



## VMware ESXi 向け Cisco HyperFlex System リリース 5.0 インストールガイド

初版：2021年11月10日

最終更新：2022年10月14日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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

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

© 2021 –2022 Cisco Systems, Inc. All rights reserved.



## 目次

### Full Cisco Trademarks with Software License ?

はじめに :

通信、サービス、偏向のない言語、およびその他の情報 xi

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

概要 3

Cisco HyperFlex HX シリーズ システム 3

Cisco HyperFlex HX シリーズ システムのコンポーネント 3

Cisco HyperFlex HX シリーズ システムの設定オプション 5

Cisco HyperFlex HX シリーズ システムの管理コンポーネント 7

Cisco HyperFlex Connect ユーザ インターフェイスとオンライン ヘルプ 9

[ダッシュボード (Dashboard)] ページ 11

[動作ステータス (Operational Status)] ダイアログボックス 13

[復元力ヘルス (Resiliency Health)] ダイアログボックス 14

第 3 章

インストールの前提条件 17

Cisco HXDP のサポートされているバージョンとシステム要件 17

必要なハードウェア ケーブル 18

ホスト要件 19

ディスクの要件 19

ポート要件 22

HyperFlex 外部接続 23

ファブリック インターコネクットのアップリンクのプロビジョニング	25
ネットワーク設定	28
VLAN と vSwitch の要件	30
Cisco UCS の要件	31
ハイパーバイザ要件	32
ストレージクラスタ要件	33
vCenter 設定要件	34
システム サービス要件	35
コントローラ VM の CPU リソース予約	37
コントローラ VM 用メモリ リソース予約	38
Auto Support 要件	40
シングルサインオンの要件	41

---

**第 4 章**

<b>Cisco HyperFlex Systems サーバーのインストール</b>	<b>43</b>
ラック設置型 Cisco HyperFlex ノード	43
ファブリック インターコネクットのセットアップ	44
Cisco UCS Manager GUI を使用したプライマリ ファブリック インターコネクットの設定	45
Cisco UCS Manager GUI を使用したセカンダリ ファブリック インターコネクットの設定	47
CLI を使用したプライマリ ファブリック インターコネクットの設定	49
CLI を使用した従属ファブリック インターコネクットの設定	50
コンソールのセットアップの確認	51
HX シリーズ サーバと Cisco UCS ファブリック インターコネクットの接続	53
概要	53
コンバージド ノードとファブリック インターコネクットの接続	53
直接接続モードのクラスタ セットアップの物理的な接続の図	55
コンピューティング専用ノードとファブリック インターコネクットの接続	56

---

**第 5 章**

<b>Cisco HyperFlex Systems の設定</b>	<b>59</b>
設置ワークフロー	59
vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開	60
静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開	63

Syslog の設定	64
HyperFlex クラスタの設定と展開	65
HyperFlex サーバの関連付け	65
UCS Manager の設定	67
ハイパーバイザの構成	71
IP アドレスの設定	73
HyperFlex クラスタの設定	74
GPU が搭載された HyperFlex ノードのインストール	78
HX Data Platform インストーラのナビゲーション支援ボタン	79
警告およびエラー メッセージ	80

---

**第 6 章**

<b>HyperFlex Data Platform でのライセンス設定</b>	<b>81</b>
スマート ライセンスと HyperFlex	81
ライセンスの遵守とフィーチャの機能	86
接続環境でのライセンスの管理	87
スマート ライセンスにクラスタを登録する	87
HX Connect を通してスマート ソフトウェア ライセンスによりクラスタを登録する	88
コントローラ VM を介してスマート ソフトウェア ライセンスとともにクラスタを登録する	90
スマート ライセンスからクラスタを登録解除する	91
スマート ライセンス承認の更新	92
非接続環境でのライセンスの管理	93
スマート ライセンスと Smart Software Manager サテライト	93
特定のライセンス予約および HyperFlex	93
特定のライセンス予約 (SLR) ライセンスのインストール	94
特定のライセンス予約 (SLR) ライセンスのキャンセル	103
特定のライセンス予約 (SLR) ライセンスを返す	104
特定のライセンスの予約のトラブルシューティング (SLR)	107

---

**第 7 章**

<b>HyperFlex ハードウェア アクセラレーション カードの設定</b>	<b>109</b>
HyperFlex ハードウェア アクセラレーション カードの概要	109

Install HyperFlex Hardware Acceleration Cards	110
vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開	111
静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開	113
HyperFlex クラスタの設定と展開	115
クレデンシャルの入力	115
HyperFlex サーバの関連付け	117
UCS Manager の設定	119
ハイパーバイザの構成	123
IP アドレスの設定	125
HyperFlex クラスタの設定	126
HyperFlex ハードウェア アクセラレーション カードの取り付けの確認	130
HyperFlex ハードウェア アクセラレーション カードのトラブルシューティング	131
HyperFlex ハードウェア アクセラレーション カードのに関する追加情報	131

## 第 8 章

クラスタ設定後のタスク	133
クラスタ設定後のガイドライン	133
ホスト上のネットワーク デバイスの PCI パススルー有効化	134
インストール後のスクリプトの実行	135
ESXi ホストのルート パスワードの変更	136
ストレージコントローラのパスワードの変更	137
VMware vCenter の Cisco HyperFlex HTML プラグイン	137
ストレージクラスタでのデータストアの追加	138
HA ハートビートの設定	138
HyperFlex の自動サポートと Smart Call Home	139
HX Connect を使用した自動サポートの設定	140
CLI を使用した通知設定の構成	142
データ収集用の Smart Call Home の設定	143
自己署名の証明書を CA 署名の証明書で置き換える	145
レプリケーション ペアリング	147
プライベート VLAN の追加	147
プライベート VLAN について	147

既存の VM を使用しない VM ネットワーク上でのプライベート VLAN の設定	148
ESX ホスト上でのプライベート VLAN の設定	148
既存の VM を使用した VM ネットワーク上でのプライベート VLAN の設定	149
vSphere 標準スイッチ上での VMNIC の削除	149
vSphere 分散型スイッチの作成	150
vSphere 分散型スイッチ上でのプライベート VLAN の作成	150
分散型ポート グループ内のプライベート VLAN の設定	151
分散型仮想スイッチと Cisco Nexus 1000v	151
HX Data Platform 上での vCenter のホスト	153
AMD GPU の展開	153

---

第 9 章	複数の HX クラスタの設定	155
	複数のクラスタの設定	155

---

第 10 章	Cisco HyperFlex システム クラスタの展開	159
	クラスタ拡張ガイドライン	159
	ESXi インストール ガイドライン	160
	M4/M5/M6 クラスタを拡張する場合の前提条件	161
	混合クラスタ展開のガイドライン - Cisco HX リリース 5.0(x)	161
	混在クラスタ拡張中の手順	162
	コンバージド (HX220c/HX240c) ノードを追加するための前提条件	163
	コンバージド ノードの準備	164
	既存のクラスタにコンバージド ノードを追加する	164
	コンピューティング専用ノードを追加するための前提条件	171
	コンピューティング専用ノードの準備	173
	HX Data Platform インストーラの確認	174
	UCS Manager を使用したコンピューティングのみ ノードへの HX プロファイルの適用	174
	コンピューティング ノードへの VMware ESXi のインストール	174
	既存のクラスタにコンピューティング専用ノードを追加する	176
	クラスタ拡張の障害の解決	182
	ロジカル アベイラビリティ ゾーン	182

---

第 11 章	<b>混在 CPU を伴うクラスタの設定</b>	<b>187</b>
	概要	187
	混合 CPU を使用するための前提条件	187
	EVC モードと CPU の互換性	188
	既存のクラスタでの vMotion との拡張された互換性 (EVC) の有効化	188
	均一クラスタへの新世代サーバの追加	189
	既存のクラスタへの混合または旧世代サーバの追加	190

---

第 12 章	<b>Cisco HyperFlex Systems のカスタマイズされたインストール方法</b>	<b>193</b>
	概要	193
	事前設定されていない Cisco HyperFlex システムのインストールおよび設定のワークフロー	193
	VMware ESXi のインストール	194
	Cisco UCS Manager での vMedia およびブート ポリシーの設定	195
	リモート KVM コンソールを開く	196
	サーバの再起動	197
	vMedia とブート ポリシーの変更を元に戻す	197

---

第 13 章	<b>Cisco HyperFlex Edge の展開</b>	<b>199</b>
	Cisco HyperFlex Edge	199
	HyperFlex Edge 導入オプション	202
	2 ノードネットワーク トポロジの選択	203
	10 または 25 ギガビット イーサネット トポロジ	204
	10 または 25GE VIC ベースのトポロジ	204
	ネットワークの共通要件チェックリスト	212
	ゲスト VM トラフィック	219
	Intersight の接続性	219
	Cisco HyperFlex Edge 非表示クラウド監視	220
	Cisco Hyperflex Edge サーバの注文	220
	1 ギガビット イーサネット トポロジ	220



1 ギガビットイーサネット トポロジ	220
3 ノードまたは 4 ノードのネットワーク トポロジの選択	227
10 または 25GE VIC ベースのトポロジ	227
10/25GE VIC ベース トポロジの Cisco IMC 接続	227
Physical Network and Cabling for 10/25GE VIC-Based Topology	228
10/25GE VIC ベースのスイッチ構成の注意事項	229
3 ノードおよび 4 ノード 10/25GE VIC ベース トポロジの仮想ネットワーク設計	231
1 ギガビットイーサネット トポロジ	232
1 ギガビットイーサネット トポロジ用 Cisco IMC 接続	233
1GE トポロジ用物理ネットワークおよびケーブル接続	233
1 ギガビットイーサネット スイッチ設定時の注意事項	234
3 および 4 ノード 1 ギガビットイーサネット トポロジの仮想ネットワーク設計	235
2 ノード 2 ルームのネットワーク トポロジの選択	237
2 ノード 2 ルームの使用例	238
2 ノード 2 ルームの要件	239
10 または 25 ギガビットイーサネット トポロジ	240
10/25GE クロス接続トポロジ用物理ネットワークとケーブル接続	240
10/25 ギガビットイーサネット クロス接続の物理的なケーブル接続	241
すべての 2 ノード 2 ルーム トポロジの Cisco IMC 接続	242
ルーム単位トポロジでの 10 または 25 ギガビットイーサネット スタック スイッチ	246
ルーム単位トポロジでの 10/25GE スタック スイッチの物理ネットワークとケーブル接続	246
10/25 ギガビットイーサネット スタック スイッチの物理的なケーブル接続	248
ルーム単位トポロジでの 10 または 25 ギガビットイーサネット シングル スイッチ	250
ルーム単位トポロジでの 10/25GE シングル スイッチの物理ネットワークとケーブル接続	250
10/25 ギガビットイーサネット シングル スイッチの物理的なケーブル接続	251
Quality of Service (QoS)	252
ネットワークの共通要件チェックリスト	253
ゲスト VM トラフィック	260
Intersight の接続性	260
Cisco HyperFlex Edge 非表示クラウド監視	261

Cisco Hyperflex Edge サーバの注文	261
インストレーションの概要	261
ラック設置型 Cisco HyperFlex ノード	263
Cisco Integrated Management Controller の構成	263
CIMC の構成：静的割り当て	263
CIMC の構成：DHCP 割り当て	265
ファームウェアバージョンの確認	265
Cisco HX Data Platform インストーラの導入	266
HyperFlex クラスタの設定	267
Cisco HX Data Platform ソフトウェア インストールの確認	274
(10/25GE のみ) HyperFlex クラスタの設定	274
HX Connect へのログイン	278
(1 GbE のみ) インストール後のスクリプトの実行	279
(10/25GE のみ) インストール後のスクリプトの実行	281
vMotion の自動構成	283
手動による vMotion の構成	284
手動によるトラフィック シェーピングの構成	285
(10 / 25GE) 追加 VIC ポートの使用 (オプション)	285
ネットワーク設定例	286



## 通信、サービス、偏向のない言語、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[シスコサービス](#)にアクセスしてください。
- サービスリクエストを送信するには、[Cisco Support](#) にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco Marketplace](#) にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

### マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。

### Cisco バグ検索ツール

[Cisco バグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアの問題に関する詳細な情報を提供します。

### 偏向のない言語

この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナルリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェ

イスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



# 第 1 章

## 新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報 \(1 ページ\)](#)

## 新機能および変更された機能に関する情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。この表は、このマニュアルに加えられた変更やこのリリースの新しい機能をすべて網羅するものではありません。

特長	説明	リリース/日付が追加されました	参照先
HyperFlex ライセンスの有効期限	HyperFlex フィーチャの機能は、有効なソフトウェアライセンスの存在によって管理されます。	5.0(2a)	<a href="#">ライセンスの遵守とフィーチャの機能 (86 ページ)</a>
VMware ESXi 向け Cisco HyperFlex System リリース 5.0 インストールガイド	5.0 ガイドの最初のリリース。	HX 5.0(1a)	このマニュアル





## 第 2 章

### 概要

この章では、Cisco HyperFlex System のコンポーネントの概要を示します。

- [Cisco HyperFlex HX シリーズ システム \(3 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システムのコンポーネント \(3 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システムの設定オプション \(5 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システムの管理コンポーネント \(7 ページ\)](#)
- [Cisco HyperFlex Connect ユーザ インターフェイスとオンラインヘルプ \(9 ページ\)](#)

## Cisco HyperFlex HX シリーズ システム

Cisco HyperFlex HX シリーズ システムは、完全内包型の仮想サーバプラットフォームを通じて、コンピューティング、ストレージ、ネットワークの 3 つのレイヤと強力な Cisco HX Data Platform ソフトウェア ツールを結合し、シングルポイント接続による簡素化された管理を実現します。Cisco HyperFlex HX-Series System は、単一の UCS 管理ドメインに HX ノードを追加することによってスケールアウトするように設計されたモジュラ システムです。ハイパーコンバージドシステムはユーザのワークロード ニーズに基づいて統一されたリソースのプールを提供します。

## Cisco HyperFlex HX シリーズ システムのコンポーネント

- **Cisco HX シリーズ サーバー**：次のいずれかのサーバーを使用して Cisco HyperFlex システムを設定できます。
  - **コンバージド ノード — オールフラッシュ**：Cisco HyperFlex HXAF240c M6、HXAF220c M6、HXAF240c M5、HXAF220c M5、HXAF240c M4 および HXAF220c M4。
  - **コンバージド ノード — ハイブリッド**：Cisco HyperFlex HX240c M6、HX220c M6、HX240c M5、HX220c M5、HX240c M4 および HX220c M4。
  - **コンピューティングのみ**：Cisco B200 M3/M4、B260 M4、B420 M4、B460 M4、B480 M5、C240 M3/M4、C220 M3/M4、C480 M5、C460 M4、B200 M5、C220 M5/M6 および C240 M5/M6。

- **Cisco HX Data Platform** : HX Data Platform は次のコンポーネントで構成されています。
  - **Cisco HX Data Platform インストーラ** : ストレージクラスタに接続されているサーバにこのインストーラをダウンロードします。HX Data Platform インストーラは、Cisco UCS Manager 内のサービス プロファイルとポリシーを設定し、コントローラ VM を展開し、ソフトウェアをインストールし、ストレージクラスタを作成し、VMware vCenter プラグインを更新します。
  - **Storage Controller VM** : HX Data Platform インストーラ を使用して、管理対象のストレージクラスタ内の各コンバージド ノードにストレージコントローラ VM をインストールします。
  - **Cisco HX Data Platform プラグイン** : この統合 VMware vSphere インターフェイスは、ストレージクラスタ内のストレージをモニタおよび管理します。

- **Cisco UCS ファブリック インターコネクト (FI)**

ファブリック インターコネクトは、接続されている Cisco HX-Series Server にネットワーク接続機能と管理機能の両方を提供します。

Cisco HyperFlex System の一部として購入されて展開された FI は、このドキュメントでは **HXFI** ドメインとも呼ばれます。サポートされているファブリック インターコネクトは次のとおりです。

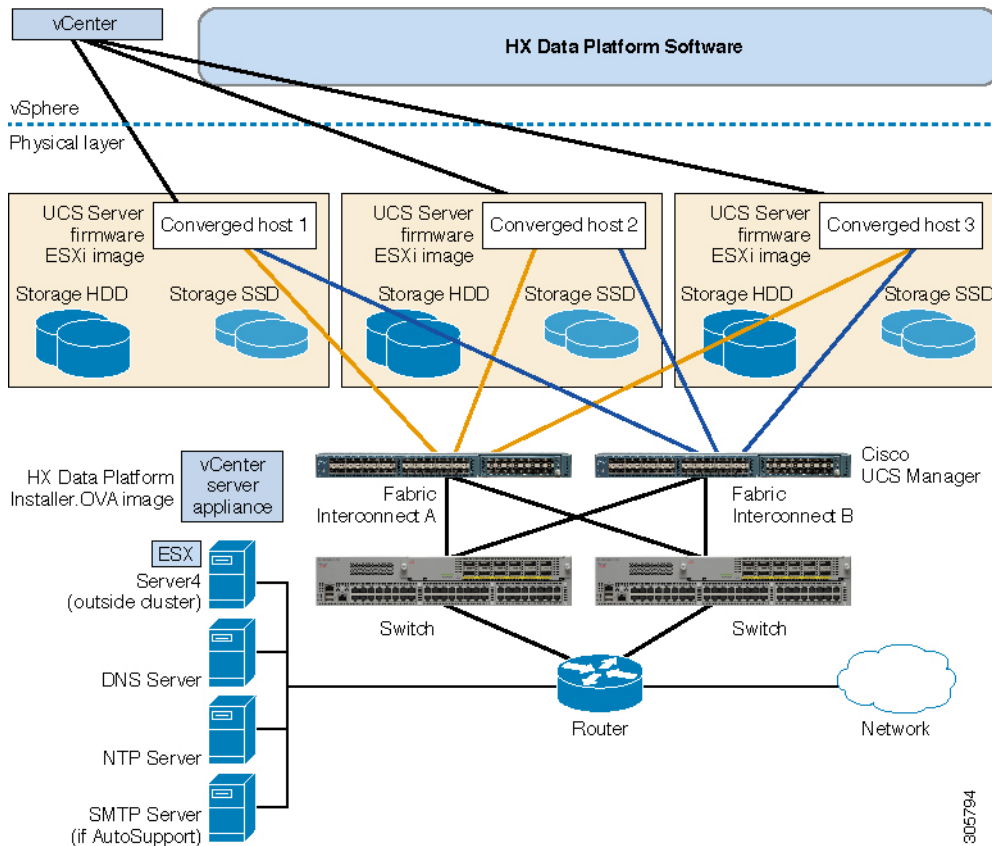
- Cisco UCS 6200 シリーズ Fabric Interconnect
- Cisco UCS 6300 シリーズ Fabric Interconnect
- Cisco UCS 6400 シリーズ ファブリック インターコネクト

- **Cisco Nexus スイッチ**

Cisco Nexus スイッチによって、高密度で設定可能なポートが提供され、柔軟なアクセスの展開と移行を実現できます。



図 1: Cisco HyperFlex HX シリーズ システムのコンポーネント



## Cisco HyperFlex HX シリーズ システムの設定オプション

Cisco HyperFlex HX シリーズ システムは、環境内でストレージおよびコンピューティング機能を拡張するための柔軟でスケーラブルなオプションを提供します。Cisco HyperFlex システムにストレージ機能を追加するには、Cisco HyperFlex Server を追加するだけです。



(注) **HX クラスタ** は HX シリーズ サーバーのグループです。クラスタ内の各 HX シリーズ サーバは、HX ノードまたはホストと呼ばれます。

HX クラスタはさまざまな方法で構成できます。次の図に、一般的な構成例を示します。最新の互換性とスケーラビリティの詳細については、『Cisco HyperFlex 推奨ソフトウェアリリースおよび要件ガイド』の [Cisco HX Data Platform Compatibility and Scalability Details - 5.0\(x\) Releases](https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/release-guidelines-and-support-timeline/b-recommended-hx-data-platform-sw-releases/m-recommended-releases.html) の章を参照してください。

図 2: Cisco HyperFlex ハイブリッド M5 設定

HX220c M5S Cluster	HX240c M5S Cluster	HX240c M5L Cluster	HX M5 + Compute Node Cluster
6.0TiB <sup>1</sup> – 171.4TiB <sup>1</sup>	6.0TiB <sup>1</sup> – 492.7TiB <sup>1</sup>	31.1TiB <sup>1</sup> – 442.4TiB <sup>1</sup>	HX M5 Cluster + HX Compatible M3, M4 & M5 Compute Nodes <small>NOTE: Consult Release Notes for Compute Node Support Details</small>
Smallest Footprint (VDI, ROBO)	Capacity-Heavy (VDI & VSI Workloads)	Capacity-Heavy (High Capacity Workloads)	Compute-Heavy Hybrid (Compute Bound Apps/VDI)
Per-Node 1 x Cache SSD 6-8 x 1.2TB or 1.8TB or 2.4TB Capacity HDDs (SED options available)	Per-Node 1 x Cache SSD 6-23 x 1.2TB or 1.8TB or 2.4TB Capacity HDDs Support up to 2 GPUs (SED options available)	Per-Node 1 x Cache SSD 6-12 x 6TB or 8TB or 12TB** Capacity HDDs	HX220 or HX240 Node Cluster + Compute Nodes Blade or Rack Local Disk, SD Card or SAN Boot

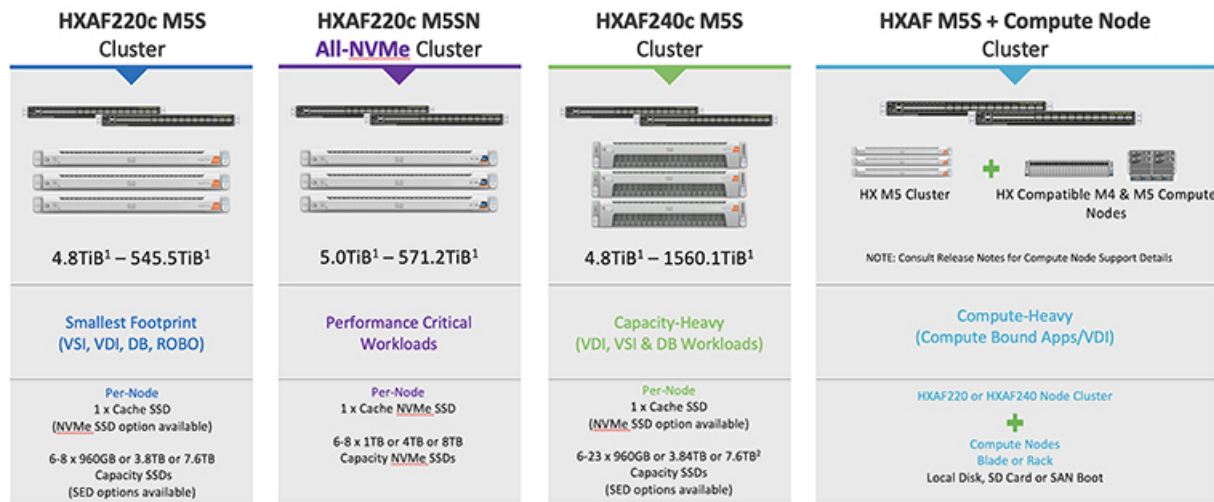
<sup>1</sup>Usable capacity w/ RFB before compression and deduplication

図 3: Cisco HyperFlex ハイブリッド M4 設定

HX220c M4 Edge Cluster	HX220c M4 Cluster	HX240c M4 Cluster	HX M4 + Compute Node Clusters
*4.51TB – 9.03TB	**6.01TB – 24.07TB	**6.01TB – 92.29TB	HX Nodes + HX Compatible M3, M4 & M5 Compute Nodes
Smallest Footprint 3 Node Cluster (VSI, ROBO)	Smallest Footprint 3-8 Node Cluster (VDI, ROBO)	Capacity-Heavy 3-8 Node Cluster (VDI & VSI Workloads)	Compute-Heavy Hybrid (Compute Bound Apps/VDI)
Per-Node 1x Cache SSD 3-6 x 1.2TB Capacity HDDs	Per-Node 1x Cache SSD 6 x 1.2TB or 1.8TB Capacity HDDs SED Options Available	Per-Node 1x Cache SSD 6-23 x 1.2TB or 1.8TB Capacity HDDs Up to 1 x GPU (2 x GPU w/ SEDs) SED Options Available	3-8 HX220 or HX240 Node Cluster + Up to 8 Compute Nodes Blade or Rack Local Disk, SD Card or SAN Boot

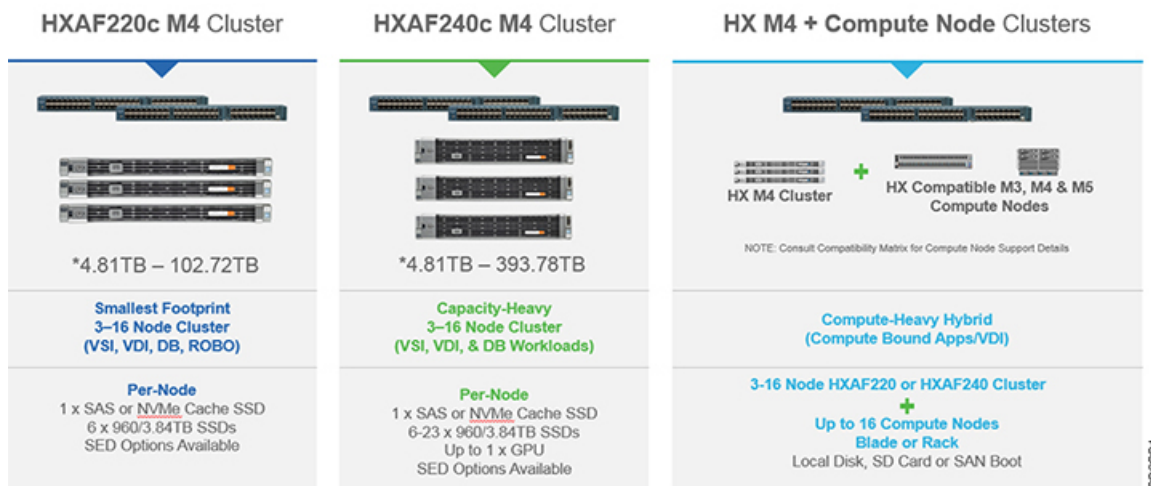
306803

図 4: Cisco HyperFlex オール フラッシュ M5 設定



<sup>1</sup>Usable capacity w/ Rf3 before compression and deduplication  
<sup>2</sup>Max Converged node limit is 16 when using more than 12 x 7.6TB drives per node

図 5: Cisco HyperFlex オール フラッシュ M4 設定



3006301

# Cisco HyperFlex HX シリーズ システムの管理コンポーネン ト

Cisco HyperFlex HX シリーズ システムは、次のシスコ ソフトウェア コンポーネントを使用して管理されます。

## Cisco UCS Manager

Cisco UCS Manager は、ファブリック インターコネクットのペア上に存在する組み込みソフトウェアで、Cisco HX-Series Server のすべての設定機能と管理機能を備えています。UCS Manager

にアクセスする最も一般的な方法は、Web ブラウザを使用して GUI を開くことです。UCS Manager は、ロールベースのアクセス制御をサポートしています。

設定情報を 2 台の UCS Fabric Interconnects (FI) 間で複製することにより、高可用性ソリューションが実現します。一方の FI が使用不能になっても、もう一方が代わりに務めます。

UCS Manager の主なメリットは、ステートレス コンピューティングという概念です。HX クラスターの各ノードには設定がありません。たとえば、MAC アドレス、UUID、ファームウェア、BIOS 設定はすべて、サービス プロファイルの UCS Manager で設定され、すべての HX シリーズサーバーに均一に適用されます。これにより、設定の一貫性が保たれ、再利用が容易になります。新しいサービス プロファイルを数分以内に適用することができます。

### Cisco HX Data Platform

Cisco HyperFlex Data Platform は、複数の Cisco サーバーをコンピューティング/ストレージリソースからなる単一のプールに変換する、ハイパーコンバージドソフトウェア アプライアンスです。これにより、ネットワーク ストレージの必要性がなくなり、VMware vSphere およびその既存の管理アプリケーションと緊密に統合して、シームレスなデータ管理エクスペリエンスが提供されます。加えて、ネイティブな圧縮と重複排除により、VM が占有する記憶域が削減されます。

HX Data Platform をインストールする場所は、vSphere などの仮想化プラットフォームです。仮想マシン、アプリケーション、およびデータ用のストレージを管理します。インストール時に Cisco HyperFlex HX クラスタ名を指定すると、HX Data Platform は各ノード上にハイパーコンバージドストレージクラスタを作成します。ストレージを増やす必要があり、HX クラスタにノードを追加する場合、Cisco HX データ プラットフォームは追加のリソース全体でストレージの平衡化を行います。

### VMware vCenter 管理

Cisco HyperFlex System には、VMware vCenter ベースの管理機能があります。vCenter サーバーは、仮想化環境をモニターするために開発されたデータセンター管理サーバーアプリケーションです。HX Data Platform にも事前設定済みの vCenter サーバーからアクセスして、すべてのストレージのタスクを実行します。vCenter は、VMware vMotion、DRS、HA、および vSphere レプリケーションをサポートします。VMware スナップショットおよびクローニング機能に代わって、より拡張性の高いネイティブの HX Data スナップショットとクローンが使用されます。

HX Data Platform にアクセスするには個別のサーバーに vCenter インストールされている必要があります。vCenter は vSphere Client を通じてアクセスされ、それは管理者のラップトップまたは PC にインストールされています。

# Cisco HyperFlex Connect ユーザ インターフェイスとオンライン ヘルプ


Cisco HyperFlex Connect (HX Connect) は、Cisco HyperFlex のユーザ インターフェイスを提供します。左側のナビゲーションペインと右側の作業ペインの2つの主要なセクションに分かれています。



**重要** HX Connect では、ほとんどのアクションの実行に管理者特権が必要です。

表 1: ヘッダー アイコン

アイコン	名前 (Name)	説明
	メニュー	フルサイズのナビゲーション ペインと、アイコンのみのホバーオーバー ナビゲーション ペインを切り替えます。
	メッセージ	ユーザが開始するアクション (データ ストアの作成やディスクの削除など) の一覧が表示されます。 すべてのメッセージを削除して、メッセージアイコンを非表示にするには、[すべて消去 (Clear All)] を使用します。
	設定	[サポート (Support)]、[通知 (Notification)]、および[クラウド管理 (Cloud Management)] の設定にアクセスします。また [サポートバンドル (Support Bundle)] ページにアクセスすることもできます。
	アラーム	現在のエラーまたは警告のアラーム カウントが表示されます。エラーと警告の両方が存在する場合、カウントはエラー数を示します。 アラーム情報の詳細については、[アラーム (Alarms)] ページを参照してください。
	ヘルプ	状況に応じた HX 接続 のオンライン ヘルプ ファイルを開きます。
	ユーザ	タイムアウト設定やログアウトなどの設定にアクセスします。 [ユーザ設定 (User Settings)] は管理者にのみ表示されます。

アイコン	名前 (Name)	説明
	情報	その要素に関する詳細データにアクセスします。

オンラインヘルプにアクセスするには：

- ユーザインターフェイスの特定のページで、ヘッダーにある **[ヘルプ (Help)]** をクリックします。
- ダイアログボックスで、そのダイアログボックスの **[ヘルプ (Help)]** ボタンをクリックします。
- ウィザードで、**[ヘルプ (Help)]** をクリックします。

#### テーブルヘッダーの共通フィールド

HX Connect 内のいくつかのテーブルには、テーブルに表示される内容を左右する次の3つのフィールドのどれかが表示されます。

UI 要素	基本的な情報
<b>[更新 (Refresh)]</b> フィールドとアイコン	<p>HX クラスタの動的更新では、テーブルが自動的に更新されます。タイムスタンプは、テーブルが最後に更新された時刻を示します。</p> <p>コンテンツを今すぐ更新するには、円形アイコンをクリックします。</p>
<b>[フィルタ (Filter)]</b> フィールド	<p>入力したフィルタテキストと一致するリスト項目のみがテーブルに表示されます。以下の表の<b>現在</b>のページに一覧表示されている項目は自動的にフィルタ処理されます。入れ子になったテーブルはフィルタ処理されません。</p> <p><b>[フィルタ (Filter)]</b> フィールドに選択テキストを入力します。</p> <p><b>[フィルタ (Filter)]</b> フィールドを空にするには、<b>x</b> をクリックします。</p> <p>テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてフィルタを適用します。</p>


UI 要素	基本的な情報
[エクスポート (Export) ]メニュー	<p>テーブルデータの現在のページのコピーを保存します。テーブルコンテンツは、選択したファイルの種類でローカルマシンにダウンロードされます。リストの項目をフィルタ処理すると、フィルタ処理されたサブセット リストがエクスポートされます。</p> <p>エクスポート ファイルの種類を選択するには、下向き矢印をクリックします。ファイルの種類オプションは、cvs、xls、および doc です。</p> <p>テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてエクスポートを適用します。</p>


## 【ダッシュボード (Dashboard)】ページ



**重要** 読み取り専用ユーザの場合は、ヘルプに記載されているすべてのオプションが表示されないことがあります。HyperFlex (HX) Connect では、ほとんどのアクションの実行に管理者権限が必要です。

HX ストレージクラスタのステータスの概要が表示されます。これは、Cisco HyperFlex Connect にログインすると最初に表示されるページです。

UI 要素	基本的な情報
[動作ステータス (Operational Status) ]セクション	<p>HX ストレージクラスタの機能ステータスとアプリケーション パフォーマンスが表示されます。</p> <p>[情報 (Information) ] (  ) をクリックして、HX ストレージクラスタ名とステータス データにアクセスします。</p>

UI 要素	基本的な情報
[クラスタライセンスの状態 (Cluster License Status)] セクション	<p>HX ストレージクラスタに初めてログインしたとき、または HX ストレージクラスタ ライセンスが登録されるまでに、次のリンクが表示されます。</p> <p>クラスタライセンスが登録されていないリンク : HX ストレージクラスタが登録されていない場合に表示されます。クラスタライセンスを登録するには、このリンクをクリックし、[スマートソフトウェアライセンス製品登録 (Smart Software Licensing Product Registration)] 画面で製品インスタンス登録トークンを指定します。製品インスタンス登録トークンを取得する方法の詳細については、『Cisco HyperFlex システムインストールガイド』の「スマートライセンスへのクラスタの登録」セクションを参照してください。</p>
[復元力ヘルス (Resiliency Health)] セクション	<p>HX ストレージクラスタのデータヘルスステータスと耐障害性が表示されます。</p> <p>[情報 (Information)] (  ) をクリックして復元力ステータスと、レプリケーションおよび障害データにアクセスします。</p>
[容量 (Capacity)] セクション	<p>ストレージ合計の内訳と使用中または未使用のストレージ容量が表示されます。</p> <p>また、ストレージの最適化、圧縮による節約、およびクラスタに格納されているデータに基づく重複排除比率も表示されます。</p>
[ノード (Nodes)] セクション	<p>HX ストレージクラスタにおけるノード数とコンバージドノード対コンピューティングノードの区分が表示されます。ノードアイコンの上にカーソルを合わせると、ノードの名前、IP アドレス、ノードタイプが表示されます。また、容量、使用率、シリアル番号、およびディスクタイプデータにアクセスできるディスクがインタラクティブに表示されます。</p>
[パフォーマンス (Performance)] セクション	<p>設定可能な時間の HX ストレージクラスタのパフォーマンススナップショットが表示され、IOPS、スループット、および遅延データが示されます。</p> <p>詳細については、[パフォーマンス (Performance)] ページを参照してください。</p>
[クラスタ時間 (Cluster Time)] フィールド	<p>クラスタのシステム日時。</p>



### テーブルヘッダーの共通フィールド

HX Connect 内のいくつかのテーブルには、テーブルに表示される内容を左右する次の3つのフィールドのどれかが表示されます。

UI 要素	基本的な情報
[更新 (Refresh)] フィールドとアイコン	<p>HX クラスタの動的更新では、テーブルが自動的に更新されます。タイムスタンプは、テーブルが最後に更新された時刻を示します。</p> <p>コンテンツを今すぐ更新するには、円形アイコンをクリックします。</p>
[フィルタ (Filter)] フィールド	<p>入力したフィルタテキストと一致するリスト項目のみがテーブルに表示されます。以下の表の現在のページに一覧表示されている項目は自動的にフィルタ処理されます。入れ子になったテーブルはフィルタ処理されません。</p> <p>[フィルタ (Filter)] フィールドに選択テキストを入力します。</p> <p>[フィルタ (Filter)] フィールドを空にするには、<b>x</b> をクリックします。</p> <p>テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてフィルタを適用します。</p>
[エクスポート (Export)] メニュー	<p>テーブルデータの現在のページのコピーを保存します。テーブルコンテンツは、選択したファイルの種類でローカルマシンにダウンロードされます。リストの項目をフィルタ処理すると、フィルタ処理されたサブセットリストがエクスポートされます。</p> <p>エクスポートファイルの種類を選択するには、下向き矢印をクリックします。ファイルの種類オプションは、cvs、xls、および doc です。</p> <p>テーブル内の他のページからコンテンツをエクスポートするには、下部までスクロールし、ページ番号をクリックしてエクスポートを適用します。</p>

### [動作ステータス (Operational Status)] ダイアログボックス

HX ストレージクラスタの機能ステータスとアプリケーションパフォーマンスが表示されます。

UI 要素	基本的な情報
[クラスタ名 (Cluster Name) ] フィールド	この HX ストレージクラスタの名前。
[クラスタステータス (Cluster Status) ] フィールド	<ul style="list-style-type: none"> <li>• <b>[オンライン (Online) ]</b> : クラスタは利用可能です。</li> <li>• <b>[オフライン (Offline) ]</b> : クラスタは使用可能ではありません。</li> <li>• <b>読み取り専用</b> : クラスタは、書き込みトランザクションを受け入れることはできませんが、静的ラスタ情報の表示を継続することはできます。</li> <li>• <b>容量不足</b> : クラスタ全体が容量不足であるか、または 1 つ以上のディスクが容量不足です。いずれの場合も、クラスタは、書き込みトランザクションを受け入れることはできませんが、静的ラスタ情報の表示を継続することはできます。</li> </ul>
[休眠データ暗号化対応 (Data-at-rest encryption capable) ] フィールド	<ul style="list-style-type: none"> <li>• <b>使用可能</b></li> <li>• <b>サポート対象外</b></li> </ul> <p>[はい (Yes) ]と[いいえ (No) ]のいずれかを使用できます。</p>
[表示する理由 (Reason to view) ] ドロップダウンリスト	現在のステータスの要因を示すメッセージの数が表示されます。

[閉じる (Close) ] をクリックします。

## [復元カヘルス (Resiliency Health) ] ダイアログボックス

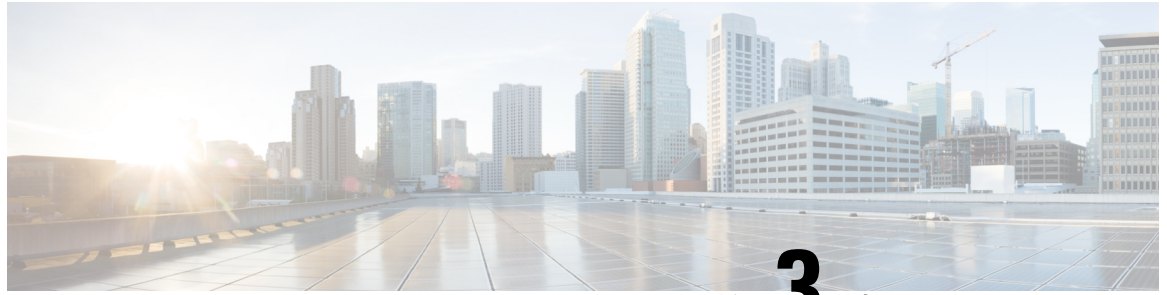
HX ストレージクラスタのデータヘルスステータスと耐障害性が表示されます。

名前 (Name)	説明
[復元カステータス (Resiliency Status) ] フィールド	<ul style="list-style-type: none"> <li>• <b>[正常 (Healthy) ]</b> : クラスタはデータおよび可用性に関して正常な状態です。</li> <li>• <b>[警告 (Warning) ]</b> : データまたはクラスタの可用性に悪影響が生じています。</li> <li>• <b>[不明 (Unknown) ]</b> : クラスタがオンラインになるまでの遷移状態。</li> </ul> <p>色分けとアイコンを使用して、さまざまなステータスの状態が示されます。追加情報を表示するには、アイコンをクリックします。</p>

名前 (Name)	説明
[データ レプリケーション コンプライアンス (Data Replication Compliance) ] フィールド	<ul style="list-style-type: none"> <li>• コンプライアンス対応</li> </ul>
[データ レプリケーション ファクタ (Data Replication Factor) ] フィールド	HX ストレージ クラスタ全体の冗長なデータ レプリカの数が表示されます。
[許容ノード障害数 (Number of node failures tolerable) ] フィールド	HX ストレージ クラスタが処理できるノード中断の数が表示されます。
[許容永続デバイス障害数 (Number of Persistent Device failures tolerable) ] フィールド	HX ストレージ クラスタが処理できる永続デバイス中断の数が表示されます。
[許容キャッシングデバイス障害数 (Number of Caching Device failures tolerable) ] フィールド	HX ストレージ クラスタが処理できるキャッシュ デバイス中断の数が表示されます。
[表示する理由 (Reason to view) ] ドロップダウンリスト	現在のステータスの要因を示すメッセージの数が表示されます。

[閉じる (Close) ] をクリックします。





## 第 3 章

# インストールの前提条件

- [Cisco HXDP のサポートされているバージョンとシステム要件](#) (17 ページ)
- [必要なハードウェア ケーブル](#) (18 ページ)
- [ホスト要件](#) (19 ページ)
- [ディスクの要件](#) (19 ページ)
- [ポート要件](#) (22 ページ)
- [HyperFlex 外部接続](#) (23 ページ)
- [ファブリック インターコネクトのアップリンクのプロビジョニング](#) (25 ページ)
- [ネットワーク設定](#) (28 ページ)
- [VLAN と vSwitch の要件](#) (30 ページ)
- [Cisco UCS の要件](#) (31 ページ)
- [ハイパーバイザ要件](#) (32 ページ)
- [ストレージクラスタ要件](#) (33 ページ)
- [vCenter 設定要件](#) (34 ページ)
- [システム サービス要件](#) (35 ページ)
- [コントローラ VM の CPU リソース予約](#) (37 ページ)
- [コントローラ VM 用メモリ リソース予約](#) (38 ページ)
- [Auto Support 要件](#) (40 ページ)
- [シングル サインオンの要件](#) (41 ページ)

## Cisco HXDP のサポートされているバージョンとシステム要件

Cisco HX Data Platform を正常にインストールするには、特定のソフトウェアおよびハードウェアのバージョン、ネットワーク設定が必要です。

表 2: Cisco HXDP リリース 5.0(x) のサポートされているバージョンとシステム要件

要件	詳細へのリンク
サーバのコンポーネント ファームウェアが、次の表に示されている最小バージョン以上であることを確認します。	詳細については、『 <a href="#">Cisco HyperFlex Software Requirements and Recommendations</a> 』ドキュメントの「 <i>FI/Server Firmware - 5.0(x)</i> リリース」トピックを参照してください。
推奨ブラウザのリスト。	詳細については、 <a href="#">[Cisco HyperFlex ソフトウェアの要件と推奨事項のドキュメント (Cisco HyperFlex Software Requirements and Recommendations)]</a> の「 <a href="#">[ブラウザの推奨事項 (Browser Recommendations)]</a> 」トピックを参照してください。

## 必要なハードウェア ケーブル

- 6200 シリーズ FI を使用する場合は、サーバごとに少なくとも 2 本の 10 Gb Small Form-Factor Pluggable (SFP) ケーブルを使用します。

6300 シリーズ FI を使用する場合は、サーバごとに少なくとも 2 本の 40 GbE QSFP ケーブルを使用します。

- ファブリック インターコネクト コンソール ケーブル (CAB-CONSOLE-RJ45) の一方の端が RJ-45 コネクタで、もう一方の端が DB9 コネクタがあることを確認します。このケーブルは、ラップトップ上の RS-232 コンソール接続に接続するために使用します。

- 標準の電源コードで、電源モジュールとの接続側に IEC C13 コネクタが付いていることを確認します。オプションのジャンパ電源コードで、電源モジュールとの接続側に IEC C13 コネクタ、IEC C13 コンセントとの接続側に IEC C14 コネクタが付いていることを確認します。

詳細については、[Cisco UCS 6200 Series Fabric Interconnect Hardware Guide](#)を確認してください。

- KVM ケーブルは、Cisco HX シリーズ サーバをシステムに接続します。DB9 シリアル コネクタ、モニター用の VGA コネクタ、およびキーボードとマウス用のデュアル USB 2.0 ポートが付いています。このケーブルを使用すると、システムで稼動するオペレーティングシステムや BIOS に直接接続できます。



- (注) この同じ KVM ケーブルが UCS ラック マウント サーバとブレード サーバの両方に使用されます。

M4またはM5サーバ用のケーブルとご注文情報の詳細については、それぞれ『[Cisco HyperFlex HX-Series Models](#)』と『[Cisco UCS B200 Blade Server Installation and Service Note](#)』を参照してください。

## ホスト要件

Cisco HyperFlex クラスタには、少なくとも3つのコンバージドHyperFlex ノードが含まれます。追加のストレージが必要ない場合に計算能力を高めるために、`compute-only` ノードを追加するオプションが用意されています。HyperFlex クラスタ内の各サーバは、HyperFlex ノードとも呼ばれます。ストレージクラスタを展開する前に、各ノードに次の設定がインストールされ、構成されていることを確認してください。

詳細については、『[Cisco HX240c/220c HyperFlex Node Installation Guides](#)』を参照してください。

次のホスト要件が満たされていることを確認します。

- クラスタ内のすべてのサーバ（ノードまたはホスト）で同じ VLAN ID を使用する。
- ストレージクラスタ全体のすべての ESXi サーバで同じ管理者ログインクレデンシャルを使用する。
- すべての ESXi ホストで SSH を有効なままにしてください。
- すべてのサーバ上で DNS と NTP を設定する。
- VMware vSphere をインストールして設定します。
- **VIC および NIC のサポート:**詳細については、『[Cisco HyperFlex Systems: ネットワーキング トポロジ](#)』のマニュアルを参照してください。

## ディスクの要件

コンバージドノードとコンピューティング専用ノードの間ではディスク要件が異なります。使用可能な CPU とメモリ容量を増やすには、必要に応じて、コンピューティング専用ノードで既存のクラスタを拡張できます。このコンピューティング専用ノードによって、ストレージパフォーマンスやストレージ容量が向上するわけではありません。

別の方法として、コンバージドノードを追加すると、CPU リソースやメモリ リソースだけでなく、ストレージパフォーマンスやストレージ容量も増えます。

ソリッドステートディスク (SSD) のみを備えたサーバはオールフラッシュサーバです。SSD とハードディスク ドライブ (HDD) の両方を備えたサーバはハイブリッドサーバです。

HyperFlex クラスタ内のすべてのディスクに以下が該当します。

- ストレージクラスタ内のすべてのディスクに同じストレージ容量が割り当てられます。ストレージクラスタ内のすべてのノードに同じ数のディスクが割り当てられます。

- すべての **SSD** で TRIM をサポートし、TRIM が有効になっている必要があります。
- すべての **HDD** を SATA と SAS のどちらかのタイプにすることができます。ストレージクラスタ内のすべての SAS ディスクをパススルーモードにする必要があります。
- SSD と HDD からディスクパーミッションを削除する必要があります。パーミッション付きのディスクは無視され、HX ストレージクラスタに追加されません。
- オプションで、ディスク上の既存のデータを削除またはバックアップすることができます。指定されたディスク上のすべての既存のデータが上書きされます。



---

(注) 新しいファクトリ サーバは、適切なディスクパーティション設定で出荷されます。新しいファクトリ サーバからディスクパーティションを削除しなくでください。

---

- Cisco から直接購入したディスクのみがサポートされます。
- 自己暗号化ドライブ (SED) を備えたサーバでは、キャッシュドライブと永続ストレージ (容量) ドライブの両方を SED 対応にする必要があります。このようなサーバは、保管中のデータの暗号化 (DARE) をサポートします。
- サポートされていないドライブまたはカタログのアップグレードに関するエラーが表示された場合は、[互換性カタログ](#)を参照してください。

下の表に示すディスクに加えて、すべての M4 コンバージド ノードに、ESX がインストールされたミラー化設定の 2 X 64-GB SD FlexFlash カードが実装されています。すべての M5/M6 コンバージド ノードに、ESX 搭載の M.2 SATA SSD が内蔵されています。





- (注) 1 台のサーバまたはストレージクラスターで、ストレージディスクのタイプやストレージサイズを混在させないでください。ストレージディスク タイプの混在はサポートされません。
- キャッシュディスクまたは永続ディスクを交換する際は、元のディスクと同じタイプとサイズを常に使用します。
  - 永続ドライブを混在させないでください。1 台のサーバでは、すべて HDD または SSD にして、同じサイズのドライブを使用します。
  - ハイブリッドキャッシュドライブタイプとオールフラッシュキャッシュドライブタイプを混在させないでください。ハイブリッドサーバではハイブリッドキャッシュデバイスを使用し、オールフラッシュサーバではオールフラッシュキャッシュデバイスを使用します。
  - 暗号化されたドライブタイプと暗号化されていないドライブタイプを混在させないでください。SED ハイブリッドドライブまたは SED オールフラッシュドライブを使用します。SED サーバでは、キャッシュドライブと永続ドライブの両方を SED タイプにする必要があります。
  - すべてのノードで SSD を同じサイズと数量にする必要があります。異なる SSD タイプを混在させることはできません。

それぞれのサーバでサポートされているドライブのキャパシティと台数の詳細については、対応するサーバモデルの仕様書を参照してください。

既存のクラスターを拡張する際の、互換性のある PID については、[Cisco HyperFlex Drive Compatibility](#) ドキュメントを参照してください。

### コンピューティング専用ノード

次の表に、コンピューティング専用機能にサポートされるコンピューティング専用ノードの構成を示します。コンピューティング専用ノード上のストレージは、ストレージクラスターのキャッシュまたはキャパシティに含まれません。



- (注) クラスターにコンピューティングノードが追加されると、そのノードは、コンピューティング専用のサービスプロファイルテンプレートによって SD カードから起動できるように自動設定されます。別の形式のブートメディアを使用する場合は、ローカルのディスク設定ポリシーを更新してください。サーバに関連したポリシーについては、[Cisco UCS Manager](#) サーバ管理ガイドを参照してください。

サポートされているコンピューティング専用ノードサーバ	ESXi のブートでサポートされている方法
<ul style="list-style-type: none"> <li>• Cisco B200 M4/M5</li> <li>• B260 M4</li> <li>• B420 M4</li> <li>• B460 M4</li> <li>• C240 M4/M5/M6</li> <li>• C220 M4/M5/M6</li> <li>• C460 M4</li> <li>• C480 M5</li> <li>• B480 M5</li> </ul>	<p>任意の方法を選択します。</p> <p><b>重要</b> ESXi インストールでサーバに 1 つの形式のブートメディアだけが公開されていることを確認します。インストール後に、さらにローカルディスクまたはリモートディスクを追加できます。</p> <p>HX コンピューティング専用ノードの USB ブートはサポートされていません。</p> <ul style="list-style-type: none"> <li>• ESXi インストールされているミラー構成での SD カード。</li> <li>• ローカルドライブの HDD または SSD。</li> <li>• SAN ブート</li> <li>• M.2 SATA SSD ドライブ。</li> </ul> <p>(注) HW RAID M.2 (UCS-M2-HWRAID および HX-M2-HWRAID) は、HX Data Platform バージョン 4.5 (1a) 以降でサポートされるブート設定です。</p>

## ポート要件

ネットワークがファイアウォールの背後にある場合は、標準のポート要件に加え、VMware には VMware ESXi および VMware vCenter に対するポートが推奨されます。

- CIP-M は、クラスタ管理 IP に使用します。
- SCVM は、コントローラ VM の管理 IP です。
- ESXi は、ハイパーバイザの管理 IP です。

HyperFlex ソリューションのコンポーネント通信に必要なポートの包括的なリストは、[HX Data Platform Security Hardening Guide](#) の付録 A に記載されています。



**ヒント** 標準設定がなく、異なるポート設定が必要な場合は、環境のカスタマイズについて、[表 C-5 ポートのリテラル値](#)を参照してください。

## HyperFlex 外部接続

外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
Intersight デバイス コネクタ	サポートされている HX システムは、各システムの管理コントローラに組み込まれているデバイスコネクタを介して Cisco Intersight に接続されます。	HTTPSポート番号 : 443 1.0.5-2084 以降 (Cisco Intersight によって自動的にアップグレード)	

外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
			<p>すべてのデバイスコネクタは、                      svc.intersight.com を適切に解決でき、かつポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。現在の HX インストーラでは、HTTP プロキシの使用がサポートされています。</p> <p>ESXi 管理の IP アドレスは、インストーラから ESXi 管理に必要なとされるすべてのポートを介して、Cisco UCS Manager から到達可能である必要があります。これにより、Cisco Intersight から ESXi 管理を展開できるようになります。</p> <p>(注) ESXi ホストによって開始されたポート 443 のアウトバウンド HTTPS 接続は、デフォルトの ESXi ファイアウォールによってブロックできます。この接続を許可するために、ESXi ファイアウォールを一時的に無効にすることができます。</p> <p>ESXi ファイアウォールを無効</p>

外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
			<p>にするには、  <code>esxcli network firewall set --enabled=false</code>                      コマンドを使用し、インストールが完了したら  <code>esxcli network firewall set --enabled=false</code>                      コマンドを使用してファイアウォールを再度有効にします。</p> <p>詳細については、                      Intersight ヘルプセンターの<a href="#">ネットワーク接続要件</a>を参照してください。</p>
Auto Support	Auto Support (ASUP) は、HX Data Platform を通じて提供されるアラート通知サービスです。	SMTP ポート番号 : 25	Auto Support は、ノードのドライブ障害などのハードウェア問題が発生した際の診断に役立つハードウェアカウンタの履歴を提供するため、有効にすることを強く推奨します。

## ファブリック インターコネク트의アップリンクのプロビジョニング

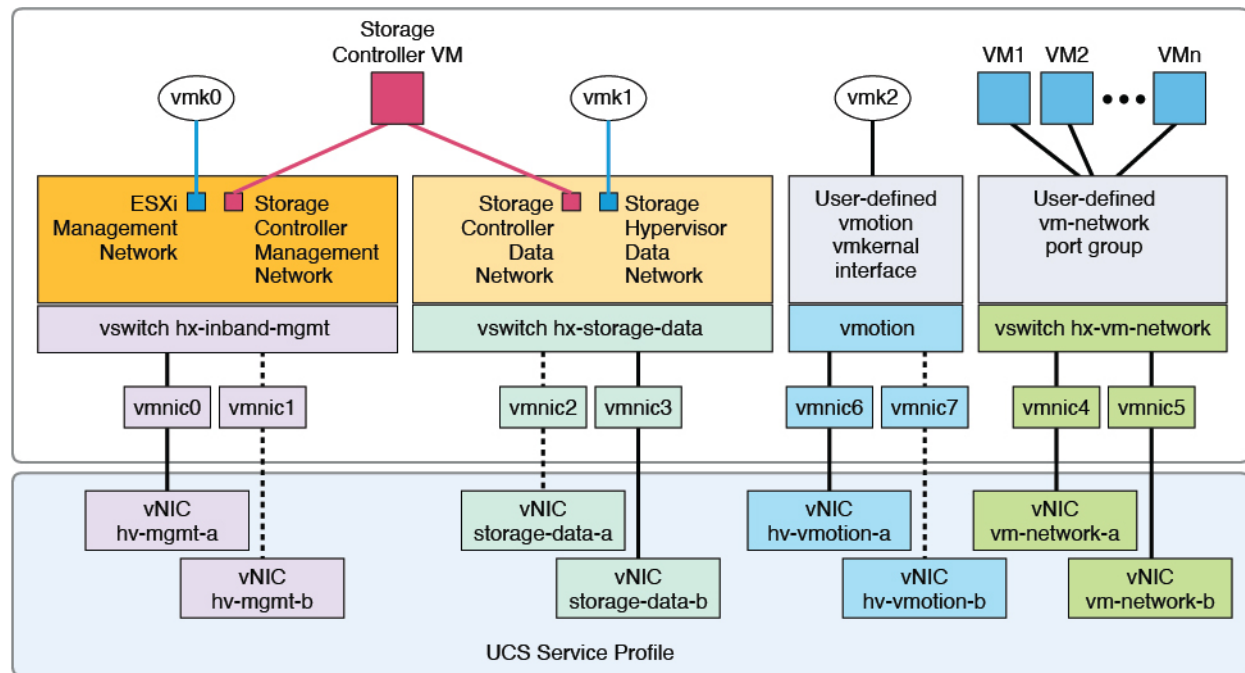
HyperFlex クラスタをセットアップする前に、最適なネットワーク トラフィック管理のためにアップストリーム帯域幅の容量を計画します。これにより、コンポーネントの障害や部分的なネットワーク停止が発生してもフローの安定状態が保証されます。

デフォルトでは、`hx-vm-network` vSwitch が**アクティブ/アクティブ**として設定されます。それ以外の vSwitch は、**アクティブ/スタンバイ**として設定されます。



- (注) FI に対して Catalyst スイッチを実行しているクラスタの場合は、最適な Quality of Service (QoS) MTU を 9216 に設定します (LAN > LAN Cloud > QoS システム クラスにあります)。そうでない場合、フェールオーバーは失敗します。

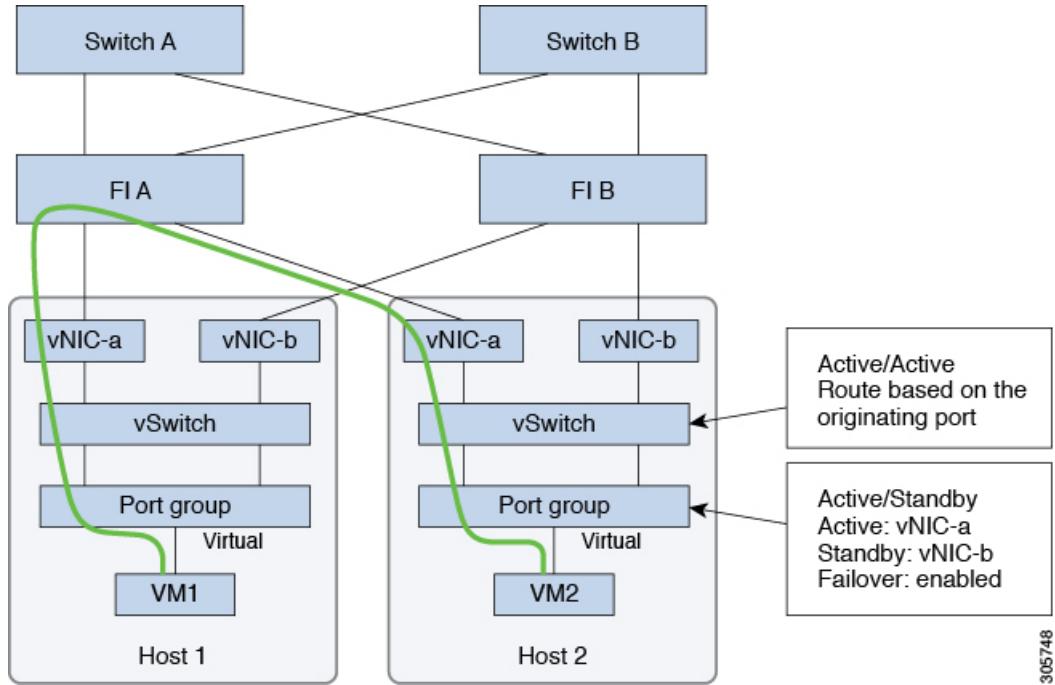
図 6: 単一ホストの *HyperFlex Data Platform* 接続



- Note: 1. Dotted lines represent a “standby” link.  
 2. All “a” vNICs connect to FI-A.  
 3. All “b” vNICs connect to FI-B.  
 4. MTU of 9000 is needed for storage-data and vmotion networks.  
 5. All VLANs by default are tagged on the FI so frames are passed untagged to each vswitch.  
 6. The vm network port groups are automatically created in 1.8 installer with vlan suffix.

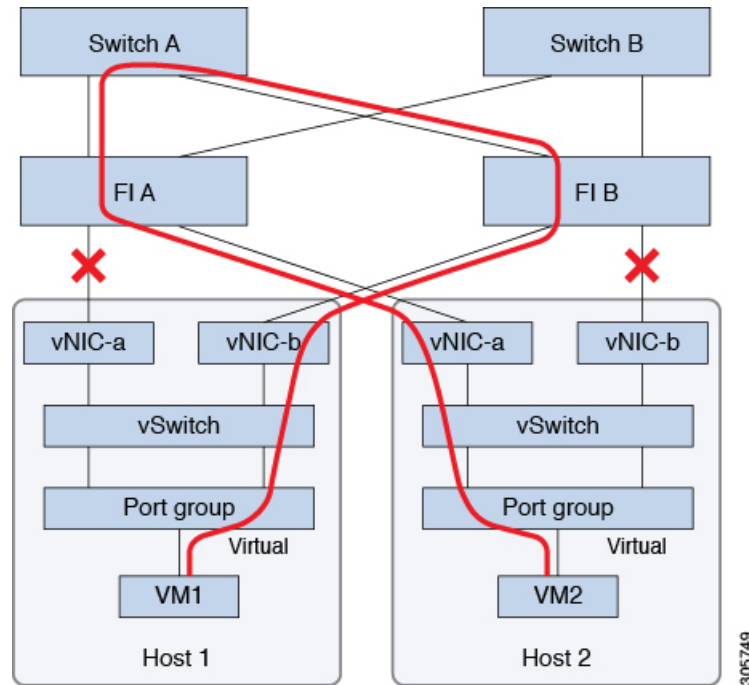
デフォルトの vSwitch NIC チューミング ポリシーとフェールオーバー ポリシーを [yes] に設定します。これにより、管理トラフィック、vMotion トラフィック、およびストレージトラフィックのすべてが、ローカルでファブリックインターコネクトに転送されるようになり、フローを安定した状態に維持できます。vNIC-a で障害が発生すると、ESXi がロードバランシングを計算し、すべての仮想ポートを vNIC-b に再ピンングします。vNIC-a がオンライン状態に戻った時点で、再びピンングが適用され、vNIC-a と vNIC-b の間で仮想ポートが元のように均等に分配されます。これにより、Cisco UCS ファブリック インターコネクトのアップストリームでの遅延と帯域幅使用量が削減されます。

図 7: 安定した状態のトラフィック フロー



1つ以上のサーバーリンクで障害が発生した場合（たとえばホスト1がファブリック A への接続を失い、ホスト2がファブリック B への接続を失った場合）は、トラフィックがアップストリームスイッチを通過する必要があります。したがってアップリンク ネットワーク帯域幅の使用率が増加し、新しいアップリンクを追加する必要があります。

図 8: リンク障害発生時のトラフィックフロー



- (注) 1つのファブリック インターコネクトから2つの異なるアップストリーム スイッチへのアップリンクが存在する場合は、FI で分離レイヤ 2 (DJL2) と呼ばれる状態が発生します。DJL2 は、FI がエンドホストモードとなっているときに DJL2 が適切に設定されていないと発生することが既知となっています。

DJL2 を適切に導入するには、『[Cisco UCS 6300 Series Fabric Interconnect Hardware Guide—Deploy Layer 2 Disjoint Networks Upstream in End Host Mode](#)』というホワイトペーパーを参照してください。

## ネットワーク設定



- 重要** すべての IP アドレスは IPv4 である必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

### ベストプラクティス

- ネットワークごとに異なるサブネットと VLAN を使用する必要があります。
- 10 Gbps ケーブルを使用して、各ホストを Cisco UCS ファブリック インターコネクトに直接接続します。



- デフォルトの VLAN である VLAN 1 を使用しないでください。特に Disjoint Layer 2 設定を使用している場合はネットワークの問題が発生する可能性があります。
- デフォルトで、インストーラは VLAN を非ネイティブとして設定します。非ネイティブ VLAN に対応するようにアップストリーム スイッチを確実に設定してください。
- UCSファブリック インターコネクトからすべての最上位ラック スイッチポートへのアップリンクは、スイッチのベンダーとモデルに応じて、**エッジトランク** モードまたは **PortFast エッジ** モードでスパニング ツリーを設定する必要があります。この追加設定により、リンクがフラップまたは状態を変更したときに、不要なスパニング ツリー ステートを介して遷移せず、トラフィック転送が開始される前に遅延が発生することがなくなります。**PortFast Edge** モードで FI アップリンクを適切に設定しないと、HyperFlex ネイティブの高可用性ネットワーク設計を活用する障害シナリオおよびインフラストラクチャアップグレード中にネットワークおよびクラスタが停止する可能性があります。
- FI側のポートは、Port-Fast、スパニングツリーポートタイプのエッジトランク、またはポートをただちにフォワーディングモードにする類似のスパニングツリー設定を持つ必要があります。

ESXi ホストごとに、次のネットワークが必要です。

- **管理トラフィック ネットワーク** : vCenter から、ハイパーバイザ (ESXi サーバ) 管理とストレージクラスタ管理を処理します。
- **データ トラフィック ネットワーク** : ハイパーバイザとストレージのデータ トラフィックを処理します。
- **vMotion ネットワーク**
- **VM ネットワーク**

4 つの vSwitch があり、それぞれが異なるネットワークを伝送します。

- **vswitch-hx-inband-mgmt** : ESXi 管理とストレージ コントローラ管理に使用されます。
- **vswitch-hx-storage-data** : ESXi ストレージデータと HX Data Platform のレプリケーションに使用されます。

この 2 つの vSwitch は、割り当てられた静的 IP アドレスでさらに 2 つのポート グループに分割され、ストレージクラスタと ESXi ホスト間のトラフィックを処理します。

- **vswitch-hx-vmotion** : VM とストレージ vMotion に使用されます。

この vSwitch には、vCenter クラスタ内のすべてのホストに接続する vSphere で定義された管理用ポート グループが 1 つあります。

- **vswitch-hx-vm-network** : VM データ トラフィックに使用されます。

Cisco UCS Manager 内の対応する vNIC テンプレート上で VLAN を追加または削除することができます。詳細な手順については、『[Managing VLANs in Cisco UCS Manager](#)』と『[Managing vNIC templates in Cisco UCS Manager](#)』を参照してください。VSwitch 上でポー

トグループを作成するには、『[Adding Virtual Port Groups to VMware Standard vSwitch](#)』を参照してください。



- (注)
1. vSwitch は HX Data Platform インストーラによって自動的に作成されます。
  2. HyperFlex ストレージクラスタの作成後に、vSphere の次のサービスを有効にする必要があります。
    - DRS (オプション、ライセンス登録されている場合)
    - VMotion
    - ハイ アベイラビリティ

## VLAN と vSwitch の要件

少なくとも3つの VLAN ID を指定します。インストール中にファブリック インターコネクタ上ですべての VLAN を設定する必要があります。

VLANタイプ	説明
(注)	次のネットワークごとに、異なるサブネットと VLAN を使用する必要があります。
VLAN ESXi および HyperFlex 管理トラフィック	VLAN名 : <user-defined> (たとえば、「hx-inband-mgmt」) VLAN ID : <user-defined>
VLAN HyperFlex ストレージトラフィック	VLAN名 : <user-defined> (たとえば、「hx-storage-data」) VLAN ID : <user-defined>
VLAN VM vMotion	VLAN名 : <user-defined> (たとえば、「hx-vmotion」) VLAN ID : <user-defined>
VLAN VM ネットワーク	VLAN VM ネットワーク : <user-defined> (たとえば、「hx-vm-network」) VLAN ID : <user-defined>

外部スイッチ VLAN タギング (EST) を使用した VLAN タギングおよび vSwitch 設定は、UCS Manager プロファイルを使って適用されます。HX Data Platform インストーラは、このプロセスを簡素化します。



- (注)
- デフォルトの VLAN である VLAN 1 を使用しないでください。特に Disjoint Layer 2 設定を使用している場合はネットワーキングの問題が発生する可能性があります。VLAN 1 以外の VLAN を使用します。
- デフォルトで、インストーラはVLANを非ネイティブとして設定します。非ネイティブ VLAN に対応するようにアップストリーム スイッチを設定します。
- インバンド管理は、VLAN 2 または VLAN 3 ではサポートされていません。

## Cisco UCS の要件

プロンプトが表示されたら、UCS ファブリック インターコネクと UCS Manager に関するリストの内容を提供してください。

### Cisco UCS ファブリック インターコネクの要件

UI 要素	基本的な情報
アップリンク スイッチ モデル	スイッチ タイプと接続タイプを指定します (SFP + Twin Ax または光)。
ファブリックインターコネクトクラスタの IP アドレス	<IP アドレス>。
FI-A の IP アドレス	<IP アドレス>。
FI-B の IP アドレス	<IP アドレス>。
MAC Address Pool	00:00:00 MAC アドレスプールを確認します。
IPブロック	KVM IPプール。少なくとも 4 つの IP アドレス。
サブネット マスク	たとえば、255.255.0.0 とします。
デフォルト ゲートウェイ	たとえば、10.193.0.1 とします。

### Cisco UCS Manager の要件

UI 要素	基本的な情報
UCS Managerのホスト名	ホスト名または IP アドレス。
ユーザ名	<管理者ユーザ名>
パスワード	<管理者ユーザ名>

## ハイパーバイザ要件

vCenter を介して、ストレージ管理ネットワークまたはストレージデータ ネットワーク上の ESXi サーバが使用できるアドレス範囲から、IP アドレスを入力します。すべてのネットワーク アドレスの静的 IP アドレスを指定します。



- (注)
- データ ネットワークと管理ネットワークは異なるサブネット上になければなりません。
  - ストレージクラスタの作成後は、IP アドレスを変更できません。Cisco TAC に連絡して、サポートを受けてください。
  - (必須の操作ではありませんが) DNS 名を指定する場合には、IP アドレスの転送と逆 DNS ルックアップを有効にしてください。
  - インストーラの IP アドレスは、ハイパーバイザおよびストレージコントローラ VM が使用する管理サブネットから到達可能である必要があります。インストーラ アプライアンスは、インストールするクラスタに含まれない VMware ワークステーションまたは ESXi ホストで動作する必要があります。

管理ネットワークの IP アドレス		データ ネットワークの IP アドレス	
ハイパーバイザ	ストレージコントローラ	ハイパーバイザ	ストレージコントローラ
<IPアドレス>	<IPアドレス>	<IPアドレス>	<IPアドレス>
<IPアドレス>	<IPアドレス>	<IPアドレス>	<IPアドレス>
<IPアドレス>	<IPアドレス>	<IPアドレス>	<IPアドレス>
<IPアドレス>	<IPアドレス>	<IPアドレス>	<IPアドレス>
[VLAN タグ (VLAN Tags) ]	VLAN_ID	[VLAN タグ (VLAN Tags) ]	VLAN_ID
サブネット マスク		サブネット マスク	
デフォルトゲートウェイ		デフォルトゲートウェイ	
インストーラ アプライアンスの IP アドレス			
<IPアドレス>		<IPアドレス>	

## ストレージクラスタ要件

ストレージクラスタは、Cisco HX Data Platform のコンポーネントです。vSphere Web クライアントで単一のデータストアが容易にプロビジョニングされ、それによりストレージの複雑さを軽減します。コントローラ リソースを活用して高可用性を実現するために、ストレージクラスタ内のすべてのサーバのディスクにデータが分散されます。

ストレージクラスタは、関連する vSphere クラスタから独立しています。vSphere クラスタ内の ESXi ホストを使用してストレージクラスタを作成できます。

ストレージクラスタを定義するには、次のパラメータを指定します。

フィールド	説明
名前 (Name)	ストレージクラスタの名前を入力します。
管理 IP アドレス	<p>これにより、各 ESXi ホスト上でストレージ管理ネットワークへのアクセスが可能になります。</p> <ul style="list-style-type: none"> <li>この IP アドレスは、ノードの管理 IP アドレスと同じサブネット上に存在する必要があります。</li> <li>同じサブネット上の他のクラスタとの間でクラスタ管理 IP が最後のオクテットを共有できないようにしてください。</li> <li>これらの IP アドレスは、「ハイパーバイザ」のセクションで各ノードに割り当てられる 4 つの IP アドレスとは別の追加的なアドレスです。</li> </ul>
ストレージクラスタ データの IP アドレス	<p>これにより、各 ESXi ホスト上でストレージデータネットワークとストレージコントローラ VM ネットワークへのアクセスが可能になります。</p> <p>同じ IP アドレスをクラスタ内のすべての ESXi ノードに適用する必要があります。</p>

フィールド	説明
データレプリケーションファクタ	<p>データレプリケーション係数により、ストレージクラスタ全体のデータの冗長レプリカの数 が定義されます。</p> <p>これは HX Data Platform のインストール中に 設定され、変更はできません。</p> <p>[データレプリケーション係数 (Data Replication Factor) ] を選択します。選択でき る基準は、次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>データ複製ファクタ 3: Hyperflex Edge</b> を除 くすべての環境で複製ファクタ 3 を強く 推奨しています。複製ファクタ 2 では、 可用性と復元性のレベルが低くなります。 コンポーネントまたはノードの障害によ る停電のリスクは、アクティブかつ定期 的なバックアップを作成することにより 軽減されます。</li> </ul> <p><b>注目</b>      これは推奨オプションです。</p> <ul style="list-style-type: none"> <li>• <b>データレプリケーション係数 2</b> : データ の冗長複製を 2 つ保持します。この場合、 ストレージリソースの消費量は少なく てすみませんが、ノードやディスクの同時 障害が発生した場合にデータ保護が低下 します。</li> </ul> <p>ストレージクラスタ内のノードまたは ディスクで障害が発生すると、クラスタ の機能に影響が生じます。複数のノード で障害が発生する場合や、1 つのノードと 別のノード上のディスクで障害が発生す る場合を、同時障害と呼びます。</p>

