



Cisco Catalyst Center 3.2.x 3

Cisco Catalyst Center
Updated May 12, 2026

短縮されたシスコの商標

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

第 1 章 : Catalyst Center アプライアンス機能の確認	7
アプライアンスのハードウェア仕様	8
中型 Catalyst Center アプライアンス	8
大規模 Catalyst Center アプライアンス	10
特大規模 Catalyst Center アプライアンス	12
前面パネルと背面パネル	14
32 コアおよび 56 コア アプライアンス	14
80 コアアプライアンス	24
物理仕様	33
32 コアおよび 56 コア アプライアンス	33
80 コアアプライアンス	33
環境仕様	35
電源装置の仕様	36
32 コアおよび 56 コア アプライアンス	36
80 コアアプライアンス	37
第 2 章 : 導入の計画	39
プランニングワークフロー	40
Catalyst CenterおよびCisco Software-Defined Access	40
インターフェイスケーブル接続	40
必要な IP アドレスおよびサブネット	44
必要なインターネット URL と完全修飾ドメイン名	48
インターネットへのアクセスを保護する	52
通信ポート	53
HTTP ポート 80 例外リスト	58
ディザスタリカバリポート	59
Cisco Software-Defined Access の必要なポートとプロトコル	62
必須の設定情報	70
必要な初期設定情報	71
パスワードポリシー	73
パスワード要件	73
第 3 章 : アプライアンスの設置	75
アプライアンスのインストール ワークフロー	76
アプライアンスを開梱して点検	76
インストール警告とガイドラインの確認	76
ステートメント 1071 - 警告の定義	78
ステートメント 1005 - 遮断器	78

ステートメント 1074 - 地域および国の電気規則への適合.....	78
ステートメント 1017 - 立ち入り制限区域.....	79
ラック要件の確認.....	79
アプライアンスの接続および電源投入.....	80
LED の確認.....	80
32 コアおよび 56 コア アプライアンス.....	81
80 コアアプライアンス.....	82

第 4 章 : アプライアンスの設定準備.....85

アプライアンス設定の準備の概要.....	86
Cisco Integrated Management Controller に対するブラウザアクセスの有効化.....	86
事前設定タスクの実行.....	91
NIC ボンディングの概要.....	94
アプライアンスサポート.....	96
アプライアンスのイメージの再作成.....	96
Catalyst Center イメージの確認.....	97
ブート可能な USB フラッシュドライブの作成.....	98
Catalyst Center アプライアンスの仮想ドライブの再初期化.....	101
Catalyst Center ISO イメージのインストール.....	102
Catalyst Center アプライアンスの設定.....	103

第 5 章 : Maglev ウィザードを使用したアプライアンスの設定.....105

アプライアンスの設定の概要.....	106
IPv4 および IPv6 の考慮事項.....	106
パスワードの考慮事項.....	106
VLAN モードの考慮事項.....	107
Maglev ウィザードを使用したプライマリノードの設定.....	107
FIPS モードのサポート.....	130
Maglev ウィザードを使用したセカンダリノードの設定.....	131
最新の Catalyst Center リリースへのアップグレード.....	153

第 6 章 : ブラウザベースのウィザードを使用した 32 コアおよび 56 コアアプライアンス

の設定.....155

アプライアンスの設定の概要.....	156
ブラウザベースの構成ウィザード.....	156
パスワードの考慮事項.....	157
VLAN モードの考慮事項.....	157
インストール構成ウィザードを使用したアプライアンスの設定.....	158
詳細インストール構成ウィザードを使用したプライマリノードの設定.....	169
詳細インストール構成ウィザードを使用したセカンダリノードの設定.....	186
最新の Catalyst Center リリースへのアップグレード.....	203

第 7 章 : ブラウザベースのウィザードを使用した 80 コアアプライアンスの設定	205
アプライアンスの設定の概要	206
ブラウザベースの構成ウィザード	206
パスワードの考慮事項	207
VLAN モードの考慮事項	207
インストール構成ウィザードを使用したアプライアンスの設定	208
詳細インストール構成ウィザードを使用したプライマリノードの設定	219
詳細インストール構成ウィザードを使用したセカンダリノードの設定	236
最新の Catalyst Center リリースへのアップグレード	253
第 8 章 : 初期設定の完了	255
初期設定ワークフロー	256
互換性のあるブラウザ	256
Catalyst Center への初回ログイン	256
クイック スタート ワークフローの完了	259
デバイスログイン情報	260
Catalyst Center の設定方法	264
Express セットアップを完了します	265
標準セットアップの完了	267
エキスパート設定の完了	269
Cisco ISE と Catalyst Center の統合	270
グループベースのアクセスコントロール : ポリシーデータの移行と同期	274
認証サーバーとポリシーサーバーの設定	276
SNMP プロパティの設定	280
第 9 章 : 展開のトラブルシューティング	283
トラブルシューティング タスク	284
ログアウト	284
構成ウィザードを使用したアプライアンスの再設定	284
アプライアンスの電源の再投入	285
SSH を使用	286
Cisco IMC GUI を使用	286
付録 A : ハイ アベイラビリティ クラスターの展開シナリオの確認	289
新しい HA の展開	290
標準インターフェイス設定を使用したプライマリノードの既存 HA の展開	290
非標準インターフェイス設定を使用したプライマリノードの既存 HA の展開	291
HA のアクティブ化	292
HA の展開に関する追加の考慮事項	292
テレメトリ	292
ワイヤレスコントローラ	293

第

1 Catalyst Center

章

- :

 - [XXXXXXXXXXXXXXXXXXXX](#)
 - [XXXXXXXXXXXX](#)
 - [XXXX](#)
 - [XXXX](#)
 - [XXXXXXX](#)
-

Catalyst Center アプライアンスのハードウェア仕様へのリンクを提供します。

シスコは、これらのハードウェア仕様を備えたラックマウント可能な物理アプライアンスとして Catalyst Center を提供しています。

Catalyst Center

第 3 世代中型 Catalyst Center アプライアンスのハードウェア仕様を示します。

次の表に、第 3 世代中型 Catalyst Center アプライアンスのハードウェア仕様を示します。

1: Catalyst Center

機能	説明
シスコ製品番号	DN3-HW-APL
シャーシ	1 ラックユニット (1RU) Cisco Unified Computing System (UCS) C220 M6 シャーシ
コア数	32
プロセッサ	2 つのインテル Xeon Gold 6326 プロセッサ
メモリ	8 x 32 GB DDR4 3200 MHz 登録済み DIMM (RDIMM)
ストレージ/ディスク管理 (RAID)	4GB FBWC を搭載した Cisco RAID コントローラ : • 2 x 960 GB SSD、RAID 1 (スロット 1 および 2) • 2 x 1.9 TB SSD、RAID 1 (スロット 3 および 4) • 6 x 1.9 TB SSD、RAID 10 (スロット 5 ~ 10)

機能	説明
ネットワークおよび管理 I/O	サポートされるコネクタ： • Intel E810-XXVDA2 ネットワークアダプタの 2 つの 1 Gbps/10 Gbps/25 Gbps イーサネット ポート • Intel E810-XXVDA4 ネットワークアダプタの 4 つの 1 Gbps/10 Gbps/25 Gbps イーサネット ポート  注 これらのポートは、アプライアンスで NIC ボンディングが有効になっている場合にのみアクティブになります。詳細については、NIC ボンディングの概要 (94 ページ) を参照してください。 • 1 Gb イーサネット専用管理ポート X1 (RJ-45 コネクタ) • 1 Gb/10 Gb BASE-T イーサネット LAN ポート X 2 (RJ-45 コネクタ) デュアル LAN ポートは、10 Gbps、1 Gbps、100 Mbps、または 10 Mbps をサポートします。LAN ポートは、リンクパートナー機能に基づいて適切なリンク速度を自動ネゴシエートします。 次のコネクタを使用できますが、通常は Catalyst Center の日常業務では使用されません。 • RS-232 シリアル ポート (RJ-45 コネクタ) X 1 • VGA ビデオ コネクタ ポート X1 (DB-15 コネクタ) • USB 3.0 ポート x 2 • KVM ブレークアウトケーブルとともに使用する前面パネルキーボード/ビデオ/マウス (KVM) コネクタ x 1。ブレイクアウト ケーブルは、タイプ A USB 2.0 コネクタ x 2、VGA (DB-15) コネクタ x 1、DB-9 シリアル コネクタ x 1 を接続可能です。
電源	2300 W AC 電源 X 2 1+1 冗長性
冷却	ホットスワップ可能なファンモジュール (前面から背面への冷却用) x 8。
ビデオ	Cisco Integrated Management Controller (CIMC) は、Matrox G200e ビデオ/グラフィックス コントローラを使用してビデオを提供します。 • ハードウェア アクセラレーションを備えた内蔵 2D グラフィックスコア • DDR3 メモリインターフェイスは最大 512MB のアドレス可能メモリをサポート (デフォルトでは 8 MB がビデオメモリに割り当てられる) • 最大 1920 X 1200 16bpp、60Hz のディスプレイ解像度をサポートします。 • 高速な内蔵 24 ビット RAMDAC • 第 2 世代の速度で動作するシングル レーン PCI-Express ホスト インターフェイス

機能	説明
ACPI	Advanced Configuration and Power Interface (ACPI) 4.0 規格をサポートしています。
組み込み管理プロセッサ	Cisco Integrated Management Controller (Cisco IMC) ファームウェアを実行するベースボード管理コントローラ (BMC)。 CIMC の設定に応じて、1GE 管理専用ポート、1GE/10GE LOM ポート、または Cisco 仮想インターフェイス カード (VIC) を介して CIMC にアクセスできます。

Catalyst Center

第 3 世代の大規模 Catalyst Center アプライアンスのハードウェア仕様を一覧表示します。

次の表に、第 3 世代の大規模 Catalyst Center アプライアンスのハードウェア仕様を示します。

2: Catalyst Center

機能	説明
シスコ製品番号	DN3-HW-APL-L
シャーシ	1RU Cisco UCS C220 M6 シャーシ
コア数	72
プロセッサ	インテル Xeon Gold 6348 プロセッサ x 2
メモリ	32 GB DDR4 3200 MHz RDIMM x 12
ストレージ/ディスク管理 (RAID)	4GB FBWC を搭載した Cisco RAID コントローラ : • 2 x 960 GB SSD、RAID 1 (スロット 1 および 2) • 2 x 3.8 TB SSD、RAID 1 (スロット 3 および 4) • 6 x 3.8 TB SSD、RAID 10 (スロット 5 ~ 10)

機能	説明
ネットワークおよび管理 I/O	サポートされるコネクタ： • Intel E810-XXVDA2 ネットワークアダプタの 2 つのイーサネット ポート (1 Gbps/10-Gbps/25 Gbps) • Intel E810-XXVDA4 ネットワークアダプタの 4 つのイーサネット ポート (1 Gbps/10-Gbps/25 Gbps)  注 これらのポートは、アプライアンスで NIC ボンディングが有効になっている場合にのみアクティブになります。詳細については、NIC ボンディングの概要 (94 ページ) を参照してください。 • 1 Gb イーサネット専用管理ポート X1 (RJ-45 コネクタ) • 1 Gb/10 Gb BASE-T イーサネット LAN ポート X 2 (RJ-45 コネクタ) デュアル LAN ポートは、10 Gbps、1 Gbps、100 Mbps、または 10 Mbps をサポートします。LAN ポートは、リンクパートナー機能に基づいて適切なリンク速度を自動ネゴシエートします。 次のコネクタを使用できますが、通常は Catalyst Center の日常業務では使用されません。 • RS-232 シリアル ポート (RJ-45 コネクタ) X 1 • VGA ビデオ コネクタ ポート X1 (DB-15 コネクタ) • USB 3.0 ポート x 2 • KVM ブレークアウトケーブルとともに使用する前面パネルキーボード/ビデオ/マウス (KVM) コネクタ x 1。ブレークアウトケーブルには、USB 2.0 X 2、VGA X 1、DB-9 シリアルコネクタ X 1 を接続できます。
電源	2300 W AC 電源 X 2 1 + 1 の冗長構成です。
冷却	ホットスワップ可能なファンモジュール (前面から背面への冷却用) x 8。
ビデオ	Cisco IMC は Matrox G200e ビデオおよびグラフィックコントローラを使用してビデオを提供します。 • ハードウェア アクセラレーションを備えた内蔵 2D グラフィックスコア • DDR3 メモリインターフェイスは最大 512MB のアドレス可能メモリをサポート (デフォルトでは 8 MB がビデオメモリに割り当てられる) • 最大 1920 X 1200 16bpp、60Hz のディスプレイ解像度をサポートします。 • 高速な内蔵 24 ビット RAMDAC • 第 2 世代の速度で動作するシングル レーン PCI-Express ホストインターフェイス
ACPI	ACPI 4.0 標準がサポートされています。

機能	説明
組み込み管理プロセッサ	Cisco IMC ファームウェアを実行する BMC。 CIMC の設定に応じて、1GE 管理専用ポート、1GE/10GE LOM ポート、または Cisco VIC を介して CIMC にアクセスできます。

Catalyst Center

第 3 世代の特大規模 Catalyst Center アプライアンスのハードウェア仕様を示します。

次の表に、第 3 世代特大規模 Catalyst Center アプライアンスのハードウェア仕様を示します。

3: Catalyst Center

機能	説明
シスコ製品番号	DN3-HW-APL-XL
シャーシ	2 ラックユニット (2RU) Cisco UCS C240 M6 シャーシ
コア数	80
プロセッサ	Intel Xeon Platinum 8380 プロセッサ x 12
メモリ	64 GB DDR4 3200 MHz RDIMM x 12
ストレージ/ディスク管理 (RAID)	4GB FBWC を搭載した Cisco RAID コントローラ : ● 2 x 960 GB SSD、RAID 1 (スロット 1 および 2) ● 2 x 3.8 TB SSD、RAID 1 (スロット 3 および 4) ● 8 x 3.8 TB SSD、RAID 10 (スロット 5 ~ 12)
ディスク管理 (RAID)	4GB FBWC を搭載した Cisco RAID コントローラ : ● スロット 1 ~ 4 の RAID 1 ● スロット 5 ~ 12 の RAID 10

機能	説明
ネットワークおよび管理 I/O	サポートされるコネクタ： • Intel E810-XXVDA2 ネットワークアダプタの 2 つのイーサネット ポート (1 Gbps/10-Gbps/25 Gbps) • Intel E810-XXVDA4 ネットワークアダプタの 4 つのイーサネット ポート (1 Gbps/10-Gbps/25 Gbps)  注 これらのポートは、アプライアンスで NIC ボンディングが有効になっている場合にのみアクティブになります。詳細については、NIC ボンディングの概要 (94 ページ) を参照してください。 • 1 Gbps イーサネット専用管理ポート x 1 (RJ-45 コネクタ) • イーサネット LAN ポート x 2 (1 Gbps/10 Gbps BASE-T) (RJ-45 コネクタ) デュアル LAN ポートは、10 Gbps、1 Gbps、100 Mbps、または 10 Mbps をサポートします。LAN ポートは、リンクパートナー機能に基づいて適切なリンク速度を自動ネゴシエートします。 次のコネクタを使用できますが、通常は Catalyst Center の日常業務では使用されません。 • RS-232 シリアル ポート (RJ-45 コネクタ) X 1 • VGA ビデオ コネクタ ポート X1 (DB-15 コネクタ) • USB 3.0 ポート x 2 • KVM ブレークアウトケーブルとともに使用する前面パネルキーボード/ビデオ/マウス (KVM) コネクタ x 1。ブレークアウトケーブルには、USB 2.0 X 2、VGA X 1、DB-9 シリアルコネクタ X 1 を接続できます。
電源	2300 W AC 電源 x 2 1+1 冗長性
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) X6。
ビデオ	Cisco IMC は Matrox G200e ビデオ/グラフィックコントローラを使用してビデオを提供します。 • ハードウェア アクセラレーションを備えた内蔵 2D グラフィックスコア • 組み込み DDR4 メモリ インターフェイスは最大 512 MB のアドレス可能メモリをサポートします (デフォルトで 8 MB がビデオメモリに割り当てられます) • 最大 1920 X 1200 16bpp、60Hz のディスプレイ解像度をサポートします。 • 高速な内蔵 24 ビット RAMDAC • 第 1 世代の速度で動作するシングル レーン PCI-Express ホスト インターフェイス

機能	説明
ACPI	ACPI 4.0 標準がサポートされています。
組み込み管理プロセッサ	Cisco IMC ファームウェアを実行する BMC。 CIMC の設定に応じて、1GE 管理専用ポート、1GE/10GE LOM ポート、または Cisco VIC を介して CIMC にアクセスできます。

第 3 世代 Catalyst 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するトピックへのリンクが含まれています。

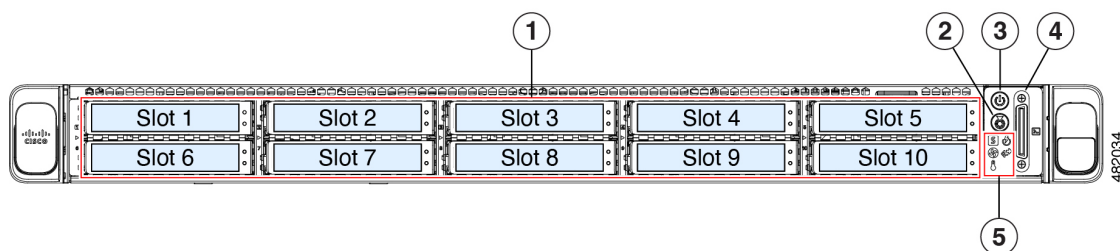
適切なリンクをクリックすると、第 3 世代 Catalyst Center アプライアンスの前面パネルと背面パネルの説明が表示されます。

32 56

32 および 56 コアの第 3 世代 Catalyst Center アプライアンスの前面パネルおよび背面パネルについて説明します。

次の図と表では、32 コアおよび 56 コアの第 3 世代 Catalyst Center アプライアンスの前面パネルおよび背面パネルについて説明します。

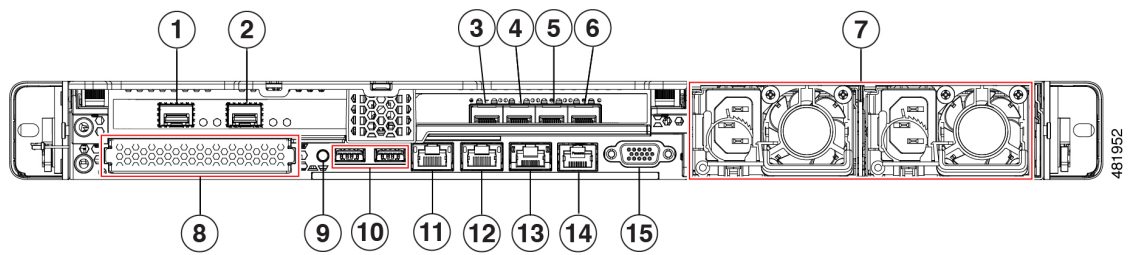
1:



コールアウト番号	説明
1	アプライアンスには 10 個のドライブが含まれています。 32 コアアプライアンス： ● 960 GB SSD X 2（スロット 1 および 2）。 ● 1.9 TB SSD X 8（スロット 3 ～ 10）。 56 コアアプライアンス： ● 960 GB SSD X 2（スロット 1 および 2）。 ● 3.8 TB SSD X 8（スロット 3 ～ 10）。 設置する各ドライブには、左側の障害 LED と右側のアクティビティ LED の 2 つの LED があります。 ドライブ障害 LED の状態とその説明： ● 消灯：ドライブは正常に動作中です。 ● オレンジ：ドライブに障害が発生しています。 ● オレンジの点滅：ドライブの再構成中です。 ドライブアクティビティ LED の状態とその説明： ● 消灯：スレッドにドライブが存在しません（アクセスなし、障害なし）。 ● 緑：ドライブの準備が完了しています。 ● 緑の点滅：ドライブはデータの読み取り中または書き込み中です。
2	ユニット識別 ( ● 消灯：ユニット識別機能は使用されていません。 ● 青の点滅：ユニット識別機能がアクティブになっています。
3	電源ボタン ( ● 消灯：サーバーに AC 電力が供給されていません。 ● オレンジ：サーバーはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機構にだけ電源が投入されています。 ● 緑：サーバーは主電源モードです。すべてのサーバコンポーネントに電力が供給されています。
4	KVM コネクタ (USB 2.0 コネクタ 2 個、DB-15 VGA 1 個、DB-9 シリアル 1 個を装備した KVM ケーブルで使用)

コールアウト番号	説明
5	システム LED クラスタ : - ファンステータス () : - 緑 : すべてのファンモジュールが正常に動作中です。 - オレンジの点滅 : 1 つ以上のファンモジュールが回復不能なしきい値を超えました。 - システムの状態 () : - 緑 : サーバーは正常動作状態で稼働しています。 - 緑の点滅 : サーバーはシステムの初期化とメモリチェックを実行しています。 - オレンジの点灯 : サーバーは縮退運転状態にあります (軽度の障害) 。 - オレンジの点滅 (2 回) : システムボードで重度の障害が発生しています。 - オレンジの点滅 (3 回) : メモリ (DIMM) で重度の障害が発生しています。 - オレンジの点滅 (4 回) : CPU で重度の障害が発生しています。 - 電源装置のステータス () : - 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。 - ネットワーク リンク アクティビティ () : - 消灯 : イーサネット LOM ポートリンクがアイドル状態です。 - 緑 : 1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 - 緑の点滅 : 1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。 - 温度ステータス () : - 緑 : サーバー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重大なしきい値を超えました。 - オレンジの点滅 : 1 つ以上の温度センサーが回復不能なしきい値を超えました。

2 :



コールアウト番号	説明
1, 4	10 Gbps エンタープライズポート（ネットワークアダプタ 1）：このポートは、Maglev 構成ウィザードでネットワークアダプタ 1 として表示されます。このポートをエンタープライズネットワークにアクセスできるスイッチに接続します。 - プライマリインスタンス（コールアウト 1）は、アプライアンスの PCIe ライザ 1/ スロット 1 の Intel E810-XXVDA2 ネットワークアダプタの左側のポートです。 - セカンダリインスタンス（コールアウト 4）は、アプライアンスの PCIe ライザ 3/ スロット 3 の Intel E810-XXVDA4 ネットワークアダプタの 2 番目のポートです。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態： - 消灯：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。 - 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。 速度 LED の状態： - 消灯：リンクが確立されていません。 - オレンジ：リンク速度は 10 Gbps 以下です。  注 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。

2, 3

コールアウト番号	説明
	10 Gbps クラスター内ポート（ネットワークアダプタ 2）：このポートは、Maglev 構成ウィザードでネットワークアダプタ 2 として表示されます。このポートをクラスター内の他のノードにアクセスできるスイッチに接続します。 - プライマリインスタンス（コールアウト 2）は、アプライアンスの PCIe ライザ 1/スロット 1 の Intel E810-XXVDA2 ネットワークアダプタの右側のポートです。 - セカンダリインスタンス（コールアウト 3）は、アプライアンスの PCIe ライザ 3/スロット 3 の Intel E810-XXVDA4 ネットワークアダプタの最初のポートです。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態： - 消灯：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。 - 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。 速度 LED の状態： - 消灯：リンクが確立されていません。 - オレンジ：リンク速度は 10 Gbps 以下です。

注

低速でも動作可能ですが、このポートは **10 Gbps** でのみ動作するように設計されています。

コールアウト番号	説明
----------	----

1 Gbps/10 Gbps インターネットポート（ネットワークアダプタ 4）：このイーサネットポートは、リンクパートナーに応じて **1 Gbps** および **10 Gbps** をサポートできます。このポートは、**Maglev** 構成ウィザードではネットワークアダプタ 4 として識別されます。このポートはオプションです。**10 Gbps** の企業ポートを使用できない場合は、インターネットへの接続に使用します。インターネットまたはインターネットに接続するプロキシサーバーに接続します。

これはインターネットポートのセカンダリインスタンスです。これは、アプライアンスの **PCIe** ライザー 3、スロット 3 にある **Intel E810-XXVDA4** ネットワークアダプタの 3 番目のポートです。

このポートにはリンクステータス（**ACT**）**LED** とリンク速度（リンク）**LED** が付いています。

- リンクステータス **LED** の状態：
 - 消灯：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。
 - 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。
- 速度 **LED** の状態：
 - 消灯：リンクが確立されていません。
 - オレンジ：リンク速度は **10 Gbps** 以下です。

 注

低速でも動作可能ですが、このポートは **10 Gbps** でのみ動作するように設計されています。

コールアウト番号	説明
	1 Gbps/10 Gbps 管理ポート（ネットワークアダプタ 3）：このイーサネットポートは、リンクパートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 3 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 これは管理ポートのセカンダリインスタンスです。これは、アプライアンスの PCIe ライザー 3、スロット 3 にある Intel E810-XXVDA4 ネットワークアダプタの 4 番目のポートです。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態： ● 消灯：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。 ● 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。 速度 LED の状態： ● 消灯：リンクが確立されていません。 ● オレンジ：リンク速度は 10 Gbps 以下です。  注 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。
7	電源装置（2、冗長 1+1）
	 注 電源レセプタクルは、写真に示されている方向とは反対方向を向けています。
8	モジュラ LAN-on-motherboard（mLOM）カード ベイ（x16 PCIe レーン）
9	ユニット識別ボタン/LED
10	USB 3.0 ポート（2 個）

コールアウト番号	説明
11	1 Gbps/10 Gbps 管理ポート（ネットワークアダプタ 3）：このイーサネットポートは、リンクパートナーの機能に応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 3 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 これは管理ポートのプライマリインスタンスです。アプライアンスの背面パネルには 1 というラベルが付いています。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 • リンクステータス LED の状態： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 • 速度 LED の状態： • 消灯：リンクが確立されていません。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。  注 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。

12

コールアウト番号	説明
----------	----

1 Gbps/10 Gbps インターネットポート（ネットワークアダプタ 4）：このイーサネットポートは、リンクパートナーの機能に応じて **1 Gbps** および **10 Gbps** をサポートできます。このポートは、**Maglev** 構成ウィザードではネットワークアダプタ **4** として識別されます。このポートはオプションです。**10 Gbps** の企業ポートを使用できない場合は、インターネットへの接続に使用します。インターネットに接続しているインターネットサーバーまたはプロキシサーバーに接続します。

これはインターネットポートのプライマリインスタンスです。アプライアンスの背面パネルに **2** というラベルが付いています。

このポートにはリンクステータス（**ACT**）**LED** とリンク速度（リンク）**LED** が付いています。

- リンクステータス **LED** の状態：
 - 消灯：リンクが確立されていません。
 - 緑の点滅：アクティブなリンクにトラフィックが存在します。
 - 緑：リンクはアクティブですが、トラフィックは存在しません。
- 速度 **LED** の状態：
 - 消灯：リンクが確立されていません。
 - 緑：リンク速度は **10 Gbps** です。
 - オレンジ：リンク速度は **1 Gbps** です。

 注

低速でも動作可能ですが、このポートは **10 Gbps** でのみ動作するように設計されています。

13

1 Gbps Cisco IMC ポート：これはインターネットポートの右側にある組み込みポートです。アプライアンスの **Cisco IMC GUI**（[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)（86ページ）を参照）へのブラウザアクセスを有効にすると、ポートは IP アドレスを受信します。このポートは、アプライアンスのシャーシおよびソフトウェアのアウトオブバンド管理用に予約されています。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。

このポートにはリンクステータス **LED** とリンク速度 **LED** が付いています。

リンクステータス **LED** の状態：

- 消灯：リンクが確立されていません。
- 緑の点滅：アクティブなリンクにトラフィックが存在します。
- 緑：リンクはアクティブですが、トラフィックは存在しません。

速度 **LED** の状態：

- 消灯：リンク速度は **10 Mbps** 以下です。
- 緑：リンク速度は **1 Gbps** です。
- オレンジ：リンク速度は **100 Mbps** です。

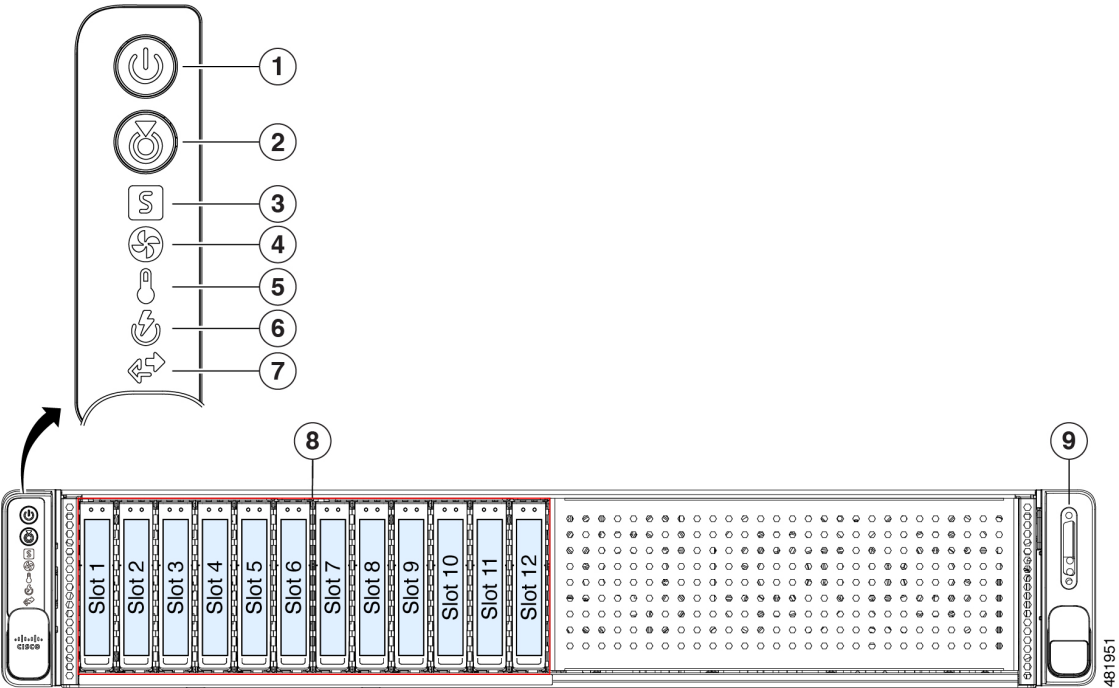
コールアウト番号	説明
14	COM ポート (RJ-45 コネクタ)
15	VGA ビデオ ポート (DB-15 コネクタ)

80

80 コアの第 3 世代 Catalyst Center アプライアンスの前面パネルおよび背面パネルについて説明します。

次の図と表では、80 コア第 3 世代 Catalyst Center アプライアンスの前面パネルおよび背面パネルについて説明します。

3:



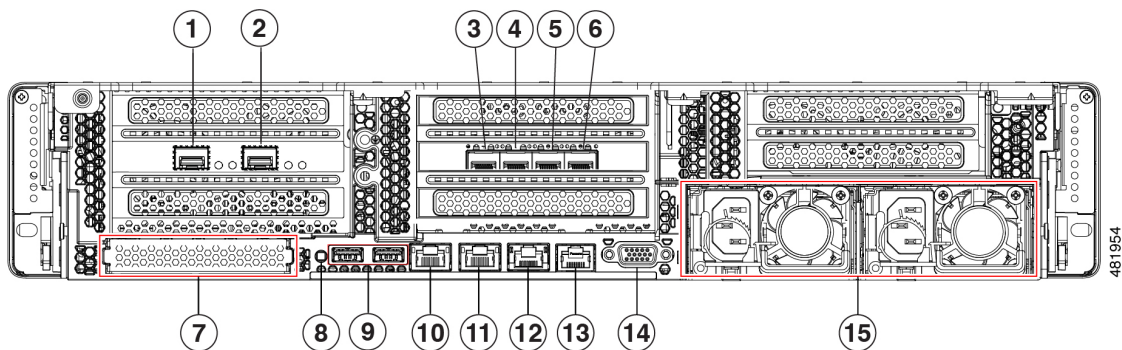
コールアウト番号	説明
----------	----

- 1
- 電源ボタン () :
- 消灯：サーバーに AC 電力が供給されていません。
 - オレンジ：サーバーはスタンバイ電源モードです。Cisco IMC と一部のマザーボード機構にだけ電源が投入されています。
 - 緑：サーバーは主電源モードです。すべてのサーバコンポーネントに電力が供給されています。
- 2
- ユニット識別 () :
- 消灯：ユニット識別機能は使用されていません。
 - 青の点滅：ユニット識別機能がアクティブになっています。

コールアウト番号	説明
3	システムの状態 () : ● 緑：サーバーは正常動作状態で稼働しています。 ● 緑の点滅：サーバーはシステムの初期化とメモリチェックを実行しています。 ● オレンジの点灯：サーバーは縮退運転状態にあります（軽度の障害）。次に例を示します。 ● 電源装置の冗長性が失われている。 ● CPU が一致しない。 ● 少なくとも 1 つの CPU に障害が発生している。 ● 少なくとも 1 つの DIMM に障害が発生している。 ● RAID 構成内の少なくとも 1 台のドライブに障害が発生している。 ● オレンジの点滅（2 回）：システムボードで重度の障害が発生しています。 ● オレンジの点滅（3 回）：メモリ（DIMM）で重度の障害が発生しています。 ● オレンジの点滅（4 回）：CPU で重度の障害が発生しています。
4	ファンステータス () : ● 緑：すべてのファンモジュールが正常に動作中です。 ● オレンジの点滅：1 つ以上のファンモジュールが回復不能なしきい値を超えました。
5	温度ステータス () : ● 緑：サーバー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重大なしきい値を超えました。 ● オレンジの点滅：1 つ以上の温度センサーが回復不能なしきい値を超えました。
6	電源装置のステータス () : ● 緑：すべての電源装置が正常に動作しています。 ● オレンジの点灯：1 台以上の電源装置が縮退運転状態にあります。 ● オレンジの点滅：1 台以上の電源装置が重大な障害発生状態にあります。
7	ネットワーク リンク アクティビティ () : ● 消灯：イーサネット LOM ポートリンクがアイドル状態です。 ● 緑：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていますが、アクティビティは存在しません。 ● 緑の点滅：1 つ以上のイーサネット LOM ポートでリンクがアクティブになっていて、アクティビティが存在します。

コールアウト番号	説明
8	アプライアンスには、次の 12 個のドライブが含まれています。 ● 960 GB SSD X 2 (スロット 1 および 2)。 ● 3.8 TB SSD X 10 (スロット 3 ~ 12)。 取り付けられたドライブにはそれぞれ、左側の障害 LED と右側のアクティビティ LED の 2 つの LED があります。 ドライブ障害 LED の状態とその説明： ● 消灯：ハード ドライブは正常に動作中です。 ● オレンジ色：ドライブ障害が検出されました。 ● オレンジの点滅：デバイスの再構成中です。 ● 1 秒間隔のオレンジの点滅：ソフトウェアでドライブ位置特定機能がアクティブ化されました。 ドライブアクティビティ LED の状態とその説明： ● 消灯：ハードドライブトレイにハードドライブが存在しません（アクセスなし、障害なし）。 ● 緑：ハードドライブの準備が完了しています。 ● 緑の点滅：ハードドライブはデータの読み取り中または書き込み中です。
9	KVM コネクタ これを、DB-15 VGA コネクタ X 1、DB-9 シリアルコネクタ X 1、USB 2.0 コネクタ X 2 を装備した KVM ケーブルで使⽤します。

4:



コールアウト番号	説明
1, 4	10 Gbps エンタープライズポート（ネットワークアダプタ 1）：このポートは、Maglev 構成ウィザードでネットワークアダプタ 1 として識別されます。このポートを、エンタープライズ ネットワークに接続しているスイッチに接続します。 - プライマリインスタンス（コールアウト 1）は、アプライアンスのライザ 1A/スロット 2 の Intel E810-XXVDA2 ネットワークアダプタの左側のポートです。 - セカンダリインスタンス（コールアウト 4）は、アプライアンスのライザ 3A/スロット 5 の Intel E810-XXVDA4 ネットワークアダプタの 2 番目のポートです。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 リンクステータス LED の状態： - 消灯：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。 - 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。 速度 LED の状態： - 消灯：リンクが確立されていません。 - オレンジ：リンク速度は 10 Gbps 以下です。  注 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。

2, 3

コールアウト番号	説明
----------	----

10 Gbps のクラスタ内ポート（ネットワークアダプタ 2）：このポートは、**Maglev** 構成ウィザードでネットワークアダプタ 2 として識別されます。このポートをクラスタ内のほかのノードに接続しているスイッチに接続します。

- プライマリインスタンス（コールアウト 2）は、アプライアンスのライザー 1A/スロット 2 にある **Intel E810-XXVDA2** ネットワークアダプタの右側のポートです。
- セカンダリインスタンス（コールアウト 3）は、アプライアンスのライザー 3A/スロット 5 にある **Intel E810-XXVDA4** ネットワークアダプタの最初のポートです。

このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。

リンクステータス LED の状態：

- 消灯：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。
- 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。

速度 LED の状態：

- 消灯：リンクが確立されていません。
- オレンジ：リンク速度は **10 Gbps** 以下です。

注

低速でも動作可能ですが、このポートは **10 Gbps** でのみ動作するように設計されています。

コールアウト番号	説明
	1 Gbps/10 Gbps インターネットポート（ネットワークアダプタ 4）：このイーサネットポートは、リンクパートナーに応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 4 として識別されます。このポートは、10 Gbps エンタープライズポートではインターネット接続ができない場合にオプションで使用されます。インターネットまたはインターネットに接続しているプロキシサーバーに接続します。 これはインターネットポートのセカンダリインスタンスです。これは、アプライアンスのライザー 3A/スロット 5 にある Intel E810-XXVDA4 ネットワークアダプタの 3 番目のポートです。 このポートにはリンクステータス LED とリンク速度 LED が付いています。ステータス LED の状態とその説明： ● リンクステータス LED の状態： ● 消灯：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。 ● 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。 ● 速度 LED の状態： ● 消灯：リンクが確立されていません。 ● オレンジ：リンク速度は 10 Gbps 以下です。

 注

低速でも動作可能ですが、このポートは **10 Gbps** でのみ動作するように設計されています。

コールアウト番号	説明
	1 Gbps/10 Gbps 管理ポート（ネットワークアダプタ 3）：このイーサネットポートは、リンクパートナーに応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 3 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 これは管理ポートのセカンダリインスタンスです。これは、アプライアンスのライザー 3A/スロット 5 にある Intel E810-XXVDA4 ネットワークアダプタの 4 番目のポートです。 このポートにはリンクステータス LED とリンク速度 LED が付いています。ステータス LED の状態とその説明： ● リンクステータス LED の状態： ● 消灯：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。 ● 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。 ● 速度 LED の状態： ● 消灯：リンクが確立されていません。 ● オレンジ：リンク速度は 10 Gbps 以下です。  注 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。
7	モジュラ LAN-on-motherboard (mLOM) カード ベイ (x16 PCIe レーン)
8	ユニット識別ボタンと LED。
9	USB 3.0 ポート (2 個)

コールアウト番号	説明
10	1 Gbps/10 Gbps 管理ポート（ネットワークアダプタ 3）：このイーサネットポートは、リンクパートナーに応じて 1 Gbps および 10 Gbps をサポートできます。このポートは、Maglev 構成ウィザードではネットワークアダプタ 3 として識別されます。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。 これは管理ポートのプライマリインスタンスです。ポートは、アプライアンスの背面パネルの 2 番目の USB ポートの右側にあります。 このポートにはリンクステータス（ACT）LED とリンク速度（リンク）LED が付いています。 • リンクステータス LED の状態： • 消灯：リンクが確立されていません。 • 緑の点滅：アクティブなリンクにトラフィックが存在します。 • 緑：リンクはアクティブですが、トラフィックは存在しません。 • 速度 LED の状態： • 消灯：リンクが確立されていません。 • 緑：リンク速度は 10 Gbps です。 • オレンジ：リンク速度は 1 Gbps です。  注 低速でも動作可能ですが、このポートは 10 Gbps でのみ動作するように設計されています。

コールアウト番号	説明
----------	----

1 Gbps/10 Gbps インターネットポート（ネットワークアダプタ 4）：このイーサネットポートは、リンクパートナーに応じて **1 Gbps** および **10 Gbps** をサポートできます。このポートは、**Maglev** 構成ウィザードではネットワークアダプタ 4 として識別されます。このポートは、**10 Gbps** エンタープライズポートではインターネット接続ができない場合にオプションで使用されます。インターネットまたはインターネットに接続しているプロキシサーバーに接続します。

これはインターネットポートのプライマリインスタンスです。これは、背面パネルで管理ポートと **Cisco IMC** ポートの間にあります。

このポートにはリンクステータス（**ACT**）**LED** とリンク速度（リンク）**LED** が付いています。

- リンクステータス **LED** の状態：
 - 消灯：リンクが確立されていません。
 - 緑の点滅：アクティブなリンクにトラフィックが存在します。
 - 緑：リンクはアクティブですが、トラフィックは存在しません。
- 速度 **LED** の状態：
 - 消灯：リンクが確立されていません。
 - 緑：リンク速度は **10 Gbps** です。
 - オレンジ：リンク速度は **1 Gbps** です。

 注

低速でも動作可能ですが、このポートは **10 Gbps** でのみ動作するように設計されています。

12

1 Gbps Cisco IMC ポート：これはインターネットポートの右側にある組み込みポートです。アプライアンスの **Cisco IMC GUI** に対するブラウザアクセスを有効にすると、IP アドレスが割り当てられます（[Cisco Integrated Management Controller に対するブラウザアクセスの有効化（86ページ）](#)を参照）。このポートは、アプライアンスのシャーシおよびソフトウェアのアウトオブバンド管理用に予約されています。このポートはエンタープライズ管理ネットワークにアクセスできるスイッチに接続します。

このポートにはリンクステータス **LED** とリンク速度 **LED** が付いています。

リンクステータス **LED** の状態：

- 消灯：リンクが確立されていません。
- 緑の点滅：アクティブなリンクにトラフィックが存在します。
- 緑：リンクはアクティブですが、トラフィックは存在しません。

速度 **LED** の状態：

- 消灯：リンク速度は **10 Mbps** 以下です。
- 緑：リンク速度は **1 Gbps** です。
- オレンジ：リンク速度は **100 Mbps** です。

コールアウト番号	説明
13	COM ポート (RJ-45 コネクタ)
14	VGA ビデオ ポート (DB-15 コネクタ)
15	電源装置 (2、冗長 1+1)

第 3 世代 Catalyst Center アプライアンスの物理仕様のリンクを示します。

適切なリンクをクリックすると、第 3 世代 Catalyst Center アプライアンスの物理的な仕様が表示されます。

32 56

32 コアおよび 56 コアの第 3 世代 Catalyst Center アプライアンスの物理仕様を一覧表示します。

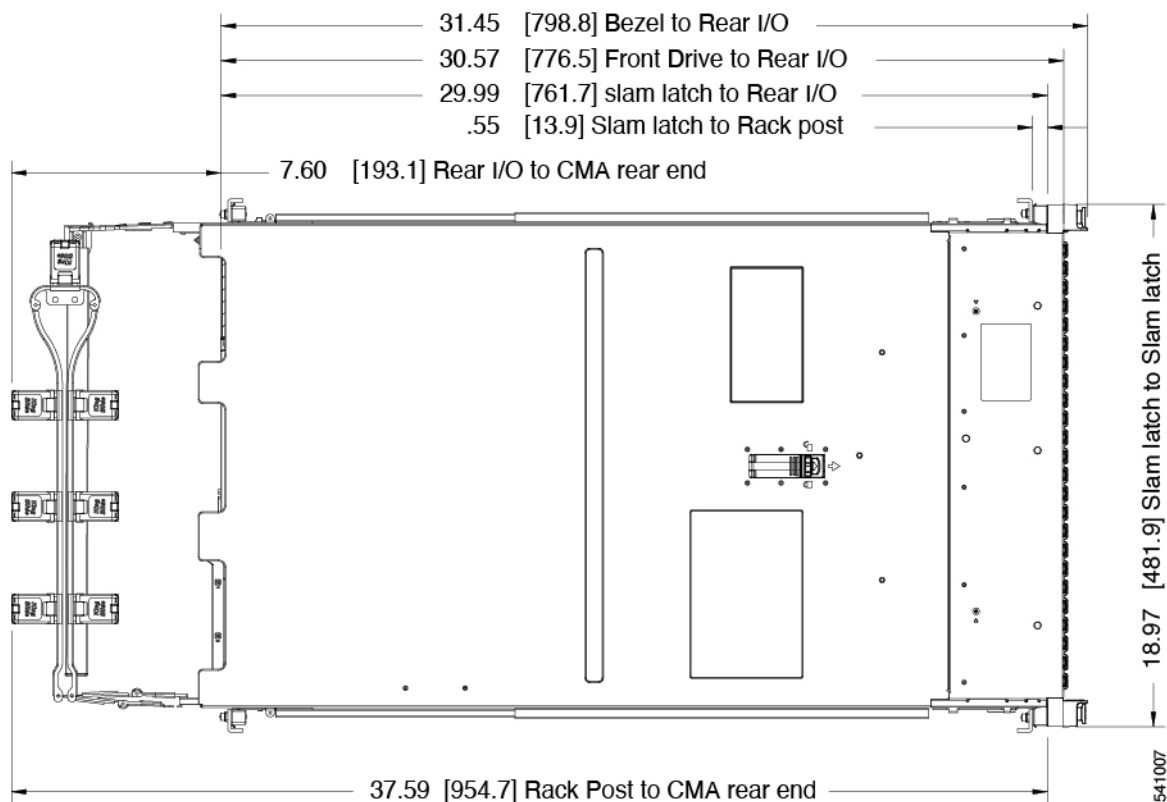
次の表に 32 コアおよび 56 コアの第 3 世代 Catalyst Center アプライアンスの物理的仕様を示します。

説明	仕様
高さ	43.2 mm (1.7 インチ)
幅	429.0 mm (16.9 インチ)
奥行 (長さ)	サーバーのみ : 762 mm (30 インチ) サーバーとスライドレール : 800.1 mm (31.5 インチ)
重量	- 最大、完全構成とレールキット : 19.25 kg (42.432 ポンド) - 最大、未構成、レールキットなし : 10.13 kg (22.32 ポンド)

80

80 コア第 3 世代 Catalyst Center アプライアンスの物理仕様を示します。

次の図は、さまざまな場所で測定したシャーシの高さ、幅、奥行きを示しています。



次の表にアプライアンスの物理的仕様を示します。

説明	仕様
サーバー重量	• SFF 12 ドライブサーバー : • 最大、レールキットで完全に設定 : 20.28 kg (49.2 ポンド) • 最小、空のシャーシ、レールキットなし : 16.2 kg (35.7 ポンド) • SFF 24 ドライブサーバー : • 最大、レールキットで完全に設定 : 26.67 kg (61.7 ポンド) • 最小、空のシャーシ、レールキットなし : 15.03 kg (33.14 ポンド) • LFF 12 ドライブサーバー : • 最大、レールキットで完全に設定 : 28.0 kg (66.75 ポンド) • 最小、空のシャーシ、レールキットなし : 17.75 kg (39.13 ポンド)
前面のスペース	76 mm (3 インチ)
周囲と側面の間に必要な隙間	25 mm (1 インチ)
背面のスペース	152 mm (6 インチ)

32 コア、56 コア、および 80 コアの第 3 世代 Catalyst Center アプライアンスの環境仕様。

表 4 : Catalyst Center アプライアンス環境仕様 (35 ページ) には、32 コア、56 コア、および 80 コアの第 3 世代 Catalyst Center アプライアンスの環境仕様を一覧表示します。

4 : Catalyst Center

説明	仕様
温度 (動作時)	10°C ~ 35°C (50°F ~ 95°F) の乾球温度 毎時 20 °C (36 °F) の最大温度変化 (変化率ではなく、一定時間内の温度変化) 湿度条件 : 非制御、50% RH 以内の開始条件 900 メートルを超える高度で 305 メートルごとに最高動作温度を 1 °C (33.8°F) 低下
温度、拡張動作	5 ~ 40°C (41 ~ 104°F) 、直射日光なし 湿度条件 : 非制御、50% RH 以内の開始条件 900 メートルを超える高度で 305 メートルごとに最高動作温度を 1 °C (33.8°F) 低下
非動作時温度 (サーバーが倉庫にあるか運送中の場合)	乾球温度 40 ~ 65 °C (-40 ~ 149 °F)
湿度 (RH) (動作時)	10 ~ 90%、最大露点温度 28°C (82.4°F) 、非凝縮環境 -12 °C (10.4 °F) の露点より高い (湿気が多い) または 8% の相対湿度 最大露点 24 °C (75.2 °F) または最大相対湿度 90%
湿度 (RH) (非動作時) (サーバーが倉庫にあるか運送中の場合)	相対湿度 5 ~ 93%、結露しないこと、乾球温度 20 ~ 40 °C の最大湿球温度は 28 °C。
動作時高度	最大標高 3,050 m (10,006 フィート)
非動作時高度 (サーバーが倉庫にあるか運送中の場合)	標高 0 ~ 12,000 m (39,370 フィート)
最長動作期間	無制限
音響出力レベル ISO7779 に基づく A 特性音響出力レベル LwAd (Bels) を測定 73°F (23°C) で動作	5.5
騒音レベル ISO7779 に基づく A 特性音圧レベル LpAm (dBA) を測定 73°F (23°C) で動作	40

Catalyst Center アプライアンスの電源の仕様へのリンクを提供します。

Catalyst Center アプライアンスに同梱されている電源の仕様は、下表に一覧表示されています。第 3 世代アプライアンスのすべてのバージョンには、**2300 W** 電源装置（シスコ製品番号 **UCSC-PSU1-2300W**）が付属しています。

適切なリンクをクリックして、アプライアンスの電源装置の仕様を表示します。

注

- 次の URL にある **Cisco UCS Power Calculator** を使用すると、ご使用のアプライアンス設定の電源に関する詳細情報を取得できます。 <http://ucspowercalc.cisco.com>
- これらのトピックに記載されている **80PLUS platinum** 認定のテスト結果は、 <https://www.clearesult.com/80plus/> で確認できます。

32 56

32 コアおよび 56 コア Catalyst Center アプライアンスの電源仕様を示します。

パラメータ	仕様			
入力コネクタ	IEC320 C20			
入力電圧範囲 (Vrms)	100 ～ 240			
最大許容入力電圧範囲 (Vrms)	90 ～ 264			
周波数範囲 (Hz)	50 ～ 60			
最大許容周波数範囲 (Hz)	47 ～ 63			
最大定格出力 (W)	2300			
	ローライン入力電圧 (100 ～ 127 V) で動作時の 1200 W に制限されます。			
最大定格スタンバイ出力 (W)	36			
公称入力電圧 (Vrms)	100	120	208	230
公称入力電流 (Arms)	13	11	12	10.8
公称入力電圧の最大入力 (W)	1338	1330	2490	2480
公称入力電圧の最大入力 (VA)	1351	1343	2515	2505
最小定格効率 (%)	92	92	93	93

80PLUS platinum 認定を取得するために必要な最小定格です。認定値については、 <http://www.80plus.org/> で公開されているテストレポートを参照してください。

パラメータ	仕様			
最小定格力率	0.99	0.99	0.97	0.97
80PLUS platinum 認定を取得するために必要な最小定格です。認定値については、 http://www.80plus.org/ で公開されているテストレポートを参照してください。				
最大突入電流 (A ピーク)	30			
最大突入電流 (ms)	0.2			
最小ライドスルー時間 (ms)	12			
入力電圧のドロップアウト時、出力電圧は 100% 負荷の状態で規制の範囲内に留まります				

80

80 コア Catalyst Center アプライアンスの電源仕様を示します。

パラメータ	仕様			
入力コネクタ	IEC320 C20			
入力電圧範囲 (Vrms)	100 ~ 240			
最大許容入力電圧範囲 (Vrms)	90 ~ 264			
周波数範囲 (Hz)	50 ~ 60			
最大許容周波数範囲 (Hz)	47 ~ 63			
最大定格出力 (W)	2300			
	ローライン入力電圧 (100 ~ 127 V) で動作時の 1200 W に制限されます。			
最大定格スタンバイ出力 (W)	36			
公称入力電圧 (Vrms)	100	120	208	230
公称入力電流 (Arms)	13	11	12	10.8
公称入力電圧の最大入力 (W)	1338	1330	2490	2480
公称入力電圧の最大入力 (VA)	1351	1343	2515	2505
最小定格効率 (%)	92	92	93	93
80PLUS platinum 認定を取得するために必要な最小定格です。認定値については、 http://www.80plus.org/ で公開されているテストレポートを参照してください。				

パラメータ	仕様			
最小定格力率	0.99	0.99	0.97	0.97
80PLUS platinum 認定を取得するために必要な最小定格です。認定値については、 http://www.80plus.org/ で公開されているテストレポートを参照してください。				
最大突入電流 (A ピーク)	30			
最大突入電流 (ms)	0.2			
最小ライドスルー時間 (ms)	12			
入力電圧のドロップアウト時、出力電圧は 100% 負荷の状態で規制の範囲内に留まります				

第

2

章

:

-
- Catalyst CenterCisco Software-Defined Access
-
- IP
- URL
-
-
- HTTP 80
-
- Cisco Software-Defined Access
-
-
-
-

