



Cisco HyperFlex Systems リリース 2.5 インストール ガイド (VMware ESXi 向け)

初版：2017年7月31日

最終更新：2018年12月10日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

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

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

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

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

THE 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 NON-INFRINGEMENT 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.

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: www.cisco.com/go/trademarks. 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)

© 2018 Cisco Systems, Inc. All rights reserved.



目次

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 コンポーネント 3
	Cisco HyperFlex HX シリーズ システム 設定オプション 5
	Cisco HyperFlex HX シリーズ システム 管理コンポーネント 6
	Cisco HyperFlex Connect ユーザ インターフェイスとオンライン ヘルプ 7
	[Dashboard] ページ 9
	[Operational Status] ダイアログボックス 11
	[Resiliency Health] ダイアログボックス 12

第 3 章	インストールの前提条件 13
	VMware ESXi のソフトウェア要件 13
	必要なハードウェア ケーブル 16
	ホスト要件 16
	ディスクの要件 17
	ブラウザの推奨事項 23
	ポート要件 24
	HyperFlex 外部接続 31
	ファブリック インターコネクタのアップリンクのプロビジョニング 32
	ネットワーク設定 35
	VLAN および vSwitch の要件 37

Cisco UCS の要件	37
ハイパーバイザ要件	38
ストレージクラスタ要件	39
vCenter 設定の要件	41
システム サービス要件	42
コントローラ VM 用 CPU リソース予約	44
コントローラ仮想マシン用メモリ リソース予約	44
自動サポート 要件	45
シングル サインオンの要件	46

第 4 章

Cisco HyperFlex Systems サーバのインストール	47
Cisco HyperFlex ノードの設置	47
ファブリック インターコネクタの設定	48
GUI によるプライマリ ファブリック インターコネクタの設定	49
GUI による従属ファブリック インターコネクタの設定	51
CLI によるプライマリ ファブリック インターコネクタの設定	53
CLI による従属ファブリック インターコネクタの設定	55
コンソールセットアップの確認	56
Cisco UCS ファブリック インターコネクタへの HX シリーズ サーバの接続	58
概要	58
ファブリック インターコネクタへのコンバージド ノードの接続	58
物理的な接続の図	60
ファブリック インターコネクタへのコンピューティング専用ノードの接続	61

第 5 章

Cisco HyperFlex Systems の設定	63
vSphere Web クライアントを使用した HX Data Platform インストーラ OVA の展開	63
静的 IP アドレスによる HX データ プラットフォーム インストーラ OVA の展開	66
Cisco HX Data Platform インストーラへのログイン	67
HX データ プラットフォーム インストーラの終了	68
Syslog の設定	68
HyperFlex クラスタの設定	69

GPU を搭載した HyperFlex ノードの設置	80
HyperFlex クラスタの作成に関する考慮事項	81

第 6 章

HyperFlex Data Platform を使用したスマート ライセンスの設定 83

スマート ライセンスと HyperFlex	83
スマート ライセンスへのクラスタの登録	88
スマート ライセンス承認の更新	90
スマート ライセンスからのクラスタの登録解除	90

第 7 章

クラスタ設定後のタスク 93

クラスタ設定後のガイドライン	93
ホスト上のネットワーク デバイスの PCI バススルー有効化	94
インストール後のスクリプトの実行	94
ESXi ホスト ルート パスワードの変更	98
ストレージ コントローラ パスワードの変更	99
vSphere を介した HX データ プラットフォーム プラグインへのアクセス	99
ストレージ クラスタでのデータストアの追加	100
HA ハートビートの設定	100
HyperFlex の Auto Support と Smart Call Home	101
HX Connect を使用した自動サポートの構成	102
CLI を使用した通知設定の構成	103
データ コレクションの Smart Call Home の構成	104
レプリケーション ペアリング	107
プライベート VLAN の追加	108
プライベート VLAN の概要	108
既存の VM がない状態で VM ネットワークのプライベート VLAN を設定する	109
ESX ホストでのプライベート VLAN の設定	109
既存の VM で VM ネットワークのプライベート VLAN を設定する	109
vSphere 標準スイッチでの VMNIC の削除	110
vSphere 分散スイッチの作成	110
vSphere 分散スイッチでのプライベート VLAN の作成	111

	分散ポートグループでのプライベート VLAN の設定	111
	分散型仮想スイッチと Cisco Nexus 1000v	112
	HX Data Platform での vCenter のホスト	113
	AMD GPU の展開	113
第 8 章	複数の HX クラスタの設定	115
	複数のクラスタの設定	115
第 9 章	HX-FI ドメインへの UCS サーバの追加	117
	既存の HX FI ドメインへの Cisco UCS サーバの追加	117
第 10 章	Cisco HyperFlex システム クラスタの展開	119
	クラスタ展開のガイドライン	119
	混合 M4/M5 クラスタを作成する場合の前提条件	120
	混合クラスタ展開中の手順	121
	コンバージド (HX220c/HX240c) ノードの追加に関する前提条件	121
	コンバージド ノードの準備	122
	既存のクラスタへのコンバージド ノードの追加	123
	コンピューティング専用ノードの追加に関する前提条件	133
	コンピューティング専用ノードの準備	134
	HX データ プラットフォーム インストーラの確認	134
	UCS Manager を使用したコンピューティング専用ノードへの HX プロファイルの適用	135
	コンピューティング ノードへの VMware ESXi のインストール	135
	既存のクラスタへのコンピューティング専用ノードの追加	137
	クラスタ展開の障害の解決	143
	ロジカルアベイラビリティゾーンの有効化	144
第 11 章	混在 CPU を伴うクラスタの設定	147
	概要	147
	混合 CPU を使用するための前提条件	147
	EVC モードとの CPU 互換性	148

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 148

第 12 章

Cisco HyperFlex Systems のカスタマイズされたインストール方法 151

概要 151

Cisco HyperFlex Systems が事前設定されていない場合のインストールおよび設定のワークフロー 151

VMware ESXi をインストールします。 152

Cisco UCS Manager を使用した vMedia およびブート ポリシーの設定 153

リモート KVM コンソールのオープン 154

サーバの再起動 154

vMedia ポリシーおよびブート ポリシーの変更の取り消し 155



第 1 章

新機能および変更された機能に関する情報

- [新機能および変更情報 \(1 ページ\)](#)

新機能および変更情報



注目 『2.X Getting Started Guide』の名前が『VMware ESXi インストレーションガイド』に変更されました。

次の表に、最新リリースでの新機能とこのガイドにおける変更点の概要を示します。

機能	説明	追加日	参照先
Auto Support の設定	Smart Call Home の HTTPS データ収集の設定。 Auto Support (ASUP) の電子メール通知の設定。	2017 年 4 月 28 日	HyperFlex の Auto Support 必須のポート
SED	保管中のデータの暗号化専用のハードウェア サポート。	2017 年 4 月 28 日	ディスクの要件



第 2 章

概要

この章では、Cisco HyperFlex Systems 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 コンポーネント \(3 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システム 設定オプション \(5 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システム 管理コンポーネント \(6 ページ\)](#)
- [Cisco HyperFlex Connect ユーザ インターフェイスとオンラインヘルプ \(7 ページ\)](#)

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 シリーズ システム 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。このハイパーコンバージドシステムでは、ワークロードのニーズに基づいて、統合されたリソースのプールが提供されます。

Cisco HyperFlex HX シリーズ システム コンポーネント

- **Cisco HX シリーズ サーバ**— Cisco HyperFlex System の設定には、次のいずれのサーバも使用できます。
 - **コンバージド ノード—全フラッシュ**: Cisco HyperFlex HXAF240c M5、HXAF220c M5、HXAF240c M4、HXAF220c M4.
 - **コンバージド ノード—ハイブリッド**: Cisco HyperFlex HX240c M5、HX220c M5、HX240c M4、HX220c M4.
 - **コンピューティング専用**—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、C240 M5.

- **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 インストーラでは、Cisco UCS Manager 内にサービス プロファイルとポリシーが設定され、コントローラ VM の導入、ソフトウェアのインストール、ストレージクラスタの作成、および VMware vCenter プラグインの更新が行われます。
 - **ストレージコントローラ VM**：HX Data Platform インストーラを使用して、管理対象ストレージクラスタの各コンバージドノードで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 Plug-in**：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 シリーズ サーバにネットワークの接続性と管理機能の両方を提供します。

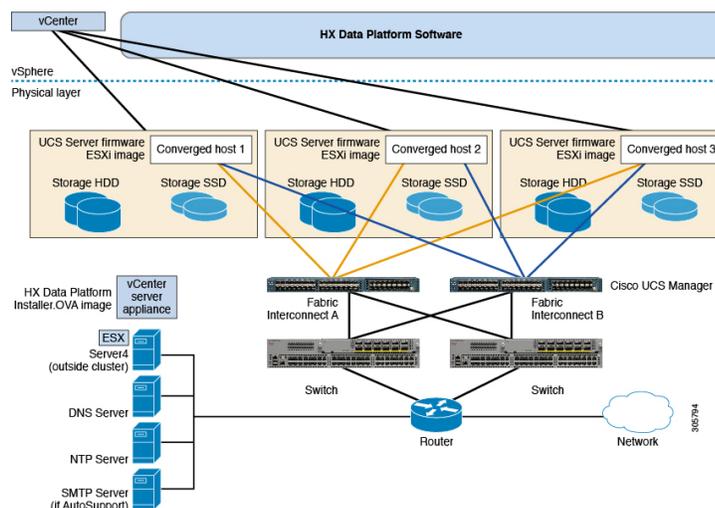
このドキュメントでは、購入して Cisco HyperFlex System の一部として導入された FI のことを **HX FI ドメイン**とも呼んでいます。サポートされているファブリック インターコネク トは次のとおりです。

- Cisco UCS 6200 シリーズ Fabric Interconnect
- Cisco UCS 6300 シリーズ 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 コンポーネント 詳細



Cisco HyperFlex HX シリーズ システム 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 System にさらにストレージ機能を追加する場合は、単に Cisco HX シリーズ サーバを追加します。



(注) **HX Cluster**は、HX シリーズサーバのグループです。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。

次の図に示すように、いずれかの方法で HX Cluster を設定できます。

HX クラスタの設定オプション

図 2: Cisco HyperFlex ハイブリッド M5 設定

HX220c M5 Edge Cluster	HX220c M5 Cluster	HX240c M5 Cluster	HX M5 + Compute Node Clusters
			
*4.51TB – 12.04TB	**6.01TB – 32.10TB	**6.01TB – 92.29TB	NOTE: Consult Release Notes for Compute Node Support Details
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 1 x Cache SSD 3-8 x 1.2TB Capacity HDDs	Per-Node 1 x Cache SSD 6-8 x 1.2TB or 1.8TB Capacity HDDs SED Options [Coming Soon]	Per-Node 1 x Cache SSD 6-23 x 1.2TB or 1.8TB Capacity HDDs Support up to 2 GPUs SED Options [Coming Soon]	3-8 HX220 or HX240 Node Cluster + Up to 8 Compute Nodes Blade or Rack Local Disk, SD Card or SAN Boot

図 3: Cisco HyperFlex ハイブリッド M4 設定

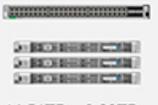
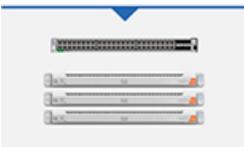
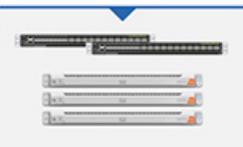
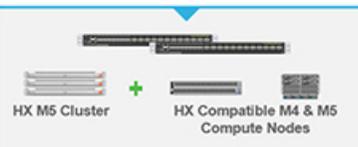
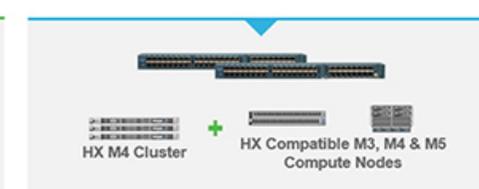
HX220c M4 Edge Cluster	HX220c M4 Cluster	HX240c M4 Cluster	HX M4 + Compute Node Clusters
			
*4.51TB – 9.03TB	**6.01TB – 24.07TB	**6.01TB – 92.29TB	
Smallest Footprint 3 Node Cluster (VSI, ROBO)	Smallest Footprint 3-8 Node Cluster (VDI, ROBO)	Capacity-Heavy 3-8 Node Cluster (VDI & VSI Workloads)	Compute-Heavy 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

図 4: Cisco HyperFlex のすべてのフラッシュ M5 設定

HXAF220c M5 Edge Cluster	HXAF220c M5 Cluster	HXAF240c M5 Cluster	HXAF M5 + Compute Node Clusters
			
*3.61TB – 38.53TB	**4.81TB – 136.97TB	**4.81TB – 393.78TB	NOTE: Consult Release Notes for Compute Node Support Details
Smallest Footprint 3 Node Cluster (VSI, ROBO)	Smallest Footprint 3–16 Node Cluster (VSI, VDI, DB, ROBO)	Capacity-Heavy 3–16 Node Cluster (VDI, VSI & DB Workloads)	Compute-Heavy Hybrid (Compute Bound Apps/VDI)
Per-Node 1 x Cache SSD 3–8 x 960GB or 3.84TB Capacity HDDs	Per-Node 1 x Cache SSD 6–8 x 960GB or 3.84TB Capacity HDDs **SED Options Orderable	Per-Node 1 x Cache SSD 6–23 x 960GB or 3.84TB Capacity HDDs Up to 2 x GPUs ***SED Options Orderable	3–16 HXAF220 or HXAF240 Node Cluster + Up to 16 Compute Nodes Blade or Rack Local Disk, SD Card or SAN Boot

306302

図 5: Cisco HyperFlex のすべてのフラッシュ M4 設定

HXAF220c M4 Cluster	HXAF240c M4 Cluster	HX M4 + Compute Node Clusters
		
*4.81TB – 102.72TB	*4.81TB – 393.78TB	NOTE: Consult Compatibility Matrix for Compute Node Support Details
Smallest Footprint 3–16 Node Cluster (VSI, VDI, DB, ROBO)	Capacity-Heavy 3–16 Node Cluster (VSI, VDI, & DB Workloads)	Compute-Heavy Hybrid (Compute Bound Apps/VDI)
Per-Node 1 x SAS or NVMe Cache SSD 6 x 960/3.84TB SSDs SED Options Available	Per-Node 1 x SAS or NVMe Cache SSD 6–23 x 960/3.84TB SSDs Up to 1 x GPU SED Options Available	3–16 Node HXAF220 or HXAF240 Cluster + Up to 16 Compute Nodes Blade or Rack Local Disk, SD Card or SAN Boot

306301

Cisco HyperFlex HX シリーズ システム 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 シリーズ サーバ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 を起動することです。UCS Manager は、ロールベース アクセス コントロールをサポートしています。

2つの Cisco UCS ファブリック インターコネクト (FI) 間で設定情報を複製して、高可用性ソリューションを実現します。一方の FI が使用不可能になっても、もう一方が代わりに務めます。

UCS Manager の主な利点は、ステートレス コンピューティングの概念です。HX Cluster の各ノードには設定情報が保持されていません。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 シリーズサーバに均一に適用されます。これにより、設定に一貫性が得られ、再利用しやすくなります。新しいサービスプロファイルは数分のうちに適用できます。

Cisco HX Data Platform

Cisco HX Data Platform は、シスコサーバをコンピューティングとストレージリソースの単一プールに変換するハイパーコンバイン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、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。また、ネイティブ圧縮と重複排除によって、VM に占有されている記憶域が削減されます。

HX Data Platform は、vSphere などの仮想化プラットフォームにインストールされます。これは、仮想マシン、アプリケーション、データ用のストレージを管理します。インストール時に、ユーザが Cisco HyperFlex HX Cluster の名前を指定すると、HX Data Platform によって各ノードにハイパーコンバインドストレージクラスタが作成されます。ストレージを増やす必要があります。HX Cluster にノードを追加する場合、HX Data Platform 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 は、VMware vCenter ベースの管理を備えています。vCenter サーバは、仮想化環境をモニタするために開発されたデータセンター管理サーバアプリケーションです。HX Data Platform には、事前設定済みの vCenter Server からアクセスし、すべてのストレージのタスクを実行できます。vCenter は、VMware vMotion、DRS、HA、および vSphere レプリケーションといった主要な共有ストレージ機能をサポートします。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 Platform 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に vCenter がインストールされている必要があります。vCenter には、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る vSphere クライアントからアクセスします。

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 へのユーザインターフェイスを提供します。これは、左側の [Navigation] ペインと右側の [Work] 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 でほとんどの操作を実行するには、管理者権限が必要です。

表 1: ヘッダーアイコン

アイコン	名前	説明
	メニュー	フルサイズのナビゲーション ウィンドウとアイコンのみの間を切り替え、ナビゲーション ウィンドウにマウスカーソルを移動します。
	メッセージ	ユーザが開始した操作の一覧が表示されます。たとえば、データストアの作成、ディスクの削除など。 [Clear All] を使用してすべてのメッセージを削除し、メッセージアイコンを非表示にします。
	設定	[Support]、[Notification]、および [Notification] の設定にアクセスします。 [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数が表示されます。エラーと警告の両方がある場合、カウントはエラーの数を示します。 アラームの詳細な情報は、[Alarms] ページを参照してください。
	ヘルプ	状況に応じた HX Connect 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、ログアウトなどのユーザの設定にアクセスします。 [User Settings] は管理者のみに表示されます。
	情報	その要素に関する、より詳細な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の場合、ヘッダー内の [Help] をクリックします。
- ダイアログボックスの場合、そのダイアログボックスの [Help] をクリックします。
- ウィザードの場合、そのウィザードの [Help] をクリックします。

テーブルヘッダーの共通のフィールド

HX Connect のいくつかのテーブルでは、テーブルの表示内容に影響する次の 3 つのフィールドのうち 1 つ以上が提供されます。

UI 要素	基本情報
[Refresh] フィールドおよびアイコン	<p>HX Cluster の動的な更新のためにテーブルを自動的に更新します。タイムスタンプは、テーブルが更新された最終時刻を示します。</p> <p>コンテンツを今すぐ更新するには円形のアイコンをクリックします。</p>
[Filter] フィールド	<p>入力したフィルタ テキストに一致する項目のみテーブルに表示します。以下の表の現在のページに記載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>[Filter] フィールドに選択テキストを入力します。</p> <p>[Filter] フィールドを空にするには、[x] 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>
[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。テーブルの内容は、選択したファイル形式でローカル 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 ファイルの形式を選択する下矢印をクリックします。ファイルの形式のオプションは、<code>cvs</code>、<code>xls</code> および <code>doc</code> 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>

