をクリックします。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Interface to Port Configuration] 画面が開きます。

Cisco DNA Center Install

Interface to Port Configuration

We are going to configure the following interfaces. Click Configure and wait for configuration to be done before proceeding to the next step.

[Configure](#)

Connected Disconnected LACP disabled

Enterprise & Management Network & Internet Access Interface ⓘ

Interface Name	enterprise
LACP Mode	Disabled ⓘ
IP Address	10.106.172.47
Netmask	255.255.255.128
Default Gateway	10.106.172.1

Intracluster Link Interface ⓘ

Interface Name	cluster
LACP Mode	Disabled ⓘ
IP Address	169.254.6.66
Subnet Mask	255.255.255.128

[Exit](#) [Back](#) [Next](#)

- e) 設定されているインターフェイス設定を確認し、[Configure] をクリックします。
- f) インターフェイスの初期設定が完了したら、[Next] をクリックしてウィザードの次の画面に進みます。

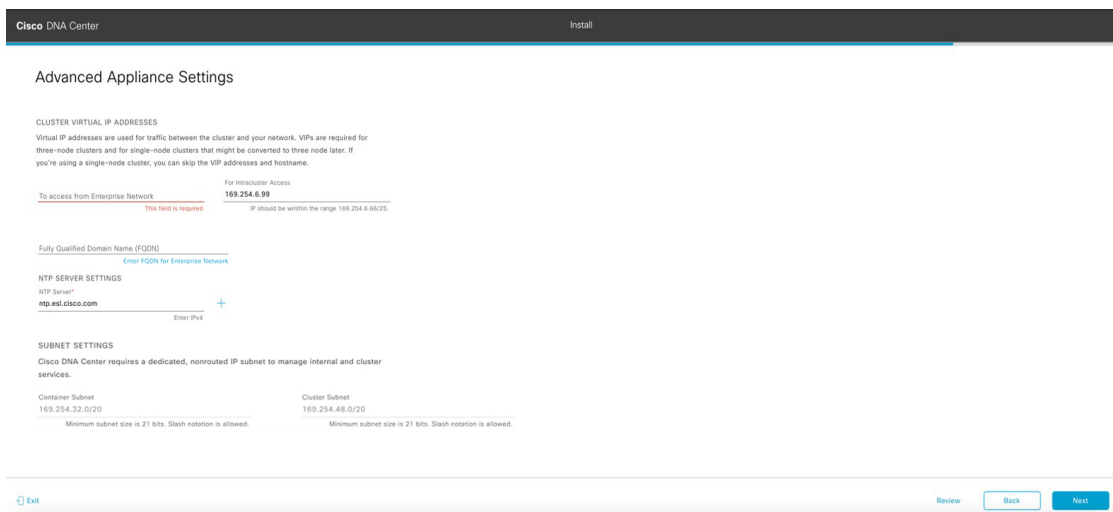
[Configure Proxy Server Information] 画面が開きます。

- g) 次のいずれかを実行します。
- ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックし、[Next] をクリックします。
 - ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、次の表に示す値を入力します。

表 33: プロキシサーバー設定のプライマリノードエントリ

[プロキシサーバ (Proxy Server)] フィールド	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。
[Port] フィールド	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。
[Username] フィールド	ネットワークプロキシへのアクセスに使用するユーザー名を入力します。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。
Password フィールド	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。

入力した情報がウィザードで検証され、ウィザードの操作を続行する前に変更が必要な設定があれば、通知されます。入力した設定が有効であれば、ウィザードの [Advanced Appliance Settings] 画面が開きます。



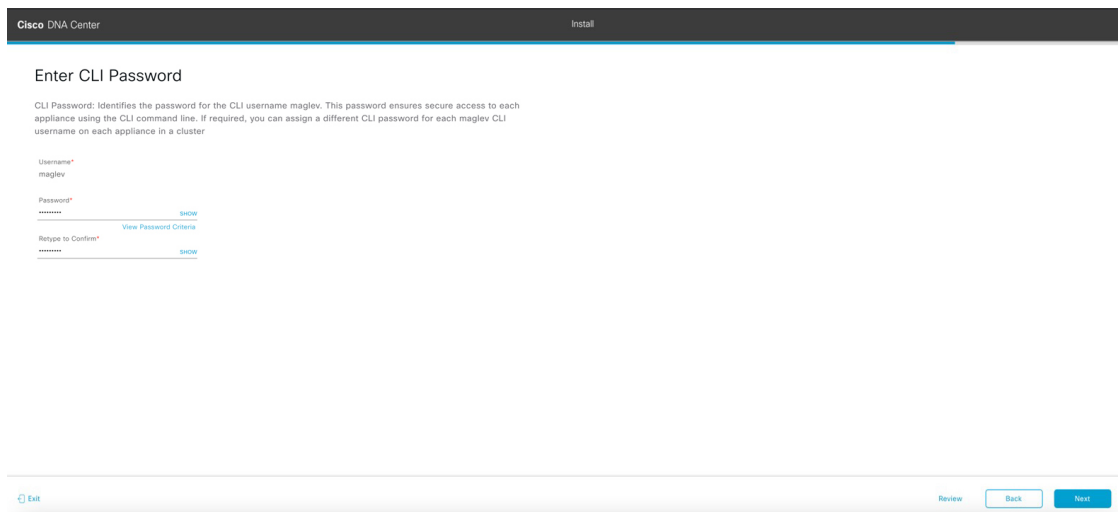
h) クラスタの構成値を入力し、[Next] をクリックします。

表 34 : [Advanced Appliance Settings] のプライマリノードエントリ

クラスタ仮想 IP アドレス	
[Enterprise Network] および [For Intracluster Access] フィールドからアクセスする場合	<p>アプライアンスのクラスタとエンタープライズおよびクラスタ内インターフェイス間のトラフィックに使用される仮想 IP アドレスを入力します。このアドレスは、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に対して入力する必要があります。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。</p> <p>重要 仮想 IP アドレスを構成する場合は、構成されたネットワーク インターフェイスごとに1つ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。</p>
[Fully Qualified Domain Name (FQDN)] フィールド	<p>クラスタの完全修飾ドメイン名 (FQDN) を指定します。Cisco DNA Center は、このホスト名を使用して次の操作を実行します。</p> <ul style="list-style-type: none"> 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。

NTP サーバー設定	
[NTP Server] フィールド	<p>少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。</p> <p>実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。</p>
サブネット設定	
[Container Subnet] フィールド	<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 に設定されているため、別のサブネットは入力できません。</p>
[Cluster Subnet] フィールド	<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 に設定されているため、別のサブネットは入力できません。</p>

[CLI パスワードの入力] 画面が開きます。



- i) maglev ユーザーのパスワードを入力して確認した後、[Next] をクリックします。

入力した情報がウィザードで検証され、ウィザードの操作を続行する前に変更の必要な設定があれば、通知されます。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in .JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Enterprise Port [Edit](#)

Enterprise & Management Network & Internet Access Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.47
Netmask	255.255.255.128
Default Gateway	10.106.172.1

Intracenter Link Interface

Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.66
Subnet Mask	255.255.255.128

(注) アプライアンスの設定を JSON ファイルとしてダウンロードするには、こちらのリンクをクリックします。

- j) 画面の下部までスクロールし、ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な [Edit] リンクをクリックして、更新を行うウィザード画面を開きます。
- k) Cisco DNA Center アプライアンスの設定を完了するには、[Start Configuration] をクリックします。プロセス中もウィザード画面が継続的に更新され、現在実行しているタスクとその進行状況、発生したエラーが示されます。この情報のローカルコピーをテキストファイルとして保存するには、[Download] アイコンをクリックします。

Appliance Configuration In Progress

It should take about 30 minutes to configure the appliance. **Do not press your browser's back button or refresh this page.** The page will update after configuration completes.

30%

Initializing the cluster using kubeadm

Started: 04/09/2020 12:15:36

[Download](#)

```

17:40:20 2021 GMT
2021-12-03T05:37:06.616Z14 | kubelet.conf Apr
13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-12-03T05:37:06.616Z15 | admin.conf Apr 13
12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-12-03T05:37:06.616Z16 | scheduler.conf Apr
13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-12-03T05:37:06.616Z17 | controller-
manager.conf Apr 13 12:12:14 2020 GMT Apr 13
17:40:22 2021 GMT
2021-12-03T05:37:06.616Z18 | -----
-----
-----


```

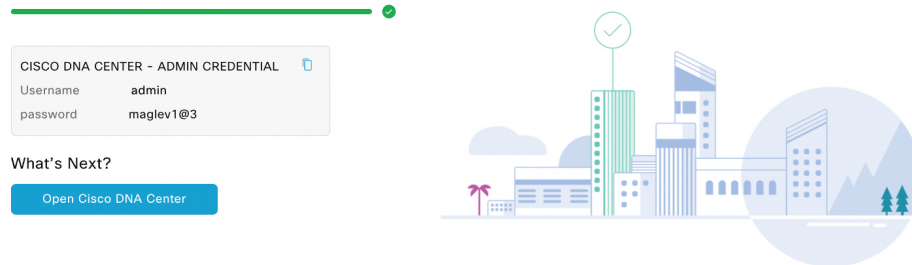
ステップ 3 アプライアンスの設定が完了したら、[Cisco DNA Center - Admin Credential] 領域のコピーアイコンをクリックして、デフォルトの管理者スーパーユーザーパスワードをコピーします。


Cisco DNA Center

Install

Appliance Configuration Complete!

Important: Take note of the credentials displayed below. You can click the copy icon  if you want to save them locally. You will use these credentials to log in to Cisco DNA Center for the first time. After logging in, you will be prompted to change the password.



CISCO DNA CENTER - ADMIN CREDENTIAL 

Username	admin
password	maglev1@3

What's Next?

[Open Cisco DNA Center](#)

重要 インストール構成ウィザードを完了すると、Cisco DNA Center はこのパスワードを自動的に設定します。続行する前に、必ずコピーアイコンをクリックしてください。クリックしないと、Cisco DNA Center への最初のログインができません。

(注) セキュリティ対策として、ログイン後にこのパスワードを変更するよう求められます。詳細については、[クイックスタートワークフローの完了 \(260 ページ\)](#) を参照してください。

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展開する場合は、初回セットアップ（「[初期設定ワークフロー](#)」）を実行して続行します。

詳細インストール構成ウィザードを使用した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、詳細インストール構成ウィザードを使用して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。

**重要**

- 次の第 2 世代 Cisco DNA Center アプライアンスは、このウィザードを使用した設定をサポートしています。
 - 44 コアアプライアンス : シスコ製品番号 DN2-HW-APL
 - 44 コア プロモーションアプライアンス : シスコ製品番号 DN2-HW-APL-U
 - 56 コアアプライアンス : シスコ製品番号 DN2-HW-APL-L
 - 56 コア プロモーションアプライアンス : シスコ製品番号 DN2-HW-APL-L-U

第 1 世代 44 コア Cisco DNA Center アプライアンス (シスコ製品番号 DN1-HW-APL) は、このウィザードを使用しても設定することはできません。

- このウィザードは、新しい Cisco DNA Center アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、[Maglev 設定ウィザード](#)を使用する必要があります ([Maglev ウィザードを使用したアプライアンスの設定 \(93 ページ\)](#) を参照)。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、(ネットワークのデバイスを検出してテレメトリを有効にするために完了する) クイック スタートワークフローが開始されません。
- 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。

すでにプライマリノードがある既存のクラスタのセカンダリノードとしてインストールされたアプライアンスを設定する場合には、代わりに[詳細インストール構成ウィザードを使用したセカンダリノードの設定 \(178 ページ\)](#) の手順を実行します。

始める前に

次のことを確認します。

- 「[アプライアンスのイメージの再作成 \(86 ページ\)](#)」の説明どおりに Cisco DNA Center ソフトウェアイメージがアプライアンスにインストールされたこと。



重要 次のアプライアンスには Cisco DNA Center ソフトウェアイメージがあらかじめインストールされていないため、これはプロモーションアプライアンスを設定する場合にのみ当てはまります。

- 44 コア プロモーション アプライアンス : シスコ製品番号 DN2-HW-APL-U
- 56 コア プロモーション アプライアンス : シスコ製品番号 DN2-HW-APL-L-U

- [必要な IP アドレスおよびサブネット \(33 ページ\)](#) と [必須の設定情報](#) で必要な情報がすべて収集されたこと。
- 「[アプライアンスのインストールワークフロー](#)」の説明に従って、最初のアプライアンスがインストールされたこと。
- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」の説明に従って、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。
- 「[事前設定タスクの実行](#)」の説明に従って、プライマリノードのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- Cisco IMC、Cisco DNA Center との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順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。ウィザードでは、ユーザの指定する DNS サーバを ping で確認します。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 詳細インストール構成ウィザードを起動します。

- a) お使いのブラウザで、実行した cisco imc GUI 設定で設定した Cisco IMC の IP アドレスをポイントし、cisco imc ユーザとして Cisco IMC GUI にログインします（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」を参照）。
ログインが成功すると、次に示すように、アプライアンスに [Cisco Integrated Management Controller Chassisの概要 (Cisco Integrated Management Controller Chassis Summary)] ウィンドウが右上の青いリンクメニューとともに表示されます。



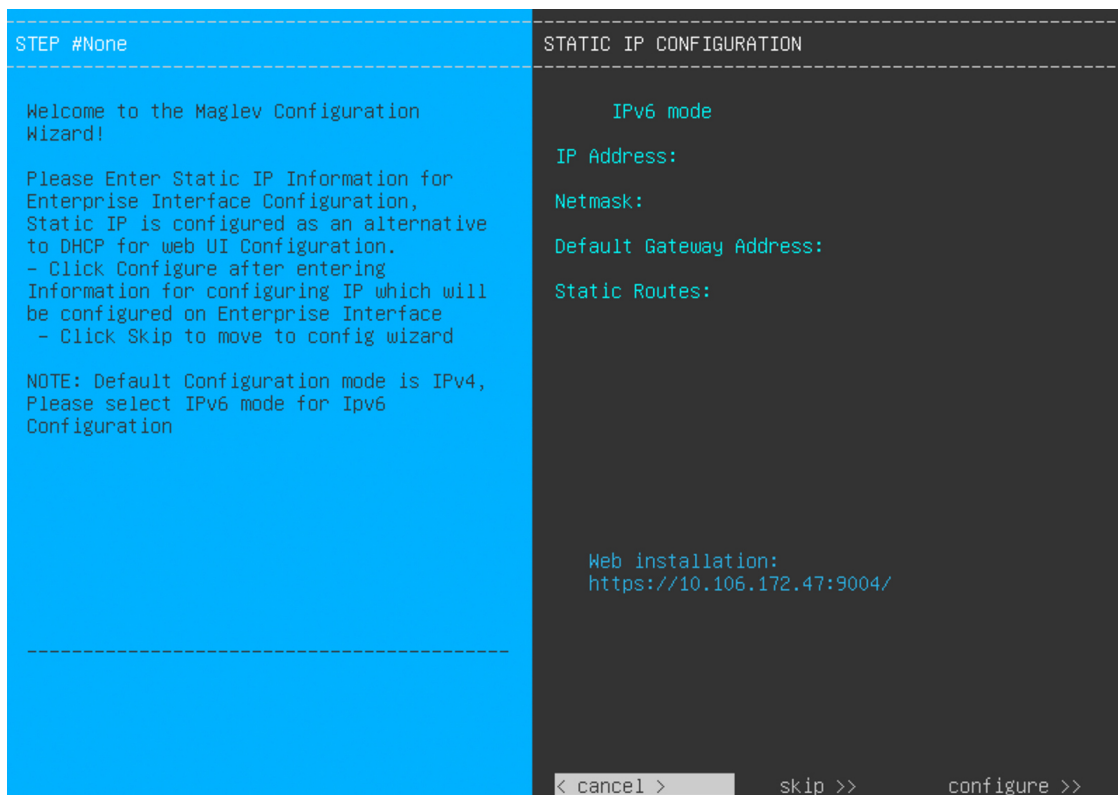
- b) 青いリンクメニューで [Launch KVM] を選択してから、[Java based KVM] と [HTML based KVM] のいずれかを選択します。[Java based KVM] を選択した場合、KVM コンソールを独自のウィンドウで表示するために、ブラウザまたはファイルマネージャから Java スタートアップファイルを起動する必要があります。[HTML based KVM] を選択すると、KVM コンソールが別個のブラウザウィンドウまたはタブで自動的に起動します。

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。

- c) 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] を選択します。その後、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 [Static IP Configuration] 画面が表示されます。



[Web インストール (Web Installation)] フィールドにリストされている URL に注意してください。

d) 次のいずれかを実行します。

- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てるようにするには、[Skip] をクリックします。
- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、[Configure] をクリックします。

(注) 指定する必要があるのは、アプライアンスのエンタープライズインターフェイスの IP アドレス、サブネットマスク、およびデフォルトゲートウェイのみです。

[IPv6 Mode] チェックボックス	IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。
[IP Address] フィールド	使用する静的 IP アドレスを入力します。
[ネットマスク (Netmask)] field	前のフィールドに指定した IP アドレスのネットマスクを入力します。 <ul style="list-style-type: none"> • IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。 • IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。

[Default Gateway Address] フィールド	トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
[Static Routes] フィールド	1つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク>/<ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。