## vCenter 設定要件

vCenter 用に管理者レベルのアカウントとパスワードを指定します。既存の vCenter サーバーが存在することを確認します。次の vSphere サービスが動作していることを確認します。

- ダイナミック リソース スケジューラ (DRS) を有効にします (オプション。ライセンス  
供与時に有効)。
- vMotion を有効にします。

- 高可用性 (HA) を有効にします (フェールオーバー容量を定義するため、またデータストア ハートビートを拡張するために必要)。
- ユーザ VM はバージョン 9 以降である必要があります (HX Data Platform、ネイティブ スナップショット、および ReadyClones を使用するために必要)。

フィールド	説明
vCenter Server	現在の vCenter サーバー web アドレスを入力します。 例 : <code>http://&lt;IP アドレス&gt;</code> など。
ユーザ名	<管理者ユーザ名> を入力します。
パスワード	<管理者パスワード> を入力します。
データセンター名 (注) 既存のデータセンターオブジェクトを使用できます。データセンターが vCenter に存在しない場合は、作成されます。	vCenter データセンター用の必要な名前を入力します。
クラスタ名	vCenter クラスタ用の必要な名前を入力します。クラスタには、3 つ以上の ESXi サーバが含まれる必要があります。

## システム サービス要件

Cisco HX Data Platform をインストールする前に、次のネットワーク接続とサービスが稼働していることを確認します。

- DNS サーバ



**注意** DNS サーバは HX ストレージクラスタの外側に配置される必要があります。ネストされた DNS サーバは、DC 電源損失時など、クラスタ全体がシャットダウンした後にクラスタが起動しない可能性があります。

- NTP サーバ



---

**注意** NTP サーバは HX ストレージ クラスタの外側に配置される必要があります。ネストされた NTP サーバは、DC 電源損失時など、クラスタ全体がシャットダウンした後にクラスタが起動しない可能性があります。

---



- (注)
- ストレージ クラスタを設定する前に、NTP サーバが稼働状態で、信頼性の高い時間のソースを提供していることを手動で確認します。
  - すべてのノード（コンバージドとコンピューティングの両方）とすべてのストレージ コントローラ VM に同じ NTP サーバを使用します。
  - NTP サーバは、安定性があり、（クラスタの存続期間中に）中断せず、静的 IP アドレス経由で到達可能である必要があります。
  - アクティブ ディレクトリを NTP サーバとして使用している場合、NTP サーバが Microsoft ベストプラクティスに従って設定されていることを確認してください。詳細については、『[Windows Time Service Tools and Settings](#)』を参照してください。NTP サーバが適切に設定されていない場合、同期が行われず、クライアント側で時間同期を修正する必要が発生する可能性があります。詳細については、『[Synchronizing ESXi/ESX time with a Microsoft Domain Controller](#)』を参照してください。
- 

- [タイムゾーン (Time Zone) ]



フィールド	基本的な情報
[DNSサーバ (DNS Server(s)) ]	<p>&lt;IP address&gt;</p> <p>HyperFlex Data Platform のインストール中にホスト名を使用する場合は、DNS サーバー アドレスが必須です。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• DNS サーバを使用しない場合は、HX Data Platform インストーラの [クラスタの設定 (Cluster Configuration) ] ページの [システムサービス (System Services) ] でホスト名を入力しないでください。IP アドレスのみを使用します。</li> <li>• 複数の DNS サーバアドレスを指定するには、アドレスをカンマで区切ります。DNS サーバアドレスが正しく入力されていることを注意深く確認してください。</li> </ul>
NTPサーバ (信頼性の高い NTP サーバが必要です)	<p>&lt;IP address&gt;</p> <p>NTP サーバは、以下の間のクロック同期に使用されます。</p> <ul style="list-style-type: none"> <li>• ストレージコントローラ VM</li> <li>• ESXi ホスト</li> <li>• vCenter Server</li> </ul> <p><b>重要</b> NTP サーバの静的 IP アドレスは、ストレージコントローラ VM、ESXi ホスト、および vCenter Server 間のクロック同期を保証するために必要です。</p> <p>インストール中に、この情報がすべてのストレージコントローラ VM および対応するホストに伝播されます。ストレージクラスタの起動時に自動的に各サーバが同期されます。</p>
[タイムゾーン (Time Zone) ]	<p>&lt;使用するタイムゾーン&gt;</p> <p>ストレージコントローラ VM のタイムゾーンを選択します。これは、スケジュール済みのスナップショットを取得するタイミングを決定するために使用されます。</p> <p>(注) すべての VM を同じタイムゾーンにする必要があります。</p>

## コントローラ VM の CPU リソース予約

ストレージコントローラ VM は HyperFlex Data Platform 用の重要な機能を提供するので、HX Data Platform インストーラはコントローラ VM の CPU リソース予約を設定します。この予約

により、コントローラ VM に最低限必要な CPU リソースが割り当てられることが保証されます。これは、ESXi ハイパーバイザー ホストの物理 CPU リソースがゲスト VM によって大量に消費される状況で役立ちます。次の表に、ストレージコントローラ VM の CPU リソース予約の詳細を示します。

製品 ID	VM CPU の数	共有	予約	制限
HXAF220C-M5SN/M6SN (すべての NVMe 220) HXAF240C-M6SN (すべての NVMe 240)	12	低	10,800 MHz	無制限
HX ブーストモードが有効な場合： HXAF220C-M5SN/M6SN (すべての NVMe 220) HXAF240C-M6SN (すべての NVMe 240)	16	低	10,800 MHz	無制限
HX ブーストモードが有効な場合： HXAF220c-M4/M5/M6 HXAF240c-M4/M5SX/M6	12	低	10,800 MHz	無制限
他のすべてのモデル	8	低	10,800 MHz	無制限

## コントローラ VM 用メモリ リソース予約

次の表に、ストレージコントローラ VM 用のメモリ リソース予約の詳細を示します。

サーバモデル	ゲストメモリの量	すべてのゲストメモリを予約
HX220c-M4/M5/M6 HX-E-220M5SX HX-E-220M6S	48 GB	はい
HXAF220C-M4	48 GB	はい
HXAF220C-M5/M6 HXAF-E-220M5SX HXAF-E-220M6SX	48 GB 7.6 TB SSD (SED および非 SED) を搭載した構成の場合は 56 GB	○

サーバモデル	ゲストメモリの量	すべてのゲストメモリを予約
HX240c-M4/M5SX/M6SX	72 GB	はい
HXAF240c-M4/M5SX/M6SX	72 GB 7.6 TB SSD (SED および非 SED) を搭載した構成の場合は 88 GB	○
HX240C-M5L HX240C-M6L	78 GB	Yes
HXAF220C-M5SN/M6SN (すべての NVMe 220)	< 8 TB NVMe キャパシティドライブを使用する構成の場合は 72 GB 8 TB NVMe 容量ドライブの構成の場合は 84 GB 15 TB NVMe キャパシティドライブの構成の場合は 96 GB  (注) 15 TB キャパシティドライブは、M6 サーバーでのみサポートされます。	はい
HXAF240C-M6SN (すべての NVMe 240)	< 8 TB NVMe キャパシティドライブを使用する構成の場合は 72 GB 8 TB NVMe 容量ドライブの構成の場合は 84 GB 15 TB NVMe キャパシティドライブの構成の場合は 110 GB	対応

サーバモデル	ゲストメモリの量	すべてのゲストメモリを予約
HXAF240C-M5SD HX240C-M5SD (奥行240)	48 GB  (注) 7.6 TB ドライブは HXAF240C-M5SD でサポートされますが、より高いメモリ構成は必要ありません。	はい

- C240 ラックサーバは、2 ラックユニット (2RU) フォームファクタで非常に優れた拡張性と高いパフォーマンスを提供します。
- C220 サーバは、1 ラックユニット (1RU) フォームファクタで拡張性を提供します。

次の表に、NVMe ドライブのストレージコントローラ VM 用のメモリ使用の詳細を示します。

表 3: コントローラ VM のメモリ使用 - NVMe ドライブ

サーバモデル	ドライブサイズ		
	1/4 TB	8 TB	15 TB (HX リリース 5.0(2a) 以降)
M5 C220 すべての NVMe	72 GB	84 GB	サポートなし
M6 C220 すべての NVMe	72 GB	84 GB	96 GB
M6 240C すべての NVMe	72 GB	84 GB	110 GB

- オールフラッシュ構成での 15 TB の永続ドライブはサポートされていません。
- 16 TB LFF ドライブのサポートは有効になっていません。

## Auto Support 要件

Auto Support (ASUP) は、HX Data Platform を通じて提供されるアラート通知サービスです。Auto Support を有効にすると、HX Data Platform から、指定されたメールアドレスまたは通知を受信したい電子メールエイリアスに通知が送信されます。

自動サポートを設定するには、次の情報が必要です。

自動サポート	
[自動サポートの有効化 (Enable Auto Support) ] チェックボックス	HX ストレージクラスタの作成時にこのボックスをオンにします。
メール サーバ	<IP address>  Auto Support を有効にするには、ネットワーク上で SMTP メールサーバを設定する必要があります。すべてのストレージコントローラ VM の IP アドレスから送信された電子メールを処理するために使用します。  (注) 未認証の SMTP のみが ASUP のサポート対象となります。
メール送信者	<username@domain.com>  Auto Support 通知の送信に使用する電子メールアドレス。
ASUP受信者	Auto Support 通知を受信する電子メールアドレスまたは電子メールエイリアスのリスト。



- (注) Auto Support は、ノードのドライブ障害などのハードウェア問題が発生した際の診断に役立つハードウェアカウンタの履歴を提供することになるため、有効にすることを強く推奨します。

## シングルサインオンの要件

SSO URL が vCenter から提供されます。コントローラ VM からその URL に直接到達できない場合は、[インストーラの詳細設定 (Installer Advanced Settings) ]を使用して場所を明示的に設定します。

シングルサインオン (SSO)	
SSO サーバの URL	SSO URL は、vCenter の [vCenter サーバ (vCenter Server) ] > [管理 (Manage) ] > [詳細設定 (Advanced Settings) ] にあります (キー config.vpxd.sso.sts.uri) 。





## 第 4 章

# Cisco HyperFlex Systems サーバーのインストール

この章では、HyperFlex クラスタをセットアップするための物理コンポーネントのインストール方法を説明します。

- [ラック設置型 Cisco HyperFlex ノード \(43 ページ\)](#)
- [ファブリック インターコネクットのセットアップ \(44 ページ\)](#)
- [HX シリーズサーバと Cisco UCS ファブリック インターコネクットの接続 \(53 ページ\)](#)
- [概要 \(53 ページ\)](#)

## ラック設置型 Cisco HyperFlex ノード

HyperFlex クラスタとノード制限の詳細については、『[Release Notes for Cisco HX Data Platform](#)』の最新版の「[Cisco HX Data Platform Storage Cluster Specifications](#)」を参照してください。

UCS C シリーズのインテグレーションの指針については、お使いのリリースの [Cisco UCS C シリーズサーバへの Cisco UCS Manager のインテグレーション設定ガイド](#) を参照してください。

Cisco HyperFlex ノードのインストールの詳細については、下の表のそれぞれのリンクを参照してください。

インストールするノードの種類	参考資料
コンバージドノード数	
HyperFlex HX220c M4/M5 ノード HyperFlex HX220c M5 ノード	<a href="#">Cisco HyperFlex HX220c M5 ノードインストールガイド</a>
HyperFlex HX240c M4/M5 ノード HyperFlex HX240c M6 ノード	<a href="#">Cisco HyperFlex HX240c M5 ノードインストールガイド</a>
コンピューティング専用ノード	

インストールするノードの種類	参考資料
Cisco UCS B200 M3/M4/M5 ノード	<a href="#">Cisco UCS B200 M3/M4/M5 Blade Server Installation and Service Note</a>
Cisco UCS B260 M4 ノード、B460 M4 ノード	<a href="#">Cisco UCS B260 M4 and B460 M4 Blade Server Installation and Service Note for Servers with E7 v4 CPUs</a> <a href="#">Cisco UCS B260 M4 and B460 M4 Blade Server Installation and Service Note for Servers with E7 v3 and E7 v2 CPUs</a>
Cisco UCS B420 M4 ノード	<a href="#">Cisco UCS B420 M4 Blade Server Installation and Service Note</a>
Cisco UCS B480 M5 ノード	<a href="#">Cisco UCS B480 M5 Blade Server Installation and Service Note</a>
Cisco UCS C240 M3/M4/M5 ラックノード Cisco UCS C240 M6 ラック ノード	<a href="#">Cisco UCS C240 サーバ インストールおよびサービス ガイド</a>
Cisco UCS C220 M3/M4/M5 ラックノード Cisco UCS C240 M6 ラック ノード	<a href="#">Cisco UCS C220 サーバ インストールおよびサービス ガイド</a>
Cisco UCS C480 M5 ノード	<a href="#">Cisco UCS C480 M5 Server Installation and Service Guide</a>
Cisco UCS B420 M4 ノード	<a href="#">Cisco UCS 460 M4 Server Installation and Service Guide</a>

## ファブリック インターコネクットのセットアップ

高度な可用性をもたらすため、次のようにファブリック インターコネクットの冗長ペアを設定します。

1. L1 または L2 の高可用性ポート間で、イーサネット ケーブルを使用して直接 2 つのファブリック インターコネクットに接続します。
2. ファブリック インターコネクット A 上のポート L1 を ファブリック インターコネクット B 上のポート L1 に接続し、ファブリック インターコネクット A 上のポート L2 をファブリック インターコネクット B 上のポート L2 に接続します。

これにより、2 つのファブリック インターコネクットは、互いのステータスを継続的にモニターします。

ファブリック インターコネクットを接続する前に、以下の情報を確認し、取得してください。



項目	説明
ファブリック インターコネクタの物理的な接続を確認します。	<ul style="list-style-type: none"> <li>• 1 つ目のファブリック インターコネクタのコンソールポートが、コンピュータまたはコンソールサーバに物理的に接続されている。</li> <li>• 管理イーサネットポート (mgmt0) が外部のハブ、スイッチ、またはルータに接続されている。</li> <li>• 両方のファブリック インターコネクタの L1 ポートが互いに直接接続されている。</li> <li>• 両方のファブリック インターコネクタの L2 ポートが互いに直接接続されている。</li> </ul>
コンピュータ端末でコンソールポートのパラメータを確認します。	<ul style="list-style-type: none"> <li>• 9600 ボー</li> <li>• 8 データ ビット</li> <li>• パリティなし</li> <li>• 1 ストップ ビット</li> </ul>
初期セットアップに関する情報を入手します。	<p>初期セットアップに関する次の情報を収集します。</p> <ul style="list-style-type: none"> <li>• システム名</li> <li>• 管理者アカウントのパスワード</li> <li>• 3 つの静的 IP アドレス</li> <li>• 3 つの静的 IP アドレスのサブネット マスク</li> <li>• デフォルト ゲートウェイの IP アドレス</li> <li>• DNS サーバの IP アドレス</li> <li>• システムのドメイン名</li> </ul>

両方のファブリック インターコネクタが同じセットアッププロセスを通過する必要があります。プライマリ ファブリック インターコネクタをセットアップして、クラスタ設定用に有効にします。同じプロセスを使用してセカンダリ ファブリック インターコネクタをセットアップするときには、最初のファブリック インターコネクタがピアとして検出されます。

## Cisco UCS Manager GUI を使用したプライマリ ファブリック インターコネクタの設定

設定を始める前に、同じサブネットでの次の 3 つの IP アドレスを指定します。

- プライマリ ファブリック インターコネクタ FIA の管理ポート IP アドレス

- セカンダリ ファブリック インターコネクタ FIB の管理ポートの IP アドレス
- HyperFlex クラスタの IP アドレス。

次のように Cisco UCS Manager GUI を使用してプライマリ ファブリック インターコネクタを設定します。

- ステップ 1** コンソールポートに接続します。詳細については、[Cisco 6200 Series Fabric Interconnect Hardware Installation guide](#)を参照してください。
- ステップ 2** ファブリック インターコネクタの電源を入れます。ファブリック インターコネクタが起動する際、電源 オン セルフテストのメッセージが表示されます。
- ステップ 3** インストール方式プロンプトに *gui* と入力します。
- ステップ 4** システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。
- ファブリック インターコネクタの管理ポートの IPv4 アドレス。
  - ファブリック インターコネクタの管理ポートの IPv4 サブネット マスク。
  - ファブリック インターコネクタに割り当てられたデフォルト ゲートウェイの IPv4。

**重要** すべての IP アドレスは IPv4 である必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

- ステップ 5** プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager 起動ページに移動します。
- ステップ 6** **[Express Setup (Express セットアップ)]** を選択します。
- ステップ 7** **[Initial Setup (初期セットアップ)]** を選択し、**[Submit (送信)]** をクリックします。
- ステップ 8** **[Cluster and Fabric Setup (クラスタおよびファブリック セットアップ)]** 領域で、次のフィールドに値を入力します。

名前	説明
<b>[Enable Cluster (クラスタの有効化)]</b> オプション	[Enable Cluster (クラスタの有効化)] オプションを選択します。
[Fabric Setup] オプション	[Fabric A (ファブリック A)] を選択します。
[Cluster IP Address] フィールド	Cisco UCS Manager が使用する IPv4 アドレスを入力します。

- ステップ 9** **[System Setup (システム セットアップ)]** 領域で、次のフィールドに値を入力します。

フィールド	説明
[システム名 (System Name) ] フィールド	Cisco UCS ドメインに割り当てられる名前。

フィールド	説明
[Admin Password] フィールド	ファブリック インターコネクタ上の管理者アカウントに使用されるパスワード。  Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。このパスワードは空にできません。
[Confirm Admin Password] フィールド	ファブリック インターコネクタ上の管理者アカウントに使用されるパスワード。
[Mgmt IP Address] フィールド	ファブリック インターコネクタ上の管理ポートの固定 IP アドレス。
[Mgmt IP Netmask] フィールド	ファブリック インターコネクタ上の管理ポートの IP サブネットマスク。
[Default Gateway] フィールド	ファブリック インターコネクタ上の管理ポートに割り当てられるデフォルトゲートウェイの IP アドレス。
[DNS Server IP] フィールド	ファブリック インターコネクタ上の管理ポートに割り当てられる DNS サーバの IP アドレス。
[Domain name] フィールド	ファブリック インターコネクタが存在するドメインの名前。

- ステップ 10** [送信 (Submit) ] をクリックします。  
セットアップ操作の結果がページに表示されます。

## Cisco UCS Manager GUI を使用したセカンダリ ファブリック インターコネクタの設定

セカンダリ ファブリック インターコネクタのコンソール ポートが、コンピュータまたはコンソール サーバに物理的に接続されていることを確認します。以前設定したプライマリ ファブリック インターコネクタでの管理者アカウントのパスワードを知っていることを確認します。

- ステップ 1** コンソール ポートに接続します。詳細については、[Cisco 6200 Series Fabric Interconnect Hardware Installation guide](#)を参照してください。
- ステップ 2** ファブリック インターコネクタの電源を入れます。ファブリック インターコネクタが起動する際、電源 オンセルフテストのメッセージが表示されます。
- ステップ 3** インストール方式プロンプトに *gui* と入力します。
- ステップ 4** システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

- ファブリック インターコネクタの管理ポートの IPv4 アドレス。
- ファブリック インターコネクタの管理ポートの IPv4 サブネット マスク。
- ファブリック インターコネクタに割り当てられたデフォルト ゲートウェイの IPv4 アドレス。

(注) 設定時に両方のファブリック インターコネクタに同じ管理インターフェイスのアドレスタイプを割り当てる必要があります。

- ステップ 5** プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。
- ステップ 6** プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager 起動ページに移動します。
- ステップ 7** **[Express Setup (Express セットアップ)]** を選択します。
- ステップ 8** **[Initial Setup (初期セットアップ)]** を選択し、**[Submit (送信)]** をクリックします。  
ファブリック インターコネクタは、第 1 ファブリック インターコネクタの設定情報を検出します。
- ステップ 9** **[Cluster and Fabric Setup (クラスタおよびファブリック セットアップ)]** 領域で、次のフィールドに値を入力します。

名前	説明
<b>[Enable Cluster (クラスタの有効化)]</b> オプション	<b>[Enable Cluster (クラスタの有効化)]</b> オプションを選択します。
<b>[Fabric Setup]</b> オプション	<b>[Fabric B (ファブリック B)]</b> を選択します。

- ステップ 10** **[System Setup (システム セットアップ)]** 領域の **[Admin Password of Master (マスターの管理者パスワード)]** フィールドに管理者アカウントのパスワードを入力します。**[Manager Initial Setup (Manager の初期セットアップ)]** 領域が表示されます。
- ステップ 11** **[Manager Initial Setup (Manager の初期セットアップ)]** 領域で表示されるフィールドは、第 1 ファブリック インターコネクタを IPv4 のどちらの管理アドレスで設定したかによって異なります。次のように、設定に適したフィールドに入力します。

フィールド	説明
<b>[Peer FI is IPv4 Cluster enabled. [local FI Mgmt0 IPv4 address (ローカル FI Mgmt0 IPv4 アドレス)]</b> フィールドに入力してください。	ローカル ファブリック インターコネクタの Mgmt0 インターフェイスの IPv4 アドレスを入力します。

- ステップ 12** **[送信 (Submit)]** をクリックします。  
セットアップ操作の結果がページに表示されます。

## CLI を使用したプライマリ ファブリック インターコネクタの設定

- ステップ 1** コンソール ポートに接続します。
- ステップ 2** ファブリック インターコネクタの電源を入れます。  
ファブリック インターコネクタが起動すると、電源投入時セルフテスト メッセージが表示されます。
- ステップ 3** 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。
- ステップ 4** **setup** と入力して、初期システム設定を続行します。
- ステップ 5** **y** と入力して、初期設定を続行することを確認します。
- ステップ 6** 管理アカウントのパスワードを入力します。
- ステップ 7** 確認のために、管理アカウントのパスワードを再入力します。
- ステップ 8** **yes** と入力して、クラスタ構成の初期設定を続行します。
- ステップ 9** ファブリック インターコネクタのファブリックを入力します (**A** または **B**)。
- ステップ 10** システム名を入力します。
- ステップ 11** ファブリック インターコネクタの管理ポートの IPv4 アドレスを入力します。  
IPv4 サブネット マスクを入力するように求められます。
- ステップ 12** IPv4 サブネット マスクを入力し、**[Enter]** を押します。  
ファブリック インターコネクタの管理ポート用に入力したアドレスタイプによって、デフォルトゲートウェイの IPv4 アドレスを求められます。
- ステップ 13** デフォルト ゲートウェイの IPv4 アドレスを入力します。
- ステップ 14** DNS サーバの IP アドレスを指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。
- ステップ 15** (任意) DNS サーバの IPv4 アドレスを入力します。  
アドレスタイプはファブリック インターコネクタの管理ポートのアドレスタイプと同じである必要があります。
- ステップ 16** デフォルトのドメイン名を指定する場合は **yes** を入力し、指定しない場合は **no** を入力します。
- ステップ 17** (任意) デフォルト ドメイン名を入力します。
- ステップ 18** 設定の概要を確認し、**yes** と入力して設定を保存および適用するか、**no** と入力して設定ウィザードを初めからやり直して設定を一部変更します。  
設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、**Enter** を押します。

### 例

次に、コンソールおよび IPv4 管理アドレスを使用してクラスタ構成の最初のファブリック インターコネクタをセットアップする例を示します。

```

Enter the installation method (console/gui)? console
Enter the setup mode (restore from backup or initial setup) [restore/setup]? setup
You have chosen to setup a new switch. Continue? (y/n): y
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Do you want to create a new cluster on this switch (select 'no' for standalone setup
or if you want this switch to be added to an existing cluster)? (yes/no) [n]: yes
Enter the switch fabric (A/B): A
Enter the system name: foo
Mgmt0 IPv4 address: 192.168.10.10
Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Virtual IPv4 address: 192.168.10.12
Configure the DNS Server IPv4 address? (yes/no) [n]: yes
  DNS IPv4 address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Join centralized management environment (UCS Central)? (yes/no) [n]: no
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Management IP Address=192.168.10.10
  Management IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  Cluster Enabled=yes
  Virtual Ip Address=192.168.10.12
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

## CLI を使用した従属ファブリック インターコネクタの設定

この手順は、管理ポートに対し IPv4 アドレスを使用して第 2 のファブリック インターコネクタをセットアップする方法について説明します。



(注) 新しいファブリック インターコネクタを既存の高可用性クラスタに追加する場合、たとえば、新規インストール時またはファブリック インターコネクタの交換時に、認証方式がリモートに設定されている限り、新しいデバイスはクラスタにログインできません。新しいファブリック インターコネクタをクラスタに正常に追加するには、認証方式を一時的にローカルに設定し、プライマリ ファブリック インターコネクタのローカル管理者資格情報を使用する必要があります。

**ステップ 1** コンソール ポートに接続します。

**ステップ 2** ファブリック インターコネクタの電源を入れます。

ファブリック インターコネクタが起動すると、電源投入時セルフテスト メッセージが表示されます。

**ステップ 3** 設定されていないシステムがブートすると、使用する設定方法の入力を要求するプロンプトが表示されます。**console** と入力して、コンソール CLI を使用した初期設定を続行します。

(注) ファブリック インターコネクトによって、クラスタ内のピア ファブリック インターコネクトが検出されます。検出されなかった場合は、L1 ポートと L2 ポート間の物理接続を調べ、ピア ファブリック インターコネクトがクラスタ設定でイネーブルになっていることを確認します。

**ステップ 4** **y** と入力して、従属ファブリック インターコネクトをクラスタに追加します。

**ステップ 5** ピア ファブリック インターコネクトの管理パスワードを入力します。

**ステップ 6** 従属ファブリック インターコネクト上の管理ポートの IP アドレスを入力します。

**ステップ 7** 設定の概要を確認し、**yes** と入力して設定を保存および適用するか、**no** と入力して設定ウィザードを初めからやり直して設定を一部変更します。

設定ウィザードのやり直しを選択した場合は、以前に入力した値が角カッコで囲まれて表示されます。以前に入力した値をそのまま使用する場合は、**Enter** を押します。

## 例

次に、ピアのコンソールおよび IPv4 アドレスを使用してクラスタ設定の第 2 のファブリック インターコネクトをセットアップする例を示します。

```
Enter the installation method (console/gui)? console
Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect
will be added to the cluster. Continue (y/n) ? y
Enter the admin password of the peer Fabric Interconnect: adminpassword%958
Peer Fabric interconnect Mgmt0 IPv4 Address: 192.168.10.11
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

## コンソールのセットアップの確認

SSH 経由でファブリック インターコネクトにログインすることにより、両方のファブリック インターコネクトの設定が完全であることを確認できます。

Cisco UCS Manager CLI から次のコマンドを使用して、クラスタのステータスを確認します。

コマンド	目的	出力例
<b>show cluster state</b>	ハイアベイラビリティクラスターの両方のファブリック インターコネクットの動作状態およびリーダーシップ ロールを表示します。	<p>次の例の表示では、両方のファブリック インターコネクットが Up 状態、HA が Ready 状態、ファブリック インターコネクット A がプライマリ ロール、ファブリック インターコネクット B が従属ロールです。</p> <pre>UCS-A# show cluster state Cluster Id: 0x4432f72a371511de-0xb97c000de1blada4  A: UP, PRIMARY B: UP, SUBORDINATE HA READY</pre>
<b>show cluster extended-state</b>	クラスタの状態に関する拡張詳細が表示され、通常は問題のトラブルシューティングにこれが使用されます。	<p>次の例は、クラスタの拡張状態の表示方法を示しています。</p> <pre>UCSC# show cluster extended-state 0x2e95deacbd0f11e2- 0x8ff35147e84f3de2Start time: Thu May 16 06:54:22 2013Last election time: Thu May 16 16:29:28 2015System Management Viewing the Cluster State A: UP, PRIMARY B: UP, SUBORDINATE  A: memb state UP, lead state PRIMARY, mgmt services state: UP B: memb state UP, lead state SUBORDINATE, mgmt services state: UP heartbeat state PRIMARY_OK HA READY Detailed state of the device selected for HA quorum data:  Device 1007, serial: a66b4c20-8692-11df-bd63-1b72ef3ac801, state: active Device 1010, serial: 00e3e6d0-8693-11df-9e10-0f4428357744, state: active Device 1012, serial: 1d8922c8-8693-11df-9133-89fa154e3fal, state: active</pre>



# HX シリーズ サーバと Cisco UCS ファブリック インターコネクットの接続

## 概要

Cisco HX220c および HX240c サーバは、ファブリック インターコネクットに直接接続します。直接接続を使用すれば、Cisco UCS Manager は、1 本のケーブルで HX シリーズ サーバの管理トラフィックとデータトラフィックの両方を管理できます。



- (注) サーバをファブリック インターコネクットに接続した後、そのサーバが検出された時点で、UCS Manager 設定フォームを使用して、Cisco UCS Manager で使用可能な C シリーズ ソフトウェア バンドルを更新します。

直接接続モードを使用する場合は、すべての Cisco UCS 管理対象アダプタをファブリック インターコネクット上のサーバポートに接続する必要があります。要件の章に列挙されている推奨ファームウェアが HX サーバにインストールされていることを確認してください。そうでない場合は、Cisco UCS Manager を使用してファームウェアを更新します。



- (注) UCS の設定に関する次の制限事項に注意してください。
- Cisco HX に固有の UCS の設定に関する制限事項：HX M4 サーバは 1227 VIC および 6332-16UP ファブリック インターコネクットと互換性がありません。
  - Cisco UCS の設定に関する一般的な制限事項：[Cisco UCS 6200、6332 および 6324 シリーズ Cisco UCS Manager コンフィギュレーション上限値ガイド](#)を参照してください。

## コンバージド ノードとファブリック インターコネクットの接続

このトピックでは、HX クラスタの作成や既存の HX クラスタへの追加を行うためにコンバージド ノードを物理的に追加する方法について説明します。

## 始める前に



## 重要

- Cisco UCS Manager と統合する前に、CIMC サーバを工場出荷時のデフォルトに設定します。
- 統合ノードでは、専用の CIMC ポートをネットワークに接続しないでください。これを行うと、サーバが Cisco UCS Manager で検出されなくなります。サーバが検出されない場合は、各サーバの CIMC を出荷時の設定にリセットします。
- 近い将来に FC ストレージを接続する必要がない場合は、ポート 1 ~ 16 のみを使用します。
- Cisco UCS FI 63xx および 64xx では、ポート 1 ~ 6 を FC ポートとして設定することだけがサポートされています。今後 FC ストレージを接続する必要がある場合は、ポート 1 ~ 6 を FC に変換します。



(注) 変換により、HX の展開が中断される場合があります。

- CIMC サーバを接続する前に、Cisco VIC 1227 が HXc240 の PCIe スロット 2 または HXc220 のライザ 1 スロット 1 に装着されており、Cisco UCS Manager と統合できることを確認します。カードが正しいスロットに装着されていないと、サーバの直接接続管理を有効にできません。
- サーバからファブリック インターコネクットへの物理的なケーブル接続を完了し、ポートをサーバポートとして設定します。

**ステップ 1** ラックに HX サーバを設置します。詳細については、[ラック設置型 Cisco HyperFlex ノード \(43 ページ\)](#) を参照してください。

**ステップ 2** ファブリック インターコネクット上のサーバポートを設定します。

- a) サーバ上の 1 つのポートから 10-Gb SFP+ ケーブルをファブリック インターコネクット A に接続します。ファブリック インターコネクット A 上の任意のポートを使用できますが、サーバトラフィックに対応可能なポートでなければなりません。

1 枚のカード用に、VIC からファブリック インターコネクットに 1 本のケーブルを接続します。両方のポートを同じファブリック インターコネクットに接続しないでください。

- b) そのポートをサーバポートとして FI-A で設定します。詳細な手順については、『[Cisco UCS Manager Network Management Guide](#)』の「[Configuring Port Modes for a 6248 Fabric Interconnect](#)」を参照してください。
- c) サーバ上のもう一方のポートから 10-Gb SFP+ ケーブルを FI B に接続します。FI B 上の任意のポートを使用できますが、サーバトラフィックに対応可能なポートでなければなりません。

(注) アップリンクでSFP+タイプを混在させないでください。混在させると、「検出が失敗しました」というエラーが発生します。

- d) そのポートをサーバポートとしてFI-Bで設定します。詳細な手順については、『[Cisco UCS Manager Network Management Guide](#)』の「[Configuring Port Modes for a 6248 Fabric Interconnect](#)」を参照してください。

**ステップ3** 電源コードをノードの各電源装置に接続し、接地されたAC電源コンセントにも接続します。初期ブート時に、スタンバイ電源でノードが起動するまで約2分待ちます。

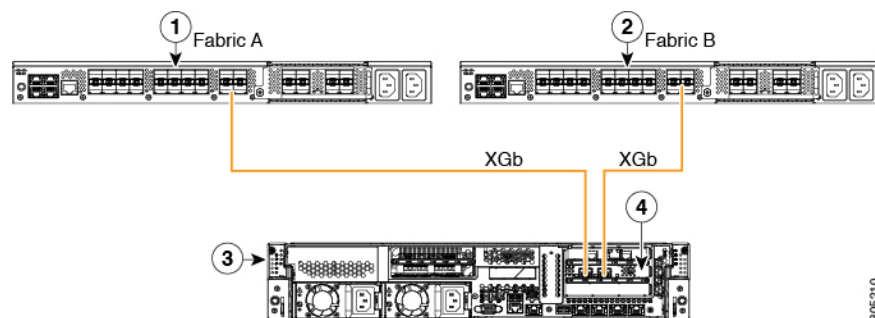
- (注)
1. 電力が供給されるようになると、ファブリック インターコネクトによってサーバが検出されます。UCS Managerでノードの検出を監視できます。
  2. 前面パネルのノードの[電源ステータスLED (Power Status LED)]を調べて、ノードの電源ステータスを確認します。LEDがオレンジ色の場合は、ノードがスタンバイ電源モードです。

**ステップ4** ステップ1～4を繰り返し、残りのHXシリーズサーバをHyperFlexクラスタに接続します。

## 直接接続モードのクラスタ セットアップの物理的な接続の図

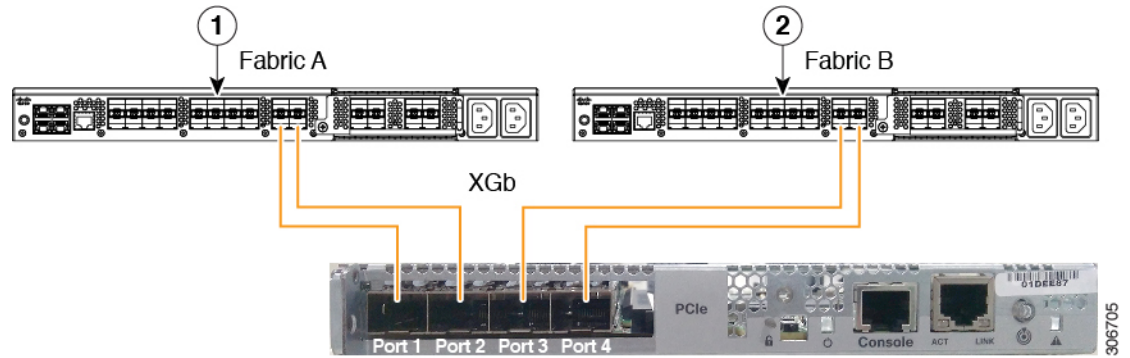
次の図は、C-Series Rack-Mount ServerとCisco UCS Domain、Cisco UCS Manager リリース 3.1以降との直接接続モードの物理接続の例を示しています。次の図は、UCS ManagerとC-Seriesラックマウントサーバを統合する場合の配線構成を示しています。金色で示されたパスでは、管理トラフィックとデータトラフィックの両方が伝送されます。

図9: 直接接続ケーブル配線の設定



305210

図 10: Cisco VIC 1455 との直接接続の配線構成



1	Cisco UCS 6454 ファブリック インターコネク トまたは Cisco UCS 6200、または 6300 シリー ズ FI (ファブリック A)	3	C シリーズ ラックマウント サーバ
2	Cisco UCS 6454 ファブリック インターコネク トまたは Cisco UCS 6200 または 6300 シリー ズ FI (ファブリック B)	4	サポート対象 PCIe スロット内の Cisco UCS VIC

XGb は 40 ギガビット イーサネット接続または 10 ギガビット イーサネット接続を表します。  
10 ギガビット イーサネットの場合、次のケーブルが使用されます。

- 4 X 10 ブレークアウト Small Form-Factor Pluggable (SFP) ケーブル
- 4 X 10 アクティブ光ケーブル (OAC)
- Qualified Security Assessor (QSA) モジュールを使用する 10G Small Form-Factor Pluggable (SFP) ケーブル

## コンピューティング専用ノードとファブリックインターコネクットの接続

このトピックでは、既存の HyperFlex クラスタにコンピューティング専用ノードを物理的に追加する方法について説明します。



- (注) HyperFlex ストレージクラスタを作成して設定した後、HyperFlex クラスタにコンピューター専用ノードを接続します。
1. HyperFlex ストレージクラスタがすでに作成されていることを確認します。
  2. コンピューティングノードとなる HX サーバを接続します。コンピューティング専用ノードのインストールの詳細については、「[ラック設置型 Cisco HyperFlex ノード \(43 ページ\)](#)」を参照してください。

3. Cisco HX Data Platform を使用してクラスタ拡張ワークフローを実行します。コンピューティング専用ノードを追加するには、クラスタ拡張ワークフローを使用します。詳細な手順については、「[既存のクラスタにコンピューティング専用ノードを追加する \(176 ページ\)](#)」を参照してください。





## 第 5 章

# Cisco HyperFlex Systems の設定

この章では、Cisco HyperFlex System のコンポーネントの設定方法について説明します。

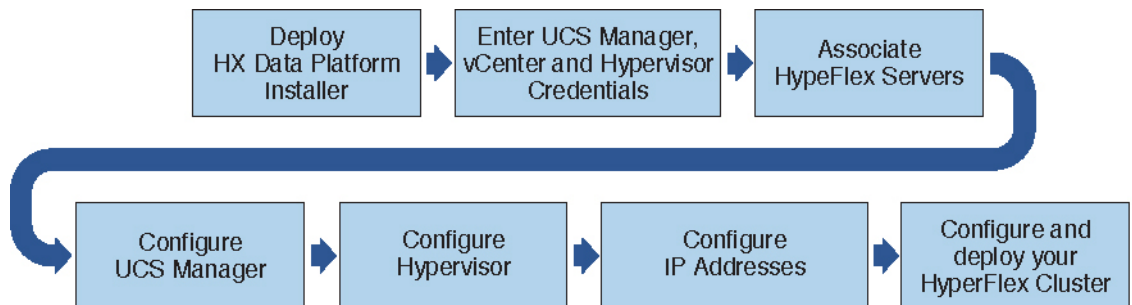
- [設置ワークフロー](#) (59 ページ)
- [vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開](#) (60 ページ)
- [静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開](#) (63 ページ)
- [Syslog の設定](#) (64 ページ)
- [HyperFlex クラスタの設定と展開](#) (65 ページ)
- [GPU が搭載された HyperFlex ノードのインストール](#) (78 ページ)
- [HX Data Platform インストーラのナビゲーション支援ボタン](#) (79 ページ)
- [警告およびエラー メッセージ](#) (80 ページ)

## 設置ワークフロー



(注) 以前に HyperFlex クラスタノードが他の HyperFlex クラスタの一部であった場合 (または工場出荷前の場合)、クラスタの導入を開始する前にノードのクリーンアップ手順を実行します。詳細については、『[HyperFlex Customer Cleanup Guides for FI and Edge](#)』を参照してください。

次のインストール ワークフローは、HX データ プラットフォーム インストーラを使用して標準クラスタを作成する手順の概要です。



8006376

インストール時に従うワークフローは次のとおりです。

1. vSphere Web Client を使用して HX データ プラットフォーム インストーラ OVA を展開します。ハイパーバイザ ウィザードが新しい VM に IP アドレスを割り当てる際の DHCP に対してデフォルトの場合、静的 IP アドレスを持つ HX データ プラットフォーム インストーラ OVA を展開します。詳細については、[vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開 \(60 ページ\)](#) または [静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開 \(63 ページ\)](#) を参照してください。
2. Syslog を設定して、syslog の一元的なリポジトリにすべてのログ情報を送信します。詳細については、[Syslog の設定 \(64 ページ\)](#) を参照してください。
3. UCS Manager、vCenter、およびハイパーバイザのクレデンシャルを入力します。
4. サーバー ポートを設定し、HyperFlex サーバーを関連付けます。詳細については、[HyperFlex サーバの関連付け \(65 ページ\)](#) を参照してください。
5. アウトオブバンド CIMC、iSCSI ストレージ、および FC ストレージの VLAN、MAC プール、'hx-ext-mgmt' IPPool を設定します。詳細については、[UCS Manager の設定 \(67 ページ\)](#) を参照してください。
6. ハイパーバイザを設定します。詳細については、[ハイパーバイザの構成 \(71 ページ\)](#) を参照してください。
7. IP アドレスを設定します。詳細については、[IP アドレスの設定 \(73 ページ\)](#) を参照してください。
8. HyperFlex クラスタを設定し、展開します。詳細については、「[HyperFlex クラスタの設定 \(74 ページ\)](#)」を参照してください。

## vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開

ESXi ホストに HX Data Platform をインストールするだけでなく、VMware Workstation、VMware Fusion または Virtual Box にも HX Data Platform インストーラを展開することができます。



- (注)
- vCenter に接続して OVA ファイルを展開し、IP アドレス プロパティを指定します。ESXi ホストから直接展開しても、値を正しく設定することはできません。
  - Cisco HX ストレージ クラスタ内のノードとなる ESXi サーバに HX Data Platform インストーラを展開しないでください。



**ステップ 1** [ソフトウェアのダウンロード (Download Software)] で HX Data Platform インストーラ OVA ファイルを特定してダウンロードします。HX Data Platform ストレージクラスタに使用されるストレージ管理ネットワーク上のノードに、HX Data Platform インストーラをダウンロードします。

Example:  
Cisco-HX-Data-Platform-Installer-v5.0.1a-26363.ova

**ステップ 2** VMware ハイパーバイザを使用して HX Data Platform インストーラを展開し、HX Data Platform インストーラ仮想マシンを作成します。

(注) 仮想ハードウェアリリース 10.0 以降をサポートする仮想化プラットフォームのリリースを使用してください。

vSphere はシステム要件です。vSphere シック クライアント、vSphere シンクライアント、または vSphere Web クライアントのいずれかを使用できます。HX Data Platform インストーラを展開するには、VMware Workstation、VMware Fusion、または VirtualBox を使用することもできます。

- vSphere、VirtualBox、Workstation、Fusion などの仮想マシン ハイパーバイザを開きます。
- HX Data Platform インストーラを展開するノードを選択します。

**重要** vSphere Web Client を使用して HX インストーラ OVA を導入する際は、ユーザー クレデンシャルを必ず指定してください。

- vSphere シック クライアントを使用する—[インベントリ リスト (Inventory list)] > [ホスト (Host)] > [ファイル (File)] > [OVA を展開 (Deploy OVA)] を展開します
- vSphere Web クライアントを使用する—[vCenter インベントリ リスト (vCenter Inventory list)] > [ホスト (Hosts)] > [ホスト (Host)] > [OVA を展開 (Deploy OVA)] を展開します

**ステップ 3** HX Data Platform インストーラ の場所を選択します。デフォルト値を使用し、適切なネットワークを選択します。

**ステップ 4** HX Data Platform インストーラ VM で使用する静的 IP アドレスを入力します。

- (注)
- ネットワークで DHCP が設定されている場合でも、静的 IP アドレスが必要です。HX Data Platform インストーラを実行し、HX Data Platform をインストールし、HX Data Platform ストレージクラスタを作成するには、静的 IP アドレスが必要です。
  - 新しい VM への IP アドレス割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開 (63 ページ) の手順を実行して、静的 IP アドレスで HX Data Platform インストーラ VM をインストールします。インストーラ VM から DNS が到達可能である必要があります。

フィールド	説明
ホスト名	この VM のホスト名。 IP アドレスの逆引きを試みるには空白のままにします。

フィールド	説明
デフォルト ゲートウェイ	この VM のデフォルト ゲートウェイ アドレス。 DHCP を使用する場合は、空白のままにします。
DNS	この VM のドメイン ネーム サーバ (カンマ区切りリスト)。 DHCP を使用する場合は、空白のままにします。
IP アドレス	このインターフェイスの IP アドレス。 DHCP を使用する場合は、空白のままにします。
ネットマスク	このインターフェイスのネットマスクまたはプレフィックス。 DHCP を使用する場合は、空白のままにします。
Root パスワード	ルート ユーザー パスワード。 このフィールドは必須フィールドです。

**ステップ 5** [次へ (Next) ] をクリックします。リストされたオプションが正しいかどうかを確認し、[導入後に電源をオンにする (Power on after deployment) ] を選択します。

HX Data Platform インストーラを手動で電源オンにするには、仮想マシンのリストに移動し、インストーラ VM の電源をオンにします。

(注) HX Data Platform インストーラ仮想マシンの推奨設定は、3 つの vCPU と 4 GB のメモリです。これらの設定を小さくすると、CPU の使用率が 100% になり、ホストのスパイクが発生する可能性があります。

**ステップ 6** [Finish] をクリックします。HX Data Platform インストーラ VM が vSphere インフラストラクチャに追加されるまで待ちます。

**ステップ 7** HX Data Platform インストーラ仮想マシンを開きます。

初期コンソール画面に、HX Data Platform インストーラ仮想マシンの IP アドレスが表示されます。

```
Data Platform Installer.
*****
You can start the installation by visiting
the following URL:
http://192.168.10.210
*****
Cisco-HX-Data-Platform-Installer login:
```

**ステップ 8** HX Data Platform インストーラにログインするための URL を使用します。

```
Example:
http://192.168.10.210
```

**ステップ 9** 自己署名証明書を受け入れます。

**ステップ 10** ユーザー名 **root** と、OVA 導入の一部として設定したパスワードを使用してログインします。

# 静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開

新しい VM への IP アドレスの割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、以下の手順を使用して HX Data Platform インストーラを展開します。

- ステップ 1** HX Data Platform ストレージクラスタに使用されるストレージ管理ネットワーク上のノードに、VMware OVF Tool 4.1 以降をインストールします。詳細については、「[OVF ツール ドキュメンテーション](#)」を参照してください。
- ステップ 2** VMware OVF がインストールされているノードの「[ソフトウェアのダウンロード](#)」から、HX Data Platform インストーラ OVA を見つけてダウンロードします。
- ステップ 3** ovftool コマンドを使用して、ダウンロードした HX Data Platform インストーラ OVA を展開します。次に例を示します。

```
root@server:/tmp/test_ova# ovftool --noSSLVerify --diskMode=thin
--acceptAllEulas=true --powerOn --skipManifestCheck --X:injectOvfEnv
--datastore=qa-048-ssd1 --name=rfsi_static_test1 --network='VM Network'
--prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1
--prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8
--prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco
--prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5
--prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36
--prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0
--prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
vi://root:password@esx_server
```

このコマンドにより、HX Data Platform インストーラが展開され、HX Data Platform インストーラ VM の電源が入り、指定された静的 IP アドレスが設定されます。以下は処理応答の例です。

```
Opening OVA source:
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
Opening VI target: vi://root@esx_server:443/
Deploying to VI: vi://root@esx_server:443/
Transfer Completed
Powering on VM: rfsi_static_test
Task Completed
Completed successfully
```

インストーラ VM から DNS が到達可能である必要があります。静的 IP アドレスを正常に設定するために必要なコマンド オプションは以下のとおりです。

コマンド	説明
powerOn	HX Data Platform インストーラ VM の展開後に電源を投入します。
X:injectOvfEnv	HX Data Platform インストーラ VM に静的 IP のプロパティを挿入します。

コマンド	説明
prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1	適切なゲートウェイ IP アドレスを指定します。
prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8	適切な DNS IP アドレスを指定します。
prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco	適切なドメインを指定します。
prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5	適切な NTP IP アドレスを指定します。
prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36	適切なインストーラの静的 IP アドレスを指定します。
prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0	適切なネットマスク アドレスを指定します。
prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword	root ユーザー パスワードを指定します。
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova	HX Data Platform インストーラ OVA の送信元アドレス。
vi://root:password@esx_server	HX データプラットフォーム インストーラ VM がインストールされている宛先 ESX サーバ。適切な ESX サーバのルート ログイン クレデンシャルが含まれます。

## Syslog の設定

集中型 syslog リポジトリにすべてのロギング情報を送信することをお勧めします。



- 注目** 一般に、監査ログの長期保持が必要な場合は、syslog を使用した監査ログのエクスポートを設定することをお勧めします。特にSDカードから起動するHX220cノードとコンピューティング専用ノード上で、永続ロギングに syslog 設定が必要です。Syslog サーバを設定しない場合、ログローテーションポリシーにより監査ログが上書きされます。



(注) ESXi の永続的なスクラッチ ロケーションの宛先として NFS データストアを選択することはできません。永続的なスクラッチ ロケーションに HX データストアを選択すると、ESXi ホストのリロード後に削除されます。

すべての M5 および M6 サーバーについては、スクラッチとして使用するために M.2 ブレート SSD が自動的に選択されます。これは、新しいインストールのボックスから設定されます。

HX240M4(非 SED)の場合、固定ログ/スクラッチに Intel SSD が使用されます (220M5/240M5 では同じですが、異なるローカル SSD にも適用されます)。

HX220M4 および HX240M4 (SED) の場合、スクラッチ パーティションを保存する場所はありません。そのため、唯一のオプションは、ネットワーク上の永続的なロギングに syslog を使用することです。

**ステップ 1** syslog サーバが稼動していること、および ESXi サーバからログを受信するために TCP/UDP ポートが開いていることを確認してください。

**ステップ 2** ESXi シェルに SSH 接続して、次のコマンドを実行します。

```
a) esxcli system syslog config set --loghost='udp://remote-syslog-server-ip'
b) esxcli system syslog reload
c) esxcli network firewall ruleset set -r syslog -e true
d) esxcli network firewall refresh
```

**ステップ 3** クラスタ内のすべての ESXi ホストに対してステップ 1～2 を繰り返します。

**ステップ 4** リモート syslog サーバで、指定されたディレクトリにログが受信されているかどうかを確認します。

## HyperFlex クラスタの設定と展開

### HyperFlex サーバの関連付け

[サーバの選択 (Server Selection)] ページで、右側にある [構成 (Configuration)] ペインの [クレデンシヤル (Credentials)] に、使用されているクレデンシヤルの詳細なリストが表示されます。[サーバの選択 (Server Selection)] ページの [関連付けなし (Unassociated)] タブには、関連付けられていない HX サーバのリストが表示され、[関連付け済み (Associated)] タブには検出されたサーバのリストが表示されます。

フィールド	説明
ロケータ LED (Locator LED)	サーバーの検索をオンにします。
サーバー名 (Server Name)	サーバーに割り当てられた名前。

フィールド	説明
Status (ステータス)	<ul style="list-style-type: none"> <li>アクセス不可—</li> </ul>
モデル (Model)	サーバー モデルが表示されます。
シリアル (Serial)	サーバーのシリアル番号を表示します。
関連付けのステータス (Assoc State)	<ul style="list-style-type: none"> <li>関連</li> <li>関連付けなし</li> </ul>
サービスプロファイル (Service Profile) (関連付けられたサーバーに対してのみ)	<p>サーバーに割り当てられているサービス プロファイル。</p> <p>(注) HyperFlex サービス プロファイル テンプレートの編集はお勧めしません。</p>
アクション (Actions)	<ul style="list-style-type: none"> <li>[<b>KVM コンソールの起動 (Launch KVM Console)</b>]: HX Data Platform から直接 KVM コンソールを起動するには、このオプションを選択します。</li> <li>[<b>サーバの関連付け解除 (Disassociate Server)</b>]: サーバからサービスプロファイルを削除するには、このオプションを選択します。</li> </ul>

### 始める前に

UCS Manager、vCenter、およびハイパーバイザ クレデンシャルの入力を完了していることを確認します。

**ステップ 1** [サーバ ポートの構成 (Configure Server Ports)] をクリックして新しい HX ノードを検出します。[サーバ ポートの構成 (Configure Server Ports)] ダイアログボックスに、サーバ ポートとして構成されるすべてのポートが一覧表示されます。[構成 (Configure)] をクリックします。

(注) 一般的に、構成を始める前に、サーバ ポートは Cisco UCS Manager で構成されます。

**ステップ 2** HyperFlex クラスタに含める [関連付けなし (Unassociated)] タブの下のサーバを選択します。

HX サーバがこのリストに表示されない場合は、[Cisco UCS Manager] をオンにして、検出されていることを確認します。

(注) 関連付けられていないサーバがない場合は、次のエラー メッセージが表示されます。

```
No unassociated servers found. Login to UCS Manager and ensure server ports are enabled.
```

ステップ 3 [続行 (Continue)] をクリックして、UCS Manager の構成を続けます。「[UCS Manager の設定 \(67 ページ\)](#)」を参照してください。

## UCS Manager の設定

[UCSM 構成 (UCSM Configuration)] ページでは、CIMC、iSCSi ストレージ、FC ストレージに関する VLAN、MAC プール、「hx-ext-mgmt」 IP プールを構成できます。

### 始める前に

HyperFlex クラスタにサーバを関連付けます。[HyperFlex サーバの関連付け \(65 ページ\)](#) を参照してください。

ステップ 1 [VLAN 設定 (VLAN Configuration)] セクションで、次のフィールドに値を入力します。

(注) 次のそれぞれのネットワークに、別個のサブネットと VLAN を使用します。

フィールド	説明
<b>ハイパーバイザとHyperFlex管理用のVLAN</b>	
VLAN 名	hx-inband-mgmt
VLAN ID (Admin. VLAN ID)	デフォルト: 3091
<b>HyperFlexストレージトラフィック用のVLAN</b>	
VLAN 名	hx-storage-data
VLAN ID (Admin. VLAN ID)	デフォルト: 3092
<b>VM vMotion用のVLAN</b>	
VLAN 名	hx-vmotion
VLAN ID (Admin. VLAN ID)	デフォルト: 3093
<b>VMネットワーク用のVLAN</b>	
VLAN 名	vm-network
VLAN ID	デフォルト: 3094 ゲスト VLAN のカンマ区切りリスト。

ステップ 2 [MAC プール (MAC Pool)] セクションの [MAC プールのプレフィックス (MAC Pool Prefix)] で、追加の 2 つの 16 進文字 (0 ~ F) を指定して MAC プールのプレフィックスを構成します。

(注) すべての UCS ドメインにわたり、他の MAC アドレス プールで使用とされていないプレフィックスを選択します。

Example:  
00:25:B5:A0:

**ステップ 3** [CIMC の 'hx-ext-mgmt' IP プール ('hx-ext-mgmt' IP Pool for CIMC) ]セクションで、次のフィールドに値を入力します。

フィールド	説明
[IP Blocks]	各 HyperFlex サーバーの CIMC に割り当てられた管理 IP アドレスの範囲。IP アドレスは範囲として指定し、複数の IP ブロックをカンマ区切りのリストとして指定できます。クラスタ内のサーバごとに少なくとも1つの一意の IP があることを確認します。アウトオブバンドの使用を選択する場合、この範囲はファブリック インターコネクットの mgmt0 インターフェイスで使用されているものと同じ IP サブネットに属している必要があります。  たとえば、10.193.211.124-127, 10.193.211.158-163 などです。
[Subnet Mask]	上記の IP 範囲のサブネット マスクを指定します。  たとえば、255.255.0.0 とします。
[ゲートウェイ (Gateway) ]	ゲートウェイの IP アドレスを入力します。  たとえば、10.193.0.1 とします。

サーバー上の CIMC へのアクセスに使用される管理 IP アドレスは、次のいずれかです。

- **アウトオブバンド** : CIMC 管理トラフィックは、ファブリック インターコネクット上の制限帯域幅管理 インターフェイス mgmt0 を介してファブリック インターコネクットを通過します。このオプションは最も一般的に使用され、ファブリック インターコネクット管理 VLAN と同じ VLAN を共有します。
- **インバンド** : CIMC 管理トラフィックは、ファブリック インターコネクットのアップリンク ポートを介してファブリック インターコネクットを通過します。この場合、管理トラフィックに使用できる帯域幅は、ファブリック インターコネクットのアップリンク帯域幅に相当します。インバンドオプションを使用している場合、Cisco HyperFlex インストーラは CIMC 管理通信専用の VLAN を作成します。このオプションは、Windows Server インストール ISO などの大きなファイルを OS インストール用の CIMC にマウントする必要がある場合に便利です。このオプションは、HyperFlex インストーラ VM でのみ使用でき、Intersight を介した展開には使用できません。

**ステップ 4** CIMC 管理アクセスに使用する接続のタイプに基づいて、**アウトオブバンド** または **インバンド** を選択します。[インバンド (In-band) ]を選択した場合は、管理 VLAN の VLAN ID を指定します。シームレスな接続のために、アップストリーム スイッチに CIMC 管理 VLAN を作成してください。



**ステップ 5** 外部ストレージを追加する場合は、次のフィールドに値を入力して [iSCSI ストレージ (iSCSI Storage)] を構成します。

フィールド	説明
[iSCSI ストレージの有効化 (Enable iSCSI Storage)] チェックボックス	iSCSI ストレージを構成する場合、このチェックボックスをオンにします。
<b>VLAN A 名 (VLAN A Name)</b>	プライマリ ファブリック インターコネクト (FI-A) で、iSCSI vNIC に関連付けられている VLAN の名前。
<b>VLAN A ID</b>	プライマリ ファブリック インターコネクト (FI-A) で、iSCSI vNIC に関連付けられている VLAN の ID。
<b>VLAN B 名 (VLAN B Name)</b>	下位のファブリック インターコネクト (FI-B) で、iSCSI vNIC に関連付けられている VLAN の名前。
<b>[VLAN B ID]</b>	下位のファブリック インターコネクト (FI-A) で、iSCSI vNIC に関連付けられている VLAN の ID。

**ステップ 6** 外部ストレージを追加する場合は、次のフィールドに値を入力して [FC ストレージ (FC Storage)] を構成します。

フィールド	説明
[FC ストレージの有効化 (Enable FC Storage)] チェックボックス	FC ストレージを有効にするには、このチェックボックスをオンにします。
<b>WWxN プール</b>	WW ノード名と WW ポート名の両方を含む WWN プール。それぞれのファブリック インターコネクトに対し、WWPN および WWNN 用の WWxN プールが作成されます。
<b>VSAN A 名 (VSAN A Name)</b>	プライマリ ファブリック インターコネクト (FI-A) の VSAN の名前。 デフォルト—hx-ext-storage-fc-a。
<b>VSAN A ID</b>	プライマリ ファブリック インターコネクト (FI-A) のネットワークに割り当てられた一意の ID。  <b>注意</b> UCS または HyperFlex システムで現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。

フィールド	説明
VSAN B名	下位のファブリック インターコネクト (FI-B) の VSAN の名前。 デフォルト—hx-ext-storage-fc-b.
VSAN B ID	下位のファブリック インターコネクト (FI-B) の ネットワークに割り当てられた一意の ID。 <b>注意</b> UCS または HyperFlex システムで現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。

ステップ 7 [詳細設定 (Advanced) ] セクションで、次の操作を行います。

フィールド	説明
UCS サーバー ファーム ウェアバージョン (UCS Server Firmware Version)	ドロップダウンリストから、HX サーバと関連付ける UCS サーバファームウェアバージョンを選択します。UCS ファームウェアバージョンは、UCSM バージョンと一致する必要があります。詳細については、最新の『 <a href="#">Cisco HX Data Platform Release Notes</a> 』を参照してください。 たとえば、3.2(1d) とします。
HyperFlex クラスタ名	ユーザ定義の名前を指定します。HyperFlex クラスタ名は、特定のクラスタ内の HX サーバグループに適用されます。HyperFlex クラスタ名によりサーバプロファイルにラベルが追加され、クラスタを識別しやすくなります。
組織名	HyperFlex 環境を UCS ドメインの残りの部分から確実に分離できるような一意の組織名を指定します。

ステップ 8 [続行 (Continue) ] をクリックして、ハイパーバイザの構成を続けます。「[ハイパーバイザの構成 \(71 ページ\)](#)」を参照してください。

## ハイパーバイザの構成



(注) [ハイパーバイザの構成 (Hypervisor Configuration)] ページの [構成 (Configuration)] ページで、VLAN、MAC プル、IP アドレス プールの情報を確認します。これらの VLAN ID は、環境によって変更されている可能性があります。デフォルトでは、HX Data Platform インストーラが VLAN を非ネイティブとして設定します。トランク構成を適切に適用することで、非ネイティブ VLAN に対応するアップストリーム スイッチを構成する必要があります。



**注目** 再インストールの場合、ESXi ネットワーキングが完了していれば、ハイパーバイザの構成をスキップできます。

### 始める前に

アウトオブバンド CIMC の VLAN、MAC プール、「hx-ext-mgmt」IP プールを構成します。外部ストレージを追加する場合は、iSCSI ストレージと FC ストレージを構成します。UCS サーバのファームウェア バージョンを選択し、HyperFlex クラスタの名前を割り当てます。UCS [Manager の設定 \(67 ページ\)](#) を参照してください。

**ステップ 1** [共通ハイパーバイザ設定の構成 (Configure Common Hypervisor Settings)] セクションで、次のフィールドに値を入力します。

フィールド	説明
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、255.255.0.0 とします。
[ゲートウェイ (Gateway)]	ゲートウェイの IP アドレス。 たとえば、10.193.0.1 とします。

フィールド	説明
[DNSサーバ (DNS Server(s)) ]	<p>DNS サーバの IP アドレス。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• DNS サーバを使用しない場合、HX Data Platform インストーラの <b>[クラスタの設定 (Cluster Configuration)]</b> ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。</li> <li>• 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。</li> </ul>

**ステップ 2** [ハイパーバイザ設定 (Hypervisor Settings) ] セクションで、[IP アドレスとホスト名を順番に選択 (Make IP Addresses and Hostnames Sequential) ] を選択し、連続的な IP アドレスにします。次のフィールドに入力します。

(注) ドラッグアンドドロップ操作を使用してサーバの順番を並び替えることができます。

フィールド	説明
名前 (Name)	サーバーに割り当てられた名前。
ロケータ LED (Locator LED)	サーバーの検索をオンにします。
シリアル (Serial)	サーバーのシリアル番号を表示します。
スタティック IP アドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。
ホスト名	ホスト名フィールドを空のままにしないでください。

**ステップ 3** [続行 (Continue) ] をクリックして、IP アドレスの構成を続けます。「[IP アドレスの設定 \(73 ページ\)](#)」を参照してください。

## IP アドレスの設定

### 始める前に

[ハイパーバイザ設定 (Hypervisor Configuration) ] ページでハイパーバイザの設定が完了していることを確認します。 [ハイパーバイザの構成 \(71 ページ\)](#) を参照してください。

**ステップ 1** [IP アドレス (IP Addresses) ] ページで、[IP アドレスを連続させる (Make IP Addresses Sequential) ] を選択し、連続的な IP アドレスにします。

**ステップ 2** ハイパーバイザ、ストレージコントローラ (管理) とハイパーバイザ、ストレージコントローラ (データ) 列の最初の行に IP アドレスを入力すると、HX Data Platform Installer により、残りのノードのノード情報が増分されて自動入力されます。ストレージクラスタ内のノードの最小数は 3 です。それより多くのノードがある場合は、[追加 (Add) ] ボタンを使用して、アドレス情報を指定します。

(注) コンピューティング専用ノードは、ストレージクラスタを作成してからでないと追加できません。

各 HX ノードについて、ハイパーバイザ、ストレージコントローラ、管理、データ IP アドレスを入力します。IP アドレスには、ネットワークがデータネットワークと管理ネットワークのどちらに属しているかを指定します。

フィールド	説明
管理ハイパーバイザ	ESXi ホストとストレージコントローラ間のハイパーバイザ管理ネットワーク接続を処理するスタティック IP アドレスを入力します。
管理ストレージコントローラ	ストレージコントローラ VM とストレージクラスタ間のストレージコントローラ VM 管理ネットワーク接続を処理する静的 IP アドレスを入力します。
Data Hypervisor	ESXi ホストとストレージコントローラ間のハイパーバイザデータ ネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージコントローラ	ストレージコントローラ VM とストレージクラスタの間のストレージコントローラ VM データ ネットワーク接続を処理するスタティック IP アドレスを入力します。

**ステップ 3** ここで指定する IP アドレスは、ストレージクラスタ内の 1 つのノードに適用されます。ノードが使用できなくなった場合は、該当する IP アドレスがストレージクラスタ内の別のノードに移動されます。すべてのノードには、これらの IP アドレスを受け入れるように構成されたポートが必要です。

次の IP アドレスを指定します。

フィールド	説明
管理クラスタ データの IP アドレス (Management Cluster Data IP Address)	HX データ プラットフォーム ストレージ クラスタ の管理 ネットワーク IP アドレス を入力 します。
データ クラスタ データ IP アドレス (Data Cluster Data IP Address)	HX Data Platform ストレージ クラスタ のデータ ネットワーク の IP アドレス を入力 します。
管理サブネットマスク	VLAN と vSwitch のサブネット情報を 入力 します。 管理 ネットワーク の値 を入力 します。たとえば、255.255.255.0 と入力 します。
データサブネットマスク	データ ネットワーク のネットワーク の値 を入力 します。たとえば、255.255.255.0 と入力 します。
管理ゲートウェイ	管理 ネットワーク のネットワーク の値 を入力 します。たとえば、10.193.0.1 とし ます。
データゲートウェイ	データ ネットワーク のネットワーク の値 を入力 します。たとえば、10.193.0.1 とし ます。

ステップ 4 [続行] をクリックして HyperFlex クラスタ を設定 します。「[HyperFlex クラスタ の設定 \(74 ページ\)](#)」を参照 してください。

## HyperFlex クラスタ の設定

[クラスタ構成 (Cluster Configuration)] ページで、Cisco HX ストレージ クラスタ に関する以下のフィールドに値 を入力 し、HyperFlex クラスタ の導入 を開始 します。

### 始める前に

[IP アドレス (IP Addresses)] ページで IP アドレス の構成 が完了 していることを確認 します。[IP アドレス の設定 \(73 ページ\)](#) を参照 してください。

ステップ 1 [Cisco HX クラスタ (Cisco HX Cluster)] セクションで、次のフィールドに値 を入力 します。

フィールド	説明
クラスタ名 (Cluster Name)	HX データ プラットフォーム ストレージ クラスタ の名前 を指定 します。

フィールド	説明
レプリケーション ファクタ (Replication Factor)	<p>ストレージクラスタ全体でのデータの冗長レプリカの数指定します。レプリケーションファクタを冗長レプリカ数 2 または 3 に設定します。</p> <ul style="list-style-type: none"> <li>ハイブリッドサーバ (SSD と HDD を含むサーバ) の場合、デフォルト値は 3 です。</li> <li>フラッシュ サーバー (SSD のみを含むサーバ) の場合は、2 または 3 を選択します。</li> <li>Hyperflex Edge を除くすべての環境で複製ファクタ 3 を強く推奨しています。複製ファクタ 2 では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。</li> </ul>

**ステップ 2** [コントローラ VM (Controller VM)] セクションで、HyperFlex クラスタの管理者ユーザの新しいパスワードを作成します。

コントローラ VM には、デフォルトの管理者ユーザ名とパスワードが適用されます。VM は、コンバージドノードとコンピューティング専用ノードのすべてにインストールされます。

- 重要**
- コントローラ VM またはコントローラ VM のデータストアの名前を変更することはできません。
  - すべてのコントローラ VM に同じパスワードを使用します。異なるパスワードの使用はサポートされていません。
  - 1 つの大文字、1 つの小文字、1 つの数字、1 つの特殊文字を含む、10 文字以上の複雑なパスワードを指定してください。
  - コントローラ VM と、作成される HX クラスタには、ユーザ定義のパスワードを指定できません。パスワードに使用できる文字と形式に関する制限事項については、『Cisco HX Data Platform Management Guide』のセクション「Guidelines for HX Data Platform Special Characters」を参照してください。

**ステップ 3** [vCenter の設定 (vCenter Configuration)] セクションで、次のフィールドに値を入力します。

フィールド	説明
vCenter データセンター名 (vCenter Datacenter Name)	Cisco HyperFlex クラスタの vCenter データセンターの名前を入力します。
vCenter クラスタ名 (vCenter Cluster Name)	vCenter クラスタ名を入力します。

**ステップ 4** [システム サービス (System Services)] セクションで、次のフィールドに値を入力します。

DNS サーバー (DNS Server(s))	各 DNS サーバーの IP アドレスのカンマ区切りリスト。
NTP サーバー (NTP Server(s))	各 NTP サーバの IP アドレスのカンマ区切りリスト。  (注) すべてのホストが同じ NTP サーバを使用して、ストレージコントローラ VM と ESXi ホストで実行されているサービスの間でクロックを同期する必要があります。
DNS ドメイン名 (DNS Domain Name)	DNS FQDN または IP アドレスが無効です
タイムゾーン (Time Zone)	コントローラ VM のローカルタイムゾーン。このタイムゾーンに基づいて、スケジュールされたスナップショットを取るタイミングが決定されます。スケジュールされたネイティブスナップショットアクションは、この設定に基づきます。

ステップ 5 [コネクテッドサービス (Connected Services)] セクションで、[コネクテッドサービスを有効にする (Enable Connected Services)] を選択して、自動サポート (Auto Support) および Intersight Management を有効にします。

フィールド	説明
コネクテッドサービスの有効化 (Enable Connected Services) (推奨)	自動サポート (Auto Support) および Intersight Management を有効にします。HX Connect にログオンしてこれらのサービスを構成するか、またはそれらを選択的にオンまたはオフにします。
サービスチケット通知の送信先 (Send service ticket notifications to)	自動サポートによってトリガーされたときに SR 通知が送信される電子メールアドレス。

ステップ 6 [詳細設定 (Advanced)] セクションで、次の操作を行います。

フィールド	説明
ジャンボフレーム ジャンボフレームを有効化 (Enable Jumbo Frames)	ホスト vSwitches と vNIC、および各ストレージコントローラ VM 上のストレージデータネットワークの MTU サイズを設定する場合は、このチェックボックスをオンにします。  デフォルト値は 9000 です。  (注) MTU サイズを 9000 以外の値に設定するには、Cisco TAC にご連絡ください。



フィールド	説明
ディスクパーティション ディスクパーティションのクリーンアップ (Clean up Disk Partitions)	<p>ストレージクラスタに追加されたすべてのノードから既存のデータとパーティションをすべて削除して手動でサーバを準備する場合は、このチェックボックスをオンにします。既存のデータやパーティションを削除するには、このオプションを選択します。保持する必要があるデータはすべてバックアップする必要があります。</p> <p><b>注目</b> 工場で準備されたシステムの場合は、このオプションを選択しないでください。工場で準備されたシステムのディスクパーティションは正しく設定されています。</p>
仮想デスクトップ(VDI)	<p>VDI のみの環境でオンにします。</p> <p>(注) ストレージクラスタの作成後に VDI 設定を変更するには、リソースをシャットダウンまたは移動し、変更を加え (下の手順に記載)、クラスタを再起動します。</p> <p>デフォルトでは、HyperFlex クラスタは VSI ワークロード用にパフォーマンス調整されるように設定されています。</p> <p>このパフォーマンスのカスタマイズは、Hyperflex Data Platform クラスタで次の手順を実行することによって変更できます。HyperFlex クラスタを VDI から VSI ワークロード (またはその逆) に変更するには、次のようにします。</p> <p><b>警告:</b> メンテナンス ウィンドウが必要です。これにより、クラスタがオフラインの間はデータが使用できなくなります。</p> <ol style="list-style-type: none"> <li>1. <code>~#stcli cluster shutdown</code> を実行してクラスタをシャットダウンします。</li> <li>2. すべてのコントローラ VM の <code>storfs cfg</code> を編集し、<code>workloadType</code> を <code>Vsi</code> または <code>Vdi</code> に変更します。</li> <li>3. クラスタの作成後に、クラスタを起動し (<code>stcli cluster start</code>)、調整の変更を有効にします。</li> </ol>

フィールド	説明
(オプション) vCenter Server のシングルサインオン (vCenter Single-Sign-On Server)	<p>この情報は、SSO URL が到達可能でない場合のみ必要です。</p> <p>(注) このフィールドは使用しないでください。これはレガシー展開に使用されます。</p> <p><b>[vCenter Server] &gt; [Manage] &gt; [Advanced Settings] &gt; [key config.vpxd.sso.sts.uri]</b> にナビゲートして、vCenter で SSO URL を見つけることができます。</p>

**ステップ 7** **[開始 (Start)]** をクリックして HyperFlex クラスタの展開を開始します。[進捗状況 (Progress)] ページには、さまざまな設定タスクの進捗状況が表示されます。

**注意** 確認に関する警告を無視しないでください。

詳細については、「警告」セクションを参照してください。

#### 次のタスク

- 検証エラーによっては、パラメータの再入力が必要になることがあります（たとえば、無効な ESXi パスワード、誤った NTP サーバ、不良 SSO サーバなどの誤った入力の原因のエラー）。**[値の再入力 (Re-enter Values)]** をクリックして **[クラスタ構成 (Cluster Configuration)]** ページに戻り、問題を解決します。
- これが完了すると、HyperFlex サーバがインストールされ、構成されます。正常にデプロイされたクラスタのステータスは、**[オンライン (Online)]** および **[正常 (Healthy)]** として示されます。
- **[HyperFlex Connect の起動 (Launch HyperFlex Connect)]** をクリックし、データストアを作成してクラスタを管理します。