適切なアプライアンスの設置と設定を行うために必要な計画と情報の収集に関する情報。

Catalyst Center アプライアンスの設置、設定、セットアップを試みる前に、次の計画と情報収集のタスクを実行する必要があります。これらのタスクが完了したら、データセンターにアプライアンスを設置します。

1. スタンドアロン設置とクラスタ設置で推奨されるケーブル接続とスイッチングの要件を確認します。[インターフェイスケーブル接続](#) (40ページ) を参照してください。
2. アプライアンスの設定時に適用する IP アドレス、サブネット、および IP トラフィック情報を収集します。[必要な IP アドレスおよびサブネット](#) (44ページ) を参照してください。
3. 必要な Web ベースのリソースに対するアクセスのソリューションを準備します。[必要なインターネット URL と完全修飾ドメイン名](#) (48ページ) および[インターネットへのアクセスを保護する](#) (52ページ) を参照してください。
4. **Catalyst Center** トラフィックのファイアウォールとセキュリティポリシーを再設定します。[通信ポート](#) (53ページ) を参照してください。**Catalyst Center** を使用して **Cisco Software-Defined Access (SD-Access)** ネットワークを管理している場合は「[Cisco Software-Defined Access に必要なポートとプロトコル](#)」も参照してください。
5. アプライアンスの構成時と初回設定時に使用される追加情報を収集します。[必須の設定情報](#) (70ページ) および[必要な初期設定情報](#) (71ページ) を参照してください。

Catalyst Center Cisco Software-Defined Access

Cisco Software-Defined Access と Catalyst Center について簡単に説明します。

Cisco SD-Access ファブリックアーキテクチャを使用するネットワークも含め、すべてのネットワークタイプで **Catalyst Center** を使用できます。**Cisco SD-Access** は、従来のネットワークをインテントベースのネットワークに変換します。これにより、構成、プロビジョニング、トラブルシューティングなどのタスクを簡単に自動化できるようになります。**Cisco SD-Access** ソリューションは、ビジネスニーズへのネットワークの適応を迅速化し、問題の解決策を向上させ、セキュリティ侵害の影響を最小限に抑えます。

このガイドでは、**Cisco SD-Access** ソリューションの概要を説明します。**Cisco SD-Access** を使用して **Catalyst Center** ファブリックを実装する場合は、以下のリソースに詳細とガイダンスがあります。

- 通常のネットワークのアプローチと技術では不可能なソリューションを自動化するために、**Catalyst Center** が **Cisco SD-Access** を活用する方法については、『[Cisco Software-Defined Access Solution Design Guide](#)』を参照してください。
- **Cisco SD-Access** アクセスセグメンテーションを使用したネットワークセキュリティの強化に関するガイダンスについては、『[SD-Access Segmentation Design Guide](#)』を参照してください。
- 他のシスコおよびサードパーティ製品と共同作業する **Catalyst Center** および **Cisco SD-Access** ソリューションの詳細については、「[Design Zone](#)」を参照してください。

必須およびオプションのインターフェイスケーブル接続について説明し、ケーブル接続のガイダンスを提供します。

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。**Catalyst Center** の機能に必要なため、少なくともエンタープライズポートおよびクラスター内ポートインターフェイスを設定する必要があります。

第3世代アプライアンスでNICボンディングが有効になっている場合、エンタープライズポート、クラスター内ポート、管理ポート、およびインターネットポートのセカンダリインスタンスはIntel E810-XXVDA4 NICに存在します。これらのポートを、各ポートのプライマリインスタンスを接続するスイッチとは異なるスイッチに接続します（[NIC ボンディングの概要](#)（94ページ）を参照してください）。

注

- アプライアンス設定中、Maglev設定ウィザードは、クラスタリンクオプションをインターフェイスに割り当てるまで続行できません。実稼働環境の単一ノード展開と3ノード展開の両方で、クラスター内ポートをクラスタリンクとして割り当てます。
- クラスタリンクとしてマークされたインターフェイスは、設定が完了した後は変更することはできません。変更するには、アプライアンスを再イメージ化する必要があります。Catalyst Center アプライアンスのイメージを作成し直すために完了する必要があるタスクの説明については、[アプライアンスのイメージの再作成](#)（96ページ）を参照してください。3ノードクラスターへの拡張をサポートするには、IP アドレスを使用してクラスターポートを設定します。クラスタ リンク インターフェイスをスイッチポートに接続し、稼働状態になっていることを確認します。
- 複数のクラスターを構築する場合は、クラスター間の相互作用と破損を防ぐために、クラスターごとに個別のIP スキームを使用する必要があります。

- **（必須）10 Gbps エンタープライズポート（ネットワークアダプタ 1）**：このポートの目的は、Catalyst Centerがネットワークと通信し、ネットワークを管理できるようにすることです。このポートを、エンタープライズ ネットワークに接続しているスイッチに接続し、ポートのサブネットマスクを使用してIP アドレスを1つ設定します。

プライマリインスタンス：

- これは、32 および 56 コアの Intel E810-XXVDA2 NIC の左側のポートで、アプライアンスの PCIe ライザー 1/スロット 1 にあります。
- これは、80 コアの Intel E810-XXVDA2 NIC の左側のポートで、アプライアンスのライザー 1A/スロット 2 にあります。

セカンダリインスタンス：

- これは、32 および 56 コアの Intel E810-XXVDA4 NIC の 2 番目のポートで、アプライアンスの PCIe ライザー 3/スロット 3 にあります。
- これは、80 コアの Intel E810-XXVDA4 ネットワークアダプタの 2 番目のポートで、アプライアンスのライザー 3A/スロット 5 にあります。

- **（必須）10 Gbps クラスター内ポート（ネットワークアダプタ 2）**：このポートの目的は、クラスター内のプライマリノードとセカンダリノード間の通信を可能にすることです。このポートをクラスター内の他のノードに接続しているスイッチに接続し、ポートのサブネットマスクを使用してIP アドレスを1つ設定します。

プライマリインスタンス：

- これは、32 および 56 コアの Intel E810-XXVDA2 NIC の右側のポートで、アプライアンスの PCIe ライザー 1/スロット 1 にあります。
- これは、80 コアの Intel E810-XXVDA2 ネットワークアダプタの右側のポートで、アプライアンスのライザー 1A/スロット 2 にあります。

セカンダリインスタンス：

- これは、32 および 56 コアの Intel E810-XXVDA4 NIC の 1 番目のポートで、アプライアンスの PCIe ライザー 3/スロット 3 にあります。
- これは、80 コアの Intel E810-XXVDA4 NIC の 1 番目のポートで、アプライアンスのライザー 3A/スロット 5 にあります。
- (オプション) **1 Gbps または 10 Gbps の管理ポート (ネットワークアダプタ 3)** : このポートから Catalyst Center GUI にアクセスできるため、アプライアンス上でソフトウェアを使用できます。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

プライマリインスタンス :

- これは、32 および 56 コアアプライアンスの背面パネルにあり **1** というラベルが付いています。
- これは、80 コアアプライアンスの背面パネルで 2 番目の USB ポートの右側にあります。

セカンダリインスタンス :

- これは、32 および 56 コアの Intel E810-XXVDA4 NIC の 4 番目のポートで、アプライアンスの PCIe ライザー 3/スロット 3 にあります。
- これは、80 コアの Intel E810-XXVDA4 ネットワークアダプタの 4 番目のポートで、アプライアンスのライザー 3A/スロット 5 にあります。
- (オプション) **1 Gbps または 10 Gbps のインターネットポート (ネットワークアダプタ 4)** : このポートは、背面パネルに **2** というラベルが付いており、オプションです。10 Gbps のエンタープライズポート (ネットワークアダプタ 1) を使用してアプライアンスをインターネット (インターネットプロキシサーバーを含む) に接続できない場合にのみ使用してください。このポートを使用する必要がある場合は、インターネットプロキシサーバーに接続しているスイッチに接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

プライマリインスタンス :

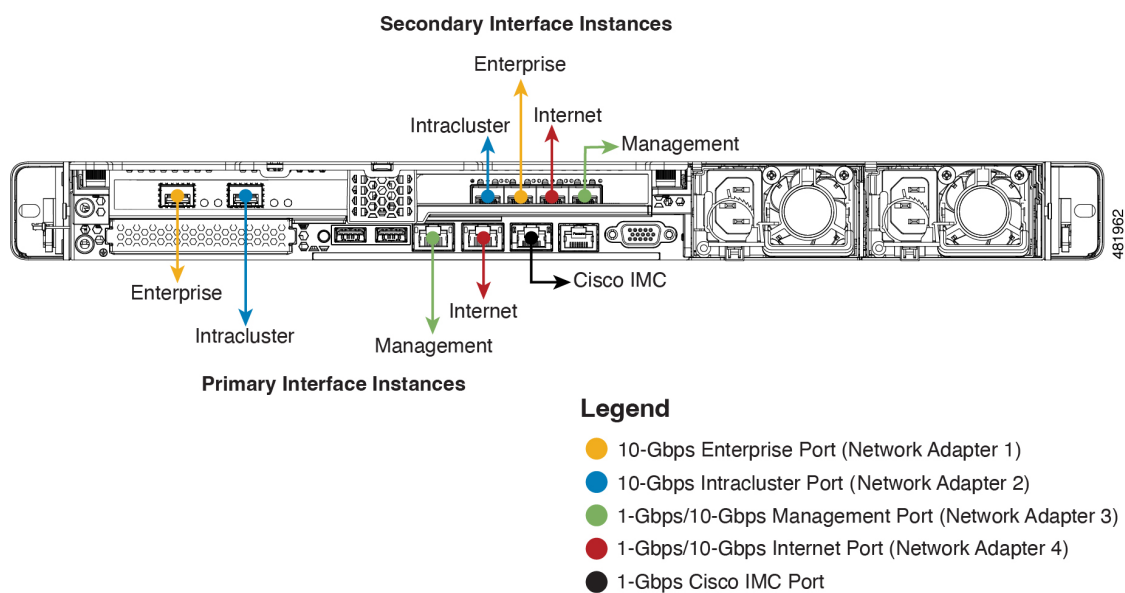
- これは、32 および 56 コアアプライアンスの背面パネルにあり **2** というラベルが付いています。
- これは、80 コアアプライアンスの背面パネルで管理ポートと Cisco IMC ポートの間にあります。

セカンダリインスタンス :

- これは、32 および 56 コアの Intel E810-XXVDA4 NIC の 3 番目のポートで、アプライアンスの PCIe ライザー 3/スロット 3 にあります。
- これは、80 コアの Intel E810-XXVDA4 ネットワークアダプタの 3 番目のポートで、アプライアンスのライザー 3A/スロット 5 にあります。
- (オプション、ただし強く推奨) **1 Gbps Cisco IMC ポート** : このポートは、すべての第 3 世代 Catalyst Center アプライアンスのインターネットポートの右側にあり、Cisco IMC アウトオブバンドアプライアンス管理インターフェイスとその GUI にブラウザ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。企業管理ネットワークに接続しているスイッチにこのポートを接続し、ポートのサブネットマスクを使用して IP アドレスを 1 つ設定します。

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

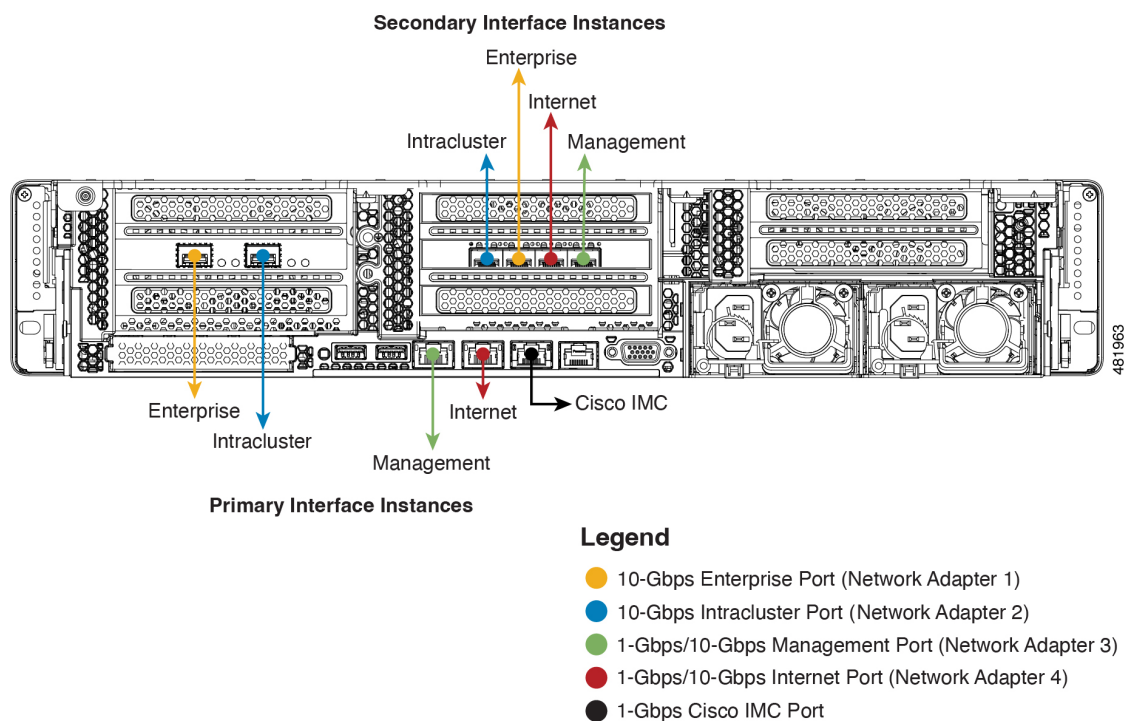
5 : 32 56



注

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

6 : 80



 注

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

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

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

各ポートの詳細については、「[前面パネルと背面パネル（14ページ）](#)」にあるシャーシの背面パネルの図と付属の説明を参照してください。

 注

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

10 Gbps の企業ポートおよびクラスターポートのケーブル接続でサポートされているメディア タイプは次のとおりです。

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

IP

単一ノードまたは **3 ノード**クラスタに必要なアプライアンスのポート（NIC）アドレス、IP アドレス、およびサブネットについて説明します。

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ーとしてインストールするか、**3 ノード**クラスターのプライマリまたはセカンダリノードとしてインストールするかによって、次のアプライアンスポート（NIC）アドレスが必要になります。

- **[Enterprise port address]**（必須）：サブネットマスクを持つ 1 つの IP アドレス。
- **[Cluster port address]**（必須）：サブネットマスクを持つ 1 つの IP アドレス。
- **[Management port address]**（オプション）：1 つの IP アドレスとサブネットマスク。

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

 注

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

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

- **[Cluster virtual IP addresses]** : クラスター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 ノードクラスターと、将来 3 ノードクラスターに変換される可能性のある単一ノードクラスターに適用されます。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、クラスター、管理、およびインターネットの 4 つのインターフェイスがあります。**Catalyst 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。

 注

- 単一ノード設定で、今後 3 ノードクラスタに変換する予定がない場合は、VIP アドレスを指定する必要はありません。ただし、これを行う場合は、設定されているすべてのネットワークインターフェイスに VIP アドレスを指定する必要があります (3 ノードクラスターの場合と同様)。
- 単一ノードクラスターのクラスター内リンクが失敗すると、管理インターフェイスとエンタープライズインターフェイスに関連付けられているVIP アドレスも失敗します。この状況が発生した場合は次のような処理が行われます。
 - Catalyst Center は、クラスター内リンクが復元されるまで使用できません。
 - ソフトウェア イメージ管理 [SWIM] および Cisco Identity Services Engine [ISE] の統合が動作しなくなります。
 - Cisco Catalyst Assurance ネットワーク データ プラットフォーム (NDP) コレクタからデータを収集できません。
- エンタープライズ インターフェイスまたは管理インターフェイスには、リンクローカルまたはルーティング不可能な IP アドレスを使用しないでください。
- **デフォルトゲートウェイ IP アドレス** : ネットワークの優先デフォルトゲートウェイの IP アドレス。他のルートがトラフィックに一致しない場合、トラフィックはこの IP アドレスを経由してルーティングされます。通常は、インターネットにアクセスするネットワーク設定内のインターフェイスにデフォルトゲートウェイを割り当てる必要があります。Catalyst 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 Catalyst Center Security Best Practices Guide](#)』を参照してください。
- **DNS サーバーの IP アドレス** : ネットワークの優先 DNS サーバーの IP アドレス。設定時に最大 3 つの DNS サーバー IP アドレスをスペース区切りのリストとして指定します。DNS サーバーに、127.0.0.1 に解決される localhost のエントリがあることを確認します。送信しないと、ネットワーク検証が失敗します。

 注意

アプライアンスに対して複数の DNS サーバーを指定すると、問題が発生する可能性があります。

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

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

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

- **NTP サーバーの 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) サーバーの IP アドレス。

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

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

- **コンテナサブネット (Container Subnet)** : アシユアランス、インベントリ収集などの内部アプリケーションサービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。デフォルトでは、Catalyst Center によりリンクローカルサブネット (**169.254.32.0/20**) がこのパラメータに設定されています。このサブネットを使用することを推奨します。別のサブネットを入力する場合は、Catalyst Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりしていないことを確認してください。また、サブネットの最小サイズが 21 ビットであることを確認してください。指定するサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。

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

詳細については、RFC 1918 では『[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。
 - Catalyst Center アプライアンスの設定が完了した後、最初にアプライアンスを再イメージ化せずに別のサブネットを割り当てることはできません（「[アプライアンスのイメージの再作成 \(96 ページ\)](#)」を参照してください）。
 - **クラスターサブネット** : データベースアクセス、メッセージバスなどのインフラストラクチャ サービス間の通信用 IP を管理および取得する際にアプライアンスが使用する 1 つの専用 IP サブネットを識別します。デフォルトでは、Catalyst Center によりリンクローカルサブネット (**169.254.48.0/20**) がこのパラメータに設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、Catalyst Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりしていないことを確認してください。また、サブネットの最小サイズが 21 ビットであることを確認してください。指定するサブネットは、次のアドレス範囲をサポートするプライベートネットワークの IETF RFC 1918 および RFC 6598 仕様に準拠している必要があります。
- 10.0.0.0/8
 - 172.16.0.0/12

- 192.168.0.0/16
- 100.64.0.0/10

詳細については、RFC 1918 では『[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。

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

重要

- 有効な CIDR サブネットが指定されていることを確認します。そうでない場合、172.17.1.0/20 および 172.17.61.0/20 サブネットに誤ったビットが表示されます。
- Catalyst Center アプライアンスの設定が完了した後、最初にアプライアンスを再イメージ化せず、別のサブネットを割り当てることはできません（「[アプライアンスのイメージの再作成](#)（96ページ）」を参照してください）。
- クラスポート、コンテナサブネット、またはクラスタサブネットの IP アドレスを入力する場合は、169.254.0.0/23 サブネット内のアドレスを指定しないでください。

コンテナとクラスタの 2 つのサブネットが推奨される合計 IP アドレス空間には、4096 のアドレスが含まれており、それぞれ 2048 のアドレスの 2/21 サブネットに分割されています。2/21 サブネットを重複させることはできません。Catalyst Center 内部サービスには、専用の IP アドレスのセットが必要です。これは Catalyst Center マイクロサービス アーキテクチャの要件です。この要件に対応するには、Catalyst 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。

アプライアンスでは、システムパフォーマンスを維持するためにこのようなアドレス空間が必要です。内部ルーティングおよびトンネリングテクノロジーがノード間通信に使用されます。重複するアドレス空間を使用すると、アプライアンスは Virtual Routing and Forwarding (VRF) FIB を内部で実行します。このプロセスでは、サービス間を移動するパケットに対して複数のカプセル化およびカプセル化解除のステップが作成されます。これらのステップにより内部遅延が大きくなるため、上位レイヤーでカスケード影響が発生します。

もう 1 つの理由は Catalyst 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、Catalyst Center は、複数の IP アドレスを必要とするサービスを 100 余りサポートしており、新しい機能と対応するサービスが常に追加されています。シスコが IP アドレスを不足することなく新しいサービスや機能を追加できるように、アドレス空間の要件を意図的に大きくしています。また、システムのアップグレード時に、連続したアドレス空間の再割り当てが必要なくなります。

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

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

URL

インターネットアドレス Catalyst Center がアクセスできないリスト。

アプライアンスを機能させるには、必要な **URL** および完全修飾ドメイン名 (**FQDN**) へのセキュアなアクセスを提供する必要があります。

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。

⚠ 注意

リストされた **URL** および **FQDN** へのアクセスを提供しない場合、関連する機能は想定どおりに動作しません。

📄 注

- インターネット宛トラフィックをルーティングするように設定されているアプライアンス インターフェイスは、すべての通信の送信元として機能します。
- 宛先ドメイン名は予告なく変更される場合があるため、ワイルドカードを使用して指定することを推奨します。

インターネットプロキシのアクセス要件の詳細については、「[インターネットへのセキュアなアクセスの提供](#)」を参照してください。

5: URL FQDN

目的

システムソフトウェアとアプリケーションパッケージにアップデートをダウンロードします。

...Catalyst Center がアクセスする必要がある URL と FQDN

推奨 : https://*.ciscoconnectdna.com/¹

ワイルドカードを回避するには、代わりに次の **URL** を指定します。

- <https://www.ciscoconnectdna.com>
- <https://catalogsvc-cdn.ciscoconnectdna.com>
- <https://catalogsvc-reg.ciscoconnectdna.com>
- <https://catalogsvc-reg-cdn.ciscoconnectdna.com>
- <https://catalogsvc-cm.ciscoconnectdna.com>
- <https://app-cdn.ciscoconnectdna.com>

製品チームにユーザーフィードバックを <https://dnacenter.uservoice.com> 送信します。

¹ シスコは ciscoconnectdna.com とそのサブドメインを所有し、管理しています。Cisco Connect DNA インフラストラクチャは、シスコの **Security and Trust** ガイドラインに準拠しています。セキュリティに関して継続的にテストされています。このインフラストラクチャは、ロードバランスおよび自動化機能が組み込まれた堅牢なインフラストラクチャです。クラウド運用チームがインフラストラクチャをモニターして維持することで、継続的な可用性を確保します。

目的	...Catalyst Center がアクセスする必要がある URL と FQDN
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/* • https://download-ssc.cisco.com/
クラウドドメインで認証します。	https://dnaservices.cisco.com
ThousandEyes と統合します。	• app.thousandeyes.com この URL では AWS が使用されており、 *.awsglobalaccelerator.com にマッピングされている可能性があります。AWS を使用する可能性のある他のサービスも AWS ドメインにマッピングできます。 • api.thousandeyes.com
API 呼び出しを許可して、Cisco CX Cloud Success Tracks へのアクセスを有効にします。そうしないと、Machine Reasoning Engine (MRE) がサポートする Security Advisories、Bug Identifier、および EOX 機能の拡張構成ベースのスキャンに追加された拡張機能が期待どおりに動作しません。	https://api-cx.cisco.com
Webex と統合します。	• http://analytics.webexapis.com • https://webexapis.com
Cisco Catalyst Cloud およびホストされているアプリケーションとの接続 (AppX MS Teams 統合、Talos 統合など)。	*.cisco.com : 443 それ以外の場合の特定の FQDN は次のとおりです。 • neoffers.cisco.com • neoffers-de.cisco.com • neoffers-sg.cisco.com • dnaservices.cisco.com
Cisco Meraki と統合します。	推奨 : *.meraki.com:443 ワイルドカードを回避したいお客様は、代わりに次の URL を指定できます。 • dashboard.meraki.com:443 • api.meraki.com:443

目的

OCSP/CRL を使用した SSL/TLS 証明書の失効ステータスを確認します。

...Catalyst Center がアクセスする必要がある URL と FQDN

- <http://validation.identrust.com>
- <http://commercial.ocsp.identrust.com>

 注

これらの URL は、直接でも Catalyst Center で構成されているプロキシサーバー経由でも到達できるようにする必要があります。

Catalyst Center リモートサポート機能が有効になっている場合、シスコの認定スペシャリストがトラブルシューティングデータを収集できるようにします。

wss://prod.radkit-cloud.cisco.com:443

cisco.com とシスコ スマート ライセンス と統合します。

*.cisco.com : 443

ワイルドカードを回避するには、代わりに次の URL を指定します。

- software.cisco.com
- cloudsso.cisco.com
- cloudsso1.cisco.com
- cloudsso2.cisco.com
- apiconsole.cisco.com
- api.cisco.com
- apx.cisco.com
- smartreceiver.cisco.com
- sso.cisco.com
- apmx-prod1-vip.cisco.com
- apmx-prod2-vip.cisco.com
- tools.cisco.com
- tools1.cisco.com
- tools2.cisco.com

Network-Based Application Recognition (NBAR) に接続します。

prod.sdavc-cloud-api.com:443

不正なベンダー名を検出するには、不正管理アプリケーションを有効にします。

<https://standards-oui.ieee.org/>

目的

サイトとロケーションマップで正確な情報をレンダリングします。

...Catalyst Center がアクセスする必要がある URL と FQDN

- www.mapbox.com
- [*.tiles.mapbox.com/*: 443](https://*.tiles.mapbox.com/*:443) プロキシの場合、宛先は *.tiles.mapbox.com/* です。

 注

- これらの URL は、ブラウザがマップをレンダリングするために必要です。
- ブラウザは WebGL (<https://webglreport.com/?v=1>) をサポートしている必要があります。

Cisco AI Network Analytics のデータ収集では、クラウドホストへのアウトバウンド HTTPS (TCP 443) アクセスを許可するようにネットワークまたは HTTP プロキシを設定します。

- <https://api.use1.prn.kairos.ciscolabs.com> (米国東部リージョン)
- <https://api.euc1.prn.kairos.ciscolabs.com> (欧州中央リージョン)

GUI から特定のタスクを完了できる対話型ヘルプフローのメニューにアクセスします。 <https://ec.walkme.com>

ライセンスサービスにアクセスします。 <https://swapi.cisco.com>

Cisco Spaces と統合します。

- <https://ciscospaces.io>
- <https://ciscospaces.eu>
- <https://ciscospaces.sg>

リモート URL に安全にアクセスするために HTTPS プロキシサーバーの使用を推奨します。

デフォルトでは、アプライアンスはインターネットに接続して、ソフトウェアの更新、ライセンス、デバイスソフトウェア、マップ情報、ユーザーからのフィードバックをダウンロードします。これらの構成タスクのためにインターネット接続を維持します。

 注

インターネット宛トラフィックをルーティングするように設定されているアプライアンス インターフェイスは、すべての通信の送信元として機能します。

リモート URL に安全にアクセスするために HTTPS プロキシサーバーを使用します。アプライアンスが「**必要なインターネット URL と完全修飾ドメイン名**」リスト内の URL にアクセスできるようにするために、

HTTPS プロキシサーバーを使用します。アプライアンスのインストール中に、プロキシサーバーの URL、ポート番号、および必要に応じてログイン情報を入力するように求められます。

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ーとの通信のみをサポートしています。HTTPS プロキシサーバーをネットワーク内の任意の場所に配置できます。プロキシサーバーは HTTPS を使用してインターネットと通信しますが、アプライアンスは HTTP 経由でプロキシサーバーと通信します。アプライアンスの設定時に、プロキシの HTTP ポートを指定します。

設定後にプロキシ設定を変更するには、GUI を使用します。

ポートの効率的な管理による Catalyst Center 展開の保護に関する情報。

この表を使用して、Catalyst Center が使用するポート、ポートを介して通信するサービス、およびそれらを使用する理由について説明します。[Recommended Action] 列は、ネットワークトラフィックを既知の IP アドレスまたは範囲に制限できるかどうか、Catalyst Center の機能に影響を与えることなく接続をブロックできるかどうか、またはポートを開いておく必要があるかどうかを示します。

重要

- Catalyst Center からのアウトバウンド通信では、サービスをホストしているノードのルーティング可能なインターフェイス IP アドレスを使用します。マルチノードクラスターの場合、プロキシおよびファイアウォールルールに各ノードのインターフェイス IP と VIP アドレスを含めます。
- セキュリティに関する推奨事項：
 - Catalyst Center と管理ネットワークまたはエンタープライズ ネットワークの間にファイアウォールを展開し、階層型アプローチを使用して Catalyst Center 展開を保護します。
 - 特定の IP アドレスまたは範囲に対してポートを開きます。

Catalyst Center の宛先ポートは一部重複しています。関連セクションを参照して、各ネットワークサービスを使用する方法と理由を確認してください。ファイアウォールルールの送信元または宛先 IP アドレスまたは範囲を制限します。サービスが Catalyst Center 展開で使用されていない場合は、ポートを閉じたままにします。

6 : Catalyst Center

Port	サービス名	目的	推奨処置
Catalyst Center の管理または設定			
TCP 443	UI、REST、HTTPS	GUI、REST、HTTPS 管理ポート。	ポートを開いたままにしておきます。
TCP 2222	Catalyst Center シェル	Catalyst Center シェルに接続します。	ポートを開いたままにしておきます。既知の IP アドレスを送信元に制限します。
TCP 9004	Web UI インストール	GUI ベースのインストールページを提供します (Web ベースのオプションを使用して Catalyst Center をインストールする場合にのみ必要です)。	ノードのインストールが完了するまで、ポートを開いたままにしておきます。

Port	サービス名	目的	推奨処置
TCP 9005	Web UI インストール API サービス	Web ベースのインストール用の API を提供します（ブラウザクライアントによってポート 9004 から接続されます。外部エージェントはアクセスを必要としません）。	クラスターの形成が完了するまでポートを開いておく必要があります。

Cisco IMC の管理または設定

TCP 22	Catalyst Center シェル	Catalyst Center シェルに接続します。	ポートを開いたままにしておきます。既知の IP アドレスを送信元として設定します。
UDP と TCP 53	DNS	DNS 名を IP アドレスに解決するために使用されます。	他のサービス（NTP DNS 名など）の IP アドレスの代わりに DNS 名を使用する場合は、ポートを開く必要があります。
UDP と TCP 389	LDAP	Cisco IMC ユーザー管理 LDAP。	LDAP を介した外部ユーザー認証が必要な場合はオプションです。
TCP 443	UI、 REST、 HTTPS	Web UI、REST、HTTPS 管理ポート。	ポートを開いたままにしておきます。
UDP と TCP 636	LDAPS	SSL を介した LDAP による Cisco IMC ユーザー管理。	LDAPS を介した外部ユーザー認証が必要な場合はオプションです。
TCP 2068	HTTPS	リモート KVM コンソールのリダイレクトポート。	ノードのインストールが完了するまで、ポートを開いたままにしておきます。
UDP 123	NTP	NTP サーバーと時刻を同期します。	ポートを開いたままにしておきます。
UDP 161	SNMP ポーリング/ 設定	SNMP サーバーのポーリングと設定。	SNMP サーバーのポーリングおよび設定のオプションです。
UDP 162	SNMP トラップ	SNMP トラップを外部 SNMP サーバーに送信します。	SNMP サーバーコレクタのオプションです。
UDP 514	Syslog	外部サーバーの障害とログを表示します。	メッセージログを外部サーバーに送信する場合のオプションです。

Catalyst Center からデバイスおよび他のシステムへのアウトバウンド

–	ICMP	Catalyst Center では、ネットワークデバイスの検出やネットワーク接続の問題のトラブルシューティングに ICMP メッセージを使用します。	ICMP を有効にします。
---	------	---	---------------

Port	サービス名	目的	推奨処置
TCP 22	SSH	Catalyst Center では、次の目的でネットワークデバイスに接続する際に SSH を使用します。 - 検出用にデバイス設定を読み取る。 - 設定を変更する。 また、Catalyst Center は、リモート同期 (rsync) ストレージサーバーへの自動バックアップに SSH (ポート 22) を使用します。	Catalyst Center と管理対象ネットワークの間で SSH を開いておく必要があります。
TCP 23	Telnet	Telnet の使用は回避してください。 SSH を利用してセキュア通信を行います。  注 Telnet は推奨されませんが、Catalyst Center では検出用のデバイス設定の読み取りや設定の変更に Telnet を使用できます。	デバイス管理に Telnet を使用する必要がある場合は、Telnet で暗号化などのセキュリティメカニズムが提供されないことを理解してください。セキュアな管理のために SSH を使用します。
TCP 49	TACACS+	Cisco ISE などの TACACS+ サーバーを使用した外部認証を使用している場合のみ必要です。	TACACS+ サーバーを使用した外部認証を使用している場合のみ、ポートを開きます。
TCP 80	HTTP	Catalyst Center は、トラストプールの更新に HTTP を使用します。	シスコのサポートする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 に対する発信トラフィックを許可するようにネットワークを設定します。 http://www.cisco.com/security/pki/
TCP 80	OCSP/CRL	Catalyst Center は、 OCSP/CRL を使用した SSL/TLS 証明書の失効ステータスを確認します。	これらの URL は、直接でも Catalyst Center で構成されているプロキシサーバー経由でも到達できるようにする必要があります。到達可能でない場合、Catalyst Center は cisco.com に接続するときに証明書失効チェックをスキップします。 http://validation.identrust.com http://commercial.ocsp.identrust.com
UDP 53	DNS	Catalyst Center では、ホスト名の解決に DNS を使用します。	DNS によるホスト名の解決用にポートを開いておく必要があります。

Port	サービス名	目的	推奨処置
TCP および UDP 111、20048、および 32767	NFS	Assurance のバックアップに使用します。	ポートを開いたままにしておきます。
UDP 123	NTP	Catalyst Center では、指定したソースとの時刻の同期に NTP を使用します。	時刻の同期用にポートを開いておく必要があります。
UDP 161	SNMP	Catalyst Center では、ネットワークデバイスの検出、デバイスタイプを含むデバイスインベントリの詳細の読み取り、CPU や RAM などのテレメトリデータの収集に SNMP を使用します。	ネットワークデバイスの管理と検出用にポートを開いておく必要があります。
TCP 443	HTTPS	Catalyst Center は HTTPS をクラウド接続型のアップグレードに使用します。	クラウド接続、テレメトリ、およびソフトウェアアップグレード用にポートを開いておく必要があります。 Cisco ISE に対してポートを開いたままにしておきます。
TCP 830	NETCONF	Catalyst Center では、デバイスのインベントリ、検出、および設定に NETCONF を使用します。	NETCONF をサポートするネットワークデバイスの管理と検出用にポートを開いておく必要があります。
UDP 1645、1812	RADIUS	RADIUS サーバーを使用した外部認証を使用する場合のみ必要です。	Catalyst Center へのユーザーログインの認証に外部 RADIUS サーバーを使用している場合のみ、ポートを開いておく必要があります。
TCP 5222、8910	Cisco ISE	Catalyst Center は Cisco ISE XMP (PxGrid 用) を使用します。	Cisco ISE に対してポートを開いたままにしておきます。
TCP 9060	Cisco ISE	Catalyst Center は Cisco ISE ERS API トラフィックを使用します。	Cisco ISE に対してポートを開いたままにしておきます。
デバイスから Catalyst Center			
–	ICMP	デバイスは ICMP メッセージを使用してネットワーク接続の問題を通知します。	デバイスの通信を許可するには、ICMP を有効にします。

Port	サービス名	目的	推奨処置
TCP 22、80、443	HTTPS、SFTP、HTTP	Catalyst Center からのソフトウェアイメージのダウンロードに HTTPS 443、SFTP 22、HTTP 80 を使用します。 Catalyst Center からの証明書のダウンロードに HTTPS 443、HTTP 80 (Cisco 9800 ワイヤレスコントローラ、PnP)、センサー/テレメトリを使用します。 Catalyst Center からの JWT (認証トークン) の取得に HTTPS:443 (Cisco Catalyst Assurance インテリジェントキャプチャ機能を使用する任意のアクセスポイント) を使用します。	これらのポートでアクセス権限が付与されたホストまたはネットワークデバイスの送信元 IP がファイアウォールルールで制限されていることを確認してください。 HTTP 80 の使用方法の詳細については、『Cisco Catalyst Center セキュリティのベストプラクティスガイド』の「HTTP ポート 80 例外リスト」のトピックを参照してください。
注 ポート 80 については、プラグアンドプレイ (PnP)、ソフトウェアイメージ管理 (SWIM)、組み込みイベント管理 (EEM)、デバイス登録、Cisco 9800 ワイヤレスコントローラを使用しない場合はブロックしてください。			
UDP 67	BOOTP	ネットワークデバイスと Catalyst Center 間の通信を開始するために使用します。	ポートを開いたままにしておきます。
UDP 123	NTP	デバイスは時刻の同期に NTP を使用します。	デバイスが時刻を同期できるようにポートを開いておく必要があります。
UDP 162	SNMP	Catalyst Center はデバイスから SNMP ネットワークテレメトリを受信します。	SNMP に基づくデータ分析用にポートを開いておく必要があります。
UDP 514	Syslog	Catalyst Center はデバイスから syslog メッセージを受信します。	syslog に基づくデータ分析用にポートを開いておく必要があります。
2049	NFS	Assurance のバックアップに使用します。	ポートを開いたままにしておきます。
UDP 6007	NetFlow	Catalyst Center はデバイスから NetFlow ネットワークテレメトリを受信します。	NetFlow に基づくデータ分析用にポートを開いておく必要があります。

Port	サービス名	目的	推奨処置
TCP 9991	Wide Area Bonjour サービス	Catalyst Center は、Bonjour 制御プロトコルを使用して、サービス検出ゲートウェイ (SDG) エージェントからマルチキャストドメインネームシステム (mDNS) トラフィックを受信します。	Bonjourアプリケーションがインストールされている場合、Catalyst Center でポートを開いておく必要があります。
UDP 21730	アプリケーション可視性サービス	アプリケーション可視性サービスの CBAR デバイス通信。	ネットワークデバイスで CBAR が有効になっている場合、ポートを開いておく必要があります。
TCP 25103	ストリーミングテレメトリが有効になっている Cisco 9800 ワイヤレスコントローラおよび Cisco Catalyst 9000 スイッチ	テレメトリに使用されます。	Catalyst Center と Catalyst 9000 デバイス間のテレメトリ接続用にポートが開いている必要があります。
TCP 32626	インテリジェントキャプチャ (gRPC) コレクタ	Cisco Catalyst Assurance インテリジェントキャプチャ機能に関連する AP/クライアント統計情報およびパケットキャプチャデータの受信用の gRPC チャネルを確立するために使用します。	Cisco Catalyst Assurance インテリジェントキャプチャ (gRPC) 機能を使用する場合、ポートを開いておく必要があります。

HTTP 80

HTTP ポート 80 例外リスト。

7: HTTP 80

エリア	HTTP ポート 80 が必要な理由	該当する Catalyst Center/デバイスバージョン	E2E 暗号化がない場合でもセキュリティを実現する方法
SCEP	RFC 8894 - Simple Certificate Enrollment Protocol	すべての Catalyst Center およびデバイスバージョン。	SCEP は、共有秘密と PKCS12 により暗号化された CSR/証明書交換を使用します。
プラグアンドプレイ	PnP Hello は HTTP 経由で実行されますが、デバイスが ios.p7b をダウンロードすると HTTPS に切り替わります。 デバイスは、ios.7b トラストバンドルにトラストを固定することで、Catalyst Center との HTTPS を確立します。	すべての Catalyst Center およびデバイスバージョン。	ios.p7b は、Cisco Manufacturing CA によって署名された暗号化ハッシュで保護されています。
テレメトリ証明書のダウンロード	証明書は HTTP を使用してダウンロードされます。	すべての Catalyst Center およびデバイスバージョン。	ダウンロードされた証明書は PKCS12 で暗号化されます。
SWIM	リモートサーバー (HTTP) から Catalyst Center イメージリポジトリにイメージをインポートすることができます。	すべての Catalyst Center バージョン。	HTTP を介してインポートされたイメージは、ファイルのハッシュをチェックすることによって完全性が検証されます。

ディザスタリカバリ設定の保護に関する情報。

実稼働環境でディザスタリカバリを使用している場合は、ディザスタリカバリの設定を保護するファイアウォールとセキュリティポリシーを使用します。表に示されているポートを開き、ネットワークのデータセンター全体でディザスタリカバリを設定するために必要なアクセス権が Catalyst Center にあることを確認します。

注

3 ノードクラスタの場合は、各ノードの送信元エンタープライズ IP アドレスが許可されていることを確認します。

8 : Catalyst Center

ソースポート	送信元	宛先ポート	接続先	説明
任意	Catalyst Center エンタープライズ IP/VIP	TCP 443	Catalyst Center エンタープライズ VIP	REST API アクセス
任意	Catalyst Center エンタープライズ IP/VIP	UDP 500	Catalyst Center エンタープライズ VIP	IPSec トンネル
任意	Catalyst Center エンタープライズ IP/VIP	TCP 873	Catalyst Center エンタープライズ VIP	rsync による GlusterFS データのレプリケーション
任意	Catalyst Center エンタープライズ IP/VIP	UDP 4500	Catalyst Center エンタープライズ VIP	IPSec トンネル
任意	Catalyst Center エンタープライズ IP/VIP	TCP 8300	Catalyst Center エンタープライズ VIP	Consul RPC 通信
任意	Catalyst Center エンタープライズ IP/VIP	TCP 8301	Catalyst Center エンタープライズ VIP	Consul SERF LAN ポート
任意	Catalyst Center エンタープライズ IP/VIP	UDP 8301	Catalyst Center エンタープライズ VIP	Consul SERF LAN ポート
任意	Catalyst Center エンタープライズ IP/VIP	TCP 8302	Catalyst Center エンタープライズ VIP	Consul SERF WAN ポート ²
任意	Catalyst Center エンタープライズ IP/VIP	UDP 8302	Catalyst Center エンタープライズ VIP	Consul SERF WAN ポート ¹
任意	Catalyst Center エンタープライズ IP/VIP	TCP 8443	Catalyst Center エンタープライズ VIP	HA プロキシ API アクセス ³

² この要件は今後の Catalyst Center リリースで排除される予定です。

³ この要件は、今後の Catalyst Center リリースで追加されます。

ソース ポート	送信元	宛先ポート	接続先	説明
任意	Catalyst Center エ ンタープライズ IP/VIP	UDP 500	監視 IP	IPSec トンネル
任意	Catalyst Center エ ンタープライズ IP/VIP	TCP 2222	監視 IP	監視システム到達可能性のための TCP ping
任意	Catalyst Center エ ンタープライズ IP/VIP	UDP 4500	監視 IP	IPSec トンネル
任意	Catalyst Center エ ンタープライズ IP/VIP	TCP 8300	監視 IP	Consul RPC 通信
任意	Catalyst Center エ ンタープライズ IP/VIP	TCP 8301	監視 IP	Consul SERF LAN ポート
任意	Catalyst Center エ ンタープライズ IP/VIP	UDP 8301	監視 IP	Consul SERF LAN ポート
任意	Catalyst Center エ ンタープライズ IP/VIP	TCP 8302	監視 IP	Consul SERF WAN ポート ¹
任意	Catalyst Center エ ンタープライズ IP/VIP	UDP 8302	監視 IP	Consul SERF WAN ポート ¹
任意	Catalyst Center エ ンタープライズ IP/VIP	TCP 8443	監視 IP	HA プロキシ API アクセス ²
任意	Catalyst Center エ ンタープライズ/ 管理 VIP	TCP 179	ネイバールータ	ネイバールータとの BGP セッション
📄 注 ディザスタリカバリ VIP をアドバタイズする ように BGP が設定されている場合は、こ のポートを開きます。				
任意	監視 IP	UDP 53	DNS サーバー	監視システムから DNS サーバーへ
任意	監視 IP	UDP 123	NTP サーバー	監視システムから NTP サーバーへ
任意	監視 IP	TCP 443	Catalyst Center エ ンタープライズ VIP	ディザスタリカバリ登録時の API へのアクセ ス

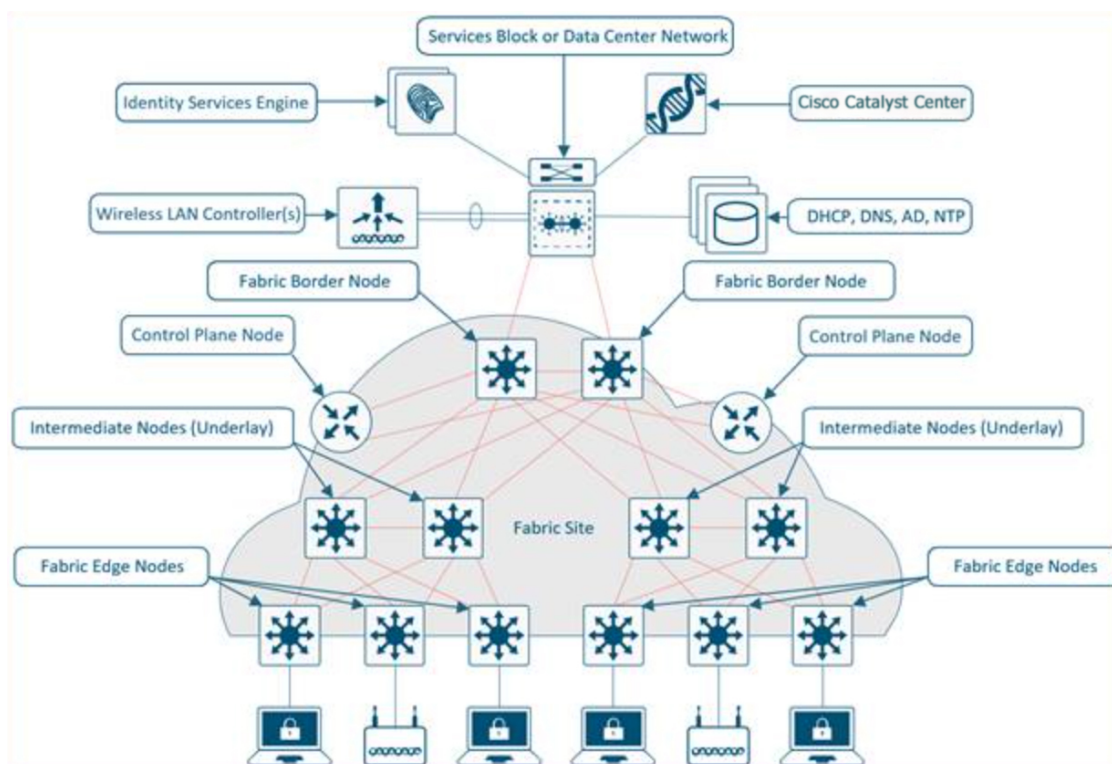
ソース ポート	送信元	宛先ポート	接続先	説明
任意	監視 IP	UDP 500	Catalyst Center エンタープライズ VIP	IPSec トンネル
任意	監視 IP	UDP 4500	Catalyst Center エンタープライズ VIP	IPSec トンネル
任意	監視 IP	TCP 8300	Catalyst Center エンタープライズ VIP	Consul RPC 通信
任意	監視 IP	TCP 8301	Catalyst Center エンタープライズ VIP	Consul SERF LAN ポート
任意	監視 IP	UDP 8301	Catalyst Center エンタープライズ VIP	Consul SERF LAN ポート
任意	監視 IP	TCP 8302	Catalyst Center エンタープライズ VIP	Consul SERF WAN ポート ¹
任意	監視 IP	UDP 8302	Catalyst Center エンタープライズ VIP	Consul SERF WAN ポート ¹
任意	監視 IP	TCP 8443	Catalyst Center エンタープライズ VIP	HA プロキシ API アクセス ²

Cisco Software-Defined Access

Cisco SD-Access インフラストラクチャで必要な追加のポート、プロトコル、ネットワークトラフィックについて説明します。

このトピックでは、図に示されているものと同様の一般的な **Cisco SD-Access** ファブリック展開に関連するポート、プロトコル、およびトラフィックのタイプについて説明します。

7 : Cisco SD-Access Fabric Infrastructure



ネットワークに **Cisco SD-Access** を実装している場合は、この表を使用して、**Cisco SD-Access** インフラストラクチャの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。このセットアップにより、**Catalyst Center** でネットワーク管理を自動化することもできます。

注

インターネット宛トラフィックをルーティングするように設定されているアプライアンス インターフェイスは、すべての通信の送信元として機能します。

9 : Catalyst Center

送信元ポート ⁴	送信元	宛先ポート	接続先	説明
任意	Catalyst Center	UDP 53	DNS サーバ	Catalyst Center から DNS サーバの間で使用
任意	Catalyst Center	TCP 22	ファブリックアンダーレイ	Catalyst Center からファブリックスイッチのループバックの間で SSH に使用
任意	Catalyst Center	TCP 23	ファブリックアンダーレイ	Catalyst Center からファブリックスイッチのループバックの間で Telnet に使用
任意	Catalyst Center	UDP 161	ファブリックアンダーレイ	Catalyst Center からファブリックスイッチのループバックの間で SNMP デバイス検出に使用

⁴ クラスタ、PKI、SFTP サーバー、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。

ICMP	Catalyst Center	ICMP	ファブリックアンダーレイ	Catalyst Center からファブリックスイッチのループバックの間でSNMPデバイス検出に使用
任意	Catalyst Center	TCP 443	ファブリックアンダーレイ	スイッチ用およびNFVIS用のホストアブリケーション
任意	Catalyst Center	UDP 6007	スイッチとルータ	Catalyst Center からスイッチおよびルータの間でNetFlowに使用
任意	Catalyst Center	TCP 830	ファブリックアンダーレイ	Catalyst Center からファブリックスイッチの間でNETCONFに使用 (Cisco SD-Access 組み込みワイヤレス)
UDP 123	Catalyst Center	UDP 123	ファブリックアンダーレイ	Catalyst Center からファブリックスイッチの間でLAN自動化中の初回期間に使用
任意	Catalyst Center	UDP 123	NTP サーバ	Catalyst Center から NTP サーバの間で使用
任意	Catalyst Center	TCP 22、UDP 161	シスコワイヤレスコントローラ	Catalyst Center からシスコワイヤレスコントローラの間で使用
ICMP	Catalyst Center	ICMP	シスコワイヤレスコントローラ	Catalyst Center からシスコワイヤレスコントローラまで
任意	AP	TCP 32626	Catalyst Center	Cisco Catalyst Assurance インテリジェントキャプチャ (gRPC) 機能で使用されるトラフィック統計情報とパケットキャプチャデータの受信に使用されます。

10 :

送信元ポート	送信元	宛先ポート	接続先	説明
任意	Catalyst Center	TCP 443	registry.ciscoconnectdna.com	Catalyst Center パッケージ更新のダウンロード
任意	Catalyst Center	TCP 443	www.ciscoconnectdna.com	Catalyst Center パッケージ更新のダウンロード
任意	Catalyst Center	TCP 443	registry-cdn.ciscoconnectdna.com	Catalyst Center パッケージ更新のダウンロード
任意	Catalyst Center	TCP 443	cdn.ciscoconnectdna.com	Catalyst Center パッケージ更新のダウンロード
任意	Catalyst Center	TCP 443	software.cisco.com	デバイスソフトウェアのダウンロード
任意	Catalyst Center	TCP 443	cloudsso.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
任意	Catalyst Center	TCP 443	cloudsso1.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
任意	Catalyst Center	TCP 443	cloudsso2.cisco.com	Cisco.com とスマートアカウントのクレデンシャルの検証
任意	Catalyst Center	TCP 443	apiconsole.cisco.com	CSSM スマートライセンス API

任意	Catalyst Center	TCP 443	sso.cisco.com	Cisco.com クレデンシャルとスマートライセンス
任意	Catalyst Center	TCP 443	api.cisco.com	Cisco.com クレデンシャルとスマートライセンス
任意	Catalyst Center	TCP 443	apx.cisco.com	Cisco.com クレデンシャルとスマートライセンス
任意	Catalyst Center	TCP 443	dashboard.meraki.com	Meraki の統合
任意	Catalyst Center	TCP 443	api.meraki.com	Meraki の統合
任意	Catalyst Center	TCP 443	n63.meraki.com	Meraki の統合
任意	Catalyst Center	TCP 443	dnacenter.uservoice.com	ユーザフィードバックの送信
任意	Catalyst Center Admin Client	TCP 443	*.mapbox.com/:443	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 *.mapbox.com/*）
任意	Catalyst Center	TCP 443	www.mapbox.com	マップとシスコワイヤレスコントローラの国コードの識別

11 : Cisco Software-Defined Access

送信元ポート ⁵	送信元	宛先ポート	接続先	説明
UDP 68	ファブリックアンダーレイ	UDP 67	DHCP サーバ	ファブリックスイッチ、ルータからDHCPサーバの間で、ファブリックエッジノードによって開始されるDHCP リレーパケットに使用。
任意	ファブリックアンダーレイ	TCP 80	Catalyst Center	ファブリックスイッチ、ルータループバック IP から Catalyst Center の間で PnP に使用
任意	ファブリックアンダーレイ	TCP 443	Catalyst Center	ファブリックスイッチ、ルータループバック IP から Catalyst Center の間でイメージのアップグレードに使用
任意	ファブリックアンダーレイ	UDP 162	Catalyst Center	ファブリックスイッチ、ルータループバック IP から Catalyst Center の間で SNMP トラップに使用
任意	ファブリックアンダーレイ	UDP 514	Catalyst Center	ファブリックスイッチ、ルータから Cisco Catalyst Assurance
任意	ファブリックアンダーレイ	UDP 6007	Catalyst Center	ファブリックスイッチおよびルータから Catalyst Center の間で NetFlow に使用
任意	ファブリックアンダーレイ	UDP 123	Catalyst Center	ファブリックスイッチから Catalyst Center の間で LAN 自動化時に使用

⁵ 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。

ICMP	ファブリックア ンダーレイ	ICMP	Catalyst Center	ファブリックスイッチ、ルータ ループバックから Catalyst Center の 間で SNMP デバイス検出に使用
UDP 161	ファブリックア ンダーレイ	任意	Catalyst Center	ファブリックスイッチ、ルータ ループバックから Catalyst Center の 間で SNMP デバイス検出に使用
任意	ファブリックア ンダーレイ	UDP 53	DNS サーバ	ファブリックスイッチ、ルータか ら DNS サーバの間で名前解決に使用
TCP およ び UDP 4342	ファブリックア ンダーレイ、コ ントロールプ レーン	任意	ファブリックルー タ、スイッチ、お よびシスコワイ ヤレスコントロー ラ	● LISP コントロールプレーン通信 ● コントロールプレーンのルー プバック IP からシスコワイ ヤレス コントローラの間でファ ブリック対応ワイヤレスに使用
TCP およ び UDP 4342	ファブリックア ンダーレイ、コ ントロールプ レーン	TCP および UDP 4342	ファブリックルー タ、スイッチ、お よびシスコワイ ヤレスコントロー ラ	● LISP でカプセル化された制御 メッセージ ● コントロールプレーンのルー プバック IP から シスコワイ ヤレス コントローラ の間でファ ブリック対応ワイヤレスに使用
任意	ファブリックア ンダーレイ	UDP 4789	ファブリックルー タおよびスイッチ	ファブリックカプセル化データパ ケット (VXLAN-GPO)
任意	ファブリックア ンダーレイ	UDP 1645/1646/1812/1813	Cisco ISE	ファブリックスイッチ、ルータ ループバック IP から Cisco ISE の間 で RADIUS に使用
ICMP	ファブリックア ンダーレイ	ICMP	Cisco ISE	ファブリックスイッチ、ルータか ら Cisco ISE の間でトラブルシュー ティングに使用
UDP 1700/3799	ファブリックア ンダーレイ	任意	Cisco ISE	ファブリックスイッチから Cisco ISE の間で気付アドレス (CoA) に 使用
任意	ファブリックア ンダーレイ	UDP 123	NTP サーバ	ファブリックスイッチ、ルータ ループバック IP から NTP サーバの 間で使用
任意	コントロール プ レーン	UDP および TCP 4342/4343	ファブリックルー タ、スイッチ、お よびシスコワイ ヤレスコントロー ラ	● LISP でカプセル化された制御 メッセージ ● コントロールプレーンのルー プバック IP からシスコワイ ヤレス コントローラの間でファ ブリック対応ワイヤレスに使用

UDP およ
び TCP
4342/4343

コントロール プ
レーン

任意

ファブリックルー
タ、スイッチ、お
よびシスコワイ
ヤレスコントロー
ラ

- LISP でカプセル化された制御
メッセージ
- コントロールプレーンのルー
プバック IP から シスコワイ
ヤレス コントローラ の間でファ
ブリック対応ワイヤレスに使用

12 :

ソース ポート	送信元	宛先ポート	接続先	説明
UDP 5246/5247/5248	シスコ ワイヤレス コントローラ	任意	AP IP アドレス プール	シスコワイヤレス コントローラ と AP サブネットの間で CAPWAP 用に使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	AP IP アドレス プール	シスコワイヤレス コントローラ と Ping を許可する AP の間でト ラブルシューティングのために 使用
任意	シスコ ワイヤレス コントローラ	● TCP 443 (Cisco AireOS ワイヤレスコン トローラ) ● TCP 25103 (ストリーミ ングテレメト リが有効に なっている Cisco 9800 ワ イヤレスコン トローラおよ び Cisco Catalyst 9000 スイッチ)	Catalyst Center	Assurance の シスコ ワイヤレス コントローラ と Catalyst Center の間で使用
任意	シスコ ワイヤレス コントローラ	UDP 69/5246/5247 TCP 22	AP IP アドレス プール	シスコワイヤレス コントローラ と AP サブネットの間で CAPWAP 用に使用
任意	シスコ ワイヤレス コントローラ	UDP および TCP 4342/4343	コントロール プ レーン	シスコワイヤレス コントローラ と コントロールプレーンループ バック IP アドレスの間で使用
任意	シスコ ワイヤレス コントローラ	TCP 22	Catalyst Center	シスコワイヤレス コントローラ と Catalyst Center の間でデバイ ス検出のために使用
UDP 161	シスコ ワイヤレス コントローラ	任意	Catalyst Center	シスコワイヤレス コントローラ と Catalyst Center の間で SNMP の ために使用
任意	シスコ ワイヤレス コントローラ	UDP 162	Catalyst Center	シスコワイヤレス コントローラ と Catalyst Center の間で SNMP ト ラップのために使用

任意	シスコ ワイヤレス コントローラ	TCP 16113	Cisco Mobility Services Engine (MSE) と Cisco SPECTRUM EXPERT	シスコワイヤレスコントローラ と Cisco MSE および Spectrum Expert の間で NMSP のために使 用
任意	シスコ ワイヤレス コントローラ	UDP 6007	Catalyst Center	ワイヤレスコントローラ と Catalyst Center の間で NetFlow ネットワークテレメトリのために 使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	Catalyst Center	シスコワイヤレスコントローラ から、トラブルシューティング に向けた Ping の許可に使用
任意	シスコ ワイヤレス コントローラ とさ まざまな syslog サーバー	UDP 514	シスコ ワイヤレ ス コントローラ	Syslog (オプション)
任意	シスコ ワイヤレス コントローラ	UDP 53	DNS サーバ	シスコワイヤレスコントローラ から DNS サーバの間で使用
任意	シスコ ワイヤレス コントローラ	TCP 443	Cisco ISE	シスコワイヤレスコントローラ と Cisco ISE の間でゲスト SSID Web 認証のために使用
任意	シスコ ワイヤレス コントローラ	UDP 1645、1812	Cisco ISE	シスコワイヤレスコントローラ と Cisco ISE の間で Radius 認証に 使用
任意	シスコ ワイヤレス コントローラ	UDP 1646、1813	Cisco ISE	シスコワイヤレスコントローラ と Cisco ISE の間で RADIUS アカ ウンティングに使用
任意	シスコ ワイヤレス コントローラ	UDP 1700、3799	Cisco ISE	シスコワイヤレスコントローラ と Cisco ISE の間で RADIUS CoA に使用
ICMP	シスコ ワイヤレス コントローラ	ICMP	Cisco ISE	シスコワイヤレスコントローラ と Cisco ISE の間で ICMP トラブ ルシューティングに使用
任意	シスコ ワイヤレス コントローラ	UDP 123	NTP サーバ	シスコワイヤレスコントローラ から NTP サーバの間で使用

13 : AP IP

送信元ポー ト	送信元	宛先ポート	接続先	説明
UDP 68	AP IP アドレスプー ル	UDP 67	DHCP サーバ	AP IP アドレスプールから DHCP サー バの間で使用
ICMP	AP IP アドレスプー ル	ICMP	DHCP サーバ	AP IP アドレスプールから ICMP の間 でトラブルシューティングに使用
任意	AP IP アドレスプー ル	514	各種	Syslog (接続先は設定可能)。 Default is 255.255.255.255.