[Dashboard] ページ



重要 読み取り専用ユーザには、ヘルプで利用可能なすべてのオプションが表示されるわけではありません。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 にログインしたときに表示される最初のページです。

UI 要素	基本情報
[Operational Status] セクション	<p>HX ストレージクラスタとアプリケーション パフォーマンスの機能の状態を示します。</p> <p>[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>
[Resiliency Health] セクション	<p>データのヘルス ステータスと、HX ストレージクラスタの耐障害性を示します。</p> <p>[Information] ⓘ をクリックして、復元カステータスと、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>
[Capacity] セクション	<p>ストレージの合計の内訳と、ストレージの使用量または未使用の容量が表示されます。</p> <p>ストレージの最適化、圧縮、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>
[Nodes] セクション	<p>HX ストレージクラスタ内のノード数と、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マウスを移動すると、そのノードの名前、IP アドレス、ノードの種類が表示され、容量、使用率、シリアル番号、およびディスクの種類へのデータへのアクセスが可能なディスクがインタラクティブに表示されます。</p>
[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 スナップショットを表示し、IOPS、スループット、および遅延データを表示します。</p> <p>詳細については、[Performance] ページを参照してください。</p>
[Cluster Time] フィールド	クラスタのシステム日付および時刻。

テーブルヘッダーの共通のフィールド

HX Connect のいくつかのテーブルでは、テーブルの表示内容に影響する次の 3 つのフィールドのうち 1 つ以上が提供されます。

UI 要素	基本情報
[Refresh] フィールドおよびアイコン	<p>HX Cluster の動的な更新のためにテーブルを自動的に更新します。タイムスタンプは、テーブルが更新された最終時刻を示します。</p> <p>コンテンツを今すぐ更新するには円形のアイコンをクリックします。</p>

UI 要素	基本情報
[Filter] フィールド	<p>入力したフィルタ テキストに一致する項目のみテーブルに表示します。以下の表の現在のページに記載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>[Filter] フィールドに選択テキストを入力します。</p> <p>[Filter] フィールドを空にするには、[x] 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>
[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。テーブルの内容は、選択したファイル形式でローカル 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 ファイルの形式を選択する下矢印をクリックします。ファイルの形式のオプションは、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>

[Operational Status] ダイアログボックス

HX ストレージ クラスタとアプリケーション パフォーマンスの機能の状態を示します。

UI 要素	基本情報
[Cluster Name] フィールド	この HX ストレージ クラスタの名前です。
[Cluster Status] フィールド	<ul style="list-style-type: none"> • [Online] : クラスタの準備ができています。 • [Offline] : クラスタの準備ができていません。 • [Read Only] : 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、静的クラスタ情報を表示し続けることはできます。 • [Out of space] : クラスタ全体でスペースが不足しているか、1つまたは複数のディスクでスペースが不足しています。どちらの場合も、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ができませんが、静的なクラスタ情報の表示は続行できます。

UI 要素	基本情報
[Data-at-rest encryption capable] フィールド	<ul style="list-style-type: none"> • [Available] • [Not supported] <p>あるいは、[Yes] と [No] を使用できます。</p>
[Reason to view] ドロップダウンリスト	現在の状況をもたらしている原因を説明するメッセージの数が表示されます。

[Close] をクリックします。

[Resiliency Health] ダイアログボックス

データのヘルス ステータスと、HX ストレージクラスタの耐障害性を示します。

名前	説明
[Resiliency Health] フィールド	<ul style="list-style-type: none"> • [Healthy] : データと可用性の点でクラスタは正常です。 • [Warning] : データまたはクラスタの可用性に対する悪影響が生じています。 • [Unknown] : クラスタがオンラインになるときの移行状態です。 <p>カラー コーディングとアイコンを使用して、さまざまなステータスの状態が表示されます。追加情報を表示するにはアイコンをクリックします。</p>
[Data Replication Compliance] フィールド	<ul style="list-style-type: none"> • [Compliant]
[Data Replication Factor] フィールド	HX ストレージクラスタ間での冗長データ レプリカの数を表示します。
[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障害の数を表示します。
[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型デバイス障害の数を表示します。
[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キャッシュ デバイス障害の数を表示します。
[Reason to view] ドロップダウンリスト	現在の状況をもたらしている原因を説明するメッセージの数が表示されます。

[Close] をクリックします。



第 3 章

インストールの前提条件

この章では、Cisco HyperFlex Systems のインストールと設定の要件について説明します。

- [VMware ESXi のソフトウェア要件 \(13 ページ\)](#)
- [必要なハードウェア ケーブル \(16 ページ\)](#)
- [ホスト要件 \(16 ページ\)](#)
- [ディスクの要件 \(17 ページ\)](#)
- [ブラウザの推奨事項 \(23 ページ\)](#)
- [ポート要件 \(24 ページ\)](#)
- [HyperFlex 外部接続 \(31 ページ\)](#)
- [ファブリック インターコネクタのアップリンクのプロビジョニング \(32 ページ\)](#)
- [ネットワーク設定 \(35 ページ\)](#)
- [VLAN および vSwitch の要件 \(37 ページ\)](#)
- [Cisco UCS の要件 \(37 ページ\)](#)
- [ハイパーバイザ要件 \(38 ページ\)](#)
- [ストレージクラスタ要件 \(39 ページ\)](#)
- [vCenter 設定の要件 \(41 ページ\)](#)
- [システム サービス要件 \(42 ページ\)](#)
- [コントローラ VM 用 CPU リソース予約 \(44 ページ\)](#)
- [コントローラ仮想マシン用メモリ リソース予約 \(44 ページ\)](#)
- [自動サポート 要件 \(45 ページ\)](#)
- [シングル サインオンの要件 \(46 ページ\)](#)

VMware ESXi のソフトウェア要件

ソフトウェア要件には、互換性のある Cisco HyperFlex Systems (HX) コンポーネントおよび VMware vSphere コンポーネントのバージョンを使用していることを確認するための検証が含まれています。

HyperFlex ソフトウェアのバージョン

Cisco HX Data Platform インストーラ、Cisco HX Data Platform、および Cisco UCS ファームウェアといった HX のコンポーネントは、さまざまなサーバにインストールされます。HX Storage Cluster とともに（またはその内部で）使用される各サーバの各コンポーネントに互換性があることを確認します。

- 事前設定された HX サーバと、インストールされている Cisco UCS サーバファームウェアのバージョンが同じであることを確認します。Cisco UCS ファブリック インターコネクタ (FI) のファームウェアバージョンが異なる場合は、ファームウェアのバージョンを調整する手順について、『[Cisco HyperFlex Systems Upgrade Guide](#)』を参照してください。
 - **M4:** 新しいハイブリッドまたはオールフラッシュ (Cisco HyperFlex HX240c M4 または HX220c M4) の導入の場合は、Cisco UCS Manager 3.1(3j) 以降がインストールされていることを確認してください。
 - **M5:** 新しいハイブリッドまたはすべてのフラッシュ (Cisco HyperFlex HX240c M5 または HX220c M5) を展開する場合は、Cisco UCS Manager 4.0(1a) またはそれ以降がインストールされていることを確認してください。
- SED ベース HyperFlex システムについては、A (インフラストラクチャ) および C (ラックサーバ) バンドルが、M4 SED システムに対して Cisco UCS Manager バージョン 3.1(3h) またはそれ以降であることが必要です。すべてのバンドルが M5 SED システムに対して、Cisco UCS Manager バージョン 4.0(1a) 以上であることを確認します。
- HX サーバを再インストールするには、サポートされている互換性のあるソフトウェアのバージョンをダウンロードします。要件と手順については『[Cisco HyperFlex Systems インストールガイド \(VMware ESXi 向け\)](#)』を参照してください。

HyperFlex のライセンス

バージョン 2.6(1a) の時点で、HyperFlex では VMware PAC のライセンスがサポートされています。既存 VMware 組み込みライセンスは常にサポートされます。

バージョン 2.5(1a) の時点で、HyperFlex ではスマートライセンス メカニズムを使用してライセンスを適用するようになっていきます。詳細および手順については、『[Cisco HyperFlex Systems インストールガイド \(VMware ESXi 向け\)](#)』を参照してください。

サポートされる VMware vSphere のバージョンとエディション

各 HyperFlex リリースは、特定バージョンの vSphere、VMware vCenter、VMware ESXi との互換性があります。

- すべての HX サーバに、互換性のある vSphere のバージョンがプレインストールされていることを確認します。
- vCenter のバージョンが ESXi のバージョンと同じ、またはそれ以降であることを確認します。

- **VMware Product Interoperability Matrix** を参照して、vCenter と ESXi のバージョンに互換性があることを確認してください。次の表で ESXi と vCenter の両方がサポートされている限り、新しいバージョンの vCenter を古いバージョンの ESXi とともに使用することができます。
- ルートレベルの権限および関連パスワードが付与された vCenter 管理者アカウントがあることを確認します。

VMware vSphere ライセンスの要件

vSphere ライセンスを HyperFlex システムに適用する方法は、そのライセンスの購入方法に応じて変わります。

• vSphere ライセンスを HyperFlex とともに購入した場合

各 HyperFlex サーバはいずれも、出荷時に Enterprise または Enterprise Plus エディションがプレインストールされています。



(注)

- HX ノードには、プレインストール OEM ライセンスがあります。HX サーバを受け取った後、ブートドライブのコンテンツを削除または上書きすると、プレインストールされたライセンスも削除されます。
- OEM ライセンス キーは、新しい VMware vCenter 6.0 U1b 機能です。以前のバージョンは OEM ライセンスをサポートしていません。
- プレインストールされた HX ノードはすべて同じ OEM ライセンス キーを共有します。vSphere OEM キーを使用すると、「Usage」の数が「Capacity」の値を超えることがあります。
- [Assign license] セクションの [Add Host] ウィザードで vCenter に HX ホストを追加する場合は、[OEM license] を選択してください。

実際の vSphere OEM ライセンス キーは難読化されています
(例：0N085-XXXXX-XXXXX-XXXXX-10LHH)。
- Standard、Essentials Plus、ROBO エディションは、HX サーバにプレインストールされていません。

• vSphere ライセンスを HyperFlex とともに購入していない場合

HX ノードには、vSphere の基本ライセンスがプレインストールされています。初期設定後、ライセンスはサポートされている vSphere のバージョンに適用されます。

• vSphere PAC ライセンスを とともに購入した場合

VMwareからのPACライセンスレターの指示に従ってライセンスを MY VMware アカウントに追加し、次に指示に従って HX ホストを vCenter に追加して PAC ライセンスを割り当てます。

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、サーバごとに最低 2 つの 10 Gb Small Form-Factor Pluggable (SFP) を使用します。6300 シリーズ FI を使用する場合は、サーバごとに最低 2 つの 40-GbE QSFP を使用します。
- 一端に RJ-45 コネクタがあり、他端に DB9 コネクタがあるファブリック インターコネクト コンソールケーブル (CAB-CONSOLE-RJ45) 。このケーブルは、ラップトップの RS-232 コンソール接続に接続するのに使用します。
- 標準の電源コードには、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。オプションのジャンパ電源コードには、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。

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 ケーブルを使用すると、システムに Cisco HX シリーズ サーバの接続が可能になります。このケーブルには、DB9 シリアルコネクタ、モニタ用の VGA コネクタ、キーボードおよび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、システムで稼働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 ケーブルは、UCS ラックマウントとブレードサーバの両方に使用されます。

M4 または M5 サーバのケーブルと注文情報に関する詳細は、それぞれ [Cisco HyperFlex HX シリーズモデル](#) と [Cisco UCS B200 ブレードサーバのインストールおよびサービス ノート](#) 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 つのコンバインド HyperFlex ノードが含まれています。コンピューティング能力を高めるには、別途ストレージを用意しなくても、コンピューティング専用ノードを追加するというオプションがあります。HyperFlex クラスタ内の各サーバは、HyperFlex ノードと呼ばれます。ストレージ クラスタを導入する前に、それぞれのノードに次の設定がインストールおよび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、『[Cisco HX240c/220c HyperFlex Node Installation Guides](#)』を参照してください。

次のホスト要件を満たしていることを確認してください。

- クラスタのすべてのサーバ（ノードまたはホスト）に同じ VLAN ID を使用していること。
- ストレージクラスタ全体ですべての ESXi サーバに同じ管理者用ログインクレデンシャルを使用していること。
- SSH をすべての ESXi ホストで有効にしていること。
- すべてのサーバに DNS と NTP を設定していること。
- VMware vSphere をインストールおよび設定していること。
- コンバージドノードまたはコンピューティング専用ノードに対して 1 つの VIC のみ使用していること。追加の VIC または PCIe NIC はサポートされていません。

ディスクの要件

ディスクの要件は、コンバージドノードとコンピューティング専用ノード間で異なります。使用可能な CPU およびメモリ容量を拡大するには、必要に応じてコンピューティング専用ノードを使用して既存のクラスタを拡張します。これらのコンピューティング専用ノードを使用すると、ストレージのパフォーマンスを向上させたり、ストレージ容量を拡大したりすることができます。

あるいはコンバージドノードを追加することで、CPU およびメモリリソースを拡大するとともに、ストレージのパフォーマンスを向上させ、ストレージ容量を拡大できます。

ソリッドステートディスク (SSD) のみが搭載されたサーバは、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) の両方が搭載されたサーバは、ハイブリッドサーバです。

以下は、HyperFlex クラスタ内のすべてのディスクに適用されます。

- ストレージクラスタ内のすべてのディスクには、同量のストレージ容量が必要です。ストレージクラスタ内のすべてのノードには、同数のディスクが必要です。
- すべての SSD は TRIM をサポートする必要があるため、TRIM が有効になっている必要があります。
- すべての HDD は、SATA または SAS タイプのいずれかです。ストレージクラスタ内のすべての SAS ディスクは、パススルーモードにする必要があります。
- ディスクパーティションは、SSD および HDD から削除する必要があります。パーティションが設定された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できます。提供されたディスク上の既存のデータはすべて上書きされます。



(注) 新規のファクトリ サーバは適切なディスク パーティションの設定で出荷されます。新規のファクトリ サーバからディスク パーティションを削除しないでください。

- シスコから直接購入され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) が搭載されたサーバでは、キャッシュ ドライブと永続ストレージ (キャパシティ) ドライブの両方が SED に対応している必要があります。これらのサーバは、保管中データの暗号化 (DARE) をサポートします。

コンバージド ノード

次の表に示すディスクに加えて、すべての M4 コンバージド ノードは、ESX がインストールされたミラー設定で 2 枚の 64 GB SD FlexFlash カードを備えています。すべての M5 コンバージド ノードには、ESXi 搭載の M.2 SATA SSD が内蔵されています。



- (注) サーバ上またはストレージ クラスタ全体でストレージ ディスクのタイプや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つのサーバでは、すべて HDD またはすべて SSD とし、ドライブのサイズを統一してください。
 - ハイブリッド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てください。
 - 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てください。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。
 - すべてのノードで同じサイズと同じ数量の SSD を使用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。

次の表に、HX サーバタイプごとの互換性のあるドライブを示します。ドライブは、指示がない限り、サーバの前面スロットに取り付けられます。複数のドライブが示されている場合、それらはオプションです。1つのドライブサイズをサーバあたりのキャパシティとして使用してください。ドライブの最小数と最大数は、コンポーネントごとに記載されています。

HX240 M5 サーバ

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
キャッシュ SSD	1 (背面)	1.6 TB SSD	1.6 TB NVMe 400 GB SSD	1.6 TB SSD	800 GB SSD
永続	6 ~ 23	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD



(注) HX240 M5 LFF サーバのディスク要件については、[LFF コンバージドノードのディスク要件ハードウェアおよびソフトウェアの要件 \(21 ページ\)](#) を参照してください。

HX240 M4 サーバ

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD	120 GB SSD 240 GB SSD
キャッシュ SSD	1	1.6 TB SSD	1.6 TB NVMe 400 GB SSD	1.6 TB SSD	1.6 TB NVMe 800 GB SSD
永続	6 ~ 23	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX220 M5 サーバ

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
キャッシュ SSD	1	480 GB SSD 800 GB SSD	1.6 TB NVMe 400 GB SSD	800 GB SSD	800 GB SSD

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッドSED	オールフラッシュ SED
永続	6 ~ 8	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

HX 220 M4 サーバ

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	120 GB SSD 240 GB SSD			
キャッシュ SSD	1	480 GB SSD	400 GB SSD	800 GB SSD	800 GB SSD
永続	6	1.2 TB HDD 1.8 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

エッジクラスタ用 HX220 M5 サーバ

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッドSED	オールフラッシュ SED
ハウスキーピング SSD	1	240 GB SSD	240 GB SSD	240 GB SSD	240 GB SSD
キャッシュ SSD	1	480 GB SSD 800 GB SSD	1.6 TB NVMe 400 GB SSD	800 GB SSD	800 GB SSD
永続	3 ~ 8	1.2 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

エッジクラスタ用 HX 220 M4 サーバ

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
ハウスキーピング SSD	1	120 GB SSD 240 GB SSD			
キャッシュ SSD	1	480 GB SSD	400 GB SSD	800 GB SSD	800 GB SSD

コンポーネント	数量	ハイブリッド	すべてフラッシュ	ハイブリッド SED	オールフラッシュ SED
永続	3 ~ 6	1.2 TB HDD	960 GB SSD 3.8 TB SSD	1.2 TB HDD	800 GB SSD 960 GB SSD 3.8 TB SSD

LFF コンバージドノードのディスク要件

次の表に、サポートされている HX240 M5 サーバ大型フォームファクタ (LFF) コンバージドノードの構成を示します。

表 2: HX240 M5 サーバ大型フォームファクタ (LFF) の構成

	説明	部品番号	数量
メモリ	16 GB、32 GB、64 GB、または 128 GB の DDR4-2666-MHz	HX MR X16G1RS H HX MR X32G2RS H HX-MR-X64G4RS-H HX-MR-128G8RS-H	最小 128 MB
プロセッサ	プロセッサの選択 : HX 240 M5 でサポートされている Skylake パーツ	可変	2
ドライブコントローラ	Cisco 12Gbps モジュラ SAS HBA	HX-SAS-M5	1
SSD1 (ブート SSD)	240 GB 2.5 インチ Enterprise Value 6G SATA SSD	HX-EV SD240G61X	1
SSD2 (キャッシュ/WL)	3.2TB 2.5 インチ Enterprise Performance 12G SAS SSD (3X)	HX-SD32T123X-EP	
HDD (容量/データ)	6TB 12G SAS 7.2K RPM LFF HDD (4K) または 8TB 12G SAS 7.2K RPM LFF HDD (4K)	HX-HD6T7KL4KN または HX-HD8T7KL4KN	6 ~ 12
ネットワーク	Cisco VIC 1387 デュアルポート 40 GB QSFP CNA MLOM	HX MLOM C40Q 03	1
ブートデバイス	240 GB SATA M.2	HX-M2 ~ 240 GB	1
ソフトウェア	Cisco HX Data Platform 1、2、3、4 または 5 年ソフトウェアサブスクリプション	HXDP-001-xYR	1

