



Cisco Digital Network Architecture Center アプリケーション イン ストール ガイド、リリース 1.2.10 (M4 シャーシ)

初版：2019年1月29日

最終更新：2019年2月21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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

シスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティングシステムの UCB パブリック ドメインバージョンの一部として開発されたプログラムを適応したものです。All rights reserved. ここに掲載されているコンテンツの全ては、カリフォルニア大学に著作権がある、

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。Cisco および上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワークトポロジー図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この文書の印刷されたハードコピーおよび複製されたソフトコピーは、すべて管理対象外と見なされます。最新版については、現在のオンラインバージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所と電話番号は、当社のウェブサイト (<http://www.cisco.com/web/JP/about/office/index.html>) をご覧ください。

Cisco および Cisco ロゴは、シスコや米国および他の国の関連会社の商標です。シスコの商標の一覧は、[www.cisco.com go trademarks](http://www.cisco.com/go/trademarks) で参照できます。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。「パートナー」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



目次

第 1 章

アプライアンス機能の確認 1

- 機能の概要 1
- 前面パネルと背面パネル 2
- 物理仕様 11
- 環境仕様 11
- 電力仕様 12

第 2 章

導入の計画 15

- プランニング ワークフロー 15
- Cisco DNA Centerおよび Software-Defined Access (SD-Access) について 16
- インターフェイスクーブル接続 17
- 必要なサブネットおよび追加の IP アドレス 20
 - インターフェイス名とウィザードの設定順序 24
- 必要なインターネット URL と完全修飾ドメイン名 25
- インターネットへのアクセスを保護する 26
- 必要なネットワーク ポート 27
- 必要な SD アクセス ポートおよびプロトコル 29
- 必要な設定情報 39
- 必要な初期設定情報 40

第 3 章

アプライアンスの設置 43

- アプライアンスのインストール ワークフロー 43
- アプライアンスを開梱して点検 45
- 設置に関する警告とガイドラインの確認 45

ラック要件の確認	47
アプライアンスの接続および電源投入	47
LED の確認	48

第 4 章**アプライアンスの設定 51**

アプライアンスの設定ワークフロー	51
CIMC へのブラウザアクセスの有効化	52
事前フライトチェックの実行	57
Cisco DNA Center ISO イメージの確認	64
ブート可能 USB ドライブの作成	65
アプライアンスのイメージの再作成	66
Cisco DNA Center ISO イメージのインストール	68
マスターノードの設定	69
アドオンノードの設定	85
ハイ アベイラビリティ クラスタの導入シナリオ	100
新しい HA の導入	100
標準インターフェイス設定を使用したマスターノードの既存の HA の導入	100
標準以外のインターフェイス設定を使用したマスターノードの既存の HA の導入	101
HA の導入のその他の考慮事項	102
テレメトリ	102
ワイヤレス コントローラ	102
Cisco DNA Center の最新リリースへのアップグレード	102

第 5 章**初期設定の完了 103**

初期設定ワークフロー	103
互換性のあるブラウザ	104
初回ログイン	105
Cisco ISE との統合 Cisco DNA Center	113
認証サーバとポリシー サーバの設定	115
SNMP プロパティの設定	117
サービスの再配布	118

第 6 章

展開のトラブルシューティング 119

トラブルシューティング タスク 119

ログアウト 120

設定ウィザードを使用したアプライアンスの再設定 120

アプライアンスの電源を切って再度入れる 122



第 1 章

アプライアンス機能の確認

- [機能の概要 \(1 ページ\)](#)
- [前面パネルと背面パネル \(2 ページ\)](#)
- [物理仕様 \(11 ページ\)](#)
- [環境仕様 \(11 ページ\)](#)
- [電力仕様 \(12 ページ\)](#)

機能の概要

シスコは、Cisco DNA Center をラックマウント可能なアプライアンス（シスコ製品番号 DN1）の形式で提供しています。アプライアンスは、Cisco UCS C220 M4 シャーシで構成されており、mLOM スロットに仮想インターフェイスカード（VIC）1227 が追加されています。Cisco DNA Center ソフトウェアイメージはアプライアンスに事前にインストールされていますが、使用するには設定する必要があります。

次の表に、アプライアンスの機能の概要を示します。

表 1: Cisco DNA Center アプライアンスシリーズの機能

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	最大 2 つの Intel Xeon E5-2600 v4 シリーズプロセッサファミリー CPU
メモリ	レジスタード DIMM（RDIMM）または低負荷 DIMM（LRDIMM）用の 24 スロット（各 CPU で 12）
ストレージ	2.5 インチ小型フォームファクタ（SFF）ソリッドステートドライブ（SSD）X 8

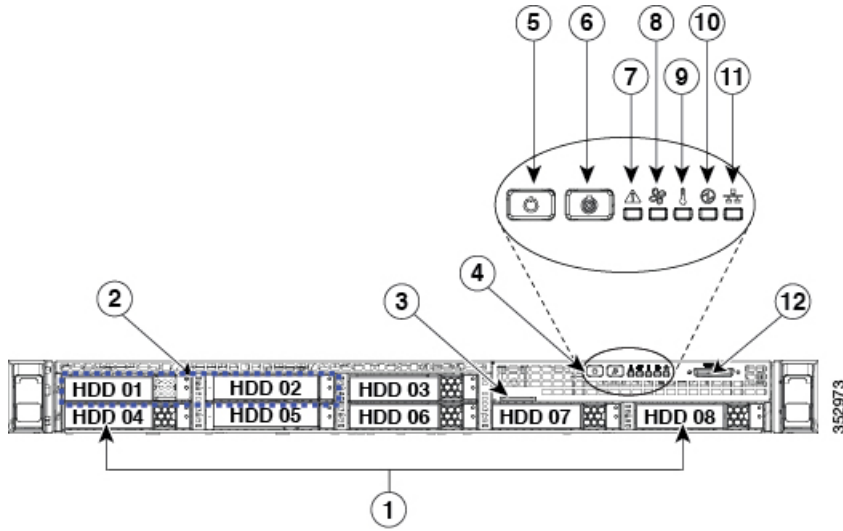
機能	説明
ディスク管理 (RAID)	事前設定済みの3つの RAID 設定：スロット 1 と 2 の RAID 1、スロット 3 と 4 の RAID 1、スロット 5、6、7、および 8 の RAID 10。これらの設定は、ユーザが設定することはできません。
ネットワークおよび管理 I/O	<p>サポートされるコネクタ：</p> <ul style="list-style-type: none"> • Cisco UCS 仮想インターフェイスカード (VIC) 1227 上の 10 Gbps イーサネットポート X 2 • 1 Gbps イーサネット専用管理ポート X 1 • 1 Gbps BASE-T イーサネット LAN ポート X 2 <p>次のコネクタを使用できますが、通常は Cisco DNA Center の日常業務では使用されません。</p> <ul style="list-style-type: none"> • RS-232 シリアルポート (RJ-45 コネクタ) X 1 • 15 ピン VGA2 コネクタ X 1 • USB 3.0 コネクタ X 2 • USB 2.0 2 個、VGA 1 個、シリアル (DB-9) コネクタ 1 個を装備した KVM ケーブルを使用する前面パネル KVM コネクタ X 1
電力	<p>デュアル AC 電源装置、各台に 770 W AC を設置</p> <p>サーバ内で異なるタイプ/ワット数の電源装置を組み合わせ使用しないでください。</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 6。
ビデオ	60 Hz で最大 1920 X 1200、16 bpp の VGA ビデオ解像度、最大 256 MB のビデオメモリ。

前面パネルと背面パネル

次の図と表では、Cisco UCS C220 M4 シャーシを備えた 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。

[このリンクをクリック](#)すると、アプライアンスの前面パネルと背面パネル、およびアプライアンスの NIC の配線方法について説明する短いビデオが表示されます。

図 1:アプライアンスの前面パネル

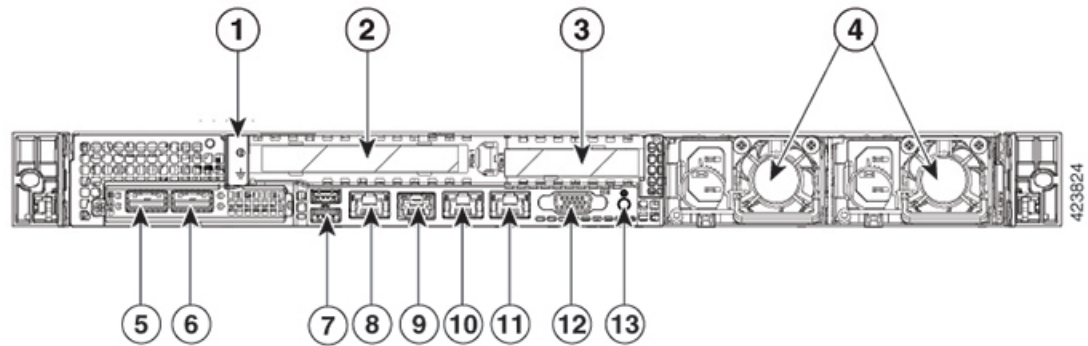


コンポーネント	説明
1	<p>2.5 インチ SDD ドライブ X 8。取り付けられている各ドライブベイには、障害 LED とアクティビティ LED があります。</p> <p>ドライブ障害 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：ドライブは正常に動作中です。 • オレンジ：ドライブで障害が発生しています。 • オレンジの点滅：ドライブの再構成中です。 <p>ドライブアクティビティ LED の状態とその説明：</p> <ul style="list-style-type: none"> • 消灯：スレッドにドライブが存在しません（アクセスなし、障害なし）。 • 緑：ドライブの準備が完了しています。 • 緑の点滅：ドライブはデータの読み取り中または書き込み中です。
2	<p>ドライブベイ 1 と 2 は、SAS/SATA および NVMe PCIe ソリッドステートドライブ（SSD）をサポートします。これらのドライブでは、障害 LED とアクティビティ LED およびその状態は、取り付けられた 2.5 インチ SDD ドライブの場合と同様です。</p>
3	<p>引き抜きアセット タグ</p>
4	<p>操作サブパネルのボタンおよび LED これらのボタンの LED の状態と、示されている条件については、次のエントリで説明します。</p>

コンポーネント	説明
5	<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。CIMC と一部のマザーボード機能にだけ電力が供給されています。 • 緑色：アプライアンスはメイン電源モードです。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。
6	<p>ユニット識別ボタンと LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 青：ユニット識別機能はアクティブです。 • 消灯：ユニット識別機能は非アクティブです。
7	<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動作状態になっています。次の 1 つ以上が原因の可能性があります。 <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"> • ブートに失敗した。 • 修復不能な CPU またはバスエラーが検出された。 • サーバが過熱状態にある。

コンポーネント	説明
8	<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。
9	<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ーが警告しきい値を超過しています。 • オレンジの点滅：1 つ以上の温度センサーが重大しきい値を超過しています。
10	<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。
11	<p>ネットワーク リンク アクティビティ LED。LED の状態とその説明：</p> <ul style="list-style-type: none"> • 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。 • 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 • 消灯：イーサネットリンクがアイドル状態です。
12	<p>KVM コネクタ USB 2.0 コネクタ X 2、VGA コネクタ X 1、シリアルコネクタ X 1 を装備した KVM ケーブルで使用します。</p>

図 2: アプライアンスの背面パネル



コンポーネント	説明
1	アース ラグの穴 (DC 電源装置の場合)
2	PCIe ライザー 1/スロット 1
3	PCIe ライザー 2/スロット 2
4	<p>電源装置 (最大 2 台、1+1 冗長) 各電源装置には、電源障害 LED と AC 電源 LED があります。</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 (たとえば、ファンの障害や過熱状態など)。 <p>AC 電源 LED の状態とその説明：</p> <ul style="list-style-type: none"> 緑の点灯：AC 電力供給も、DC 出力も OK。 緑の点滅：AC 電力供給は OK、DC 出力は使用できません。 消灯：電源装置に AC 電力が供給されていません。 <p>詳細については、「電力仕様」を参照してください。</p>

コンポーネント	説明
5	<p>10 Gbps クラスタポート（ポート 2、enp10so、ネットワークアダプタ 1）：これは、アプライアンスの mLOM スロットの Cisco Virtual Interface Card (VIC) 1227 の 2 番目の 10 Gbps ポートです。背面パネルにはポート 2とラベルが付いており、Maglev 設定ウィザードはそれを Enp10s0 およびネットワークアダプタ 1として識別します。このポートを、Cisco DNA Center クラスタ内の他のノードに接続しているスイッチに接続します。</p> <p>このポートには、リンクステータス（「ACT」）LED とリンク速度（「リンク」）LED があります。</p> <p>リンクステータス LED の状態とその説明：</p> <ul style="list-style-type: none"> • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 • 消灯：リンクが確立されていません。 <p>リンク速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 • 消灯：リンク速度は 100 Mbps 以下です。 <p>(注) エンタープライズポートとクラスタポートは、10 Gbps でのみ動作する必要があります。</p>

コンポーネント	説明
6	<p>10 Gbps エンタープライズポート（ポート 1、enp9s0、ネットワークアダプタ 1）：これは、アプライアンスの mLOM スロットの Cisco Virtual Interface Card (VIC) 1227 の最初の 10 Gbps ポートです。背面パネルにはポート 1とラベルが付いており、Maglev 設定ウィザードはそれを Enp9s0 および ネットワークアダプタ 4 として識別します。このポートを、Cisco DNA Center の管理対象のネットワーキング機器への IP 到達可能性があるスイッチに接続します。</p> <p>このポートには、リンクステータス（「ACT」）LED とリンク速度（「リンク」）LED があります。</p> <p>リンクステータス LED の状態とその説明：</p> <ul style="list-style-type: none"> • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 • 消灯：リンクが確立されていません。 <p>速度 LED の状態とその説明：</p> <ul style="list-style-type: none"> • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。 • 消灯：リンク速度は 100 Mbps 以下です。 <p>(注) Cisco DNA Center アプライアンスのエンタープライズポートとクラスタポートは、10 Gbps でのみ動作する必要があります。</p>
7	USB 3.0 ポート（2 個）

コンポーネント	説明
8	<p>1 Gbps CIMC ポート (M) : これは、2つの USB ポートの右側にある組み込みポートで、RJ45 シリアルポートの左側にあります。背面パネルには M というラベルが付いており、アプライアンスの CIMC GUI へのブラウザアクセスを有効にすると、IP アドレスが割り当てられます (「CIMC へのブラウザアクセスの有効化」を参照)。このポートは、Cisco DNA Center アプライアンスのシャーシおよびソフトウェアのアウトオブバンド (OOB) 管理用に予約されています。専用の OOB エンタープライズ管理ネットワークへのアクセスを提供するスイッチに接続します。</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 があります。リンクステータス LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 緑の点滅 : アクティブなリンクにトラフィックが存在します。 • 緑 : リンクはアクティブですが、トラフィックは存在しません。 • 消灯 : リンクが確立されていません。 <p>速度 LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 緑 : リンク速度は 1 Gbps です。 • オレンジ : リンク速度は 100 Mbps です。 • 消灯 : リンク速度は 10 Mbps 以下です。
9	シリアルポート (RJ-45 コネクタ)

コンポーネント	説明
10 日	<p>1 Gbps Cisco DNA Center GUI ポート (1、Enp1s0f0、ネットワークアダプタ 2) : これは、最初の Intel i350 1g GB イーサネット コントローラ ポートです。アプライアンスのマザーボードに組み込まれています。背面パネルには 1 とラベルが付いており、Maglev 設定ウィザードはそれを Enp1s0f0 と ネットワークアダプタ 2 として識別します。専用のエンタープライズ管理ネットワークへのアクセスを提供するスイッチに接続します。</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 があります。ステータス LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 緑の点滅 : アクティブなリンクにトラフィックが存在します。 • 緑 : リンクはアクティブですが、トラフィックは存在しません。 • 消灯 : リンクが確立されていません。 <p>速度 LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 緑 : リンク速度は 1 Gbps です。 • オレンジ : リンク速度は 100 Mbps です。 • 消灯 : リンク速度は 10 Mbps 以下です。
11	<p>1 Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ 3) : これは 2 番目の組み込み 1 Gbps イーサネット コントローラ ポートです。背面パネルには 2 とラベルが付いており、Maglev 設定ウィザードはそれを enp1s0f1 と ネットワークアダプタ 3 として識別します。このポートはオプションです。インターネット接続が 10 Gbps エンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ 4) 経由では実行できない場合に使用されます。</p> <p>このポートには、リンクステータス LED とリンク速度 LED があります。リンクステータス LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 緑の点滅 : アクティブなリンクにトラフィックが存在します。 • 緑 : リンクはアクティブですが、トラフィックは存在しません。 • 消灯 : リンクが確立されていません。 <p>速度 LED の状態とその説明 :</p> <ul style="list-style-type: none"> • 緑 : リンク速度は 1 Gbps です。 • オレンジ : リンク速度は 100 Mbps です。 • 消灯 : リンク速度は 10 Mbps 以下です。
12	<p>VGA ビデオポート (DB-15) このポートの周囲のパネル領域は青色です。</p>

コンポーネント	説明
13	青色 LED ロケータボタン

物理仕様

次の表に、アプライアンスの物理仕様を示します。

表 2: 物理仕様

説明	仕様
高さ	4.32 cm (1.7 インチ)
幅	43.0 cm (16.89 インチ) ハンドルを含めた場合： 48.2 cm (18.98 インチ)
奥行 (長さ)	75.6 cm (29.8 インチ) ハンドルを含めた場合： 78.7 cm (30.98 インチ)
機材設置で、前面に必要な最小隙間	76 mm (3 インチ)
機材設置で、横に必要な最小隙間	25 mm (1 インチ)
機材設置で、背面に必要な最小隙間	152 mm (6 インチ)
最大重量 (フル装備シャーシ)	17.2 kg (37.9 ポンド)

環境仕様

次の表に、アプライアンスの環境仕様を示します。

表 3: 環境仕様

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

説明	仕様
温度（非動作時）（アプライアンスの保管時または移送時）	-40 ~ 65 °C (-40 ~ 149 °F)
湿度（RH）（動作時）	10 ~ 90 % (28 °C (82 °F) 時、結露なし)
非動作時湿度	5 ~ 93 % (28 °C (82 °F) 時)
高度（動作時）	0 ~ 3000 m (0 ~ 10,000 フィート)
高度（非動作時）（アプライアンスの保管時または移送時）	0 ~ 12,192 m (0 ~ 40,000 フィート)
音響出力レベル、ISO7779 に基づく A 特性 LWA _d (B) を測定、23 °C (73 °F) での動作時	5.4
音圧レベル、ISO7779 に基づく A 特性 LpA _m (dBA) を測定、23 °C (73 °F) での動作時	37

電力仕様

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



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

表 4: AC 電源の仕様

説明	仕様
AC 入力電圧	公称範囲：100 ~ 120 VAC、200 ~ 240 VAC (範囲：90 ~ 132 VAC、180 ~ 264 VAC)
AC 入力周波数	公称範囲：50 ~ 60 Hz (範囲：47 ~ 63 Hz)
最大 AC 入力電流	100 VAC で 9.5 A 208 VAC で 4.5 A
最大入力電圧	950 VA @ 100 VAC

説明	仕様
PSU あたりの最大出力電力	770 W
最大突入電流	15 A (サブサイクル期間)
最大保留時間	12 ms @ 770 W
電源の出力電圧	12 VDC
電源スタンバイ電圧	12 VDC
効率評価	Climate Savers Platinum Efficiency (80Plus Platinum 認定)
フォーム ファクタ	RSP2
入力コネクタ	IEC320 C14

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



第 2 章

導入の計画

- [プランニング ワークフロー](#) (15 ページ)
- [Cisco DNA Center および Software-Defined Access \(SD-Access\) について](#) (16 ページ)
- [インターフェースケーブル接続](#) (17 ページ)
- [必要なサブネットおよび追加の IP アドレス](#) (20 ページ)
- [必要なインターネット URL と完全修飾ドメイン名](#) (25 ページ)
- [インターネットへのアクセスを保護する](#) (26 ページ)
- [必要なネットワーク ポート](#) (27 ページ)
- [必要な SD アクセス ポートおよびプロトコル](#) (29 ページ)
- [必要な設定情報](#) (39 ページ)
- [必要な初期設定情報](#) (40 ページ)

プランニング ワークフロー

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

Cisco DNA Center の設置および設定プロセスの概要を示すビデオシリーズについては、[このリンクをクリックしてください](#)。

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

表 5: 計画作業

ステップ	説明
1	スタンドアロン設置およびクラスタ設置で推奨されるケーブル接続とスイッチングの要件を確認します： インターフェースケーブル接続 。
2	アプライアンスの設定時に適用する IP アドレッシング、サブネット化、およびその他の IP トラフィック情報を収集します： 必要なサブネットおよび追加の IP アドレス 。

ステップ	説明
3	Webベースのリソースへのアクセスに必要なソリューションを準備します： 必要なインターネット URL と完全修飾ドメイン名 、インターネットへのアクセスを保護する。
4	Cisco DNA Center トラフィックのファイアウォールおよびセキュリティポリシーを再設定します： 必要なネットワーク ポート 。Cisco DNA Center を使用して SDA ネットワークを管理している場合は、「 必要な SD アクセス ポートおよびプロトコル 」も参照してください。
5	アプライアンスの設定時および初回のセットアップ時に使用される追加情報を収集します： 必要な設定情報 と 必要な初期設定情報 。

Cisco DNA Centerおよび Software-Defined Access (SD-Access) について

Cisco DNA Center を使用すると、シスコの Software-Defined Access ファブリックアーキテクチャ（別名 SD-Access または SDA）を採用しているネットワークを含めて、あらゆるタイプのネットワークを管理できます。この画期的な SDA アプローチは、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、設定、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。シスコの 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。

SDA 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 SDA 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。

- SDA と Cisco Digital Network Architecture の簡単な説明については、ホワイトペーパー『[Cisco Digital Network Architecture のビジョン：概要](#)』を参照してください。
- 通常のネットワークのアプローチと技術では不可能なソリューションを自動化するために、Cisco DNA Center が 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クの実現](#)』を参照してください。
- ネットワークで SDA を実装する方法を示す検証済みデザインについては、最新バージョンの『[シスコソフトウェア定義型アクセス設計ガイド](#)』を参照してください。
- SDA 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。
- ワイヤレス固有の設計ガイダンスについては、『[SD-Access ワイヤレス設計および導入ガイド](#)』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 および SDA 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およびサードパーティの製品およびソリューションが果たす役割については、『[Cisco DNA Design Zone](#)』を参照してください。
- その他の設計ガイド、導入ガイド、ホワイトペーパーについては、『[Cisco Design Zone](#)』を参照してください。

インターフェイスケーブル接続

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

- **(必須) 10 Gbps クラスタポート (ポート 2、enp10so、ネットワークアダプタ 1)** : これは、アプライアンスの mLOM スロットの VIC 1227 カードの左側のポートです。その目的は、Cisco DNA Center クラスタ内のマスターノードとアドオンノード間の通信を可能にすることです。このポートをクラスタ内の他のノードに接続しているスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

設定中、Maglev 設定ウィザードは、クラスタリンクオプションをインターフェイスに割り当てるまで続行できません。ポート enp10so をクラスタリンクとして指定することを推奨します。ただし、クラスタリンクとしてマークされたインターフェイスは、設定が完了した後は変更できないことに注意してください。後でクラスタリンクとしてマークされたインターフェイスを変更する必要がある場合は、再インストールが必要になります。将来的に 3 ノードクラスタへの拡張を可能にするために、IP アドレスを使用してクラスタポートを設定することを推奨します。また、クラスタリンクインターフェイスがスイッチポートに接続されており、稼働状態になっていることを確認します。

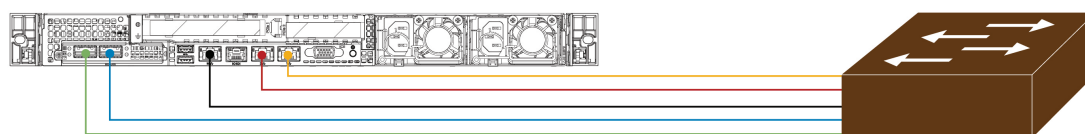
- **(オプション) 1 Gbps Cisco DNA Center GUI ポート (1、enp1s0f0、ネットワークアダプタ 2)** : このポートは、Cisco DNA Center グラフィック ユーザインターフェイスへのアクセスを提供します。その目的は、ユーザがアプライアンスでソフトウェアを使用できるようにすることです。このポートを、企業管理ネットワークに接続しているスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
- **(オプション) 1 Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ 3)** : このポートはオプションです。10 Gbps のエンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ 4) を使用してアプライアンスをインターネット (インターネットプロキシサーバを含む) に接続できない場合のみ使用してください。クラウドポートを使用する必要がある場合は、インターネットプロキシサーバに接続しているスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。
- **(必須) 10 Gbps エンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ 4)** : これは、アプライアンス mLOM スロットの VIC 1227 カードの右側のポートです。