任意	AP IP アドレスプ ール	UDP 69/5246/5247/5248	シスコ ワイヤレ ス コントローラ	AP IP アドレスプールと シスコ ワイ ヤレス コントローラ の間で CAPWAP 用に使用
ICMP	AP IP アドレスプ ール	ICMP	シスコ ワイヤレ ス コントローラ	AP IP アドレスプールから シスコ ワ イヤレス コントローラ の間でトラ ブルシューティング用の ping を許 可するために使用

14 : Cisco ISE

送信元ポート ⁶	送信元	宛先ポート	接続先	説明
任意	Cisco ISE	TCP 64999	Border	Cisco ISE と ボーダーノード の間で SGT Exchange Protocol (SXP) に使用
任意	Cisco ISE	UDP 514	Catalyst Center	Cisco ISE と syslog サーバー (Catalyst Center) の間で使用
UDP 1645/1646/1812/1813	Cisco ISE	任意	ファブリックアン ダーレイ	Cisco ISE と ファブリックスイッチ、ルー タ の間で RADIUS と 認証 用に使用
任意	Cisco ISE	UDP 1700/3799	ファブリックアン ダーレイ シスコ ワイ ヤレス コントローラ	Cisco ISE と ファブリックスイッチ、ルー ター プバック IP アドレス の間で RADIUS 認可 変更 (CoA) に使用 Cisco ISE から ワイヤレス コントローラ の 間で CoA に 使用する 場合、UDP ポー ト 3799 も 開いている 必要があります。
ICMP	Cisco ISE	ICMP	ファブリックアン ダーレイ	Cisco ISE から ファブリックスイッチの 間で トラブルシューティング に 使用
任意	Cisco ISE	UDP 123	NTP サーバ	Cisco ISE から NTP サーバ の間で 使用
UDP 1812/1645/1813/1646	Cisco ISE	任意	シスコ ワイヤレ ス コントローラ	Cisco ISE と シスコ ワイヤレス コント ローラ の間の RADIUS のために 使用
ICMP	Cisco ISE	ICMP	シスコ ワイヤレ ス コントローラ	Cisco ISE と シスコ ワイヤレス コント ローラ の間の トラブルシューティング のために 使用

15 : DHCP

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 67	DHCP サー バ	UDP 68	AP IP アドレスプール	DHCP サーバから ファブリック AP の間で 使用
ICMP	DHCP サー バ	ICMP	AP IP アドレスプール	トラブルシューティング 用の ICMP : ファ ブリックから DHCP の間で 使用
UDP 67	DHCP サー バ	UDP 68	ファブリックアン ダーレイ	DHCP から ファブリックスイッチ、ルー タ の間で 使用
ICMP	DHCP サー バ	ICMP	ファブリックアン ダーレイ	トラブルシューティング 用の ICMP : ファ ブリックから DHCP の間で 使用

⁶ 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。

UDP 67	DHCP サーバ	UDP 68	ユーザー IP アドレスプール	DHCP サーバからファブリックスイッチ、ルータの間で使用
ICMP	DHCP サーバ	ICMP	ユーザー IP アドレスプール	トラブルシューティング用の ICMP : ユーザと DHCP の間で使用

16 : NTP

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 123	NTP サーバ	任意	Cisco ISE	NTP サーバから Cisco ISE
UDP 123	NTP サーバ	任意	Catalyst Center	NTP サーバから Catalyst Center
UDP 123	NTP サーバ	任意	ファブリックアンダーレイ	NTP サーバからファブリックスイッチ、ルータループバックの間で使用
UDP 123	NTP サーバ	任意	シスコ ワイヤレス コントローラ	NTP サーバから シスコ ワイヤレス コントローラ

17 : DNS

送信元ポート	送信元	宛先ポート	接続先	説明
UDP 53	DNS サーバ	任意	ファブリックアンダーレイ	DNS サーバからファブリックスイッチの間で使用
UDP 53	DNS サーバ	任意	シスコワイヤレスコントローラ	DNS サーバーから シスコ ワイヤレス コントローラ

アプライアンスの設定中に入力する必要がある必須情報について説明します。

アプライアンスの設定時には、[必要な IP アドレスおよびサブネット](#)（44 ページ）に示されている項目に加えて、次の情報を入力する必要があります。

- **Linux ユーザー名** : これは **maglev** です。プライマリノードおよびセカンダリノードを含む、クラスター内のすべてのアプライアンスでこのユーザー名を使用します。ユーザー名は変更できません。
- **Linux パスワード** : Linux ユーザー名 **maglev** のパスワードを指定します。このパスワードは、Linux コマンドラインを使用して各アプライアンスへのセキュアなアクセスを保証します。必要に応じて、クラスター内の各アプライアンスで設定されている **maglev** ユーザーに異なる **Linux** パスワードを割り当てることができます。

設定するパスワードが [パスワード要件](#)（73 ページ）に準拠していることを確認してください。

Linux パスワードは暗号化され、Catalyst 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ーを展開している場合は、各セカンダリノードにプライマリノードの Linux パスワードを入力することも求められます。

- **パスワード生成シード（オプション）** : Linux パスワードを作成する代わりに、シードフレーズを入力し、**[Generate Password]** をクリックする方法もあります。**[Maglev Configuration]** ウィザードでは、このシードフレーズを使用してランダムで安全なパスワードが生成されます。**[Auto Generated Password]** フィールドを使用すると、生成されたパスワードをさらに編集できます。

- **管理者パズフレーズ**：クラスター内の **Catalyst Center** への Web アクセスに使用されるパスワードを指定します。これはスーパーユーザーアカウント **admin** のパスワードであり、初めて **Catalyst Center** にログインするときに使用します（[Catalyst Center への初回ログイン](#)（256ページ）を参照）。初めてログインすると、このパスワードを変更するよう求められます。

設定するパスワードが [パスワード要件](#)（73ページ）に準拠していることを確認してください。

- **CISCO IMC ユーザーパスワード**：Cisco IMC GUI へのアクセスに使用するパスワードを指定します。工場出荷時のデフォルトは「**password**」ですが、Web ブラウザを使用してアクセスするために **Cisco IMC** を初めて設定するとき、変更を求められます（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)（86ページ）」を参照）。

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

- **Primary Node IP Address**：クラスターにセカンダリノードをインストールする場合にのみ必要です。これは、プライマリノード上のクラスタポートの IP アドレスです（「[インターフェースケーブル接続](#)（40ページ）」を参照）。

Catalyst Center の初回セットアップ時に入力する必要がある情報について説明します。

アプライアンスを設定したら、**Catalyst Center** にログインして、必須の設定タスクを完了します。初回セットアップ時には、次の情報を入力します。

- **スーパーユーザー権限を持つ管理者の新しいパスワード（New admin superuser password）**：**Catalyst Center** 管理者の新しいスーパーユーザーパスワードを入力するように求められます。スーパーユーザー権限を持つ管理者のパスワードをリセットすると、運用上のセキュリティが向上します。これは、たとえば **Catalyst Center** アプライアンスを設置して設定した企業スタッフが **Catalyst Center** のユーザーまたは管理者ではない場合に特に重要です。
- **cisco.com ログイン情報（Cisco.com credentials）**：ソフトウェアのダウンロードを登録し、電子メールでシステム通信を受信するために組織が使用する **Cisco.com** ユーザー ID とパスワード。
- **シスコ スマートアカウントのクレデンシャル（Cisco Smart Account credentials）**：組織がデバイスとソフトウェアライセンスの管理に使用する **cisco.com** スマートアカウントのユーザー ID とパスワード。
- **IP アドレスマネージャの URL とクレデンシャル（IP address manager URL and credentials）**：**Catalyst 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）サーバーのホスト名、URL、管理者ユーザー名、管理者パスワード。このリリースでは **InfoBlox** と **Bluecat** がサポートされています。
- **プロキシURL、ポート、クレデンシャル（Proxy URL, Port and Credentials）**：**Catalyst Center** ソフトウェアのアップデートの取得、デバイスライセンスの管理などのダウンロード可能なコンテンツの取得のために **Catalyst Center** で使用するプロキシサーバーの URL（ホスト名または IP アドレス）、ポート番号、ユーザー名、ユーザーパスワード。
- **Catalyst Center ユーザー**：作成する新規 **Catalyst Center** ユーザーのユーザー名、パスワード、権限の設定。常に新しいユーザーアカウントのいずれかを通常の **Catalyst Center** 操作に使用してください。管理者スーパーユーザーアカウントは、**Catalyst Center** の再設定およびスーパーユーザー権限を必要とする操作にのみ使用してください。

重要

Catalyst Center ユーザーと管理者スーパーユーザーに設定するパスワードが [パスワード要件](#) (73ページ) に準拠していることを確認してください。

この情報を入力する初回セットアップウィザードを起動して対応する方法の詳細については、[初期設定の完了](#) (255ページ) を参照してください。

この情報を使用して、最初のログイン後に実行できる追加のセットアップタスクを完了します。

- **Catalyst Center サーバーの IP アドレスとクレデンシャル (server IP address and credentials) :** Cisco ISE サーバーの IP アドレスとログイン情報、管理ユーザー名、パスワードが必要です。これらは「[CISCO ISE と Catalyst Center の統合](#)」で説明されているように、組織の ISE サーバにログインして Catalyst Center とのデータ共有設定を行うために必要です。

Catalyst Center の最新リリースをインストールまたはアップグレードすると、Cisco ISE が認証およびポリシー (AAA) サーバーとして設定されているかどうかを確認します。正しいバージョンの Cisco ISE がすでに設定されている場合、Cisco ISE から Catalyst Center へのグループポリシーデータの移行を開始できます。

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

Catalyst Center 以前のバージョンに存在するデータは、アップグレード時に保持されます。データ移行操作では Catalyst Center と Cisco ISE のデータがマージされます。移行中に競合が発生した場合、システムは Cisco ISE のデータを使用します。

Catalyst Center が使用できなくなった場合、さらに Catalyst Center より前のポリシーを管理する必要がある場合、Cisco ISE には読み取り専用設定を上書きするオプションがあります。これで Cisco ISE のポリシーを直接変更できます。Catalyst Center が再び使用可能になったら、Cisco ISE の読み取り専用設定を無効にして、Catalyst Center の [グループベースのアクセスコントロール設定 (Group Based Access Control Settings)] ページを同期しなおす必要があります。

注意

このオプションは、必要な場合にのみ使用してください。Cisco ISE で直接行われた変更は Catalyst Center に転送されません。

- **承認およびポリシーサーバーの情報 :** 認証およびポリシーサーバーとして Cisco ISE を使用している場合は、前の項目でリストされているものと同じ情報に加えて、次の情報が必要です。
 - ISE CLI ユーザー名
 - CLI パスワード
 - サーバー FQDN
 - サブスクライバ名 (例 : cc)
 - ISE SSH キー (オプション)
 - プロトコルの選択 (RADIUS または TACACS)
 - 認証ポート
 - アカウンティングポート

- 再試行とタイムアウトの設定

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

この情報は、選択した認証サーバ、ポリシーサーバと **Catalyst Center** を統合するために必要です。詳細については、[認証サーバーとポリシーサーバーの設定](#)（276ページ）を参照してください。

- **SNMP の再試行とタイムアウト値（SNMP Retry and Timeout Values）**：これは「[SNMP プロパティの設定](#)（280ページ）」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。

Catalyst Center のパスワードポリシーについて説明します。

Catalyst Center をデプロイしたら、以下のパスワードポリシーの要件を確認します。

Catalyst Center

このセクションでは、新規のデプロイ用のパスワードポリシーについて説明します。

- **maglev** ユーザーおよび管理者スーパーユーザーのデフォルトパスワードは、**P@ssword9** です。
初めて **Catalyst Center GUI** にログインすると、管理者スーパーユーザーのパスワードを変更するように求められます。
- ユーザーのパスワードを変更するか、新しいユーザーを設定する場合は、そのユーザーのパスワードが新しい要件に準拠していることを確認します。

Catalyst Center

このセクションでは、システムアップグレード時のパスワードの動作について説明します。

- 以前のバージョンの **Catalyst Center** で設定されたロールベースアクセスコントロール（RBAC）ユーザーは、引き続き現在のパスワードを使用して **Catalyst Center 2.3.7.9** 以降にログインできます。
たとえば、アプライアンスをバージョン **2.3.7.6** から **2.3.7.11** にアップグレードしたとします。アプライアンスからデータをバックアップしました。その後、**Catalyst Center 2.3.7.11** がインストールされている別のアプライアンスにバックアップファイルを復元しました。既存の RBAC ユーザーは、現在のパスワードを使用してログインできます。
- ユーザーのパスワードを変更するか、新しい RBAC ユーザーを設定する場合は、そのユーザーのパスワードが新しい要件に準拠していることを確認します。

新しいパスワードが満たす必要がある基準については、「[パスワード要件](#)（73ページ）」を参照してください。

Catalyst Center のパスワード要件について説明します。

Catalyst Center 2.3.7.11 以降で設定したユーザーパスワードは、次の要件を満たしている必要があります。

- 9 文字以上である必要があること。
- 次のうち少なくとも 3 つのカテゴリの文字を含むこと。

- 大文字の A ～ Z
 - 小文字の a ～ z
 - 数字 (0 ～ 9)
 - 特殊文字 (例 : !, \$, # など)
- 英語の QWERTY キーボード上で連続する文字を 4 文字以上含まないこと。
たとえば、59Asdfpj! は、a、s、d、および f の文字が連続して含まれているため、有効なパスワードではありません。
 - 関連するユーザー名にある連続する文字を 2 文字以上含まないこと。
 - 任意の言語の完全な単語を含まないこと。
 - 個人情報に基づくフレーズを含まないこと。

注

24 個の異なるパスワードを使用した後にのみ、以前のパスワードを再利用できます。

第3

章

$$\vdots$$

- □□□□□□□□□□□□□□□□□□
□□
- □□□□□□□□□□□□□□□□
- □□□□□□□□□□□□□□□□□□
- □□□□□□□□□□
- □□□□□□□□□□□□□□□□□□
- LED □□□

Catalyst Center アプライアンスのインストールワークフローの概要。

Catalyst Center アプライアンスを物理的にインストールするには、インストールする各アプライアンスについて、この章で説明するタスクを完了します。プライマリノードを設定する前に、すべてのアプライアンスをインストールします。

これらのタスクがすべて完了したら、「[アプライアンス設定の準備の概要（86ページ）](#)」で説明されている手順に進みます。

Catalyst Center アプライアンスのパッケージを開梱する際の確認事項について説明します。

 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。

-
1. 段ボール箱からアプライアンスを取り出します。将来アプライアンスを出荷する必要がある場合に備えて、すべての梱包材を保存してください。
 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。すべての品目を受信していることを確認してください。
 3. 損傷を確認します。欠品または破損がある場合は、ただちにカスタマーサービス担当者に報告してください。次の情報を用意しておきます。
 - 梱包明細に記載されている発送元の請求書番号
 - 破損している装置のモデル番号とシリアル番号
 - 破損状態の説明
 - 破損による設置への影響
-

アプライアンスを設置する際に従う警告、注意、ガイドライン。

アプライアンスの設置時には、以下のガイドラインが適用されます。

- 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。推奨されるサイトの計画および準備タスクについては、『[Cisco UCS Site Preparation Guide](#)』を参照してください。
- アプライアンスの周囲に、保守作業とエアフローのための十分なスペースがあることを確認します。空気はアプライアンスの前面から入り、背面から出ます。
- 設置場所の空調が、[環境仕様（35ページ）](#)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](#)（79ページ）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、[電源装置の仕様](#)（36ページ）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。
- 次の注意と警告を慎重に確認します。

 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します。レールキットのないユニットをスタックすると、アプライアンスの上部の空気出口がブロックされます。これにより、オーバーヒート、ファン速度の上昇、および消費電力の増加につながります。設置の際にアプライアンスをレールキットに取り付けて、ユニット間に必要な最小間隔を確保します。レールキットを使用してユニットをマウントすると、間隔を余分にとる必要がありません。

 注意

鉄共振技術を採用している無停電電源装置（UPS）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。

1071 - **Warning**

安全上の重要な注意事項

装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。使用、設置、電源への接続を行う前にインストール手順を読んでください。各警告の冒頭に記載されているステートメント番号を基に、装置の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

**1005 -** **Warning**

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。感電または火災のリスクを軽減するため、保護対象の装置は次の定格を超えないようにします。

250 V、15 A。

1074 -

 Warning

感電または火災のリスクを軽減するため、機器は地域および国の電気規則に従って設置する必要があります。

1017 - **Warning**

この装置は、出入りが制限された場所に設置されることを想定しています。熟練者、教育を受けた担当者、または資格保持者のみが立ち入り制限区域に入ることができます。

ラック要件情報を提供します。

ラックが次の要件を満たしていることを確認します。

- 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) を使用します。
- シスコが用意しているスライドレールを使用します。ラックポストの穴のタイプは、方形 0.38 インチ (9.6 mm)、丸型 0.28 インチ (7.1 mm)、サイズ 12 ~ 24 UNC、サイズ 10 ~ 32 UNC です。
- 32 コアまたは 56 コアのアプライアンスサーバーごとに少なくとも 1 つのラックユニット (RU) または 1.75 インチ (44.45 mm) の垂直ラックスペースを確保します。
- 80 コアアプライアンスサーバーごとに少なくとも 2 つのラックユニット (RU) または 3.5 インチ (88.9 mm) の垂直ラックスペースを確保します。

サーバーは、次のレール キット オプションをサポートします。

- 部品 UCSC-RAIL-M6 は、ボール ベアリング スライド レール キットです。
- 部品 UCSC-CMA-C220M6 は、32 コアおよび 56 コアアプライアンスで使用されるボール ベアリング スライド レール キット用の可逆的ケーブル管理アームです。
- 部品 UCSC-CMA-C240M6 は、80 コアアプライアンスのボール ベアリング スライド レール キット用の可逆的ケーブル管理アームです。

シスコが販売するこのサーバー用のスライド レールの場合、設置に必要な工具はありません。

このサーバーのスライド レールの調整範囲は 24 ~ 36 インチ (610 ~ 914 mm) です。

オプションのケーブルマネジメントアームを使用する場合、長さの要件がさらに追加されます。

- 32 コアおよび 56 コアのアプライアンスの場合、サーバーの背面からケーブル管理アームの背面までの距離は 137.4 mm (5.4 インチ) です。80 コアアプライアンスの場合、この距離は 193 mm (7.6 インチ) です。
- 32 コアおよび 56 コアのアプライアンスの場合、ケーブル管理アームを含むサーバーの合計長は 894 mm (35.2 インチ) です。80 コア アプライアンスの場合、長さは 955 mm (37.6 インチ) です。

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

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

1. アプライアンスの各電源に、付属の電源コードを接続します。アース付き AC 電源コンセントに電源コードを接続します。詳細については、「[電源装置の仕様 \(36 ページ\)](#)」を参照してください。

注

アプライアンスに付属の電源のいずれかまたは両方を使用できます。最低 1 台の電源ユニットが必須です。さらに 1 台を追加して 1 + 1 の冗長性を確保できます。

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

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

- 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。

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、該当するアプライアンスの「前面パネルと背面パネル」のトピックを参照してください。

- [32 コアおよび 56 コアアプライアンス](#)
- [80 コアアプライアンス](#)

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

LED

Catalyst Center アプライアンスの LED が示す意味について説明するトピックへのリンクを提供します。

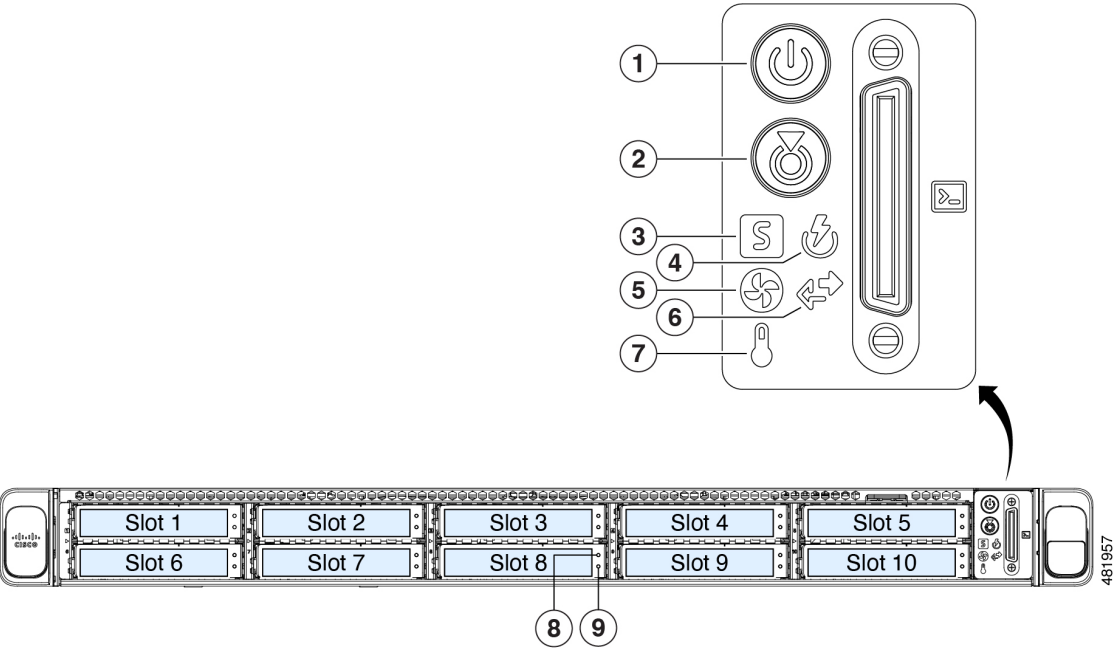
アプライアンスの電源を投入したら、前面パネルと背面パネルの **LED** の状態をチェックし、機能していることを確認します。適切なリンクをクリックすると、アプライアンスの **LED** の説明が表示されます。

32 56

32 コアまたは 56 コアの第 3 世代 Catalyst Center アプライアンスの **LED** が示す内容について説明します。

これらの図は、設置後電源投入後、アプライアンスを構成する前に、アプライアンスの **LED** の識別に役立ちます。

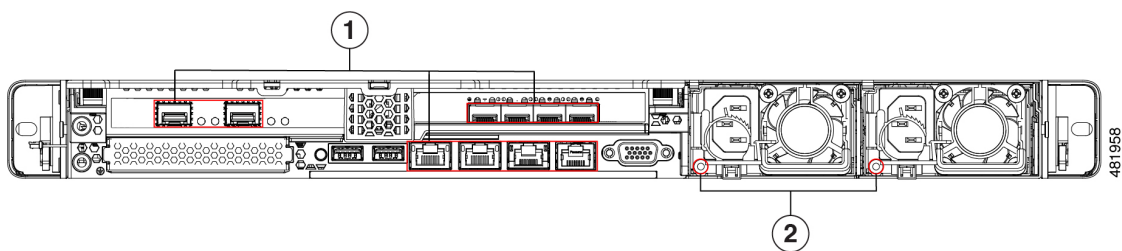
8 : 32 56 LED



この表は、前面パネル **LED** インジケータとその意味を示します。

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

9 : 32 56 LED



次の表に、背面パネル LED インジケータとその意味を示します。

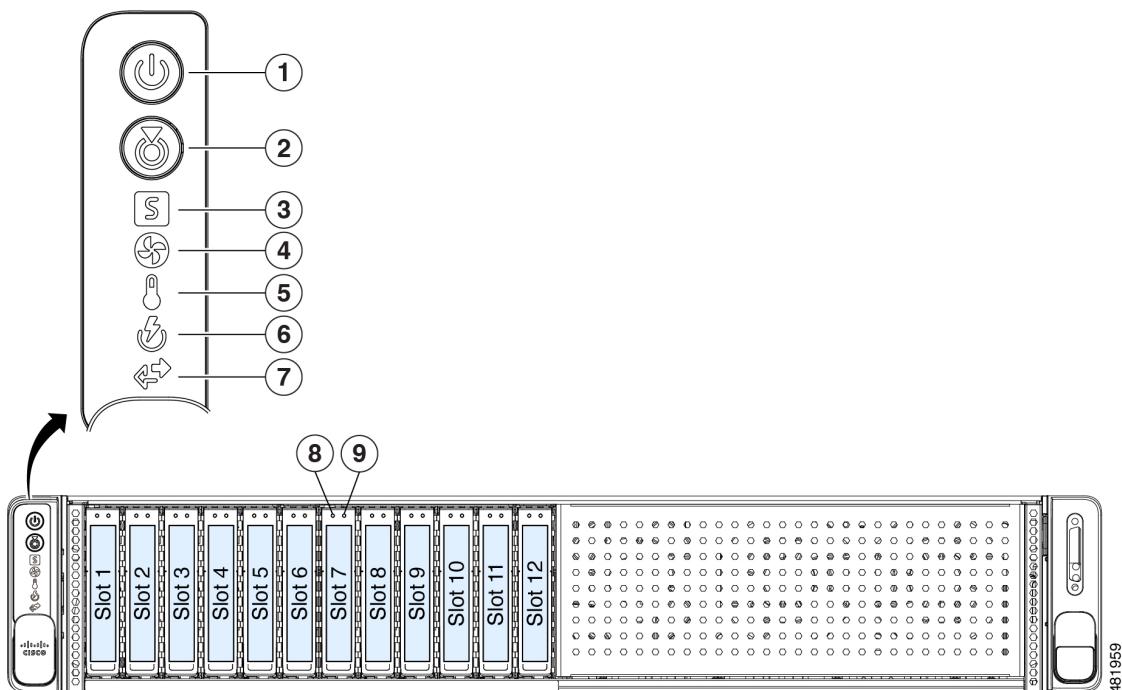
LED	ステータスインジケータ
1	最初の電源投入後、すべてのポートのリンクステータスとリンク速度 LED はオフになっているはずで す。 Mapping 設定ウィザードまたはブラウザベースの設定ウィザードを使用してネットワーク構成を設定し、テストした後は、すべての ケーブル接続 ポートのリンクステータスとリンク速度の LED が緑色になります。すべての [uncabled] ポートの LED はオフのままです。
2	AC 電源ステータス LED : 緑

80

80 コア第 3 世代 Catalyst Center アプライアンスの LED が示す内容について説明します。

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

10 : 80 LED

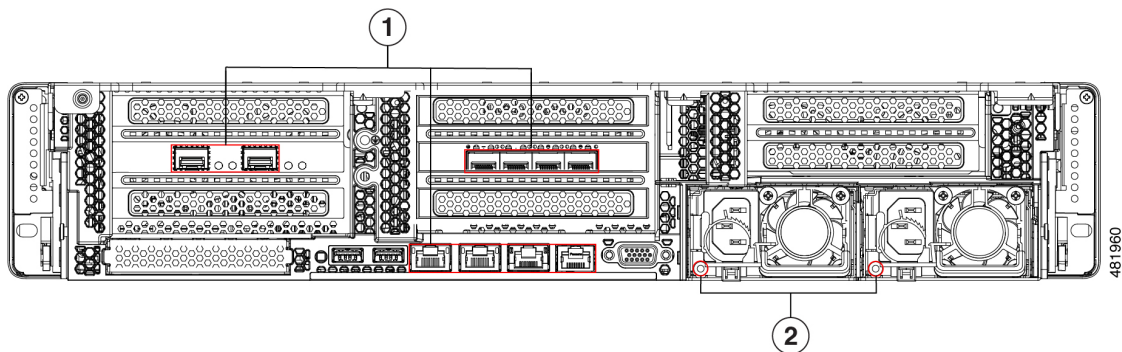


この表は、前面パネル LED インジケータとその意味を示します。

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

次の表に、背面パネル LED インジケータとその意味を示します。

11 : 80 LED



LED	ステータスインジケータ
1	最初の電源投入後、すべてのポートのリンクステータスとリンク速度 LED はオフになっているはずで す。 Mapping 設定ウィザードまたはブラウザベースの設定ウィザードを使用してネットワーク構成を設定し、テストした後は、すべての ケーブル接続 ポートのリンクステータスとリンク速度の LED が緑色になります。すべての [uncabled] ポートの LED はオフのままです。
2	AC 電源ステータス LED：緑

第4

章

- ：
- [Cisco Integrated Management Controller](#)
- [NIC](#)
- [Catalyst Center](#)

設定用の **Catalyst Center** アプライアンスの準備方法について説明します。これには、アプライアンスの設定に進む前に、**Cisco Integrated Management Controller (IMC)** へのブラウザアクセスを有効にする方法、事前設定タスクを実行する方法、必要に応じて **Catalyst Center** ソフトウェアを再インストールする方法が含まれます。

アプライアンス設定プロセスの概要を表示します。

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

1. アプライアンスの **Cisco IMC** へのブラウザアクセスを有効にします（「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化（86ページ）](#)」を参照）。
2. **Cisco IMC 事前設定タスクの実行（91ページ）** を使用して、ハードウェアとスイッチの重要な設定を確認、調整します。
3. 特定の状況において、事前インストール済みの **Catalyst Center** ソフトウェアを再インストールします。たとえば、現在のクラスターリンク設定を変更する前に再インストールします。ソフトウェアを再インストールする必要がある場合は、[アプライアンスのイメージの再作成（96ページ）](#) のタスクを完了してください。

注

アプライアンスのイメージを作成しなおす必要がない場合は、使用する設定ウィザードに固有の「アプライアンスの設定の概要」のトピックに進みます。

- **Maglev 設定ウィザード**
- **ブラウザベースの構成ウィザード（32 コアおよび 56 コアアプライアンス）**
- **ブラウザベースの構成ウィザード（80 コアアプライアンス）**

Cisco Integrated Management Controller

Cisco IMC 設定ユーティリティを使用して **Catalyst Center** アプライアンスの **Cisco IMC** ポートを設定する方法について説明します。

「[アプライアンスのインストール ワークフロー（76ページ）](#)」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 **CIMC** ポートに **IP** アドレスとゲートウェイを割り当てます。**Cisco IMC GUI** にアクセスして、アプライアンスを設定できます。

Cisco IMC の設定が完了したら、**Cisco IMC** にログインし、「[事前設定タスクの実行（91ページ）](#)」に記載されているタスクを実行して、設定が正しいことを確認します。

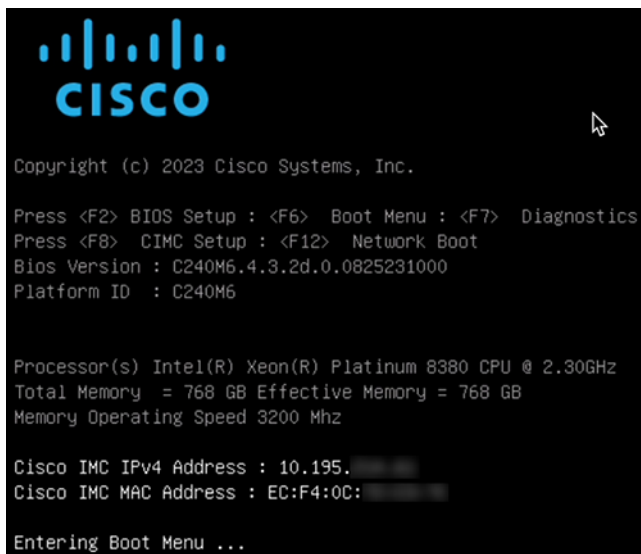
注

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

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

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。
 - KVM ケーブルをアプライアンスの前面パネルの KVM コネクタに接続します。
 - キーボードとモニターをアプライアンスの背面パネルにある USB および VGA ポートに接続します。
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。
3. 前面パネルの電源ボタンを押して、アプライアンスをブートします。

Cisco IMC 設定ユーティリティのブート画面が開きます。



4. [F8] を押して、Cisco IMC の設定を実行します。
次に示すように、Cisco IMC 設定ユーティリティに [CIMC User Details] 画面が表示されます。

CIMC User Details (Press Enter to Save / Continue)	
Enter current CIMC password	[]
Enter new CIMC password	[]
Re-Enter new CIMC password	[]

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

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

```

Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc.
*****
NIC Properties
NIC mode                                NIC redundancy
Dedicated:      [X]                    None:          [X]
Shared LOM:     [ ]                    Active-standby: [ ]
Cisco Card:     [ ]                    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

```

7. 次のアクションを実行します。
 - **NIC モード (NIC mode)** : **[Dedicated]** を選択します。
 - **IP (基本)** : **[IPV4]** を選択します。
 - **CIMC IP** : CIMC ポートの IP アドレスを入力します。
 - **プレフィックス/サブネット (Prefix/Subnet)** : CIMC ポート IP アドレスのサブネットマスクを入力します。
 - **ゲートウェイ (Gateway)** : 優先するデフォルトゲートウェイの IP アドレスを入力します。
 - **優先DNSサーバ (Pref DNS Server)** : 優先 DNS サーバの IP アドレスを入力します。
 - **NIC 冗長性 (NIC Redundancy)** : **[なし (None)]** を選択します。
8. **F1** を押して **[Additional Settings]** を指定します。

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

```

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

```

9. 次のアクションを実行します。

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

10. F10 を押して、設定を保存します。

11. Esc キーを押して終了し、アプライアンスをリブートします。

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、アプライアンスサブネットにアクセスできるクライアントマシンでブラウザを開き、次の URL を入力します。

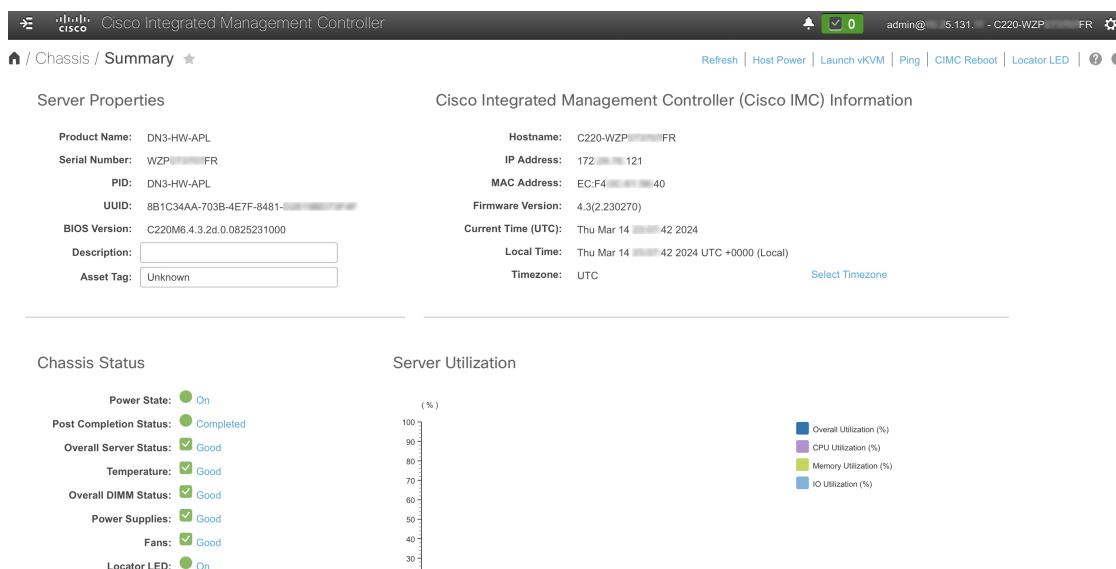
https://CIMC_ip_address (この **CIMC_ip_address** は先ほどステップ 7 で入力した Cisco IMC ポート IP アドレスです。

ブラウザに次のような Cisco IMC GUI のメインログインウィンドウが表示されます。



- 13 ステップ 5 で設定した Cisco IMC ユーザのユーザ ID とパスワードを使用してログインします。

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



- 14 このバージョンの Cisco IMC が、インストールする Catalyst Center リリースでサポートされていることを確認します。

- [Firmware Version] フィールドにリストされているバージョンを確認します。
- インストールする Catalyst Center リリースの [リリースノート](#) を参照してください。「Supported Firmware」セクションには、ご使用の Catalyst Center リリースでサポートされている Cisco IMC のバージョンが示されています。
- 次のいずれか 1 つのタスクを実行します。
 - 適切な Cisco IMC バージョンがインストールされている場合は、ここで終了できます。
 - Cisco IMC のバージョンを更新する必要がある場合は、『[Cisco Host Upgrade Utility User Guide](#)』を参照してください。

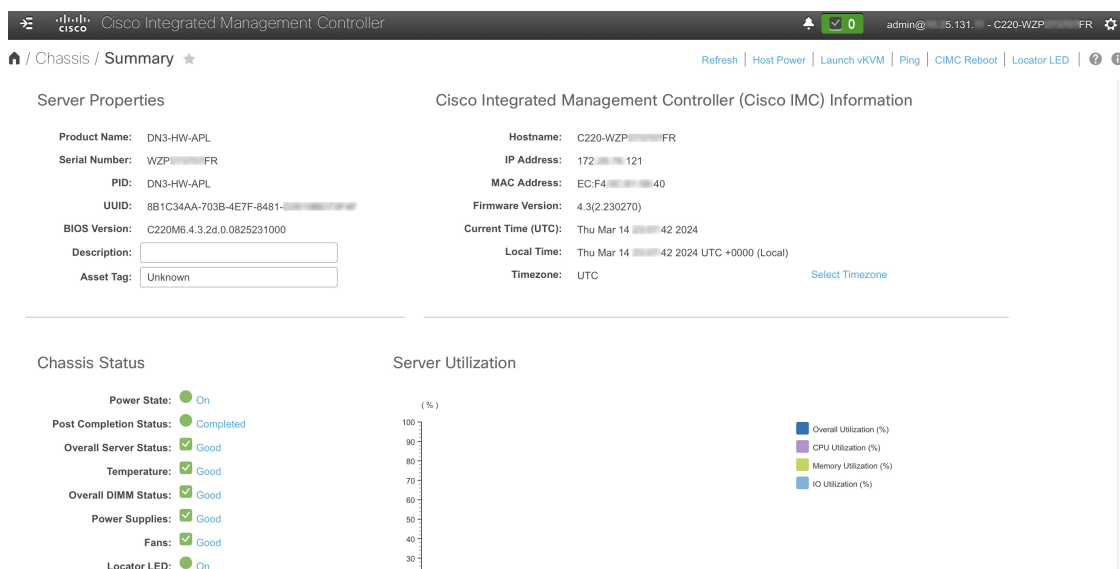
Catalyst Center アプライアンスの適切な設定と展開を確実にするために完了しなければならないタスクについて説明します。

最初に、アプライアンスをインストールし、**Cisco IMC GUI** へのアクセスを設定します。[アプライアンスのインストールワークフロー](#) (76ページ) および[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#) (86ページ) を参照してください。その後、**Cisco IMC** を使用して事前設定タスクを完了し、正しい設定と展開を確保します。

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)** サーバーと同期します。[必要な IP アドレスおよびサブネット](#) (44ページ) 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** サーバーを使用します。この同期は、**Catalyst Center** データをネットワーク全体で適切に同期しておくために重要です。
2. **10 Gbps** アプライアンスポートに接続されているスイッチを再設定して、高スループット設定がサポートされるようにします。

1. 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#) (86ページ)」で設定した **Cisco IMC IP** アドレス、ユーザー ID、パスワードを使用して、アプライアンスの **Cisco IMC** にログインします。

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



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

🏠 / ... / Networking / NTP Setting ★

Network	Network Security	NTP Setting
---------	------------------	-------------

NTP Properties

NTP Enabled: ☒

Server 1:

Server 2:

Server 3:

Server 4:

Status: NTP service disabled ?