	説明	部品番号	数量
オプションの VMware ライセンス	出荷時にインストール済み： VMware vSphere6 Enterprise Plus/ 標準ソフトウェアライセンスお よびサブスクリプション		2
FI のサポート	2G FI および 3G FI		

ハードウェアおよびソフトウェアの要件

ハードウェア

- 構成可能なメモリ
- 構成可能な CPU
- HDD ストレージ数量

ソフトウェア

- ストレージコントローラ
 - 72 GB RAM を予約
 - 8 vCPU、10.800 GHz CPU を予約
- VAAI VIB
- IO Visor VIB

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対しサポートされているコンピューティング専用ノードの設定を示します。コンピューティング専用ノードのストレージは、ストレージクラスタのキャッシュまたは容量に含まれていません。



- (注) HyperFlex クラスタ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。サーバ関連のポリシーについては、『*Cisco UCS Manager Server Management Guide*』を参照してください。

サポートされ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"> • Cisco B200 M3/M4/M5 • B260 M4 • B420 M4 • B460 M4 • C240 M3/M4/M5 • C220 M3/M4/M5 • C460 M4 • C480 M5 • B480 M5 	<p>方法を選択します。</p> <p>重要 ESXi インストールの際は、ブートメディアの形式が1つだけサーバに通知されるようにしてください。ローカルまたはリモートのディスクの追加は、インストール後に実行できます。</p> <p>USB ブートは HX コンピューティング専用のノードに対してサポートされていません。</p> <ul style="list-style-type: none"> • ESXi がインストールされているミラー設定での SD カード。 • ローカルドライブの HDD または SSD。 • SAN ブート。 • M.2 SATA SSD ドライブ。

ブラウザの推奨事項

リストされている HyperFlex コンポーネントを実行するには、次のいずれかのブラウザを使用します。これらのブラウザはテストおよび承認済みです。他のブラウザでも動作する可能性はありますが、すべての機能をテストし、確認しているわけではありません。

表 3: 対応ブラウザ

ブラウザ	Cisco UCS Manager	HX Data Platform インストーラ	HX Connect
Microsoft Internet Explorer	9 以上	サポート対象外	11 以上
Google Chrome	14 以上	52 以上	54 以上
Mozilla Firefox	7 以上	54 以上	52 以上

注

- **Cisco HyperFlex Connect**
推奨される最小解像度は 1024 x 768 です。
- **Cisco HX Data Platform Plug-in**

Cisco HX Data Platform Plug-inは、vSphere で実行されます。VMware Host Client システムのブラウザ要件については、<https://www.vmware.com/support/pubs/>にある VMware のマニュアルを参照してください。

• Cisco UCS Manager

ブラウザで次のものがサポートされている必要があります。

- Java Runtime Environment 1.6 以降。
- 一部の機能には、Adobe Flash Player 10 以降が必要です。

Cisco UCS Manager に関するブラウザの最新情報については、最新の『[Cisco UCS Manager スタートアップ ガイド](#)』を参照してください。

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、標準的なポート要件の他に、VMware では VMware ESXi と VMware vCenter 用のポートが推奨されています。

- CIP-M はクラスタ管理 IP 用です。
- 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。

次のファイアウォール ポートが開いていることを確認します。

タイム サーバ

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
123	NTP/UDP	各 ESXi ノード 各 SVCM ノード UCSM HX Data Platform インストーラ	タイム サーバ	双方向

HX Data Platform インストーラ

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
22	SSH/TCP	HX Data Platform インストーラ	各 ESXi ノード	管理アドレス
			各 SVCМ ノード	管理アドレス
			CIP-M	クラスタ管理
			UCSM	UCSM管理アドレス
80	HTTP/TCP	HX Data Platform インストーラ	各 ESXi ノード	管理アドレス
			各 SVCМ ノード	管理アドレス
			CIP-M	クラスタ管理
			UCSM	UCSM管理アドレス
443	HTTPS/TCP	HX Data Platform インストーラ	各 ESXi ノード	管理アドレス
			各 SVCМ ノード	管理アドレス
			CIP-M	クラスタ管理
			UCSM	UCSM管理アドレス
8089	vSphere SDK/TCP	HX Data Platform インストーラ	各 ESXi ノード	管理アドレス
902	Heartbeat/UDP/TCP	HX Data Platform インストーラ	vCenter	
7444	ICMP	HX Data Platform インストーラ	ESXi IPs CVM IPs	管理アドレス
9333	UDP/TCP	HX Data Platform インストーラ	CIP-M	クラスタ管理

メールサーバ

クラスタ イベントへの電子メール サブスクリプションではオプションです。

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
25	SMTP/TCP	各 SVCN ノード CIP-M UCSM	メールサーバ	任意

モニタリング

UCS インフラストラクチャをモニタリングするためのオプション。

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
161	SNMP Poll/UDP	モニタリングサーバ	UCSM	任意
162	SNMP トラップ/UDP	UCSM	モニタリングサーバ	任意

DNS サーバ

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
53 (外部ルックアップ)	DNS/TCP/UDP	各 ESXi ノード	DNS	管理アドレス
		各 SVCN ノード	DNS	管理アドレス
		CIP-M	DNS	クラスタ管理
		UCSM	DNS	

vCenter

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
80	HTTP/TCP	vCenter	各 SCVM ノード CIP-M	双方向
443	HTTPS (プラグイン)/TCP	vCenter	各 ESXi ノード 各 SVCN ノード CIP-M	双方向

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
7444	HTTPS (VC SSO)/TCP	vCenter	各 ESXi ノード 各 SVCM ノード CIP-M	双方向
9443	HTTPS (プラグイン)/TCP	vCenter	各 ESXi ノード 各 SVCM ノード CIP-M	双方向
5989	CIM サーバ/TCP	vCenter	各 ESXi ノード	
902	Heartbeat/TCP/UDP	vCenter	HX Data Platform インストーラ ESXi サーバ	このポートは、各ホストからアクセス可能である必要があります。このポートが HX インストーラから ESXi ホストに開かれていない場合、インストールはエラーになります。

ユーザ

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
22	SSH/TCP	ユーザ	各 ESXi ノード	管理アドレス
			各 SVCM ノード	管理アドレス
			CIP-M	クラスタ管理
			HX Data Platform インストーラ	
			UCSM	UCSM 管理アドレス
			vCenter	
			SSO Server	

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
80	HTTP/TCP	ユーザ	各 SVCN ノード	管理アドレス
			CIP-M	クラスタ管理
			UCSM	
			HX Data Platform インストーラ	
			vCenter	
443	HTTPS/TCP	ユーザ	各 SVCN ノード	
			CIP-M	
			UCSM	UCSM管理アドレス
			HX Data Platform インストーラ	
			vCenter	
7444	HTTPS (SSO)/TCP	ユーザ	vCenter SSO Server	
9443	HTTPS (プラグイン)/TCP	ユーザ	vCenter	
2068	virtual keyboard/ビデオ/マウス (vKVM)/TCP	ユーザ	UCSM	UCSM管理アドレス

SSO Server

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
7444	HTTPS (SSO)/TCP	SSO Server	各 ESXi ノード 各 SCVM ノード CIP-M	双方向

ストレッチ ウィットネス

HyperFlex ストレッチ クラスタを展開する場合にのみ必要です。

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
2181 2888 3888	ウィットネス ノード/TCP	ウィットネス	各 CVM ノード	双方向, 管理アドレス
8180	ウィットネス ノード/TCP	ウィットネス	各 CVM ノード	双方向, 管理アドレス
80	HTTP/TCP	ウィットネス	各 CVM ノード	潜在的な将来の必要条件
443	HTTPS/TCP	ウィットネス	各 CVM ノード	潜在的な将来の必要条件

Replication

ネイティブ HX 非同期クラスタからクラスタへの複製を構成する場合にのみ必要です。

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
9338	データ サービス マネージャ ピア/TCP	各 CVM ノード	各 CVM ノード	双方向, クラスタ 管理 IP アドレス を含める
9339	データ サービス マネージャ/TCP	各 CVM ノード	各 CVM ノード	双方向, クラスタ 管理 IP アドレス を含める
3049	CVM/TCP の複製	各 CVM ノード	各 CVM ノード	双方向, クラスタ 管理 IP アドレス を含める
4049	クラスタ マッ プ/TCP	各 CVM ノード	各 CVM ノード	双方向, クラスタ 管理 IP アドレス を含める
4059	NR NFS/TCP	各 CVM ノード	各 CVM ノード	双方向, クラスタ 管理 IP アドレス を含める
9098	複製サービス	各 CVM ノード	各 CVM ノード	双方向, クラスタ 管理 IP アドレス を含める

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
8889	コーディネーション用 NR マスター/TCP	各 CVM ノード	各 CVM ノード	双方向, クラスタ管理 IP アドレスを含める
9350	ハイパーバイザサービス/TCP	各 CVM ノード	各 CVM ノード	双方向, クラスタ管理 IP アドレスを含める
443	HTTPS/TCP	各 CVM ノード	各 CVM ノード	双方向, クラスタ管理 IP アドレスを含める

SED クラスタ

ポート番号	サービス/プロトコル	ソース	ポート宛先	基本情報
443	HTTPS	各 SCVM 管理 IP (クラスタ管理 IP を含む)	UCSM (ファブリック A、ファブリック B、VIP)	ポリシーの設定
5696	TLS	CIMC	KVM サーバ	Key Exchange



ヒント 標準構成がなく、別の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)	すべてのデバイスコネクタは svc.ucs-connect.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 接続が許可されている必要があります。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。
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。

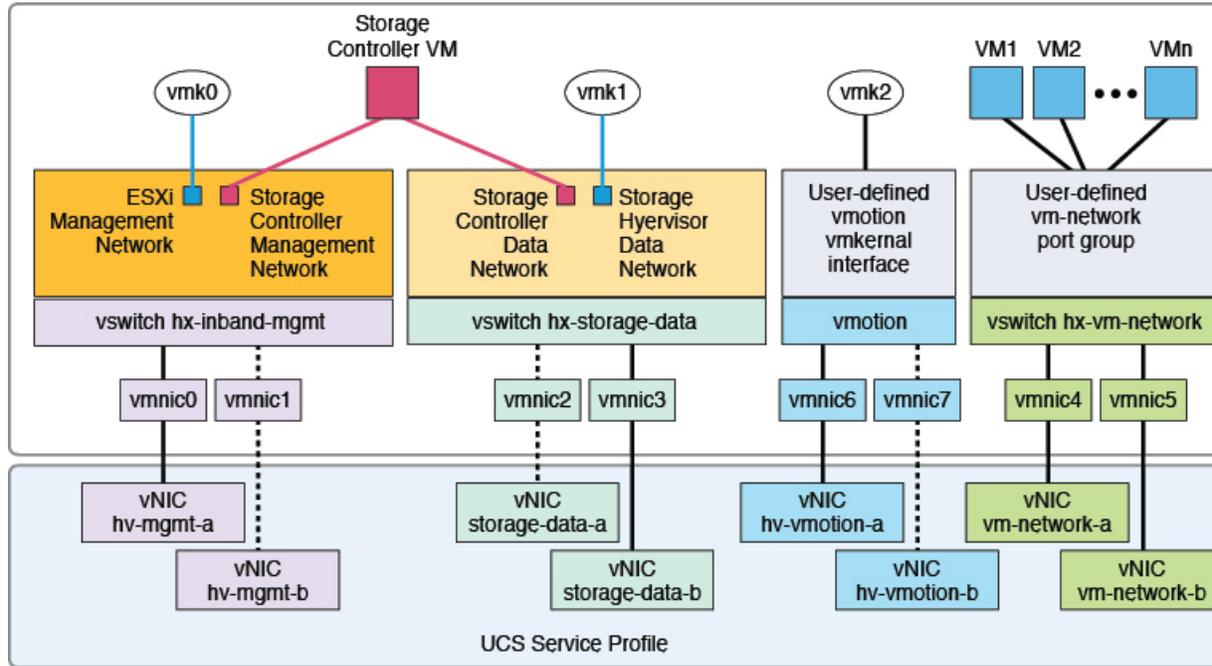
外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
インストール後のスクリプト	インストール後のタスクを完了するために、インストーラ VM にインストール後スクリプトを実行できます。スクリプトは、すべてのネットワークインターフェイス（管理、vMotion、およびストレージネットワーク）に ping を実行して、ファブリックが完全に利用できることを確認します。また、ノースバウンドスイッチで VLAN のタグging が正しいことと、ジャンボフレーム設定を検証します。	HTTP ポート番号 : 80	インストール後のスクリプトでは、ポート 80 (HTTP) 経由での http://cs.co/hx-scripts への名前解決が必要です。

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

HyperFlex クラスタを設定する前に、ネットワーク トラフィック管理を最適化するアップストリーム帯域幅容量を計画してください。これにより、コンポーネントで障害が発生したり、ネットワークが部分的に停止したりした場合でも、トラフィックフローを安定した状態に維持できます。

デフォルトでは、「`hx-vm-network`」 vSwitch は `[active/active]` に設定されています。これ以外のすべての vSwitch は、`[active/standby]` に設定されています。

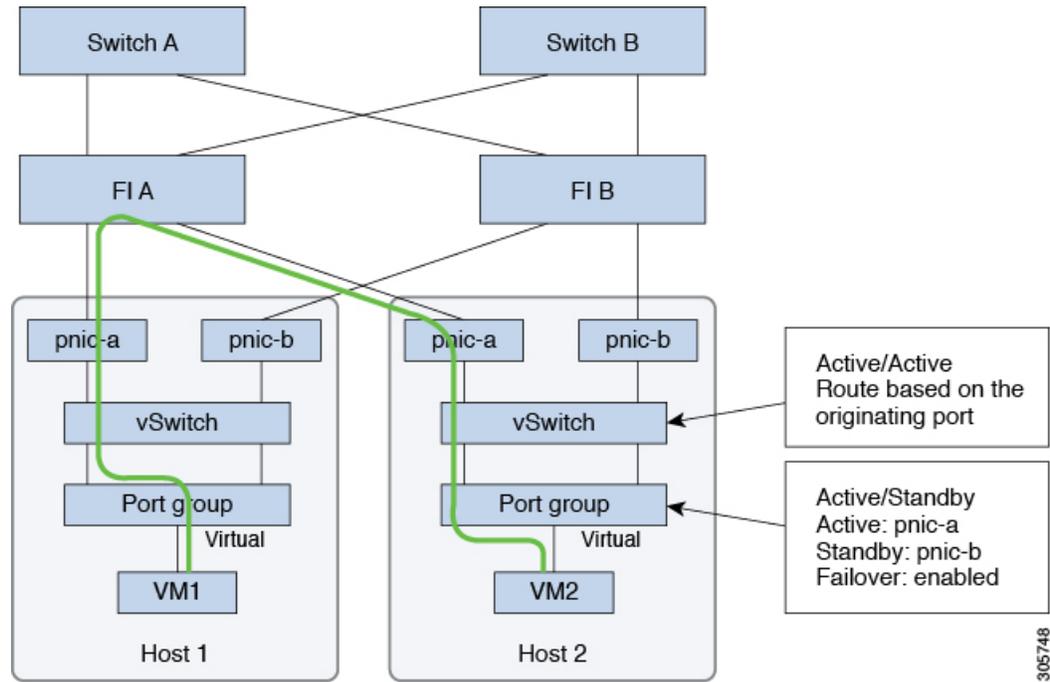
図 6: 単一ホストの HyperFlex Data Platform 接続



- 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.

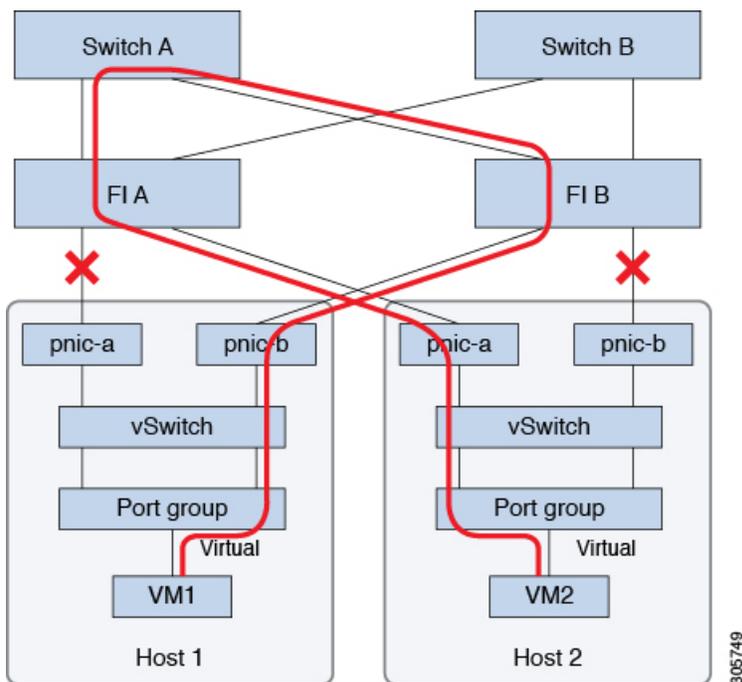
デフォルトの vSwitch NIC チューミング ポリシーとフェールオーバー ポリシーを [yes] に設定します。これにより、管理トラフィック、vMotion トラフィック、およびストレージトラフィックのすべてが、ローカルでファブリック インターコネク트에転送されるようになり、フローを安定した状態に維持できます。vNIC-a で障害が発生すると、ESXi がロード バランシングを計算し、すべての仮想ポートを vNIC-b に再ピンングします。vNIC-a がオンライン状態に戻った時点で、再びピンングが適用され、vNIC-a と vNIC-b の間で仮想ポートが元のように均等に分配されます。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

図 8: リンク障害中のトラフィック フロー



- (注) 1つのファブリックインターコネクタから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 6200 Series Fabric Interconnects—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

ベスト プラクティス

- ネットワークごとにそれぞれ個別のサブネットとVLANを使用します。
- 10 Gbps のケーブルを使用して、各ホストを直接 Cisco UCS ファブリック インターコネクタに接続します。
- 特に Disjoint Layer 2 設定が使用されている場合は、ネットワークの問題を引き起こす可能性があるため、デフォルト VLAN である VLAN 1 は使用しないでください。
- インストーラは、デフォルトで 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てください。