## GPU が搭載された HyperFlex ノードのインストール

GPU が搭載された HyperFlex ノードをインストールする際は、特定の BIOS ポリシーを変更する必要があります。サポートされているすべての GPU カードで、4 GB 以上のメモリマップド I/O (MMIO) を許可する BIOS 設定を有効にする必要があります。詳細については、「[サポートされているすべての GPU に関する要件](#)」を参照してください。

#### HyperFlex クラスタ作成後の GPU のインストール

クラスタの作成後に GPU をインストールする場合は、サーバに関連付けられたサービス プロファイルを変更して、BIOS ポリシー設定を有効にする必要があります。

「[Cisco UCS Manager で制御されるサーバ](#)」の記述に従って、BIOS 設定を有効にします。ステップ3で指定したように、4 GB を超えるメモリ マップド I/O を [有効 (Enabled)] に設定します。

### HyperFlex クラスタ作成前の GPU のインストール

クラスタの作成前に GPU カードをインストールする場合は、クラスタの作成中に、[高度なワークフロー (Advanced workflow)] を選択します。

1. HX データ プラットフォーム インストーラ ページで、[私は自分のやっていることがわかっている、ワークフローをカスタマイズできるようにしてください (I know what I'm doing, let me customize my workflow)] を選択します。
2. [UCS マネージャ設定の実行 (Run UCS Manager Configuration)] をクリックし、[続行 (Continue)] をクリックします。  
これにより、HyperFlex ノードに必要なサービス プロファイルが作成されます。
3. 「[Cisco UCS Manager で制御されるサーバ](#)」の記述に従って、BIOS 設定を有効にします。ステップ3で指定したように、4 GB を超えるメモリ マップド I/O を [有効 (Enabled)] に設定します。
4. HX データ プラットフォーム インストーラ ページの [高度なワークフロー (Advanced workflow)] に戻って、[ESX 設定の実行 (Run ESX Configuration)]、[HX ソフトウェアの展開 (Deploy HX Software)]、および [HX クラスタの作成 (Create HX Cluster)] に進み、クラスタの作成を完了します。

## HX Data Platform インストーラのナビゲーション支援ボタン

- **エクスポート設定 (Export Configuration)** : JSON 設定ファイルをダウンロードするには、下矢印アイコンをクリックします。
- **ワークフロー情報 (Workflow Info)** : 現在のワークフローを表示するには、情報アイコンの上にカーソルを移動します。HyperFlex クラスタの作成に関するワークフロー情報は [ワークフローの作成 = Esx (Create Workflow = Esx)] です。
- **テクニカル サポート (Tech Support)** : HyperFlex Data Platform ソフトウェアのバージョンに関連する詳細を表示するには、疑問符アイコンをクリックします。Cisco TAC 用にテクニカルサポートバンドルを作成するには、[新しいバンドルの作成 (Create New Bundle)] をクリックします。
- **変更の保存 (Save Changes)** : HyperFlex クラスタの設定パラメータの変更内容を保存するには、円アイコンをクリックします。
- **設定 (Settings)** : もう一度やり直すか、またはログアウトするには、歯車アイコンをクリックします。

## 警告およびエラーメッセージ

- UCSM の設定とハイパーバイザの設定は正常に完了したものの、導入またはクラスタ作成は失敗した：[設定アイコン (Settings Icon)] > [初めからやり直す (Start Over)] をクリックします。[操作内容を理解しているのでワークフローをカスタマイズします (I know what I'm doing, let me customize my workflow)] を選択すると、障害が発生した時点からクラスタの設定を開始できます。
- 値の再入力のために戻ると、IP アドレス画面が空白になっている：IP アドレスを手動で追加します。[サーバの追加 (Add Server)] をクリックし、クラスタに含めるサーバをそれぞれ追加して、すべての IP アドレスをこのページで再入力します。
- インストーラ VM で DNS が正しく設定されていない (SSO エラー) ときに、サーバ到達可能性の問題が見られる：[SSO] フィールドを手動で編集して FQDN の代わりに IP アドレスを使用するか、DNS 設定をトラブルシューティングして修正します。
- 別のクラスタを作成するときに、Cisco HyperFlexバージョンに一致する Cisco UCS Manager バージョンが選択されていることを確認してください。一致するバージョンが選択されていない場合は、正しいバージョンを手動で入力します。

現在の互換性マトリックスについては、『[Release Notes for Cisco HX Data Platform](#)』のソフトウェアバージョンの表を参照してください。



## 第 6 章

# HyperFlex Data Platform でのライセンス設定

- [スマートライセンスと HyperFlex \(81 ページ\)](#)
- [ライセンスの遵守とフィーチャの機能 \(86 ページ\)](#)
- [接続環境でのライセンスの管理 \(87 ページ\)](#)
- [非接続環境でのライセンスの管理 \(93 ページ\)](#)

## スマートライセンスと HyperFlex

### 概要

シスコスマートソフトウェアライセンシング（スマートライセンス）はインテリジェントなソフトウェアライセンス管理システムで、組織全体でライセンスを調達、導入、管理するなど、時間のかかる手動のライセンスタスクを自動化します。ライセンスの所有権と使用状況が可視化されるので、何を所有し、どのくらい使用しているかを把握できます。

スマートライセンシングは、企業全体のライセンスプーリングを導入します。サーバベースのライセンスやスマートライセンスは、デバイスにノードロックされないため、企業が所有する互換性のあるデバイスでこれらを使用できます。仮想アカウントを使用して、会社のライセンスと製品インスタンスを論理エンティティ（事業単位、製品タイプ、ITグループなど）に体系化すると、仮想アカウント間でデバイスとライセンスを簡単に移転できるようになります。

スマートライセンシング機能は Cisco HyperFlex に統合されており、HX ストレージクラスタを作成するとすぐに自動的に有効になります。HX ストレージクラスタでライセンス消費の報告を開始するには、Cisco スマートアカウントを介して Cisco Smart Software Manager (SSM) に登録する必要があります。スマートアカウントは、会社全体のシスコソフトウェアライセンスと製品インスタンスに関する完全な可視性とアクセス制御を提供するクラウドベースのリポジトリです。登録は、1年間有効です。

登録すると、HyperFlex がスマートアカウントで識別され、ライセンス使用状況が Cisco Smart Software Manager または Smart Software Manager サテライトに報告されるようになります。登録後、HyperFlex はライセンス使用状況と現在のライセンスステータスを Cisco Smart Software

Manager または Smart Software Manager サテライトに報告します。詳細については、以下のライセンス ステータス セクションを参照してください。



- (注) これを機能させるには、すべての HyperFlex 管理 IP のポート 80 および 443 を `tools.cisco.com` に対して開く必要があります。

HX ストレージクラスタを登録した後、Cisco Smart Software Manager または Smart Software Manager サテライトに対して HyperFlex を特定するために使われる証明書が通信メッセージに署名します。HyperFlex は次の要求を自動的に送信します。

- 6 か月ごとの登録更新要求。自動登録更新が発生しない場合は、`stcli license renew id` コマンドを使用して手動で更新してください。
- スマートライセンスでは、30 日ごとの承認更新要求が必要とされます。自動承認更新が発生しない場合は、`stcli license renew auth` コマンドを使用して手動で更新してください。スマートライセンス承認を手動で更新する必要があるのは、更新しようとしたときに接続が使用不可である場合、または更新時刻が接続ウィンドウの範囲外である場合のみです。
- さらに、ライセンスの使用状況が変化するたびに、承認更新要求が Cisco Smart Software Manager または Smart Software Manager サテライトに送信されます。この承認は、90 日間有効です。90 日間承認を更新するよう HyperFlex が Cisco Smart Software Manager または Smart Software Manager サテライトに連絡しない場合は、HyperFlex によって消費されたライセンスが回収され、プールに戻されます。

### ライセンスステータス

登録ステータス	説明	ステータスの検証	システム機能
評価モード	スマートライセンスは有効になっていますが、HX ストレージクラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されておらず、90 日間の評価期間内です。	ステータスを検証するか、または評価期間の残り時間を確認するには、実行します。  #stcli license show all  Result: Mode = Eval & Remaining period (Number of Days:Hours:Minutes)	特性や機能には影響ありません。

登録ステータス	説明	ステータスの検証	システム機能
評価期限切れ	スマート ライセンシングは有効になっていますが、HX ストレージクラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていません。ライセンスは初期未確認状態です。コンプライアンス違反とは見なされません。	ステータスを検証するには、 <code>#stcli license show all</code> を実行します。  Result: Mode = Evaluation Expired	特性や機能には影響ありません。  <ul style="list-style-type: none"> <li>• Syslog メッセージを生成します。</li> <li>• HX Connect UI で評価期限切れアラームを生成します。</li> </ul>
適合	スマート ライセンシングが有効で、HX ストレージクラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されています。所有している数よりも少ないライセンスを消費しています。	—	—
HyperFlex リリース 5.0(2a) 以降は[コンプライアンス違反 (Out of Compliance) ]	-	-	フィーチャと機能への影響については、セクションを参照してください。 <a href="#">ライセンスの遵守とフィーチャの機能 (86 ページ)</a>

登録ステータス	説明	ステータスの検証	システム機能
HyperFlex リリース 5.0 (1b) 以前のコンプライアンス違反 (Out of Compliance) ]	<p>所有している数よりも多いライセンスを消費しています。</p> <p><b>重要</b> デバイスがコンプライアンス違反の場合に、シスコがお客様のネットワークに干渉したり、シャットダウンしたりすることはありません。</p> <ul style="list-style-type: none"> <li>初期登録状態でのコンプライアンス違反—スマートライセンスは有効で、HXストレージクラスタは Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、最初の登録後に十分なライセンスがありません。</li> <li>初期状態後または一定期間のインコンプライアンス状態後のコンプライアンス違反—スマートライセンスは有効で、HXストレージクラスタは Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、十分なライセンスがありません。</li> </ul>	<p>ステータスを検証するには、#stcli license show all を実行します。</p> <pre>Result: Mode = Out of Compliance</pre>	<p>特性や機能には影響ありません。</p> <ul style="list-style-type: none"> <li>Syslog メッセージを生成します。</li> <li>クラスタ レベルの HX Connect UI でコンプライアンス違反アラームを生成します。</li> </ul> <p>(注) コンプライアンス違反状態は知的財産 EULA を侵害するため、サポートを継続的に受けるにはライセンスの購入または更新が必要です。</p>



登録ステータス	説明	ステータスの検証	システム機能
認証が期限切れ	スマート ライセンシングが有効で、HX ストレージ クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、90 日間を超えて Cisco Smart Software Manager または Smart Software Manager サテライトと通信していません。	ステータスを検証するには、 <code>#stcli license show status</code> を実行します。  Result: Mode = Authorization Expired	特性や機能には影響ありません。  <ul style="list-style-type: none"> <li>• Syslog メッセージを生成します。</li> <li>• HX Connect 上でイベントやアラームは発生しません。</li> <li>• Cisco Smart Software Manager ポータルに、フラグと通知が表示されます。</li> </ul>
エクスポート制御フラグが「不可」に設定された	スマート ライセンシングが有効で、HX ストレージ クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、エクスポート制御を使用するように登録できません。	—	動作は、Cisco Smart Software Manager サーバによってほとんど制御されます。  (注) このステータスは、HX ストレージ クラスタに制限付き機能が含まれている場合にのみ該当します。
ID 証明書が期限切れ	スマート ライセンシングが有効で、HX ストレージ クラスタが Cisco Smart Software Manager または Smart Software Manager サテライトに登録されていますが、6 か月を超えて ID 証明書が更新されていません。ライセンスは後続未確認状態で、コンプライアンス違反と見なされます。	ステータスを確認するには、次を実行します。  <code>#stcli license show status</code>  Result: Mode: ID Certificate Expired  すべての条件をクリアしてコンプライアンス ステータスに戻すには、次のコマンドを実行します。  <code>#stcli license renew &lt;auth&gt;/&lt;id&gt;</code>	<ul style="list-style-type: none"> <li>• Syslog メッセージを生成します。</li> <li>• HX Connect 上でイベントやアラームは発生しません。</li> <li>• Cisco Smart Software Manager ポータルに、フラグと通知が表示されます。</li> </ul>

## ライセンスの遵守とフィーチャの機能

Cisco HXDP リリース 5.0(2a) 以降、有効な Cisco HyperFlex ソフトウェア ライセンスが必要です。ライセンスが期限切れまたは不十分な HX Connect ユーザーは、特定のフィーチャにアクセスできないか、フィーチャの機能が制限されます。フィーチャがロックされる前に、目立つカウントダウン バナーが表示され、ライセンス コンプライアンスの必要性和ライセンス更新 ページへのリンクをユーザーに警告します。

Cisco HXDP リリース 5.0 (2a) 以降、評価の終了時またはライセンス遵守日の後の猶予期間が終了した時点でライセンスが期限切れまたは不十分な HX コネクトユーザーは、期限切れになる前にアクセスできたすべての機能にアクセスできなくなります。現在の構成では限られた情報しか得られず、構成の変更はサポートされていません。

機能がロックされる前に、目立つライセンス遵守カウントダウンバナーが表示され、ライセンス遵守の必要性和ライセンス更新ページへのリンクをユーザーに警告します。

Cisco EULA を表示するには、[https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end\\_user\\_license\\_agreement.html](https://www.cisco.com/c/en/us/about/legal/cloud-and-software/end_user_license_agreement.html) を参照してください。

図 11: 30 日間の猶予期間を示すカウントダウンバナーの例



(注) 日数が減少して、フィーチャの機能がいつロックされるかが示されます。

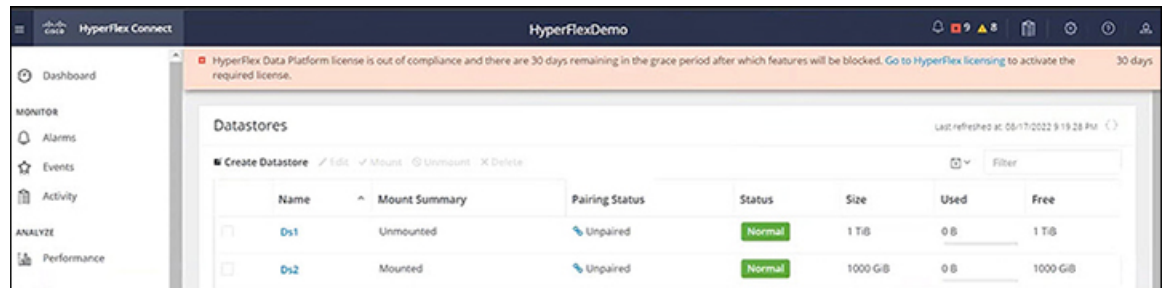
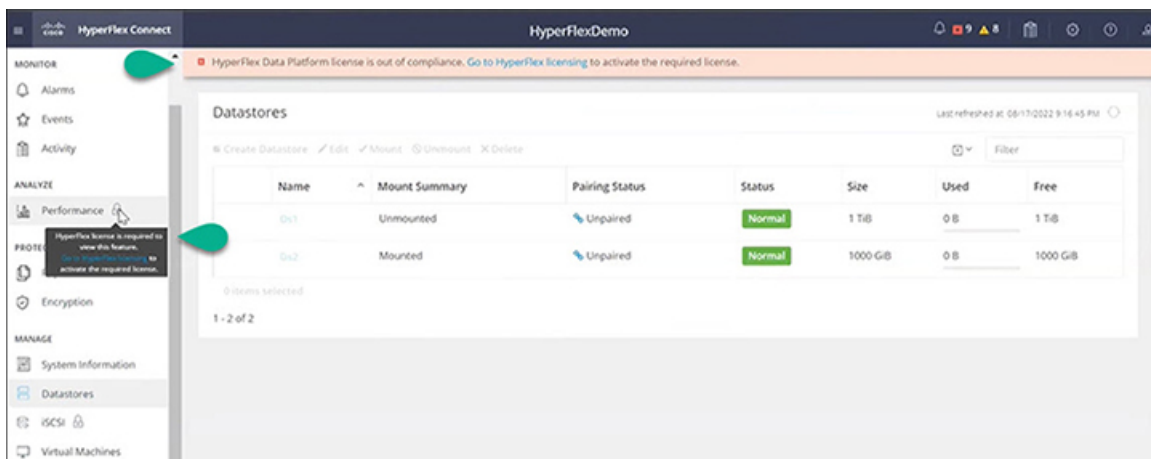


図 12: ライセンスの有効期限が切れたときに表示されるバナーとアイコン



1.	期限切れのライセンス バナー	HXDP ライセンスが遵守違反状態として示されます。「HyperFlex ライセンスに移動」リンクからライセンス更新ページが開きます。
2.	フィーチャのロックとホバーテキスト	特定のフィーチャがロックされていることを示します。ロックにカーソルをホバーさせると、ライセンス遵守ノートが表示され、ライセンス更新ページへのリンクが表示されます。

## 接続環境でのライセンスの管理

接続環境でライセンスを管理するには、次の手順を実行します。

### スマート ライセンスにクラスタを登録する

スマート ライセンスは自動的に HX ストレージ クラスタに組み込まれ、デフォルトで有効になります。スマート ライセンスをインストールする必要はありません。HX ストレージ クラスタはスマート ライセンスに登録されず、90 日間の評価モードに入ります。90 日以内に、HX ストレージ クラスタを登録して機能をすべて使用できるようにする必要があります。



**注目** HyperFlex クラスタを Smart Software Manager サテライトに登録する前に、プロキシが設定されていないことを確認します。プロキシが設定されている場合は、クラスタを Smart Software Manager サテライトに登録する前にプロキシを削除してください。

#### はじめる前に

- スマート ライセンスは、Cisco HX リリース 2.5 で導入されました。クラスタで HX 4.0 リリース以降が実行されていることを確認することをお勧めします。

## HX Connect を通してスマート ソフトウェア ライセンスによりクラスタを登録する

- スマートライセンスの使用を開始する前に、Cisco スマートアカウントを持っている必要があります。ご注文時にスマートアカウントを作成（または選択）するか、ご注文時以外にスマートアカウントを作成して新規または既存のライセンスを追加して行うことができます。

スマートアカウントを作成するには、**[Cisco Software Central] > [スマート アカウントの申請 (Request a Smart Account)]**

(<https://webapps.cisco.com/software/company/smartaccounts/home?route=module/accountcreation>)  
を参照してください。

HX ストレージクラスタは、次のいずれかの方法で Cisco スマート ソフトウェア マネージャ (SSM) に登録できます。

## HX Connect を通してスマート ソフトウェア ライセンスによりクラスタを登録する

Cisco では、HX Connect を通してスマート ソフトウェア ライセンスを持つクラスターを登録することを推奨します。

### 始める前に

- 製品インスタンス登録トークンが必要です。トークンがない場合、Cisco スマート ソフトウェア マネージャでトークンを作成できます。製品インスタンス登録用のトークンを作成する方法の詳細については、[登録トークンの作成 \(90 ページ\)](#) を参照してください。

**ステップ 1** HX Connect にログインします。

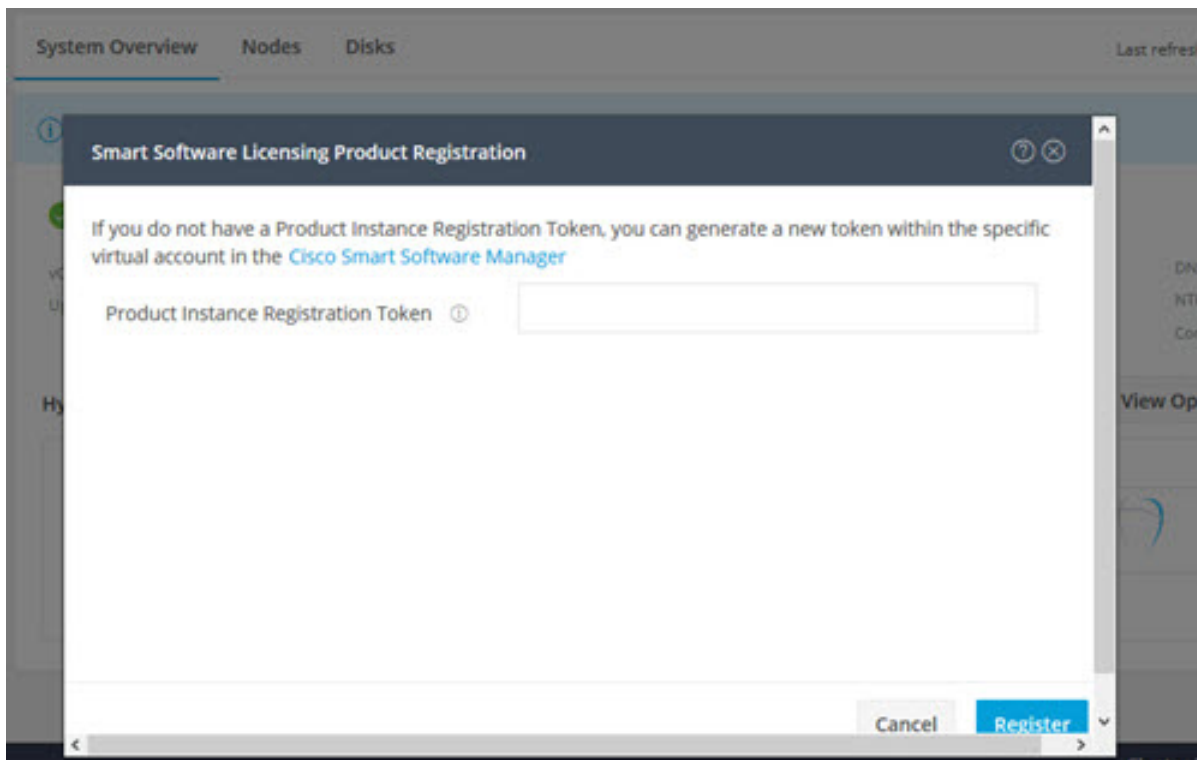
**ステップ 2** **[Dashboard (ダッシュボード)]** ページで、**[Cluster License not registered (クラスタ ライセンスが登録されていません)]** をクリックします。

The screenshot shows the HyperFlex Connect dashboard for a cluster named 'rk-4.2-source'. The dashboard includes a left-hand navigation menu with categories like MONITOR, ANALYZE, PROTECT, and MANAGE. The main content area displays several key metrics and warnings:

- OPERATIONAL STATUS:** Online. A warning icon indicates 'Cluster License not registered'.
- RESILIENCY HEALTH:** Warning. A message states 'No Node failure can be tolerated'.
- CAPACITY:** 1.8 TB total, with 27.4 GB used (1.5%) and 1.8 TB free.
- STORAGE OPTIMIZATION:** A note indicates that optimization ratios will be calculated once sufficient information is gathered.
- NODES:** 1 VMWARE VIRTUAL PLATFORM Converged.
- VIRTUAL MACHINES:** 0 VMs. Status indicators show 0 Powered On, 0 Suspended, and 0 Powered Off.
- Performance Graphs:** IOPS Last 1 hour and Throughput (Mbps) Last 1 hour are shown with line graphs and summary statistics.

または、**[System Information (システム情報)]** ページの **[Register Now (今すぐ登録)]** リンクをクリックして登録を行うことができます。

ステップ 3 [Smart Software Licensing Product Registration (スマートソフトウェアライセンス製品登録)] ダイアログボックスで、[Product Instance Registration Token (製品インスタンス登録トークン)] フィールドに登録トークンを入力します。



製品インスタンス登録用のトークンを作成する方法の詳細については、[登録トークンの作成 \(90ページ\)](#)を参照してください。

ステップ 4 [Register] をクリックします。

登録に成功すると、[System Information (システム情報)] ページにライセンスの種類とライセンスの状態が表示されます。

- **ライセンス タイプ** : 評価、Edge、標準、またはエンタープライズを HX ストレージクラスタ ライセンス タイプとして表示します。
- **ライセンス ステータス** : HX ストレージクラスタ ライセンス ステータスとして次のいずれかを表示します。
  - コンプライアンス
  - ライセンスの期限が <n> 日後に切れます。クラスタが登録されていません - 今すぐ登録します。(このステータスは評価タイプライセンスの場合にのみ表示されます。)
  - ライセンスの期限が切れています。クラスタが登録されていません - 今すぐ登録します。(このステータスは評価タイプライセンスの場合にのみ表示されます。)
  - コンプライアンス違反 - ライセンスが不十分です

- 認証の有効期限切れ：HX が Cisco Smart Software Manager および Smart Software Manager サテライトと 90日 以上通信できない場合、このステータスが表示されます。

## 登録トークンの作成

登録トークンを使用して、製品にスマートライセンスを登録し、消費します。製品を登録し、製品インスタンスを特定のバーチャルアカウントに追加するには、トークンを生成する必要があります。

**ステップ 1** 使用しているリリースに応じて、ソフトウェア マネージャにログインします。

オプション	説明
Cisco Smart Software Manager	<b>Cisco Software Central</b> ( <a href="https://software.cisco.com/">https://software.cisco.com/</a> ) にナビゲートし、スマートアカウントにログインします。[ライセンス (License)] ペインで、[スマートソフトウェアライセンシング (Smart Software Licensing)] をクリックします。[インベントリ (Inventory)] をクリックします。
Smart Software Manager サテライト	<a href="https://&lt;IP address of the satellite&gt;:8443">https://&lt;IP address of the satellite&gt;:8443</a> にアクセスし、管理者のクレデンシャルを使用してサテライトにログインします。

**ステップ 2** HX ストレージクラスタを登録するバーチャルアカウントから、[全般 (General)] をクリックして、[新しいトークン (New Token)] をクリックします。

**ステップ 3** [登録トークンの作成 (Create Registration Token)] ダイアログボックスで、次の操作を行い、[トークンの作成 (Create Token)] をクリックします。

- トークンの簡潔な [説明 (Description)] を追加します。
- トークンをアクティブにして他の製品で使用できるようにする日数を入力します。最大 = 365 日
- [このトークンに登録された製品の輸出規制された機能を許可する (Allow export-controlled functionality on the products registered with this token)] をオンにします。

**ステップ 4** [新しい ID トークン (New ID Token)] 行で、[アクション (Actions)] ドロップダウン リストをクリックし、[コピー (Copy)] をクリックします。

## コントローラ VM を介してスマートソフトウェアライセンスとともにクラスタを登録する

このセクションでは、スマートソフトウェアライセンスとともにクラスタを登録する別の方法を説明しています。

**ステップ 1** コントローラ VM にログインします。

**ステップ 2** HX ストレージクラスタがスマートライセンス モードになっていることを確認します。

```
# stcli license show status
```

フィードバックには、[スマートライセンスは有効です (Smart Licensing is ENABLED)]、[ステータス：未登録 (Status: UNREGISTERED)]、および 90 日の評価期間の残り時間 (日、時、分、秒) が表示されます。スマートライセンスの評価期間は、HX ストレージクラスタでライセンス機能を使用し始めたときに開始され、これを更新することはできません。評価期間が過ぎると、スマートエージェントが通知を送信します。

**ステップ 3** HX ストレージクラスタを登録します。ここで *idtoken-string* は Cisco Smart Software Manager またはスマートソフトウェアマネージャ サテライトからの新しい ID トークンです。

```
# stcli license register --idtoken idtoken-string
```

**ステップ 4** HX ストレージクラスタが登録されていることを確認します。

```
# stcli license show summary
```

別の方法として、[Cisco Smart Software Manager] > [インベントリ (Inventory)] > [製品インスタンス (Product Instances)] でも、HX ストレージクラスタが登録されていることを確認できます。

例：

```
root@SpringpathController80IWIHJOKW:~# stcli license show summary
```

```
Smart Licensing is ENABLED
```

```
Registration:
```

```
Status: REGISTERED
Smart Account: Corp X HyperFlex License
Virtual Account: west-region
Last Renewal Attempt: None
Next Renewal Attempt: Aug 1 17:47:06 2017 PDT
```

```
License Authorization:
```

```
Status: AUTHORIZED
Last Communication Attempt: SUCCEEDED
Next Communication Attempt: Mar 4 16:47:11 2017 PST
```

```
License Usage:
```

```
License                               Entitlement Tag
Count Status
```

```
-----
Cisco Vendor String XYZ
regid.2016-11.com.cisco.HX-SP-DP-S001,1.0_1c06ca12-18f2-47bd-bcea-518ab1fd4520 3      InCompliance
```

## スマートライセンスからクラスタを登録解除する

ライセンスを解除して別の HX ストレージクラスタ用にプールに戻すか、または Cisco Smart Software Manager 登録を削除する (たとえばクラスタをデコミッションする) 場合には、HX ストレージクラスタを登録解除します。HX ストレージクラスタを登録解除すると、評価期間が残っていれば HyperFlex は評価モードで実行されます。そうでない場合、HyperFlex は評価

の有効期限切れの状態になります。期限切れの評価状態にあるクラスタを登録解除しても、クラスタの実稼働データには影響しません。

スマートエージェントは、ライセンスクラウドにアクセスして自身を登録解除します。プラットフォーム上のすべてのスマートライセンス資格と証明書が削除されます。信頼されているストアのすべての証明書と登録情報が削除されます。スマートエージェントは、登録解除のためにシスコと通信できない場合でも、非登録状態になることができます。スマートライセンスを再び使用する必要が生じた場合には、HXストレージクラスタを再登録してください。[コントローラ VM を介してスマートソフトウェアライセンスとともにクラスタを登録する \(90 ページ\)](#) を参照してください。

#### 始める前に

- 次のコマンドを使用して、HXストレージクラスタがスマートライセンスに登録されていることを確認します。

```
# stcli license show status
```

**ステップ 1** コントローラ VM にログインします。

**ステップ 2** スマートライセンスから HX ストレージクラスタを登録解除します。

```
# stcli license deregister
```

**ステップ 3** HX ストレージクラスタが登録解除されたことを確認します。

```
# stcli license show summary
```

## スマートライセンス承認の更新

#### 始める前に

- 次のコマンドを使用して、HXストレージクラスタがスマートライセンスに登録されていることを確認します。

```
# stcli license show status
```

**ステップ 1** コントローラ VM にログインします。

**ステップ 2** 次のコマンドを使用してスマートライセンス承認を更新します。

```
# stcli license renew id
```

```
# stcli license renew auth
```

**ステップ 3** HX ストレージクラスタが更新され、承認されていることを確認します。

```
# stcli license show summary
```



# 非接続環境でのライセンスの管理

非接続環境でライセンサーを管理するには、次の手順を実行します。

## スマート ライセンスと Smart Software Manager サテライト

インターネット接続を使用してインストール ベースを管理することが許可されていない場合は、Smart Software Manager サテライトをオンプレミスでインストールし、Cisco Smart Software Manager のサブセットを使用してライセンスをローカルで管理できます。[Smart Software Manager サテライトのダウンロード](#)。

HyperFlex 用に Smart Software Manager サテライトを設定するには、HX Data Platform CLI から次のコマンドを実行します。

```
stcli services sch set --portal-url http://<satellite-host>/Transportgateway/services/  
DeviceRequestHandler --email <user-email-address>
```

Smart Software Manager サテライトが Cisco Smart Software Manager に登録されて稼働するようになったら、30 日ごとに Cisco Smart Software Manager と同期する必要があります。同期するには次の 2 つのオプションがあります。

- ネットワーク接続時に行うオンデマンドまたはスケジュール済み同期。
- 手動による同期。ライセンス ファイルをダウンロードした後、アップロードします。



(注) HX クラスタに Smart Satellite Server が構成されている場合、トークンは Smart Satellite Server の UI で生成される必要があるため、スマートポータルスマートライセンス登録では生成されなくなります。

## 特定のライセンス予約および HyperFlex

シスコ固有ライセンスの予約 (SLR) は、ユーザが切断モードでデバイスを使用できるようにする新しいソフトウェアライセンス管理システムです。特に、外部ネットワーク接続 (airギャップ) のない環境向けです。SLR には次のような追加の利点もあります。

- 時間のかかるライセンス タスクを自動化する
- ライセンスのステータスとソフトウェアの使用状況の傾向を追跡できます。
- コアの購入、管理、およびレポート機能をシンプル化

SLR により、顧客は仮想アカウントからライセンスを予約し、デバイス UDI に関連付けることができます。その後、これらのライセンスを使用してデバイスを切断モードで使用できます。また、お客様は、Cisco Smart Software Manager (CSSM) またはスマートソフトウェア サテ

ライト (オンサイト コレクタ) のいずれかと継続的に通信することなく、正常に動作させることができます。

### HyperFlex SLR 対応 PID

次の HyperFlex PID のみが SLR モードで使用できます。

表 4: 非接続およびエアギャップ展開用の *Cisco HyperFlex Data Platform (HXDP)* ソフトウェア SKU

HXDP SKU	説明
特定ライセンス登録	
HXDP-S-SLR	Cisco HyperFlex Data Platform 標準エディション 特定ライセンス登録サブスクリプション
HXDP-P-SLR	Cisco HyperFlex Data Platform エンタープライズ エディション特定ライセンス登録サブスクリプション
HXDP-E-SLR	Cisco HyperFlex Data Platform エッジエディション 特定ライセンス登録サブスクリプション

## 特定のライセンス予約 (SLR) ライセンスのインストール

この手順では、SLR ライセンスをインストールする方法、SLR ライセンスを返却する方法 (CSSM で再利用する場合)、または SLR ライセンス要求をキャンセルする方法について説明します。

SLR のインストールプロセスは、通常のスマートライセンスのインストールプロセスと非常によく似ています。クラスタとスマートアカウントの間に通信がないため、手動プロセスを使用して、HTTP 接続で以前に存在していたのと同じ会話を行なう必要があります。

これらの会話は、要求コードが生成された場合に、Cisco ハードウェア クラスタから始まります。要求コードには、いくつかの基本的なクラスタ識別情報が含まれています。要求は、Cisco ポータルでスマートアカウントに転送され、要求コードに基づいて承認コードを要求します。Cisco がライセンス ID と権限付与情報の両方を含む承認コードを取得すると、承認コードがクラスタに戻され、インストールを開始できます。インストールが完了すると、ライセンスはクラスタで完全にアクティブ化されます。

Enable/Disable コマンドは、予約モードにするためのものです。これは、現在の登録機能のデフォルトモードです。コマンド内のすべての予約を設定するには、予約モードを明示的に有効にする必要があります。すでに CSSM に登録されているライセンスがある場合は、そのライセンスを再登録して、再利用できるようにする必要があります。CSSM から承認コードを取得したら、`reservation install` コマンドを使用して予約コードをインストールできます。ある時点で、クラスタを破棄するか、またはライセンスを再度 CSSM に戻して再利用できるようにする場合は、`reservation return` コマンドを使用して、再度登録できる返還コードを生成できます。

次の手順では、SLR ライセンスをインストール、返却、キャンセルする方法について説明します。

**ステップ 1** HX ノードで `stcli license reservation enable` コマンドを入力して、予約モードを有効にします。

このコマンドを入力すると、設定モードが予約モードに切り替わります。ライセンスステータスは変更されません。

次の画面の左側には、通常の登録で一般的なクラスタのステータスが表示されます。予約モードでは、そのステータスの違いを確認できます。一般的なデバイスの場合、予約ステータスを確認すると、登録済みとして表示されます。ライセンス認証ステータスが承認されます。個々にライセンスがある場合は、どのライセンスが準拠しているかがわかります。

右側には、システムが未登録の状態で、評価ライセンスを使用していることが表示されます。

```

root@SpringpathControllerGVSTXU9951:~# stcli license show all
Smart Licensing Status
*****
Smart Licensing is ENABLED

Registration:
Status: REGISTERED
Smart Account: BU Production Test
Virtual Account: HXDP-Lic-Production-Test
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Jun 14 15:49:41 2017 PDT
Last Renewal Attempt: SUCCEEDED on Jun 14 15:49:41 2017 PDT
Next Renewal Attempt: Dec 11 14:49:41 2017 PST
Registration Expires: Jun 14 15:43:40 2018 PDT

License Authorization:
Status: AUTHORIZED on Jun 14 15:49:48 2017 PDT
Last Communication Attempt: SUCCEEDED on Jun 14 15:49:48 2017 PDT
Next Communication Attempt: Jul 14 15:49:48 2017 PDT
Communication Deadline: Sep 12 15:43:48 2017 PDT

Evaluation Period:
Evaluation Mode: Not In Use
Evaluation Period Remaining: 89 days, 12 hr, 40 min, 5 sec

License Usage
*****
License Authorization Status: AUTHORIZED as of Jun 14 15:49:48 2017 PDT
Cisco SP HyperFlex HX Data Platform SW v2.0 (regid.2016-11.com.cisco.HX-SP-OP-5001.1.0_1c06)
Description: Cisco SP HyperFlex HX Data Platform SW v2.0
Count: 3
Version: 3.0
Status: InCompliance

Product Information
*****
UDI: PID:HX240C-M45X,SN:9140586151354678828,VID: 5510173717264294049

Agent Version
*****
Smart Agent for Licensing: 1.3.5

```

- Login to control VM console
- stcli license reservation enable

```

root@SpringpathController2SAPEP8VJ9:~# stcli license reservation enable
root@SpringpathController2SAPEP8VJ9:~# stcli license show status
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
Status: UNREGISTERED
Export-Controlled Functionality: Not Allowed

License Authorization:
Status: EVAL MODE
Evaluation Period Remaining: 89 days, 23 hr, 54 min, 59 sec
Last Communication Attempt: NONE

License Conversion:
Automatic Conversion Enabled: true
Status: NOT STARTED

Utility:
Status: DISABLED

Transport:
Type: TransportCallHome

```

**ステップ 2** `stcli license reservation request` コマンドを入力して、予約要求を作成します。

ライセンス要求コードは、次の画面の青色のボックスに表示されます。

```

root@SpringpathController2SAPEP8VJ9:~# stcli license reservation request
CB-PHX240C-M4SX,S1743837435069904050,V7822371211685355448-B6jnU5MNT-D4

root@SpringpathController2SAPEP8VJ9:~# stcli license show status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
Status: RESERVATION IN PROGRESS
Reservation process started on: Thu Aug 30 15:04:25 PDT 2018
Export-Controlled Functionality: Not Allowed

License Authorization:
Status: Evaluation Mode (84 days, 16 hr, 54 min, 14 sec remaining)

Utility:
Status: DISABLED

Transport:
Type: TransportCallHome
root@SpringpathController2SAPEP8VJ9:~# stcli license show reservation

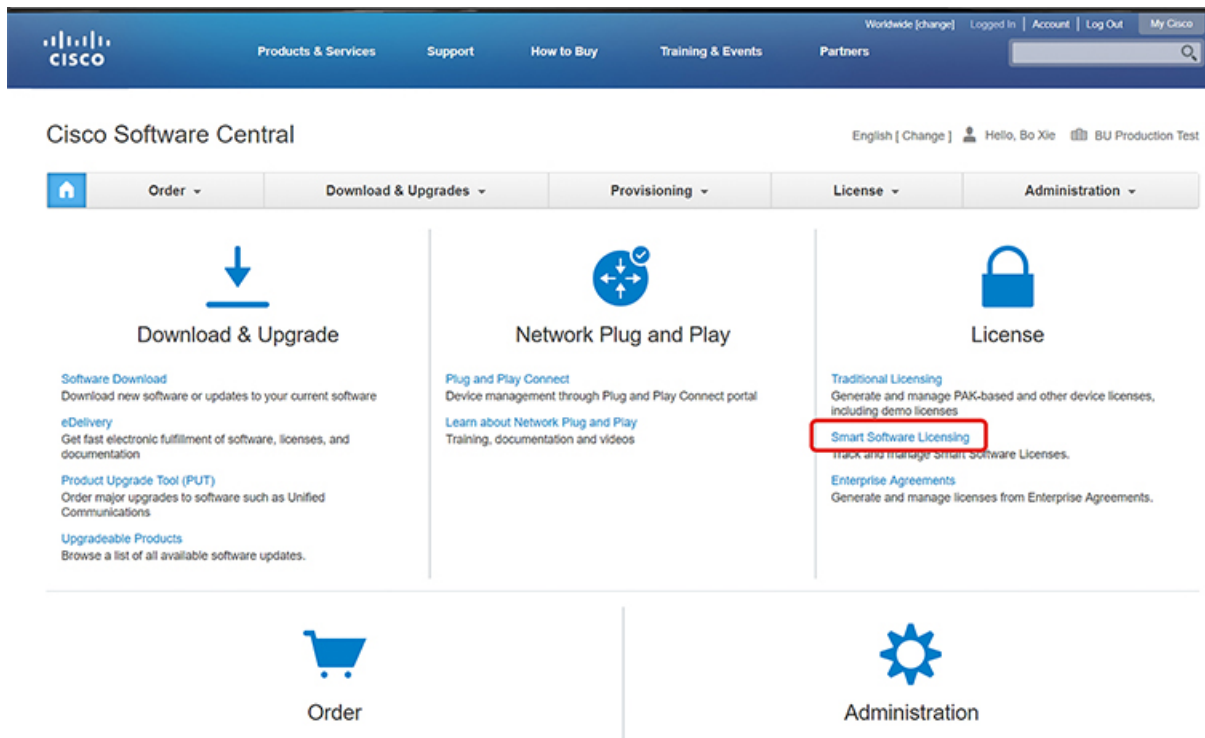
Smart Licensing is ENABLED
License Reservation is ENABLED
RESERVATION IN PROGRESS
Request Code:CE-PHX240C-M4SX,S1743837435069904050,V7822371211685355448-B6jnU5MNT-B3
Last Return Code:CABuDC-HKhr56-uRDagz-poweUt-16GFAX-tkF

```

予約要求を開始すると、登録ステータスが RESERVATION IN PROGRESS であることがわかります (赤いボックスに示されています)。要求コードがあれば、CSSM に移動して承認コードに変換できます。

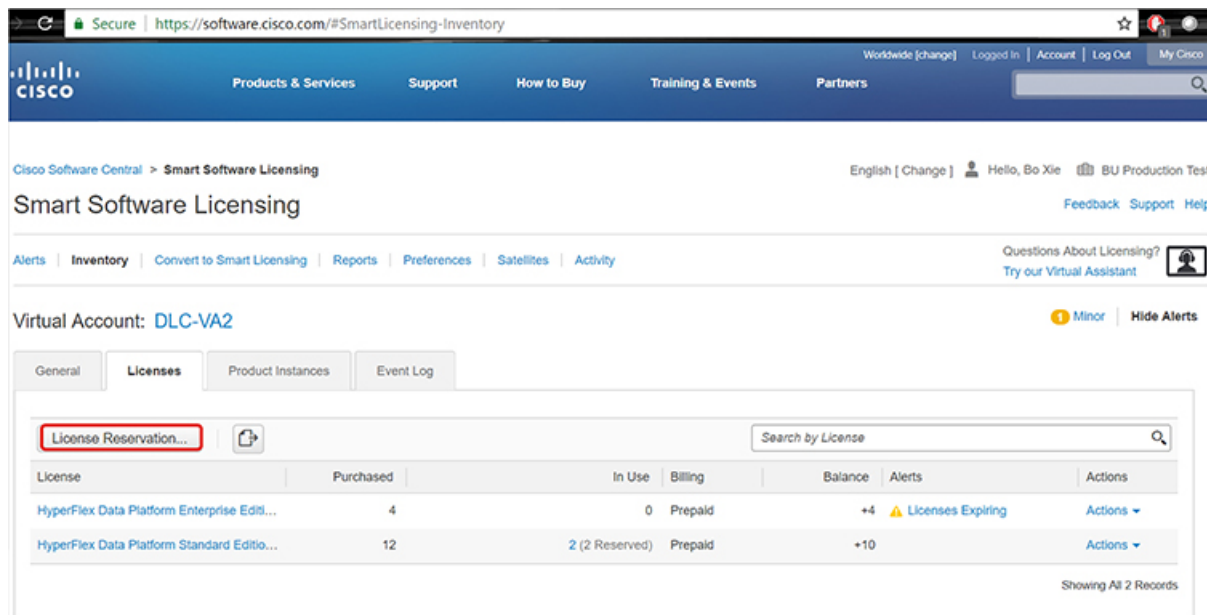
ステップ 3 CSSM (<https://software.cisco.com>) にログインします。

ステップ 4 [ライセンス (License)] セクションで、[スマート ソフトウェア ライセンシング (Smart Software Licensing)] リンクをクリックします。



これにより、[スマート ソフトウェア ライセンシング (Smart Software Licensing)] ページが表示されます。

**ステップ 5** [ライセンス (Licenses)] タブの下で、[ライセンス予約 (License Reservation)] をクリックします。



The screenshot shows the Cisco Smart Software Licensing interface. The page title is "Smart Software Licensing". The user is logged in as "Hello, Bo Xie" with a "BU Production Test" account. The "Licenses" tab is selected, and the "License Reservation..." link is highlighted with a red box. Below the tabs, there is a table of licenses with columns for License, Purchased, In Use, Billing, Balance, Alerts, and Actions.

License	Purchased	In Use	Billing	Balance	Alerts	Actions
HyperFlex Data Platform Enterprise Editi...	4	0	Prepaid	+4	⚠ Licenses Expiring	Actions ▾
HyperFlex Data Platform Standard Editio...	12	2 (2 Reserved)	Prepaid	+10		Actions ▾

Showing All 2 Records

**ステップ 6** 4 ステップの SLR プロセスを完了して、要求コードを入力し、[ライセンス (Licenses)] を選択し、承認コードを確認して確認し、承認コードをダウンロードします。

1. [要求コードを入力 (Enter the Request Code)]: クラスタで生成された予約要求コードを入力します。

Smart License Reservation

STEP 1 Enter Request Code | STEP 2 Select Licenses | STEP 3 Review and confirm | STEP 4 Authorization Code

You can reserve licenses for product instances that cannot connect to the Internet for security reasons. You will begin by generating a Reservation Request Code from the product instance. To learn how to generate this code, see the configuration guide for the product being licensed.

Once you have generated the code:

- 1) Enter the Reservation Request Code below
- 2) Select the licenses to be reserved
- 3) Generate a Reservation Authorization Code
- 4) Enter the Reservation Authorization Code on the product instance to activate the features

• Reservation Request Code:

CB-PHX240C-M4SX S1743837435069904050 V7822371211685355448-B6jnU5MNT-D4

Browse Upload

To learn how to enter this code, see the configuration guide for the product being licensed.

Cancel Next

2. [ライセンスを選択 (Select Licenses)]: この画面には、ライセンスの内容や、製品タイプ、UDI PID、UDI シリアル番号、UDI VID などの製品インスタンスの詳細が表示されます。提供された情報を確認し、チェックボックスをオンにして特定のライセンスを予約します。

Smart License Reservation

STEP 1 ✓ Enter Request Code

STEP 2 Select Licenses

STEP 3 Review and confirm

STEP 4 Authorization Code

**Product Instance Details**

Product Type: UCSHX

UDI PID: HX240C-M5SX

UDI Serial Number: 5317480753370517264

UDI VID: 5119877367947641800

**Licenses to Reserve**

In order to continue, ensure that you have a surplus of the licenses you want to reserve in the Virtual Account.

Reserve a HyperFlex Data Platform Standard Edition - Permanent License Reservation Only universal license

Reserve a specific license

License	Description	Expires	Available	Quantity To Reserve
Cisco SP HyperFlex HX Data Platform ...	Cisco SP HyperFlex HX Data Platform ...	multiple terms	44	3

Cancel Next

選択した特定のライセンスの予約について、予約する数量を入力します。

HyperFlex Data Platform Specific License Reservation

Start Date	Expires	Sub ID	Available	Quantity To Reserve
-	-	-	20	
2019-Mar-11	2019-Sep-07	-	10	3

Total: 3

Maximum: 30

If you don't specify quantities, the licenses with the longest time remaining before expiration will be selected by default.

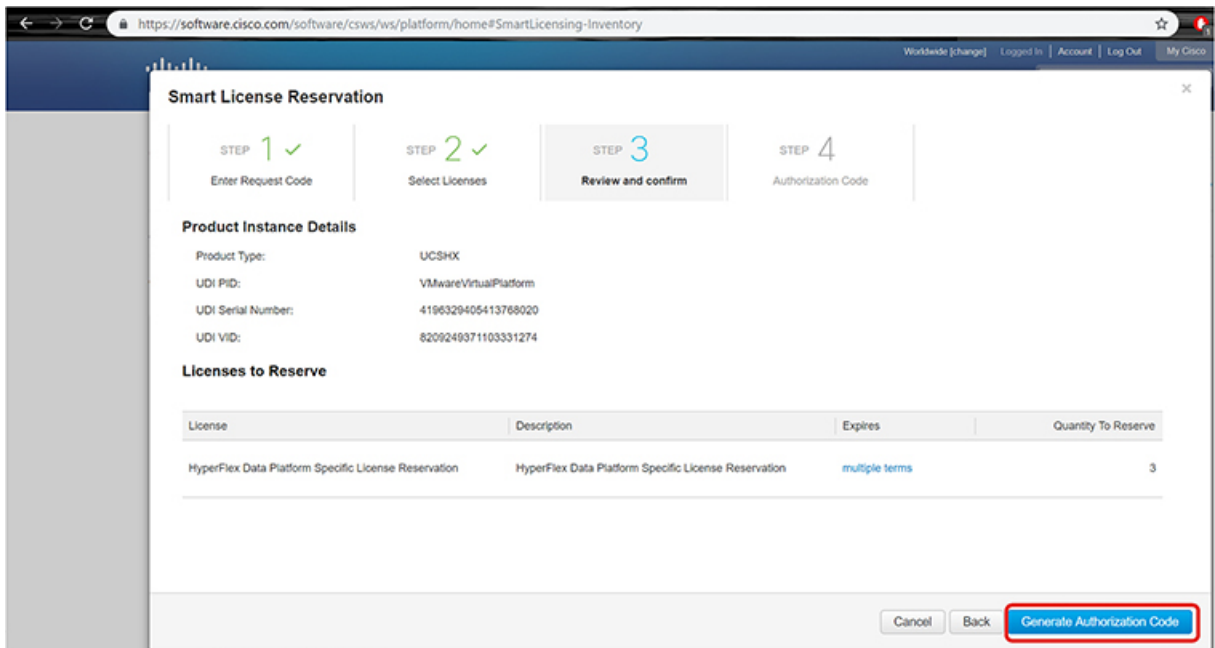
Show detail

Cancel OK

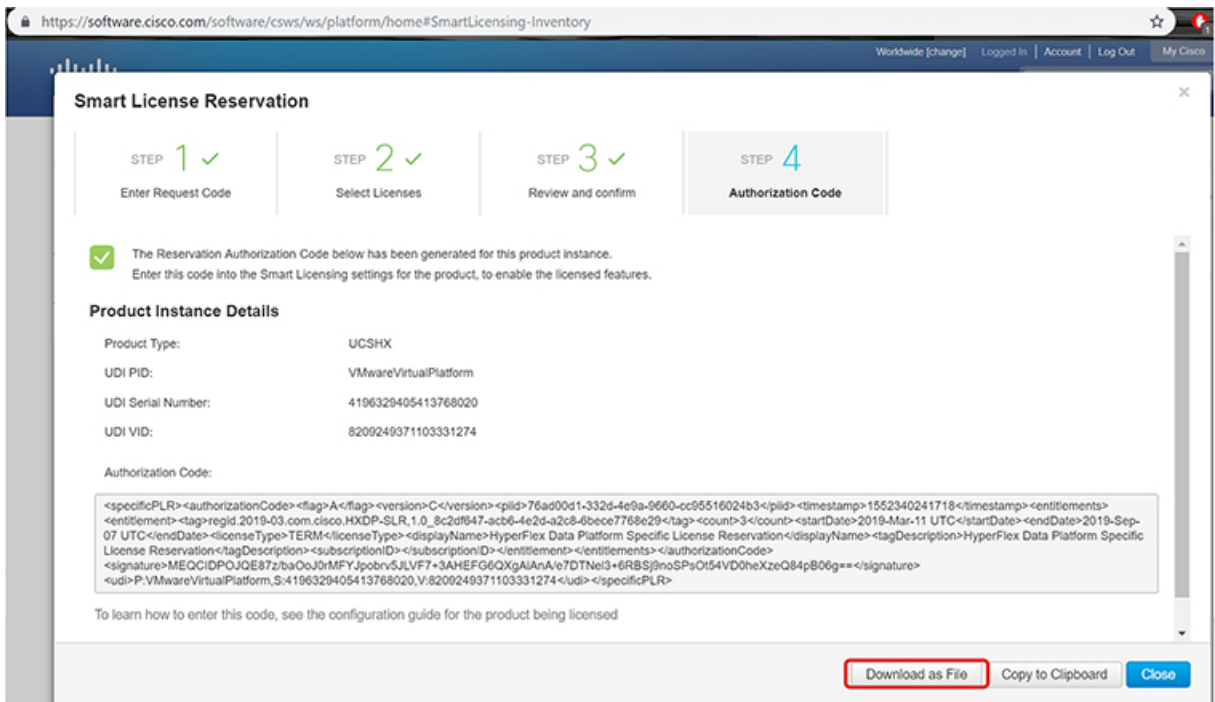
multiple terms

Cancel Next

3. [検証と確認 (Review and Confirm)]: 製品インスタンスの詳細と予約するライセンスを検証して確認し、画面の下部にある [承認コードの生成 (Generate Authorization Code)] ボタンをクリックします。

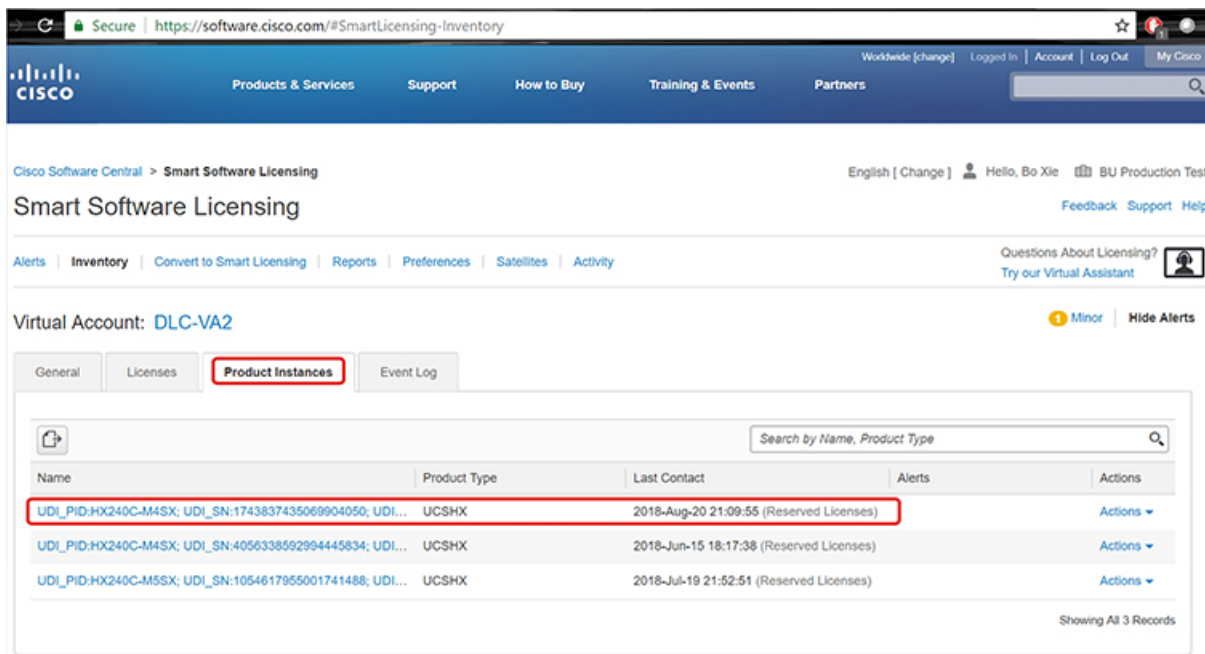


4. [承認コード (Authorization code)]: デバイス側で使用できる承認コードを表示し、画面下部の [ファイルとしてダウンロード (Download as File)] ボタンをクリックします。





ステップ7 [製品インスタンス (Product Instances)] タブに移動して、予約のクラスとシリアル番号に対応する行にある予約済みのライセンスを表示します。この行のリンクをクリックします(赤いボックスに表示されます)。



The screenshot shows the Cisco Smart Software Licensing interface. The 'Product Instances' tab is selected. A table displays the following data:

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:HX240C-M4SX; UDI_SN:1743837435069904050; UDI...	UCSHX	2018-Aug-20 21:09:55 (Reserved Licenses)		Actions
UDI_PID:HX240C-M4SX; UDI_SN:4056338592994445834; UDI...	UCSHX	2018-Jun-15 18:17:38 (Reserved Licenses)		Actions
UDI_PID:HX240C-M5SX; UDI_SN:1054617955001741488; UDI...	UCSHX	2018-Jul-19 21:52:51 (Reserved Licenses)		Actions

ライセンスの説明を示すダイアログ ボックスが表示されます。

UDI\_PID:HX240C-M5SX; UDI\_SN:930350977339931241; UDI\_VID:9128284972903402947;

**Overview** | Event Log

**Description**  
Cisco HyperFlex HX Data Platform Software License

**General**

Name: UDI\_PID:HX240C-M5SX; UDI\_SN:930350977339931241; UDI\_VID:9128284972903402947;  
 Product: Cisco HyperFlex HX Data Platform Software License  
 Host Identifier: -  
 MAC Address: -  
 PiD: HX240C-M5SX  
 Serial Number: 930350977339931241  
 Virtual Account: DLC-VA2  
 Registration Date: 2018-Aug-28 18:09:25  
 Last Contact: 2018-Aug-28 18:09:25 (Reserved Licenses) [Download Reservation Authorization Code](#)

**License Usage** These licenses are reserved on this product instance [Update reservation](#)

License	Billing	Expires	Required
HyperFlex Data Platform Standard Edition - Perman.	Prepaid	-	1

Showing all 1 Rows

Actions ▾

このページから、ライセンスの一般的な詳細を表示できます。特定のインスタンスで失われた場合に備えて、予約承認コード(上の赤色で強調表示)をダウンロードすることもできます。このページに戻って再度取得することもできます。

その後、[ライセンス (Licenses)] タブに戻り、現在のライセンスの使用状況を表示できます。

**ステップ 8** HX ノードに `stcli license reservation install <enter authorization code>` コマンドを入力して、続いて承認コードを入力します。

```
root@SpringpathControllerR8Kw22DM0U:~# stcli license reservation install --file ~/AuthorizationCode.txt
root@SpringpathControllerR8Kw22DM0U:~# stcli license show reservation

Smart Licensing is ENABLED
License Reservation is ENABLED
Specified License Reservations:
Status: SPECIFIC INSTALLED - SUCCEEDED on Mon Mar 11 10:49:05 PDT 2019
Export-Controlled Functionality: Allowed
Request Code: CB-PHX240C-M5SX,S5317480753370517264,V5119877367947641800-86jnu5MNT-86
Last Authorization Code: <specificPLR><authorizationCode><flag>A</flag><version>C</version><pid>50f8e2da-bbfb-4af4-bbb1-9beb6d6ab8ed</pid><timestamp>1552325956764</timestamp><entitlements><entitlement><tag>regid.2016-11.com.cisco.HX-SP-DP-S001,1.0_1c06ca12-18f2-47bd-bcea-518ab1fd4520</tag><count>3</count><startDate>2018-Oct-29 UTC</startDate><endDate>2019-Apr-27 UTC</endDate><licenseType>TERM</licenseType><displayName>Cisco SP HyperFlex HX Data Platform SW v2.0</displayName><tagDescription>Cisco SP HyperFlex HX Data Platform SW v2.0</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>MEQCIBaYGBvLzSLxmWzSHw6dU17Y2f1QoI71zqdJLtg9wd9A1AVvh2aShbY3oztP8vu21IuJ1AsZutJKA6JqhJLCbbi/g==</signature><udi>P:HX240C-M5SX,S:5317480753370517264,V:5119877367947641800</udi></specificPLR>
Last Confirmation Code: f40513fe
License Type: TERM
Description: Cisco SP HyperFlex HX Data Platform SW v2.0
Start Date: 2018-Oct-29 UTC
End Date: 2019-Apr-27 UTC
Count: 3
```

予約が成功すると、REGISTERED - SPECIFIC LICENSE RESERVATION として表示されるステータスを表示できます。認証では、UTHORIZED - RESERVED であることを示しています。

```

root@slcvm3:~# stcli license show all
Smart Licensing Status
=====
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Thu Feb 21 09:23:52 PST 2019
Last Renewal Attempt: None

License Authorization:
Status: AUTHORIZED - RESERVED on Thu Feb 21 09:23:52 PST 2019

Export Authorization Key:
Last request status:
Features Authorized:
None
Last return status:
Return Keys in process:
None

Utility:
Status: DISABLED

Transport:
Type: TransportCallHome

Evaluation Period:
Evaluation Mode: Not In Use
Evaluation Period Remaining: 87 days, 4 hr, 20 min, 45 sec

License Usage
=====
License Authorization Status:
Status: AUTHORIZED - RESERVED on Mon Mar 04 14:37:18 PST 2019
Last Communication Attempt: SUCCEEDED on Mar 4 14:37:18 2019 PST
Next Communication Attempt: NONE

HyperFlex Data Platform Enterprise Edition Subscription (regid.2017-12.com.cisco.HXDP-P001.1.0_454a6b54-8b33-45bd-9d11-b1567c4a741e)
Description:
Count: 3
Version: 0
Status: ReservedInCompliance
Export status: NO_RESTRICTION
Feature Name: null
Feature Description: null
Reservation:
Reservation Status: SPECIFIC INSTALLED
Total Reserved Count: 4

Product Information
=====
UDI: PID:HX240C-M5SX,SN:2432415792187588918,VID: 6984912678611873514

Agent Version
=====
Smart Agent for Licensing: 2.1.3

```

また、HX ノードで `stcli license show reservation` コマンドを入力して、SLR 予約を表示することもできます。この応答は、SLR がインストールされていることを示しています。

## 特定のライセンス予約 (SLR) ライセンスのキャンセル

この手順では、SLR ライセンス要求をキャンセルする方法について説明します。

- ステップ 1 (承認コードを取得するために CSSM に進む前に) 開始した予約要求をキャンセルするには、`stcli license reservation cancel` コマンドを使用します。
- ステップ 2 `stcli license show reservation` コマンドを使用して予約要求がキャンセルされたことを確認します。  
このコマンドを入力すると、ステータスが未登録に戻ったことを確認できます。

## 特定のライセンス予約 (SLR) ライセンスを返す

Virtual Account: [DLC-VA2](#) 1 Minor | Hide Alerts

General Licenses Product Instances Event Log

License Reservation... Search by License

License	Purchased	In Use	Billing	Balance	Alerts	Actions
HyperFlex Data Platform Enterprise Editio...	4	0	Prepaid	+4	Licenses Expiring	Actions
HyperFlex Data Platform Standard Editio...	12	2 (2 Reserved)	Prepaid	+10		Actions

Showing All 2 Records

## 特定のライセンス予約 (SLR) ライセンスを返す

クラスタのライセンスが完全にアクティブになったので、後でクラスタを破棄し、別のクラスタに再利用できるようにCSSMにライセンスを戻すことができます。次の手順では、SLRライセンスを返す方法について説明します。

**ステップ 1** `stcli license reservation return` コマンドを入力します。その後、CSSMで使用できる返還コードが生成されます。ステータスを確認すると、ライセンスは登録前と同様に、未登録の評価ライセンスに戻ります。

```

root@SpringpathController2SAPEP8VJ9:~# stcli license reservation return
CABeUN-BvP26i-yju9Pc-Tw59i1-cNTFmt-MRq
root@SpringpathController2SAPEP8VJ9:~# stcli license show reservation

Smart Licensing is ENABLED
License Reservation is ENABLED
  Last Return Code:CABeUN-BvP26i-yju9Pc-Tw59i1-cNTFmt-MRq
root@SpringpathController2SAPEP8VJ9:~# stcli license show status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 23 hr, 32 min, 3 sec
  Last Communication Attempt: SUCCEEDED on Aug 20 14:12:06 2018 PDT
  Next Communication Attempt: NONE

License Conversion:
  Automatic Conversion Enabled: true
  Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: TransportCallHome

```

ステップ2 [CSSM]に戻り、ライセンスをプールに戻します。[製品インスタンス (Product Instances)]タブに戻り、[アクション (Actions)]メニューを使用して、[削除 (Remove)]をクリックします。

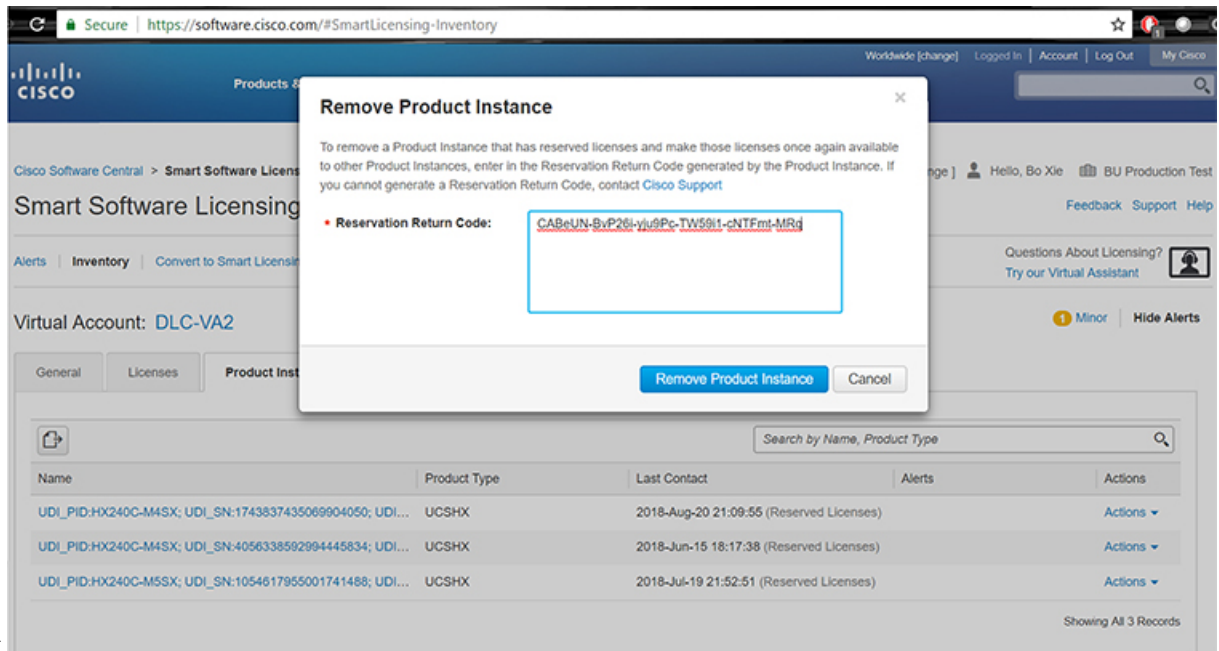
The screenshot shows the Cisco Smart Software Licensing (SSL) web interface. The 'Product Instances' tab is selected, displaying a table of reserved licenses. A red box highlights a row with the following details:

Name	Product Type	Last Contact	Alerts	Actions
UDI_PID:HX240C-M4SX; UDI_SN:1743837435069904050; UDI...	UCSHX	2018-Aug-20 21:09:55 (Reserved Licenses)		Actions
UDI_PID:HX240C-M4SX; UDI_SN:4056338592994445834; UDI...	UCSHX	2018-Jun-15 18:17:38 (Reserved Licenses)		
UDI_PID:HX240C-M5SX; UDI_SN:1054617955001741488; UDI...	UCSHX	2018-Jul-19 21:52:51 (Reserved Licenses)		

The 'Remove...' button in the 'Actions' column of the first row is highlighted with a red box.