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。

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >

```

- e) [Appliance Configuration] 画面を表示するには、[Static IP Configuration] 画面に表示された URL を開きます。

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

<p>Start A Cisco DNA Center Cluster <input checked="" type="radio"/></p> <hr/> <p>This appliance will be the primary node of a cluster.</p>	<p>Join A Cisco DNA Center Cluster <input type="radio"/></p> <hr/> <p>This appliance will be added as a node to the primary node of a cluster.</p>
---	--



Next

- f) [Start a Cisco DNA Center Cluster] オプションボタンをクリックし、[Next] をクリックします。

Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.
Which workflow matches your needs?

Install


Configure a standalone node or **cluster's primary node**.

Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.

Advanced Install

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.



- g) [Advanced Install] オプションボタンをクリックし、[Start] をクリックします。

[Advanced Install Overview] スライドが開きます。[>] をクリックして、ウィザードで実行するタスクの概要を表示します。

Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.



- h) [Start Workflow] をクリックしてウィザードを起動します。

[Appliance Interface Overview] 画面が開き、設定可能な 4 つのアプライアンス インターフェイスの説明が表示されます。

Cisco DNA Center Advanced Install

Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracluster Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA Center GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the Internet.

In this workflow, the Enterprise Network Interface and the Intracluster Link Interface will each have their own dedicated port. You can choose to have either Management Network Interface and/or Internet Access Interface be on the same port as the Enterprise Network Interface or assign them to a separate designated port.

Exit Next

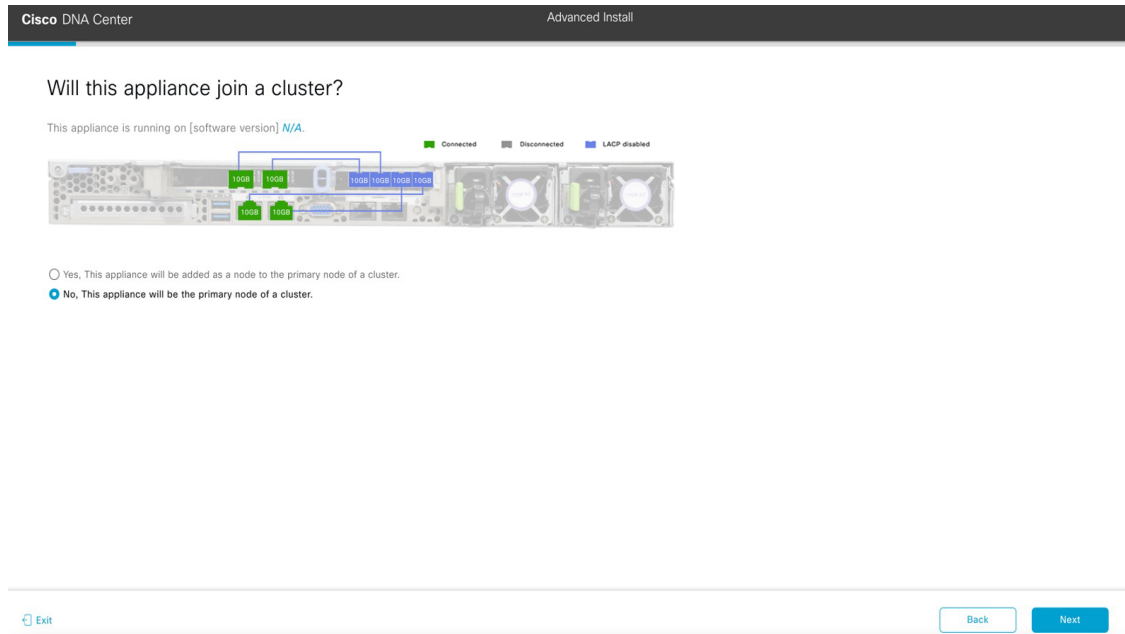
重要

Cisco DNA Center の機能に必要なため、少なくともアプライアンスのエンタープライズポートおよびクラスタポートにインターフェイスを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか1つまたは両方が表示されない場合、表示されない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。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザード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「[事前設定タスクの実行](#)」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 2 詳細インストール構成ウィザードを完了します。

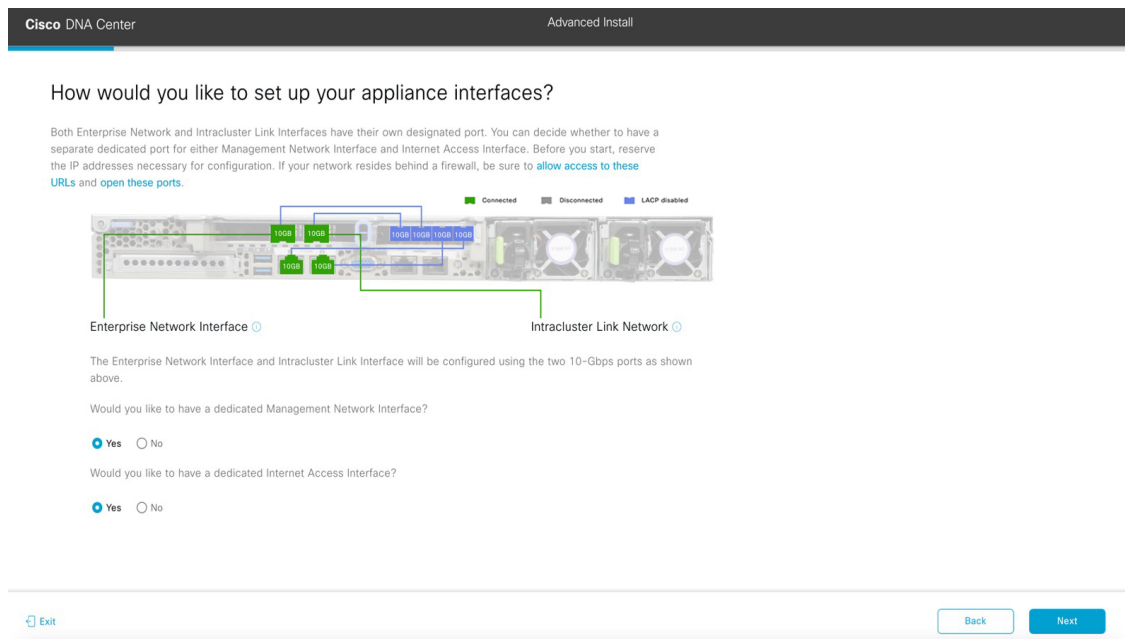
- a) [Next] をクリックします。

[Will this appliance join a cluster?] 画面が開きます。



- b) [No] オプションボタンをクリックし（クラスタのプライマリノードを設定する場合）、[Next] をクリックします。

[How would you like to set up your appliance interfaces?] 画面が開きます。



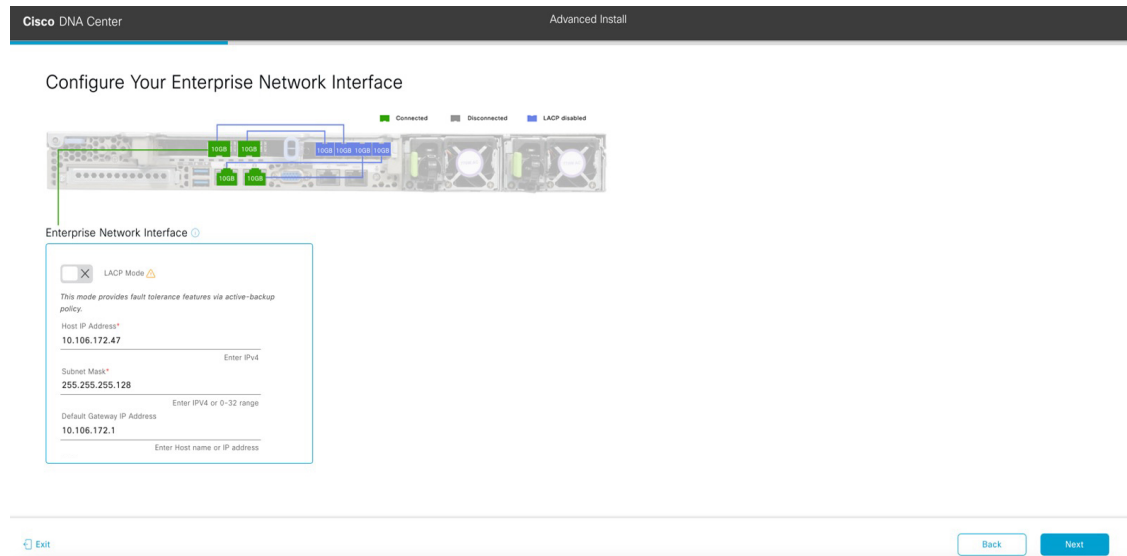
ネットワークがファイアウォールの背後にある場合は、次の手順を実行します。

- [allow access to these URLs] リンクをクリックすると、Cisco DNA Center がアクセスできる必要がある URL を一覧表示するポップアップウィンドウが表示されます。

- [open these ports] リンクをクリックすると、Cisco DNA Center が使用できる必要があるネットワークサービスポートを一覧表示するポップアップウィンドウが表示されます。

- c) 専用の管理およびインターネット アクセス インターフェイスを設定するかどうかを指定し、[Next] をクリックします。

[Configure Your Enterprise Network Interface] 画面が開きます。



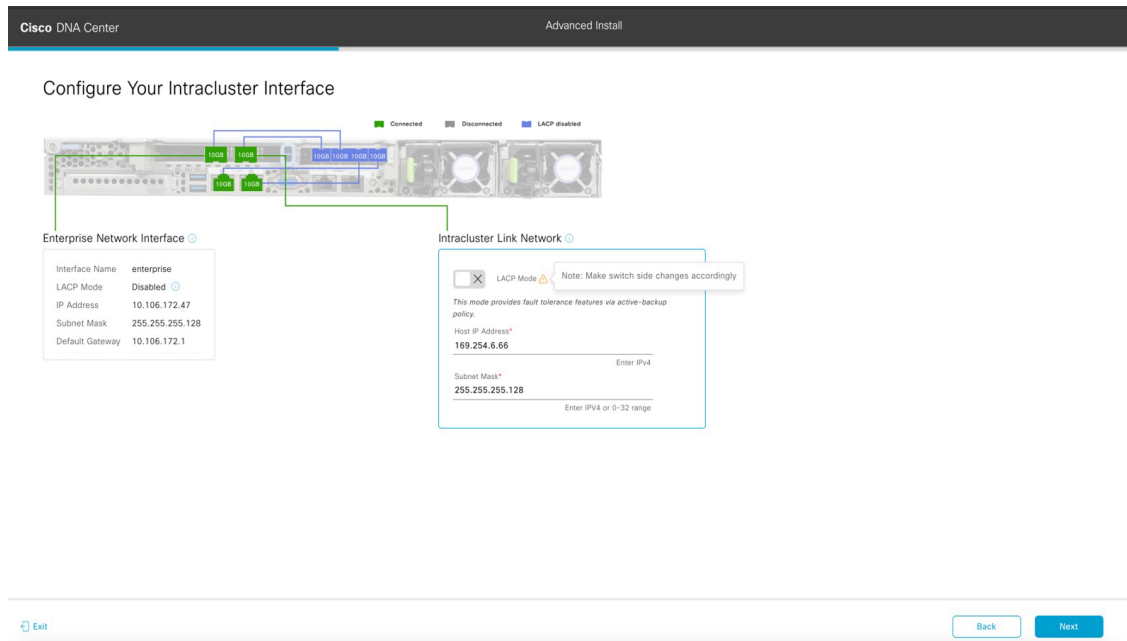
- d) エンタープライズ インターフェイスの構成値を入力し、[Next] をクリックします。

「[インターフェイスケーブル接続](#)」で説明したように、このインターフェイスは、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インターフェイスです。入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

表 35: エンタープライズ インターフェイスのプライマリノードエントリ

<p>[LACP Mode] スライダ</p>	<p>エンタープライズ インターフェイスに対して、次のネットワーク インターフェイスコントローラ (NIC) ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード：このモードでは、2つのイーサネット インターフェイスを1つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード：このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネット インターフェイスが1つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
<p>[Host IP Address] フィールド</p>	<p>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。</p>
<p>[Subnet Mask] フィールド</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 (Default Gateway IP Address)] フィールド</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>(注) このインターフェイスは、DHCP サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. このフィールドに現在一覧表示されている IP アドレスを削除し、[Exit] をクリックします。 この操作でウィザードの最初の画面に戻ります。 2. エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ IP アドレスを入力します。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Intracluster Interface] 画面が開きます。



- e) クラスタ内インターフェイスの構成値を入力し、[Next] をクリックします。

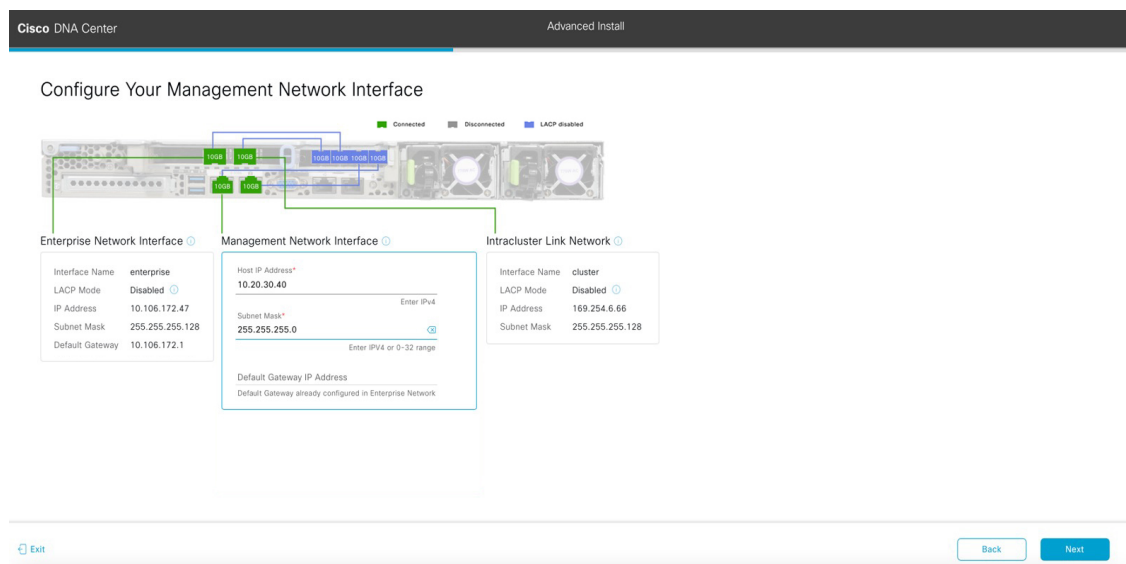
「[インターフェイスケーブル接続](#)」で説明したように、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

- (注)
- 同じポートでエンタープライズ インターフェイスとインターネット アクセス インターフェイスを設定する場合は、この手順を実行してから、ステップ 2f (管理インターフェイスの設定方法が記載) に進みます。
 - エンタープライズ インターフェイスと管理インターフェイスを同じポートに設定する場合は、この手順を実行してから、ステップ 2g (インターネット アクセス インターフェイスの設定方法が記載) に進みます。
 - 同じポートでエンタープライズ、管理、およびインターネット アクセス インターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 36: クラスタ内インターフェイスのプライマリノードエントリ

<p>[LACP Mode] スライダ</p>	<p>クラスタ内インターフェイスに対して、次の NIC ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード：このモードでは、2つのイーサネットインターフェイスを1つの論理チャンネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード：このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネットインターフェイスが1つの論理チャンネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
<p>[Host IP Address] フィールド</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>[Subnet Mask] フィールド</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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Management Network Interface] 画面が開きます。



f) (任意) 管理ポートの構成値を入力し、[Next] をクリックします。

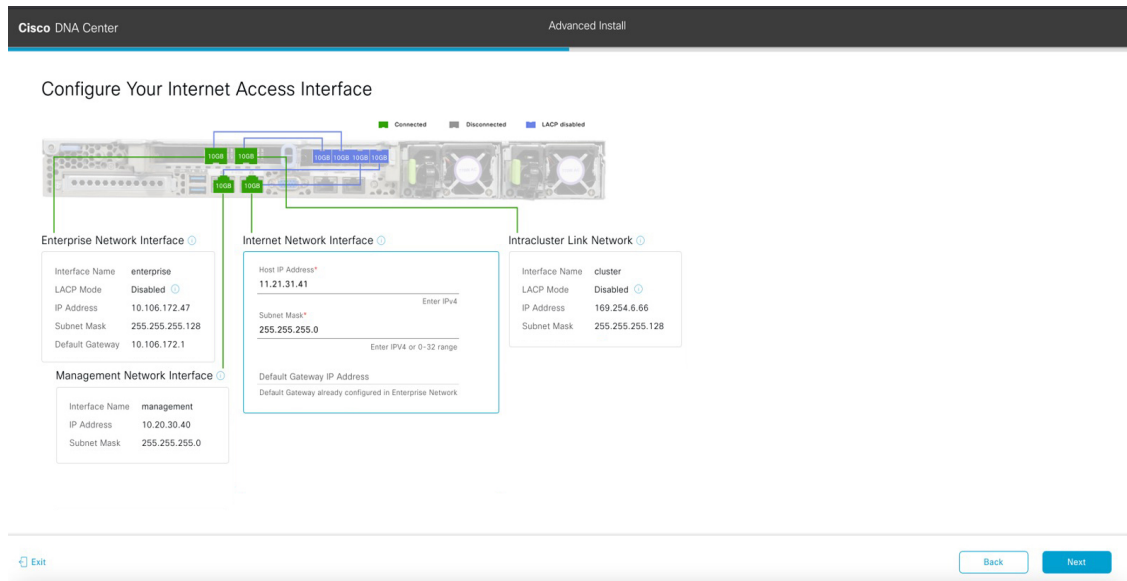
「[インターフェースケーブル接続](#)」で説明したように、このポートは管理ネットワークから Cisco DNA Center GUI にアクセスするために使用されます。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。（入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください）

(注) 同じポートでエンタープライズインターフェイスとインターネットアクセスインターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 37: 管理ポートのプライマリノードエントリ

[Host IP Address] フィールド	管理ポートの IP アドレスを入力します。
[Subnet Mask] フィールド	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。
[デフォルトゲートウェイ IP アドレス (Default Gateway IP Address)] フィールド	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。 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。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Internet Access Interface] 画面が開きます。



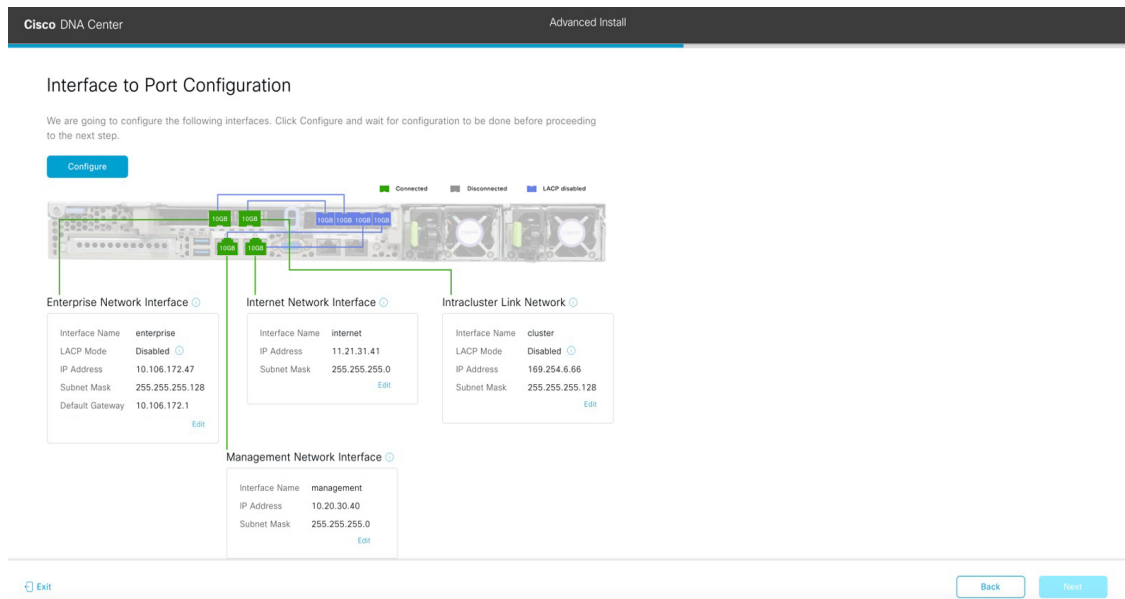
- g) (任意) インターネットアクセスインターフェイスの構成値を入力し、[Next] をクリックします。
- 「[インターフェースケーブル接続](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。専用インターネットアクセスインターフェイスを設定す

る場合は、次の表に示す情報を入力します。（入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください）

表 38: インターネット アクセス ポートのプライマリノードエントリ

[Host IP Address] フィールド	インターネット アクセス ポートの IP アドレスを入力します。
[Subnet Mask] フィールド	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、前のフィールドに 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 (Default Gateway IP Address)] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Interface to Port Configuration] 画面が開きます。



- h) プライマリノードのインターフェイスに入力した設定を確認します。
変更が必要な場合は、該当するインターフェイスの [Edit] リンクをクリックします。
- i) インターフェイスの設定に問題がなければ、[Configure] をクリックします。
- j) インターフェイスの初期設定が完了したら、[Next] をクリックします。
[DNS Configuration] 画面が開きます。

Cisco DNA Center Advanced Install

DNS Configuration

Enter the IP address of the preferred DNS server. To enter additional DNS servers, click the Add (+) configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS appliances.

DNS* +

Exit Review Back Next

- k) 優先 DNS サーバーの IP アドレスを入力して、[Next] をクリックします。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバーを設定します。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。
- NTP の場合、Cisco DNA Center と NTP サーバー間でポート 123 (UDP) が開いていることを確認します。

[Configure Proxy Server Information] 画面が開きます。

Cisco DNA Center Advanced Install

Configure Proxy Server Information

Does your network use a proxy server to access the internet?

Yes No

Proxy Server* E.g. http://example.com

Port* Enter port number between 0 to 65535.

Username

Password

Exit Review Back Next

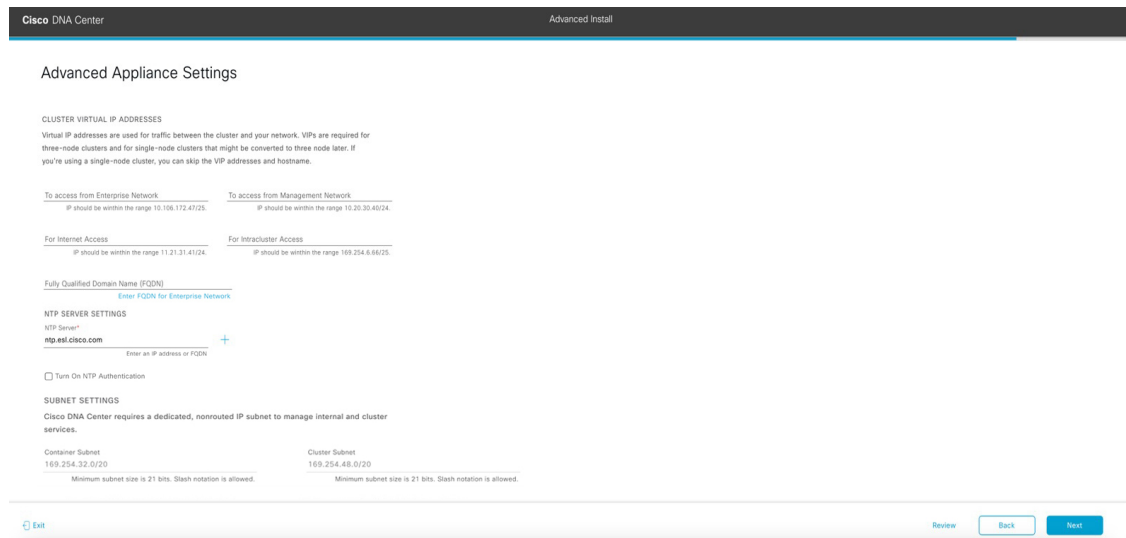
- l) 次のいずれかを実行し、[Next] をクリックします。

- ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックします。
- ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、次の表に示す値を入力します。

表 39: プロキシサーバー設定のプライマリノードエントリ

[プロキシサーバ (Proxy Server)] フィールド	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。
[Port] フィールド	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。
[Username] フィールド	ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
Password フィールド	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Advanced Appliance Settings] 画面が開きます。



- m) クラスタの構成値を入力し、[Next] をクリックします。

表 40 : [Advanced Appliance Settings] のプライマリノードエントリ

クラスタ仮想 IP アドレス	
<p>[To access from Enterprise Network]、[To access from Management Network]、[For Internet Access]、および [For Intracluster Access] フィールド</p> <p>(注) エンタープライズ インターフェイスと同じポートで管理インターフェイスまたはインターネット アクセス インターフェイスを設定した場合、対応するフィールドはこのセクションに表示されません。</p>	<p>プライマリノードに設定したクラスタとインターフェイス間のトラフィックに使用される仮想 IP アドレスを入力します。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。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。</p> <p>重要 仮想 IP アドレスを構成する場合は、構成されたネットワーク インターフェイスごとに 1 つ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。</p>
[Fully Qualified Domain Name (FQDN)] フィールド	<p>クラスタの完全修飾ドメイン名 (FQDN) を指定します。Cisco DNA Center は、このホスト名を使用して次の操作を実行します。</p> <ul style="list-style-type: none"> 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。
NTP サーバー設定	
[NTP Server] フィールド	<p>少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。</p> <p>実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。</p>

<p>[Turn On NTP Authentication] チェックボックス</p>	<p>Cisco DNA Center と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> • NTP サーバーのキー ID。有効な値の範囲は 1 ~ 4294967295 (2³²-1) です。 <p>この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。</p> <ul style="list-style-type: none"> • NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。 <p>(注) 前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。</p>
<p>サブネット設定</p>	
<p>[Container Subnet] フィールド</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。</p>
<p>[Cluster Subnet] フィールド</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。</p>

[Enter CLI Password] 画面が開きます。

The screenshot shows the 'Enter CLI Password' step in the Cisco DNA Center installation wizard. The page title is 'Cisco DNA Center' and 'Advanced Install'. The main heading is 'Enter CLI Password'. Below the heading, there is a descriptive text: 'CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster'. The form contains three input fields: 'Username*' with the value 'maglev', 'Password*' with masked characters and a 'SHOW' button, and 'Retype to Confirm*' with masked characters and a 'SHOW' button. A 'View Password Criteria' link is positioned between the password and retype fields. At the bottom of the form, there are four buttons: 'Exit', 'Review', 'Back', and 'Next'.

n) maglev ユーザーのパスワードを入力して確認した後、[Next] をクリックします。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。

Cisco DNA Center Advanced Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Ports Configuration Completed

Connected Disconnected LACP disabled

Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.47
Subnet Mask	255.255.255.128
Default Gateway	10.106.172.1

Internet Network Interface

Interface Name	internet
IP Address	11.21.31.41
Subnet Mask	255.255.255.0

Intracluster Link Network

Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.66
Subnet Mask	255.255.255.128

Management Network Interface

Interface Name	management
IP Address	10.20.30.40
Subnet Mask	255.255.255.0

Exit Start Configuration

(注) アプライアンスの設定を JSON ファイルとしてダウンロードするには、こちらのリンクをクリックします。

- o) ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な [Edit] リンクをクリックして、更新を行うウィザード画面を開きます。
- p) Cisco DNA Center アプライアンスの設定を完了するには、[Start Configuration] をクリックします。

プロセス中もウィザード画面が継続的に更新され、現在実行しているタスクとその進行状況、発生したエラーが示されます。この情報のローカルコピーをテキストファイルとして保存するには、ダウンロードアイコンをクリックします。

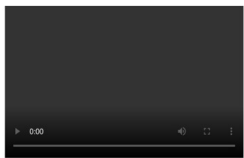
Cisco DNA Center
Configuration

Appliance Configuration In Progress

It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.

Initializing the cluster using kubectl 30%

ABOUT STARTING CISCO DNA CENTER



Started: 04/09/2020 12:15:36

```

2021-05-05T16:56:59.32524 | -----
2021-05-05T16:56:59.32525 | credentialmanager.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32526 | kong.pem Apr 13 16:49:51 2020 GMT Apr 13 16:49:51 2021 GMT
2021-05-05T16:56:59.32527 | kube-admin.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT
2021-05-05T16:56:59.32528 | kube-worker-1.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32529 | maglev-registry.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32530 | apiserver.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.32531 | apiserver-kubelet-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.32532 | front-proxy-ca.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.32533 | front-proxy-client.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.32534 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.32535 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.32536 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.32537 | controller-manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.32538 | -----

```

次のタスク

タスクが完了した後：

- このアプライアンスをスタンドアロンモードのみで展開する場合には、初回セットアップ（「初期設定ワークフロー」）を実行して続行します。
- 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 番目のインストール済みアプライアンスを設定します（[詳細インストール構成ウィザードを使用したセカンダリノードの設定（178 ページ）](#)）。

詳細インストール構成ウィザードを使用したセカンダリノードの設定

詳細インストール構成ウィザードを使用して、クラスタ内の 2 番目と 3 番目のノードを設定するには、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。
- 次の第 2 世代 Cisco DNA Center アプライアンスでは、詳細インストール構成ウィザードを使用した設定がサポートされています。
 - 44 コアアプライアンス：シスコ製品番号 DN2-HW-APL
 - 44 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-U
 - 56 コアアプライアンス：シスコ製品番号 DN2-HW-APL-L
 - 56 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-L-U

第 1 世代 44 コア Cisco DNA Center アプライアンス（シスコ製品番号 DN1-HW-APL）は、このウィザードを使用しても設定することはできません。

- このウィザードは、新しい Cisco DNA Center アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、[Maglev 設定ウィザード](#)を使用する必要があります（[Maglev ウィザードを使用したアプライアンスの設定（93 ページ）](#)を参照）。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、（ネットワークのデバイスを検出してテレメトリを有効にするために完了する）クイック スタート ワークフローが開始されません。
- 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。

新しいセカンダリ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アプライアンスをプライマリノードとして指定する必要があります。クラスタにセカンダリノードを結合する際、次の点に注意してください。

- クラスタに新しいノードを追加する前に、インストールされているすべてのパッケージがプライマリノードに展開されていることを確認してください。展開されているかどうかを確認するには、セキュアシェルを使用して、プライマリノードの Cisco DNA Center 管理ポートに Linux ユーザ（maglev）としてログインしてから、`maglev package status` コマンドを実行します。インストールされているすべてのパッケージは、コマンド出力で「展開済み (DEPLOYED)」と表示されます。

詳細インストール構成ウィザードを使用したセカンダリノードの設定

```

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]
NAME                                DISPLAY_NAME                                DEPLOYED    AVAILABLE    STATUS    PROGRESS
-----
access-control-application          Access Control Application                  -            2.1.369.60050    NOT_DEPLOYED
ai-network-analytics                AI Network Analytics                       -            2.6.10.494      NOT_DEPLOYED
app-hosting                         Application Hosting                         -            1.6.6.2201241723    NOT_DEPLOYED
application-policy                  Application Policy                           -            2.1.369.170033    NOT_DEPLOYED
application-registry                Application Registry                         -            2.1.369.170033    NOT_DEPLOYED
application-visibility-service      Application Visibility Service               -            2.1.369.170033    NOT_DEPLOYED
assurance                            Assurance - Base                            2.2.2.485     -                DEPLOYED
automation-core                    NCP - Services                             2.1.368.60015  2.1.369.60050    DEPLOYED
base-provision-core                 Automation - Base                           2.1.368.60015  2.1.369.60050    DEPLOYED
cloud-connectivity-contextual       Cloud Connectivity - Contextual Content     1.3.1.364     -                DEPLOYED
cloud-connectivity-data-hub         Cloud Connectivity - Data Hub               1.6.0.380     -                DEPLOYED
cloud-connectivity-tethering         Cloud Connectivity - Tethering              2.12.1.2     -                DEPLOYED
cloud-provision-core                Cloud Device Provisioning Application       -            2.1.369.60050    NOT_DEPLOYED
command-runner                      Command Runner                              2.1.368.60015  2.1.369.60050    DEPLOYED
device-onboarding                  Device Onboarding                           2.1.368.60015  2.1.369.60050    DEPLOYED
disaster-recovery                  Disaster Recovery                           -            2.1.367.360196    NOT_DEPLOYED
dna-core-apps                       Network Experience Platform - Core         2.1.368.60015  2.1.369.60050    DEPLOYED
dnac-platform                       Cisco DNA Center Platform                  1.5.1.180     1.5.1.182       DEPLOYED
dnac-search                         Cisco DNA Center Global Search             1.5.0.466     -                DEPLOYED
endpoint-analytics                  AI Endpoint Analytics                       -            1.4.375         NOT_DEPLOYED
group-based-policy-analytics        Group-Based Policy Analytics               -            2.2.1.401       NOT_DEPLOYED
icap-automation                    Automation - Intelligent Capture           2.1.369.60050  2.1.369.60050    NOT_DEPLOYED
image-management                    Image Management                           2.1.368.60015  2.1.369.60050    DEPLOYED
machine-reasoning                  Machine Reasoning                           2.1.368.210017  2.1.369.210024    DEPLOYED
ncp-system                          NCP - Base                                 2.1.368.60015  2.1.369.60050    DEPLOYED
ndp-base-analytics                 Network Data Platform - Base Analytics      1.6.1028     1.6.1031        DEPLOYED
ndp-platform                       Network Data Platform - Core               1.6.596     -                DEPLOYED
ndp-ui                             Network Data Platform - Manager            1.6.543     -                DEPLOYED
network-visibility                  Network Controller Platform                 2.1.368.60015  2.1.369.60050    DEPLOYED
path-trace                          Path Trace                                  2.1.368.60015  2.1.369.60050    DEPLOYED
platform-ui                         Cisco DNA Center UI                         1.6.2.446     1.6.2.448       DEPLOYED
rbac-extensions                     RBAC Extensions                            2.1.368.1910001  2.1.369.1910003    DEPLOYED
rogue-management                   Rogue and aWIPS                             -            2.2.0.51        NOT_DEPLOYED
sd-access                           SD Access                                   -            2.1.369.60050    NOT_DEPLOYED
sensor-assurance                    Assurance - Sensor                          -            2.2.2.484       NOT_DEPLOYED
sensor-automation                  Automation - Sensor                         2.1.369.60050  2.1.369.60050    NOT_DEPLOYED
ssa                                 Stealthwatch Security Analytics             2.1.368.1091226  2.1.369.1091317    DEPLOYED
system                              System                                       1.6.594     -                DEPLOYED
system-commons                      System Commons                              2.1.368.60015  2.1.369.60050    DEPLOYED
umbrella                            Cisco Umbrella                              -            2.1.368.592066    NOT_DEPLOYED
wide-area-bonjour                   Wide Area Bonjour                           -            2.4.368.75006    NOT_DEPLOYED

[Wed Nov 30 15:45:08 UTC] maglev@192.0.2.1 (maglev-master-192.0.2.1) ~
    
```

- 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う予期しない動作が発生します。
- 各セカンダリノードのクラスタ接続プロセス中に、一部のサービスのダウンタイムが発生することが予想されます。サービスはすべてのノードに再配布される必要があり、そのプロセスの間、クラスタはダウンします。

始める前に

次のことを確認します。

- 「[アプライアンスのイメージの再作成 \(86 ページ\)](#)」の説明どおりに Cisco DNA Center ソフトウェアイメージがアプライアンスにインストールされたこと。



重要 次のアプライアンスには Cisco DNA Center ソフトウェアイメージがあらかじめインストールされていないため、これはプロモーションアプライアンスを設定する場合にのみ当てはまります。

- 44 コア プロモーションアプライアンス：シスコ製品番号 DN2-HW-APL-U
- 56 コア プロモーションアプライアンス：シスコ製品番号 DN2-HW-APL-L-U

- 詳細インストール構成ウィザードを使用したプライマリノードの設定 (157 ページ) 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 \(33 ページ\)](#) と [必須の設定情報](#) で必要な情報がすべて収集されたこと。
- 「[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、両方のセカンダリノードで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「[事前設定タスクの実行](#)」の説明に従って、セカンダリノードのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- 互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順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。ウィザードでは、ユーザの指定する DNS サーバを ping で確認します。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 詳細インストール構成ウィザードを起動します。

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

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



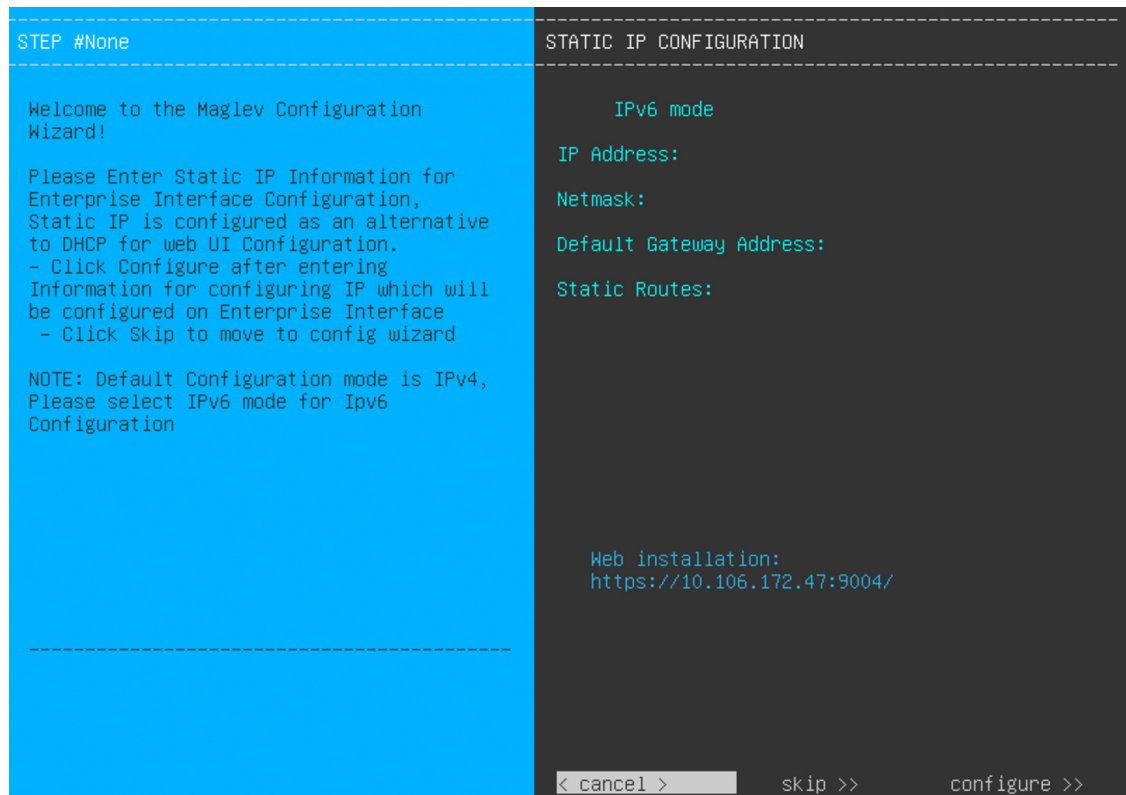
- b) 青いリンクメニューで [Launch KVM] を選択してから、[Java based KVM] と [HTML based KVM] のいずれかを選択します。[Java based KVM] を選択した場合、KVM コンソールを独自のウィンドウで表示するために、ブラウザまたはファイルマネージャから Java スタートアップファイルを起動する必要があります。[HTML based KVM] を選択すると、KVM コンソールが別個のブラウザウィンドウまたはタブで自動的に起動します。

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。

- c) 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] を選択します。その後、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 [Static IP Configuration] 画面が表示されます。



[Web インストール (Web Installation)] フィールドにリストされている URL に注意してください。

d) 次のいずれかを実行します。

- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てるようにするには、[Skip] をクリックします。
- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、[Configure] をクリックします。

[IPv6 Mode] チェックボックス	IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。
[IP Address] フィールド	使用する静的 IP アドレスを入力します。
[ネットマスク (Netmask)] field	<p>前のフィールドに指定した IP アドレスのネットマスクを入力します。</p> <ul style="list-style-type: none"> • IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。 • IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。

[Default Gateway Address] フィールド	トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
[Static Routes] フィールド	1つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク>/<ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。

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。

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >

```

- e) [Appliance Configuration] 画面を表示するには、[Static IP Configuration] 画面に表示された URL を開きます。

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

<p>Start A Cisco DNA Center Cluster <input type="radio"/></p> <hr/> <p>This appliance will be the primary node of a cluster.</p>	<p>Join A Cisco DNA Center Cluster <input checked="" type="radio"/></p> <hr/> <p>This appliance will be added as a node to the primary node of a cluster.</p>
--	---



Next

- f) [Join a Cisco DNA Center Cluster] オプションボタンをクリックし、[Next] をクリックします。

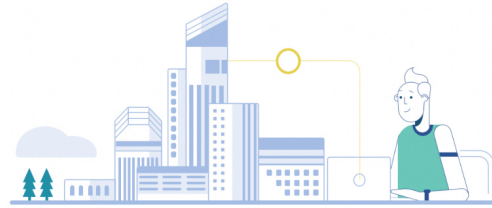
Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.
Which workflow matches your needs?