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

📄 注

- 第 3 世代 Catalyst Center アプライアンスでは、仮想インターフェイスカード (VIC) が使用されません。第 3 世代アプライアンスに標準搭載のネットワーク インターフェイス カード (NIC) では、高スループットがすでにデフォルトで有効になっているため、Cisco IMC で NIC を設定する必要はありません。
- Cisco IMC で NTP 認証を使用することはできません。

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

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

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

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

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

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

```
N7K2(config-if)# no lldp transmit
N7K2(config-if)# no lldp receive
```

注

- これらのコマンドは単なる例です。
- 正常に機能させるには、第 3 世代 Catalyst Center アプライアンスのスイッチポートをアクセスモードに設定する必要があります。トランクモードはサポートされていません。

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

```
MySwitch#show interface tengigabitethernet 1/1/3
TenGigabitEthernet1/1/3 is up, line protocol is up (connected)
  Hardware is Ten Gigabit Ethernet, address is XXXe.310.8000 (bia
  XXX.310.8000)
  MTU 1500 bytes, BW 100000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 10GB/s, link type is auto, media type is SFP-10Gbase-SR
```

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

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

MySwitch#
```

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

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

MySwitch#
```

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

Cisco Integrated Management Controller

Home / Compute / BIOS ★

BIOS | Remote Management | Troubleshooting | Power Policies | PID Catalog

[Enter BIOS Setup](#) | [Clear BIOS CMOS](#) | [Restore Manufacturing Custom Settings](#) | [Restore Defaults](#)

Configure BIOS | **Configure Boot Order** | Configure BIOS Profile

BIOS Properties

Running Version C220M6.4.3.2d.0.0825231000

UEFI Secure Boot ☐

Actual Boot Mode Legacy

Configured Boot Mode Legacy ▼

Last Configured Boot Order Source CIMC

Configured One time boot device ▼

Save Changes

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

- Cisco IMC GUI の左上隅から、[Toggle Navigation] アイコン (☰) をクリックします。
- Cisco IMC メニューから、[**Compute**] > [**BIOS**] > [**Configure Boot Order**] を選択します。

⚠ 注意

[**Legacy**] ブートモード設定を維持します。[**UEFI**] ブートモード設定が原因で、Catalyst Center アプライアンスインターフェイスが ping に応答しない場合があります。

このタスクを完了した後、次のいずれかのタスクを実行します。

- アプライアンスを設定する前に **Catalyst Center** ソフトウェアを再インストールする必要がある場合は、「[アプライアンスのイメージの再作成 \(96ページ\)](#)」を参照してください。
- アプライアンスを設定する準備ができている場合は、使用する設定ウィザードに一致する「アプライアンス設定の概要」のトピックに進みます。
 - [Maglev 設定ウィザード](#)
 - [ブラウザベースの構成ウィザード \(32 コアおよび 56 コアアプライアンス\)](#)
 - [ブラウザベースの構成ウィザード \(80 コアアプライアンス\)](#)

NIC

ネットワーク インターフェイス コントローラのボンディング機能の概要を示します。

任意の **Catalyst Center** アプライアンスで、エンタープライズインターフェイス、クラスター内インターフェイス、管理インターフェイス、およびインターネットインターフェイスを設定できます。アプライアンスでネットワーク インターフェイス コントローラ (NIC) のボンディングを有効にすると、各インターフェイスには **2** つのインスタンスがあります。プライマリインスタンス (アプライアンスのマザーボードまたは **Intel E810-XXVDA2** ネットワークアダプタのいずれかにある) が **1** 台のスイッチに接続されています。セカンダリインスタンス (アプライアンスの **Intel E810-XXVDA4** ネットワークアダプタにある) が別のスイッチに接続されています。**NIC** ボンディングを使用すると、各インターフェイスの **2** つのインスタンスが単一の論理インターフェイスに統合されます。単一の **MAC** アドレスを持つ単一のデバイスとして表示されます。この機能を有効にすると、アプライアンスのインターフェイスの設定時に選択したボンディングモードに応じて、利点を得られます。利点を次に示します。

注

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

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

注

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

- **LACP モード**：このモードを選択すると、**Catalyst Center** によりグループ化された **2** つのインターフェイスで同じ速度とデュプレックス設定が共有されます。このモードでは、インターフェイスにロードバランシングとより高い帯域幅が提供されます。このモードを有効にするには、最初に次の点を確認する必要があります。
 - **Linux** ユーティリティ **ethtool** は、各インターフェイスの速度とデュプレックスモードを取得するために使用されるベースドライバをサポートしている必要があります。
 - エンタープライズポートに接続されているスイッチは、ダイナミック インターフェイス集約をサポートしている必要があります。
 - スイッチ上で **LACP** を有効にした後、次のことを確認します。
 - **LACP** モードは **[active]** に設定されています。この設定により、アプライアンスに接続されているスイッチポートをアクティブネゴシエーションステートにします。これによりポートは **LACP** パケットを送信し、リモートポートとのネゴシエーションを開始します。
 - **LACP** レートが **[fast]** に設定されています。この設定により、**LACP** サポート対象インターフェイスに **LACP** 制御パケットが送信されるレートが、デフォルトの **30** 秒から **1** 秒に変更されます。

 注

- LACP モードは、アプライアンスのエンタープライズおよびクラスター内インターフェイスでのみ有効にできます。管理およびインターネット アクセス インターフェイスは、アクティブ/バックアップモードのみをサポートします。
- アプライアンスの初期設定時に、アプライアンスのインタークラスターインターフェイスでのみ LACP モードを有効にできます。

実稼働環境で NIC ボンディングを使用する前に、以下の作業を実施してください。

- アプライアンスでこの機能がサポートされていることを確認します。「[アプライアンスサポート](#) (96 ページ)」を参照してください。
- アプライアンスの背面パネルにあるセカンダリポートの位置を確認します。「[前面パネルと背面パネル](#) (14 ページ)」を参照してください。
- 推奨されるアプライアンス (スイッチのケーブル接続) を確認します。[インターフェイスケーブル接続](#) (40 ページ) を参照してください。

NIC ボンディングをサポートする第 3 世代 Catalyst Center アプライアンスを示します。

すべての第 3 世代 Catalyst Center アプライアンスは NIC ボンディングをサポートします。

- 32 コアアプライアンス : シスコ部品番号 DN3-HW-APL
- 56 コアアプライアンス : シスコ部品番号 DN3-HW-APL-L
- 80 コアアプライアンス : シスコ部品番号 DN3-HW-APL-XL

Catalyst Center アプライアンスのイメージを再作成するために完了すべき手順について説明します。

バックアップからの回復やクラスターリンク設定の変更など、Catalyst Center アプライアンスを再イメージ化する必要がある場合があります。アプライアンスを再イメージ化するには、次の手順を実行します。

-
1. Catalyst Center ISO イメージをダウンロードします。それが正規の Cisco イメージであることを確認します。
「[Catalyst Center イメージの確認](#) (97 ページ)」を参照してください。
 2. Catalyst Center ISO イメージを含むブート可能 USB ドライブを作成します。
「[ブート可能な USB フラッシュドライブの作成](#) (98 ページ)」を参照してください。
 3. アプライアンスの RAID コントローラ : [Catalyst Center アプライアンスの仮想ドライブの再初期化](#) (101 ページ) によって管理されている仮想ドライブを再初期化します。
 4. アプライアンスに Catalyst Center を再インストールします。

[Catalyst Center ISO イメージのインストール](#)（102ページ）を参照してください。

Catalyst Center

ダウンロードした **Catalyst Center** イメージが正規のシスコイメージであることを確認する方法について説明します。

Catalyst Center を展開する前に、ダウンロードしたイメージが正規の **Cisco** イメージであることを確認するよう強くお勧めします。

Catalyst Center イメージの場所を把握します（電子メールを使用するか、シスコサポートチームと連絡を取ります）。

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

オペレーティングシステムに応じて、次のコマンドのいずれかを実行します。

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

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

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

次に例を示します。

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

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

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

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

6. 署名を確認し、イメージが正規のものでシスコ製であることを確認します。


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

注

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

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

7. **Cisco** イメージをダウンロードしたことを確認してから、**Catalyst Center** イメージを含むブート可能 **USB** ドライブを作成します。[ブート可能な USB フラッシュドライブの作成 \(98ページ\)](#) を参照してください。

USB

Catalyst Center ISO イメージのインストール用に起動可能な **USB** フラッシュドライブを作成する方法を説明するセクションの紹介。

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

始める前に

- **Catalyst Center ISO** イメージのコピーをダウンロードして確認します。[Catalyst Center イメージの確認 \(97ページ\)](#) 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が次の要件を満たしていることを確認します。
 - **USB 3.0** 以降
 - **64 GB** 最小
 - 非暗号化

注

Etcher、**Linux CLI**、または **Mac CLI** のみを使用して **Catalyst Center ISO** イメージを書き込みます。

USB ドライブは、再イメージ化やリカバリなどの一時的なメンテナンス作業にのみ使用してください。タスクが完了したら、すぐに **USB** ドライブを取り外します。**USB** ドライブを常時接続したままにしないでください。

Etcher

Etcher ユーティリティを使用してブート可能な **USB** ドライブを作成する方法について説明します。

1. 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。無料のオープンソースユーティリティを使用して、ラップトップまたはデスクトップにブート可能な USB ドライブを作成できます。

Linux、macOS、または Windows 用の Etcher は、<https://www.balena.io/etcher/> でダウンロードできます。

注

互換性の問題を回避するため、Windows 10 以降でのみ Etcher を使用してください。

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。
3. ウィンドウの右上隅にある  をクリックし、Etcher が次のように設定されていることを確認します。
 - 成功時に自動マウント解除する
 - 成功時に書き込みを検証する
4. [Back] をクリックして、メインウィンドウに戻ります。
5. [Select Image] をクリックします。
6. 以前にダウンロードした Catalyst Center ISO イメージに移動します。それを選択し、[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。

- a. [Select drive] をクリックします。
 - b. 正しい USB ドライブのオプションボタンをクリックしてから、[Continue] をクリックします。
7. [Flash!] をクリックして、ISO イメージを USB ドライブにコピーします。

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

Linux CLI

Linux CLI を使用してブート可能な USB ドライブを作成する方法について説明します。

1. 次のとおり、ご使用のマシンで USB フラッシュドライブが認識されていることを確認します。
 - a) フラッシュドライブをマシンの USB ポートに挿入します。
 - b) Linux シェルを開き、次のコマンドを実行します。 **lsblk**

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

```
$ lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
```

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

c) sdd パーティションが表示されていることを確認します。このパーティションは、USB フラッシュドライブの存在を示します。

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

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

Mac CLI

Mac CLI を使用してブート可能な USB ドライブを作成する方法について説明します。

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

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

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

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

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

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

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

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

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

 注

ISO イメージを Box パーティションに配置しないでください。

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

この例を続け、次のコマンドを実行します。 `sudo dd if=CC-1.330.dmg of=/dev/disk2 bs=1m status=progress`
ISO イメージのサイズは約 18 GB であるため、完了までに時間がかかることがあります。

Catalyst Center

Catalyst Center アプライアンスの仮想ドライブを再初期化する方法について説明します。

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

1. 「[Cisco Integrated Management Controller に対するブラウザーアクセスの有効化 \(86ページ\)](#)」で設定した Cisco IMC IP アドレス、ユーザー ID、パスワードを使用して、アプライアンスの Cisco IMC にログインします。
2. Cisco IMC GUI の左上隅から、**[Toggle Navigation]** アイコン (☰) をクリックします。
3. Cisco IMC メニューから、**[Storage] > [Cisco 12G Modular Raid Controller]** を選択します。
4. **[Virtual Drive Info]** タブをクリックします。
5. リストされている最初の仮想ドライブ (ドライブ番号 237) のチェックボックスをオンにします。 **[初期化 (Initialize)]** をクリックします。
6. **[Initialize Type]** ドロップダウンリストから **[Full Initialize]** を選択します。
7. **[Initialize VD]** をクリックします。
8. アプライアンスの残りの仮想ドライブにそれぞれステップ 5 ~ 7 を繰り返しますが、**[Fast Initialize]** を選択します。

完全な初期化が必要なのは最初の仮想ドライブのみです。

9. ドライブで実行しているタスクのステータスを表示するには、**[Operations]** エリアで **[Refresh]** をクリックします。

次の詳細が表示されます。

フィールド	説明
動作	ドライブで実行中の操作の名前。
[Progress in %]	操作の進行状況 (完了した割合)。
[Elapsed Time in secs]	操作開始から経過した時間 (秒数)。

Catalyst Center ISO

ブート可能な USB ドライブからアプライアンスに Catalyst Center ISO イメージをインストールする方法について説明します。

アプライアンスに Catalyst 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。

Catalyst Center ISO イメージのインストール元となるブート可能 USB ドライブを作成します。[ブート可能な USB フラッシュドライブの作成](#) (98ページ) を参照してください。

1. Catalyst 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。
2. Cisco IMC にログインし、KVM セッションを開始します。
3. アプライアンスの電源を投入または再投入します。
 - アプライアンスが実行されていない場合には、**[Power] > [Power On System]** を選択します。
 - アプライアンスがすでに実行されている場合には、**[Power] > [Power Cycle System (cold boot)]** を選択します。
4. 表示されたウィンドウで **[Yes]** をクリックして、サーバー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。
5. シスコのロゴが表示されたら、**F6** キーを押すか、**[KVM]** メニューから **[Macros] > [User Defined Macros] > [F6]** を選択します。
ブートデバイス選択メニューが表示されます。
6. USB ドライブを選択してから、**Enter** を押します。

注

ドライブを取り外し可能ディスクとしてマウントします。

7. **[GNU GRUB]** ブートローダーウィンドウで、**Catalyst Center** インストーラー を選択し、**[Enter]** を押します。

注

30 秒以内に選択しなかった場合、ブートローダーが自動的に Catalyst Center インストーラを起動します。

インストーラが再起動し、ウィザードのウェルカム画面が表示されます。プライマリクラスターノードとセカンダリクラスターノードのどちらを設定するかに応じて、適切な手順を使用してステップ 4 に進みます。

- [Maglev ウィザードを使用したプライマリノードの設定](#) (107ページ)

- [Maglev ウィザードを使用したセカンダリノードの設定](#) (131ページ)
-

Catalyst Center

Catalyst Center アプライアンスの再イメージ化後に完了する必要がある手順についてのアドバイスを提供します。

Catalyst Center ISO イメージのインストールが完了すると、インストーラがリブートし、**Maglev** 設定ウィザードの初期画面が開きます。アプライアンスの再イメージ化を完了するには、[Maglev ウィザードを使用したアプライアンスの設定](#) (105ページ) の手順を実行します。

第

5 Maglev

章

⋮

- □□□□□□□□□□□□□□
- **IPv4** □□□ **IPv6** □□□□□□
- □□□□□□□□□□
- **VLAN** □□□□□□□□
- **Maglev** □□□□□□□□□□□□□□□□
□□□□□□
- **Maglev** □□□□□□□□□□□□□□□□
□□□□□□
- □□□ **Catalyst Center** □□□□□□□□
□□□□□□

展開モードに応じたアプライアンスの設定手順に関する情報。

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

- **スタンドアロン**：すべての機能を提供する単一のノードとして。このオプションは通常、初期展開、テスト展開、小規模なネットワーク環境での使用に適しています。初期展開でスタンドアロンモードを選択した場合は、後でクラスター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、クラスター内の最初のノード、つまりプライマリノードとして設定されていることを確認してください。
- **クラスタ**：3 ノードクラスタに属するノードとして。このモードでは、すべてのサービスとデータがホスト間で共有されます。これは、大規模な展開で推奨されるオプションです。初期展開でクラスタモードを選択した場合は、セカンダリノードの設定に進む前に、プライマリノードの設定を完了してください。

続行するには、次のタスクを完了します。

1. クラスタのプライマリノードを設定します。 [Maglev ウィザードを使用したプライマリノードの設定](#)（107 ページ）を参照してください。
2. 3 つのアプライアンスを設置し、クラスタに 2 番目と 3 番目のノードを追加する場合、「[Maglev ウィザードを使用したセカンダリノードの設定](#)（131 ページ）」を参照してください。

IPv4 IPv6

IPv4 および IPv6 アドレッシングに関する注意事項を示します。

Catalyst Center および IPv4/IPv6 アドレッシングに関する次の点を理解してください。

- Catalyst Center は、デュアルスタック アドレッシング（IPv4 と IPv6 の両方のアドレッシングを同時に使用）をサポートしていません。
- あるアドレス方式から別のアドレス方式に切り替えるには、[アプライアンスのイメージの再作成](#)（96 ページ）を実行する必要があります。
- IPv4 を使用するアプライアンスから IPv6 を使用するアプライアンスにバックアップファイルを復元することはできません。その逆も同様です。
- アプライアンスが IPv6 アドレッシングを使用している場合、サポートされていない機能の説明は、『[Release Notes for Cisco Catalyst Center](#)』の「IPv6 Limitations」のセクションを参照してください。

Catalyst Center のパスワードポリシーと要件へのポインタを提供します。

これらのトピックを参照して、Catalyst Center のパスワード実装の説明を確認してください。

- [パスワードポリシー](#)（73 ページ）
- [パスワード要件](#)（73 ページ）

VLAN

Catalyst Centerで VLAN モードが有効になっている場合、ディザスタリカバリを使用できません。

VLAN モードについては次の詳細を考慮してください。

- VLAN モードの説明については、「」 [「Maglev ウィザードを使用したプライマリノードの設定（107ページ）」](#) を参照してください。
- VLAN モード：
 - Maglev 設定ウィザードを使用して Catalyst Center アプライアンスを設定する場合にのみ有効にできます。
 - ブラウザベースの構成ウィザードを使用して有効にすることはできません。
 - アプライアンスを再イメージ化せずに無効にすることはできません。
- ディザスタリカバリは、VLAN モードが有効になっている Catalyst Center 展開ではサポートされません。

Maglev

Maglev 構成ウィザードを使用して、クラスタ内の最初のアプライアンスを設定できます。

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

すでにプライマリノードがある既存のクラスタのセカンダリノードとしてインストールされたアプライアンスを設定する場合には、代わりに [Maglev ウィザードを使用したセカンダリノードの設定（131ページ）](#) に記載されている手順を実行します。

重要

- この手順の実行中に入力するすべての IP アドレスが有効なネットマスクを持つ有効なアドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。
- 3 ノードクラスターでアプライアンスを設定する前に、それらのアプライアンスからログアウトします。ログインしたままにしている場合、クラスターのアプライアンスを設定し、Catalyst Center に最初にログインした後に、ネットワークデバイスを検出してテレメトリを有効にするために使用するクイックスタートワークフローが開始されません。

次の前提条件を満たしていることを確認してください。

- 「[必要な IP アドレスおよびサブネット（44ページ）](#)」および「[必須の設定情報（70ページ）](#)」で指定されているすべての情報を収集したこと。
- 「[アプライアンスのインストール ワークフロー（76ページ）](#)」の説明に従って、1 番目のアプライアンスを設置したこと。
- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化（86ページ）](#)」の説明に従って、プライマリノードで Cisco IMC に対するブラウザのアクセス権が設定されたこと。

- **事前設定タスクの実行** (91ページ) の説明に従って、プライマリ ノードアプライアンスのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- 互換性のあるブラウザを使用していることを確認済みであること。互換性のあるブラウザの一覧については、インストールしている **Catalyst Center** のリリースに対応する **リリースノート** ドキュメントを参照してください。
- 次の手順で指定するデフォルトゲートウェイおよび **DNS** サーバーと **Catalyst Center** の間のファイアウォールで **ICMP** が許可されていること。Maglev 設定ウィザードでは **ping** を使用して、ユーザが指定したゲートウェイおよび **DNS** サーバを確認します。

 注意

ICMP が有効になっておらず、ファイアウォールが設置されている場合、**ping** がブロックされる可能性があります。これにより、ウィザードを完了できなくなります。

1. お使いのブラウザで、実行した **Cisco IMC GUI** 設定で設定した **Cisco IMC** の IP アドレスをポイントし、**Cisco IMC** ユーザーとして **Cisco IMC GUI** にログインします (**Cisco Integrated Management Controller に対するブラウザアクセスの有効化** (86ページ) を参照)。
ログインが成功すると、アプライアンスに **Cisco Integrated Management Controller Chassis Summary** ウィンドウが、上部のハイパーリンクメニューとともに表示されます。
2. ハイパーリンクメニューで **[Launch KVM]** を選択してから **[HTML-based KVM]** を選択します。
KVM コンソールが別ウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、Maglev 構成ウィザードのプロンプトに応答します。
3. KVM が表示されたら、次のいずれかを選択してアプライアンスをリブートします。
 - メインの **Cisco IMC GUI** ブラウザウィンドウで、**[Host Power] > [Power Cycle]** を選択し、KVM コンソールに切り替えて続行します。
 - KVM コンソールで、**[Power] > [Power Cycle System (cold boot)]** を選択します。

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

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

The screenshot displays the 'Static IP Configuration' screen of the Maglev Configuration Wizard. The interface is split into two main sections: a blue left pane and a dark gray right pane. The blue pane contains the following text:

STEP #None

Welcome to the Maglev Configuration Wizard!

Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration.

- Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface
- Click Skip to move to config wizard

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

The dark gray right pane contains the following text:

STATIC IP CONFIGURATION

IPv6 mode

IP Address:

Netmask:

Default Gateway Address:

Static Routes:

Web installation:
https://10.10.10.10:9004/

At the bottom of the screen, there are three buttons: '< cancel >', 'skip >>', and 'configure >>'.

4. [Skip] をクリックします。

KVM コンソールに **Maglev** 構成ウィザードのウェルカム画面が表示されます。

```

Welcome to the Maglev Configuration Wizard!

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

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

< exit >

```

 注

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

5. プライマリノードの設定を開始するには、**[Start a Catalyst Center Cluster]** を選択します。
画面が更新されます。

```

Welcome to Maglev Configuration Wizard!

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

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

< back >                                < exit >

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

```

6. 次のオプションのいずれか 1 つを選択します。
- **[Start using DNAC pre manufactured cluster]** : デフォルトの設定でアプライアンスを設定するには、このオプションを選択します。
 - クラスタ内インターフェイスの IP アドレス : 169.254.6.66
 - クラスタ内インターフェイスのサブネットマスク : 255.255.255.128
 - コンテナサブネット : 169.254.32.0/20
 - クラスタサブネット : 169.254.48.0/20
 - IPv4 アドレス指定
 - 管理スーパーユーザーのパスワード : P@ssword9

これらの設定は変更できないため、使用する場合にのみこのオプションを選択してください。

重要

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

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

画面が更新されます。

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

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

アプライアンスで **FIPS** モードを有効にする際の注意事項については、[FIPS モードのサポート](#) (130 ページ) を参照してください。

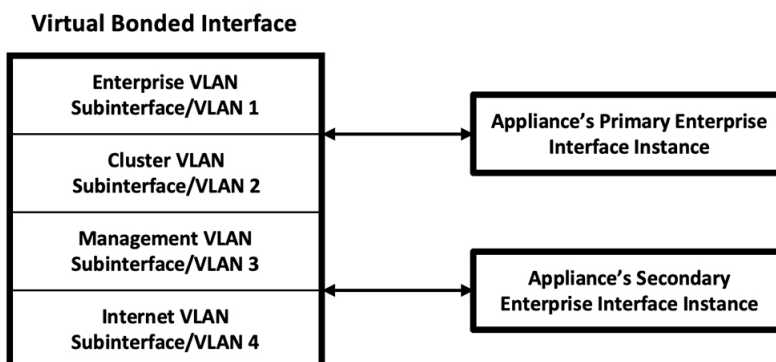
重要

次のウィザード画面では、**[VLAN mode]** 機能を有効にできます。このモードが有効になると、アプライアンスのエントリープライズインターフェイスのプライマリインスタンスとセカンダリインスタンスの両方を使用してネットワークに接続する、単一の結合インターフェイスが作成されます。この機能は通常使用されません。**Catalyst Center** 展開で必要な場合にのみ有効にしてください。

- この場合は、次の手順を実行します。
- それ以外の場合は、次のウィザード画面で何も選択せずに **[next>>]** をクリックします。このガイドで前述した **NIC** ボンディング機能は、ウィザードの **[Enterprise]** および **[Intracluster]** インターフェイス構成画面で有効にできます。

8. (オプション) 画面の指示に従って、アプライアンスのレイヤ 2 ポートチャネルモード (VLAN タグ付き) を有効にします。選択したら、**[next>>]** をクリックして続行します。

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



- b) 代わりにこのインターフェイスを **[LACP]** モード (ロードバランシングとより高い帯域幅を有効にする) で動作させる場合は、**LACP** オプションも選択する必要があります。

- c) アプライアンスのエンタープライズおよびクラスタインターフェイスの設定を入力するときは、仮想結合インターフェイスで設定するサブインターフェイスの **[VLAN ID of Interface]** フィールドに一意の **VLAN ID** を入力してください。

重要

1つの物理アプライアンスインターフェイス（エンタープライズインターフェイス）が接続されている場合でも、仮想結合インターフェイスに存在するすべてのサブインターフェイスを設定できます。

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

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

設定の過程でウィザードがエンタープライズポートとクラスタポートのいずれかまたは両方を表示できない場合は、これらのポートが機能していないか、または無効になっている可能性があります。Catalyst Center 機能にはこの2つのポートが必要です。機能していないことが判明した場合には、**[cancel]** を選択し、すぐに設定を終了します。設定を再開したり、Cisco Technical Assistance Center に連絡したりする前に、「[事前設定タスクの実行](#) (91ページ)」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。

9. ウィザードにより、最初に 10 Gbps エンタープライズポートが **NETWORK ADAPTER #1** として表示されます。「[インターフェイスケーブル接続](#) (40ページ)」で説明されているとおり、これは、アプライアンスをエンタープライズネットワークにリンクするために必要なポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します（入力する値については、「[必要な IP アドレスおよびサブネット](#) (44ページ)」と「[必須の設定情報](#) (70ページ)」を参照してください）。

STEP #3	NETWORK ADAPTER #1 (enterprise)
The wizard has discovered 4 physical network adapter(s) installed on the appliance. Enter the network settings for the 1st network adapter (- 0 - enterprise network). Recommended use: enterprise network Select 'Cluster Link' if used for cluster communication. Phy Interfaces: ens1f1 ens9f1	Host IPv4 Address: 17. IPv4 Netmask: 255. Default Gateway IPv4 Address: 17. IPv4 DNS Servers: IPv4 Static Routes: Vlan Id of Interface: 1102 Cluster Link LACP Mode
< cancel > done >> next >>	

次の表に **NETWORK ADAPTER #1** に入力する設定値を示します。

18 : #1 10 Gbps

[Host IPv4/IPv6 Address] フィールド エンタープライズポートのIPアドレスを入力します。これは必須です。

[IPv4 Netmask/IPv6 Prefix Length] フィールド 次のいずれか 1 つのタスクを実行します。

- IPv4 アドレッシングを選択した場合は、ポートのIPアドレスのネットマスクを入力します。これは必須です。
- IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ～ 127 です。

[Default Gateway IPv4/IPv6 Address] フィールド

ポートに使用するデフォルトゲートウェイのIPアドレスを入力してください。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド 優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

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

[VLAN ID of Interface] フィールド 前の手順で有効にした結合インターフェイスの VLAN ID を入力します。有効にしていない場合、このフィールドは表示されません。

[Cluster Link] フィールド このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

[LACP Mode] フィールド 次のいずれか 1 つのタスクを実行します。

- このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2 つのイーサネットインターフェイスを 1 つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- このポートの [LACP] モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する 2 つのイーサネットインターフェイスが 1 つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#) (94 ページ) を参照してください。

注

このフィールドは、前の手順でオプションを選択しなかった場合に表示されます。

設定値の入力が完了したら、[next>>] をクリックして続行します。入力した値がウィザードによって検証され、正しくない値が含まれていた場合にはエラーメッセージが表示されます。エラーメッセージが表示された場合には、入力した値が正しいことを確認してから、再入力します。必要に応じて [<<back] をクリックして再入力します。

- 10 入力したエンタープライズポート値の検証が成功すると、ウィザードに 10 Gbps クラスタポートが **NETWORK ADAPTER #2** として表示されます。「[インターフェイスケーブル接続](#) (40 ページ)」で説明したように、このポートはアプライアンスをクラスタにリンクするために使用されるため、ホスト IP アドレス、ネットマスク、およびこの目的に適した他の値を適用します (入力する値については、「必

要な IP アドレスおよびサブネット (44ページ) 」と「必須の設定情報 (70ページ) 」を参照してください)。

STEP #3	OPTIONAL - NETWORK ADAPTER #2 (cluster)
(Optional) Enter the network settings for the 2nd network adapter - (- 0 - intra-cluster link). Recommended use: intra-cluster link Select 'Cluster Link' if used for cluster communication. Phy Interfaces: ens1f0 ens9f0	Host IPv4 Address: 169. IPv4 Netmask: 255. Default Gateway IPv4 Address: IPv4 DNS Servers: IPv4 Static Routes: Vlan Id of Interface: 1102 ☒ Cluster Link LACP Mode
<< back < cancel > done >> next >>	

次の表に **NETWORK ADAPTER #2** に入力する設定値を示します。

19 : #2 10 Gbps

[Host IPv4/IPv6 address] フィールド クラスターポートの IP アドレスを入力します。これは必須です。クラスターポートのアドレスは後で変更できません。

 注

以前に [Start using DNAC pre manufactured cluster] オプションを選択した場合、[169.254.6.66] がこのフィールドにすでに設定されているため、別のアドレスを入力することはできません。

[IPv4 Netmask/IPv6 Prefix Length] フィールド 次のいずれか 1 つのタスクを実行します。

- IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。

 注

以前に [Start using DNAC pre manufactured cluster] オプションを選択した場合、[255.255.255.128] がこのフィールドにすでに設定されているため、別のネットマスクを入力することはできません。

- IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ~ 127 です。

[Default Gateway IPv4/IPv6 address] フィールド

ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド

優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

[IPv4/IPv6 Static Routes] フィールド

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

[Cluster Link] フィールド

このポートが **Catalyst Center** クラスタへのリンクであるとして設定するには、このチェックボックスをオンにします。この操作はクラスタポートでのみ必要になります。

[LACP Mode] フィールド

次のいずれか 1 つのタスクを実行します。

- このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2 つのイーサネットインターフェイスを 1 つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- このポートの **[LACP]** モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する 2 つのイーサネットインターフェイスが 1 つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#) (94 ページ) を参照してください。

 注

- このフィールドは、ステップ 8 でオプションを選択しなかった場合に表示されます。
- アプライアンスの初期設定時に、アプライアンスのインタークラスターインターフェイスでのみ **LACP** モードを有効にできます。

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

11. 入力したクラスタポート値の検証が成功すると、ウィザードに **1 Gbps/10 Gbps** 管理ポートが **NETWORK ADAPTER #3** として表示されます。[インターフェイスケーブル接続](#) (40 ページ) で説明されており、このポートは管理ネットワークから **Catalyst Center GUI** にアクセスするために使用されます。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します (入力する値については、「[必要な IP アドレスおよびサブネット](#) (44 ページ)」と「[必須の設定情報](#) (70 ページ)」を参照してください)。

STEP #3	OPTIONAL - NETWORK ADAPTER #3 (management)
(Optional) Enter the network settings for the 3rd network adapter - (- 0 - management network). Recommended use: management network. Select 'Cluster Link' if used for cluster communication. Phy Interfaces: eno1 ens9f3	Host IPv4 Address: 172. IPv4 Netmask: 255. Default Gateway IPv4 Address: IPv4 DNS Servers: 171. 173. IPv4 Static Routes: 10. /255. /172. 171. /255. /172. Cluster Link
<< back < cancel > done >> next >>	

次の表に **NETWORK ADAPTER #3** に入力する設定値を示します。

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

20 : #3 1 Gbps/10 Gbps

[Host IPv4/IPv6 address] フィールド 管理ポートの IP アドレスを入力します。これは、このポートを使用して管理ネットワークから **Catalyst Center GUI** にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。

[IPv4 Netmask/IPv6 Prefix Length] フィールド IP アドレスを入力した場合は、次のいずれかのタスクを実行します。

- IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。
- IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ～ 127 です。

[Default Gateway IPv4/IPv6 address] フィールド

ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド 優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

- NTP の場合、**Catalyst Center** と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。
- クラスタ内の各アプライアンスに対して、最大 **3** つの DNS サーバを設定します。アプライアンスに対して **3** つを超える DNS サーバを設定すると、問題が発生する可能性があります。

[IPv4/IPv6 Static Routes] フィールド 1 つ以上のスタティックルートスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。

[Cluster Link] フィールド このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

- 12** 入力した管理ポート値の検証が成功すると、ウィザードに **1 Gbps/10 Gbps** インターネットポートが **[NETWORK ADAPTER #4]** として表示されます。「[インターフェイスケーブル接続 \(40ページ\)](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、**10 Gbps** エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します (入力する値については、「[必要な IP アドレスおよびサブネット \(44ページ\)](#)」と「[必須の設定情報 \(70ページ\)](#)」を参照してください)。

STEP #3	OPTIONAL - NETWORK ADAPTER #4 (internet)
(Optional) Enter the network settings for the 4th network adapter - (- 0 - internet-access network).	Host IPv4 Address:
Recommended use: internet-access network	IPv4 Netmask:
Cable status: disconnected	Default Gateway IPv4 Address:
Select 'Cluster Link' if used for cluster communication.	IPv4 DNS Servers:
Phy Interfaces: eno2 ens9f2	IPv4 Static Routes:
	Cluster Link
	<< back < cancel > done >> next >>

次の表に **NETWORK ADAPTER #4** に入力する設定値を示します。

21 : #4 1 Gbps/10 Gbps

[Host IPv4/IPv6 address] フィールド インターネットポートのIPアドレスを入力します。この操作はインターネット接続にインターネットポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにできます。

[IPv4 Netmask/IPv6 Prefix Length] フィールド IP アドレスを入力した場合は、次のいずれかのタスクを実行します。

- **IPv4** アドレッシングを選択した場合は、ポートのIPアドレスのネットマスクを入力します。これは必須です。
- **IPv6** アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は **10 ~ 127** です。

[Default Gateway IPv4/IPv6 address] フィールド

インターネットポートに使用するデフォルトゲートウェイのIPアドレスを入力します。

重要

アプライアンスの少なくとも1つのインターフェイスに対してデフォルトゲートウェイIPアドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド

優先DNSサーバのIPアドレスを入力します。複数のDNSサーバを入力する場合には、リスト内のIPアドレスをスペースで区切ります。

重要

クラスタ内の各アプライアンスに対して、最大3つのDNSサーバを設定します。アプライアンスに対して3つを超えるDNSサーバを設定すると、問題が発生する可能性があります。

[IPv4/IPv6 Static Routes] フィールド

1つ以上のスタティックルートスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ>の形式で入力します。これは通常、管理ポートでのみ必要です。

[Cluster Link] フィールド

このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

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

13. ネットワークアダプタの設定が完了すると、次に示す通り、ウィザードは使用しているDNSサーバのIPアドレスを入力するように求めます。

STEP #4	DNS Configuration
DNS configuration for the cluster. Note: In dual stack mode, ensure that DNS servers must provide DNS resolution for both IPv4 (A records) and IPv6 (AAAA records) to ensure proper network connectivity. * Indicates a mandatory field.	IP address of the DNS servers: * 2001: :a
	<< back < cancel > next >>

注

Catalyst Center アプライアンスでデュアルスタック モードを有効にする場合は、DNS サーバーが IPv4 と IPv6 の両方をサポートしていることを確認してください。

- 14** DNS サーバーの設定が完了すると、次に示すように、ウィザードは使用している **NETWORK PROXY** の設定値を入力するように求めます。

STEP #4	NETWORK PROXY
The controller appears to be behind a network proxy. Enter your network proxy configuration settings to enable cloud connectivity.	HTTPS Proxy: http://proxy- .com:80 HTTPS Proxy Username: HTTPS Proxy Password:
	<< back < cancel > next >>

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

22 :

[HTTPS Proxy] フィールド

インターネットにアクセスする **HTTPS** ネットワークプロキシの **URL** またはホスト名を入力します。

注

- **Catalyst Center** から **HTTPS** プロキシへの接続は、このリリースの **HTTP** 経由のみでサポートされます。
- ポート番号を含む **IPv6 URL** を入力する場合は、**URL** の **IP アドレス** 部分を角カッコで囲みます。次の例では、**443** がポート番号です。**http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/**

[HTTPS Proxy Username] フィールド

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

[HTTPS Proxy Password] フィールド

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

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

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

STEP #5	MAGLEV CLUSTER DETAILS
Cluster's hostname is the FQDN identifier of the cluster. Virtual IP address(s) is a list of IP(s) through which the Cluster's Management, Enterprise Interfaces can be accessible. Note that these are different from node's individual IP.	Cluster Virtual IP Address(s): 169. 172. 17. Cluster's hostname: Cdnac.example.cisco.com
<< back < cancel > next >>	

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

重要

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

クラスター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。**Catalyst Center** ではこのドメイン名を使用して次のタスクを実行します。

- 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、**Catalyst 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。
- Catalyst Center** 証明書の **[Subject Alternative Name (SAN)]** フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイサーバーが定義されます。

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

- 16 クラスターの詳細を入力すると、次に示すとおり、ウィザードに **[USER ACCOUNT SETTINGS]** の値を入力するよう促すプロンプトが表示されます。

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

この表は、[USER ACCOUNT SETTINGS] に入力する設定値を示します。

23 :

- | | |
|----------------------------------|--|
| [Linux Password] フィールド | maglev ユーザーの Linux パスワードを入力します。パスワード要件（73 ページ） に準拠していることを確認してください。 |
| [Re-enter Linux Password] フィールド | Linux パスワードをもう一度入力して確認します。 |
| [Password Generation Seed] フィールド | Linux パスワードを自動生成するには、このフィールドにシードフレーズを入力してから、[Generate Password] を押します。 |
| [Auto Generated Password] フィールド | （オプション）生成されたパスワードにはシードフレーズが含まれます。このパスワードを使用するか、自動生成されたパスワードを編集できます。 |
| | [<Use Generated Password>] を押してパスワードを保存します。 |

[Administrator Password] フィールド スーパーユーザ権限を持つ管理者のデフォルトのパスワードを入力します。このパスワードは **Catalyst Center** に初めてログインするときに使用します。このパスワードが [パスワード要件](#) (73ページ) に準拠していることを確認してください。

注

以前の手順で **[Start using DNAC pre manufactured cluster]** オプションを選択した場合、アプライアンスにはデフォルトのパスワード (**P@ssword9**) がすでに設定されているため、構成ウィザードで変更することはできません。その結果、このフィールドと次のフィールドはこの画面に表示されません。

[Re-enter Administrator Password] 管理者パスワードをもう一度入力して確認します。
フィールド

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

17. ユーザーアカウントの詳細を入力すると、**[NTP SERVER SETTINGS]** の値を入力するようウィザードからメッセージが表示されます。

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

次の表に、**[NTP SERVER SETTINGS]** に入力する構成値を示します。

[NTP Server] フィールド

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

[NTP Authentication] チェックボックス

NTP サーバーが同期する前に **Catalyst Center NTP** サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- **NTP** サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。

この値は、**NTP** サーバーのキーファイルで定義されているキー ID に対応します。

- **NTP** サーバーのキー ID に関連付けられた **SHA-1** キー値。この 40 文字の 16 進文字列は、**NTP** サーバーのキーファイルにあります。

 注

前のフィールドで構成した各 **NTP** サーバーのキー ID とキー値を入力してください。

必要な情報を入力したら、**[next>>]** をクリックして続行します。以前の画面でしたように、検証エラーを修正します。ウィザードによって、**NTP** サーバの設定が検証され、適用されます。

18. 適切な **NTP** サーバーを指定すると、次に示すように、**[MAGLEV ADVANCED SETTINGS]** の値を入力するようウィザードに求められます。

注

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

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

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

24 : Maglev

[Container Subnet] フィールド	内部サービスを管理するために Catalyst Center で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは 169.254.32.0/20 にあらかじめ設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、 Catalyst Center の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりしていないことを確認してください。詳細については、 必要な IP アドレスおよびサブネット (44ページ) のコンテナサブネット (Container Subnet) に関する説明を参照してください。
---------------------------------	---

- [Cluster Subnet]** フィールド 内部クラスタサービスを管理するために **Catalyst Center** で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.48.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。別のサブネットを入力する場合は、**Catalyst Center** の内部ネットワークまたは任意の外部ネットワークで使用されている他のサブネットと競合したり、重複したりしていないことを確認してください。詳細については、[必要な IP アドレスおよびサブネット](#) (44 ページ) のクラスタサブネット (**Cluster Subnet**) に関する説明を参照してください。
- [Enable Intracluster IPsec]** チェックボックス 3 ノードの高可用性 (HA) クラスタ内のノード間の IPsec 接続を有効にする場合にオンにします。

完了したら、**[next>>]** をクリックして続行します。以前の画面でしたように、検証エラーを修正します。

- 19. Maglev** 詳細設定の入力が完了すると、ウィザードで設定を適用する準備ができたことを示す最終メッセージが表示されます (以下参照)。

```
The wizard is now ready to apply the configuration on the controller.

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

<< back < cancel > proceed >>

[Proceed >>] をクリックして、設定ウィザードを完了します。

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

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

```

CONFIGURATION SUCCEEDED

The configuration wizard has completed successfully!

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

To access the Maglev Web Console, please point your browser to one of the following URLs:
https://17.
https://169.
https://172.

The wizard will automatically close in 30 seconds

```

- 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](#)（256ページ）」）を実行します。
- アプライアンスをクラスタ内のプライマリノードとして展開する場合には、クラスタ内の2番目と3番目のインストール済みアプライアンスを設定します（[Maglev ウィザードを使用したセカンダリノードの設定](#)（131ページ））。

FIPS

アプライアンスで FIPS モードが有効になっている場合の注意事項を示します。

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

- 以前の **Catalyst Center** バージョンからアップグレードされたアプライアンスでは FIPS モードを有効化できません。最新バージョンがすでにインストールされているアプライアンスでのみ有効化できます。
- FIPS モードが有効になっている場合、URL からイメージをインポートすることはできません。コンピュータまたは **cisco.com** からのみイメージをインポートできます。
- **USER ACCOUNT SETTINGS** 画面で、デフォルトの管理スーパーユーザー用にパスワードを入力する必要があります。[パスワード要件](#)（73ページ）
- アプライアンスで FIPS モードが有効になっている場合、外部認証を有効にすることはできません。
- バックアップは、送信元クラスターと同じ FIPS モード設定を持つ **Catalyst Center** クラスターでのみ復元できます。FIPS モード設定が異なるクラスターを含むバックアップおよび復元操作は失敗します（**Catalyst Center** はバックアップに互換性なしのラベルを付けるため）。
- **Maglev** 設定ウィザードの完了時に **[Start using DNAC pre manufactured cluster]** オプションを選択した場合、**[IP addressing and Security mode used for the services]** 画面は表示されません。このシナリオでは、FIPS モードを有効にすることはできません。
- **Catalyst Center** は、FIPS モードが有効になっている場合、SNMPv2c デバイスクレデンシャルをサポートしません。代わりに、SNMPv3 クレデンシャルを指定する必要があります。
- アプライアンスで FIPS モードを有効化した後で、無効化できる唯一の方法は、アプライアンスのイメージを再作成することです（既存のデータはすべて消去されます）。その後、FIPS モードを無効化してアプライアンスを再構成できます。詳細については、「[アプライアンスのイメージの再作成](#)（96ページ）」を参照してください。
- FIPS モードが有効になっている場合、KeyWrap を有効化できるのは、**Catalyst Center** と **Cisco ISE** がまだ統合されていない場合のみです。詳細については、「[認証サーバーとポリシーサーバーの設定](#)（276ページ）」を参照してください。

- アプライアンスを構成した後、次の操作を実行して、FIPS モードが有効になっているかどうかを確認できます。
 1. アプライアンスの SSH コンソールを開き、**ssh -p 2222 maglev@appliance's-IP-address** コマンドを実行します。
 2. デフォルトの管理スーパーユーザーのパスワードを入力して、アプライアンスにログインします。
 3. **magctl fips status** コマンドを実行します。
- Cisco Wide Area Bonjour アプリケーションは FIPS モードをサポートしていません。そのため、このアプリケーションを Catalyst Center GUI または CLI からインストールすることはできません。
- FIPS モードが有効になっている場合、エンドポイント分析に関連する一部の機能は Catalyst Center GUI で使用できません。
- FIPS モードは、マップアーカイブのエクスポートとインポートに影響します。

FIPS モードが有効の場合：

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

FIPS モードが無効の場合：

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

Maglev

Maglev 構成ウィザードを使用して、クラスタに付加的なアプライアンスを追加できます。

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

重要

- 3 ノードクラスタを構築するには、同じバージョンのシステムパッケージが 3 つの Catalyst Center アプライアンスにインストールされている必要があります。この条件が整わない場合、予期しない動作とダウンタイムの可能性が生じることがあります。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、Catalyst Center に初めてログインした後に、（ネットワークのデバイスを検出してテレメトリを有効にするために完了する）クイック スタート ワークフローが開始されません。
- この手順の実行中に入力するすべての IP アドレスが有効なネットマスクを持つ有効なアドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

新しいセカンダリノードをクラスタに結合する場合には、クラスタ内の最初のホストのクラスタリンクの物理 IP アドレスを指定する必要があります。

HA 対応クラスタのノードを交換する場合は、残りのノードのいずれかのクラスタリンクの物理 IP アドレスを使用します。

セカンダリノードをクラスターに参加させる場合は、次のことを理解してください。

- 一度に 1 つのノードのみをクラスター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。
- クラスターに新しいノードを追加する前に、インストールされているすべてのパッケージがプライマリノードに展開されていることを確認してください。展開されているかどうかを確認するには、セキュアシェルを使用して、プライマリノードの **Catalyst Center** 管理ポートに **Linux** ユーザー (**maglev**) としてログインしてから、`maglev package status` コマンドを実行します。インストールされているすべてのパッケージは、コマンド出力で「展開済み (DEPLOYED)」と表示されます。

```
maglev-1 [main - https://kong- :443]
```

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

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

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

次のことを確認します。

- Maglev ウィザードを使用したプライマリノードの設定** (107ページ) の手順に従って、クラスター内の最初のアプライアンスが設定されたこと。
- 「**必要な IP アドレスおよびサブネット** (44ページ)」および「**必須の設定情報** (70ページ)」で指定されているすべての情報を収集したこと。
- 「**アプライアンスのインストール ワークフロー** (76ページ)」の説明に従って、2 番目と 3 番目のアプライアンスを設置したこと。
- 次の手順を完了しました。

1. 最初のアプライアンスで **maglev package status** コマンドを実行したこと。

Catalyst Center GUI からこの情報にアクセスできます。**[Help]** アイコン (🔍) をクリックし、**[About]** > **[Packages]** の順に選択してください。

2. Cisco TAC に連絡し、このコマンドの出力を提供して 2 番目と 3 番目のアプライアンスにインストールする必要がある ISO をポイントするよう依頼したこと。

- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(86ページ\)](#)」の説明に従って、両方のセカンダリアプライアンスで **Cisco IMC** に対するブラウザのアクセス権が設定されたこと。
- 「[事前設定タスクの実行 \(91ページ\)](#)」の説明に従って、セカンダリアプライアンスのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- 互換性のあるブラウザを使用していることを確認済みであること。互換性のあるブラウザの一覧については、インストールしている **Catalyst Center** のバージョンに対応する [リリースノート](#) ドキュメントを参照してください。
- 次の手順で指定するデフォルトゲートウェイおよび **DNS** サーバーと **Catalyst Center** の間のファイアウォールで **ICMP** が許可されていること。**Maglev** 設定ウィザードでは **ping** を使用して、ユーザが指定したゲートウェイおよび **DNS** サーバを確認します。

注意

ファイアウォールが配置されており、そのファイアウォールで **ICMP** が許容されていない場合、この **ping** がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. お使いのブラウザで、実行した **cisco imc** GUI 設定で設定した **Cisco IMC** の IP アドレスをポイントし、**cisco imc** ユーザとして **Cisco IMC GUI** にログインします ([Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(86ページ\)](#) を参照)。
ログインが成功すると、アプライアンスに **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウが、ウィンドウ上部のハイパーリンクメニューとともに表示されます。
2. ハイパーリンクメニューで **[Launch KVM]** を選択してから **[HTML-based KVM]** を選択します。
KVM コンソールが別ウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、**Maglev** 構成ウィザードのプロンプトに応答します。
3. KVM が表示されたら、次のいずれかのオプションを選択してアプライアンスをリブートします。
 - メインの **Cisco IMC GUI** ブラウザウィンドウで、**[Host Power] > [Power Cycle]** を選択し、KVM コンソールに切り替えて続行します。
 - KVM コンソールで、**[Power] > [Power Cycle System (cold boot)]** を選択します。

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

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

STEP #None	STATIC IP CONFIGURATION
Welcome to the Maglev Configuration Wizard! Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration. - Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface - Click Skip to move to config wizard NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration	<pre> IPv6 mode IP Address: Netmask: Default Gateway Address: Static Routes: Web installation: https://10.10.10.10:9004/ < cancel > skip >> configure >></pre>

4. [Skip] をクリックします。

KVM コンソールに **Maglev** 構成ウィザードのウェルカム画面が表示されます。

```

Welcome to the Maglev Configuration Wizard!