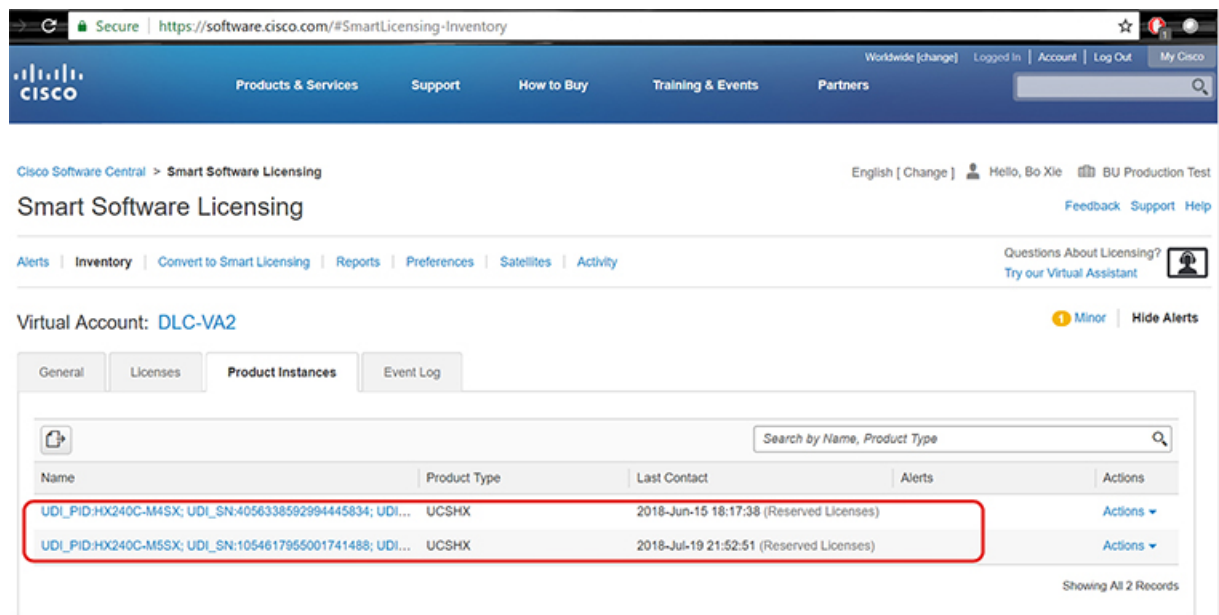
特定のライセンス予約 (SLR) ライセンスを返す

[製品インスタンスの削除 (Remove Product Instance)] ダイアログボックスが表示され、返還コードを入力できます。返還コードを入力し、[製品インスタンスの削除 (Remove Product Instance)] をクリックし



ます。

[製品インスタンス (Product Instances)] タブで、以前登録した SLR ライセンスが削除されたことを確認できます。3 個使用されるのに対して、使用中なのは 2 個だけです。この時点で、ライセンスが正常に返却されています。



## 特定のライセンスの予約のトラブルシューティング (SLR)

このセクションでは、特定のライセンス予約(SLR)を設定して使用する際に表示される可能性のある一般的なエラーメッセージについて説明します。また、該当する場合のトラブルシューティング方法に関する推奨事項も提供します。

表示される可能性のある 2 個の一般的なエラーメッセージは次のとおりです。

- 設定中に予約モードを有効にする前に予約要求コマンドを発行すると、「ライセンス予約が有効になっていません」というエラーメッセージが表示されます。または、要求しなかった操作をキャンセルするよう要求した場合は、「保留中の予約プロセスはありません」というメッセージが表示されます。次の図は、これらのエラーを示しています。

```

• Error you see from command line configuration output.
  • Making reservation request before reservation is enabled. Issue "stcli license reservation enable" first
root@SpringpathController2SAPEP8VJ9:~# stcli license reservation request
Internal error processing slRequestReservation: 'com.cisco.nesla.agent.SmartAgentException: License Reservation is not enabled.

  • Making reservation cancellation when there is no pending request to cancel
root@SpringpathController2SAPEP8VJ9:~# stcli license reservation cancel
Internal error processing slCancelReservation: 'com.cisco.nesla.agent.SmartAgentException: No reservation process is pending

```

- ライセンスステータスが変更されたランタイム時に、最初の登録が通信の送信エラーで失敗します。通常、このメッセージは、`show status` コマンドを入力したときに表示されません。ライブラリはエラーを上位に伝播しませんが、ログを使用して実際の理由を確認できます。

```

• Smart Licensing Agent only runs on the node with the mgmtip.
• Do "stcli license show status" or "stcli license show tech-support" for check the status
root@SpringpathController2SAPEP8VJ9:~# stcli license show status
Smart Licensing is ENABLED
Registration:
Status: UNREGISTERED - REGISTRATION FAILED
Initial Registration: FAILED
Failure Reason: Communication send error.
Export-Controlled Functionality: Not Allowed

License Authorization:
Status: EVAL MODE
Evaluation Period Remaining: 84 days, 17 hr, 48 min, 14 sec
Last Communication Attempt: NONE

License Conversion:
Automatic Conversion Enabled: true
Status: NOT STARTED

Utility:
Status: DISABLED

Transport:
Type: TransportCallHome

```

**ステップ 1** `grep` コマンドを発行し、SL カラムを表示して、ログに記録されているエラーおよびその他のすべての SL 関連メッセージを特定します。たとえば、次の図は、プロキシが使用されていること、およびプロキシ接続が失敗したことを示しています。これにより、ライセンスサーバのプロキシ設定が正しくないことが分かります。

- `grep` for "ERROR\|SL:" in `/var/log/springpath/stNodeMgr.log`

```

2018-08-30-21:10:37.833 [] [Thread-6067] DEBUG c.s.s.stNodeMgr.StNodeMgrImp1$ - SL: getRegInfo model: Set(HX240C-M4SX), serials: Set(FCH2025V301, FCH2025V3HP, FCH2025V3FK)
2018-08-30-21:10:37.895 [] [Thread-6067] ERROR event_msg_sender_log - exception
2018-08-30-21:10:37.895 [] [Thread-6067] ERROR event_msg_sender_log - GCH Internal Set HTTPS Proxy [proxy-1.cisco.com : 0]connection Failed, Please check it.
2018-08-30-21:10:37.896 [] [Thread-6067] ERROR event_msg_sender_log - proxy check exception
2018-08-30-21:10:37.896 [] [Thread-6067] ERROR send_client_msg_log - send sl data to URL [https://tools.cisco.com/its/service/oddce/services/DOCEService] failed:GCH Internal Set HTTPS Proxy [proxy-1.cisco.com : 0]connection Failed, Please check it.
2018-08-30-21:10:37.896 [] [Thread-6067] ERROR c.c.n.p.EmbeddedGCHCommunication - ResultEntity.getError_msg(): Cannot send out SL Message.GCH Internal Set HTTPS Proxy [proxy-1.cisco.com : 0]connection Failed, Please check it.
2018-08-30-21:10:37.901 [] [Thread-6067] ERROR c.c.n.a.impl.AsyncRequestProcessor - failed to send request / process response: SmartAgentMessageReg
2018-08-30-21:10:37.901 [] [Thread-6067] ERROR c.c.n.a.impl.AgentKeyStoreManager - saving to keystore failed
2018-08-30-21:10:37.901 [] [Thread-6067] ERROR c.c.n.a.impl.AgentKeyStoreManager - saving to keystore failed
2018-08-30-21:10:37.901 [] [Thread-6067] ERROR c.c.n.a.impl.AsyncRequestProcessor - scheduled RegisterRetryJob
2018-08-30-21:10:37.901 [] [Thread-6067] INFO c.s.s.stNodeMgr.StNodeMgrImp1$ - SL: --> received global notification...
2018-08-30-21:10:37.901 [] [Thread-6067] INFO c.s.s.stNodeMgr.StNodeMgrImp1$ - SL: notification type: NotifyRegisterFailed
2018-08-30-21:10:37.901 [] [Thread-6067] INFO c.s.s.stNodeMgr.StNodeMgrImp1$ - SL: enforce mode: NotApplicable
  
```

- "`stcli services sch show`" reveals the proxy server setting error

**ステップ 2** これを解決するには、`stcli services sch show` コマンドを使用して、プロキシのセットアップを確認し、エラーを修正してから、もう一度やり直してください。

**ステップ 3** また、「CISCO-SMART-LIC」で `grep` コマンドを発行して、移行中に生成されたスマートライセンスの `syslog` メッセージを確認することもできます。

- `grep "CISCO-SMART-LIC" /var/log/syslog`

```

Aug 20 23:30:42.373 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% Smart Agent is initialized
Aug 20 23:30:42.376 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% Smart Agent is enabled
Aug 20 23:30:42.551 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% Smart Agent is initialized
Aug 20 23:31:34.420 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% Smart Agent DeRegistration with CSSM failed: Agent is not registered.
Aug 20 23:32:23.359 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% CD-PHX240C-M4SX,S1743837435069904050,V7822371211685355448-B6jnuSMNT-BD License Reservation process must be completed with the 'license smart reservation install' command. Reservation started on PHX240C-M4SX,S1743837435069904050,V7822371211685355448
Aug 23 16:09:07.265 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% CE-PHX240C-M4SX,S1743837435069904050,V7822371211685355448-B6jnuSMNT-B3 License Reservation process must be completed with the 'license smart reservation install' command. Reservation started on PHX240C-M4SX,S1743837435069904050,V7822371211685355448
Aug 23 16:17:32.621 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% CAABYP-doDLDA-qs2XGw-uZwHeY-XXwZF7-7n23 License Reservation Authorization code installed
Aug 23 16:17:32.622 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% Usage of export controlled features is true
Aug 23 16:17:32.793 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% Smart Agent Registration with Cisco licensing cloud successful
Aug 23 16:17:32.800 SpringpathController2SAPEP8V39 root: %CISCO-SMART-LIC% All entitlements are authorized
  
```





## 第 7 章

# HyperFlex ハードウェア アクセラレーションカードの設定

この章では、Cisco HyperFlex ハードウェア アクセラレーションカードを設定する方法について説明します。

- [HyperFlex ハードウェア アクセラレーションカードの概要](#) (109 ページ)
- [Install HyperFlex Hardware Acceleration Cards](#) (110 ページ)
- [vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開](#) (111 ページ)
- [静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開](#) (113 ページ)
- [HyperFlex クラスタの設定と展開](#) (115 ページ)
- [HyperFlex ハードウェア アクセラレーションカードの取り付けの確認](#) (130 ページ)
- [HyperFlex ハードウェア アクセラレーションカードのトラブルシューティング](#) (131 ページ)
- [HyperFlex ハードウェア アクセラレーションカードに関する追加情報](#) (131 ページ)

## HyperFlex ハードウェア アクセラレーションカードの概要

この章では、HyperFlex ノード上の HyperFlex ハードウェア アクセラレーションカード (PID: HX-PCIE-OFFLOAD-1) のインストール、ポストインストール、およびトラブルシューティングの詳細と、初期クラスタの設定について説明します。これらのカードにより、ほとんどのストレージワークロードのパフォーマンスと圧縮効率が向上します。



(注) HyperFlex ハードウェア アクセラレーションカードをインストールおよび設定するには、HXDP-P エンタープライズ ライセンスが必要です。

PCIe スロットおよびライザーカード(およびその他の関連情報)の説明については、『[Cisco HX240c M5 HyperFlex ノード\(ハイブリッドおよびオールフラッシュモデル\)インストールガイド](#)』を参照してください。

# Install HyperFlex Hardware Acceleration Cards

## 始める前に

HyperFlex ハードウェア アクセラレーション カードの取り付けプロセスを開始する前に、次の点に注意してください。

- インストールは、新規展開でのみサポートされています。
- インストールは、次の HX 240 M5/M6 サーバーでのみサポートされています。
  - HXAF240C-M5SX Cisco HyperFlex HX240c M5 All Flash
  - HXAF240C-M6S Cisco HyperFlex HX240c M6 All Flash
  - HX240C-M5SX Cisco HyperFlex HX240c M5
  - HX240C-M6SX Cisco HyperFlex HX240c M6
  - HX240C-M5L HyperFlex HX240c M5 LFF
  - HX240C-M6S HyperFlex HX240c M6 LFF
- インストールは Hyper-v ではサポートされておらず、ストレッチ クラスタにもサポートされていません。
- HX クラスタ内のすべてのノードには、HyperFlex ハードウェア アクセラレーション カードが含まれている必要があります。



(注) 検証中にいずれかのノードにアクセラレーション カードが含まれていない場合は、インストーラが機能不全になり、エラー メッセージが表示されます。

- クラスタ タイプは、すべてフラッシュ/ハイブリッド ESXi である必要があります。
- インストールは、HX 240 M5/M6 サーバーでのみサポートされています。
- ハードウェア アクセラレーション カードは、Cisco HX データ複製では動作しません。
- HX リリース 4.0(2b) 以降、ストレッチ クラスタ構成のハードウェア オフロード オプションがサポートされています。

**ステップ 1** 新しい PCIe カードを取り付けます。これは、Cisco がサポートするインストールです。

**ステップ 2** HX インストーラを使用してクラスタを設定します。詳細については、以下を参照してください。

- [VSphere Web Client](#) を使用した [HX データ プラットフォーム インストーラ OVA](#) を展開します。

- HX クラスタの設定と展開

## vSphere Web Client を使用した HX Data Platform インストーラ OVA の展開

ESXi ホストに HX Data Platform をインストールするだけでなく、VMware Workstation、VMware Fusion または Virtual Box にも HX Data Platform インストーラを展開することができます。



- (注)
- vCenter に接続して OVA ファイルを展開し、IP アドレス プロパティを指定します。ESXi ホストから直接展開しても、値を正しく設定することはできません。
  - Cisco HX ストレージクラスタ内のノードとなる ESXi サーバに HX Data Platform インストーラを展開しないでください。

**ステップ 1** [ソフトウェアのダウンロード (Download Software)] で HX Data Platform インストーラ OVA ファイルを特定してダウンロードします。HX Data Platform ストレージクラスタに使用されるストレージ管理ネットワーク上のノードに、HX Data Platform インストーラをダウンロードします。

Example:  
Cisco-HX-Data-Platform-Installer-v5.0.1a-26363.ova

**ステップ 2** VMware ハイパーバイザを使用して HX Data Platform インストーラを展開し、HX Data Platform インストーラ仮想マシンを作成します。

- (注) 仮想ハードウェアリリース 10.0 以降をサポートする仮想化プラットフォームのリリースを使用してください。

vSphere はシステム要件です。vSphere シック クライアント、vSphere シンククライアント、または vSphere Web クライアントのいずれかを使用できます。HX Data Platform インストーラを展開するには、VMware Workstation、VMware Fusion、または VirtualBox を使用することもできます。

- vSphere、VirtualBox、Workstation、Fusion などの仮想マシンハイパーバイザを開きます。
- HX Data Platform インストーラを展開するノードを選択します。

**重要** vSphere Web Client を使用して HX インストーラ OVA を導入する際は、ユーザー クレデンシャルを必ず指定してください。

- vSphere シック クライアントを使用する—[インベントリ リスト (Inventory list)] > [ホスト (Host)] > [ファイル (File)] > [OVA を展開 (Deploy OVA)] を展開します
- vSphere Web クライアントを使用する—[vCenter インベントリ リスト (vCenter Inventory list)] > [ホスト (Hosts)] > [ホスト (Host)] > [OVA を展開 (Deploy OVA)] を展開します

**ステップ 3** HX Data Platform インストーラの場所を選択します。デフォルト値を使用し、適切なネットワークを選択します。

**ステップ 4** HX Data Platform インストーラ VM で使用する静的 IP アドレスを入力します。

- (注)
- ネットワークで DHCP が設定されている場合でも、静的 IP アドレスが必要です。HX Data Platform インストーラを実行し、HX Data Platform をインストールし、HX Data Platform ストレージクラスタを作成するには、静的 IP アドレスが必要です。
  - 新しい VM への IP アドレス割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、[静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開 \(63 ページ\)](#) の手順を実行して、静的 IP アドレスで HX Data Platform インストーラ VM をインストールします。インストーラ VM から DNS が到達可能である必要があります。

フィールド	説明
ホスト名	この VM のホスト名。 IP アドレスの逆引きを試みるには空白のままにします。
デフォルト ゲートウェイ	この VM のデフォルト ゲートウェイ アドレス。 DHCP を使用する場合は、空白のままにします。
DNS	この VM のドメイン ネーム サーバ (カンマ区切りリスト)。 DHCP を使用する場合は、空白のままにします。
IP アドレス	このインターフェイスの IP アドレス。 DHCP を使用する場合は、空白のままにします。
ネットマスク	このインターフェイスのネットマスクまたはプレフィックス。 DHCP を使用する場合は、空白のままにします。
Root パスワード	ルート ユーザー パスワード。 このフィールドは必須フィールドです。

**ステップ 5** [次へ (Next) ] をクリックします。リストされたオプションが正しいかどうかを確認し、[導入後に電源をオンにする (Power on after deployment) ] を選択します。

HX Data Platform インストーラを手動で電源オンにするには、仮想マシンのリストに移動し、インストーラ VM の電源をオンにします。

- (注) HX Data Platform インストーラ仮想マシンの推奨設定は、3 つの vCPU と 4 GB のメモリです。これらの設定を小さくすると、CPU の使用率が 100% になり、ホストのスパイクが発生する可能性があります。

**ステップ 6** [Finish] をクリックします。HX Data Platform インストーラ VM が vSphere インフラストラクチャに追加されるまで待ちます。

**ステップ 7** HX Data Platform インストーラ仮想マシンを開きます。

初期コンソール画面に、HX Data Platform インストーラ仮想マシンの IP アドレスが表示されます。

```
Data Platform Installer.
*****
You can start the installation by visiting
the following URL:
http://192.168.10.210
*****
Cisco-HX-Data-Platform-Installer login:
```

**ステップ 8** HX Data Platform インストーラにログインするための URL を使用します。

```
Example:
http://192.168.10.210
```

**ステップ 9** 自己署名証明書を受け入れます。

**ステップ 10** ユーザー名 **root** と、OVA 導入の一部として設定したパスワードを使用してログインします。

## 静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開

新しい VM への IP アドレスの割り当て用に、ハイパーバイザ ウィザードのデフォルト DHCP が設定されている場合は、以下の手順を使用して HX Data Platform インストーラを展開します。

**ステップ 1** HX Data Platform ストレージ クラスタに使用されるストレージ管理ネットワーク上のノードに、VMware OVF Tool 4.1 以降をインストールします。詳細については、「[OVF ツール ドキュメンテーション](#)」を参照してください。

**ステップ 2** VMware OVF がインストールされているノードの「ソフトウェアのダウンロード」から、HX Data Platform インストーラ OVA を見つけてダウンロードします。

**ステップ 3** ovftool コマンドを使用して、ダウンロードした HX Data Platform インストーラ OVA を展開します。次に例を示します。

```
root@server:/tmp/test_ova# ovftool --noSSLVerify --diskMode=thin
--acceptAllEulas=true --powerOn --skipManifestCheck --X:injectOvfEnv
--datastore=qa-048-ssd1 --name=rfsi_static_test1 --network='VM Network'
--prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1
--prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8
--prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco
--prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5
--prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36
--prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0
--prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
vi://root:password@esx_server
```

## 静的 IP アドレスを使用した HX Data Platform インストーラ OVA の展開

このコマンドにより、HX Data Platform インストーラが展開され、HX Data Platform インストーラ VM の電源が入り、指定された静的 IP アドレスが設定されます。以下は処理応答の例です。

```
Opening OVA source:
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
Opening VI target: vi://root@esx_server:443/
Deploying to VI: vi://root@esx_server:443/
Transfer Completed
Powering on VM: rfsi_static_test
Task Completed
Completed successfully
```

インストーラ VM から DNS が到達可能である必要があります。静的 IP アドレスを正常に設定するために必要なコマンド オプションは以下のとおりです。

コマンド	説明
powerOn	HX Data Platform インストーラ VM の展開後に電源を投入します。
X:injectOvfEnv	HX Data Platform インストーラ VM に静的 IP のプロパティを挿入します。
prop:hx.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1	適切なゲートウェイ IP アドレスを指定します。
prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8	適切な DNS IP アドレスを指定します。
prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco	適切なドメインを指定します。
prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5	適切な NTP IP アドレスを指定します。
prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36	適切なインストーラの静的 IP アドレスを指定します。
prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0	適切なネットマスク アドレスを指定します。
prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword	root ユーザー パスワードを指定します。
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova	HX Data Platform インストーラ OVA の送信元アドレス。
vi://root:password@esx_server	HX データプラットフォーム インストーラ VM がインストールされている宛先 ESX サーバ。適切な ESX サーバのルート ログイン クレデンシャルが含まれます。

# HyperFlex クラスタの設定と展開

## クレデンシャルの入力

[クレデンシャル (Credentials)] ページでは、必要な設定データを JSON ファイルからインポートすることも、必須フィールドに手動でデータを入力することもできます。



- (注) HyperFlex クラスタの初回インストールの場合は、シスコの担当者に連絡して工場出荷時のプレインストール JSON ファイルを入手してください。

クラスタを作成するには、JSON 設定ファイルから設定データをインポートするために次の操作を行います。

1. [ファイルの選択 (Select a file)] をクリックし、該当する JSON ファイルを選択して設定データを読み込みます。[構成を使用 (Use Configuration)] を選択します。
2. インポートした Cisco UCS Manager の値が異なる場合は、[Overwrite Imported Values] ダイアログボックスが表示されます。[Use Discovered Values] を選択します。

**ステップ 1** Web ブラウザで、HX Data Platform Installer VM の IP アドレスまたはノード名を入力します。[承認 (Accept)] または [続行 (Continue)] をクリックして SSL 証明書エラーをバイパスします。[HX Data Platform Installer] ログインページで、ログイン画面の右下隅にある [HX Data Platform Installer **Build ID**] を確認します。

**ステップ 2** ログイン ページで、次のクレデンシャルを入力します。

[ユーザ名 (Username)] : root

[パスワード (Password)] (デフォルト) : Cisco123

**注目** システムに同梱されているデフォルトのパスワード Cisco123 は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

**ステップ 3** [利用規約に同意します (I accept the terms and conditions)] チェック ボックスをオンにして、[ログイン (Login)] をクリックします。

**ステップ 4** [ワークフローの選択 (Select a Workflow)] ページで、[クラスタの作成 (Create Cluster)] ドロップダウン リストから [標準クラスタ (Standard Cluster)] を選択します。

**ステップ 5** [クレデンシャル (Credentials)] ページで、次の設定データを入力します。

フィールド	説明
UCS Manager のホスト名 (UCS Manager Host Name)	UCS Manager の FQDN または IP アドレスを入力します。 たとえば、10.193.211.120 とします。

フィールド	説明
UCS Manager のユーザー名 (UCS Manager User Name)	[administrative username] を入力します。
パスワード (Password)	管理者パスワードを入力します。

## vCenter クレデンシャル

フィールド	説明
vCenter サーバー (vCenter Server)	vCenter Server の FQDN または IP アドレスを入力します。 たとえば、 <i>10.193.211.120</i> とします。  (注) <ul style="list-style-type: none"> <li>• クラスタを動作可能にするには、その前に vCenter Server を準備する必要があります。</li> <li>• vCenter のアドレスとクレデンシャルには、vCenter に対するルートレベルの管理者権限が必要です。</li> <li>• ネストされた vCenter を構築する場合、vCenter Server の入力はおプションです。詳細については <a href="#">Nested vCenter TechNote</a> を参照してください。</li> </ul>
ユーザ名	管理者ユーザ名を入力します。 たとえば、 <i>administrator@vsphere.local</i> とします。
[管理パスワード (Admin Password) ]	管理者パスワードを入力します。

ステップ 6 [ハイパーバイザの設定 (Hypervisor Configuration) ] ページで、次の設定データを入力します。

## ハイパーバイザのクレデンシャル

フィールド	説明
管理者ユーザー名 (Admin User Name)	管理者ユーザ名を入力します。 工場出荷時のノードでのユーザ名は <b>root</b> です。



フィールド	説明
新しいパスワード (New Password)	<p><b>重要</b> ハイパーバイザの工場出荷時パスワードを変更する必要があります。</p> <p>次のガイドラインを使用してハイパーバイザの新しいパスワードを作成します。</p> <ul style="list-style-type: none"> <li>• 長さは 6 ~ 80 字である必要があります。</li> <li>• 1 個の大文字、1 個の小文字、1 個の数字、1 個の特殊文字が必要です。</li> <li>• パスワードが大文字で始まる場合、2 個の大文字が必要です。</li> <li>• パスワードが数字で終わる場合、2 桁の数字が必要です。</li> </ul>
新しいパスワードの確認 (Confirm New Password)	ハイパーバイザ用の新しいパスワードを再入力します。

**ステップ 7** [続行 (Continue)] をクリックして、HyperFlex サーバの関連付けを開始します。「[HyperFlex サーバの関連付け \(65 ページ\)](#)」を参照してください。

## HyperFlex サーバの関連付け

[サーバの選択 (Server Selection)] ページで、右側にある [構成 (Configuration)] ペインの [クレデンシヤル (Credentials)] に、使用されているクレデンシヤルの詳細なリストが表示されます。[サーバの選択 (Server Selection)] ページの [関連付けなし (Unassociated)] タブには、関連付けられていない HX サーバのリストが表示され、[関連付け済み (Associated)] タブには検出されたサーバのリストが表示されます。

フィールド	説明
ロケータ LED (Locator LED)	サーバーの検索をオンにします。
サーバー名 (Server Name)	サーバーに割り当てられた名前。
Status (ステータス)	<ul style="list-style-type: none"> <li>• アクセス不可—</li> </ul>
モデル (Model)	サーバー モデルが表示されます。
シリアル (Serial)	サーバーのシリアル番号を表示します。

フィールド	説明
関連付けのステータス (Assoc State)	<ul style="list-style-type: none"> <li>• 関連</li> <li>• 関連付けなし</li> </ul>
サービスプロファイル (Service Profile) (関連付けられたサーバーに対してのみ)	<p>サーバーに割り当てられているサービスプロファイル。</p> <p>(注) HyperFlex サービスプロファイルテンプレートの編集はお勧めしません。</p>
アクション (Actions)	<ul style="list-style-type: none"> <li>• <b>[KVM コンソールの起動 (Launch KVM Console) ]</b>: HX Data Platform から直接 KVM コンソールを起動するには、このオプションを選択します。</li> <li>• <b>[サーバの関連付け解除 (Disassociate Server) ]</b>: サーバからサービスプロファイルを削除するには、このオプションを選択します。</li> </ul>

### 始める前に

UCS Manager、vCenter、およびハイパーバイザ クレデンシャルの入力を完了していることを確認します。

**ステップ 1** [サーバ ポートの構成 (Configure Server Ports) ] をクリックして新しい HX ノードを検出します。[サーバ ポートの構成 (Configure Server Ports) ] ダイアログボックスに、サーバ ポートとして構成されるすべてのポートが一覧表示されます。[構成 (Configure) ] をクリックします。

(注) 一般的に、構成を始める前に、サーバ ポートは Cisco UCS Manager で構成されます。

**ステップ 2** HyperFlex クラスタに含める [ 関連付けなし (Unassociated) ] タブの下のサーバを選択します。

HX サーバがこのリストに表示されない場合は、[Cisco UCS Manager] をオンにして、検出されていることを確認します。

(注) 関連付けられていないサーバがない場合は、次のエラー メッセージが表示されます。

No unassociated servers found. Login to UCS Manager and ensure server ports are enabled.

**ステップ 3** [続行 (Continue) ] をクリックして、UCS Manager の構成を続けます。「[UCS Manager の設定 \(67 ページ\)](#)」を参照してください。

## UCS Manager の設定

[UCSM 構成 (UCSM Configuration)] ページでは、CIMC、iSCSi ストレージ、FC ストレージに関する VLAN、MAC プール、「hx-ext-mgmt」 IP プールを構成できます。

### 始める前に

HyperFlex クラスタにサーバを関連付けます。[HyperFlex サーバの関連付け \(65 ページ\)](#) を参照してください。

**ステップ 1** [VLAN 設定 (VLAN Configuration)] セクションで、次のフィールドに値を入力します。

(注) 次のそれぞれのネットワークに、別個のサブネットと VLAN を使用します。

フィールド	説明
<b>ハイパーバイザとHyperFlex管理用のVLAN</b>	
VLAN 名	hx-inband-mgmt
VLAN ID (Admin. VLAN ID)	デフォルト: 3091
<b>HyperFlexストレージトラフィック用のVLAN</b>	
VLAN 名	hx-storage-data
VLAN ID (Admin. VLAN ID)	デフォルト: 3092
<b>VM vMotion用のVLAN</b>	
VLAN 名	hx-vmotion
VLAN ID (Admin. VLAN ID)	デフォルト: 3093
<b>VMネットワーク用のVLAN</b>	
VLAN 名	vm-network
VLAN ID	デフォルト: 3094 ゲスト VLAN のカンマ区切りリスト。

**ステップ 2** [MAC プール (MAC Pool)] セクションの [MAC プールのプレフィックス (MAC Pool Prefix)] で、追加の 2 つの 16 進文字 (0 ~ F) を指定して MAC プールのプレフィックスを構成します。

(注) すべての UCS ドメインにわたり、他の MAC アドレス プールで使用とされていないプレフィックスを選択します。

Example:  
00:25:B5:A0:

ステップ 3 [CIMC の 'hx-ext-mgmt' IP プール ('hx-ext-mgmt' IP Pool for CIMC) ] セクションで、次のフィールドに値を入力します。

フィールド	説明
[IP Blocks]	各 HyperFlex サーバーの CIMC に割り当てられた管理 IP アドレスの範囲。IP アドレスは範囲として指定し、複数の IP ブロックをカンマ区切りのリストとして指定できます。クラスタ内のサーバごとに少なくとも 1 つの一意の IP があることを確認します。アウトオブバンドの使用を選択する場合、この範囲はファブリック インターコネクットの mgmt0 インターフェイスで使用されているものと同じ IP サブネットに属している必要があります。  たとえば、10.193.211.124-127, 10.193.211.158-163 などです。
[Subnet Mask]	上記の IP 範囲のサブネット マスクを指定します。  たとえば、255.255.0.0 とします。
[ゲートウェイ (Gateway) ]	ゲートウェイの IP アドレスを入力します。  たとえば、10.193.0.1 とします。

サーバー上の CIMC へのアクセスに使用される管理 IP アドレスは、次のいずれかです。

- **アウトオブバンド** : CIMC 管理トラフィックは、ファブリック インターコネクット上の制限帯域幅管理 インターフェイス mgmt0 を介してファブリック インターコネクットを通過します。このオプションは最も一般的に使用され、ファブリック インターコネクット管理 VLAN と同じ VLAN を共有します。
- **インバンド** : CIMC 管理トラフィックは、ファブリック インターコネクットのアップリンク ポートを通じてファブリック インターコネクットを通過します。この場合、管理トラフィックに使用できる帯域幅は、ファブリック インターコネクットのアップリンク帯域幅に相当します。インバンドオプションを使用している場合、Cisco HyperFlex インストーラは CIMC 管理通信専用の VLAN を作成します。このオプションは、Windows Server インストール ISO などの大きなファイルを OS インストール用の CIMC にマウントする必要がある場合に便利です。このオプションは、HyperFlex インストーラ VM でのみ使用でき、Intersight を介した展開には使用できません。

ステップ 4 CIMC 管理アクセスに使用する接続のタイプに基づいて、アウトオブバンドまたはインバンドを選択します。[インバンド (In-band) ] を選択した場合は、管理 VLAN の VLAN ID を指定します。シームレスな接続のために、アップストリーム スイッチに CIMC 管理 VLAN を作成してください。

ステップ 5 外部ストレージを追加する場合は、次のフィールドに値を入力して [iSCSI ストレージ (iSCSI Storage) ] を構成します。

フィールド	説明
[iSCSI ストレージの有効化 (Enable iSCSI Storage) ] チェックボックス	iSCSI ストレージを構成する場合、このチェックボックスをオンにします。
<b>VLAN A 名 (VLAN A Name)</b>	プライマリ ファブリック インターコネク ト (FI-A) で、iSCSI vNIC に関連付けられている VLAN の名前。
<b>VLAN A ID</b>	プライマリ ファブリック インターコネク ト (FI-A) で、iSCSI vNIC に関連付けられている VLAN の ID。
<b>VLAN B 名 (VLAN B Name)</b>	下位のファブリック インターコネク ト (FI-B) で、iSCSI vNIC に関連付けられている VLAN の名前。
<b>[VLAN B ID]</b>	下位のファブリック インターコネク ト (FI-A) で、iSCSI vNIC に関連付けられている VLAN の ID。

**ステップ 6** 外部ストレージを追加する場合は、次のフィールドに値を入力して [FC ストレージ (FC Storage) ] を構成します。

フィールド	説明
[FC ストレージの有効化 (Enable FC Storage) ] チェックボックス	FC ストレージを有効にするには、このチェックボックスをオンにします。
<b>WWxN プール</b>	WW ノード名と WW ポート名の両方を含む WWN プール。それぞれのファブリック インターコネク トに対し、WWPN および WWNN 用の WWxN プールが作成されます。
<b>VSAN A 名 (VSAN A Name)</b>	プライマリ ファブリック インターコネク ト (FI-A) の VSAN の名前。  デフォルト—hx-ext-storage-fc-a。
<b>VSAN A ID</b>	プライマリ ファブリック インターコネク ト (FI-A) のネットワークに割り当てられた一意の ID。  <b>注意</b> UCS または HyperFlex システムで現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。
<b>VSAN B 名</b>	下位のファブリック インターコネク ト (FI-B) の VSAN の名前。  デフォルト—hx-ext-storage-fc-b。

フィールド	説明
<b>VSAN B ID</b>	<p>下位のファブリック インターコネクト (FI-B) のネットワークに割り当てられた一意の ID。</p> <p><b>注意</b> UCS または HyperFlex システム で現在使用されている VSAN ID を入力しないでください。UCS ゾーン分割を使用するインストーラに既存の VSAN ID を入力すると、その VSAN ID の既存の環境でゾーン分割が無効になります。</p>

**ステップ 7** [詳細設定 (Advanced)] セクションで、次の操作を行います。

フィールド	説明
<b>UCS サーバー ファーム ウェアバージョン (UCS Server Firmware Version)</b>	<p>ドロップダウン リストから、HX サーバと関連付ける UCS サーバファームウェアバージョンを選択します。UCS ファームウェアバージョンは、UCSM バージョンと一致する必要があります。詳細については、最新の『<a href="#">Cisco HX Data Platform Release Notes</a>』を参照してください。</p> <p>たとえば、3.2(1d) とします。</p>
<b>HyperFlex クラスタ名</b>	<p>ユーザ定義の名前を指定します。HyperFlex クラスタ名は、特定のクラスタ内の HX サーバグループに適用されます。HyperFlex クラスタ名によりサーバプロファイルにラベルが追加され、クラスタを識別しやすくなります。</p>
<b>組織名</b>	<p>HyperFlex 環境を UCS ドメインの残りの部分から確実に分離できるような一意の組織名を指定します。</p>

**ステップ 8** [続行 (Continue)] をクリックして、ハイパーバイザの構成を続けます。「[ハイパーバイザの構成 \(71 ページ\)](#)」を参照してください。

## ハイパーバイザの構成



(注) [ハイパーバイザの構成 (Hypervisor Configuration)] ページの [構成 (Configuration)] ページで、VLAN、MAC プール、IP アドレス プールの情報を確認します。これらの VLAN ID は、環境によって変更されている可能性があります。デフォルトでは、HX Data Platform インストーラが VLAN を非ネイティブとして設定します。トランク構成を適切に適用することで、非ネイティブ VLAN に対応するアップストリーム スイッチを構成する必要があります。



注目 再インストールの場合、ESXi ネットワーキングが完了していれば、ハイパーバイザの構成をスキップできます。

### 始める前に

アウトオブバンド CIMC の VLAN、MAC プール、「hx-ext-mgmt」IP プールを構成します。外部ストレージを追加する場合は、iSCSI ストレージと FC ストレージを構成します。UCS サーバのファームウェア バージョンを選択し、HyperFlex クラスタの名前を割り当てます。UCS Manager の設定 (67 ページ) を参照してください。

**ステップ 1** [共通ハイパーバイザ設定の構成 (Configure Common Hypervisor Settings)] セクションで、次のフィールドに値を入力します。

フィールド	説明
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、255.255.0.0 とします。
[ゲートウェイ (Gateway)]	ゲートウェイの IP アドレス。 たとえば、10.193.0.1 とします。

フィールド	説明
[DNSサーバ (DNS Server(s)) ]	<p>DNS サーバの IP アドレス。</p> <p>(注)</p> <ul style="list-style-type: none"> <li>• DNS サーバを使用しない場合、HX Data Platform インストーラの <b>[クラスタの設定 (Cluster Configuration)]</b> ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。</li> <li>• 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。</li> </ul>

**ステップ 2** [ハイパーバイザ設定 (Hypervisor Settings) ] セクションで、[IP アドレスとホスト名を順番に選択 (Make IP Addresses and Hostnames Sequential) ] を選択し、連続的な IP アドレスにします。次のフィールドに入力します。

(注) ドラッグアンドドロップ操作を使用してサーバの順番を並び替えることができます。

フィールド	説明
名前 (Name)	サーバーに割り当てられた名前。
ロケータ LED (Locator LED)	サーバーの検索をオンにします。
シリアル (Serial)	サーバーのシリアル番号を表示します。
スタティック IP アドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。
ホスト名	ホスト名フィールドを空のままにしないでください。

**ステップ 3** [続行 (Continue) ] をクリックして、IP アドレスの構成を続けます。「[IP アドレスの設定 \(73 ページ\)](#)」を参照してください。



## IP アドレスの設定

### 始める前に

[ハイパーバイザ設定 (Hypervisor Configuration) ] ページでハイパーバイザの設定が完了していることを確認します。 [ハイパーバイザの構成 \(71 ページ\)](#) を参照してください。

**ステップ 1** [IP アドレス (IP Addresses) ] ページで、[IP アドレスを連続させる (Make IP Addresses Sequential) ] を選択し、連続的な IP アドレスにします。

**ステップ 2** ハイパーバイザ、ストレージコントローラ (管理) とハイパーバイザ、ストレージコントローラ (データ) 列の最初の行に IP アドレスを入力すると、HX Data Platform Installer により、残りのノードのノード情報が増分されて自動入力されます。ストレージクラスタ内のノードの最小数は 3 です。それより多くのノードがある場合は、[追加 (Add) ] ボタンを使用して、アドレス情報を指定します。

(注) コンピューティング専用ノードは、ストレージクラスタを作成してからでないと追加できません。

各 HX ノードについて、ハイパーバイザ、ストレージコントローラ、管理、データ IP アドレスを入力します。IP アドレスには、ネットワークがデータネットワークと管理ネットワークのどちらに属しているかを指定します。

フィールド	説明
管理ハイパーバイザ	ESXi ホストとストレージコントローラ間のハイパーバイザ管理ネットワーク接続を処理するスタティック IP アドレスを入力します。
管理ストレージコントローラ	ストレージコントローラ VM とストレージクラスタ間のストレージコントローラ VM 管理ネットワーク接続を処理する静的 IP アドレスを入力します。
Data Hypervisor	ESXi ホストとストレージコントローラ間のハイパーバイザデータ ネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージコントローラ	ストレージコントローラ VM とストレージクラスタの間のストレージコントローラ VM データ ネットワーク接続を処理するスタティック IP アドレスを入力します。

**ステップ 3** ここで指定する IP アドレスは、ストレージクラスタ内の 1 つのノードに適用されます。ノードが使用できなくなった場合は、該当する IP アドレスがストレージクラスタ内の別のノードに移動されます。すべてのノードには、これらの IP アドレスを受け入れるように構成されたポートが必要です。

次の IP アドレスを指定します。

フィールド	説明
管理クラスタ データの IP アドレス (Management Cluster Data IP Address)	HX データ プラットフォーム ストレージ クラスタ の 管理 ネットワーク IP アドレス を 入力 します。
データ クラスタ データ IP アドレス (Data Cluster Data IP Address)	HX Data Platform ストレージ クラスタ の データ ネットワーク の IP アドレス を 入力 します。
管理サブネットマスク	VLAN と vSwitch の サブネット 情報 を 入力 します。 管理 ネットワーク の 値 を 入力 します。たとえば、255.255.255.0 と 入力 します。
データサブネットマスク	データ ネットワーク の ネットワーク の 値 を 入力 します。たとえば、255.255.255.0 と 入力 します。
管理ゲートウェイ	管理 ネットワーク の ネットワーク の 値 を 入力 します。たとえば、10.193.0.1 と します。
データゲートウェイ	データ ネットワーク の ネットワーク の 値 を 入力 します。たとえば、10.193.0.1 と します。

ステップ 4 [続行] を クリック して HyperFlex クラスタ を 設定 します。「[HyperFlex クラスタ の 設定 \(74 ページ\)](#)」を 参照 してください。

## HyperFlex クラスタ の 設定

[クラスタ構成 (Cluster Configuration)] ページで、Cisco HX ストレージ クラスタ に関する 以下の フィールド に 値 を 入力 し、HyperFlex クラスタ の 導入 を 開始 します。

### 始める前に

[IP アドレス (IP Addresses)] ページで IP アドレス の 構成 が 完了 している こと を 確認 します。[IP アドレス の 設定 \(73 ページ\)](#) を 参照 してください。

ステップ 1 [Cisco HX クラスタ (Cisco HX Cluster)] セクションで、次のフィールドに値を入力します。

フィールド	説明
クラスタ名 (Cluster Name)	HX データ プラットフォーム ストレージ クラスタ の 名前 を 指定 します。

フィールド	説明
レプリケーション ファクタ (Replication Factor)	<p>ストレージクラスタ全体でのデータの冗長レプリカの数指定します。レプリケーションファクタを冗長レプリカ数 2 または 3 に設定します。</p> <ul style="list-style-type: none"> <li>ハイブリッドサーバ (SSD と HDD を含むサーバ) の場合、デフォルト値は 3 です。</li> <li>フラッシュ サーバー (SSD のみを含むサーバ) の場合は、2 または 3 を選択します。</li> <li>Hyperflex Edge を除くすべての環境で複製ファクタ 3 を強く推奨しています。複製ファクタ 2 では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。</li> </ul>

**ステップ 2** [コントローラ VM (Controller VM) ]セクションで、HyperFlex クラスタの管理者ユーザの新しいパスワードを作成します。

コントローラ VM には、デフォルトの管理者ユーザ名とパスワードが適用されます。VM は、コンバージドノードとコンピューティング専用ノードのすべてにインストールされます。

- 重要**
- コントローラ VM またはコントローラ VM のデータストアの名前を変更することはできません。
  - すべてのコントローラ VM に同じパスワードを使用します。異なるパスワードの使用はサポートされていません。
  - 1 つの大文字、1 つの小文字、1 つの数字、1 つの特殊文字を含む、10 文字以上の複雑なパスワードを指定してください。
  - コントローラ VM と、作成される HX クラスタには、ユーザ定義のパスワードを指定できません。パスワードに使用できる文字と形式に関する制限事項については、『Cisco HX Data Platform Management Guide』のセクション「Guidelines for HX Data Platform Special Characters」を参照してください。

**ステップ 3** [vCenter の設定 (vCenter Configuration) ]セクションで、次のフィールドに値を入力します。

フィールド	説明
vCenter データセンター名 (vCenter Datacenter Name)	Cisco HyperFlex クラスタの vCenter データセンターの名前を入力します。
vCenter クラスタ名 (vCenter Cluster Name)	vCenter クラスタ名を入力します。

**ステップ 4** [システム サービス (System Services) ]セクションで、次のフィールドに値を入力します。

DNS サーバー (DNS Server(s))	各 DNS サーバーの IP アドレスのカンマ区切りリスト。
NTP サーバー (NTP Server(s))	各 NTP サーバの IP アドレスのカンマ区切りリスト。  (注) すべてのホストが同じ NTP サーバを使用して、ストレージコントローラ VM と ESXi ホストで実行されているサービスの間でクロックを同期する必要があります。
DNS ドメイン名 (DNS Domain Name)	DNS FQDN または IP アドレスが無効です
タイムゾーン (Time Zone)	コントローラ VM のローカルタイムゾーン。このタイムゾーンに基づいて、スケジュールされたスナップショットを取るタイミングが決定されます。スケジュールされたネイティブスナップショットアクションは、この設定に基づきます。

ステップ 5 [コネクテッドサービス (Connected Services)] セクションで、[コネクテッドサービスを有効にする (Enable Connected Services)] を選択して、自動サポート (Auto Support) および Intersight Management を有効にします。

フィールド	説明
コネクテッドサービスの有効化 (Enable Connected Services) (推奨)	自動サポート (Auto Support) および Intersight Management を有効にします。HX Connect にログオンしてこれらのサービスを構成するか、またはそれらを選択的にオンまたはオフにします。
サービスチケット通知の送信先 (Send service ticket notifications to)	自動サポートによってトリガーされたときに SR 通知が送信される電子メールアドレス。

ステップ 6 [詳細設定 (Advanced)] セクションで、次の操作を行います。

フィールド	説明
ジャンボフレーム ジャンボフレームを有効化 (Enable Jumbo Frames)	ホスト vSwitches と vNIC、および各ストレージコントローラ VM 上のストレージデータネットワークの MTU サイズを設定する場合は、このチェックボックスをオンにします。  デフォルト値は 9000 です。  (注) MTU サイズを 9000 以外の値に設定するには、Cisco TAC にご連絡ください。

フィールド	説明
ディスク パーティション ディスク パーティションのクリーンアップ (Clean up Disk Partitions)	<p>ストレージクラスタに追加されたすべてのノードから既存のデータとパーティションをすべて削除して手動でサーバを準備する場合は、このチェックボックスをオンにします。既存のデータやパーティションを削除するには、このオプションを選択します。保持する必要があるデータはすべてバックアップする必要があります。</p> <p><b>注目</b> 工場で準備されたシステムの場合は、このオプションを選択しないでください。工場で準備されたシステムのディスクパーティションは正しく設定されています。</p>
仮想デスクトップ(VDI)	<p>VDI のみの環境でオンにします。</p> <p>(注) ストレージクラスタの作成後に VDI 設定を変更するには、リソースをシャットダウンまたは移動し、変更を加え (下の手順に記載)、クラスタを再起動します。</p> <p>デフォルトでは、HyperFlex クラスタは VSI ワークロード用にパフォーマンス調整されるように設定されています。</p> <p>このパフォーマンスのカスタマイズは、Hyperflex Data Platform クラスタで次の手順を実行することによって変更できます。HyperFlex クラスタを VDI から VSI ワークロード (またはその逆) に変更するには、次のようにします。</p> <p><b>警告:</b> メンテナンス ウィンドウが必要です。これにより、クラスタがオフラインの間はデータが使用できなくなります。</p> <ol style="list-style-type: none"> <li>1. <code>~#stcli cluster shutdown</code> を実行してクラスタをシャットダウンします。</li> <li>2. すべてのコントローラ VM の <code>storfs cfg</code> を編集し、<code>workloadType</code> を <code>Vsi</code> または <code>Vdi</code> に変更します。</li> <li>3. クラスタの作成後に、クラスタを起動し (<code>stcli cluster start</code>)、調整の変更を有効にします。</li> </ol>

フィールド	説明
(オプション) vCenter Server のシングル サインオン (vCenter Single-Sign-On Server)	<p>この情報は、SSO URL が到達可能でない場合のみ必要です。</p> <p>(注) このフィールドは使用しないでください。これはレガシー展開に使用されます。</p> <p><b>[vCenter Server] &gt; [Manage] &gt; [Advanced Settings] &gt; [key config.vpxd.sso.sts.uri]</b> にナビゲートして、vCenter で SSO URL を見つけることができます。</p>

**ステップ 7** **[開始 (Start)]** をクリックして HyperFlex クラスタの展開を開始します。[進捗状況 (Progress)] ページには、さまざまな設定タスクの進捗状況が表示されます。

**注意** 確認に関する警告を無視しないでください。

詳細については、「警告」セクションを参照してください。

#### 次のタスク

- 検証エラーによっては、パラメータの再入力が必要になることがあります (たとえば、無効な ESXi パスワード、誤った NTP サーバ、不良 SSO サーバなどの誤った入力の原因のエラー)。[値の再入力 (Re-enter Values)] をクリックして [クラスタ構成 (Cluster Configuration)] ページに戻り、問題を解決します。
- これが完了すると、HyperFlex サーバがインストールされ、構成されます。正常にデプロイされたクラスタのステータスは、[オンライン (Online)] および [正常 (Healthy)] として示されます。
- [HyperFlex Connect の起動 (Launch HyperFlex Connect)] をクリックし、データストアを作成してクラスタを管理します。

## HyperFlex ハードウェア アクセラレーション カードの取り付けの確認

HyperFlex ハードウェア アクセラレーション カードが正常にインストールされたことを確認するには、次の手順を実行します。

**ステップ 1** コントローラ VM にログインします。

**ステップ 2** 次の調整ファイルを探します。 /opt/springpath/config/offload.tunes

- (注) 調整ファイルは、システム管理者とルートユーザーのみが表示できます。これらのユーザーがこのファイルにアクセスできる場合、インストールは成功しています。システム管理者またはルートユーザー権限を持っていない場合は、UI にエラー メッセージまたはイベント存在しないことで、インストールが成功したことを確認できます。

## HyperFlex ハードウェア アクセラレーション カードのトラブルシューティング

次のように、インストール後の HyperFlex ハードウェア アクセラレーション カードに関連する問題をトラブルシューティングします。

症状	回避策
クラスタは動作していますが、vCenter と HX Connect UI で汎用アラートに注意するようにしてください。	サポートについては、Cisco の営業担当者にご連絡ください。
NR ペアリングが試行されると、クラスタはペアリング エラーを報告します。	<p>いずれかのクラスタが 4.5(1a) より前のリリースであり、HX ハードウェア アクセラレーション カードで有効になっている場合、NR ペアリングは許可されません。</p> <p>HX ハードウェア アクセラレーション カードとの NR ペアリングは、ペアの両方のクラスタに HX ハードウェア アクセラレーション カードがある場合にのみサポートされます。</p>

## HyperFlex ハードウェア アクセラレーション カードのに関する追加情報

HyperFlex ハードウェア アクセラレーション カードに関するその他の注意事項は、次のとおりです。

- 圧縮ゲインの値は、HX connect UI ダッシュボードに表示されます。
- 次のコマンドを使用して、8K の読み取りワークロードのパフォーマンスを向上させます。
  - `root @ ucs984scvm: ~ # echo 3 >/sys/module/fdma/parameters/decompress_min_t`
  - `root@ucs984scvm:~# echo 3 >/sys/module/fdma/parameters/decompress_max_t`







## 第 8 章

# クラスタ設定後のタスク

---

- クラスタ設定後のガイドライン (133 ページ)
- ホスト上のネットワーク デバイスの PCI パススルー有効化 (134 ページ)
- インストール後のスクリプトの実行 (135 ページ)
- ESXi ホストのルート パスワードの変更 (136 ページ)
- ストレージコントローラのパスワードの変更 (137 ページ)
- VMware vCenter の Cisco HyperFlex HTML プラグイン (137 ページ)
- ストレージクラスタでのデータストアの追加 (138 ページ)
- HA ハートビートの設定 (138 ページ)
- HyperFlex の自動サポートと Smart Call Home (139 ページ)
- 自己署名の証明書を CA 署名の証明書で置き換える (145 ページ)
- レプリケーション ペアリング (147 ページ)
- プライベート VLAN の追加 (147 ページ)
- 分散型仮想スイッチと Cisco Nexus 1000v (151 ページ)
- HX Data Platform 上での vCenter のホスト (153 ページ)
- AMD GPU の展開 (153 ページ)

## クラスタ設定後のガイドライン



### 重要

- すべての ESXi ホストで SSH を有効なままにしてください。これは、これ以降の Cisco HyperFlex post クラスタ設定後の作業で必要となります。
  - これらの事前設定された値は、シスコの承認を得ずに変更しないでください。
-

# ホスト上のネットワーク デバイスの PCI パススルー有効化

パススルーデバイスは、より効率的にリソースを使用して環境内のパフォーマンスを向上させるための手段を提供します。PCI パススルーを有効化することで、VM はホストデバイスを、VM に直接接続されているように使用できます。



**注意** HXDP クラスタの重要なデバイスを PCI パススルー用にセットアップしないでください。

次の手順では、ESXi ホスト上の PCI パススルー用にネットワーク デバイス (NVIDIA GPU など) を設定する方法を説明します。

- ステップ 1 vSphere Client のナビゲーションパネルで ESXi ホストを参照します。
- ステップ 2 GPU がインストールされているノードで、HX メンテナンス モードを開始します。メンテナンス モードを開始するには、ノードを右クリックし、**[Cisco HX Maintenance Mode (Cisco HX メンテナンス モード)]** > **[Enter HX Maintenance Mode (HX メンテナンス モードの開始)]** の順に選択します。
- ステップ 3 新しいブラウザ ウィンドウで、ESXi ノードに直接ログインします。
- ステップ 4 **[Manage]** をクリックします。
- ステップ 5 **[Hardware]** タブで、**[PCI Devices]** をクリックします。利用可能なパススルー デバイスのリストが表示されます。
- ステップ 6 パススルーに対して有効にする PCI デバイスを選択します。**[Toggle passthrough (パススルーのトグル)]** をクリックします。
- ステップ 7 ホストを再起動して、PCI デバイスを利用可能にします。
- ステップ 8 リブートが完了したら、ノードがメンテナンス モードになっていないことを確認します。
- ステップ 9 vCenter Server にログインします。
- ステップ 10 VM を検索して右クリックし、**[Edit Settings (設定の編集)]** を選択します。
- ステップ 11 **[New device]** ドロップダウンメニューで **[PCI Device]** を選択して、**[Add]** をクリックします。
- ステップ 12 使用するパススルー デバイス (例: NVIDIA GPU) をクリックして、**[OK]** をクリックします。
- ステップ 13 ESXi ホストにログインし、仮想マシンの設定ファイル (.vmx) をテキスト エディタで開きます。

```
cd /vmfs/volumes/[datastore_name]/[vm_name]
vi [vmname].vmx
```

- ステップ 14 次の行を追加して保存し、テキスト エディタを終了します。

```
# pciPassthru.64bitMMIOSizeGB = "64"
# Firmware = "efi"
# pciPassthru.use64bitMMIO = "TRUE"
```

# インストール後のスクリプトの実行

インストーラ後のスクリプトを実行することで、インストール後のタスクを完了できます。



**重要** • HyperFlex System を展開した後、ただちに `hx_post_install` を実行して、ネットワークの動作を確認してください。

1. SSH クライアントを使用して、`admin` ログインを使用してクラスタ仮想 IP に接続します。
2. 「`hx_post_install`」と入力して、`Enter` キーを押します。
3. 次の表に指定しているように、インストール後スクリプトパラメータを設定します。



(注) インストール後スクリプトに問題が発生した場合は、インストール後スクリプトのパラメータを手動で設定します。

パラメータ	説明
Enable HA/DRS on cluster? (クラスタで HA/DRS を有効にするか)	ベストプラクティスに従って vSphere 高可用性 (HA) 機能を有効にします。
Disable SSH warning? (SSH 警告を無効にするか)	vCenter 内での SSH 警告とシェル警告を抑制します。
Add vMotion interfaces (vMotion インターフェイスの追加)	ベストプラクティスに従って vMotion インターフェイスを設定します。IP アドレスと VLAN ID の入力が必要です。
Add VM network VLANs (VM ネットワーク VLAN の追加)	すべてのクラスタ ホスト上の ESXi 内、および Cisco UCS Manager にゲスト VLAN を追加します。

4. ネットワーク エラーが報告された場合には修正します。

サンプルのインストール後のスクリプト: オプション 1 新規/既存のクラスタ

サンプルのインストール後のスクリプト: オプション 3 Generate Certificate

ネットワーク エラーの例

```
Host: esx-hx-5.cpoc-rtp.cisco.com
No errors found
```

```

Host: esx-hx-6.cpoc-rtp.clsco.com
No errors found

Host: esx-hx-1.cpoc-rtp.cisco.com
No errors found

Host: esx-hx-2.cpoc-rtp.cisco.com
No errors found

controller VM clocks:
stctlVM-FCH1946V34Y - 2016-09-16 22:34:04
stCtlVM-FCH1946V23M - 2016-09-16 22:34:04
stctIVM-FCH1951V2TT - 2016-09-16 22:34:04
stctlVM-FCH2004VINS - 2016-09-16 22:34:04

Cluster:
Version - 1.8.1a-19499
Model - HX220C-M4S
Health - HEALTHY
Access policy - LENIENT
ASUP enabled - False
SMTP server - smtp.cisco.com

```

## ESXi ホストのルートパスワードの変更

次のシナリオで、デフォルトの ESXi パスワードを変更できます。

- 標準およびストレッチ クラスタの作成時（コンバージド ノードのみをサポート）
- 標準クラスタの拡張時（コンバージド ノードまたはコンピューティング ノードの両方の拡張をサポート）
- エッジクラスタの作成時



(注) 上記の場合、インストールが完了するとすぐに ESXi のルートパスワードが保護されます。後続のパスワード変更が必要である場合、下に概要を示している手順をインストール後に使用して、ルートパスワードを手動で変更することができます。

ESXi は工場出荷時のデフォルトパスワードで提供されているため、セキュリティ上の理由からパスワードを変更する必要があります。インストール後のデフォルトの ESXi ルートパスワードを変更するには、次の手順を実行します。



(注) ESXi ルートパスワードを忘れた場合は、パスワードの復旧について Cisco TAC にお問い合わせください。

**ステップ 1** SSH を使用して ESXi ホスト サービス制御にログインします。

**ステップ 2** ルート権限を取得します。

```
su -
```

**ステップ3** 現在のルートパスワードを入力します。

**ステップ4** ルートパスワードを変更します。

```
passwd root
```

**ステップ5** 新しいパスワードを入力し、**Enter** キーを押します。確認のためにパスワードを再入力します。

(注) 2回目に入力したパスワードが一致しない場合は、最初からやり直す必要があります。

---

## ストレージコントローラのパスワードの変更

インストール後にHyperFlexストレージコントローラのパスワードをリセットするには、次の手順を実行します。

**ステップ1** ストレージコントローラVMにログインします。

**ステップ2** Cisco HyperFlex ストレージコントローラパスワードを変更します。

```
# stcli security password set
```

このコマンドによって、ストレージクラスタ内のすべてのコントローラVMに変更が適用されます。

(注) 新しいコンピューティングノードを追加し、**stcli security password set** コマンドを使用してクラスタパスワードをリセットしようとする、コンバージドノードは更新されますが、コンピューティングノードはデフォルトパスワードのままになることがあります。コンピューティングノードのパスワードを変更するには、次の手順を使用します。

**ステップ3** 新しいパスワードを入力します。

**ステップ4** **Enter** を押します。

---

## VMware vCenter の Cisco HyperFlex HTML プラグイン

Cisco HyperFlex vCenter プラグインは、vSphere Webクライアントと統合され、HX Data Platformのインストール後の管理およびモニタリング機能をすべてサポートします。インストールと使用法に関する完全な情報については、『Cisco HyperFlex Data Platform Administration Guide』の「[Cisco HyperFlex HTML Plugin for VMware vCenter](#)」の章を参照してください。

## ストレージクラスタでのデータストアの追加

新しい HyperFlex クラスタでは、仮想マシンストレージ用のデフォルト データストアが設定されていないため、VMware vSphere Web クライアントを使用してデータストアを作成する必要があります。



(注) 高可用性を実現するために、最低 2 つのデータストアを作成することを推奨します。

- ステップ 1 Web クライアント ナビゲータの [Global Inventory Lists] で、[Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [cluster] > [Manage] > [Datastores] の順に展開します。
- ステップ 2 [データストアの作成 (Create Datastore)] アイコンをクリックします。
- ステップ 3 データストアの名前を入力します。vSphere Web クライアントはデータストア名に 42 文字の制限を適用します。各データストアに固有の名前を割り当てます。
- ステップ 4 データストアのサイズを指定します。ドロップダウンリストから、[GB] または [TB] を選択します。[OK] をクリックします。
- ステップ 5 新しいデータストアを表示するには、[Refresh] ボタンをクリックします。
- ステップ 6 新しいデータストアの [マウント ステータス (Mount Status)] を表示するには、[ホスト (Hosts)] タブをクリックします。

## HA ハートビートの設定

vSphere HA の設定では、使用可能なデータストアのリストから任意のデータストアを選択できるように、[ハートビティングのデータストア (Datastore for Heartbeating)] オプションを必ず設定してください。

- ステップ 1 vSphere にログインします。
- ステップ 2 DRS が有効になっていることを確認します。  
vSphere の [ホーム (Home)] > [ホストとクラスタ (Hosts and Clusters)] > [クラスタ (cluster)] > [設定 (Configure)]、[サービス (Services)] を選択します。[vSphere DRS] をクリックします。
- ステップ 3 [Edit] ボタンをクリックします。[vSphere HA] をクリックします。[編集 (Edit)] をクリックします。
- ステップ 4 選択されていない場合は、[vSphere HA をオンにする (Turn on vSphere HA)] を選択します。
- ステップ 5 ドロップダウンメニューから [アドミッション コントロール (Admission Control)] > [フェールオーバー容量の定義 (Define Failover capacity by)] > [クラスタ リソース割合 (Cluster resource percentage)] を展開します。デフォルト値を使用することも、[Override calculated failover capacity] を有効にしてパーセンテージを入力することもできます。

ステップ 6 [Heartbeat Datastores] を展開し、[Use datastore only from the specified list] を選択します。含めるデータストアを選択します。

ステップ 7 [OK] をクリックします。

## HyperFlex の自動サポートと Smart Call Home

HX ストレージクラスタを構成して、文書化されたイベントに関する自動化された電子メール通知を送信することができます。通知内の収集されたデータを使用して、HX ストレージクラスタの問題のトラブルシューティングに役立てることができます。



- (注) Auto Support (ASUP) および Smart Call Home (SCH) は、プロキシサーバの使用をサポートしています。プロキシサーバの使用を有効にし、HX Connect を使用して、両方のプロキシ設定を構成できます。

### Auto Support (ASUP)

Auto Support は、HX Data Platform を通じて提供されるアラート通知サービスです。Auto Support を有効にすると、HX Data Platform から、指定されたメールアドレスまたは通知を受信したい電子メールエイリアスに通知が送信されます。通常、Auto Support は、HX ストレージクラスタの作成時に、SMTP メールサーバを設定し、電子メールの受信者を追加して設定します。



- (注) 未認証の SMTP のみが ASUP のサポート対象となります。

構成中に **[Enable Auto Support (Auto Support を有効にする)]** チェックボックスが選択されていない場合、次の方法を使用して Auto Support をクラスタの作成後に有効にすることができます。

クラスタ作成後の ASUP 構成方法	関連トピック
HX Connect ユーザ インターフェイス	<a href="#">HX Connect を使用した自動サポートの設定 (140 ページ)</a>
コマンドライン インターフェイス (CLI)	<a href="#">CLI を使用した通知設定の構成 (142 ページ)</a>
REST API	Cisco HyperFlex は <a href="#">Cisco DevNet</a> での REST API をサポートします。

Auto Support は、監視ツールに HX ストレージクラスタを接続するためにも使用できます。

### Smart Call Home (SCH)

Smart Call Home は、HX ストレージクラスタを監視し、ビジネスの運営に影響をおよぼす前に問題にフラグ付けして解決を開始する、自動化されたサポート機能です。これにより高いネットワーク可用性と運用効率の向上をもたらします。

Call Home は、さまざまな障害や重要なシステムイベントを検出してユーザーに通知する、Cisco デバイスのオペレーティングシステムに埋め込まれている製品機能です。Smart Call Home は、基本的な Call Home 機能を強化するための自動化と便利な機能を追加します。Smart Call Home を有効にすると、Call Home のメッセージとアラートは Smart Call Home に送信されます。

Smart Call Home は Cisco の多くのサービス契約に含まれており、次が含まれます。

- 自動化された、24 時間の機器監視、プロアクティブな診断、リアルタイムの電子メールアラート、サービス チケットの通知、および修復の推奨。
- Call Home 診断とインベントリ アラームをキャプチャおよび処理することにより指定された連絡先に送信される、プロアクティブなメッセージング。これらの電子メールメッセージには、自動的に作成された場合に Smart Call Home ポータルと TAC ケースへのリンクが含まれています。
- Cisco Technical Assistance Center (TAC) による優先サポート。Smart Call Home では、アラートが十分に重大な場合、TAC ケースが自動的に生成され、デバッグおよび他の CLI 出力が添付されて、https 経由で適切なサポート チームにルーティングされます。
- カスタマイズ可能なステータス レポートおよびパフォーマンス分析。
- 次に対する Web ベースのアクセス 1 箇所における修復のためのすべての Call Home メッセージ、診断、および推奨、TAC ケースのステータス、すべての Call Home デバイスの最新のインベントリおよび構成情報。

HX ストレージクラスタ、ユーザー、サポートの間で自動的に通信が行われるように設定する方法については、[データ収集用の Smart Call Home の設定 \(143 ページ\)](#) を参照してください。

## HX Connect を使用した自動サポートの設定

一般に、Auto Support (ASUP) は HX ストレージクラスタの作成中に設定されます。設定されなかった場合は、クラスタ作成後に HX Connect ユーザーインターフェイスを使用して有効にすることができます。

**ステップ 1** HX Connect にログインします。

**ステップ 2** バナーで、[設定の編集 (Edit settings)] (歯車アイコン) > [自動サポートの設定 (Auto Support Settings)] をクリックして、次のフィールドに値を入力します。



UI 要素	基本的な情報
[自動サポートの有効化 (推奨) (Enable Auto Support (Recommended))] ] チェックボックス	以下を有効にすることにより、この HX ストレージクラスタの Call Home を設定します。 <ul style="list-style-type: none"> <li>• Cisco TAC への分析用データの配信。</li> <li>• プロアクティブ サポートの一環としてのサポートからの通知。</li> </ul>
[サービスチケット通知の送信先 (Send service ticket Notifications to) ] フィールド	通知を受信する電子メールアドレスを入力します。
[Terms and Conditions (使用条件)] チェック ボックス	エンドユーザー使用契約。自動サポート機能を使用するには、このチェック ボックスをオンにする必要があります。
[プロキシサーバを使用 (Use Proxy Server) ] チェックボックス	<ul style="list-style-type: none"> <li>• Web プロキシ サーバ URL</li> <li>• [ポート (Port) ]</li> <li>• ユーザー名 (Username)</li> <li>• パスワード</li> </ul>

ステップ 3 [OK] をクリックします。

ステップ 4 パナーで、[設定の編集 (Edit settings) ] (歯車アイコン) > [通知の設定 (Notifications Settings) ] をクリックして、次のフィールドに値を入力します。

UI 要素	基本的な情報
[電子メール通知によるアラームの送信 (Send email notifications for alarms) ] チェックボックス	オンにした場合は、次のフィールドに値を入力します。 <ul style="list-style-type: none"> <li>• メールサーバアドレス</li> <li>• 送信元アドレス (From Address) : サポート サービス チケットで HX ストレージクラスタを特定するために使われる電子メールアドレスを、自動サポート通知の送信者として入力します。現在、この電子メールアドレスにはサポート情報が送信されません。</li> <li>• 受信者リスト(カンマ区切り)</li> </ul>

ステップ 5 [OK] をクリックします。

## CLI を使用した通知設定の構成

HX ストレージクラスタからアラーム通知を受信する設定を構成および検証するには、次の手順に従います。



(注) 未認証の SMTP のみが ASUP のサポート対象となります。

**ステップ 1** ssh を使用して HX ストレージクラスタ内のストレージコントローラ VM にログインします。

**ステップ 2** SMTP メールサーバを設定し、設定を確認します。

指定された受信者に電子メール通知を送信するために SMTP メールサーバで使用される電子メールアドレスです。

構文 : `stcli services smtp set [-h] --smtp SMTPSERVER --fromaddress FROMADDRESS`

例 :

```
# stcli services smtp set --smtp mailhost.eng.mycompany.com --fromaddress smtpnotice@mycompany.com
```

```
# stcli services smtp show
```

**ステップ 3** ASUP 通知を有効にします。

```
# stcli services asup enable
```

**ステップ 4** 受信者の電子メールアドレスを追加して、設定を確認します。

電子メール通知を受信する一連の電子メールアドレスまたは電子メールエイリアスのリストです。複数の電子メールはスペースで区切ります。

構文 : `stcli services asup recipients add --recipients RECIPIENTS`

例 :

```
# stcli services asup recipients add --recipients user1@mycompany.com user2@mycompany.com
```

```
# stcli services asup show
```

**ステップ 5** HX ストレージクラスタの eth1:0 IP アドレスを所有しているコントローラ VM から、電子メールでテスト ASUP 通知を送信します。

```
# sendasup -t
```

eth1:0 IP アドレスを所有しているノードを判別するには、ssh を使用して HX ストレージクラスタの各ストレージコントローラ VM にログインし、ifconfig コマンドを実行します。他のノードから sendasup コマンドを実行しても、出力は何も返されず、受信者はテストを受信しません。

**ステップ 6** すべてのストレージコントローラ VM の IP アドレスから電子メールを送信できるように電子メールサーバを設定します。

## データ収集用の Smart Call Home の設定

データコレクションはデフォルトで有効にされますが、インストール時にオプトアウト（無効化）することができます。クラスタ作成後のデータコレクションを有効にすることもできます。アップグレード中、Smart Call Home の有効化はレガシー構成によって決まります。たとえば、`stcli services asup show` を有効にすると、アップグレード時に Smart Call Home が有効になります。

HX ストレージクラスタに関するデータコレクションは、https を介して Cisco TAC に転送されます。インストールされているファイアウォールがある場合、Smart Call Home のプロキシサーバの構成は、クラスタ作成の後に完了します。



(注) HX クラスタからの発信接続がプロキシサーバを通過する必要がある展開では、Smart Call Home はプロキシサーバの使用をサポートしていません。



(注) HyperFlex Data Platform リリース 2.5(1.a) では、Smart Call Home Service Request (SR) の生成でプロキシサーバは使用されません。

Smart Call Home を使用するには、次のものがが必要です。

- 対応する Cisco Unified Computing Support Service 契約または Cisco Unified Computing Mission Critical Support Service 契約と関連付けられた Cisco.com ID。
- 登録されるデバイス用の Cisco Unified Computing Support Service または Cisco Unified Computing Mission Critical Support Service

**ステップ 1** HX ストレージクラスタ内のストレージコントローラ VM にログインします。

**ステップ 2** HX ストレージクラスタをサポートに登録します。

HX ストレージクラスタに登録すると、収集されたデータに ID を追加し、Smart Call Home を自動的に有効にします。HX ストレージクラスタに登録するには、電子メールアドレスを指定する必要があります。登録後、問題が発生して TAC サービス要求が生成されるたびに、このメールアドレスはサポート通知を受け取ります。

構文：

```
stcli services sch set [-h] --email EMAILADDRESS
```

例：

```
# stcli services sch set --email name@company.com
```

**ステップ 3** HX ストレージクラスタからサポートへのデータフローが機能していることを確認します。

データフローが機能していれば、問題が発生した場合にサポートがそれをトラブルシューティングするうえで役立つ関連情報が確実に得られます。

(注) TAC に連絡して接続を確認してください。

```
# asupcli [--all] ping
```

--all オプションは、HX クラスタ内のすべてのノード上でコマンドを実行します。

**ステップ 4** (省略可能) ポート 443 を介した Smart Call Home のアクセスを有効にするためにプロキシサーバを設定します。

クラスタの作成後、HX ストレージクラスタがファイアウォールの背後にある場合は、Smart Call Home プロキシサーバを構成する必要があります。サポートは、url: https://diag.hyperflex.io:443 エンドポイントでデータを収集します。

1. 既存の登録メールとプロキシ設定をすべてクリアします。

```
# stcli services sch clear
```

2. プロキシと登録メールを設定します。

構文：

```
stcli services sch set [-h] --email EMAILADDRESS [--proxy-url PROXYURL] [--proxy-port PROXYPORT]
[--proxy-user PROXYUSER] [--portal-url PORTALURL] [--enable-proxy ENABLEPROXY]
```

構文の説明	Option	必須またはオプション	説明
	<b>--email EMAILADDRESS</b>	必須。	シスコ サポートから電子メールを受信するユーザのために、電子メールアドレスを追加します。配信リストまたはエイリアスを使用することをお勧めします。
	<b>--enable-proxy ENABLEPROXY</b>	オプション。	プロキシの使用を明示的に有効または無効にします。
	<b>--portal-url PORTALURL</b>	オプション。	代替の Smart Call Home ポータル URL を指定します (該当する場合)。
	<b>--proxy-url PROXYURL</b>	オプション。	HTTP または HTTPS プロキシの URL を指定します (該当する場合)。
	<b>--proxy-port PROXYPORT</b>	オプション。	HTTP または HTTPS プロキシのポートを指定します (該当する場合)。
	<b>--proxy-user PROXYUSER</b>	オプション。	HTTP または HTTPS プロキシの URL を指定します (該当する場合)。  HTTP または HTTPS プロキシのパスワードを指定します (メッセージが表示される場合)。

例：

```
# stcli services sch set
--email name@company.com
--proxy-url www.company.com
--proxy-port 443
--proxy-user admin
--proxy-password adminpassword
```

3. プロキシサーバが動作していること、および HX ストレージクラスタからサポート ロケーションにデータが流れることを確認するために ping を送信します。

(注) TAC に連絡して接続を確認してください。

```
# asupcli [--all] ping
```

--all オプションは、HX クラスタ内のすべてのノード上でコマンドを実行します。

**ステップ 5** Smart Call Home が有効になっていることを確認します。

Smart Call Home 構成が設定されると、自動的に有効になります。

```
# stcli services sch show
```

**ステップ 6** 自動サポート (ASUP) 通知を有効にします。

一般に、Auto Support (ASUP) は HX ストレージクラスタの作成中に設定されます。設定されなかった場合、HX Connect または CLI を使用してクラスタ作成後の設定を有効にすることができます。

Smart Call Home が無効になっている場合は、手動で有効にします。

```
# stcli services sch enable
```

---

## 自己署名の証明書を CA 署名の証明書で置き換える



- (注) リリース 5.0(1x) 以前の場合、次の証明書置換スクリプトを実行するには、コントローラ VM へのルートレベルのアクセスが必要です。TAC に連絡して、証明書置換プロセスを完了してください。リリース 5.0(2a) 以降では、**diag** ユーザー シェルにアクセスして CAPTCHA テストを完了する必要があります。プロセスの説明については、『[Cisco HyperFlex Data Platform 管理ガイド、リリース 5.0](#)』の「[Diag ユーザーの概要](#)」を参照してください。

CA 証明書のインポートは、シェルスクリプトによって自動化されています。任意の CVM、できれば CIP ノードから CSR (証明書署名要求) を生成します。各 CVM は同じ証明書でインストールする必要があるため、クラスタに必要な CSR は 1 つだけです。CSR を生成するときに、管理 CIP に割り当てられたホスト名をサブジェクトの識別名の共通名として入力する必要があります。

次に例を示します。

```

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:HyperFlex
Common Name (e.g. server FQDN or YOUR name) []:<hostname-cluster-management-IP>
Email Address []:support@cisco.com

```

CA 証明書を取得した後で、自動スクリプトを使用して証明書をインポートします。スクリプトは、その CVM の証明書のみを更新します。



(注) クラスタ拡張の場合は、証明書をインポートするために、同じ証明書とキーファイルを使用して、拡張されたノード CVM でスクリプトを再度実行する必要があります。

**diag** シェルにアクセスしたら、次の手順を実行します。

**ステップ 1** CVM でのスクリプトの場所は、`/usr/share/springpath/storfs-misc/hx-scripts/` です。

```

diag/usr/share/springpath/storfs-misc/hx-scripts/certificate_import_input.certificate_import_input.sh

run stcli cluster reregister

```

**ステップ 2** コントローラ VM (CIP を指す) で、このコマンドを実行して CSR 要求を生成します。

```

openssl req -nodes -newkey rsa:2048 -keyout /etc/ssl/private/<Host Name of the CVM>.key -out
/etc/ssl/certs/<Host Name of the CVM>.csr
cat /etc/ssl/certs/<host name mapped to the management CIP>.csr - Copy the request to any notepad.

Send the request to CA to generate the certificate

```

**ステップ 3** CA (.crt ファイル) から証明書を受信したら、証明書とキーを各 CVM にコピーします。

**ステップ 4** 各CVMで、`./certificate_import_input.sh` スクリプトを使用して証明書をインポートします。

```

root@SpringpathControllerVUFSTDS58L:/usr/share/springpath/storfs-misc/hx-scripts#
./certificate_import_input.sh

```

**ステップ 5** キーのパスとして、`/etc/ssl/private/<CVM のホスト名>.key` を入力します。

**ステップ 6** <CA へのパス.crt ファイル> という証明書形式で証明書のパスを入力します。

(注) すべての入力を入力した後、インポートプロセスが完了するまでにいくらか時間がかかります。

**ステップ 7** CIP をポイントしている CVM から **stcli reregister** コマンドを実行して、クラスタを vCenter に再登録します。証明書をインポートしたら、クラスタを再登録する必要があります。

## レプリケーション ペアリング

レプリケーション クラスタ ペアの作成は、VM をレプリケーション用にセットアップするための前提条件です。レプリケーション ペアを作成する前に、レプリケーション ネットワークと少なくとも1つのデータストアを設定する必要があります。

クラスタ2とクラスタ1をペアリングすることによって、レプリケーション用に明示的に設定されたクラスタ1上のすべてのVMはクラスタ2にレプリケートでき、レプリケーション用に明示的に設定されたクラスタ2上のすべてのVMはクラスタ1にレプリケートできることを指定しています。

クラスタ1のデータストアAとクラスタ2のデータストアBをペアリングすることによって、レプリケーション用に明示的に設定されたクラスタ1上のすべてのVMでは、データストアAにファイルがある場合、それらのファイルはクラスタ2のデータストアBにレプリケートされることを指定しています。同様に、レプリケーション対象として明示的に設定されたクラスタ2上のすべてのVMでは、データストアBにファイルがある場合、それらのファイルがクラスタ1のデータストアAにレプリケートされます。

ペアリングは厳密に1対1で行われます。クラスタは、他のクラスタのうち1つとだけペアリング可能です。ペアリングされるクラスタ上のデータストアは、もう一方のクラスタ上の1つのデータストアとだけペアリングできます。

レプリケーションペアの作成、編集、および削除の詳細な手順については、『[Cisco HyperFlex Systems Administration Guide](#)』を参照してください。

## プライベート VLAN の追加

### プライベート VLAN について

プライベート VLAN では VLAN のレイヤ2ブロードキャスト ドメインがサブドメインに分割されるので、スイッチで相互にポートを分離できます。サブドメインは、1つのプライマリ VLAN と1つまたは複数のセカンダリ VLAN で構成されます。プライベート VLAN ドメインには、プライマリ VLAN が1つのみ含まれています。プライベート VLAN ドメインの各ポートは、プライマリ VLAN のメンバーで、プライマリ VLAN は、プライベート VLAN ドメイン全体です。