各 ESXi ホストには、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) の管理、およびストレージクラスタの管理を処理します。
- **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、それぞれ異なるネットワークを伝送します。

- **vswitch-hx-inband-mgmt** : ESXi 管理および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、および HX Data Platform の複製に使用されます。

これら 2 つの vSwitch は、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するための静的 IP アドレスが割り当てられます。

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

この vSwitch には管理用に 1 つのポート グループがあり、vCenter クラスタ内のすべてのホストに接続する vSphere を介して定義されます。

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

VLAN を、Cisco UCS Manager の対応する vNIC テンプレートに追加または削除できます。手順の詳細については、「[Managing VLANs in Cisco UCS Manager](#)」および「[Managing vNIC templates in Cisco UCS Manager](#)」を参照してください。vSwitch 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. Cisco HX Data Platform インストーラは、自動的に vSwitch を作成します。
 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 および vSwitch の要件

少なくとも3つの VLAN ID を提供します。すべての VLAN がインストール時にファブリック インターコネクタに設定されている必要があります。

VLAN タイプ	説明
(注)	次の各ネットワークにそれぞれ個別のサブネットと VLAN を使用します。
VLAN ESXi および HyperFlex 管理トラフィック	VLAN 名 : hx-inband-mgmt VLAN ID
VLAN HyperFlex ストレージトラフィック	VLAN 名 : hx-storage-data VLAN ID
VLAN VM vMotion	VLAN 名 : hx-vmotion VLAN ID
VLAN VM データ	ユーザ定義
IP ブロック	KVM IP プール ホストごとに1つの IP アドレス。
サブネット マスク	例 : 255.255.0.0
デフォルト ゲートウェイ	例 : 10.193.0.1

外部スイッチ VLAN タギング (EST) を使用する VLAN タギングと vSwitch の設定は、UCS Manager プロファイルを使用して適用されます。HX Data Platform インストーラにより、このプロセスが簡単になります。



- (注)
- 特に Disjoint Layer 2 設定が使用されている場合は、ネットワークの問題を引き起こす可能性があるため、デフォルト VLAN である VLAN 1 は使用しないでください。VLAN 1 ではない別の VLAN を使用してください。

インストーラは、デフォルトで VLAN を非ネイティブとして設定します。非ネイティブの 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。

Cisco UCS の要件

プロンプトが表示されたら、UCS ファブリック インターコネクタおよび UCS Manager に関してリストされているコンテンツを提示します。

Cisco UCS ファブリック インターコネクトの要件

UI 要素	基本情報
[Uplink Switch Model]	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)。
[Fabric Interconnect Cluster IP address]	<IPアドレス>
[FI-A IP Address]	<IPアドレス>
[FI-B IP Address]	<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 Blocks]	KVM IP プール。少なくとも 4 つの IP アドレス。
[Subnet mask]	たとえば、255.255.0.0 と指定します。
[Default Gateway]	たとえば、10.193.0.1 と指定します。

Cisco UCS Manager の要件

UI 要素	基本情報
[UCS Manager Host Name]	ホスト名または IP アドレス
[User Name]	<admin ユーザ名>
[Password]	<admin ユーザ名>

ハイパーバイザ要件

vCenter 経由で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 サーバに使用可能なアドレス範囲から IP アドレスを入力します。すべてのネットワーク アドレスに静的 IP アドレスを提供します。



- (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。
 - IPアドレスは、ストレージクラスタの作成後は変更できません。Cisco TACに連絡して、サポートを受けてください。
 - 単独では必要ありませんが、DNS 名を指定する場合は、IP アドレスの正逆方向の DNS ルックアップを有効にします。
 - インストーラの IP アドレスは、ハイパーバイザとストレージコントローラ VM で使用される管理サブネットから到達できる必要があります。インストーラ アプライアンスは、ESXi ホスト上か、またはインストールされるクラスタの一部ではない VMware ワークステーション上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_ID	VLAN タグ	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。ストレージクラスタ内のすべてのサーバにおいて、データがディスク全体に配布され、コントローラ リソースの活用と高可用性を実現します。

ストレージクラスタは、関連する vCenter クラスタには依存しません。vCenter クラスタ内にある 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
[Name]	ストレージクラスタの名前を入力します。
[Management IP Address]	<p>これによって、各 ESXi ホストにストレージ管理ネットワークへのアクセスが提供されます。</p> <ul style="list-style-type: none"> • 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ある必要があります。 • クラスタ管理 IP が同じサブネット上の別のクラスタと最後のオクテットを共有することを許可しないでください。 • これらの IP アドレスは、4 つの IP アドレスに加えて、シスコが [Hypervisor] セクションで各ノードに割り当てます。
[Storage Cluster Data IP Address]	<p>これによって、各 ESXi ホストにストレージデータネットワークおよび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提供されます。</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
[Data Replication Factor]	<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 のインストール時に設定され、その後は変更できません。</p> <p>[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"> • [Data Replication Factor] 3 : データの冗長複製を 3 つ保持します。この場合、ストレージリソースの消費量は多くなりますが、ノード障害やディスク障害が同時に発生した場合にデータを最大限に保護します。 <p>注目 これは推奨オプションです。</p> <ul style="list-style-type: none"> • [Data Replication Factor] 2 : 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はなりますが、ノード障害やディスク障害が同時に発生した場合にデータ保護が低下します。 <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、クラスタの動作能力に影響が生じます。複数のノードで障害が発生した場合や 1 つのノードと別のノードのディスクで障害が発生した場合は、同時障害と呼ばれます。</p>

vCenter 設定の要件

vCenter に管理者レベル アカウントとパスワードを指定します。既存の vCenter サーバがあ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) (フェールオーバー キャパシティを定義し、データストア ハートビートを拡張するために必要) を有効にします。

- 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 ReadyClone を使用するために必要）。

フィールド	説明
[vCenter Server]	現在の vCenter サーバの Web アドレスを入力します。 たとえば、http://<IP アドレス> とします。
[User Name]	<admin ユーザ名> を入力します。
[Password]	<admin パスワード> を入力します。
[Datacenter Name]	vCenter データセンターに必要な名前を入力します。
[Cluster Name]	vCenter クラスタに必要な名前を入力します。 クラスタには、少なくとも 3 つの ESXi サーバが含まれている必要があります。

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やサービスが動作していることを確認します。

- DNS サーバ



(注) DNS サーバは、HX ストレージクラスタの外部に存在する必要があります。

- NTP サーバ



- (注)
- NTP サーバは、HX ストレージ クラスタの外部に存在する必要があります。
 - ストレージ クラスタを設定する前に、NTP サーバが動作していて、信頼できる時間のソースを提供していることを手動で確認します。
 - コンバージド ノード、コンピューティング ノード双方のすべてのノード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 サーバは安定していて、(クラスタの有効期間に対し) 継続性があり、静的 IP アドレスから到達できる必要があります。

• Time Zone

フィールド	基本情報
[DNS Server(s)]	<p><IP アドレス></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 サーバアドレスが必要になります。</p> <p>(注)</p> <ul style="list-style-type: none"> • DNS サーバがない場合は、HX Data Platform インストーラの [Cluster Configuration] ページの [System Services] に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。 • 複数の DNS サーバアドレスを入力するには、アドレスをカンマで区切ります。DNS サーバのアドレスが正しく入力されていることを慎重に確認します。

フィールド	基本情報
[NTP Server(s)] (信頼できる NTP サーバが必要です)	<p><IP アドレス></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"> • ストレージコントローラ VM • ESXi ホスト • vCenter サーバ <p>重要 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 サーバ間でクロック同期を確保するために必要です。</p> <p>インストール時に、この情報は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搬されます。サーバは、ストレージクラスタの起動時に自動的に同期されます。</p>
[Time Zone]	<p><利用するタイムゾーン></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。スケジュールされたスナップショットをいつ取得するかを決定するために使用されます。</p> <p>(注) すべての VM が同じタイムゾーンにある必要があります。</p>

コントローラ VM 用 CPU リソース予約

ストレージコントローラ VM から HyperFlex Data Platform に重要な機能が提供されるため、HX Data Platform インストーラはコントローラ VM 用に 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 では最低限必要な CPU リソースが確保されます。これは、ESXi ハイパーバイザホストの物理 CPU リソースがゲスト VM によって大量に消費されるような状況で役立ちます。次の表に、ストレージコントローラ VM 用 CPU リソース予約の詳細を示します。

VM CPU の数	共有	予約	制限
8	Low	10,800 MHz	制限なし

コントローラ仮想マシン用メモリ リソース予約

以下の表に、ストレージコントローラ VM 用メモリ 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	全ゲストメモリに対する予約
HX220c-M4/M5s HXAF220C-M4/M5s	48 GB	○
HX240c-M4/M5SX HXAF240C-M4/M5SX	72 GB	○
HX240C-M5L	78 GB	○

- B200 コンピューティング専用ブレードは軽量ストレージコントローラ VM を備えており、この VM は 1 つの vCPU と 512 MB のメモリ予約でのみ設定されています。
- C240 ラックサーバは、2 ラックユニット（2 RU）フォームファクタで卓越した拡張性とパフォーマンスを発揮します。
- C220 サーバは、1 ラックユニット（1 RU）フォームファクタで拡張性を実現します。

自動サポート要件

自動サポート（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。自動サポートを有効にすると、HX Data Platform から、通知の受信先として指定された電子メールアドレスまたは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	
[Enable Auto Support] チェックボックス	このボックスは、HX ストレージクラスタの作成時にオンにします。
メールサーバ	<IP アドレス> 自動サポートを有効にするには、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> 自動サポート通知の送信に使用する電子メールアドレス。
ASUP 受信者	自動サポート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) 自動サポートを有効にすることを強くお勧めします。それにより、ノードのドライブ障害など、将来のハードウェアの問題を診断するのに役立つハードウェアカウンタ履歴が提供されます。

シングルサインオンの要件

SSO URL は、vCenter から提供されます。この URL にコントローラ VM から直接到達できない場合は、[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 URL	SSO URL は、vCenter の [vCenter Server] > [Manage] > [Advanced Settings] にある <code>config.vpxd.sso.sts.uri</code> キーで確認できます。



第 4 章

Cisco HyperFlex Systems サーバのインストール

この章では、HyperFlex クラスタをセットアップするために物理コンポーネントをインストールする方法について説明します。

- [Cisco HyperFlex ノードの設置 \(47 ページ\)](#)
- [ファブリック インターコネクトの設定 \(48 ページ\)](#)
- [Cisco UCS ファブリック インターコネクトへの HX シリーズ サーバの接続 \(58 ページ\)](#)
- [概要 \(58 ページ\)](#)

Cisco HyperFlex ノードの設置

HyperFlex クラスタとノードの制限の詳細については、[Cisco HX データ プラットフォームのリリース ノート](#)の最新バージョンで、[Cisco HX データ プラットフォーム ストレージ クラスタ仕様](#)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、次の表からそれぞれのリンクを参照してください。

インストール先のノードのタイプ	参照先
コンバージドノード	
HyperFlex HX220c M4/M5 ノード	Cisco HyperFlex HX220c M4/M5 ノードインストールガイド
HyperFlex HX240c M4/M5 ノード	Cisco HyperFlex HX240c M4/M5 ノードインストールガイド
コンピューティング専用ノード	
Cisco UCS B200 M3/M4/M5 ノード	Cisco UCS B200 M3/M4/M5 ブレードサーバ設置/サービスノート

インストール先のノードのタイプ	参照先
Cisco UCS B260 M4 ノード、B460 M4 ノード	E7 v4 CPU 搭載サーバ向け Cisco UCS B260 M4 および B460 M4 ブレード サーバ設置および サービス ノート E7 v3、E7 v2 の CPU 搭載サーバ向け Cisco UCS B260 M4、B460 M4 ブレード サーバ設置および サービス ノート
Cisco UCS B420 M4 ノード	Cisco UCS B420 M4 ブレード サーバ設置および サービス ノート
Cisco UCS B480 M5 ノード	Cisco UCS B480 M5 ブレード サーバ設置および サービス ノート
Cisco UCS C240 M3/M4/M5 ラック ノード	Cisco UCS C240 M3/M4/M5 サーバ インストールおよび サービス ガイド
Cisco UCS C220 M3/M4/M5 ラック ノード	Cisco UCS C220 M3/M4/M5 サーバ インストールおよび サービス ガイド
Cisco UCS C480 M5 ノード	Cisco UCS C480 M5 サーバ インストールおよび サービス ガイド
Cisco UCS C460 M4 ノード	Cisco UCS 460 M4 サーバ設置および サービス ガイド

ファブリック インターコネクタの設定

高度な可用性をもたらすため、次のようにファブリック インターコネクタ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 インターコネクタに接続します。
2. ファブリック インターコネクタ A 上のポート L1 をファブリック インターコネクタ B 上のポート L1 に接続し、ファブリック インターコネクタ A 上のポート L2 をファブリック インターコネクタ 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 インターコネクタは、互いのステータスを継続的にモニタします。

ファブリック インターコネクタを接続する前に、次の情報を確認して入手してください。

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の確認。	<ul style="list-style-type: none"> 第1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必要があります。 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必要があります。 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必要があります。 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必要があります。
コンピュータ端末でのコンソールポートパラメータの確認。	<ul style="list-style-type: none"> 9600 ボー 8 データ ビット パリティなし 1 ストップ ビット
初期設定の情報の取得。	<p>初期設定に関する次の情報を収集します。</p> <ul style="list-style-type: none"> システム名 admin アカウントのパスワード 3つの静的 IP アドレス 3つの静的 IP アドレスのサブネット マスク デフォルト ゲートウェイの IP アドレス DNS サーバの IP アドレス。 システムのドメイン名

両方のファブリック インターコネクタで、同じセットアッププロセスを実施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、クラスタ設定を有効にします。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設定すると、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。

GUIによるプライマリ ファブリック インターコネクタの設定

プライマリ ファブリック インターコネクタを設定するための下記の手順に従うか、「[Cisco UCS Manager Initial Setup part 1](#)」をご覧ください。

- ステップ 1** ファブリック インターコネクトの電源を入れます。
ファブリック インターコネクトが起動すると、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 2** システムがリリースを取得したら、手順 6 に進みます。それ以外の場合は次の手順に進みます。
- ステップ 3** コンソール ポートに接続します。
- ステップ 4** 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 5** 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 インターコネクトの管理ポートの IPv4 アドレスまたは IPv6 アドレス。
 - ファブリック インターコネクトの管理ポートの IPv4 サブネット マスクまたは IPv6 プレフィックス。
 - ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IPv4 または IPv6 アドレス。
- (注) クラスタ設定では、設定時に両方のファブリック インターコネクト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 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 GUI 起動ページに移動します。
- ステップ 7** Cisco UCS Manager GUI 起動ページで [Express Setup] を選択します。
- ステップ 8** [Express Setup] ページで [Initial Setup] を選択し、[Submit] をクリックします。
- ステップ 9** [Cluster and Fabric Setup] 領域で、以下の操作を行います。
- a) [Enable Clustering] オプションをクリックします。
 - b) [Fabric Setup] オプションに対して [Fabric A] を選択します。
 - c) [Cluster IP Address] フィールドに、Cisco UCS Manager で使用する IPv4 アドレスまたは IPv6 アドレスを入力します。
- ステップ 10** [System Setup] 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
[System Name]	Cisco UCS ドメインに割り当てる名前。 スタンドアロン設定では、システム名に「-A」が追加されます。クラスタ設定では、ファブリック A に割り当てられたファブリック インターコネクトに「-A」が、ファブリック B に割り当てられたファブリック インターコネクトに「-B」が追加されます。

フィールド	説明
[Admin Password]	ファブリック インターコネクタ上の Admin 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]	ファブリック インターコネクタ上の Admin アカウントに使用されるパスワード。
[Mgmt IP Address]	ファブリック インターコネクタの管理ポートのスタティック IPv4 または IPv6 アドレス。
[Mgmt IP Netmask] または [Mgmt IP Prefix]	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 マスクまたは IPv6 プレフィクス。 (注) [Mgmt IP Address] に入力したアドレス タイプに基づいて、[Mgmt IP Netmask] または [Mgmt IP Prefix] の入力が必要になります。
[Default Gateway]	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 IPv4 または IPv6 アドレス。 (注) [Mgmt IP Address] フィールドに入力したアドレス タイプに基づいて、システムから [Default Gateway] アドレス タイプへの入力が必要になります。
[DNS Server IP]	ファブリック インターコネクタに割り当てられる DNS サーバの IPv4 または IPv6 アドレス。
[Domain Name]	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 11 [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。

GUIによる従属ファブリック インターコネクタの設定

従属ファブリック インターコネクタを設定するための下記の手順に従うか、「[Cisco UCS Manager Initial Setup part 2](#)」をご覧ください。



(注) 既存の高可用性クラスタに新しいファブリック インターコネクタを追加するとき（新規インストールやファブリック インターコネクタの交換時など）、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** 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 2** システムがリリースを取得したら、手順 6 に進みます。それ以外の場合は次の手順に進みます。
- ステップ 3** コンソール ポートに接続します。
- ステップ 4** 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 5** 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 アドレスまたは IPv6 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 マスクまたは IPv6 プレフィックス
 - 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 アドレスまたは IPv6 アドレス
- (注) クラスタ設定では、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 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 GUI 起動ページに移動します。
- ステップ 7** Cisco UCS Manager GUI 起動ページで [Express Setup] を選択します。
- ステップ 8** [Express Setup] ページで [Initial Setup] を選択し、[Submit] 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] 領域で、以下の操作を行います。
- a) [Enable Clustering] オプションを選択します。
 - b) [Fabric Setup] オプションに対して [Fabric B] が選択されていることを確認します。
- ステップ 10** [System Setup] 領域の [Admin Password of Master] フィールドに Admin アカウントのパスワードを入力します。
[Manager Initial Setup] 領域が表示されます。
- ステップ 11** [Manager Initial Setup] 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 または IPv6 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
[Peer FI is IPv4 Cluster enabled. Please Provide Local fabric interconnect Mgmt0 IPv4 Address]	ローカル ファブリック インターコネクトの Mgmt0 インターフェイスの IPv4 アドレスを入力します。
[Peer FI is IPv6 Cluster Enabled. Please Provide Local fabric interconnect Mgmt0 IPv6 Address]	ローカル ファブリック インターコネクトの Mgmt0 インターフェイスの IPv6 を入力します。

- ステップ 12 [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によるプライマリ ファブリック インターコネクトの設定