Advanced Install ▶

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.



Back

Start

- g) [Advanced Install] オプションボタンをクリックし、[Start] をクリックします。

[Advanced Install Overview] スライドが開きます。[>] をクリックして、ウィザードで実行するタスクの概要を表示します。

Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.



Start Workflow



- h) [Start Workflow] をクリックしてウィザードを起動します。

[Appliance Interface Overview] 画面が開き、設定可能な 4 つのアプライアンス インターフェイスの説明が表示されます。

Cisco DNA Center Advanced Install

Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracluster Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA Center GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the Internet.

In this workflow, the Enterprise Network Interface and the Intracluster Link Interface will each have their own dedicated port. You can choose to have either Management Network Interface and/or Internet Access Interface be on the same port as the Enterprise Network Interface or assign them to a separate designated port.

Exit Next

重要 Cisco DNA Center の機能に必要なため、少なくともアプライアンスのエンタープライズポートおよびクラスタポートにインターフェイスを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか1つまたは両方が表示されない場合、表示されない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。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザード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「[事前設定タスクの実行](#)」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 2 詳細インストール構成ウィザードを完了します。


- a) [Next] をクリックします。

[Will this appliance join a cluster?] 画面が開きます。

Cisco DNA Center Advanced Install

Will this appliance join a cluster?

This appliance is running on [software version] *N/A*.



Yes, This appliance will be added as a node to the primary node of a cluster.
 No, This appliance will be the primary node of a cluster.

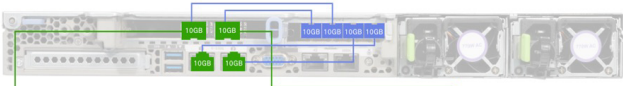
[Exit](#) [Back](#) [Next](#)

- b) [Yes] オプションボタンをクリックし、[Next] をクリックします。
 [How would you like to set up your appliance interfaces?] 画面が開きます。

Cisco DNA Center Advanced Install

How would you like to set up your appliance interfaces?

Both Enterprise Network and Intracluster Link Interfaces have their own designated port. You can decide whether to have a separate dedicated port for either Management Network Interface and Internet Access Interface. Before you start, reserve the IP addresses necessary for configuration. If your network resides behind a firewall, be sure to [allow access to these URLs](#) and [open these ports](#).



Enterprise Network Interface Intracluster Link Network

The Enterprise Network Interface and Intracluster Link Interface will be configured using the two 10-Gbps ports as shown above.

Would you like to have a dedicated Management Network Interface?

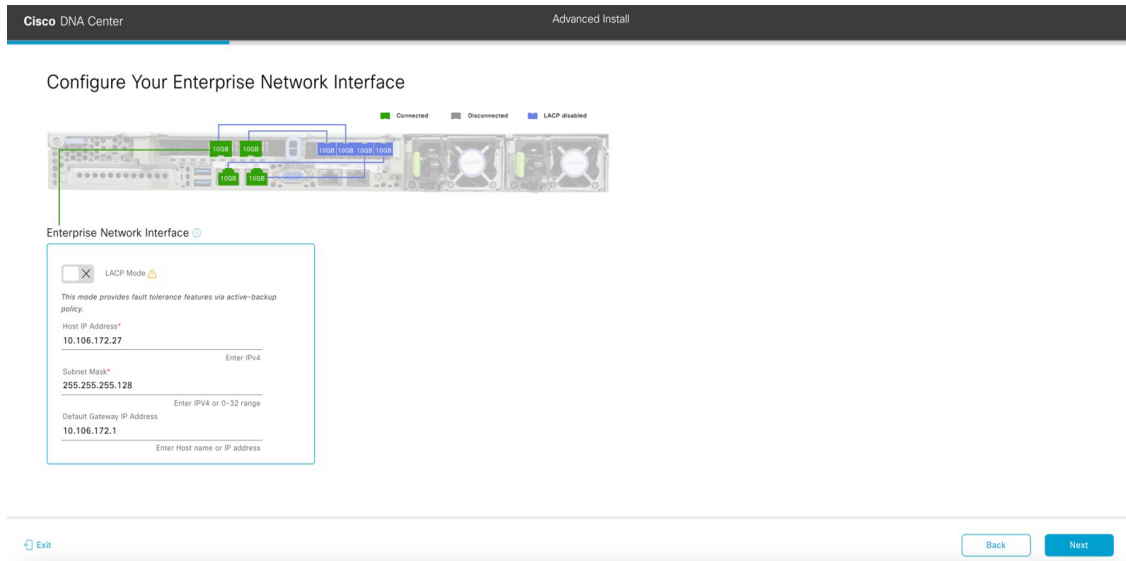
Yes No

Would you like to have a dedicated Internet Access Interface?

Yes No

[Exit](#) [Back](#) [Next](#)

- c) 専用の管理およびインターネット アクセス インターフェイスを設定するかどうかを指定し、[Next] をクリックします。
 [Configure Your Enterprise Network Interface] 画面が開きます。



d) エンタープライズインターフェイスの構成値を入力し、[Next] をクリックします。

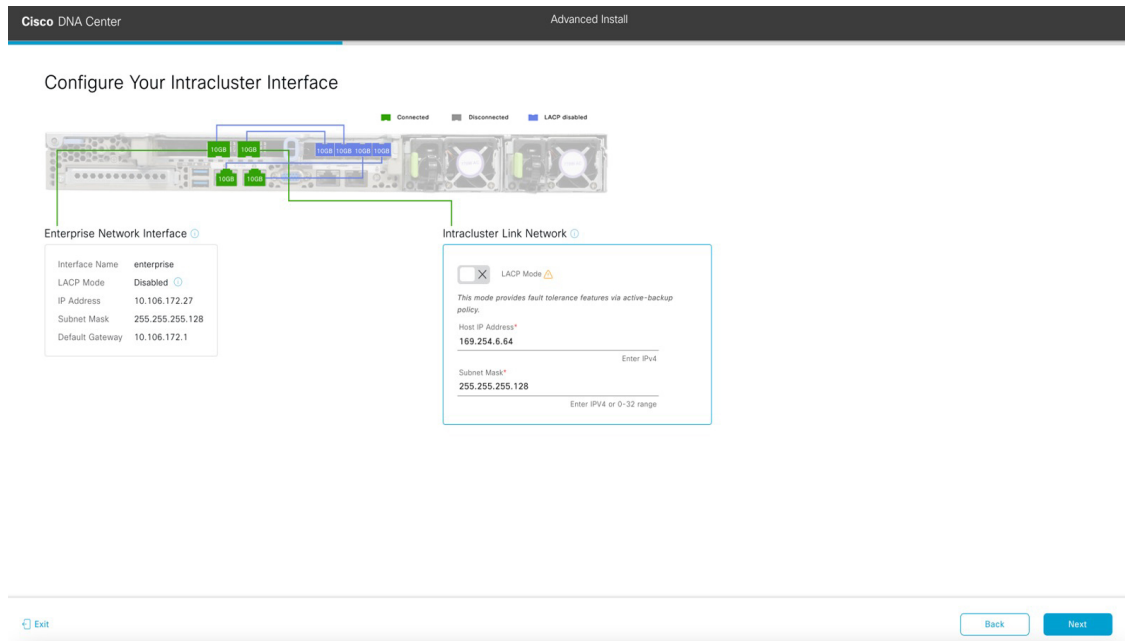
「[インターフェイスケーブル接続](#)」で説明したように、このインターフェイスは、アプライアンスをエンタープライズネットワークにリンクするために必要なインターフェイスです。入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

表 41: エンタープライズインターフェイスのセカンダリノードエントリ

<p>[LACP Mode] スライダ</p>	<p>エンタープライズインターフェイスに対して、次のネットワークインターフェイスコントローラ (NIC) ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード：このモードでは、2つのイーサネットインターフェイスを1つの論理チャンネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード：このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネットインターフェイスが1つの論理チャンネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
<p>[Host IP Address] フィールド</p>	<p>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。</p>
<p>[Subnet Mask] フィールド</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 (Default Gateway IP Address)] フィールド</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>(注) このインターフェイスは、DHCP サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。</p> <ol style="list-style-type: none"> このフィールドに現在一覧表示されている IP アドレスを削除し、[Exit] をクリックします。 この操作でウィザードの最初の画面に戻ります。 エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ IP アドレスを入力します。
--	--

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Intracluster Interface] 画面が開きます。



- e) クラスタ内インターフェイスの構成値を入力し、[Next] をクリックします。

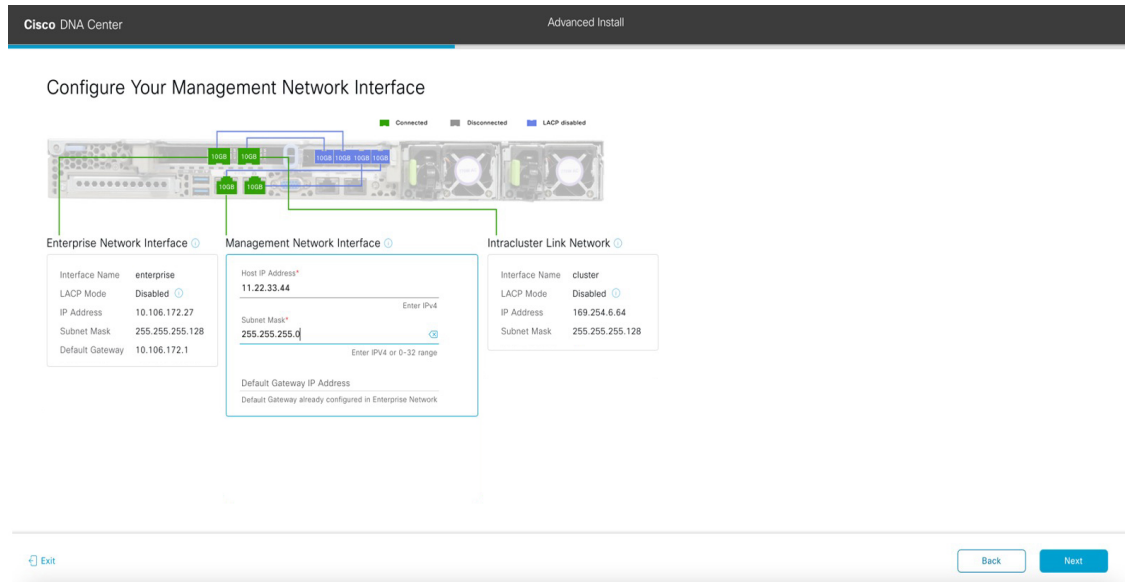
「[インターフェイスケーブル接続](#)」で説明したように、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

- (注)
- 同じポートでエンタープライズ インターフェイスとインターネット アクセス インターフェイスを設定する場合は、この手順を実行してから、ステップ 2f (管理 インターフェイスの設定方法が記載) に進みます。
 - エンタープライズ インターフェイスと管理 インターフェイスを同じポートに設定する場合は、この手順を実行してから、ステップ 2g (インターネット アクセス インターフェイスの設定方法が記載) に進みます。
 - 同じポートでエンタープライズ、管理、およびインターネット アクセス インターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 42: クラスタ内インターフェイスのセカンダリノードエントリ

[LACP Mode] スライダ	<p>クラスタ内インターフェイスに対して、次の NIC ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード：このモードでは、2つのイーサネット インターフェイスを1つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード：このモードでは、同じ速度とデデュプレックス設定を共有する2つのイーサネット インターフェイスが1つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
[Host IP Address] フィールド	<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>
[Subnet Mask] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Management Network Interface] 画面が開きます。



f) (任意) 管理ポートの構成値を入力し、[Next] をクリックします。

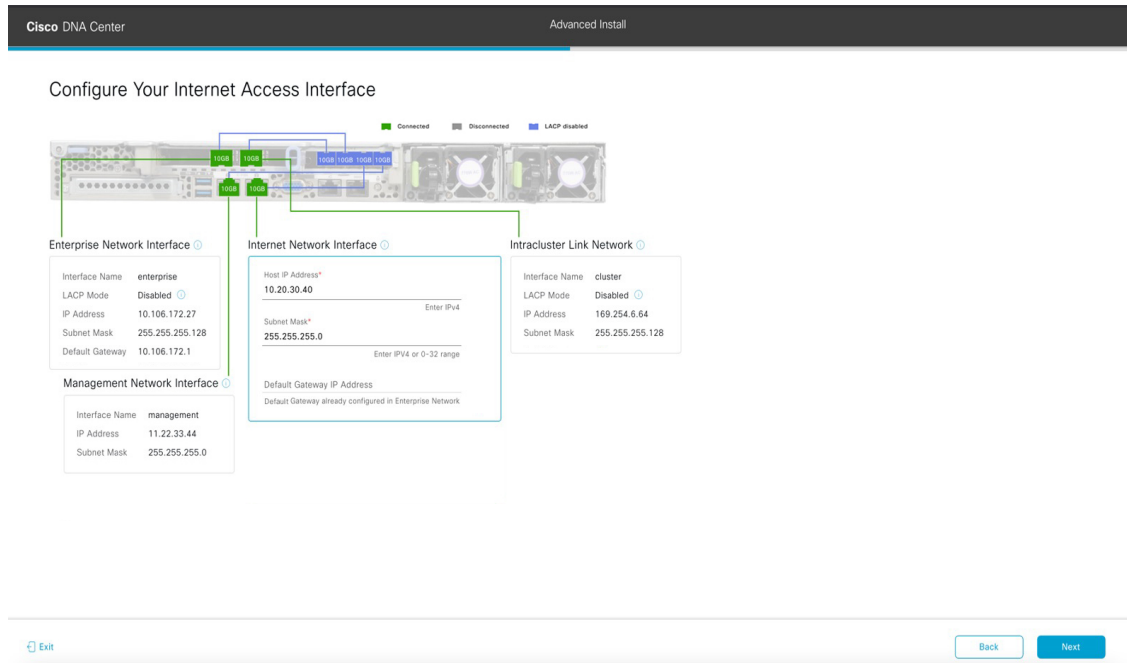
「[インターフェイスクーブル接続](#)」で説明したように、このポートは管理ネットワークから Cisco DNA Center GUI にアクセスするために使用されます。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。（入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください）

(注) 同じポートでエンタープライズインターフェイスとインターネットアクセスインターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 43: 管理ポートのセカンダリノードエントリ

[Host IP Address] フィールド	管理ポートの IP アドレスを入力します。これは必須です。
[Subnet Mask] フィールド	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 (Default Gateway IP Address)] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Internet Access Interface] 画面が開きます。



- g) (任意) インターネットアクセスインターフェイスの構成値を入力し、[Next] をクリックします。
- 「[インターフェースケーブル接続](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。専用インターネットアクセスインターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください)

表 44: インターネットアクセスポートのセカンダリノードエントリ

[Host IP Address] フィールド	インターネットアクセスポートの IP アドレスを入力します。
[Subnet Mask] フィールド	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 (Default Gateway IP Address)] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Interface to Port Configuration] 画面が開きます。

詳細インストール構成ウィザードを使用したセカンダリノードの設定

Cisco DNA Center Advanced Install

Interface to Port Configuration

We are going to configure the following interfaces. Click Configure and wait for configuration to be done before proceeding to the next step.

[Configure](#)

Connected Disconnected LACP disabled

Enterprise Network Interface	Internet Network Interface	Intracluster Link Network
Interface Name: enterprise	Interface Name: internet	Interface Name: cluster
LACP Mode: Disabled	IP Address: 10.20.30.40	LACP Mode: Disabled
IP Address: 10.106.172.27	Subnet Mask: 255.255.255.0	IP Address: 169.254.6.64
Subnet Mask: 255.255.255.128	Edit	Subnet Mask: 255.255.255.128
Default Gateway: 10.106.172.1		Edit

Management Network Interface

Interface Name: management
IP Address: 11.22.33.44
Subnet Mask: 255.255.255.0
Edit

[Exit](#) [Back](#) [Next](#)

- h) セカンダリノードのインターフェイスに入力した設定を確認します。
変更が必要な場合は、関連するインターフェイスの [Edit] リンクをクリックして、ウィザード画面に戻ります。
- i) インターフェイスの設定に問題がなければ、[Configure] をクリックします。
- j) インターフェイスの初期設定が完了したら、[Next] をクリックしてウィザードの次の画面に進みます。
- [DNS Configuration] 画面が開きます。

Cisco DNA Center Advanced Install

DNS Configuration

Enter the IP address of the preferred DNS server. To enter additional DNS servers, click the Add (+) configure a maximum of three DNS servers. Problems can occur if you configure more than three DNS appliances.

DNS* +
Enter an IPv4 address

[Exit](#) [Review](#) [Back](#) [Next](#)

- k) 優先 DNS サーバーの IP アドレスを入力して、[Next] をクリックします。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバーを設定します。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。
- NTP の場合、Cisco DNA Center と NTP サーバー間でポート 123 (UDP) が開いていることを確認します。

[Configure Proxy Server Information] 画面が開きます。

The screenshot shows the 'Configure Proxy Server Information' configuration page. At the top, it says 'Cisco DNA Center' and 'Advanced Install'. The main heading is 'Configure Proxy Server Information'. Below this, it asks 'Does your network use a proxy server to access the internet?' with radio buttons for 'Yes' (selected) and 'No'. There are input fields for 'Proxy Server*' (containing 'http://proxy.cisco.com'), 'Port*' (containing '80'), 'Username', and 'Password'. A small note under the port field says 'Enter port number between 0 to 65535'. At the bottom, there are buttons for 'Exit', 'Review', 'Back', and 'Next'.

1) 次のいずれかを実行し、[Next] をクリックします。

- ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックします。
- ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、次の表に示す値を入力します。

表 45: プロキシサーバー設定のセカンダリノードエントリ

[プロキシサーバ (Proxy Server)] フィールド	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。
[Port] フィールド	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

[Username] フィールド	ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
Password フィールド	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Primary Node Details] 画面が開きます。

Cisco DNA Center Advanced Install

Primary Node Details

This appliance is getting added as a node for the multi-node setup with software version *N/A*. This information will be used when you need to log into the Maglev CLI.

Primary Node IP*
IP should be within Intra-Cluster's 169.254.6.66/25

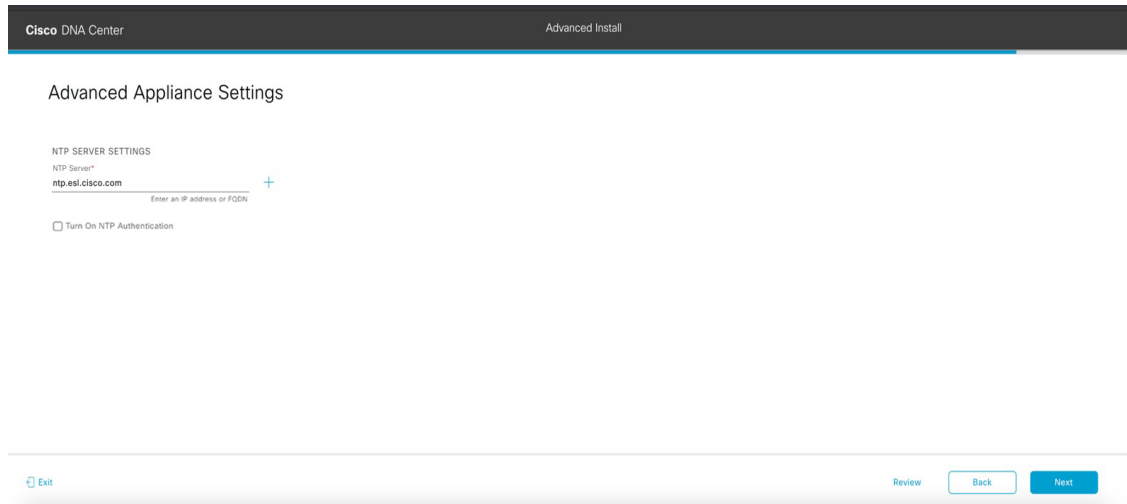
CLI Username
 maglev

CLI Password*
Enter CLI Password

Exit Review Back Next

- m) クラスタのプライマリノードとの接続を確立するには、その IP アドレスとログイン情報を入力し、[Next] をクリックします。

[Advanced Appliance Settings] 画面が開きます。



- n) クラスタの構成値を入力し、[Next] をクリックします。

表 46 : [Advanced Appliance Settings] のセカンダリノードエントリ

NTP サーバー設定	
[NTP Server] フィールド	<p>少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。</p> <p>実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。</p>
[Turn On NTP Authentication] チェックボックス	<p>Cisco DNA Center と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> • NTP サーバーのキー ID。有効な値の範囲は 1 ~ 4294967295 (2³²-1) です。 この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。 • NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。 <p>(注) 前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。</p>

[CLI パスワードの入力] 画面が開きます。

Cisco DNA Center Advanced Install

Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster

Username*
maglev

Password*
..... [SHOW](#)

[View Password Criteria](#)

Retype to Confirm*
..... [SHOW](#)

[Review](#) [Back](#) [Next](#)

- o) maglev ユーザーのパスワードを入力して確認した後、[Next] をクリックします。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。

Cisco DNA Center Advanced Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Ports Configuration Completed ■ Connected ■ Disconnected ■ LACP disabled

Interface Name	LACP Mode	IP Address	Subnet Mask	Default Gateway
enterprise	Disabled	10.106.172.27	255.255.255.128	10.106.172.1
internet		10.20.30.40	255.255.255.0	
cluster	Disabled	169.254.6.64	255.255.255.128	
management		11.22.33.44	255.255.255.0	

[Exit](#) [Start Configuration](#)

(注) アプライアンスの設定を JSON ファイルとしてダウンロードするには、こちらのリンクをクリックします。

- p) ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な [Edit] リンクをクリックして、更新を行うウィザード画面を開きます。
- q) Cisco DNA Center アプライアンスの設定を完了するには、[Start Configuration] をクリックします。

プロセス中もウィザード画面が継続的に更新され、現在実行しているタスクとその進行状況、発生したエラーが示されます。この情報のローカルコピーをテキストファイルとして保存するには、ダウンロードアイコンをクリックします。

Cisco DNA Center
Configuration

Appliance Configuration In Progress

It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.