## プライベート VLAN ポートの概要

表 5: プライベート VLAN ポートのタイプ

VLAN ポート	説明
Promiscuous Primary VLAN	プライマリ VLAN に属しています。無差別ポートに関連付けられているセカンダリ VLAN に属しているインターフェイス、およびプライマリ VLAN に関連付けられているインターフェイスのすべてと通信できます。それらのインターフェイスには、コミュニティ ポートと独立ホスト ポートも含まれます。セカンダリ VLAN からのすべてのパケットは、この VLAN を経由します。
独立したセカンダリ VLAN	度クリスしたセカンダリ VLAN に属するホスト ポートです。このポートは同じプライベート VLAN ドメイン内のその他のポートから完全に分離されていますが、関連付けられている無差別ポートとは通信できます。
コミュニティ セカンダリ VLAN	コミュニティ セカンダリ VLAN に属するホスト ポートです。コミュニティ ポートは、同じコミュニティ VLAN にある他のポートおよびアソシエートされている無差別ポートと通信します。

HX の導入に従い、VM ネットワークはデフォルトで通常の VLAN を使用します。VM ネットワークにプライベート VLAN を使用する場合は、次のセクションを参照してください。

- [既存の VM を使用しない VM ネットワーク上でのプライベート VLAN の設定 \(148 ページ\)](#)。
- [既存の VM を使用した VM ネットワーク上でのプライベート VLAN の設定 \(149 ページ\)](#)。

## 既存の VM を使用しない VM ネットワーク上でのプライベート VLAN の設定

- 
- ステップ 1** Cisco UCS Manager でプライベート VLAN を設定するには、『[Cisco UCS Manager Network Management Guide](#)』を参照してください。
- ステップ 2** 上流に位置するスイッチでプライベート VLAN を設定するには、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。
- ステップ 3** ESX ホストでプライベート VLAN を設定するには、『[ESX ホスト上でのプライベート VLAN の設定 \(148 ページ\)](#)』を参照してください。
- 

## ESX ホスト上でのプライベート VLAN の設定

ESX ホストでプライベート VLAN を設定するには、次の手順を実行します。



- 
- ステップ1 VMware vSphere クライアントから vSphere 標準スイッチ上の VMNIC を削除します。
- ステップ2 前の手順で削除した VMNIC を使用して新しい vSphere 分散型スイッチを作成します。
- ステップ3 無差別（プロミスキャス）、独立、およびコミュニティ VLAN を作成します。
- 

## 既存の VM を使用した VM ネットワーク上でのプライベート VLAN の設定

---

- ステップ1 Cisco UCS Managerでプライベート VLAN を設定するには、『[Cisco UCS Manager Network Management Guide](#)』を参照してください。
- ステップ2 上流に位置するスイッチでプライベート VLAN を設定するには、『[Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide](#)』を参照してください。
- ステップ3 ESX ホストでプライベート VLAN を設定するには、『[ESX ホスト上でのプライベート VLAN の設定 \(148 ページ\)](#)』を参照してください。
- ステップ4 vSphere 標準スイッチから、新しく作成された vSphere 分散型スイッチに VM を移行します。
- vCenter 仮想マシンを右クリックして、[Migrate Virtual Machine Networking] をクリックします。
  - ドロップダウン リストから、[送信元ネットワーク (source network)] および [送信先ネットワーク (destination network)] を選択します。
  - [次へ (Next)] をクリックします。
  - 移行する [仮想マシン (Virtual Machines)] を選択します。
  - [Finish] をクリックします。
- ステップ5 VM 上のネットワーク アダプタのネットワーク接続をプライベート VLAN に変更します。
- vCenter 仮想マシンを右クリックして、[設定の編集 (Edit Settings)] をクリックします。
  - [ハードウェア (Hardware)] タブから、変更するネットワーク アダプタを選択します。
  - [ネットワーク ラベル (Network Label)] ドロップダウン リストから、使用する [ネットワーク接続 (Network Connection)] を選択します。
  - [OK] をクリックします。
- 

## VSphere 標準スイッチ上での VMNIC の削除

---

- ステップ1 VMware vSphere クライアントにログオンします。
- ステップ2 [ホーム (Home)] > [ホストとクラスタ (Hosts and Clusters)] を選択します。
- ステップ3 削除する VMNIC がある ESX ホストを選択します。
- ステップ4 [設定 (Configuration)] タブを開きます。
- ステップ5 [Networking] をクリックします。

- ステップ6 VMNIC を削除するスイッチを選択します。
- ステップ7 [Manage the physical adapters connected to the selected switch] ボタンをクリックします。
- ステップ8 削除する **vmnic** を選択し、[削除 (Remove) ] をクリックします。
- ステップ9 [はい (Yes) ] をクリックして、選択内容を確認します。
- ステップ10 [閉じる (Close) ] をクリックします。
- 

## vSphere 分散型スイッチの作成

---

- ステップ1 VMware vSphere クライアントにログオンします。
- ステップ2 [Home] > [Networking] を選択します。
- ステップ3 クラスタを右クリックして、[Distributed Switch] > [New Distributed Switch] を選択します。
- ステップ4 [Name and Location] ダイアログボックスに、分散スイッチの名前を入力します。
- ステップ5 [Select Version] ダイアログボックスで、バージョンと構成の要件に対応する分散スイッチバージョンを選択します。
- ステップ6 [Next] をクリックします。
- ステップ7 [Edit Settings] ダイアログボックスで、次のように指定します。
- [Number of uplink ports]
  - [Network I/O Control] を有効化します。
  - [Create a default port group] をオンにします。
  - [Port Group Name] ボックスに、デフォルト ポート グループの名前を入力します。
- ステップ8 [Next] をクリックします。
- ステップ9 [Ready to Complete] ダイアログボックスで、設定した内容を確認します。
- ステップ10 [終了] をクリックします。
- 

## vSphere 分散型スイッチ上でのプライベート VLAN の作成

---

- ステップ1 VMware vSphere クライアントから、[インベントリ (Inventory) ] > [ネットワーキング (Networking) ] を選択します。
- ステップ2 dvSwitch を右クリックします。
- ステップ3 [Edit Settings] をクリックします。
- ステップ4 [プライベート VLAN (Private VLAN) ] タブを選択します。
- ステップ5 [プライマリ プライベート VLAN ID (Primary private VLAN ID) ] タブで、**プライベート VLAN ID** を入力します。

**ステップ 6** [セカンダリ プライベート VLAN ID (Secondary private VLAN ID) ] タブで、**プライベート VLAN ID** を入力します。

**ステップ 7** [タイプ (Type) ] ドロップダウンリストから、VLAN のタイプを選択します。有効な値は次のとおりです。

- 隔離
- コミュニティ
- 無差別(デフォルト)

**ステップ 8** [OK] をクリックします。

---

## 分散型ポートグループ内のプライベート VLAN の設定

始める前に

vSphere 分散スイッチでプライベート VLAN を作成します。

**ステップ 1** [dvSwitch] の下の [dvPortGroup] を右クリックして、[設定の編集 (Edit Settings) ] をクリックします。

**ステップ 2** [ポリシー (Policies) ] > [VLAN] をクリックします。

**ステップ 3** [VLAN タイプ (VLAN type) ] ドロップダウンリストから [プライベート VLAN (Private VLAN) ] を選択します。

**ステップ 4** [プライベート VLAN エントリ (Private VLAN Entry) ] ドロップダウンリストから、プライベート VLAN のタイプを選択します。次のいずれかを指定できます。

- 隔離
- コミュニティ

(注) コミュニティプライベート VLAN が推奨されています。

混合モードポートはサポートされていません。

**ステップ 5** [OK] をクリックします。

---

## 分散型仮想スイッチと Cisco Nexus 1000v

分散型スイッチを導入する際の検討事項



- (注)
- 分散型仮想スイッチ (DVS) または Cisco Nexus 1000v (NK1v) の使用はオプションであり、必須の手順ではありません。
  - vMotion ネットワークの DVS は、環境に vSphere の Enterprise Plus ライセンスが設定されている場合にのみ使用できます。
  - 特定の時点で 2 つのスイッチのどちらかだけを使用できます。
  - Hyperflex と Nexus 1000v の間で Quality of Service (QoS) ポリシーが競合する可能性があります。HyperFlex ポリシーに従って N1Kv の QoS クラスが設定されていることを確認する必要があります。『[Network and Storage Management Guide](#)』の「*Creating a QoS Policy*」を参照してください。
  - N1Kv スイッチを導入する場合は、HyperFlex ホスト間のトラフィックが安定した状態で FI 上をローカルに流れるように、説明に従って設定を適用します。正確に設定しない場合、ほとんどのトラフィックがアップストリームスイッチを通過して遅延が発生する可能性があります。このシナリオを回避するには、ストレージコントローラ、管理ネットワーク、および vMotion ポートグループがアクティブ/スタンバイで設定され、フェールオーバーが有効になっていることを確認してください。
1. UCS Manager を使用して、[ネットワーク制御ポリシー (Network Control Policies)] の [リンク ステータス (link status)] を設定します。詳細については、『[Cisco UCS Manager GUI Configuration Guide](#)』の「Configuring Network Control Policy」のセクションを参照してください。
  2. vCenter で vSwitch プロパティを設定します。
    - a. [ネットワーク障害検出 (Network Failure Detection)] を [リンク ステータスのみ (Link Status only)] に設定します。
    - b. [フェールバック (Failback)] を [はい (Yes)] に設定します。詳細については、『[Cisco UCS Manager VM-FEX for VMware Configuration guide](#)』の「Configuring the VM-FEX for VMware」のセクションを参照してください。

分散型スイッチにより、各ノードで同じ設定が確実に使用されます。こうしてトラフィックに優先順位を付けることができ、アクティブな vMotion トラフィックがないときに、使用可能な帯域幅を他のネットワーク ストリームで活用できるようになります。

HyperFlex (HX) Data Platform では、非 HyperFlex 依存ネットワークに分散型仮想スイッチ (DVS) ネットワークを使用できます。

このような非 HX 依存ネットワークには以下のものが含まれます。

- VMware vMotion ネットワーク
- VMware アプリケーション ネットワーク

HX Data Platform には、次のネットワークが標準的な vSwitch を使用するという依存関係があります。

- vswitch-hx-inband-mgmt : ストレージコントローラ管理ネットワーク
- vswitch-hx-inband-mgm : 管理ネットワーク
- vswitch-hx-storage-data : ストレージハイパーバイザデータネットワーク
- vswitch-hx-storage-data : ストレージコントローラデータネットワーク

HX Data Platform のインストール時に、すべてのネットワークで標準 vSwitch ネットワークが設定されます。ストレージクラスタを設定した後、非 HX 依存ネットワークを DVS ネットワークに移行することができます。次に例を示します。

- vswitch-hx-vm-network : VM ネットワーク
- vmotion : vmotion pg

vMotion ネットワークを分散型仮想スイッチに移行する方法の詳細については、『[Network and Storage Management Guide](#)』の「*Migrating vMotion Networks to Distributed Virtual Switches (DVS) or Cisco Nexus 1000v (N1Kv)*」を参照してください。

## HX Data Platform 上での vCenter のホスト

HyperFlex クラスタ上で vCenter の展開をサポートする場合、いくつかの制約があります。詳細については、『[How to Deploy vCenter on the HX Data Platform](#)』テクニカル ノートを参照してください。

## AMD GPU の展開

AMD FirePro S7150 シリーズ GPU は HX240c M5/M6 ノードでサポートされます。これらのグラフィックアクセラレータでは、非常に安全な高いパフォーマンス、そしてコスト効率の良い VDI 展開を有効にします。HyperFlex に AMD GPU を展開するには、次の手順に従います。

ステップ	アクション	手順の説明
1	サーバに接続されているサービスプロファイルの BIOS ポリシーを変更します。	<a href="#">サポートされるすべての GPU に関する要件：メモリマップド I/O 4 GB 以上</a>
2	サーバに GPU カードをインストールします。	<a href="#">GPU カードのインストール</a>
3	サーバの電源をオンにして、GPU がサーバの Cisco UCS Manager インベントリに表示されることを確認します。	—

ステップ	アクション	手順の説明
4	AMD GPU カードの vSphere インストールバンドル (VIB) をインストールして、再起動します。	<a href="#">Cisco ソフトウェア ダウンロード</a> から、VMware ESXi 上の AMD 用の C シリーズ スタンドアロンファームウェア/ソフトウェアバージョンバンドル 3.1(3) の最新ドライバ ISO を含むインベントリリストをダウンロードします。
5	VM 設定を使用してクラスタ上で Win10 VM を作成します。	<a href="#">対象の仮想マシンの指定</a>
6	各 ESXi ホストで、MxGPU.sh スクリプトを実行して GPU を設定し、GPU から仮想機能を作成します。	<a href="#">MxGPU セットアップ スクリプトの使用</a>
7	前のステップで作成した仮想機能 (VF) を Win10 Vm に割り当てます。	—



## 第 9 章

# 複数の HX クラスタの設定

- [複数のクラスタの設定 \(155 ページ\)](#)

## 複数のクラスタの設定

複数の HyperFlex クラスタを同じ UCS ドメイン (ファブリック インターコネクトのペア) の下に共存させることができます。次のガイドラインに従い、ドメインに接続されているすべての機器に対して、スムーズに運用できるようにする必要があります。



- (注) 2つの異なる HX リリースの HX クラスタを同じ UCSM ドメインで使用する構成は、必要なサーバー ファームウェア バンドルが UCSM インフラストラクチャ リリースでサポートされている限りサポートされます。HXDP リリースは、リリース ノートごとに UCSM サーバー ファームウェア バンドルにマッピングされます。UCSM インフラストラクチャのリリースには依存しません。

### 推奨事項

- 標準 HXDP ライセンスを使用する場合、コンピューティング専用ノードの数は、コンバインド ノードの数以下にする必要があります。エンタープライズ HXDP ライセンスでは、コンバインド ノードに対して、最大 2:1 比のコンピューティングを使用できます。
- 新しい HyperFlex クラスタを作成するには、第 2 章に示されている要件をすべて満たしていることを確認してください。また、第 4 章に示されているプロセスに従ってください。
- HX クラスタのすべてのノードは、同じポリシーとサービス プロファイルを参照する必要があります。



- (注) HyperFlex サービス プロファイル テンプレートの編集は推奨されません。
- 各 HX クラスタの一意的な名前を割り当てます。

- 各 HX クラスタは、インストールの一部として固有のサブ組織に作成されます。この階層は、固有のポリシーがクラスタごとに作成されるようにするため、変更しないでください。
- 各クラスタは、固有のストレージデータ VLAN を使用して、すべてのストレージトラフィックを分離しておく必要があります。複数のクラスタにわたってこの VLAN を再利用することは推奨されません。
- Cisco では、ストレッチクラスタを含む、ファブリック インターコネクต์に接続されたクラスタごとに固有のストレージデータ VLAN が必要です。このようなデプロイメントでのストレージデータへの共有 VLAN の使用は、クラスターの停止につながる可能性があるため、サポートされていません。

他のデプロイメントタイプでは、すべてのストレージトラフィックを分離しておくために、クラスタごとに一意のストレージデータ VLAN を使用することを強くお勧めします。複数のクラスタに同じストレージデータ VLAN を使用している場合は、適切なネットワーク分離を確認してください。適切なネットワーク分離なしで複数のクラスターで同じストレージデータ VLAN を使用することはサポートされていません。

- VLAN (管理およびゲスト トラフィック VLAN など) を再利用する場合は、UCSM にすでに存在していても、VLAN ごとに新しい固有の VLAN 名を作成します。これにより、そのドメイン内の他のクラスタやサーバが中断されることはなくなります。
- 互換性のある Cisco UCS Manager と Cisco HyperFlex リリースを選択していることを確認します。

最新の互換性マトリックスについては、『[Release Notes for Cisco HX Data Platform](#)』のソフトウェアバージョンの表を参照してください。

- 同じ Cisco HX データ プラットフォーム インストーラを使用して別の vCenter に 2 番目のクラスタを設定する前に、ブラウザのキャッシュをクリアしてください。これにより、古いクラスタの IP アドレスがキャッシュされ展開が失敗するなどの問題が回避されます。



- 
- (注) トラフィックに応じて、さらにアップリンク ポートを追加する必要がある場合があります。
- 



- 
- (注) ファブリック インターコネクต์の同じペアに接続されている複数のクラスタ間で、同じ VLAN を使用することができます (管理、vMotion、VM ゲスト VLAN など)。これは、IP が重複しない限り可能です。ただし、ストレージトラフィックが安全に分離されるように、クラスタごとに HX ストレージ VLAN を異なる状態に保つことを推奨します。ベストプラクティスに対してストレージ VLAN を再利用する場合は、IP の重複を避けるために細心の注意をしてください。重複 IP があると、別のクラスタの既存のストレージトラフィックが中断される可能性があります。
-



---

**ステップ 1** HX Data Platform インストーラにログインします。

**ステップ 2** 標準クラスタの [Create Cluster] ワークフローに従って、追加のクラスタを作成します。詳細については、[Cisco HyperFlex Systems の設定 \(59 ページ\)](#) を参照してください。

---





## 第 10 章

# Cisco HyperFlex システム クラスタの展開

- クラスタ拡張ガイドライン (159 ページ)
- M4/M5/M6 クラスタを拡張する場合の前提条件 (161 ページ)
- 混合クラスタ展開のガイドライン - Cisco HX リリース 5.0(x) (161 ページ)
- 混在クラスタ拡張中の手順 (162 ページ)
- コンバージド (HX220c/HX240c) ノードを追加するための前提条件 (163 ページ)
- コンバージドノードの準備 (164 ページ)
- 既存のクラスタにコンバージドノードを追加する (164 ページ)
- コンピューティング専用ノードを追加するための前提条件 (171 ページ)
- コンピューティング専用ノードの準備 (173 ページ)
- 既存のクラスタにコンピューティング専用ノードを追加する (176 ページ)
- クラスタ拡張の障害の解決 (182 ページ)
- ロジカルアベイラビリティゾーン (182 ページ)

## クラスタ拡張ガイドライン

クラスタを拡張する前に、これらのガイドラインを確認してください。



- (注) LAZ が設定されている場合 (サイズ 8 以上のクラスタではデフォルトで有効)、拡張を進める前に [ロジカルアベイラビリティゾーン \(182 ページ\)](#) を確認してください。
- レプリケーションが設定済みの場合は、アップグレード、拡張、またはクラスタメンテナンスを実行する前に、レプリケーションを一時停止モードにしてください。アップグレードや拡張、クラスタのメンテナンスが完了した後、レプリケーションを再開します。タスクを実行するローカルクラスタとの間でレプリケーションが設定されているすべてのクラスタで、一時停止と再開を実行します。
  - RESTful API を使用してクラスタ拡張を実行する場合は、タスクの実行時間が予想以上に長くなる場合があります。

- ESXi インストールは、M4 コンバージド ノードの SD カードおよび M5/M6 コンバージド ノードの M.2 SATA SSD でサポートされています。コンピューティング専用ノードの場合、ESXi インストールは SD カード、SAN ブート、フロントアクセス対応 SSD/HDD、または M.2 SSD (UCS-MSTOR-M2 コントローラを使用) でサポートされています。コンピューティング専用ノードでは、USB フラッシュへの ESXi のインストールはサポートされていません。



(注) HW RAID M.2 (UCS-M2-HWRAID および HX-M2-HWRAID) は、HX Data Platform リリース 4.5(1a) 以降でサポートされるブート設定です。

- 検出されたクラスタをクリックして、3.5x またはそれ以前のリリースの標準 ESX クラスタの拡張を続行します。そうしないとエラーになります。
- 拡張ワークフローの中でコントローラ VM の管理ログイン情報のみを使用します。管理以外の他のクレデンシャルを使用すると、拡張に失敗する可能性があります。
- サポートされていないドライブまたはカタログのアップグレードに関するエラーが表示された場合は、[互換性カタログ](#) を参照してください。

• HX リリース 4.0(2e) 以降では、Intersight を介して 3 ノードで ESXi ベースの 10/25 GbE HyperFlex Edge クラスタを拡張できます。

HX リリース 5.0(1b) 以降では、Intersight を介して 2 ノードで ESXi ベースの 10/25 GbE HyperFlex Edge クラスタを拡張できます。

HyperFlex エッジクラスタの拡張は、Intersight を使用して展開されたクラスタの場合のみサポートされます。Intersight を使用したエッジクラスタの拡張は、HyperFlex OVA インストーラを介して展開されたクラスタではサポートされていません。

すべての要件については、Intersight のドキュメントを参照してください：[クラスタ拡張要件](#)

## ESXi インストール ガイドライン

1. コンピューティング ノードのブート ポリシーを変更します。

M5/M6 サーバの HyperFlex ストレッチ クラスタ コンピューティング専用ノードのテンプレートおよびブート ポリシーを変更するには:

1. テンプレートの複製
2. コンピューティング M5/M6 ノードにフラッシュ カードがない場合、ローカルブート ポリシーから Flex flash のチェックを外します。
3. 適切な WWPN で SAN ブートをブート順序に追加します。

2. DPI 拡張ワークフローを開始します。

3. プロンプトされる場合、ISO イメージを使用して ESXi をインストールします。
4. DPI 拡張ワークフローに戻り、ESXi インストール ワークフローを完了します。



- (注) Hypervisor 設定が失敗し、SOL ログイングの障害メッセージが表示される場合、ルートおよびデフォルト パスワードを使用して SSH で インストーラ CLI にアクセスし、ESXi ハイパーバイザを設定します。そして、高度なインストーラを実行し、**[HX Storage Software (HX ストレージ ソフトウェア)]** および **[Expand Cluster (クラスタの拡張)]** チェック ボックスをチェックして、ESXi インストール プロセスを続行します。

## M4/M5/M6 クラスタを拡張する場合の前提条件

M4/M5/M6 クラスタ内でクラスタ拡張を開始する前に、次のタスクを実行する必要があります。

- **Hypercheck ヘルス チェック ユーティリティ**: アップグレードする前に、Hypercheck クラスタでこの予防的ヘルス チェック ユーティリティを実行することを推奨します。これらのチェックにより、注意が必要なエリアがすぐに見やすくなり、シームレスなアップグレードエクスペリエンスを保証します。Hypercheck のインストールと実行方法の完全な手順の詳細については、『[Hyperflex 健全性および事前アップグレード チェック ツール](#)』を参照してください。
- HX クラスタと UCS Manager を、展開に適した推奨リリースにアップグレードします。詳細については、[Cisco HyperFlex 推奨ソフトウェア リリースおよび要件ガイド](#)を参照してください。
- 拡張ワークフローを実行するには、一致するリリース HX データ プラットフォーム インストーラ (クラスタと同じリリース) をダウンロードして展開します。
- M4 サーバ: 既存の M4 サーバファームウェアを 3.2(1) 以降のファームウェアにアップグレードします。
- vCenter を 6.5 以降にアップグレードします。vCenter 6.5 がないと、Broadwell EVC モードを有効にできません。vCenter のアップグレードのみが必要です。ESXi については、VMware ソフトウェア相互運用性マトリクスに従って古いバージョンのままにすることができます。EVC モードをオフにしたまま先に進むことはできず、将来的に運用上の問題が生じる可能性があります。

## 混合クラスタ展開のガイドライン - Cisco HX リリース 5.0(x)

- M6 コンバージド ノードを使用して既存の M4、M5 または M4 + M5 クラスタを拡張する操作はサポートされます。

- M4 または M5 コンバージド ノードを使用して既存の M6 クラスタを拡張する操作はサポートされません。
- M4 または M5 または M6 コンバージド ノードを持つ既存の混合 M4/M5/M6 クラスタの展開がサポートされています。
- サポートされているコンピューティング専用ノードを追加することは、HX Data Platform 5.0 またはそれ以降のインストーラを使用した M4、M5、混合 M4/M5/M6 クラスタすべてで許可されています。組み合わせの例を以下に示しますが、他にもさまざまな組み合わせが可能です。
- 混在クラスタを作成する場合は、拡張ワークフローのみがサポートされます。混在 M4/M5/M6 サーバを使用した初期クラスタの作成はサポートされません。
- すべてのサーバは、クラスタのフォームファクタ (220/240)、タイプ (Hybrid/AF)、セキュリティ機能 (非 SED のみ) およびディスク設定 (数量、容量、非 SED) と一致する必要があります。
- HX220c M6 は、HX220 M4 と混在する場合、最大 6 台の容量ディスク (2 つのディスクロットは空の状態) を使用します。
- HX240c M6 は、M5 または M4 ノードを持つクラスタで組み合わせた場合、追加のロットを使用できません。
- Intel と AMD M6 の混在はサポートされていません。

## 混在クラスタ拡張中の手順

- 検証手順では、拡張が開始される前に EVC チェックが実行されます。表示される指示に従い、既存のクラスタの EVC モードをこの時点で手動で有効にしてください。



**注意** 警告が出されたときに EVC を有効にしない場合、後の時点で、ストレージクラスタおよび関連するすべての VM を完全にシャットダウンする必要が生じます。この警告をスキップしないでください。

- vCenter で EVC モード設定を実行した後、検証をやり直してください。
- クラスタ拡張で 2 回目の検証が行われ、拡張が続行されます。

## コンバージド (HX220c/HX240c) ノードを追加するための前提条件

コンバージドノードは、クラスター作成後に HyperFlex クラスターに追加可能です。コンバージドノード上のストレージは、自動的にクラスターのストレージ容量に追加されます。

既存のストレージクラスターへのコンバージドノードの追加を開始する前に、次の前提条件が満たされていることを確認します。

- ストレージクラスターの状態が正常であることを確認します。
- 新しいノードが、「インストールの前提条件」に記載されたシステム要件（ネットワーク要件とディスク要件を含む）を満たしていることを確認します。
- 新しいノードがストレージクラスター内の他のノードと同じ設定を使用していることを確認します。これには、VLANIDとスイッチタイプ（vSwitchかどうか）、外部スイッチVLANタギング（EST）を使用したVLANタギング、仮想スイッチタギング（VST）を使用したVLANタギング、または仮想分散型スイッチが含まれます。



(注) ストレージクラスターが容量不足の状態にある場合は、新しいノードを追加すると、システムが自動的にストレージクラスターを再調整します。これは、24時間ごとに実施される再調整とは別の追加的な動作です。

- 追加するノードが、同じモデル（HX220またはHX240）タイプ（ハイブリッドまたはオールフラッシュ）および同じディスク設定（SEDまたはSED以外）になっていることを確認します。加えて、容量ディスクの数が既存のクラスターノードの数と一致することを確認します。
- HyperFlex クラスターですでに使用されているものとは異なるCPUファミリーを持つノードを追加するには、EVCを有効にします。詳細については、『Cisco HyperFlex Systems インストールガイド (VMware ESXi向け)』の「混在CPUを伴うクラスターの設定」の項を参照してください。
- ノードのソフトウェアリリースが、Cisco HX Data Platform バージョン、ESXi バージョン、vCenter バージョンと一致していることを確認します。ソフトウェアリリースを特定するには、vCenterの[ストレージクラスターの概要 (Storage Cluster Summary)] タブに移動し、最上部のセクションで [HX Data Platform のリリース (HX Data Platform release)] を確認します。必要に応じてアップグレードします。



(注) クラスタをアップグレードする場合は、クラスタで実行されている HXDP の現在のリリースに一致する新しいインストーラ VM をダウンロードしてインストールする必要があります。

- 新しいノードで少なくとも 1 つの有効な DNS と NTP サーバが設定されていることを確認します。
- SSO または自動サポートを使用する場合は、ノードが SSO サービスと SMTP サービス用に設定されていることを確認します。
- HX Data Platform インストーラおよび既存のクラスタ管理 IP アドレス間で ping するために ICMP が許可されていること。

## コンバージドノードの準備

コンバージドノードを既存のストレージクラスタのハードウェアとネットワークに接続します。

## 既存のクラスタにコンバージドノードを追加する



(注) RESTful API を使用してクラスタ展開を実行する場合、そのタスクに想定よりも時間がかかることがあります。

**ステップ 1** Cisco HX Data Platform インストーラ を起動します。

- Web ブラウザで、HX データ プラットフォーム インストーラ VM の IP アドレスまたはノード名を入力します。[承認 (Accept)] または [続行 (Continue)] をクリックして SSL 証明書エラーをバイパスします。Cisco HX Data Platform インストーラ のログイン ページが表示されます。ログイン画面の右下隅で HX データ プラットフォーム インストーラ **ビルド ID** を確認します。
- ログイン ページで、次のクレデンシャルを入力します。

[ユーザ名 (Username) ] : root

[パスワード (Password) ] (デフォルト) : Cisco123

(注) システムに同梱されているデフォルトのパスワード Cisco123 は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。



- c) EULA の内容を読み、[利用規約に同意します (I accept the terms and conditions)] チェックボックスをオンにして、[ログイン (Login)] をクリックします。

**ステップ 2** [ワークフロー (Workflow)] ページで [クラスター展開 (Cluster Expansion)] を選択します。

**ステップ 3** [クレデンシャル (Credentials)] ページで、次のフィールドに値を入力します。

クラスターを作成するには、必要な構成データが格納された *JSON* コンフィギュレーション ファイルをインポートできます。JSON ファイルをインポートする場合は、次の 2 つのステップを行います。インポートしない場合は、必須フィールドに手動でデータを入力できます。

- (注) 初回インストールの場合は、シスコの担当者に連絡して工場出荷時のプレインストール JSON ファイルを入手してください。
- [ファイルの選択 (Select a file)] をクリックし、該当する *JSON* ファイルを選択して構成をロードします。[構成を使用 (Use Configuration)] を選択します。
  - インポートされた値が Cisco UCS Manager の値と異なる場合には、[インポートされた値を上書きする (Overwrite Imported Values)] ダイアログボックスが表示されます。[検出された値を使用 (Use Discovered Values)] を選択します。

フィールド	説明
<b>UCS Manager クレデンシャル</b>	
UCS Manager のホスト名	UCS Manager の FQDN または IP アドレス たとえば、 <i>10.193.211.120</i> とします。
ユーザ名	<管理者> ユーザ名
パスワード	<管理者> パスワード。
<b>vCenter クレデンシャル</b>	
vCenter Server	vCenter Server の FQDN または IP アドレス たとえば、 <i>10.193.211.120</i> とします。  (注) <ul style="list-style-type: none"> <li>クラスターを動作可能にするには、その前に vCenter Server を準備する必要があります。</li> <li>vCenter のアドレスとクレデンシャルには、vCenter に対するルート レベルの管理者権限が必要です。</li> <li>ネストされた vCenter を構築する場合、vCenter Server の入力オプションです。詳細については <a href="#">Nested vCenter TechNote</a> を参照してください。</li> </ul>
ユーザ名	<管理者> ユーザ名 たとえば、 <i>administrator@vsphere.local</i> とします。

フィールド	説明
[管理パスワード (Admin Password) ]	<root> パスワード。
ハイパーバイザのクレデンシャル	
管理者ユーザ名	<管理者> ユーザ名。 これはファクトリ ノードのルートです。
[管理パスワード (Admin Password) ]	<root> パスワード。 デフォルトのパスワードは、ファクトリ ノードの Cisco123 です。  (注) システムに同梱されているデフォルトのパスワード Cisco123 は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

**ステップ 4** [続行 (Continue) ]をクリックします。[クラスタ展開の設定 (Cluster Expand Configuration) ]ページが表示されます。拡張する HX クラスタを選択します。

拡張する HX クラスタが見つからない場合、もしくはクラスタのロードに時間がかかる場合、[管理 IP アドレス (Management IP Address) ]フィールドにクラスタ管理アドレスの IP を入力します。

**ステップ 5** [サーバの選択 (Server Selection) ]ページの [関連付けなし (Unassociated) ]タブには関連付けられていない HX サーバのリストが表示され、[関連付け済み (Associated) ]タブには検出されたサーバのリストが表示されます。[関連付けなし (Unassociated) ]タブで、HyperFlex クラスタに含めるサーバを選択します。

HX サーバがこのリストに表示されていない場合は、Cisco UCS Manager を調べて、HX サーバが検出されていることを確認します。

サーバごとに、[アクション (Actions) ] ドロップダウンリストのを使用して、以下を設定できます。

- **[KVM コンソールの起動 (Launch KVM Console) ]**: HX データ プラットフォーム インストーラ から直接 KVM コンソールを起動するには、このオプションを選択します。
- **[サーバの関連付け解除 (Disassociate Server) ]**: サーバからサービスプロファイルを削除するには、このオプションを選択します。

(注) 関連付けられていないサーバがない場合は、次のエラー メッセージが表示されます。

```
No unassociated servers found. Please login to UCS Manager and ensure server ports are enabled.
```

[サーバポートの設定 (Configure Server Ports) ] ボタンを使用すると、新しい HX ノードをすべて検出できます。通常は、構成の開始前から Cisco UCS Manager でサーバポートが構成されています。

**ステップ 6** [続行 (Continue) ]をクリックします。[UCSM の設定 (UCSM Configuration) ]ページが表示されます。

(注) 最初にJSONファイルをインポートした場合、既存のHXクラスターから得られた必要な設定データが **[Credentials]** ページに取り込まれているはずですが、この情報は、既存のクラスター構成に一致している必要があります。

**ステップ 7** **[続行 (Continue)]** をクリックします。**[ハイパーバイザの設定 (Hypervisor Configuration)]** ページが表示されます。次のフィールドに入力します。

**注目** 再インストールの場合や、ESXi ネットワーキングがすでに完了している場合は、この手順で説明したフィールドの入力を省略できます。

フィールド	説明
<b>共通ハイパーバイザ設定の構成</b>	
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、255.255.0.0 とします。
<b>[ゲートウェイ (Gateway)]</b>	ゲートウェイの IP アドレス。 たとえば、10.193.0.1 とします。
<b>[DNSサーバ (DNS Server(s))]</b>	DNS サーバの IP アドレス。 DNS サーバを使用しない場合、HX Data Platform インストーラの <b>[クラスターの設定 (Cluster Configuration)]</b> ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。  (注) 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。
<b>ハイパーバイザ設定</b>	
<b>[IP アドレスとホスト名を連続的に入力する (Make IP Addresses and Hostnames Sequential)]</b> を選択して、IP アドレスが順番に並ぶようにしてください。  (注) ドラッグ アンド ドロップ操作を使用してサーバの順番を並び替えることができます。	
名前	サーバ名。
シリアル	サーバのシリアル番号。
スタティック IP アドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。
ホスト名	ホスト名フィールドを空のままにしないでください。

**ステップ 8** [続行 (Continue)] をクリックします。[IP アドレス (IP Addresses)] ページが表示されます。[コンピューティング サーバの追加] または [コンバージド サーバの追加] をクリックして、さらにコンピューティング または コンバージド サーバを追加できます。

[IP アドレスを連続させる (Make IP Addresses Sequential)] を選択して、IP アドレスを順番に並べるようにしてください。IP アドレスには、ネットワークがデータ ネットワークと管理ネットワークのどちらに属するかを指定します。

各 HX ノードでは、ハイパーバイザ管理 IP アドレスとデータ IP アドレスに関する次のフィールドに値を入力します。

フィールド	説明
管理ハイパーバイザ	ESXi ホストとストレージコントローラ間のハイパーバイザ管理ネットワーク接続を処理するスタティック IP アドレスを入力します。
管理ストレージコントローラ	ストレージコントローラ VM とストレージクラスタの間の HX Data Platform ストレージコントローラ VM 管理ネットワーク接続を処理する静的 IP アドレスを入力します。
Data Hypervisor	ESXi ホストとストレージコントローラ間のハイパーバイザデータネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージコントローラ	ストレージコントローラ VM とストレージクラスタの間の HX Data Platform ストレージコントローラ VM データ ネットワーク接続を処理する静的 IP アドレスを入力します。
<p>[ハイパーバイザ (管理) (Hypervisor (Management)) ]、[ストレージコントローラ VM (管理) (Storage Controller VM (Management) ) ]、[ハイパーバイザ (データ) (Hypervisor (Data) ) ]、および [ストレージコントローラ VM (データ) (Storage Controller VM (Data) ) ] 列の最初の行に IP アドレスを入力すると、HX データ プラットフォーム インストーラによって、他のノードのノード情報に増分自動入力 that 適用されます。ストレージクラスタ内のノードの最小数は 3 です。それより多くのノードがある場合は、[追加 (Add) ] ボタンを使用して、アドレス情報を指定します。</p> <p>(注) コンピューティング専用ノードは、ストレージクラスタを作成してからでないと追加できません。</p>	

フィールド	説明
<b>コントローラVMパスワード</b>	<p>デフォルトの管理者ユーザー名とパスワードがコントローラ VM に適用されます。VM は、コンバージド ノードとコンピューティング専用ノードのすべてにインストールされます。</p> <p><b>重要</b></p> <ul style="list-style-type: none"> <li>• コントローラ VM またはコントローラ VM のデータストアの名前を変更することはできません。</li> <li>• すべてのコントローラ VM に同じパスワードを使用します。異なるパスワードの使用はサポートされていません。</li> <li>• 1つの大文字、1つの数字、1つの特殊文字を含み、合計で少なくとも 10 文字になる複雑なパスワードを指定してください。</li> <li>• コントローラ VM と、作成される HX クラスターには、ユーザ定義のパスワードを指定できます。パスワードに使用できる文字と形式に関する制限事項については、『Cisco HX Data Platform Management Guide』のセクション「Guidelines for HX Data Platform Special Characters」を参照してください。</li> </ul>
<b>詳細設定</b>	
<b>ジャンボ フレーム</b> [ジャンボ フレームを有効化 (Enable Jumbo Frames) ] チェックボックス	<p>ホスト vSwitches と vNIC、および各ストレージコントローラ VM 上のストレージデータ ネットワークの MTU サイズを設定する場合は、このチェックボックスをオンにします。</p> <p>デフォルト値は <b>9000</b> です。</p> <p>(注) MTU サイズを <b>9000</b> 以外の値に設定するには、Cisco TAC にご連絡ください。</p>
<b>ディスク パーティション</b> [ディスク パーティションのクリーンアップ (Clean up Disk Partitions) ] チェックボックス	<p>ストレージクラスターに追加されたすべてのノードから既存のデータおよびパーティションをすべて削除するには、オンにします。保持する必要があるデータはすべてバックアップする必要があります。</p> <p><b>重要</b> 工場で準備されたシステムの場合は、このオプションを選択しないでください。工場で準備されたシステムのディスクパーティションは正しく設定されています。手動で準備されたサーバで、既存のデータとパーティションを削除するにはこのオプションを選択します。</p>

**ステップ 9** [スタート (Start) ] をクリックします。[進捗状況 (Progress) ] ページに、さまざまな設定タスクの進捗状況が表示されます。

(注) vCenter クラスターで EVC が有効になっている場合、展開プロセスが失敗し、「The host needs to be manually added to vCenter」というメッセージが出されます。展開操作を正常に実行するには、次のようにします。

- vSphere クライアント に追加する ESXi ホストにログインします。
- コントローラ VM の電源をオフにします。
- vSphere Web クライアント でホストを vCenter クラスターに追加します。
- HX データ プラットフォーム インストーラ で、[Retry Deploy] をクリックします。

**ステップ 10** クラスター展開が完了したら、[HyperFlex Connect を起動 (Launch HyperFlex Connect)] をクリックしてストレージクラスターの管理を開始します。

(注) 既存のストレージクラスターにノードを追加した場合、スケジュールされた時間に自動再調整が行われるまでの間、クラスターの HA 復元力は引き続き元のストレージクラスターと同じです。

再調整は通常、24 時間の期間でスケジュールされ、ノードの障害発生後の 2 時間後、またはストレージクラスターの領域がなくなったときに行われます。

スケジュールされた時間よりも前にストレージクラスターを再調整するために、ストレージクラスターの再調整コマンドを手動で開始するために、次の手順を実行します。

1. ストレージクラスター コントローラ VM コマンドラインから、`# stcli rebalance start --force` コマンドを実行します。
2. リバランスステータスをモニタするには、`stcli rebalance status` コマンドを実行します。

**ステップ 11** HyperFlex `hx_post_install` スクリプトを使用して、または手動でクラスター内の他のノードと一致するように、必要な VM ネットワーク ポート グループと vMotion vmkernel インターフェイスを作成します。

- a) HyperFlex クラスター管理 IT への SSH。
- b) `admin` ユーザとしてログインします。
- c) `hx_post_install` コマンドを実行します。
- d) vMotion と VM ネットワークの作成から始まる画面上の指示に従います。設定ステップはオプションです。

**ステップ 12** 新しいノードがストレージクラスターに追加された後、高可用性 (HA) サービスがリセットされ、HA が追加されたノードを認識できるようになります。

- a) vCenter にログインします。
- b) vSphere Web Client で、[Home] > [vCenter] > [Inventory Lists] > [Hosts and Clusters] > [vCenter] > [Server] > [Datacenter] > [Cluster] > [Host] でホストに移動します。
- c) 新規ノードを選択します。
- d) 右クリックして [Reconfigure for vSphere HA] を選択します。

# コンピューティング専用ノードを追加するための前提条件

クラスタ作成後にコンピューティング専用ノードを HyperFlex クラスタに追加できます。これを追加すると、追加的なコンピューティングリソースが提供されます。Cisco UCS サーバは、クラスタにストレージ容量をもたらさないため、キャッシュドライブまたは永久ドライブを装備する必要はありません。

コンピューティング専用ノードを追加する前に、次の前提条件が満たされていることを確認します。

- ストレージクラスタの状態が正常であることを確認します。
- 新しいノードが、ネットワークやディスクの要件などインストールの前提条件に記載されているコンピューティング専用システム要件を満たしていることを確認します。
- サービス プロファイルを関連付けた後に、ESXi ハイパーバイザをインストールします。
- 新しいノードがストレージクラスタ内の他のノードと同じ設定を使用していることを確認します。これには、VLANID とスイッチタイプ (vSwitch かどうか)、外部スイッチ VLAN タギング (EST) を使用した VLAN タギング、仮想スイッチ タギング (VST) を使用した VLAN タギング、または仮想分散型スイッチが含まれます。



(注) ストレージクラスタが容量不足の状態にある場合は、新しいノードを追加すると、システムが自動的にストレージクラスタを再調整します。これは、24 時間ごとに実施される再調整とは別の追加的な動作です。

- 追加する新しいノードに、HX クラスタ内ですでに使用されているものとは異なる CPU ファミリが使用されている場合は、EVC を有効にします。詳細については、『*Cisco HyperFlex Systems インストール ガイド (VMware ESXi 向け)*』の「混在 CPU を伴うクラスタの設定」の項を参照してください。
- ノードのソフトウェア リリースが、Cisco HX Data Platform リリース、ESXi リリース、vCenter リリースと一致していることを確認します。ソフトウェア リリースを特定するには、vCenter の [ストレージクラスタの概要 (Storage Cluster Summary)] タブに移動し、最上部のセクションで [HX Data Platform バージョン (HX Data Platform version)] を確認します。必要に応じてアップグレードします。
- 新しいノードで少なくとも 1 つの有効な DNS と NTP サーバが設定されていることを確認します。
- SSO または自動サポートを使用する場合は、ノードが SSO サービスと SMTP サービス用に設定されていることを確認します。

- ESXi インストールは、M4 コンバージド ノードの SD カードおよび M5/M6 コンバージド ノードの M.2 SATA SSD でサポートされています。コンピューティング専用ノードの場合、ESXi インストールは SD カード、SAN ブート、フロントアクセス対応 SSD/HDD、または M.2 SSD (UCS-MSTOR-M2 コントローラを使用) でサポートされています。コンピューティング専用ノードでは、USB フラッシュへの ESXi のインストールはサポートされていません。



(注) HW RAID M.2 (UCS-M2-HWRAID および HX-M2-HWRAID) は、HX Data Platform リリース 4.5(1a) 以降でサポートされるブート設定です。

- ブートハードウェアに基づいてディスクおよびブートポリシーを自動的に検出および設定することで、コンピューティング専用ノードが展開されました。

HX Data Platform リリース 4.5(1a) 以降、コンピューティング専用ノードは、インベントリされたブートハードウェアに基づいて、ディスクおよびブートポリシーの自動検出および設定を使用して展開されます。ユーザーは UCSM ポリシーを直接選択できません。代わりに、ブートデバイスは、サーバで検出された最初の受け入れ可能なブートメディアに基づいて自動的に決定されます。次の表に、M4/M5/M6 世代サーバの優先順位を示します。上から下に読むと、インベントリされたハードウェアに基づいて一致する最初のエントリがクラスター拡張時に自動的に選択されます。たとえば、単一の M.2 ブート SSD を備えた B200 コンピューティングノードで拡張する場合、次の表の 2 番目のルールは一致し、SPT の関連付けに使用されます。

リストされていないメカニズム (SAN ブートなど) を使用してサーバが起動された場合、**anyld** の包括的ポリシーが選択され、管理者は必要に応じて UCSM ポリシーとプロファイルを変更してサーバを起動できます。

表 6: M6 の優先順位

M6 の優先順位			
優先度 (Priority)	SPT 名	ブート デバイス	ディスク数
1	compute-nodes-m6-m2r1	M6 - M.2 - 2 ディスク	2
2	compute-nodes-m6-m2sd	M6 - M.2 - 1 ディスク	1
3	compute-nodes-m6-ldr1	MegaRAID コントローラ	2
4	compute-nodes-m6-anyld	M6 : 汎用	すべて



表 7: M5 の優先順位

M5 の優先順位			
優先度 (Priority)	SPT 名	ブート デバイス	ディスク数
1	compute-nodes-m5-m2r1	M.2 Raid	2
2	compute-nodes-m5-m2pch	PCH/Non-RAID M.2	1
3	compute-nodes-m5-sd	[FlexFlash]	2
4	compute-nodes-m5-ldr1	MegaRAID	2
5	compute-nodes-m5-sd	[FlexFlash]	1
6	compute-nodes-m5-anyld	その他の設定	いずれか (Any)

表 8: M4 の優先順位

M4 の優先順位			
優先度 (Priority)	SPT 名	ブート デバイス	ディスク数
1	compute-nodes-sd	[FlexFlash]	1 または 2
2	compute-nodes-anyld	その他の設定	いずれか (Any)

## コンピューティング専用ノードの準備

**ステップ 1** サポート対象の HX サーバであること、およびサーバの要件を満たしていることを確認します。詳細については、『*Cisco HyperFlex Systems インストールガイド (VMware ESXi 向け)*』の「ホスト要件」の項を参照してください。

**ステップ 2** Cisco UCS Manager にログインします。

- ブラウザを開き、ストレージクラスタ ネットワークのファブリック インターコネク ト用の Cisco UCS Manager アドレスを入力します。
- [**UCS Manager の起動 (Launch UCS Manager)**] ボタンをクリックします。
- プロンプトが表示された場合は、Java をダウンロードし、インストールして、受け入れます。
- 管理者クレデンシャルを使用してログインします。

[ユーザ名 (Username) ]: **admin**

[パスワード (Password) ]: <管理者パスワード>

**ステップ3** サーバを見つけて、ストレージクラスタと同じFIドメインにサーバが追加済みであること、承認されたコンピューティング専用モデルであることを確認します。互換性のあるコンピューティング専用ノードの詳細なリストについては、最新の『[Cisco HX Data Platform のリリース ノート](#)』を確認してください。

---

## HX Data Platform インストーラの確認

---

**ステップ1** ストレージクラスタに追加されるコンピューティングノードおよびストレージクラスタ内のすべてのノードと通信できる1つのノード上に、HX Data Platform インストーラがインストールされていることを確認します。

**ステップ2** HX Data Platform インストーラがインストールされていない場合は、「HX Data Platform インストーラの展開」を参照してください。

---

## UCS Manager を使用した コンピューティングのみ ノードへの HX プロファイルの適用

Cisco UCS Manager では、ネットワーク ポリシーが HX プロファイルにグループ化されます。HX インストーラは、コンピューティング専用ノードの自動サービスプロファイルアソシエーション（関連付け）を処理します。手動アソシエーションは不要です。

インストールが開始したら、UCS Manager でコンピューティング専用ノードのサービスプロファイルアソシエーションを監視してください。ESXiのインストールに進む前に、サーバが完全に関連付けられるまで待ちます。

---

## コンピューティング ノードへの VMware ESXi のインストール



**重要** 各コンピューティング専用ノード上に VMware ESXi をインストールします。

サポートされている ESXi のリリース Cisco HX Data Platform をインストールします。サポートされている ESXi バージョンのリストについては、『[Cisco HyperFlex Data Platform Release Notes](#)』を参照してください。

コンピューティング専用ノードに ESXi がすでにインストール済みの場合、Cisco HX カスタム イメージで再イメージ化する必要があります。

---

### 始める前に

必要なハードウェアとネットワークの設定が満たされていることを確認します。詳細については、『Cisco HyperFlex Systems インストール ガイド (VMware ESXi 向け)』の「インストールの前提条件」の項を参照してください。前の手順でサービスプロファイルの関連付けが完了していることを確認します。

- 
- ステップ 1** ESXi の HX カスタム イメージ を Cisco HyperFlex の Cisco.com ダウンロード サイト からダウンロード します。「ソフトウェアのダウンロード」を参照してください。
- Cisco UCS Manager を介してアクセス可能なネットワーク ロケーションを選択します。
- ステップ 2** Cisco UCS Manager にログインします。
- ステップ 3** Cisco UCS Manager からサーバーの KVM コンソールにログインします。
- ナビゲーション ウィンドウで、[サーバー (Servers)]>[サービス プロファイル (Service Profiles)]>[サブ組織 (Sub-Organizations)]>[hx-cluster] をクリックします。
  - [hx-cluster] を右クリックして、[KVM コンソール (KVM Console)] を選択します。
- ステップ 4** コンピューティング サーバの KVM パスに HX-Vmware.iso イメージをコピーします。
- 例：
- HX-Vmware-ESXi-60U3-5050593-Cisco-Custom-6.0.3.1.iso
- ステップ 5** KVM コンソールセッションから、[仮想メディア (Virtual Media)]>[マップ CD/DVD (Map CD/DVD)] を選択し、ESXi の HX カスタム イメージをマウントします。[マップ CD/DVD (Map CD/DVD)] オプションが表示されない場合は、まず仮想デバイスをアクティブにします。
- [仮想メディア (Virtual Media)]>[仮想デバイスのアクティブ化 (Activate Virtual Devices)] を選択します。
- これはポップアップ ウィンドウで開きます。
- [セッションの受け入れ (Accept the session)]>[適用 (Apply)] をクリックします。
- ステップ 6** [マップ CD/DVD (Map CD/DVD)] オプションから、HX-Vmware.iso ファイルの場所にマップします。
- HX-Vmware.iso ファイルを選択します。
  - [マップ デバイス (Map Device)] を選択します。
- プロセスが完了したら、マップされた場所にファイルがあることを示すチェック マークが付きます。マッピングされたファイルのフルネームには ESXi ビルド ID が含まれます。
- ステップ 7** コンピューティング サーバをリセットします。
- KVM コンソールで [リセット (Reset)] ボタンをクリックします。[OK] をクリックして確定します。
  - [電源の再投入 (Power Cycle)] を選択します。[OK] をクリックします。
- ステップ 8** HX-Vmware.iso ファイルを指すようにブート パスを変更します。
- F6** キーを押します。

- b) [起動選択の入力 (Enter boot selection) ]メニューから、矢印キーを使用して *Cisco vKVM-Mapped vDVD1.22* オプションを強調表示します。
- c) **Enter** キーを押して選択します。

これにより ESXi インストーラ ブートローダーが起動します。目的のブートタイプに基づいて3つのコンピューティング専用ノードオプション (SDカード、ローカルディスク、またはリモートディスク) のいずれかを選択します。**yes** (すべて小文字) を入力して選択を確定します。インストールの残りの部分は自動化されています。ESXi は数回、再起動します。警告が表示されて短い待機期間の後に自動的に消える場合は、正常な動作です。インストールが終了すると *ESXi DCUI* が完全に表示されるので、それまで待ちます。

**ステップ 9** 各 Cisco HyperFlex サーバに対してステップ 3 ~ 8 を繰り返します。

**ステップ 10** ESXi が完全にインストールされたら、[**続行 (Continue)** ] をクリックします。次に [**Hypervisor 設定の再試行 (Retry Hypervisor Configuration)** ] をクリックして、クラスタ拡張の残りの部分を完了します。

## 既存のクラスタにコンピューティング専用ノードを追加する

既存の HyperFlex システム クラスタに HyperFlex コンピューティング専用ノードを追加するには、次の手順を実行します。



(注) RESTful API を使用してクラスタ拡張を実行する場合は、タスクの実行時間が予想以上に長くなる場合があります。



(注) 既存のクラスタにコンピューティング専用ノードを追加した後、vmotion の vmk2 インターフェイスを手動で設定する必要があります。

**ステップ 1** Cisco HX Data Platform インストーラ を起動します。

- a) Web ブラウザで、HX データプラットフォーム インストーラ VM の IP アドレスまたはノード名を入力します。[**承認 (Accept)** ] または [**続行 (Continue)** ] をクリックして SSL 証明書エラーをバイパスします。Cisco HX Data Platform インストーラ のログインページが表示されます。ログイン画面の右下隅で HX データプラットフォーム インストーラ **ビルド ID** を確認します。
- b) ログイン ページで、次のクレデンシャルを入力します。

[**ユーザ名 (Username)** ] : root

[**パスワード (Password)** ] (デフォルト) : Cisco123

(注) システムに同梱されているデフォルトのパスワード `cisco123` は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

- c) EULA の内容を読み、**[利用規約に同意します (I accept the terms and conditions)]** チェックボックスをオンにして、**[ログイン (Login)]** をクリックします。

**ステップ 2** **[ワークフロー (Workflow)]** ページで **[クラスター展開 (Cluster Expansion)]** を選択します。

**ステップ 3** **[クレデンシャル (Credentials)]** ページで、次のフィールドに値を入力します。

クラスターを作成するには、必要な構成データが格納された *JSON* コンフィギュレーションファイルをインポートできます。JSON ファイルをインポートする場合は、次の2つのステップを行います。インポートしない場合は、必須フィールドに手動でデータを入力できます。

- (注) 初回インストールの場合は、シスコの担当者に連絡して工場出荷時のプレインストール JSON ファイルを入手してください。
- [ファイルの選択 (Select a file)]** をクリックし、該当する *JSON* ファイルを選択して構成をロードします。**[構成を使用 (Use Configuration)]** を選択します。
  - インポートされた値が Cisco UCS Manager の値と異なる場合には、**[インポートされた値を上書きする (Overwrite Imported Values)]** ダイアログボックスが表示されます。**[検出された値を使用 (Use Discovered Values)]** を選択します。

フィールド	説明
<b>UCS Manager クレデンシャル</b>	
UCS Manager のホスト名	UCS Manager の FQDN または IP アドレス たとえば、 <code>10.193.211.120</code> とします。
ユーザ名	<管理者> ユーザ名
パスワード	<管理者> パスワード。
<b>vCenter クレデンシャル</b>	
vCenter Server	vCenter Server の FQDN または IP アドレス たとえば、 <code>10.193.211.120</code> とします。  (注) <ul style="list-style-type: none"> <li>クラスターを動作可能にするには、その前に vCenter Server を準備する必要があります。</li> <li>vCenter のアドレスとクレデンシャルには、vCenter に対するルート レベルの管理者権限が必要です。</li> <li>ネストされた vCenter を構築する場合、vCenter Server の入力はオプションです。詳細については <a href="#">Nested vCenter TechNote</a> を参照してください。</li> </ul>

既存のクラスタにコンピューティング専用ノードを追加する

フィールド	説明
ユーザ名	<管理者> ユーザ名 たとえば、 <i>administrator@vsphere.local</i> とします。
[管理パスワード (Admin Password) ]	<root> パスワード。
ハイパーバイザのクレデンシャル	
管理者ユーザ名	<管理者> ユーザ名。 これはファクトリ ノードのルートです。
[管理パスワード (Admin Password) ]	<root> パスワード。 デフォルトのパスワードは、ファクトリ ノードの <i>Cisco123</i> です。  (注) システムに同梱されているデフォルトのパスワード <i>Cisco123</i> は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

**ステップ 4** [続行 (Continue) ]をクリックします。[クラスタ展開の設定 (Cluster Expand Configuration) ]ページが表示されます。拡張する *HX* クラスタを選択します。

拡張する *HX* クラスタが見つからない場合、もしくはクラスタのロードに時間がかかる場合、[管理 IP アドレス (Management IP Address) ]フィールドにクラスタ管理アドレスの IP を入力します。

**ステップ 5** [続行 (Continue) ]をクリックします。[サーバの選択 (Server Selection) ]ページが表示されます。[サーバの選択 (Server Selection) ]ページの [関連付け (Associated) ]タブに、接続済みのすべての *HX* サーバが一覧表示されます。それらを選択しないでください。[関連付けなし (Unassociated) ]タブで、クラスタに追加するサーバを選択します。

**ステップ 6** [続行 (Continue) ]をクリックします。[ハイパーバイザの設定 (Hypervisor Configuration) ]ページが表示されます。次のフィールドに入力します。

**注目** 再インストールの場合や、ESXi ネットワーキングがすでに完了している場合は、この手順で説明したフィールドの入力を省略できます。

フィールド	説明
共通ハイパーバイザ設定の構成	
サブネット マスク	IP アドレスを制限および制御するために、サブネットを適切なレベルに設定します。 たとえば、 <i>255.255.0.0</i> とします。
[ゲートウェイ (Gateway) ]	ゲートウェイの IP アドレス。 たとえば、 <i>10.193.0.1</i> とします。

フィールド	説明
[DNSサーバ (DNS Server(s)) ]	DNS サーバの IP アドレス。  DNS サーバを使用しない場合、HX Data Platform インストーラの [クラスターの設定 (Cluster Configuration) ] ページのどのフィールドにもホスト名を入力しないでください。すべての ESXi ホストにスタティック IP アドレスとホスト名のみを使用します。  (注) 複数の DNS サーバを指定する場合、両方の DNS サーバをカンマで区切って正確に入力するよう十分に注意してください。
ハイパーバイザ設定  [IP アドレスとホスト名を連続的に入力する (Make IP Addresses and Hostnames Sequential) ] を選択して、IP アドレスが順番に並ぶようにしてください。  (注) ドラッグアンドドロップ操作を使用してサーバの順番を並び替えることができます。	
名前	サーバ名。
シリアル	サーバのシリアル番号。
スタティック IP アドレス	すべての ESXi ホストのスタティック IP アドレスとホスト名を入力します。
ホスト名	ホスト名フィールドを空のままにしないでください。

**ステップ 7** [続行 (Continue) ] をクリックします。[IP アドレス (IP Addresses) ] ページが表示されます。[コンピューティング専用ノードの追加 (Add Compute-only Node) ] をクリックし、新しいノードを追加します。複数のコンピューティング専用ノードを追加する場合は、[IP アドレスをシーケンシャルにする (Make IP Addresses Sequential) ] を選択します。

フィールド	情報
管理ハイパーバイザ	ESXi ホストとストレージコントローラ間のハイパーバイザ管理ネットワーク接続を処理する静的 IP アドレスを入力します。
管理ストレージコントローラ	なし。
Data Hypervisor	ESXi ホストとストレージコントローラ間のハイパーバイザデータ ネットワーク接続を処理するスタティック IP アドレスを入力します。
データ ストレージコントローラ	なし。

フィールド	情報
コントローラ VM	<p>コントローラ VM が既存の HX クラスターにインストールされたときにそれらの VM に適用されたデフォルトの管理者ユーザ名とパスワードを入力します。</p> <p>(注) コントローラ VM の名前は変更できません。既存のクラスター パスワードを使用してください。</p>

**ステップ 8** [スタート (Start)] をクリックします。[進捗状況 (Progress)] ページに、さまざまな設定タスクの進捗状況が表示されます。

(注) デフォルトで、FlexFlash (SD カード) からブートする場合にはユーザの介入は必要はありません。ただし、ローカル ディスクからブートするようコンピューティング専用ノードを設定する場合は、Cisco UCS Manager の次の手順を完了します。

1. HX データ プラットフォーム インストーラ によって作成されたサービス プロファイル をクリックします。  
たとえば *blade-1(HX\_Cluster\_Name)* です。
2. [全般 (General)] タブで、[テンプレートからアンバインドする (Unbind from the Template)] をクリックします。
3. 作業中のペインで、[ストレージ (Storage)] タブ をクリックします。[ローカル ディスクの設定ポリシー (Local Disk Configuration Policy)] サブ タブ をクリックします。
4. [アクション (Actions)] 領域で、[ローカル ディスク設定のポリシーの変更 (Change Local Disk Configuration Policy)] > [ローカル ディスク設定ポリシーの作成 (Create Local Disk Configuration Policy)] を選択します。
5. [ローカル ディスク設定ポリシーの作成 (Create Local Disk Configuration Policy)] で、ポリシーの名前を入力し、残りの部分をデフォルトのままにします。[OK] をクリックします。
6. [ローカル ディスク設定のポリシーの変更 (Change Local Disk Configuration Policy)] の [アクション (Actions)] 領域で、ドロップダウン リストから、新しく作成されたローカル ディスク設定ポリシーを選択します。[OK] をクリックします。



7. それから HX データ プラットフォーム インストーラ UI に戻り、**[Continue (続行)]** をクリックして、**[Retry UCSM Configuration (UCSM 構成の再試行)]** をクリックします。

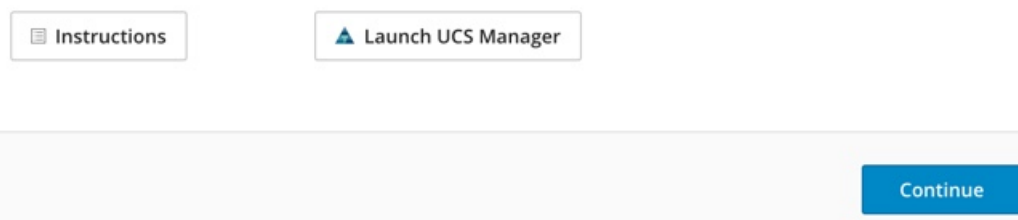
### Compute Node Expansion - ESXi Installation Required

ESXi must be installed on all nodes being added at this point using the HX ESXi ISO on [cisco.com](https://www.cisco.com)

Using an existing installation of ESXi will cause installation to fail. Other ESXi ISOs other than the one posted on Cisco are not supported.

Once ESXi is installed, select Continue and then Retry to continue installation.  
Full instructions can be found below.

If ESXi is already installed using the HX ESXi ISO wait for it to boot and then select Continue and Retry to continue installation.



(注) vCenter クラスターで EVC が有効になっている場合、展開プロセスが失敗し、「ホストは手動で vCenter に追加する必要があります (The host needs to be manually added to vCenter)」というメッセージが出されます。展開操作を正常に実行するには、次のようにします。

- vSphere クライアントに追加する ESXi ホストにログインします。
- コントローラ VM の電源をオフにします。
- vCenter で vSphere Web クライアント クラスターにホストを追加します。
- HX インストーラで、**[展開を再試行 (Retry Deploy)]** をクリックします。

**ステップ 9** インストールが完了したら、**[HyperFlex Connect の起動 (Launch HyperFlex Connect)]** をクリックしてストレージクラスターの管理を開始します。

**ステップ 10** 新しいノードがストレージクラスターに追加された後、HA サービスがリセットされ、追加されたノードを HA が認識できるようになります。

- VMware vSphere クライアントにログインします。
- [Home] > [Hosts and Clusters] > [Datacenter] > [Cluster] > [Host] の順に選択します。
- 新規ノードを選択します。
- 右クリックして **[Reconfigure for vSphere HA]** を選択します。

**ステップ 11** 既存のクラスターにコンピューティング専用ノードを追加した後、vMotion の vmk2 インターフェイスを手動で設定する必要があります。

## クラスター拡張の障害の解決

エラー ダイアログボックスが表示され、ストレージクラスターの拡張が完了しない場合は、次に示す解決オプションに進みます。

- 
- ステップ 1 [構成の編集 (Edit Configuration)] :** [クラスターの設定 (Cluster Configuration)] ページに戻ります。検証ページに記載されている問題を修正してください。
- ステップ 2 [初めからやり直す (Start Over)] :** 進捗テーブル エントリを消去することで、適用した設定を無効にし、[Cluster Configuration] ページに戻って新しい展開を再度開始できます。テクニカルアシスタンス センター (TAC) を参照してください。
- ステップ 3 [続行 (Continue)] :** 障害でエラーが発生した状態のまま、ストレージクラスターにノードを追加します。テクニカルアシスタンス センター (TAC) を参照してください。

(注) 障害についてよく理解し、予測できない動作の可能性を受け入れる用意がある場合にのみ、[続行 (Continue)] ボタンを選択してください。

HyperFlex の再展開を目的としたノードのクリーンアップの詳細については、『[HyperFlex Customer Cleanup Guides for FI and Edge](#)』を参照してください。

---

## ロジカル アベイラビリティ ゾーン

論理アベイラビリティゾーン (LAZ) 機能は、高い復元力を可能にするノードの固定数プールにクラスター ストレージ ノードをグループ化します。レプリケーション係数やクラスター サイズなどのクラスター パラメータに基づいて自動的に設定するか、手動で選択できるゾーンの数。8 つ以上のストレージノードを持つ HyperFlex クラスターでは、LAZ はデフォルトで有効になっています。この機能は、インストール時またはインストール後のいずれかで明示的に無効にしない限り、クラスターのライフサイクルを通じて有効のままになります。

### ロジカル アベイラビリティ ゾーンの利点

分散システムで大規模なクラスターの障害を減らすことは、インストール時に LAZ を有効にする主な利点です。分散ストレージシステムでは、クラスター内のリソースの数が増えると、障害リスクも増大します。複数の障害が同時に発生すると、永続的なデータが使用できなくなる可能性があります。

LAZ は、複数のコンポーネントおよびノードの同時障害が致命的な障害を引き起こすリスクを軽減するのに役立ちます。これは、いくつかの基本的な制約に基づいてリソースをグループ化することで実現します。LAZ を使用しない同じクラスターと比較して、可用性を 20%~70% 向上させることができます。改善の程度は、クラスター レプリケーション係数 (RF) および設定されているゾーンの数によって異なります。原則として、クラスターの数が少なく、レプリケーション係数が高いほど、最適な結果が得られます。さらに、LAZ は同じゾーンにグループ化さ

れた複数のリソースでメンテナンスタスクを実行することで時間を節約します。これは、LAZがないクラスタでは不可能なオプションです。

HyperFlex クラスターのインストール時に LAZ を有効にすることをお勧めします。インストール時に LAZ を有効にすると、最適なクラスタ パフォーマンスとデータ可用性が提供されます。サポートのガイダンスに従って、LAZ はコマンドライン インターフェイス (CLI) を使用して後で有効または無効にできます。無効にする前に、LAZ のガイドラインを確認してください。

### ゾーン数の指定とバランスの最適化

ゾーンの数にはデフォルトで自動的に設定され、推奨されます。インストーラでゾーン数を決定する場合、ゾーン数はクラスタのノード数に基づいて決定されます。

容量の利用とデータの分散を最もバランス良く保つため、クラスタ内のノード数をゾーン、3、4、または5の倍数にすることをお勧めします。たとえば、8ノードは2台のサーバーによる4つのゾーンに均等に分割され、9ノードは3台のサーバーによる3つのゾーンに均等に分割されます。11ノードでは、ゾーン間でノード数のバランスが悪くなり、ノードにおける容量の利用のバランスが悪くなります。必要なユーザは、3、4、または5ゾーンを手動で指定できます。

### LAZ のガイドラインと考察事項

- HyperFlex クラスタは、各ゾーンに参加するノードを決定します。この設定は変更できません。
- リソースの数を変更する場合は、設定された各ゾーンから同じ数のリソースを追加または削除します。
- **クラスタ拡張**：バランスの取れたゾーンを維持するために、ゾーンに見合っただけノード数も増やして拡張を実行します。バランスの取れたゾーンとは、インストールまたは拡張時に追加されたゾーンごとのノード数（またはゾーンのノードの永続的な障害が発生して変化したゾーンごとのノード数）が等しい場合、そのように考えます。たとえば、12ノードと4ゾーンのクラスタはバランスの取れたゾーンです（各ゾーンに3ノードずつ）。この場合、拡張時には4つのノードを追加することをお勧めします。
- **アンバランスなゾーン**：インストールまたは拡張時に追加されたゾーンごとのノード数（またはゾーンのノードの永続的な障害が発生して変化したゾーンごとのノード数）が等しくない場合、ゾーンはアンバランスなものとなる可能性があります。アンバランスなゾーンはパフォーマンスの最適化を損なう可能性があるため、**お勧めしません**。たとえば、11ノードと4ゾーンのクラスターでは、最後のゾーンを除き、ゾーンごとに3つのノードが存在するようになります。この場合、バランスを取るために1つのノードを追加する必要があります。新しいノードは、最後のゾーンに自動的に追加されます。
- **LAZ の無効化と再有効化**：LAZ を動的に無効または有効にできます。ゾーンの数異なる同じクラスタで LAZ を無効にしてから再度有効にすることは推奨されません。これを行うと、すでにデータが含まれているクラスタで LAZ がオンになっている場合に、既存のデータ分散ルールに準拠するために、クラスタ全体でデータの移動と再編成が過剰に行

われる可能性があります。これにより、クラスタの使用率がすでに 25% を超えている場合など、クラスタがゾーンに準拠しなくなることがあります。

### LAZ のステータスと接続

- HX Connect ダッシュボードから LAZ 情報を表示するには、HX Connect にログインし、[システム情報 (System information)] および [HyperFlex Connect] > [ダッシュボード (Dashboard)] メニューを使用します。
- `stcli cluster get-zone` コマンドを実行して、CLI から LAZ の詳細を表示することもできます。次に、`stcli cluster get-zone` コマンドの出力例を示します。

```
stcli cluster get-zone

zones:
-----
pNodes:
-----
state: ready
name: 10.10.18.61
-----
state: ready
name: 10.10.18.59
-----
zoneId: 0000000057eebaab:0000000000000003
numNodes: 2
-----
pNodes:
-----
state: ready
name: 10.10.18.64
-----
state: ready
name: 10.10.18.65
-----
zoneId: 0000000057eebaab:0000000000000001
numNodes: 2
-----
pNodes:
-----
state: ready
name: 10.10.18.60
-----
state: ready
name: 10.10.18.63
-----
zoneId: 0000000057eebaab:0000000000000004
numNodes: 2
-----
pNodes:
-----
state: ready
name: 10.10.18.58
-----
state: ready
name: 10.10.18.62
-----
zoneId: 0000000057eebaab:0000000000000002
numNodes: 2
-----
isClusterZoneCompliant: True
```

```
zoneType: logical
isZoneEnabled: True
numZones: 4
AboutCluster Time : 08/22/2019 2:31:39 PM PDT
```

### LAZ 関連コマンド

次の STCLI コマンドは、LAZ 操作に使用されます。詳細については、『[Cisco HyperFlex Data Platform CLI ガイド](#)』を参照してください。

この手順で LAZ の無効化操作と LAZ の有効化操作を連続的に実行する場合、実行の間隔を少なくとも 10 秒ほど空けるようにしてください。

コマンド	説明
<b>stcli cluster get-zone</b>	ゾーンの詳細を取得します。Gets the zone details. このオプションは、ゾーンが有効になっているか確認するために使用されます。
<b>stcli cluster set-zone --zone 0</b>	ゾーンを有効または無効にします。
<b>stcli cluster set-zone --zone 1</b> <b>stcli rebalance start</b>	<p>(推奨) ゾーンを有効化して作成します (デフォルトのゾーン数)</p> <p><b>重要</b> ゾーンを有効化および作成したら、<b>rebalance start</b> コマンドを実行する必要があります。</p> <p>ゾーン分割を有効化せずに作成されたクラスタは、ゾーン分割を有効化し、再調整を正常に完了した後にのみゾーンに対応できるようになります。</p> <p><b>警告</b> リバランスは重要なバックグラウンドサービスです。サービスを無効にすると、クラスタの復元力が失われるなど、予期しない動作が発生する可能性があります。このコマンドのサポートは、シスコ テクニカル サポートに限定されます。一般的な使用はサポートされていません。</p> <p>再調整アクティビティをトリガーすると、クラスタ内の複数のノード間で大規模なデータ移動が行われる場合があります。これにより、クラスタ内の IO パフォーマンスが低下する可能性があります。</p>

コマンド	説明
<pre>stcli cluster set-zone --zone 1 --numzones &lt;integer-value&gt; stcli rebalance start</pre>	<p>ゾーンを有効化し、特定の数のゾーンを作成します。</p> <p><b>重要</b>      ゾーンの数、3、4、または5のみです。</p> <p><b>重要</b>      ゾーンを有効化および作成したら、<b>rebalance start</b> コマンドを実行する必要があります。</p> <p><b>警告</b>      リバランスは重要なバックグラウンドサービスです。サービスを無効にすると、クラスタの復元力が失われるなど、予期しない動作が発生する可能性があります。このコマンドのサポートは、シスコテクニカルサポートに限定されません。一般的な使用はサポートされていません。</p>



## 第 11 章

# 混在 CPU を伴うクラスタの設定

この章では、同じ FI 上に複数の Intel CPU バージョンが搭載された HX ノードを追加する方法について説明します。

- [概要 \(187 ページ\)](#)
- [混合 CPU を使用するための前提条件 \(187 ページ\)](#)
- [EVC モードと CPU の互換性 \(188 ページ\)](#)
- [既存のクラスタでの vMotion との拡張された互換性 \(EVC\) の有効化 \(188 ページ\)](#)

## 概要

HyperFlex は、同じファブリック インターコネクト上で Intel v3 CPU と Intel v4 CPU をサポートします。Intel v3 CPU と Intel v4 CPU の間で仮想マシンを移行するには、VMware の拡張 vMotion 互換性 (EVC) を有効にします。EVC を有効にすると、HyperFlex クラスタ内のすべてのホストの設定で、下位モデル CPU の機能を伴う基準が適用されます。どのホストで稼働しているかに関係なく、同一の CPU 機能が仮想マシンに公開されるので、HyperFlex クラスタ内のホスト間で仮想マシンを移行できます。これにより、ホストの基盤となるハードウェアが異なる場合でも、vMotion の CPU 互換性が保証されます。