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

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

< exit >

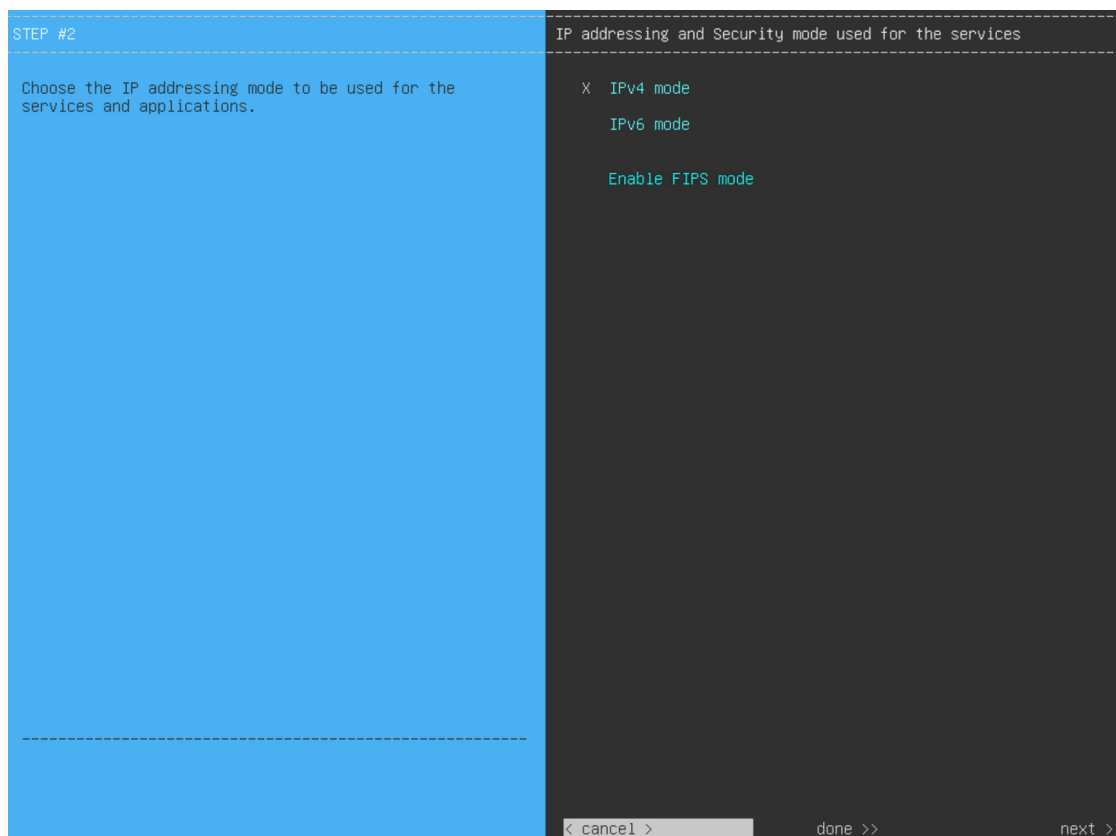
```

 注

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

5. [Join a Catalyst Center Cluster] を選択して、セカンダリノードの設定を開始します。

画面が更新されます。



6. 次の手順を実行し、[next>>] をクリックして続行します。

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

アプライアンスで FIPS モードを有効にする際の注意事項については、[FIPS モードのサポート](#)（130 ページ）を参照してください。

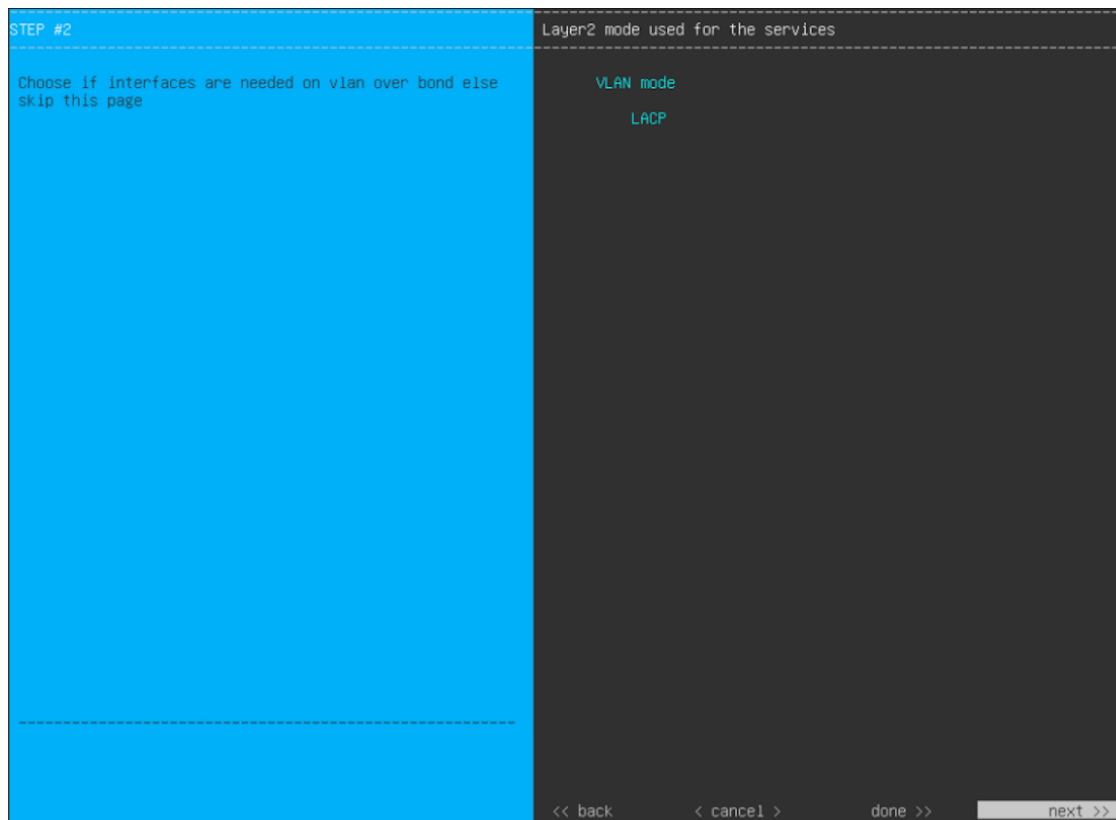
重要

次のウィザード画面では、[VLAN mode] 機能を有効にできます。このモードが有効になると、アプライアンスのエンタープライズ インターフェイスのプライマリインスタンスとセカンダリインスタンスの両方を使用してネットワークに接続する、単一の結合インターフェイスが作成されます。この機能

は一般的に使用されないため、**Catalyst Center** 展開で必要であることがわかっている場合にのみ有効にしてください。

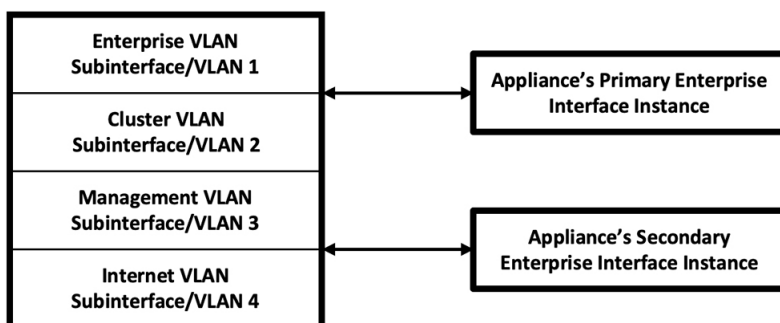
- この場合は、次の手順を実行します。
- それ以外の場合は、次のウィザード画面で何も選択せずに **[next>>]** をクリックします。このガイドで前述した **NIC** ボンディング機能は、ウィザードの **[Enterprise]** および **[Intracuster]** インターフェイス構成画面で有効にできます。

7. (オプション) 次のステップを実行して、アプライアンスのレイヤ 2 ポートチャネルモード (VLAN タグ付き) を有効にします。選択したら、[next>>]** をクリックして続行します。**



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

Virtual Bonded Interface



- b) 代わりにこのインターフェイスを **[LACP]** モード（ロードバランシングとより高い帯域幅を有効にする）で動作させる場合は、**LACP** オプションも選択する必要があります。
- c) アプライアンスのエンタープライズおよびクラスタインターフェイスの設定を入力するときは、仮想結合インターフェイスで設定するサブインターフェイスの **[VLAN ID of Interface]** フィールドに一意の **VLAN ID** を入力してください。

重要

1つの物理アプライアンスインターフェイス（エンタープライズインターフェイス）が接続されている場合でも、仮想結合インターフェイスに存在するすべてのサブインターフェイスを設定できます。

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

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

設定の過程でウィザードがエンタープライズポートとクラスタポートのいずれかまたは両方を表示できない場合は、これらのポートが機能していないか、または無効になっている可能性があります。**Catalyst Center** 機能にはこの2つのポートが必要です。機能していないことが判明した場合には、**[cancel]** を選択し、すぐに設定を終了します。設定を再開したり、**Cisco Technical Assistance Center** に連絡したりする前に、「[事前設定タスクの実行（91ページ）](#)」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。

8. ウィザードにより、最初に **10 Gbps** エンタープライズポートが **NETWORK ADAPTER #1** として表示されます。「[インターフェイスケーブル接続（40ページ）](#)」で説明されているとおり、これは、アプライアンスをエンタープライズネットワークにリンクするために必要なポートです。この目的に適したホストIPアドレス、ネットマスク、およびその他の値を適用します（入力する値については、「[必要なIPアドレスおよびサブネット（44ページ）](#)」と「[必須の設定情報（70ページ）](#)」を参照してください）。

STEP #3	NETWORK ADAPTER #1 (enterprise)
The wizard has discovered 4 physical network adapter(s) installed on the appliance. Enter the network settings for the 1st network adapter (- 0 - enterprise network). Recommended use: enterprise network Select 'Cluster Link' if used for cluster communication. Phy Interfaces: ens1f1 ens9f1	Host IPv4 Address: 17. IPv4 Netmask: 255. Default Gateway IPv4 Address: 17. IPv4 DNS Servers: IPv4 Static Routes: Vlan Id of Interface: 1102 Cluster Link LACP Mode
< cancel > done >> next >>	

次の表のとおり **NETWORK ADAPTER #1** の設定値を入力します。

25 : **#1** **10 Gbps**

[Host IPv4/IPv6 Address] フィールド エンタープライズポートのIPアドレスを入力します。これは必須です。

[IPv4 Netmask/IPv6 Prefix Length] フィールド IP アドレスを入力した場合は、次のいずれかのタスクを実行します。

- IPv4 アドレッシングを選択した場合は、ポートのIPアドレスのネットマスクを入力します。これは必須です。
- IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は 10 ～ 127 です。

[Default Gateway IPv4/IPv6 address] フィールド

ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド 優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

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

[Vlan Id of Interface] フィールド 設定するアプライアンス用に作成される LACP リンク上でタグ付けされる VLAN ID を入力します。

注

このフィールドは、前の手順で両方のオプションを選択してアプライアンスのレイヤ 2 LACP ポートチャネルモードを設定した場合にのみ表示されます。

[Cluster Link] フィールド このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

[LACP Mode] フィールド

次のいずれか 1 つのタスクを実行します。

- このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2 つのイーサネットインターフェイスを 1 つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- このポートの **[LACP]** モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する 2 つのイーサネット インターフェイスが 1 つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#) (94 ページ) を参照してください。

 注

このフィールドは、前の手順でオプションを選択しなかった場合に表示されます。

設定値の入力が完了したら、**[next>>]** をクリックして続行します。入力した値がウィザードによって検証され、正しくない値が含まれていた場合にはエラーメッセージが表示されます。エラーメッセージが表示された場合には、入力した値が正しいことを確認してから、再入力します。必要に応じて **[<<back]** をクリックして再入力します。

9. 入力したエンタープライズポート値の検証が成功すると、ウィザードに **10 Gbps クラスタポート** が **[NETWORK ADAPTER #2]** として表示されます。「[インターフェイスケーブル接続](#) (40 ページ)」で説明したように、このポートはアプライアンスをクラスタにリンクするために使用されるため、ホスト IP アドレス、ネットマスク、およびこの目的に適した他の値を適用します (入力する値については、「[必要な IP アドレスおよびサブネット](#) (44 ページ)」と「[必須の設定情報](#) (70 ページ)」を参照してください)。

STEP #3	OPTIONAL - NETWORK ADAPTER #2 (cluster)
(Optional) Enter the network settings for the 2nd network adapter - (- 0 - intra-cluster link). Recommended use: intra-cluster link Select 'Cluster Link' if used for cluster communication. Phy Interfaces: ens1f0 ens9f0	Host IPv4 Address: 169. IPv4 Netmask: 255. Default Gateway IPv4 Address: IPv4 DNS Servers: IPv4 Static Routes: Vlan Id of Interface: 1102 ☒ Cluster Link ☐ LACP Mode
<< back < cancel > done >> next >>	

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

26 : **#2** **10 Gbps**

[Host IPv4/IPv6 address] フィールド クラスターポートの IP アドレスを入力します。これは必須です。



注

クラスターポートのアドレスは後で変更できません。

[IPv4 Netmask/IPv6 Prefix Length] フィールド IP アドレスを入力した場合は、次のいずれかのタスクを実行します。

- IPv4 アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。
- IPv6 アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は **10 ~ 127** です。

[Default Gateway IPv4/IPv6 address] フィールド

ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。

重要

アプライアンスの少なくとも **1** つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド 優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

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

[Vlan Id of Interface] フィールド 設定するアプライアンス用に作成される LACP リンク上でタグ付けされる VLAN ID を入力します。

注

このフィールドは、ステップ 7 で両方のオプションを選択してアプライアンスのレイヤ 2 LACP ポートチャネルモードを設定した場合にのみ表示されます。

[Cluster Link] フィールド このポートが Catalyst Center クラスタへのリンクであるとして設定するには、このチェックボックスをオンにします。この操作はクラスタポートでのみ必要になります。

[LACP Mode] フィールド

次のいずれか 1 つのタスクを実行します。

- このフィールドを空白のままにすると、ポートはアクティブ/バックアップモードで動作します。このモードでは、2 つのイーサネットインターフェイスを 1 つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- このポートの **[LACP]** モードを有効にするには、このチェックボックスをオンにします。このモードでは、同じ速度とデュプレックス設定を共有する 2 つのイーサネットインターフェイスが 1 つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#) (94 ページ) を参照してください。

 注

- このフィールドは、ステップ 7 でオプションを選択しなかった場合に表示されます。
- アプライアンスの初期設定時に、アプライアンスのインタークラスターインターフェイスでのみ **LACP** モードを有効にできます。

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

10. 入力したクラスターポート値の検証が成功すると、ウィザードに **1 Gbps/10 Gbps** 管理ポートが **NETWORK ADAPTER #3** として表示されます。[インターフェイスケーブル接続](#) (40 ページ) で説明されているとおり、このポートは管理ネットワークから **Catalyst Center GUI** にアクセスするために使用されます。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します (入力する値については、「[必要な IP アドレスおよびサブネット](#) (44 ページ)」と「[必須の設定情報](#) (70 ページ)」を参照してください)。

STEP #3	OPTIONAL - NETWORK ADAPTER #3 (management)
(Optional) Enter the network settings for the 3rd network adapter - (- 0 - management network). Recommended use: management network. Select 'Cluster Link' if used for cluster communication. Phy Interfaces: eno1 ens9f3	Host IPv4 Address: 172. IPv4 Netmask: 255. Default Gateway IPv4 Address: IPv4 DNS Servers: 171. 173. IPv4 Static Routes: 10. /255. /172. 171. /255. /172. Cluster Link
<< back < cancel > done >> next >>	

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

27 : **#3** **1 Gbps/10 Gbps**

[Host IPv4/IPv6 address] フィールド 管理ポートの IP アドレスを入力します。これは、このポートを使用して管理ネットワークから **Catalyst Center GUI** にアクセスする場合にのみ必要です。それ以外の場合は、空白のままにします。

[IPv4 Netmask/IPv6 Prefix Length] フィールド 次のいずれか 1 つのタスクを実行します。

- **IPv4** アドレッシングを選択した場合は、ポートの IP アドレスのネットマスクを入力します。これは必須です。
- **IPv6** アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は **10 ~ 127** です。

[Default Gateway IPv4/IPv6 address] フィールド

ポートに使用するデフォルトゲートウェイの IP アドレスを入力してください。

重要

アプライアンスの少なくとも **1** つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド 優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

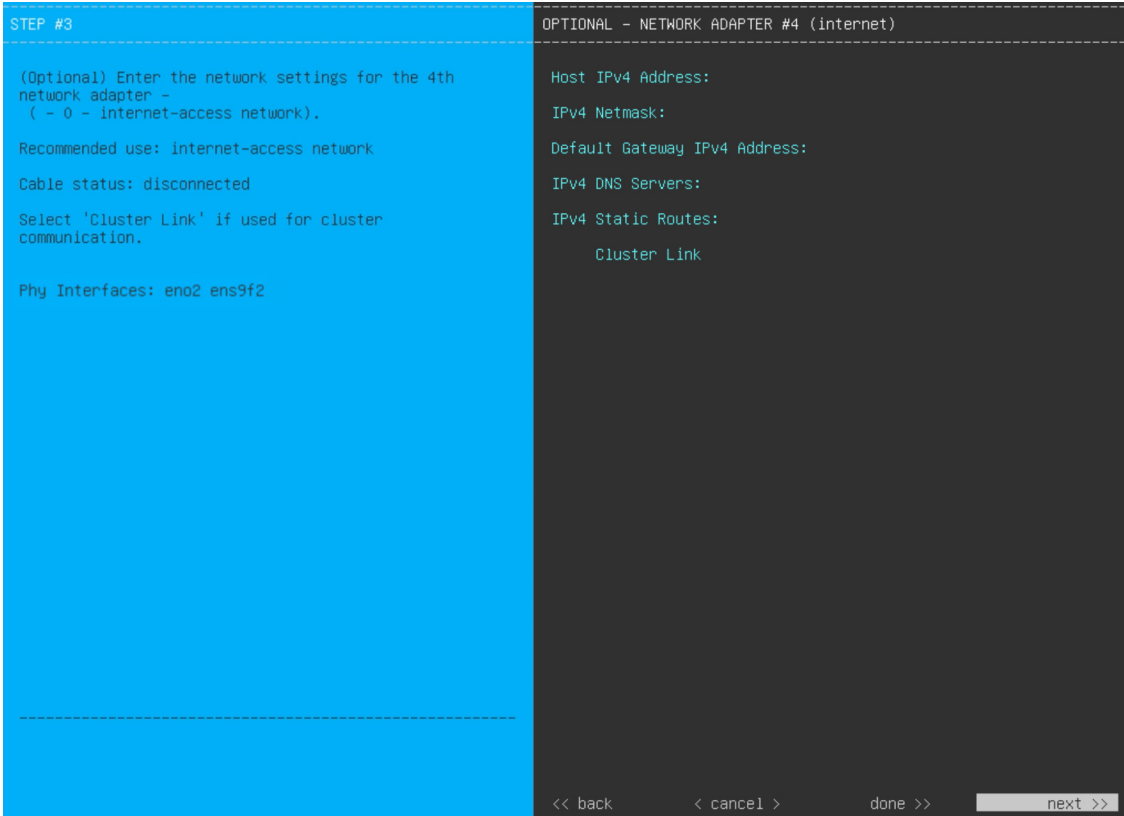
- NTP の場合、Catalyst Center と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。
- クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

[IPv4/IPv6 Static Routes] フィールド 1 つ以上のスタティックルートをスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。

[Cluster Link] フィールド このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

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

11. 入力した管理ポート値の検証が成功すると、ウィザードに 1 Gbps/10 Gbps インターネットポートが **[NETWORK ADAPTER #4]** として表示されます。「[インターフェイスケーブル接続 \(40 ページ\)](#)」で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、10 Gbps エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。この目的に適したホスト IP アドレス、ネットマスク、およびその他の値を適用します (入力する値については、「[必要な IP アドレスおよびサブネット \(44 ページ\)](#)」と「[必須の設定情報 \(70 ページ\)](#)」を参照してください)。



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

28 : **#4** **1 Gbps/10 Gbps**

[Host IPv4/IPv6 address] フィールド インターネットポートのIPアドレスを入力します。この操作はインターネット接続にインターネットポートを使用している場合にのみ必要です。それ以外の場合は、空白のままにできます。

[IPv4 Netmask/IPv6 Prefix Length] フィールド 次のいずれか 1 つのタスクを実行します。

- **IPv4** アドレッシングを選択した場合は、ポートのIPアドレスのネットマスクを入力します。これは必須です。
- **IPv6** アドレッシングを選択した場合は、プレフィックス長（ビット単位）を入力します。有効な値の範囲は **10 ~ 127** です。

[Default Gateway IPv4/IPv6 address] フィールド インターネットポートに使用するデフォルトゲートウェイのIPアドレスを入力します。

重要

アプライアンスの少なくとも **1** つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[IPv4/IPv6 DNS Servers] フィールド 優先 DNS サーバの IP アドレスを入力します。複数の DNS サーバを入力する場合には、リスト内の IP アドレスをスペースで区切ります。

重要

クラスタ内の各アプライアンスに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。

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

[Cluster Link] フィールド このフィールドは空欄のままにします。この操作はクラスタポートでのみ必要になります。

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

- 12 ネットワークアダプタの設定が完了すると、次に示すように、ユーザーの使用する [NETWORK PROXY] の設定値を入力するようウィザードから求められます。

STEP #4	NETWORK PROXY
The controller appears to be behind a network proxy. Enter your network proxy configuration settings to enable cloud connectivity.	HTTPS Proxy: http://proxy-.....com:80 HTTPS Proxy Username: HTTPS Proxy Password:
<< back < cancel > next >>	

次の表に示すように [NETWORK PROXY] の設定値を入力します。

29 :

[HTTPS Proxy] フィールド

インターネットにアクセスする HTTPS ネットワークプロキシの URL またはホスト名を入力します。

 注

- Catalyst Center から HTTPS プロキシへの接続は、このリリースの HTTP 経由のみでサポートされます。
- ポート番号を含む IPv6 URL を入力する場合は、URL の IP アドレス部分を角カッコで囲みます。次の例では、443 がポート番号です。http://[2001:db8:85a3:8d3:1319:8a2e:370:7348]:443/

[HTTPS Proxy Username] フィールド

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

[HTTPS Proxy Password] フィールド

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

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

- 13 ネットワークプロキシの設定が完了すると、次に示すように、[MAGLEV CLUSTER DETAILS] に、プライマリノードのクラスターポートとプライマリノードのログインに関する詳細を特定するためのウィザードのプロンプトが表示されます。

STEP #5

Virtual IP address(s) is a list of IP(s) through which the Cluster's Management, Enterprise Interfaces can be accessible.

Note that these are different from node's individual IP.

MAGLEV CLUSTER DETAILS

Maglev Primary Node: *

169.

Username: *

maglev

Password: *

<< back < cancel > next >>

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

30 : MAGLEV CLUSTER DETAILS

[Maglev Primary Node] フィールド	クラスタ内のプライマリノードのクラスタポートの IP アドレスを入力します。ポート割り当ての推奨事項に従っている場合、これはプライマリノードのネットワークアダプタ #2 の IP アドレスです。
[Username] フィールド	maglev と入力します。
[Password] フィールド	プライマリノードで設定した Linux パスワードを入力します。

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

- 14 クラスターの詳細を入力すると、次に示すとおり、ウィザードに **[USER ACCOUNT SETTINGS]** の値を入力するよう促すプロンプトが表示されます。

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

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

31 : USER ACCOUNT SETTINGS

[Linux Password] フィールド	maglev ユーザーの Linux パスワードを入力します。パスワード要件 (73 ページ) に準拠していることを確認してください。
[Re-enter Linux Password] フィールド	Linux パスワードをもう一度入力して確認します。
[Password Generation Seed] フィールド	Linux パスワードを自分で作成しない場合には、このフィールドにシードフレーズを入力してから、 [パスワードの生成 (Generate password)] を押してパスワードを生成します。
[Auto Generated Password] フィールド	(オプション) シードフレーズは、ランダムで安全なパスワードの一部として表示されます。必要に応じて、このパスワードを「そのまま」使用することも、この自動生成パスワードをさらに編集することもできます。 [<Use Generated Password>] をクリックしてパスワードを保存します。
[Administrator Password] フィールド	スーパーユーザ権限を持つ管理者のデフォルトのパスワードを入力します。このパスワードは Catalyst Center に初めてログインするときに使用します。このパスワードが パスワード要件 (73 ページ) に準拠していることを確認してください。
[Re-enter Administrator Password] フィールド	管理者パスワードをもう一度入力して確認します。

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

15. ユーザーアカウントの詳細を入力すると、**[NTP SERVER SETTINGS]**の値を入力するようウィザードからメッセージが表示されます。

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

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

[NTP Server] フィールド

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

[NTP Authentication] チェックボックス

NTP サーバーが同期する前に **Catalyst Center** NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。

この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。

- NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

必要な情報を入力したら、**[next>>]** をクリックして続行します。以前の画面でしたように、検証エラーを修正します。ウィザードによって、NTP サーバの設定が検証され、適用されます。

16. NTP サーバー設定の入力が完了すると、ウィザードで設定を適用する準備ができたことを示す最終メッセージが表示されます（以下参照）。

```
The wizard is now ready to apply the configuration on the controller.

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

<< back
< cancel >
proceed >>

[Proceed >>] をクリックして、設定ウィザードを完了します。

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

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

```
CONFIGURATION SUCCEEDED

The configuration wizard has completed successfully!

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

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

https://17.
https://169.
https://172.

The wizard will automatically close in 30 seconds
```

- クラスタ内の3番目および最後のノードとして展開する追加のアプライアンスがある場合には、この手順を繰り返します。
- クラスタへのホストの追加が終了したら、初回セットアップ：[初期設定ワークフロー](#)（256ページ）を実行します。

Catalyst Center

最新の **Catalyst Center** リリースにアップグレードできます。

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

:	
•	□□□□□□□□□□□□
•	□□□□□□□□□□
•	VLAN □□□□□□□□
•	□□□□□□□□□□□□□□□□ □□□□□□□□□□
•	□□□□□□□□□□□□□□□□ □□□□□□□□□□□□
•	□□□□□□□□□□□□□□□□ □□□□□□□□□□□□
•	□□□ Catalyst Center □□□□□□□□ □□□□□□

展開モードに基づいた 32 コアおよび 56 コア アプライアンスの設定に関する情報を提供します。

次のいずれかのモードを使用して、32 または 56 コアアプライアンスをネットワークに展開できます。

- **スタンドアロン**：すべての機能を提供する単一のノードとして。このオプションは通常、初期展開、テスト展開、小規模なネットワーク環境での使用に適しています。初回展開でスタンドアロンモードを選択すると、プライマリノードになります。

注

後でさらにアプライアンスを追加してクラスターを形成できます。

- **クラスター**：3 ノードクラスターに属するノードとして。このモードでは、すべてのサービスとデータがホスト間で共有されます。これは、大規模な展開で推奨されるオプションです。初期展開でクラスターモードを選択した場合は、セカンダリノードの設定に進む前に、プライマリノードの設定を完了してください。

続行するには、クラスター内でプライマリノードを設定します。3つのアプライアンスを設置済みで、クラスターに 2 番目と 3 番目のノードを追加する場合は、次に、セカンダリノードを設定します。

インストール構成ウィザードまたは詳細インストール構成ウィザードを使用してアプライアンスを設定する必要があるかどうかを判断するのに役立つ情報。

Catalyst Center は、アプライアンスの設定に使用できる 2 種類のブラウザベースのウィザードを提供します。説明を読んで、完了するウィザードを決定してください。

重要

これらのウィザードは、**Catalyst Center** の最新リリースがすでにインストールされている新しいアプライアンスを設定している場合に使用できます。以前のバージョンからアップグレードし、これらのウィザードを使用する場合は、**Cisco TAC** にサポートを依頼してください。

このウィザードは、クラスター内のインターフェイスだけでなく、企業インターフェイス、管理インターフェイス、およびインターネットアクセスインターフェイスにもデフォルト値を設定し、アプライアンスの設定プロセスを合理化します。すべてのインターフェイスは、アプライアンスのエンタープライズポート上にあります。デフォルトのインターフェイス設定を使用することに同意し、アプライアンスを迅速にアクティブ化する場合は、このウィザードを使用します。

 注

このウィザードではクラスターのセカンダリノードは設定できません。

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

ブラウザベースのウィザードのいずれかを使用してアプライアンスを正しく設定するには、次のタスクを完了します。

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

または、[Static IP Address Settings] ページを完了して、アプライアンスの企業インターフェイスに独自の IP アドレス、サブネットマスク、およびデフォルトゲートウェイを指定することもできます。

Catalyst Center のパスワードポリシーと要件へのポイントを提供します。

これらのトピックを参照して、Catalyst Center のパスワード実装の説明を確認してください。

- [パスワードポリシー](#) (73ページ)
- [パスワード要件](#) (73ページ)

VLAN

Catalyst Center で VLAN モードが有効になっている場合、ディザスタリカバリを使用できません。

VLAN モードについては次の詳細を考慮してください。

- VLAN モードの説明については、「」 [「Maglev ウィザードを使用したプライマリノードの設定](#) (107ページ) 」を参照してください。
- VLAN モード：
 - Maglev 設定ウィザードを使用して Catalyst Center アプライアンスを設定する場合にのみ有効にできます。
 - ブラウザベースの構成ウィザードを使用して有効にすることはできません。

- アプライアンスを再イメージ化せずに無効にすることはできません。
- ディザスタリカバリは、VLAN モードが有効になっている Catalyst Center 展開ではサポートされません。

インストール構成ウィザードを使用して、3 ノードクラスタのプライマリ ノードまたはスタンドアロン ノードを設定できます。

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

- 32 コアアプライアンス：シスコ部品番号 DN3-HW-APL
- 56 コアアプライアンス：シスコ部品番号 DN3-HW-APL-L

重要

- このウィザードは、新しい Catalyst Center アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、Maglev 設定ウィザードを使用する必要があります (Maglev ウィザードを使用したアプライアンスの設定 (105 ページ) を参照)。
- このウィザードを使用して、3 ノードクラスタの 2 番目または 3 番目のアプライアンスを設定することはできません。これを実行するには、詳細インストール構成ウィザードを使用したセカンダリ ノードの設定 (186 ページ) で説明されている手順を完了します。また、このウィザードを使用して、アプライアンスのエンタープライズおよびクラスタ内インターフェイスで LACP モードを有効にすることはできません。
- 3 ノードクラスター内のアプライアンスは、設定前にログアウトします。ログアウトしていない場合、クラスタのアプライアンスを設定し、Catalyst Center に初めてログインした後に、(ネットワークのデバイスを検出してテレメトリを有効にするために完了する) クイック スタート ワークフローが開始されません。
- この手順の実行中に入力するすべての IP アドレスが有効な IPv4 ネットマスクを持つ有効な IPv4 アドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

次のことを確認します。

- 必要な IP アドレスおよびサブネット (44 ページ) と 必須の設定情報 (70 ページ) で必要な情報がすべて収集されたこと。
- 「アプライアンスのインストール ワークフロー (76 ページ)」の説明に従って、1 番目のアプライアンスを設置したこと。
- 「Cisco Integrated Management Controller に対するブラウザアクセスの有効化 (86 ページ)」の説明に従って、Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「事前設定タスクの実行 (91 ページ)」の説明に従って、アプライアンスのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。

- Cisco IMC、Catalyst Center との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている Catalyst Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順で指定する DNS サーバーと Catalyst Center の間のファイアウォールで ICMP が許容されること。このウィザードでは、ユーザの指定する DNS サーバを ping で確認します。Catalyst Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. インストール構成ウィザードを起動します。

- a) お使いのブラウザで、実行した Cisco IMC GUI 設定で設定した Cisco IMC の IP アドレスをポイントしてから、Cisco IMC ユーザーとして Cisco IMC GUI にログインします ([Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(86ページ\)](#) を参照)。

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

- b) 青いリンクメニューで [Launch KVM] を選択してから [HTML based KVM] を選択します。

KVM コンソールが別のブラウザウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、Maglev 構成ウィザードのプロンプトに応答します。

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

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

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

リブートメッセージが表示された後、KVM コンソールに [Static IP Configuration] ウィンドウが表示されます。

The screenshot displays the 'Static IP CONFIGURATION' screen of the Maglev Configuration Wizard. The interface is split into two main panels. The left panel, with a blue background, contains the following text: 'Welcome to the Maglev Configuration Wizard!', 'Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration.', a bulleted list: '- Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface' and '- Click Skip to move to config wizard', and a note: 'NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration'. The right panel, with a dark gray background, lists configuration options: 'IPv6 mode', 'IP Address:', 'Netmask:', 'Default Gateway Address:', and 'Static Routes:'. At the bottom of the right panel, the 'Web installation:' URL is shown as 'https://10.10.10.10:9004/'. A dashed line separates the main content from the bottom navigation bar. The navigation bar includes buttons for '< cancel >', 'skip >>', and 'configure >>'.

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

d) 次のいずれか 1 つのタスクを実行します。

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

 注

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

[IPv6 Mode] チェックボックス **IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。**

[IP Address] フィールド 使用する静的 IP アドレスを入力します。

[Netmask] フィールド 前のフィールドに指定したIPアドレスのネットマスクを入力します。

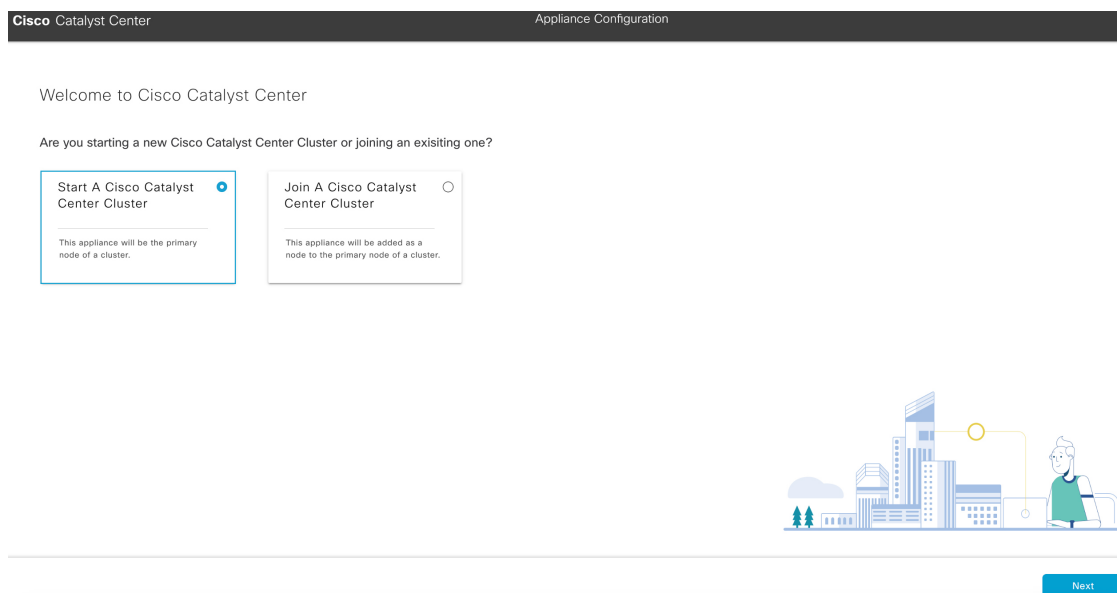
- **IPv4** アドレスを入力した場合は、ネットマスクまたは **CIDR** アドレスのいずれかを入力できます。
- **IPv6** アドレスを入力した場合は、**CIDR** アドレスのみを入力できます。

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

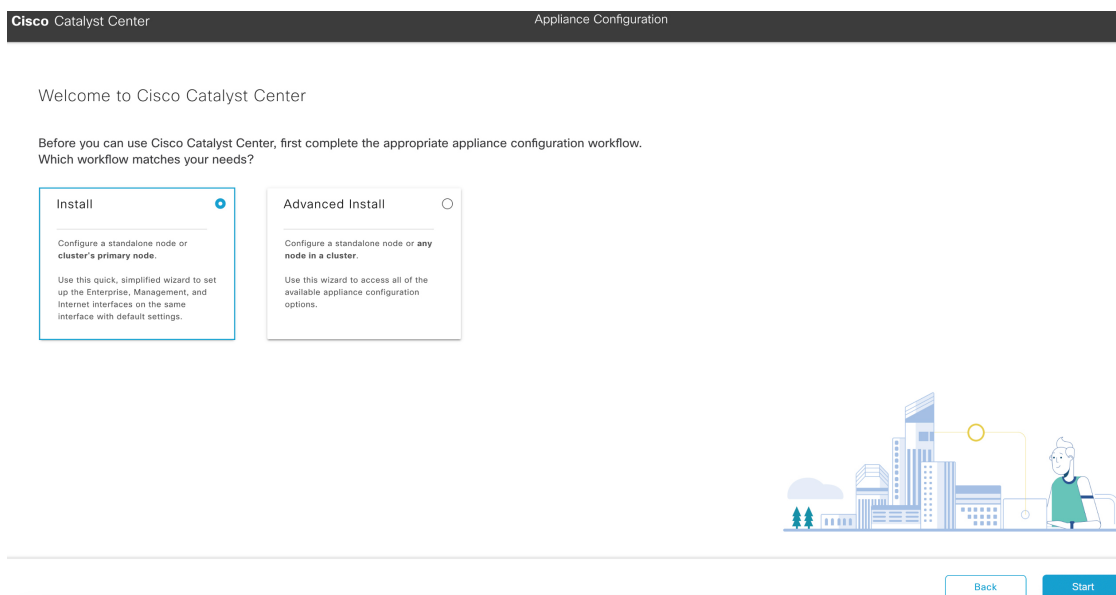
KVM コンソールに **Maglev** 構成ウィザードのウェルカムページが表示されます。



- e) **[Appliance Configuration]** ウィンドウを表示するには、**[Static IP Configuration]** ウィンドウに表示された URL を開きます。

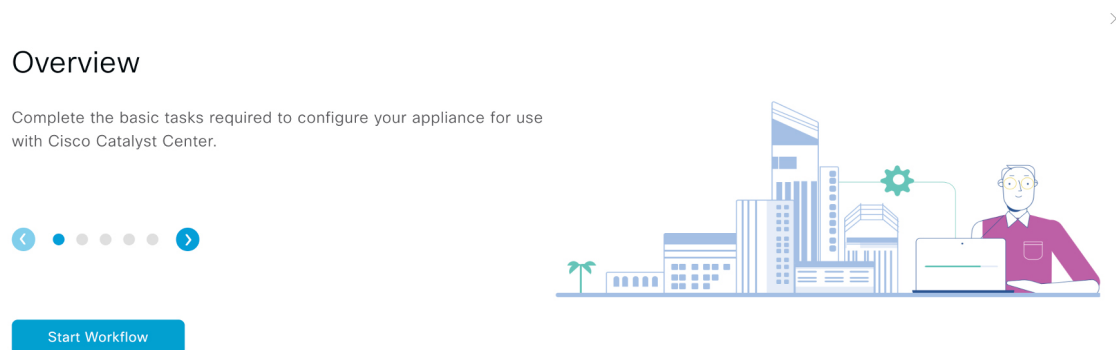


- f) **[Start a Cisco Catalyst Center Cluster]** オプションボタンをクリックし、**[Next]** をクリックします。



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

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



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

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

Cisco Catalyst Center
Install

Appliance Interface Overview

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

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

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

Exit
Next

このウィザードは、**Catalyst Center** 機能に必要なエンタープライズポートとクラスタ内ポートの設定に役立ちます。ウィザードの次のページにこれらのポートのいずれかまたは両方が表示されない場合、表示されないポートは機能していないか、無効になっている可能性があります。ポートが機能していないことが判明した場合には、**[Exit]** を選択してウィザードをすぐに終了します。設定を再開したり、**Cisco Technical Assistance Center (TAC)** に連絡したりする前に、[事前設定タスクの実行](#)（91 ページ）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。

2. インストール構成ウィザードを完了します。

a) **[Next]** をクリックします。

[Configure The Enterprise Port] ページが開きます。

Cisco Catalyst Center
Install

Configure the Enterprise Port

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

Enterprise & Management Network & Internet Access Interface

LACP Mode: Disabled

IP Address: 22

Netmask: 24

Default Gateway: 12

Static Routes: 2

DNS: 71

Enter an IPv4 address

Intracuster Link Interface

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169

Subnet Mask: 255

Exit
Next

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

ネットワークがファイアウォールの背後にある場合は、次のタスクを実行します。

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

b) **[DNS]** フィールドに、優先 DNS サーバーの IP アドレスを入力します。

追加の DNS サーバーを入力するには、**[Add]** (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大3つのDNSサーバーを設定します。アプライアンスに対して3つを超えるDNSサーバを設定すると、問題が発生する可能性があります。
- NTP の場合、**Catalyst Center** と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

c) **[Next]** をクリックします。

d) プロンプトが表示されたら、**[Yes]** をクリックして、クラスター内インターフェイスの IP アドレスとサブネットマスクをコピーします。

Did you save the Intracluster Link interface's information?

[Download](#) the **Intracluster Link interface's IP address** and **Subnet Mask**. You will need them to set up the other nodes in your cluster.

No

Yes

この情報は、クラスターのセカンダリノードを設定するときに必要になります。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Interface to Port Configuration]** ページが開きます。

Interface to Port Configuration

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

Enterprise & Management Network & Internet Access Interface

- LACP Mode: Disabled
- IP Address: 22
- Netmask: 24
- Default Gateway: 12
- Static Routes: 2
- DNS: 71

Intracluster Link Interface

- Interface Name: cluster
- LACP Mode: Disabled
- IP Address: 169
- Subnet Mask: 255

Exit Next

e) **[Next]** をクリックします。

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

[Configure Proxy Server Information] ページが開きます。

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

32 :

[Proxy Server]
フィールド

インターネットにアクセスする **HTTPS** ネットワークプロキシの **URL** またはホスト名を入力します。



注

Catalyst Center から **HTTPS** プロキシへの接続は、このリリースの **HTTP** 経由のみでサポートされます。

[Port] フィールド

アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

[Username] フィールド

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

[Password] フィールド

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

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

- i) クラスタの構成値を入力し、**[Next]** をクリックします。

33 : [Advanced Appliance Settings]

[Cluster virtual IP addresses]

[Enterprise Network] および **[For Intracluster Access]** フィールドからアクセスする場合

アプライアンスのクラスタとエンタープライズおよびクラスタ内インターフェイス間のトラフィックに使用される仮想 IP アドレスを入力します。このアドレスは、将来 3 ノードクラスタに変換されるシングルノードクラスタに対して入力する必要があります。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。

重要

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

[Fully Qualified Domain Name (FQDN)] フィールド

クラスターの完全修飾ドメイン名 (FQDN) を入力します。Catalyst 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、Catalyst 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。
- Catalyst Center 証明書の **[Subject Alternative Name (SAN)]** フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイ サーバが定義されます。

CLI クレデンシャル

maglev ユーザーのパスワードを入力して確認します。

重要

このパスワードが [パスワード要件 \(73ページ\)](#) に準拠していることを確認してください。

[NTP server settings]

[NTP Server] フィールド

少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。

[Turn On NTP Authentication] チェックボックス

NTP サーバーが同期する前に Catalyst Center NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 (2³²-1) です。

この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。

- NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

[Subnet settings]

[Container Subnet] フィールド

内部サービスを管理するために Catalyst Center で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.32.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

[Cluster Subnet] フィールド

内部クラスタサービスを管理するために Catalyst Center で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.48.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

ウィザードは入力した情報を検証し、ウィザードを続行する前に変更が必要な設定を通知します。入力した設定が有効な場合、ウィザードの [Summary] ページが開きます。

Cisco Catalyst Center Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. [Download the generated configuration in JSON format here](#), this will be important for future reference. When you are happy with your settings, click Start Configuration.

Enterprise Port [Edit](#)

Enterprise & Management Network & Internet Access Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22
Netmask	24
Default Gateway	12
Static Routes	2
DNS Servers	71

Intracluster Link Interface

Interface Name	cluster
LACP Mode	Disabled
IP Address	169
Subnet Mask	255

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

- j) ページの下部までスクロールし、ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な **Edit** リンクをクリックして、更新を行うウィザードページを開きます。

注

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

- k) Catalyst Center アプライアンスの設定を完了するには、[Start Configuration] をクリックします。

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

Cisco Catalyst Center Install

Appliance Configuration In Progress

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

Initializing the cluster using kubeadm 50%

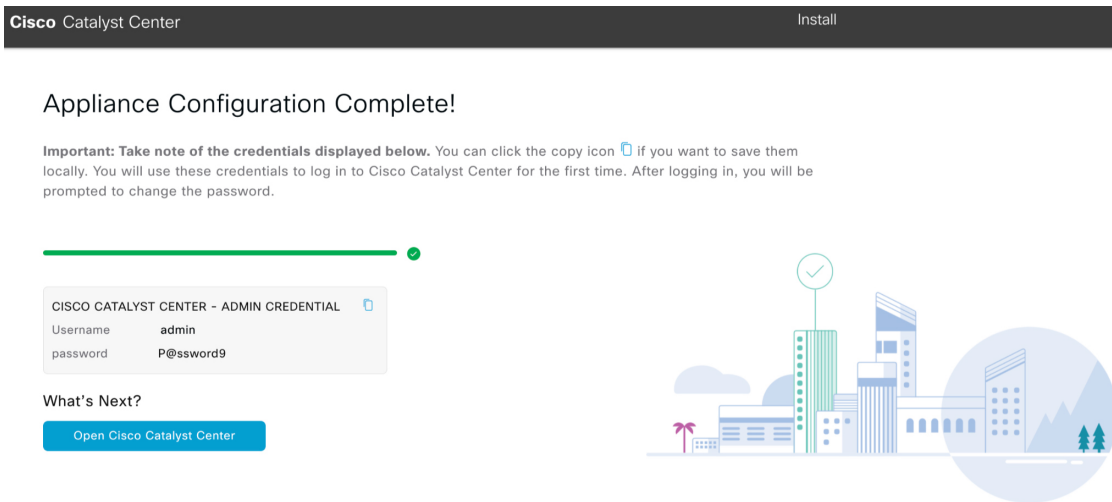
Started: 04/09/2020 12:15:36

[Download](#)

```

Apr 11 17:40:20 2020 GMT
2024-03-22T16:04:38.088Z13 | front-proxy-client.crt Apr 13 17:40:20 2020
GMT Apr 13 17:40:20 2021 GMT
2024-03-22T16:04:38.088Z14 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z15 | admin.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z16 | scheduler.conf Apr 13 12:12:14 2020 GMT
Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z17 | controller-manager.conf Apr 13 12:12:14
2020 GMT Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z18 | -----
  
```

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



インストール構成ウィザードを完了すると、**Catalyst Center** はパスワード「**P@ssword9**」を自動的に設定します。初回はこのパスワードを使用して **Catalyst Center** にログインします。

注

セキュリティ対策として、ログイン後にこのパスワードを変更するよう求められます。詳細については、[Catalyst Center への初回ログイン \(256ページ\)](#) を参照してください。

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 \(256ページ\)](#)」）を実行して続行します。

詳細インストール構成ウィザードを使用して、クラスタ内の最初のアプライアンスを設定できます。

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、またはクラスターの一部として運用するかにかかわらず、常にプライマリノードとして設定する必要があります。

すでにプライマリノードがある既存のクラスタのセカンダリノードとしてインストールされたアプライアンスを設定する場合には、代わりに[詳細インストール構成ウィザードを使用したセカンダリノードの設定 \(186ページ\)](#) の手順を実行します。

最初にインストールされたアプライアンスをプライマリノードとして設定するには、詳細インストール構成ウィザードを使用します。

重要

- 次の第 3 世代 **Catalyst Center** アプライアンスは、このウィザードを使用した設定をサポートしています。
 - 32 コアアプライアンス：シスコ部品番号 DN3-HW-APL
 - 56 コアアプライアンス：シスコ部品番号 DN3-HW-APL-L
- このウィザードは、新しい **Catalyst Center** アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、**Maglev** 設定ウィザードを使用する必要があります (**Maglev ウィザードを使用したアプライアンスの設定** (105 ページ) を参照)。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。そうしないと、クラスタのアプライアンスを設定し、**Catalyst Center** に初めてログインした後に、クイック スタート ワークフロー (ネットワークのデバイスを検出してテレメトリを有効にする) が開始されません。
- この手順の実行中に入力する IP アドレスが有効なネットマスクを持つ有効なアドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

次のことを確認します。

- 必要な **IP アドレスおよびサブネット** (44 ページ) と **必須の設定情報** (70 ページ) で必要な情報がすべて収集されたこと。
- 「**アプライアンスのインストール ワークフロー** (76 ページ)」の説明に従って、1 番目のアプライアンスを設置したこと。
- 「**Cisco Integrated Management Controller に対するブラウザアクセスの有効化** (86 ページ)」の説明に従って、プライマリノードで **Cisco IMC** に対するブラウザのアクセス権が設定されたこと。
- 「**事前設定タスクの実行** (91 ページ)」の説明に従って、プライマリノードのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- **Cisco IMC**、**Catalyst Center** との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている **Catalyst Center** のバージョンに対応する **リリースノート** を参照してください。
- 次の手順で指定するデフォルトゲートウェイおよび **DNS** サーバーと **Catalyst Center** の間のファイアウォールで **ICMP** が許容されること。ウィザードでは、ユーザの指定する **DNS** サーバを **ping** で確認します。ファイアウォールが配置されており、そのファイアウォールで **ICMP** が許容されていない場合、この **ping** がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. 詳細インストール構成ウィザードを起動します。

- お使いのブラウザで、実行した **Cisco IMC GUI** 設定で設定した **Cisco IMC** の IP アドレスを指定してから、**Cisco IMC** ユーザーとして **Cisco IMC GUI** にログインします (**Cisco Integrated Management Controller に対するブラウザアクセスの有効化** (86 ページ) を参照)。
ログインが成功すると、アプライアンスに **[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。
- 青いリンクメニューで **[Launch KVM]** を選択してから **[HTML based KVM]** を選択します。

KVM コンソールが別のブラウザウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、**Maglev** 構成ウィザードのプロンプトに応答します。

c) KVM が表示されたら、次のいずれかを選択してアプライアンスをリポートします。

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

アプライアンスをリ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、KVM コンソールに **[Static IP Configuration]** 画面が表示されます。

STEP #None	STATIC IP CONFIGURATION
Welcome to the Maglev Configuration Wizard! Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration. - Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface - Click Skip to move to config wizard NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration	IPv6 mode IP Address: Netmask: Default Gateway Address: Static Routes: Web installation: https://10. :9004/
	< cancel > skip >> configure >>

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

d) 次のいずれか 1 つのタスクを実行します。

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

 注

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

- [IPv6 Mode]** チェックボックス **IPv6** アドレスを設定する場合は、このチェックボックスをオンにします。
- [IP Address]** フィールド 使用する静的 **IP** アドレスを入力します。
- [Netmask]** フィールド 前のフィールドに指定した **IP** アドレスのネットマスクを入力します。
- **IPv4** アドレスを入力した場合は、ネットマスクまたは **CIDR** アドレスのいずれかを入力できます。
 - **IPv6** アドレスを入力した場合は、**CIDR** アドレスのみを入力できます。
- [Default Gateway Address]** フィールド トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。
- [Static Routes]** フィールド 1 つ以上のスタティックルートスペースで区切り、<ネットワーク>/<ネットマスク>/<ゲートウェイ> の形式で入力します。これは通常、管理ポートでのみ必要です。

KVM コンソールに **Maglev** 構成ウィザードのウェルカム画面が表示されます。

```
Welcome to the Maglev Configuration Wizard!

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

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

< exit >
```

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

Cisco Catalyst Center Appliance Configuration

Welcome to Cisco Catalyst Center

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

Start A Cisco Catalyst Center Cluster ☒

This appliance will be the primary node of a cluster.

Join A Cisco Catalyst Center Cluster ☐

This appliance will be added as a node to the primary node of a cluster.



Next

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

Cisco Catalyst Center Appliance Configuration

Welcome to Cisco Catalyst Center

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

Install ☐

Configure a standalone node or cluster's primary node.

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

Advanced Install ☒

Configure a standalone node or any node in a cluster.

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



Back Start

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

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

Overview

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

< ● ● ● ● ● >

Start Workflow



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

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

Cisco Catalyst Center
Advanced Install

Appliance Interface Overview

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

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

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

Exit
Next

重要

Catalyst Center の機能に必要なため、少なくともアプライアンスのエンタープライズポートおよびクラスターポートにインターフェイスを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか 1 つまたは両方が表示されない場合、表示されないポートは機能しないか無効になっている可能性があります。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザードをすぐに終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に、[事前設定タスクの実行](#) (91ページ) に記載されている手順が完了していることを確認してください。

2. 詳細インストール構成ウィザードを完了します。

a) [Next] をクリックします。

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

Cisco Catalyst Center
Advanced Install

How would you like to set up your appliance interfaces?

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

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

Would you like to have a dedicated Management Network Interface?

☒ Yes ☐ No

Would you like to have a dedicated Internet Access Interface?

☒ Yes ☐ No

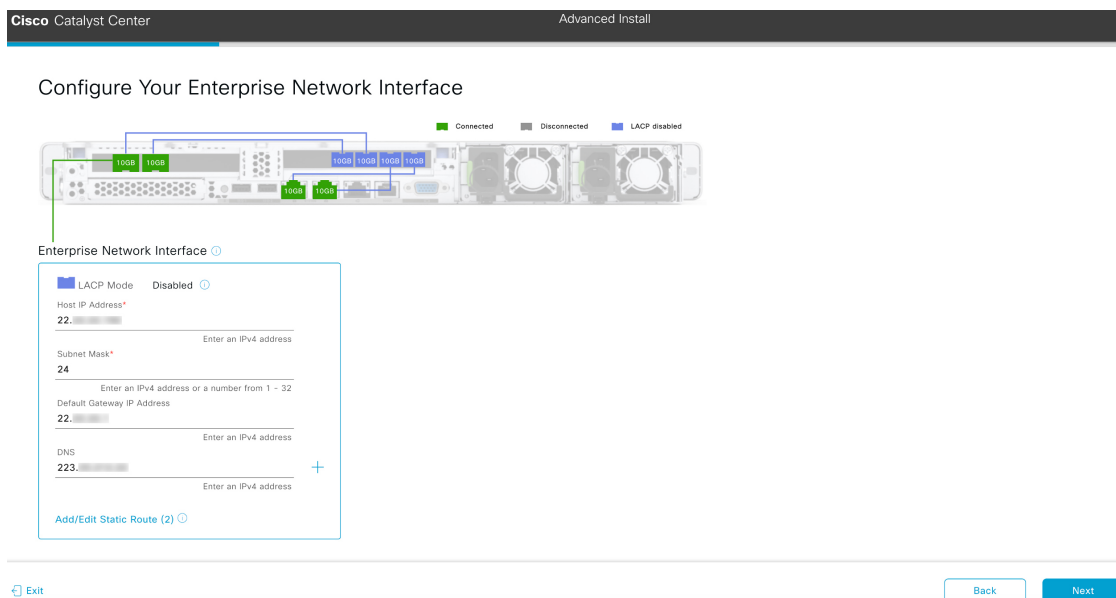
Exit
Back
Next

ネットワークがファイアウォールの背後にある場合は、次のタスクを実行します。

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

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

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



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

[インターフェースケーブル接続 \(40ページ\)](#) で説明されているとおり、このインターフェイスは、アプライアンスをエンタープライズネットワークにリンクするために必要なインターフェイスです。入力する必要がある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と[必須の設定情報 \(70ページ\)](#) を参照してください。

34 :

[LACP Mode] スライド

エンタープライズ インターフェイスに対して、次のネットワーク インターフェイス コントローラ (NIC) ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、**2つのイーサネット インターフェイスを 1つの論理チャネルに集約すること**で、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデブレックス設定を共有する **2つのイーサネット インターフェイスが 1つの論理チャネルに集約されます**。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要 \(94ページ\)](#) を参照してください。

[Host IP Address] フィールド	エンタープライズ インターフェイスの IP アドレスを入力します。これは必須です。
[Subnet Mask] フィールド	インターフェイスの 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。
[Default Gateway IP Address] フィールド	インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

デフォルトゲートウェイ：少なくとも 1 つのインターフェイスの IP アドレスを入力します。そうしないと、構成ウィザードを完了できません。

 注

このインターフェイスは、DHCP サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。

1. このフィールドに現在一覧表示されている IP アドレスを削除し、[Exit] をクリックします。
この操作でウィザードの最初の画面に戻ります。
2. エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ IP アドレスを入力します。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

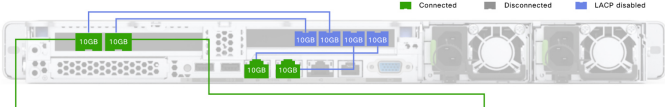
重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバーを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、Catalyst Center と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

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

Cisco Catalyst Center
Advanced Install

Configure Your Intracluster Interface



Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22.
Subnet Mask	24
Default Gateway	22.
DNS Servers	223.
Static Routes	2

Intracluster Link Network

LACP Mode Disabled

Host IP Address* 169.

Enter an IPv4 address

Subnet Mask* 255.

Enter an IPv4 address or a number from 1 - 32

[Exit](#)

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

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

[インターフェイスケーブル接続 \(40ページ\)](#) で説明されているとおり、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要がある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と [必須の設定情報 \(70ページ\)](#) を参照してください。

 注

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

35 :

[LACP Mode] スライダー

クラスター内インターフェイスに対して、次の NIC ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、2つのイーサネットインターフェイスを 1つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデブレッक्स設定を共有する 2つのイーサネットインターフェイスが 1つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

重要

アプライアンスのクラスター内インターフェイスで **LACP** モードを有効にする場合は、今すぐ有効にします。このウィザードを完了すると、次は実行できなくなります。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#)（94ページ）を参照してください。

[Host IP Address] フィールド

クラスター内インターフェイスの IP アドレスを入力します。これは必須です。

 注

クラスター内インターフェイス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。

[Subnet Mask] フィールド

インターフェイスの 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。

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

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

インターフェースケーブル接続 (40ページ) で説明されているとおり、このポートは管理ネットワークから **Catalyst Center GUI** にアクセスするために使用されます。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要がある値の詳細な説明については、**必要な IP アドレスおよびサブネット** (44ページ) と **必須の設定情報** (70ページ) を参照してください)。

注

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

36 :

[Host IP Address] フィールド 管理インターフェイスの **IP アドレス**を入力します。

[Subnet Mask] フィールド インターフェイスの **IP アドレス**に対応するネットマスクを入力します。

[Default Gateway IP Address] フィールド インターフェイスに使用するデフォルトゲートウェイ **IP アドレス**を入力します。

重要

アプライアンスの少なくとも **1** つのインターフェイスに対してデフォルトゲートウェイ **IP アドレス**を入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、**[Add]** (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 **3** つの DNS サーバを設定します。アプライアンスに対して **3** つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- **NTP** の場合、**Catalyst Center** と **NTP** サーバの間のポート **123** (**UDP**) が開いていることを確認します。

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

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

インターフェイスクーブル接続 (40ページ) で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。専用インターネットアクセスインターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要のある値の詳細な説明については、**必要な IP アドレスおよびサブネット (44ページ)** と **必須の設定情報 (70ページ)** を参照してください)。

37 :

[Host IP Address] フィールド

インターネットアクセスインターフェイスの IP アドレスを入力します。

[Subnet Mask] フィールド

インターフェイスの IP アドレスに対応するネットマスクを入力します。この操作は、前のフィールドに IP アドレスを入力する場合に必要になります。

[Default Gateway IP Address]
フィールド

インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、**[Add]** (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、**Catalyst Center** と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

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

Cisco Catalyst Center Advanced Install

Interface to Port Configuration

We are going to configure the following interfaces. Clicking Next will begin the configuration process. This may take up to a minute to configure.

Enterprise Network Interface

Interface Name: enterprise

LACP Mode: Disabled

IP Address: 22

Subnet Mask: 24

Default Gateway: 22

DNS Servers: 223

Static Routes: 2

[Edit](#)

Internet Network Interface

Interface Name: internet

IP Address: 212

Subnet Mask: 255

[Edit](#)

Intracluster Link Network

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169

Subnet Mask: 255

Static Routes: 2

[Edit](#)

Management Network Interface

Interface Name: management

IP Address: 123

Subnet Mask: 255

[Edit](#)

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

g) プライマリノードのインターフェイスに入力した設定を確認します。

変更が必要な場合は、該当するインターフェイスの **[Edit]** リンクをクリックします。

h) インターフェイスの設定に問題がなければ、**[Next]** をクリックします。

初期インターフェイス設定が完了すると、**[Configure Proxy Server Information]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Configure Proxy Server Information

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

☒ Yes ☐ No

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

Port* Enter port number between 1 to 65535.

Username

Password

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

i) 次のいずれかのタスクを実行してから、**[Next]** をクリックします。

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

38 :

[Proxy Server] フィールド

インターネットにアクセスする **HTTPS** ネットワークプロキシの **URL** またはホスト名を入力します。



注

Catalyst Center から **HTTPS** プロキシへの接続は、このリリースの **HTTP** 経由のみでサポートされます。

[Port] フィールド

アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

[Username] フィールド

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

[Password] フィールド

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

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

- j) クラスターの構成値を入力し、**[Next]** をクリックします。

39 : [Advanced Appliance Settings]

[Cluster virtual IP addresses]

[To access from Enterprise Network]、[For Intracuster Access]、[To access from Management Network]、および [For Internet Access] フィールド

注

エンタープライズインターフェイスと同じポートで管理インターフェイスまたはインターネットアクセスインターフェイスを設定した場合、対応するフィールドはこのセクションに表示されません。

プライマリノードに設定したクラスタとインターフェイス間のトラフィックに使用される仮想IPアドレスを入力します。この操作は、3 ノードクラスタと、将来3 ノードクラスタに変換されるシングルノードクラスタの両方の場合に必要です。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。

重要

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

[Fully Qualified Domain Name (FQDN)] フィールド

クラスターの完全修飾ドメイン名 (FQDN) を入力します。Catalyst 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、Catalyst 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。
- Catalyst Center 証明書の [Subject Alternative Name (SAN)] フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイ サーバが定義されます。

CLI クレデンシャル

maglev ユーザーのパスワードを入力して確認します。

重要

このパスワードが [パスワード要件](#) (73ページ) に準拠していることを確認してください。

Cisco Catalyst Center 管理者ログイン情報

スーパーユーザ権限を持つ管理者のデフォルトのパスワードを入力します。このパスワードは **Catalyst Center** に初めてログインするときに使用します。

重要

このパスワードが [パスワード要件](#) (73ページ) に準拠していることを確認してください。

[NTP server settings]

[NTP Server] フィールド

少なくとも 1 つの **NTP** サーバーアドレスまたはホスト名を入力します。追加の **NTP** サーバーアドレスまたはホスト名を入力するには、**[Add]** (+) アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の **NTP** サーバを設定するようお勧めします。

[Turn On NTP Authentication] チェックボックス

NTP サーバーが同期する前に **Catalyst Center** **NTP** サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- **NTP** サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 (2³²-1) です。

この値は、**NTP** サーバーのキーファイルで定義されているキー ID に対応します。

- **NTP** サーバーのキー ID に関連付けられた **SHA-1** キー値。この 40 文字の 16 進文字列は、**NTP** サーバーのキーファイルにあります。

注

前のフィールドで構成した各 **NTP** サーバーのキー ID とキー値を入力してください。

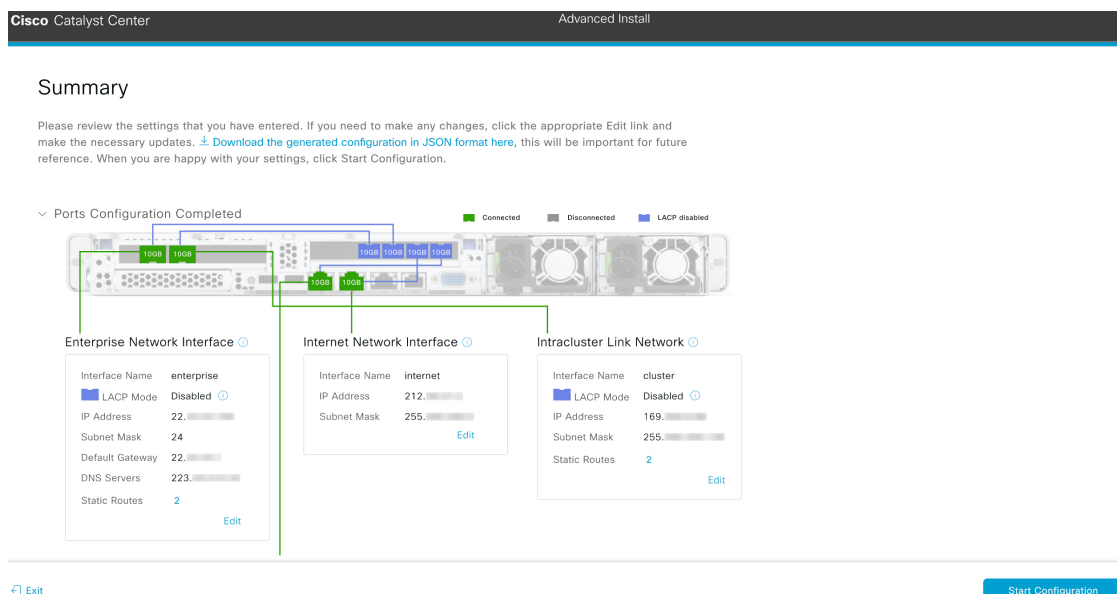
[Subnet settings]

[Container Subnet] フィールド

内部サービスを管理するために **Catalyst Center** で使用する、ルーティングされない専用の **IP** サブネット。デフォルトでは、これは **169.254.32.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

[Cluster Subnet] フィールド 内部クラスタサービスを管理するために **Catalyst Center** で使用する、ルーティングされない専用の **IP サブネット**。デフォルトでは、これは **169.254.48.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

入力した情報がウィザードで検証されます。また、ウィザードを続行する前に、変更が必要な設定についても通知されます。入力した設定が有効な場合、ウィザードの **[Summary]** 画面が開きます。



 注

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

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

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

Appliance Configuration In Progress

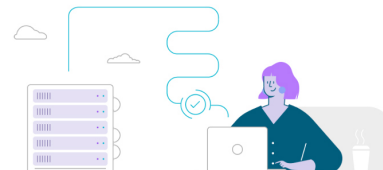
It should take about 30 minutes to configure the appliance. Do not press your browser's back button or refresh this page. The page will update after configuration completes.