Initializing the cluster using kubeadm 30%

ABOUT STARTING CISCO DNA CENTER

▶ 0:00

Started: 04/09/2020 12:15:36

2021-05-05T16:56:59.32524 | -----

2021-05-05T16:56:59.32525 | credentialmanager.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.32526 | kong.pem Apr 13 16:49:51 2020 GMT Apr 13 16:49:51 2021 GMT

2021-05-05T16:56:59.32527 | kube-admin.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT

2021-05-05T16:56:59.32528 | kube-worker-1.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.32529 | majiein-registry.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.325210 | apiserver.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325211 | apiserver-kubelet-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325212 | front-proxy-ca.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2030 GMT

2021-05-05T16:56:59.325213 | front-proxy-client.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325214 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT

2021-05-05T16:56:59.325215 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT

2021-05-05T16:56:59.325216 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT

2021-05-05T16:56:59.325217 | controller-manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT

2021-05-05T16:56:59.325218 | -----

次のタスク

タスクが完了した後：

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

最新の Cisco DNA Center リリースへのアップグレード

Cisco DNA Center の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 7 章

ブラウザベースのウィザードを使用した 112 コアアプライアンスの設定

- [アプライアンスの設定の概要 \(201 ページ\)](#)
- [インストール構成ウィザードを使用したアプライアンスの設定 \(203 ページ\)](#)
- [詳細インストール構成ウィザードを使用したプライマリノードの設定 \(218 ページ\)](#)
- [詳細インストール構成ウィザードを使用したセカンダリノードの設定 \(238 ページ\)](#)
- [最新の Cisco DNA Center リリースへのアップグレード \(258 ページ\)](#)

アプライアンスの設定の概要

次のいずれかのモードを使用して、112 コア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。初期展開でスタンドアロンモードを選択した場合は、これが最初のノード、つまりプライマリノードになります。後でさらにアプライアンスを追加してクラスタを形成できます。
- **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。初期展開でクラスタモードを選択した場合は、セカンダリ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、最初にクラスタのプライマリノードを設定します。3 つのアプライアンスを設置済みで、クラスタに 2 番目と 3 番目のノードを追加する場合は、次に、セカンダリノードを設定します。

ブラウザベースの構成ウィザード

Cisco DNA Center は、アプライアンスの設定に使用できる 2 種類のブラウザベースのウィザードを提供します。説明を読んで、どのウィザードを完了する必要があるかを判断してください。



重要 これらのウィザードは、Cisco DNA Center 2.3.5 がすでにインストールされている新しいアプライアンスを設定している場合に使用できます。以前のバージョンからアップグレードし、これらのウィザードを使用する場合は、Cisco TAC に連絡して支援を受けてください。

インストール構成ウィザード

このウィザードは、クラスタ内のインターフェイスだけでなく、企業インターフェイス、管理インターフェイス、およびインターネット アクセス インターフェイス（すべてアプライアンスのエンタープライズポートに存在）にもデフォルト値を設定し、アプライアンスの設定プロセスを合理化します。デフォルトのインターフェイス設定を使用しても問題がなく、アプライアンスを可能な限り早く稼働させたい場合は、このウィザードを使用します。このウィザードではクラスタのセカンダリノードは設定できないので注意してください。

高度なインストール構成ウィザード

このウィザードは、すべての利用可能なアプライアンスの設定（ユーザーによる変更が可能）へのアクセスを提供します。デフォルト設定とは異なるインターフェイス設定を指定する場合は、このウィザードを使用します。クラスタ内の 2 番目または 3 番目のノードを設定する場合にも、このウィザードを使用します。

ブラウザベースのウィザードの前提条件

ブラウザベースのウィザードのいずれかを使用して、アプライアンスの設定が正しいことを確認するには、次の手順を実行します。

- DHCP サーバーが割り当てる IP アドレス、サブネットマスク、デフォルトゲートウェイを使用するために、アプライアンス上のエンタープライズインターフェイスを指定します。ウィザードでこのインターフェイスを設定する場合、割り当てられている IP アドレスまたはサブネットマスクは変更できません。デフォルトゲートウェイのみ変更できます。この章で扱うトピックでは、エンタープライズインターフェイスがこの目的で選択されていることが前提となっています。
- DHCP サーバの割り当てた IP アドレスが、ウィザードを完了するマシンから到達できることを確認します。
- エンタープライズおよびクラスタ内インターフェイスの場合、両方のインターフェイスが接続されていて、[UP] 状態であることを確認します。

アプライアンスのエンタープライズインターフェイスに独自の IP アドレス、サブネットマスク、およびデフォルトゲートウェイを指定する場合（および DHCP サーバーによって割り当てられた値を使用しない場合）は、静的 IP アドレス設定画面が完了していることを確認します。

インストール構成ウィザードを使用したアプライアンスの設定

インストール構成ウィザードを使用して3 ノードクラスタのプライマリノードまたはスタンバイノードを設定するには、次の手順を実行します。ウィザードでは、デフォルト設定を使用して同じポートでエンタープライズ、管理、およびインターネットインターフェイスを設定することで、設定プロセスが簡素化されます。次の第2 世代 Cisco DNA Center アプライアンスは、このウィザードを使用した設定をサポートしています。

- 112 コアアプライアンス：シスコ製品番号 DN2-HW-APL-XL
- 112 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-XL-U



重要

- このウィザードを使用して、3 ノードクラスタの2 番目または3 番目のアプライアンスを設定することはできません。設定するには、[詳細インストール構成ウィザードを使用したセカンダリノードの設定 \(238 ページ\)](#) に記載されている手順を実行します。また、このウィザードを使用して、アプライアンスのエンタープライズおよびクラスタ内インターフェイスで LACP モードを有効にすることはできません。
- 3 ノードクラスタのいずれかのアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、(ネットワークのデバイスを検出してテレメトリを有効にするために完了する) クイック スタート ワークフローが開始されません。
- 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。

このウィザードは、新しい Cisco DNA Center アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、[Maglev 設定ウィザード](#)を使用する必要があります ([Maglev ウィザードを使用したアプライアンスの設定 \(93 ページ\)](#) を参照)。

始める前に

次のことを確認します。

- 「[アプライアンスのイメージの再作成 \(86 ページ\)](#)」の説明どおりに Cisco DNA Center ソフトウェアイメージがアプライアンスにインストールされたこと。



重要 Cisco DNA Center ソフトウェアイメージは 112 コア プロモーションアプライアンス（シスコ製品番号 DN2-HW-APL-XL-U）にあらかじめインストールされていないため、これはプロモーションアプライアンスを設定する場合にのみ当てはまります。

- [必要な IP アドレスおよびサブネット（33 ページ）](#) と [必須の設定情報](#) で必要な情報がすべて収集されたこと。
- 「[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、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、このアプライアンスで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「[事前設定タスクの実行](#)」の説明に従って、アプライアンスのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- Cisco IMC、Cisco DNA Center との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順で指定する DNS サーバと Cisco DNA Center の間のファイアウォールで ICMP が許容されること。このウィザードでは、ユーザの指定する DNS サーバを ping で確認します。Cisco DNA Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

ステップ 1 インストール構成ウィザードを起動します。

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

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



- b) 青いリンクメニューで [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。

- c) 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] を選択します。その後、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 [Static IP Configuration] 画面が表示されます。

```

STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration,
Static IP is configured as an alternative to DHCP for web UI Configuration.
- Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration

-----
STATIC IP CONFIGURATION

IPv6 mode

IP Address:
Netmask:
Default Gateway Address:
Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>

```

[Web インストール (Web Installation)] フィールドにリストされている URL に注意してください。

- d) 次のいずれかを実行します。
- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てるようにするには、[Skip] をクリックします。

- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、[Configure] をクリックします。

(注) 指定する必要があるのは、アプライアンスのエンタープライズインターフェイスの IP アドレス、サブネットマスク、およびデフォルトゲートウェイのみです。

[IPv6 Mode] チェックボックス	IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。
[IP Address] フィールド	使用する静的 IP アドレスを入力します。
[ネットマスク (Netmask)] field	前のフィールドに指定した IP アドレスのネットマスクを入力します。 <ul style="list-style-type: none"> • IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。 • IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。
[Default Gateway Address] フィールド	トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
[Static Routes] フィールド	1つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク><ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。

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。



- e) [Appliance Configuration] 画面を表示するには、[Static IP Configuration] 画面に表示された URL を開きます。


Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA Center Cluster
This appliance will be the primary node of a cluster.

Join A Cisco DNA Center Cluster
This appliance will be added as a node to the primary node of a cluster.



Next

- f) [Start a Cisco DNA Center Cluster] オプションボタンをクリックし、[Next] をクリックします。

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.
Which workflow matches your needs?

Install <input checked="" type="radio"/>	Advanced Install <input type="radio"/>
Configure a standalone node or cluster's primary node .	Configure a standalone node or any node in a cluster .
Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.	Use this wizard to access all of the available appliance configuration options.



Back

Start

- g) [Install] オプションボタンをクリックし、[Start] をクリックします。

[Overview] スライドが開きます。[>] をクリックして、ウィザードで実行するタスクの概要を表示します。

X

Overview

Complete the basic tasks required to configure your appliance for use with Cisco DNA Center.



Start Workflow

- h) [Start Workflow] をクリックしてウィザードを起動します。

[Appliance Interface Overview] 画面が開き、Cisco DNA Center アプライアンスで使用可能な 4 つのインターフェイスの説明が表示されます。

Cisco DNA Center Install

Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracluster Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the internet.

In this workflow, the Intracluster Link Interface is predefined. The other three interfaces will be configured together on the Enterprise port.

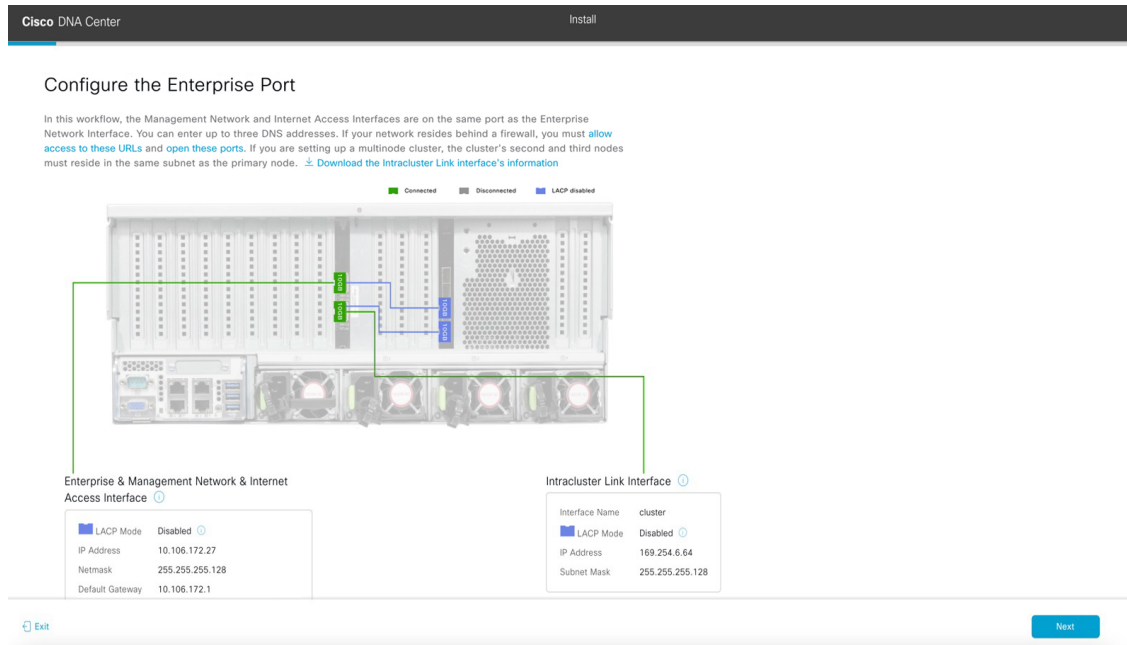
Exit Next

このウィザードを使用すると、Cisco DNA Center の機能に必要なエンタープライズポートとクラスタポートを設定できます。ウィザードの次の画面にこれらのポートのいずれかまたは両方が表示されない場合、表示されないポートは機能していないか、無効になっている可能性があります。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザード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「事前設定タスクの実行」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 2 インストール構成ウィザードを完了します。

- a) [Next] をクリックします。

[Configure The Enterprise Port] 画面が開きます。



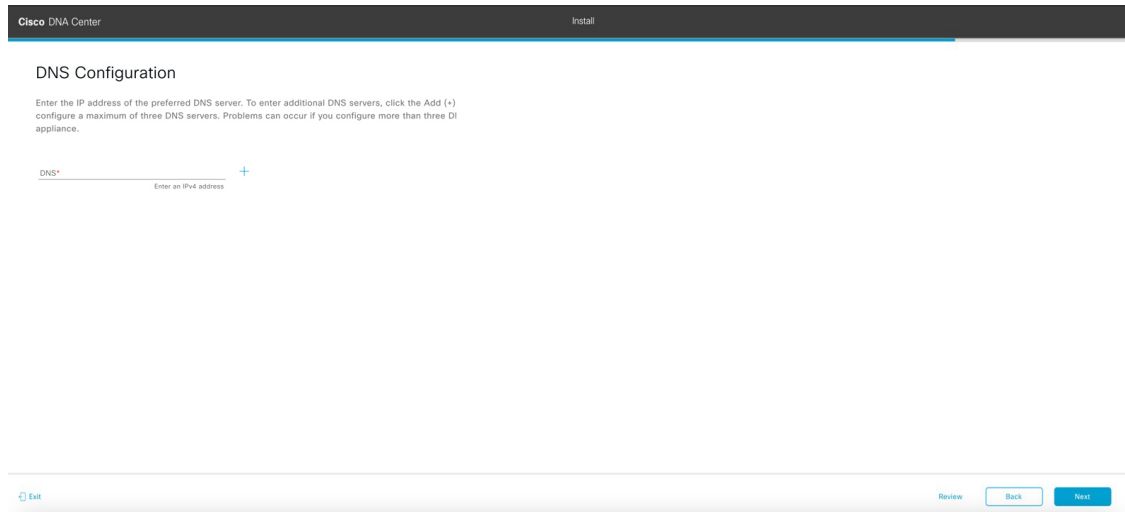
構成ウィザードにより、エンタープライズポートにエンタープライズ、管理、およびインターネットアクセスインターフェイスが設定されます。リストされているほぼすべてのパラメータの値も事前入力されます。

ネットワークがファイアウォールの背後にある場合は、次の手順を実行します。

- [\[allow access to these URLs\]](#) リンクをクリックすると、Cisco DNA Center がアクセスできる必要がある URL を一覧表示するポップアップウィンドウが表示されます。
- [\[open these ports\]](#) リンクをクリックすると、Cisco DNA Center が使用できる必要があるネットワークサービスポートを一覧表示するポップアップウィンドウが表示されます。

b) **[Next]** をクリックします。

[DNS Configuration] 画面が開きます。

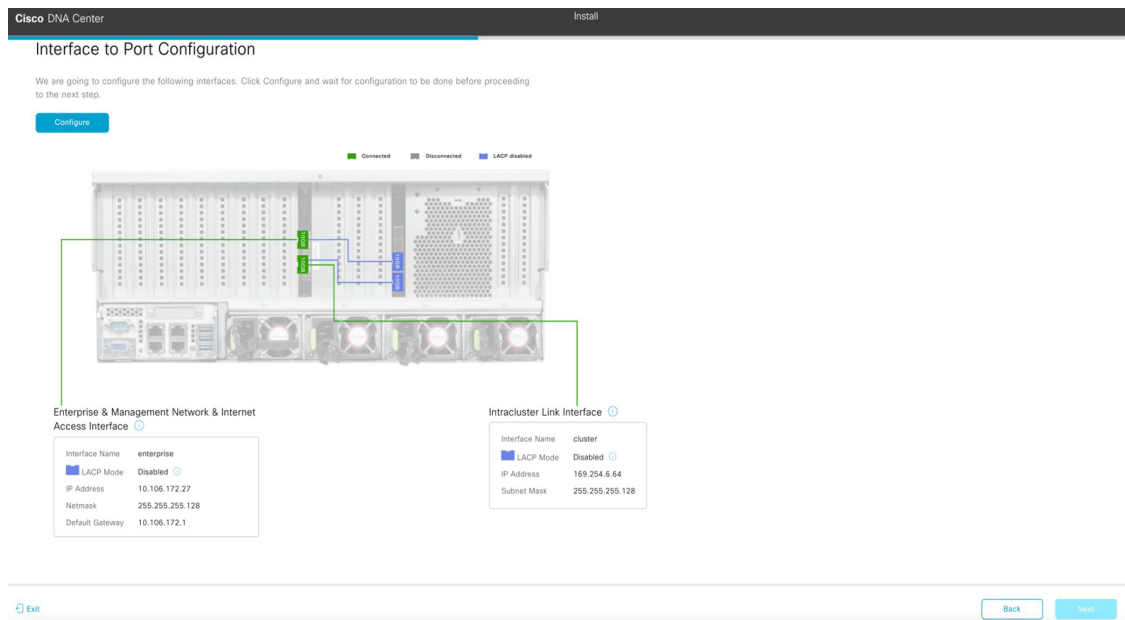


- c) [DNS] フィールドに、優先 DNS サーバーの IP アドレスを入力します。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要 最大 3 つの DNS サーバーを設定できます。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。

- d) [Next] をクリックします。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Interface to Port Configuration] 画面が開きます。



- e) 設定されているインターフェイス設定を確認し、[Configure] をクリックします。

- f) インターフェイスの初期設定が完了したら、[Next] をクリックしてウィザードの次の画面に進みます。

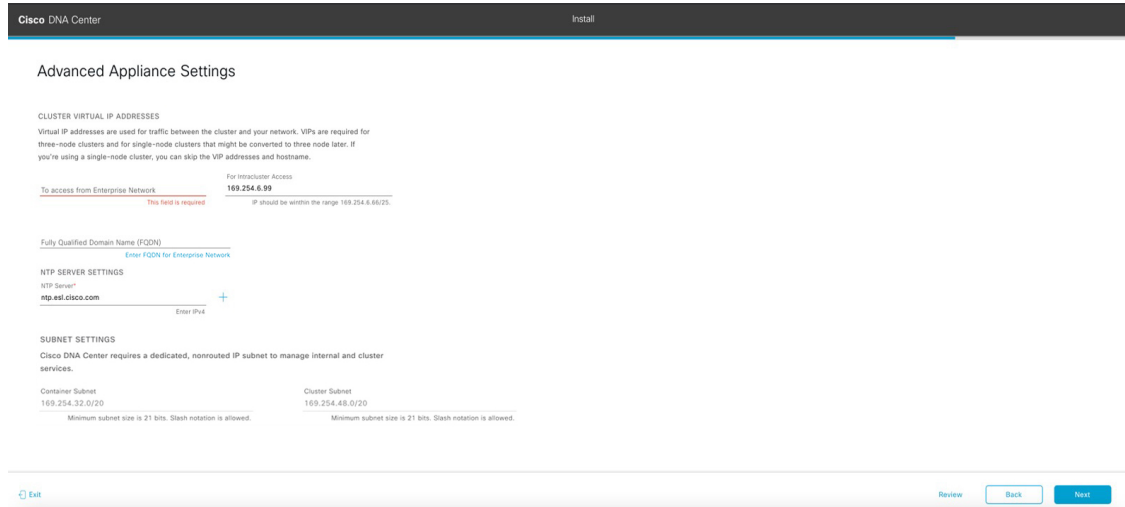
[Configure Proxy Server Information] 画面が開きます。

- g) 次のいずれかを実行し、[Next] をクリックします。
- ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックします。
 - ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、次の表に示す値を入力します。

表 47: プロキシサーバー設定のプライマリノードエントリ

[プロキシサーバ (Proxy Server)] フィールド	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。
[Port] フィールド	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。
[Username] フィールド	ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
Password フィールド	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効であれば、ウィザードの [Advanced Appliance Settings] 画面が開きます。



- h) クラスタの構成値を入力し、[Next] をクリックします。

表 48 : [Advanced Appliance Settings] のプライマリノードエントリ

クラスタ仮想 IP アドレス	
<p>[Enterprise Network] および [For Intracluster Access] フィールドからアクセスする場合</p>	<p>アプライアンスのクラスタとエンタープライズおよびクラスタ内インターフェイス間のトラフィックに使用される仮想 IP アドレスを入力します。このアドレスは、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に対して入力する必要があります。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。</p> <p>重要 仮想 IP アドレスを構成する場合は、構成されたネットワーク インターフェイスごとに 1 つ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。</p>

[Fully Qualified Domain Name (FQDN)] フィールド	<p>クラスタの完全修飾ドメイン名 (FQDN) を指定します。Cisco DNA Center は、このホスト名を使用して次の操作を実行します。</p> <ul style="list-style-type: none"> 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。
NTP サーバー設定	
[NTP Server] フィールド	<p>少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。</p> <p>実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。</p>
サブネット設定	
[Container Subnet] フィールド	<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 に設定されているため、別のサブネットは入力できません。</p>
[Cluster Subnet] フィールド	<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 に設定されているため、別のサブネットは入力できません。</p>

[CLI パスワードの入力] 画面が開きます。

インストール構成ウィザードを使用したアプライアンスの設定

Cisco DNA Center Install

Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster

Username*
maglev

Password*
..... [SHOW](#)

[View Password Criteria](#)

Retype to Confirm*
..... [SHOW](#)

[Review](#) [Back](#) [Next](#)

- i) maglev ユーザーのパスワードを入力して確認した後、[Next] をクリックします。

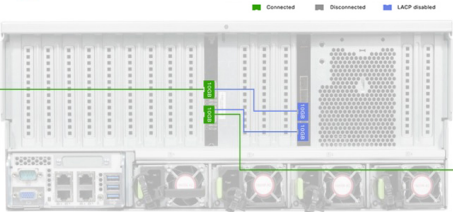
入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。

Cisco DNA Center Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

▼ Enterprise Port [Edit](#)



Enterprise & Management Network & Internet Access Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	10.106.172.27
Netmask	255.255.255.128
Default Gateway	10.106.172.1

Intracluster Link Interface

Interface Name	cluster
LACP Mode	Disabled
IP Address	169.254.6.64
Subnet Mask	255.255.255.128

[Exit](#) [Start Configuration](#)

- (注) アプライアンスの設定を JSON ファイルとしてダウンロードするには、こちらのリンクをクリックします。

- j) 画面の下部までスクロールし、ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な [Edit] リンクをクリックして、更新を行うウィザード画面を開きます。
- k) Cisco DNA Center アプライアンスの設定を完了するには、[Start Configuration] をクリックします。

プロセス中もウィザード画面が継続的に更新され、現在実行しているタスクとその進行状況、発生したエラーが示されます。この情報のローカルコピーをテキストファイルとして保存するには、[Download] アイコンをクリックします。

Cisco DNA Center

Install

Appliance Configuration In Progress

It should take about 30 minutes to configure the appliance. **Do not press your browser's back button or refresh this page.** The page will update after configuration completes.

30%
Initializing the cluster using kubeadm

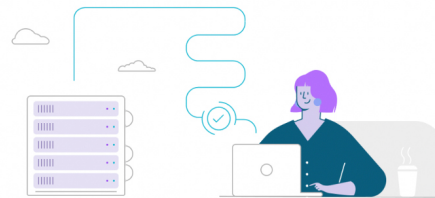
Started: 04/09/2020 12:15:36

Download

```

17:40:20 2021 GMT
2021-12-03T05:37:06.616Z14 | kubelet.conf Apr
13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-12-03T05:37:06.616Z15 | admin.conf Apr 13
12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-12-03T05:37:06.616Z16 | scheduler.conf Apr
13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-12-03T05:37:06.616Z17 | controller-
manager.conf Apr 13 12:12:14 2020 GMT Apr 13
17:40:22 2021 GMT
2021-12-03T05:37:06.616Z18 | -----
-----

```




ステップ 3 アプライアンスの設定が完了したら、[Cisco DNA Center - Admin Credential] 領域のコピーアイコンをクリックして、デフォルトの管理者スーパーユーザーパスワードをコピーします。

Cisco DNA Center

Install

Appliance Configuration Complete!

Important: Take note of the credentials displayed below. You can click the copy icon  if you want to save them locally. You will use these credentials to log in to Cisco DNA Center for the first time. After logging in, you will be prompted to change the password.

100% 

CISCO DNA CENTER - ADMIN CREDENTIAL 

Username admin
password maglev1@3

What's Next?

Open Cisco DNA Center



重要

インストール構成ウィザードを完了すると、Cisco DNA Center はこのパスワードを自動的に設定します。続行する前に、必ずコピーアイコンをクリックしてください。クリックしないと、Cisco DNA Center への最初のログインができません。

- (注) セキュリティ対策として、ログイン後にこのパスワードを変更するよう求められます。詳細については、[クイック スタート ワークフローの完了 \(260 ページ\)](#) を参照してください。

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展開する場合は、初回セットアップ（「[初期設定ワークフロー](#)」）を実行して続行します。

詳細インストール構成ウィザードを使用した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、詳細インストール構成ウィザードを使用して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。



重要

- 次の第 2 世代 Cisco DNA Center アプライアンスは、このウィザードを使用した設定をサポートしています。
 - 112 コアアプライアンス：シスコ製品番号 DN2-HW-APL-XL
 - 112 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-XL-U
- このウィザードは、新しい Cisco DNA Center アプライアンスの初期設定を完了するためだけにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、[Maglev 設定ウィザード](#)を使用する必要があります（[Maglev ウィザードを使用したアプライアンスの設定 \(93 ページ\)](#) を参照）。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、（ネットワークのデバイスを検出してテレメトリを有効にするために完了する）クイック スタート ワークフローが開始されません。
- 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。

すでにプライマリノードがある既存のクラスタのセカンダリノードとしてインストールされたアプライアンスを設定する場合には、代わりに[詳細インストール構成ウィザードを使用したセカンダリノードの設定 \(238 ページ\)](#) の手順を実行します。

始める前に

次のことを確認します。

- 「[アプライアンスのイメージの再作成 \(86 ページ\)](#)」の説明どおりに Cisco DNA Center ソフトウェアイメージがアプライアンスにインストールされたこと。



重要 Cisco DNA Center ソフトウェアイメージは 112 コア プロモーションアプライアンス (シスコ製品番号 DN2-HW-APL-XL-U) にあらかじめインストールされていないため、これはプロモーションアプライアンスを設定する場合にのみ当てはまります。

- [必要な IP アドレスおよびサブネット \(33 ページ\)](#) と [必須の設定情報](#) で必要な情報がすべて収集されたこと。
- 「[アプライアンスのインストールワークフロー](#)」の説明に従って、最初のアプライアンスがインストールされたこと。
- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)」の説明に従って、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。
- 「[事前設定タスクの実行](#)」の説明に従って、プライマリノードのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- Cisco IMC、Cisco DNA Center との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順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。ウィザードでは、ユーザの指定する DNS サーバを ping で確認します。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 詳細インストール構成ウィザードを起動します。

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

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



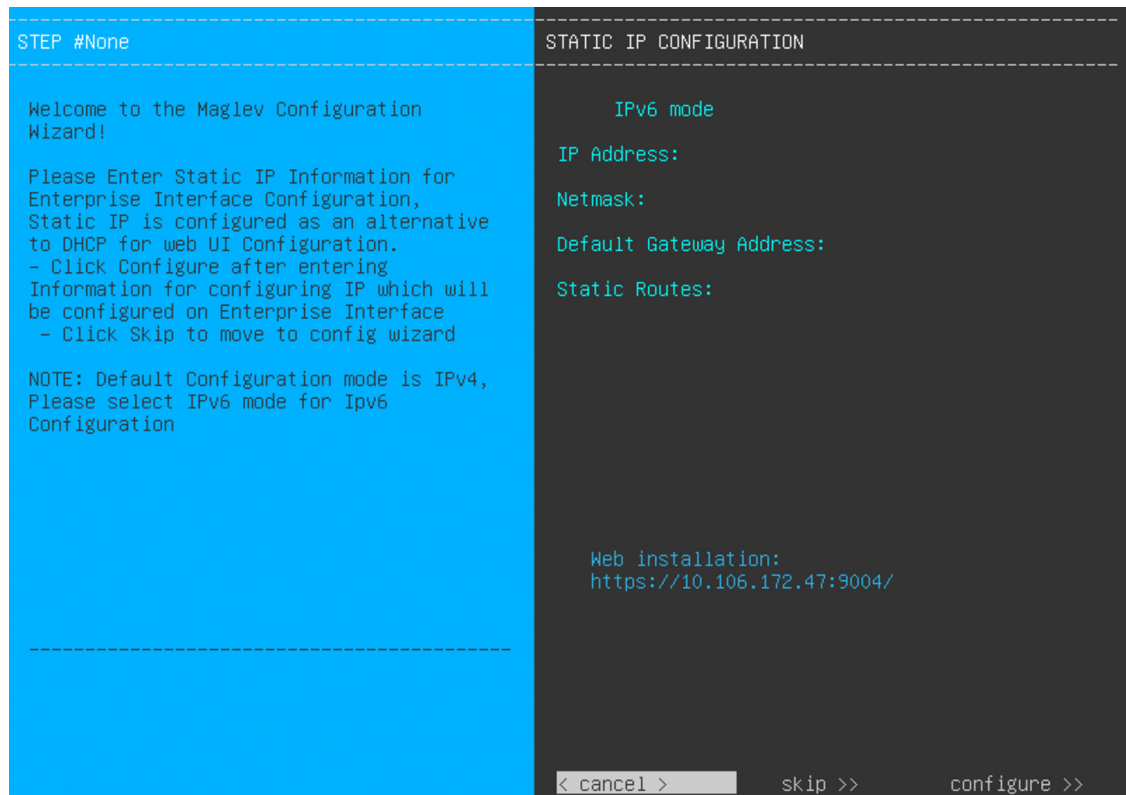
- b) 青いリンクメニューで [Launch KVM] を選択してから、[Java based KVM] と [HTML based KVM] のいずれかを選択します。[Java based KVM] を選択した場合、KVM コンソールを独自のウィンドウで表示するために、ブラウザまたはファイルマネージャから Java スタートアップファイルを起動する必要があります。[HTML based KVM] を選択すると、KVM コンソールが別個のブラウザウィンドウまたはタブで自動的に起動します。