## 混合 CPU を使用するための前提条件

- EVC 対応クラスタでは、単一のベンダー製の CPU だけを使用できます。EVC 対応クラスタに別のベンダー製のホストを追加することはできません。
- 複数のリビジョン番号 (v2、v3、または v4) を持つ Xeon E3 または Xeon E5 ファミリの Intel プロセッサを搭載したクラスタ用に EVC を有効にする場合は、EVC 基準が必要です。
- 高度な仮想 CPU 機能が使用可能な場合は、BIOS でこれを有効にします。そうしないと、EVC 互換性チェックで特定の CPU に存在するはずの機能を検出が機能不全になり、EVC の有効化で問題が発生する可能性があります。

- 次のシナリオでは、EVC クラスタ内に仮想マシンが存在しても、vMotion を使用した仮想マシンの移行が失敗する可能性があります。
  - ホストが vCenter Server システムに接続されていない場合。
  - ホストが vMotion 用に設定されていない場合。
  - 仮想マシンが送信元ホストと宛先ホストの共有ストレージ上に存在しない場合。

## EVC モードと CPU の互換性

ご使用の CPU と互換性のある拡張 VMotion 互換性 (EVC) モードを特定するには、『[VMware Compatibility Guide](#)』を検索してください。サーバモデルまたは CPU ファミリを検索し、CPU シリーズ列のエントリをクリックすると、互換性のある EVC モードが表示されます。

### ホストの現在の EVC モードの検索

各 EVC モードは、同じ名前のプロセッサで使用できる機能に緊密に対応しています。

### vSphere Web クライアントの使用

1. vSphere Web Client Navigator から [ホストとクラスタ (Hosts and Cluster)] > [HX クラスタ (HX Cluster)] > [サマリー (Summary)] を選択します。[サマリー (Summary)] タブには、EVC が有効になっているかどうかと、ホストの現在の EVC モードが表示されます。
2. ホストでサポートされるすべての EVC モードのリストを表示するには、EVC モードの横にある青色のアイコンをクリックします。

### VMware 共有ユーティリティ ツールの使用

VMware は、互換性 EVC モードを表示する無料 CPU 識別ユーティリティに加えて、他の CPU 機能も備えています。このユーティリティをダウンロードし、[共有ユーティリティ](#)を使って ISO イメージからホストを起動できます。

## 既存のクラスタでの vMotion との拡張された互換性 (EVC) の有効化

クラスタ内のホスト間で vMotion による移行が確実に行われるようにするには、EVC を有効にします。EVC モードは、同じ HyperFlex クラスタ内で異なる CPU ファミリを混在させる場合に必要です。EVC モードが有効になると、設定された EVC モードの最小要件を満たすホストだけがクラスタに追加されます。クラスタの拡張中でも、中断することなく EVC モードを有効にすることができます。





- (注)
- EVC はデフォルトで無効になっています。クラスタ設定の [VMware EVC] で EVC を有効にすることができます。
  - これは HX Data Platform の制約ではなく、VMware の制限です。詳細については、VMware KB の記事『[EVC and CPU Compatibility FAQ \(1005764\)](#)』を参照してください。



- (注)
- EVC モードを有効にする場合は、EVC モードが Advanced Encryption Standard New Instructions (AES-NI) をサポートしていることを確認します。
  - これは HX Data Platform の制約ではなく、VMware の制限です。詳細については、VMware KB の記事『[EVC and CPU Compatibility FAQ \(1005764\)](#)』を参照してください。

新世代のサーバを追加する統一クラスタ、そしてサーバの世代が混合した既存のクラスタという考慮すべき 2 つのパスがあります。

## 均一クラスタへの新世代サーバの追加

クラスタが現在均一で、新世代サーバをクラスタに追加する場合は、VC で現在の世代の EVC モードを選択することで、EVC オンラインを中断せずに有効にすることができます。次に、拡張を使用して通常どおりに続行します(コンバージドまたはコンピューティングのみ)。拡張が試行される前に、EVC モードが設定されていることが必須です。

クラスタ拡張を実行する前に、均一クラスタで EVC モードを有効にするには、次の手順を実行します。

### ステップ 1 HX クラスタで vMotion との拡張された互換性 (EVC) を有効にする

- a) vSphere Web Client Navigator から [ホストとクラスタ (Hosts and Cluster)] > [データセンター (Datacenter)] > [HX クラスタ (HX Cluster)] を選択します。
- b) EVC を有効にする対象となるクラスタを選択します。[ワーク (Work)] ペインで、[管理 (Manage)] または [設定 (Configure)] タブをクリックします。[VMware EVC] を選択します。
- c) [編集 (Edit)] ボタンをクリックし、該当する [EVC モード (EVC mode)] を選択します。[OK] をクリックします。

### ステップ 2 HyperFlex インストーラを使用したコンピューティングのみまたはコンバージド ノードの展開を続行します。

## 既存のクラスタへの混合または旧世代サーバの追加

クラスタにはすでにサーバの世代が混在しているか、既存のクラスタに旧世代のサーバを追加する必要があります (コンピューティング専用ノード)。



(注) 新しいノードを持つクラスタ拡張ワークフロー中に EVC モードが有効になっていない場合は、これらの手順に従ってください。

旧世代サーバを既存のクラスタに追加するには、次の手順を実行します。

**ステップ 1** 開始する前に、HyperFlex クラスタが正常であり、すべてのノードがオンラインであることを確認してください。

### • vSphere Web クライアントの使用

vSphere Web クライアントナビゲータから、[Home]>[Global Inventory Lists]>[Cisco HyperFlex Systems]>[Cisco HX Data Platform]>[HX Cluster]>[Summary] の順に選択します。

レスポンスの例：

```
Operational Status: Online
Resiliency Status: Healthy
```

### • コントローラ VM を使用

コントローラ VM で、`#stcli cluster info` コマンドを実行します。

レスポンスの例：

```
healthstate: healthy
state: online
```

**ステップ 2** すべての非ストレージコントローラ仮想マシンの電源をオフにします。

**ステップ 3** 1 つのストレージコントローラ VM にログインし、`stcli cluster shutdown` コマンドを実行します。実行が完了するまで待ちます。

**ステップ 4** すべてのストレージコントローラ VM をシャットダウンします。

- vSphere Web Client ナビゲータから、[VM とテンプレート (VMs and Templates)]>[vCenter サーバー (vCenter server)]>[データセンター (Datacenter)]>[検出された仮想マシン (Discovered virtual machine)]>[仮想マシン (Virtual Machines)]>[`controller_vm`]を選択します。
- `controller_vm` を右クリックするか、[Actions] メニューから [Power]>[Shut Down Guest OS] を選択します。

**ステップ 5** 各 HX ホストをメンテナンス モードにします。

- vSphere Web Client Navigator から [ホストとクラスタ (Hosts and Cluster)]>[データセンター (Datacenter)]>[HX クラスタ (HX Cluster)]>[ノード (node)]を選択します。
- ノードを右クリックし、[Maintenance Mode]>[Enter Maintenance Mode] の順に選択します。

(注) この操作に [Cisco HX メンテナンス モード (Cisco HX Maintenance Mode) ] メニューを使用しないでください。

**ステップ 6** HX クラスタで vMotion との拡張された互換性 (EVC) を有効にする

- a) vSphere Web Client Navigator から [ホストとクラスタ (Hosts and Cluster) ] > [データセンター (Datacenter) ] > [HX クラスタ (HX Cluster) ] を選択します。
- b) EVC を有効にする対象となるクラスタを選択します。[ワーク (Work) ] ペインで、[管理 (Manage) ] または [設定 (Configure) ] タブをクリックします。[VMware EVC] を選択します。
- c) [編集 (Edit) ] ボタンをクリックし、該当する [EVC モード (EVC mode) ] を選択します。[OK] をクリックします。

**ステップ 7** メンテナンス モードを終了します。

- a) vSphere Web Client Navigator から [ホストとクラスタ (Hosts and Cluster) ] > [データセンター (Datacenter) ] > [HX クラスタ (HX Cluster) ] > [ノード (node) ] を選択します。
- b) ノードを右クリックし、[Maintenance Mode] > [Exit Maintenance Mode] の順に選択します。

(注) この操作に [Cisco HX メンテナンス モード (Cisco HX Maintenance Mode) ] メニューを使用しないでください。

**ステップ 8** ホストのメンテナンス モードが終了した後、コントローラ VM が自動的に電源オンになるはずですが、コントローラ VM の電源が自動的にオンにならない場合は、次の操作を行います。

- a) vSphere Web Client ナビゲータから、[VM とテンプレート (VMs and Templates) ] > [vCenter サーバ (vCenter server) ] > [データセンター (Datacenter) ] > [ESXi エージェント (ESXi Agents) ] > [仮想マシン (Virtual Machines) ] > [controller\_vm] を選択します。
- b) [controller\_vm] を右クリックするか、[アクション (Actions) ] メニューからクリックします。[電源 (Power) ] > [電源オンまたは電源 (Power On or Power) ] > [電源オン (Power ON) ] を選択します。

**ステップ 9** すべてのコントローラ VM が完全に起動していることを確認してください。次に、コントローラ VM の 1 つにログインし、`stcli cluster start` コマンドを実行します。

**ステップ 10** すべてのデータストアが vCenter HX プラグインからマウントされていることを確認し、クラスタが正常であることを確認します。

**ステップ 11** ユーザ VM を開始します。

**ステップ 12** HyperFlex インストーラを使用したコンピューティングのみの展開を続行します。





## 第 12 章

# Cisco HyperFlex Systems のカスタマイズされたインストール方法

- [概要 \(193 ページ\)](#)
- [事前設定されていない Cisco HyperFlex システムのインストールおよび設定のワークフロー \(193 ページ\)](#)
- [VMware ESXi のインストール \(194 ページ\)](#)

## 概要

この章では、インストール手順に移る前に手動で HyperFlex サーバを準備するプロセスについて説明します。このカスタマイズされたインストール方法を、次のシナリオで使用することができます。

- HyperFlex クラスタにコンピューティング専用ノードを追加する。
- Cisco HyperFlex システムの再展開。

実行するタスクは、事前設定された HyperFlex Systems を展開する場合と基本的に同じです。事前設定されていないシステムに固有の新しいタスクは、VMware ESXi のインストールです。

## 事前設定されていない Cisco HyperFlex システムのインストールおよび設定のワークフロー

### 始める前に

Cisco HyperFlex System のインストールと設定の要件を確認します。詳細については、「インストールの前提条件」を参照してください。

**ステップ 1** vCenter でクラスタを削除することにより、既存の環境をクリーンアップします。Cisco UCS で、vCenter MOB エントリ、UCS Manager サービス プロファイル、および VLAN を削除します。

**ステップ 2** 「ソフトウェアのダウンロード」から **Cisco HyperFlex Data Platform インストーラ OVA** ファイルをダウンロードします。

例：

Cisco-HX-Data-Platform-Installer-v2.5.1b-26284.ova

**ステップ 3** HX Data Platform のインストーラを起動してサインインします。

- a) [カスタマイズされたワークフロー (Customized Workflow)] を選択します。
- b) [UCS Manager 設定の実行 (Run UCS Manager configuration)] を選択して、UCS サービス プロファイルを設定します。『Cisco HyperFlex Systems Installation Guide for VMware ESXi』の「Configuring Cisco UCS Manager and HX Data Platform」のセクションに記載されている手順に従います。

**ステップ 4** vMedia を使用して、新規の ESXi インストールを実行します。

- (注) 自動 IP アドレス割り当てに Dynamic Host Configuration Protocol (DHCP) を使用することは推奨されません。デフォルトでは、HX Data Platform Installer によって、ESXi サーバーに静的 IP アドレスが割り当てられます。DHCP を使用する場合は、適切な VLAN を使用して ESXi でネットワークを手動で設定します。

**ステップ 5** HX Data Platform のインストーラを再び起動します。

- a) [カスタマイズされたワークフロー (Customized Workflow)] を選択します。
- b) [ESX 設定の実行 (Run ESX Configuration)]、[HX ソフトウェアの展開 (Deploy HX Software)]、および [HX クラスタの作成 (Create HX Cluster)] を選択します。

ウィザードで必ず [既存のパーティションの削除 (Delete Existing Partitions)] を選択してください。

## VMware ESXi のインストール

サーバーには、VMware ESXi のサポートされているバージョンが必要です。最適な HX スナップショットのパフォーマンスと機能を実現するには、ESXi 7.0 U2 以降をインストールすることを推奨します。サポートされる ESXi バージョンのリストについては、最新の『[Release notes for Cisco HX Data Platform](#)』を参照してください。



**重要** 各 HX サーバで ESXi をインストールします。

Cisco HyperFlex Data Platform の [ソフトウェアダウンロード](#) ページから VMware ESXi イメージをダウンロードします。Cisco UCS Manager を介してアクセス可能なネットワーク ロケーションを選択します。

HX カスタム ISO は、Cisco カスタム ESXi リリースに基づいています。

たとえば、

```
HX-Vmware-ESXi-60U2-4192238-Cisco-Custom-6.0.2.3.iso
```

。

### 次のタスク

- Cisco UCS Manager を通じた vMedia およびブート ポリシーの構成
- リモート KVM コンソールを開きます。
- サーバを再起動してインストールを開始します。
- Cisco UCS Manager を介して vMedia およびブート ポリシーの変更を元に戻します。

## Cisco UCS Manager での vMedia およびブート ポリシーの設定

Cisco UCS vMedia ポリシーとブート ポリシーを設定するには、次の手順を実行します。

### 始める前に

HX Data Platform インストーラにログインします。Cisco UCS Manager の設定に応じて、標準クラスタ用の [クラスタの作成 (Create Cluster)] ワークフローを実行します。



(注) サーバからサービス プロファイルの関連付けを解除する際に特定しやすくするために、*Temporary* という名前のクラスタを作成してください。

- ステップ 1 Cisco UCS Manager のナビゲーション ペインで [サーバ (Servers)] タブをクリックします。
- ステップ 2 [サーバ (Servers)] > [ポリシー (Policies)] > [ルート (root)] > [下位組織 (Sub-Organizations)] > [hx-cluster] > [vMedia ポリシー (vMedia Policies)] を展開します。
- ステップ 3 [vMedia ポリシー HyperFlex (vMedia Policy HyperFlex)] をクリックします。
- ステップ 4 設定ペインで、[vMedia マウントの作成 (Create vMedia Mount)] をクリックします。
- ステップ 5 マウントの名前を入力します (例: **ESX**)。
- ステップ 6 [CDD オプション (CDD option)] を選択します。
- ステップ 7 プロトコルとして [HTTP] を選択します。
- ステップ 8 [IP アドレス (IP Address)] に HyperFlex インストーラ VM の IP アドレスを入力します (例: **192.168.10.210**)。
- ステップ 9 [変数イメージ名 (Image Variable Name)] として [なし (None)] を選択します。

## リモート KVM コンソールを開く

- ステップ 10 [Remote File (リモート ファイル) ]に **HX-Vmware-ESXi-6.0.0-3380124-Custom-Cisco-6.0.1.2.iso** と入力します。
- ステップ 11 [リモートパス (Remote Path) ]に **/images/** と入力します。
- ステップ 12 [変更の保存 (Save Changes) ]をクリックし、[OK] をクリックします。
- ステップ 13 設定ペインで、[サーバ (Servers) ]>[サービス プロファイル テンプレート (Service Profile Templates) ]>[ルート (root) ]>[サブ組織 (Sub-Organizations) ]>[hx-cluster] >[サービス テンプレート hx-nodes (Service Template hx-nodes) ]を選択します。
- ステップ 14 [vMedia Policy] タブをクリックします。
- ステップ 15 [vMedia ポリシーの変更 (Modify vMedia Policy) ]をクリックします。
- ステップ 16 ドロップダウン選択項目から [HyperFlex vMedia ポリシー (HyperFlex vMedia Policy) ]を選択して、[OK] を 2 回クリックします。
- ステップ 17 [サーバ (Servers) ]>[ポリシー (Policies) ]>[ルート (root) ]>[サブ組織 (Sub-Organizations) ]>[hx-cluster] > [Boot Policy HyperFlex] を選択します。
- ステップ 18 ナビゲーション ペインで、[CIMC マウント vMedia (CIMC Mounted vMedia) ] というセクションを展開します。
- ステップ 19 [CIMC マウント CD/DVD の追加 (Add CIMC Mounted CD/DVD) ] という名前のエントリをクリックします。
- ステップ 20 [ブート順序 (Boot Order) ] リストで [CIMC マウント CD/DVD (CIMC Mounted CD/DVD) ] エントリを選択し、[上へ (Move Up) ] ボタンを何度かクリックして [CIMC マウント CD/DVD (CIMC Mounted CD/DVD) ] エントリをリストの先頭に移動させます。
- ステップ 21 [変更の保存 (Save Changes) ] をクリックし、[OK] をクリックします。

### 次のタスク

サブ組織 *Temporary* を削除します。

## リモート KVM コンソールを開く

1 つ以上のサーバの進行状況をモニタするには、リモート KVM コンソールセッションを開いてインストール状況を監視することを推奨します。

KVM コンソールを開くには、以下の手順を実行します。

- ステップ 1 Cisco UCS Manager のナビゲーション ペインで [サーバ (Servers) ] をクリックします。
- ステップ 2 [サーバ (Servers)]>[サービス プロファイル (Service Profiles)]>[ルート (Root)]>[サブ組織 (Sub-Organizaitons)]>[HX クラスタ (hx-cluster)]>[ラック ユニット番号 (rack-unit-number)] の順に展開します。
- ステップ 3 [ワーク (Work) ] ペインで、[全般 (General) ] タブをクリックします。
- ステップ 4 [アクション (Actions) ] 領域で、[KVM コンソール (KVM Console) ] をクリックします。



- ステップ 5** セキュリティ アラートが表示される場合は [続行 (Continue)] をクリックします。しばらくしてリモート **KVM コンソール** ウィンドウが開き、サーバのローカル コンソール出力が表示されます。
- ステップ 6** インストール中に **KVM コンソール** をモニタする対象のサーバごとに、ステップ 2 ~ 4 をさらに繰り返します。

---

## サーバの再起動

vMedia ポリシー、ブート ポリシー、およびサービス プロファイル テンプレートを変更した後、インストールを開始するにはサーバを再起動します。

サーバを再起動するには、次の手順を実行します。

### 始める前に

サーバの再起動の進行状況をモニタリングするには、リモート KVM コンソールセッションを開きます。

- 
- ステップ 1** Cisco UCS Manager のナビゲーション ペインで [サーバ (Servers)] をクリックします。
- ステップ 2** [機器 (Equipment)] > [ラック マウント (Rack Mounts)] > [サーバ (Servers)] を展開します。
- ステップ 3** [ワーク (Work)] ペインで、最初に再起動するサーバをクリックし、最後に再起動するサーバを **Shift** キーを押しながらクリックして、すべてのサーバを選択します。
- ステップ 4** マウスを右クリックして、[リセット (Reset)] をクリックします。
- ステップ 5** [OK] をクリックします。
- ステップ 6** [電源の再投入 (Power Cycle)] を選択し、[OK] をクリックします。

これにより、KVM コンソール ウィンドウでモニタしているサーバが即時に再起動し、リモート vMedia マウントから起動して Cisco カスタマイズ ESXi ISO をインストールします。エラー メッセージがある場合は、無視しても差し支えありません。

---

## VMedia とブート ポリシーの変更を元に戻す

サーバがブート ループに陥ってインストール用 ISO ファイルから起動し続けることを防ぐには、ブート ポリシーの変更を元に戻します。

### 始める前に

すべてのサーバがリモート vMedia ファイルからすでに起動し、インストールプロセスが開始済みであることを確認します。

- 
- ステップ 1** Cisco UCS Manager のナビゲーション ペインで [サーバ (Servers)] をクリックします。

- ステップ 2 [サーバ (Servers) ] > [ポリシー (Policies) ] > [ルート (Root) ] > [サブ組織 (Sub-Organizaitons) ] > [hx-cluster\_name] > [ブート ポリシー (Boot Policies) ] > [ブート ポリシー HyperFlex (Boot Policy HyperFlex) ] を展開します。
- ステップ 3 [ワーク (Work) ] ペインで、[全般 (General) ] タブをクリックします。
- ステップ 4 [アクション (Actions) ] 領域で、**CIMC マウント CD/DVD** をクリックします。
- ステップ 5 [ブート順序 (Boot Order) ] リストから [CIMC マウント CD/DVD (CIMC Mounted CD/DVD) ] エントリを選択し、[削除 (Delete) ] をクリックします。
- ステップ 6 [変更の保存 (Save Changes) ] をクリックし、[OK] をクリックします。
- 

### 次のタスク

#### 新しいノード

過去にクラスタ内で使用したことがない新しいノードを追加する場合は、HX クラスタを拡張します。詳細については、「[クラスタ拡張ガイドライン](#)」を参照してください。

#### 既存のノードの再インストール

このノードが過去にクラスタに含まれ、何かを修正するためにイメージを再作成した場合には、Cisco TAC に連絡して指示を受けてください。



## 第 13 章

# Cisco HyperFlex Edge の展開

- [Cisco HyperFlex Edge](#) (199 ページ)
- [HyperFlex Edge 導入オプション](#) (202 ページ)
- [2 ノード ネットワーク トポロジの選択](#) (203 ページ)
- [3 ノードまたは 4 ノードのネットワーク トポロジの選択](#) (227 ページ)
- [2 ノード 2 ルームのネットワーク トポロジの選択](#) (237 ページ)
- [インストレーションの概要](#) (261 ページ)
- [\(1 GbE のみ\) インストール後のスクリプトの実行](#) (279 ページ)
- [\(10/25GE のみ\) インストール後のスクリプトの実行](#) (281 ページ)
- [vMotion の自動構成](#) (283 ページ)
- [手動による vMotion の構成](#) (284 ページ)
- [手動によるトラフィック シェーピングの構成](#) (285 ページ)
- [\(10 / 25GE\) 追加 VIC ポートの使用 \(オプション\)](#) (285 ページ)
- [ネットワーク設定例](#) (286 ページ)

## Cisco HyperFlex Edge

### はじめに

Cisco HyperFlex Edge は、リモートオフィス/ブランチオフィス (ROBO) 環境およびエッジ環境にシンプルなハイパーコンバージェンスを提供します。このドキュメントでは、HyperFlex Edge の導入について説明します。



**重要** M6 ノードでの HX Edge クラスターの展開では、初期展開と進行中の管理のために Intersight が必要です。

## 制限事項とサポート可能性の概要

制限対象	サポート
クラスタサイズとタイプ	

制限対象	サポート
	<p>2 ノード クラスタ</p> <ul style="list-style-type: none"> <li>• HX220c M6 Hybrid/HXAF220c M6 オールフラッシュ</li> <li>• HX225c M6 Hybrid/HXAF225c M6 オールフラッシュ</li> <li>• HX220c M5 Hybrid/HXAF220c M5 オールフラッシュ</li> <li>• HX240c M6 Hybrid/HXAF240c M6 オールフラッシュ</li> <li>• HX245c M6 Hybrid/HXAF245c M6 オールフラッシュ</li> <li>• HX240c M5 Hybrid/HXAF240c M5 オールフラッシュ</li> <li>• HX240c M5SD Hybrid/HX240c M5SD オールフラッシュ</li> </ul> <p>(注) 2 ノード クラスタには、初期展開と継続的な管理のためのインターサイトが必要です。</p> <p>3 ノード クラスタ</p> <ul style="list-style-type: none"> <li>• HX220c M6 Hybrid/HXAF220c M6 オールフラッシュ</li> <li>• HX225c M6 Hybrid/HXAF225c M6 オールフラッシュ</li> <li>• HX220c M5 Hybrid/HXAF220c M5 オールフラッシュ</li> <li>• HX220c M4 Hybrid/HXAF220c M4 オールフラッシュ</li> <li>• HX240c M6 Hybrid/HXAF240c M6 オールフラッシュ</li> <li>• HX245c M6 Hybrid/HXAF245c M6 オールフラッシュ</li> <li>• HX240c M5 Hybrid/HXAF240c M5 オールフラッシュ</li> <li>• HX240c M5SD Hybrid/HX240c M5SD オールフラッシュ</li> </ul> <p>(注) M6 または HX240 Edge (ショートデプスとフルデプス) ノードでの HX Edge クラスタの展開では、初期展開と進行中の管理のために Intersight が必要です。</p> <p>4 ノード クラスタ</p> <ul style="list-style-type: none"> <li>• HX220c M6 Hybrid/HXAF220c M6 オールフラッシュ</li> <li>• HX225c M6 Hybrid/HXAF225c M6 オールフラッシュ</li> <li>• HX220c M5 Hybrid/HXAF220c M5 オールフラッシュ</li> <li>• HX240c M6 Hybrid/HXAF240c M6 オールフラッシュ</li> <li>• HX245c M6 Hybrid/HXAF245c M6 オールフラッシュ</li> <li>• HX240c M5 Hybrid/HXAF240c M5 オールフラッシュ</li> </ul>

制限対象	サポート
	<ul style="list-style-type: none"> <li>• HX240c M5SD Hybrid/HX240c M5SD オールフラッシュ</li> </ul> <p>(注) M6 または HX 240 (ショートデプスとフルデプス) ノードでの HX Edge クラスターの展開では、初期展開と進行中の管理のために Intersight が必要です。</p>
レプリケーションファクタ	<p>レプリケーションファクタの推奨事項：</p> <ul style="list-style-type: none"> <li>• 3 または 4 ノードエッジクラスタの場合：3</li> <li>• 2 ノードエッジクラスタの場合：2</li> </ul> <p>(注) RF2 を選択した場合、実稼働データが適切に保護されることを確実にするため、信頼性の高いバックアップ戦略が強く推奨されます。</p>
Networking	<p>1 GE または 10/25GE ネットワーキング (Cisco UCS ファブリック インターコネクタなし)。</p> <p>HX Edge システムは、QoS の実装を行いません。</p>
vCenter あたりの HX クラスタ数	最大 100 台

## HyperFlex Edge 導入オプション

HyperFlex Edge は、Cisco Intersight を使用してクラウドから、またはオンプレミスのインストーラアプライアンスを使用して導入できます。要件に応じて、次の2つのオプションから選択できます。

- **HyperFlex オンプレミス OVA インストーラ**：3～4 個のノードクラスタのオンプレミスでの Edge の導入には、このオプションを使用します。このタイプの導入は3つすべてのネットワークトポロジをサポートし、アプライアンスのダウンロードとインストールに加えて、ローカルネットワークアクセスが必要です。



(注) オンプレミスのインストーラの使用は、2つのノードの HyperFlex Edge クラスタではサポートされていません。

- **Intersight インストーラ**：クラウドから HyperFlex Edge を導入するには、Edge のこのオプションを使用します。この導入オプションは、すべての Edge クラスタ サイズとネットワークトポロジをサポートします。

本書では、オンプレミス OVA インストーラを使用した導入についてのみ説明します。

Cisco Intersight を使用して HyperFlex Edge クラスタを導入するには、『[Cisco Intersight 向け Cisco HyperFlex システム インストール ガイド](#)』で詳細な導入方法を参照してください。Cisco Intersight HX インストーラを使用すると、HyperFlex Edge クラスタを短時間で展開できます。このインストーラにより、「HX クラスタ プロファイル」と呼ばれるクラスタの事前構成定義が作成されます。この定義は、HX Edge クラスタ内の HX ノードの論理的表現です。HX クラスタ プロファイルで、Cisco Intersight 内にプロビジョニングされる各 HX ノードが指定されます。

追加ゲスト VM VLAN はオプションです。シンプルなネットワーク設計の維持を望む環境では、ゲスト VM トラフィックに上記の同じ管理 VLAN を使用できます。



- (注) 各クラスタは、固有のストレージデータ VLAN を使用して、すべてのストレージトラフィックを分離しておく必要があります。複数のクラスタにわたってこの VLAN を再利用することは推奨されません。



- (注) Cisco VIC の特性は、同じ物理ポートから複数の vNICs から切り離されているため、同じホスト上で実行されているインターフェイスまたはサービスに L2 で通信するために、vswitch-hx-vm-network 上でゲスト VM トラフィックを設定することはできません。a) 別の VLAN を使用し L3 ルーティングを実行するか、b) 管理インターフェイスへのアクセスが必要なゲスト VM が vswitch-hx-inband-mgmt vSwitch に配置されていることを推奨します。一般に、vm-network vSwitch を除き、ゲスト VM を HyperFlex で設定された vSwitches のいずれにも配置しないでください。使用例としては、いずれかのノードで vCenter を実行する必要があり、実行している ESXi ホストを管理するための接続が必要な場合があります。この場合は、上記の推奨事項のいずれかを使用して、接続が中断されないようにします。

## 2 ノード ネットワーク トポロジの選択

2 ノード トポロジを選択するとき、初期展開時に選択されるネットワーク トポロジは、完全な再インストールなしで変更またはアップグレードすることはできないことにご注意ください。将来のニーズを念頭に置いてネットワーク トポロジを慎重に選択し、次の Cisco HyperFlex 製品を考慮してください。

- Cisco VIC ベース ハードウェアまたは Intel NIC ベース アダプタを搭載した 10/25 Gigabit (GE) トポロジ
- ノード拡張を必要とせず、トップ オブラック (ToR) スイッチに使用可能な 10GE ポートがないクラスタ向けの 1GE トポロジ。

Cisco IMC 接続、物理ケーブル、ネットワーク設計、および構成ガイドラインの詳細については、次の使用可能なトポロジのリストから選択してください。

- [10 または 25GE VIC ベースのトポロジ \(204 ページ\)](#)

- [10 または 25GE NIC ベース トポロジ](#)
- [1 ギガビットイーサネット トポロジ \(220 ページ\)](#)

10/25GE または 1GE ToR 物理ネットワークとケーブルのセクションが完了したら、[ネットワークの共通要件チェックリスト \(253 ページ\)](#) に進みます。

## 10 または 25 ギガビットイーサネット トポロジ

### 10 または 25GE VIC ベースのトポロジ

10 または 25 ギガビットイーサネット (GE) スイッチ トポロジは、スイッチ (デュアルまたはスタック構成のスイッチを使用している場合)、リンクおよびポートの障害から保護する、フル冗長型のデザインを提供します。10/25GE スイッチは、1 台または 2 台のスタンドアロンスイッチとして、またはスイッチ スタック構成で使用することができます。

#### Cisco IMC Connectivity for 10/25GE VIC-Based Topology

Choose one of the following Cisco IMC Connectivity options for the 2-node 10/25 Gigabit Ethernet (GE) topology:

- Use of a dedicated 1GE Cisco IMC management port is recommended. This option requires additional switch ports and cables, however it avoids network contention and ensures always on, out of band access to each physical server.
- Use of shared LOM extended mode (EXT). In this mode, single wire management is used and Cisco IMC traffic is multiplexed onto the 10/25GE VIC connections. When operating in this mode, multiple streams of traffic are shared on the same physical link and uninterrupted reachability is not guaranteed. This deployment option is not recommended.
  - In fabric interconnect-based environments, built in QoS ensures uninterrupted access to Cisco IMC and server management when using single wire management. In HyperFlex Edge environments, QoS is not enforced and hence the use of a dedicated management port is recommended.
- Assign an IPv4 management address to the Cisco IMC following the procedures in the [Server Installation and Service Guide](#) for the equivalent Cisco UCS C-series server. HyperFlex does not support IPv6 addresses.

#### 10/25GE VIC ベース トポロジ用物理ネットワークおよびケーブル接続

VLAN 機能を備えたマネージド スイッチ (1 または 2) が必要です。Cisco は、Catalyst および Nexus スイッチングプラットフォームのリファレンス構成を完全にテストし、提供します。これらのスイッチのいずれかを選択すると、最高レベルの互換性が提供され、円滑な展開とシームレスな継続的運用が可能になります。

デュアルスイッチの設定には、スイッチの障害、リンクの障害、ポートの障害から保護する完全な冗長性を備えた、少し複雑なトポロジが含まれます。スタンドアロンまたはスタック構成が行われている 2 つのスイッチと、2 つの 10/25GE ポート、CIMC 管理用の 1 つの 1GE ポー



ト、サーバごとに1つの Cisco VIC 1457が必要です。トランクポートは、唯一サポートされているネットワークポート設定です。

シングルスイッチの設定では、サーバごとに1台のスイッチ、2つの 10/25GE ポート、CIMC 管理の 1GE ポート、1個の Cisco VIC 1457 のみを必要とするシンプルなトポロジが実現します。スイッチレベルの冗長性は提供されませんが、すべてのリンク/ポートおよび関連するネットワークサービスは完全に冗長であり、障害を許容することができます。

## 10 および 25GE トポロジ両方の要件

次の要件は両方の 10/25GE トポロジに共通であり、展開を開始する前に満たす必要があります。

- サーバごとの専用 1 ギガビットイーサネット (GE) Cisco IMC 管理ポート (推奨)
  - 専用 Cisco IMC 管理ポート (お客様が提供) 用の 2 個の 1GE ToR スイッチポートと、2 本のカテゴリ 6 イーサネットケーブル
- Cisco VIC 1457 (各サーバの MLOM スロットに取り付けられている)
  - 旧世代の Cisco VIC ハードウェアは、2 ノードまたは 4 ノードの HX Edge クラスタではサポートされていません。
  - 4 個の 10/25GE ToR スイッチポートおよび 4 本の 10/25GE SFP+ または SFP28 ケーブル (お客様が提供。選択したケーブルがスイッチモデルと互換性があることを確認します。)
  - Cisco VIC 1457 は Cisco HyperFlex リリース 4.0(1a) 以降で 10GE インターフェイスの速度をサポートしています。
  - Cisco VIC 1457 は Cisco HyperFlex リリース 4.0(2a) 以降で 25GE インターフェイスの速度をサポートしています。
  - Cisco VIC 1457 は 40GE インターネットの速度をサポートしていません。

## 25GE を使用した HX Edge クラスタの要件



- (注) 25GE モードを使用するには、通常、選択したケーブルのタイプと長さに応じて、前方誤り訂正 (FEC) を使用する必要があります。デフォルトでは、VIC 1400 シリーズは CL91 FEC モードで設定されます (Cisco IMC UI で使用可能な場合、FEC モード「auto」は CL91 と同じです)。自動 FEC ネゴシエーションはサポートされません。特定のスイッチでリンクステートをアップにするには、この FEC モードに合わせて手動で設定する必要があります。リンクをアップにするには、スイッチと VIC ポートの両方で FEC モードが一致している必要があります。使用中のスイッチが CL91 をサポートしていない場合、スイッチで使用可能な FEC モードと一致させて、VIC ポートが CL74 を使用するように設定できます。これには、[VIC 設定 (VIC configuration)] タブの [CIMC UI] で、手動で FEC モードを変更する必要があります。HyperFlex Edge の展開は、スイッチと VIC ポートからリンクステートがアップになったと報告されるまで、開始しないでください。CL74 は FC-FEC (ファイアコード) と呼ばれ、CL91 は RS-FEC (リードソロモン) と呼ばれています。Cisco IMC GUI を使用して VIC で設定されている FEC モードを変更する方法については、『[CISCO UCS C シリーズ Integrated Management Controller リリース 4.1 GUI コンフィギュレーションガイド](#)』を参照してください。

## 次の手順：

物理的なケーブル接続を続行するには、シングルスイッチまたはデュアルスイッチの設定を選択します。

## 10/25GE VIC ベースのデュアルスイッチの物理ケーブル配線



**警告** 適切なケーブル配線は、ネットワークの完全な冗長性を確保するために重要です。

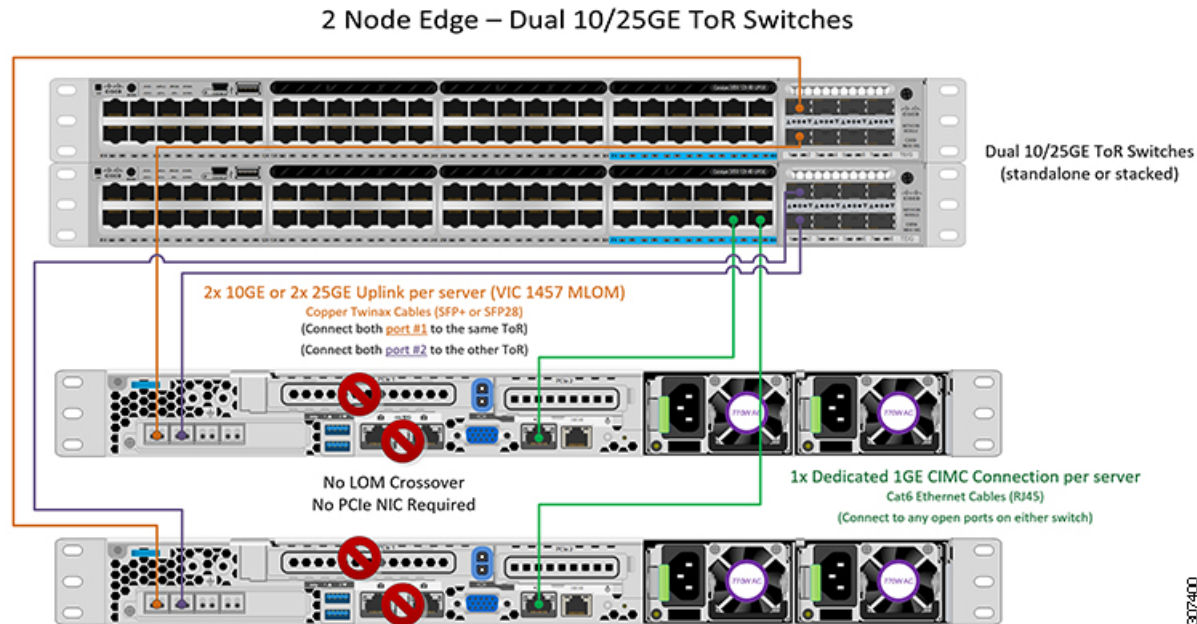
冗長性を追加するためデュアル ToR を使用して展開する場合 (ビジュアルレイアウトについては、次の図を参照してください)。

- 専用の Cisco IMC を使用している場合は、各サーバ (サーバの背面に「M」というラベルが付いている) の 1GE 管理ポートを 2 つのスイッチのいずれかに接続します。
- Cisco VIC の 4 つの 10/25GE ポートのうち 1 個を、各サーバから同じ ToR スイッチに接続します。
  - 同じスイッチに接続するには、各サーバで同じポート番号を使用します。



- (注) 同じ VIC ポート番号を使用しない場合、サーバ間のトランジションに対して余分なホップが発生し、2 つのスイッチ間で不必要に帯域幅が消費されます。

- Cisco VIC の 2 番目の 10/25GE ポートを、各サーバからもう一方の ToR スwitch に接続します。同じ Switch に接続するには、各サーバで同じポート番号を使用します。
- クラスターのインストール前に追加の 10/25GE ポートを接続しないでください。クラスター展開後、追加で 2 つの 10/25GE ポートをゲスト VM トラフィックにオプションで使用することができます。



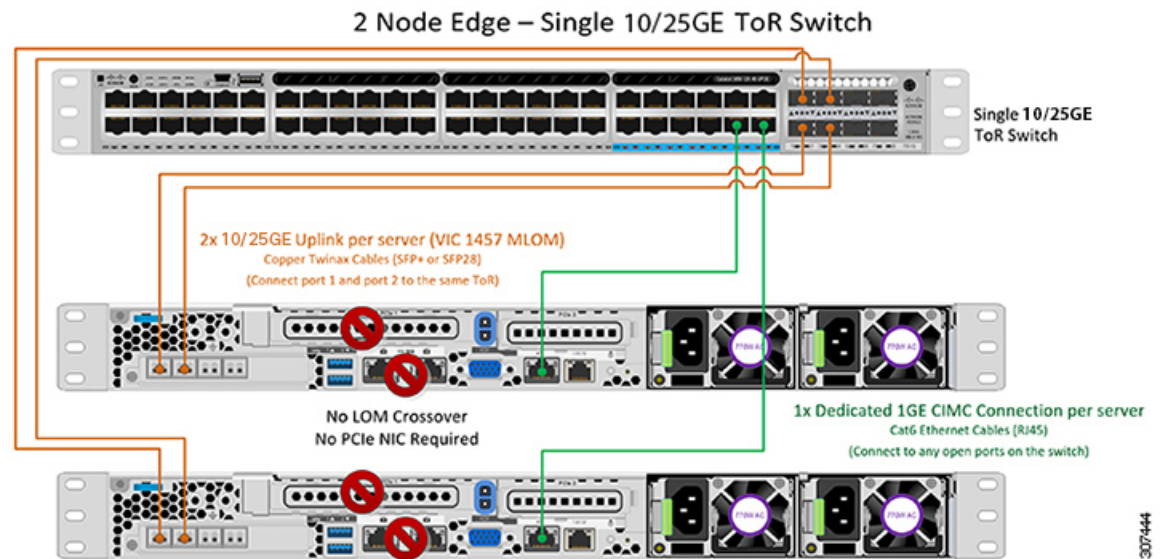
### 10/25GE VIC ベースの単一スイッチの物理ケーブル接続



**警告** 適切なケーブル配線は、ネットワークの完全な冗長性を確保するために重要です。

1 個の ToR を使用して展開する場合 (ビジュアル レイアウトについては、次の図を参照してください)。

- 専用の Cisco IMC を使用している場合は、各サーバ (サーバの背面にある「M」というラベルが付いた) の 1GE 管理ポートをスイッチに接続します。
- Cisco VIC の 4 つの 10/25GE ポートのうち 2 つを、各サーバから同じ ToR スwitch に接続します。
- クラスターのインストール前に追加の 10/25GE ポートを接続しないでください。クラスター展開後、追加で 2 つの 10/25GE ポートをゲスト VM トラフィックにオプションで使用することができます。



## 2 ノード 10/25GE VIC ベース トポロジの仮想ネットワーク設計

このセクションでは、仮想ネットワーク セットアップについて説明しています。HyperFlex 展開プロセスにより自動で仮想ネットワークがセットアップされるため、アクションは必要ありません。これらの詳細は、情報およびトラブルシューティング目的で下記に記載されています。

### 仮想スイッチ

vSwitch が 4 つ必要です。

- **vswitch-hx-inband-mgmt** : ESXi 管理 (vmk0) 、ストレージコントローラ管理ネットワーク
- **vswitch-hx-storage-data** : ESXi ストレージインターフェイス (vmk1) 、HX ストレージコントローラ データ ネットワーク
- **vmotion**—vMotion インターフェイス (vmk2)
- **vswitch-hx-vm-network** : VM ゲスト ポート グループ



- VMware ESXi 管理およびストレージコントローラ VM 管理は、同じサブネットおよび VLAN に存在する必要があります
- 専用 Cisco IMC 管理ポートは、上記の管理インターフェイスと同じ VLAN を共有できます。または、オプションで専用サブネットおよび VLAN を使用できます。別の VLAN を使用している場合、L3 接続が上記の管理 VLAN に必要です。また、Intersight 接続要件を満たす必要があります。
- Cisco IMC 管理の共有 LOM 拡張モードを使用する場合は、専用の VLAN が推奨されます。
- Cisco HyperFlex のストレージトラフィック用 1 VLAN これは、独立した、またはルーティングされていない VLAN である必要があります。固有である必要があります、管理 VLAN と重複することはできません。
- vMotion トラフィック用 1 VLAN これは、独立した、またはルーティングされていない VLAN にすることができます。



(注) これらの VLAN の必要性を縮小したり、削除したりすることはできません。このインストールが試行された場合は失敗します。

- ゲスト VM トラフィックには、追加の VLAN が必要です。これらの VLAN は、ESXi の追加ポートグループとして設定され、ToR スイッチでポートに面するすべての接続をリンクおよび許可する必要があります。
- これらの追加ゲスト VM VLAN はオプションです。シンプルなネットワーク設計の維持を望む環境では、ゲスト VM トラフィックに上記の同じ管理 VLAN を使用できます。



(注) 同じ物理ポートから複数の vNIC を分割する Cisco VIC の性質により、vswitch-hx-vm-network で構成されたゲスト VM トラフィックが、同じホストで実行されているインターフェイスまたはサービスと L2 を通信することはできません。a) 別の VLAN を使用して L3 ルーティングを実行するか、b) 管理インターフェイスへのアクセスが必要なゲスト VM を vswitch-hx-inband-mgmt vSwitch に配置することをお勧めします。一般に、vm-network vSwitch を除き、ゲスト VM を HyperFlex で設定された vSwitches のいずれにも配置しないでください。使用例としては、いずれかのノードで vCenter を実行する必要があります、実行している ESXi ホストを管理するための接続が必要な場合があります。この場合は、上記の推奨事項のいずれかを使用して、接続が中断されないようにします。

- Cisco VIC に接続されているスイッチポートは、パスが許可された適切な VLAN を使用して、トランク モードで設定する必要があります。
- 専用 Cisco IMC 管理ポートに接続されているスイッチポートは、適切な VLAN で「アクセス モード」で設定する必要があります。
- すべてのクラスタ トラフィックは、10/25GE トポロジ内の ToR スイッチを通過します。
- スパニング ツリー PortFast トランク (トランク ポート) は、すべてのネットワーク ポートで有効にする必要があります。



(注) PortFast の設定に失敗すると、ESXi の起動時に断続的に切断され、物理リンク障害時に必要なネットワークの再コンバージェンスよりも長く時間がかかります。

#### その他の考慮事項

- 必要に応じて、HX Edge ノードにサードパーティ製の NIC カードをさらにインストールできます。ネットワーク ガイドへのリンクについては、第 1 章の項を参照してください。
- VIC 以外のすべてのインターフェイスは、インストールが完了するまでシャットダウンするか、ケーブルを切断している必要があります。
- MLOM スロットでは、HX Edge ノードごとに 1 つの VIC のみがサポートされます。PCIe ベース VIC アダプタは、HX Edge ノードではサポートされていません。

#### 10/25 GE VIC ベースのジャンボ フレーム

通常、ジャンボフレームは、ネットワーク上で送信されるパケット数を減らし、効率を向上させるために使用されます。以下では、10/25GE トポロジでジャンボフレームを使用する際のガイドラインについて説明します。

- ジャンボフレームを有効にするオプションは、最初のインストール中にのみ提示され、後で変更することはできません。
- ジャンボ フレームは不要です。ジャンボ フレームをオプトアウトする場合は、すべてのネットワーク スイッチで MTU を 1500 バイトに設定したままにします。
- 最適なパフォーマンスのために、ジャンボフレームをオプションで有効にできます。フルパス MTU が 9000 バイト以上であることを確認します。ジャンボ フレームを有効にする場合は、次の点に注意してください。
  - デュアル スイッチ セットアップを実行する場合、すべてのスイッチ インターコネク トおよびスイッチ アップリンクでジャンボフレームが有効であることが不可欠です。フルパス MTU を確認しないと、リンクまたはスイッチの失敗後、トラフィックのパスが許可されない場合にクラスタがオフになる可能性があります。
  - HyperFlex インストーラは、ノードのいずれかでスタンバイ リンクを使用するため、フェールオーバーを強制する初期展開で、ワンタイムテストを実行します。スイッチ

のケーブル接続が適切に行われている場合、エンドツーエンドパス MTU をテストします。障害が検出された場合、この警告をバイパスしないでください。問題を修正し、インストーラを再実行して、検証チェックに合格するようにしてください。

- これらの理由と削除が複雑なため、デュアル スイッチ セットアップを使用する場合はジャンボ フレームを無効にすることをお勧めします。
- ジャンボ フレームを有効にするためのオプションは、ネットワーク設定ポリシーの下の HyperFlex クラスタ プロファイルの下にあります。ボックスをチェックすると、ジャンボ フレームが有効になります。ボックスをチェックしないと、ジャンボフレームは無効のままになります。

次の手順：

[ネットワークの共通要件チェックリスト \(253 ページ\)](#) を完了します。

## ネットワークの共通要件チェックリスト

インストールを開始する前に、お使いの環境が次の特定のソフトウェアおよびハードウェア要件を満たしていることを確認します。

### VLAN の要件



- 重要** 予約済み VLAN ID：指定する VLAN ID は、HyperFlex ノードが接続されている Top of Rack (ToR) スイッチでサポートされている必要があります。たとえば、VLAN ID 3968～4095 は Nexus スイッチによって予約され、VLAN ID 1002～1005 は Catalyst スイッチによって予約されています。HyperFlex で使用する VLAN ID を決定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

ネットワーク	VLAN ID	説明
次の各ネットワークに個別のサブネットと VLAN を使用します。		
VMware ESXi および Cisco HyperFlex 管理用 VLAN		ESXi、HyperFlex、および VMware vCenter 間の管理トラフィック用に使用され、ルーティング可能な必要があります。  (注) この VLAN は、Intersight にアクセスできる必要があります (Intersight で展開している場合)。



ネットワーク	VLAN ID	説明
CIMC VLAN		管理 VLAN と同じまたは異なる VLAN を指定できます。  (注) この VLAN は、Intersight にアクセスできる必要があります (Intersight で展開している場合)。
HX ストレージトラフィック用の VLAN		ストレージトラフィックに使用され、L2 接続のみ必要です。
VLAN for VMware vMotion		vMotion VLAN に使用されます (該当する場合)。  (注) 管理 VLAN と同じ VLAN を指定できますが、推奨されません。
VM ネットワーク用の VLAN		VM/アプリケーション ネットワークに使用されます。  (注) ESXi の VM ポートグループによって分けられている複数の VLAN であることがあります。

### サポートされている vCenter トポロジ

次の表を使用して、vCenter のサポートされているトポロジを決定します。

トポロジ	説明	推奨
シングル vCenter	外部サーバで実行され、サイトに対してローカル扱いとなる仮想または物理 vCenter。このサーバには、管理ラックマウントサーバを使用できます。	強く推奨
一元化された vCenter	WAN 全体の複数のサイトを管理する vCenter。	強く推奨

トポロジ	説明	推奨
ネストされた vCenter	展開予定のクラスタ内で実行される vCenter。	HyperFlex Edge クラスタのインストールは、vCenter がなくても先に実行できます。また、外部 vCenter を使用して展開し、クラスタに移行することもできます。いずれの場合も、実稼働ワークロードを実行する前に、クラスタを vCenter サーバに登録する必要があります。  最新情報については、『 <a href="#">How to Deploy vCenter on the HX Data Platform</a> 』テクニカルノートを参照してください。

### 3 ノード顧客の展開情報

一般的な 3 ノードの HyperFlex Edge の導入の場合、13 個の IP アドレスが必要です - 管理ネットワーク用の 10 個の IP アドレスと vMotion ネットワーク用の 3 個の IP アドレス。



**重要** すべての IP アドレスは IPv4 である必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

### 4 ノード顧客の展開情報

一般的な 4 ノードの HyperFlex Edge の導入の場合、17 個の IP アドレスが必要です - 管理ネットワーク用の 13 個の IP アドレスと vMotion ネットワーク用の 3 個の IP アドレスです。



**重要** すべての IP アドレスは IPv4 である必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

### CIMC 管理 IP アドレス

サーバ	CIMC 管理 IP アドレス
サーバ 1 :	
サーバ 2 :	
サーバ 3 :	

サーバ	CIMC 管理 IP アドレス
サーバー 4:	
サブネット マスク	
ゲートウェイ	
DNS サーバ	
NTP サーバ  (注) 適切な Intersight 接続を確保するためには、CIMC に NTP を設定する必要があります。	

### ネットワークの IP アドレス



- (注) デフォルトでは、HX インストーラにより、ハイパーバイザ データ ネットワークとストレージコントローラ データ ネットワークに 169.254.1.X の範囲内の IP アドレスが自動的に割り当てられます。この IP サブネットをユーザーが設定することはできません。



- (注) スパニング ツリー PortFast トランク (トランク ポート) は、すべてのネットワーク ポートで有効にする必要があります。

PortFast の設定に失敗すると、ESXi の起動時に断続的に切断され、物理リンク障害時に必要なネットワークの再コンバージェンスよりも長く時間がかかります。

管理ネットワークの IP アドレス (ルーティング可能であること)	
ハイパーバイザ管理ネットワーク	ストレージコントローラの管理ネットワーク
サーバ 1 :	サーバ 1 :
サーバ 2 :	サーバ 2 :
サーバ 3 :	サーバ 3 :
サーバー 4:	サーバ 4:
ストレージクラスタ管理 IP アドレス	クラスタ IP:
サブネット マスク	

管理ネットワークの IP アドレス (ルーティング可能であること)	
デフォルト ゲートウェイ	

### VMware vMotion ネットワーク IP アドレス

vMotion サービスの場合、固有の VMKernel ポートを設定します。必要であれば、vMotion の管理 VLAN を使用している場合は vmk0 を再使用することもできます (非推奨)。

サーバ	vMotion ネットワークの IP アドレス (post_install スクリプトを使用して設定されている)
サーバ 1 :	
サーバ 2 :	
サーバ 3 :	
サーバ 4 :	
サブネット マスク	
ゲートウェイ	

### VMware vCenter の構成



- (注) HyperFlex は標準ポートを介して vCenter と通信します。ポート 80 はリバース HTTP プロキシで使用されますが、TAC のサポートを受けて変更できます。ポート 443 は vCenter SDK へのセキュア通信に使用され、変更することはできません。

vCenter 管理ユーザ名 <i>username@domain</i>	
vCenter 管理パスワード	
vCenter データセンターの名前 (注) 既存のデータセンターオブジェクトを使用できます。データセンターが vCenter に存在しない場合は、作成されます。	

<p><b>VMware vSphere コンピューティング クラスタおよびストレージ クラスタの名前</b></p> <p>(注) vCenter に表示される クラスタ名。</p>	
--	--

## ポート要件



**重要** [Intersight の接続性 \(219 ページ\)](#) に記載されている前提条件に加えて、次のポート要件も満たしていることを確認します。

ネットワークがファイアウォールの背後にある場合は、標準のポート要件に加え、VMware には VMware ESXi および VMware vCenter に対するポートが推奨されます。

- CIP-M は、クラスタ管理 IP に使用します。
- SCVM は、コントローラ VM の管理 IP です。
- ESXi は、ハイパーバイザの管理 IP です。

HyperFlex ソリューションのコンポーネント通信に必要なポートの包括的なリストは、[HX Data Platform Security Hardening Guide](#) の付録 A に記載されています。



**ヒント** 標準設定がなく、異なるポート設定が必要な場合は、環境のカスタマイズについて、[表 C-5 ポートのリテラル値](#)を参照してください。

## ネットワーク サービス



- (注)
- DNS サーバと NTP サーバは、HX ストレージ クラスタの外側に配置する必要があります。
  - 現時点では、信頼性の高いソースを提供するには、内部でホストされている NTP サーバを使用してください。
  - すべての DNS サーバは、展開を開始する前に、ESXi の各ホストについて順方向 (A) および逆方向 (PTR) の DNS レコードを事前設定しておく必要があります。DNS を前もって正しく設定しておけば、ESXi ホストを、IP アドレスではなく FQDN で vCenter に追加できます。

この手順をスキップした場合には、ホストは IP アドレスで vCenter インベントリに追加され、ユーザは「[vCenter クラスタのノードの識別方法を IP から FQDN に変更する](#)」で説明されている手続きに従って、FQDN に変換することが必要になります。

<b>DNS サーバ</b> <Primary DNS Server IP address, Secondary DNS Server IP address, ...>	
<b>NTP サーバ</b> <Primary NTP Server IP address, Secondary NTP Server IP address, ...>	
<b>タイムゾーン</b> 例 : US/Eastern、US/Pacific	

### コネクテッドサービス

コネクテッドサービスの有効化 (推奨) [はい (Yes) ] または [いいえ (No) ] が必要	
<b>サービス要求通知用の電子メール</b> 例 : name@company.com	

### Proxy Server

- Intersight への直接接続が使用できない場合、プロキシサーバの使用は任意です。
- プロキシを使用する場合は、サーバを Intersight アカウントに要求するためにプロキシを使用するように、各サーバのデバイス コネクタを設定する必要があります。さらに、HyperFlex Data Platform を正常にダウンロードできるようにするには、HX クラスタ プロファイルでプロキシ情報を指定する必要があります。
- ユーザー名/パスワードの使用はオプションです。

<b>プロキシが必要です:イエスマ          またはノー</b>	
<b>Proxy Host</b>	
<b>プロキシポート (Proxy Port)</b>	
<b>Username</b>	
<b>パスワード</b>	

## ゲスト VM トラフィック

ゲスト VM トラフィックに関する考慮事項は、トポロジの選択に基づいて上記に示されます。通常、正しい vSwitch に適用される限り、必要に応じてゲスト ポート グループを作成できません。

- 10/25GE トポロジ: **vswitch-hx-vm-network** を使用して、新しい VM ポート グループを作成します。

Post\_install スクリプトを実行して、クラスタ内のすべてのホスト上で正しい vSwitches に自動的に VLAN を追加することを推奨します。後ほど、任意の時点で新しいゲスト VLAN をクラスタに追加するには、**hx\_post\_install --vla** (スペースの後には 2 つのダッシュ) を実行します。

残りの vmnic またはサードパーティ製のネットワーク アダプタを使用する追加の vSwitches が作成される場合があります。HyperFlex によって定義された vSwitches に変更が加えられないように注意する必要があります。



- (注) ユーザーが作成した追加の vSwitches は、管理者単独で責任を有し、HyperFlex によって管理されません。

## Intersight の接続性

Intersight の接続性に関する次の前提条件を考慮してください。

- HX サーバのセットに HX クラスタをインストールする前に、対応する Cisco IMC インスタンスのデバイス コネクタが Cisco Intersight に接続するように適切に設定され、登録されていることを確認します。
- インストールフェーズ中のポート 80、443、および 8089 を介した CIMC と vCenter 間の通信。
- すべてのデバイス コネクタは、*svc.intersight.com* を適切に解決でき、かつポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。現在の HX インストーラバージョンでは、HTTP プロキシの使用がサポートされています。
- すべてのコントローラの VM 管理インターフェイスは、*svc.intersight.com* を適切に解決でき、ポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。現在の HX インストーラバージョンは、インターネットへの直接接続がない場合、HTTP プロキシの使用をサポートしています。
- IP 接続 (L2 または L3) は、各サーバの CIMC 管理 IP から次のすべてに必要です。ESXi 管理インターフェイス、HyperFlex コントローラ VM 管理インターフェイス、vCenter サーバ。このパスのファイアウォールは、『[Hyperflex Hardening ガイド](#)』で説明されている必要なポートを許可するように設定する必要があります。
- HXDP リリース 3.5(2a) 以降、Intersight インストーラでは、HyperFlex サーバ上に工場出荷時にインストールされるコントローラ VM が不要になりました。

同じサーバに HyperFlex を再展開する場合、新しいコントローラ VM を Intersight からすべての ESXi ホストにダウンロードする必要があります。これには、各 ESXi ホストが svc.intersight.com を解決し、ポート 443 上の発信側で開始した HTTPS 接続を許可することが必要です。コントローラ VM のダウンロードにプロキシサーバを使用することはサポートされており、必要に応じて HyperFlex クラスタ プロファイルで設定できます。

- クラスタの展開後、継続的な管理のために Intersight 内で新しい HX クラスタが自動的に登録されます。

## Cisco HyperFlex Edge 非表示クラウド監視

Cisco Hyperflex Edge 非表示クラウド監視は、監視 VM または調停ソフトウェアの必要性を排除する、Cisco Hyperflex Edge の導入における革新的なテクノロジーです。

Cisco Hyperflex Edge 非表示クラウド監視は、2 ノード HX Edge 展開にのみ必要です。監視には、追加のインフラストラクチャ、セットアップ、設定、バックアップ、パッチ、または管理は必要ありません。この機能は、2 ノード HyperFlex Edge のインストールの一部として自動的に設定されます。リモートサイトでのアウトバウンドアクセスは、相互に接続するために存在している必要があります (Intersight.com または Intersight 仮想アライアンス)。HyperFlex Edge 2 ノードクラスタは、この接続が確立されていないと動作しません。

非表示クラウド監視機能の利点、運用、および障害のシナリオの詳細については、次を参照してください。 <https://www.cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/whitepaper-c11-741999.pdf>

## Cisco Hyperflex Edge サーバの注文

Cisco HyperFlex Edge サーバを注文する場合は、[HyperFlex Edge 仕様シート](#)の説明に従って、正しいコンポーネントを選択してください。ネットワークトポロジの選択に注意して、目的の設定と一致することを確認します。ネットワークトポロジの PID 選択の詳細については、仕様シートの補足資料セクションを参照してください。

## 1 ギガビット イーサネット トポロジ

### 1 ギガビット イーサネット トポロジ

1 ギガビット イーサネット (GE) スイッチ トポロジは、スイッチ (デュアルまたはスタックスイッチを使用している場合)、リンクおよびポートの障害からネットワークを保護する完全冗長設計を提供します。1 GE スイッチは、1 つまたは 2 つのスタンドアロンスイッチとして使用したり、スイッチスタックの構成に使用したりすることができます。



- (注) シングルまたはデュアル 1Gb スイッチ接続は、仮想マシンが得られる最大パフォーマンスを制限するため、高いパフォーマンスを必要とするアプリケーションには推奨されません。



## 1 ギガビットイーサネットトポロジ用 Cisco IMC 接続

2 ノード 1 ギガビットイーサネット (GE) トポロジの Cisco IMC 接続では、専用の 1GE Cisco IMC 管理ポートを使用する必要があります。このトポロジで直接接続ケーブルを使用しているため、共有 LOM モードを含む他の動作モードは使用できません。

同様の Cisco UCS C シリーズ サーバについては、『サーバ設置およびサービス ガイド』の次の手順に従い、Cisco IMC に IPv4 管理アドレスを割り当てます。HyperFlex は IPv6 アドレスをサポートしていません。

## 1 GE トポロジ用物理ネットワークおよびケーブル接続

VLAN 機能を備えたマネージドスイッチ (1 または 2) が必要です。Cisco は、Catalyst および Nexus スイッチングプラットフォームのリファレンス構成を完全にテストし、提供します。これらのスイッチのいずれかを選択すると、最高レベルの互換性が提供され、円滑な展開とシームレスな継続的運用が可能になります。

デュアルスイッチのケーブル接続には、スイッチの障害、リンクの障害、スイッチポートの障害から保護する完全な冗長性を備えた、少し複雑なトポロジが含まれます。スタンドアロンまたはスタックの 2 個のスイッチと、サーバごとに 3 個の 1 ギガビットイーサネット (GE) スイッチポートが必要です。シングルスイッチのケーブル接続では、サーバごとに 1 台のスイッチと 3 つの 1 GE スイッチポートのみを必要とする単純なトポロジが実現します。スイッチレベルの冗長性は提供されませんが、すべてのリンク/ポートおよび関連するネットワークサービスは完全に冗長であり、障害を許容することができます。

1GE トポロジは、10GE 用スイッチが必要なく、2 個のノード間的高速、冗長、10GE 接続に直接接続ケーブルを使用します。



(注) このトポロジは、今後のノード展開機能はサポートせず、今後さらなる HX Edge ノードの追加を制御する要件が存在する場合、避ける必要があります。

次の要件は両方の 1GE トポロジに共通であり、展開を開始する前に満たす必要があります。

- サーバごとの専用 1 ギガビットイーサネット (GE) Cisco IMC 管理ポート (必須)
- Intel i350 クアッドポート PCIe NIC カード (各サーバの PCIe スロットにインストール) (必須)
  - Cisco VIC はこのトポロジでは使用されません
- 2 x 10GE DirectConnect LAN-on-Motherboard (LOM) 接続 (スイッチポートを消費しない)
  - 直接接続リンクのイーサネットケーブルを通して 2 x カテゴリ 6 ストレート (顧客提供)
- 6 x 1GE Top of Rack (ToR) スイッチポートおよび 6x カテゴリ 6 イーサネットケーブル (顧客提供)

物理的なケーブル接続を続行するには、シングルスイッチまたはデュアルスイッチの設定を選択します。

### 1 ギガビットイーサネットデュアルスイッチケーブル接続



**警告** 適切なケーブル配線は、ネットワークの完全な冗長性を確保するために重要です。

冗長性を追加するためデュアル ToR を使用して展開する場合 (ビジュアルレイアウトについては、次の図を参照してください)。

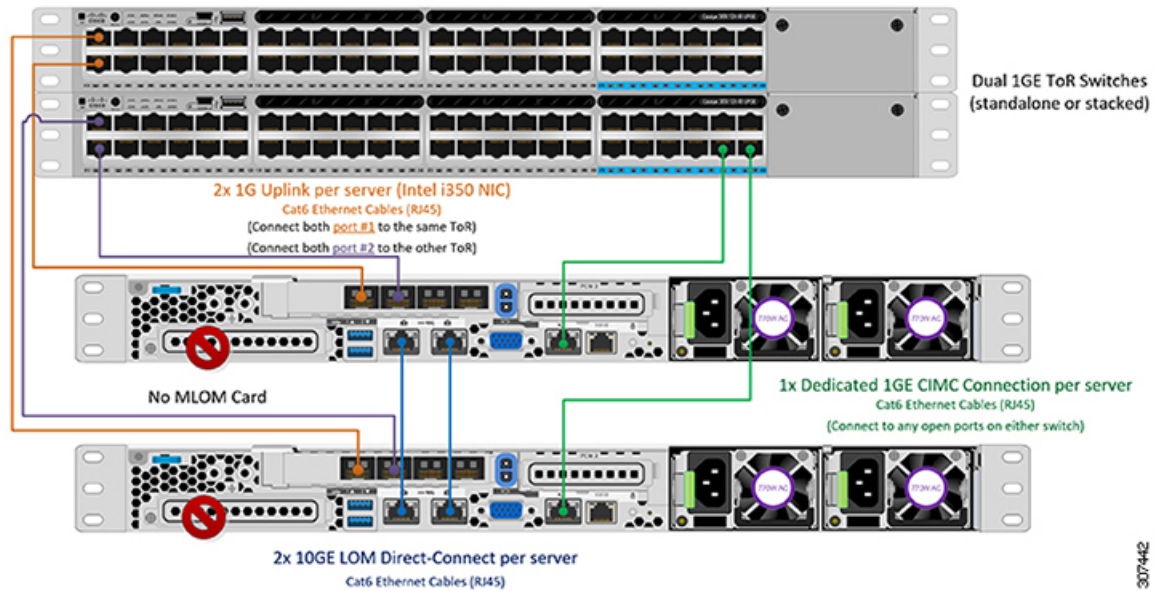
- 各サーバ (サーバの背面に「M」というラベルが付いている) の 1GE 専用の Cisco IMC を 2 つのスイッチのいずれかに接続します。
- 通常のイーサネットケーブルを使用して、サーバ上の Lan-on-motherboard (LOM) ポート 1 を別のサーバ上の LOM ポート 1 に接続します。
- サーバ上の LOM ポート 2 を第二サーバ上の LOM ポート 2 に接続します。
- i350 NIC の 4 つの 1GE ポートのうち 1 つを、各サーバから同じ ToR スwitch に接続します。同じ Switch に接続するには、各サーバで同じポート番号を使用します。



(注) 同じポート番号を使用しない場合、サーバ間のトラフィックに対して余分なホップが発生し、2 つのスイッチ間で不必要に帯域幅が消費されます。

- i350 NIC の 2 番目の 1GE ポートを、各サーバからもう一方の ToR スwitch に接続します。同じ Switch に接続するには、各サーバで同じポート番号を使用します。
- クラスターのインストール前に追加の 1GE ポートを接続しないでください。クラスター展開後、追加で 2 つの 1GE ポートをゲスト VM トラフィックにオプションで使用することができます。

## 2 Node Edge – Dual 1GE ToR Switches



307442

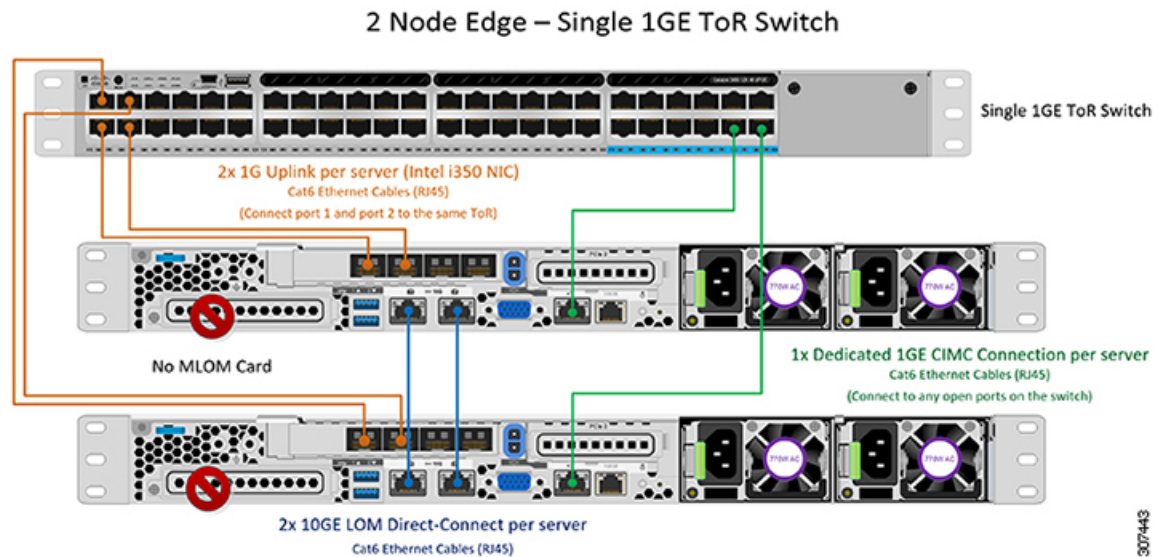
## 1ギガビットイーサネット シングルスイッチ ケーブル接続



**警告** 適切なケーブル配線は、ネットワークの完全な冗長性を確保するために重要です。

1 個の ToR を使用して展開する場合 (ビジュアル レイアウトについては、次の図を参照してください)。

- 各サーバ (サーバの背面にある「M」というラベルが付いた) の 1GE 専用 Cisco IMC 管理ポートをスイッチに接続します。
- 通常のイーサネットケーブルを使用して、サーバ上の Lan-on-motherboard (LOM) ポート 1 を別のサーバ上の LOM ポート 1 に接続します。
- サーバ上の LOM ポート 2 を第二サーバ上の LOM ポート 2 に接続します。
- i350 NIC の 4 つの 1GE ポートのうち 2 つを、各サーバから同じ ToR スwitch に接続します。
- クラスターのインストール前に追加の 1GE ポートを接続しないでください。クラスター展開後、追加で 2 つの 1GE ポートをゲスト VM トラフィックにオプションで使用することができます。



## 2ノード1ギガビットイーサネットトポロジの仮想ネットワーク設計

このセクションでは、仮想ネットワーク セットアップについて説明しています。HyperFlex 展開プロセスにより自動で仮想ネットワークがセットアップされるため、アクションは必要ありません。これらの詳細は、情報およびトラブルシューティング目的で下記に記載されています。

### 仮想スイッチ

次のネットワークに対する各 ESXi コールの実推奨構成は分離する必要があります。

- 管理トラフィック ネットワーク
- データ トラフィック ネットワーク
- vMotion ネットワーク
- VM ネットワーク

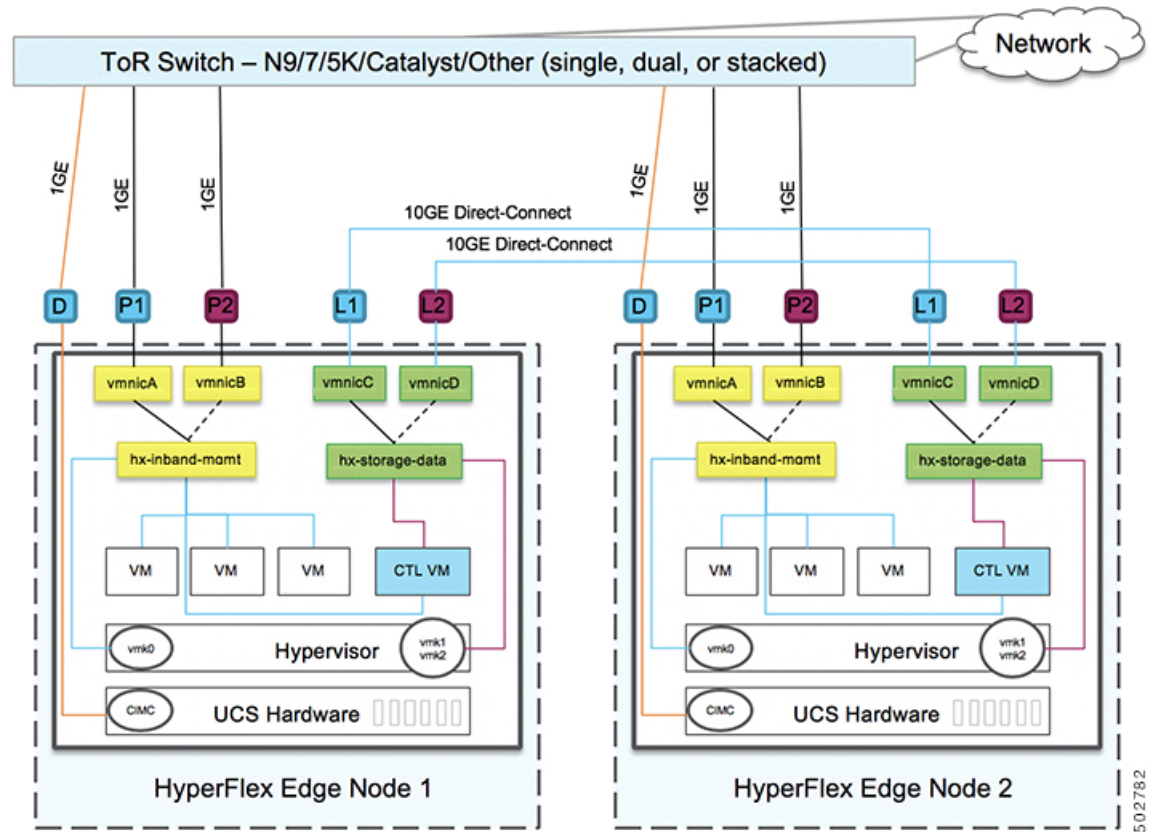
最小ネットワーク構成では、最小限で次の2つの個別ネットワークが必要です。

- 管理ネットワーク (vMotion と VM ネットワークを含む)
- データ ネットワーク (ストレージトラフィック用)

それぞれのネットワークに対応する2つの vSwitch が必要です。

- **vswitch-hx-inband-mgmt** : ESXi 管理 (vmk0)、HyperFlex ストレージコントローラ管理、VM ゲスト ポートグループ
- **vswitch-hx-storage-data** : ESXi ストレージインターフェイス (vmk1)、HyperFlex インターフェイス (vmk2)、HyperFlex ストレージコントローラ データ ネットワーク。

## ネットワーク トポロジ (Network Topology)



## フェールオーバーの順序 :

**vswitch-hx-inband-mgmt** : 2つのアップリンク上で、vSwitch全体がアクティブ/スタンバイに設定されます。デフォルトでは、すべてのサービスが1つのアップリンクポートを使用し、必要に応じてフェールオーバーされます。VMポートグループのフェールオーバー順序は、必要に応じて、かつより適切なロードバランシングになるようにオーバーライドできます。

**vswitch-hx-storage-data** : HyperFlexストレージデータネットワークとvmmk1は、同じアクティブ/スタンバイ順序に設定されます。post\_installスクリプトを使用して設定されている場合、vMotion VMKernelポートは反対の順序を使用するように設定されます。これにより、直接接続リンクの完全な使用率が確保されます。

## 1 ギガビットイーサネットスイッチ設定時の注意事項

- 次の条件で最小の1 VLAN: VMware ESXi 管理、ストレージコントローラ VM 管理および Cisco IMC 管理。
  - VMware ESXi 管理およびストレージコントローラ VM 管理は、同じサブネットおよび VLAN に存在する必要があります
  - 専用 Cisco IMC 管理ポートは、上記の管理インターフェイスと同じ VLAN を共有できます。または、オプションで専用サブネットおよび VLAN を使用できます。別の

VLANを使用している場合、L3接続が上記の管理VLANに必要です。また、Intersight接続要件を満たす必要があります。

- ゲストVMトラフィックには、追加のVLANが必要です。これらのVLANは、ESXiの追加ポートグループとして設定され、すべての接続をToRスイッチにトランクする必要があります。
- これらの追加ゲストVMVLANはオプションです。シンプルなネットワーク設計の維持を望む環境では、ゲストVMトラフィックに上記の同じ管理VLANを使用できます。
- Intel i350に接続されているスイッチポートは、パスが許可された適切なVLANを使用して、トランクモードで設定する必要があります。
- 専用Cisco IMC管理ポートに接続されているスイッチポートは、適切なVLANで「アクセスモード」で設定する必要があります。
- VMware vMotionトラフィックおよびCisco HyperFlexデータトラフィックは、直接接続LOMをトラバースするため、top of rackスイッチを利用しません。したがって、追加のVLANがこれらのサービスには必要ありません。
  - ToRスイッチのジャンボフレームの設定は、アップストリームスイッチをトラバースする必要なく、すべてのトラフィックがローカルに残るためこのトポロジでは必要ありません。したがって、このトポロジはデフォルトで、ジャンボフレームを使用して高パフォーマンスを実現するトラフィックをvMotionします。
- スパニングツリーPortFastトランク(トランクポート)は、すべてのネットワークポートで有効にする必要があります。



(注) PortFastの設定に失敗すると、ESXiの起動時に断続的に切断され、物理リンク障害時に必要なネットワークの再コンバージェンスよりも長く時間がかかります。

## 1ギガビットイーサネットのジャンボフレーム

通常、ジャンボフレームは、ネットワーク上で転送されるパケット数を減らすために使用されます。以下では、1GEトポロジでジャンボフレームを使用する際のガイドラインについて説明します。

- ジャンボフレームは、追加のセットアップは必要ないため、vMotionネットワーク上で自動的に設定されます。
- ジャンボフレームを有効にするためのオプションは、ネットワーク設定ポリシーの下のHyperFlexクラスタプロファイルの下にあります。1GEトポロジを使用する場合は、展開を開始する前にチェックボックスが有効になっていることを確認して、ジャンボフレームを有効にすることができます。

次の手順：

[ネットワークの共通要件チェックリスト](#)を完了します。

## 3 ノードまたは 4 ノードのネットワーク トポロジの選択

3 ノードまたは 4 ノード トポロジを選択するとき、初期展開時に選択されるネットワーク トポロジは、完全な再インストールなしで変更またはアップグレードすることはできないことにご注意ください。将来のニーズを念頭に置いてネットワーク トポロジを慎重に選択し、次の Cisco HyperFlex 製品を考慮してください。

- Cisco VIC ベース ハードウェアまたは Intel NIC ベース アダプタを搭載した 10/25 Gigabit (GE) トポロジ
- ノード拡張を必要とせず、トップ オブラック (ToR) スイッチに使用可能な 10GE ポートがないクラスタ向けの 1GE トポロジ。

Cisco IMC 接続、物理ケーブル配線、ネットワーク設計、および構成の注意事項の詳細については、次の使用可能なトポロジのリストから選択してください。

- [10 または 25GE VIC ベースのトポロジ \(227 ページ\)](#)
- [10 または 25GE NIC ベース トポロジ](#)
- [1 ギガビット イーサネット トポロジ \(232 ページ\)](#)

10/25GE または 1GE ToR 物理ネットワークとケーブルのセクションが完了したら、[ネットワークの共通要件チェックリスト \(212 ページ\)](#) に進みます。

## 10 または 25GE VIC ベースのトポロジ

10 または 25 ギガビット イーサネット (GE) スイッチ トポロジは、スイッチ (デュアルまたはスタック構成のスイッチを使用している場合)、リンクおよびポートの障害から保護する、フル冗長型のデザインを提供します。10/25GE スイッチは、1 台または 2 台のスタンドアロン スイッチとして、またはスイッチ スタック構成で使用することができます。

## 10/25GE VIC ベース トポロジの Cisco IMC 接続

3 ノードおよび 4 ノード 10/25 ギガビット イーサネット (GE) トポロジに、次の Cisco IMC 接続オプションのいずれかを選択します。

- 専用の 1GE Cisco IMC 管理ポートを使用することが推奨されます。このオプションには追加のポートとケーブルが必要ですが、ネットワークの競合を防ぎ、各物理サーバへのアウト オブ バンド アクセスを常にオンにすることができます。
- 共有 LOM 拡張モード (EXT) の使用。このモードでは、シングルワイヤ管理が使用され、Cisco IMC トラフィックが 10/25GE VIC 接続に多重化されます。このモードで操作する場

合、トラフィックの複数のストリームが同じ物理リンク上で共有され、妨害のない到達可能性は保証されません。この展開オプションは推奨されません。

- ファブリック インターコネクトベース環境では、シングルワイヤ管理を使用する場合、内蔵 QpS により Cisco IMC およびサーバ管理への妨害のないアクセスが保証されます。HyperFlex Edge 環境では、QoS が適用されないため、専用管理ポートの使用が推奨されます。

上記の Cisco IMC 接続の選択にかかわらず、同様の Cisco UCS C シリーズサーバについては、『サーバ設置およびサービス ガイド』の次の手順に従い、Cisco IMC に IPv4 管理アドレスを割り当てる必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

## Physical Network and Cabling for 10/25GE VIC-Based Topology

A managed switch (1 or 2) with VLAN capability is required. Cisco fully tests and provides reference configurations for Catalyst and Nexus switching platforms. Choosing one of these switches provides the highest level of compatibility and ensures a smooth deployment and seamless ongoing operations.