その目的は、Cisco DNA Center のネットワークとの通信および管理を有効にすることです。このポートを、エンタープライズネットワークに接続しているスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

- (オプション、ただし強く推奨) **1 Gbps CIMC ポート (M)** : このポートは、CIMC アウトオブバンドアプライアンス管理インターフェイスとそのグラフィック ユーザインターフェイスへのブラウザアクセスを提供します。その目的は、アプライアンスとそのハードウェアを管理できるようにすることです。このポートを、企業管理ネットワークに接続してスイッチにケーブル接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

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

図 3: シングルノードクラスタの推奨される配線

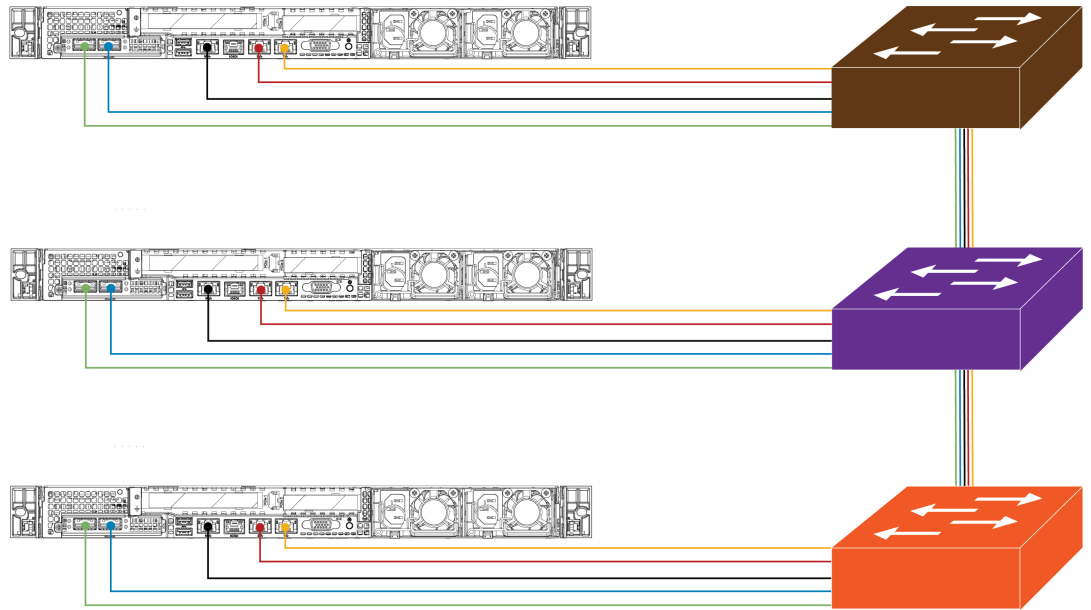


凡例

- 10 Gbps クラスターポート
(ポート 2、enp10s0、ネットワーク アダプタ 1)
- 10 Gbps エンタープライズポート
(ポート 1、enp9s0、ネットワーク アダプタ 4)
- 1 Gbps Cisco DNA Center GUI ポート
(1、enp1s0f0、ネットワーク アダプタ 2)
- 1 Gbps クラウドポート
(2、enp1s0f1、ネットワーク アダプタ 3)
- 1 Gbps CIMC ポート (M)

次の図は、3 ノード Cisco DNA Center クラスタの推奨される接続を示しています。3 ノードクラスタ内の各ノードの接続は 1 つ以外すべて、シングルノードクラスタの場合と同じであり、同じポートを使用します。例外はクラスターポート (ポート 2、enp10so、ネットワークアダプタ 1) であり、これは 3 ノードクラスタ内の各ホストが他のホストと通信できるようにするために必要です。

図 4:3 ノードクラスタの推奨される配線



凡例

- 10 Gbps クラスタポート
(ポート 2、enp10s0、ネットワーク アダプタ 1)
- 10 Gbps エンタープライズポート
(ポート 1、enp9s0、ネットワーク アダプタ 4)
- 1 Gbps CIMC ポート (M)
- 1 Gbps Cisco DNA Center GUI ポート
(1、enp1s0f0、ネットワーク アダプタ 2)
- 1 Gbps クラウドポート
(2、enp1s0f1、ネットワーク アダプタ 3)

439812

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

各ポートの詳細については、[前面パネルと背面パネル](#)にある Cisco UCS C220 M4 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、両方のポートで次のメディアタイプのみがサポートされていることに注意してください。

- SFP-10G-USR (ウルトラショートレンジ、MMF)
- SFP-10G-SR (ショートレンジ、MMF)
- SFP-10G-LR (ロングレンジ、SMF)
- SFP-H10GB-CU1M (Twinax ケーブル、パッシブ、1 m)

- SFP-H10GB-CU3M (Twinax ケーブル、パッシブ、3 m)
- SFP-H10GB-CU5M (Twinax ケーブル、パッシブ、5 m)
- SFP-H10GB-CU7M (Twinax ケーブル、パッシブ、7 m)
- SFP-H10GB-ACU7M (Twinax ケーブル、アクティブ、7 m)

必要なサブネットおよび追加の IP アドレス

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するのに十分な IP アドレスがネットワークにあることを確認する必要があります。アプライアンスをシングルノードクラスタとしてインストールするか、3 ノードクラスタのマスターまたはアドオンノードとしてインストールするかによって、次のアプライアンスポート (NIC) アドレスが必要になります。

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



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

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

1. [クラスタ仮想IPアドレス (Cluster Virtual IP Addresses)] : クラスタごとに設定されたネットワーク インターフェイスごとに 1 つの仮想 IP (VIP) アドレス。この要件は、3 ノードクラスタと、将来 3 ノードクラスタに変換される可能性のある単一ノードクラスタに適用されます。設定するネットワーク インターフェイスごとに VIP を指定する必要があります。各 VIP は、対応する設定済みインターフェイスの IP アドレスと同じサブネットからのものである必要があります。各アプライアンスには、エンタープライズ、クラスタ、管

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

次の点に注意してください。

- 単一ノード設定で、今後3ノードクラスタに変換する予定がない場合は、仮想IPアドレスを指定する必要はありません。ただし、これを行う場合は、設定されているすべてのネットワーク インターフェイスに仮想IPアドレスを指定する必要があります (3ノードクラスタの場合と同様)。
 - 単一ノードクラスタのクラスタ内リンクがダウンすると、管理インターフェイスとエンタープライズ インターフェイスに関連付けられている仮想IPアドレスもダウンします。このような状況が発生すると、Cisco DNA Center はクラスタ内リンクが復元されるまで使用できなくなります (SWIMとISEの統合は動作しなくなり、NDP コレクタから情報を収集できないため、アシユアランスデータは表示されません)。
2. [デフォルトゲートウェイIPアドレス (Default Gateway IP Address)]: ネットワークの優先デフォルトゲートウェイのIPアドレス。他のルートがトラフィックに一致しない場合、トラフィックはこのIPアドレスを介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。
 3. [DNSサーバのIPアドレス (DNS Server IP Addresses)]: 1つ以上のネットワークの優先DNSサーバのIPアドレス。設定時に、複数のDNSサーバのIPアドレスとネットマスクを、スペースで区切ったリストとして入力することによってそれらを指定できます。
 4. (オプション) [スタティックルートアドレス (Static Route Addresses)]: 1つ以上のスタティックルートのIPアドレス、サブネットマスク、およびゲートウェイ。設定時に、複数のスタティックルートのIPアドレス、ネットマスク、およびゲートウェイを、スペースで区切ったリストとして入力することによってそれらを指定できます。

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

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

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

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

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

6. [サービスサブネット (Services Subnet)] : アシユアランス、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。専用 IPv4 サービスサブネットは、Cisco DNA Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりすることはできません。サブネットの最小サイズは 21 ビットです。IPv4 サービスサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。

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

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



重要

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

7. [クラスタサービスサブネット (Cluster Services Subnet)] : データベースアクセス、メッセージバスなどのインフラストラクチャ サービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。専用 IPv4 クラスタサービスサブネットは、Cisco DNA Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりすることはできません。サブネットの最小サイズは 21 ビットです。IPv4 クラスタサービスサブネットは、次のアド

レス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。

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

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

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



重要

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

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

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

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

や機能を追加できるようにするために、アドレス空間の要件は最初は意図的に大きく維持されています。

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

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

インターフェイス名とウィザードの設定順序

インターフェイス名と、これらのインターフェイスを Maglev 設定ウィザードで設定する順序は、次の表に示すように、Cisco DNA Center アプライアンスの M4 および M5 シャーシモデルによって異なります。

表 6: インターフェイス名とウィザードの設定順序

機能	Cisco DNA Center アプライアンス シャーシモデル	インターフェイス名	Maglev 設定ウィザードでの設定順序
[クラスタ (Cluster)]: アプライアンスをクラスタノードにリンクします。	M4	enp10s0	ネットワークアダプタ #1
	M5	enp94s0f1	ネットワークアダプタ #4
[管理 (Management)]: 管理ネットワークから Cisco DNA Center GUI にアクセスできます。	M4	enp1s0f0	ネットワークアダプタ #2
	M5	eno1	ネットワークアダプタ #1
[クラウド (Cloud)]: この目的で別のインターフェイスを使用できない場合にインターネットアクセスを提供します。	M4	enp1s0f1	ネットワークアダプタ #3
	M5	eno2	ネットワークアダプタ #2
[エンタープライズ (Enterprise)]: アプライアンスをエンタープライズネットワークにリンクします。	M4	enp9s0	ネットワークアダプタ #4
	M5	enp94s0f0	ネットワークアダプタ #3

必要なインターネット URL と完全修飾ドメイン名

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

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

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

表 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
Cシステムおよびアプリケーションパッケージソフトウェアにアップデートをダウンロードし、製品チームにユーザからのフィードバックを送信します。	推奨 : * ciscoconnectdna.com:443 ¹ ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 <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 パッケージの更新	https://* ciscoconnectdna. com/*
スマートアカウントおよび SWIM ソフトウェアのダウンロード	https://apx.cisco.com https://cloudsso.cisco.com/as/token.oauth2 https://* .cisco.com/*
ユーザフィードバック	https://dnacenter.uservoice.com
Cisco Meraki との統合	推奨 : * .meraki.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 <ul style="list-style-type: none"> • dashboard.meraki.com:443 • api.meraki.com:443 • n63.meraki.com:443

目的	Cisco DNA Center がアクセスする必要がある URL と FQDN
Cisco.com とシスコ スマートライセンスとの統合	<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
サイトとロケーションマップで正確な情報をレンダリング	<ul style="list-style-type: none"> • www.mapbox.com • *.tiles.mapbox.com/*:443. プロキシの場合、宛先は *.tiles.mapbox.com/* です。

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によって監視および保守されます。

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 Cisco.com およびその他の URL にアクセスして、ソフトウェアアップデート、ライセンス、およびデバイスソフトウェアをダウンロードしたり、最新のマップ情報、ユーザフィードバックなどを提供したりするように設定されています。

これらの目的でインターネット接続を提供することは必須要件です。

HTTPS プロキシサーバを使用することは、リモート URL に安全にアクセスするための信頼性の高い方法です。[必要なインターネット URL と完全修飾ドメイン名](#)に記載されている URL に必要とするアクセスをアプライアンスに提供するには、HTTPS プロキシサーバを使用するこ

とをお勧めします。設置時に、この目的で使用するプロキシサーバの URL とポート番号を、プロキシのログインクレデンシャルとともに入力するように求められます（プロキシが必要な場合）。

このリリースでは、アプライアンスは HTTP を介したプロキシサーバとの通信のみをサポートしています。HTTPS プロキシサーバは、ネットワーク内の任意の場所に配置できます。プロキシサーバは HTTPS を使用してインターネットと通信できますが、アプライアンスは HTTP 経由でプロキシサーバと通信します。このような理由から、設定時にプロキシを設定する場合は、必ずプロキシの HTTP ポートを指定する必要があります。

何らかの理由で設定後にプロキシ設定を変更する必要がある場合は、GUI インターフェイスを使用して行うことができます。

必要なネットワーク ポート

次の表に、アプライアンスが使用する既知のネットワークサービスポートを示します。これらのポートが、ファイアウォール設定またはプロキシゲートウェイのどちら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している必要があります。詳細については、「[必要な SD アクセス ポートおよびプロトコル](#)」を参照してください。



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

表 8: ポート : 着信トラフィック

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

表 9: ポート : 発信トラフィック

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

ポート番号	許可されたトラフィック	プロトコル (TCPまたはUDP)
23	Telnet (ネットワークデバイスへ)	TCP
53	DNS	UDP
80	<p>ポート 80 は、発信プロキシ設定に使用できます。</p> <p>さらに、プロキシが設定ウィザードによって設定されている場合 (プロキシがすでにネットワークに使用されている場合)、8080 などの他の一般的なポートも使用できます。</p> <p>シスコでサポートされている証明書およびトラストプールにアクセスするには、アプライアンスから次の URL にあるシスコのアドレスへの発信 IP トラフィックを許可するようにネットワークを設定できます。</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	PxGrid の ISE XMP	TCP
9060	ISE ERS の API トラフィック	TCP

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

表 10: ポート : IP トラフィック

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

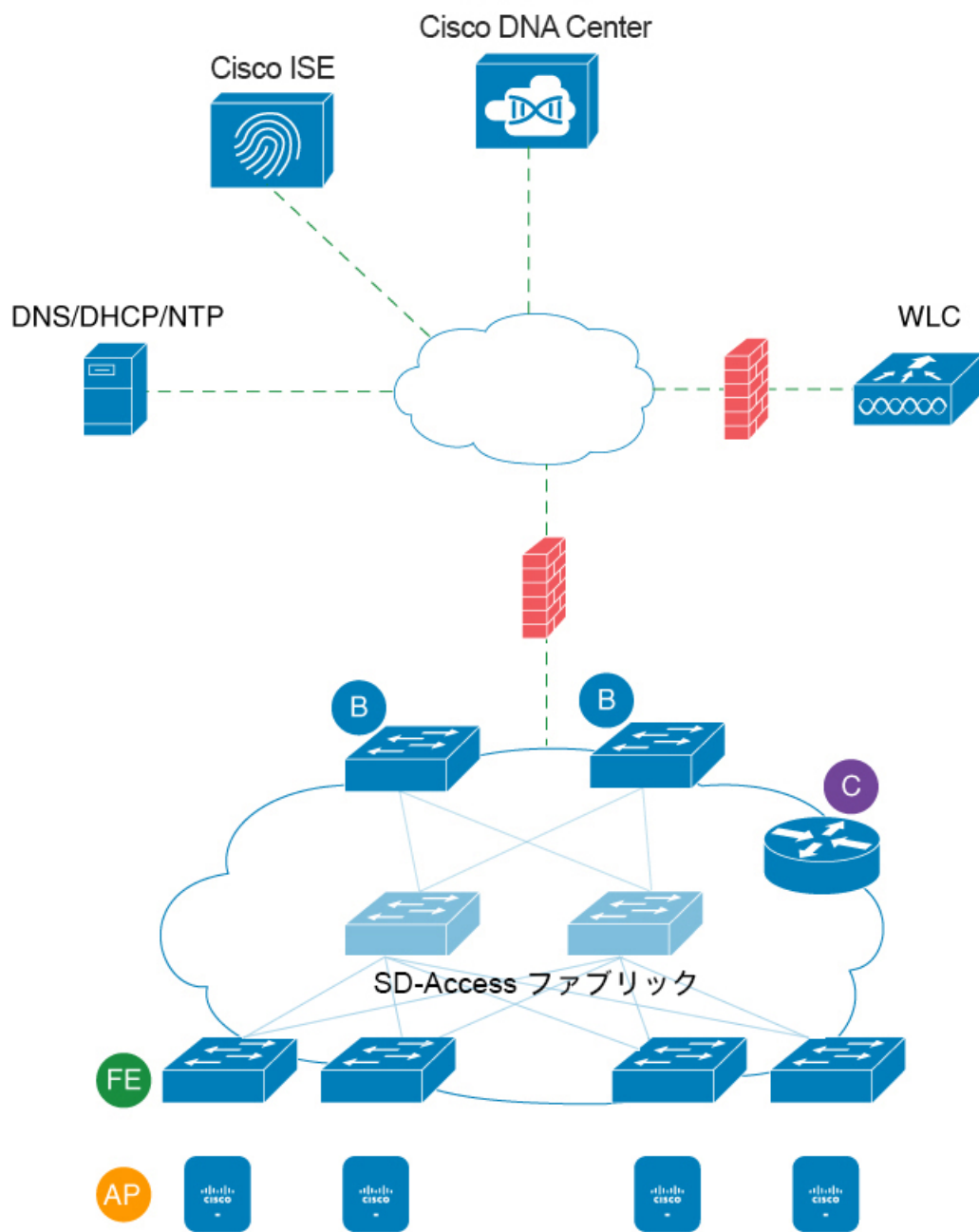
プロトコル (TCPまたはUDP)	ポート番号	トラフィック タイプ
TCP	443	HTTPS
UDP	67	bootps
UDP	123	NTP
UDP	162	SNMP

さらに、アプライアンスから次の URL にあるシスコのアドレスへの発信 IP トラフィックを許可するようにネットワークを設定できます。<https://www.cisco.com/security/pki/アプライアンス> は、上記の URL に記載されている IP アドレスを使用して、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します。

必要な SD アクセス ポートおよびプロトコル

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

図 5: SDA ファブリック インフラストラクチャ



355637

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

表 11: Cisco DNA Center トラフィック

送信元ポート ²	ソース	宛先ポート	宛先	説明
すべて	Cisco DNA Center	UDP 53	DNS サーバ	Cisco DNA Center から DNS サーバへ
すべて	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へ (SSH 用)
すべて	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へ (TELNET 用)
すべて	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へ (SNMP デバイス検出用)
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へ (SNMP デバイス検出用)
すべて	Cisco DNA Center	TCP 443	ファブリックア ンダーレイ	Cisco DNA Center からファブリック スイッチへ (ソフトウェアア ップグレード用) (プロキシがない 場合はインターネットにも)
すべて	Cisco DNA Center	TCP 80	ファブリックア ンダーレイ	Cisco DNA Center からファブリック スイッチへ (PnP 用) (プロキ シがない場合はインターネットに も)
すべて	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 スイッチへ (Netconf 用) (SDA 組み込みワイヤレス)
UDP 123	Cisco DNA Center	UDP 123	ファブリックア ンダーレイ	Cisco DNA Center からファブリック スイッチへ (LAN の自動化中 の初回時間用)
すべて	Cisco DNA Center	UDP 123	NTP サーバ (NTP Server)	Cisco DNA Center から NTP サー バへ
すべて	Cisco DNA Center	TCP 22、 UDP 161	WLC	Cisco DNA Center から WLC へ

ICMP	Cisco DNA Center	ICMP	WLC	Cisco DNA Center から WLC へ
すべて	Cisco DNA Center	TCP 80、TCP 443	AP	Cisco DNA Center からセンサーおよびアクティブセンサーとしての AP へ (Cisco Aironet 1800S)
すべて	Cisco DNA Center	TCP 32626	AP	Cisco DNA Center から AP へ (GRPC 用)

² のクラスタ、PKI、SFTP サーバ、および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 12: インターネット接続トラフィック

送信元ポート	ソース (Source)	宛先ポート	宛先 (Destination)	説明 (Description)
すべて	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
すべて	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
すべて	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
すべて	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
すべて	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
すべて	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
すべて	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
すべて	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
すべて	Cisco DNA Center	TCP 443	apiconsole.cisco.com	CSSM スマートライセンスの API

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

表 13: SDA ファブリック アンダーレイ トラフィック

送信元ポート ³	ソース	宛先ポート	宛先	説明
UDP 68	ファブリックアンダーレイ	UDP 67	DHCP サーバ	ファブリックスイッチおよびルータと DHCP サーバの間で、ファブリックエッジノードによって開始される DHCP リレーパケット用に使用されます。
すべて	ファブリックアンダーレイ	TCP 80	Cisco DNA Center	ファブリックスイッチおよびルータのループバック IP と Cisco DNA Center の間で PnP 用に使用

すべて	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および ルータのループバック IP と Cisco DNA Center の間でイメー ジのアップグレードのために 使用
すべて	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および ルータのループバック IP と Cisco DNA Center の間で SNMP トラップのために使用
すべて	ファブリックア ンダーレイ	UDP 514	Cisco DNA Center	ファブリックスイッチおよび ルータと Cisco DNA Center の 間でアシュアランス用に使用
すべて	ファブリックア ンダーレイ	UDP 6007	Cisco DNA Center	ファブリックルータと Cisco DNA Center の間で NetFlow 用 に使用
すべて	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と Cisco DNA Center の間で、LAN 自動 化の実行時に使用
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および ルータのループバックと Cisco DNA Center の間で SNMP デバ イス検出のために使用
UDP 161	ファブリックア ンダーレイ	すべて	Cisco DNA Center	ファブリックスイッチおよび ルータのループバックと Cisco DNA Center の間で SNMP デバ イス検出のために使用
すべて	ファブリックア ンダーレイ	UDP 53	DNS サーバ	ファブリックスイッチおよび ルータと DNS サーバの間で名 前解決のために使用
TCP およ び UDP 4342	ファブリックア ンダーレイ	TCP および UDP 4342	ファブリッ クルータお よびスイッ チ	LISP カプセル化制御メッセー ジ
TCP およ び UDP 4342	ファブリックア ンダーレイ	すべて	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

すべて	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)
すべて	ファブリックア ンダーレイ	UDP 1645/1646/1812/1813	ISE	ファブリックスイッチおよび ルータのループバック IP と ISE の間で RADIUS 用に使用
ICMP	ファブリックア ンダーレイ	ICMP	ISE	ファブリックスイッチおよび ルータと ISE の間でトラブル シューティングのために使用
UDP 1700/3799	ファブリックア ンダーレイ	すべて	ISE	ファブリックスイッチと ISE の間で CoA 用に使用
すべて	ファブリックア ンダーレイ	UDP 123	NTP サーバ (NTP Server)	ファブリックスイッチおよび ルータのループバック IP と NTP サーバの間で使用
すべて	control-plane	UDP および TCP 4342/4343	WLC	コントロールプレーンのルー プバック IP と WLC の間でファ ブリック対応ワイヤレス用に 使用

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

表 14: ワイヤレス LAN コントローラ (WLC) トラフィック

送信元ポート	ソース	宛先ポート	宛先	説明
UDP 5246/5247/5248	WLC	すべて	AP IP プール	WLC と AP サブネットの間で CAPWAP 用に使用
ICMP	WLC	ICMP	AP IP プール	WLC と Ping を許可する AP の間 でトラブルシューティングのため に使用
すべて	WLC	UDP 69/5246/5247 TCP 22	AP IP プール	WLC と AP サブネットの間で CAPWAP 用に使用
すべて	WLC	UDP および TCP 4342/4343	コントロールプ レーン	WLC とコントロールプレーン ループバック IP の間で使用
すべて	WLC	TCP 32222	Cisco DNA Center	WLC と Cisco DNA Center の間 でデバイス検出のために使用
UDP 161	WLC	すべて	Cisco DNA Center	WLC と Cisco DNA Center の間 で SNMP 用に使用

すべて	WLC	UDP 162	Cisco DNA Center	WLC と Cisco DNA Center の間で SNMP トラップのために使用
すべて	WLC	TCP 16113	MSE および Spectrum Expert	WLC と MSE および Spectrum Expert の間で NMSP 用に使用
ICMP	WLC	ICMP	Cisco DNA Center	WLC から、トラブルシューティングに向けた Ping の許可に使用
すべて	HA サーバ	TCP 1315	Cisco DNA Center	データベースサーバ HA (QoS)
すべて	HA サーバ	TCP 1316 ~ 1320	Cisco DNA Center	HA データベースポート
すべて	HA Web サーバ	TCP 8082	Cisco DNA Center	HA Web サーバのヘルスマニタポート
すべて	WLC および各種 Syslog サーバ	UDP 514	WLC	Syslog (オプション)
すべて	WLC	UDP 53	DNS サーバ	WLC と DNS サーバの間で使用
すべて	WLC	TCP 443	ISE	WLC と ISE の間でゲスト SSID Web 認証のために使用
すべて	WLC	UDP 1645、1812	ISE	WLC と ISE の間で RADIUS 認証のために使用
すべて	WLC	UDP 1646、1813	ISE	WLC と ISE の間で RADIUS アカウンティングのために使用
すべて	WLC	UDP 1700、3799	ISE	WLC と ISE の間で RADIUS CoA 用に使用
ICMP	WLC	ICMP	ISE	WLC と ISE ICMP の間でトラブルシューティングのために使用
すべて	WLC	UDP 123	NTP サーバ	WLC と NTP サーバの間で使用

表 15: ファブリック対応ワイヤレスアクセスポイント (AP) の IP プールトラフィック

送信元ポート	ソース	宛先ポート	宛先	説明
UDP 68	AP IP プール	UDP 67	DHCP サーバ	AP IP プールと DHCP サーバの間で使用
ICMP	AP IP プール	ICMP	DHCP サーバ	AP IP プールと ICMP の間でトラブルシューティングのために使用