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。

- c) 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] を選択します。その後、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 [Static IP Configuration] 画面が表示されます。



[Web インストール (Web Installation)] フィールドにリストされている URL に注意してください。

d) 次のいずれかを実行します。

- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てるようにするには、[Skip] をクリックします。
- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、[Configure] をクリックします。

(注) 指定する必要があるのは、アプライアンスのエンタープライズインターフェイスの IP アドレス、サブネットマスク、およびデフォルトゲートウェイのみです。

[IPv6 Mode] チェックボックス	IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。
[IP Address] フィールド	使用する静的 IP アドレスを入力します。
[ネットマスク (Netmask)] field	前のフィールドに指定した IP アドレスのネットマスクを入力します。 <ul style="list-style-type: none"> • IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。 • IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。

[Default Gateway Address] フィールド	トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
[Static Routes] フィールド	1つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク>/<ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。

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。

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >

```

- e) [Appliance Configuration] 画面を表示するには、[Static IP Configuration] 画面に表示された URL を開きます。

Cisco DNA Center

Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

<p>Start A Cisco DNA Center Cluster <input checked="" type="radio"/></p> <hr/> <p>This appliance will be the primary node of a cluster.</p>	<p>Join A Cisco DNA Center Cluster <input type="radio"/></p> <hr/> <p>This appliance will be added as a node to the primary node of a cluster.</p>
---	--



Next

- f) [Start a Cisco DNA Center Cluster] オプションボタンをクリックし、[Next] をクリックします。

Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.
Which workflow matches your needs?

Install


Configure a standalone node or **cluster's primary node**.

Use this quick, simplified wizard to set up the Enterprise, Management, and Internet interfaces on the same interface with default settings.

Advanced Install

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.



- g) [Advanced Install] オプションボタンをクリックし、[Start] をクリックします。

[Advanced Install Overview] スライダが開きます。[>] をクリックして、ウィザードで実行するタスクの概要を表示します。

Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.



- h) [Start Workflow] をクリックしてウィザードを起動します。

[Appliance Interface Overview] 画面が開き、設定可能な 4 つのアプライアンス インターフェイスの説明が表示されます。

Cisco DNA Center Advanced Install

Appliance Interface Overview

In order for Cisco DNA Center to operate properly, you need to configure four interfaces on your appliance:

1. **Enterprise Network Interface:** Connects your appliance to the Enterprise network.
2. **Intracluster Link Interface:** Connects your appliance to your cluster.
3. **Management Network Interface:** (Optional) Accesses the Cisco DNA Center GUI from your Management network.
4. **Internet Access Interface:** (Optional) Accesses the Internet.

In this workflow, the Enterprise Network Interface and the Intracluster Link Interface will each have their own dedicated port. You can choose to have either Management Network Interface and/or Internet Access Interface be on the same port as the Enterprise Network Interface or assign them to a separate designated port.

Exit Next

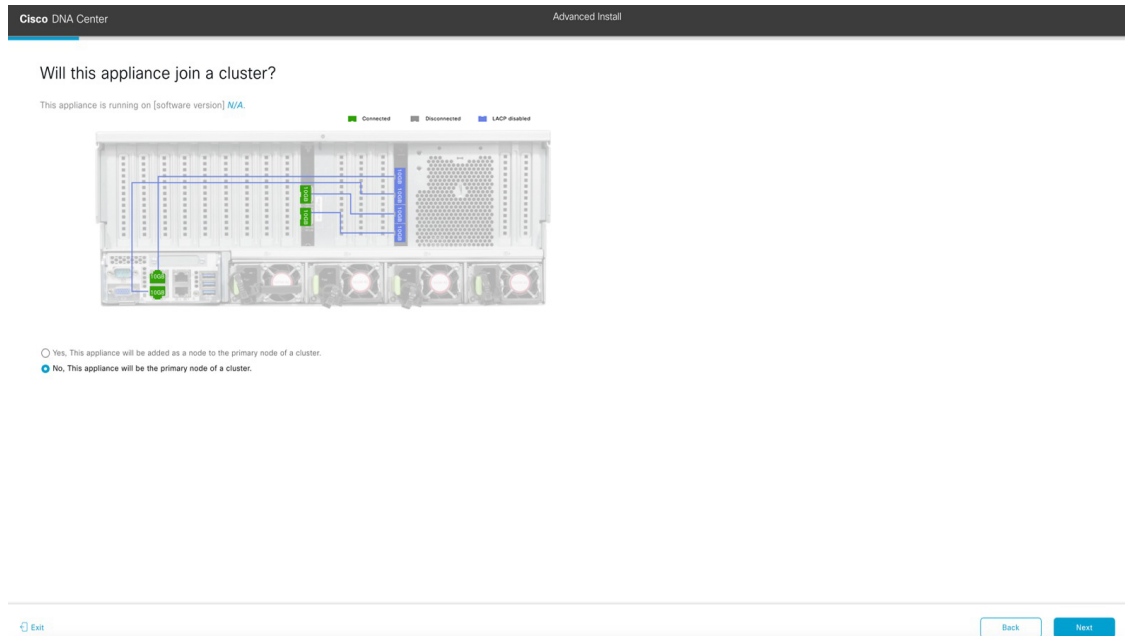
重要 Cisco DNA Center の機能に必要なため、少なくともエンタープライズポートとクラスタポートを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか 1 つまたは両方が表示されない場合、表示されないポートは機能しないか無効になっている可能性があります。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザードをすぐに終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に「[事前設定タスクの実行](#)」に記載されているすべての手順が完了していることを確認してください。

ステップ 2 詳細インストールウィザードを完了します。

- a) [Next] をクリックします。

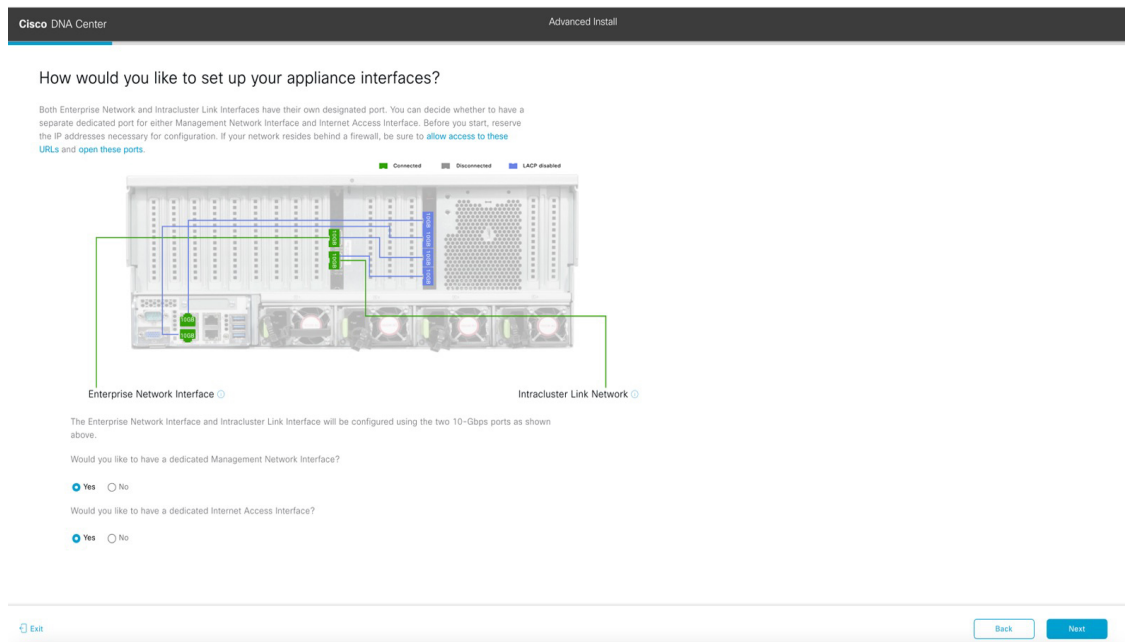
[Will this appliance join a cluster?] 画面が開きます。

詳細インストール構成ウィザードを使用したプライマリノードの設定



- b) [No] オプションボタンをクリックし（クラスタのプライマリノードを設定する場合）、[Next] をクリックします。

[How would you like to set up your appliance interfaces?] 画面が開きます。



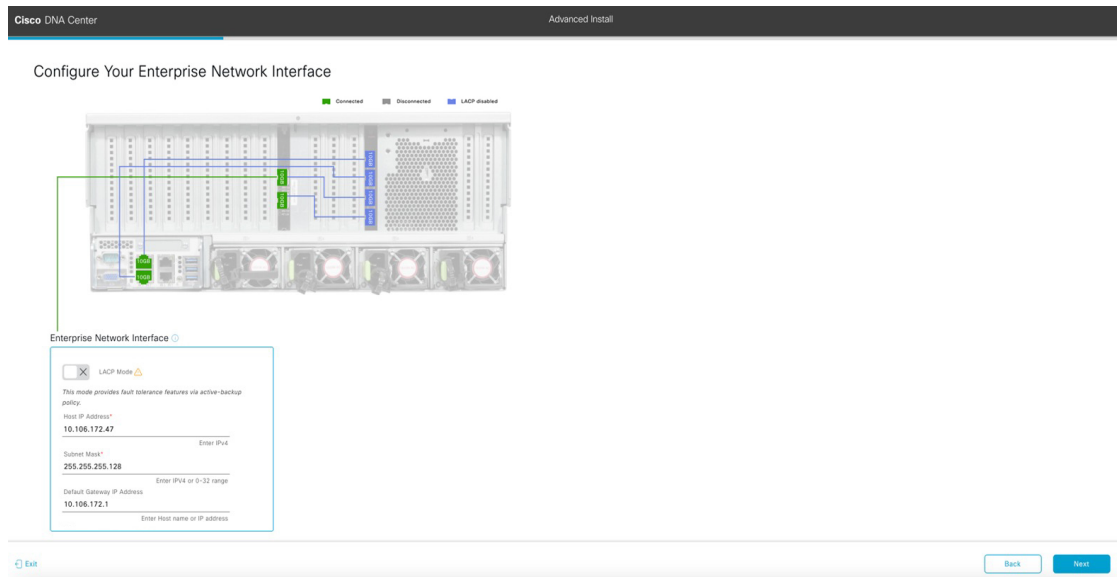
ネットワークがファイアウォールの背後にある場合は、次の手順を実行します。

- [allow access to these URLs] リンクをクリックすると、Cisco DNA Center がアクセスできる必要がある URL を一覧表示するポップアップウィンドウが表示されます。

- [open these ports] リンクをクリックすると、Cisco DNA Center が使用できる必要があるネットワークサービスポートを一覧表示するポップアップウィンドウが表示されます。

- c) 専用の管理およびインターネット アクセス インターフェイスを設定するかどうかを指定し、[Next] をクリックします。

[Configure Your Enterprise Network Interface] 画面が開きます。



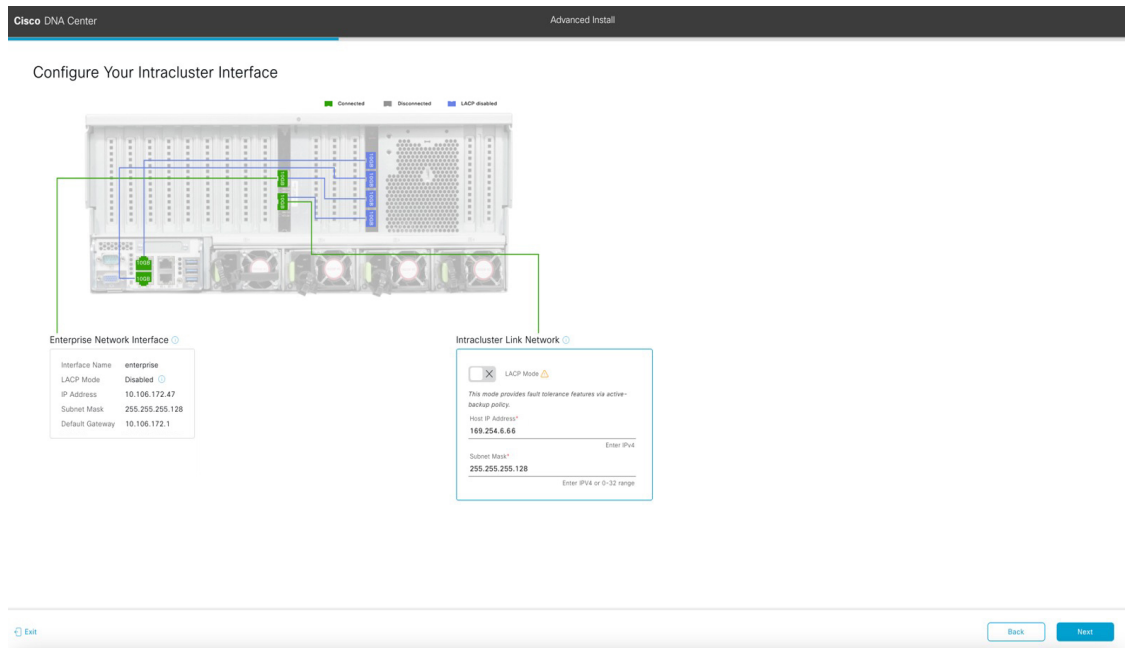
- d) エンタープライズ インターフェイスの構成値を入力し、[Next] をクリックします。

「[インターフェースケーブル接続](#)」で説明したように、このインターフェイスは、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インターフェイスです。入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

表 49: エンタープライズ インターフェイスのプライマリノードエントリ

<p>[LACP Mode] スライダ</p>	<p>エンタープライズ インターフェイスに対して、次のネットワーク インターフェイスコントローラ (NIC) ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード：このモードでは、2つのイーサネット インターフェイスを1つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード：このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネット インターフェイスが1つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
<p>[Host IP Address] フィールド</p>	<p>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。</p>
<p>[Subnet Mask] フィールド</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 (Default Gateway IP Address)] フィールド</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>(注) このインターフェイスは、DHCP サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. このフィールドに現在一覧表示されている IP アドレスを削除し、[Exit] をクリックします。 この操作でウィザードの最初の画面に戻ります。 2. エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ IP アドレスを入力します。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Intracluster Interface] 画面が開きます。



- e) クラスタ内インターフェイスの構成値を入力し、[Next] をクリックします。

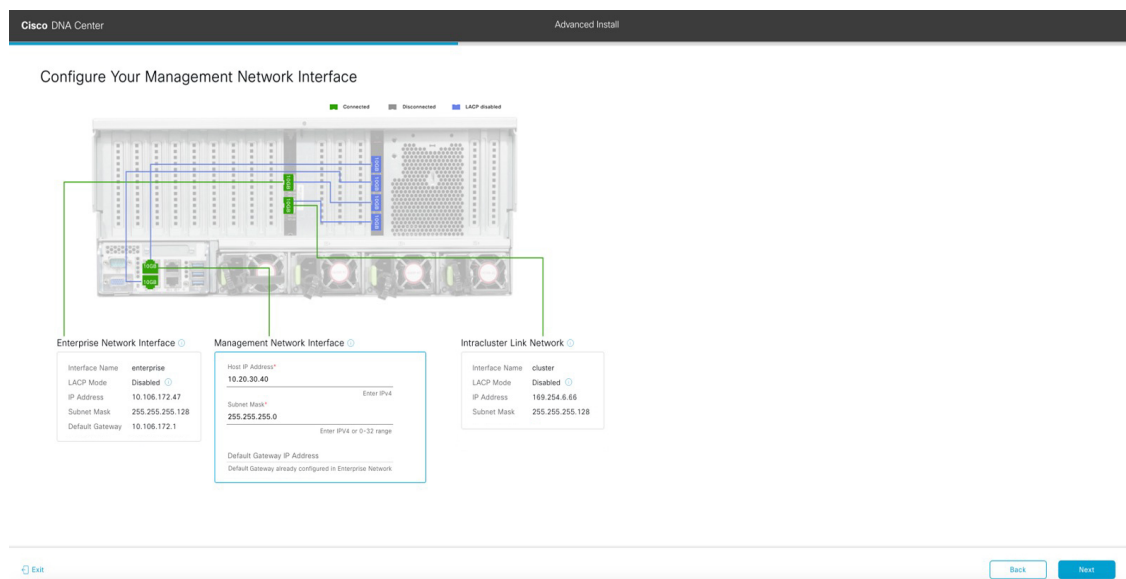
「[インターフェイスケーブル接続](#)」で説明したように、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

- (注)
- 同じポートでエンタープライズインターフェイスとインターネットアクセスインターフェイスを設定する場合は、この手順を実行してから、ステップ 2f (管理インターフェイスの設定方法が記載) に進みます。
 - エンタープライズインターフェイスと管理インターフェイスを同じポートに設定する場合は、この手順を実行してから、ステップ 2g (インターネットアクセスインターフェイスの設定方法が記載) に進みます。
 - 同じポートでエンタープライズ、管理、およびインターネットアクセスインターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 50: クラスタ内インターフェイスのプライマリノードエントリ

<p>[LACP Mode] スライダ</p>	<p>クラスタ内インターフェイスに対して、次の NIC ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード：このモードでは、2つのイーサネット インターフェイスを1つの論理チャンネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード：このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネット インターフェイスが1つの論理チャンネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
<p>[Host IP Address] フィールド</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>[Subnet Mask] フィールド</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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Management Network Interface] 画面が開きます。



- f) (任意) 管理ポートの構成値を入力し、[Next] をクリックします。

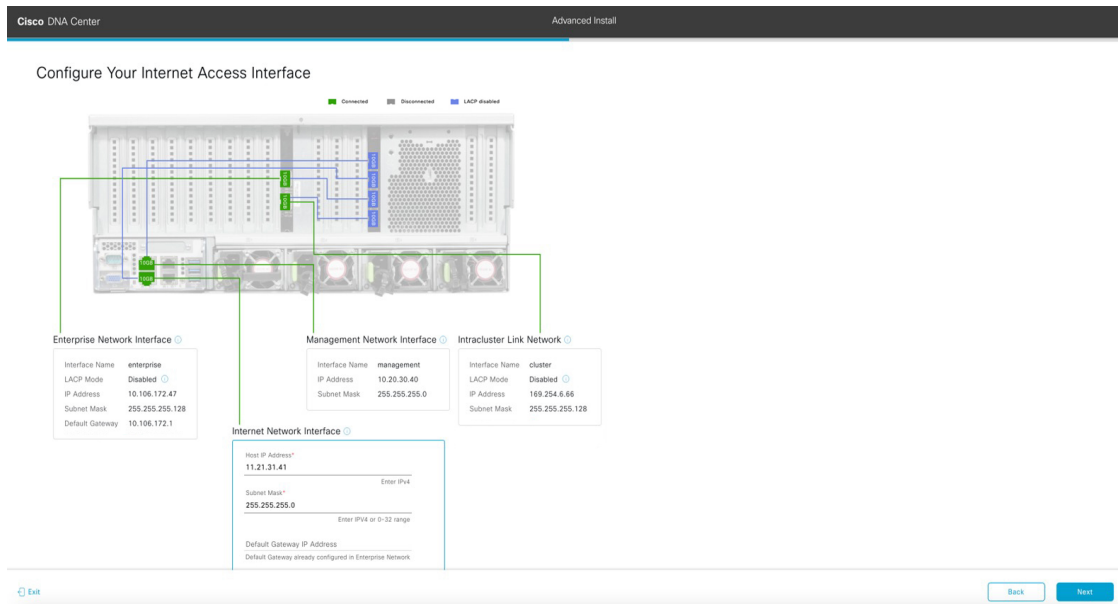
「[インターフェースケーブル接続](#)」で説明したように、このポートは管理ネットワークから Cisco DNA Center GUI にアクセスするために使用されます。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。（入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください）

(注) 同じポートでエンタープライズインターフェイスとインターネットアクセスインターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 51: 管理ポートのプライマリノードエントリ

[Host IP Address] フィールド	管理ポートの IP アドレスを入力します。
[Subnet Mask] フィールド	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。
[デフォルトゲートウェイ IP アドレス (Default Gateway IP Address)] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Internet Access Interface] 画面が開きます。



g) (任意) インターネットアクセスインターフェイスの構成値を入力し、[Next] をクリックします。

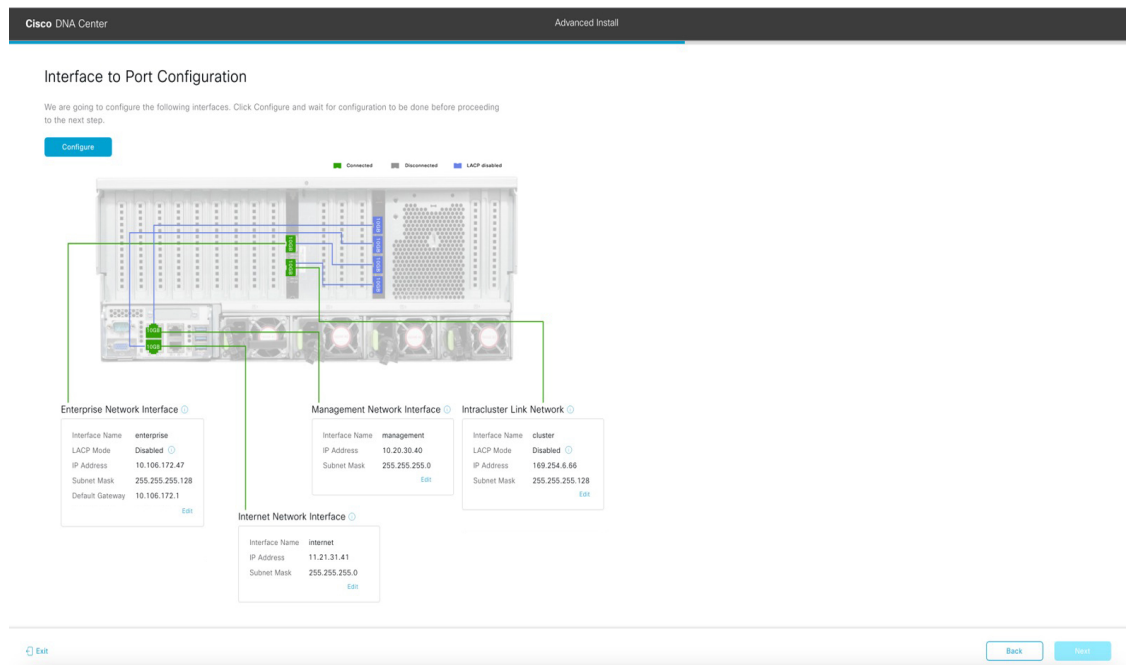
「[インターフェースケーブル接続](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場

合に使用されるオプションのポートです。専用インターネットアクセスインターフェイスを設定する場合は、次の表に示す情報を入力します。（入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット（33 ページ）](#)」と「[必須の設定情報](#)」を参照してください）

表 52: インターネットアクセスポートのプライマリノードエントリ

[Host IP Address] フィールド	インターネットアクセスポートの IP アドレスを入力します。
[Subnet Mask] フィールド	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、前のフィールドに 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 (Default Gateway IP Address)] フィールド	<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>

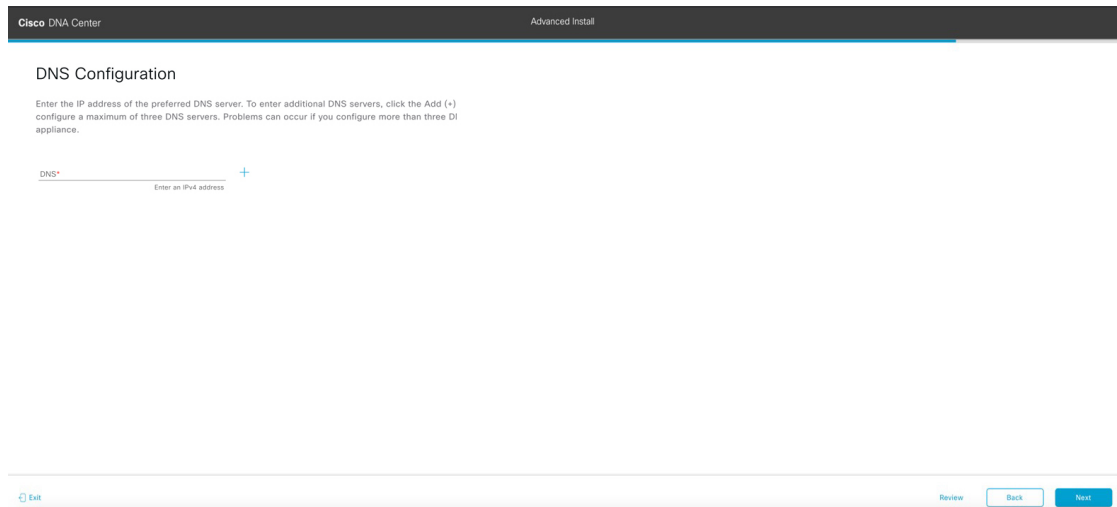
入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Interface to Port Configuration] 画面が開きます。



- h) プライマリノードのインターフェイスに入力した設定を確認します。変更が必要な場合は、該当するインターフェイスの [Edit] リンクをクリックします。
- i) インターフェイスの設定に問題がなければ、[Configure] をクリックします。

- j) インターフェイスの初期設定が完了したら、[Next] をクリックしてウィザードの次の画面に進みます。

[DNS Configuration] 画面が開きます。



- k) 優先 DNS サーバーの IP アドレスを入力して、[Next] をクリックします。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバーを設定します。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。
- NTP の場合、Cisco DNA Center と NTP サーバー間でポート 123 (UDP) が開いていることを確認します。

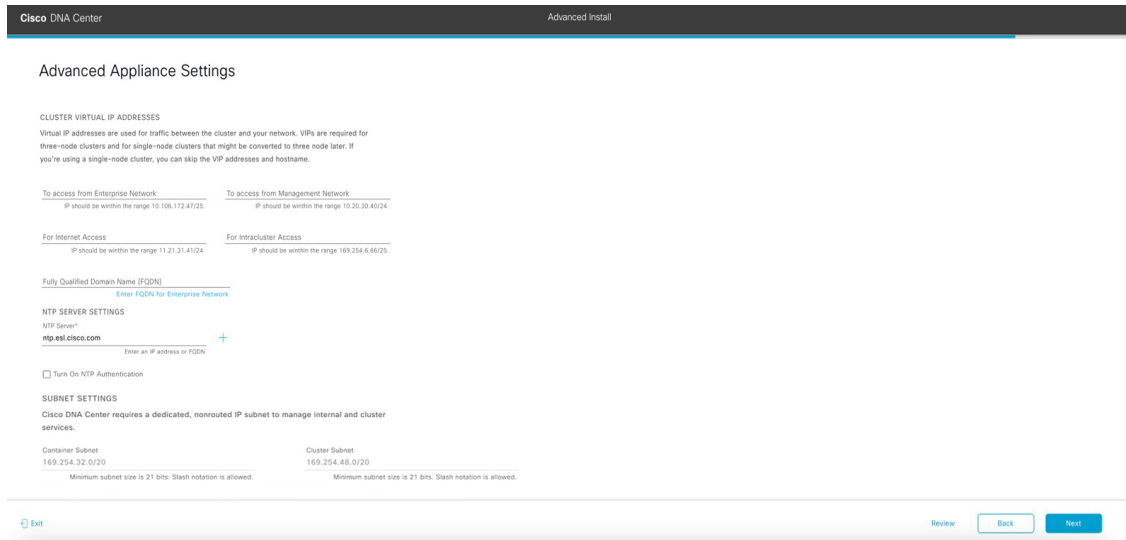
[Configure Proxy Server Information] 画面が開きます。

- 1) 次のいずれかを実行し、[Next] をクリックします。
- ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックします。
 - ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、次の表に示す値を入力します。

表 53: プロキシサーバー設定のプライマリノードエントリ

[プロキシサーバ (Proxy Server)] フィールド	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。
[Port] フィールド	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。
[Username] フィールド	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。
Password フィールド	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。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Advanced Appliance Settings] 画面が開きます。



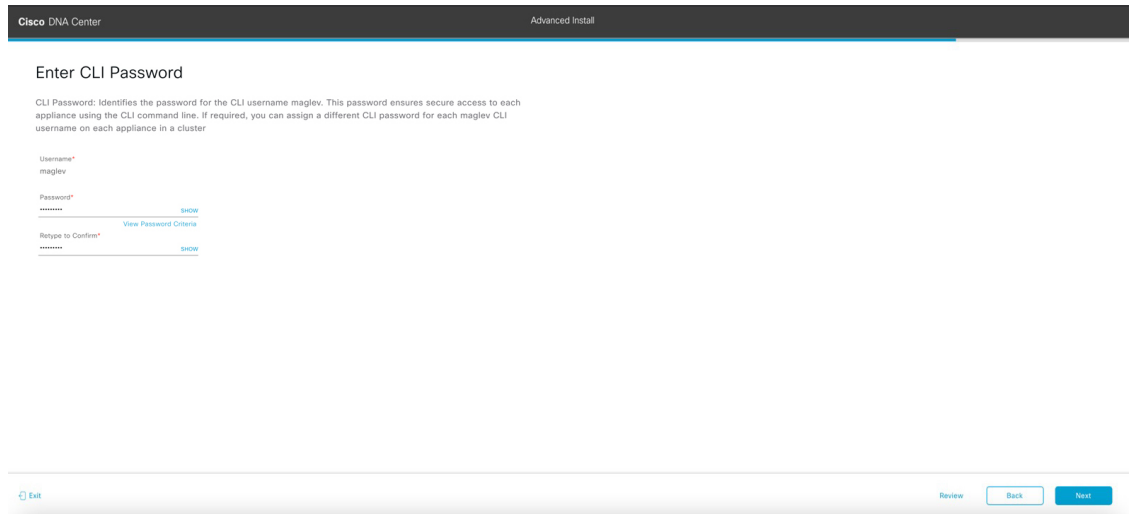
- m) クラスタの構成値を入力し、[Next] をクリックします。

表 54: [Advanced Appliance Settings] のプライマリノードエントリ

クラスタ仮想 IP アドレス	
<p>[To access from Enterprise Network]、[To access from Management Network]、[For Internet Access]、および [For Intracluster Access] フィールド</p> <p>(注) エンタープライズインターフェイスと同じポートで管理インターフェイスまたはインターネットアクセスインターフェイスを設定した場合、対応するフィールドはこのセクションに表示されません。</p>	<p>プライマリノードに設定したクラスタとインターフェイス間のトラフィックに使用される仮想 IP アドレスを入力します。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。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。</p> <p>重要 仮想 IP アドレスを構成する場合は、構成されたネットワーク インターフェイスごとに 1 つ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。</p>

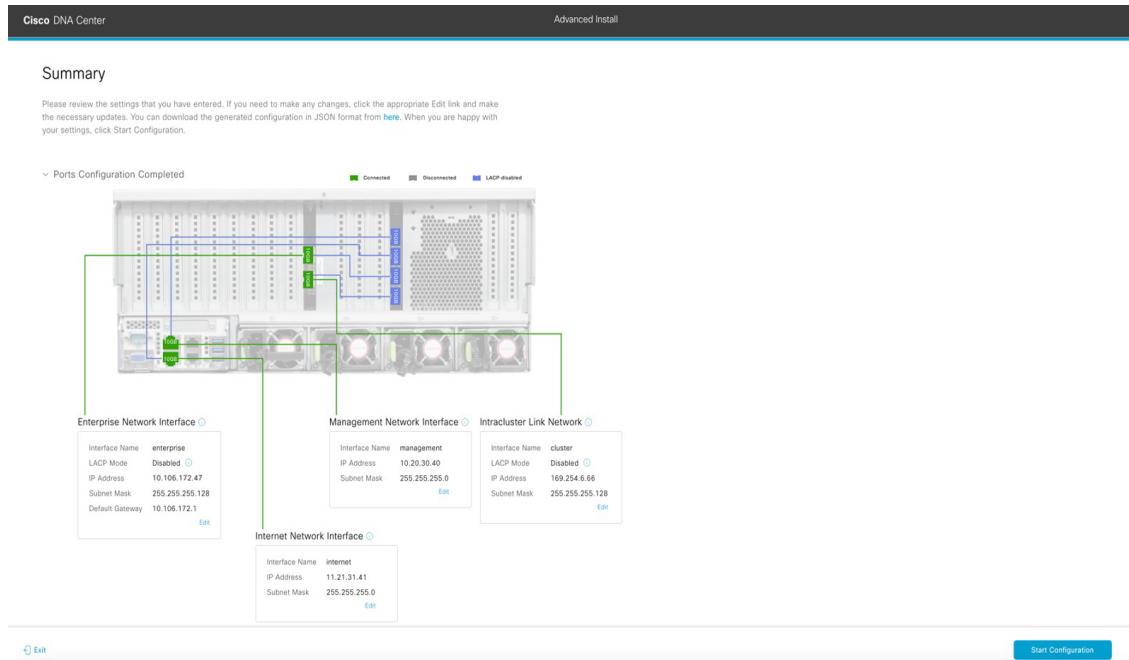
<p>[Fully Qualified Domain Name (FQDN)] フィールド</p>	<p>クラスタの完全修飾ドメイン名 (FQDN) を指定します。Cisco DNA Center は、このホスト名を使用して次の操作を実行します。</p> <ul style="list-style-type: none"> このホスト名を使用して、クラスタの Web インターフェイスと、Cisco DNA Center が管理するエンタープライズ ネットワーク内のデバイスによって使用される Representational State Transfer (REST) API にアクセスします。 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。
<p>NTP サーバー設定</p>	
<p>[NTP Server] フィールド</p>	<p>少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。</p> <p>実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。</p>
<p>[Turn On NTP Authentication] チェックボックス</p>	<p>Cisco DNA Center と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> NTP サーバーのキー ID。有効な値の範囲は 1 ~ 4294967295 (2³²-1) です。 <p>この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。</p> <ul style="list-style-type: none"> NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。 <p>(注) 前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。</p>
<p>サブネット設定</p>	
<p>[Container Subnet] フィールド</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。</p>
<p>[Cluster Subnet] フィールド</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。</p>

[Enter CLI Password] 画面が開きます。



- n) maglev ユーザーのパスワードを入力して確認した後、[Next] をクリックします。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。



(注) アプライアンスの設定を JSON ファイルとしてダウンロードするには、こちらのリンクをクリックします。

- o) ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な [Edit] リンクをクリックして、更新を行うウィザード画面を開きます。
- p) Cisco DNA Center アプライアンスの設定を完了するには、[Start Configuration] をクリックします。

詳細インストール構成ウィザードを使用したセカンダリノードの設定

プロセス中もウィザード画面が継続的に更新され、現在実行しているタスクとその進行状況、発生したエラーが示されます。この情報のローカルコピーをテキストファイルとして保存するには、ダウンロードアイコンをクリックします。

Cisco DNA Center Configuration

Appliance Configuration In Progress

It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.

30%

Initializing the cluster using kubernetes

Started: 04/09/2020 12:15:36

2021-05-05T16:56:59.32524 | -----

2021-05-05T16:56:59.32525 | credentialmanager.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.32526 | kong.pem Apr 13 16:49:51 2020 GMT Apr 13 16:49:51 2021 GMT

2021-05-05T16:56:59.32527 | kube-admin.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT

2021-05-05T16:56:59.32528 | kube-worker-1.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.32529 | masjiev-registry.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT

2021-05-05T16:56:59.325210 | apiserver.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325211 | apiserver-kubelet-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325212 | front-proxy-ca.crt Apr 13 17:40:20 2020 GMT Apr 11 17:40:20 2030 GMT

2021-05-05T16:56:59.325213 | front-proxy-client.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT

2021-05-05T16:56:59.325214 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT

2021-05-05T16:56:59.325215 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT

2021-05-05T16:56:59.325216 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT

2021-05-05T16:56:59.325217 | controller-manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT

2021-05-05T16:56:59.325218 | -----

次のタスク

タスクが完了した後：

- このアプライアンスをスタンドアロンモードのみで展開する場合には、初回セットアップ（「[初期設定ワークフロー](#)」）を実行して続行します。
- 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番目のインストール済みアプライアンスを設定します（[詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)（238 ページ））。

詳細インストール構成ウィザードを使用したセカンダリノードの設定

詳細インストール構成ウィザードを使用して、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。
- 次の第 2 世代 Cisco DNA Center アプライアンスは、このウィザードを使用した設定をサポートしています。
 - 112 コアアプライアンス：シスコ製品番号 DN2-HW-APL-XL
 - 112 コア プロモーション アプライアンス：シスコ製品番号 DN2-HW-APL-XL-U
- このウィザードは、新しい Cisco DNA Center アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、[Maglev 設定ウィザード](#)を使用する必要があります ([Maglev ウィザードを使用したアプライアンスの設定 \(93 ページ\)](#) を参照)。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Cisco DNA Center に初めてログインした後に、(ネットワークのデバイスを検出してテレメトリを有効にするために完了する) クイック スタート ワークフローが開始されません。
- 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。

新しいセカンダリ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。クラスタにセカンダリノードを結合する際、次の点に注意してください。

- クラスタに新しいノードを追加する前に、インストールされているすべてのパッケージがプライマリノードに展開されていることを確認してください。展開されているかどうかを確認するには、セキュアシェルを使用して、プライマリノードの Cisco DNA Center 管理ポートに Linux ユーザ (maglev) としてログインしてから、`maglev package status` コマンドを実行します。インストールされているすべてのパッケージは、コマンド出力で「展開済み (DEPLOYED)」と表示されます。

詳細インストール構成ウィザードを使用したセカンダリノードの設定