Dual switch configuration provides a slightly more complex topology with full redundancy that protects against: switch failure, link failure, and port failure. It requires two switches that may be standalone or stacked, and two 10/25GE ports, one 1GE port for CIMC management, and one Cisco VIC 1457 per server. Trunk ports are the only supported network port configuration.

Single switch configuration provides a simple topology requiring only a single switch, and two 10/25GE ports, one 1GE port for CIMC management, and one Cisco VIC 1457 per server. Switch level redundancy is not provided, however all links/ports and associated network services are fully redundant and can tolerate failures.

### Requirements for both 10 and 25GE Topologies

The following requirements are common to both 10/25GE topologies and must be met before starting deployment:

- Dedicated 1 Gigabit Ethernet (GE) Cisco IMC management port per server (recommended)
  - 1 x 1GE ToR switch ports and one (1) Category 6 ethernet cable for dedicated Cisco IMC management port per HyperFlex node (customer supplied)
- Cisco VIC 1457 (installed in the MLOM slot in each server)
  - Prior generation Cisco VIC hardware is not supported for 2 node or 4 node HX Edge clusters.
  - 2 x 10/25GE ToR switch ports and 2 x 10/25GE SFP+ or SFP28 cables per HyperFlex node (customer supplied. Ensure the cables you select are compatible with your switch model).
  - Cisco VIC 1457 supports 10GE interface speed in Cisco HyperFlex Release 4.0(1a) and later.
  - Cisco VIC 1457 supports 25GE interface speed in Cisco HyperFlex Release 4.0(2a) and later.
  - 40GE interfaces speed is not supported is not supported on the Cisco VIC 1457



## Requirements for HX Edge clusters using 25GE



**Note** Using 25GE mode typically requires the use of forward error correction (FEC) depending on the transceiver or the type & length of cabling selected. The VIC 1400 series by default is configured in CL91 FEC mode (FEC mode “auto” if available in the Cisco IMC UI is the same as CL91) and does not support auto FEC negotiation. Certain switches will need to be manually set to match this FEC mode to bring the link state up. The FEC mode must match on both the switch and VIC port for the link to come up. If the switch in use does not support CL91, you may configure the VIC ports to use CL74 to match the FEC mode available on the switch. This will require a manual FEC mode change in the CIMC UI under the VIC configuration tab. Do not start a HyperFlex Edge deployment until the link state is up as reported by the switch and the VIC ports. CL74 is also known as FC-FEC (Firecode) and CL91 is also known as RS-FEC (Reed Solomon). See the [Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide, Release 4.1](#) for further details on how to change the FEC mode configured on the VIC using the Cisco IMC GUI.

Select either a single switch or dual switch configuration to continue with physical cabling:

## 10/25GE VIC ベースのスイッチ構成の注意事項

最低でも 3 つの VLAN が必要です。

- 次の条件で 1 VLAN: VMware ESXi 管理、ストレージコントローラ VM 管理および Cisco IMC 管理。
  - VMware ESXi 管理およびストレージコントローラ VM 管理は、同じサブネットおよび VLAN に存在する必要があります
  - 専用 Cisco IMC 管理ポートは、上記の管理インターフェイスと同じ VLAN を共有できます。または、オプションで専用サブネットおよび VLAN を使用できます。別の VLAN を使用している場合、L3 接続が上記の管理 VLAN に必要です。また、Intersight 接続要件を満たす必要があります (Cisco Intersight による管理)。
  - Cisco IMC 管理の共有 LOM 拡張モードを使用する場合は、専用の VLAN が推奨されます。
- Cisco HyperFlex のストレージトラフィック用 1 VLAN これは、独立した、またはルーティングされていない VLAN である必要があります。固有である必要があります、管理 VLAN と重複することはできません。
- vMotion トラフィック用 1 VLAN これは、独立した、またはルーティングされていない VLAN にすることができます。



(注) これらの VLAN の必要性を縮小したり、削除したりすることはできません。このインストールが試行された場合は失敗します。

- ゲスト VM トラフィックには、追加の VLAN が必要です。これらの VLAN は、ESXi の追加ポートグループとして設定され、ToR スイッチでポートに面するすべての接続をトランクおよび許可する必要があります。
- これらの追加ゲスト VM VLAN はオプションです。シンプルなネットワーク設計の維持を望む環境では、ゲスト VM トラフィックに上記の同じ管理 VLAN を使用できます。



(注) 同じ物理ポートから複数の vNIC を分割する Cisco VIC の性質により、vswitch-hx-vm-network で構成されたゲスト VM トラフィックが、同じホストで実行されているインターフェイスまたはサービスと L2 を通信することはできません。a) 別の VLAN を使用して L3 ルーティングを実行するか、b) 管理インターフェイスへのアクセスが必要なゲスト VM を vswitch-hx-inband-mgmt vSwitch に配置することをお勧めします。一般に、vm-network vSwitch を除き、ゲスト VM を HyperFlex で設定された vSwitches のいずれにも配置しないでください。使用例としては、いずれかのノードで vCenter を実行する必要があり、実行している ESXi ホストを管理するための接続が必要な場合があります。この場合は、上記の推奨事項のいずれかを使用して、接続が中断されないようにします。

- Cisco VIC に接続されているスイッチポートは、パスが許可された適切な VLAN を使用して、トランク モードで設定する必要があります。
- 専用 Cisco IMC 管理ポートに接続されているスイッチポートは、適切な VLAN で「アクセス モード」で設定する必要があります。
- すべてのクラスタ トラフィックは、10/25GE トポロジ内の ToR スイッチを通過します。
- スパニング ツリー PortFast トランク (トランク ポート) は、すべてのネットワーク ポートで有効にする必要があります。



(注) PortFast の設定に失敗すると、ESXi の起動時に断続的に切断され、物理リンク障害時に必要なネットワークの再コンバージェンスよりも長く時間がかかります。

#### その他の考慮事項

- 必要に応じて、HX Edge ノードにサードパーティ製の NIC カードをさらにインストールできます。ネットワーク ガイドへのリンクについては、第 1 章の項を参照してください。

- VIC 以外のすべてのインターフェイスは、インストールが完了するまでシャットダウンするか、ケーブルを切断している必要があります。
- MLOM スロットでは、HX Edge ノードごとに 1 つの VIC のみがサポートされます。PCIe ベース VIC アダプタは、HX Edge ノードではサポートされていません。

## 3 ノードおよび 4 ノード 10/25GE VIC ベース トポロジの仮想ネットワーク設計

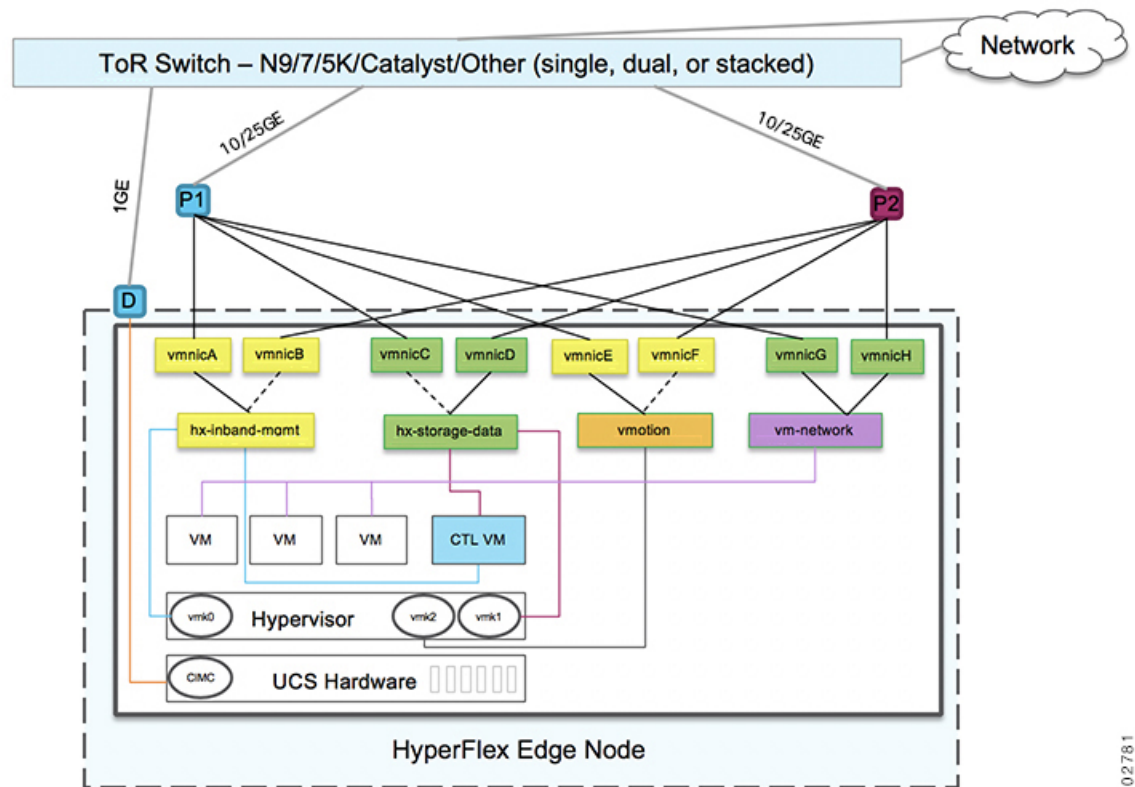
このセクションでは、仮想ネットワーク セットアップについて説明しています。HyperFlex 展開プロセスにより自動で仮想ネットワークがセットアップされるため、アクションは必要ありません。これらの詳細は、情報およびトラブルシューティング目的で下記に記載されています。

### 仮想スイッチ

vSwitch が 4 つ必要です。

- **vswitch-hx-inband-mgmt** : ESXi 管理 (vmk0) 、ストレージコントローラ管理ネットワーク
- **vswitch-hx-storage-data** : ESXi ストレージインターフェイス (vmk1) 、HX ストレージコントローラ データ ネットワーク
- **vmotion** : vMotion インターフェイス (vmk2)
- **vswitch-hx-vm-network** : VM ゲスト ポート グループ

ネットワーク トポロジ:



502781

フェールオーバーの順序 :

- **vswitch-hx-inband-mgmt** : vSwitch 全体がアクティブ/スタンバイに設定されます。デフォルトでは、すべてのサービスが1つのアップリンクポートを使用し、必要に応じてフェールオーバーされます。
- **vswitch-hx-storage-data** : HyperFlex ストレージデータ ネットワークと vmk1 は、インバンド管理および vmotion vSwitches としての逆のフェールオーバー順序を使用して、トラフィックの負荷分散を行います。
- **vmotion** : vMotion VMKernel ポート (vmk2) は post\_install スクリプトの使用時に設定されます。フェールオーバーの順序は、アクティブ/スタンバイに設定されます。
- **vswitch-hx-vm-network** : vSwitch がアクティブ/アクティブに設定されます。必要に応じて、個々のポート グループを上書きできます。

## 1 ギガビットイーサネット トポロジ

1 ギガビットイーサネット (GE) スイッチ トポロジは、要件に応じて2つの設計を提供します。デュアルスイッチ設計は、スイッチ (デュアルまたはスタック スイッチを使用している場合)、リンクおよびポートの障害からネットワークを保護する完全な冗長設計です。他の単一スイッ

トポロジではネットワークの冗長性が提供されないため、実稼働クラスタには推奨されません。

## 1 ギガビットイーサネットトポロジ用 Cisco IMC 接続

3 ノードおよび 4 ノード 10 ギガビットイーサネット (GE) トポロジに、次の Cisco IMC 接続オプションのいずれかを選択します。

- 専用の 1GE Cisco IMC 管理ポートを使用することが推奨されます。このオプションには追加のポートとケーブルが必要ですが、ネットワークの競合を防ぎ、各物理サーバへのアウトオブバンドアクセスを常にオンにすることができます。
- 共有 LOM 拡張モード (EXT) の使用。このモードでは、シングルワイヤ管理が使用され、Cisco LOM トラフィックが 1GE VIC 接続に多重化されます。このモードで操作する場合、トラフィックの複数のストリームが同じ物理リンク上で共有され、妨害のない到達可能性は保証されません。この展開オプションは推奨されません。
  - ファブリック インターコネクトベース環境では、シングルワイヤ管理を使用する場合、内蔵 QoS により Cisco IMC およびサーバ管理への妨害のないアクセスが保証されます。HyperFlex Edge 環境では、QoS が適用されないため、専用管理ポートの使用が推奨されます。

上記の Cisco IMC 接続の選択にかかわらず、同様の Cisco UCS C シリーズサーバについては、『[サーバ設置およびサービス ガイド](#)』の次の手順に従い、Cisco IMC に IPv4 管理アドレスを割り当てる必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

## 1GE トポロジ用物理ネットワークおよびケーブル接続

VLAN 機能を備えたマネージドスイッチ (1 または 2) が必要です。Cisco は、Cisco Catalyst および Cisco Nexus スイッチングプラットフォームのリファレンス構成を完全にテストし、提供します。これらのスイッチのいずれかを選択すると、最高レベルの互換性が提供され、円滑な展開とシームレスな継続的運用が可能になります。

デュアルスイッチのケーブル接続には、スイッチの障害、リンクの障害、スイッチポートの障害、LOM/PCIe NIC HW の障害から保護する完全な冗長性を備えた、少し複雑なトポロジが含まれます。サーバごとに、スタンドアロンまたはスタック構成が行われている 2 つのスイッチ、クラスタおよび VM トラフィックに 4 個の 1GE ポート、CIMC 管理に 1 個の 1GE ポート、1 個の Intel i350 PCIe NIC が必要です。トランクポートは、唯一サポートされているネットワークポート設定です。

シングルスイッチの設定では、1 台のスイッチを必要とするシンプルなトポロジ、クラスタと VM トラフィック用に 2 個の 1GE ポート、CIMC 管理用に 1 個の 1GE ポートを提供し、追加の PCIe NIC は必要ありません。リンクまたはスイッチの冗長性はありません。サポートされている 2 つのネットワークポート設定は、アクセスポートとトランクポートです。



- (注) 冗長性の欠如により、シングルスイッチ 1GE 設定は非実稼働環境に対してのみ推奨されます。

物理的なケーブル接続を続行するには、シングルスイッチまたはデュアルスイッチの設定を選択します。

## 1 ギガビットイーサネットスイッチ設定時の注意事項

- 次の条件で最小の 1 VLAN: VMware ESXi 管理、ストレージコントローラ VM 管理および Cisco IMC 管理。
  - VMware ESXi 管理およびストレージコントローラ VM 管理は、同じサブネットおよび VLAN に存在する必要があります
  - 専用 Cisco IMC 管理ポートは、上記の管理インターフェイスと同じ VLAN を共有できます。または、オプションで専用サブネットおよび VLAN を使用できます。別の VLAN を使用している場合、L3 接続が上記の管理 VLAN に必要です。また、Intersight 接続要件を満たす必要があります (Cisco Intersight による管理)。
- Cisco HyperFlex のストレージトラフィック用 1 VLAN これは、独立した、またはルーティングされていない VLAN である必要があります。固有である必要があり、管理 VLAN と重複することはできません。



- (注) 管理 VLAN と 2 番目のデータ VLAN の両方の必要性を縮小したり、なくしたりすることはできません。このインストールが試行された場合は失敗します。

- ゲスト VM トラフィックには、追加の VLAN が必要です。これらの VLAN は、ESXi の追加ポートグループとして設定され、すべての接続を ToR スイッチにトランクする必要があります。
  - これらの追加ゲスト VM VLAN はオプションです。シンプルなネットワーク設計の維持を望む環境では、ゲスト VM トラフィックに上記の同じ管理 VLAN を使用できます。
- Intel i350 に接続されているスイッチポートは、パスが許可された適切な VLAN を使用して、トランクモードで設定する必要があります。
- 専用 Cisco IMC 管理ポートに接続されているスイッチポートは、適切な VLAN で「アクセスモード」で設定する必要があります。
- VMware vMotion トラフィックは、次の 2 つのパスのいずれかに従います。

- **デュアルスイッチトポロジ:** vMotion は、ストレージデータ ネットワークとは反対のフェールオーバー順序を使用し、ネットワーク障害が発生しない場合は専用の 1GE パスを使用します。Post\_install スクリプトを使用すると、正しい vSwitch の VMkernel インターフェイスが正しいフェールオーバー設定でセットアップされます。ESXi で新しいインターフェイスが作成される (vmk2) ため、専用の VLAN が必要です。
- **シングルスイッチトポロジ:** vMotion は、管理ネットワークと共有されます。Post\_install スクリプトを使用すると、デフォルトのトラフィック シェーパードを持つ新しい ESX インターフェイス (vmk2) で、vMotion がリンクを完全に飽和状態にならないようにします。新しいインターフェイスが作成されるため、専用の VLAN が必要です。

VMware vMotion トラフィックの詳細については、『Cisco HyperFlex Edge 展開ガイド』の「インストール後のタスク」の項を参照してください。

- スパニング ツリー PortFast トランク (トランク ポート) は、すべてのネットワーク ポートで有効にする必要があります。



- (注) PortFast の設定に失敗すると、ESXi の起動時に断続的に切断され、物理リンク障害時に必要なネットワークの再コンバージェンスよりも長く時間がかかります。

## 3 および 4 ノード 1 ギガビットイーサネットトポロジの仮想ネットワーク設計

このセクションでは、仮想ネットワーク セットアップについて説明しています。HyperFlex 展開プロセスにより自動で仮想ネットワークがセットアップされるため、アクションは必要ありません。これらの詳細は、情報およびトラブルシューティング目的で下記に記載されています。

### 仮想スイッチ

各 ESXi ホストで推奨される設定では、次のネットワークを切り分ける必要があります。

- 管理トラフィック ネットワーク
- データ ネットワーク
- vMotion ネットワーク
- VM ネットワーク

最小ネットワーク構成では、最小限で次の 2 つの個別ネットワークが必要です。

- 管理ネットワーク (vMotion と VM ネットワークを含む)
- データ ネットワーク (ストレージトラフィック用)

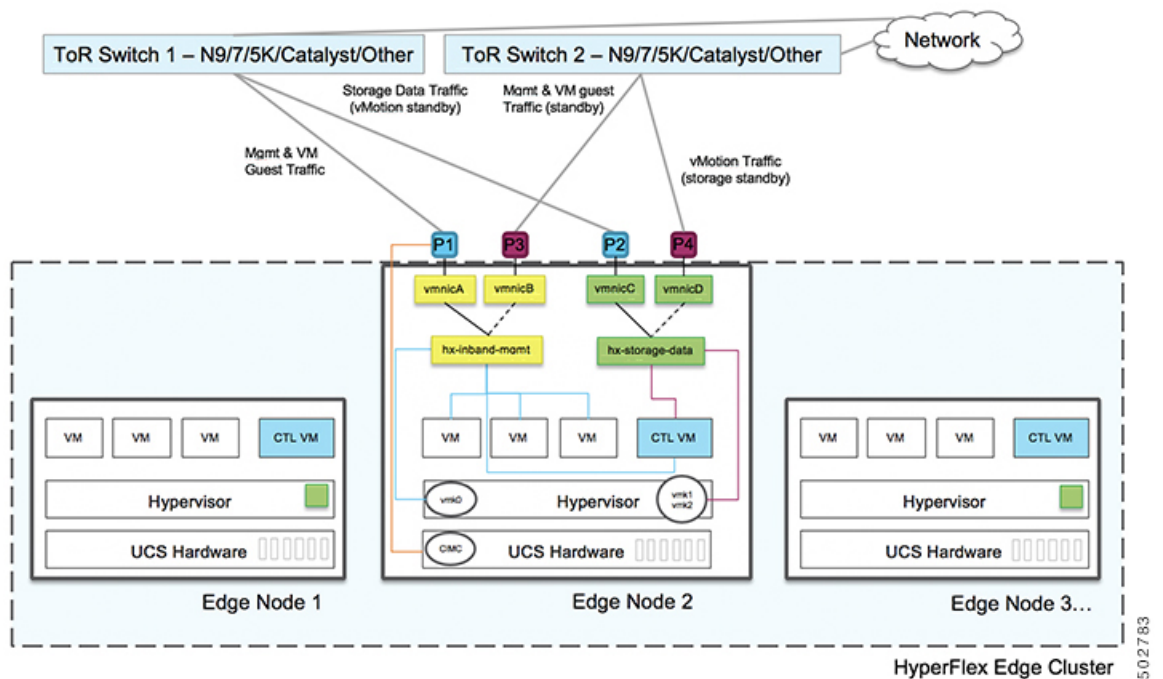
それぞれのネットワークに対応する 2 つの vSwitch が必要です。

- **vswitch-hx-inband-mgmt** : ESXi 管理 (vmk0)、HyperFlex ストレージ コントローラ管理、VM ゲスト ポートグループ
- **vswitch-hx-storage-data**—HyperFlex ESXi ストレージ インターフェイス (vmk1)、HyperFlex ストレージ データ ネットワーク、vMotion (vmk2)。



(注) シングル スイッチの設定を使用して HyperFlex Edge を導入すると、ストレージ データ vSwitch および関連付けられたポートグループのフェールオーバー順序 (スタンバイ アダプタのみ追加された状態) が表示されます。アクティブ アダプタが不足している場合でも、それが原因でクラスタに機能上の問題が生じることはありません。フェールオーバー順序はインストール プロセスで設定された順序のままにしておくことを推奨します。

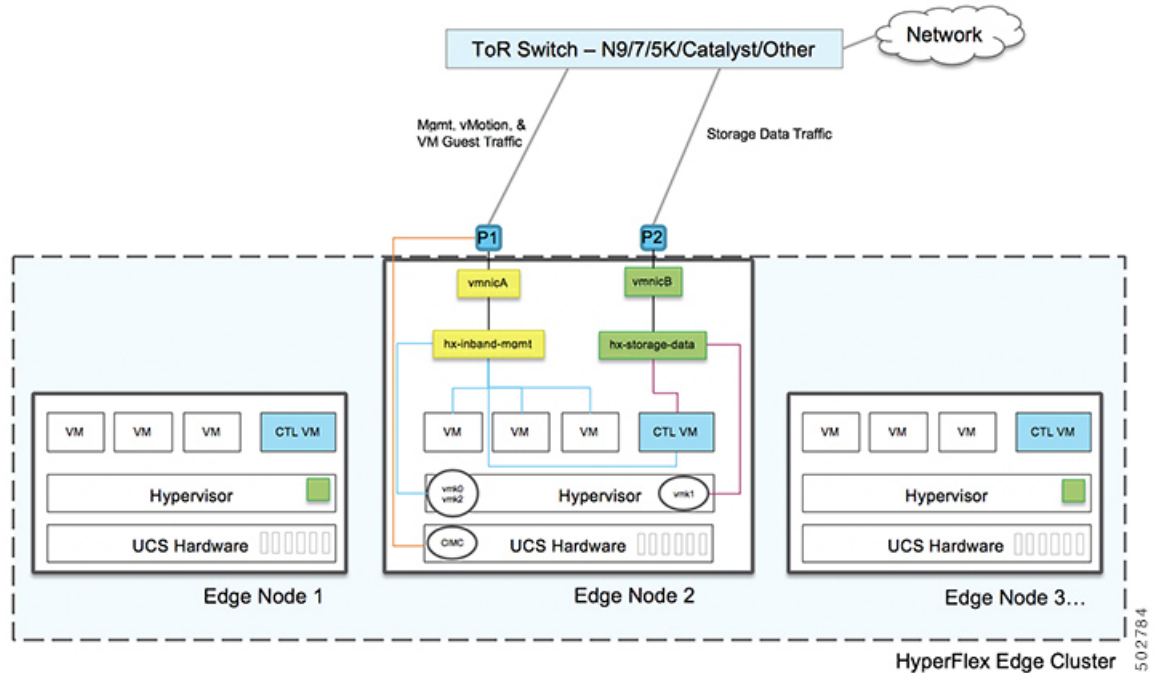
### ネットワーク トポロジ: デュアル スイッチの設定



5.02783



## ネットワーク トポロジ: シングル スイッチの設定



## フェールオーバー順序: -デュアルスイッチ設定のみ:

**vswitch-hx-inband-mgmt** : 2つのアップリンク上で、vSwitch全体がアクティブ/スタンバイに設定されます。デフォルトでは、すべてのサービスが1つのアップリンクポートを使用し、必要に応じてフェールオーバーされます。VMポートグループのフェールオーバー順序は、必要に応じて、かつより適切なロードバランシングになるようにオーバーライドできます。

**vswitch-hx-storage-data** : HyperFlexストレージデータネットワークとvnic1は、同じアクティブ/スタンバイ順序に設定されます。post\_installスクリプトを使用して設定されている場合、vMotion VMKernelポートは反対の順序を使用するように設定されます。これにより、直接接続リンクの完全な使用率が確保されます。

## 2 ノード 2 ルームのネットワーク トポロジの選択

開始するには、以下の使用可能なネットワーク トポロジのいずれかを選択します。トポロジは、シスコの推奨事項に基づいて優先順位順に表示されます。

- [10 または 25 ギガビット イーサネット トポロジ \(240 ページ\)](#)
- [ルーム単位トポロジでの 10 または 25 ギガビット イーサネット スタック スイッチ \(246 ページ\)](#)
- [ルーム単位トポロジでの 10 または 25 ギガビット イーサネット シングル スイッチ \(250 ページ\)](#)

物理ネットワークとケーブルのセクションが完了したら、[ネットワークの共通要件チェックリスト \(253 ページ\)](#) に進みます。

## 2 ノード 2 ルームの使用例

HyperFlex Edge は、ワークロードの要件に応じて、多くの柔軟な導入オプションを提供しています。標準のトポロジについては、シングルスイッチ、デュアルスイッチ、1GE、10GE、および 25GE オプションがあり、[2 ノード ネットワーク トポロジの選択 \(203 ページ\)](#) および [3 ノードまたは4ノードのネットワーク トポロジの選択 \(227 ページ\)](#) で説明されています。一部の設計では、建物またはキャンパス内の 2 つの部屋に「引き延ばされた」2 ノードクラスタを配置する必要があります。このタイプのネットワークトポロジは、完全な HyperFlex ストレッチクラスタ導入と区別するために、2 ノード 2 ルーム設計とも呼ばれます。

この設計は、クラスタの可用性と特定の障害シナリオを許容する能力を高めるために選択されることがあります。シスコでは現在、このタイプのトポロジの導入を推奨しておらず、同じラック内に置かれる、適切に設計された 2 ノードクラスタを推奨しています。次に、このトポロジがシスコ推奨のベストプラクティスと見なされない理由をいくつか示します。

- 電源障害の問題は、信頼性の高い電源と無停電電源 (UPS) を使用すれば緩和できます。
- この設計では、より多くのシングルポイント障害が発生します。オーバーサブスクライブの可能性があり、適切な QoS の実装を必要とする、スイッチ間リンクを備えた追加のスイッチングインフラストラクチャが必要だからです。
- アップグレード手順が複雑になるため、すべてのコンポーネントをエンドツーエンドでアップグレードするように慎重に計画する必要があります。
- HyperFlex ストレッチクラスタと同じレベルのミッションクリティカルなアプリケーションの可用性を提供できません (詳細については、[Cisco HyperFlex Systems Stretched Cluster Guide, Release 4.5](#) を参照してください)。HyperFlex Edge は Edge ワークロードを実行するように設計されており、同じパフォーマンス、データ復元力、および可用性の保証を提供しません。ミッションクリティカルなアプリケーションを実行するときには、適切なストレッチクラスタを展開してください。
- 10GE エンドツーエンド、最大 1.5ms RTT、および Intersight またはローカル監視への独立したネットワークパスの要件があります (以下に詳細を記載します)
- 本来はシンプルな設計の、全体的な複雑さが高くなります

2 ノード 2 ルーム トポロジでは、本来は単純な手段 (たとえば、デュアル冗長スイッチ、冗長電源/UPS など) で軽減できるはずの、不要な複雑さが環境に追加されるため、意図せずに可用性が低下する可能性があります。

これらのベストプラクティスの推奨事項はありますが、このトポロジを選択して HyperFlex Edge を展開することは可能であり、完全にサポートされています。この章の残りの部分では、このようなトポロジを展開するためのさまざまな要件と詳細について説明します。



- (注) 2 ノード 2 ルーム トポロジは、2 つのコンバージド ノードを超えて拡張することはできません。以前の章で説明したように、他の 10GE+ トポロジは、より大きなクラスタに拡張できます。将来クラスタの拡張が必要になる可能性がある場合は、このトポロジを展開しないでください。

## 2 ノード 2 ルームの要件

2 ノード 2 ルームの展開を計画する場合は、次の要件を満たす必要があります。

- ネットワーキング速度は、エンドツーエンドで 10 / 25GE 以上である必要があります。これは、すべてのサーバがネイティブ 10 / 25GE を使用してトップ オブ ラック (ToR) スイッチに接続し、すべてのスイッチが少なくとも 1 つの 10GE インターフェイスで相互接続される必要があることを意味します。
- ラウンドトリップ時間 (RTT) とは、トラフィックが両方向に移動するのにかかる時間ですが、これは各サーバ ルーム間で 1.5ms を超えてはなりません。このしきい値を超えると、ストレージクラスタのパフォーマンスが大幅に低下します。最適化されたローカル読み取り用のサイト親和性を備えた HyperFlex ストレッチクラスタとは異なり、2 ノード 2 ルーム設計のすべての読み取りと書き込みはスイッチ間リンク (ISL) を通過するので、パフォーマンスはネットワーク遅延に直接比例します。これらの理由から、このトポロジはキャンパスの距離を超えて使用しないでください (例: 1 km 未満)。
- 他のバックグラウンドトラフィックが ISL を飽和させ、ストレージのパフォーマンスに影響を与えないように、ストレージデータ ネットワークには最低限の Quality of Service (QoS) を実装する必要があります。付録には、Catalyst 9300 スイッチのサンプル QoS 設定が含まれています。
- 両方のルームには、クラスタ監視として機能する Intersight (SaaS またはアプライアンス) への独立したネットワークパスが必要です。独立したパスがないと、どちらの部屋で損失が生じた場合でも、許容できない問題になります。たとえば、ルーム #1 とルーム #2 のインターネット接続がルーム #1 から提供されている場合、ルーム #1 に障害が発生すると、ルーム #2 のインターネットは動作できなくなります。このような厳格な要件があるため、一部の環境では 2 ノード 2 ルーム設計を使用できません。
- ローカル監視は、設計で使用することもできます。この場合、同じ原則が適用されます。ローカルの監視サーバに到達できるようにするには、両方のルームが互いに依存しない独立したパスを持つ必要があります。
- HyperFlex Edge 2 ノード 2 ルーム トポロジは、HyperFlex Data Platform (HXDP) リリース 4.5 (1a) で導入されたもので、それ以降でサポートされています。

## 10 または 25 ギガビットイーサネット トポロジ

クロス接続の 10 または 25 ギガビットイーサネット (GE) スイッチ トポロジは、ルーム、スイッチ、リンクおよびポートの障害から保護する、フル冗長型のデザインを提供します。各ルームに 1 つの 10/25GE スイッチが必要です。

このトポロジでは、各サーバが両方のルームに直接クロス接続されます。これにより、専用リンクが提供され、スイッチ間リンク (ISL) へのオーバーサブスクリプションが防止されます。このトポロジでは、サーバリンクの障害発生時に高帯域幅を処理するために、各ルーム間に最低 10GE ISL が必要です。

### 10/25GE クロス接続トポロジ用物理ネットワークとケーブル接続

それぞれのルームには、VLAN 機能を備えたマネージド 10GE スイッチが必要です。Cisco は、Catalyst および Nexus スイッチングプラットフォームのリファレンス構成を完全にテストし、提供します。これらのスイッチのいずれかを選択すると、最高レベルの互換性が提供され、円滑な展開とシームレスな継続的運用が可能になります。

それぞれのルームには、1 つのスイッチ、および 2 つの 10/25GE ポート、1 つの 1GE ポート (CIMC 管理用)、およびサーバごとに 1 つの Cisco VIC 1457 が必要です。冗長性は、ルームレベルで提供されます。いずれかのルームの損失および小規模な障害 (スイッチ障害、リンク障害、ポート障害など) を許容できます。

#### 10/25GE クロス接続トポロジの要件

展開を開始する前に、両方のルームで次の要件を満たす必要があります。

- サーバごとの専用 1 ギガビットイーサネット (GE) Cisco IMC 管理ポート (推奨)
- 専用 Cisco IMC 管理ポート (お客様が提供) 用の 2 個の 1GE ToR スイッチポートと、2 本のカテゴリ 6 イーサネットケーブル
- Cisco VIC 1457 (各サーバの MLOM スロットに取り付けられている)
- 旧世代の Cisco VIC ハードウェアは、2 ノードの HX Edge クラスタではサポートされていません。
- 4 個の 10/25GE ToR スイッチポートおよび 4 本の 10/25GE SFP+ または SFP28 ケーブル (お客様が提供。選択したケーブルがスイッチモデルと互換性があることを確認します。)
- Cisco VIC 1457 は、10GE または 25GE のインターフェイス速度をサポートします。
- Cisco VIC 1457 は、40GE のインターフェイス速度をサポートしていません。

### 25GE を使用する HX Edge クラスタの要件



- (注) 25GE モードを使用するには、通常、選択したケーブルのタイプと長さに応じて、前方誤り訂正 (FEC) を使用する必要があります。デフォルトでは、VIC 1400 シリーズは CL91 FEC モードで設定されます (Cisco IMC UI で使用可能な場合、FEC モード「auto」は CL91 と同じです)。自動 FEC ネゴシエーションはサポートされません。特定のスイッチでリンクステートをアップにするには、この FEC モードに合わせて手動で設定する必要があります。リンクをアップにするには、スイッチと VIC ポートの両方で FEC モードが一致している必要があります。使用中のスイッチが CL91 をサポートしていない場合、スイッチで使用可能な FEC モードと一致させて、VIC ポートが CL74 を使用するように設定できます。これには、[VIC 設定 (VIC configuration)] タブの [CIMC UI] で、手動で FEC モードを変更する必要があります。HyperFlex Edge の展開は、スイッチと VIC ポートからリンクステートがアップになったと報告されるまで、開始しないでください。CL74 は FC-FEC (ファイアコード) と呼ばれ、CL91 は RS-FEC (リードソロモン) と呼ばれています。Cisco IMC GUI を使用して VIC で設定されている FEC モードを変更する方法については、[Cisco UCS C シリーズ統合管理コントローラ、リリース 4.1 GUI コンフィギュレーションガイド](#)を参照してください。

## 10/25 ギガビットイーサネット クロス接続の物理的なケーブル接続



**警告** 適切なケーブル配線は、ネットワークの完全な冗長性を確保するために重要です。

- 専用の Cisco IMC を使用している場合は、各サーバの 1GE 管理ポート (サーバの背面にある「M」というラベルが付いた) をローカルスイッチに接続します。
- 各サーバの Cisco VIC の 4 つの 10/25GE ポートのうち 1 つを、ルーム 1 の同一の ToR スイッチに接続します。
  - 同じスイッチに接続するには、各サーバで同じポート番号を使用します。



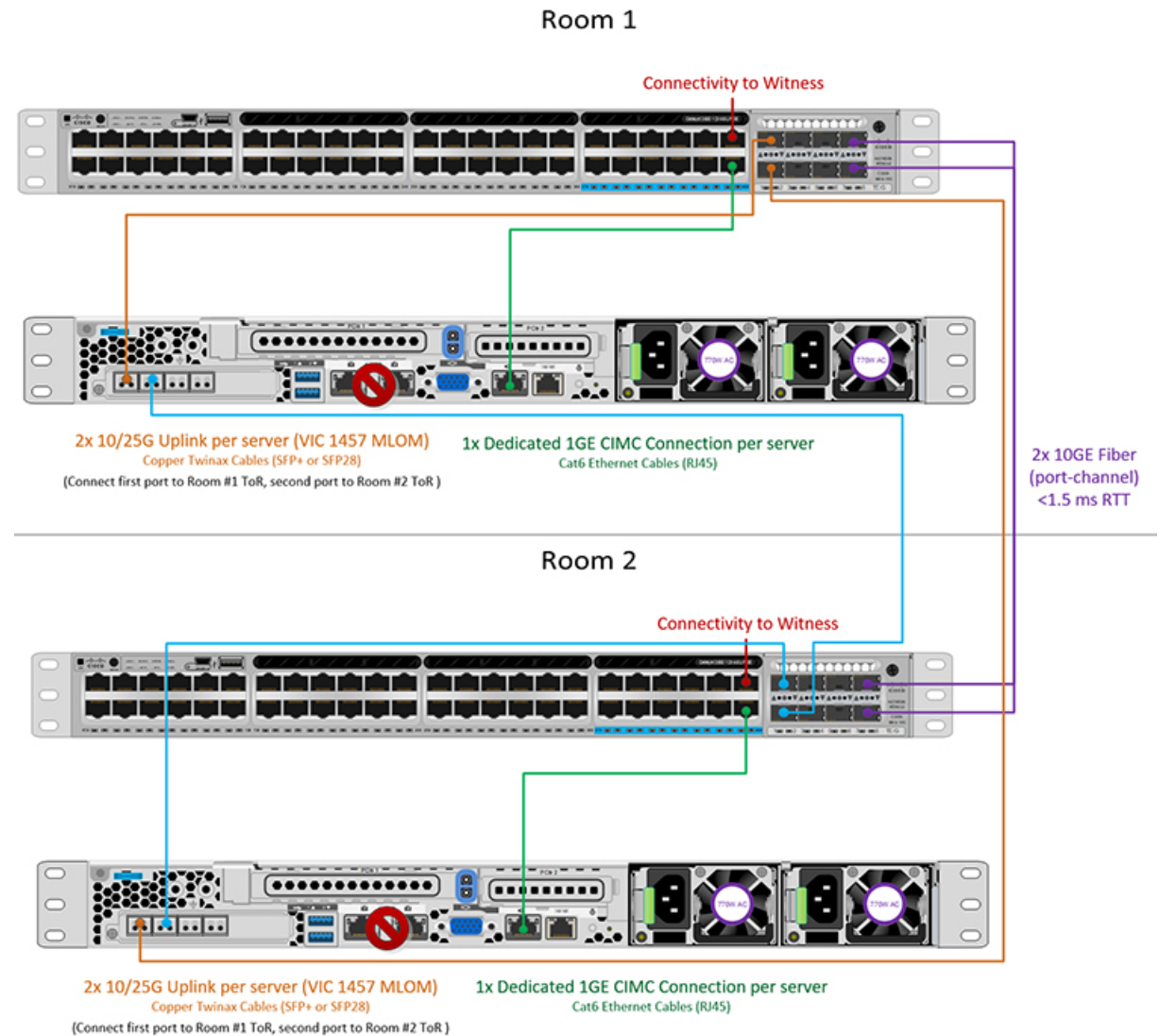
- (注) 同じ VIC ポート番号を使用しない場合、サーバ間のトラフィックに対して余分なホップが発生し、2 つのスイッチ間で不必要に帯域幅が消費されます。

- 各サーバの Cisco VIC の 2 番目の 10/25GE ポートを、ルーム 2 の ToR スイッチに接続します。
- クラスタのインストール前に追加の 10/25GE ポートを接続しないでください。クラスタ展開後、追加で 2 つの 10/25GE ポートをゲスト VM トラフィックにオプションで使用することができます。

## すべての2ノード2ルームトポロジのCisco IMC接続

- 各スイッチに、Intersightまたはローカル監視サーバへの独立したネットワークパスがあることを確認します。

## 2ノード2ルームクロス接続



## すべての2ノード2ルームトポロジのCisco IMC接続

2ノード10/25ギガビットイーサネット (GE) トポロジに、次のCisco IMC接続オプションのいずれかを選択します。

- 専用の1GE Cisco IMC管理ポートを使用することが推奨されます。このオプションには追加のポートとケーブルが必要ですが、ネットワークの競合を防ぎ、各物理サーバへのアウトオブバンドアクセスを常にオンにすることができます。

- 共有 LOM 拡張モード (EXT) の使用。このモードでは、シングルワイヤ管理が使用され、Cisco IMC トラフィックが 10/25GE VIC 接続に多重化されます。このモードで操作する場合、トラフィックの複数のストリームが同じ物理リンク上で共有され、妨害のない到達可能性は保証されません。この展開オプションは推奨されません。
- ファブリック インターコネクトベース環境では、シングルワイヤ管理を使用する場合、内蔵 QpS により Cisco IMC およびサーバ管理への妨害のないアクセスが保証されます。HyperFlex Edge 環境では、QoS が適用されないため、専用管理ポートの使用が推奨されません。
- Cisco IMC に IPv4 管理アドレスを割り当てます。詳細については、対応する Cisco UCS C シリーズサーバの [Server Installation and Service Guide](#) の手順を参照してください。HyperFlex は IPv6 アドレスをサポートしていません。

### 10/25GE VIC ベースのスイッチ構成の注意事項

最低でも 3 つの VLAN が必要です。

- 次の条件で 1 VLAN: VMware ESXi 管理、ストレージコントローラ VM 管理および Cisco IMC 管理。
  - VMware ESXi 管理およびストレージコントローラ VM 管理は、同じサブネットおよび VLAN に存在する必要があります
  - 専用 Cisco IMC 管理ポートは、上記の管理インターフェイスと同じ VLAN を共有できます。または、オプションで専用サブネットおよび VLAN を使用できます。別の VLAN を使用している場合、L3 接続が上記の管理 VLAN に必要です。また、Intersight 接続要件を満たす必要があります。
  - Cisco IMC 管理の共有 LOM 拡張モードを使用する場合は、専用の VLAN が推奨されます。
- Cisco HyperFlex のストレージトラフィック用 1 VLAN これは、独立した、またはルーティングされていない VLAN である必要があります。固有である必要があります、管理 VLAN と重複することはできません。
- vMotion トラフィック用 1 VLAN これは、独立した、またはルーティングされていない VLAN にすることができます。



(注) これらの VLAN の必要性を縮小したり、削除したりすることはできません。このインストールが試行された場合は失敗します。

- ゲスト VM トラフィックには、追加の VLAN が必要です。これらの VLAN は、ESXi の追加ポートグループとして設定され、ToR スイッチでポートに面するすべての接続をリンクおよび許可する必要があります。

- これらの追加ゲスト VM VLAN はオプションです。シンプルなネットワーク設計の維持を望む環境では、ゲスト VM トラフィックに上記の同じ管理 VLAN を使用できません。



(注) 同じ物理ポートから複数の vNIC を分割する Cisco VIC の性質により、vswitch-hx-vm-network で構成されたゲスト VM トラフィックが、同じホストで実行されているインターフェイスまたはサービスと L2 を通信することはできません。a) 別の VLAN を使用して L3 ルーティングを実行するか、b) 管理インターフェイスへのアクセスが必要なゲスト VM を vswitch-hx-inband-mgmt vSwitch に配置することをお勧めします。一般に、vm-network vSwitch を除き、ゲスト VM を HyperFlex で設定された vSwitches のいずれにも配置しないでください。使用例としては、いずれかのノードで vCenter を実行する必要があるため、実行している ESXi ホストを管理するための接続が必要な場合があります。この場合は、上記の推奨事項のいずれかを使用して、接続が中断されないようにします。

- Cisco VIC に接続されているスイッチポートは、パスが許可された適切な VLAN を使用して、トランク モードで設定する必要があります。
- 専用 Cisco IMC 管理ポートに接続されているスイッチポートは、適切な VLAN で「アクセス モード」で設定する必要があります。
- すべてのクラスター トラフィックは、10/25GE トポロジ内の ToR スイッチを通過します。
- スパニング ツリー PortFast トランク (トランク ポート) は、すべてのネットワーク ポートで有効にする必要があります。



(注) PortFast の設定に失敗すると、ESXi の起動時に断続的に切断され、物理リンク障害時に必要なネットワークの再コンバージェンスよりも長く時間がかかります。

### その他の考慮事項

- 必要に応じて、HX Edge ノードにサードパーティ製の NIC カードをさらにインストールできます。ネットワーク ガイドへのリンクについては、第 1 章の項を参照してください。
- VIC 以外のすべてのインターフェイスは、インストールが完了するまでシャットダウンするか、ケーブルを切断している必要があります。
- MLOM スロットでは、HX Edge ノードごとに 1 つの VIC のみがサポートされます。PCIe ベース VIC アダプタは、HX Edge ノードではサポートされていません。



## 2 ノード 10/25GE VIC ベース トポロジの仮想ネットワーク設計

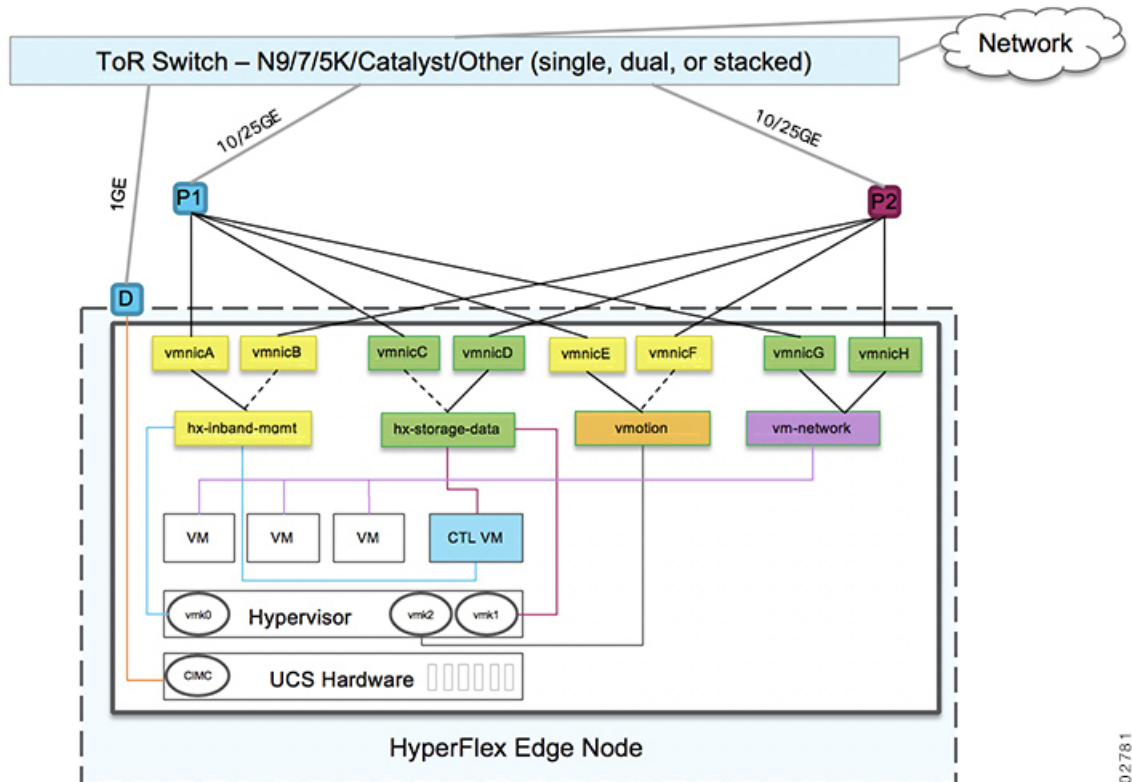
このセクションでは、仮想ネットワーク セットアップについて説明しています。HyperFlex 展開プロセスにより自動で仮想ネットワークがセットアップされるため、アクションは必要ありません。これらの詳細は、情報およびトラブルシューティング目的で下記に記載されています。

### 仮想スイッチ

vSwitch が 4 つ必要です。

- **vswitch-hx-inband-mgmt** : ESXi 管理 (vmk0)、ストレージコントローラ管理ネットワーク
- **vswitch-hx-storage-data** : ESXi ストレージインターフェイス (vmk1)、HX ストレージコントローラ データ ネットワーク
- **vmotion**—vMotion インターフェイス (vmk2)
- **vswitch-hx-vm-network** : VM ゲスト ポート グループ

### ネットワーク トポロジ (Network Topology)



5.02781

## フェールオーバーの順序：

- **vswitch-hx-inband-mgmt** : vSwitch 全体がアクティブ/スタンバイに設定されます。デフォルトでは、すべてのサービスが1つのアップリンクポートを使用し、必要に応じてフェールオーバーされます。
- **vswitch-hx-storage-data** : HyperFlex ストレージデータ ネットワークと vmk1 は、インバンド管理および vmotion vSwitches としての逆のフェールオーバー順序を使用して、トラフィックの負荷分散を行います。
- **vmotion** : vMotion VMKernel ポート (vmk2) は post\_install スクリプトの使用時に設定されます。フェールオーバーの順序は、アクティブ/スタンバイに設定されます。
- **vswitch-hx-vm-network** : vSwitch がアクティブ/アクティブに設定されます。必要に応じて、個々のポート グループを上書きできます。

## ルーム単位トポロジでの 10 または 25 ギガビットイーサネット スタック スイッチ

この 10 または 25 ギガビットイーサネット (GE) スイッチ トポロジは、ルーム、スイッチ、リンクおよびポートの障害から保護する、フル冗長型のデザインを提供します。各ルームには、少なくとも 2 台の 10/25GE スイッチのスイッチ スタックが必要です。スイッチスタックが使用できない場合は、デュアルスタンドアロン スイッチを組み合わせると同様の結果を得ることができます。各ルームの 2 台のスイッチ間、およびルーム間の両方のスイッチスタック間に十分な帯域幅があることを確認します。

このトポロジでは、各サーバは各ルームのローカルスイッチだけに直接接続されます。クロス接続トポロジとは異なり、ルーム間のすべてのクラスタストレージと管理トラフィックを伝送するためのコンポーネントとして、スイッチ間リンク (ISL) が重要な役割を果たします。ISL は、最小 10GE で動作し、最大 RTT 遅延は 1.5ms である必要があります。また、リンクが飽和状態にならないように、ポートチャネル内の複数のリンクで構成する必要があります。このトポロジでは、2つのルーム間でストレージトラフィックが他のすべてのバックグラウンドトラフィックとともに混在するため、ストレージデータトラフィックにサービス品質 (QoS) を実装することが不可欠です。HyperFlex ストレージの信頼性とパフォーマンスを維持するには、ストレージトラフィックに何らかの優先度キューイングを実装する必要があります。

## ルーム単位トポロジでの 10/25GE スタック スイッチの物理ネットワークとケーブル接続



**警告** 適切なケーブル配線は、ネットワークの完全な冗長性を確保するために重要です。

デュアルまたはスタック スイッチを使用して展開するには (ビジュアル レイアウトについては、次の図を参照してください)。

- 専用の Cisco IMC を使用している場合は、各サーバ (サーバの背面に「M」というラベルが付いている) の 1GE 管理ポートを 2 つのスイッチのいずれかに接続します。

- 各サーバの Cisco VIC の 4 つの 10/25GE ポートのうち 1 つを、**同じルームの**同一の ToR スイッチに接続します。
- 同じスイッチに接続するには、各サーバで同じポート番号を使用します。



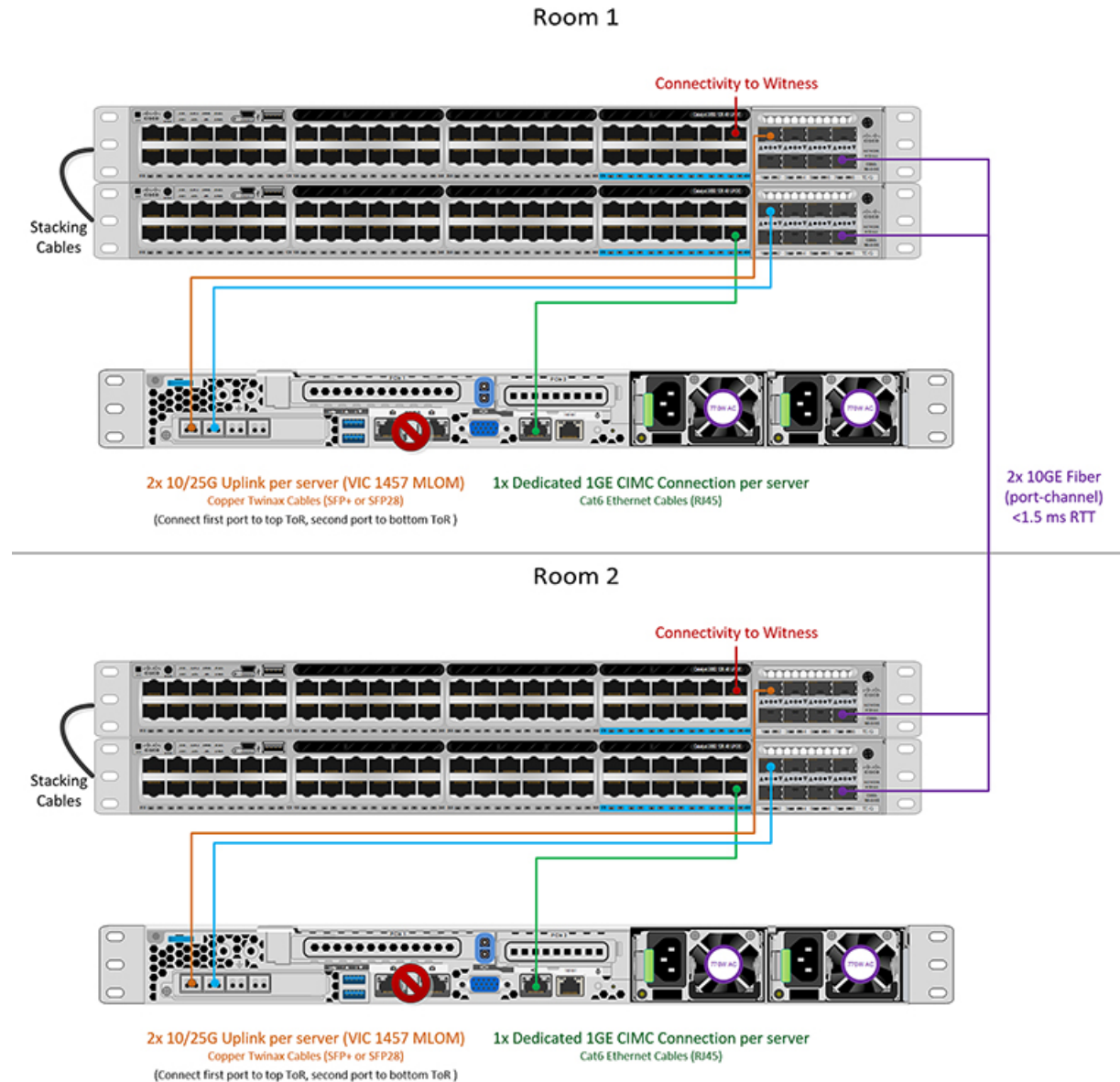
---

(注) 同じ VIC ポート番号を使用しない場合、サーバ間のトラフィックに対して余分なホップが発生し、2 つのスイッチ間で不必要に帯域幅が消費されます。

---

- 各サーバの Cisco VIC の 2 番目の 10/25GE ポートを、**同じルームの** ToR スイッチに接続します。同じスイッチに接続するには、各サーバで同じポート番号を使用します。
- クラスターのインストール前に追加の 10/25GE ポートを接続しないでください。クラスター展開後、追加で 2 つの 10/25GE ポートをゲスト VM トラフィックにオプションで使用することができます。
- 各スイッチに、Intersight またはローカル監視サーバへの独立したネットワークパスがあることを確認します。

## 2 ノード 2 ルーム デュアル/スタック スイッチ



## 10/25 ギガビットイーサネット スタック スイッチの物理的なケーブル接続

各ルームには、VLAN 機能を備えた管理対象 10GE スイッチのペアが必要です。Cisco は、Catalyst および Nexus スイッチングプラットフォームのリファレンス構成を完全にテストし、提供します。これらのスイッチのいずれかを選択すると、最高レベルの互換性が提供され、円滑な展開とシームレスな継続的運用が可能になります。

それぞれのルームには、デュアルまたはスタック スイッチ、および 2 つの 10/25GE ポート、CIMC 管理用の 1 つの 1 GE ポート、そしてサーバごとに 1 つの Cisco VIC 1457 サーバが必要

です。冗長性は、ルームレベルで提供されます。いずれかのルームの損失および小規模な障害（スイッチ障害、リンク障害、ポート障害など）を許容できます。

### 10/25GE スタック スイッチ トポロジの要件

展開を開始する前に、両方のルームで次の要件を満たす必要があります。

- サーバごとの専用 1 ギガビットイーサネット (GE) Cisco IMC 管理ポート (推奨)
- 専用 Cisco IMC 管理ポート (お客様が提供) 用の 2 個の 1GE ToR スイッチ ポートと、2 本のカテゴリ 6 イーサネット ケーブル
- Cisco VIC 1457 (各サーバの MLOM スロットに取り付けられている)
- 旧世代の Cisco VIC ハードウェアは、2 ノードの HX Edge クラスタではサポートされていません。
- 4 個の 10/25GE ToR スイッチ ポートおよび 4 本の 10/25GE SFP + または SFP28 ケーブル (お客様が提供。選択したケーブルがスイッチモデルと互換性があることを確認します。)
- Cisco VIC 1457 は、10GE または 25GE のインターフェイス速度をサポートします。
- Cisco VIC 1457 は、40GE のインターフェイス速度をサポートしていません。

### 25GE を使用する HX Edge クラスタの要件



- (注) 25GE モードを使用するには、通常、選択したケーブルのタイプと長さに応じて、前方誤り訂正 (FEC) を使用する必要があります。デフォルトでは、VIC 1400 シリーズは CL91 FEC モードで設定されます (Cisco IMC UI で使用可能な場合、FEC モード「auto」は CL91 と同じです)。自動 FEC ネゴシエーションはサポートされません。特定のスイッチでリンク ステータスをアップにするには、この FEC モードに合わせて手動で設定する必要があります。リンクをアップにするには、スイッチと VIC ポートの両方で FEC モードが一致している必要があります。使用中のスイッチが CL91 をサポートしていない場合、スイッチで使用可能な FEC モードと一致させて、VIC ポートが CL74 を使用するように設定できます。これには、[VIC 設定 (VIC configuration)] タブの [CIMC UI] で、手動で FEC モードを変更する必要があります。HyperFlex Edge の展開は、スイッチと VIC ポートからリンク ステータスがアップになったと報告されるまで、開始しないでください。CL74 は FC-FEC (ファイアコード) と呼ばれ、CL91 は RS-FEC (リードソロモン) と呼ばれています。Cisco IMC GUI を使用して VIC で設定されている FEC モードを変更する方法については、[Cisco UCS C シリーズ統合管理コントローラ、リリース 4.1 GUI コンフィギュレーションガイド](#)を参照してください。

## ルーム単位トポロジでの 10 または 25 ギガビットイーサネット シングル スイッチ

この 10 または 25 ギガビットイーサネット (GE) スイッチトポロジは、ルーム、スイッチ、リンクおよびポートの障害から保護する、フル冗長型のデザインを提供します。各ルームに 1 つの 10/25GE スイッチが必要です。ルームを結ぶ 2 台のスイッチ間に十分な帯域幅があることを確認します。

このトポロジでは、各サーバは各ルームのローカルスイッチに直接接続されます。クロス接続トポロジとは異なり、ルーム間のすべてのクラスタストレージと管理トラフィックを伝送するためのコンポーネントとして、スイッチ間リンク (ISL) が重要な役割を果たします。ISL は、最小 10GE で動作し、最大 RTT 遅延は 1.5ms である必要があります。また、リンクが飽和状態にならないように、ポートチャンネル内の複数のリンクで構成する必要があります。このトポロジでは、2 つのルーム間でストレージトラフィックが他のすべてのバックグラウンドトラフィックとともに混在するため、ストレージデータトラフィックにサービス品質 (QoS) を実装することが不可欠です。HyperFlex ストレージの信頼性とパフォーマンスを維持するには、ストレージトラフィックに何らかの優先度キューイングを実装する必要があります。

## ルーム単位トポロジでの 10/25GE シングル スイッチの物理ネットワークとケーブル接続

それぞれのルームには、VLAN 機能を備えたマネージド 10GE スイッチが必要です。Cisco は、Catalyst および Nexus スイッチングプラットフォームのリファレンス構成を完全にテストし、提供します。これらのスイッチのいずれかを選択すると、最高レベルの互換性が提供され、円滑な展開とシームレスな継続的運用が可能になります。

それぞれのルームには、1 つの 10/25GE スイッチと、2 つの 10/25GE ポート、CIMC 管理用の 1 つの 1 GE ポート、サーバごとに 1 つの Cisco VIC 1457 サーバが必要です。冗長性は、ルームレベルで提供されます。いずれかのルームの損失および小規模な障害 (スイッチ障害、リンク障害、ポート障害など) を許容できます。

### 10/25GE シングル スイッチ トポロジの要件

展開を開始する前に、両方のルームで次の要件を満たす必要があります。

- サーバごとの専用 1 ギガビットイーサネット (GE) Cisco IMC 管理ポート (推奨)
- 専用 Cisco IMC 管理ポート (お客様が提供) 用の 2 個の 1GE ToR スイッチポートと、2 本のカテゴリ 6 イーサネットケーブル
- Cisco VIC 1457 (各サーバの MLOM スロットに取り付けられている)
- 旧世代の Cisco VIC ハードウェアは、2 ノードの HX Edge クラスタではサポートされていません。
- 4 個の 10/25GE ToR スイッチポートおよび 4 本の 10/25GE SFP+ または SFP28 ケーブル (お客様が提供。選択したケーブルがスイッチモデルと互換性があることを確認します。)
- Cisco VIC 1457 は、10GE または 25GE のインターフェイス速度をサポートします。

- Cisco VIC 1457 は、40GE のインターフェイス速度をサポートしていません。

### 25GE を使用する HX Edge クラスタの要件



- (注) 25GE モードを使用するには、通常、選択したケーブルのタイプと長さに応じて、前方誤り訂正 (FEC) を使用する必要があります。デフォルトでは、VIC 1400 シリーズは CL91 FEC モードで設定されます (Cisco IMC UI で使用可能な場合、FEC モード「auto」は CL91 と同じです)。自動 FEC ネゴシエーションはサポートされません。特定のスイッチでリンクステータスをアップにするには、この FEC モードに合わせて手動で設定する必要があります。リンクをアップにするには、スイッチと VIC ポートの両方で FEC モードが一致している必要があります。使用中のスイッチが CL91 をサポートしていない場合、スイッチで使用可能な FEC モードと一致させて、VIC ポートが CL74 を使用するように設定できます。これには、[VIC 設定 (VIC configuration)] タブの [CIMC UI] で、手動で FEC モードを変更する必要があります。HyperFlex Edge の展開は、スイッチと VIC ポートからリンクステータスがアップになったと報告されるまで、開始しないでください。CL74 は FC-FEC (ファイアコード) と呼ばれ、CL91 は RS-FEC (リードソロモン) と呼ばれています。Cisco IMC GUI を使用して VIC で設定されている FEC モードを変更する方法については、[Cisco UCS C シリーズ統合管理コントローラ、リリース 4.1 GUI コンフィギュレーションガイド](#)を参照してください。

## 10/25 ギガビットイーサネットシングルスイッチの物理的なケーブル接続

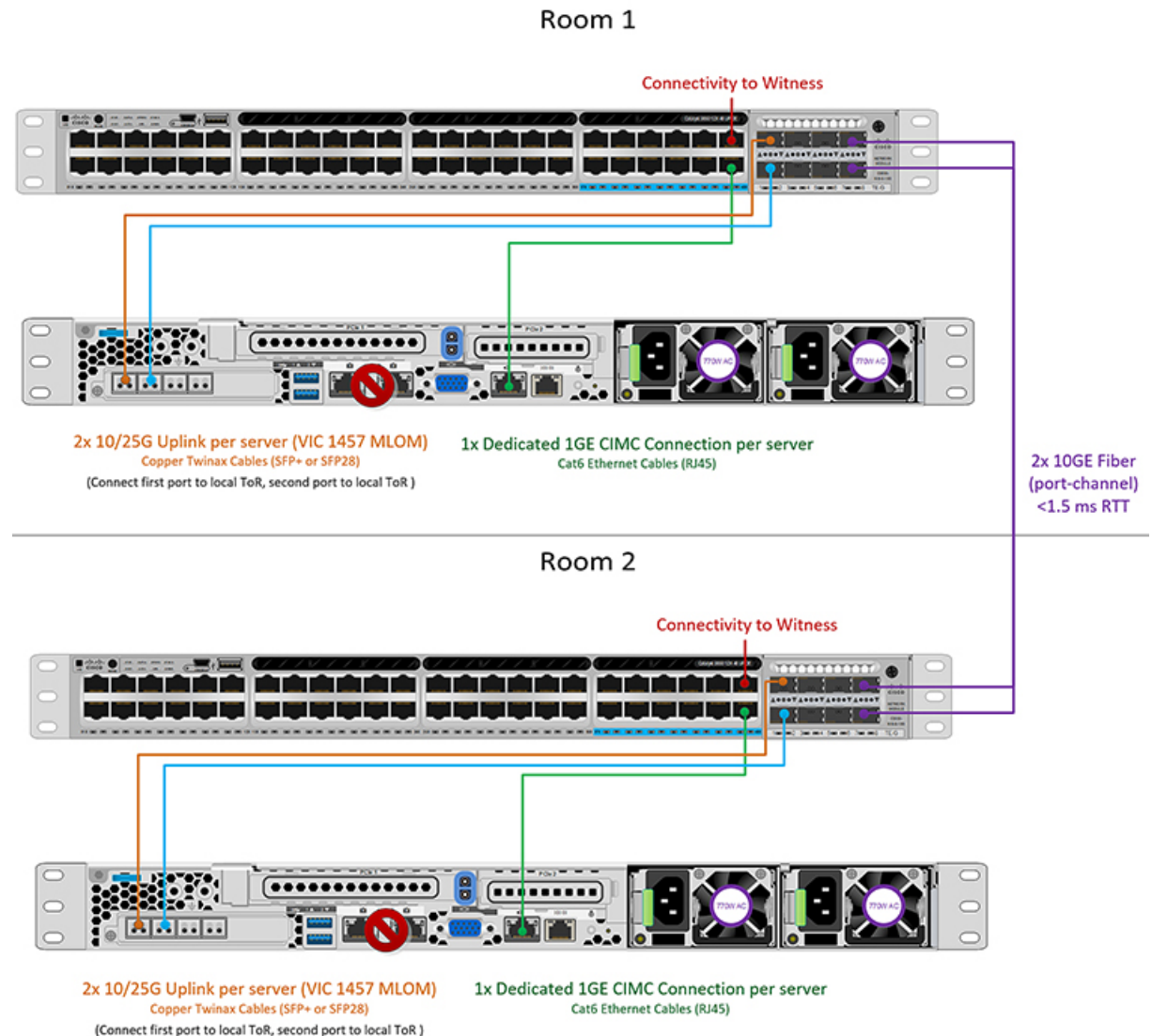


**警告** 適切なケーブル配線は、ネットワークの完全な冗長性を確保するために重要です。

ルームごとに1つのスイッチを試用して展開する場合（レイアウトについては、次の図を参照してください）。

- 専用の Cisco IMC を使用している場合は、各サーバの 1GE 管理ポート（サーバの背面にある「M」というラベルが付いた）をローカルスイッチに接続します。
- 各サーバの Cisco VIC の 4 つの 10/25GE ポートのうち 1 つを、**同じルームの**同一の ToR スイッチに接続します。
- 各サーバの Cisco VIC の 2 番目の 10/25GE ポートを、**同じルームの** ToR スイッチに接続します。
- クラスタのインストール前に追加の 10/25GE ポートを接続しないでください。クラスタ展開後、追加で 2 つの 10/25GE ポートをゲスト VM トラフィックにオプションで使用することができます。
- 各スイッチに、Intersight またはローカル監視サーバへの独立したネットワークパスがあることを確認します。