すべて	AP IP プール	514	複数ページ	Syslog : 宛先設定可能。デフォルトは 255.255.255.255
すべて	AP IP プール	UDP 69/5246/5247/5248	WLC	AP IP プールと WLC の間で CAPWAP 用に使用
ICMP	AP IP プール	ICMP	WLC	AP IP プールから WLC に送信。トラブルシューティングのために Ping を許可

表 16: Identity Services Engine (ISE) トラフィック

送信元ポート ⁴	ソース (Source)	宛先ポート	宛先 (Destination)	説明 (Description)
すべて	ISE	TCP 64999	境界	ISE とボーダーノードの間で SXP 用に使用
すべて	ISE	UDP 514	Cisco DNA Center	ISE と Syslog サーバ (Cisco DNA Center) の間で使用
UDP 1645/1646/1812/1813	ISE	すべて	ファブリックアンダーレイ	ISE とファブリックスイッチおよびルータの間で RADIUS および認証用に使用
すべて	ISE	UDP 1700/3799	ファブリックアンダーレイ	ISE とファブリックスイッチおよびルータのループバック IP の間で気付アドレス用に使用
ICMP	ISE	ICMP	ファブリックアンダーレイ	ISE とファブリックスイッチの間でトラブルシューティングのために使用
すべて	ISE	UDP 123	NTP サーバ (NTP Server)	ISE と NTP サーバの間で使用
UDP 1812/1645/1813/1646	ISE	すべて	WLC	ISE と WLC の間で RADIUS 用に使用
ICMP	ISE	ICMP	WLC	ISE と WLC の間でトラブルシューティングのために使用

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

表 17: DHCP サーバトラフィック

送信元ポート	ソース	宛先ポート	宛先	説明
UDP 67	DHCP サーバ	UDP 68	AP IP プール	DHCP サーバとファブリック AP の間で使用

ICMP	DHCP サーバ	ICMP	AP IP プール	トラブルシューティング用の ICMP : ファブリックと 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 とファブリックスイッチおよびルータの間で使用
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 : ファブリックと DHCP の間で使用
UDP 67	DHCP サーバ	UDP 68	ユーザ IP プール	DHCP サーバとファブリックスイッチおよびルータの間で使用
ICMP	DHCP サーバ	ICMP	ユーザ IP プール	トラブルシューティング用の ICMP : ユーザと DHCP の間で使用

表 18: NTP サーバトラフィック

送信元ポート	ソース	宛先ポート	宛先	説明
UDP 123	NTP サーバ (NTP Server)	すべて	ISE	NTP サーバと ISE の間で使用
UDP 123	NTP サーバ (NTP Server)	すべて	Cisco DNA Center	NTP サーバから Cisco DNA Center
UDP 123	NTP サーバ (NTP Server)	すべて	ファブリックアンダーレイ	NTP サーバとファブリックスイッチおよびルータのループバックの間で使用
UDP 123	NTP サーバ (NTP Server)	すべて	WLC	NTP サーバと WLC の間で使用

表 19: DNS サーバトラフィック

送信元ポート	ソース (Source)	宛先ポート	宛先 (Destination)	説明 (Description)
UDP 53	DNS サーバ	すべて	ファブリックアンダーレイ	DNS サーバとファブリックスイッチの間で使用
UDP 53	DNS サーバ	すべて	WLC	DNS サーバと WLC の間で使用

必要な設定情報

アプライアンスの設定時に、必要なサブネットおよび追加の IP アドレスに加えて、次の情報を入力するように求められます。

1. [Linux ユーザ名 (Linux User Name)] : これは **maglev** です。このユーザ名は、マスターノードとアドオンノードの両方を含む、クラスタ内のすべてのアプライアンスで同じであり、変更することはできません。
2. [Linux パスワード (Linux Password)] : Linux ユーザ名 **maglev** のパスワードを指定します。このパスワードは、Linux コマンドラインを使用して各アプライアンスへのセキュアなアクセスを保証します。選択した場合は、クラスタ内の各アプライアンスの Linux ユーザ名 **maglev** ごとに異なる Linux パスワードを割り当てることができます。

デフォルト値はないため、Linux パスワードは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。

- 8 文字以上
- タブまたは改行を「含まない」
- 次のカテゴリのうち 3 種類以上の文字を含む。
 - 大文字の英字
 - 小文字の英字
 - 数字
 - 特殊文字 (! や # など)

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

3. [パスワード生成シード (Password Generation Seed)] (オプション) : Linux パスワードを作成する代わりに、シードフレーズを入力し、[パスワードの生成 (Generate Password)] を押すことができます。Maglev 設定ウィザードは、そのシードフレーズを使用してランダムかつ安全なパスワードを生成します。[自動生成パスワード (Auto Generated Password)] フィールドを使用して、生成されたパスワードをさらに編集できます。
4. [管理者パスフレーズ (Administrator Passphrase)] : クラスタ内の Cisco DNA Center への Web アクセスに使用されるパスワードを指定します。これはスーパーユーザアカウント **admin** のパスワードであり、初めて Cisco DNA Center にログインするときに使用します (「初回ログイン」を参照)。安全であることを確認するため、初回ログイン時にこのパスワードを変更するように求められます。

デフォルト値はないため、このパスワードは作成する必要があります。管理者のパスフレーズは、上記で説明した Linux パスワードと同じ要件を満たす必要があります。

5. [CIMCユーザパスワード (CIMC User Password)] : CIMC グラフィック ユーザ インターフェイスへのアクセスに使用するパスワードを指定します。工場出荷時のデフォルトは *password* ですが、Web ブラウザ経由でアクセスするために CIMC を初回セットアップするときに変更するように求められます (「[CIMC へのブラウザアクセスの有効化](#)」を参照)。

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

必要な初期設定情報

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

1. [新しい管理者のスーパーユーザパスワード (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。スーパーユーザパスワードをリセットすると、運用上のセキュリティが向上します。これは、たとえば、Cisco DNA Center アプライアンスを設置して設定した企業スタッフが Cisco DNA Center のユーザまたは管理者ではない場合に特に重要です。
2. [Cisco.com ログイン情報 (Cisco.com Credentials)] : ソフトウェアのダウンロードを登録し、電子メールでシステム通信を受信するために組織が使用する Cisco.com ユーザ ID とパスワード。
3. [Cisco スマートアカウントのログイン情報 (Cisco Smart Account Credentials)] : 組織がデバイスおよびソフトウェアライセンスの管理に使用する Cisco.com スマートアカウントのユーザ ID とパスワード。
4. [IP アドレスマネージャの URL とログイン情報 (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、および管理者パスワード。現在のリリースでは、InfoBlox または Bluecat がサポートされています。
5. [プロキシ URL、ポート、ログイン情報 (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、およびその他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、およびユーザパスワード。
6. [ユーザ (Users)] **Cisco DNA Center** : 作成する新しい Cisco DNA Center ユーザのユーザ名、パスワード、および権限の設定。シスコでは、通常の Cisco DNA Center のすべての操作に対して、これらの新しいユーザアカウントのいずれかを常に使用することを推奨して

います。Cisco DNA Center の再設定や、スーパーユーザ権限が明示的に必要なその他の操作を除き、管理者スーパーユーザアカウントを使用することは避けてください。

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

また、残りのセットアップタスクを完了するために次の情報が必要になります。これは、初回ログイン後に実行できます。

1. [ISEサーバのIPとログイン情報 (ISE Server IP and Credentials)] : Cisco Identify Services Engine (ISE) サーバの IP アドレス、管理ユーザ名、およびパスワードが必要です。これらは、「[Cisco ISE との統合 Cisco DNA Center](#)」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 とデータを共有する設定を行うために必要です。
2. [認証およびポリシーサーバ情報 (Authorization and Policy Server Information)] : 認証およびポリシーサーバとして Cisco ISE を使用している場合は、上記の ISE の統合と同じ情報に加えて、ISE CLI ユーザ名、CLI パスワード、サーバ FQDN、サブスクライバ名 (cdnac など)、ISE SSH キー (オプション)、プロトコル選択 (RADIUS または TACACS)、認証ポート、アカウンティングポート、および再試行/タイムアウト設定が必要です。

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

この情報を使用して、選択した認証およびポリシーサーバと Cisco DNA Center を統合します。これについては、「[認証サーバとポリシーサーバの設定](#)」で説明しています。
3. [SNMPの再試行とタイムアウト値 (SNMP Retry and Timeout Values)] : 「[SNMP プロパティの設定](#)」で説明されているように、デバイスのポーリングとモニタリングをセットアップするために必要です。



第 3 章

アプライアンスの設置

- [アプライアンスのインストールワークフロー](#) (43 ページ)
- [アプライアンスを開梱して点検](#) (45 ページ)
- [設置に関する警告とガイドラインの確認](#) (45 ページ)
- [ラック要件の確認](#) (47 ページ)
- [アプライアンスの接続および電源投入](#) (47 ページ)
- [LED の確認](#) (48 ページ)

アプライアンスのインストールワークフロー

次の表に、物理的な設置タスクとその実行順序を詳しく説明します。設置する Cisco DNA Center アプライアンスごとに、次の手順を実行します。最初のマスターノードを設定する前に、必ずすべてのアプライアンスを設置してください。

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

Cisco DNA Center アプライアンスのボックス化解除、設置、および設定プロセスを示す[ビデオ](#)については、[このリンクをクリックしてください](#)。

表 20: Cisco DNA Center アプライアンスの設置タスク

ステップ	説明
1	<p>設定およびセットアップ時に提供する必要がある情報の収集など、導入計画の要件を確認して対処します。</p> <ul style="list-style-type: none"> • Cisco DNA Centerおよび Software-Defined Access (SD-Access) について • インターフェイスクーブル接続 • 必要なサブネットおよび追加の IP アドレス • 必要なインターネット URL と完全修飾ドメイン名 • インターネットへのアクセスを保護する • 必要なネットワーク ポート • 必要な設定情報 • 必要な初期設定情報
2	<p>アプライアンスの機能と仕様を確認します。</p> <ul style="list-style-type: none"> • 機能の概要 • 前面パネルと背面パネル • 物理仕様 • 環境仕様 • 電力仕様
3	<p>アプライアンスを開梱します: アプライアンスを開梱して点検</p>
4	<p>アプライアンスに関する操作上の警告とガイドラインを確認します: 設置に関する警告とガイドラインの確認</p>
5	<p>ラックにアプライアンスを設置します: ラック要件の確認</p>
6	<p>アプライアンスに電源を接続し、電源をオンにします: アプライアンスの接続および電源投入</p>
7	<p>前面および背面パネルの LED をチェックして、アプライアンスが機能していることを確認します: LED の確認</p>

アプライアンスを開梱して点検



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



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



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

- ステップ 1** 段ボール箱からアプライアンスを取り出します。梱包材はすべて保管しておいてください。
- ステップ 2** カスタマー サービス担当者から提供された機器リストと梱包品の内容を照合します。すべての品目が揃っていることを確認してください。
- ステップ 3** 破損の有無を調べ、内容品の間違いや破損がある場合には、カスタマー サービス担当者に連絡してください。次の情報を用意しておきます。
- 発送元の請求書番号（梱包明細を参照）
 - 破損している装置のモデルとシリアル番号
 - 破損状態の説明
 - 破損による設置への影響

設置に関する警告とガイドラインの確認



警告 システムの過熱を防ぐため、最大推奨周囲温度の 35°C（95°F）を超えるエリアで操作しないでください。ステートメント 1047



警告 いつでも装置の電源を切断できるように、プラグおよびソケットにすぐ手が届く状態にしておいてください。ステートメント 1019



警告 この製品は、設置する建物にショート（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 機器の取り付けは各地域および各国の電気規格に適合する必要があります。ステートメント 1074



注意 アプライアンスを取り付ける際は、適切なエアフローを確保するために、レールキットを使用する必要があります。レールキットを使用せずに、ユニットを別のユニットの上に物理的に置く、つまり積み重ねると、アプライアンスの上部にある通気口がふさがれ、過熱したり、ファンの回転が速くなったり、電力消費が高くなったりする原因となる可能性があります。アプライアンスをラックに取り付けるときは、これらのレールによりアプライアンス間で必要な最小の間隔が提供されるので、レールキットにアプライアンスをマウントすることを推奨します。レールキットを使用して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無停電電源装置（UPS）タイプは使用しないでください。このタイプの UPS は、Cisco UCS などのシステムに使用すると、データトラフィックパターンの変化によって入力電流が大きく変動し、動作が不安定になるおそれがあります。

アプライアンスを設置する際には、次のガイドラインに従ってください。

- アプライアンスを設置する前に、設置場所を検討して準備します。設置場所を計画する際に推奨される作業については、『[Cisco UCS サイト計画および準備作業 \(Cisco UCS Site Preparation Guide\)](#)』を参照してください。
- アプライアンスの周囲に、保守作業および適切な通気のための十分なスペースがあることを確認します。このアプライアンスでのエアフローは、前面から背面に流れます。
- 設置場所の空調が、「[環境仕様](#)」に記載された温度要件に適合していることを確認します。
- キャビネットまたはラックが、「[ラック要件の確認](#)」に記載された要件に適合していることを確認します。
- 設置場所の電源が、「[電力仕様](#)」に記載された要件に適合していることを確認します。使用可能な場合は、電源障害に備えて UPS を使用してください。

ラック要件の確認

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

- 標準的な 19 インチ (48.3 cm) 幅 4 支柱 EIA ラック (ANSI/EIA-310-D-1992 のセクション 1 に準拠した英国ユニバーサル ピッチに適合するマウント支柱付き)。
- 付属のスライド レールを使用する場合、ラック支柱の穴は、0.38 インチ (9.6 mm) の正方形、0.28 インチ (7.1 mm) の丸形、#12-24 UNC、または #10-32 UNC になります。
- サーバあたりの縦方向の最小ラック スペースは、1 RU、つまり 1.75 インチ (44.45 mm) である必要があります。

アプライアンスの接続および電源投入

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

ステップ 1 付属の電源コードをアプライアンスの各電源装置に接続してから、接地された 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。

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

電源ステータスは、次のように電源ステータス LED で確認できます。

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

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

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

次のタスク

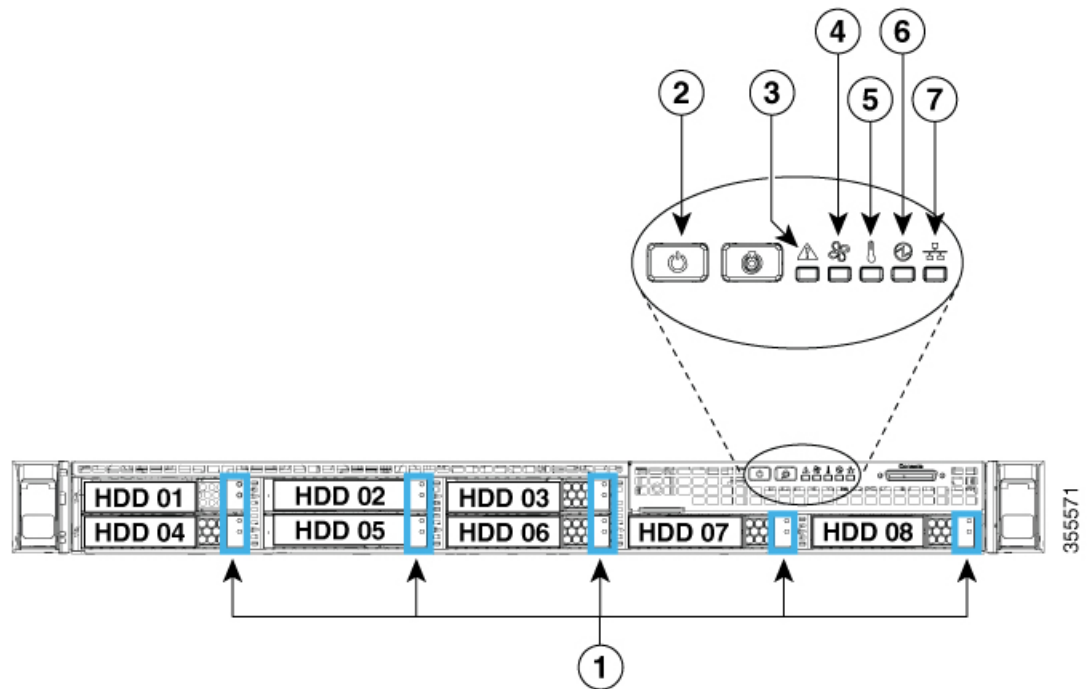
「[LED の確認](#)」で説明されている手順に従って続行します。

LED の確認

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

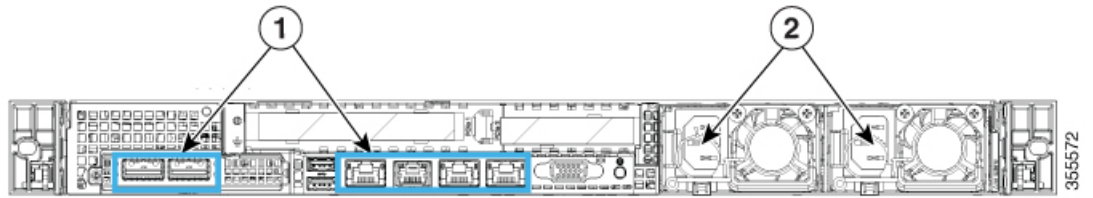
次の図は、物理的な設置および初回の電源投入後（設定前）の Cisco UCS C220 M4 シャーシを備えた、機能しているアプライアンスの LED を示しています。

図 6: 前面パネルの LED



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

図 7: 背面パネル LED



LED	望ましいステータスインジケータ
1	<p>最初の電源投入時には、すべてのポートのリンクステータスとリンク速度 LED がオフであり、電源ステータス LED がグリーンになっているはずで</p> <p>す。</p> <p>Maglev 設定ウィザードを使用してネットワーク設定を構成およびテストした後（「マスターノードの設定」および「アドオンノードの設定」を参照）、すべてのケーブル接続ポートのリンクステータス、リンク速度、および電源ステータス LED がグリーンになります。すべてのケーブル接続されていないポートの LED は変化しません。</p>
2	<p>電源装置障害 LED：オフ</p> <p>AC 電源 LED：グリーン</p>

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



第 4 章

アプライアンスの設定

- [アプライアンスの設定ワークフロー](#) (51 ページ)
- [CIMC へのブラウザアクセスの有効化](#) (52 ページ)
- [事前フライトチェックの実行](#) (57 ページ)
- [Cisco DNA Center ISO イメージの確認](#) (64 ページ)
- [ブート可能 USB ドライブの作成](#) (65 ページ)
- [アプライアンスのイメージの再作成](#) (66 ページ)
- [Cisco DNA Center ISO イメージのインストール](#) (68 ページ)
- [マスターノードの設定](#) (69 ページ)
- [アドオンノードの設定](#) (85 ページ)
- [ハイアベイラビリティクラスタの導入シナリオ](#) (100 ページ)

アプライアンスの設定ワークフロー

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

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

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

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

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

アプライアンスの設定プロセスを示す[ビデオ](#)については、[このリンクをクリックしてください](#)。

表 21: アプライアンスの設定タスク

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

CIMC へのブラウザアクセスの有効化

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

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



ヒント

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

- ☰ > [管理者 (Admin)] > [ユーザ管理 (User Management)] > [ローカルユーザ (Local user)] [管理 (Management)] を選択します。
- ID [1] を選択してから、[ユーザの変更 (Modify User)] をクリックします。
新しいパスワードを [パスワードの変更 (Change Password)] フィールドに入力してから、[保存 (Save)] をクリックします。

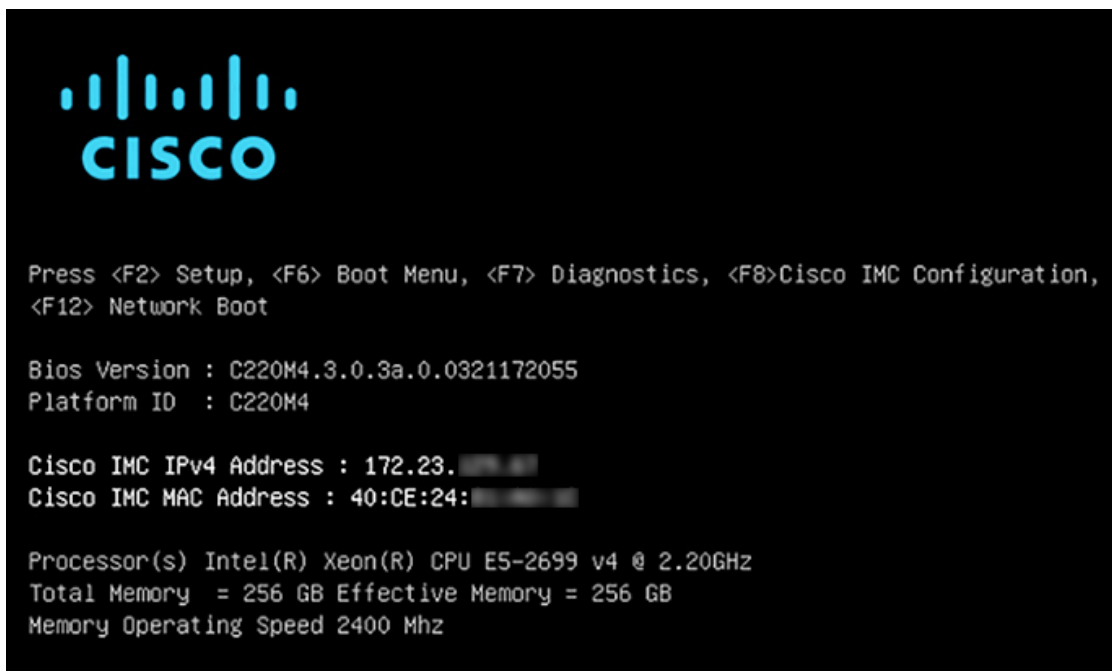
ステップ 1 次のいずれかを接続して、アプライアンスコンソールにアクセスします。

- アプライアンスの前面パネルにある KVM コネクタ（「[前面パネルと背面パネル](#)」の前面パネル図のコンポーネント 12）に接続する KVM ケーブルか、

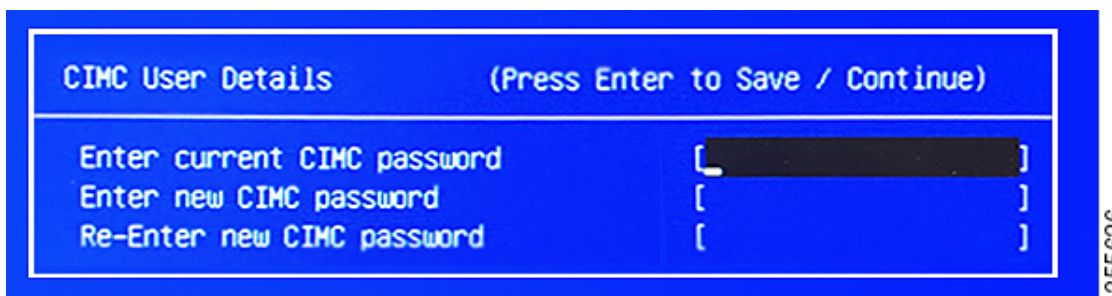
- アプライアンスの背面パネルにある USB ポートと VGA ポート（「前面パネルと背面パネル」の背面パネル図のコンポーネント 7 および 12）に接続するキーボードとモニタ。

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

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



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



ステップ 5 [現在のCIMCパスワードを入力 (Enter CURRENT CIMC Password)] フィールドに、デフォルトの CIMC ユーザパスワード (新しいアプライアンスにおけるデフォルトは **password**) を入力します。次に、[新しいCIMCパスワードを入力 (Enter New CIMC Password)] フィールドと [新しいCIMCパスワードを再入力 (Re-Enter New CIMC Password)] フィールドに新しい CIMC ユーザパスワードを入力して確認します。

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

```

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:     [ ]                   Active-active:  [ ]
  Riser1:       [ ]                   VLAN (Advanced)
  Riser2:       [ ]                   VLAN enabled:   [ ]
  MLOm:         [ ]                   VLAN ID:        1
Shared LOM Ext: [ ]                   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 次の変更を加えます。

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

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

```

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 次の変更を加えます。

- [ホスト名 (Hostname)] : このアプライアンスにおける CIMC のホスト名を入力します。
- [ダイナミックDNS (DynamicDNS)] : 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。
- [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して、この機能を無効にします。

ステップ 10 **F10** を押して、設定を保存します。

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

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

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

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



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

Server Properties

- Product Name: UCS C220 M4SX
- Serial Number: FCH212
- PID: UCSC-C220-M4SX
- UUID: 1DB0E03F-59AF-4B5B-BAB7-
- BIOS Version: C220M4.3.1.3c.0.0307181404
- Description:
- Asset Tag:

Cisco Integrated Management Controller (Cisco IMC) Information

- Hostname: C220-FCH212
- IP Address: 172.25
- MAC Address: 70:79:F0
- Firmware Version: 3.1(3a)
- Current Time (UTC): Tue Aug 14 15 2018
- Local Time: Tue Aug 14 15 2018 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

(%)

Utilization Type	Value (%)
Overall Utilization (%)	~10
CPU Utilization (%)	~10
Memory Utilization (%)	~10
IO Utilization (%)	~10

Buttons:

次のタスク

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

事前フライトチェックの実行

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

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

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

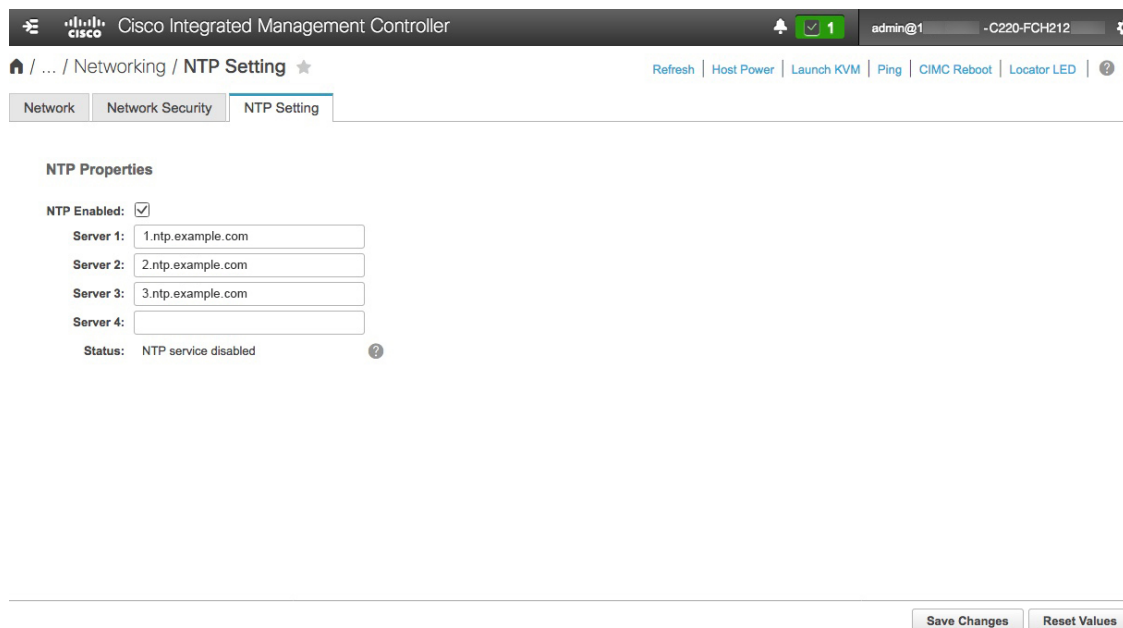
The screenshot displays the Cisco Integrated Management Controller (CIMC) Summary page. The top navigation bar includes the Cisco logo, the title 'Cisco Integrated Management Controller', and user information 'admin@1' for device '-C220-FCH212'. The main content area is titled 'Chassis / Summary' and contains four primary sections:

- Server Properties:** Lists hardware details such as Product Name (UCS C220 M4SX), Serial Number (FCH212), PID (UCSC-C220-M4SX), UUID (1DB0E03F-59AF-4B5B-BAB7-), BIOS Version (C220M4.3.1.3c.0.0307181404), and Asset Tag (Unknown).
- Cisco Integrated Management Controller (Cisco IMC) Information:** Provides system-level data including Hostname (C220-FCH212), IP Address (172.25), MAC Address (70:79:F0), Firmware Version (3.1(3a)), Current Time (UTC: Tue Aug 14 15 2018), Local Time (Tue Aug 14 15 2018 UTC +0000), and Timezone (UTC).
- Chassis Status:** A list of health indicators for various components: Power State (On), Overall Server Status (Good), Temperature (Good), Overall DIMM Status (Good), Power Supplies (Good), Fans (Good), Locator LED (Off), and Overall Storage Status (Good).
- Server Utilization:** A bar chart showing resource usage for the server. The Y-axis represents percentage utilization from 0 to 100%. The chart includes bars for Overall Utilization, CPU Utilization, Memory Utilization, and IO Utilization.

At the bottom right of the page, there are two buttons: 'Save Changes' and 'Reset Values'.


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。

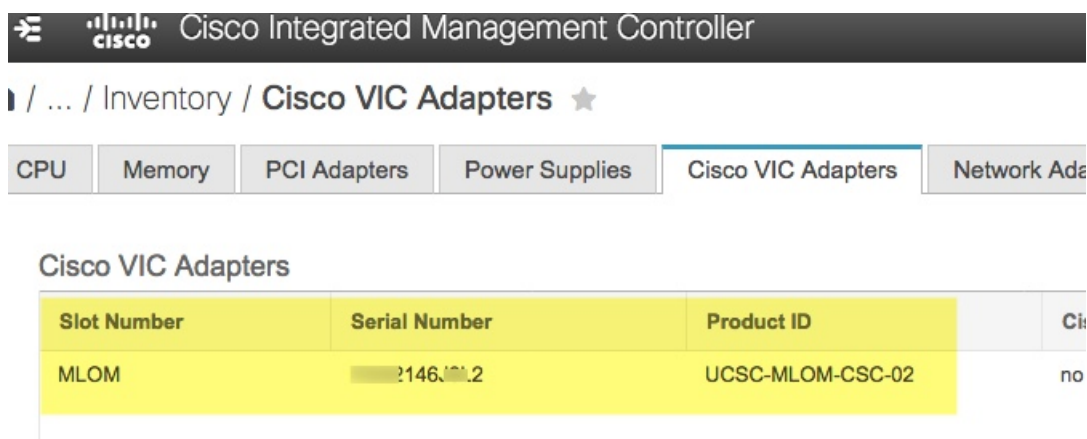
- [シャーシの概要 (device Summary)] ウィンドウが表示されたら、 アイコンをクリックして [CIMC] メニューを表示します。
- [CIMC] メニューで、[管理者 (Admin)] > [ネットワーキング (Networking)] > [NTP設定 (NTP Setting)] を選択します。CIMC に [NTP設定 (NTP Setting)] タブが表示されます。
- [NTP有効化 (NTP Enabled)] ボックスがオンになっていることを確認してから、次に示す例のように、4つの番号付き [サーバ (Server)] フィールドに最大4つの NTP サーバホスト名またはアドレスを入力します。




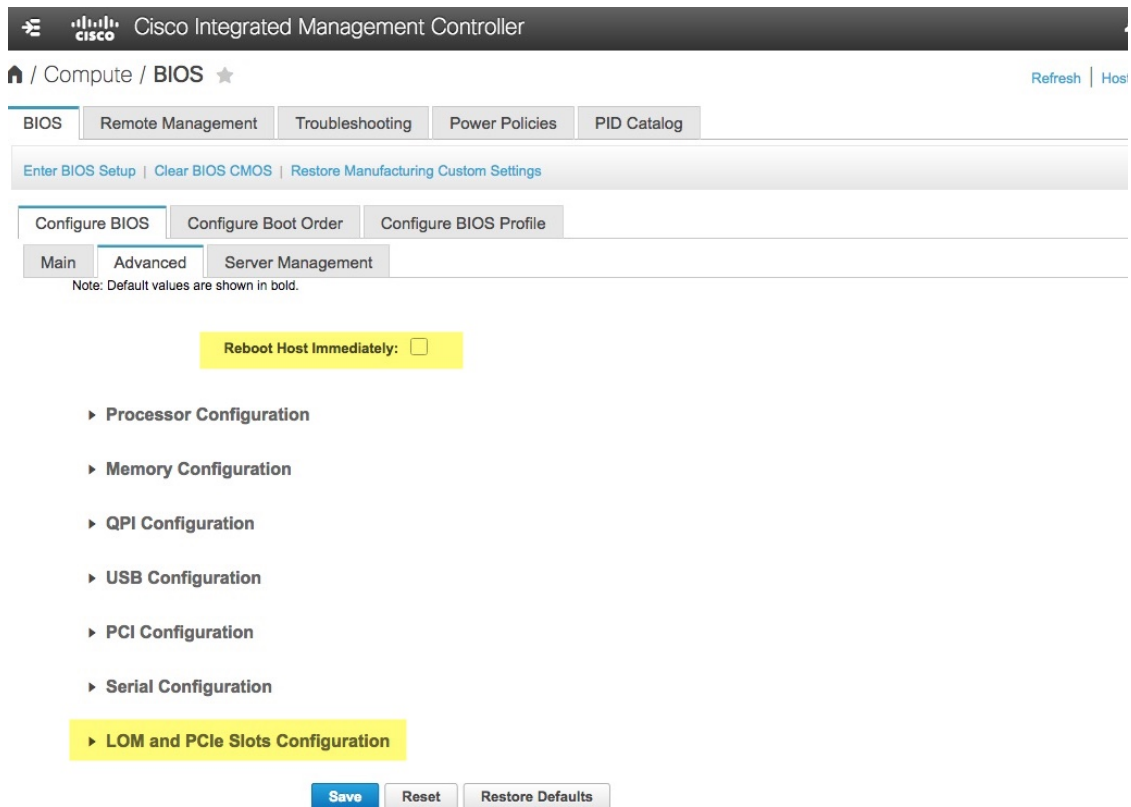
- d) 完了したら、[変更の保存 (Save Changes)] をクリックします。CIMC は、エントリを検証した後、アプライアンスハードウェアの時刻と NTP サーバの時刻の同期を開始します。

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

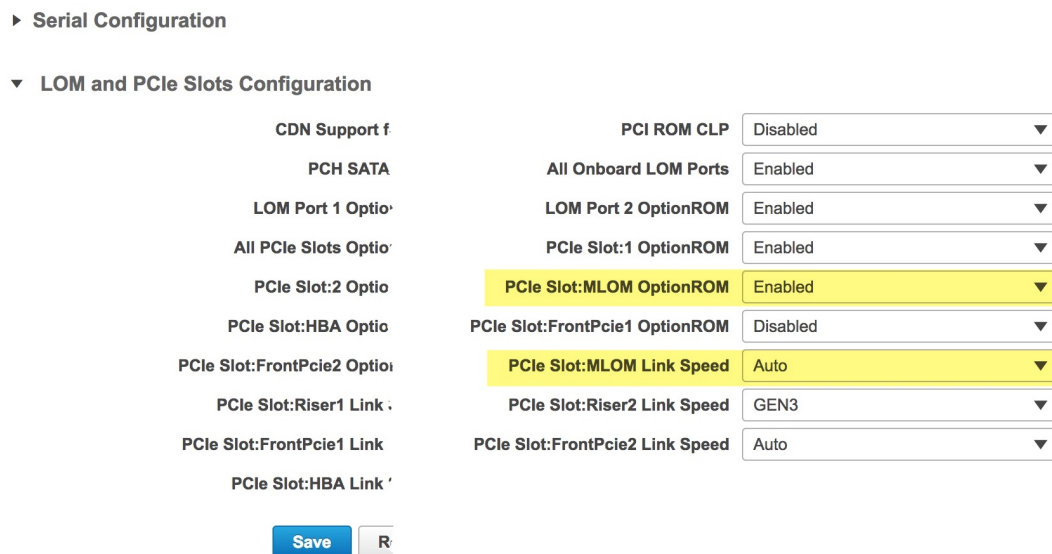
- a) 必要に応じて、 アイコンをクリックして [CIMC] メニューを表示します。
- b) [CIMC] メニューで、[シャーシ (Chassis)] > [インベントリ (Inventory)] > [Cisco VICアダプタ (Cisco VIC Adapters)] を選択します。次に示すように、製品 ID 「UCSC-MLOM-CSC-02」 が MLOM スロット用にリストされていることを確認します。




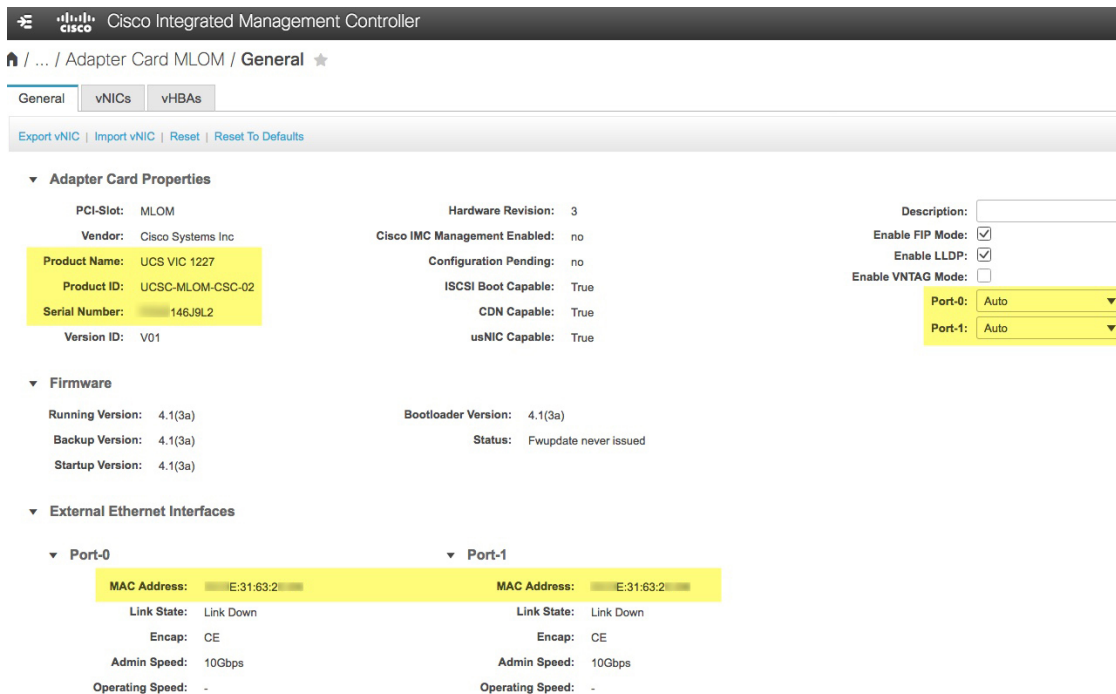
- c)  > [コンピューティング (Compute)] > [BIOS] > [BIOSの設定 (Configure BIOS)] > [詳細設定 (Advanced)] を選択します。[ホストを即座にリブート (Reboot Host Immediately)] チェックボックスがオフになっていることを確認し、[LOMおよびPCIeスロットの設定 (LOM and PCIe Slots Configuration)]] ドロップダウンの場所を確認します。



- d) [LOMおよびPCIeスロットの設定 (LOM and PCIe Slots Configuration)] を選択します。次に、ドロップダウンセレクトを使用して、[PCIeスロット : MLOM OptionROM (PCIe Slot MLOM OptionROM)] を [有効化 (Enabled)] に、[PCIeスロット : MLOMリンク速度 (PCIe Slot: MLOM Link Speed)] を [自動 (Auto)] に設定します。

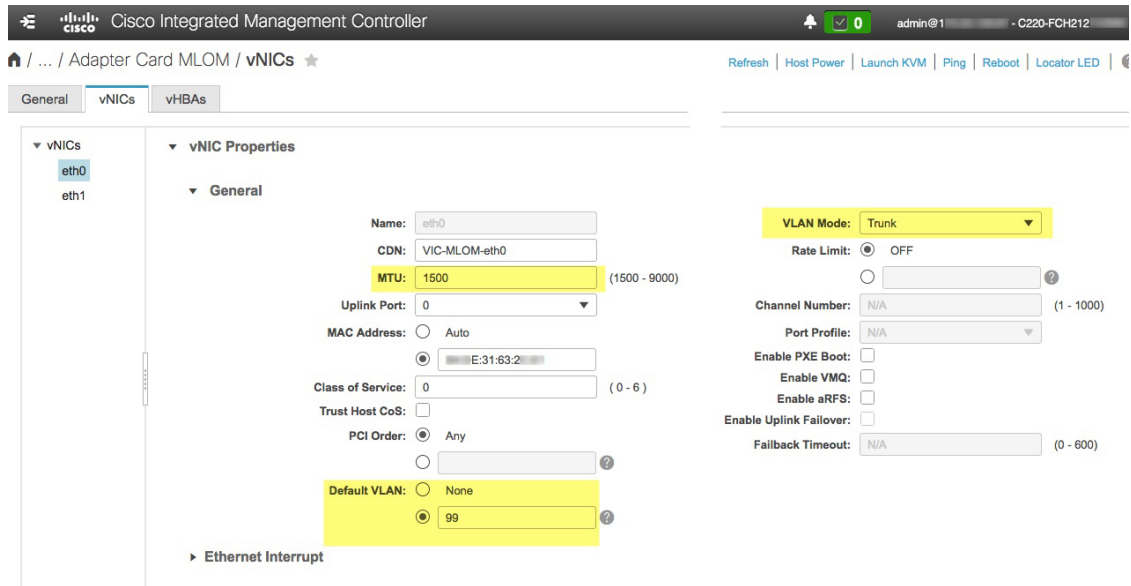


- e) [保存 (Save)] をクリックします。ホストをリブートするよう求められます。[キャンセル (Cancel)] をクリックして、リブートせずに続行します。
- f)  > [ネットワーク (Networking)] > [アダプタカード MLOM (Adapter Card MLOM)] > [全般 (General)] を選択します。[ポート0 (Port-0)] と [ポート1 (Port-1)] の MAC アドレスを確認します (ページ下部にある [外部イーサネットインターフェイス (External Ethernet Interfaces)] セクションに表示されます)。次に示すように、[アダプタカードのプロパティ (Adapter Card Properties)] セクションで、[ポート0 (Port-0)] と [ポート1 (Port-1)] の横にあるドロップダウンセクタを使用して、両方のポートの速度を [自動 (Auto)] に設定します。[変更の保存 (Save Changes)] をクリックします。



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

- **VLAN モード : トランク (Trunk)**
- **MTU: 1500**
- **デフォルト VLAN : 99** (「99」は一例にすぎないことに注意してください。アプライアンスとそのスイッチで使用するデフォルト VLAN を入力する必要があります)



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

- h) **[Save Changes]** をクリックします。ホストをもう一度リブートするよう求められます。[キャンセル (Cancel)] をクリックして、リブートせずに続行します。
- i) [vNIC (vNICs)] ドロップダウンで **[eth1]** を選択します。ドロップダウンセレクタを使用して、**[eth0]** に対して設定したものと同じ値を **[eth1]** に設定します。
- j) 完了したら、[変更の保存 (Save Changes)] をクリックします。ホストをリブートするよう求められます。今回は、**[OK]** をクリックしてアプライアンスをリブートします。
- k) アプライアンスのリブートが完了したら、CIMCGUI に再度ログインします。☰>[ネットワークング (Networking)]>[アダプタカード MLOM (Adapter Card MLOM)]>[全般 (General)]>[vNIC (vNICs)] を選択します。vNIC MAC アドレスと、以前に設定した [MTU]、[VLAN]、[VLAN モード (VLAN Mode)] の各パラメータが正確かどうかを確認します。
- l) 終了したら、右上の [ホストの電源 (Host Power)] メニューをクリックして、[電源の再投入 (Power Cycle)] を選択します。次に **[OK]** をクリックします。



ステップ 4 次に、以下の手順に従って、アプライアンスの高スループット設定と一致するようにスイッチを再設定します。

- a) セキュアシェル (SSH) クライアントを使用して、設定するスイッチにログインし、スイッチプロンプトで EXEC モードを開始します。
- b) 次の一連のコマンドを入力して、スイッチポートを設定します。

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

これらのコマンドは単なる例であることに注意してください。アプライアンス NIC を設定する際に入力したものと同一 VLAN ID と MTU の値を使用します。スイッチの例では、リンク速度、デュプレックス、および MTU のコマンド値がデフォルトになっているので、デフォルト値を変更した場合にのみ入力する必要があります。アプライアンス NIC と同様に、スループットが向上するように MTU を設定することもできます (上限は 9000)。

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

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

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

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

MySwitch#

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

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

```
Total Mac Addresses for this criterion: 1

MySwitch#
```

ステップ 5 最後に、10Gbps アプライアンスポートに接続されているスイッチを再設定して、オーバーサイズの 802.1p フレームがサポートされるようにします。

- a) まだ実行していない場合には、セキュアシェル (SSH) クライアントを使用して、設定するスイッチにログインし、スイッチプロンプトで EXEC モードを開始します。
- b) 次の一連のコマンドを入力して、802.1P フレームをサポートするようにスイッチポートを設定します。

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitEthernet 1/1/3
MySwitch(config-if)#switchport voice vlan dot1p
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#copy running-config startup-config
```

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

```
MySwitch#show run interface tengigabitEthernet 1/1/3
Building configuration...

Current configuration : 62 bytes
!
interface tengigabitEthernet1/1/3
switchport mode trunk
switchport voice vlan dot1p
MySwitch#end
```

次のタスク

最初にインストールしたアプライアンスをクラスタのマスターノードとして設定して、続行します。「[マスターノードの設定](#)」を参照してください。

Cisco DNA Center ISO イメージの確認

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

始める前に

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

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

ステップ 2 シスコによって指定され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** シスコによって指定された場所から ISO イメージ用のセキュア ハッシュ アルゴリズム (SHA512) チェックサムファイルをダウンロードします。
- ステップ 4** シスコサポートから電子メールで、またはセキュアなシスコの Web サイト (利用可能な場合) からダウンロードして、ISO イメージのシグニチャファイル (.sig) を入手します。
- ステップ 5** (オプション) 不完全なダウンロードが原因で ISO イメージが破損していないかどうかを判断するには、SHA 検証を実行します。

(オペレーティングシステムに応じて) 次のコマンドのいずれかを実行します。

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

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

- ステップ 6** 署名を確認して、ISO 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 ISO-image-filename`

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

ISO イメージが正規のものの場合、このコマンドを実行すると「**検証 OK (Verified OK)**」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には、ISO イメージをインストールせず、シスコサポートにお問い合わせください。

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

ブート可能 USB ドライブの作成

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

始める前に

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

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

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

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

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

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

- 成功時に自動マウント解除する
- 成功時に書き込みを検証する

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

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

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

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

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

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

Etcher 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 ドライブを設定します。

アプライアンスのイメージの再作成

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

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

「Cisco DNA Center IOS 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 USB ドライブの作成」を参照してください。

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

- a) Cisco IMC にログインし、KVM セッションを開始します。
- b) 次のメニューオプションのいずれかを選択して、アプライアンスの電源をオンにするか、電源を再投入します。
 - [電源 (Power)]>[システムの電源オン (Power On System)]
 - [電源 (Power)]>[システムの電源の再投入 (コールドブート) (Power Cycle System (cold boot))]

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

```

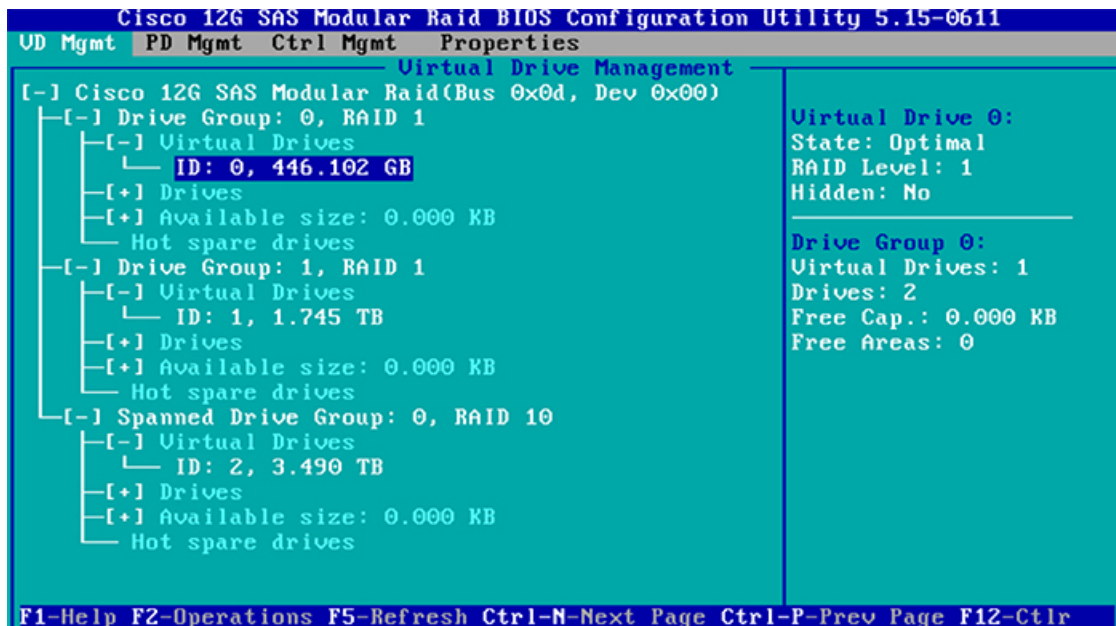
ID  LUN  VENDOR      PRODUCT                REVISION      CAPACITY
--  ---  -
15  0    ATA         INTEL SSDSC2BB48      CS01          457862MB
   0    AVAGO      Virtual Drive         RAID1         456809MB
   1    AVAGO      Virtual Drive         RAID1         1830101MB
   2    AVAGO      Virtual Drive         RAID10        3660202MB