```

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]
NAME                                DISPLAY_NAME                                DEPLOYED    AVAILABLE    STATUS    PROGRESS
-----
access-control-application          Access Control Application                  -            2.1.369.60050    NOT_DEPLOYED
ai-network-analytics               AI Network Analytics                       -            2.6.10.494      NOT_DEPLOYED
app-hosting                        Application Hosting                         -            1.6.6.2201241723 NOT_DEPLOYED
application-policy                 Application Policy                          -            2.1.369.170033  NOT_DEPLOYED
application-registry               Application Registry                        -            2.1.369.170033  NOT_DEPLOYED
application-visibility-service      Application Visibility Service              -            2.1.369.170033  NOT_DEPLOYED
assurance                          Assurance - Base                           2.2.2.485     -                DEPLOYED
automation-core                   NCP - Services                            2.1.368.60015 2.1.369.60050  DEPLOYED
base-provision-core                Automation - Base                          2.1.368.60015 2.1.369.60050  DEPLOYED
cloud-connectivity-contextual      Cloud Connectivity - Contextual Content    1.3.1.364     -                DEPLOYED
cloud-connectivity-data-hub        Cloud Connectivity - Data Hub              1.6.0.380     -                DEPLOYED
cloud-connectivity-tethering        Cloud Connectivity - Tethering             2.12.1.2     -                DEPLOYED
cloud-provision-core               Cloud Device Provisioning Application      -            2.1.369.60050  NOT_DEPLOYED
command-runner                     Command Runner                             2.1.368.60015 2.1.369.60050  DEPLOYED
device-onboarding                  Device Onboarding                          2.1.368.60015 2.1.369.60050  DEPLOYED
disaster-recovery                  Disaster Recovery                          -            2.1.367.360196  NOT_DEPLOYED
dna-core-apps                      Network Experience Platform - Core         2.1.368.60015 2.1.369.60050  DEPLOYED
dnac-platform                     Cisco DNA Center Platform                  1.5.1.180     1.5.1.182      DEPLOYED
dnac-search                        Cisco DNA Center Global Search            1.5.0.466     -                DEPLOYED
endpoint-analytics                 AI Endpoint Analytics                     -            1.4.375         NOT_DEPLOYED
group-based-policy-analytics        Group-Based Policy Analytics              -            2.2.1.401      NOT_DEPLOYED
icap-automation                    Automation - Intelligent Capture          -            2.1.369.60050  NOT_DEPLOYED
image-management                   Image Management                          2.1.368.60015 2.1.369.60050  DEPLOYED
machine-reasoning                  Machine Reasoning                          2.1.368.210017 2.1.369.210024 DEPLOYED
ncp-system                         NCP - Base                                2.1.368.60015 2.1.369.60050  DEPLOYED
ndp-base-analytics                 Network Data Platform - Base Analytics     1.6.1028     1.6.1031      DEPLOYED
ndp-platform                       Network Data Platform - Core              1.6.596      -                DEPLOYED
ndp-ui                             Network Data Platform - Manager           1.6.543      -                DEPLOYED
network-visibility                 Network Controller Platform                2.1.368.60015 2.1.369.60050  DEPLOYED
path-trace                         Path Trace                                 2.1.368.60015 2.1.369.60050  DEPLOYED
platform-ui                        Cisco DNA Center UI                       1.6.2.446     1.6.2.448      DEPLOYED
rbac-extensions                    RBAC Extensions                           2.1.368.1910001 2.1.369.1910003 DEPLOYED
rogue-management                   Rogue and aWIPS                            -            2.2.0.51       NOT_DEPLOYED
sd-access                          SD Access                                  -            2.1.369.60050  NOT_DEPLOYED
sensor-assurance                   Assurance - Sensor                         -            2.2.2.484     NOT_DEPLOYED
sensor-automation                  Automation - Sensor                        -            2.1.369.60050  NOT_DEPLOYED
ssa                                Stealthwatch Security Analytics            2.1.368.1091226 2.1.369.1091317 DEPLOYED
system                              System                                      1.6.594      -                DEPLOYED
system-commons                     System Commons                             2.1.368.60015 2.1.369.60050  DEPLOYED
umbrella                            Cisco Umbrella                             -            2.1.368.592066 NOT_DEPLOYED
wide-area-bonjour                  Wide Area Bonjour                         -            2.4.368.75006  NOT_DEPLOYED

[Wed Nov 30 15:45:08 UTC] maglev@192.0.2.1 (maglev-master-192.0.2.1) ~

```

- 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う予期しない動作が発生します。
- 各セカンダリノードのクラスタ接続プロセス中に、一部のサービスのダウンタイムが発生することが予想されます。サービスはすべてのノードに再配布される必要があり、そのプロセスの間、クラスタはダウンします。

始める前に

次のことを確認します。

- 「[アプライアンスのイメージの再作成 \(86 ページ\)](#)」の説明どおりに Cisco DNA Center ソフトウェアイメージがアプライアンスにインストールされたこと。



重要 Cisco DNA Center ソフトウェアイメージは 112 コア プロモーションアプライアンス (シスコ製品番号 DN2-HW-APL-XL-U) にあらかじめインストールされていないため、これはプロモーションアプライアンスを設定する場合にのみ当てはまります。

- 「[詳細インストール構成ウィザードを使用したプライマリノードの設定 \(218 ページ\)](#)」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 \(33 ページ\)](#)」と「[必須の設定情報](#)」で必要な情報がすべて収集されたこと。
- 「[アプライアンスのインストールワークフロー](#)」の説明に従って、2 番目と 3 番目のアプライアンスがインストールされたこと。

- 以下を完了していること。
 1. 最初のアプライアンスで **maglev package status** コマンドを実行したこと。

この情報には Cisco DNA Center ホームページからもアクセスできます。[Help] アイコン (🔊) をクリックし、[About] > [Show Packages] の順に選択してください。
 2. Cisco TAC に連絡し、このコマンドの出力を提供して 2 番目と 3 番目のアプライアンスにインストールする必要がある ISO をポイントするよう依頼したこと。
- 「Cisco Integrated Management Controller に対するブラウザアクセスの有効化」の説明に従って、両方のセカンダリノードで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「事前設定タスクの実行」の説明に従って、セカンダリノードのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- 互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順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。ウィザードでは、ユーザの指定する DNS サーバを ping で確認します。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 詳細インストール構成ウィザードを起動します。

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

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



- b) 青いリンクメニューで [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。

c) 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] を選択します。その後、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 [Static IP Configuration] 画面が表示されます。

```

STEP #None
-----
Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration,
Static IP is configured as an alternative to DHCP for web UI Configuration.
- Click Configure after entering Information for configuring IP which will
be configured on Enterprise Interface
- Click Skip to move to config wizard

NOTE: Default Configuration mode is IPv4,
Please select IPv6 mode for Ipv6 Configuration

-----
STATIC IP CONFIGURATION
-----

IPv6 mode

IP Address:

Netmask:

Default Gateway Address:

Static Routes:

Web installation:
https://10.106.172.47:9004/

-----
< cancel >      skip >>      configure >>

```

[Web インストール (Web Installation)] フィールドにリストされている URL に注意してください。

d) 次のいずれかを実行します。

- DHCP サーバーが IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てるようにするには、[Skip] をクリックします。

- 独自の IP アドレス、サブネットマスク、デフォルトゲートウェイをアプライアンスのエンタープライズインターフェイスに割り当てる場合は、次の表に記載されている情報を入力し、[Configure] をクリックします。

[IPv6 Mode] チェックボックス	IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。
[IP Address] フィールド	使用する静的 IP アドレスを入力します。
[ネットマスク (Netmask)] field	前のフィールドに指定した IP アドレスのネットマスクを入力します。 <ul style="list-style-type: none"> • IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。 • IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。
[Default Gateway Address] フィールド	トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
[Static Routes] フィールド	1つ以上のスタティックルートをスペースで区切り、<ネットワーク><ネットマスク><ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。

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。

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one of the options below to specify how you
would like to configure this host:

Start a Cisco DNA Center Cluster
Join a Cisco DNA Center Cluster

< exit >
    
```

- e) [Appliance Configuration] 画面を表示するには、[Static IP Configuration] 画面に表示された URL を開きます。


Cisco DNA Center Appliance Configuration

Welcome to Cisco DNA Center

Are you starting a new Cisco DNA Center Cluster or joining an existing one?

Start A Cisco DNA Center Cluster
This appliance will be the primary node of a cluster.

Join A Cisco DNA Center Cluster
This appliance will be added as a node to the primary node of a cluster.



Next

- f) [Join a Cisco DNA Center Cluster] オプションボタンをクリックし、[Next] をクリックします。

Welcome to Cisco DNA Center

Before you can use Cisco DNA Center, first complete the appropriate appliance configuration workflow.
Which workflow matches your needs?

Advanced Install

Configure a standalone node or **any node in a cluster**.

Use this wizard to access all of the available appliance configuration options.

[Back](#)[Start](#)

- g) [Advanced Install] オプションボタンをクリックし、[Start] をクリックします。

[Advanced Install Overview] スライドが開きます。[>] をクリックして、ウィザードで実行するタスクの概要を表示します。

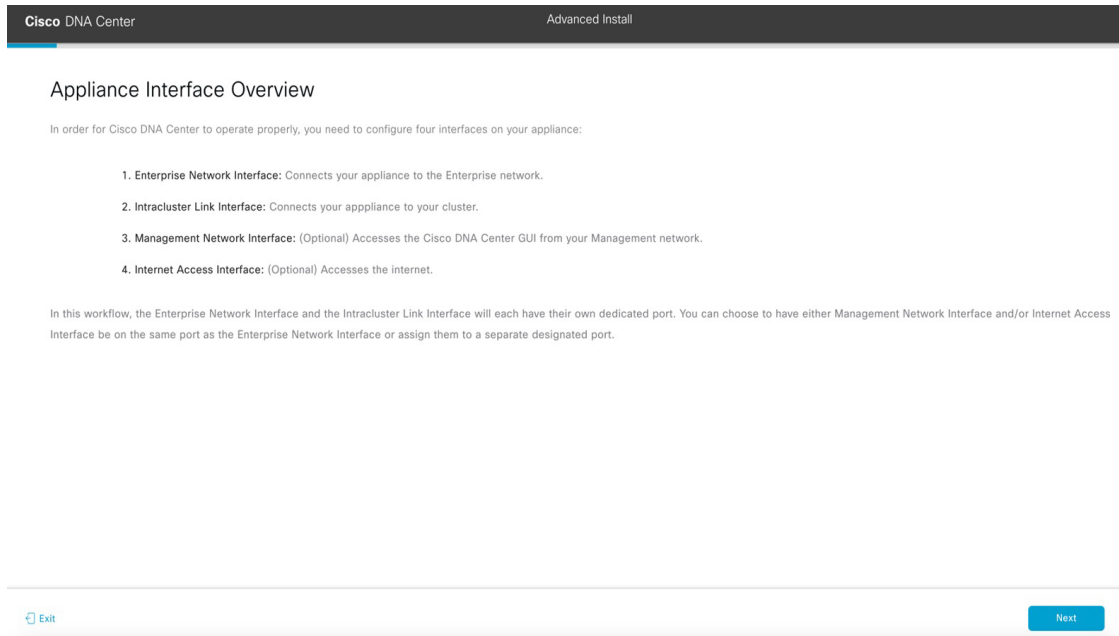
Advanced Install Overview

Prepare your appliance for use with Cisco DNA Center by configuring its interfaces and entering cluster and other required information.

[Start Workflow](#)

- h) [Start Workflow] をクリックしてウィザードを起動します。

[Appliance Interface Overview] 画面が開き、設定可能な 4 つのアプライアンス インターフェイスの説明が表示されます。

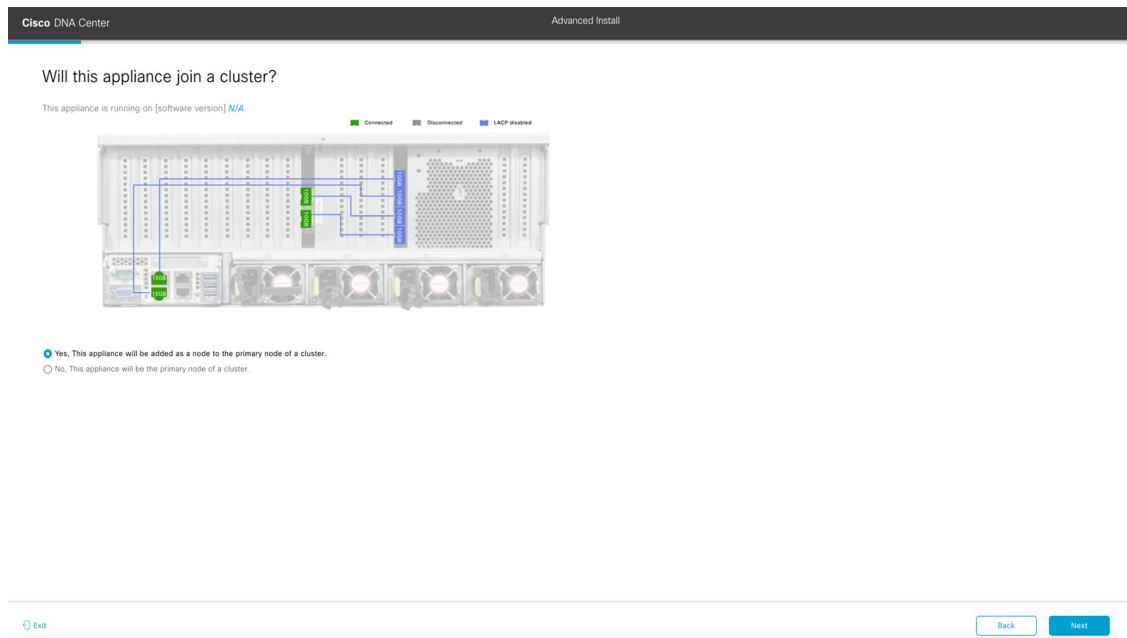


重要 Cisco DNA Center の機能に必要なため、少なくともアプライアンスのエンタープライズポートおよびクラスタポートにインターフェイスを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか1つまたは両方が表示されない場合、表示されないポートは機能しないか無効になっている可能性があります。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザードをすぐに終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に「[事前設定タスクの実行](#)」に記載されているすべての手順が完了していることを確認してください。

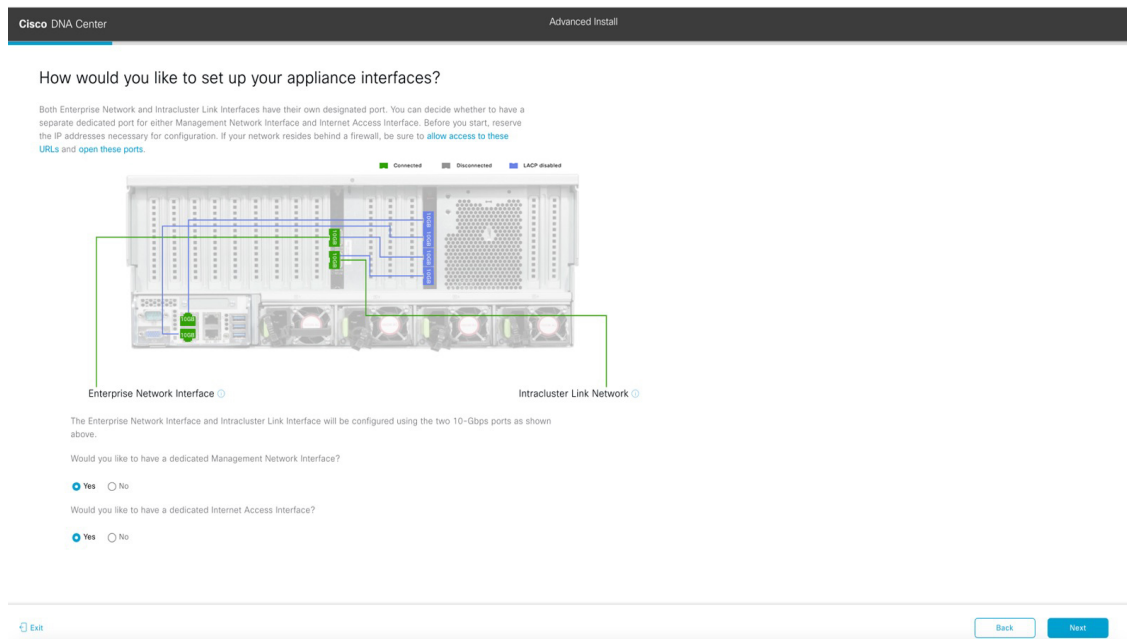
ステップ 2 詳細インストール構成ウィザードを完了します。

- a) [Next] をクリックします。

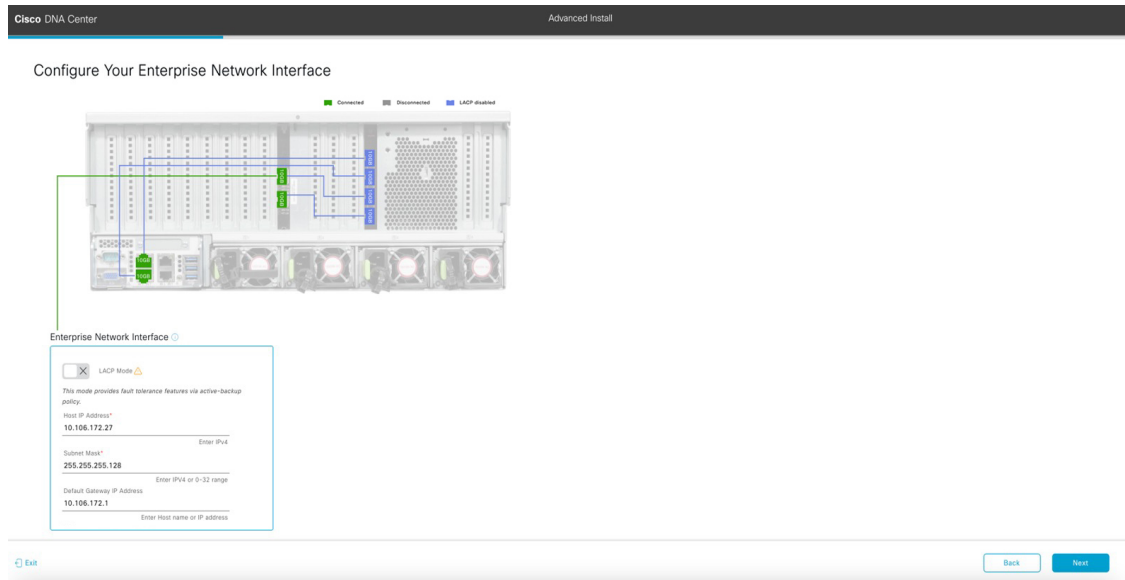
[Will this appliance join a cluster?] 画面が開きます。