## 2 ノード 2 ルーム シングル スイッチ



## Quality of Service (QoS)

この章に記載されているすべてのトポロジでは、少なくとも HyperFlex ストレージデータトラフィックに QoS を実装することを強く推奨します。これらの 2 ノード 2 ルーム構成は、2 つの HyperFlex ノード間でストレージトラフィックを伝送するためにサイト間リンク (ISL) に大きく依存していますが、このリンクは他のバックグラウンドトラフィックによって飽和状態になる可能性があります。次のことを推奨します。

- ISL に十分な帯域幅とリンク冗長性を確保します。ポートチャネルで複数の高帯域幅リンクを使用すれば、ルーム間のすべてのタイプのトラフィックに十分なキャパシティを確保できるため、QoS の必要性を軽減できます。速度のミスマッチによってネットワークの



トルネックが発生する可能性があるため、エンドツーエンドのストレージパスでのリンク速度のミスマッチを回避します。

- IP アドレスに基づいてスイッチへの着信トラフィックを分類します。HyperFlex Edge はトラフィックの事前マーキングを行わないので、トラフィックの分類はスイッチの役割です。この分類には、HyperFlex Data Platform ストレージネットワークの IP アドレスを使用します。通常、これらの IP アドレスは 169.254.xx の範囲に /24 ネットワークとして存在します。適切な範囲を見つけるには、vCenter でコントローラ VM の設定を調べるか、コントローラ VM で `ifconfig` コマンドを実行し、`eth1` インターフェイスで使用されているサブネットを確認します。
- /24 サブネット全体をマッチさせることをお勧めします。これにより、より多くのノードでクラスタが拡張されても、すべてのストレージトラフィックが適切に分類され続けるようになります。
- 環境のニーズに応じてストレージトラフィックをマークします。Catalyst 9000 の設定例では、DSCP EF が使用されます。エンドツーエンド QoS は、DSCP ヘッダー値のみを使用して実現されます。
- スイッチプラットフォームの機能に基づくキューを設定します。Catalyst 9000 の例では、プライオリティキューの1つを使用して、サイト間リンク全体で HX ストレージトラフィック (EF とマーク) を優先します。HyperFlex ストレージトラフィックは、低遅延で高帯域幅の高優先度キューで最高のパフォーマンスを発揮します。キューの割り当て済みバッファを増やすと、リンクの伝送遅延がある場合の packet 損失を減らすのにも役立ちます。
- 入力インターフェイス (マーキング用) と出力インターフェイス (キューイング用) に QoS 設定を適用します。
- 管理トラフィック、vMotion、およびアプリケーショントラフィックに必要な追加の QoS 設定を適用します。次の順序でトラフィックに優先順位を付けることをお勧めします。
  1. 管理 : DSCP CS6
  2. VM またはアプリケーショントラフィック : DSCP CS4
  3. vMotion – DSCP CS0

上記の DSCP 値を推奨します。ただし、環境のニーズを満たすために必要に応じて任意の値を使用できます。トラフィックのタイプごとに、IP 範囲に基づいてマーキング用の ACL を作成します。それからの ACL とマッチするクラスマップを作成します。既存のマーキングポリシークラスに追加し、設定アクションを指定します。最後に、DSCP マーキングとマッチし、必要な帯域幅を指定するトラフィックタイプごとの専用クラスで出力キューイングポリシーを更新します。

## ネットワークの共通要件チェックリスト

インストールを開始する前に、お使いの環境が次の特定のソフトウェアおよびハードウェア要件を満たしていることを確認します。

## VLAN の要件



**重要** 予約済み VLAN ID : 指定する VLAN ID は、HyperFlex ノードが接続されている Top of Rack (ToR) スイッチでサポートされている必要があります。たとえば、VLAN ID 3968～4095 は Nexus スイッチによって予約され、VLAN ID 1002～1005 は Catalyst スイッチによって予約されています。HyperFlex で使用する VLAN ID を決定する前に、その同じ VLAN ID がスイッチで使用可能であることを確認してください。

ネットワーク	VLAN ID	説明
次の各ネットワークに個別のサブネットと VLAN を使用します。		
VMware ESXi および Cisco HyperFlex 管理用 VLAN		ESXi、HyperFlex、および VMware vCenter 間の管理トラフィック用に使用され、ルーティング可能な必要があります。  (注) この VLAN は、Intersight にアクセスできる必要があります(2 ノードの展開には、Intersight が必要です)。
CIMC VLAN		管理 VLAN と同じまたは異なる VLAN を指定できます。  (注) この VLAN は、Intersight にアクセスできる必要があります(2 ノードの展開には、Intersight が必要です)。
HyperFlex ストレージトラフィック用 VLAN		raw ストレージトラフィック用に使用されます。L2 接続のみを必要とします。
VLAN for VMware vMotion		vMotion VLAN に使用されます。
VM ネットワーク用の VLAN		VM/アプリケーション ネットワークに使用されます。  (注) ESXi の異なる VM ポートグループでバックアップされた複数の VLAN を指定できます。

### サポートされている vCenter トポロジ

次の表を使用して、vCenter のサポートされているトポロジを決定します。

トポロジ	説明	推奨
シングル vCenter	外部サーバで実行され、サイトに対してローカル扱いとなる仮想または物理 vCenter。このサーバには、管理ラックマウントサーバを使用できません。	強く推奨
一元化された vCenter	WAN 全体の複数のサイトを管理する vCenter。	強く推奨
ネストされた vCenter	展開予定のクラスタ内で実行される vCenter。	HyperFlex Edge クラスタのインストールは、vCenter がなくても先に実行できます。また、外部 vCenter を使用して展開し、クラスタに移行することもできます。いずれの場合も、実稼働ワークロードを実行する前に、クラスタを vCenter サーバに登録する必要があります。  最新情報については、『 <a href="#">HX Data Platform への vCenter 導入方法</a> 』テクニカル ノートを参照してください。

### 顧客導入情報

一般的な 2 ノードの HyperFlex Edge の導入の場合、9 個の IP アドレスが必要です - 管理ネットワーク用の 7 個の IP アドレスと vMotion ネットワーク用の 3 個の IP アドレスです。



**重要** すべての IP アドレスは IPv4 である必要があります。HyperFlex は IPv6 アドレスをサポートしていません。

### CIMC 管理 IP アドレス

サーバ	CIMC 管理 IP アドレス
サーバ 1 :	

サーバ	CIMC 管理 IP アドレス
サーバ 2 :	
サブネット マスク	
ゲートウェイ	
DNS サーバ	
NTP サーバ (注) 適切な Intersight 接続を確保するためには、CIMC に NTP を設定する必要があります。	

### ネットワークの IP アドレス



- (注) デフォルトでは、HX インストーラにより、ハイパーバイザ データ ネットワークとストレージコントローラ データ ネットワークに、169.254.X.X の /24 ネットワークとしての範囲内にある IP アドレスが自動的に割り当てられます。この IP サブネットをユーザーが設定することはできません。



- (注) スパニング ツリー PortFast トランク (トランク ポート) は、すべてのネットワーク ポートで有効にする必要があります。

PortFast の設定に失敗すると、ESXi の起動時に断続的に切断され、物理リンク障害時に必要なネットワークの再コンバージェンスよりも長く時間がかかります。

管理ネットワークの IP アドレス (ルーティング可能であること)	
ハイパーバイザ管理ネットワーク	ストレージコントローラの管理ネットワーク
サーバ 1 :	サーバ 1 :
サーバ 2 :	サーバ 2 :
ストレージ クラスタ管理 IP アドレス	クラスタ IP:
サブネット マスク	
デフォルト ゲートウェイ	

**VMware vMotion ネットワーク IP アドレス**

vMotion サービスの場合、固有の VMKernel ポートを設定します。必要であれば、vMotion の管理 VLAN を使用している場合は vmk0 を再使用することもできます（非推奨）。

サーバ	vMotion ネットワークの IP アドレス（ <code>post_install</code> スクリプトを使用して設定されている）
サーバ 1 :	
サーバ 2 :	
サブネット マスク	
ゲートウェイ	

**VMware vCenter の構成**

- (注) HyperFlex は標準ポートを介して vCenter と通信します。ポート 80 はリバース HTTP プロキシで使用されますが、TAC のサポートを受けて変更できます。ポート 443 は vCenter SDK へのセキュア通信に使用され、変更することはできません。

<b>vCenter 管理ユーザ名</b> <i>username@domain</i>	
<b>vCenter 管理パスワード</b>	
<b>vCenter データセンターの名前</b> (注) 既存のデータセンターオブジェクトを使用できます。データセンターが vCenter に存在しない場合は、作成されます。	
<b>VMware vSphere コンピューティング クラスタおよびストレージ クラスタの名前</b> (注) vCenter に表示される クラスタ名。	

## ポート要件



**重要** [Intersight の接続性 \(219 ページ\)](#) に記載されている前提条件に加えて、次のポート要件も満たしていることを確認します。

ネットワークがファイアウォールの背後にある場合は、標準のポート要件に加え、VMware には VMware ESXi および VMware vCenter に対するポートが推奨されます。

- CIP-M は、クラスタ管理 IP に使用します。
- SCVM は、コントローラ VM の管理 IP です。
- ESXi は、ハイパーバイザの管理 IP です。

HyperFlex ソリューションのコンポーネント通信に必要なポートの包括的なリストは、[HX Data Platform Security Hardening Guide](#) の付録 A に記載されています。



**ヒント** 標準設定がなく、異なるポート設定が必要な場合は、環境のカスタマイズについて、[表 C-5 ポートのリテラル値](#)を参照してください。

## ネットワーク サービス



- (注)
- DNS サーバと NTP サーバは、HX ストレージ クラスタの外側に配置する必要があります。
  - 現時点では、信頼性の高いソースを提供するには、内部でホストされている NTP サーバを使用してください。
  - すべての DNS サーバは、展開を開始する前に、ESXi の各ホストについて順方向 (A) および逆方向 (PTR) の DNS レコードを事前設定しておく必要があります。DNS を前もって正しく設定しておけば、ESXi ホストを、IP アドレスではなく FQDN で vCenter に追加できます。

この手順をスキップした場合には、ホストは IP アドレスで vCenter インベントリに追加され、ユーザは「[vCenter クラスタのノードの識別方法を IP から FQDN に変更する](#)」で説明されている手続きに従って、FQDN に変換することが必要になります。

<b>DNS サーバ</b> <Primary DNS Server IP address, Secondary DNS Server IP address, ...>	
---	--

<b>NTP サーバ</b> <Primary NTP Server IP address, Secondary NTP Server IP address, ...>	
<b>タイムゾーン</b> 例 : US/Eastern、US/Pacific	

#### コネクテッド サービス

コネクテッドサービスの有効化 (推奨) [はい (Yes) ] または [いいえ (No) ] が必要	
<b>サービス要求通知用の電子メール</b> 例 : name@company.com	

#### Proxy Server

- Intersight への直接接続が使用できない場合、プロキシサーバの使用は任意です。
- プロキシを使用する場合は、サーバを Intersight アカウントに要求するためにプロキシを使用するように、各サーバのデバイス コネクタを設定する必要があります。さらに、HyperFlex Data Platform を正常にダウンロードできるようにするには、HX クラスタ プロファイルでプロキシ情報を指定する必要があります。
- ユーザー名/パスワードの使用はオプションです。

<b>プロキシが必要です:イエスマ          たはノー</b>	
<b>Proxy Host</b>	
<b>プロキシポート (Proxy Port)</b>	
<b>Username</b>	
<b>パスワード</b>	

## ゲスト VM トラフィック

ゲスト VM トラフィックに関する考慮事項は、トポロジの選択に基づいて上記に示されます。通常、正しい vSwitch に適用される限り、必要に応じてゲスト ポート グループを作成できます。

- 10/25GE トポロジ: **vswitch-hx-vm-network** を使用して、新しい VM ポート グループを作成します。

Post\_install スクリプトを実行して、クラスタ内のすべてのホスト上で正しい vSwitches に自動的に VLAN を追加することを推奨します。後ほど、任意の時点で新しいゲスト VLAN をクラスタに追加するには、**hx\_post\_install --vla** (スペースの後には2つのダッシュ) を実行します。

残りの vmnic またはサードパーティ製のネットワーク アダプタを使用する追加の vSwitches が作成される場合があります。HyperFlex によって定義された vSwitches に変更が加えられないように注意する必要があります。



- 
- (注) ユーザーが作成した追加の vSwitches は、管理者単独で責任を有し、HyperFlex によって管理されません。
- 

## Intersight の接続性

Intersight の接続性に関する次の前提条件を考慮してください。

- HX サーバのセットに HX クラスタをインストールする前に、対応する Cisco IMC インスタンスのデバイス コネクタが Cisco Intersight に接続するように適切に設定され、登録されていることを確認します。
- インストール フェーズ中のポート 80、443、および 8089 を介した CIMC と vCenter 間の通信。
- すべてのデバイス コネクタは、*svc.intersight.com* を適切に解決でき、かつポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。現在の HX インストーラバージョンでは、HTTP プロキシの使用がサポートされています。
- すべてのコントローラの VM 管理インターフェイスは、*svc.intersight.com* を適切に解決でき、ポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。現在の HX インストーラバージョンは、インターネットへの直接接続がない場合、HTTP プロキシの使用をサポートしています。
- IP 接続 (L2 または L3) は、各サーバの CIMC 管理 IP から次のすべてに必要です。ESXi 管理インターフェイス、HyperFlex コントローラ VM 管理インターフェイス、vCenter サーバ。このパスのファイアウォールは、『[Hyperflex Hardening ガイド](#)』で説明されている必要なポートを許可するように設定する必要があります。
- HXDP リリース 3.5(2a) 以降、Intersight インストーラでは、HyperFlex サーバ上に工場出荷時にインストールされるコントローラ VM が不要になりました。



同じサーバに HyperFlex を再展開する場合、新しいコントローラ VM を Intersight からすべての ESXi ホストにダウンロードする必要があります。これには、各 ESXi ホストが `svc.intersight.com` を解決し、ポート 443 上の発信側で開始した HTTPS 接続を許可することが必要です。コントローラ VM のダウンロードにプロキシサーバを使用することはサポートされており、必要に応じて HyperFlex クラスタ プロファイルで設定できます。

- クラスタの展開後、継続的な管理のために Intersight 内で新しい HX クラスタが自動的に登録されます。

## Cisco HyperFlex Edge 非表示クラウド監視

Cisco Hyperflex Edge 非表示クラウド監視は、監視 VM または調停ソフトウェアの必要性を排除する、Cisco Hyperflex Edge の導入における革新的なテクノロジーです。

Cisco Hyperflex Edge 非表示クラウド監視は、2 ノード HX Edge 展開にのみ必要です。監視には、追加のインフラストラクチャ、セットアップ、設定、バックアップ、パッチ、または管理は必要ありません。この機能は、2 ノード HyperFlex Edge のインストールの一部として自動的に設定されます。リモートサイトでのアウトバウンドアクセスは、相互に接続するために存在している必要があります (Intersight.com または Intersight 仮想アライアンス)。HyperFlex Edge 2 ノード クラスタは、この接続が確立されていないと動作しません。

非表示クラウド監視機能の利点、運用、および障害のシナリオの詳細については、次を参照してください。 <https://www.cisco.com/c/dam/en/us/products/collateral/hyperconverged-infrastructure/hyperflex-hx-series/whitepaper-c11-741999.pdf>

## Cisco Hyperflex Edge サーバの注文

Cisco HyperFlex Edge サーバを注文する場合は、[HyperFlex Edge 仕様シート](#)の説明に従って、正しいコンポーネントを選択してください。ネットワーク トポロジの選択に注意して、目的の設定と一致することを確認します。ネットワーク トポロジの PID 選択の詳細については、仕様シートの補足資料セクションを参照してください。

## インストールの概要



- (注) 以前に HyperFlex クラスタノードが他の HyperFlex クラスタの一部であった場合 (または工場出荷前の場合)、クラスタの導入を開始する前にノードのクリーンアップ手順を実行します。詳細については、『[HyperFlex Customer Cleanup Guides for FI and Edge](#)』を参照してください。

Edge 導入のためのインストール ワークフローの概要を示す次の表を参照してください。手順 1 ~ 3 は、1 GE と 10/25GE の展開で共通です。ただし、手順 4 は 1GE の展開に適用され、残り手順 5 ~ 6 は 10/25 GE の展開に適用されます。

手順	説明	参考資料	1GE および 10/25GE、1GE、または 10/25GE に適用可能
1	インストール前のチェックリストに記入します。	<p>スイッチの設定に基づいて、以下から選択します。</p> <p>2 ノードエッジの展開:</p> <ul style="list-style-type: none"> <li>• 10 または 25GE VIC ベースのトポロジ (204 ページ) または、</li> <li>• 10 または 25GE NIC ベース トポロジ</li> <li>• 1 ギガビット イーサネット トポロジ (220 ページ)</li> </ul> <p>3 および 4 ノードエッジの展開:</p> <ul style="list-style-type: none"> <li>• 10 または 25GE VIC ベースのトポロジ (227 ページ) または、</li> <li>• 10 または 25GE NIC ベース トポロジ</li> <li>• 1 ギガビット イーサネット トポロジ (232 ページ)</li> </ul>	1GE および 10/25GE
2	インストールの前提条件を準備します。	<ul style="list-style-type: none"> <li>• ラック設置型 Cisco HyperFlex ノード (263 ページ)</li> <li>• Cisco Integrated Management Controller の構成 (263 ページ)</li> <li>• ファームウェアバージョンの確認 (265 ページ)</li> </ul>	1GE および 10/25GE
3	Cisco HX Data Platform インストーラをダウンロードして導入します。	Cisco HX Data Platform インストーラの導入 (266 ページ)	1GE および 10/25GE

手順	説明	参考資料	1GE および 10/25GE、1GE、または 10/25GE に適用可能
4	HyperFlex Edge クラスタを展開します。	次の手順を実行して Edge クラスタを設定し、インストールが成功したことを確認します。  <ul style="list-style-type: none"> <li>• <a href="#">HyperFlex クラスタの設定 (267 ページ)</a></li> <li>• <a href="#">Cisco HX Data Platform ソフトウェアインストールの確認 (274 ページ)</a></li> </ul>	1GE のみ
[6]	HyperFlex Edge クラスタを展開します。	<a href="#">(10/25GE のみ) HyperFlex クラスタの設定 (274 ページ)</a>	10/25GE のみ

## ラック設置型 Cisco HyperFlex ノード

Cisco HX220c M5 HyperFlex ノードまたは Cisco HX220c M6 HyperFlex ノードの詳細については、『[Cisco Hardware Install Guides](#)』を参照してください。



**重要** CIMC 構成のために、コンソール ドングルを使用して VGA モニタとキーボードを接続できます。また、サーバの背面で VGA および USB ポートを直接接続することもできます。あるいは、ネットワーク内で DHCP サーバを使用できる場合は、CIMC の Lights-Out 構成を行うこともできます。

## Cisco Integrated Management Controller の構成

CIMC ネットワークを構成する方法として、静的（スタティック）割り当てまたは DHCP 割り当てのいずれかを選択します。

### CIMC の構成：静的割り当て

Cisco Integrated Management Controller (CIMC) を構成するには、CIMC スタンドアロンモードを有効にし、CIMC パスワードと設定を構成し、KVM を使用して手動で静的 IP アドレスを構成する必要があります。それには、モニタとキーボードを備えた各サーバに物理的にアクセスできる必要があります。一度に 1 台ずつサーバを構成する必要があります。

アウトオブバンド用途では専用 CIMC 管理ポートを使用することもできます。ユーザーはアップストリーム スイッチの設定を計画する際は、この 3 番目の 1GE ポートを考慮する必要があります。さらに、CIMC の構成中は、CIMC を専用モードに設定する必要があります。専用 NIC

モードにおける CIMC の構成の詳細については、[Cisco UCS C シリーズのドキュメンテーション](#)を参照してください。[NIC プロパティ (NIC properties)] の下で、NIC モードを [専用 (dedicated)] に設定してから構成を保存します。

### 始める前に

- 展開に適用されるこのガイドの「物理的なケーブル接続」の項の説明に従って、すべてのイーサネット ケーブルが接続されていることを確認します。
- サーバに VGA ドングルを接続し、モニタと USB キーボードを接続します。

**ステップ 1** サーバの電源を入れ、画面に Cisco ロゴが表示されるまで待ちます。

**ステップ 2** プロンプトが表示されたら、**F8** キーを押して、**Cisco IMC Configuration** ユーティリティを起動します。

**ステップ 3** [CIMC ユーザの詳細 (CIMC User Details)] で、**password** と、[現在の CIMC パスワード (current CIMC password)] に入力し、**新しい CIMC パスワード** を 2 回入力してから **Enter** キーを押して新しいパスワードを保存します。

**重要** システムには、インストール時に変更する必要があるデフォルトパスワード *Cisco123* が付属しています。新しいユーザ指定のパスワードを指定しない限り、インストールを続行することはできません。

**ステップ 4** [IP (基本) (IP (Basic))] で、[IPv4] をオンにし、[DHCP を使う (DHCP Enabled)] をオフにして、[CIMC IP]、[プレフィックス/サブネット (Prefix/Subnet)] マスク、[ゲートウェイ (Gateway)] に値を入力します

**ステップ 5** [VLAN (詳細設定) (VLAN (Advanced))] で、[VLAN を使う (VLAN enabled)] をオンにして、次の操作を行います。

- トランク ポートを使用する場合は、適切な [VLAN ID] を設定します。
- アクセス ポートを使用する場合は、このフィールドを空白のままにします。

**ステップ 6** 他の設定はデフォルトのままにして、**F10** キーを押して構成を保存し、**ESC** キーを押してユーティリティを終了します。

**ステップ 7** Web ブラウザで、CIMC ページ (<https://CIMC IP アドレス>) に直接移動します。

**ステップ 8** ユーザ名 **admin** と新しい CIMC パスワードを入力し、[ログイン (Log In)] をクリックします。

**ステップ 9** [サーバ (Server)] > [電源ポリシー (Power Policies)] に移動して、目的の動作と一致する電源ポリシーを手動で設定します。

サーバはデフォルトで、電力復元ポリシーを工場出荷時の設定 [電源オフ (Power Off)] に設定します。

### 次のタスク

仮想 KVM コンソールを使用することも、物理 KVM を引き続き使用することもできます。SD カードには工場出荷時に ESXi がプリインストールされているので、インストール時に自動的に起動します。

## CIMC の構成 : DHCP 割り当て

Cisco Integrated Management Controller (CIMC) を構成するには、CIMC スタンドアロンモードを有効にし、CIMC パスワードと設定を構成し、DHCP から取得した動的 IP アドレスを構成する必要があります。この場合、ネットワークの設定作業が増えますが、HyperFlex Edge ノードの Lights-Out セットアップを有効にすることで構成が容易になります。すべてのサーバが同時に自動的にアドレスをリースするため、導入時間が短縮されます。

### 始める前に

- 展開に適用されるこのガイドの「物理的なケーブル接続」の項の説明に従って、すべてのイーサネットケーブルが接続されていることを確認します。
- DHCP サーバが有効なスコープで構成されて稼働していることを確認します。
- DHCP サーバが管理 VLAN で直接リッスンしているか、スイッチ上に IP ヘルパーが構成されていることを確認します。
- インバンド CIMC とアウトオブバンド CIMC のどちらを使用するかを決定します。
  - インバンド CIMC を使用する場合、すべての HyperFlex Edge スイッチポートに対応するネイティブ VLAN が正しい DHCP VLAN とマッチするように構成します。CIMC が自動的にアドレスをリースできるようにするには、これが唯一の方法です。
  - アウトオブバンド CIMC を使用する場合、DHCP VLAN 上にアクセスモード専用のスイッチポートを構成します。

---

**ステップ 1** 電源ケーブルを接続します。

**ステップ 2** DHCP ログまたはリーステーブルにアクセスして、取得した CIMC アドレスを確認します。

**ステップ 3** C220-**<S/N>** のホスト名を検索して HyperFlex サーバを見つけ、HX Data Platform Installer に入力する必要があるアドレスをメモします。

---

### 次のタスク

DHCP を使用する場合、HX Data Platform のインストールを開始する前に手動でユーザ定義 CIMC パスワードを設定する必要があります。Web UI または CLI セッションのいずれかを使用して、新しいパスワードを設定します。デフォルトのパスワード **password** を変更する必要があります。そうしない場合、インストールが失敗します。

## ファームウェアバージョンの確認

現在の BIOS、CIMC、SAS HBA、およびドライブのファームウェアバージョンを表示して、それらのバージョンが、リリース ノートのデータと一致していることを確認します。

- 
- ステップ 1** お使いのブラウザで <https://<CIMC IP>> にアクセスして、CIMC Web UI にログインします。
- ステップ 2** ナビゲーション ウィンドウで [サーバ (Server)] をクリックします。
- ステップ 3** [サーバ (Server)] ページで [概要 (Summary)] をクリックします。
- ステップ 4** [Cisco Integrated Management Controller (CIMC) 情報 (Cisco Integrated Management Controller (CIMC) Information)] セクション ([サーバの概要 (Server Summary)] ページ) で、[BIOS バージョン (BIOS Version)] と [CIMC ファームウェア バージョン (CIMC Firmware Version)] を検索してメモします。
- ステップ 5** CIMC で、[インベントリ (Inventory)] > [PCIe アダプタ (PCIe Adapters)] の順に移動し、[SAS HBA のバージョン (SAS HBA Version)] を見つけて値をメモします。
- ステップ 6** CIMC では、使用しているサーバーのタイプに応じて [ストレージ (Storage)] に移動し、以下のうちのいずれかに移動してください。
- M4 の場合、[Cisco 12G モジュラー SAS (Cisco 12G Modular SAS)] > [物理ドライブ情報 (Physical Drive Info)] に移動し、ドライブ タイプ、製造業者、およびファームウェア バージョンをメモしてください。
  - M5 および M6 の場合、[Cisco 12G モジュラー SAS HBA (Cisco 12G Modular SAS HBA)] > [物理ドライブ情報 (Physical Drive Info)] に移動し、ドライブ タイプ、製造業者、およびファームウェア バージョンをメモしてください。
- ステップ 7** 現在の BIOS、CIMC、SAS HBA、およびドライブのファームウェア バージョンと、Cisco HyperFlex Edge とファームウェアの互換性マトリックスに記載されているバージョンを比較します。
- ステップ 8** 最小バージョンを満たしていない場合、互換性マトリックスの Host Update Utility (HUU) ダウンロードリンクを基に、システムで実行中のファームウェアのバージョン (Cisco 仮想インターフェイスカード (VIC)、PCI アダプタ、RAID コントローラ、ドライブ (HDD/SSD) ファームウェアを含む) をアップグレードします。Cisco HUU ユーザ ガイドの最新および以前のリリースは、<http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html> で確認できます。
- 

## Cisco HX Data Platform インストーラの導入

HX データプラットフォーム インストーラは、ESXi サーバと、VMware ワークステーション、VMware Fusion、または仮想ボックスに展開できます。HyperFlex ソフトウェアは、オープン仮想アプライアンス (OVA) ファイル形式の導入可能な仮想マシンとして配布されます。VMware vSphere (シック) クライアントを使用して HX Data Platform インストーラを展開するには、次の手順を使用します。

- 
- ステップ 1** HX Data Platform インストーラ OVA を [Cisco.com](http://www.cisco.com) からダウンロードし、このパッケージをローカルに保存します。
- ダウンロードしたバージョンが、展開に推奨されるバージョンと一致することを確認します。
- ステップ 2** vSphere クライアントを使用して vCenter にログインします。
- ステップ 3** [ファイル (File)] > [OVF テンプレートの導入 (Deploy OVF Template)] の順に選択します。

- ステップ 4 [OVF テンプレートの導入 (Deploy OVF Template)] ウィザードの [送信元 (Source)] ページで、送信元の場所を指定し、[次へ (Next)] をクリックします。
- ステップ 5 [OVF テンプレートの詳細 (OVF Template Details)] ページで、情報を確認してから [次へ (Next)] をクリックします。
- ステップ 6 (任意) [名前と場所 (Name and Location)] ページで、仮想アプライアンスの名前と場所を編集し、[次へ (Next)] をクリックします。
- ステップ 7 [ホスト/クラスタ (Host/Cluster)] ページで、導入先のホストまたはクラスタを選択し、[次へ (Next)] をクリックします。
- ステップ 8 [リソース プール (Resource Pool)] ページで、OVF テンプレートの実行場所となるリソース プールを選択し、[次へ (Next)] をクリックします。
- ステップ 9 [ストレージ (Storage)] ページで、導入後の OVF テンプレートを保管するデータベースを選択し、[次へ (Next)] をクリックします。
- ステップ 10 [ディスク フォーマット (Disk Format)] ページで、仮想マシンの仮想ディスクを保管するディスク フォーマットを選択し、[次へ (Next)] をクリックします。
- ステップ 11 [ネットワーク マッピング (Network Mapping)] ページで、OVF テンプレートで指定されているそれぞれのネットワークについて、[宛先ネットワーク (Destination Network)] 列を右クリックしてインフラストラクチャ内のネットワークを選択し、[次へ (Next)] をクリックします。
- ステップ 12 インストーラ VM の OVF プロパティとして、ホスト名、デフォルト ゲートウェイ、DNS サーバ、IP アドレス、およびサブネット マスクを指定します。
- あるいは、DHCP で割り当てられるアドレスを使用するには、すべての OVF プロパティを空白のままにします。
- ステップ 13 [準備完了 (Ready to Complete)] ページで、[展開後に電源をオン (Power On After Deployment)] を選択し、[終了 (Finish)] をクリックします。

## HyperFlex クラスタの設定

- ステップ 1 Web ブラウザで、インストーラ VM の IP アドレスを入力し、[承認 (Accept)] または [続行 (Continue)] をクリックして SSL 証明書エラーをバイパスします。
- ステップ 2 ログイン画面の右下隅にある [ビルド ID (Build ID)] で HyperFlex インストーラのビルド ID を確認します。
- ステップ 3 ユーザー名 **root** とパスワード **Cisco123** を使用して Cisco HX Data Platform にログインします。
- 重要** システムに同梱されているデフォルトのパスワード *Cisco123* は、インストール時に変更する必要があります。HyperFlex オンプレミス インストーラでは、導入の一部としてルート パスワードを変更する必要があります。新しいパスワードを指定しない限り、インストールを続行できません。設定の手順のこの時点で、新しいパスワードを使用します。
- ステップ 4 エンドユーザ ライセンス契約書を読み、[利用規約に同意する (I accept terms and conditions)] をオンにしてから、[ログイン (Login)] をクリックします。

**ステップ 5** [Workflow (ワークフロー)] ページで、[HyperFlex によるクラスタ作成 (Cluster Creation with HyperFlex Edge)] をクリックします

**ステップ 6** クラスタを作成するには、必要な構成データが格納された *JSON* コンフィギュレーション ファイルをインポートできます。JSON ファイルをインポートする場合は、次の2つのステップを行います。インポートしない場合は、必須フィールドに手動でデータを入力できます。

(注) 初回インストールの場合は、シスコの担当者に連絡して工場出荷時のプレインストール JSON ファイルを入手してください。

1. [ファイルの選択 (Select a file)] をクリックし、該当する *JSON* ファイルを選択して構成をロードします。[構成を使用 (Use Configuration)] を選択します。
2. インポートした Cisco UCS Manager の値が異なる場合は、[Overwrite Imported Values] ダイアログボックスが表示されます。[Use Discovered Values] を選択します。

**ステップ 7** [クレデンシャル (Credentials)] ページで、次のフィールドに値を入力してから、[続行 (Continue)] をクリックします。

名前 (Name)	説明
<b>Cisco IMC クレデンシャル</b>	
Cisco IMC ユーザー名	Cisco IMC ユーザー名。ユーザー名のデフォルトは <b>admin</b> です。
パスワード	CIMC のパスワード。デフォルトのパスワードは <b>password</b> です。
<b>vCenter クレデンシャル (vCenter Credentials)</b>	
HyperFlex クラスタ サーバの設定	vCenter サーバの FQDN または IP アドレス。vCenter のルート レベル管理者権限があるアカウントを使用する必要があります。
ユーザ名	管理者ユーザ名。
[管理パスワード (Admin Password)]	管理者パスワード。
<b>ハイパーバイザのクレデンシャル</b>	
管理者ユーザ名	管理者ユーザ名。デフォルトのユーザ名は <b>root</b> です。
ハイパーバイザ パスワード	デフォルトのパスワードは <b>Cisco123</b> です。  <b>重要</b> システムに同梱されているデフォルトのパスワード <i>Cisco123</i> は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

次のスクリーンショットを参照して、このページのフィールドに入力してください。



**ステップ 8** [IP Addresses] ページで、サーバごとに割り当てられたアドレスを入力します。

名前 (Name)	説明
Cisco IMC	Cisco IMC の IP アドレス
ハイパーバイザ	ハイパーバイザの管理 IP
ストレージ コントローラ	ストレージ コントローラの管理 IP
クラスタの IP アドレス	クラスタ管理 IP アドレス
サブネット マスク	クラスタ管理のサブネットマスク
ゲートウェイ	クラスタ管理 IP のゲートウェイ IP アドレス

次のスクリーンショットを参照して、このページのフィールドに入力してください。

**ステップ 9** [クラスタ構成 (Cluster Configuration)] ページで、次のフィールドに値を入力してから、[続行 (Continue)] をクリックします。

(注) プリインストールワークシートを使用して、すべてのフィールドに値を入力します。

名前 (Name)	説明
<b>Cisco HX クラスタ</b>	
クラスタ名	HyperFlex ストレージクラスタの名前 (ユーザが指定した名前)。
レプリケーションファクタ	3 ノードおよび 4 ノード エッジクラスタのレプリケーションファクタ 3 のサポートは、HXDP リリース 4.5 で導入されました。 2 ノードエッジクラスタのデフォルトのレプリケーションファクタは <b>2</b> です。
<b>コントローラ VM</b>	
管理者パスワードの作成	コントローラ VM のデフォルトパスワードはありません。ユーザーはこのフィールドを設定する必要があります
管理者パスワードの確認	管理者パスワードを再入力して確認します。
<b>vCenter の設定</b>	

名前 (Name)	説明
vCenter データセンター名	HyperFlex ホストが追加された vCenter データセンターの名前。
vCenter Cluster Name	HyperFlex ホストが追加された vCenter クラスタの名前。
<b>システムサービス</b>	
[DNS サーバ (DNS Server(s)) ]	各 DNS サーバの IP アドレスのカンマ区切りリスト。
NTP サーバ	各 NTP サーバの IP アドレスのカンマ区切りリスト。 <b>重要</b> 信頼性の高い NTP サーバが必要です。
[タイムゾーン (Time Zone) ]	コントローラ VM のローカル タイムゾーン。
<b>コネクテッド サービス</b>	
[Enable Connected Services] (推奨)	オンにして、接続サービスを有効にします。  (注) 接続サービスを有効にして Cisco TAC にメールアラートを送信できるようにすることを強く推奨します。
サービス チケット通知の送信先 : 例 : <i>admin@cisco.com</i>	サービス要求通知を受信する電子メールアドレス。
<b>詳細ネットワーク</b>	
管理 VLAN タグ データ VLAN タグ	トランク ポートを使用する場合は、適切な VLAN タグを入力します。トランクモードを使用する場合は、VLAN タグが異なる必要があります。  アクセス ポートを使用している場合は、両方の VLAN タグに <b>0</b> を入力します。  (注) トランク ポートを使用している場合は、 <b>0</b> を入力しないでください。
管理 vSwitch データ vSwitch	自動入力された vSwitch 名を変更しないでください。
<b>Advanced Configuration</b>	

名前 (Name)	説明
データネットワーク上のジャンボフレームを有効化	このチェックボックスをオフにして、HyperFlex Edge 展開で標準サイズの packets が使用されるようにする必要があります。ネットワーク構成によっては、必要に応じて 10/25GE 展開のジャンボフレームを有効にすることができます。導入を容易にするため、このオプションをオフにすることをお勧めします。
ディスクパーティションのクリーンアップ	既存のすべてのデータとパーティションを HX ストレージクラスタから削除する場合は、このチェックボックスをオンにします。たとえば、クラスタにこのソフトウェアをインストールするのは初めてではない場合、このチェックボックスをオンにします。
[VDI のみの展開用に最適化 (Optimize for VDi only deployment) ]	VDI 展開を最適化する場合は、このチェックボックスをオンにします。デフォルトでは、HyperFlex は仮想サーバインフラストラクチャ (VSI) 用にパフォーマンスが最適化されています。VDI 展開の場合にパフォーマンスパラメータを調整するには、このボックスをオンにします。このオプションは、オールフラッシュ HX モデルには影響しません。ハイブリッド HX クラスタでのみ有効にする必要があります。VDI と VSI が混在するワークロードを実行している場合は、このオプションを選択しないでください。
vCenter Single-Sign-On Server	このフィールドには、Cisco TAC から指示があった場合にのみ値を入力してください。

次のスクリーンショットを参照して、このページのフィールドに入力してください。

Cisco HyperFlex Installer
① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨ ⑩

Credentials
IP Addresses
Cluster Configuration

### Cisco HX Cluster

Cluster Name:       Replication Factor:

---

### Controller VM

Create Admin Password:       Confirm Admin Password:

---

### vCenter Configuration

vCenter Datacenter Name:       vCenter Cluster Name:

---

### System Services

DNS Server(s):       NTP Server(s):       DNS Domain Name:

Time Zone:

---

### Connected Services

Connected Services:  Enable Connected Services (Recommended)      Send service ticket notifications to:

---

### Advanced Networking

Management VLAN Tag:       Management vSwitch:

Data VLAN Tag:       Data vSwitch:

---

### Advanced Configuration

Jumbo Frames:  Enable Jumbo Frames on Data Network      Disk Partitions:  Clean up disk partitions      Virtual Desktop (VDI):  Optimize for VDI only deployment

vCenter Single-Sign-On Server:

### Configuration

#### Credentials

vCenter Server: 10.64.53.54  
User Name: administrator@vsphere.local  
Cisco IMC User Name: eng-f155.eng.com  
Admin User name: root

#### IP Addresses

Cluster Name: EDGE\_CLUSTER  
Management Cluster: 10.10.10.40  
Management Subnet Mask: 255.0.0.0  
Management Gateway: 10.10.10.1

#### Server 1

Management Cisco IMC: 10.10.10.10  
Management Hypervisor: 10.10.10.20  
Management Storage Controller: 10.10.10.30

#### Server 2

Management Cisco IMC: 10.10.10.11

ステップ 10 導入が完了すると、[導入の概要 (Summary Deployment)] ページに導入の詳細が要約されて表示されず。

### 次のタスク

HX Data Platform プラグインのインストールを確認します。「[Cisco HX Data Platform ソフトウェア インストールの確認 \(274 ページ\)](#)」を参照してください。

## Cisco HX Data Platform ソフトウェア インストールの確認

ステップ 1 vSphere を起動し、管理者として vCenter Server にログインします。

ステップ 2 vCenter Inventory Lists で、Cisco HX Data Platform が表示されることを確認します。

Cisco HX Data Platform のエントリが表示されていない場合は、vCenter からログアウトしてブラウザを閉じ、再度ログインします。ほとんどの場合はこの操作で問題が解決します。

vCenter からログアウトしても問題が解決されない場合は、vCenter Web クライアントを再起動する必要があります。VCSA に SSH で接続し、`service vsphere-client restart` を実行します。Windows 対応の vCenter の場合、MMC のサービス ページで VMware vSphere Web クライアントを再起動します。

ステップ 3 新しいクラスタがオンライン状態になっていて、登録済みであることを確認してください。

## (10/25GE のみ) HyperFlex クラスタの設定

ステップ 1 Web ブラウザで、インストーラ VM の IP アドレスを入力し、[承認 (Accept)] または [続行 (Continue)] をクリックして SSL 証明書エラーをバイパスします。

ステップ 2 ログイン画面の右下隅にある [ビルド ID (Build ID)] で HyperFlex インストーラのビルド ID を確認します。

ステップ 3 ユーザー名 **root** とパスワード **Cisco123** を使用して Cisco HX Data Platform にログインします。

**重要** システムは、デフォルトのパスワード [Cisco123] で出荷されますので、インストール中にこれを変更する必要があります。HyperFlex オンプレミスインストーラでは、導入の一部としてルートパスワードを変更する必要があります。新しいパスワードを指定しない限り、インストールを続行できません。設定の手順のこの時点で、新しいパスワードを使用します。

ステップ 4 エンドユーザーライセンス契約書を読み、[利用規約に同意する (I accept terms and conditions)] をオンにしてから、[ログイン (Login)] をクリックします。

ステップ 5 [Workflow (ワークフロー)] ページで、[HyperFlex によるクラスタ作成 (Cluster Creation with HyperFlex Edge)] をクリックします

ステップ 6 [クレデンシャル (Credentials)] ページで、次のフィールドに値を入力してから、[続行 (Continue)] をクリックします。

名前 (Name)	説明
<b>vCenter クレデンシャル</b>	
vCenter Server	vCenter サーバの FQDN または IP アドレス。vCenter のルート レベル管理者権限があるアカウントを使用する必要があります。
ユーザ名	管理者ユーザ名。
[管理パスワード (Admin Password) ]	管理者パスワード。
<b>[CIMC クレデンシャル (CIMC Credentials) ]</b>	
[CIMC ユーザ名 (CIMC User Name) ]	CIMC のユーザ名。ユーザー名のデフォルトは <b>admin</b> です。
パスワード	CIMC のパスワード。デフォルトのパスワードは <b>password</b> です。
<b>ハイパーバイザのクレデンシャル</b>	
管理者ユーザ名	管理者ユーザ名。デフォルトのユーザ名は <b>root</b> です。
[管理パスワード (Admin Password) ]	デフォルトのパスワードは <b>Cisco123</b> です。 <b>重要</b> システムに同梱されているデフォルトのパスワード <b>Cisco123</b> は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。

**ステップ 7** **[IP アドレス (IP Addresses)]** ページで、サーバごとに割り当てられたアドレスを入力します。

名前 (Name)	説明
Cisco IMC	Cisco IMC の IP アドレス
ハイパーバイザ	ハイパーバイザの管理 IP
ストレージコントローラ	ストレージコントローラの管理 IP
クラスタの IP アドレス	クラスタ管理 IP アドレス
サブネット マスク	クラスタ管理のサブネットマスク
ゲートウェイ	クラスタ管理 IP のゲートウェイ IP アドレス

**ステップ 8** [クラスタ構成 (Cluster Configuration) ] ページで、次のフィールドに値を入力してから、[続行 (Continue) ] をクリックします。

(注) プリインストール ワークシートを使用して、すべてのフィールドに値を入力します。

名前 (Name)	説明
<b>Cisco HX クラスタ</b>	
クラスタ名	HyperFlex ストレージクラスタの名前 (ユーザが指定した名前)。
レプリケーション ファクタ	
<b>コントローラ VM</b>	
管理者パスワードの作成	デフォルトのパスワードは Cisco123 です。 <b>重要</b> システムに同梱されているデフォルトのパスワード Cisco123 は、インストール時に変更する必要があります。新しいユーザがパスワードを指定していない限り、インストールを続行できません。
管理者パスワードの確認	管理者パスワードを再入力して確認します。
<b>vCenter の設定</b>	
vCenter データセンター名	HyperFlex ホストが追加された vCenter データセンターの名前。
vCenter Cluster Name	HyperFlex ホストが追加された vCenter クラスタの名前。
<b>システムサービス</b>	
[DNS サーバ (DNS Server(s)) ]	各 DNS サーバの IP アドレスのカンマ区切りリスト。
NTP サーバ	各 NTP サーバの IP アドレスのカンマ区切りリスト。 <b>重要</b> 信頼性の高い NTP サーバが必要です。
[タイムゾーン (Time Zone) ]	コントローラ VM のローカル タイムゾーン。
<b>自動サポート</b>	



名前 (Name)	説明
自動サポートを有効にします (推奨)。	自動サポートを有効にするには、このチェックボックスをオンにします。  (注) 自動サポートを有効にして、メールアドレスを Cisco TAC に送信できるようにすることを強くお勧めします。
サービスチケット通知をに送信します (例: name@company.com)。	サービス リクエスト通知を受信するメールアドレス。

**ステップ 9** [クラスタ構成の詳細設定 (Advanced Cluster Configuration) ] ページで、次のフィールドに値を入力してから、[開始 (Start) ] をクリックします。

名前 (Name)	説明
<b>詳細ネットワーク</b>	
アップリンク スイッチの速度	<b>10/25GE</b> のラジオ ボタンをオンにします。[ <b>MAC アドレス プレフィックス (MAC Address Prefix)</b> ] フィールドが表示されます。MAC アドレス プレフィックスを設定します。  (注) MAC アドレス プレフィックスは、Cisco VIC の仮想インターフェイスに一意の MAC アドレスを割り当てるために使用されます。既存のネットワーク機器と重複しないように、一意の範囲を選択してください。
管理 VLAN タグ データ VLAN タグ	トランク ポートを使用する場合は、適切な VLAN タグを入力します。トランクモードを使用する場合は、VLAN タグが異なる必要があります。  アクセス ポートを使用している場合は、両方の VLAN タグに <b>0</b> を入力します。  (注) トランク ポートを使用している場合は、 <b>0</b> を入力しないでください。
管理 vSwitch データ vSwitch	自動入力された vSwitch 名を変更しないでください。
<b>詳細設定</b>	
データネットワーク上のジャンボフレームを有効化	10/25G 展開のジャンボフレームを有効にするには、チェックを付けます。

名前 (Name)	説明
ディスクパーティションのクリーンアップ	既存のすべてのデータとパーティションを HX ストレージクラスタから削除する場合は、このチェックボックスをオンにします。たとえば、クラスタにこのソフトウェアをインストールするのは初めてではない場合、このチェックボックスをオンにします。
[VDI のみの展開用に最適化 (Optimize for VDi only deployment) ]	VDI 展開を最適化する場合は、このチェックボックスをオンにします。デフォルトでは、HyperFlex は仮想サーバインフラストラクチャ (VSI) 用にパフォーマンスが最適化されています。VDI 展開の場合にパフォーマンスパラメータを調整するには、このボックスをオンにします。このオプションは、オールフラッシュ HX モデルには影響しません。ハイブリッド HX クラスタでのみ有効にする必要があります。VDI と VSI が混在するワークロードを実行している場合は、このオプションを選択しないでください。
vCenter Single-Sign-On Server	このフィールドには、Cisco TAC から指示があった場合にのみ値を入力してください。

[進捗状況 (Progress) ] ページで、すべてのクラスタ構成タスクの進捗状況を確認します。導入が完了するまでには 20 ~ 45 分かかります。

ステップ 10 導入が完了すると、[導入の概要 (Summary Deployment) ] ページに導入の詳細が要約されて表示されず。

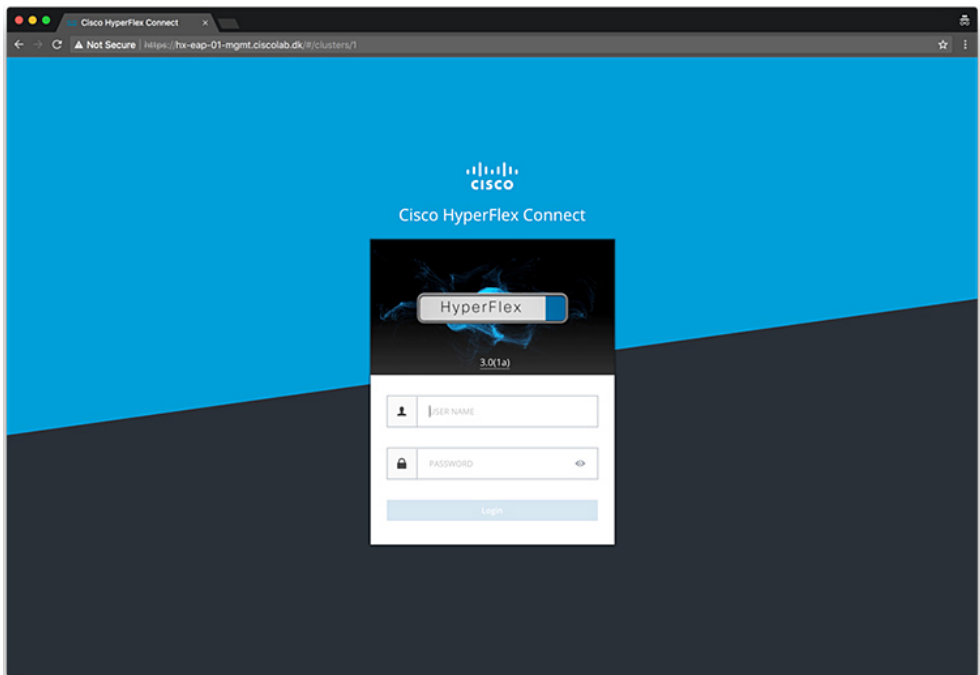
### 次のタスク

HX Data Platform プラグインのインストールを確認します。

## HX Connect へのログイン

Cisco HyperFlex コネクトは、HX ストレージのモニタリング、およびレプリケーション、暗号化、データストア、および仮想マシンのタスクに対し、HTML5 ベースのアクセスを提供します。この手順では、HX Connect の起動およびログインの概要を説明します。HX Connect へのログイン手順の詳細については、『[Cisco HyperFlex データ プラットフォーム管理者ガイド](#)』を参照してください。

ステップ 1 任意のブラウザで [https://Cluster\\_IP/](https://Cluster_IP/) または <https://FQDN> にアクセスして、HX Connect UI を起動します。



**ステップ 2** 次のクレデンシャルでログインします。

- ユーザ名 : **admin**
- パスワード : クラスタのインストール中に設定されたパスワードを使用します。

#### 次のタスク

HyperFlex クラスタが実稼働で使用できるようになる前に、インストール後のスクリプトを実行します。1GEと10/25GEのどちらのスイッチ設定を実行しているかに応じて、次を参照してください。

## (1 GbE のみ) インストール後のスクリプトの実行

**ステップ 1** Web ブラウザで、`http://<インストーラ VM の IP アドレス>/mssh` に移動し、ユーザ名 **admin** と、自分のパスワードを使用してログインし、`hx_post_install` を実行します。

**ステップ 2** **Enter** キーを押して、Web ベースの SSH ウィンドウでインストール後のタスクを開始します。

インストール後のスクリプトの実行時に、要件に応じ、次のオプションのいずれかを選択します。

- **1:** 新しく作成されたクラスタまたは既存のクラスタでインストール後スクリプトを実行します。このオプションを選択すると、スクリプトはクラスタ内のすべてのノードでインストール後の操作を実行します。

- **2:** 拡張ワークフローを実行した後、拡張ノードまたは新しく追加されたノードでインストール後スクリプトを実行します。このオプションを選択すると、スクリプトは拡張されたノードのリストを取得し、拡張されたノードでインストール後の操作を実行します。
- **3:** クラスタ内に固有の SSL 証明書を設定します。このオプションを選択すると、現在の証明書が新しく作成された SSL 証明書に置換されます。このオプションは、クラスタの拡張には必要ありません。

**ステップ 3** 画面の指示に従って、インストールを完了します。  
*hx\_post\_install* スクリプトは以下の事柄を行います。

- vCenter ホストのライセンス付与。
- ベスト プラクティスごとのクラスタの HA/DRS の有効化。
- vCenter の SSH/シェル警告の抑制。
- ベスト プラクティスに沿った vMotion の設定。
- ゲスト VLAN/ポートグループの追加。
- HyperFlex Edge 構成のチェックの実行。

Post\_install ワークフローが正常に完了すると、選択したオプションに基づいて実行された設定の概要が **[Cluster summary (クラスタ概要)]** の下に表示されます。

インストール後スクリプトの例は次のとおりです。

```
Select post_install workflow-
```

- ```
1. New/Existing Cluster
2. Expanded Cluster (for non-edge clusters)
3. Generate Certificate
```

```
Note: Workflow No.3 is mandatory to have unique SSL certificate in the cluster. By Generating this
certificate, it will replace your current certificate. If you're performing cluster expansion, then
this option is not required.
```

```
Selection: 1
Logging in to controller localhost
HX CVM admin password:
Getting ESX hosts from HX cluster...
vCenter URL: 10.121.48.111
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Found datacenter ucs659_dc
Found cluster ucs659-hx-cluster
```

```
post_install to be run for the following hosts:
ucs659.eng.storvisor.com
ucs660.eng.storvisor.com
```

```
Enter ESX root password:
HX Edge configuration detected
Uplink speed is detected as: 1G
Uplink count is detected as: 2
```

```
Enter vSphere license key? (y/n) n
```

```
Enable HA/DRS on cluster? (y/n) y
Successfully completed configuring cluster HA.
Successfully completed configuring cluster DRS.

Disable SSH warning? (y/n) y

Add vmotion interfaces? (y/n) y
Netmask for vMotion: 255.255.240.0
vMotion IP for ucs659.eng.storvisor.com: 10.64.73.131
Adding vmotion to ucs659.eng.storvisor.com
Adding vmkernel to ucs659.eng.storvisor.com
Updating portgroup vmotion on ucs659.eng.storvisor.com
Successfully updated portgroup vmotion on host ucs659.eng.storvisor.com. activeNic: vmnic0 standbyNic:
vmnic1
vMotion IP for ucs660.eng.storvisor.com: 10.64.73.132
Adding vmotion to ucs660.eng.storvisor.com
Adding vmkernel to ucs660.eng.storvisor.com
Updating portgroup vmotion on ucs660.eng.storvisor.com
Successfully updated portgroup vmotion on host ucs660.eng.storvisor.com. activeNic: vmnic0 standbyNic:
vmnic

Add VM network VLANs? (y/n) y

Run health check? (y/n) y

Validating cluster health and configuration...

Cluster Summary:
  Version - 4.0.2f-35930
  Model - HX220C-M5SX
  Health - HEALTHY
  ASUP enabled - False
```

## (10/25GE のみ) インストール後のスクリプトの実行

**ステップ 1** Web ブラウザで、`http://<インストーラ VM の IP アドレス>/mssh` に移動し、ユーザ名 **admin** と、自分のパスワードを使用してログインし、`hx_post_install` を実行します。

**ステップ 2** **Enter** キーを押して、Web ベースの SSH ウィンドウでインストール後のタスクを開始します。

インストール後のスクリプトの実行時に、要件に応じ、次のオプションのいずれかを選択します。

- **1:** 新しく作成されたクラスタまたは既存のクラスタでインストール後スクリプトを実行します。このオプションを選択すると、スクリプトはクラスタ内のすべてのノードでインストール後の操作を実行します。
- **2:** 拡張ワークフローを実行した後、拡張ノードまたは新しく追加されたノードでインストール後スクリプトを実行します。このオプションを選択すると、スクリプトは拡張されたノードのリストを取得し、拡張されたノードでインストール後の操作を実行します。
- **3:** クラスタ内に固有の SSL 証明書を設定します。このオプションを選択すると、現在の証明書が新しく作成された SSL 証明書に置換されます。このオプションは、クラスタの拡張には必要ありません。

**ステップ 3** 画面の指示に従って、インストールを完了します。  
*hx\_post\_install* スクリプトは以下の事柄を行います。

- vCenter ホストのライセンス付与。
- ベスト プラクティスごとのクラスタの HA/DRS の有効化。
- vCenter での SSH/シェル警告の削除。
- ベスト プラクティスに沿った vMotion の設定。
- 新しい VM ポートグループの追加。
- HyperFlex Edge のヘルス チェック。

Post\_install ワークフローが正常に完了すると、選択したオプションに基づいて実行された設定の概要が **[Cluster summary (クラスタ概要)]** の下に表示されます。

インストール後スクリプトの例は次のとおりです。

```
Select post_install workflow-
```

1. New/Existing Cluster
2. Expanded Cluster (for non-edge clusters)
3. Generate Certificate

```
Note: Workflow No.3 is mandatory to have unique SSL certificate in the cluster. By Generating this certificate, it will replace your current certificate. If you're performing cluster expansion, then this option is not required.
```

```
Selection: 1
Cluster IP/FQDN : 10.1.22.13
HX CVM admin password:
Getting ESX hosts from HX cluster...
vCenter URL: 10.1.22.150
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Found datacenter spiderman
Found cluster spiderman
```

```
post_install to be run for the following hosts:
hx-node-1.spiderman.hx.local
hx-node-2.spiderman.hx.local
```

```
Enter ESX root password:
HX Edge configuration detected
Uplink speed is detected as: 10G
Uplink count is detetec as: 2
```

```
Enter vSphere license key? (y/n) n
```

```
Enable HA/DRS on cluster? (y/n) y
Successfully completed configuring cluster HA.
```

```
Disable SSH warning? (y/n) y
```

```
Add vmotion interfaces? (y/n) y
Netmask for vMotion: 255.255.255.0
VLAN ID: (0-4096) 2032
vMotion MTU is set to use jumbo frames (9000 bytes). Do you want to change to 1500 bytes? (y/n) n
Do you wish to enter the range of vMotion IPs (y/n) y
```

```
Please enter vMotion Ip range (format: IP_start-IP_end) 10.20.32.16-10.20.32.17
Vmotion ip 10.20.32.16 used for hx-node-1.spiderman.hx.local
Adding vmkernel to hx-node-1.spiderman.hx.local
Vmotion ip 10.20.32.17 used for hx-node-2.spiderman.hx.local
Adding vmkernel to hx-node-2.spiderman.hx.local

Add VM network VLANs? (y/n) y
  Port Group Name to add (VLAN ID will be appended to the name in ESXi host): infra
  VLAN ID: (0-4096) 199
  Adding infra-199 to hx-node-1.spiderman.hx.local
  Adding infra-199 to hx-node-2.spiderman.hx.local
Add additional VM network VLANs? (y/n) n

Run health check? (y/n) y

Validating cluster health and configuration...

Cluster Summary:
Version - 5.0.2a-41212
Model - HXAF220C-M5SX
Health - HEALTHY
ASUP enabled - False
hxshell:~$
```

## vMotion の自動構成

hx\_post\_install スクリプトにより、ネットワーク トポロジに基づいて自動的に vMotion が構成されます。

### 1GE シングル スイッチの考慮事項

- 自動構成では、トランク ポートのみがサポートされ、専用 vMotion VLAN を使用した構成のみが可能です。
- アクセス ポートを使用する場合や、共有 vMotion VLAN を使用して構成する場合は、既存の管理 VMkernel ポート (vmk0) 上に vMotion を手動で構成する必要があります。
- vMotion は、1GE 管理および VM ネットワーク アップリンクで共有されます。
- vMotion によってリンクが完全に飽和状態にならないよう、デフォルトの 500Mbps トラフィック シェーパを使用して新しい VMKernel ポート (vmk2) が作成されます。このデフォルト値は、hx\_post\_install の実行後に変更することができます。[手動によるトラフィック シェーピングの構成 \(285 ページ\)](#) を参照してください。

### 1GE デュアル スイッチの考慮事項

- vMotion は専用の 1GE アップリンクで設定されます。
- 新しい VMKernel ポート (vmk2) が作成されます。フェールオーバーの順序は、通常のネットワーク条件下でストレージ データと vMotion が分離されるように自動構成されます。

- この設定では、トラフィック シェーパは不要です。

### 10/25GE スイッチの考慮事項

- vMotion は、専用の vMotion vSwitch 上で専用のアクティブ/スタンバイ vNIC と共に設定されています。
- 新しい VMKernel ポート (vmk2) が作成されます。フェールオーバーの順序は、通常のネットワーク条件下でストレージデータと vMotion が分離されるように自動構成されません。
- この設定ではトラフィック シェーパは必要ありませんが、帯域幅は管理、vMotion、およびゲスト VM ポート グループで共有されます。ネットワーク要件に応じて、オプションのトラフィック シェーパを適用することができます。

## 手動による vMotion の構成

vMotion は環境のニーズに応じてさまざまな方法で構成できます。このタスクで説明するのは構成の一例です。この手順を基に、必要に応じてバリエーションを適用できます。

この設定では、ポート 1 でランキングされる固有の VLAN を vMotion に使用します。

- 
- ステップ 1 vSphere を起動し、管理者として vCenter Server にログインします。
  - ステップ 2 [vCenter Inventory リスト (vCenter Inventory Lists)] で HyperFlex ホストをクリックし、[管理 (Manage)] > [ネットワークング (Networking)] > [仮想スイッチ (Virtual Switches)] の順に移動します。
  - ステップ 3 [ホスト ネットワークの追加 (Add Host Networking)] をクリックします。
  - ステップ 4 [ネットワークの追加ウィザード: 接続タイプ (Add Network Wizard: Connection Type)] ページで、[VMkernel] をクリックしてから、[次へ (Next)] をクリックします。
  - ステップ 5 [vswitch-hx-inband-mgmt を使用 (Use vswitch-hx-inband-mgmt)] をクリックしてから、[次へ (Next)] をクリックします。
  - ステップ 6 [ネットワーク ラベル (Network Label)] に識別しやすいラベル (vMotion などを入力し、正しい [VLAN ID] を入力してから、[vMotion にこのポート グループを使用 (Use this portgroup for vMotion)] をオンにし、[次へ (Next)] をクリックします。
  - ステップ 7 [次の IP 設定を使用 (Use the following IP settings)] をクリックし、スタティックな IPv4 アドレスと [サブ ネットマスク (Subnet Mask)] の値を入力してから、[次へ (Next)] をクリックします。
  - ステップ 8 設定内容を確認し、[Finish (終了)] をクリックします。
  - ステップ 9 HyperFlex ストレージクラスタに含まれるすべての HyperFlex ホストとコンピューティング専用ホストについて、上記の手順を繰り返します。
-



## 手動によるトラフィックシェーピングの構成

1GE シングルスイッチ展開で、共有アップリンクでのネットワーク輻輳を防ぐためのベストプラクティスは、vMotion インターフェイスでトラフィックシェーピングを有効にすることです。トラフィックシェーピングを設定しないと、vMotion トラフィックのため、同じ物理 1GE ポートを共有する管理トラフィックと VM ゲストトラフィックが使える帯域幅が非常に少なくなります。vMotion 標準スイッチでは、出力トラフィックのシェーピングのみを設定できません。

**ステップ 1** vSphere を起動し、管理者として vCenter Server にログインします。

**ステップ 2** [vCenter Inventory リスト (vCenter Inventory Lists)] で HyperFlex ホストをクリックし、[管理 (Manage)] > [ネットワークング (Networking)] > [仮想スイッチ (Virtual Switches)] の順に移動します。

**ステップ 3** vMotion ポートグループが含まれている vSwitch を選択します。

**ステップ 4** vMotion ポートグループ名をクリックし、[設定の編集 (Edit Settings)] (鉛筆アイコン) をクリックします。

**ステップ 5** 左側のメニューで、[トラフィックシェーピング (Traffic shaping)] を選択します。

**ステップ 6** [オーバーライド (Override)] チェックボックスをオンにしてトラフィックシェーピングを有効にします。

**ステップ 7** 平均帯域幅とピーク帯域幅を、環境のニーズに適合する値に設定します。たとえば、1GE アップリンクで使用可能な総帯域幅の 50% を表す 500,000 kbit/sec を両方の帯域幅に使用できます。

**ステップ 8** [OK] を選択して設定を保存します。

(注) 平均帯域幅を適切な値に設定するよう注意してください。ピーク帯域幅はトラフィックのバーストにのみ適用され、vMotion の動作時には短時間で枯渇します。

## (10 / 25GE) 追加 VIC ポートの使用 (オプション)

(異なる VLAN などの) 異なるスイッチへのアップリンクが必要な場合、またはゲスト VM に追加の専用帯域幅が必要な場合は、HX のインストール後に VIC からポート 3 と 4 を接続できます。ここでは、デフォルトで作成される設定と、追加ポートで追加の vNIC を作成する方法について説明します。

**デフォルトの 10GE VIC 設定 :**

インストール時に、HyperFlex は VIC 1457 を次のように設定します。

- ポートチャンネルを無効にします。
- HyperFlex が動作するために必要な 8 つの vNIC を設定します (VIC の最初の 2 つのポートに対応するアップリンクポート番号は 0 または 1 に設定します)。

| Name                          | CDN          | MAC Address       | MTU  | usNIC | Uplink Port | CoS | VLAN | VLAN Mode | ISCSI Boot | PXE Boot | Channel | Port Profile | Uplink Fallback |
|-------------------------------|--------------|-------------------|------|-------|-------------|-----|------|-----------|------------|----------|---------|--------------|-----------------|
| <input type="checkbox"/> eth0 | hv-mgmt-a    | 00:25:B5:50:A1:01 | 9000 | 0     | 0           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |
| <input type="checkbox"/> eth1 | hv-mgmt-b    | 00:25:B5:50:B2:01 | 9000 | 0     | 1           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |
| <input type="checkbox"/> eth2 | storage-d... | 00:25:B5:50:A3:01 | 9000 | 0     | 0           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |
| <input type="checkbox"/> eth3 | storage-d... | 00:25:B5:50:B4:01 | 9000 | 0     | 1           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |
| <input type="checkbox"/> eth4 | vm-netwo...  | 00:25:B5:50:A5:01 | 9000 | 0     | 0           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |
| <input type="checkbox"/> eth5 | vm-netwo...  | 00:25:B5:50:B6:01 | 9000 | 0     | 1           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |
| <input type="checkbox"/> eth6 | hv-vmolo...  | 00:25:B5:50:A7:01 | 9000 | 0     | 0           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |
| <input type="checkbox"/> eth7 | hv-vmolo...  | 00:25:B5:50:B8:01 | 9000 | 0     | 1           | 0   | NONE | TRUNK     | disabled   | disabled | N/A     | N/A          | N/A             |

## ネットワーク設定例

### 1GE シングル スイッチ

トランク ポートを使用している Nexus 5548

```

vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-VMOTION
vlan 104
  name HX-GUESTVM
...
interface Ethernet2/11
  description HX-01-Port1
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/12
  description HX-01-Port2
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/13
  description HX-02-Port1
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/14
  description HX-02-Port2
  switchport mode trunk
  switchport trunk allowed vlan 101-104
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/15
  description HX-03-Port1

```

```
switchport mode trunk
switchport trunk allowed vlan 101-104
spanning-tree port type edge trunk
speed 1000
interface Ethernet2/16
description HX-03-Port2
switchport mode trunk
switchport trunk allowed vlan 101-104
spanning-tree port type edge trunk
speed 1000
```

### トランク ポートを使用している Catalyst 3850-48T

```
vlan 101
name HX-MGMT
vlan 102
name HX-STORAGE
vlan 103
name HX-vMOTION
vlan 104
name HX-GUESTVM
...
interface GigabitEthernet1/0/1
description HX-01-Port1
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/2
description HX-01-Port2
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/3
description HX-02-Port1
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/4
description HX-02-Port2
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/5
description HX-03-Port1
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
interface GigabitEthernet1/0/6
description HX-03-Port2
switchport trunk allowed vlan 101-104
switchport mode trunk
speed 1000
spanning-tree portfast trunk
```

### 1GE デュアル スイッチ

#### トランク ポートを使用している Nexus 5548

この設定では、ネイティブ vlan 105 を使用しているインバンド管理とともに DHCP を使用します。このスイッチは両方の 1GE LOM に接続して、dhcp relay を使用します。

```
ip dhcp relay
...
interface Vlan105
  ip address 10.1.2.1/24
  ip dhcp relay address 10.1.1.2
  no shutdown
vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-vMOTION
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-DHCP-CIMC
...
interface Ethernet2/11
  description HX-01-Port1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/12
  description HX-01-Port2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/13
  description HX-02-Port1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/14
  description HX-02-Port2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/15
  description HX-03-Port1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
interface Ethernet2/16
  description HX-03-Port2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk
  speed 1000
```

スイッチ #2 で同じ設定を繰り返します。dhcp relay コマンドと interface Vlan 105 コマンドは削除します。

### トランク ポートを使用している Catalyst 3850-48T

この構成では、vlan 105 に静的に割り当てられている CIMC IP を使用します。すべてのトランク インターフェイスですべての vlans が許可されます。セキュリティ上の理由から、すべてのポート設定に switchport trunk allowed vlan ステートメントを追加し、VLAN を HyperFlex の展開に必要なものに限定することを推奨します。

```
vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-VMOTION
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-CIMC
...
interface GigabitEthernet1/0/1
  description HX-01-Port1
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/2
  description HX-01-Port2
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/3
  description HX-02-Port1
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/4
  description HX-02-Port2
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/5
  description HX-03-Port1
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
interface GigabitEthernet1/0/6
  description HX-03-Port2
  switchport mode trunk
  speed 1000
  spanning-tree portfast trunk
```

スイッチ #2 で同じ設定を繰り返します。

### 10GE デュアルスイッチ

#### トランク ポートを使用している Nexus 9000

```
vlan 101
  name HX-MGMT
```

```

vlan 102
  name HX-STORAGE
vlan 103
  name HX-vMOTION
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-DHCP-CIMC
...
interface Ethernet1/35
  description M5-Edge-Node1-VIC1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/36
  description M5-Edge-Node1-VIC2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/37
  description M5-Edge-Node2-VIC1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/38
  description M5-Edge-Node2-VIC2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/39
  description M5-Edge-Node3-VIC1
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

interface Ethernet1/40
  description M5-Edge-Node3-VIC2
  switchport mode trunk
  switchport trunk native vlan 105
  switchport trunk allowed vlan 101-105
  spanning-tree port type edge trunk

```

### トランクポートを使用している Catalyst 9300

```

vlan 101
  name HX-MGMT
vlan 102
  name HX-STORAGE
vlan 103
  name HX-vMOTION
vlan 104
  name HX-GUESTVM
vlan 105
  name HX-CIMC
...

```

```
interface GigabitEthernet1/0/1
description M5-Edge-16W9-LOM1
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/2
description M5-Edge-16W9-LOM2
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/3
description M5-Edge-16UQ-LOM1
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/4
description M5-Edge-16UQ-LOM2
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/5
description M5-Edge-05G9-LOM1
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk

interface GigabitEthernet1/0/6
description M5-Edge-05G9-LOM2
switchport trunk allowed vlan 101-105
switchport mode trunk
spanning-tree portfast trunk
```

## 10/25GE 2 ノード 2 ルーム

### QoS を備えた Catalyst 9300

この設定では、Quality of Service を使用して、ルーム トポロジごとに 10 または 25 ギガビットイーサネット スタック スイッチを使用し、HyperFlex ストレージ トラフィックにマーキングし、優先順位を付けます。

```
class-map match-all PQ_Storage
match dscp ef
class-map match-all Storage
match access-group name Storage
...
policy-map Storage_Mark
class Storage
set dscp ef
class class-default
policy-map Storage_Queue
class PQ_Storage
priority level 1
queue-buffers ratio 80
class class-default
bandwidth remaining percent 100
queue-buffers ratio 20
...
interface Port-channel98
```

```
switchport trunk allowed vlan 101,102,103,104,105
switchport mode trunk
!
interface GigabitEthernet1/0/3
description SERVER1-Dedicated-CIMC
switchport access vlan 145
switchport mode access
spanning-tree portfast
!
interface TenGigabitEthernet1/1/1
description SERVER1-VIC-1
switchport trunk allowed vlan 101,102,103,104,105
switchport mode trunk
spanning-tree portfast trunk
service-policy input Storage_Mark
!
interface TenGigabitEthernet2/1/1
description SERVER1-VIC-2
switchport trunk allowed vlan 101,102,103,104,105
switchport mode trunk
spanning-tree portfast trunk
service-policy input Storage_Mark
!

interface TenGigabitEthernet1/1/8
description cross-connect-01
switchport trunk allowed vlan 101,102,103,104,105
switchport mode trunk
channel-group 98 mode on
service-policy output Storage_Queue
!
interface TenGigabitEthernet2/1/8
description cross-connect-02
switchport trunk allowed vlan 101,102,103,104,105
switchport mode trunk
shutdown
channel-group 98 mode on
service-policy output Storage_Queue
!
...
ip access-list extended Storage
10 permit ip 169.254.1.0 0.0.0.255 169.254.1.0 0.0.0.255
```

スイッチ スタック #2 で同じ設定を繰り返します。



## 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。