Initializing the cluster using kubeadm 50%

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

[Download](#)

```
Apr 11 17:40:20 2020 GMT
2024-03-22T16:04:38.088Z13 | front-proxy-client.crt Apr 13 17:40:20 2020
GMT Apr 13 17:40:20 2021 GMT
2024-03-22T16:04:38.088Z14 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z15 | admin.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z16 | scheduler.conf Apr 13 12:12:14 2020 GMT
Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z17 | controller-manager.conf Apr 13 12:12:14
2020 GMT Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z18 | -----
-----
```



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](#)（256ページ）」）を実行して続行します。
- アプライアンスをクラスタ内のプライマリノードとして展開する場合には、クラスタ内の 2 番目と 3 番目のインストール済みアプライアンスを設定します（[詳細インストール構成ウィザードを使用したセカンドリノードの設定](#)（186ページ））。

詳細インストール構成ウィザードを使用して、クラスタに付加的なノードを追加できます。

詳細インストール構成ウィザードを使用して、クラスター内の 2 番目と 3 番目のノードを設定するには、次の手順を実行します。

重要

- 3 ノードクラスタを構築するには、同じバージョンのシステムパッケージが 3 つの Catalyst Center アプライアンスにインストールされている必要があります。この条件が整わない場合、予期しない動作とダウンタイムの可能性が生じることがあります。
- 次の第 3 世代 Catalyst Center アプライアンスでは、詳細インストール構成ウィザードを使用した設定がサポートされています。
 - 32 コアアプライアンス：シスコ部品番号 DN3-HW-APL
 - 56 コアアプライアンス：シスコ部品番号 DN3-HW-APL-L

- このウィザードは、新しい **Catalyst Center** アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、**Maglev** 設定ウィザードを使用する必要があります (**Maglev** ウィザードを使用したアプライアンスの設定 (105ページ) を参照)。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、**Catalyst Center** に初めてログインした後に、(ネットワークのデバイスを検出してテレメトリを有効にするために完了する) クイック スタート ワークフローが開始されません。
- この手順で、有効な IP アドレスとネットマスクを入力してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

新しいセカンダリノードをクラスタに結合する場合には、クラスタ内の最初のアプライアンスをプライマリノードとして指定する必要があります。セカンダリノードをクラスタに参加させる際には、次の情報を考慮してください。

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

```
maglev-1 [main - https://kong-:443]
```

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

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

- 一度に 1 つのノードのみをクラスタに結合してください。複数のノードを同時に追加しないでください。同時に追加しようとすると予期しない動作が発生します。
- 各セカンダリノードのクラスタ接続プロセス中に、一部のサービスのダウンタイムが発生することが予想されます。サービスはすべてのノードに再配布される必要があり、そのプロセスの間、クラスタはダウンします。

次のことを確認します。

- 詳細インストール構成ウィザードを使用したプライマリノードの設定 (169ページ) の手順に従って、クラスター内の最初のアプライアンスが設定されたこと。
- 必要な IP アドレスおよびサブネット (44ページ) と 必須の設定情報 (70ページ) で必要な情報がすべて収集されたこと。
- 「アプライアンスのインストール ワークフロー (76ページ)」の説明に従って、2 番目と 3 番目のアプライアンスを設置したこと。
- 次のタスクを完了しました。
 1. 最初のアプライアンスで **maglev package status** コマンドを実行したこと。
 Catalyst Center GUIからもこの情報にアクセスできます。[Help] アイコン (🔍) をクリックし、[About] > [Packages] の順に選択してください。
 2. Cisco TAC に連絡し、このコマンドの出力を提供して 2 番目と 3 番目のアプライアンスにインストールする必要がある ISO をポイントするよう依頼したこと。
- 「Cisco Integrated Management Controller に対するブラウザアクセスの有効化 (86ページ)」の説明に従って、両方のセカンダリノードで Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 事前設定タスクの実行 (91ページ) の説明に従って、セカンダリノードのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- 互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている Catalyst Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次のトピックの手順で指定するデフォルトゲートウェイおよび DNS サーバーと Catalyst Center の間のファイアウォールで ICMP が許容されること。ウィザードでは、ユーザの指定する DNS サーバを ping で確認します。ファイアウォールが配置されており、そのファイアウォールで ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. 詳細インストール構成ウィザードを起動します。

- a) お使いのブラウザで、実行した Cisco IMC GUI 設定で設定した Cisco IMC の IP アドレスをポイントしてから、Cisco IMC ユーザーとして Cisco IMC GUI にログインします ([Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(86ページ\)](#) を参照)。
 ログインが成功すると、アプライアンスに [Cisco Integrated Management Controller Chassis Summary] ウィンドウが右上の青いリンクメニューとともに表示されます。
- b) 青いリンクメニューで [Launch KVM] を選択してから [HTML based KVM] を選択します。
 KVM コンソールが別のブラウザウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、Maglev 構成ウィザードのプロンプトに応答します。
- c) KVM が表示されたら、次のいずれかを選択してアプライアンスをリブートします。
 - メインの Cisco IMC GUI ブラウザウィンドウで、[Host Power] > [Power Cycle] を選択します。その後、KVM コンソールに切り替えて続行します。
 - KVM コンソールで、[Power] > [Power Cycle System (cold boot)] を選択します。

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

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

STEP #None	STATIC IP CONFIGURATION
Welcome to the Maglev Configuration Wizard! Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration. - Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface - Click Skip to move to config wizard NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration	IPv6 mode IP Address: Netmask: Default Gateway Address: Static Routes: Web installation: https://10. :9004/ < cancel > skip >> configure >>

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

d) 次のいずれか 1 つのタスクを実行します。

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

[IPv6 Mode] チェックボックス IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。

[IP Address] フィールド 使用する静的 IP アドレスを入力します。

[Netmask] フィールド 前のフィールドに指定した IP アドレスのネットマスクを入力します。

- IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。
- IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。

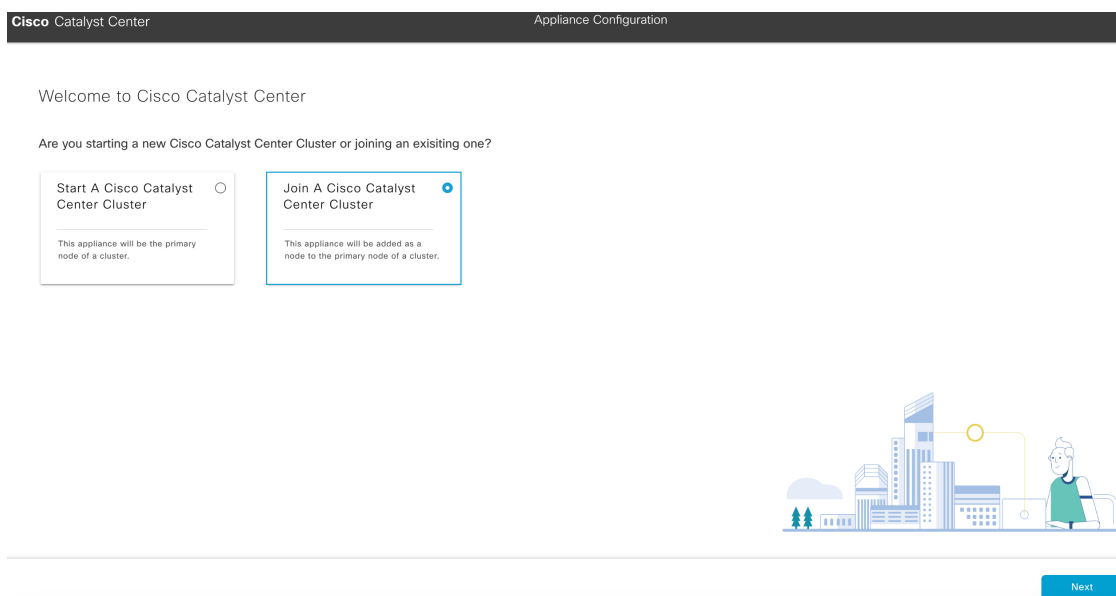
[Default Gateway Address] フィールド トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。

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

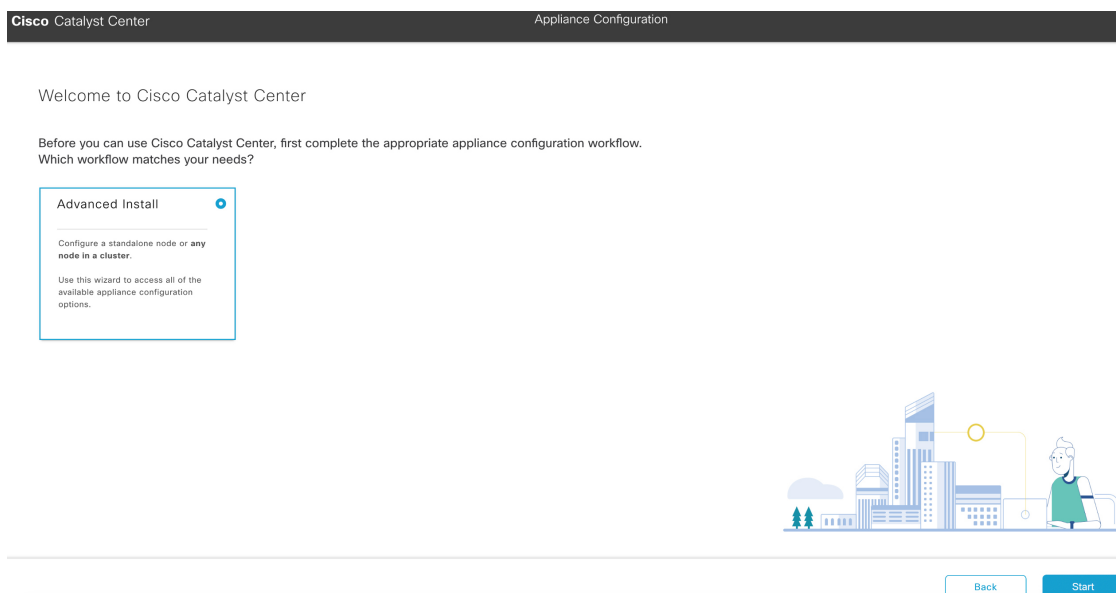
KVM コンソールに Maglev 構成ウィザードのウェルカム画面が表示されます。



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

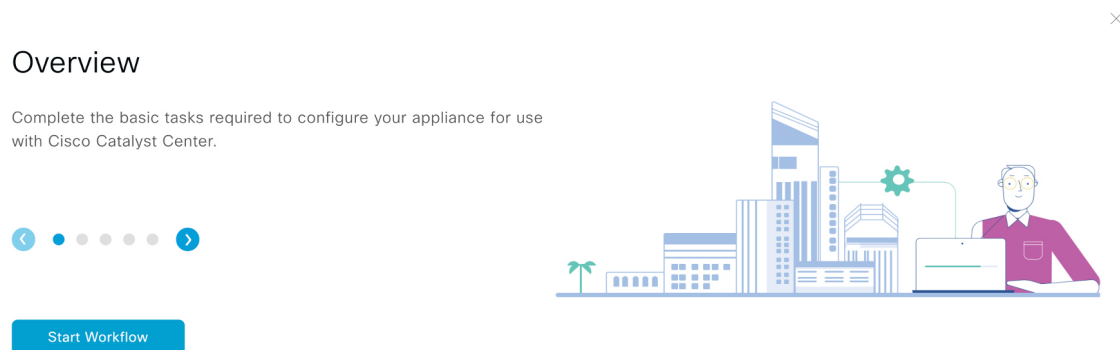


- f) [Join a Cisco Catalyst Center Cluster] オプションボタンをクリックし、[Next] をクリックします。



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

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



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

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

Appliance Interface Overview

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

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

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

[Exit](#)
[Next](#)
重要

Catalyst Center の機能に必要なため、少なくともアプライアンスのエンタープライズポートおよびクラスタポートにインターフェイスを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか 1 つまたは両方が表示されない場合、表示されないポートは機能しないか無効になっている可能性があります。ポートが機能していないことが判明した場合には、**[Exit]** を選択してウィザードをすぐに終了します。設定を再開したり、**Cisco Technical Assistance Center (TAC)** に連絡したりする前に、[事前設定タスクの実行 \(91ページ\)](#) 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。

2. 詳細インストール構成ウィザードを完了します。

a) **[Next]** をクリックします。

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

Cisco Catalyst Center
Advanced Install

How would you like to set up your appliance interfaces?

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

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

Would you like to have a dedicated Management Network Interface?

☒ Yes
☐ No

Would you like to have a dedicated Internet Access Interface?

☒ Yes
☐ No

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

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

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

Cisco Catalyst Center
Advanced Install

Configure Your Enterprise Network Interface

Enterprise Network Interface

☒ LACP Mode
 Disabled

Host IP Address*
 22.

Subnet Mask*
 24

Default Gateway IP Address
 22.

DNS
 223.

+

Add/Edit Static Route (2)

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

インターフェースケーブル接続 (40ページ) で説明されているとおり、このインターフェイスは、アプライアンスをエンタープライズネットワークにリンクするために必要なインターフェイスです。入力する必要のある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と [必須の設定情報 \(70ページ\)](#) を参照してください。

40 :

[LACP Mode] スライダ

エンタープライズインターフェイスに対して、次のネットワーク インターフェイスコントローラ (NIC) ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、**2つのイーサネットインターフェイスを1つの論理チャネルに集約すること**で、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデュプレックス設定を共有する **2つのイーサネット インターフェイスが1つの論理チャネルに集約**されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#)（94ページ）を参照してください。

[Host IP Address] フィールド

エンタープライズ インターフェイスの IP アドレスを入力します。これは必須です。

[Subnet Mask] フィールド

インターフェイスの 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。

[Default Gateway IP Address]
フィールド

インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

 注

このインターフェイスは、DHCP サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。

1. このフィールドに現在一覧表示されている IP アドレスを削除し、[Exit] をクリックします。
この操作でウィザードの最初の画面に戻ります。
2. エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ IP アドレスを入力します。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

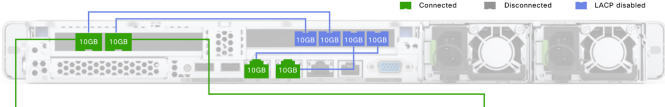
重要

- クラスタ内のノードごとに最大3台の DNS サーバーを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、Catalyst Center と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Intracluster Interface]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Configure Your Intracluster Interface



Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22.
Subnet Mask	24
Default Gateway	22.
DNS Servers	223.
Static Routes	2

Intracluster Link Network

LACP Mode	Disabled
Host IP Address*	169.
Subnet Mask*	255.

Enter an IPv4 address

Enter an IPv4 address or a number from 1 - 32

Exit Back Next

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

[インターフェイスケーブル接続 \(40ページ\)](#) で説明されているとおり、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要がある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と [必須の設定情報 \(70ページ\)](#) を参照してください。

 注

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

41 :

[LACP Mode] スライダー

クラスター内インターフェイスに対して、次の **NIC** ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、**2**つのイーサネットインターフェイスを **1**つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデブレッक्स設定を共有する **2**つのイーサネットインターフェイスが **1**つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

重要

アプライアンスのクラスター内インターフェイスで **LACP** モードを有効にする場合は、今すぐ有効にします。このウィザードを完了すると、次は実行できなくなります。

Catalyst Center の **NIC** ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#)（94ページ）を参照してください。

[Host IP Address] フィールド

クラスター内インターフェイスの **IP** アドレスを入力します。これは必須です。

 注

クラスター内インターフェイス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。

[Subnet Mask] フィールド

インターフェイスの **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。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Management Network Interface]** 画面が開きます。

- e) (任意) 管理インターフェイスの構成値を入力し、**[Next]** をクリックします。

インターフェイスクーブル接続 (40ページ) で説明されているとおり、このポートは管理ネットワークから **Catalyst Center GUI** にアクセスするために使用されます。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要がある値の詳細な説明については、**必要なIPアドレスおよびサブネット** (44ページ) と**必須の設定情報** (70ページ) を参照してください)。

注

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

42 :

[Host IP Address] フィールド 管理インターフェイスのIPアドレスを入力します。これは必須です。

[Subnet Mask] フィールド インターフェイスの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。

[Default Gateway IP Address] フィールド インターフェイスに使用するデフォルトゲートウェイIPアドレスを入力します。

重要

アプライアンスの少なくとも1つのインターフェイスに対してデフォルトゲートウェイIPアドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、[Add] (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、Catalyst Center と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Internet Access Interface]** 画面が開きます。

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

インターフェースケーブル接続 (40ページ) で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。専用インターネットアクセスインターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要のある値の詳細な説明については、**必要な IP アドレスおよびサブネット (44ページ)** と **必須の設定情報 (70ページ)** を参照してください)。

43 :

[Host IP Address] フィールド

インターネットアクセスインターフェイスの IP アドレスを入力します。

[Subnet Mask] フィールド

インターフェイスの 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。

[Default Gateway IP Address]
フィールド

インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、**[Add]** (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、**Catalyst Center** と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの**[Interface to Port Configuration]** 画面が開きます。

Interface to Port Configuration

We are going to configure the following interfaces. Clicking Next will begin the configuration process. This may take up to a minute to configure.

Connected Disconnected LACP disabled

Enterprise Network Interface

Interface Name enterprise
LACP Mode Disabled
IP Address 22
Subnet Mask 24
Default Gateway 22
DNS Servers 223
Static Routes 2

Internet Network Interface

Interface Name internet
IP Address 212
Subnet Mask 255

Intracluster Link Network

Interface Name cluster
LACP Mode Disabled
IP Address 169
Subnet Mask 255
Static Routes 2

Management Network Interface

Interface Name management
IP Address 123
Subnet Mask 255

Exit Back Next

- g) セカンダリノードのインターフェイスに入力した設定を確認します。
変更が必要な場合は、該当するインターフェイスの **[Edit]** リンクをクリックします。
- h) インターフェイスの設定に問題がなければ、**[Next]** をクリックします。
初期インターフェイス設定が完了すると、**[Configure Proxy Server Information]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Configure Proxy Server Information

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

☒ Yes ☐ No

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

Port* Enter port number between 1 to 65535.

Username

Password

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

i) 次のいずれかのタスクを実行し、**[Next]** をクリックします。

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

44 :

[Proxy Server] フィールド

インターネットにアクセスする **HTTPS** ネットワークプロキシの **URL** またはホスト名を入力します。

注

Catalyst Center から **HTTPS** プロキシへの接続は、このリリースの **HTTP** 経由のみでサポートされます。

[Port] フィールド

アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

[Username] フィールド

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

[Password] フィールド

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

ウィザードは入力した情報を検証し、ウィザードを続行する前に変更が必要な設定を通知します。入力した設定が有効な場合、ウィザードの **[Primary Node Details]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Primary Node Details

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

Primary Node IP*

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

CLI Username
maglev

CLI Password*

Enter CLI Password

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

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

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

Cisco Catalyst Center Advanced Install

Advanced Appliance Settings

CLI CREDENTIALS

Username*

maglev

Password*

[Show](#) [Obtains](#)

Confirm Password*

[Show](#)

NTP SERVER SETTINGS

NTP Server*

[Add](#)

Enter an IP address or FQDN

☐ Turn On NTP Authentication

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

- k) クラスタの構成値を入力し、**[Next]** をクリックします。

45 : [Advanced Appliance Settings]

CLI Credentials

maglev ユーザーのパスワードを入力して確認します。

重要

このパスワードが [パスワード要件](#) (73ページ) に準拠していることを確認してください。

NTP サーバー設定

[NTP Server] フィールド

少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。

[Turn On NTP Authentication] チェックボックス

NTP サーバーが同期する前に **Catalyst Center** NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。

この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。

- NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。

Cisco Catalyst Center
Advanced Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. [Download the generated configuration in JSON format here](#), this will be important for future reference. When you are happy with your settings, click Start Configuration.

▼ Ports Configuration Completed ■ Connected ■ Disconnected ■ LACP disabled



Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22
Subnet Mask	24
Default Gateway	22
DNS Servers	223
Static Routes	2

Internet Network Interface

Interface Name	internet
IP Address	212
Subnet Mask	255

Intraccluster Link Network

Interface Name	cluster
LACP Mode	Disabled
IP Address	169
Subnet Mask	255
Static Routes	2

Exit
Start Configuration

 注

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

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

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

Cisco Catalyst Center
Advanced Install

Appliance Configuration In Progress

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

50%

Initializing the cluster using kubeadm

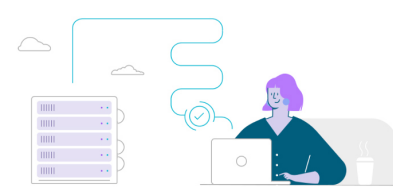
Started: 04/09/2020 12:15:36

Download

```

Apr 11 17:40:20 2020 GMT
2024-03-22T16:04:38.088Z13 | front-proxy-client.crt Apr 13 17:40:20 2020
GMT Apr 13 17:40:20 2021 GMT
2024-03-22T16:04:38.088Z14 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z15 | admin.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z16 | scheduler.conf Apr 13 12:12:14 2020 GMT
Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z17 | controller-manager.conf Apr 13 12:12:14
2020 GMT Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z18 | -----

```



タスクが完了した後：

- クラスタ内の 3 番目および最後のノードとして展開する追加のアプライアンスがある場合には、この手順を繰り返します。
- クラスタへのノードの追加が終了したら、初回セットアップを実行して続行します。 [初期設定ワークフロー](#) (256 ページ)

Catalyst Center

最新の Catalyst Center リリースにアップグレードできます。

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

:	
•	□□□□□□□□□□□□
•	□□□□□□□□□□
•	VLAN □□□□□□□□
•	□□□□□□□□□□□□□□□□□□ □□□□□□□□□□
•	□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□
•	□□□□□□□□□□□□□□□□□□ □□□□□□□□□□□□
•	□□□ Catalyst Center □□□□□□□□ □□□□□□

展開モードに応じた 80 コアアプライアンスの設定手順に関する情報。

次のいずれかのモードを使用して、80 コアアプライアンスをネットワークに展開できます。

- **スタンドアロン**：すべての機能を提供する単一のノードとして動作します。このオプションは通常、初期展開、テスト展開、小規模なネットワーク環境での使用に適しています。初回展開でスタンドアロンモードを選択すると、プライマリノードになります。

注

後でさらにアプライアンスを追加してクラスターを形成できます。

- **クラスター**：3 ノードクラスターに属するノードとして。このモードでは、ホストはすべてのサービスとデータを共有します。大規模な展開で推奨されるオプションです。初期展開でクラスターモードを選択した場合は、セカンダリノードの設定に進む前に、プライマリノードの設定を完了してください。

まず、クラスターのプライマリノードを設定します。3つのアプライアンスを設置済みで、クラスターに2番目と3番目のノードを追加する場合は、次に、セカンダリノードを設定します。

インストール構成ウィザードまたは詳細インストール構成ウィザードを使用してアプライアンスを設定する必要があるかどうかを判断するのに役立つ情報。

Catalyst Center は、アプライアンスの設定に使用できる 2 種類のブラウザベースのウィザードを提供します。説明を読んで、使用するウィザードを決定してください。

重要

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

このウィザードは、クラスター内のインターフェイスだけでなく、企業インターフェイス、管理インターフェイス、およびインターネットアクセスインターフェイスにもデフォルト値を設定し、アプライアンスの設定プロセスを合理化します。これらの各インターフェイスは、アプライアンスの企業ポートにあります。デフォルトのインターフェイス設定を使用しても問題がなく、アプライアンスを迅速に設定したい場合は、このウィザードを使用します。

 注

このウィザードではクラスターのセカンダリノードは設定できません。

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

ブラウザベースのウィザードのいずれかを使用してアプライアンスを正しく設定するには、次のタスクを完了します。

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

または、[Static IP Address Settings] ページを完了して、アプライアンスの企業インターフェイスに独自の IP アドレス、サブネットマスク、およびデフォルトゲートウェイを指定することもできます。

Catalyst Center のパスワードポリシーと要件へのポインタを提供します。

これらのトピックを参照して、Catalyst Center のパスワード実装の説明を確認してください。

- [パスワードポリシー](#) (73ページ)
- [パスワード要件](#) (73ページ)

VLAN

Catalyst Center で VLAN モードが有効になっている場合、ディザスタリカバリを使用できません。

VLAN モードについては次の詳細を考慮してください。

- VLAN モードの説明については、「」 [「Maglev ウィザードを使用したプライマリノードの設定](#) (107ページ) 」を参照してください。
- VLAN モード：
 - Maglev 設定ウィザードを使用して Catalyst Center アプライアンスを設定する場合にのみ有効にできます。

- ブラウザベースの構成ウィザードを使用して有効にすることはできません。
- アプライアンスを再イメージ化せずに無効にすることはできません。
- ディザスタリカバリは、VLAN モードが有効になっている Catalyst Center 展開ではサポートされません。

インストール構成ウィザードを使用して、3 ノードクラスターのプライマリノードまたはスタンドアロンノードを設定できます。

インストール構成ウィザードを使用して、3 ノードクラスターのプライマリノードまたはスタンドアロンノードを設定するには、次の手順を実行します。ウィザードでは、デフォルト設定を使用して同じポートでエンタープライズ、管理、およびインターネット インターフェイスを設定することで、設定プロセスが簡素化されます。第 3 世代 80 コア Catalyst Center アプライアンス（シスコ製品番号 DN3-HW-APL-XL）は、このウィザードを使用した設定をサポートします。

重要

- このウィザードを使用して、3 ノードクラスターの 2 番目または 3 番目のアプライアンスを設定することはできません。設定するには、[詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)（236 ページ）に記載されている手順を実行します。また、このウィザードを使用して、アプライアンスのエンタープライズおよびクラスター内インターフェイスで LACP モードを有効にすることはできません。
- アプライアンスを設定する前に、3 ノードクラスター内のアプライアンスからログアウトします。ログアウトしていない場合、クラスターのアプライアンスを設定し、Catalyst Center に初めてログインした後に、（ネットワークのデバイスを検出してテレメトリを有効にするために完了する）クイックスタート ワークフローが開始されません。
- この手順の実行中に入力するすべての IP アドレスが有効なネットマスクを持つ有効なアドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

このウィザードは、新しい Catalyst Center アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、[Maglev 設定ウィザード](#)を使用する必要があります（[Maglev ウィザードを使用したアプライアンスの設定](#)（105 ページ）を参照）。

次のことを確認します。

- [必要な IP アドレスおよびサブネット](#)（44 ページ）と [必須の設定情報](#)（70 ページ）で必要な情報がすべて収集されたこと。
- 「[アプライアンスのインストール ワークフロー](#)（76 ページ）」の説明に従って、1 番目のアプライアンスを設置したこと。
- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)（86 ページ）」の説明に従って、Cisco IMC に対するブラウザのアクセス権が設定されたこと。
- 「[事前設定タスクの実行](#)（91 ページ）」の説明に従って、アプライアンスのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。

- Cisco IMC、Catalyst Center との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている Catalyst Center のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順で指定する DNS サーバーと Catalyst Center の間のファイアウォールで ICMP が許容されること。このウィザードでは、ユーザの指定する DNS サーバを ping で確認します。Catalyst Center と DNS サーバの間にファイアウォールが存在し、そのファイアウォールで DNS サーバと ICMP が許容されていない場合、この ping がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. インストール構成ウィザードを起動します。

- a) お使いのブラウザで、実行した Cisco IMC GUI 設定で設定した Cisco IMC の IP アドレスをポイントしてから、Cisco IMC ユーザーとして Cisco IMC GUI にログインします ([Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(86ページ\)](#) を参照)。

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

- b) 青いリンクメニューで [Launch KVM] を選択してから [HTML based KVM] を選択します。

KVM コンソールが別のブラウザウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、Maglev 構成ウィザードのプロンプトに応答します。

- c) KVM コンソールが表示されたら、次のいずれかを選択してアプライアンスを再起動します。

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

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

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

STEP #None	STATIC IP CONFIGURATION
Welcome to the Maglev Configuration Wizard! Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration. - Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface - Click Skip to move to config wizard NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration	IPv6 mode IP Address: Netmask: Default Gateway Address: Static Routes: Web installation: https://10.10.10.10:9004/
< cancel > skip >> configure >>	

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

d) 次のいずれか 1 つのタスクを実行します。

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

 注

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

[IPv6 Mode] チェックボックス **IPv6** アドレスを設定する場合は、このチェックボックスをオンにします。

[IP Address] フィールド 使用する静的 IP アドレスを入力します。

[Netmask] フィールド 前のフィールドに指定したIPアドレスのネットマスクを入力します。

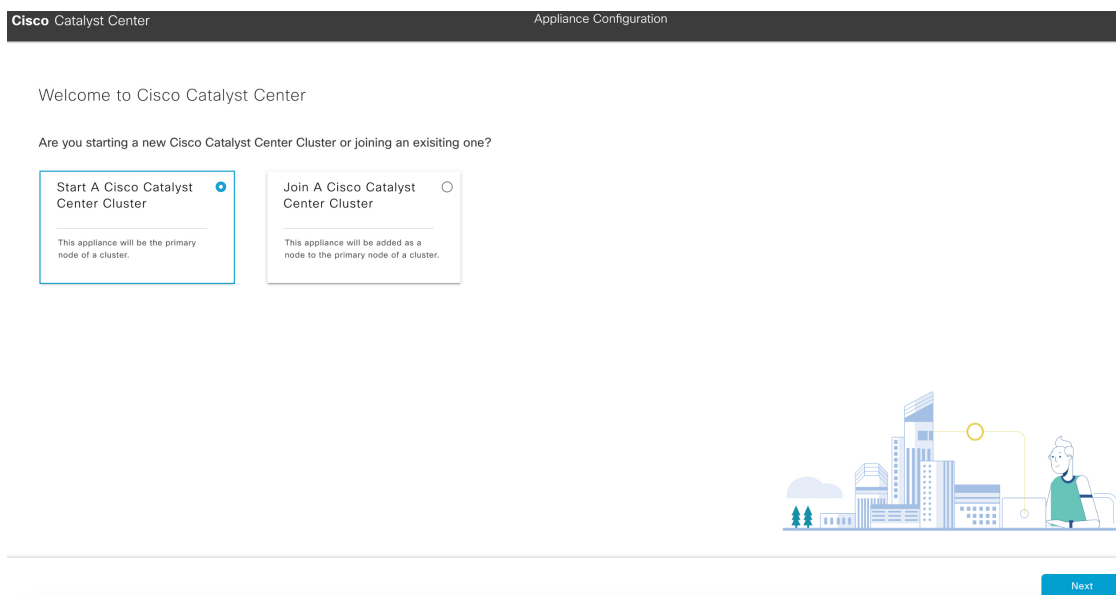
- **IPv4** アドレスを入力した場合は、ネットマスクまたは **CIDR** アドレスのいずれかを入力できます。
- **IPv6** アドレスを入力した場合は、**CIDR** アドレスのみを入力できます。

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

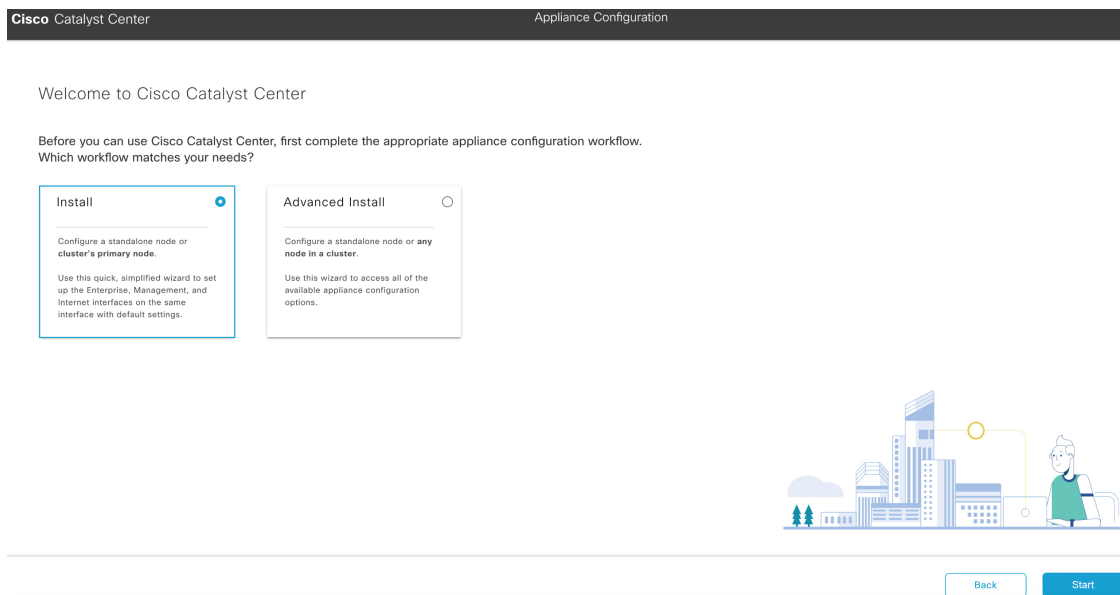
KVM コンソールに **Maglev** 構成ウィザードのウェルカム画面が表示されます。



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

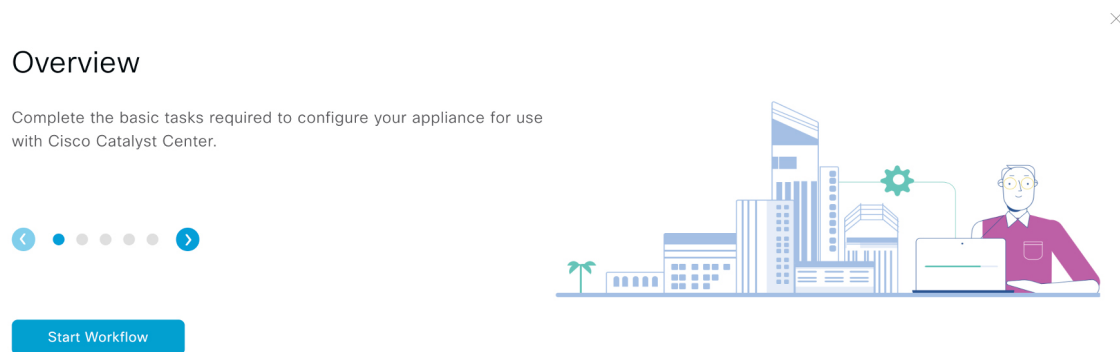


- f) **[Start a Cisco Catalyst Center Cluster]** オプションボタンをクリックし、**[Next]** をクリックします。



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

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



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

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

Cisco Catalyst Center Install

Appliance Interface Overview

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

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

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

Exit Next

このウィザードを使用すると、**Catalyst Center**機能に必要なエンタープライズポートとクラスターポートを設定できます。ウィザードの次の画面にこれらのポートのいずれかまたは両方が表示されない場合、表示されないポートは機能していないか、無効になっている可能性があります。ポートが機能していないことが判明した場合には、**[Exit]**を選択してウィザードをすぐに終了します。設定を再開したり、**Cisco Technical Assistance Center (TAC)**に連絡したりする前に、[事前設定タスクの実行](#)（91 ページ）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。

2. インストール構成ウィザードを完了します。

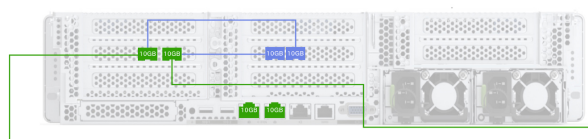
a) **[Next]** をクリックします。

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

Cisco Catalyst Center Install

Configure the Enterprise Port

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



Enterprise & Management Network & Internet Access Interface

IP Address: 22.
Netmask: 24
Default Gateway: 22.
Static Routes: 2
DNS*: 123.
Enter an IPv4 address

Intracenter Link Interface

Interface Name: cluster
IP Address: 169.
Subnet Mask: 255.

Exit Next

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

ネットワークがファイアウォールの背後にある場合は、次の手順を実行します。

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

b) **[DNS]** フィールドに、優先 DNS サーバーの IP アドレスを入力します。

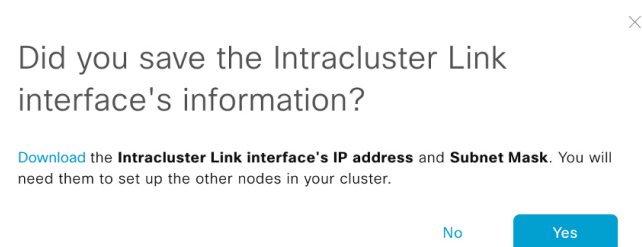
追加の DNS サーバーを入力するには、[Add] (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大**3**つの**DNS**サーバーを設定します。アプライアンスに対して**3**つを超える**DNS**サーバを設定すると、問題が発生する可能性があります。
- **NTP**の場合、**Catalyst Center**と**NTP**サーバの間のポート**123**（**UDP**）が開いていることを確認します。

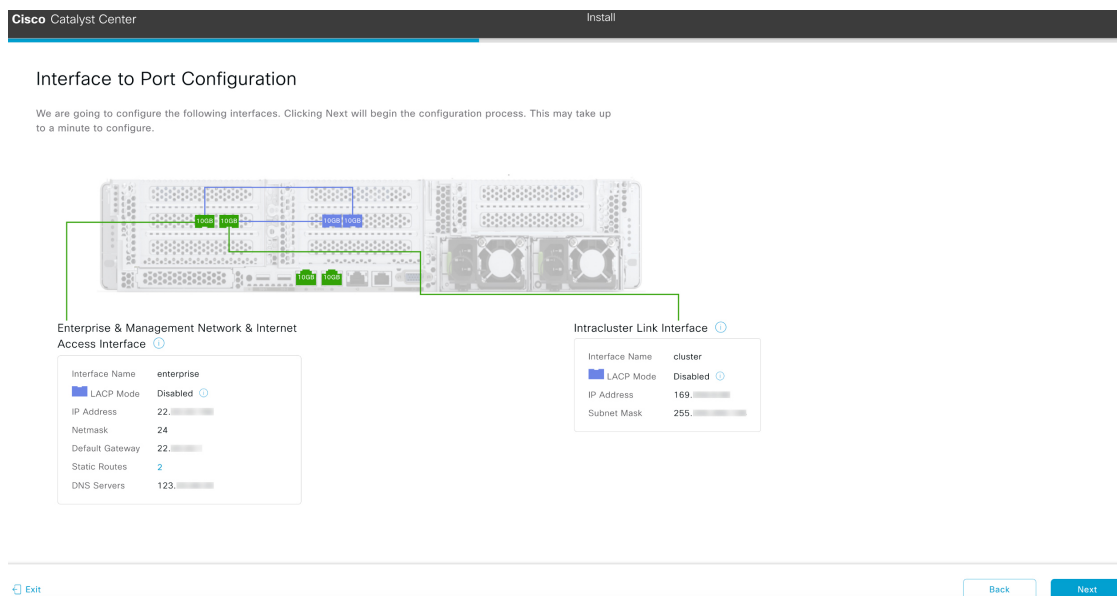
c) [Next] をクリックします。

d) プロンプトが表示されたら、**[Yes]**をクリックして、クラスター内インターフェイスのIPアドレスとサブネットマスクをコピーします。



この情報は、クラスターのセカンダリノードを設定するときに必要になります。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Interface to Port Configuration]** 画面が開きます。



e) [Next] をクリックします。

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

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

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

46 :

[Proxy Server]
フィールド

インターネットにアクセスする **HTTPS** ネットワークプロキシの **URL** またはホスト名を入力します。



注

Catalyst Center から **HTTPS** プロキシへの接続は、このリリースの **HTTP** 経由のみでサポートされます。

[Port] フィールド

アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

[Username] フィールド

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

[Password] フィールド

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

ウィザードは入力した情報を検証し、ウィザードを続行する前に変更が必要な設定を通知します。入力した設定が有効であれば、ウィザードの **[Advanced Appliance Settings]** 画面が開きます。

- i) クラスタの構成値を入力し、**[Next]** をクリックします。

47 : **[Advanced Appliance Settings]**

[Cluster virtual IP addresses]

[Enterprise Network] および **[For Intracluster Access]** フィールドからアクセスする場合

アプライアンスのクラスタとエンタープライズおよびクラスタ内インターフェイス間のトラフィックに使用される仮想 IP アドレスを入力します。このアドレスは、将来 3 ノードクラスタに変換されるシングルノードクラスタに対して入力する必要があります。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。

重要

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

[Fully Qualified Domain Name (FQDN)] フィールド

クラスターの完全修飾ドメイン名 (FQDN) を入力します。Catalyst 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、Catalyst 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。
- Catalyst Center 証明書の **[Subject Alternative Name (SAN)]** フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイ サーバが定義されます。

CLI クレデンシャル

maglev ユーザーのパスワードを入力して確認します。

重要

このパスワードが [パスワード要件 \(73ページ\)](#) に準拠していることを確認してください。

[NTP server settings]

[NTP Server] フィールド

少なくとも 1 つの NTP サーバーアドレスまたはホスト名を入力します。追加の NTP サーバーアドレスまたはホスト名を入力するには、[Add] (+) アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の NTP サーバを設定するようお勧めします。

[Turn On NTP Authentication] チェックボックス

NTP サーバーが同期する前に Catalyst Center NTP サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- NTP サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 (2³²-1) です。

この値は、NTP サーバーのキーファイルで定義されているキー ID に対応します。

- NTP サーバーのキー ID に関連付けられた SHA-1 キー値。この 40 文字の 16 進文字列は、NTP サーバーのキーファイルにあります。

注

前のフィールドで構成した各 NTP サーバーのキー ID とキー値を入力してください。

[Subnet settings]

[Container Subnet] フィールド

内部サービスを管理するために Catalyst Center で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.32.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

[Cluster Subnet] フィールド

内部クラスタサービスを管理するために Catalyst Center で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.48.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

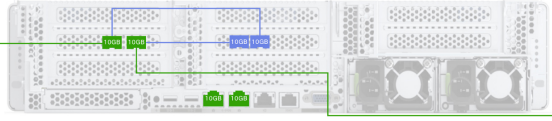
ウィザードは入力した情報を検証し、ウィザードを続行する前に変更が必要な設定を通知します。入力した設定が有効な場合、ウィザードの [Summary] 画面が開きます。

Cisco Catalyst Center Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. [Download the generated configuration in JSON format here](#), this will be important for future reference. When you are happy with your settings, click Start Configuration.

▼ Enterprise Port [Edit](#)



Enterprise & Management Network & Internet Access Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22
Netmask	24
Default Gateway	22
Static Routes	2
DNS Servers	123

Intracuster Link Interface

Interface Name	cluster
LACP Mode	Disabled
IP Address	169
Subnet Mask	255

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

- j) 画面の下部までスクロールし、ウィザードの完了時に入力したすべての設定を確認します。必要に応じて、適切な **[Edit]** リンクをクリックして、更新を行うウィザード画面を開きます。

注

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

- k) **Catalyst Center** アプライアンスの設定を完了するには、**[Start Configuration]** をクリックします。

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

Cisco Catalyst Center Install

Appliance Configuration In Progress

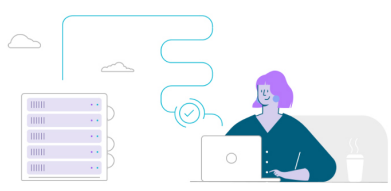
It should take about 30 minutes to configure the appliance. **Do not press your browser's back button or refresh this page.** The page will update after configuration completes.

Initializing the cluster using kubeadm 50%

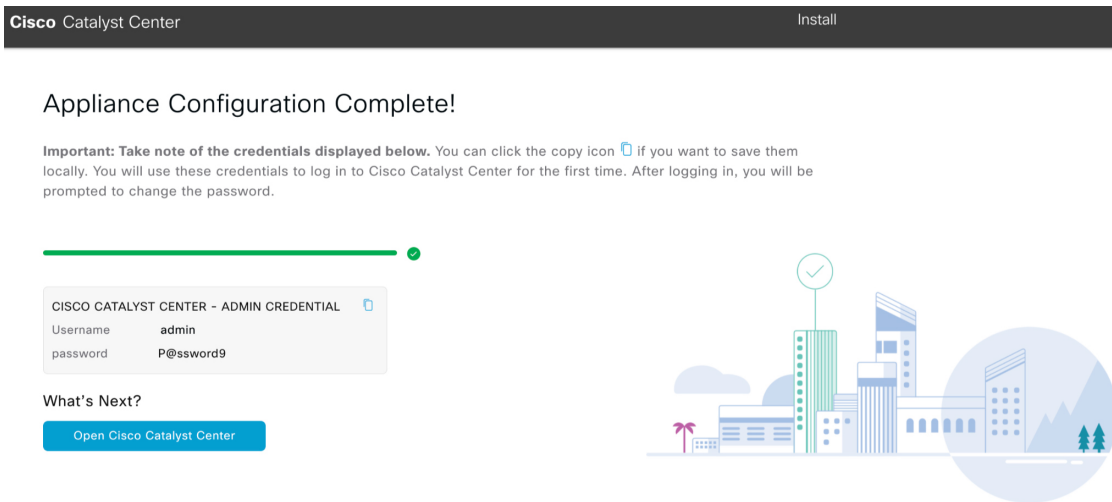
Started: 04/09/2020 12:15:36 [Download](#)

```

2024-03-22T16:04:38.088Z13 | front-proxy-client.crt Apr 13 17:40:20 2020
GMT Apr 13 17:40:20 2021 GMT
2024-03-22T16:04:38.088Z14 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z15 | admin.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z16 | scheduler.conf Apr 13 12:12:14 2020 GMT
Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z17 | controller-manager.conf Apr 13 12:12:14
2020 GMT Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z18 | -----
  
```



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



重要

インストール構成ウィザードを完了すると、**Catalyst Center** はパスワード「**P@ssword9**」を自動的に設定します。初回はこのパスワードを使用して **Catalyst Center** にログインします。

注

セキュリティ対策として、ログイン後にこのパスワードを変更するよう求められます。詳細については、[Catalyst Center への初回ログイン \(256ページ\)](#) を参照してください。

このアプライアンスをスタンドアロンモードで展開する場合には、初回セットアップ：[初期設定ワークフロー \(256ページ\)](#) を実行します。

詳細インストール構成ウィザードを使用して、クラスタ内の最初のアプライアンスを設定できます。

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

重要

- 第3世代 80 コア **Catalyst Center** アプライアンス（シスコ製品番号 DN3-HW-APL-XL）は、このウィザードを使用した設定をサポートします。

- このウィザードは、新しい **Catalyst Center** アプライアンスの初期設定を完了するためにのみ使用できます。以前に設定したアプライアンスを再イメージ化するには、**Maglev** 設定ウィザードを使用する必要があります (**Maglev ウィザードを使用したアプライアンスの設定** (105ページ) を参照)。
- 3 ノードクラスタでアプライアンスを設定する前に、それらのアプライアンスからログアウトしていることを確認します。ログアウトしていない場合、クラスタのアプライアンスを設定し、**Catalyst Center** に初めてログインした後に、(ネットワークのデバイスを検出してテレメトリを有効にするために完了する) クイック スタート ワークフローが開始されません。
- この手順の実行中に入力するすべての IP アドレスが有効なネットマスクを持つ有効なアドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

すでにプライマリノードがある既存のクラスタのセカンダリノードとしてインストールされたアプライアンスを設定する場合には、代わりに**詳細インストール構成ウィザードを使用したセカンダリノードの設定** (236ページ) の手順を実行します。

次のことを確認します。

- **必要な IP アドレスおよびサブネット** (44ページ) と **必須の設定情報** (70ページ) で必要な情報がすべて収集されたこと。
- 「**アプライアンスのインストール ワークフロー** (76ページ)」の説明に従って、1 番目のアプライアンスを設置したこと。
- 「**Cisco Integrated Management Controller に対するブラウザアクセスの有効化** (86ページ)」の説明に従って、プライマリノードで **Cisco IMC** に対するブラウザのアクセス権が設定されたこと。
- 「**事前設定タスクの実行** (91ページ)」の説明に従って、プライマリノードのポートとそれらのポートによって使用されるスイッチが適切に設定されていること。
- **Cisco IMC**、**Catalyst Center** との互換性があるブラウザを使用しています。互換性のあるブラウザの一覧については、インストールしている **Catalyst Center** のバージョンに対応する **リリースノート** を参照してください。
- 次の手順で指定するデフォルトゲートウェイおよび **DNS** サーバーと **Catalyst Center** の間のファイアウォールで **ICMP** が許可されていること。ウィザードでは、ユーザの指定する **DNS** サーバを **ping** で確認します。ファイアウォールが配置されており、そのファイアウォールで **ICMP** が許容されていない場合、この **ping** がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. 詳細インストール構成ウィザードを起動します。

- お使いのブラウザで、実行した **Cisco IMC GUI** 設定で設定した **Cisco IMC** の IP アドレスをポイントしてから、**Cisco IMC** ユーザーとして **Cisco IMC GUI** にログインします (**Cisco Integrated Management Controller に対するブラウザアクセスの有効化** (86ページ) を参照)。
ログインが成功すると、アプライアンスに **[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。
- 青いリンクメニューで **[Launch KVM]** を選択してから **[HTML based KVM]** を選択します。
KVM コンソールが別のブラウザウィンドウまたはタブで自動的に開きます。**KVM** コンソールを使用して、設定の進行状況をモニターし、**Maglev** 構成ウィザードのプロンプトに応答します。
- KVM** が表示されたら、次のいずれかを選択してアプライアンスをリブートします。

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

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

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

STEP #None	STATIC IP CONFIGURATION
Welcome to the Maglev Configuration Wizard! Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration. - Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface - Click Skip to move to config wizard NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration	IPv6 mode IP Address: Netmask: Default Gateway Address: Static Routes: Web installation: https://10. :9004/ < cancel > skip >> configure >>

[Web Installation] フィールドにリストされている URL をレコードします。

d) 次のいずれか 1 つのタスクを実行します。

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

注

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

[IPv6 Mode] チェックボックス IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。

[IP Address] フィールド 使用する静的 IP アドレスを入力します。

[Netmask] フィールド

前のフィールドに指定した IP アドレスのネットマスクを入力します。

- IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。
- IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。

[Default Gateway Address] フィールド

トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。

[Static Routes] フィールド

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

KVM コンソールに **Maglev** 構成ウィザードのウェルカム画面が表示されます。

```

Welcome to the Maglev Configuration Wizard!

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

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

< exit >

```

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

Cisco Catalyst Center Appliance Configuration

Welcome to Cisco Catalyst Center

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

Start A Cisco Catalyst Center Cluster ☒

This appliance will be the primary node of a cluster.

Join A Cisco Catalyst Center Cluster ☐

This appliance will be added as a node to the primary node of a cluster.



Next

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

Cisco Catalyst Center Appliance Configuration

Welcome to Cisco Catalyst Center

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

Install ☐

Configure a standalone node or cluster's primary node.