0 JBOD(s) found on the host adapter
0 JBOD(s) handled by BIOS

3 Virtual Drive(s) found on the host adapter.
3 Virtual Drive(s) handled by BIOS

Press <Ctrl><R> to Run MegaRAID Configuration Utility
    
```

- c) この画面が表示されたらすぐに、**Ctrl+R** を押して、MegaRAID 設定ユーティリティを実行します。操作するまでの時間が長すぎると、この画面は消えてしまいます。この画面に戻るには、KVM メニューから [電源 (Power)]>[システムのリセット (ウォームブート) (Reset System (warm boot))] を選択して、アプライアンスをリブートします。
- d) ドライブのエントリ (ID : 0、446.102 GB など) を選択してから、**F2** を押します。



この操作により、ドライブの [詳細プロパティ (Advanced Properties)] 画面が開きます。

- e) 表示されるメニューで、[初期化 (Initialization)]>[高速初期化 (Fast Initialization)]を選択します。
- f) アプライアンスの他の仮想ドライブごとに、ステップ 3b ~ 3e を繰り返します。

ステップ 4 アプライアンスに Cisco DNA Center を再インストールします。

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

Cisco DNA Center ISO イメージのインストール

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

始める前に

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

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

ステップ 2 CIMC にログインし、KVM セッションを開始します。

ステップ 3 アプライアンスの電源を投入または再投入します。

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

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

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

ブートデバイス選択メニューが表示されます。

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

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

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

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

マスターノードの設定

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

すでにマスターノードがある既存のクラスタのアドオンノードとしてインストールされたアプライアンスを設定する場合には、「[アドオンノードの設定](#)」の手順を実行します。



重要 クラスタ内のアプライアンスごとに、1つのインターフェイスのみで DNS サーバを設定します。複数のインターフェイスで 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。

始める前に

次のことを確認します。

- 「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」で必要とされているすべての情報が収集されたこと。
- 「[アプライアンスのインストールワークフロー](#)」の説明に従って、最初のアプライアンスがインストールされたこと。

- 「[CIMC へのブラウザアクセスの有効化](#)」の説明に従って、マスターノードで CIMC ブラウザアクセスが設定されたこと。
- 「[事前フライトチェックの実行](#)」の説明に従って、マスターノードアプライアンスのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- CIMC および Cisco DNA Center と互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリースノート](#) を参照してください。
- Cisco DNA Center と、次の手順のステップ 8 で指定する DNS サーバとの間のファイアウォールで ICMP が有効になっていること。Maglev 構成ウィザードでは、Ping を使用して、指定した DNS サーバを確認します。Cisco DNA Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が有効になっていない場合、この Ping はブロックされる可能性があります。ブロックされた場合、ウィザードを完了することはできません。

- ステップ 1** CIMC GUI の設定時に設定した CIMC IP アドレスにブラウザでアクセスし、CIMC ユーザとして CIMC GUI にログインします（「[CIMC へのブラウザアクセスの有効化](#)」を参照）。
- ログインが成功すると、次に示すように、アプライアンスに [Cisco Integrated Management Controller Chassis の概要 (Cisco Integrated Management Controller Chassis Summary)] ウィンドウが右上の青いリンクメニューとともに表示されます。



- ステップ 2** 青いリンクメニューで [KVMの起動 (Launch KVM)] を選択してから、[Java ベースの KVM (Java based KVM)] と [HTML ベースの KVM (HTML based KVM)] のいずれかを選択します。Java ベースの KVM を選択した場合、KVM コンソールを独自のウィンドウで表示するために、ブラウザまたはファイルマネージャから Java スタートアップファイルを起動する必要があります。HTML ベースの KVM を選択すると、KVM コンソールが別個のブラウザウィンドウまたはタブで自動的に起動します。
- 選択した KVM のタイプに関係なく、KVM コンソールを使用して、設定の進行状況をモニタし、Maglev 構成ウィザードのプロンプトに応答します。
- ステップ 3** KVM が表示されたら、次のいずれかを選択してアプライアンスをリブートします。
- a) メインの CIMC GUI ブラウザウィンドウで、[ホストの電源 (Host Power)] > [電源の再投入 (Power Cycle)] を選択します。その後、KVM コンソールに切り替えて続行します。

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

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

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

```

Welcome to the Maglev Configuration Wizard!

The wizard will walk you through the steps to configure this host. Select one or more 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 >
    
```

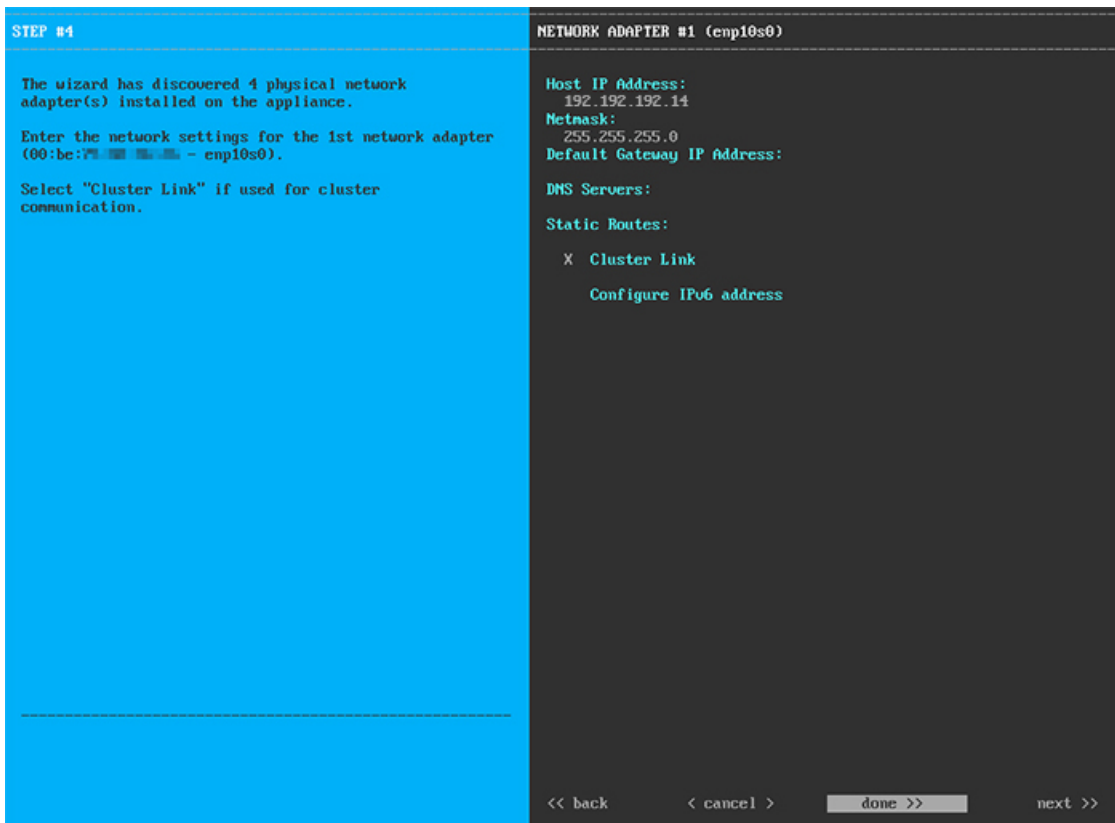
- ステップ 4** マスターノードの設定を開始するには、[DNA-C クラスターを開始する (Start a DNA-C Cluster)] を選択します。

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

1. 10Gbps クラスターポート (ポート 2、enp10s0、ネットワークアダプタ #1)
2. 1Gbps Cisco DNA Center GUI ポート (1、enp1s0f0、ネットワークアダプタ #2)
3. 1Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ #3)
4. 10Gbps エンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ #4)

(注) 設定の過程でウィザードに 10Gbps ポートのうちの 1 つまたは両方が表示されない場合、これらのポートは機能しないか無効になっている可能性があります。これらの 10Gbps ポートは、Cisco DNA Center 機能に必要です。10Gbps ポートが機能していないことが判明した場合には、[キャンセル (Cancel)] を選択して、設定をすぐに終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に「事前フライトチェックの実行」に記載されているすべての手順が完了していることを確認してください。

ステップ 5 ウィザードでは、まず 10Gbps クラスタポート (ポート 2、enp10s0) が検出され、[ネットワークアダプタ #1 (NETWORK ADAPTER #1)] として表示されます。「インターフェイスクーブル接続」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、「必要なサブネットおよび追加の IP アドレス」と「必要な設定情報」を参照してください)。



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

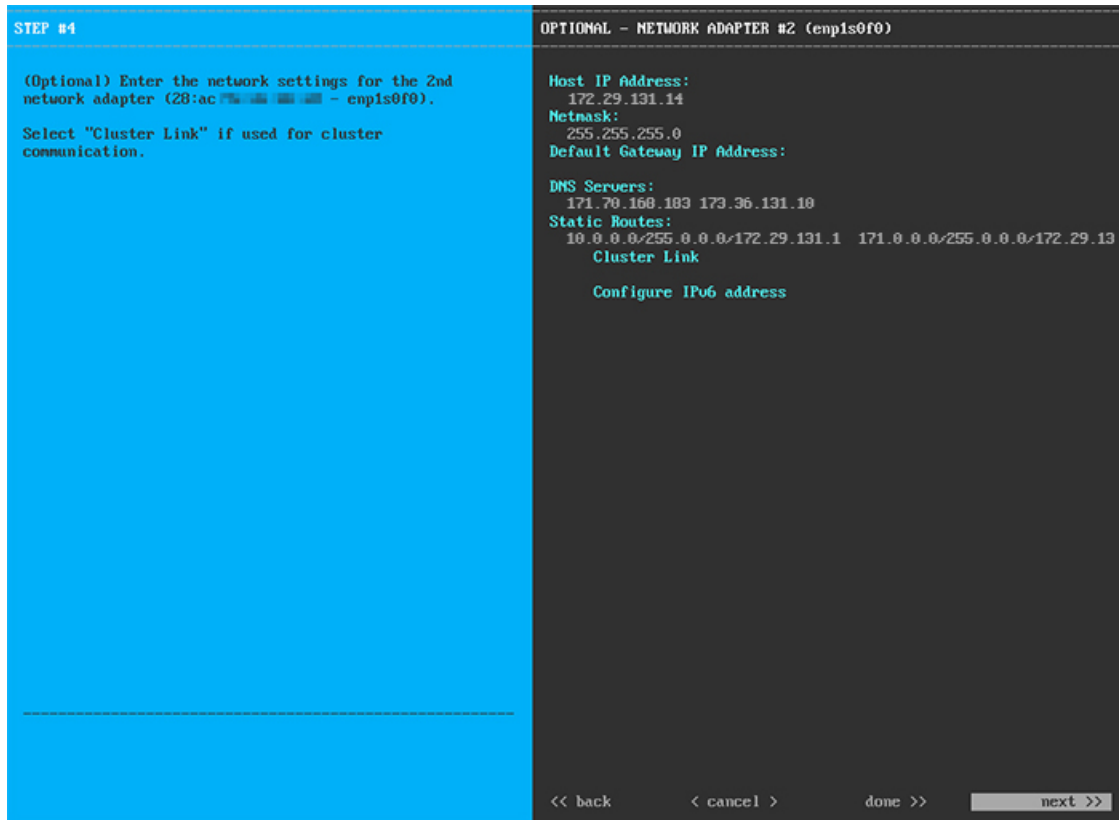
表 22: ネットワークアダプタ #1 のマスターノードエントリ: 10Gbps クラスタポート (enp10s0)

ホスト IP アドレス	クラスタポートの IP アドレスを入力します。これは必須です。クラスタポートのアドレスは後で変更できないことに注意してください。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。

デフォルト ゲートウェイの IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
DNS サーバ (DNS Servers)	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。このスタティックルートは、通常、GUI ポートのみで必要になります。
クラスタ リンク	このポートがクラスタへのリンクであることを示すには、このチェックボックスをオンにします。この操作はクラスタポートのみで必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

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

- ステップ 6** 入力したクラスタポート値の検証が成功すると、ウィザードに 1Gbps Cisco DNA Center GUI ポート (1、enp1s0f0) が [ネットワークアダプタ#2 (NETWORK ADAPTER #2)] としてが表示されます。「[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。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、「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」を参照してください)。



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

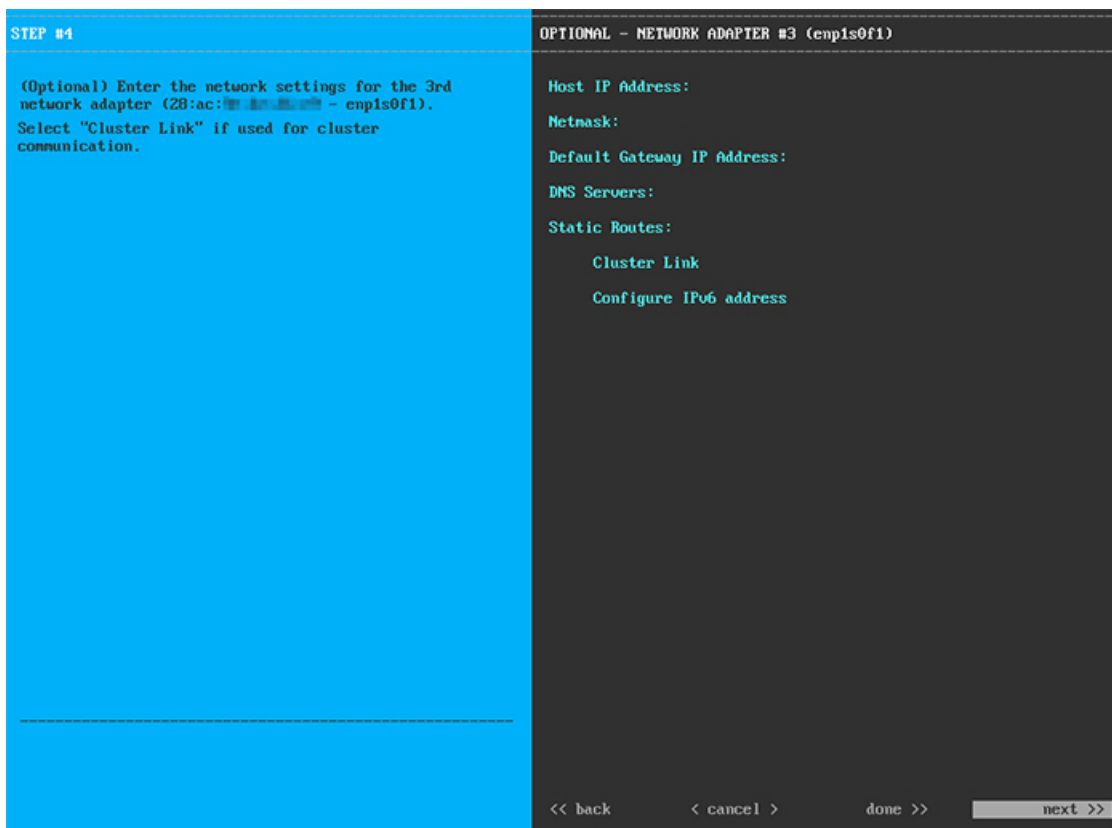
表 23: ネットワークアダプタ #2 のマスターノードエントリ : 1Gbps GUI ポート (enp1s0f0)