- 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 インターコネクトの電源を入れます。
 ファブリック インターコネクトが起動すると、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 **admin** 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、**admin** 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 インターコネクト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 インターコネクトの管理ポートの IPv4 または IPv6 アドレスを入力します。
 IPv4 アドレスを入力する場合は、IPv4 サブネットマスクを入力するように求められます。IPv6 アドレスを入力する場合は、IPv6 ネットワーク プレフィックスを入力するように求められます。
- ステップ 12 各 IPv4 サブネットマスク、または IPv6 ネットワーク プレフィックスを入力し、**Enter** キーを押します。
 ファブリック インターコネクト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 または IPv6 アドレスを求められます。
- ステップ 13 次のいずれかを入力します。
- デフォルト ゲートウェイの IPv4 アドレス
 - デフォルト ゲートウェイの IPv6 アドレス
- 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 または IPv6 アドレスを入力します。
アドレスタイプはファブリック インターコネクト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かっこ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設定の最初のファブリック 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
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

```

次に、コンソールおよび IPv6 管理アドレスを使用してクラスタ設定の最初のファブリック 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
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%652

```

```

Confirm the password for "admin": adminpassword%652
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 address: 2001::107
Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
DNS IP address: 2001::101
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
Enforced Strong Password=no
Physical Switch Mgmt0 IPv6 Address=2001::107
Physical Switch Mgmt0 IPv6 Prefix=64
Default Gateway=2001::1
Ipv6 value=1
DNS Server=2001::101
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes

```

CLIによる従属ファブリック インターコネクタの設定

ここでは、管理ポートに対し IPv4 または IPv6 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手順について説明します。



- (注) 既存の高可用性クラスタに新しいファブリック インターコネクタを追加するとき（新規インストールやファブリック インターコネクタの交換時など）、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 インターコネクタによって、クラスタ内のピアファブリック インターコネクタが検出されます。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 インターコネクタ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 インターコネクタをクラスタに追加します。

ステップ 5 ピアファブリック インターコネクタ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 インターコネクタ上の管理ポートの 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かっこ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 インターコネクタ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
```

次に、ピアのコンソールおよび IPv6 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 インターコネクタ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 IPv6 Address: 2001::107
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

コンソールセットアップの確認

SSH を介してファブリック インターコネクタにログインすることで、両方のファブリック インターコネクタが完了していることを確認できます。

Cisco UCS Manager CLI を使用してクラスタのステータス確認するには、次のコマンドを使用します。

表 4:

コマンド	目的	出力の例
show cluster state	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 インターコネクタの動作状態およびリーダーシップ ロールを表示します。	次の例の表示では、両方のファブリック インターコネクタが Up 状態、HA が Ready 状態、ファブリック インターコネクタ A がプライマリ ロール、ファブリック インターコネクタ B が従属ロールです。 UCS-A# show cluster state Cluster Id: 0x4432f72a371511de-0xb97c000de1blada4 A: UP, PRIMARY B: UP, SUBORDINATE HA READY
show cluster extended-state	クラスタの状態を詳細に表示します。通常は問題をトラブルシューティングする場合に使用します。	次の例は、クラスタの詳細な状態を表示する方法について示します。 UCSC# show cluster extended-state 0x2e95deadd0f11e2-0x8ff35147e84f3de2Start 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

Cisco UCS ファブリック インターコネクタへの HX シリーズ サーバの接続

概要

Cisco HX220c および HX240c サーバはファブリック インターコネクタに直接接続します。直接接続することで、Cisco UCS Manager は管理トラフィックとデータトラフィックの両方に対し、1つのケーブルを使用して HX シリーズ サーバを管理できます。



- (注) サーバをファブリック インターコネクタに接続した後、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 インターコネクタのサーバポートに接続する必要があります。「要件」の章に記載されているように、HX サーバに推奨されるファームウェアがあることを確認します。推奨ファームウェアがない場合は、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 インターコネクタ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, and 6324 Series Configuration Limits for Cisco UCS Manager](#)」を参照してください。

ファブリック インターコネクタへのコンバージド ノードの接続

このトピックでは、HX クラスタの作成または既存の HX クラスタへの追加のために、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 サーバを出荷時のデフォルト設定に設定します。
- 統合ノード用には、専用 CIMC ポートをネットワークに接続しないでください。そうすると、Cisco UCS Manager でサーバが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。
- 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場合、サーバの直接接続管理を有効にできません。
- ファブリック インターコネクタへのサーバ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、[Cisco HyperFlex ノードの設置 \(47 ページ\)](#) を参照してください。
- ステップ 2** ファブリック インターコネクタのサーバポートを構成します。
- a) サーバ上の一方のポートから 10-Gb SFP+ ケーブルをファブリック インターコネクタ A に接続します。ファブリック インターコネクタ A 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 枚のカードの VIC からファブリック インターコネクタに 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 インターコネクタ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](#)」の項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 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+ タイプを混在使用しないでください。混在させると、「Discovery Failed」エラーが表示されます。
 - 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](#)」の項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、次に接地された AC 電源コンセントに接続します。初期ブート時には、スタンバイ電源でノードが起動するまで約 2 分かかります。

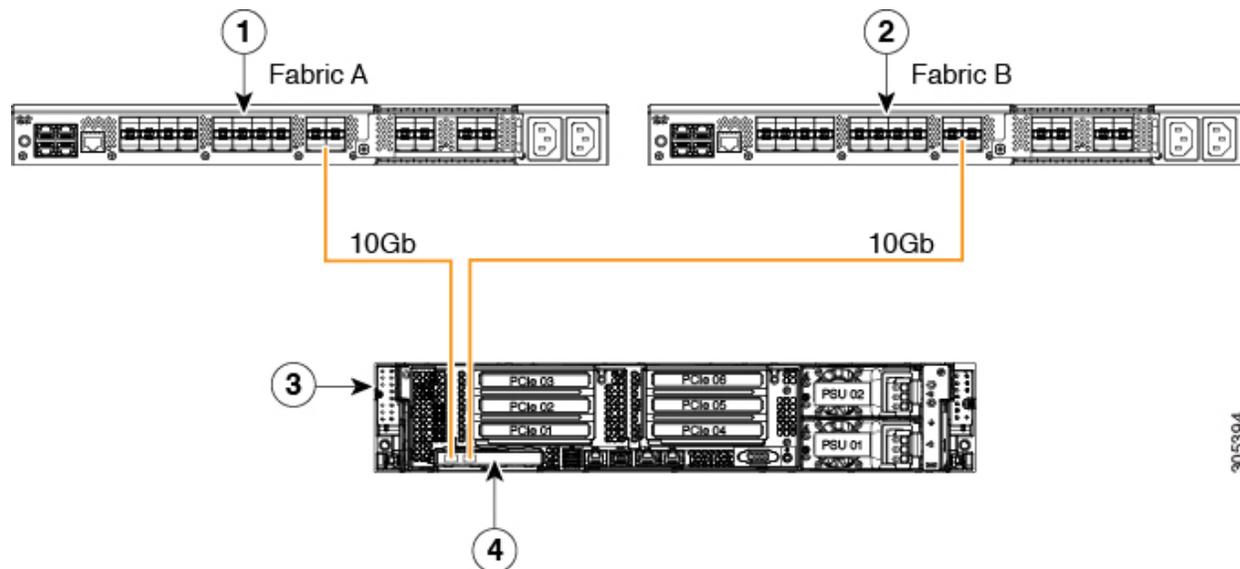
- (注)
1. 電源を入れると、ファブリックインターコネクトによってサーバが検出されます。UCS Manager でノードの検出を監視できます。
 2. 前面パネルのノードの**電源ステータス LED**を調べて、ノードの電源ステータスを確認します。LED がオレンジの場合、ノードはスタンバイ電源モードです。

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

物理的な接続の図

次の図は、直接接続モードでの Cisco UCS Manager と HX シリーズサーバとの統合に関するケーブル配線の設定を示しています。ゴールド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: 直接接続の配線設定



1	Cisco UCS 6248 シリーズ ファブリック インターコネクト (ファブリック A)	3	HX シリーズサーバ
2	Cisco UCS 6248 シリーズ ファブリック インターコネクト (ファブリック B)	4	サポート対象の mLOM スロット内の Cisco UCS VIC 1227

ファブリックインターコネクタへのコンピューティング専用ノードの接続

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および設定後、コンピューティング専用ノードを HyperFlex クラスタに接続します。

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、[Cisco HyperFlex ノードの設置 \(47 ページ\)](#) を参照してください。
3. Cisco HX Data Platform を使用してクラスタ展開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、クラスタ展開ワークフローを使用します。詳細な手順については、[既存のクラスタへのコンピューティング専用ノードの追加 \(137 ページ\)](#) 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 のコンポーネントを設定する方法について説明します。

- vSphere Web クライアントを使用した HX Data Platform インストーラ OVA の展開 (63 ページ)
- Syslog の設定 (68 ページ)
- HyperFlex クラスタの設定 (69 ページ)
- GPU を搭載した HyperFlex ノードの設置 (80 ページ)
- HyperFlex クラスタの作成に関する考慮事項 (81 ページ)

vSphere Web クライアントを使用した 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 アドレスの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。
 - HX Data Platform インストーラを、Cisco HX ストレージクラスタのノードになる ESXi サーバに展開しないでください。

ステップ 1 [Download Software]<https://software.cisco.com/download/home/286305544/type/286305994/release/3.0%25281c%2529?catid=286305510> 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 インストーラをストレージ管理ネットワーク上のノードにダウンロードします。これは HX Data Platform ストレージクラスタに使用されます。

Example:
Cisco-HX-Data-Platform-Installer-v2.5.1d-26363.ova

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

(注) 仮想ハードウェアバージョン 10.0 以上をサポートする仮想化プラットフォームのバージョン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 Client 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。

- a) vSphere、VirtualBox、ワークステーション、または Fusion などの仮想マシンハイパーバイザを開きます。
- b) 以下のように、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—[Inventory list] > [Host] > [File] > [Deploy OVA] を展開
- vSphere Web クライアントを使用する—[vCenter Inventory list] > [Hosts] > [Host] > [Deploy OVA] を展開

ステップ 3 HX Data Platform インストーラが置かれている場所を選択します。デフォルトを受け入れて、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 で使用するための静的 IP アドレスを入力します。

- (注)
- 静的 IP アドレスは、DHCP がネットワークに設定されていても必要です。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。
 - IP アドレスを新しい VM に割り当てるためにハイパーバイザウィザードのデフォルトが DHCP になっている場合は、[静的 IP アドレスによる HX データ プラットフォーム インストーラ OVA の展開 \(66 ページ\)](#) の手順を実行して、静的 IP アドレスを持つ HX Data Platform インストーラ VM をインストールします。DNS はインストーラ VM から到達できる必要があります。

フィールド	説明
[Hostname]	この VM のホスト名。 空白のままにして、IP アドレスの逆引きを試みます。
[Default Gateway]	この VM のデフォルトゲートウェイアドレス。 DHCP が必要な場合は空白のままにしてください。
[DNS]	この VM のドメインネームサーバ (カンマ区切り)。 DHCP が必要な場合は空白のままにしてください。

フィールド	説明
[IP Address]	このインターフェイスの IP アドレスです。 DHCP が必要な場合は空白のままにしてください。
[Netmask]	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 が必要な場合は空白のままにしてください。

ステップ 5 [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確認し、**展開後に電源をオンにします**。

HX Data Platform インストーラを手動で起動するには、仮想マシンのリストに移動し、インストーラ VM の電源を入れます。

(注) HX Data Platform インストーラの仮想マシンの推奨設定は、3つの vCPU と 4GB 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、ホストへ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機します。

ステップ 7 HX Data Platform インストーラ仮想マシン コンソールを開きます。

初期コンソール表示には、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 URL を使用して HX Data Platform インストーラにログインします。

```
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。

(注) HXDP 3.5(1a) 以降では、デフォルトパスワードの Cisco123 は有効ではありません。OVA を導入するときに、パスワードを指定する必要があります。Cisco123 でログインしようとして成功しない場合は、導入時にパスワードを設定済みであることを意味します。

静的 IP アドレスによる HX データ プラットフォーム インストーラ OVA の展開

新しい VM に IP アドレスを割り当てる際に、DHCP がハイパーバイザ ウィザードのデフォルトである場合は、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** VMware OVF Tool 4.1 以降を、HX データ プラットフォーム ストレージ クラスター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 データ プラットフォーム インストーラ を検索し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 データ プラットフォーム 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.gateway.Cisco_HX_Installer_Appliance=10.64.8.1
--prop:hx.DNS.Cisco_HX_Installer_Appliance=10.64.1.8
--prop:hx.ip0.Cisco_HX_Installer_Appliance=10.64.8.36
--prop:hx.netmask0.Cisco_HX_Installer_Appliance=255.255.248.0
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
vi://root:password@esx_server
```

このコマンドでは、HX データ プラットフォーム インストーラ が展開され、HX データ プラットフォーム 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
```

DNS はインストーラ VM から到達できる必要があります。静的 IP アドレスが正常に設定され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 データ プラットフォーム インストーラ VM の展開後に電源を投入します。
X:injectOvfEnv	HX データ プラットフォーム インストーラ VM にスタティック IP のプロパティを挿入します。
prop:hx.gateway.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.DNS.Cisco_HX_Installer_Appliance=10.64.1.8	適切な DNS IP アドレスを指定します。

コマンド	説明
prop:hx.ip0.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.netmask0.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。
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova	HX データ プラットフォーム 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アルを含めます。

Cisco HX Data Platform インストーラへのログイン

HX データプラットフォームソフトウェアをインストールするには、次の手順を実行します。

ステップ 1 ブラウザで、HX データプラットフォームインストーラがインストールされた VM の URL を入力します。このアドレスは、前述の項「Deploying HX Data Platform インストーラの展開」から入手します。たとえば、<http://10.64.4.254> などとします。

ステップ 2 クレデンシアルを使用します。

ユーザ名 : *root*

パスワード : *Cisco123*

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。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。

EULA を読みます。[I accept the terms and conditions] をクリックします。

右下隅に記載された製品バージョンが正しいことを確認します。[Login] をクリックします。

ステップ 3 HX Data Platform インストーラの [Workflow] ページが表示されます。このページには、ワークフローのオプションが 3 つ表示されます。

1. **HyperFlex (FI) を使用したクラスタの作成。**
2. **HyperFlex Edge を使用したクラスタの作成** : HX ノードと ESXi を設定し、Edge サイト用の HX データプラットフォームソフトウェアを展開するには、このボタンをクリックします。詳細なインストール手順については、『[HyperFlex Edge deployment guide](#)』を参照してください。
3. **クラスタ展開**

- [Cluster Creation] : UCS Manager、ESXi を設定して HX Data Platform ソフトウェアを導入する場合は、このボタンをクリックします。
- [Cluster Expansion] : コンバージド ノードおよびコンピューティング ノードを既存のストレージクラスターに追加する場合は、このボタンをクリックし、表示される [Expand Cluster] ページでデータを入力します。詳細については、「[コンバージド \(HX220c/HX240c\) ノードの追加に関する前提条件](#)」を参照してください。

新規クラスターを作成するために [Cluster Creation] オプションを選択し、[Continue] をクリックします。

HX データ プラットフォーム インストーラの終了

ログインしている間は、HX データプラットフォームインストーラを使用可能です。任意の時点で HX データプラットフォームインストーラを終了するには、ログアウトする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	右上の [Navigate] ボタンに移動して、[Logout] を選択します。	
ステップ 2	再ログインするには、新しいブラウザウィンドウを開き、ログインクレデンシャルを入力します。	HX データプラットフォームインストーラのウェルカム ページに戻ります。

Syslog の設定

syslog の一元的なリポジトリにすべてのログ情報を送信することをお勧めします。



注目 永続ログには、SD カードから起動する HX220c M4 ノードとコンピューティング専用ノード上に syslog が必要です。

ステップ 1 syslog サーバが稼働していることと、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ます。

ステップ 2 ESXi シェルに対して SSH を行い、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

Cisco HX Data Platform インストーラを使用して Cisco HyperFlex クラスタをインストールおよび設定するには、次の手順を使用します。



注意 出荷時にインストールされた ESXi ではシステム設定をリセットしないでください。リセットすると工場出荷時設定が失われ、インストールが失敗することになります。

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 Data Platform 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。
[Accept] または [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に表示される HX Data Platform インストーラ インストーラの [Build 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 : root

パスワード (デフォルト): Cisco123

(注) 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。インストールを継続するには、ユーザー提供の新規パスワードを作成する必要があります。

- c) EULA を読んで、[I accept the terms and conditions] チェックボックスをオンにし、[Login] をクリックします。

ステップ 2 [Workflow] ページで、[Cluster Creation with HyperFlex (FI)] を選択します。

ステップ 3 [Credentials] ページで、次のフィールドに値を入力します。

クラスタ作成を実行するために、必要な設定データとともに *JSON configuration* ファイルをインポートすることもできます。次の 2 つの手順は、JSON ファイルをインポートする場合はオプションです。インポートしない場合には、データを必須フィールドに手動で入力できます。

(注) 初めてのインストールでは、ファクトリ プレインストール JSON ファイルの調達についてシスコの担当者にお問い合わせください。

1. [Select a file] をクリックして、使用する JSON ファイルを選択して設定をロードします。
[Use Configuration] を選択します。
2. Cisco UCS Manager 用にインポートした値が異なる場合は、[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。

フィールド	説明
[UCS Manager Credentials]	
[UCS Manager Host Name]	UCS Manager FQDN または IP アドレス たとえば <i>10.193.211.120</i> と入力します。
[User Name]	<admin> ユーザ名。
[Password]	<admin> パスワード。
[vCenter Credentials]	
[vCenter Server]	vCenter Server の FQDN または IP アドレス。 たとえば <i>10.193.211.120</i> と入力します。 (注) <ul style="list-style-type: none"> • vCenter Server は、クラスタが動作可能になる前に必要です。 • vCenter アドレスとクレデンシヤルは、vCenter へのルートレベルの管理者権限が必要です。 • vCenter Server 入力は、ネストされた vCenter を構築する場合には省略可能です。詳細については、『Nested vCenter TechNote』を参照してください。
[User Name]	<admin> ユーザ名。 例 : <i>administrator@vsphere.local</i> 。
[Admin Password]	<root> パスワード。
[Hypervisor Credentials]	
[Admin User Name]	<admin> ユーザ名。 これはファクトリ ノードの root です。

フィールド	説明
[Admin Password]	<p><root> パスワード。</p> <p>デフォルトのパスワードは、ファクトリ ノードの Cisco123 です。</p> <p>(注) 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。インストールを継続するには、ユーザー提供の新規パスワードを作成する必要があります。</p>

ステップ 4 [Continue] をクリックします。[Server Selection] ページが表示されます。右側の [Configuration] ペインには、使用された [Credentials] の詳細リストが表示されます。

ステップ 5 [Server Selection] ページには、[Unassociated] タブの下に関連付けされていない HX サーバのリストと、[Associated] タブの下に検出されたサーバのリストが表示されます。[Unassociated] タブからサーバを選択し、HyperFlex クラスタに含めます。

HX サーバがこの一覧に表示されていない場合、Cisco UCS Manager を調べてそれらが検出されていることを確認します。

サーバごとに、[Actions] ドロップダウン リストを使用して、以下を設定できます。

- [Launch KVM Console]—HX Data Platform 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。
- [Disassociate Server] : サービスプロファイルをそのサーバから削除するには、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.