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

Advanced Install ☒

Configure a standalone node or any node in a cluster.

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



Back Start

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

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

Overview

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

< ● ○ ○ ○ ○ ○ >

Start Workflow



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

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

Cisco Catalyst Center
Advanced Install

Appliance Interface Overview

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

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

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

Exit
Next

重要

Catalyst Center の機能に必要なため、少なくともエンタープライズポートとクラスタポートを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか 1 つまたは両方が表示されない場合、表示されないポートは機能しないか無効になっている可能性があります。ポートが機能していないことが判明した場合には、[Exit] を選択してウィザードをすぐに終了します。設定を再開したり、Cisco Technical Assistance Center (TAC) に連絡したりする前に、[事前設定タスクの実行](#) (91ページ) 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。

2. 詳細インストール構成ウィザードを完了します。

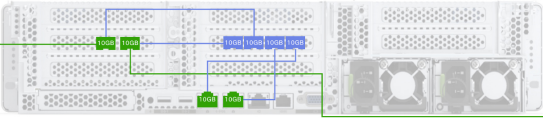
a) [Next] をクリックします。

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

Cisco Catalyst Center
Advanced Install

How would you like to set up your appliance interfaces?

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



Enterprise Network Interface
Intracenter Link Network

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

Would you like to have a dedicated Management Network Interface?

☒ Yes ☐ No

Would you like to have a dedicated Internet Access Interface?

☒ Yes ☐ No

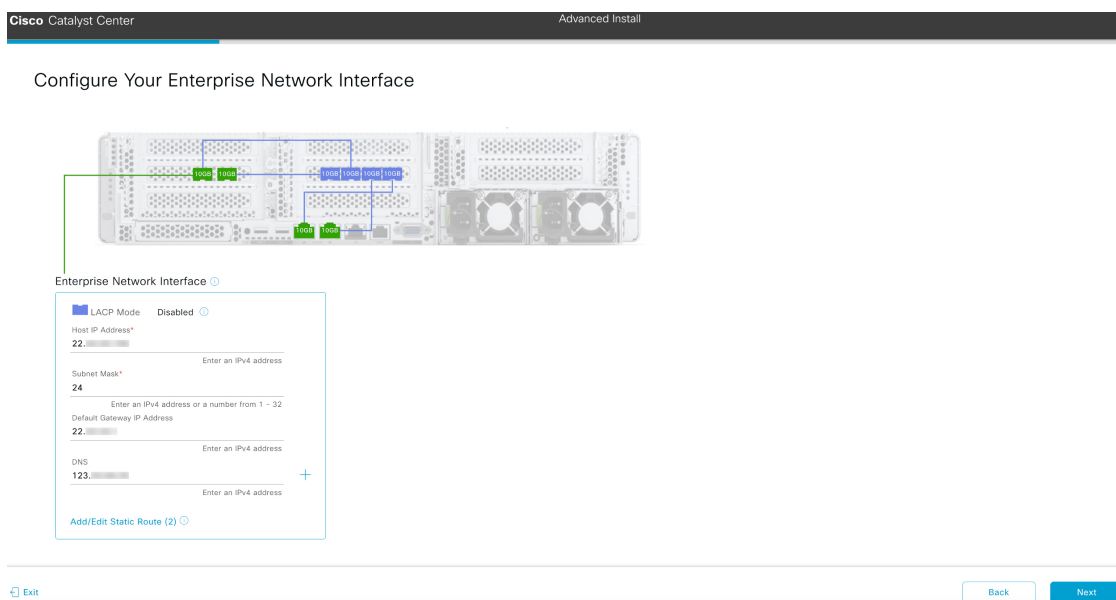
Exit
Back
Next

ネットワークがファイアウォールの背後にある場合は、次のタスクを実行します。

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

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

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



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

[インターフェースケーブル接続 \(40ページ\)](#) で説明されているとおり、このインターフェイスは、アプライアンスをエンタープライズネットワークにリンクするために必要なインターフェイスです。入力する必要がある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と [必須の設定情報 \(70ページ\)](#) を参照してください。

48 :

[LACP Mode] スライド

エンタープライズ インターフェイスに対して、次のネットワーク インターフェイス コントローラ (NIC) ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、**2**つのイーサネット インターフェイスを **1**つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデブレックス設定を共有する **2**つのイーサネット インターフェイスが **1**つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要 \(94ページ\)](#) を参照してください。

[Host IP Address] フィールド	エンタープライズ インターフェイスの IP アドレスを入力します。これは必須です。
[Subnet Mask] フィールド	インターフェイスの 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。
[Default Gateway IP Address] フィールド	インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも **1** つのインターフェイスに対してデフォルトゲートウェイ **IP** アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

 注

このインターフェイスは、**DHCP** サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。

1. このフィールドに現在一覧表示されている **IP** アドレスを削除し、**[Exit]** をクリックします。
この操作でウィザードの最初の画面に戻ります。
2. エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ **IP** アドレスを入力します。

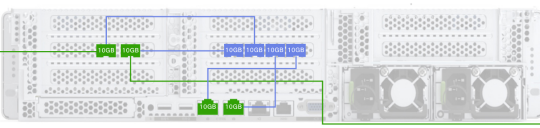
[DNS] フィールド	優先 DNS サーバの IP アドレスを入力します。 追加の DNS サーバーを入力するには、 [Add] (+) アイコンをクリックします。
-------------	--

重要

- クラスタ内の各ノードに対して、最大 **3** つの **DNS** サーバーを設定します。アプライアンスに対して **3** つを超える **DNS** サーバを設定すると、問題が発生する可能性があります。
- **NTP** の場合、**Catalyst Center** と **NTP** サーバの間のポート **123** (**UDP**) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Intracluster Interface]** 画面が開きます。

Configure Your Intracluster Interface



Enterprise Network Interface ⓘ

Interface Name	enterprise
LACP Mode	Disabled ⓘ
IP Address	22.
Subnet Mask	24
Default Gateway	22.
DNS Servers	123.
Static Routes	2

Intracluster Link Network ⓘ

LACP Mode	Disabled ⓘ
Host IP Address*	169.
Subnet Mask*	255.

Enter an IPv4 address

Enter an IPv4 address or a number from 1 - 32

Exit

Back

Next

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

[インターフェイスケーブル接続 \(40ページ\)](#) で説明されているとおり、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要がある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と [必須の設定情報 \(70ページ\)](#) を参照してください。

 注

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

49 :

[LACP Mode] スライダー

クラスター内インターフェイスに対して、次の **NIC** ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、**2**つのイーサネットインターフェイスを **1**つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデブレッक्स設定を共有する **2**つのイーサネットインターフェイスが **1**つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

重要

アプライアンスのクラスター内インターフェイスで **LACP** モードを有効にする場合は、今すぐ有効にします。このウィザードを完了すると、次は実行できなくなります。

Catalyst Center の **NIC** ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#)（94ページ）を参照してください。

[Host IP Address] フィールド

クラスター内インターフェイスの **IP** アドレスを入力します。これは必須です。

 注

クラスター内インターフェイス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。

[Subnet Mask] フィールド

インターフェイスの **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。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Management Network Interface]** 画面が開きます。

Configure Your Management Network Interface

Enterprise Network Interface

Interface Name: enterprise

LACP Mode: Disabled

IP Address: 22

Subnet Mask: 24

Default Gateway: 22

DNS Servers: 123

Static Routes: 2

Management Network Interface

Host IP Address*: 32

Subnet Mask*: 255

Default Gateway IP Address:

DNS:

Add/Edit Static Route (0)

Intracuster Link Network

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169

Subnet Mask: 255

Static Routes: 2

Exit Back Next

- e) (任意) 管理インターフェイスの構成値を入力し、**[Next]** をクリックします。

インターフェースケーブル接続 (40ページ) で説明されているとおり、このポートは管理ネットワークから **Catalyst Center GUI** にアクセスするために使用されます。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要がある値の詳細な説明については、**必要なIPアドレスおよびサブネット** (44ページ) と**必須の設定情報** (70ページ) を参照してください)。

注

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

50 :

[Host IP Address] フィールド 管理インターフェイスの **IP** アドレスを入力します。

[Subnet Mask] フィールド インターフェイスの **IP** アドレスに対応するネットマスクを入力します。

[Default Gateway IP Address] フィールド インターフェイスに使用するデフォルトゲートウェイ **IP** アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ **IP** アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、**[Add] (+)** アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 **3** つの DNS サーバを設定します。アプライアンスに対して **3** つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- **NTP** の場合、**Catalyst Center** と **NTP** サーバの間のポート **123 (UDP)** が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Internet Access Interface]** 画面が開きます。

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

インターフェースケーブル接続 (40ページ) で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。専用インターネットアクセスインターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要がある値の詳細な説明については、**必要な IP アドレスおよびサブネット (44ページ)** と **必須の設定情報 (70ページ)** を参照してください)。

51 :

[Host IP Address] フィールド

インターネットアクセスインターフェイスの IP アドレスを入力します。

[Subnet Mask] フィールド

インターフェイスの IP アドレスに対応するネットマスクを入力します。この操作は、前のフィールドに IP アドレスを入力する場合に必要になります。

[Default Gateway IP Address]
フィールド

インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、**[Add]** (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、**Catalyst Center** と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの**[Interface to Port Configuration]** 画面が開きます。

Interface to Port Configuration

We are going to configure the following interfaces. Clicking Next will begin the configuration process. This may take up to a minute to configure.

Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22
Subnet Mask	24
Default Gateway	22
DNS Servers	123
Static Routes	2

Management Network Interface

Interface Name	management
IP Address	32
Subnet Mask	255

Intracuster Link Network

Interface Name	cluster
LACP Mode	Disabled
IP Address	169
Subnet Mask	255
Static Routes	2

Internet Network Interface

Interface Name	internet
IP Address	55
Subnet Mask	255

Exit Back Next

- g) プライマリノードのインターフェイスに入力した設定を確認します。
変更が必要な場合は、該当するインターフェイスの **[Edit]** リンクをクリックします。
- h) インターフェイス設定が正しいことを確認したら、**[Next]** をクリックします。
初期インターフェイス設定が完了すると、**[Configure Proxy Server Information]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Configure Proxy Server Information

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

☒ Yes ☐ No

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

Port* Enter port number between 1 to 65535.

Username

Password

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

i) 次のいずれかのタスクを実行してから、**[Next]** をクリックします。

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

52 :

[Proxy Server] フィールド

インターネットにアクセスする **HTTPS** ネットワークプロキシの **URL** またはホスト名を入力します。



注

Catalyst Center から **HTTPS** プロキシへの接続は、このリリースの **HTTP** 経由のみでサポートされます。

[Port] フィールド

アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

[Username] フィールド

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

[Password] フィールド

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

ウィザードは入力した情報を検証し、ウィザードを続行する前に変更が必要な設定を通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Advanced Appliance Settings]** 画面が開きます。

j) クラスタの構成値を入力し、[Next] をクリックします。

53 : [Advanced Appliance Settings]

[Cluster virtual IP addresses]

[To access from Enterprise Network]、[For Intracluster Access]、[To access from Management Network]、および [For Internet Access] フィールド

プライマリノードに設定したクラスタとインターフェイス間のトラフィックに使用される仮想IPアドレスを入力します。この操作は、3 ノードクラスタと、将来3 ノードクラスタに変換されるシングルノードクラスタの両方の場合に必要です。シングルノードクラスタのセットアップがあり、3 ノードクラスタのセットアップに移行する予定がない場合は、このセクションのフィールドを空白のままにすることができます。

注

エンタープライズインターフェイスと同じポートで管理インターフェイスまたはインターネットアクセスインターフェイスを設定した場合、対応するフィールドはこのセクションに表示されません。

重要

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

[Fully Qualified Domain Name (FQDN)] フィールド

クラスターの完全修飾ドメイン名 (FQDN) を入力します。Catalyst 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、クラスターの **Web** インターフェイスと、Catalyst 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。
- Catalyst Center 証明書の **[Subject Alternative Name (SAN)]** フィールドで、FQDN を使用して、デバイスのプロビジョニングに使用されるプラグアンドプレイサーバが定義されます。

CLI クレデンシャル

maglev ユーザーのパスワードを入力して確認します。

重要

このパスワードが [パスワード要件 \(73ページ\)](#) に準拠していることを確認してください。

Cisco Catalyst Center 管理者ログイン情報

スーパーユーザ権限を持つ管理者のデフォルトのパスワードを入力します。このパスワードは **Catalyst Center** に初めてログインするときに使用します。

重要

このパスワードが [パスワード要件 \(73ページ\)](#) に準拠していることを確認してください。

[NTP server settings]

[NTP Server] フィールド

少なくとも 1 つの **NTP** サーバーアドレスまたはホスト名を入力します。追加の **NTP** サーバーアドレスまたはホスト名を入力するには、**[Add] (+)** アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の **NTP** サーバを設定するようお勧めします。

[Turn on NTP Authentication] チェックボックス

NTP サーバーが同期する前に **Catalyst Center** **NTP** サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- **NTP** サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。

この値は、**NTP** サーバーのキーファイルで定義されているキー ID に対応します。

- **NTP** サーバーのキー ID に関連付けられた **SHA-1** キー値。この 40 文字の 16 進文字列は、**NTP** サーバーのキーファイルにあります。

注

前のフィールドで構成した各 **NTP** サーバーのキー ID とキー値を入力してください。

[Subnet settings]

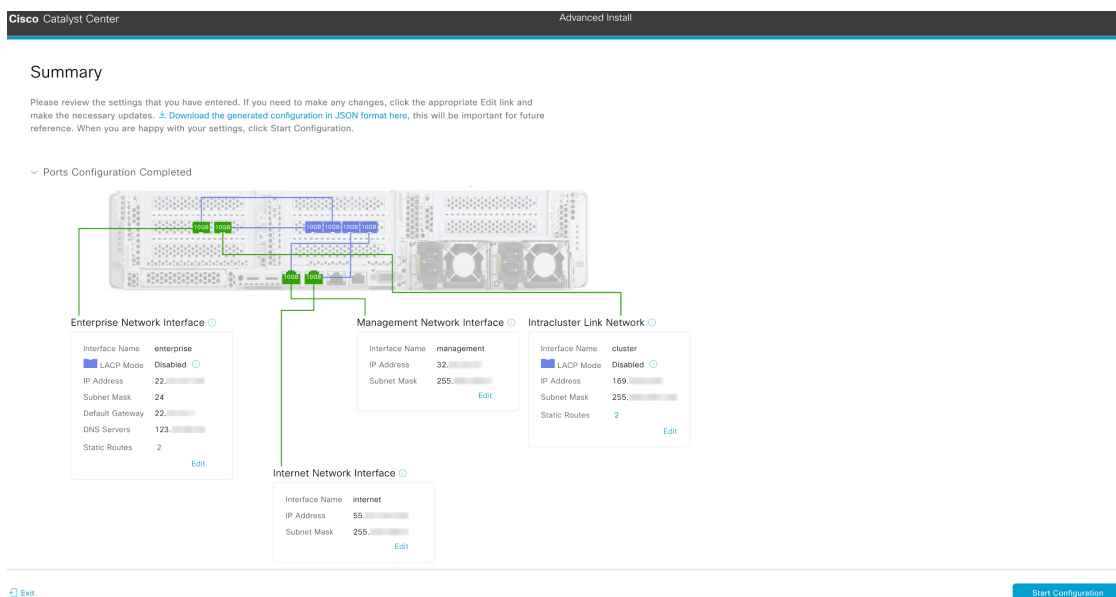
[Container Subnet] フィールド

内部サービスを管理するために **Catalyst Center** で使用する、ルーティングされない専用の **IP** サブネット。デフォルトでは、これは **169.254.32.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

[Cluster Subnet] フィールド

内部クラスターサービスを管理するために **Catalyst Center** で使用する、ルーティングされない専用の IP サブネット。デフォルトでは、これは **169.254.48.0/20** にあらかじめ設定されています。このサブネットを使用することをお勧めします。

ウィザードは入力した情報を検証し、ウィザードを続行する前に変更が必要な設定を通知します。入力した設定が有効な場合、ウィザードの **[Summary]** 画面が開きます。



 注

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

- k) ウィザードの完了時に入力したすべての設定を確認します。設定を更新する必要がある場合は、関連する **[Edit]** リンクをクリックして、対応するウィザード画面を開きます。
- l) **Catalyst Center** アプライアンスの設定を完了するには、**[Start Configuration]** をクリックします。

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

Appliance Configuration In Progress

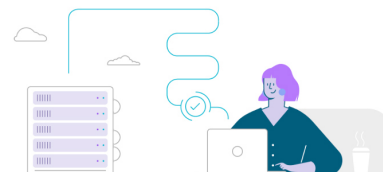
It should take about 30 minutes to configure the appliance. Do not press your browser's back button or refresh this page. The page will update after configuration completes.

Initializing the cluster using kubeadm 50%

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

[Download](#)

```
Apr 13 17:40:20 2020 GMT
2024-03-22T16:04:38.088Z13 | front-proxy-client.crt Apr 13 17:40:20 2020
GMT Apr 13 17:40:20 2021 GMT
2024-03-22T16:04:38.088Z14 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z15 | admin.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z16 | scheduler.conf Apr 13 12:12:14 2020 GMT
Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z17 | controller-manager.conf Apr 13 12:12:14
2020 GMT Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z18 | -----
-----
```



このタスクが完了したら、次の手順を実行します。

- 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](#)（256ページ）」）を実行します。
- アプライアンスをクラスタ内のプライマリノードとして展開する場合には、クラスタ内の2番目と3番目のインストール済みアプライアンスを設定します（[詳細インストール構成ウィザードを使用したセカンドリノードの設定](#)（236ページ））。

詳細インストール構成ウィザードを使用して、クラスタに付加的なノードを追加できます。

詳細インストール構成ウィザードを使用して、クラスター内の2番目と3番目のアプライアンスを設定するには、次の手順を実行します。

重要

- 3 ノードクラスタを構築するには、同じバージョンのシステムパッケージが3つの Catalyst Center アプライアンスにインストールされている必要があります。この条件が整わない場合、予期しない動作とダウンタイムの可能性が生じることがあります。
- 第3世代80 コア Catalyst Center アプライアンス（シスコ製品番号 DN3-HW-APL-XL）は、このウィザードを使用した設定をサポートします。
- このウィザードは、新しい Catalyst Center アプライアンスの初期設定を完了するためののみ使用できます。以前に設定したアプライアンスを再イメージ化するには、Maglev 設定ウィザードを使用する必要があります（[Maglev ウィザードを使用したアプライアンスの設定](#)（105ページ）を参照）。

- 3 ノードクラスターでは、アプライアンスを設定する前にログアウトします。ログアウトしていない場合、クラスターのアプライアンスを設定し、**Catalyst Center** に初めてログインした後に、（ネットワークのデバイスを検出してテレメトリを有効にするために完了する）クイック スタート ワークフローが開始されません。
- この手順の実行中に入力するすべての IP アドレスが有効なネットマスクを持つ有効なアドレスであることを確認してください。また、アドレスと対応するサブネットが重複していないことを確認してください。重複している場合、サービスの通信の問題が発生する可能性があります。

新しいセカンダリノードをクラスターに結合する場合には、クラスター内の最初のホストをプライマリノードとして指定する必要があります。セカンダリノードをクラスターに参加させる際には、次の詳細を考慮してください。

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

```
maglev-1 [main - https://kong-:443]
```

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

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

- 一度に 1 つのノードのみをクラスターに結合してください。複数のノードを同時に追加しないでください。同時に追加しようとすると予期しない動作が発生します。
- 各セカンダリノードのクラスター接続プロセス中に、一部のサービスのダウンタイムが発生することが予想されます。サービスはすべてのノードに再配布される必要があり、そのプロセスの間、クラスターはダウンします。

次のことを確認します。

- [詳細インストール構成ウィザードを使用したプライマリノードの設定](#)（219 ページ）の手順に従って、クラスター内の最初のアプライアンスが設定されたこと。
- [必要な IP アドレスおよびサブネット](#)（44 ページ）と [必須の設定情報](#)（70 ページ）で必要な情報がすべて収集されたこと。

- 「[アプライアンスのインストール ワークフロー \(76ページ\)](#)」の説明に従って、2 番目と 3 番目のアプライアンスを設置したこと。
- 次の手順を完了しました。
 1. 最初のアプライアンスで **maglev package status** コマンドを実行したこと。
 この情報には **Catalyst Center** ホームページからもアクセスできます。**[Help]** アイコン (🔍) をクリックし、**[About] > [Show Packages]** の順に選択してください。
 2. **Cisco TAC** に連絡し、このコマンドの出力を提供して 2 番目と 3 番目のアプライアンスにインストールする必要がある ISO をポイントするよう依頼したこと。
- 「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(86ページ\)](#)」の説明に従って、両方のセカンダリノードで **Cisco IMC** に対するブラウザのアクセス権が設定されたこと。
- [事前設定タスクの実行 \(91ページ\)](#) の説明に従って、セカンダリノードのポートとそれらのポートによって使用されるスイッチの両方が適切に設定されていること。
- 互換性のあるブラウザを使用していること。互換性のあるブラウザの一覧については、インストールしている **Catalyst Center** のバージョンに対応する [リリースノート](#) を参照してください。
- 次の手順で指定するデフォルトゲートウェイおよび **DNS** サーバーと **Catalyst Center** の間のファイアウォールで **ICMP** が許可されていること。ウィザードでは、ユーザの指定する **DNS** サーバを **ping** で確認します。ファイアウォールが配置されており、そのファイアウォールで **ICMP** が許可されていない場合、この **ping** がブロックされる可能性があります。ブロックされた場合、ウィザードを完了できません。

1. 詳細インストール構成ウィザードを起動します。

- a) お使いのブラウザで、実行した **Cisco IMC GUI** 設定で設定した **Cisco IMC** の IP アドレスをポイントしてから、**Cisco IMC** ユーザーとして **Cisco IMC GUI** にログインします ([Cisco Integrated Management Controller に対するブラウザアクセスの有効化 \(86ページ\)](#) を参照)。
 ログインが成功すると、アプライアンスに **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウが右上の青いリンクメニューとともに表示されます。
- b) 青いリンクメニューで **[Launch KVM]** を選択してから **[HTML based KVM]** を選択します。
 KVM コンソールが別のブラウザウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、**Maglev** 構成ウィザードのプロンプトに応答します。
- c) KVM が表示されたら、次のいずれかを選択してアプライアンスをリブートします。
 - メインの **Cisco IMC GUI** ブラウザウィンドウで、**[Host Power] > [Power Cycle]** を選択します。その後、KVM コンソールに切り替えて続行します。
 - KVM コンソールで、**[Power] > [Power Cycle System (cold boot)]** を選択します。

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

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

STEP #None	STATIC IP CONFIGURATION
Welcome to the Maglev Configuration Wizard! Please Enter Static IP Information for Enterprise Interface Configuration, Static IP is configured as an alternative to DHCP for web UI Configuration. - Click Configure after entering Information for configuring IP which will be configured on Enterprise Interface - Click Skip to move to config wizard NOTE: Default Configuration mode is IPv4, Please select IPv6 mode for Ipv6 Configuration	IPv6 mode IP Address: Netmask: Default Gateway Address: Static Routes: Web installation: https://10. :9004/ < cancel > skip >> configure >>

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

d) 次のいずれか 1 つのタスクを実行します。

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

[IPv6 Mode] チェックボックス IPv6 アドレスを設定する場合は、このチェックボックスをオンにします。

[IP Address] フィールド 使用する静的 IP アドレスを入力します。

[Netmask] フィールド 前のフィールドに指定した IP アドレスのネットマスクを入力します。

- IPv4 アドレスを入力した場合は、ネットマスクまたは CIDR アドレスのいずれかを入力できます。
- IPv6 アドレスを入力した場合は、CIDR アドレスのみを入力できます。

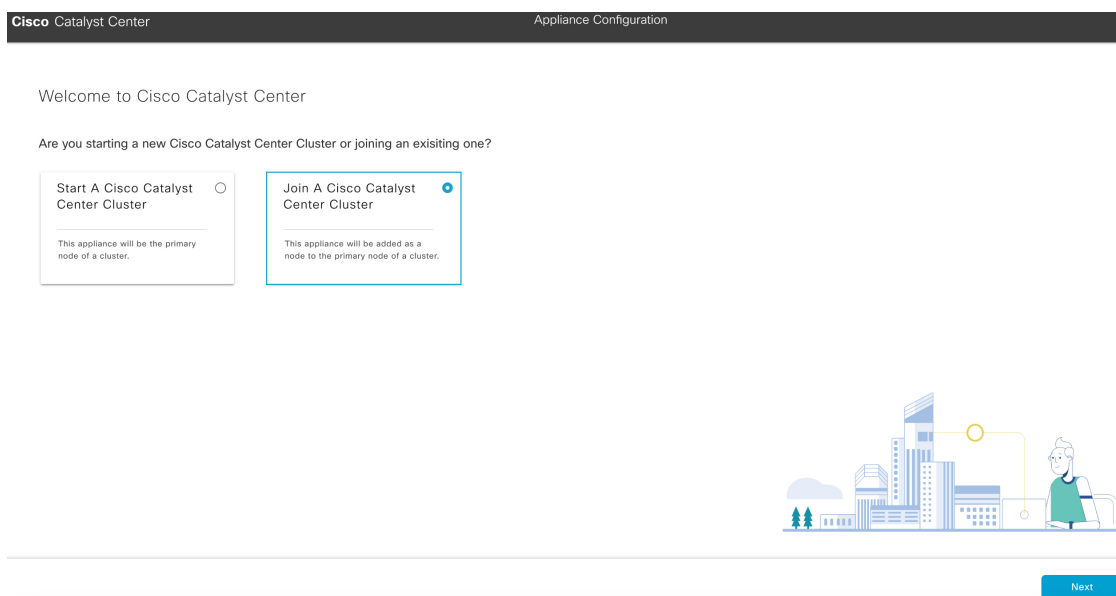
[Default Gateway Address] フィールド トラフィックのルーティングに使用されるデフォルトゲートウェイを指定します。

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

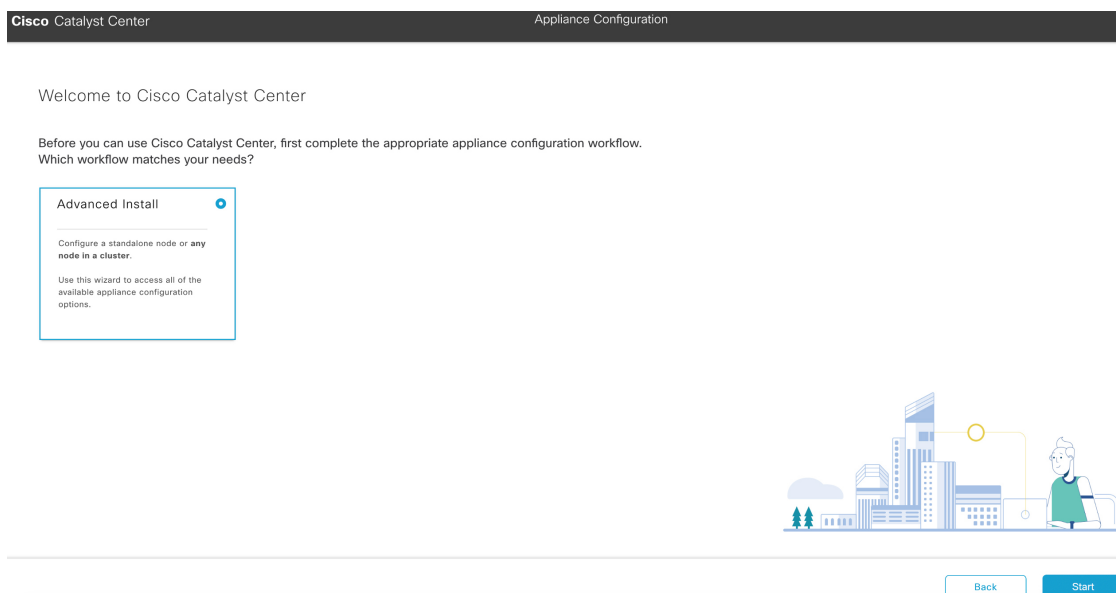
KVM コンソールに Maglev 構成ウィザードのウェルカム画面が表示されます。



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

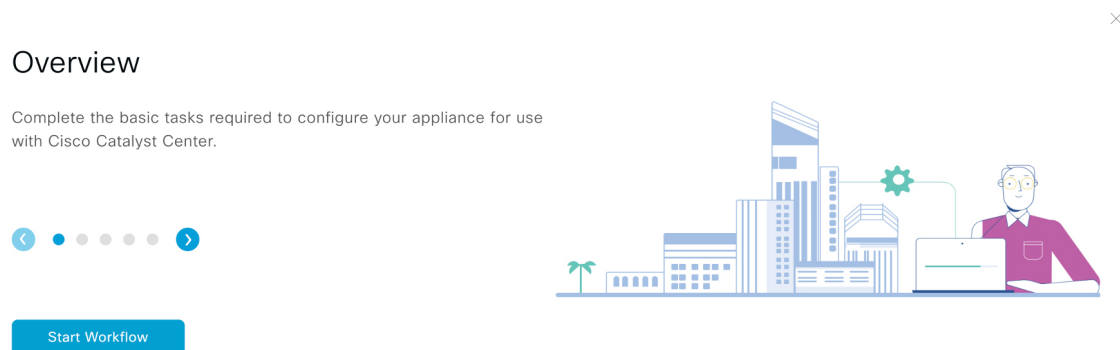


- f) [Join a Cisco Catalyst Center Cluster] オプションボタンをクリックし、[Next] をクリックします。



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

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



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

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

Appliance Interface Overview

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

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

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

[Exit](#)
[Next](#)
重要

Catalyst Center の機能に必要なため、少なくともアプライアンスのエンタープライズポートおよびクラスターポートにインターフェイスを設定する必要があります。設定の過程でウィザードにこれらのポートのいずれか 1 つまたは両方が表示されない場合、表示されないポートは機能しないか無効になっている可能性があります。ポートが機能していないことが判明した場合には、**[Exit]** を選択してウィザードをすぐに終了します。設定を再開したり、**Cisco Technical Assistance Center (TAC)** に連絡したりする前に、[事前設定タスクの実行](#) (91 ページ) 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。

2. 詳細インストール構成ウィザードを完了します。

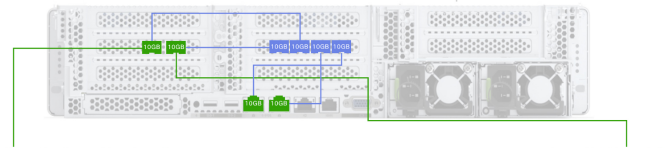
a) **[Next]** をクリックします。

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

Cisco Catalyst Center
Advanced Install

How would you like to set up your appliance interfaces?

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



Enterprise Network Interface
Intracuster Link Network

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

Would you like to have a dedicated Management Network Interface?

☒ Yes ☐ No

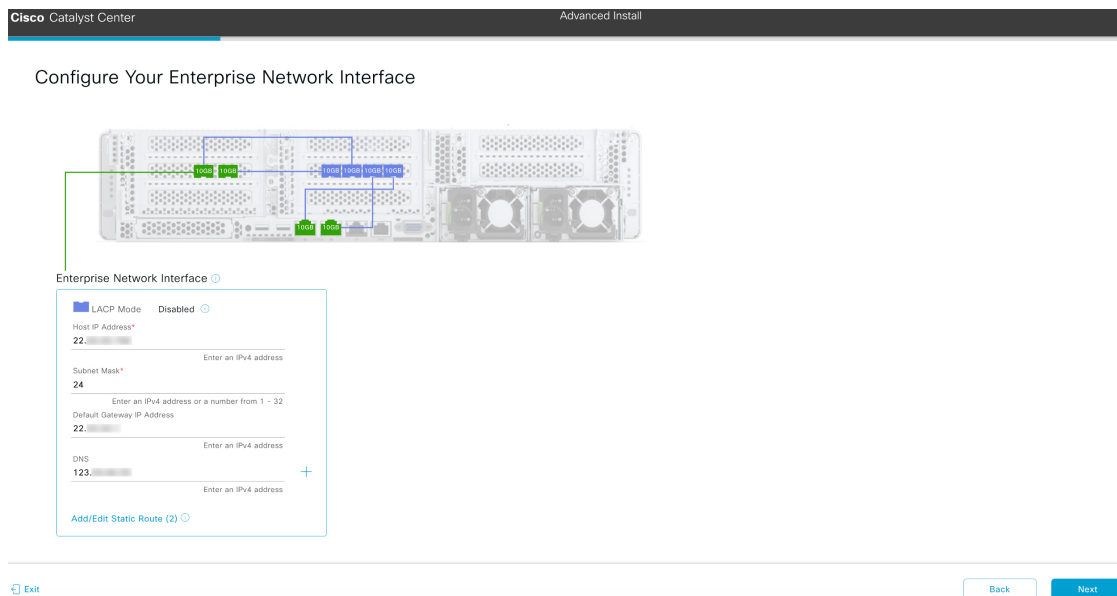
Would you like to have a dedicated Internet Access Interface?

☒ Yes ☐ No

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

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

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



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

[インターフェイスケーブル接続 \(40ページ\)](#) で説明されているとおり、このインターフェイスは、アプライアンスをエンタープライズネットワークにリンクするために必要なインターフェイスです。入力する必要がある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と[必須の設定情報 \(70ページ\)](#) を参照してください。

54 :

[LACP Mode] スライド

エンタープライズ インターフェイスに対して、次のネットワーク インターフェイスコントローラ (NIC) ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、**2つのイーサネット インターフェイスを 1つの論理チャネルに集約すること**で、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデュプレックス設定を共有する **2つのイーサネット インターフェイスが 1つの論理チャネルに集約されます**。これにより、ロードバランシングとより高い帯域幅が提供されます。

Catalyst Center の NIC ボンディングの実装に関する詳細については、[NIC ボンディングの概要 \(94ページ\)](#) を参照してください。

[Host IP Address] フィールド

エンタープライズ インターフェイスの IP アドレスを入力します。これは必須です。

[Subnet Mask] フィールド

インターフェイスの 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。

[Default Gateway IP Address]
フィールド

インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

構成ウィザードを完了できるように、アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。

 注

このインターフェイスは、DHCP サーバーによって割り当てられたデフォルトゲートウェイを使用するように指定されています。別のゲートウェイを指定するには、次の手順を実行します。

1. このフィールドに現在一覧表示されている IP アドレスを削除し、**[Exit]** をクリックします。
この操作でウィザードの最初の画面に戻ります。
2. エンタープライズポートのウィザード画面に戻り、使用するゲートウェイ IP アドレスを入力します。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

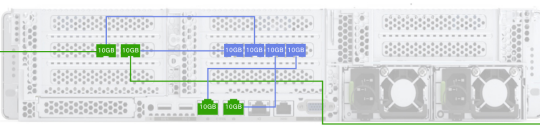
追加の DNS サーバーを入力するには、**[Add]** (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバーを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、**Catalyst Center** と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Intracluster Interface]** 画面が開きます。

Configure Your Intracluster Interface



Enterprise Network Interface ⓘ

Interface Name	enterprise
LACP Mode	Disabled ⓘ
IP Address	22.
Subnet Mask	24
Default Gateway	22.
DNS Servers	123.
Static Routes	2

Intracluster Link Network ⓘ

LACP Mode	Disabled ⓘ
Host IP Address*	169.
Subnet Mask*	255.

Enter an IPv4 address

Enter an IPv4 address or a number from 1 - 32

Exit

Back

Next

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

[インターフェイスケーブル接続 \(40ページ\)](#) で説明されているとおり、このポートはアプライアンスをクラスタにリンクするために必要なポートです。入力する必要がある値の詳細な説明については、[必要な IP アドレスおよびサブネット \(44ページ\)](#) と [必須の設定情報 \(70ページ\)](#) を参照してください。

 注

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

55 :

[LACP Mode] スライダー

クラスター内インターフェイスに対して、次の **NIC** ボンディングモードのいずれかを選択します。

- **アクティブ/バックアップモード**：このモードでは、**2**つのイーサネット インターフェイスを **1**つの論理チャネルに集約することで、耐障害性が提供されます。現在アクティブなインターフェイスがダウンすると、他のインターフェイスが代わりにアクティブになります。
- **LACP モード**：このモードでは、同じ速度とデブレックス設定を共有する **2**つのイーサネット インターフェイスが **1**つの論理チャネルに集約されます。これにより、ロードバランシングとより高い帯域幅が提供されます。

重要

アプライアンスのクラスター内インターフェイスで **LACP** モードを有効にする場合は、今すぐ有効にします。このウィザードを完了すると、次は実行できなくなります。

Catalyst Center の **NIC** ボンディングの実装に関する詳細については、[NIC ボンディングの概要](#)（94ページ）を参照してください。

[Host IP Address] フィールド

クラスター内インターフェイスの **IP** アドレスを入力します。これは必須です。クラスター内インターフェイス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。

[Subnet Mask] フィールド

インターフェイスの **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。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Management Network Interface]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Configure Your Management Network Interface

Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22
Subnet Mask	24
Default Gateway	22
DNS Servers	123
Static Routes	2

Management Network Interface

Host IP Address* 32 Enter an IPv4 address

Subnet Mask* 255 Enter an IPv4 address or a number from 1 - 32

Default Gateway IP Address Default Gateway already configured in Enterprise Network

DNS Enter an IPv4 address

[Add/Edit Static Route \(0\)](#)

Intracuster Link Network

Interface Name	cluster
LACP Mode	Disabled
IP Address	169
Subnet Mask	255
Static Routes	2

Exit Back Next

- e) (任意) 管理インターフェイスの構成値を入力し、**[Next]** をクリックします。

[インターフェイスケーブル接続 \(40ページ\)](#) で説明されているとおり、このポートは管理ネットワークから **Catalyst Center GUI** にアクセスするために使用されます。専用管理インターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要がある値の詳細な説明については、[必要なIPアドレスおよびサブネット \(44ページ\)](#) と[必須の設定情報 \(70ページ\)](#) を参照してください)。

注

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

56 :

[Host IP Address] フィールド 管理インターフェイスの **IP アドレス**を入力します。

[Subnet Mask] フィールド インターフェイスの **IP アドレス**に対応するネットマスクを入力します。

[Default Gateway IP Address] フィールド インターフェイスに使用するデフォルトゲートウェイ **IP アドレス**を入力します。

重要

アプライアンスの少なくとも **1** つのインターフェイスに対してデフォルトゲートウェイ **IP アドレス**を入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、[Add] (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 **3** つの DNS サーバを設定します。アプライアンスに対して **3** つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- **NTP** の場合、**Catalyst Center** と **NTP** サーバの間のポート **123** (**UDP**) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの **[Configure Your Internet Access Interface]** 画面が開きます。

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

インターフェースケーブル接続 (40ページ) で説明されているとおり、このポートは、アプライアンスをインターネットにリンクする際、エンタープライズポート経由でアプライアンスをリンクできない場合に使用されるオプションのポートです。専用インターネットアクセスインターフェイスを設定する場合は、次の表に示す情報を入力します。(入力する必要がある値の詳細な説明については、**必要な IP アドレスおよびサブネット (44ページ)** と **必須の設定情報 (70ページ)** を参照してください)。

57 :

[Host IP Address] フィールド

インターネットアクセスインターフェイスの IP アドレスを入力します。

[Subnet Mask] フィールド

インターフェイスの IP アドレスに対応するネットマスクを入力します。この操作は、前のフィールドに IP アドレスを入力する場合に必要になります。

[Default Gateway IP Address]
フィールド

インターフェイスに使用するデフォルトゲートウェイ IP アドレスを入力します。

重要

アプライアンスの少なくとも 1 つのインターフェイスに対してデフォルトゲートウェイ IP アドレスを入力してください。入力しないと、設定ウィザードを完了できません。

[DNS] フィールド

優先 DNS サーバの IP アドレスを入力します。

追加の DNS サーバを入力するには、**[Add]** (+) アイコンをクリックします。

重要

- クラスタ内の各ノードに対して、最大 3 つの DNS サーバを設定します。アプライアンスに対して 3 つを超える DNS サーバを設定すると、問題が発生する可能性があります。
- NTP の場合、**Catalyst Center** と NTP サーバの間のポート 123 (UDP) が開いていることを確認します。

ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効で、ポートが稼働している場合は、ウィザードの**[Interface to Port Configuration]** 画面が開きます。

Enterprise Network Interface

Interface Name	enterprise
LACP Mode	Disabled
IP Address	22
Subnet Mask	24
Default Gateway	22
DNS Servers	123
Static Routes	2

Management Network Interface

Interface Name	management
IP Address	32
Subnet Mask	255

Intracuster Link Network

Interface Name	cluster
LACP Mode	Disabled
IP Address	169
Subnet Mask	255
Static Routes	2

Internet Network Interface

Interface Name	internet
IP Address	55
Subnet Mask	255

- g) セカンダリノードのインターフェイスに入力した設定を確認します。
変更が必要な場合は、該当するインターフェイスの **[Edit]** リンクをクリックします。
- h) インターフェイスの設定に問題がなければ、**[Next]** をクリックします。
初期インターフェイス設定が完了すると、**[Configure Proxy Server Information]** 画面が開きます。

Cisco Catalyst Center
Advanced Install

Configure Proxy Server Information

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

☒ Yes
☐ No

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

Port*
Enter port number between 1 to 65535.

Username

Password

Exit
Review
Back
Next

i) 次のいずれかのタスクを実行してから、**[Next]** をクリックします。

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

58 :

[Proxy Server] フィールド

インターネットにアクセスする **HTTPS** ネットワークプロキシの **URL** またはホスト名を入力します。



注

Catalyst Center から **HTTPS** プロキシへの接続は、このリリースの **HTTP** 経由のみでサポートされます。

[Port] フィールド

アプライアンスがネットワークプロキシにアクセスするために使用したポートを入力します。

[Username] フィールド

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

[Password] フィールド

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

ウィザードは入力した情報を検証し、ウィザードを続行する前に変更が必要な設定を通知します。入力した設定が有効な場合、ウィザードの **[Primary Node Details]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Primary Node Details

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

Primary Node IP*

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

CLI Username
maglev

CLI Password*

Enter CLI Password

Exit Review Back Next

- j) クラスタのプライマリノードとの接続を確立するには、その IP アドレスとパスワード（デフォルトでは、ユーザー名がすでに **maglev** に設定されている場合、そのユーザー名）を入力し、**[Next]** をクリックします。

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

Cisco Catalyst Center Advanced Install

Advanced Appliance Settings

CLI CREDENTIALS

Username*

maglev

Password*

show Details

Confirm Password*

show

NTP SERVER SETTINGS

NTP Server*

ntp [masked] +

Enter an IP address or FQDN

☐ Turn On NTP Authentication

Exit Review Back Next

- k) クラスタの構成値を入力し、**[Next]** をクリックします。

59 : [Advanced Appliance Settings]

CLI クレデンシャル

maglev ユーザーのパスワードを入力して確認します。

重要

このパスワードが **パスワード要件**（73ページ）に準拠していることを確認してください。

[NTP server settings]**[NTP Server]** フィールド

少なくとも 1 つの **NTP** サーバーアドレスまたはホスト名を入力します。追加の **NTP** サーバーアドレスまたはホスト名を入力するには、**[Add]** (+) アイコンをクリックします。

実稼働環境への展開では、少なくとも 3 台の **NTP** サーバを設定するようお勧めします。

[Turn On NTP Authentication]
チェックボックス

NTP サーバーが同期する前に **Catalyst Center** **NTP** サーバーの認証を有効にするには、このチェックボックスをオンにして、次の情報を入力します。

- **NTP** サーバーのキー ID。有効な値の範囲は 1 ～ 4294967295 ($2^{32}-1$) です。

この値は、**NTP** サーバーのキーファイルで定義されているキー ID に対応します。

- **NTP** サーバーのキー ID に関連付けられた **SHA-1** キー値。この 40 文字の 16 進文字列は、**NTP** サーバーのキーファイルにあります。

 注

前のフィールドで構成した各 **NTP** サーバーのキー ID とキー値を入力してください。

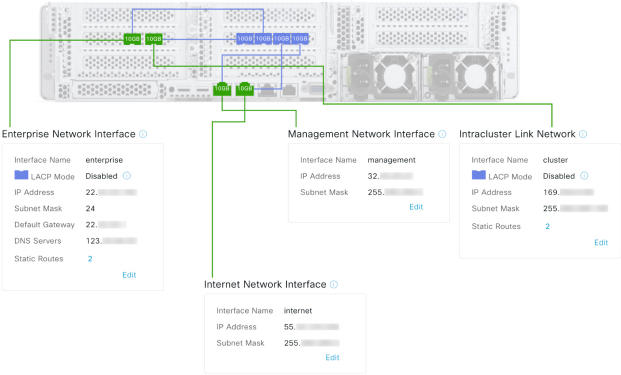
ウィザードは入力した情報を検証し、ポートが稼働していることを確認し、変更が必要な設定があれば通知します。入力した設定が有効な場合、ウィザードの **[Summary]** 画面が開きます。

Cisco Catalyst Center Advanced Install

Summary

Please review the settings that you have entered. If you need to make any changes, click the appropriate Edit link and make the necessary updates. [Download the generated configuration in JSON format here](#), this will be important for future reference. When you are happy with your settings, click Start Configuration.

Ports Configuration Completed



Enterprise Network Interface

Interface Name: enterprise

LACP Mode: Disabled

IP Address: 22

Subnet Mask: 24

Default Gateway: 22

DNS Servers: 123

Static Routes: 2

[Edit](#)

Management Network Interface

Interface Name: management

IP Address: 32

Subnet Mask: 255

[Edit](#)

Intracluster Link Network

Interface Name: cluster

LACP Mode: Disabled

IP Address: 169

Subnet Mask: 255

Static Routes: 2

[Edit](#)

Internet Network Interface

Interface Name: internet

IP Address: 55

Subnet Mask: 255

[Edit](#)

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



注

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

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

この設定プロセスには約 **90** 分かかります。プロセス中もウィザード画面が継続的に更新され、現在実行しているタスクとその進行状況、発生したエラーが示されます。この情報のローカルコピーをテキストファイルとして保存するには、ダウンロードアイコンをクリックします。

Cisco Catalyst Center
Advanced Install

Appliance Configuration In Progress

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

Initializing the cluster using kubeadm

50%

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

Download

```

2024-03-22T16:04:38.088Z13 | front-proxy-client.crt Apr 13 17:40:20 2020
GMT Apr 13 17:40:20 2021 GMT
2024-03-22T16:04:38.088Z14 | kubelet.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z15 | admin.conf Apr 13 12:12:14 2020 GMT Apr
13 17:40:21 2021 GMT
2024-03-22T16:04:38.088Z16 | scheduler.conf Apr 13 12:12:14 2020 GMT
Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z17 | controller-manager.conf Apr 13 12:12:14
2020 GMT Apr 13 17:40:22 2021 GMT
2024-03-22T16:04:38.088Z18 | -----
                
```

タスクが完了した後：

- クラスタ内の3番目および最後のノードとして展開する追加のアプライアンスがある場合には、この手順を繰り返します。
- クラスタへのノードの追加が終了したら、初回セットアップを実行して続行します。 [初期設定ワークフロー](#) (256ページ)

Catalyst Center

最新の **Catalyst Center** リリースにアップグレードできます。

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

第8章

章

:

- [Cisco Catalyst Center](#)
- [Cisco Catalyst Center](#)
- [Cisco Catalyst Center](#)
- [Cisco Catalyst Center](#)
- [Cisco ISE](#) [Cisco Catalyst Center](#)
- [Cisco Catalyst Center](#)
- [SNMP](#)

Catalyst Center アプライアンスの初期セットアップに関する情報を表示します。

Catalyst Center アプライアンスの設置に関する情報。

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

- この作業を完了するために必要なパラメータ情報については、[必要な初期設定情報](#)（71ページ）を参照してください。
- 実稼働環境に高可用性（HA）を展開している場合、HA の動作を最適化するためにクラスタノード間でサービスを再配布する必要があります（[HA のアクティブ化](#)（292ページ）を参照）。アプライアンスの SNMP 設定を行った後、この手順を完了します。

Catalyst Center ブラウザのサポートに関する情報。

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

- Google Chrome : バージョン 93 以降
- Mozilla Firefox : バージョン 92 以降

Catalyst 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。

Catalyst Center

Catalyst Center アプライアンスをインストールして設定した後、次の手順に従って初めてその GUI にログインします。

Catalyst Center アプライアンスをインストールして設定した後、次の手順に従って初めてその GUI にログインします。初回は管理者スーパーユーザーとしてログインします（ユーザー名は「admin」でPER-ADMIN-ROLE が割り当てられます）。

注

Catalyst Center にアクセスする際には、互換性のある HTTPS 対応ブラウザを使用してください。詳細については、『[互換性のあるブラウザ](#)（256ページ）を参照してください。

Before you begin

Catalyst Center にログインできるように、次の情報を用意してください。

- **admin** スーパーユーザーのユーザー名とパスワードを、**Catalyst Center** アプライアンスの設定時に指定しました。
- 『[必要な初期設定情報](#)（71ページ）に記載されている情報。

1. Catalyst Center GUI にアクセスします。

a) Catalyst Center アプライアンスの再起動が完了したら、次のいずれかのタスクを実行します。

- ブラウザベースの構成ウィザードを使用した場合：ウィザードの最後のページで **[Open Catalyst Center Virtual Appliance]** をクリックします。
- Maglev 構成ウィザードを使用した場合：互換性のある HTTPS 対応のブラウザを起動します。
HTTPS:// と設定プロセスの最後に表示された **Catalyst Center GUI** の IP アドレスを使用して、**Catalyst Center GUI** にアクセスするホスト IP アドレスを入力します。

次のいずれかのメッセージが表示されます（使用しているブラウザによって異なります）。

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

b) **[Advanced]** をクリックして続行します。

次のいずれかのメッセージが表示されます。

- **Google Chrome**：

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

- **Mozilla Firefox**：

```
Someone could be trying to impersonate the site and you should not
continue.
Websites prove their identity via certificates.
Firefox does not trust GUI-IP-address because its certificate issuer is
unknown,
the certificate is self-signed, or the server is not sending the correct
intermediate certificates.
```

こうしたメッセージが表示されるのは、コントローラが自己署名証明書を使用しているためです。
Catalyst Center での証明書の使用方法については、『[Cisco Catalyst Center Administrator Guide](#)』の
「**Certificate and private key support**」の項を参照してください。

c) 続行するには、次のいずれかのタスクを実行します。

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

2. Catalyst Center にログインします。

a) Catalyst Center ログインウィンドウが開いたら、次のいずれかの構成ウィザード完了タスクを実行します。

- Maglev 構成ウィザードを完了し、**[Start using DNAC pre manufactured cluster]** オプションを選択した場合は、管理者のユーザー名（**admin**）とパスワード（**P@ssword9**）を入力します。
- Maglev 構成ウィザードを完了し、**[Start configuration of DNAC in advanced mode]** オプションを選択した場合は、**Catalyst Center** アプライアンスの構成時に設定した管理者のユーザー名（**admin**）とパスワードを入力します。

- インストール構成ウィザードを完了したら、管理者のユーザー名 (**admin**) を入力し、ウィザードの最後のウィンドウからコピーしたパスワード (**P@ssword9**) を貼り付けます。
- 高度なインストール構成ウィザードを完了した場合は、**Catalyst Center** アプライアンスの構成時に設定した管理者のユーザー名 (**admin**) とパスワードを入力します。

b) [Log In] をクリックします。

3. セキュリティ対策として新しい管理ユーザーを設定します。

a) 次の情報を入力します。

- **[Roles]** : SUPER-ADMIN ロールがすでに設定されていることを確認します。
- **[New Username]** : 管理者ユーザーのユーザー名を入力します。
- **[Email]** : 管理者ユーザーの電子メールアドレスを入力します。
- **[New Password]** および **[Confirm Password]** : 管理者ユーザーのパスワードを入力します。このパスワードが、[パスワード要件 \(73ページ\)](#) の「Plan the Deployment」の章にある「Password requirements」を参照してください。



注

デフォルトパスワードの変更は、特に仮想アプライアンスをセットアップするユーザーがその管理者となるユーザーと異なる場合に、ネットワークセキュリティにとって重要です。

b) [Submit] をクリックします。

Catalyst Center ログアウトされます。

4. Catalyst Center に再度ログインします :

- [Log In] をクリックします。
- 新しい管理者ユーザーに関して設定したユーザー名とパスワードを入力します。
- [Log In] をクリックします。

cisco.com のログイン情報を使用して認証するように求められます。これらのログイン情報は、ソフトウェアダウンロードの登録と、システム通信の受信に使用されます。

5. [Authenticate] をクリックします。



注

今すぐ認証を行わない場合は、[Skip] をクリックします。

6. [Activate your device] ポップアップウィンドウで、アクティベーションコードが表示されていることを確認し、[Next] をクリックします。

[Terms & Conditions] 画面が開き、ソフトウェアのシスコ エンドユーザー ライセンス契約 (EULA) および現在利用可能な補足条件へのリンクが表示されます。

7. 各ドキュメントを確認したら、[Next] をクリックして EULA に同意します。

[Quick Start Overview] スライドが開きます。[>] をクリックすると、**Catalyst Center** の使用を開始するために、クイック スタート ワークフローで完了までサポートされるタスクの説明が表示されます。