- b) [Yes] オプションボタンをクリックし、[Next] をクリックします。
[How would you like to set up your appliance interfaces?] 画面が開きます。



- c) 専用の管理およびインターネット アクセス インターフェイスを設定するかどうかを指定し、[Next] をクリックします。
[Configure Your Enterprise Network Interface] 画面が開きます。



d) エンタープライズ インターフェイスの構成値を入力し、[Next] をクリックします。

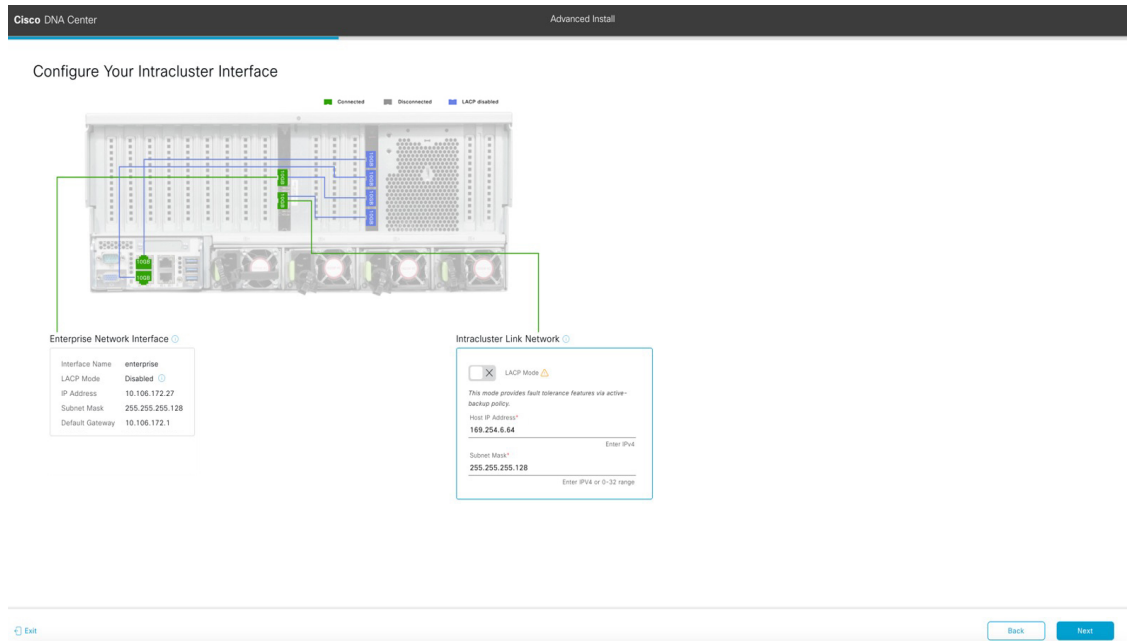
「[インターフェイスケーブル接続](#)」で説明したように、このインターフェイスは、アプライアンスをエンタープライズ ネットワークにリンクするために必要なインターフェイスです。入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

表 55: エンタープライズ インターフェイスのセカンダリノードエントリ

<p>[LACP Mode] スライダ</p>	<p>エンタープライズ インターフェイスに対して、次のネットワーク インターフェイスコントローラ (NIC) ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード：このモードでは、2つのイーサネット インターフェイスを1つの論理チャンネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード：このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネット インターフェイスが1つの論理チャンネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
<p>[Host IP Address] フィールド</p>	<p>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。</p>

[Subnet Mask] フィールド	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 (Default Gateway IP Address)] フィールド	<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>(注) このインターフェイスは、DHCP サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。</p> <ol style="list-style-type: none"> このフィールドに現在一覧表示されている IP アドレスを削除し、[Exit] をクリックします。 この操作でウィザードの最初の画面に戻ります。 エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ IP アドレスを入力します。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Intracluster Interface] 画面が開きます。



- e) クラスタ内インターフェイスの構成値を入力し、[Next] をクリックします。

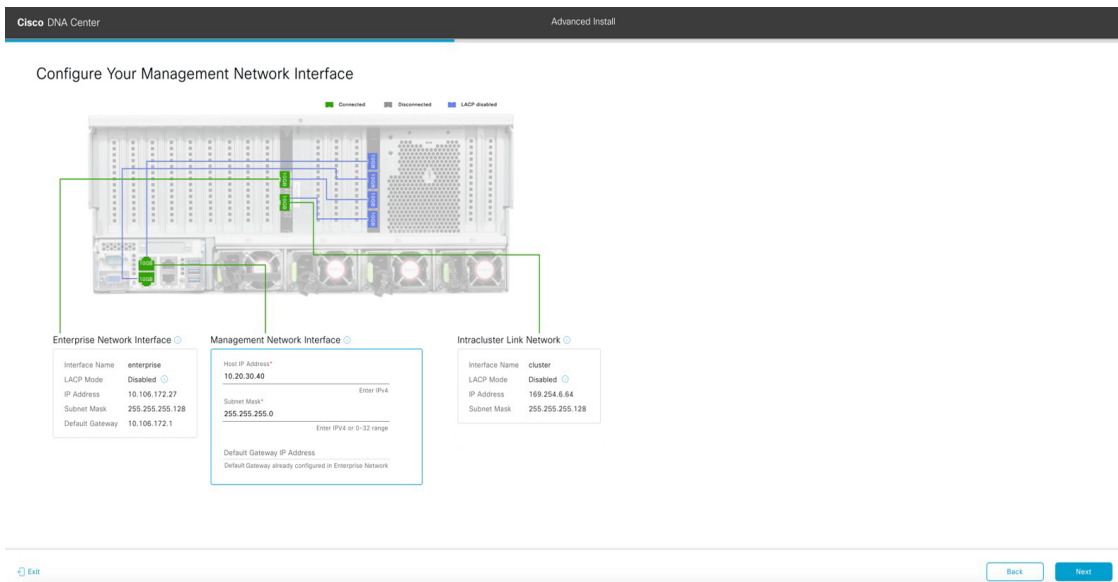
「[インターフェイスケーブル接続](#)」で説明したように、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください。

- (注)
- 同じポートでエンタープライズ インターフェイスとインターネット アクセス インターフェイスを設定する場合は、この手順を実行してから、ステップ 2f (管理 インターフェイスの設定方法が記載) に進みます。
 - エンタープライズ インターフェイスと管理インターフェイスを同じポートに設定する場合は、この手順を実行してから、ステップ 2g (インターネット アクセス インターフェイスの設定方法が記載) に進みます。
 - 同じポートでエンタープライズ、管理、およびインターネット アクセス インターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 56: クラスタ内インターフェイスのセカンダリノードエントリ

[LACP Mode] スライダ	<p>クラスタ内インターフェイスに対して、次の NIC ボンディングモードのいずれかを選択します。</p> <ul style="list-style-type: none"> • アクティブ/バックアップモード: このモードでは、2つのイーサネット インターフェイスを1つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。 • LACPモード: このモードでは、同じ速度とデュプレックス設定を共有する2つのイーサネット インターフェイスが1つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。 <p>Cisco DNA Center の NIC ボンディングの実装に関する詳細については、NIC ボンディングの概要 (77 ページ) を参照してください。</p>
[Host IP Address] フィールド	<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>
[Subnet Mask] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Management Network Interface] 画面が開きます。



f) (任意) 管理ポートの構成値を入力し、[Next] をクリックします。

「[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。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要がある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください)

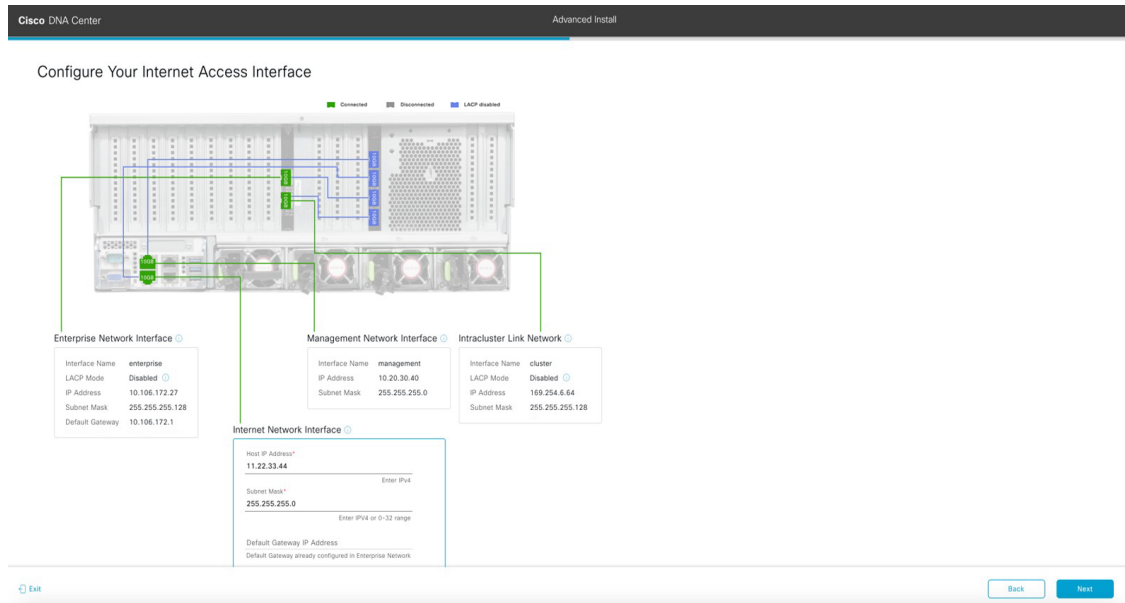
(注) 同じポートでエンタープライズインターフェイスとインターネットアクセスインターフェイスを設定する場合は、この手順を実行してから、ステップ 2h に進みます。

表 57: 管理ポートのセカンダリノードエントリ

[Host IP Address] フィールド	管理ポートの IP アドレスを入力します。
[Subnet Mask] フィールド	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。
[デフォルトゲートウェイ IP アドレス (Default Gateway IP Address)] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Configure Your Internet Access Interface] 画面が開きます。

詳細インストール構成ウィザードを使用したセカンダリノードの設定

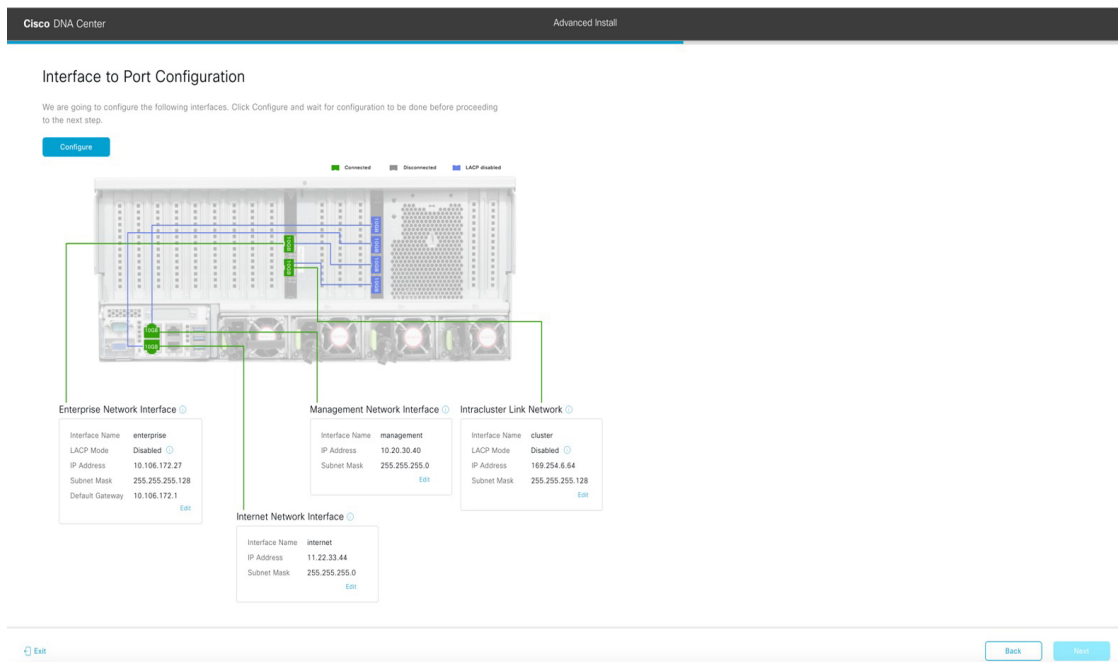


- g) (任意) インターネット アクセス インターフェイスの構成値を入力し、[Next] をクリックします。
- 「[インターフェイスケーブル接続](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。専用インターネット アクセス インターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要のある値の詳細説明については「[必要な IP アドレスおよびサブネット \(33 ページ\)](#)」と「[必須の設定情報](#)」を参照してください)

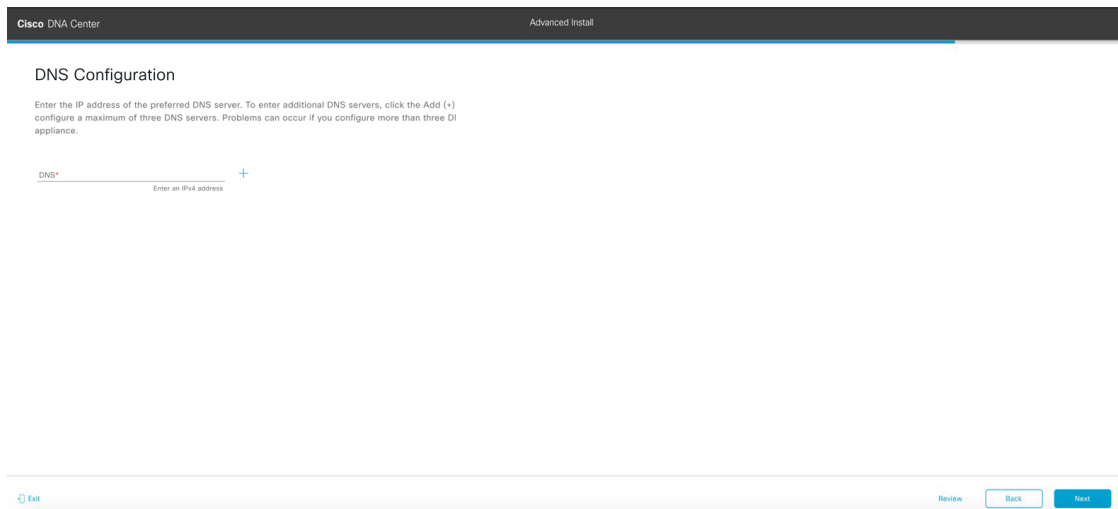
表 58: インターネット アクセス ポートのセカンダリノードエントリ

[Host IP Address] フィールド	インターネット アクセス ポートの IP アドレスを入力します。
[Subnet Mask] フィールド	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、前のフィールドに 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 (Default Gateway IP Address)] フィールド	<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>

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効で、ポートが稼働している場合は、ウィザードの [Interface to Port Configuration] 画面が開きます。



- h) セカンダリノードのインターフェイスに入力した設定を確認します。
変更が必要な場合は、関連するインターフェイスの [Edit] リンクをクリックして、ウィザード画面に戻ります。
- i) インターフェイスの設定に問題がなければ、[Configure] をクリックします。
- j) インターフェイスの初期設定が完了したら、[Next] をクリックしてウィザードの次の画面に進みます。
- [DNS Configuration] 画面が開きます。



- k) 優先 DNS サーバーの IP アドレスを入力して、[Next] をクリックします。追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

- 重要**
- クラスタ内の各ノードに対して、最大 3 つの DNS サーバーを設定します。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。
 - NTP の場合、Cisco DNA Center と NTP サーバー間でポート 123 (UDP) が開いていることを確認します。

[Configure Proxy Server Information] 画面が開きます。

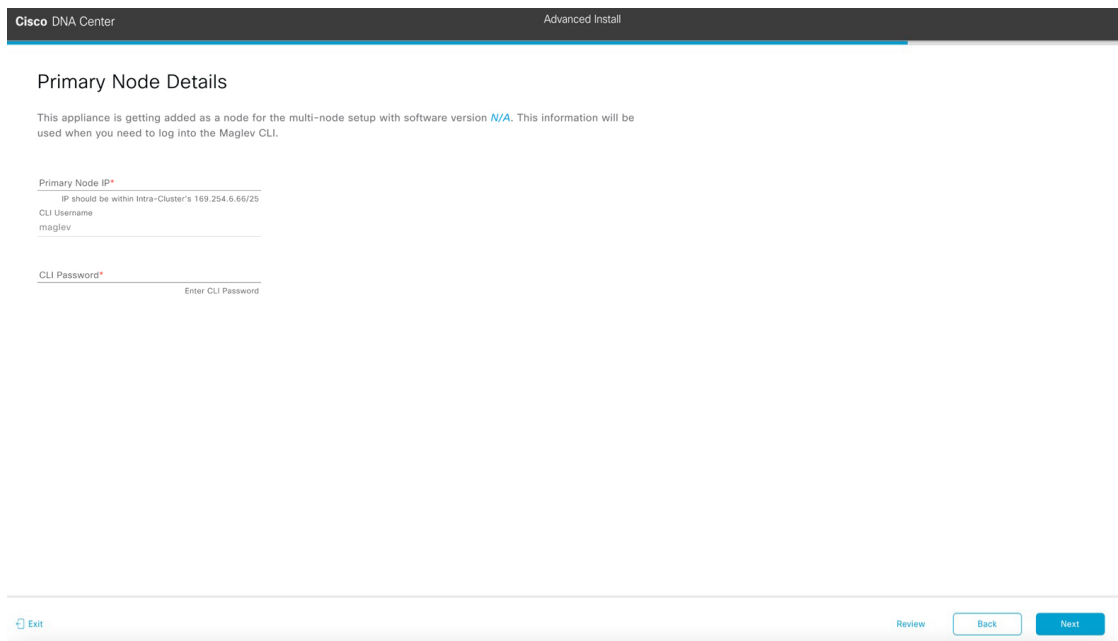
- 1) 次のいずれかを実行し、[Next] をクリックします。
- ネットワークでプロキシサーバーを使用しないでインターネットにアクセスする場合は、[No] オプションボタンをクリックします。
 - ネットワークでプロキシサーバーを使用してインターネットにアクセスする場合は、次の表に示す値を入力します。

表 59: プロキシサーバー設定のセカンダリノードエントリ

[プロキシサーバ (Proxy Server)] フィールド	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。
[Port] フィールド	アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

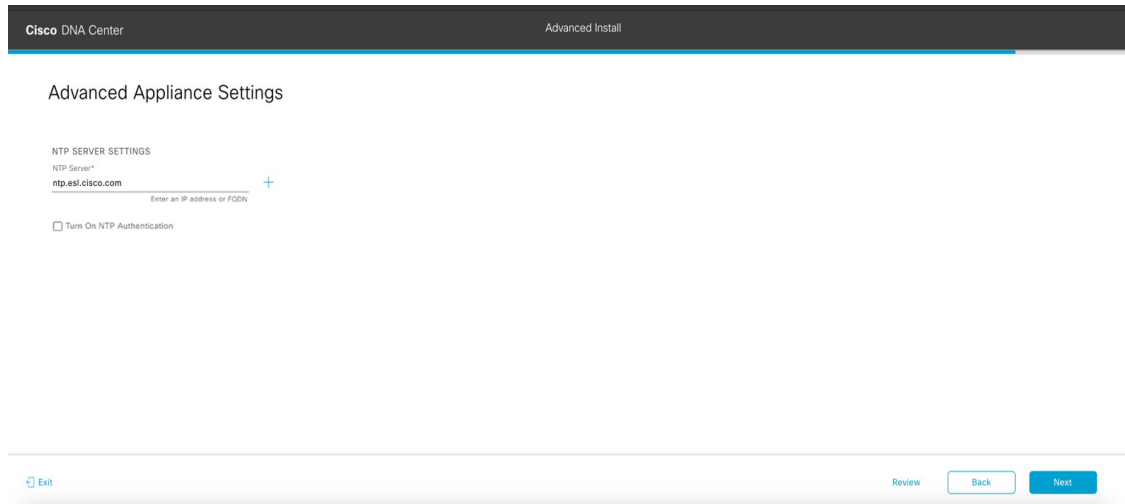
[Username] フィールド	ネットワークプロキシへのアクセスに使用するユーザ名を入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。
Password フィールド	ネットワークプロキシへのアクセスに使用するパスワードを入力します。プロキシログインが必要ない場合には、このフィールドを空白のままにします。

入力した情報がウィザードで検証され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Primary Node Details] 画面が開きます。



- m) クラスタのプライマリノードとの接続を確立するには、その IP アドレスとパスワード（デフォルトでは、ユーザー名がすでに **maglev** に設定されている場合、そのユーザー名）を入力し、[Next] をクリックします。

[Advanced Appliance Settings] 画面が開きます。



n) クラスタの構成値を入力し、[Next] をクリックします。

表 60 : [Advanced Appliance Settings] のセカンダリノードエントリ

NTP サーバー設定	
[NTP Server] フィールド	<p>少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。</p> <p>実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。</p>
[Turn On NTP Authentication] チェックボックス	<p>Cisco DNA Center と同期する前に NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。</p> <ul style="list-style-type: none"> • NTP サーバーのキー ID。有効な値の範囲は 1 ~ 4294967295 (2³²-1) です。 この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。 • NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。 <p>(注) 前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。</p>

[CLI パスワードの入力] 画面が開きます。

Cisco DNA Center Advanced Install

Enter CLI Password

CLI Password: Identifies the password for the CLI username maglev. This password ensures secure access to each appliance using the CLI command line. If required, you can assign a different CLI password for each maglev CLI username on each appliance in a cluster

Username*
maglev

Password*
***** [SHOW](#)

[View Password Criteria](#)

Retype to Confirm*
***** [SHOW](#)

[Review](#) [Back](#) [Next](#)

- o) maglev ユーザーのパスワードを入力して確認した後、[Next] をクリックします。

入力した情報がウィザードで検証され、対応するポートが稼働していることが確認され、変更の必要な設定があれば、ウィザードの操作を続行する前に通知されます。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。

Cisco DNA Center Advanced Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. You can download the generated configuration in JSON format from [here](#). When you are happy with your settings, click Start Configuration.

Ports Configuration Completed

Enterprise Network Interface

Interface Name: enterprise

LACP Mode: Disabled

IP Address: 10.106.172.27

Subnet Mask: 255.255.255.128

Default Gateway: 10.106.172.1

[Edit](#)

Management Network Interface

Interface Name: management

IP Address: 10.20.30.40

Subnet Mask: 255.255.255.0

[Edit](#)

Intracenter Link Network

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169.254.6.64

Subnet Mask: 255.255.255.128

[Edit](#)

Internet Network Interface

Interface Name: internet

IP Address: 11.22.33.44

Subnet Mask: 255.255.255.0

[Edit](#)

[Exit](#) [Start Configuration](#)

- (注) アプライアンスの設定を JSON ファイルとしてダウンロードするには、こちらのリンクをクリックします。

- p) ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な [Edit] リンクをクリックして、更新を行うウィザード画面を開きます。
- q) Cisco DNA Center アプライアンスの設定を完了するには、[Start Configuration] をクリックします。

この設定プロセスには約 90 分かかります。プロセス中もウィザード画面が継続的に更新され、現在実行しているタスクとその進行状況、発生したエラーが示されます。この情報のローカルコピーをテキストファイルとして保存するには、ダウンロードアイコンをクリックします。

Cisco DNA Center
Configuration

Appliance Configuration In Progress

It should take about 90 minutes to complete the configuration of your appliance. As you wait, you can view a video that explains the next steps in the Cisco DNA Center setup process.