ホスト IP アドレス	1Gbps GUI ポートの IP アドレスを入力します。これは必須です。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルト ゲートウェイの IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 (注) NTP の場合、Cisco DNA Center と NTP サーバの間のポート 121 (UDP) が開いていることを確認します。

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

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

ステップ7 入力した Cisco DNA Center GUI ポート値の検証が成功すると、ウィザードに 1Gbps クラウドポート (2、enp1s0f0) が [ネットワークアダプタ#3 (NETWORK ADAPTER #3)] としてが表示されます。「[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、アプライアンスをインターネットにリンクする際、10Gbps エンタープライズポート (ポート 1、enp9s0) 経由でリンクを実行できない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します (入力する値については、「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」を参照してください)。



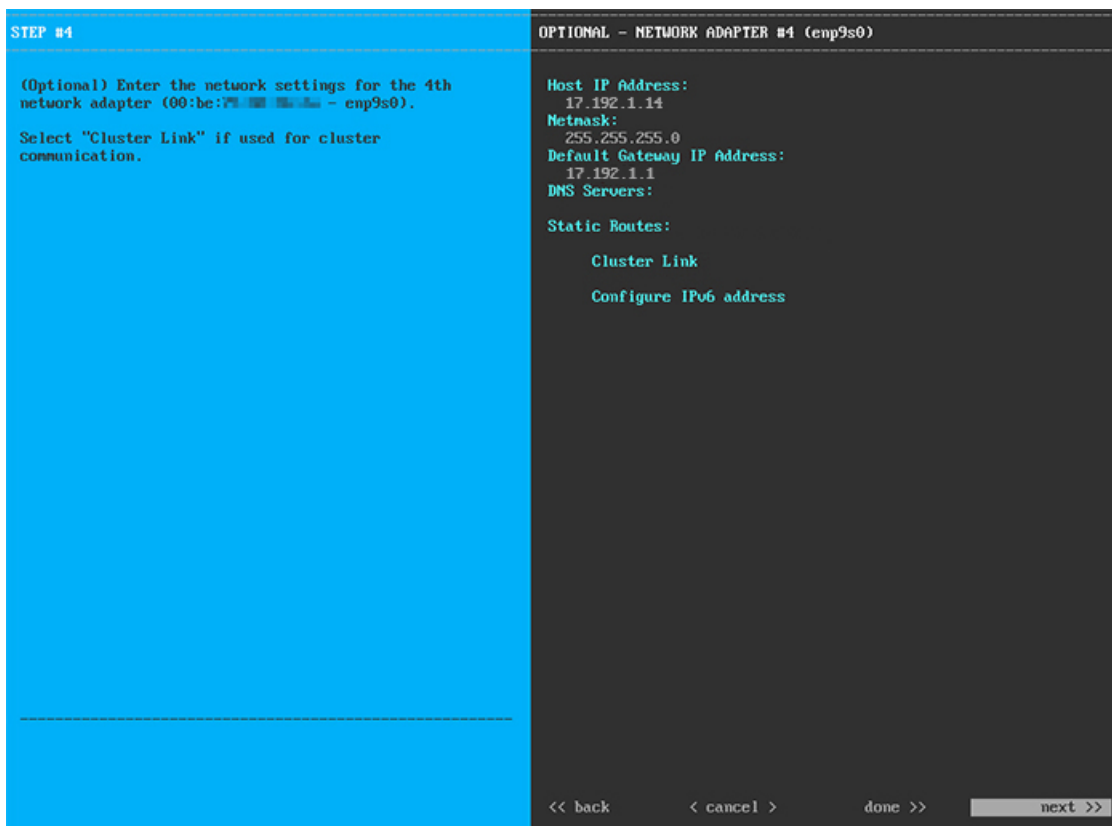
次の表に示すように、[ネットワークアダプタ#3 (NETWORK ADAPTER #3)] の設定値を入力します。

表 24: ネットワークアダプタ #3のマスターノードエントリ: 1Gbpsクラウドポート (enp1s0f1)

ホスト IP アドレス	クラウドポートの IP アドレスを入力します。この操作は、インターネット接続にクラウドポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにしておくことができます。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。この操作は、IP アドレスを入力する場合に必要になります。
[デフォルトゲートウェイの IP アドレス (Default Gateway IP address)]	クラウドポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。
スタティック ルート	1つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。このスタティックルートは、通常、Cisco DNA Center GUI ポートのみで必要になります。
クラスタ リンク (Cluster Link)	このフィールドは空欄のままにします。この操作はクラスタポートのみで必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

- ステップ 8** 入力したクラウドポート値の検証が成功すると、ウィザードに10Gbpsエンタープライズポート (ポート 1、enp9s0) が [ネットワークアダプタ#4 (NETWORK ADAPTER #4)] として表示されます。「[インターフェイスケーブル接続](#)」で説明したように、このポートは、アプライアンスを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、「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」を参照してください)。



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

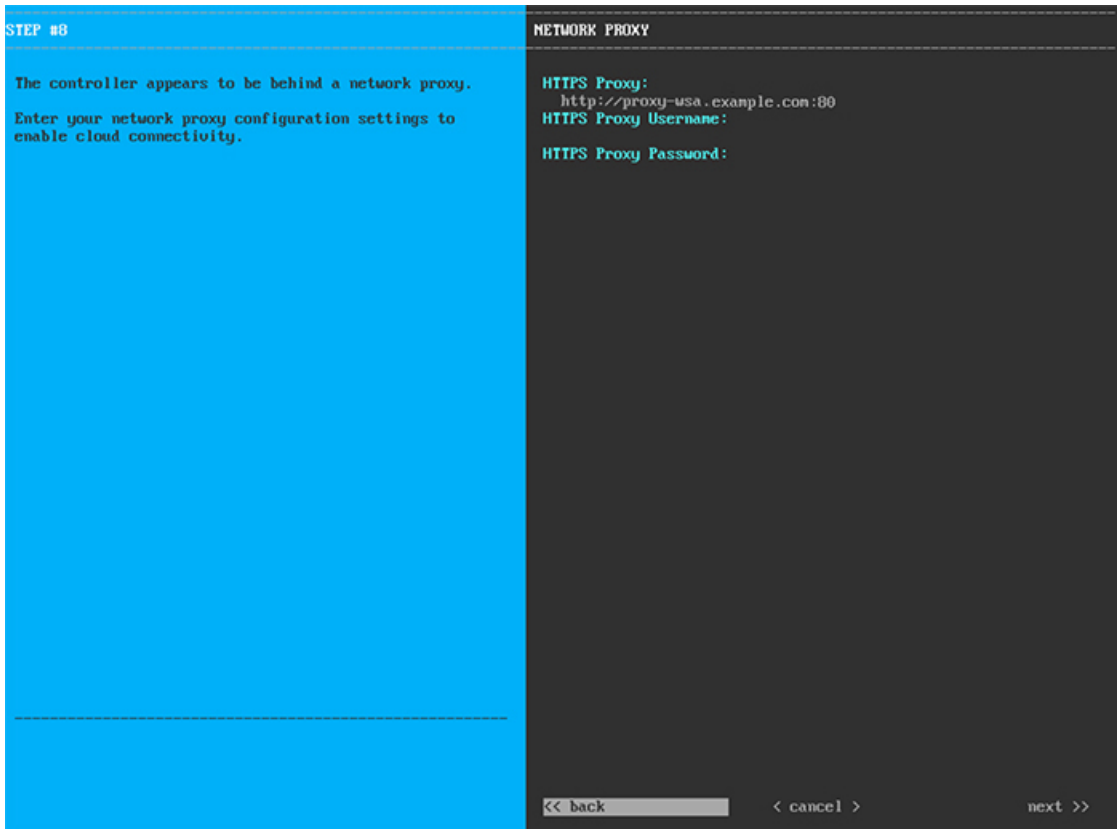
表 25: ネットワークアダプタ #4 のマスターノードエントリ: 10Gbps エンタープライズポート (enp9s0)

ホスト IP アドレス	10Gbps エンタープライズポートの IP アドレスを入力します。これは必須です。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルト ゲートウェイの IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは必須です。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。このスタティックルートは、通常、Cisco DNA Center GUI ポートのみで必要になります。
クラスタ リンク	このフィールドは空欄のままにします。この操作はクラスタポートのみで必要になります。

IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。
--------------	---------------------------------------

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

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



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

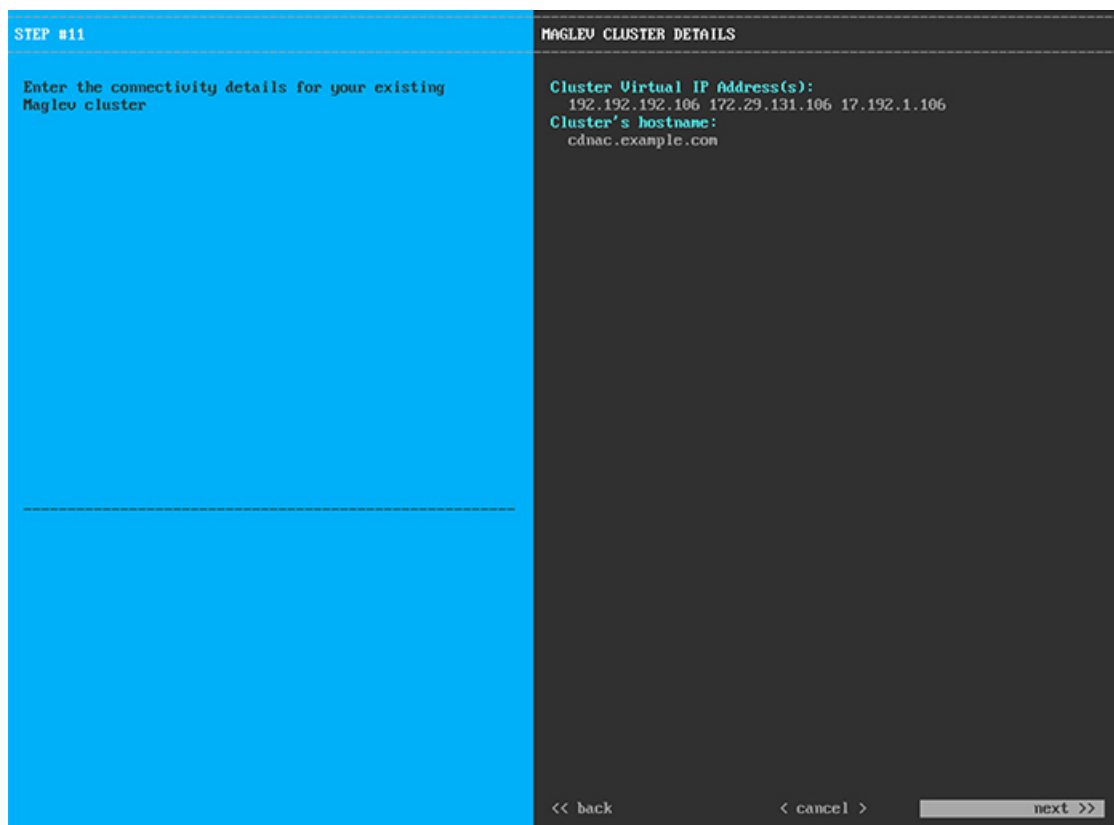
表 26: ネットワークプロキシのマスターノードエントリ

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

<p>HTTPS プロキシパスワード</p>	<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>
-------------------------------	--

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

ステップ 10 ネットワークプロキシの設定が完了すると、次に示すように、[MAGLEV クラスタの詳細 (MAGLEV CLUSTER DETAILS)] で、マスターノードの仮想 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単一ノードクラスタの両方の場合に必要です。単一ノードクラスタをセットアップした後、単一ノードクラスタのまま使用し続ける予定の場合には、このステップをスキップしてステップ 11 に進みます。

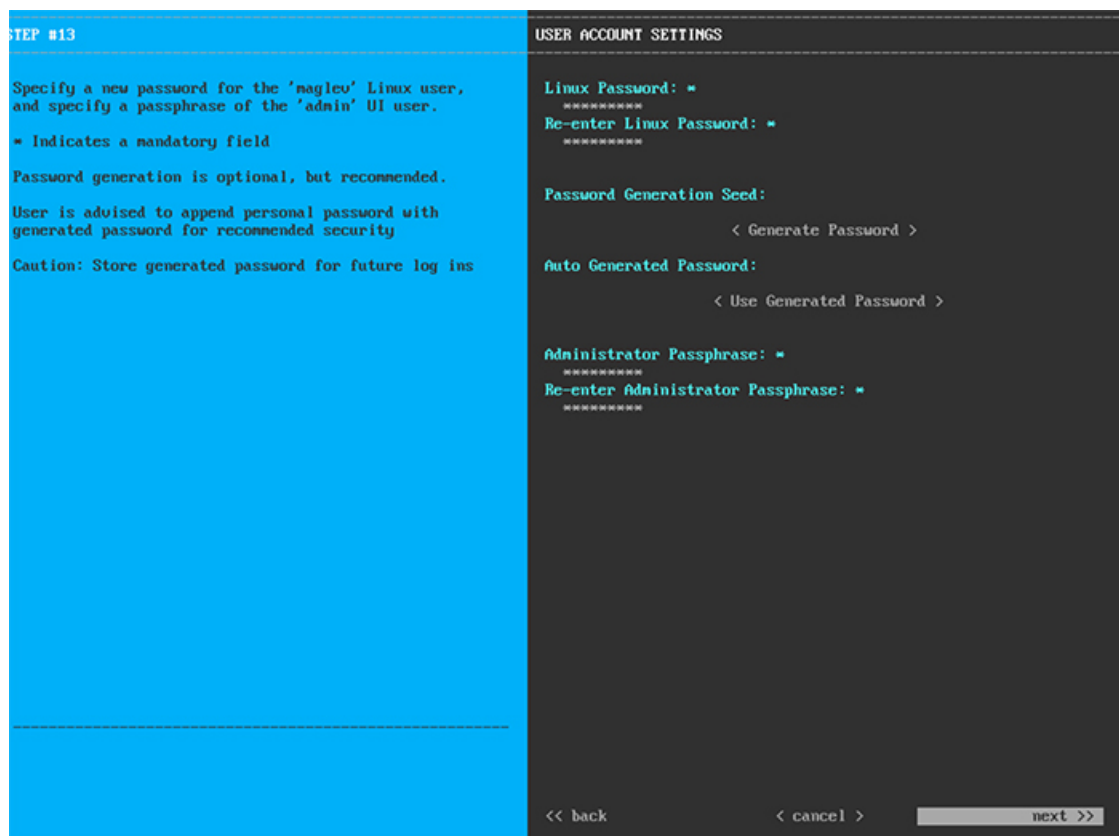
重要 設定済みのネットワークインターフェイスごとに 1 つの仮想 IP アドレスを入力する必要があります。この操作を行わない限り、ウィザードを完了することはできません。これらのアドレスは、クラスタリンクのステータスに関連付けられており、ステータスは [アップ (UP)] の状態である必要があります。

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

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

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

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



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

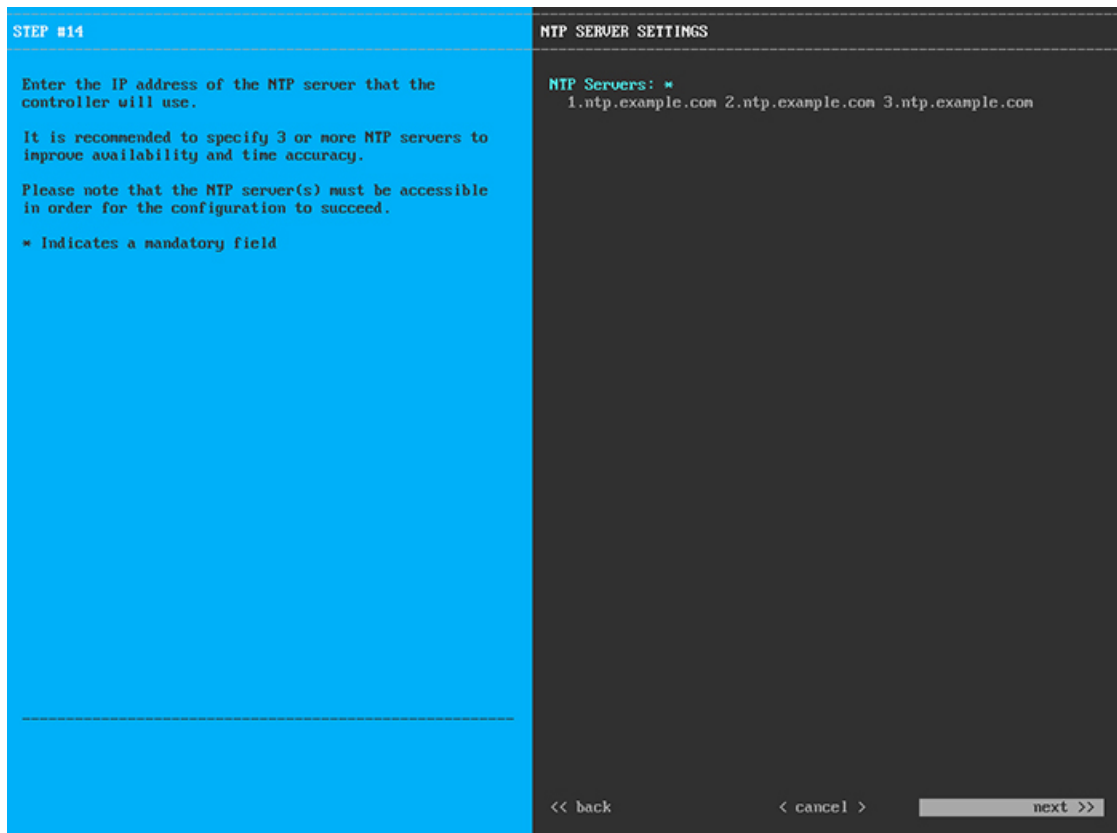
表 27: ユーザアカウント設定のマスターノードエントリ

[Linuxパスワード (Linux Password)]	maglev ユーザに対して設定されている Linux パスワードを入力します。
Linux パスワードの再入力	Linux パスワードをもう一度入力して確認します。

<p>パスワード生成シード</p>	<p>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。</p>
<p>自動生成パスワード</p>	<p>(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。</p> <p>パスワードを保存するには、[生成されたパスワードを使用 (Use Generated Password)] を押します。</p>
<p>管理者パスフレーズ (Administrator Passphrase)</p>	<p>デフォルトの管理スーパーユーザ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>管理者パスフレーズの再入力</p>	<p>管理者パスフレーズをもう一度入力して確認します。</p>

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

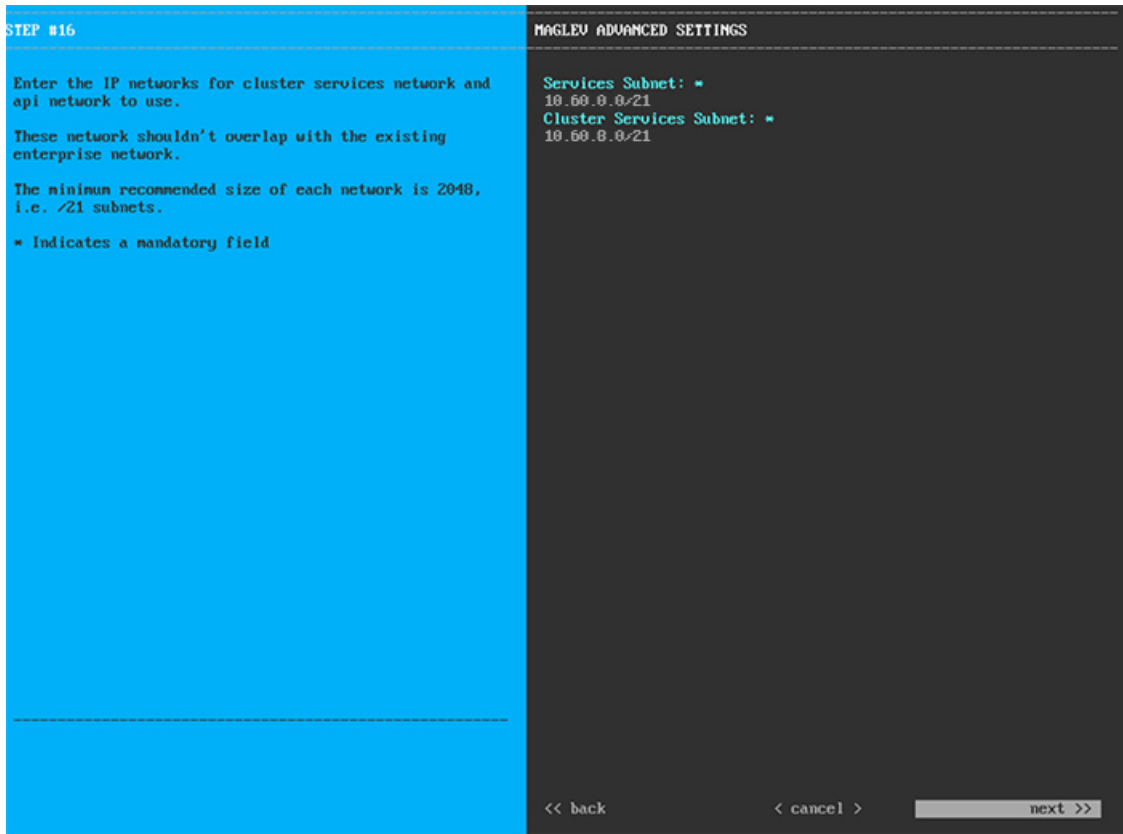
ステップ 12 ユーザアカウントの詳細を入力すると、次に示すように、[NTPサーバの設定 (NTP SERVER SETTINGS)] の値を入力するようウィザードに求められます。



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

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

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



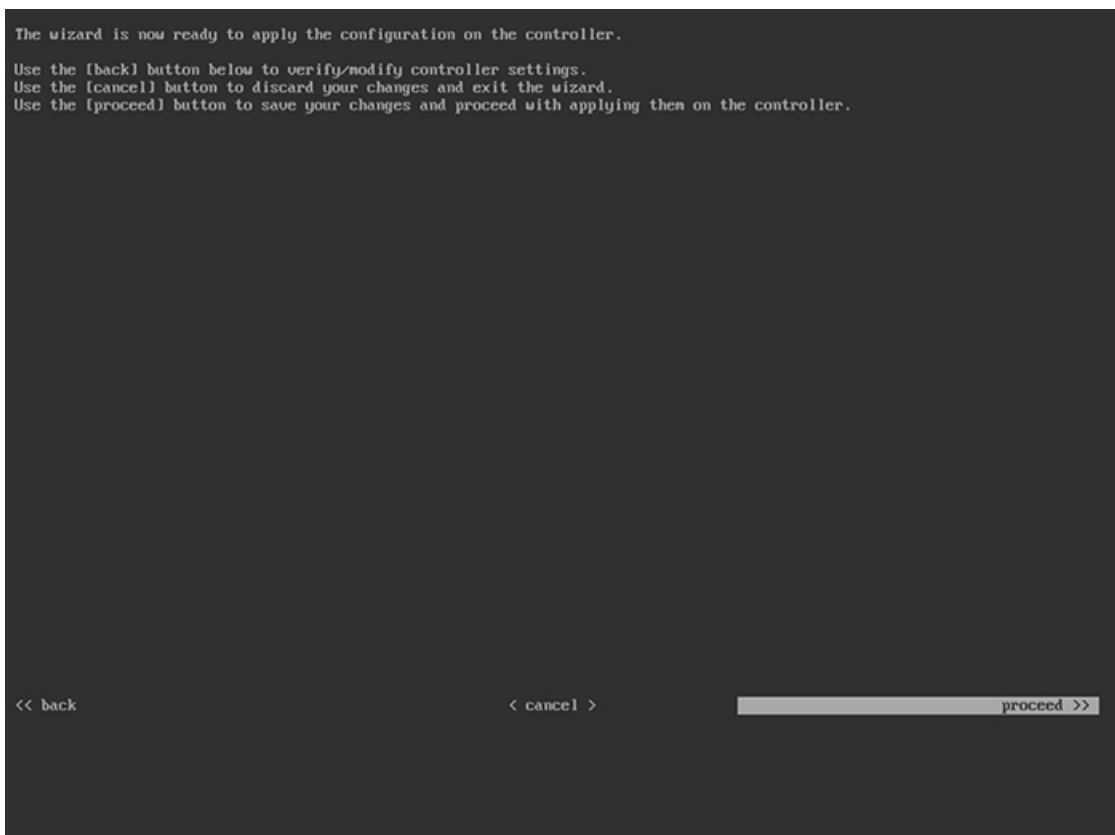
次の表に示すように、[MAGLEV詳細設定 (MAGLEV ADVANCED SETTINGS)] の設定値を入力します。

表 28: *Maglev* 詳細設定のマスターノードエントリ

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

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

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



[続行>> (proceed>>)] を選択して設定を完了します。

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

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

次のタスク

タスクが完了した後：

- このアプライアンスをスタンドアロンモードのみで展開する場合には、初回セットアップ（「[初期設定ワークフロー](#)」）を実行して続行します。
- Cisco DNA Center アプライアンスをクラスタ内のマスター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（「[アドオンノードの設定](#)」）。

アドオンノードの設定

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



重要

クラスタ内のアプライアンスごとに、1 つのインターフェイスのみで DNS サーバを設定します。複数のインターフェイスで 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。

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

- 一度に 1 つのノードのみをクラスタに結合してください。複数のノードを同時に追加しないでください。同時に追加しようとすると予期しない動作が発生します。
- クラスタに新しいノードを追加する前に、インストールされているすべてのパッケージがマスターノードに展開されていることを確認してください。展開されているかどうかを確認するには、セキュアシェルを使用して、マスターノードの Cisco DNA Center GUI ポートに Linux ユーザ (maglev) としてログインしてから、`maglev package status` コマンドを実行します。インストールされているすべてのパッケージは、コマンド出力で「展開済み (DEPLOYED)」と表示されます。次の例では、アプリケーションポリシー、SD アクセス、センサーアシュアランス、およびセンサー自動化の各パッケージはインストールされていないため、これらのパッケージのステータスのみが「未展開 (NOT_DEPLOYED)」になります。アドオンノードを設定する前に、パッケージのステータスが前述のように表示されている必要があります。