クイック スタート ワークフローまたはいずれかの高度なセットアップ方式を完了することで、初回セットアップを続行できます。詳細については、「[クイック スタート ワークフローの完了 \(259ページ\)](#)」および「[Catalyst Center の設定方法 \(264ページ\)](#)」を参照してください。

デバイスを検出し、それらのデバイスのテレメトリ収集を有効にする方法について説明します。

このワークフローを完了して、**Catalyst Center** がデバイスからのテレメトリの収集を管理および有効化するデバイスを検出します。

注

または、強化されたセットアップ方式のいずれかを使用して **Catalyst Center** を設定することもできます。詳細については、[Catalyst Center の設定方法 \(264ページ\)](#) を参照してください。

管理者スーパーユーザーとして初めてログインすると（ユーザー名 admin と **SUPER-ADMIN-ROLE** が割り当てられた）、クイック スタート ワークフローが自動的に開始されます。

Before you begin

以下の前提条件を満たしていることを確認します。

- 初期セットアップ：初めて **Catalyst Center** にログインし、新しい管理者ユーザーを作成した。詳細については、[Catalyst Center への初回ログイン \(256ページ\)](#) を参照してください。
- 必要な情報：『[Cisco Catalyst Center Installation Guide](#)「必要な初期設定情報」に記載されている情報を手元に用意してください。

次の機能が含まれています。

- ユーザーアクセス計画：システムにアクセスする必要があるユーザーのリスト（そのユーザーのロール、一意のパスワード、権限設定を含む）。
- サービス統合（オプション）：IPAM サーバーまたは **Cisco Identity Services Engine (ISE)** を使用する場合は、関連する URL とログイン情報を用意しておきます。

1. [Quick Start Overview] スライドで、[Let's Do it] を選択します。

2. [Discover Devices: Provide IP Ranges] 画面で、次の情報を入力し、[Next] を選択します。

- デバイス検出ジョブの名前。
- 検出するデバイスの IP アドレスの範囲。追加の範囲を入力するには、[+] を選択します。

- アプライアンスのループバックアドレスを優先管理 IP アドレスとして指定するかどうかを指定します。詳細については、『[Cisco Catalyst Center User Guide](#)』の「[Discover Your Network](#)」章の「[Preferred management IP address](#)」トピックを参照してください。

3. **[Discover Devices: Provide Credentials]** 画面で、設定するログイン情報のタイプに関する情報（「[デバイスログイン情報](#)（260ページ）」を参照）を入力し、**[Next]** を選択します。

4. **[Create Site]** 画面で、テレメトリを容易にするために検出するデバイスを 1 つのサイトにグループ化し、**[Next]** を選択します。

サイトの情報を手動で入力するか、提供されたマップで使用する場所をクリックします。

5. **[Enable Telemetry]** 画面で、**Catalyst Center** にテレメトリを収集させるネットワークコンポーネントを選択し、**[Next]** をクリックします。

注

[Enable Telemetry] オプションと **[Disable Telemetry]** オプションの両方がグレー表示されている場合、これは、デバイスがテレメトリをサポートできないか、デバイスがテレメトリの有効化をサポートしていない OS バージョンを実行していることを示しています。

6. **[Summary]** 画面で、入力した設定を確認し、次のいずれかを実行します。

- 変更を加える場合は、該当する **[Edit]** リンクをクリックして、関連画面を開きます。
- 設定に問題がなければ、**[Start Discovery and Telemetry]** をクリックします。**Catalyst Center** によって設定が検証され、問題が発生しないことが確認されます。検証が完了すると、画面が更新されます。

Catalyst Center により、ネットワークのデバイスを検出し、選択したネットワークコンポーネントのテレメトリを有効にするプロセスが開始されます。このプロセスには 30 分以上かかります（大規模なネットワークの場合はさらに長くなります）。

ホームページの上部に、クイック スタート ワークフローが完了したことを示すメッセージが表示されます。

- **[View Discovery]** を選択して **[Discovery]** ページを開き、ネットワーク内のデバイスが検出されたことを確認します。
- **[Go to Network Settings]** リンクを選択し、**[Device Credentials]** ページを開きます。ここから、以前に入力したログイン情報がサイトに設定されていることを確認できます。
- **[View Activity Page]** リンクを選択して **[タスク (Tasks)]** ページを開き、**Catalyst Center** ですでに実行がスケジュールされているタスク（セキュリティアドバイザリの毎週のネットワークスキャンなど）を表示します。
- **[Workflow Home]** リンクを選択し、ネットワークのセットアップと維持に役立つガイド付きワークフローにアクセスします。

[Discover Devices: Provide Credentials] 画面で入力する必要がある情報について説明します。

次の表に、クイックスタートワークフローを完了するときに[デバイスの検出：ログイン情報の入力（Discover Devices: Provide Credentials）]画面に入力する必要がある情報を示します。

60 :

フィールド	説明
[CLI (SSH) Credentials]	
Username	ネットワーク内のデバイスの CLI にログインするために使用するユーザー名。
パスワード	ネットワーク内のデバイスの CLI にログインするために使用するパスワード。入力するパスワードは、 8 文字以上にする必要があります。
Name/Description	CLI ログイン情報の名前または説明。
パスワードの有効化	CLI でより高い権限レベルを有効にするために使用するパスワード。ネットワークデバイスで必要な場合にのみ、このパスワードを設定します。

[SNMP Credentials: SNMPv2c Read] タブ



Catalyst Center は、**FIPS** モードが有効になっている場合、**SNMPv2c** ログイン情報をサポートしません。代わりに、**SNMPv3** ログイン情報を入力する必要があります。**FIPS** モードの詳細については、[Maglev ウィザードを使用したプライマリノードの設定（107ページ）](#)を参照してください。

Name/Description	SNMPv2c 読み取りコミュニティストリングの名前または説明。
Community String	デバイス上の SNMP 情報を表示するためにのみ使用される読み取り専用コミュニティストリングパスワード。

[SNMP Credentials: SNMPv2c Write] タブ

Name/Description	SNMPv2c 書き込みコミュニティストリングの名前または説明。
Community String	デバイス上の SNMP 情報を変更するために使用される書き込みコミュニティストリング。

[SNMP Credentials: SNMPv3]

Name/Description	SNMPv3 ログイン情報の名前または説明。
Username	SNMPv3 ログイン情報に関連付けられているユーザー名。

フィールド	説明
Mode	SNMP メッセージを必要とするセキュリティレベル。 • [No Authentication, No Privacy] (noAuthnoPriv) : 認証も暗号化も行いません。 • [Authentication, No Privacy] (authNoPriv) : 認証は行いますが、暗号化は行いません。 • [Authentication and Privacy] (authPriv) : 認証と暗号化の両方を行います。  注 FIPS モードが有効な場合、Catalyst Center では [Authentication and Privacy] モードのみがサポートされます。

Authentication Password

SNMPv3 を使用するデバイスから情報にアクセスするために必要なパスワード。パスワードの長さは、最低 8 文字である必要があります。次の点に注意してください。

- 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレスコントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスではCatalyst Centerによる検出、監視、管理が行われなくなります。
- パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

フィールド	説明
Authentication Type	[Authentication and Privacy] または [Authentication、No Privacy] が認証モードとして設定されている場合に使用されるハッシュベースのメッセージ認証コード (HMAC) タイプ。 • [SHA] : HMAC-SHA 認証。 • [MD5] : HMAC-MD5 認証。  注 Catalyst Center は、FIPS モードが有効になっている場合、この認証タイプをサポートしません。
Privacy Type	プライバシー タイプ。([Mode] として [Authentication and Privacy] を選択した場合に有効になります)。次のいずれかのプライバシー タイプを選択します。 • [AES128] : 暗号化の 128 ビット CBC モード AES。 • CISCOAES192 : シスコのデバイス上での暗号化の 192 ビット CBC モード AES。 • CISCOAES256 : シスコのデバイス上での暗号化の 256 ビット CBC モード AES。  注 • 検出機能とインベントリ機能の使用は、プライバシータイプ CISCOAES192 および CISCOAES256 のみでサポートされています。Assurance 機能はサポートされていません。 • プライバシー タイプ AES128 は、検出、インベントリ、および Assurance でサポートされています。
Privacy Password	

フィールド	説明
	AES128、AES192、および AES256 暗号化標準規格でサポートされているデバイスで交換されるメッセージを暗号化するための秘密鍵を生成するために使用される SNMPv3 プライバシーパスワード。パスワード（またはパスフレーズ）は、8 文字以上にする必要があります。  注 - 一部のワイヤレスコントローラでは、パスワードは少なくとも 12 文字以上にする必要があります。ワイヤレス コントローラのパスワードの最小要件を必ず確認してください。パスワードに必要な最低限の文字数が守られないと、デバイスでは Catalyst Center による検出、監視、管理が行われなくなります。 - パスワードはセキュリティ上の理由から暗号化されており、この設定では表示されません。

NETCONF

Port Cisco IOS-XE を実行するワイヤレスコントローラを検出するために **Catalyst Center** が使用する必要がある **NETCONF** ポート。

Catalyst Center

利用可能なセットアップ方法のいずれかを使用して **Catalyst Center** を設定できます。

初めてログインすると、クイックスタートワークフローが自動的に開始します。高度なセットアップ方法を表示するには、クイックスタートワークフローを終了し、デフォルトのホームページに移動します。デフォルトのホームページには、利用可能なセットアップ方法が表示されます。

Welcome, Admin1

Connect, secure, and automate your network operations using Catalyst Center.
Select your preferred set up method.

Express set up

In the Express set up, you will complete the steps that are needed to onboard network devices.

- Create network hierarchy
- Configure telemetry settings
- Discover devices
- Assign devices to site

Select express

Standard set up Recommended

In the Standard set up, you will complete the steps that are needed to set up the system and onboard network devices.

System set up

- Update Catalyst Center software
- Connect to Smart account
- Add authentication and policy servers
- Add users (local and external auth)
- Configure backup [Backup guide](#)

Network device onboarding

- Create network hierarchy
- Configure telemetry settings
- Discover devices
- Assign devices to site

Select standard

Expert set up

In the Expert set up, you can follow a self-guided approach to set up the system and onboard network devices with your own steps using the navigation menu. Once the sites or devices are available in the system, the dashboard will be shown with health and monitoring data.

Select expert

SUPER-ADMIN-ROLE 権限または **NETWORK-ADMIN-ROLE** 権限がある場合は、次のいずれかの方法を使用して **Catalyst Center** を設定できます。

- **エクスプレスセットアップ**：このセットアップは、ネットワークデバイスの導入準備に役立ちます。手順については、[\[Complete the express setup method\]](#) を参照してください。

- 標準セットアップ：この推奨セットアップは、システムの設定およびネットワークデバイスの導入準備に役立ちます。手順については、「[Complete the standard setup method](#)」を参照してください。
- エキスパートセットアップ：この自己指定セットアップでは、システムとオンボーディングのネットワークデバイスを個別に設定できます。このオプションは、エキスパートユーザーにのみ推奨します。この説明については、[エキスパート設定の完了](#)（269ページ）を参照してください。

注

あるセットアップ方法を開始した後で、別のセットアップ方法を使用する場合は、選択した方法を変更できます。デフォルトのホームページに戻り、[Select <setup method name>] をクリックして、別のセットアップ方法を開始してください。

Express

高速セットアップメソッドを使用して **Catalyst Center** を設定するには、次の手順に従います。

高速セットアップメソッドを使用して **Catalyst Center** を設定するには、次の手順に従います。

Before you begin

[Catalyst Center](#) への初回ログイン（256ページ）が正常に完了したことを確認してください。

1. ホームページで、[Select express] をクリックします。

Expressセットアップメソッドが起動し、[Design > Network Hierarchy] ページが開きます。[Express set up] スライドインペインでは、このセットアップメソッドを完了するための手順が表示されます。

ヒント

- 提示されている順序で手順を完了することを推奨します。
- [Go to this step] をクリックすると、任意の手順の関連ページを表示できます。
- [Expressセットアップ] スライドインペインをいつでも閉じるには、[Exit] をクリックします。ダイアログボックスで、[Exit] をもう一度クリックします。
- リストされている手順のいずれかを完了した後、**Catalyst Center** の右上にある [Express set up] をクリックすることで、このスライドインペインを再度開くことができます。
- このスライドインペインの最下部までスクロールし、[<Number of> steps completed] セクションを開きます。完了した手順を未完了としてマークするには、その手順の [Mark as complete] チェックボックスをオンにします。手順が不完全になり、進行状況バーがこの変更を反映して更新されます。

2. ネットワーク階層の作成手順を完了します。

a) [Design > Network Hierarchy] ページで、エリア、建物、フロアを含むネットワーク階層を作成します。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Design the Network Hierarchy」の章を参照してください。

- b) **[Create network hierarchy]** で、この手順では **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、4 つの手順のうちいずれかが完了したことが示されます。

3. テレメトリ設定の手順を完了します。

- a) **[Configure telemetry settings]** で、**[Go to this step]** をクリックします。
- b) **[Telemetry]** の **[Design > Network Settings]** ページのテレメトリデータ収集に必要な設定を行います。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry」を参照してください。

- c) **[Configure telemetry settings]** で、この手順の **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、4 つの手順のうち 2 つの手順が完了したことが示されます。

4. デバイスの検出手順を完了します。

- a) **[Discover devices]** で、**[Go to this step]** をクリックします。

デバイスのオンボーディングワークフローが開始されます。

- b) オンボーディングデバイスワークフローを完了して、デバイスを検出します。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Do Discovery」を参照してください。

- c) **[Discover devices]** で、**[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、4 つの手順のうち 3 つの手順が完了したことが示されます。

5. サイトへのデバイスの割り当て手順を完了します。

- a) **[Assign devices to site]** で、**[Go to this step]** をクリックします。
- b) **[Provision > Inventory]** ページで、関連するサイトにデバイスを割り当てます。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Assign an unprovisioned device to a site」または「Assign a provisioned device to a different site」を参照してください。

- c) **[Assign devices to site]** で、**[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、4 つの手順のうち 4 つの手順が完了したことが示されます。完了メッセージには、作成されたサイト数と検出されたデバイス数が要約されます。

6. **[Launch home page]** をクリックして、Catalyst Center のエクスプレスセットアップを完了します。

Catalyst Center のエクスプレスセットアップが完了すると、ホームページが表示されます。

注

検出されたデバイスがホームページに表示されるまでに時間がかかる場合があります。

標準のセットアップ方法を使用して **Catalyst Center** を設定するには、次の手順に従います。

標準のセットアップ方法を使用して **Catalyst Center** を設定するには、次の手順に従います。

Before you begin

Catalyst Center への初回ログイン (256ページ) が正常に完了したことを確認してください。

1. ホームページから、[Select standard] をクリックします。

標準のセットアップ方法では、起動して **[System > Software Management]** ページを開きます。標準セットアップスライドインペインでは、このセットアップ方法を完了するための手順が表示されます。

ヒント

- 提示されている順序で手順を完了することを推奨します。
- **[Go to this step]** をクリックすると、任意の手順の関連ページを表示できます。
- 標準セットアップスライドインペインは、**[Exit]** をクリックすることでいつでも閉じることができます。ダイアログボックスで、**[Exit]** をもう一度クリックします。
- リストされている手順のいずれかを完了した後、**Catalyst Center** の右上にある **[Standard set up]** をクリックすると、このスライドインペインを再度開くことができます。
- このスライドインペインの最下部までスクロールし、**[<Number of> steps completed]** セクションを開きます。完了した手順を未完了としてマークするには、その手順の **[Mark as complete]** チェックボックスをオンにします。手順が不完全になり、進行状況バーがこの変更を反映して更新されます。

2. Catalyst Center ソフトウェアの更新の手順を完了します。

- [System > Software Management]** ページで、**Catalyst Center** ソフトウェアを最新の推奨バージョンに更新します。

手順については、「[Cisco Catalyst Center Upgrade Guide](#)」を参照してください。

- [Update Catalyst Center software]** で、この手順の **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうちいずれかが完了したことが示されます。

3. スマートアカウントへの接続の手順を完了します。

- [Connect to Smart account]** で、**[Go to this step]** をクリックします。
- [Smart Account]** ページで、シスコスマートアカウントをスマートライセンス アカウントに接続します。

手順については、『[Cisco Catalyst Center Administrator Guide](#)』の「Configure Smart Account」を参照してください。

- [Connect to Smart account]** で、この手順は **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 2 つが完了したことが示されます。

4. 認証サーバーおよびポリシーサーバーの追加手順を完了します。

- a) **[Add authentication and policy servers]** で、**[Go to this step]** をクリックします。
- b) **[Authentication and Policy Servers]** ページで、Cisco Identity Services Engine (Cisco ISE) または AAA サーバーを追加します。

Catalyst Center は AAA サーバーをユーザー認証に使用し、Cisco ISE をユーザー認証とアクセス制御の両方に使用します。手順については、『[Cisco Catalyst Center Administrator Guide](#)』の「Configure authentication and policy servers」を参照してください。

- c) **[Add authentication and policy servers]** で、[この手順では **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 3 つが完了したことが示されます。

5. ユーザーの追加手順を完了します。

- a) **[Add users (local and external auth)]** で、**[Go to this step]** をクリックします。
- b) **[User Management]** ページで、必要なユーザーを追加して、ユーザーが Catalyst Center にアクセスできるようにします。

手順については、『[Cisco Catalyst Center Administrator Guide](#)』の「Create an internal user」を参照してください。

- c) 外部ユーザーの認証と許可に外部サーバーを使用している場合、外部認証を有効にする必要があります。

手順については、『[Cisco Catalyst Center Administrator Guide](#)』の「Configure external authentication」を参照してください。

- d) **[Add users (local and external auth)]** で、この手順の **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 4 つが完了したことが示されます。

6. バックアップの設定手順を完了します。

- a) **[Configure backup]** で、**[Go to this step]** をクリックします。
- b) **[System > Backup & Restore]** ページで、Catalyst Center の自動化および Assurance データをバックアップするようにリモートサーバーを設定し、Catalyst Center の自動化および Assurance データを復元するようにリモートサーバーを接続します。

手順については、『[Cisco Catalyst Center Administrator Guide](#)』の「Configure the location to store backup files」および「Restore data from backups」を参照してください。

- c) **[Configure backup]** で、この手順の **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 5 つが完了したことが示されます。

7. ネットワーク階層の作成手順を完了します。

- a) **[Create network hierarchy]** で、**[Go to this step]** をクリックします。
- b) **[Design > Network Hierarchy]** ページで、エリア、建物、フロアを含むネットワーク階層を作成します。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Design the Network Hierarchy」の章を参照してください。

- c) **[Create network hierarchy]** で、この手順では **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つ中 6 つの手順が完了したことが示されます。

8. テレメトリ設定の手順を完了します。

- a) **[Configure telemetry settings]** で、**[Go to this step]** をクリックします。

- b) **[Telemetry]** の **[Design > Network Settings]** ページのテレメトリデータ収集に必要な設定を行います。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Configure syslog, SNMP traps, NetFlow Collector servers, and wired client data collection using telemetry」を参照してください。

- c) **[Configure telemetry settings]** で、この手順の **[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つの手順のうち 7 つが完了したことが示されます。

9. デバイスの検出手順を完了します。

- a) **[Discover devices]** で、**[Go to this step]** をクリックします。

デバイスのオンボーディングワークフローが開始されます。

- b) オンボーディングデバイスワークフローを完了して、デバイスを検出します。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Do Discovery」を参照してください。

- c) **[Discover devices]** で、**[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つのうち 8 つの手順が完了したことが示されます。

10. サイトへのデバイスの割り当て手順を完了します。

- a) **[Assign devices to site]** で、**[Go to this step]** をクリックします。

- b) **[Provision > Inventory]** ページで、関連するサイトにデバイスを割り当てます。

手順については、『[Cisco Catalyst Center User Guide](#)』の「Assign an unprovisioned device to a site」または「Assign a provisioned device to a different site」を参照してください。

- c) **[Assign devices to site]** で、**[Mark as complete]** チェックボックスをオンにします。

進行状況バーが更新され、9 つ中 9 つの手順が完了したことが示されます。完了メッセージには、作成されたサイト数と検出されたデバイス数が要約されます。

11. [Launch home page] をクリックして、Catalyst Center の標準セットアップを完了します。

Catalyst Center の標準セットアップが完了すると、ホームページが表示されます。



注

検出されたデバイスがホームページに表示されるまでに時間がかかる場合があります。

エキスパート設定メソッドを使用して Catalyst Center を設定するには、次の手順に従います。

エキスパート設定メソッドを使用して Catalyst Center を設定するには、次の手順に従います。

Before you begin

 注

専門ネットワーク管理者のみがこのセットアップ方法を使用することを推奨します。このメソッドでは、詳細なセットアップ手順は提供されません。Express および標準のセットアップ方法では、アップグレード方法が順に説明されています。詳細については、[Catalyst Center の設定方法](#) (264ページ) を参照してください。

Before you begin

[Catalyst Center](#) への初回ログイン (256ページ) が正常に完了したことを確認してください。

1. ホームページで、[Select expert] をクリックします。
2. [Expert set up] ダイアログボックスで、[OK] をクリックして続行します。
3. ネットワークの必要に応じて **Catalyst Center** を設定してください。

ネットワーク設定の一般的な手順については、次の情報を参照してください。

- 『[Cisco Catalyst Center User Guide](#)』の「ネットワーク階層の設計」の章を参照してください。
- 『[Cisco Catalyst Center User Guide](#)』の「ネットワークの検出」の章を参照してください。
- 『[Cisco Catalyst Center User Guide](#)』の「インベントリの管理」の章を参照してください。

デバイス検出が完了すると、デフォルトのホームページが表示され、**Catalyst Center** のエキスパート設定が完了したことを示します。

Cisco ISE Catalyst Center

Cisco ISE と Catalyst Center を統合する方法について説明します。

Catalyst Center は、Cisco ISE と信頼された通信リンクを作成するメカニズムを備えており、Cisco ISE と安全な方法でデータを共有できます。Cisco ISE が Catalyst Center に登録されると、Catalyst Center が検出するすべてのデバイスが、関連する設定データやその他のデータとともに Cisco ISE にプッシュされます。ユーザーは Catalyst Center を使用してデバイスを検出でき、検出されたデバイスは両方のアプリケーションに表示されるため、Catalyst Center と Cisco ISE の両方の機能を適用できます。また Catalyst Center デバイスと Cisco ISE デバイスはすべて、デバイス名で一意に識別されます。

Catalyst Center デバイスは、Catalyst Center サイト階層内の特定のサイトにプロビジョニングされて割り当てられると、すぐに Cisco ISE にプッシュされます。Catalyst Center デバイスのアップデート (IP アドレス、SNMP または CLI のログイン情報、Cisco ISE 共有秘密情報など) はすべて、自動的に ISE 上の対応するデバイスインスタンスに送信されます。

 注

Catalyst Center デバイスが Cisco ISE にプッシュされるのは、Cisco ISE が AAA サーバー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りです。

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

- ネットワークに 1 つ以上の Cisco ISE ホストを展開済みであること。サポートされている Cisco ISE バージョンの詳細については、『[Catalyst Center Compatibility Matrix](#)』を参照してください。Cisco ISE のインストールについては、『[Cisco Identity Services Engine インストールおよびアップグレードガイド](#) [英語]』を参照してください。
- スタンドアロン Cisco ISE 展開環境がある場合は、Catalyst Center を Cisco ISE ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス (ERS) を有効にする必要があります。

 注

pxGrid 2.0 では Cisco ISE の展開で最大 4 つの pxGrid ノードを使用できますが、Catalyst Center 2.2.1.x 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 Cisco ISE 展開がある場合 :
 - Catalyst Center をプライマリポリシー管理ノード (PAN) と統合し、PAN 上で ERS を有効にする必要があります。

 注

PAN 経由で ERS を使用することを推奨します。ただし、バックアップの場合は、PSN 上で ERS を有効にできます。

- 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。これを行うこともできますが、PAN 上で pxGrid サービスを有効化する必要はありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
- TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers] > [Trustsec] > [Trustsec Servers] > [Trustsec AAA Servers]** でも定義する必要があります。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』を参照してください。
- ネットワーク管理者ロールの権限を持つユーザーのみが Cisco ISE と Catalyst Center を統合できます。
- Cisco ISE で [Use CSRF Check for Enhanced Security] オプションが有効になっている場合、Catalyst Center は ERS API アクセスをサポートしません。
- ポート 443、5222、8910、9060 で Catalyst Center と Cisco ISE の通信を有効にする必要があります。

- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Catalyst Center から到達できる必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリック アンダーレイ ネットワークに到達できません。
- Cisco ISE サービスで使用する証明書に対してオンライン証明書ステータスプロトコル (OCSP) または証明書失効リスト (CRL) 検証が定義されている場合、Catalyst Center は証明書失効ステータスをチェックします。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名 (SAN) のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- FQDN のみのシステム証明書を使用できるかどうかは、Catalyst Center 展開で LAN 自動化が有効になっているかどうかによって異なります。詳細については、『[Catalyst Center Security Best Practices Guide](#)』の「alt_names」セクションを参照してください。

注

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

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、[Cisco Cloud APIC リリースノート \[英語\]](#) を参照してください。

Catalyst Center に対応した Cisco ISE の設定の詳細については、『[Cisco Identity Services Engine 管理者ガイド](#)』の「Integration with Catalyst Center」を参照してください。

1. Cisco ISE の pxGrid サービスと ERS を有効にします。
 - a) プライマリポリシー管理ノードにログインします。
 - b) Cisco ISE GUI で、メニューアイコンをクリックして次を選択します。[Administration] > [System] > [Deployment]。
[Deployment Nodes] ウィンドウが表示されます。
 - c) pxGrid サービスを有効化する Cisco ISE ノードのホスト名をクリックします。分散型展開の場合、これは展開環境内の任意の Cisco ISE ノードです。
[ノードの編集 (Edit Node)] ウィンドウが表示されます。
 - d) [General Settings] タブをクリックし、[pxGrid] チェックボックスをオンにして、[Save] をクリックします。
 - e) Cisco ISE GUI で、メニューアイコンをクリックして次を選択します。[Administration] > [System] > [Settings]。
 - f) 左側のナビゲーションペインから、[API Settings > API Service Settings] を選択します。
 - g) [ERS (Read/Write)] を有効にして、[OK] をクリックします。
 - h) [保存 (Save)] をクリックします。
2. Cisco ISE ノードを AAA サーバとして Catalyst Center に追加します。
 - a) Catalyst Center GUI にログインします。
 - b) メインメニューから次を選択します。[System] > [System 360] の順に選択します。

- c) [Identity Services Engine (ISE)] ペインで、[設定 (Configure)] リンクをクリックします。
- d) [Authentication and Policy Servers] ウィンドウで、[Add] をクリックし、ドロップダウンリストから [ISE] を選択します。
- e) [Add ISE server] スライドインペインで、次の情報を入力します。

- [Server IP Address] フィールドに、Cisco ISE サーバーの IP アドレスを入力します。
- ネットワークデバイスと Cisco ISE の通信を保護するために使用する [共有秘密 (Shared Secret)] を入力します。
- 該当する Cisco ISE 管理ログイン情報を [Username] と [Password] フィールドに入力します。
- Cisco ISE ノードの FQDN を入力します。
- (任意) Cisco ISE PSN が背後に配置されているロードバランサの仮想 IP アドレスを入力します。異なるロードバランサの背後に複数のポリシー サービス ノードファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。
- [Connect to pxGrid] : pxGrid 接続を有効にするには、[Advanced Settings] でこのチェックボックスをオンにします。

Catalyst Center システム証明書を pxGrid クライアント証明書として使用する場合 (pxGrid クライアントとして Catalyst Center システムを認証するために ISE に送信)、[Use Catalyst Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ認証局 (CA) で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Catalyst Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Catalyst Center 証明書が、Cisco ISE で使用中の CA と同じ CA によって生成されていること (そうでない場合、pxGrid 認証は失敗します)。
- [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。
- [Advanced Settings] エリアで、以下の手順を実行します。
 - [RADIUS] または [TACACS] のチェックボックスをオンにして、使用する必要があるプロトコルを選択できます。
 - 次のフィールドに必要な値を入力します：[Authentication Port]、[Accounting Port]、[Retries]、および [Timeout seconds]。

注

このオプションは、Catalyst Center がサードパーティの証明書を使用している場合にのみ使用できます。Catalyst Center がデフォルトの自己署名システム証明書を使用する場合、このオプションは無効になっています。

- f) [Add] をクリックします。

Cisco ISE との統合を開始すると、Cisco ISE からの証明書がまだ信頼されていないという通知が表示されます。証明書を表示して詳細を確認できます。

[Accept] をクリックして証明書を信頼し、統合プロセスを続行するか、証明書を信頼せず、統合プロセスを終了する場合は、[Decline] を選択します。

統合が正常に完了すると、確認メッセージが表示されます。

統合プロセスに問題がある場合は、エラーメッセージが表示されます。必要に応じて、編集または再試行のオプションが表示されます。

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

3. Catalyst Center が Cisco ISE に接続していること、Cisco ISE SGT グループとデバイスが Catalyst Center にプッシュされることを確認します。

- Catalyst Center GUI にログインします。
- メインメニューから次を選択します。[System] > [System 360] の順に選択します。
- [Identity Services Engine (ISE)] ペインで、リストされているすべての ISE サーバーのステータスの表示が [Available] または [Configured] になっていることを確認します。
- [Identity Services Engine (ISE)] ペインで、[Update (更新)] リンクをクリックします。
- [認証サーバとポリシーサーバ (Authentication And Policy Servers)] ウィンドウで、Cisco ISE AAA サーバのステータスがまだ [アクティブ (Active)] であることを確認します。

4. 次のように Cisco ISE が Catalyst 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。

- [Identity Services Engine (ISE) Deployment] ペインで pxGrid サーバーとして表示されている Cisco ISE ノードにログインします。
- [Administration] > [pxGrid Services] の順に選択し、[Web Clients] タブをクリックします。

Catalyst Center サーバーの IP アドレスとともに pxGrid クライアントがリストに表示されます。

Catalyst Center をインストールまたはアップグレードする場合、Cisco ISE からポリシーデータを移行する必要があります。この作業で Catalyst Center と Cisco ISE のポリシーデータが同期されます。グループベースのアクセスコントロールポリシー機能を使用する前に、この同期を完了しておく必要があります。

Catalyst Center

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

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

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

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

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

ポリシーで参照される Cisco ISE の SGACL はすべて、Catalyst Center の契約と比較されます。

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

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

注

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

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

- 送信元グループと宛先グループのポリシーで Cisco ISE の同じ SGACL または契約名を参照している場合、変更は行われません。

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

注

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

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

- 1つのポリシーに含まれる複数の SGACL。
- ポリシーレベルの catch-all ルールは [Permit] または [Deny] に設定されています現在の移行では [None] の値のみ Catalyst Center サポートされています。
- お客様が作成した SGACL を使用するよう設定されたデフォルトポリシー。ただし、Catalyst Center への移行では現在、[Permit IP]、[Permit_IP_Log]、[Deny IP]、[Deny_IP_Log] の標準値のみサポートされています。

ポリシーの移行と同期の操作中に前述のいずれかの SGACL が検出された場合、通知が生成されます。続行するには、次のいずれかのオプションを選択する必要があります。

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

Catalyst Center の AAA サーバーおよび Cisco ISE を設定するための手順。

Catalyst 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。

- **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、**Catalyst Center** および **Cisco ISE** が統合されていることを確認します。
- **Catalyst Center** の FIPS モードが有効になっている場合は、**Catalyst Center** と **Cisco ISE** の統合時に **KeyWrap** を有効にしてください。「[Integrate Cisco ISE with Catalyst Center](#)」の手順 2e を参照してください。

注

Catalyst Center と **Cisco ISE** がすでに統合されている場合、**KeyWrap** を有効にすることはできません。この機能を有効にするには、**Cisco ISE** を削除してから **Catalyst Center** と再統合する必要があります。

- 他の製品（**Cisco ISE** 以外）で AAA 機能を使用している場合、必ず次のタスクを実行してください。
 - AAA サーバーで **Catalyst Center** を登録します。これには、AAA サーバーと **Catalyst Center** の共有秘密を定義することが含まれます。
 - AAA サーバーで **Catalyst Center** の属性名を定義します。
 - **Catalyst Center** マルチホストクラスタの設定の場合は、AAA サーバーのマルチホストクラスタに、すべての個別のホスト IP アドレスと仮想 IP アドレスを定義します。
- **Cisco ISE** を設定する前に、以下の点を確認してください。
 - **Cisco ISE** をネットワークに展開していること。サポートされている **Cisco ISE** バージョンの詳細については、『[Catalyst Center Compatibility Matrix](#)』を参照してください。**Cisco ISE** のインストールについては、『[Cisco Identity Services Engine Install and Upgrade Guides](#)』を参照してください。
 - スタンドアロン ISE 展開環境がある場合は、**Catalyst Center** を **Cisco ISE** ノードと統合し、そのノード上で pxGrid サービスと外部 RESTful サービス（ERS）を有効にする必要があります。

注

pxGrid 2.0 では **Cisco ISE** の展開で最大 4 つの pxGrid ノードを使用できますが、**Catalyst Center 2.2.1.x** 以前のリリースは 2 つを超える pxGrid ノードをサポートしていません。

- 分散型 **Cisco ISE** 展開がある場合：
 - **Catalyst Center** をプライマリポリシー管理ノード（PAN）と統合し、PAN 上で ERS を有効にする必要があります。

 注

PAN経由でERSを使用することを推奨します。ただし、バックアップの場合は、PSN上でERSを有効にできます。

- 分散型展開環境内のいずれかの Cisco ISE ノード上で pxGrid サービスを有効化する必要があります。これを行うこともできますが、PAN 上で pxGrid サービスを有効化する必要はありません。分散型展開環境にある任意の Cisco ISE ノード上で pxGrid を有効にできます。
- TrustSec または SD-Access のコンテンツと PAC を処理するように Cisco ISE で設定する PSN は、**[Work Centers] > [Trustsec] > [Trustsec Servers] > [Trustsec AAA Servers]** でも定義する必要があります。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』を参照してください。
- ポート 443、5222、8910、9060 で Catalyst Center と Cisco ISE の通信を有効にする必要があります。
- pxGrid が有効化されている Cisco ISE ホストには、Cisco ISE eth0 インターフェイスの IP アドレス上の Catalyst Center から到達する必要があります。
- Cisco ISE ノードは、アプライアンス NIC 経由でファブリックアンダーレイ ネットワークに到達できます。
- Cisco ISE 管理ノード証明書のサブジェクト名またはサブジェクト代替名 (SAN) のいずれかに Cisco ISE の IP アドレスまたは FQDN が含まれている必要があります。
- Catalyst Center システム証明書の SAN フィールドに、Catalyst Center アプライアンスの IP アドレスと FQDN の両方がリストされている必要があります。

 注

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

この問題は Cisco ISE 3.0 以降では発生しません。詳細については、[Cisco Cloud APIC リリースノート \[英語\]](#) を参照してください。

1. メインメニューから次を選択します。[System] > [Settings] > [External Services] > [Authentication and Policy Servers]。
2. [Add] ドロップダウンリストから、[AAA] または [ISE] を選択します。
3. プライマリ AAA サーバーを設定するには、次の情報を入力します。
 - [Server IP Address] : AAA サーバの IP アドレス。
 - [Shared Secret] : デバイス認証のキー。共有秘密の長さは、最大 100 文字です。

4. Cisco ISE サーバーを設定するには、次の詳細情報を入力します。

- [Server IP Address] : ISE サーバーの IP アドレス。
- [Shared Secret] : デバイス認証のキー。
- [Username] : Cisco ISE CLI にログインするために使用するユーザー名。

注

このユーザーにはスーパーユーザーの管理権限が必要です。

- [Password] : Cisco ISE CLI ユーザー名に対応するパスワード。
- [FQDN] : Cisco ISE サーバーの完全修飾ドメイン名 (FQDN) 。

注

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

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

hostname.domainname.com

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

- [Virtual IP Address (es)] : Cisco ISE ポリシーサービスノード (PSN) が背後に配置されているロードバランサの仮想 IP アドレス。異なるロードバランサの背後に複数の PSN ファームがある場合は、最大 6 つの仮想 IP アドレスを入力できます。

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

- [Connect to pxGrid] : pxGrid 接続を有効にするには、このチェックボックスをオンにします。

Catalyst Center システム証明書を pxGrid クライアント証明書として使用する場合 (pxGrid クライアントとして Catalyst Center システムを認証するために Cisco ISE に送信)、[Use Catalyst Center Certificate for pxGrid] チェックボックスをオンにします。動作環境で使用されるすべての証明書を同じ CA で生成する必要がある場合は、このオプションを使用できます。このオプションを無効にすると、Catalyst Center は、システムが使用する pxGrid クライアント証明書を生成するための要求を Cisco ISE に送信します。

このオプションを有効にする場合は、次のことを確認してください。

- Catalyst Center 証明書が、Cisco ISE で使用中の CA と同じ認証局 (CA) によって生成されていること (そうでない場合、pxGrid 認証は失敗します)。
- [Certificate Extended Key Use (EKU)] フィールドに「クライアント認証」が含まれていること。
- [Protocol] : [TACACS] と [RADIUS] (デフォルト)。両方のプロトコルを選択できます。

⚠ 重要

ここで Cisco ISE サーバーの TACAS を有効にしない場合は、ネットワークデバイス認証用に AAA サーバーを設定するときに、**[Design] > [Network Settings] > [Network]**で Cisco ISE サーバーを TACAS サーバーとして設定できません。

- **[Authentication Port]** : AAA サーバーへの認証メッセージのリレーに使用されるポート。デフォルトの UDP ポートは 1812 です。
- **[Accounting Port]** : AAA サーバーへの重要なイベントのリレーに使用されるポート。デフォルトの UDP ポートは 1813 です。
- **[Port]** : デフォルトの TACACS ポートは 49 です。
- **[Retries]** : 接続の試行が中止される前に、Catalyst Center が AAA サーバへの接続を試みた回数。デフォルトの試行回数は 3 回です。
- **[Timeout]** : 接続の試行が中止される前に、デバイスが AAA サーバーの応答を待機するタイムアウト期間。デフォルトのタイムアウトは 4 秒です。

📄 注

必要な情報を入力すると、Cisco ISE は 2 つのフェーズを経て Catalyst Center と統合されます。統合が完了するまでには数分かかります。フェーズごとの統合ステータスは、**[Authentication and Policy Servers]** ウィンドウと **[System 360]** ウィンドウに表示されます。

Cisco ISE サーバー登録フェーズ :

- **[Authentication and Policy Servers]** ウィンドウ : 「進行中」
- **[System 360]** ウィンドウ : 「プライマリ使用可能」

pxGrid サブスクリプション登録フェーズ :

- **[Authentication and Policy Servers]** ウィンドウ : 「アクティブ」
- **[System 360]** ウィンドウ : 「プライマリ使用可能」および「pxGrid 使用可能」

設定された Cisco ISE サーバーのステータスがパスワードの変更により **[FAILED]** と表示されている場合は、**[Retry]** をクリックし、パスワードを更新して Cisco ISE 接続を再同期します。

6. **[Add]** をクリックします。
7. セカンダリサーバーを追加するには、前述の手順を繰り返します。

SNMP

再試行とタイムアウトを含む、SNMP プロパティの設定に関する情報。

SNMP の再試行とタイムアウトの値を設定できます。

SUPER-ADMIN-ROLE 権限を持つユーザー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 Catalyst Center Administrator Guide](#)を参照してください。

1. メインメニューから次を選択します。[System] > [Settings] > [Device Settings] > [SNMP] の順に選択します。
2. 次のフィールドを設定します。
 - [Retries] : 許容されるデバイス接続の最大試行回数。有効な値は 1 ～ 3 です。デフォルトは 3 です。
 - [Timeout (in Seconds)] : タイムアウトになるまでにデバイスとの接続の確立を試みる際に、Catalyst Center が待機する秒数。有効な値は 5 秒間隔で 1 ～ 300 秒の範囲内です。デフォルトは 5 秒です。
3. [保存 (Save)] をクリックします。

 注

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

第9

章

- :
- [\[日本語\] Catalyst Center アプライアンスの展開に関するトラブルシューティング](#)
 - [\[英語\] Catalyst Center アプライアンスの展開に関するトラブルシューティング](#)
 - [\[英語\] Catalyst Center アプライアンスの展開に関するトラブルシューティング](#)
 - [\[英語\] Catalyst Center アプライアンスの展開に関するトラブルシューティング](#)

Catalyst Center アプライアンスの展開に関するトラブルシューティングについて説明します。

アプライアンスで問題が発生したときに使用できるトラブルシューティング タスクへのリンク。

アプライアンス設定に関連する問題をトラブルシュートする場合は、次の手順を実行します。

1. 現在、**Catalyst Center GUI** を使用している場合は、[ログアウト](#) (284ページ)。
2. アプライアンス ハードウェアを再設定するには、「[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#) (86ページ)」での説明のとおり、**CIMC GUI** にログインします。
3. アプライアンス設定を変更するには、[構成ウィザードを使用したアプライアンスの再設定](#) (284ページ) で説明されているように、**Maagelev** 設定ウィザードを起動して使用します。

アプライアンスのネットワークアダプタの詳細については、『[Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide](#)』の「[Managing Adapters section](#)」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。

Catalyst Center GUI からログアウトする手順。

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

Catalyst Center GUI からログアウトするには、右上隅に表示されているユーザー名をクリックし、**[Log Out]** を選択します。

これにより、セッションが終了してログアウトされます。

Catalyst Center アプライアンスを再設定し、構成ウィザードを使用してその設定を更新する手順。

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

アプライアンスを構成した後は、この一部のアプライアンス設定を変更する場合にのみ構成ウィザードを使用します。

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

- 管理ユーザのパスワード。
- NIC ボンディングの有効化

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

1. お使いのブラウザで、Cisco IMC GUI 設定で設定した Cisco IMC の IP アドレスを指定し、Cisco IMC ユーザーとして Cisco IMC GUI にログインします ([Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#) (86ページ) を参照)。
ログインすると、アプライアンスは **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウを表示します。
2. ウィンドウの上部にあるハイパーリンクされたメニューで、**[Launch KVM]** を選択してから、**[HTML based KVM]** を選択します。
KVM コンソールが別ウィンドウまたはタブで自動的に開きます。KVM コンソールを使用して、設定の進行状況をモニターし、Maglev 構成ウィザードのプロンプトに応答します。
3. プロンプトが表示されたら、Linux パスワードを入力します。
4. 次のコマンドを入力して設定ウィザードにアクセスします。

sudo maglev-config update

Catalyst Center 2.3.7.7 以降 :

- **[maglev]** のユーザーパスワードを変更するには、**[Linux Password]** および **[Re-enter Linux Password]** フィールドに新しいパスワードを指定します。パスワードは、[パスワード要件](#) (73ページ) で説明されている要件に準拠している必要があります。これらのフィールドを空白のままにすると、現在のパスワードが引き続き使用されます。
 - その他の設定は、**[maglev]** のユーザーパスワードを入力せずに変更できます。
5. 設定ウィザードには、[Maglev ウィザードを使用したセカンダリノードの設定](#) (131ページ) のように、表示されている画面シリーズの短縮バージョンを示しています。表示された設定を適宜変更します。画面ごとに変更を終えたら **[Next]** を選択して設定ウィザードを続行します。
 6. 設定プロセスの最後に、設定ウィザードが変更の適用を実行できる状態になったことを示すメッセージが表示されます。次のオプションを使用できます。
 - **[戻る (back)]** : 変更を確認して検証します。
 - **[キャンセル (cancel)]** : 変更を破棄して設定ウィザードを終了します。
 - **[続行 (proceed)]** : 変更を保存して、それらの適用を開始します。

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

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

Catalyst Center アプライアンスでウォームリセットを停止または開始する手順。

Catalyst Center アプライアンスで次のいずれかの手順を実行して、アプライアンスを停止するか、ウォームリスタートを実行します。ハードウェアを修復する前にアプライアンスを停止することも、ソフトウェアの問題を修正した後にウォームリスタートを開始することもできます。

注

SSH 手順を完了して、アプライアンスの正常なシャットダウンを実行します。**Catalyst Center** が無応答で、SSH 経由で再起動できない場合にのみ、**Cisco IMC** 手順を完了します。

SSH

SSH を使用してアプライアンスを停止またはウォームリスタートするには、次の手順を実行します。

この手順の前提条件を次に示します。

- **Secure Shell (SSH)** クライアント ソフトウェア。
- 再設定が必要なアプライアンス上の **10 Gbps** エンタープライズポートに設定された **IP アドレス**。ポート **2222** でこのアドレスのアプライアンスにログインします。
前面および背面パネルの背面パネル図を参照して、エンタープライズポートを識別できます。
- 現在ターゲットアプライアンスに設定されている **Linux ユーザ名** (**maglev**) とパスワード。

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

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

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。
3. 次のタスクに適したコマンドを入力します。
 - アプライアンスを停止するには、次のように入力します。 **sudo shutdown -h now**
 - ウォームリスタートを開始するには、次のように入力します。 **sudo shutdown -r now**
Linux パスワードを入力するようプロンプトが表示されたら、再度入力します。
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。
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。

Cisco IMC GUI

Cisco IMC GUI を使用してアプライアンスを停止またはウォームリスタートするには、次の手順を実行します。

 注

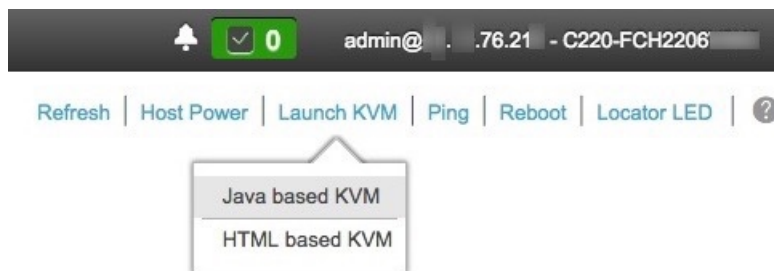
- ターゲットアプライアンスに現在設定されている **Linux** ユーザー名 (*maglev*) とパスワードが必要になります。
- **Cisco IMC GUI** を使用して行ったハードウェアの変更は、アプライアンスのリポート後に適用されることに注意してください。

 注意

データ損失を防ぐには、**SSH**、**Cisco IMC** コンソール、または物理コンソールに応答していない場合にのみ、**Cisco IMC GUI** からアプライアンスの電源をオフにしてください。

1. お使いのブラウザで、**Cisco IMC GUI** 設定で設定した **Cisco IMC** の IP アドレスを指定し、**Cisco IMC** ユーザーとして **Cisco IMC GUI** にログインします。（[Cisco Integrated Management Controller に対するブラウザアクセスの有効化](#)（86ページ）を参照）。

ログインが成功すると、アプライアンスに **[Cisco Integrated Management Controller Chassis Summary]** ウィンドウが、ウィンドウ上部のハイパーリンクメニューとともに表示されます。



2. **[Host Power > Power Cycle]** の順に選択してアプライアンスをリブートします。
アプライアンスの再起動を確認するプロンプトが表示されたら、**[OK]** をクリックします。
3. プロンプトが表示されたら、**Linux** パスワードを入力します。

付録

A

:

- □□□ HA □□□
- □□□□□□□□□□□□□□□□□□
□□□□□□□□ HA □□□
- □□□□□□□□□□□□□□□□□□
□□□□□□□□□ HA □□□
- HA □□□□□□□
- HA □□□□□□□□□□□□□□□□

Catalyst Center の HA クラスタ展開シナリオ。

Catalyst Center の HA の実装については、『[Cisco Catalyst Center High Availability Guide](#)』を参照してください。最初にこの情報を確認してから、実稼働環境に HA を展開するかどうかを決定するようお勧めします。続行する場合は、次のタスクを完了します。

1. 次のとおりネットワークに適した導入手順を実行します。
 - [新しい HA の展開](#) (290ページ)
 - [標準インターフェイス設定を使用したプライマリノードの既存 HA の展開](#) (290ページ)
 - [非標準インターフェイス設定を使用したプライマリノードの既存 HA の展開](#) (291ページ)
2. [HA のアクティブ化](#) (292ページ) クラスタ上の Catalyst Center 。
3. 「[HA の展開に関する追加の考慮事項](#) (292ページ)」を参照し、必要に応じて追加のテレメトリまたはワイヤレスコントローラの設定を行います。

HA

Catalyst Center 用の新しい HA クラスターをインストールする手順。

新しい HA クラスターをインストールするには、次の手順を実行します。

1. 次のとおり、最初にインストールされたアプライアンスをプライマリノードとして設定します。

- Maglev 設定ウィザードを使用している場合は「[Maglev ウィザードを使用したプライマリノードの設定 \(107ページ\)](#)」を参照してください。
- ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「[詳細インストール構成ウィザードを使用したプライマリノードの設定](#)」を参照してください。
 - [32 または 56 コアアプライアンス](#)
 - [80 コアアプライアンス](#)

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

- Maglev 設定ウィザードを使用している場合は「[Maglev ウィザードを使用したセカンダリノードの設定 \(131ページ\)](#)」を参照してください。
 - ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「[詳細インストール構成ウィザードを使用したセカンダリノードの設定](#)」を参照してください。
 - [32 または 56 コアアプライアンス](#)
 - [80 コアアプライアンス](#)
-

HA

プライマリノードが標準のインターフェイス設定を使用する既存の Catalyst Center HA クラスターを展開する手順。

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

1. プライマリノードを Catalyst Center の最新バージョンにアップグレードします。

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

2. プライマリノードに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 \(40ページ\)](#) を参照してください。

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

構成ウィザードを使用したアプライアンスの再設定 (284ページ) を参照してください。

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

- Maglev 設定ウィザードを使用するアプライアンスを設定している場合は「[Maglev ウィザードを使用したセカンダリノードの設定 \(131ページ\)](#)」を参照してください。
- ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「詳細インストール構成ウィザードを使用したセカンダリアプライアンスの設定」を参照してください。
 - [32 または 56 コアアプライアンス](#)
 - [80 コアアプライアンス](#)

5. GlusterFS サイズを確認します。

- Cisco TAC に連絡してチャレンジトークンを取得します。
- 制限されたシェルを開き、**sudo du -h /data/maglev/srv/maglev-system/glusterfs/mnt/bricks/default_brick/ | tail -1 | awk '{print \$1}'** コマンドを実行します。

GlusterFS ファイルシステムのサイズが 150 GBを超えている場合は、[非標準インターフェイス設定を使用したプライマリノードの既存 HA の展開 \(291ページ\)](#) に記載されている手順を完了します。

HA

プライマリノードが標準以外のインターフェイス設定を使用する既存の **Catalyst Center HA** クラスタを展開する手順。

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

1. プライマリノードを **Catalyst Center** の最新バージョンにアップグレードします。

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

2. リモートリポジトリのバックアップを作成します。

[『Cisco Catalyst Center Administrator Guide』](#) の「Backup and Restore」の章を参照してください。

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

[インターフェイスケーブル接続 \(40ページ\)](#) および[Catalyst Center ISO イメージのインストール \(102ページ\)](#) を参照してください。VIP がプライマリノードで正しく設定されていることを確認します。

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

5. ステップ 2 で作成したバックアップファイルを使用して、リモートリポジトリのデータを復元します。

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

- Maglev 設定ウィザードを使用するアプライアンスを設定している場合は「[Maglev ウィザードを使用したセカンダリノードの設定 \(131ページ\)](#)」を参照してください。

- ブラウザベースの構成ウィザードを使用してアプライアンスを設定する場合は、お使いのアプライアンスに固有の「詳細インストール構成ウィザードを使用したセカンダリアプライアンスの設定」を参照してください。
- [32 または 56 コアアプライアンス](#)
- [80 コアアプライアンス](#)

HA

Catalyst Center で HA をアクティブ化する手順。

Catalyst Center の HA の実装については、『[Cisco Catalyst Center High Availability Guide](#)』を参照してください。情報を確認した後、HAが実稼働環境に適しているかどうかを判断してください。続行する場合は、次の展開手順を実行します。

1. メインメニューから次を選択します。[System] > [Settings] > [System Configuration] > [High Availability] の順に選択します。
2. [Activate High Availability] をクリックします。

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

注

Catalyst Center は、データベースの復元、システムアップグレード（パッケージアップグレードではない）の実行、HA のアクティブ化を実行するたび、（前述のとおり）メンテナンスモードになります。

HA

既存の HA 展開の追加設定。

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。

デバイスのテレメトリ設定。

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。

1. `sudo maglev-config update` コマンドを使用して、クラスタ VIP を更新します。
2. デバイスでテレメトリを無効にします。
 - a. Catalyst Center ホームページで [Network Telemetry] を [Tools] エリアから選択します。
[Telemetry] ウィンドウが表示されます。

- b. [Site View] タブをクリックします。
 - c. テレメトリを無効にするデバイスのチェックボックスをオンにします。次に、[Actions] > [Disable Telemetry] を選択します。
3. 以前デバイスに関連付けたプロファイルを使用して、テレメトリをもう一度有効にします。
-

ワイヤレスコントローラの設定。

ワイヤレスコントローラ の新しい VIP を使用してネットワーク内の **Catalyst Center** を更新する必要があります。

翻訳について

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

翻訳について

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

翻訳について

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

翻訳について

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

翻訳について

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

翻訳について

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

翻訳について

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

翻訳について

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