Initializing the cluster using kubernetes 30%

ABOUT STARTING CISCO DNA CENTER

▶
0:00

Started: 04/09/2020 12:15:36

```

2021-05-05T16:56:59.32524 | -----
2021-05-05T16:56:59.32525 | credentialmanager.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32526 | kong.pem Apr 13 16:49:51 2020 GMT Apr 13 16:49:51 2021 GMT
2021-05-05T16:56:59.32527 | kube-admin.pem Apr 13 16:49:50 2020 GMT Apr 13 16:49:50 2021 GMT
2021-05-05T16:56:59.32528 | kube-worker-1.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32529 | masjiev-registry.pem Apr 13 16:49:52 2020 GMT Apr 13 16:49:52 2021 GMT
2021-05-05T16:56:59.32530 | apiserver.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.32531 | apiserver-kubelet-client.crt Apr 13 12:12:14 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.32532 | front-proxy-ca.crt Apr 13 17:40:20 2020 GMT Apr 11 17:40:20 2030 GMT
2021-05-05T16:56:59.32533 | front-proxy-client.crt Apr 13 17:40:20 2020 GMT Apr 13 17:40:20 2021 GMT
2021-05-05T16:56:59.32534 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.32535 | admin.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:21 2021 GMT
2021-05-05T16:56:59.32536 | scheduler.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.32537 | controller-manager.conf Apr 13 12:12:14 2020 GMT Apr 13 17:40:22 2021 GMT
2021-05-05T16:56:59.32538 | -----

```

次のタスク

タスクが完了した後：

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

最新の Cisco DNA Center リリースへのアップグレード

Cisco DNA Center の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 8 章

初期設定の完了

- [初期設定ワークフロー](#) (259 ページ)
- [互換性のあるブラウザ](#) (259 ページ)
- [クイック スタート ワークフローの完了](#) (260 ページ)
- [Cisco ISE と Cisco DNA Center の統合](#) (265 ページ)
- [認証サーバとポリシーサーバの設定](#) (273 ページ)
- [SNMP プロパティの設定](#) (277 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 ([HA のアクティブ化 \(288 ページ\)](#) 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 93 以降
- Mozilla Firefox : バージョン 92 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。

クイックスタートワークフローの完了

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。

(ユーザー名 `admin` と `SUPER-ADMIN-ROLE` が割り当てられた) 管理者スーパーユーザーとして初めてログインすると、クイックスタートワークフローが自動的に開始されます。このワークフローを完了して、Cisco DNA Center がデバイスからのテレメトリの収集を管理および有効化するデバイスを検出します。

始める前に

Cisco DNA Center にログインしてクイックスタートワークフローを完了するには、次の内容が必要です。

- 次のいずれかの手順を実行する際に指定したスーパーユーザ権限を持つ管理者のユーザ名とパスワード。
 - [Maglev ウィザードを使用したプライマリノードの設定 \(94 ページ\)](#)
 - [詳細インストール構成ウィザードを使用したプライマリノードの設定 \(157 ページ\)](#) (44 または 56 コアアプライアンス)
 - [詳細インストール構成ウィザードを使用したプライマリノードの設定 \(218 ページ\)](#) (112 コアアプライアンス)
- [必要な初期設定情報 \(53 ページ\)](#) に記載されている情報。

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

ステップ 2 `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 DNA Center 管理者ガイド](#)』の「Certificate and Private Key Support」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。

Cisco DNA Center ログイン画面が表示されます。

ステップ 5 次のいずれかを実行し、[Log In] をクリックします。

- Maglev 構成ウィザードを完了し、[Start using DNAC pre manufactured cluster] オプションを選択した場合は、管理者のユーザー名 (**admin**) とパスワード (**maglev1@3**) を入力します。
- Maglev 構成ウィザードを完了し、[Start configuration of DNAC in advanced mode] オプションを選択した場合は、Cisco DNA Center アプライアンスの構成時に設定した管理者のユーザー名 (**admin**) とパスワードを入力します。
- インストール構成ウィザードを完了したら、管理者のユーザー名 (**admin**) を入力し、ウィザードの最後の画面からコピーしたパスワード (**maglev1@3**) を貼り付けます。
- 高度なインストール構成ウィザードを完了した場合は、Cisco DNA Center アプライアンスの構成時に設定した管理者のユーザー名 (**admin**) とパスワードを入力します。

次の画面で、(セキュリティ対策として) 新しい管理者パスワードを指定するよう求められます。

ステップ 6 次のいずれかを実行します。

- この時点で管理者パスワードを変更しない場合は、[Skip] をクリックします。
- 新しい管理者パスワードを設定するには、次の手順を実行します。
 1. ステップ 5 で指定したのと同じパスワードを入力します。
 2. 新しい管理者パスワードを入力し、確認します。
 3. [Next] をクリックします。

ステップ 7 cisco.com のユーザー名とパスワード (ソフトウェアダウンロードの登録とシステム通信の受信に使用される) を入力し、[Next] をクリックします。

(注) 現時点でこれらのログイン情報を入力したくない場合は、代わりに [Skip] をクリックします。

[Terms & Conditions] 画面が開き、ソフトウェアのシスコエンドユーザー ライセンス契約 (EULA) および現在利用可能な補足条件へのリンクが表示されます。

ステップ 8 各ドキュメントを確認したら、[Next] をクリックして EULA に同意します。

[Quick Start Overview] スライダが開きます。[>] をクリックすると、Cisco DNA Center の使用を開始するために、クイックスタートワークフローで完了までサポートされるタスクの説明が表示されます。

ステップ 9 クイックスタートワークフローを完了します。

- a) [Let's Do it] をクリックします。
- b) [Discover Devices: Provide IP Ranges] 画面で、次の情報を入力し、[Next] をクリックします。
 - デバイス検出ジョブの名前。
 - 検出するデバイスの IP アドレスの範囲。追加の範囲を入力するには、[+] をクリックします。
 - アプライアンスのループバックアドレスを優先管理 IP アドレスとして指定するかどうかを指定します。詳細については、『Cisco DNA Center ユーザーガイド』の「Preferred Management IP Address」を参照してください。
- c) [Discover Devices: Provide Credentials] 画面で、設定するログイン情報のタイプに関する情報（次の表を参照）を入力し、[Next] をクリックします。

フィールド	説明
[CLI (SSH) Credentials]	
ユーザ名	ネットワーク内のデバイスの CLI にログインするために使用するユーザー名。
Password	ネットワーク内のデバイスの CLI にログインするために使用するパスワード。入力するパスワードは、8 文字以上にする必要があります。
名前/説明	CLI ログイン情報の名前または説明。
Enable Password	CLI でより高い権限レベルを有効にするために使用するパスワード。ネットワークデバイスが必要な場合にのみ、このパスワードを設定します。
[SNMP Credentials: SNMPv2c Read] タブ	
(注) Cisco DNA Center は、FIPS モードが有効になっている場合、SNMPv2c ログイン情報をサポートしません。代わりに、SNMPv3 ログイン情報を入力する必要があります。FIPS モードの詳細については、 Maglev ウィザードを使用したプライマリノードの設定 (94 ページ) を参照してください。	
名前/説明	SNMPv2c 読み取りコミュニティストリングの名前または説明。
コミュニティストリング	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティストリングパスワード。

フィールド	説明
[SNMP Credentials: SNMPv2c Write] タブ	
名前/説明	SNMPv2c 書き込みコミュニティストリングの名前または説明。
コミュニティストリング	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。
[SNMP Credentials: SNMPv3]	
名前/説明	SNMPv3 ログイン情報の名前または説明。
ユーザ名	SNMPv3 ログイン情報に関連付けられているユーザー名。
モード	<p>SNMP メッセージを必要とするセキュリティレベル。</p> <ul style="list-style-type: none"> • [No Authentication, No Privacy] (noAuthnoPriv) : 認証も暗号化も行いません。 • [Authentication, No Privacy] (authNoPriv) : 認証は行いますが、暗号化は行いません。 • [Authentication and Privacy] (authPriv) : 認証と暗号化の両方を行います。 <p>(注) FIPS モードが有効な場合、Cisco DNA Center では [Authentication and Privacy] モードのみがサポートされます。</p>
Authentication Password	<p>SNMPv3 を使用するデバイスから情報にアクセスするために必要なパスワード。パスワードの長さは、最低 8 文字である必要があります。次の点に注意してください。</p> <ul style="list-style-type: none"> • 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCisco DNA Centerによる検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
認証タイプ	<p>[Authentication and Privacy] または [Authentication, No Privacy] が認証モードとして設定されている場合に使用されるハッシュベースのメッセージ認証コード (HMAC) タイプ。</p> <ul style="list-style-type: none"> • [SHA] : HMAC-SHA 認証。 • [MD5] : HMAC-MD5 認証。 <p>(注) Cisco DNA Center は、FIPS モードが有効になっている場合、この認証タイプをサポートしません。</p>
Privacy Type	<p>[Authentication and Privacy] が認証モードとして設定されている場合に使用されるプライバシータイプ。次のいずれかのプライバシータイプを選択します。</p> <ul style="list-style-type: none"> • [AES128] : 暗号化の 128 ビット CBC モード AES。 • [CISCOAES192] : 暗号化の 192 ビット CBC モード AES。 • [CISCOAES256] : 暗号化の 256 ビット CBC モード AES。 <p>(注)</p> <ul style="list-style-type: none"> • 検出およびインベントリ機能は、AES192 および AES256 プライバシータイプのみをサポートします。 • Cisco DNA アシユアランスは、これらのプライバシータイプをサポートしていません。
Privacy Password	<p>AES128、AES192、および AES256 暗号化標準規格でサポートされているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード (またはパスフレーズ) は、8 文字以上にする必要があります。</p> <p>次の点に注意してください。</p> <ul style="list-style-type: none"> • 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Cisco DNA Center による検出、監視、管理が行われなくなります。 • パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。
NETCONF	
ポート	Cisco IOS-XE を実行するワイヤレスコントローラを検出するために Cisco DNA Center が使用する必要がある NETCONF ポート。

- d) [Create Site] 画面で、テレメトリを容易にするために検出するデバイスを1つのサイトにグループ化し、[Next] をクリックします。
- サイトの情報を手動で入力するか、提供されたマップで使用する場所をクリックします。
- e) [Enable Telemetry] 画面で、Cisco DNA Center にテレメトリを収集させるネットワークコンポーネントを選択し、[Next] をクリックします。
- (注) [Enable Telemetry] オプションと [Disable Telemetry] オプションの両方がグレー表示されている場合、これは、デバイスがテレメトリをサポートできないか、デバイスがテレメトリの有効化をサポートしていない OS バージョンを実行していることを示しています。
- f) [Summary] 画面で、入力した設定を確認し、次のいずれかを実行します。
- 変更を加える場合は、該当する [Edit] リンクをクリックして、関連画面を開きます。
 - 設定に問題がなければ、[Start Discovery and Telemetry] をクリックします。Cisco DNA Center により設定が検証され、問題が発生しないことが確認されます。検証が完了すると、画面が更新されます。
- Cisco DNA Center により、ネットワークのデバイスを検出し、選択したネットワークコンポーネントのテレメトリを有効にするプロセスが開始されます。このプロセスには 30 分以上かかります（大規模なネットワークの場合はさらに長くなります）。
- ホームページの上部に、クイックスタートワークフローが完了したことを示すメッセージが表示されます。
- g) 次のいずれかを実行します。
- [View Discovery] をクリックして [Discovery] ページを開き、ネットワーク内のデバイスが検出されたことを確認します。
 - [Go to Network Settings] リンクをクリックして、[Device Credentials] ページを開きます。ここから、以前に入力したログイン情報がサイトに設定されていることを確認できます。
 - [View Activity Page] リンクをクリックして [Tasks] ページを開き、Cisco DNA Center ですでに実行がスケジュールされているタスク（セキュリティアドバイザリの毎週のネットワークスキャンなど）を表示します。
 - [Workflow Home] リンクをクリックして、ネットワークのセットアップと維持に役立つガイド付きワークフローにアクセスします。

Cisco ISE と Cisco DNA Center の統合

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 ISE と安全な方法で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。ユーザーは Cisco DNA Center を使用してデバイスを検出でき、検出されたデバイスは両方のアプリケーションに表示されるため、Cisco DNA Center と Cisco ISE の両方の機能を適用できます。また Cisco DNA Center デバイスと Cisco ISE デバイスはすべて、デバイス名で一意に識別されます。

Cisco DNA Center デバイスは、Cisco DNA Center サイト階層内の特定のサイトにプロビジョニングされて割り当てられると、すぐに 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 ISE 上の対応するデバイスインスタンスに送信されます。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 ホストを展開済みであること。サポートされている Cisco ISE バージョンの詳細については、『[Cisco DNA Center Compatibility Matrix](#)』を参照してください。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 \[英語\]](#) 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 DNA Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。



(注) 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 をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。



(注) PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

- 分散型展開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。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。

- TrustSec または 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 Identity Services Engine Administrator Guide』を参照してください。
- ネットワーク管理者ロールの権限を持つユーザーのみが Cisco ISE と Cisco DNA Center を統合できます。
- Cisco ISE で [Use CSRF Check for Enhanced Security] オプションが有効になっている場合、Cisco DNA Center は ERS API アクセスをサポートしません。
- ポート 443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信を有効にする必要があります。
- 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 サービスで使用される証明書に対してオンライン証明書ステータスプロトコル (OCSP) または証明書失効リスト (CRL) 検証が定義されている場合、Cisco DNA Center は証明書失効ステータスをチェックします。
- 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。
- FQDN のみのシステム証明書を使用できるかどうかは、Cisco DNA Center 展開で LAN 自動化が有効になっているかどうかによって異なります。詳細については、『Cisco DNA Center Security Best Practices Guide』の「Generate a Certificate Request Using Open SSL」トピックのステップ 3 にある「alt_names」セクションの箇条書きを参照してください。



- (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。詳細については、[Cisco Cloud APIC リリースノート \[英語\]](#) 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 Identity Services Engine 管理者ガイド』の「Integration with Cisco DNA Center」を参照してください。<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html>

ステップ 1 Cisco ISE の pxGrid サービスと ERS を有効にします。

- a) プライマリポリシー管理ノードにログインします。
- b) Cisco ISE GUI で、メニューアイコン (☰) をクリックして、**[Administration] > [System] > [Deployment]** を選択します。
[Deployment Nodes] ウィンドウが表示されます。
- c) pxGrid サービスを有効化する Cisco ISE ノードのホスト名をクリックします。分散型展開の場合、これは展開環境内の任意の Cisco ISE ノードです。
[ノードの編集 (Edit Node)] ウィンドウが表示されます。
- d) **[General Settings]** タブをクリックし、**[pxGrid]** チェックボックスをオンにして、**[Save]** をクリックします。
- e) Cisco ISE GUI で、メニューアイコン (☰) をクリックして、**[Administration] > [System] > [Settings]** を選択します
- f) 左側のナビゲーションウィンドウで **[設定 (Settings)]** をクリックして、**[設定 (Settings)]** ウィンドウを開きます。
- g) **[Enable ERS for Read/Write]** オプションボタンをクリックし、通知プロンプトで **[OK]** をクリックします。
- h) **[保存 (Save)]** をクリックします。

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

- a) Cisco DNA Center GUI にログインします。
- b) メニューアイコン (☰) をクリックして、**[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) **[Add ISE server]** スライドインペインで、次の情報を入力します。
 - **[Server IP Address]** フィールドに、Cisco ISE サーバーの 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。
 - **[Connect to pxGrid]** : pxGrid 接続を有効にするには、**[Advanced Settings]** でこのチェックボックスをオンにします。

Cisco DNA Center システム証明書を pxGrid クライアント証明書として使用する場合 (pxGrid クライアントとして Cisco DNA Center システムを認証するために ISE に送信) 、**[Use Cisco DNA Center**

Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ認証局 (CA) で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Cisco DNA Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ CA によって生成されていること (そうでない場合、pxGrid 認証は失敗します)。
- [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。
- [Advanced Settings] エリアで、以下の手順を実行します。
 - [RADIUS] または [TACACS] のチェックボックスをオンにして、使用する必要があるプロトコルを選択できます
 - 次のフィールドに必要な値を入力します。[Authentication Port]、[Accounting Port]、[Retries]、[Timeout seconds]。

(注) このオプションは、Cisco DNA Center がサードパーティの証明書を使用している場合にのみ使用できます。Cisco DNA Center がデフォルトの自己署名システム証明書を使用する場合、このオプションは無効になっています。

f) [Add] をクリックします。

Cisco ISE との統合を開始すると、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] をクリックして証明書を信頼し、統合プロセスを続行するか、証明書を信頼せず、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。

統合プロセスに問題がある場合は、エラーメッセージが表示されます。必要に応じて、編集または再試行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) メニューアイコン (☰) をクリックして、[System] > [System 360] の順に選択します。
- c) [Identity Services Engine (ISE)] ペインで、リストされているすべての ISE サーバーのステータスの表示が [Available] または [Configured] になっていることを確認します。
- d) [Identity Services Engine (ISE)] ペインで、[Update (更新)] リンクをクリックします。

- e) **[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、接続にサブスクリプションがあることを確認します。

- a) **[Identity Services Engine (ISE) Deployment]** ペインで pxGrid サーバー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 サーバーの IP アドレスとともに 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 の使用開始時

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。そのため、新規またはアップグレードで 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、次の手順を実行する必要があります。

- Cisco ISE を Cisco DNA Center と統合する（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を実行する。

「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。

- セキュリティグループ：数値であるセキュリティグループタグ (SGT) は、セキュリティグループを一意に識別します。Cisco ISEセキュリティグループが Cisco DNA Center のセキュリティ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 に新しいセキュリティグループが作成されます。新しいセキュリティグループには「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 のセキュリティ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 セキュリティ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

ポリシーで参照される 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、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、Cisco DNA Center によってテキストコマンドラインが解析され、それらの SGACL コマンドが可能な限りモデル化されたアクセス契約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 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、Cisco ISE ではこのオプションはデフォルトで無効になっていて、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、そ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。[multiple SGACL] オプションを利用し、移行できない具体的なポリシー機能は次のとおりです。

- 1つのポリシーに含まれる複数の 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。
- お客様が作成した 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、Cisco DNA Center への移行では現在、[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。

ポリシーの移行と同期の操作中に前述のいずれかの SGACL が検出された場合、通知が生成されます。続行するには、次のいずれかのオプションを選択する必要があります。

- [Manage Group-Based Access Control policy in Cisco DNA Center] : 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 [Permit] に設定されます。

- [Manage Group-Based Access Control Policy in Cisco ISE] : 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。
- [Manage Group-Based Access Control policy in both Cisco DNA Center and Cisco ISE] : このオプションの場合、Cisco ISE で加えられたポリシーの変更が 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 の更新に関してより多くの時間と柔軟性が必要な場合は、このオプションを使用できます。

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 および Cisco ISE が統合されていることを確認します。
- Cisco DNA Center の FIPS モードが有効になっている場合は、Cisco DNA Center と Cisco ISE の統合時に KeyWrap を有効にしてください。[Cisco ISE と Cisco DNA Center の統合 \(265 ページ\)](#) の手順 2e を参照してください。



(注) Cisco DNA Center と Cisco ISE がすでに統合されている場合、KeyWrap を有効にすることはできません。この機能を有効にするには、Cisco ISE を削除してから Cisco DNA Center と再統合する必要があります。

- 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 サーバーで Cisco DNA Center を登録します。これには、AAA サーバーと Cisco DNA Center の共有秘密を定義することが含まれます。
 - AAA サーバーで 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 サーバー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。
- Cisco ISE を設定する前に、以下の点を確認してください。

- Cisco ISE をネットワークに展開していること。サポートされている Cisco ISE バージョンの詳細については、『[Cisco DNA Center Compatibility Matrix](#)』を参照してください。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 \[英語\]](#) を参照してください。
- スタンドアロン ISE 展開環境がある場合は、Cisco DNA Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス (ERS) を有効にする必要があります。



(注) 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 をプライマリポリシー管理ノード (PAN) と統合し、PAN 上で ERS を有効にする必要があります。



(注) PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

- 分散型展開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。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
- TrustSec または 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 Identity Services Engine Administrator Guide](#)』を参照してください。
- ポート 443、5222、8910、9060 で Cisco DNA Center と Cisco ISE の通信を有効にする必要があります。
- 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。詳細については、[Cisco Cloud APIC リリースノート \[英語\]](#) を参照してください。

ステップ 1 メニューアイコン (☰) をクリックして、**[System] > [Settings] > [External Services] > [Authentication and Policy Servers]**。

ステップ 2 [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。

ステップ 3 プライマリ AAA サーバーを設定するには、次の情報を入力します。

- [Server IP Address] : AAA サーバの IP アドレス。
- [Shared Secret] : デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

ステップ 4 Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address] : ISE サーバーの IP アドレス。
- [Shared Secret] : デバイス認証のキー。
- [Username] : Cisco ISE CLI にログインするために使用するユーザー名。
(注) このユーザーにはスーパーユーザーの管理権限が必要です。
- [Password] : Cisco ISE CLI ユーザー名に対応するパスワード。
- [FQDN] : Cisco ISE サーバーの完全修飾ドメイン名 (FQDN)。
(注)
 - Cisco ISE (**[Administration] > [Deployment] > [Deployment Nodes] > [List]**) で定義されている FQDN をコピーして、このフィールドに直接貼り付けることをお勧めします。
 - 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名 (CN) または Subject Alternative Name (SAN) と一致する必要があります。

FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。

hostname.domainname.com

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

- [Virtual IP Address (es)] : Cisco ISE ポリシーサービスノード (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。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

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

- [Connect to pxGrid] : pxGrid 接続を有効にするには、このチェックボックスをオンにします。

Cisco DNA Center システム証明書を pxGrid クライアント証明書として使用する場合 (pxGrid クライアントとして Cisco DNA Center システムを認証するために Cisco ISE に送信)、[Use Cisco DNA Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Cisco DNA Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Cisco DNA Center 証明書が、Cisco ISE で使用中の CA と同じ認証局 (CA) によって生成されていること (そうでない場合、pxGrid 認証は失敗します)。
- [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。

- [Protocol] : [TACACS] と [RADIUS] (デフォルト)。両方のプロトコルを選択できます。

注目 ここで Cisco ISE サーバーの TACAS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design] > [Network Settings] > [Network]** で Cisco ISE サーバーを TACAS サーバーとして設定できません。

- [Authentication Port] : AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- [Accounting Port] : AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- [Port] : デフォルトの TACACS 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 サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

(注) 必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Cisco DNA Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、[Authentication and Policy Servers] ウィンドウと [System 360] ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「進行中」
- [System 360] ウィンドウ：「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ：

- [Authentication and Policy Servers] ウィンドウ：「アクティブ」
- [System 360] ウィンドウ：「プライマリ使用可能」および「pxGrid 使用可能」

設定された Cisco ISE サーバーのステータスがパスワードの変更により [FAILED] と表示されている場合は、[Retry] をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。

ステップ 6 [Add] をクリックします。

ステップ 7 セカンダリサーバーを追加するには、前述の手順を繰り返します。

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 メニューアイコン (☰) をクリックして、[System] > [Settings] > [Device Settings] > [SNMP] の順に選択します。

ステップ 2 次のフィールドを設定します。

- **再試行回数 (Retries)**：許容されるデバイス接続の最大試行回数。有効な値は 1 ~ 3 です。デフォルトは 3 です。
- **[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 9 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 \(279 ページ\)](#)
- [ログアウト \(279 ページ\)](#)
- [設定ウィザードを使用したアプライアンスの再設定 \(280 ページ\)](#)
- [アプライアンスの電源の再投入 \(282 ページ\)](#)

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、CIMC GUI にログインして使用します。
3. アプライアンスの設定を変更する必要がある場合は、「[設定ウィザードを使用したアプライアンスの再設定](#)」の説明に従って、Maglev 設定ウィザードを起動して使用します。
4. 変更が有効になるようにアプライアンスの電源を入れ直します：[アプライアンスの電源の再投入 \(282 ページ\)](#)

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、CIMC GUI または Maglev 設定ウィザードのみを使用します。

ログアウト

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

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

ステップ 1 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、構成ウィザードを使用してアプライアンスの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、構成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。

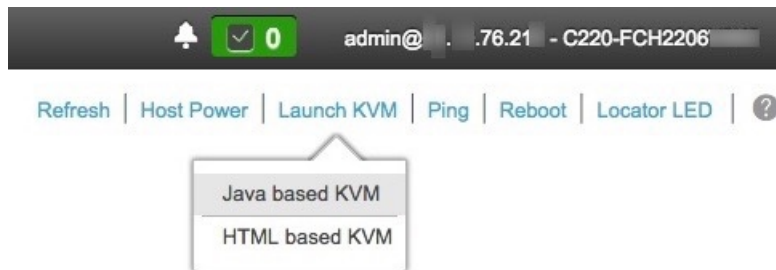
- アプライアンスのホスト IP アドレス
- DNS サーバの IP アドレス
- デフォルトゲートウェイ IP アドレス
- NTP サーバの IP アドレス
- クラスタ仮想 IP アドレス (Cluster Virtual IP address)
- クラスタホスト名 (FQDN)
- スタティック ルート
- プロキシサーバの IP アドレス
- Maglev ユーザのパスワード
- 管理ユーザのパスワード。
- NIC ボンディングの有効化

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 ユーザー名 (*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 ユーザーとして 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 設定ウィザードでは、「[Maglev ウィザードを使用したセカンダリノードの設定](#)」に示される一連の画面のセッションが簡略化されています。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再投入

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

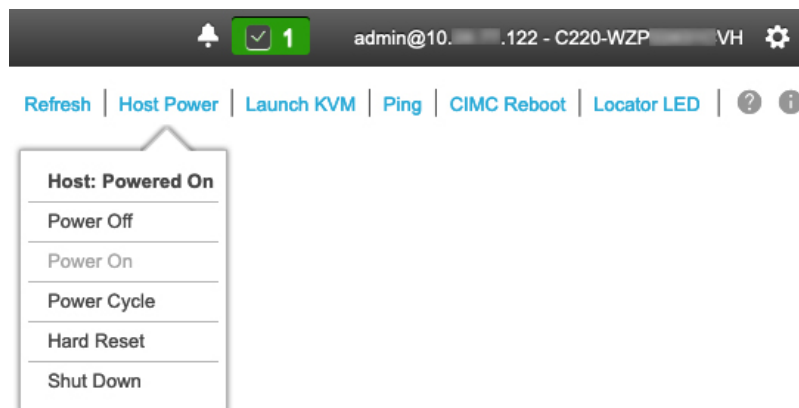
Cisco IMC GUI を使用して行ったハードウェアの変更は、アプライアンスのリポート後に適用されることに注意してください。



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 \(68 ページ\)](#) 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ポートします。

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

次の内容が必要になります。

- 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 \(5 ページ\)](#) の背面パネルを参照してください。
- 現在ターゲットアプライアンスに設定されている Linux ユーザ名 (*maglev*) とパスワード。

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

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

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

ステップ 3 実行するタスクに適したコマンドを入力します。

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

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

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

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



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 [HA 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 \(285 ページ\)](#)
 - [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 \(286 ページ\)](#)
 - [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 \(287 ページ\)](#)
 - [HA のアクティブ化 \(288 ページ\)](#)
 - [HA の展開に関する追加の考慮事項 \(288 ページ\)](#)

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

- Maglev 設定ウィザードを使用している場合は「[Maglev ウィザードを使用したプライマリノードの設定 \(94 ページ\)](#)」を参照してください。

- ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「詳細インストール構成ウィザードを使用したプライマリノードの設定」を参照してください。
 - 44 または 56 コアアプライアンス [詳細インストール構成ウィザードを使用したプライマリノードの設定](#) (157 ページ)
 - [詳細インストール構成ウィザードを使用したプライマリノードの設定](#)

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

- Maglev 設定ウィザードを使用している場合は「[Maglev ウィザードを使用したセカンダリノードの設定](#) (117 ページ)」を参照してください。
- ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「詳細インストール構成ウィザードを使用したセカンダリノードの設定」を参照してください。
 - 44 または 56 コアアプライアンス [詳細インストール構成ウィザードを使用したセカンダリノードの設定](#) (178 ページ)
 - [詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)

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 2.3.5 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。

- Maglev 設定ウィザードを使用するアプライアンスを設定している場合は「[Maglev ウィザードを使用したセカンダリノードの設定 \(117 ページ\)](#)」を参照してください。
- ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「[詳細インストール構成ウィザードを使用したセカンダリアプライアンスの設定](#)」を参照してください。
 - [詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)
 - [詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)

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 2.3.5 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 Digital Network Architecture Center 管理者ガイド](#)』の「Backup and Restore」の章を参照してください。

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

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

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

ステップ 5 ステップ 2 で作成したバックアップファイルを使用して、リモートリポジトリのデータを復元します。

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

- Maglev 設定ウィザードを使用するアプライアンスを設定している場合は「[Maglev ウィザードを使用したセカンダリノードの設定 \(117 ページ\)](#)」を参照してください。
- ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「[詳細インストール構成ウィザードを使用したセカンダリアプライアンスの設定](#)」を参照してください。
 - [詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)
 - [詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)

HA 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. メニューアイコン (☰) をクリックして、**[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 `sudo 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。