```
$ ssh maglev@172.29.131.14 -p 2222
The authenticity of host '[172.29.131.14]:2222 ([172.29.131.14]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:scye+2116NFHAKOZDs0cNLHBR75j1KV3ZXIKuUaiadk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.29.131.14]:2222' (ECDSA) to the list of known hosts.
Welcome to the Maglev Appliance
maglev@172.29.131.14's password:

Welcome to the Maglev Appliance

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

System load: 4.08                IP address for enp9s0: 17.192.1.14
Usage of /: 59.8% of 28.03GB     IP address for enp10s0: 192.192.192.14
Memory usage: 21%              IP address for enp1s0f0: 172.29.131.14
Swap usage: 0%                 IP address for docker0: 169.254.0.1
Processes: 831                  IP address for tun10: 10.60.3.0
Users logged in: 0

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

[Thu Dec 20 03:07:13 UTC] maglev@192.192.192.14 (maglev-master-1) ~
$ maglev package status
[administration] password for 'admin':
```

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

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

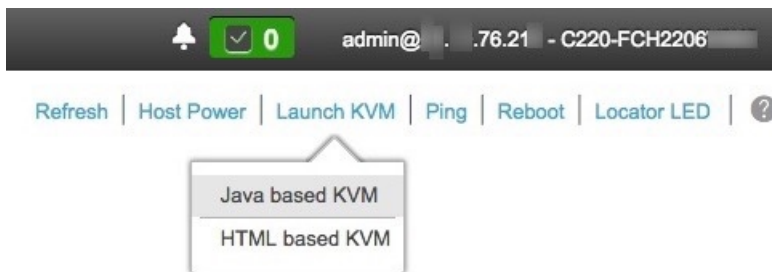
- 各アドオンノードのクラスタ接続プロセス中に、サービスのダウンタイムが発生することが予想されます。サービスはすべてのノードに再配布される必要があり、そのプロセスの間、クラスタはダウンします。

始める前に

次のことを確認します。

- 「[マスターノードの設定](#)」の手順に従って、クラスタ内の最初のアプライアンスが設定されたこと。
- 「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」で必要とされているすべての情報が収集されたこと。
- 「[アプライアンスのインストール ワークフロー](#)」の説明に従って、2 番目と 3 番目のアプライアンスがインストールされたこと。
- 「[CIMC へのブラウザアクセスの有効化](#)」の説明に従って、両方のアドオンアプライアンスで CIMC ブラウザアクセスが設定されたこと。
- 「[事前フライトチェックの実行](#)」の説明に従って、アドオンノードアプライアンスのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- CIMC および Cisco DNA Center と互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する [リリース ノート](#) を参照してください。
- Cisco DNA Center と、次の手順のステップ 8 で指定する DNS サーバとの間のファイアウォールで ICMP が有効になっていること。Maglev 構成ウィザードでは、Ping を使用して、指定した DNS サーバを確認します。Cisco DNA Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が有効になっていない場合、この Ping はブロックされる可能性があります。ブロックされた場合、ウィザードを完了することはできません。

- ステップ 1** CIMC GUI の設定時に設定した CIMC IP アドレスにブラウザでアクセスし、CIMC ユーザとして CIMC GUI にログインします（「[CIMC へのブラウザアクセスの有効化](#)」を参照）。
- ログインが成功すると、次に示すように、アプライアンスに [Cisco Integrated Management Controller Chassis の概要（Cisco Integrated Management Controller Chassis Summary）] ウィンドウが右上の青いリンクメニューとともに表示されます。



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

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

- ステップ 3** KVM が表示されたら、次のいずれかを選択してアプライアンスをリポートします。
- メインの CIMC GUI ブラウザウィンドウで、[ホストの電源（Host Power）] > [電源の再投入（Power Cycle）] を選択します。その後、KVM コンソールに切り替えて続行します。
 - KVM コンソールで、[電源（Power）] > [システムの電源の再投入（コールドブート）（Power Cycle System (cold boot)）] を選択します。

アプライアンスをリポ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、次に示すように、KVM コンソールに Maglev 構成ウィザードのウェルカム画面が表示されます。



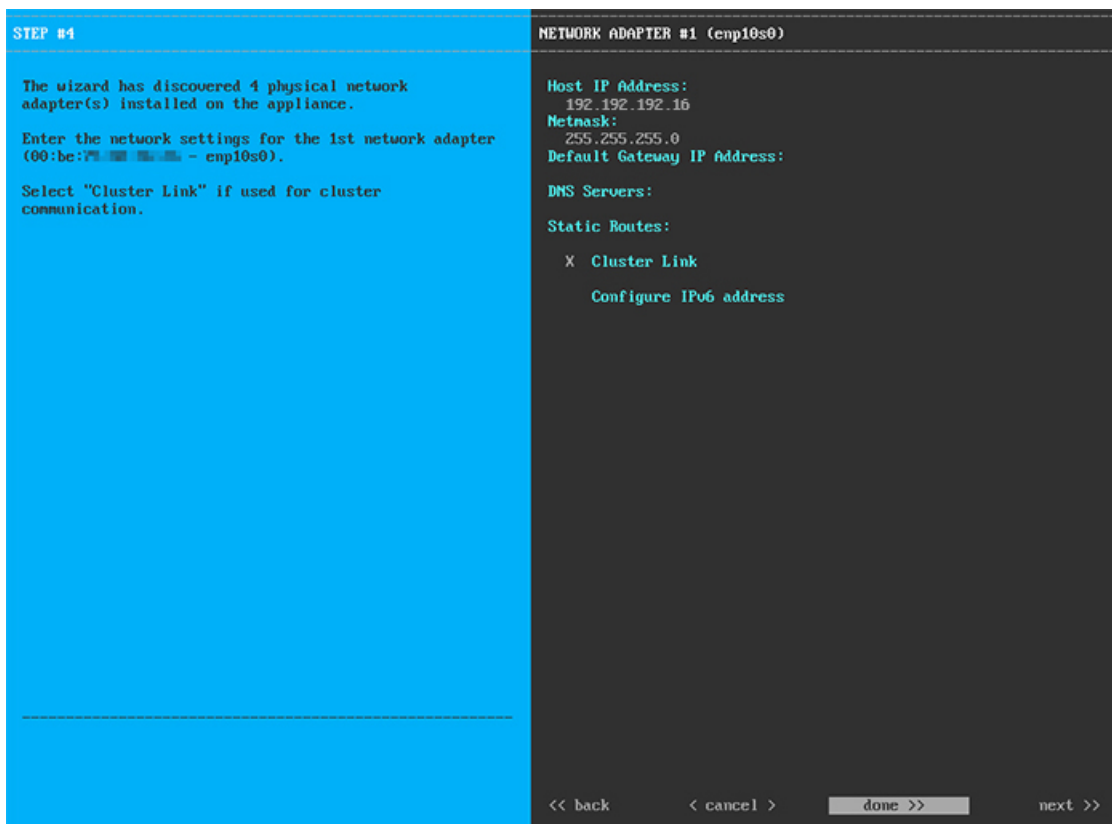
ステップ 4 [DNA-Cクラスタに追加 (Join a DNA-C cluster)] を選択して、アドオンノードの設定を開始します。

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

1. 10Gbps クラスタポート (ポート 2、enp10s0、ネットワークアダプタ #1)
2. 1Gbps Cisco DNA Center GUI ポート (1、enp1s0f0、ネットワークアダプタ #2)
3. 1Gbps クラウドポート (2、enp1s0f1、ネットワークアダプタ #3)
4. 10Gbps エンタープライズポート (ポート 1、enp9s0、ネットワークアダプタ #4)

(注) 設定の過程でウィザードに10Gbpsポートのうちの1つまたは両方が表示されない場合、これらのポートは機能しないか無効になっている可能性があります。これらの10Gbpsポートは、Cisco DNA Center 機能に必要です。10Gbpsポートが機能していないことが判明した場合には、[キャンセル (Cancel)] を選択して、設定をすぐに終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に「[事前フライトチェックの実行](#)」に記載されているすべての手順が完了していることを確認してください。

ステップ 5 ウィザードでは、まず10Gbps クラスタポート (ポート 2、enp10s0) が検出され、[ネットワークアダプタ#1 (NETWORK ADAPTER #1)] として表示されます。「[インターフェイスクーブル接続](#)」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、「[必要なサブネットおよび追加のIPアドレス](#)」と「[必要な設定情報](#)」を参照してください)。



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

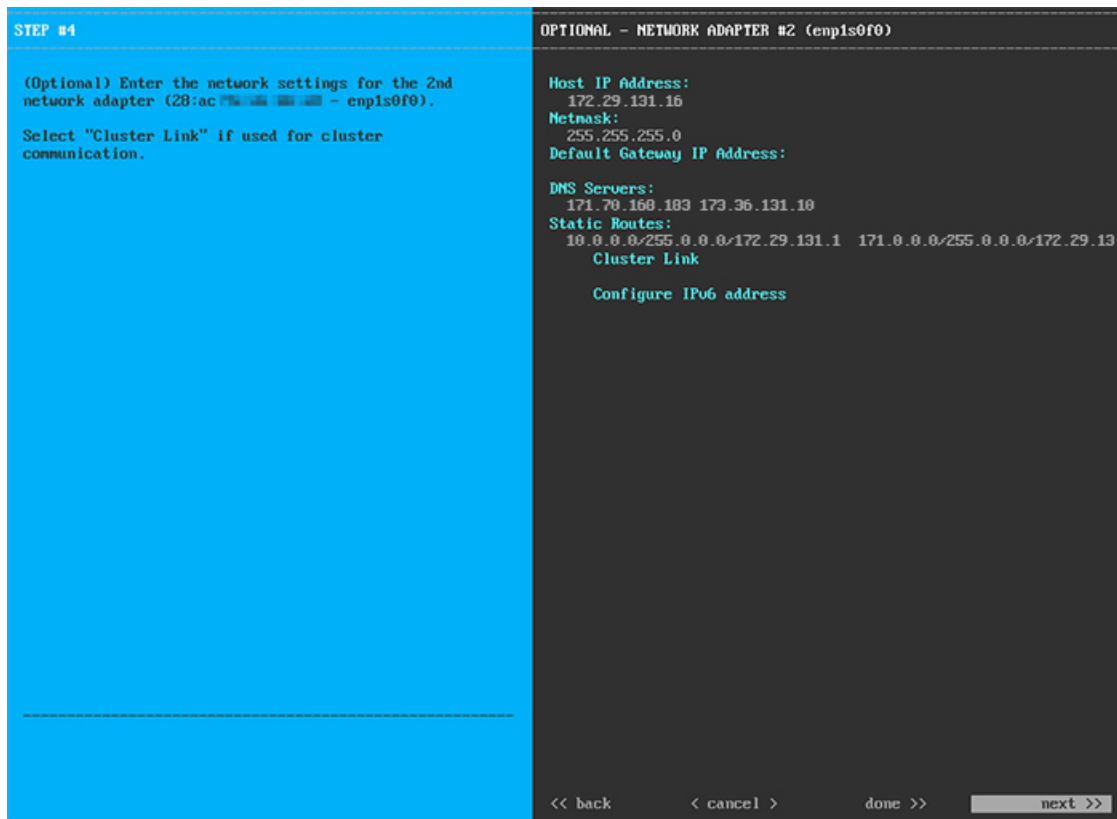
表 29: ネットワークアダプタ #1 のアドオンノードエントリ: 10Gbps クラスタポート (enp10s0)

ホスト IP アドレス	クラスタポートの IP アドレスを入力します。これは必須です。クラスタポートのアドレスは後で変更できないことに注意してください。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルト ゲートウェイの IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

スタティック ルート	1つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。このスタティックルートは、通常、Cisco DNA Center GUI ポートのみで必要になります。
クラスタ リンク	このポートがクラスタへのリンクであることを示すには、このチェックボックスをオンにします。この操作はクラスタポートのみで必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

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

ステップ 6 入力したクラスタポート値の検証が成功すると、ウィザードに 1Gbps Cisco DNA Center GUI ポート (1, enp1s0f0) が [ネットワークアダプタ#2 (NETWORK ADAPTER #2)] としてが表示されます。「[インターフェイスクラスター接続](#)」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、「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」を参照してください)。



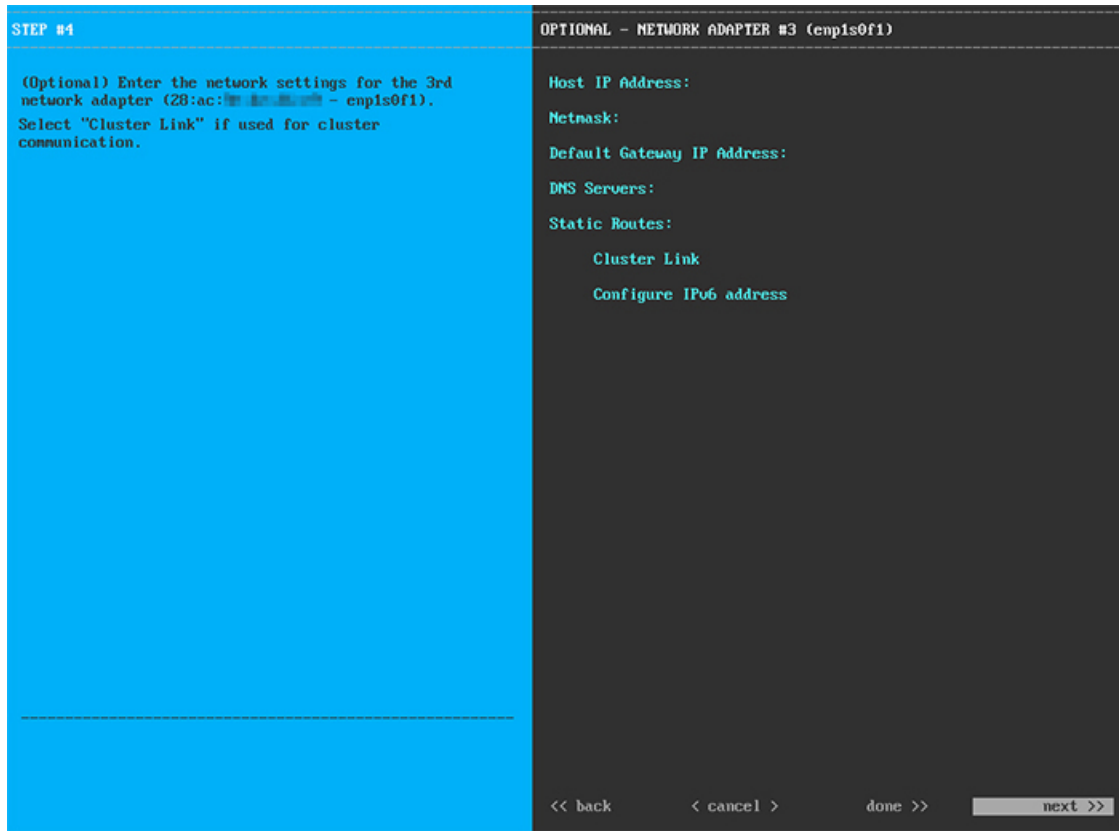
次の表に示すように、[ネットワークアダプタ#2 (NETWORK ADAPTER #2)] の設定値を入力します。

表 30: ネットワークアダプタ #2 のアドオンノードエントリ: 1Gbps GUI ポート (enp1s0f0)

ホスト IP アドレス	1Gbps Cisco DNA Center GUI ポートの IP アドレスを入力します。これは必須です。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルト ゲートウェイの IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。 (注) NTP の場合、Cisco DNA Center と NTP サーバの間のポート 121 (UDP) が開いていることを確認します。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。
クラスタ リンク	このフィールドは空欄のままにします。この操作はクラスタポートのみで必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

- ステップ 7** 入力した Cisco DNA Center GUI ポート値の検証が成功すると、ウィザードに 1Gbps クラウドポート (2、enp1s0f0) が [ネットワークアダプタ#3 (NETWORK ADAPTER #3)] としてが表示されます。「[インターフェイスケーブル接続](#)」で説明したように、このポートは、アプライアンスをインターネットにリンクする際、10Gbps エンタープライズポート (ポート 1、enp9s0) 経由でリンクを実行できない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します (入力する値については、「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」を参照してください)。



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

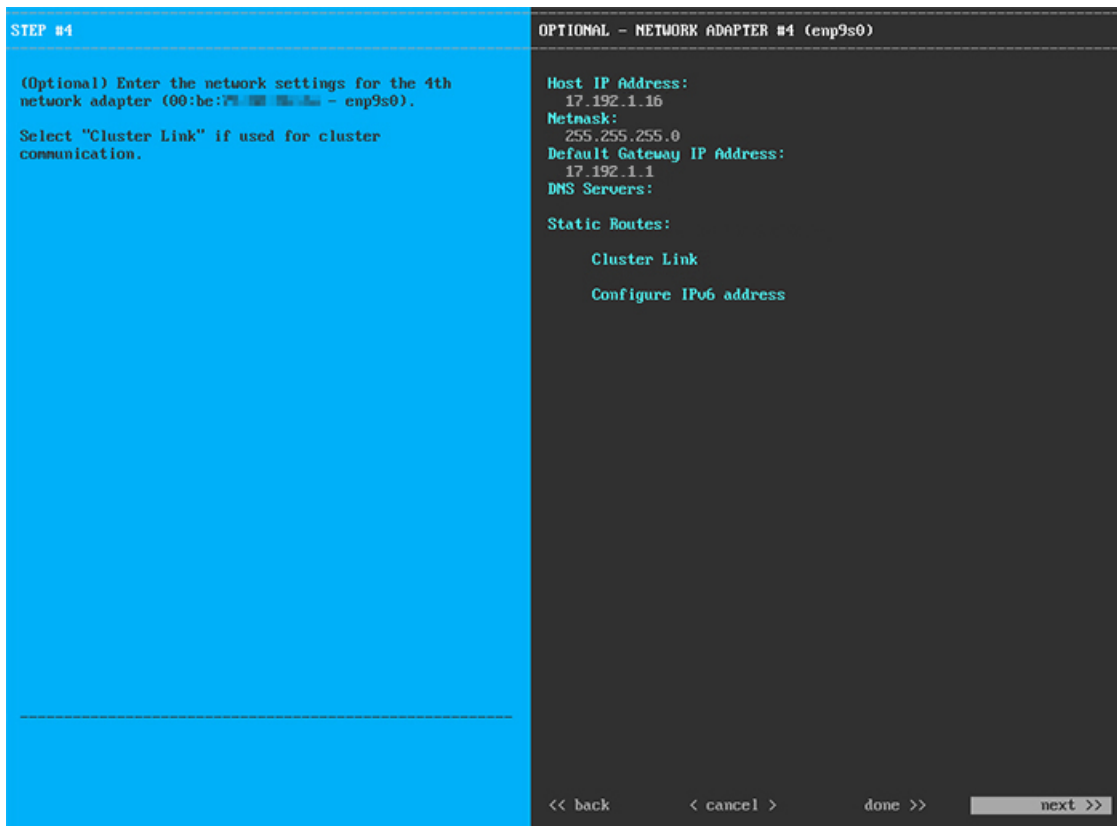
表 31: ネットワークアダプタ #3 のアドオンノードエントリ : 1Gbps クラウドポート (enp1s0f1)

ホスト IP アドレス	クラウドポートの IP アドレスを入力します。この操作は、インターネット接続にクラウドポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにしておくことができます。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。この操作は、IP アドレスを入力する場合に必要になります。
デフォルト ゲートウェイの IP アドレス	クラウドポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。この IP アドレスは、通常、エンタープライズポートのみで必要になります。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

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

終了したら、[次へ>> (next>>)]を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

ステップ 8 入力したクラウドポート値の検証が成功すると、ウィザードに10Gbps エンタープライズポート（ポート 1、enp9s0）が[ネットワークアダプタ#4（NETWORK ADAPTER #4）]として表示されます。「[インターフェイスケーブル接続](#)」で説明したように、このポートは、アプライアンスをエンタープライズ 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、「[必要なサブネットおよび追加の IP アドレス](#)」と「[必要な設定情報](#)」を参照してください）。



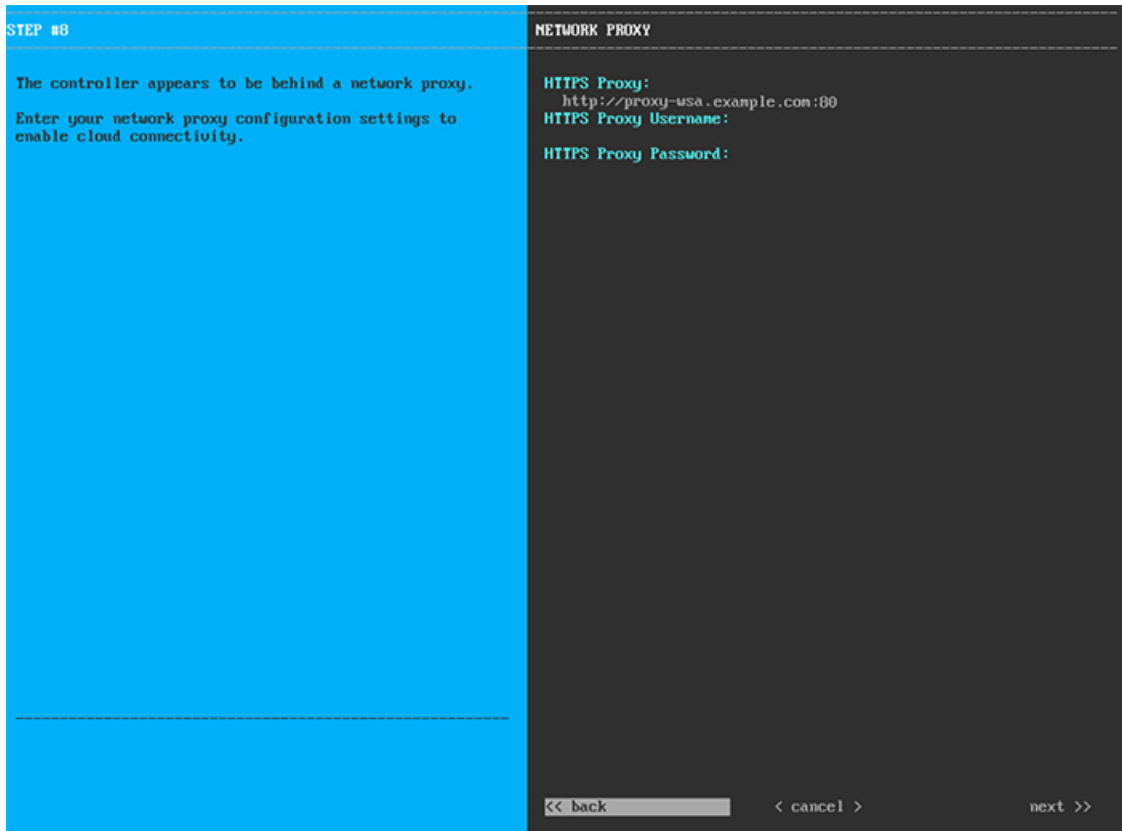
次の表に示すように、[ネットワークアダプタ#4（NETWORK ADAPTER #4）]の設定値を入力します。

表 32: ネットワークアダプタ #4 のアドオンノードエントリ: 10Gbps エンタープライズポート (enp9s0)

ホスト IP アドレス	10Gbps エンタープライズポートの IP アドレスを入力します。これは必須です。
ネットマスク	ポートの IP アドレスに対応するネットマスクを入力します。これは必須です。
デフォルト ゲートウェイの IP アドレス	ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。これは必須です。
DNS サーバ	優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。
スタティック ルート	1 つ以上のスタティックルートをスペースで区切り、<network>/<netmask>/<gateway> の形式で入力します。このスタティックルートは、通常、GUI ポートのみで必要になります。
クラスタ リンク	このフィールドは空欄のままにします。この操作はクラスタポートのみで必要になります。
IPv6 アドレスの設定	将来的な使用のために予約されています。このフィールドは空欄のままにします。

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

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



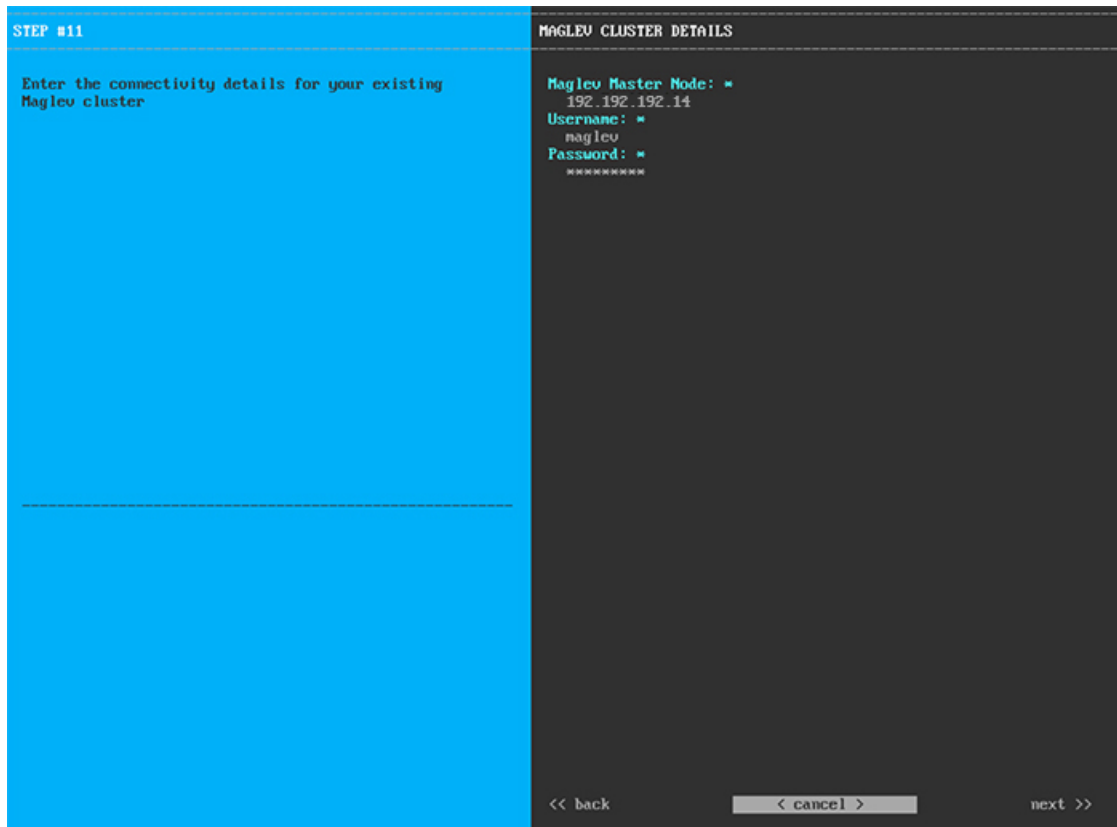
次の表に示すように、[ネットワークアダプタ (NETWORK ADAPTER)] の設定値を入力します。

表 33: ネットワークプロキシのアドオンノードエントリ

<p>HTTPS プロキシ</p>	<p>インターネットへのアクセスに使用される 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) 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。</p>
<p>HTTPS プロキシユーザ名</p>	<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不要ない場合には、このフィールドを空白のままにします。</p>
<p>HTTPS プロキシパスワード</p>	<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不要ない場合には、このフィールドを空白のままにします。</p>

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

ステップ 10 ネットワークプロキシの設定が完了すると、次に示すように、[MAGLEVクラスタの詳細 (MAGLEV CLUSTER DETAILS)] で、マスターノードのクラスタポートとマスターノードのログインの詳細を確認するプロンプトがウィザードに表示されます。



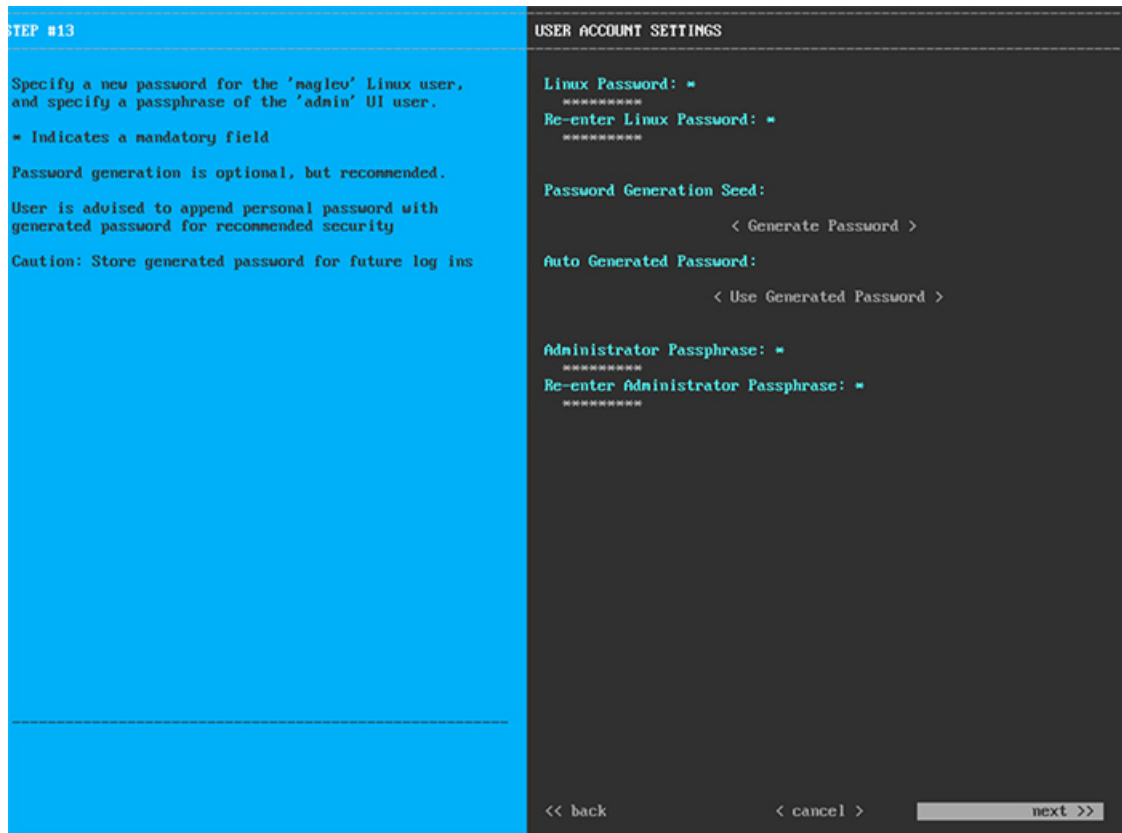
次の表の説明に従って、[MAGLEVクラスタの詳細 (MAGLEV CLUSTER DETAILS)] に値を入力します。

表 34: *Maglev* クラスタの詳細へのアドオンノードエントリ

Maglevマスターノード	クラスタ内のマスターノードでクラスタポートの IP アドレスを入力します。ポート割り当ての推奨事項に従っている場合、この IP アドレスは、マスターノード上のポート 2、enp10s0、ネットワークアダプタ #1 の IP アドレスです。
ユーザ名	maglev と入力します。
パスワード	マスターノードで設定した Linux パスワードを入力します。

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

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



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

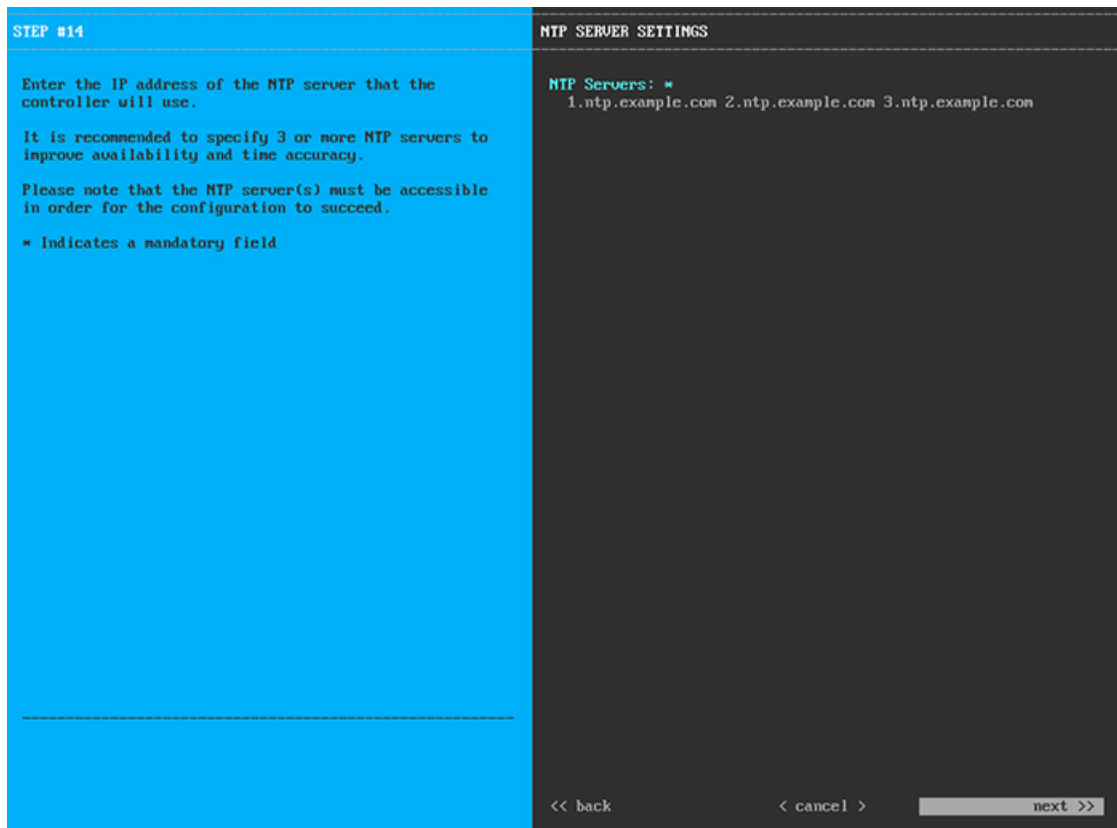
表 35: ユーザアカウント設定のアドオンノードエントリ

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

自動生成パスワード	<p>(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。</p> <p>パスワードを保存するには、[生成されたパスワードを使用 (Use Generated Password)] を押します。</p>
管理者パスフレーズ	<p>デフォルトの管理スーパーユーザ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>
管理者パスフレーズの再入力	<p>管理者パスフレーズをもう一度入力して確認します。</p>

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

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



1 つまたは複数の NTP サーバアドレスまたはホスト名をスペースで区切って入力します。少なくとも 1 つのホスト名または IP アドレスが必要です。このサーバは、マスターノードに対して指定したものと同一 NTP サーバである必要があります。

終了したら、[次へ>> (next>>)] を選択して続行します。以前の画面の場合と同じように、検証エラーを修正します。

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