[Configure Server Ports] ボタンを使用することで、新しいすべての HX ノードを検出できます。一般に、設定を開始する前に Cisco UCS Manager でサーバポートを設定します。

ステップ 6 [Continue] をクリックします。[UCSM Configuration] ページが表示されます。

ステップ 7 [UCSM Configuration] ページで、ネットワークごとに次のフィールドに値を入力します。

フィールド	説明
[VLAN Configuration]	(注) 次の各ネットワークにそれぞれ個別のサブネットと VLAN を使用します。
[VLAN for Hypervisor and HyperFlex management]	

フィールド	説明
[VLAN Name] [VLAN ID]	名前 : hx-inband-mgmt デフォルトの VLAN ID : 3091
[VLAN for HyperFlex Storage traffic]	
[VLAN Name] [VLAN ID]	名前 : hx-storage-data デフォルトの VLAN ID : 3092
[VLAN for VM vMotion]	
[VLAN Name] [VLAN ID]	名前 : hx-vmotion デフォルトの VLAN ID : 3093
[VLAN for VM Network]	
[VLAN Name] [VLAN ID]	名前: vm-network デフォルトの VLAN ID : 3094 ゲスト VLAN のカンマ区切りリスト。
[MAC Pool]	
[MAC Pool Prefix]	さらに 2 つの 16 進文字 (0-F) を追加することで、MAC プールプレフィックスを設定します。 たとえば、00:25:B5:A0 などです。
['hx-ext-mgmt' IP Pool for Out-of-Band CIMC]	
[IP Blocks]	HyperFlex ノードに指定された IP アドレスの範囲。 これは、ゲスト VLAN の値のカンマ区切りリストにできます。 例えば、10.193.211.124-127, 10.193.211.158-163
[Subnet Mask]	IP アドレスを制限して制御するために、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 と指定します。
[Gateway]	IP アドレス。 たとえば、10.193.0.1 と指定します。
[iSCSI Storage]	
(注) 将来的に任意の時点で外部ストレージの利用を希望する場合は、これを事前に設定する必要があります。	

フィールド	説明
[Enable iSCSI Storage] チェックボックス	iSCSIストレージを設定するには、オンにします。
[VLAN A Name]	プライマリファブリックインターコネクタ (FI-A) で、iSCSI vNIC に関連付けられている VLAN の名前。
[VLAN A ID]	プライマリファブリックインターコネクタ (FI-A) で、iSCSI vNIC に関連付けられている VLAN の ID。
[VLAN B Name]	下位のファブリックインターコネクタ (FI-B) で、iSCSI vNIC に関連付けられている VLAN の名前。
[VLAN B ID]	下位のファブリックインターコネクタ (FI-A) で、iSCSI vNIC に関連付けられている VLAN の ID。
[FC Storage] (注) 将来的に任意の時点で外部ストレージの利用を希望する場合は、これを事前に設定する必要があります。	
[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、オンにします。
[WWxN Pool]	WW ノード名および 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 インターコネクタに対し、WWPN および WWNN 用の WWxN プールが作成されます。
[VSAN A Name]	プライマリファブリックインターコネクタ (FI-A) の VSAN の名前。デフォルトでは、 <code>hx-ext-storage-fc-a</code> に設定されています。
[VSAN A ID]	プライマリファブリックインターコネクタ (FI-A) のネットワークに割り当てられた一意の ID。 注意 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 ゾーニングを使用する既存の VSAN ID をインストーラに入力すると、その VSAN ID の既存の環境でゾーニングが無効になります。
[VSAN B Name]	下位のファブリック インターコネクタ (FI-B) の VSAN の名前。デフォルトでは、 <code>hx-ext-storage-fc-b</code> に設定されています。

フィールド	説明
[VSAN B ID]	<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>注意 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 ゴーニングを使用する既存の VSAN ID をインストーラに入力すると、その VSAN ID の既存の環境でゴーニングが無効になります。</p>
[Advanced]	
[UCS Firmware Version]	<p>ドロップダウン リストから HX サーバに関連付ける UCS 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 Cisco HX データプラットフォームのリリースノート を確認してください。</p> <p>たとえば 3.2 (1日) と入力します。</p>
[HyperFlex Cluster Name]	<p>特定のクラスタ内の HX サーバのグループに適用される名前。これはユーザ定義の名前です。HyperFlex クラスタ名は、簡単に識別できるようにサービス プロファイルにラベルを追加します。</p>
[Org Name]	<p>一意の <i>Org Name</i> を指定します。これにより、残りの UCS ドメインからの HyperFlex 環境の分離が保証されます。</p>

(注) [Configuration] ペインで VLAN、MAC プール、および IP アドレス プールの情報を確認します。これらの VLAN ID は、環境に応じて変更できます。デフォルトでは、インストーラによって VLAN が非ネイティブとして設定されます。トランク設定を適切に適用することで、非ネイティブ VLAN に対応するようにアップストリーム スイッチを設定する必要があります。

ステップ 8 [Continue] をクリックします。[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
[Configure Common Hypervisor Settings]	

フィールド	説明
[Subnet Mask]	IP アドレスを制限して制御するために、サブネットマスクを適切なレベルに設定します。 たとえば、255.255.0.0 と指定します。
[Gateway]	ゲートウェイの IP アドレス。 たとえば、10.193.0.1 と指定します。
[DNS Server(s)]	DNS サーバの IP アドレス。 DNS サーバがない場合は、HX データプラットフォームインストーラの [Cluster Configuration] ページのいずれ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 ホストに静的 IP アドレスとホスト名のみを使用します。 (注) 複数の DNS サーバを提供する場合は、両方の DNS サーバが正しく入力されていることを慎重に確認し、カンマで区切ってください。
[Hypervisor Settings]	IP アドレスを順番に並べるには、[Make IP Addresses and Hostnames Sequential] を選択してください。 (注) ドラッグアンドドロップを使用してサーバを並べ替えることができます。
[Name]	サーバ名。
[Serial]	サーバのシリアル番号。
[Static IP Address]	すべての ESXi ホストに静的 IP アドレスとホスト名を入力します。
[Hostname]	ホスト名フィールドを空欄のままにしないでください。

ステップ 9 [Continue] をクリックします。[IP Addresses] ページが表示されます。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 アドレスの次のフィールドに値を入力します。IP アドレスについては、ネットワークがデータネットワークまたは管理ネットワークに属すべきかどうかを指定します。

[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。

フィールド	説明
[Management Hypervisor]	ESXi ホストとストレージクラスタ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。

フィールド	説明
[Management Storage Controller]	ストレージコントローラ VM とストレージクラスタ間の HX データ プラットフォーム 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クラスタ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静的 IP アドレスを入力します。
[Data Storage Controller]	ストレージコントローラ VM とストレージクラスタ間の HX データ プラットフォーム 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>[Hypervisor]、[Storage Controller VM (Management)]、[Hypervisor (Data)]、および [Storage Controller VM (Data)] 列の最初の行に IP アドレスを入力すると、Cisco 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、[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>	
[Cluster Management 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。
[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。
<p>ここで指定した各 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。ノードが利用不能になった場合、影響を受けた 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、これらの IP アドレスを受け入れるように設定されたポートが必要です。</p>	
[Management Subnet Mask]	<p>VLAN と vSwitch についてのサブネット情報を入力します。「ネットワーク VLAN および vSwitch の要件」の項を参照してください。</p> <p>管理ネットワークのネットワーク値を入力します。たとえば、255.255.255.0 と指定します。</p>
[Data Subnet Mask]	データ ネットワークのネットワーク値を指定します。たとえば、255.255.255.0 と指定します。
[Management Gateway]	管理ネットワークのネットワーク値を指定します。たとえば、10.193.0.1 と指定します。

フィールド	説明
[Data Gateway]	データ ネットワークのネットワーク値を指定します。たとえば、 <i>10.193.0.1</i> と指定します。

ステップ 10 [Continue] をクリックします。[Cluster Configuration] ページが表示されます。作成中のストレージクラスタの次のフィールドに値を入力します。

フィールド	説明
[Cisco HX Cluster]	
[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。
[Replication Factor] ドロップダウンリスト	<p>ストレージクラスタ間のデータの冗長レプリカの数。これは2個または3個の冗長レプリカになります。</p> <ul style="list-style-type: none"> ハイブリッドサーバ (SSDおよびHDDを含むサーバ) の場合、デフォルト値は3です。 フラッシュサーバ (SSDのみを含むサーバ) の場合は、2 または 3 を選択します。 稼働ワークロードには3を推奨します。

フィールド	説明
[Controller VM Password]	<p>デフォルトの管理者ユーザ名とパスワードがコントローラ VM に適用されます。VM は、コンバージドとコンピューティング専用のすべてのノードにインストールされています。</p> <p>重要</p> <ul style="list-style-type: none"> 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は変更できません。 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 文字になる複合パスワードを指定してください。 作成するコントローラ VM および HX クラスタにユーザ定義のパスワードを指定できます。パスワードの文字と形式の制限事項については、『Cisco HX Data Platform Management Guide』の「Guidelines for HX Data Platform Special Characters」の項を参照してください。
[vCenter Configuration]	
[vCenter Datacenter Name]	Cisco HyperFlex クラスタの vCenter データセンターの名前。
[vCenter Cluster Name]	vCenter クラスタ名。
System Services	
[DNS Servers]	各 DNS サーバの IP アドレスのカンマ区切りリスト。
[NTP Servers]	各 NTP サーバの IP アドレスのカンマ区切りリスト。ホストはすべて、同じ NTP サーバを使用する必要があります。これは、ストレージコントローラ VM および ESXi ホスト上で動作するサービス間のクロック同期に使用されます。

フィールド	説明
[Time Zone] ドロップダウン リスト	スケジュールされたスナップショットをいつ取得するかを決定する、コントローラ VM のローカルタイムゾーン。スケジュールされたネイティブスナップショットの処理はこの設定に基づきます。
[Connected Services]	
[Enable Connected Services] (推奨)	自動サポートを有効化します。HX Connect にログイ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。
[Send service ticket notifications to]	ASUP によるトリガー時に SR 通知が送信される電子メールアドレス。
[Advanced Networking]	
重要 これらの vSwitch 名を変更しないでください。	
[Management vSwitch]	デフォルトは <i>vswitch-hx-inband-mgmt</i> です。
[Data vSwitch]	デフォルトは <i>vswitch-hx-storage-data</i> です。
[Advanced Configuration]	
[Jumbo frames] [Enable Jumbo Frames] チェックボックス	ホスト vSwitch と vNIC、および各ストレージコントローラ VM 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にオンにします。 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 にお問い合わせください。
[Disk Partitions] [Clean up Disk Partitions] チェックボックス	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、バックアップする必要があります。 (注) 既存のデータおよび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。 これは、手動で準備されたサーバ用です。工場出荷時のシステムにはこのオプションを選択しないでください。工場出荷時の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。

フィールド	説明
[Virtual Desktop (VDI)] チェックボックス	VDI のみの環境でオンにします。 (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、クラスタを再起動します。
[vCenter Single-Sign-On Server]	この情報は、SSO URL が到達不可の場合のみ必要です。 重要 Cisco TAC からの指示がある場合以外は、このフィールドを使用しないでください。 [vCenter Server] > [Manage] > [Advanced Settings] > [key config.vpxd.sso.sts.uri] にナビゲートして、vCenter で SSO URL を見つけることができます。

ステップ 11 [Start] をクリックして、導入を開始します。[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」の項を参照してください。

次のタスク

- 一部の検証エラー（無効な ESXi パスワード、正しくない NTP サーバ、不正な SSO サーバ、または他の誤った入力）では、パラメータの再入力が必要になる場合があります。
[Re-enter Values] をクリックして [Cluster Configuration] ページに戻り、問題を解決します。
- 完了すると、HyperFlex サーバがインストールされて設定されます。展開されたクラスタステータスは、[Online] および [Healthy] のステータスを表示します。
- 必要に応じて、[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 を搭載した HyperFlex ノードの設置

GPU を搭載した HyperFlex ノードを設置するときには、特定の BIOS ポリシーの変更が必要になります。サポート対象のすべての GPU カードでは、4GB を超えるメモリマップ 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、『[Requirement for All Supported GPUs](#)』を参照してください。

HyperFlex クラスタ作成後の GPU の設置

クラスタを作成した後に GPU を設置する場合は、BIOS ポリシー設定が有効になるように、サーバに関連付けられているサービス プロファイルを変更する必要があります。

BIOS 設定を有効にするには、『[Cisco UCS Manager Controlled Server](#)』の詳細な説明に従います。ステップ 3 に指定されているように、4 GB 構成を超えたメモリ マップ I/O を [Enabled] に設定します。

HyperFlex クラスタ作成前の GPU の設置

クラスタを作成する前に GPU カードを設置する場合は、クラスタの作成時に、詳細ワークフローを選択します。

1. HX Data Platform インストーラページで、[I know what I'm doing, let me customize my workflow] を選択します。
2. [Run UCS Manager Configuration] をオンにし、[Continue] をクリックします。
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. BIOS 設定を有効にするには、『[Cisco UCS Manager Controlled Server](#)』の詳細な説明に従います。ステップ 3 に指定されているように、4 GB 構成を超えたメモリ マップ I/O を [Enabled] に設定します。
4. HX Data Platform インストーラページの詳細ワークフローに戻って [Run ESX Configuration]、[Deploy HX Software]、および [Create HX Cluster] を続行して、クラスタの作成を完了します。

HyperFlex クラスタの作成に関する考慮事項

HX Data Platform インストーラ タスク

HX Data Platform インストーラは、次のタスクを実行します。

- ハイパーバイザの設定。
- ESXi ホストの準備。
- ストレージコントローラ VM の導入。
- 確認検査の実行。
- クラスタ作成ステータスの表示。

インストーラのナビゲーション支援ボタン

- [Export Configuration] : 下向きの矢印アイコンをクリックすると、JSON 設定ファイルをダウンロードできます。

- [Tech Support] : 疑問符アイコンをクリックして、HyperFlex Data Platform ソフトウェアバージョンに関連する詳細を表示します。Cisco TAC 用にテクニカルサポートバンドルを作成するには、[Create New Bundle] をクリックします。
- [Save Changes] : 円のアイコンをクリックすると、HyperFlex クラスタ設定パラメータに加えられた変更を保存できます。
- [Settings] : 歯車のアイコンをクリックすると、[Start over] または [Log Out] を実行できます。

考慮事項

- 完全なクラスタの作成ワークフローが選択された場合、UCS Manager の設定に基づいて、VLAN が自動的に ESXi に設定されます。
- 導入とクラスタ作成のみが選択されている場合には、管理ネットワークとデータ ネットワークの VLAN ID を入力できます。

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 : [Settings] アイコン > [Start Over] をクリックします。[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。このページの [Add Server] をクリックすると、クラスタに含めるサーバをそれぞれ追加し、すべての IP アドレスを再入力できます。
- DNS がインストーラ VM に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、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 を使用したスマートライセンスの設定

- [スマートライセンスと HyperFlex \(83 ページ\)](#)
- [スマートライセンスへのクラスタの登録 \(88 ページ\)](#)
- [スマートライセンス承認の更新 \(90 ページ\)](#)
- [スマートライセンスからのクラスタの登録解除 \(90 ページ\)](#)

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）は新しいインテリジェントなソフトウェアライセンス管理ソリューションで、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。どのようなライセンスをどのように使用しているかを把握できるように、ライセンスの所有権および消費状況を可視化します。

スマートライセンスにより、会社全体でライセンスがプールされます。サーバベースのライセンスまたはスマートライセンスは、会社が所有する互換性のあるデバイスで使用できるように、デバイスにノードロックされません。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たとえば事業部門や製品タイプや IT グループ別に論理エンティティに編成すると、仮想アカウント間でデバイスとライセンスを簡単に転送できるようになります。

スマートライセンス機能は、Cisco HyperFlex と統合されており、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による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通じて、そのクラスタを 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、会社全体でシスコのソフトウェアライセンスおよび製品インスタンスを完全に可視化し、それらへのアクセスを制御するクラウドベースのリポジトリです。登録の有効期間は 1 年です。

登録すると、スマートアカウント側で HyperFlex を識別し、ライセンスの使用状況を Cisco Smart Software Manager または Smart Software Manager サテライトに報告できます。登録後、HyperFlex はライセンスの使用状況を現在のライセンス状況とともに、Cisco Smart Software

Manager または Smart Software Manager 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。

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により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 ヶ月ごとの更新登録要求。自動登録更新が行われない場合は、`stcli license renew id` コマンドを使用して手動で更新します。
- スマートライセンスでは、30 日ごとの更新承認要求が必要です。自動承認更新が行われない場合は、`stcli license renew auth` コマンドを使用して手動で更新します。更新を試みたときに接続が利用できない場合か、更新時間が接続時間帯外である場合にのみ、スマートライセンス承認を手動で更新する必要があります。
- また、更新の承認要求は、ライセンスの消費が変更されるたびに Cisco Smart Software Manager または Smart Software Manager に送信されます。この承認の有効期間は 90 日です。HyperFlex が 90 日の間に Cisco Smart Software Manager または Smart Software Manager に問い合わせた自身の承認を更新しなかった場合、HyperFlex で消費されているライセンスは回収され、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	ステータスの確認	システム機能性
評価モード	スマートライセンスは有効ですが、HX ストレージクラスタは、90 日間の評価期間および Cisco Smart Software Manager または Smart Software Manager に登録されません。	ステータスを確認するか、残りの評価期間を確認するには、 <code>#stcli license show all</code> を実行します。 Result: Mode = Eval & Remaining period (Number of Days:Hours:Minutes)	特長または機能性に影響はありません。
評価期限切れ	スマートライセンスは有効ですが、HX ストレージクラスタは、Cisco Smart Software Manager または Smart Software Manager に登録されません。ライセンスは最初の未確認状態で、コンプライアンス違反とは見なされません。	ステータスを確認するには、 <code>#stcli license show all</code> を実行します。 Result: Mode = Evaluation Expired	特長または機能性に影響はありません。 • Syslog メッセージを生成します。 • HX 接続 UI で 評価の期限が切れ警告を生成します。