```

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 >>
    
```

[続行>> (proceed>>)] を選択して設定を完了します。

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

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

次のタスク

タスクが完了した後：

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

ハイアベイラビリティクラスタの導入シナリオ

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

クラスタに導入する場合は、ネットワークに適した導入シナリオを選択します。

- 新しい HA の導入
- 標準インターフェイス設定を使用したマスターノードの既存の HA の導入
- 標準以外のインターフェイス設定を使用したマスターノードの既存の導入

次の項では、各シナリオについて説明します。

新しい HA の導入

最新の HA クラスタをインストールするには、次の手順を実行します。

ステップ1 最初にインストールされたアプライアンスをマスターノードとして設定します。

「[マスターノードの設定](#)」を参照してください。

ステップ2 クラスタ内の2番目と3番目のアプライアンスを設定します。

「[アドオンノードの設定](#)」を参照してください。

標準インターフェイス設定を使用したマスターノードの既存の HA の導入

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

ステップ1 マスターノードを Cisco DNA Center 1.2.10 にアップグレードします。

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

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

「[インターフェイスケーブル接続](#)」を参照してください。

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

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

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

「[アドオンノードの設定](#)」を参照してください。

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

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

glusterfs ファイルシステムのサイズが 150 GB を超える場合には、「[標準以外のインターフェイス設定を使用したマスターノードの既存の HA の導入](#)」の手順を実行します。

標準以外のインターフェイス設定を使用したマスターノードの既存の HA の導入

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

ステップ 1 マスターノードを Cisco DNA Center 1.2.10 にアップグレードします。

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

ステップ 2 リモートリポジトリのバックアップを作成します。

『[Cisco Digital Network Architecture Center 管理者ガイド](#)』の「Backup and Restore」の章を参照してください。

ステップ 3 必要なインターフェイスケーブル設定を使用して、マスターノードを再イメージ化します。

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

ステップ 4 マスターノードで、バックアップ中に選択したものと同一連のパッケージをインストールします。

ステップ 5 ステップ 2 で作成したバックアップファイルを復元します。

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

「[アドオンノードの設定](#)」を参照してください。

HA の導入のその他の考慮事項

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、『[Release Notes for Cisco Digital Network Architecture Center](#)』の「Open Bugs—HA」を参照してください。

テレメトリ

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

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

ステップ 2 デバイスでテレメトリを無効にします。

1. Cisco DNA Center のホーム ページで、[ツール (Tools)] 領域から [テレメトリ (Telemetry)] を選択します。
[テレメトリ (Telemetry)] ウィンドウが表示されます。
2. [サイトの表示 (Site View)] タブをクリックします。
3. テレメトリを無効にするデバイスのチェックボックスをオンにします。次に、[アクション (Actions)] > [テレメトリの無効化 (Disable_Telemetry)] を選択します。

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

ワイヤレス コントローラ

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

Cisco DNA Center の最新リリースへのアップグレード

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



第 5 章

初期設定の完了

- 初期設定ワークフロー (103 ページ)
- 互換性のあるブラウザ (104 ページ)
- 初回ログイン (105 ページ)
- Cisco ISE との統合 Cisco DNA Center (113 ページ)
- 認証サーバとポリシーサーバの設定 (115 ページ)
- SNMP プロパティの設定 (117 ページ)
- サービスの再配布 (118 ページ)

初期設定ワークフロー

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

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

表 36: Cisco DNA Center アプライアンスの初期設定タスク

ステップ	説明
1	互換性のあるブラウザを使用して、Cisco DNA Center にアクセスしていることを確認してください。 互換性のあるブラウザの一覧については、インストールしている Cisco DNA Center のバージョンに対応する リリースノート を参照してください。

ステップ	説明
2	<p>最初に管理者として Cisco DNA Center GUI にログインします。最初の管理ログイン中、次のプロンプトが表示されます。</p> <ol style="list-style-type: none"> 1. 管理スーパーユーザーの新規パスワードを提供します。 2. ソフトウェアイメージをダウンロードし、シスコから電子メール通信を受信するために組織が使用する cisco.com ユーザ名とパスワードを入力します。 3. 組織がスマート アカウント ライセンスを管理するために使用する cisco.com ユーザ名とパスワードを入力します。 4. Cisco DNA Center で使用する予定の IP アドレスマネージャ (IPAM) サーバを設定します。 <p>これらのタスクの詳細については、「初回ログイン」を参照してください。</p>
3	<p>Cisco DNA Center を Cisco Identity Services Engine (ISE) と一緒に使用する予定の場合は、2つが適切に統合されていることを確認してください：Cisco ISE との統合 Cisco DNA Center の統合</p>
4	<p>Cisco DNA Center にポリシーおよび AAA サーバ (ISE を含む) を接続します：認証サーバとポリシー サーバの設定</p>
5	<p>基本的な SNMP の再試行およびポーリングパラメータを設定します：SNMP プロパティの設定</p>
6	<p>HA 動作を最適化するために、クラスタノード間でサービスを再配布します：サービスの再配布</p>
7	<p>初回設定を完了したら：ログアウト</p>

互換性のあるブラウザ

Cisco DNA Center Web インターフェイスは、次の HTTPS 対応ブラウザと互換性があります。

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

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

初回ログイン

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

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

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

始める前に

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

- 「[マスターノードの設定](#)」の手順に従って指定した「管理者」スーパーユーザのユーザ名とパスワード。
- 「[必要な初期設定情報](#)」で必要とされている情報。

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

ステップ 2 Cisco DNA Center GUI へのアクセスに使用するホスト IP アドレスを入力します。

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

ステップ 3 ブラウザに IP アドレスを入力すると、「Your connection is not private（この接続はプライベート接続ではありません）」というメッセージが表示されます。

メッセージを無視して、[詳細設定（Advanced）] をクリックします。

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

このメッセージは、コントローラが自己署名証明書を使用しているために表示されます。後ほど、Cisco DNA Center GUI を使用して信頼できる証明書をアップロードするオプションが表示されます。

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

Cisco DNA Center

Design, Automate and Assure your Network

Username*

Password*

Log In

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



Cisco DNA Center

The Network. Intuitive.

Welcome, Admin! For extra security after the installation please reset the admin password.

Old Password *

New Password *

Confirm New Password *

Skip


Save

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



Welcome to Cisco DNA Center

Please provide your Cisco.com (CCO) ID. This ID will be used to register software downloads, and receive system communications.

Username *	Password *
user123 


[Skip](#)[Next](#)

ステップ7 Cisco.com ユーザのユーザ名とパスワードを入力してから、[次へ (Next)] をクリックします。Cisco.com ユーザログインが既知の Cisco スマート アカウント ユーザ ログインと一致しない場合には、[スマート アカウント (Smart Account)] ウィンドウが表示されます。



Smart Account

Entered CCO didn't match a Smart Account that manages your Cisco software licenses across the entire organization. You can [request a Smart Account](#) or enter a CCO ID that's already associated with one.

Username *	Password *
<input type="text" value="user123"/>	<input type="password" value="....."/> 

[Skip](#)[Back](#)[Next](#)

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




IP Address Manager


If you have an IPAM server, connect it here.


Server Name *
IPAM_Server1

Server URL *
https://sample.ipamserver.com

Username *
user123

Password *
..... 

Provider *
INFOBLOX 

View *
sample_view1 

[Skip](#)[Back](#)[Next](#)

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

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

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



Enter Proxy Server

Proxy Server URL *

http://proxy-wsa.example.com

Port

80

Username

user123

Password

.....



Validate Settings ⓘ

Skip

Back

Next

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

続行する前にこの情報を検証する（推奨）場合には、[設定の検証（Validate Settings）] チェックボックスがオンになっていることを確認します。

確認したら、[Next] をクリックします。ソフトウェアの [EULA] ウィンドウが表示されます。



Terms and Conditions

Your use of the Cisco DNA Center is subject to the [Cisco End User License Agreement \(EULA\)](#) and any relevant supplemental terms (SEULA) found at <https://www.cisco.com>

Cisco DNA Center may collect the following information:

- Usage data, such as Cisco DNA Center feature usage and user response times.
- Network administrator's contact information, including the administrator's e-mail address and phone number, if provided by the administrator.

The usage data collected by Cisco DNA Center will be used to improve offering functionality and features. Users may opt out of this data collection by turning off this feature in the "Settings" menu.

The network administrator's contact information will be used only to contact the administrator for any issues pertaining to Cisco DNA Center. Cisco will not use the contact information for any marketing purposes, and Cisco will not resell or transmit this information to any third-party. Network administrator data is only collected when actually provided by the administrator.

Back

Next

ステップ 11 [次へ (Next)] をクリックして、ソフトウェアのエンドユーザライセンス契約書に同意します。[準備完了 (Ready to go!)] ウィンドウが表示されます。



Ready to go!

You can also go to

- [System 360](#) to check system running status
- [App Management](#) to install Advantage packages.
- [User Management](#) to add new users

You may also go to the Cisco DNA Center Home screen where you can:

- [Get Started](#) to Discover Devices
- Set up your [Site Hierarchy](#) or [Network Profiles](#)

Once devices are onboarded to Cisco DNA Center, you can:

- Provision the devices
- Monitor their health and troubleshoot issues

[Back](#)[Go to System 360](#)

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

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

次のタスク

他の管理セットアップタスクを任意の順序で実行します。

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

Cisco ISE との統合 Cisco DNA Center

このリリースの Cisco DNA Center は、Cisco Identity Services Engine (ISE) との信頼できる通信リンクを作成するメカニズムを提供し、Cisco DNA Center は安全な方法で ISE とデータを共有できます。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 ISE にプッシュされます。ユーザは、Cisco DNA Center を使用してデバイスを検出し、Cisco DNA Center と ISE の両方の機能をそれらに適用できます。これは、これらのデバイスが両方のアプリケーションに公開されるためです。Cisco DNA Center および ISE デバイスはすべてデバイス名で一意的に識別されます。

Cisco DNA Center デバイスは、Cisco DNA Center サイト階層内の特定のサイトにプロビジョニングされて所属すると、即座に ISE にプッシュされます。Cisco DNA Center デバイスに対するすべての更新 (IP アドレス、SNMP または CLI クレデンシャル、ISE 共有秘密の変更など) は、ISE の対応デバイス インスタンスに自動的に流れます。Cisco DNA Center デバイスが削除されると、ISE から削除されます。Cisco DNA Center デバイスが ISE にプッシュされるのは、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

ISE を Cisco DNA Center に統合する前に、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 ISE バージョン 2.3 (以降) のホストを展開済みである。ISE のインストールについては、『[Cisco Identity Services Engine インストールおよびアップグレードガイド](#)』 (バージョン 2.3 以降用) を参照してください。
- スタンドアロン ISE 導入環境がある場合は、ISE ノード上で pxGrid サービスおよび ERS と統合し、これらを有効化する必要がある。
- 分散型 ISE 導入環境がある場合は、次の要件を満たす必要がある。
 - Cisco DNA Center を ISE 管理ノード (PAN プライマリ) に統合し、PAN 上で ERS を有効化する必要がある。
 - 単一ノードの導入環境と同様に、分散型の導入環境内のいずれかの ISE ノード上で pxGrid サービスを有効化する必要がある。PAN 上で pxGrid サービスを有効化することを選択できますが、必須ではありません。分散型の導入環境では、他の任意の ISE ノード上で pxGrid を有効化できます。
- pxGrid が有効化されている ISE ホストには、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る。
- ISE ノードが、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る。
- ISE ノードで、SSH が有効化されている。

- ISE CLI および GUI のユーザアカウントには、同じユーザ名とパスワードが使用されている必要がある。
- ISE 管理ノードの証明書には、証明書の件名または SAN のいずれかに ISE の IP アドレスまたは完全修飾ドメイン名 (FQDN) が含まれている必要がある。
- Cisco DNA Center システム証明書の [サブジェクト代替名 (SAN) (Subject Alternative Name (SAN))] フィールドに、Cisco DNA Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要がある。

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

- a) ISE プライマリ管理ノード (PAN) にログインします。
- b) [管理 (Administration)] > [展開 (Deployment)] を選択します。
- c) pxGrid サービスを有効化する ISE ノードのホスト名を選択します。分散型の導入環境の場合、これは導入環境内の任意の ISE ノードです。
- d) [全般設定 (General Settings)] タブで、[pxGrid] チェック ボックスがオンになっていることを確認します。
- e) [Save (保存)] をクリックします。
- f) [管理 (Administration)] > [システム (System)] > [設定 (Settings)] > [ERS設定 (ERS Settings)] の順に選択し、[ERSの読み取り/書き込みの有効化 (Enable ERS for Read/Write)] をクリックします。確認プロンプトで、[OK] をクリックします。

ステップ 2 次のように、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 Web ベースの GUI にログインします。
- b)  をクリックして、[システム設定 (System Settings)] を選択します。
- c) Cisco ISE パネルで、[設定の構成 (Configure Settings)] リンクを選択します。
- d) [設定 - 認証サーバとポリシーサーバ (Settings - Authentication and Policy Servers)] ページで、大きいプラス (+) アイコンをクリックして AAA の設定を表示します。
- e) [Cisco ISE] スライダーをクリックして、すべての ISE 関連フィールドが表示されていることを確認します。
- f) [IP アドレス (IP address)] フィールドに、ISE 管理 IP アドレスを入力します。
- g) ネットワークデバイスと ISE 間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。
- h) 該当する ISE 管理クレデンシャルを [ユーザ名 (Username)] と [パスワード (Password)] フィールドに入力します。
- i) ISE ノードの [FQDN] を入力します。
- j) [サブスクライバ名 (Subscriber Name)] を入力します (例: `cdnacenter`)。
- k) [SSH キー (SSH Key)] はオプションであり、空白のままにできます。


ステップ 3 これらのフィールドに入力したら、[更新 (Update)] をクリックして、サーバのステータスが [アクティブ (Active)] として表示されるまで待機します。

ステップ 4 ISE が Cisco DNA Center に接続され、接続にサブスクライバがあることを確認します。

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

- b) [管理 (Administration)] > [pxGrid サービス (pxGrid Services)] を選択します。入力した名前 (例: **cdnacenter**) を持つサブスクリバの現在のステータスが [オンライン (online)] であることを確認できます。
- c) サブスクリバのステータスが [保留中 (Pending)] である場合は、[保留中の承認の合計 (Total Pending Approval)] > [すべてのクライアントの承認 (Approve All Clients)] の順に選択し、このサブスクリバを承認します。サブスクリバのステータスが [オンライン (online)] に変わります。

ステップ 5 次のように、Cisco DNA Center が ISE に接続されており、ISE SGT のグループとデバイスが Cisco DNA Center にプッシュされていることを確認します。

- a) Cisco DNA Center Web ベースの GUI にログインします。
- b)  をクリックして、[システム設定 (System Settings)] を選択します。
- c) Cisco ISE パネルで、[設定の構成 (Configure Settings)] リンクを選択します。
- d) [設定 - 認証サーバとポリシーサーバ (Settings - Authentication and Policy Servers)] ページで、大きいプラス (+) アイコンをクリックして AAA の設定を表示します。
- e) Cisco ISE の 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。
- f) [ポリシー (Policy)] > [レジストリ (Registry)] > [スケーラブルグループ (Scalable Groups)] の順に選択します。スケーラブルグループのリストに ISE SGT グループが表示されます。

認証サーバとポリシーサーバの設定

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

始める前に

- Cisco ISE を使用してポリシーと AAA 機能の両方を実行する場合、Cisco DNA Center および Cisco ISE が「[Cisco ISE との統合 Cisco DNA Center](#)」の説明に従って統合されたことを確認します。
- 他の製品 (Cisco ISE 以外) を使用して AAA 機能を実行している場合は、必ず次の操作を実行してください。
 - AAA サーバで Cisco DNA Center を登録します。これには、AAA サーバと Cisco DNA Center の共有秘密キーを定義することを含めます。
 - AAA サーバで Cisco DNA Center の属性名を定義します。
 - Cisco DNA Center 複数ホスト クラスタの設定の場合は、AAA サーバの複数ホスト クラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。

ステップ 1 Cisco DNA Center のホームページで、 > [システム設定 (System Settings)] > [設定 (Settings)] > [認証サーバとポリシーサーバ (Authentication and Policy Servers)] の順に選択します。

ステップ2  **Add** をクリックします。

ステップ3 次の情報を入力して、プライマリ AAA サーバを設定します。

- **サーバの IP アドレス** : AAA サーバの IP アドレス。
- **[共有秘密キー (Shared Secret)]** : デバイス認証キー。共有秘密キーの長さは、最大 128 文字です。

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

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

- **[Cisco ISE]** : サーバが Cisco ISE サーバかどうかを示す設定。 **[Cisco ISE]** 設定をクリックして Cisco ISE を有効化します。
- **[ユーザ名 (Username)]** : Cisco ISE コマンドライン インターフェイス (CLI) にログインするために使用する名前。
(注) このユーザはスーパー管理者である必要があります。
- **[パスワード (Password)]** : Cisco ISE CLI ユーザ名に対応するパスワード。
- **[FQDN]** : Cisco ISE サーバの完全修飾ドメイン名 (FQDN)。
(注)
 - Cisco ISE (**[管理 (Administration)]**) > **[導入 (Deployment)]** > **[導入ノード (Deployment Nodes)]** > **[リスト (List)]** で定義されている FQDN をコピーして、このフィールドに直接貼り付けすることをお勧めします。
 - 入力した FQDN は、Cisco ISE 証明書で定義されている FQDN、共通名 (CN) または Subject Alternative Name (SAN) と一致する必要があります。

FQDN は、次の形式で、ホスト名およびドメイン名の 2 つのパートで構成されています。

hostname.domainname.com

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

- **[サブスクライバ名 (Subscriber Name)]** : Cisco ISE pxGrid サービス登録時の pxGrid クライアントを識別する一意のテキスト文字列。acme など。ユーザ名は Cisco DNA Center を Cisco ISE に統合中に使用されます。
- **[SSH キー (SSH Key)]** : Cisco ISE と接続し、認証するために使用される Diffie-Hellman-Group14-SHA1 SSH キー。
- **[仮想 IP アドレス (Virtual IP address(es))]** : Cisco ISE ポリシー サービス ノード (PSN) の前面にあるロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN フェームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

ステップ5 **[詳細設定の表示 (View Advanced Settings)]** をクリックして、次の設定を行います。

- [プロトコル (Protocol)] : TACACS または RADIUS。
(注) グレー表示されるオプションは、選択したオプションです (デフォルトでは RADIUS)。
TACACS オプションを選択するには、TACACS オプションを選択してから、RADIUS オプションの選択を手動で解除する必要があります。
- [認証ポート (Authentication Port)] : AAA サーバへの認証メッセージのリレーに使用されるポート。
デフォルト値は UDP ポート 1812 です。
- [アカウンティング ポート (Accounting Port)] : AAA サーバへの重要なイベントのリレーに使用されるポート。これらのイベントの情報は、セキュリティおよび請求目的で使用されます。デフォルトの UDP ポートは 1813 です。
- [再試行回数 (Retries)] : 接続の試行が中止される前に、Cisco DNA Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は 1 回です。
- [タイムアウト (Timeout)] : 接続の試行が中止される前に、デバイスが AAA サーバの応答を待機する時間。

ステップ 6 [追加 (Add)] をクリックします。

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

SNMP プロパティの設定

SNMP の再試行とタイムアウトの値を設定することができます。

始める前に

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

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

ステップ 2 次のフィールドを設定します。

表 37: SNMP Properties


フィールド	説明
リトライ (Retries)	デバイスへ接続可能な試行回数。有効な値は 1 ~ 3 です。デフォルトは 3 です。
タイムアウト(秒)	タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Cisco DNA Center が待機する秒数。有効な値は、5 秒間隔で 1 ~ 300 秒です。デフォルトは 5 秒です。

ステップ 3 [Apply] をクリックします。

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

サービスの再配布

Cisco DNA Center のハイアベイラビリティ (HA) の実装については、『[Cisco Digital Network Architecture Center Administrator Guide](#)』を参照してください。最初にこの情報を確認してから、実稼働環境に HA を導入するかどうかを決定することを推奨します。導入を選択する場合は、クラスタノード間でサービスを再配布することによって HA の動作を最適化します。

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

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

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

[サービス配布の有効化 (Enable Service Distribution)] をクリックすると、Cisco DNA Center がメンテナンスモードになります。メンテナンス モードでは、プロセスが完了するまで Cisco DNA Center を利用できなくなります。HA 導入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 のためのサービス再配布の有効化を実行すると、(前述のとおり) メンテナンスモードになります。
-



第 6 章

展開のトラブルシューティング

- [トラブルシューティング タスク \(119 ページ\)](#)
- [ログアウト \(120 ページ\)](#)
- [設定ウィザードを使用したアプライアンスの再設定 \(120 ページ\)](#)
- [アプライアンスの電源を切って再度入れる \(122 ページ\)](#)

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。

表 38: 基本的なトラブルシューティング タスク

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

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 Web ベース GUI インターフェイスからログアウトします。

セキュリティ上の理由から、作業セッションの完了時には毎回ログアウトすることを推奨します。ユーザーがログアウトしない場合、非アクティブ状態になってから 30 分後に自動的にログアウトされます。

ステップ 1 * をクリックします。

ステップ 2 [サインアウト (SignOut)] をクリックします。これにより、セッションが終了してログアウトされます。

設定ウィザードを使用したアプライアンスの再設定

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

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

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

始める前に

次のものがが必要です。

- Secure Shell (SSH) クライアント ソフトウェア。

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

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

```
ssh maglev@エンタープライズポートの IP アドレス -p 2222
```

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

ステップ 3 次のコマンドを入力して設定ウィザードにアクセスします。

```
$ sudo maglev-config update
```

Linux パスワードのプロンプトが表示されたら、再度入力します。

ステップ 4 設定ウィザードには、「[アドオンノードの設定](#)」の場合に表示される画面と同じ一連の画面の短縮バージョンが表示されます。必要に応じて、表示されている設定を変更します。各画面で変更を終えたら、**[次へ (Next)]** を選択して設定ウィザードを続行します。

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

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

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

設定プロセスの最後に、「**設定に成功しました (CONFIGURATION SUCCEEDED!)**」というメッセージが表示されます。

次のタスク

「[アプライアンスの電源を切って再度入れる](#)」のトピックで説明されているように、アプライアンスの電源を切ってから再度電源を入れて、変更が適用され、アクティブになっていることを確認します。



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

アプライアンスの電源を切って再度入れる

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

Cisco ICM GUI と、Cisco IMC GUI からアクセス可能な KVM コンソールを使用して、アプライアンスの電源を再投入することも可能であることに注意してください。詳細については、「[マスターノードの設定](#)」または「[アドオンノードの設定](#)」の手順 1～3 を参照してください。



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

始める前に

次のものがが必要です。

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

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

```
ssh maglev@[エンタープライズポートの IP アドレス] -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 パスワードの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。

■ アプライアンスの電源を切って再度入れる