登録ステータス	説明	ステータスの確認	システム機能性
コンプライアンス	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 に登録されます。ライセンスの消費数は所有数を下回っています。	—	—
コンプライアンス違反	<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>重要 シスコは、デバイスが不適合であっても、お客様のネットワークに干渉することもシャットダウンすることはありません。</p> <ul style="list-style-type: none"> • 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。 • 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、十分なライセンスがありません。 	<p>ステータスを確認するには、<code>#stcli license show all</code> を実行します。</p> <p>Result: Mode = Out of Compliance</p>	<p>特長または機能性に影響はありません。</p> <ul style="list-style-type: none"> • Syslog メッセージを生成します。 • クラスタレベルで HX 接続 UI にコンプライアンス違反 警告を生成します。 <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す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	ステータスの確認	システム機能性
認証が期限切れ	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ますが、90 日以上 Cisco Smart Software Manager または Smart Software Manager サテライトと通信していません。	ステータスを確認するには、 <code>#stcli license show status</code> を実行します。 Result: Mode = Authorization Expired	特長または機能性に影響はありません。 <ul style="list-style-type: none"> • Syslog メッセージを生成します。 • HX 接続のイベントまたはアラームはありません。 • Cisco Smart Software Manager ポータルでは、フラグと通知が表示されます。
エクスポートコントロールフラッグを「許可しない」に設定する	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ますが、エクスポートコントロールを使用するために登録することはできません。	—	動作は Cisco Smart Software Manager サーバによってほとんどコントロールされています。 (注) このステータスは、HX ストレージクラスタに制限機能が含まれている場合にのみ適用されます。

登録ステータス	説明	ステータスの確認	システム機能性
ID 証明書の有効期限が切れています	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ますが、ID 証明書は 6 か月以上更新されていません。ライセンスは不特定未確認状態で、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、 <code>#stcli license show status</code> を実行します。 Result: Mode: ID Certificate Expired すべての条件を消去しコンプライアンス ステータス に戻るには、次のコマンドを実行します。 <code>#stcli license renew <auth>/<id></code>	<ul style="list-style-type: none"> • Syslog メッセージを生成します。 • HX 接続のイベントまたはアラームはありません。 • Cisco Smart Software Manager ポータルでは、フラグと通知が表示されます。

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 サテライトを Cisco Smart Software Manager に登録し、完全に機能した後、30 日おきに Cisco Smart Software Manager を同期する必要があります。同期には次の 2 つのオプションがあります。

- ネットワークが接続されているときのオンデマンドまたはスケジュール済み同期。
- ライセンス ファイルをダウンロードおよびアップロードして手動で同期します。



(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 ポータルのスマート ライセンス登録では生成されなくなります。

スマート ライセンスへのクラスタの登録

スマート ライセンスは自動的に HX ストレージクラスタと統合し、デフォルトでは有効です。スマート ライセンスはインストールしません。HX ストレージクラスタはスマート ライセンスでは登録されておらず、90 日間評価モードです。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する必要があります。



注目 Smart Software Manager サテライトとともに HyperFlex クラスタを登録する前に、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、Smart Software Manager サテライトとともにクラスタを登録する前にプロキシを削除します。

始める前に

- HX ストレージクラスタが HyperFlex Data Platform 2.5 (1a) 移行を実行していることを確認します。
- スマート ライセンスの使用を開始する前には、Cisco スマートアカウントを持っている必要があります。スマートアカウントは発注時に作成（または選択）できます。または長期ではスマートアカウントを発注外で作成して、新規または既存のライセンスを追加することもできます。

スマートアカウントを作成するには、**[Cisco Software Central]** > **[Request a Smart Account]** (<https://webapps.cisco.com/software/company/smartaccounts/home?route=module/accountcreation>) を参照してください。

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 モードで HX ストレージクラスタを確認します。

```
# stcli license show status
```

フィードバックには [Smart Licensing is ENABLED]、[Status: UNREGISTERED] と表示され、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、更新はできません。評価期間の期限が切れた後に、スマート エージェントは通知を送信します。

ステップ 3 使用するバージョンに応じて、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]	[Cisco Software Central] (https://software.cisco.com/) に移動し、スマートアカウントにログインします。[License] ウィンドウで、[Smart Software Licensing] をクリックします。[Inventory] をクリックします。
[Smart Software Manager satellite]	<a href="https://<サテライトの IP アドレス>:8443">https://<サテライトの IP アドレス>:8443 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 4 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、[General] をクリックして、[New Token] をクリックします。

ステップ 5 [Create Registration Token] ダイアログボックスで、次を実行して、[Create Token] をクリックします。

- トークンの簡潔な [Description] を追加します。
- トークンをアクティブであり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
- [Allow export-controlled functionality on the products registered with this token] をオンにします。

ステップ 6 [New ID Token] 行から、[Actions] ドロップダウン リストをクリックし、[Copy] をクリックします。

ステップ 7 コントローラ VM にログインします。

ステップ 8 HX ストレージクラスタを登録します。 *idtoken-string* は、Cisco Smart Software Manager または Smart Software Manager サテライトからの **新規 ID トークン** です。

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

ステップ 9 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、HX ストレージクラスタが登録されていることは、[Cisco Smart Software Manager] > [Inventory] > [Product Instances] で確認できます。

例：

```
root@SpringpathController80IW1HJOKW:~# 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承認の更新

始める前に

- HXストレージクラスタがスマートライセンスに次のコマンドを使用して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
```

スマートライセンスからのクラスタの登録解除

ライセンスを解放してプールに戻して別の HX ストレージクラスタで使用されるようにするか、または Cisco Smart Software Manager の登録を削除する場合（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、HyperFlex は評価期間が残っていれば評価モードで実行します。そうでない場合は、HyperFlex は評価の有効期限切れの状態になります。

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、それ自体を登録解除します。プラットフォーム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に通信できない場合でも登録解除できます。スマートライセンスを再び使用することが必要な場合、HX ストレージクラスタを再登録します。[スマートライセンスへのクラスタの登録 \(88 ページ\)](#) を参照してください。

始める前に

- HXストレージクラスタがスマートライセンスに次のコマンドを使用して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
```



第 7 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](#) (93 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](#) (94 ページ)
- [インストール後のスクリプトの実行](#) (94 ページ)
- [ESXi ホストルートパスワードの変更](#) (98 ページ)
- [ストレージコントローラパスワードの変更](#) (99 ページ)
- [vSphere を介した HX データ プラットフォーム プラグインへのアクセス](#) (99 ページ)
- [ストレージクラスタでのデータストアの追加](#) (100 ページ)
- [HA ハートビートの設定](#) (100 ページ)
- [HyperFlex の Auto Support と Smart Call Home](#) (101 ページ)
- [レプリケーションペアリング](#) (107 ページ)
- [プライベート VLAN の追加](#) (108 ページ)
- [分散型仮想スイッチと Cisco Nexus 1000v](#) (112 ページ)
- [HX Data Platform での vCenter のホスト](#) (113 ページ)
- [AMD GPU の展開](#) (113 ページ)

クラスタ設定後のガイドライン



重要

- SSH をすべての ESXi ホストで有効なままにします。これは、次の Cisco HyperFlex クラスタ設定後操作に必要です。
 - 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。

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 [Configure] タブをクリックして、[Settings] をクリックします。
 - ステップ 3 [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 4 デバイス（NVIDIA GPU など）を選択して、[Toggle passthrough] をクリックします。
 - ステップ 5 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 6 vSphere Web Client を使用して vCenter にログインします。
 - ステップ 7 VM を特定して [Manage] タブをクリックします。[Settings] > [VM Hardware] を選択します。[Edit] をクリックします。
 - ステップ 8 [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 9 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 10 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 11 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 VM でインストール後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。スクリプトは、すべてのネットワーク インターフェイス（管理、vMotion、およびストレージ ネットワーク）に ping を実行して、ファブリックが完全に利用できることを確認します。また、ノースバウンド スイッチで VLAN のタグging が正しいことと、ジャンボ フレーム設定を検証します。



重要

- `post_install` スクリプトは、ノースバウンドスイッチ経由で強制的に接続を確立します。ネットワークが正しく設定されていない場合は、1つのノードがクラスタ内で接続を一時的に失う可能性があります。テストが完了すると、設定が元に戻ります。
- HyperFlex システムを導入したら、すぐに `post_install` を実行し、ネットワークが動作することを確認します。
- アップストリームネットワークを以前に検証したことがある場合を除き、実稼働システムでこのスクリプトを実行しないでください。
- Web ベースの SSH がロードされていない場合、優先クライアントを使用してインストーラ VM に SSH で接続し、`post_install` スクリプトを実行します。

1. Web ブラウザから、`http://<installer VM IP>/mssh` にアクセスします。
2. インストーラ VM のルートクレデンシャルでログインします。
3. `post_install` と入力し、[Enter] を押します。
4. 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
クラスタで HA/DRS を有効にするか (Enable HA/DRS on cluster?)	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。
SSH 警告を無効にするか (Disable SSH warning?)	vCenter で SSH とシェル警告を抑制します。HyperFlex システムを適切に機能させるには、SSH を有効のままにしておく必要があります。
vMotion インターフェイスを追加する (Add vMotion interfaces)	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 の入力は必須です。
VM ネットワーク VLAN を追加する (Add VM network VLANs)	Cisco UCS Manager およびすべてのクラスタホスト上の ESXi 内にゲスト VLAN を追加します。
ESXi ホストで NTP を有効にする (Enable NTP on ESXi hosts)	ESXi ホストで NTP を設定し、有効にします。

パラメータ	説明
寛容モードを有効にする (Enable Lenient Mode?)	寛容モードはデフォルトになりました。[Y]を押して処理を続行します。
テストメールを送信する (Send test email?)	SMTP メールサーバと自動サポートパラメータが設定されている場合は、SMTP リレーが動作していることを確認するためにテストメールが送信されます。

5. 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

```

root@Cisco-HX-Data-Platform-Installer:~# post_install
Setting ESX hosts from HX cluster...
vCenter URL: 172.26.17.177
Enter vCenter username (user@domain): administrator@vsphere local
vCenter password:
Found datacenter RTP-DC
Found cluster HX-Cluster

Enable HA/DRS on cluster? (y/n) y

Disable SSH warning? (y/n) y

configure ESXi logging onto HX datastore? (y/n) y
No datastores found
Creating datastore...
Name of datastore: HX-Logs
size (6B): 50
Storing logs on datastore HX-Logs
Creating folder [HX-Logs]/esxi_logs

Add vmotion interfaces? (y/n) y
Netmask for vMotion: 255.255.255.0
VLAN ID: (0-4096) 3093
vMotion IP for esx-hx-6.cpoc-rtp.cisco.com: 192.168.11.154
Adding vmKernel to esx-hx-6.cpoc-rtp.cisco.com
vMotion IP for esx-hx-1.cpoc-rtp.cisco.com: 192.168.11.151
Adding vmotion to esx-hx-1.cpoc-rtp.cisco.com
Adding vmKernel to esx-hx-1.cpoc-rtp.cisco.com
vMotion IP for esx-hx-5 .cpoc- rtp.cisco.com: 192.168.11.153
Adding vmKernel to esx-hx-5.cpoc-rtp.cisco.com
vMotion IP for esx-hx-2.cpoc- rtp.cisco.com: 192.168.11.152
Adding vmKernel to esx-hx-2.cpoc-rtp.cisco.com

Add VM network VLANs? (y/n) n

Enable NTP on ESX hosts? (y/n) y
Starting ntpd service on esx-hx-6.cpoc-rtp.cisco.com
Starting ntpd service on esx-hx-1.cpoc-rtp.cisco.com
Starting ntpd service on esx-hx-5.cpoc-rtp.cisco.com
Starting ntpd service on esx-hx-2.cpoc-rtp.cisco.com

Enable Lenient Mode? (y/n) y
Lenient mode is already set

Send test email? (y/n) n

```

```
Validating cluster health and configuration...
Found UCSM hyper-ucs.cpoc-rtp.cisco.com, logging with username admin. Org is hx-cluster
```

```
UCSM Password:
```

```
Checking MTU settings
pinging 192.168.16.164 from vmk1
pinging 192.168.10.161 from vmk1
pinging 192.168.16.163 from vmk1
pinging 192.168.10.162 from vmk1
Setting vnic2 to active and vmic3 to standby
Pinging 192.168.10.164 from vmk1
pinging 192.168.16.164 with mtu 8972 from vmk1
Pinging 192.168.10.161 from vmk1
pinging 192.168.10.161 with mtu 8972 from vmk1
pinging 192.168.16.163 from vmk1
pinging 192.168.10.163 with mtu 8972 from vmk1
pinging 192.168.10.162 from vmk1
pinging 192.168.16.162 with mtu 8972 from vmk1
Setting vmnic3 to active and vnic2 to standby
pinging 172.26.17.154 from vmk0
pinging 172.26.17.151 from vmk0
pinging 172.26.17.153 from vmk0
Pinging 172.26.17.152 from vmk0
Setting vnic1 to active and vmnic0 to standby
pinging 172.26.17.154 from vmk0
Pinging 172.26.17.151 from vmk0
pinging 172.26.17.153 from vmk0
pinging 172.26.17.152 from vmk0
Setting vmnic0 to active and vnic1 to standby
pinging 192.168.11.154 from vmk2
pinging 192.168.11.151 from vmk2
pinging 192.168.11.153 from vmk2
pinging 192.168.11.152 from vmk2
Setting vnic7 to active and vmnic6 to standby
pinging 192.168.11.154 from vmk2
pinging 192.168.11.154 with mtu 8972 from vmk2
pinging 192.168.11.151 from vmk2
pinging 192.168.11.151 with mtu 8972 from vmk2
Pinging 192.168.11.153 from vmk2
pinging 192.168.11.153 with mtu 8972 from vmk2
pinging 192.168.11.152 from vmk2
pinging 192.168.11.152 with mtu 8972 from vmk2
Setting vmnic6 to active and vnic7 to standby
```

サンプルのネットワーク エラー

```
Host: esx-hx-5.cpoc-rtp.cisco.com
Np errors found
```

```
Host: esx-hx-6.cpoc-rtp.cisco.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
stctlVM-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 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 HyperFlex ストレージコントローラの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、変更がストレージクラスタ内のすべてのコントローラ VM に適用されます。

(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再設定しようとする、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。

コンピューティング ノードでパスワードを変更するには：

1. ESXi ホストからすべてのユーザー VM を vMotion します。
2. VCenter からストレージコントローラ VM コンソールを起動し、root ユーザーとしてログインします。
3. **passwd** コマンドを実行して、パスワードを変更します。
4. ログアウトして再度ログインし、パスワードが正常に変更されたことを確認します。
5. **stcli node add -f** コマンドを実行し、ノードをクラスタに再び追加します。

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。

vSphere を介した HX データ プラットフォーム プラグインへのアクセス

GUI を介してストレージクラスタを管理するには、vSphere Web クライアントを起動します。vSphere Web クライアントおよび HX データ プラットフォーム プラグインを使用してストレージクラスタにアクセスします。

-
- ステップ 1** HX データ プラットフォーム インストーラから、インストールの完了後に、[Summary] ページで [Launch vSphere Web Client] をクリックします。
- ステップ 2** ログイン ページが表示され、[Login to vSphere Web Client] をクリックして、vSphere クレデンシャルを入力します。
- ステップ 3** HX データ プラットフォーム プラグインが表示されます。
- vSphere Web クライアント ナビゲータから、[vCenter Inventory Lists] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] を選択します。
-

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** vSphere 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** [Create Datastore] アイコンをクリックします。
- ステップ 3** [Name] にデータストアの名前を入力します。vSphere Web クライアントでは、データストア名に 42 文字の制限が適用されます。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 [Size] 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** [Hosts] タブをクリックして、新しいデータストアの [Mount Status] を確認します。
-

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、[Datastore for Heartbeating] オプションを設定します。

-
- 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 **[Home]** > **[Hosts and Clusters]**、**[cluster]** > **[Configure]**、**[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。**[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、**[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 **[Admission Control]** > **[Define Fallover capacity by]** > **[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 Auto Support 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。

自動サポート (ASUP)

自動サポートは、HX Data Platform を通じて提供されるアラート通知サービスです。自動サポートを有効にすると、HX Data Platform から、通知の受信先として指定された電子メールアドレスまたは電子メールエイリアスに通知が送信されます。自動サポートは通常、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]** 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自動サポート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	HX Connect を使用した自動サポートの構成 (102 ページ)
コマンドライン インターフェイス (CLI)	CLI を使用した通知設定の構成 (103 ページ)
REST API	Cisco HyperFlex は Cisco DevNet での REST API をサポートします。

自動サポートを使用して、HX ストレージクラスタをモニタリング ツールに接続することもできます。

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 システムに組み込まれている製品機能です。Smart Call Home は Call Home の基本機能を高めるために自動化機能と利便性向上機能を追加します。Smart Call Home を有効にすると、Smart Call Home に Call Home メッセージ/アラートが送信されます。

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。
- カスタマイズされたステータス 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、あなた、そしてサポートの間で自動通信を確保するには、[データコレクションの Smart Call Home の構成 \(104 ページ\)](#) を参照してください。

HX Connect を使用した自動サポートの構成

通常は、HX ストレージクラスタの作成中に自動サポート (ASUP) が設定されます。設定されなかった場合、HX Connect ユーザーインターフェイス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。

ステップ 1 HX Connect にログインします。

ステップ 2 バナーで、**[Edit settings]** (歯車アイコン) > **[Auto Support Settings]** の順にクリックして次のフィールドに記入します。

UI 要素	基本情報
[Enable Auto Support (Recommended)] チェック ボックス	次を有効にすることで、この HX ストレージクラスタの自宅に発信を構成します。 <ul style="list-style-type: none"> • 分析のための Cisco TAC へのデータ配信。 • プロアクティブサポートの一環としてサポートからの通知。
[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。
[Enable Remote Support] チェック ボックス	クラスタ操作に関する情報を収集して報告された異常のトラブルシューティングを高速化するために、サポートの HX ストレージクラスタへのアクセスを有効にします。
[Use Proxy Server] チェックボックス	<ul style="list-style-type: none"> • Web プロキシ サーバ url • Port • Username • Password

ステップ 3 [OK] をクリックします。

ステップ 4 バナーで、[Edit settings] (歯車アイコン) > [Notifications Settings] の順にクリックして次のフィールドに記入します。

UI 要素	基本情報
[Send email notifications for alarms] チェック ボックス	オンにした場合は、次のフィールドを入力します。 <ul style="list-style-type: none"> • [Mail Server Address] • [From Address] : サポート サービス チケットの HX ストレージクラスタを識別するために使用し、また自動サポート通知の送信者として使用するメールアドレスを入力します。現在、サポート情報はこのメールアドレスには送信されません。 • [Recipient list] (カンマ区切り)

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確認するには、次の手順に従ってください。



(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。

シンタックス : `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、設定を確認します。

電子メール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です。電子メールが複数ある場合はスペースで区切ります。

シンタックス : `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 の IP アドレスを所有しているコントローラ VM から、電子メールにテスト ASUP 通知を送信します。

```
# sendasup -t
```

eth1:0 の IP アドレスを所有しているノードを確認するには、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。

データコレクションの Smart Call Home の構成

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。アップグレード中に、Smart Call Home がレガシー構成に基づいて設定されます。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) 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 サポート付きの HX ストレージ クラスタを登録します。

HX ストレージ クラスタを登録すると、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 クラスタを登録するには、電子メールアドレスを指定する必要があります。登録後、このメールアドレスは、問題があり TAC のサービス要求が生成されるたびにサポート通知を受け取ります。

(注) Hyperflex で Smart Call Home を設定するときに、登録を完了するためのリンクを含む電子メールが設定済みのアドレスに送信されます。この手順を完了していない場合、デバイスは非アクティブ状態のままになり、自動サービス リクエストはオープンになりません。

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 フローが稼働していることを確認します。

稼働しているデータ フローにより、生じる可能性のある問題のトラブルシューティングをサポートできる関連情報をすぐに利用できます。

-すべて オプションの HX クラスタ内のすべてのノードのコマンドを実行します。

```
# asupcli [--all] ping
```

HX ストレージ クラスタを HyperFlex 1.7.1 から 2.1.1b にアップグレードする場合は、次のコマンドも実行します。

```
# asupcli [--all] post --type alert
```

次のエラーが表示される場合はサポートにお問い合わせください。

```
root@ucs-stctlv-554-1:/tmp# asupcli post --type alert
/bin/sh: 1: ansible: not found
Failed to post - not enough arguments for format string
root@ucs-stctlv-554-1:/tmp#
```

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	オプション	必須またはオプション	説明
	--email EMAILADDRESS	必須です。	Cisco サポートからのメールを受信する人の電子メールアドレスを追加します。配布リストまたはエイリアスを使用することを推奨します。
	--enable-proxy ENABLEPROXY	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。
	--portal-url PORTALURL	オプション。	代替の Smart Call Home ポータルの URL を指定します (該当する場合)。
	--proxy-url PROXYURL	オプション。	HTTP プロキシの URL を指定します (該当する場合)。
	--proxy-port PROXYPORT	オプション。	HTTP プロキシのポートを指定します (該当する場合)。
	--proxy-user PROXYUSER	オプション。	HTTP プロキシのユーザを指定します (該当する場合)。 HTTP 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おり、データが HX ストレージクラスタからサポート ロケーションに流れることを確認するために Ping を送信します。

```
# asupcli [--all] ping
```

-すべて オプションが HX クラスタ内のすべてのノードで、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 の設定が `set` の場合、自動的に有効になります。

```
# stcli services sch show
```

Smart Call Home が無効の場合は手動で有効にします。

```
# stcli services sch enable
```

- ステップ 6 自動サポート (ASUP) 通知を有効にします。

通常は、HX ストレージクラスタの作成中に自動サポート (ASUP) が設定されます。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。詳細については、「[HyperFlex の Auto Support と Smart Call Home](#)」を参照してください。

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、レプリケーション用 VM の設定の前提条件です。レプリケーション ネットワークと少なくとも 1 つのデータストアは、レプリケーション ペアを作成する前に構成しなければなりません。

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。1 つのクラスタを 2 つ以上の他のクラスタとペアリングすることはできません。ペアになっているクラスタ上の 1 つのデータストアは、他のクラスタ上の 1 つのデータストアとしかペアリングできません。

レプリケーションペアの作成、編集、および削除の詳細手順については、「[Cisco HyperFlex Systems アドミニストレーションガイド](#)」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 の概要

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 のメンバーであり、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 に属します。無差別ポートに関連付けられ、プライマリ VLAN に関連付けられているセカンダリ VLAN に属するすべてのインターフェイスと通信できます。これらのインターフェイスには、コミュニティポートと隔離されたホストポートが含まれます。セカンダリ VLAN からのすべてのパケットがこの VLAN を通過します。
隔離されたセカンダリ VLAN	隔離されたセカンダリ VLAN に属するホストポート。このポートは、アソシエートされている無差別ポートと通信できることを除き、同じプライベート VLAN ドメイン内の他のポートから、完全に隔離されています。
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。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 配備後、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 を使用するには、次のセクションを参照してください。

- 既存の VM がない状態で VM ネットワークのプライベート VLAN を設定する (109 ページ)。
- 既存の VM で VM ネットワークのプライベート VLAN を設定する (109 ページ)。

既存の VM がない状態で VM ネットワークのプライベート VLAN を設定する

-
- 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 ネットワーク管理ガイド](#)』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 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド](#)』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 ホストでのプライベート VLAN の設定 \(109 ページ\)](#)』を参照してください。
-

ESX ホストでのプライベート 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 分散スイッチを作成します。
- ステップ 3** 無差別、独立、およびコミュニティ VLAN を作成します。
-

既存の VM で VM ネットワークのプライベート VLAN を設定する

-
- 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 ネットワーク管理ガイド](#)』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 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド](#)』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、以下を参照してください。『[ESX ホストでのプライベート VLAN の設定 \(109 ページ\)](#)』
- 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、[source network] および [destination network] を選択します。
 - [Next] をクリックします。
 - 移行する仮想マシンを選択します。
 - [Finish] をクリックします。
- ステップ 5** VM 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、[Edit Settings] をクリックします。
 - [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。

- c) [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を選択します。
- d) [OK] をクリックします。

vSphere 標準スイッチでの VMNIC の削除

- ステップ1 VMware vSphere クライアントにログインします。
 - ステップ2 [Home] > [Hosts and Clusters] を選択します。
 - ステップ3 VMNIC を削除する ESX ホストを選択します。
 - ステップ4 [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、[Remove] をクリックします。
 - ステップ9 [Yes] をクリックして、選択内容を確認します。
 - ステップ10 [Close] をクリックします。
-

vSphere 分散スイッチの作成

- ステップ1 VMware vSphere クライアントにログインします。
- 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 [Finish] をクリックします。

vSphere 分散スイッチでのプライベート VLAN の作成

ステップ 1 VMware vSphere クライアントから、[Inventory] > [Networking] を選択します。

ステップ 2 dvSwitch を右クリックして、[Edit Settings] をクリックします。

ステップ 3 [Private VLAN] タブを選択します。

ステップ 4 [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 5 [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 6 [Type] ドロップダウン リストから、VLAN のタイプを選択します。次のいずれかを設定できます。

- [Isolated]
- [Community]

(注) 無差別プライベート VLAN が自動的に作成されます。

ステップ 7 [OK] をクリックします。

分散ポート グループでのプライベート 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、[Edit Settings] をクリックします。

ステップ 2 [Policies] > [VLAN] をクリックします。

ステップ 3 [VLAN type] ドロップダウン リストから [Private VLAN] を選択します。

ステップ 4 [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。次のいずれかを設定できます。

- [Isolated]
- [Community]

(注) コミュニティプライベート VLAN が推奨されます。

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 ネットワーク用の DVS は、ご使用の環境に vSphere 用の Enterprise Plus ライセンスがある場合にのみ使用できます。
 - 同時に使用できるスイッチは、常にこの2つのうちのいずれか1つだけです。
 - HyperFlex と Nexus 1000v の間では、Quality of Service (QoS) ポリシーが競合する可能性があります。N1Kv の QoS クラスが HyperFlex ポリシーに従って設定されるようにしてください。『[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、説明のとおりを設定を適用し、HyperFlex ホスト間のトラフィックが FI 上を定常状態でローカルに流れるようにします。正しく設定されていないと、トラフィックの大半がアップストリームスイッチを経由することになる可能性があります。その場合には遅延が発生します。このような事態を避けるには、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 グループをアクティブ/スタンバイ構成で設定し、フェールオーバーを有効にしてください。
1. UCS Manager を使用して、[Network Control Policy] にリンク ステータスを設定します。詳細については、『[Cisco UCS Manager GUI Configuration Guide](#)』の「Configuring Network Control Policy」を参照してください。
 2. vCenter で vSwitch のプロパティを設定します。
 - a. [Network Failure Detection] を [Link Status only] に設定します。
 - b. [Failback] を [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」を参照してください。

分散スイッチにより、各ノードが同じ構成を使用することになります。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) データ プラットフォームは、HyperFlex 非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。

これらの HX 非依存ネットワークには次のものがあります。

- VMware vMotion ネットワーク

- VMware アプリケーション ネットワーク

HX データ プラットフォームには依存関係があり、次のネットワークが標準の vSwitch を使用します。

- 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-mgmt : 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 データプラットフォームのインストール時に、すべてのネットワークが標準の vSwitch ネットワークで設定されます。ストレージクラスタが設定された後、HX 非依存ネットワークを DVS ネットワークに移行できます。次に例を示します。

- vswitch-hx-vm-network : VM ネットワーク
- vmotion : vmotion pg

分散仮想スイッチに vMotion ネットワークを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 での vCenter のホスト

HyperFlex クラスタへの vCenter の導入をサポートするには、いくつかの制約事項が伴います。詳細については、[HX データ プラットフォームで vCenter を展開する方法](#) 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 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 の 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	手順の指示
1	サーバに接続されているサービスプロファイルに関して BIOS ポリシーを変更します。	サポートされるすべての GPU の要件 : 4 GB を超えるメモリマップド I/O
2	サーバで GPU カードをインストールします。	GPU カードの取り付け

ステップ	アクション	手順の指示
3	サーバの電源を入れて、GPUがサーバのCisco UCS Manager インベントリで表示されていることを確認します。	—
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。	VMware ESXi で AMD 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 Cisco ソフトウェアダウンロード から、インベントリリストをダウンロードします。
5	VM 設定済みのクラスタで Win10 VM を作成します。	対象の仮想マシンを指定する
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。	MxGPU セットアップスクリプトを使用する
7	Win10 Vm に対して前のステップで作成された仮想機能 (VFs) を割り当てます。	—



第 8 章

複数の HX クラスタの設定

- [複数のクラスタの設定 \(115 ページ\)](#)

複数のクラスタの設定

HyperFlex クラスタには、最大 8 つのコンバインド ノードと 8 つの コンピューティング専用 ノードを設定できます。HX クラスタ を 16 個以上のノードに拡張するには、最大 8 つの HX クラスタを Cisco UCS ファブリック インターコネクットのペアに接続できます。



- (注) 2 つの異なる HX バージョンの 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 バージョンは、リリース ノートごとに UCSM サーバ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バージョンには依存しません。

推奨事項

1. 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。
2. 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。
3. 展開については、HX Data Platform インストーラを使用します。
4. HX クラスタのすべての HX ノードで同じポリシーおよびサービス プロファイル テンプレートを使用します。
5. すべてのクラスタ上で、同じデータセンターと vCenter 設定を使用します。
6. 各 HX クラスタの一意的な名前を割り当てます。
7. 個別のポリシーを設定してクラスタ間の自律性を確保できるよう、クラスタごとにサブ組織を作成します。このようにすると、アップグレードの際に役立ちます。

8. 各サブ組織に新しいユーザー定義の VLAN ID を作成します。
9. 互換性のある Cisco UCS Manager と Cisco HyperFlex バージョン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。

10. 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。

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 \(63 ページ\)](#) を参照してください。



第 9 章

HX-FI ドメインへの UCS サーバの追加

- [既存の HX FI ドメインへの Cisco UCS サーバの追加](#) (117 ページ)

既存の HX FI ドメインへの Cisco UCS サーバの追加

HX 1.8 リリースでは、Cisco UCS ドメイン内のサーバを既存の HX FI ドメインに追加できます。HX FI ドメインの一部ではないサーバを追加するには、最初に Cisco UCS Manager でサブ組織を作成します。これにより、Cisco UCS サーバ用の個別のサーバプロファイルとポリシーを作成できます。新しいサブ組織の作成手順の詳細については、『**Cisco UCS Manager Administration Management Guide**』を参照してください。以下のリンクを使用できます。

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1_chapter_01000.html

HX FI ドメインに Cisco UCS サーバを追加する際の考慮事項は以下のとおりです。

- [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](#) (32 ページ) を参照して、ネットワーク帯域幅を処理するのに十分なアップリンク容量があることを確認します。
- HX サーバには、Cisco UCS ファームウェアに関する最小要件があります。また、HX FI ドメインに追加する Cisco UCS サーバにも同じ Cisco UCS ファームウェアを導入する必要があります。詳細については、**HX 相互運用性の表**を参照してください。以下のリンクを使用できます。

<http://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-technical-reference-list.html>

- Cisco UCS の設定に関する制限事項は、HX サーバと Cisco UCS サーバの両方に適用されます。詳細については、『**Cisco UCS Manager Configuration Limits Guide**』を参照してください。以下のリンクを使用できます。

<http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-and-configuration-guides-list.html>

- HX サーバには、VLAN および QoS クラスに関する特定の要件があります。Cisco UCS サーバの VLAN および QoS の設定が HX サーバと両立するようにならなければなりません。VLAN および QoS 設定の詳細については、『**HyperFlex Getting Started Guide**』の「**Appendix**」を参照してください。以下のリンクを使用できます。

http://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/GettingStartedGuide/b_HyperFlexSystems_GettingStartedGuide/b_HyperFlexSystems_GettingStartedGuide_chapter_0111.html

- HX ストレージ VLAN は HX クラスタ専用にする必要があります。この VLAN を Cisco UCS サーバに再利用しないでください。ネットワーク設定の詳細については、『**Getting Started Guide**』の「**Requirements**」に記載されているネットワーク構成図を参照してください。

http://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/GettingStartedGuide/b_HyperFlexSystems_GettingStartedGuide/b_HX_BookMap_chapter_01.html#id_13169

- ハイパーバイザ管理 VLAN、vMotion VLAN、および VM ネットワーク VLAN は、Cisco UCS サーバの間で共有できます。



第 10 章

Cisco HyperFlex システム クラスタの展開

この章は、次の項で構成されています。

- [クラスタ展開のガイドライン \(119 ページ\)](#)
- [混合 M4/M5 クラスタを作成する場合の前提条件 \(120 ページ\)](#)
- [混合クラスタ展開中の手順 \(121 ページ\)](#)
- [コンバージド \(HX220c/HX240c\) ノードの追加に関する前提条件 \(121 ページ\)](#)
- [コンバージド ノードの準備 \(122 ページ\)](#)
- [既存のクラスタへのコンバージド ノードの追加 \(123 ページ\)](#)
- [コンピューティング専用ノードの追加に関する前提条件 \(133 ページ\)](#)
- [コンピューティング専用ノードの準備 \(134 ページ\)](#)
- [既存のクラスタへのコンピューティング専用ノードの追加 \(137 ページ\)](#)
- [クラスタ展開の障害の解決 \(143 ページ\)](#)
- [ロジカル アベイラビリティ ゾーンの有効化 \(144 ページ\)](#)

クラスタ展開のガイドライン

- 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。
- 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 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、またはフロントアクセス対応 SSD/HDD 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。

混合クラスタ展開のガイドライン 2.6

混合クラスタは、同じストレージクラスタ内の M4 および M5 HX コンバージド ノードの両方を持つことで定義されます。混合クラスタを設定するとき、以下のガイドラインが適用されます。

- M5 コンバージド ノードを持つ既存の M4 クラスタの展開がサポートされています。
- M4 コンバージド ノードを持つ既存の M5 クラスタの展開がサポートされています。
- M4 または M5 コンバージド ノードを持つ既存の混合 M4/M5 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 2.6 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 クラスタすべてで許可されています。いくつかの例となる組み合わせがここにリストされています。その他多くの組み合わせが可能です。

Example combinations:

Expand mixed M4/M5 cluster with compute-only B200, C220, C240 M4/M5

Expand M4 cluster with compute-only B200 M5, C220 M5, C240M5

- 混合クラスタを作成するには、展開ワークフローのみがサポートされています。混合 M4/M5 サーバを持つ最初のクラスタ作成はサポートされていません。
- すべての M5 サーバは、既存の M4 サーバのフォーム 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。
 - HX220-M4 と組み合わせるとき、HX220-M5 は最大 6 の容量ディスク (2 ディスク スロットは空のまま) を使用します。
- HyperFlex Edge は混合クラスタをサポートしません。
- SED SKU は混合クラスタをサポートしません。

混合 M4/M5 クラスタを作成する場合の前提条件

混合クラスタでクラスタ展開を開始する前に、次のタスクを実行する必要があります。

- UCS Manager を 3.2(1d) 以降にアップグレードします。
- 既存の HX クラスタを 2.6(1a) 以降に完全にアップグレードします。
- 2.6(1A) 以降の HX Data Platform インストーラをダウンロードして展開し、展開ワークフローを実行します。
- 既存の M4 サーバファームウェアを最新の 3.2(1) パッチ リリース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 モードのオフはサポートされておらず、将来的に運用上の問題が発生します。

混合クラスター展開中の手順

- 検証手順を実行中、展開が開始する前に EVC チェックが実行されます。この時点で、既存のクラスターで EVC モードを手動で有効にするにあたり表示される指示に従います。



注意 警告時に EVC の有効化に失敗すると、ストレージクラスターと後で関連付けられた VM の完全なシャットダウンが必要となります。この警告はスキップしないでください。

- VCenter で EVC モードの設定を実行し、検証を再試行してください。
- クラスター展開は、2 回検証し展開を続行します。

コンバージド（HX220c/HX240c）ノードの追加に関する前提条件

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では、クラスターのストレージ容量が自動的に追加されます。

既存のストレージクラスターにコンバージド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ーの状態が正常であること。
- 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システム要件を満たしていること。
- 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。この設定には、VLAN ID、スイッチタイプ（vSwitch かどうか）、外部スイッチ VLAN タギング（EST）を使用する VLAN タギング、仮想スイッチタギング（VST）を使用する VLAN タギング、仮想分散スイッチ（vDS）があります。



(注) ストレージクラスターが領域不足の状態にある場合に、新しいノードを追加すると、システムは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時間ごとに実行される再調整に加えて行われるものです。

- 追加するノードが同じモデル (HX220 または HX240) のタイプ (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構成 (SED または非 SED) であること。また、キャパシティ ディスクの数が既存のクラスタ ノードと一致すること。
- HyperFlex クラスタですでに使用されているものとは異なる CPU ファミリ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 を伴うクラスタの設定」の項を参照してください。
- ノードのソフトウェアバージョンが、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。ソフトウェアのバージョンを確認するには、vCenter の [Storage Cluster Summary] タブに移動し、上部のセクションで HX Data Platform のバージョンを確認します。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 の現在のバージョン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。

- 新しいノードに 1 つ以上の有効な DNS サーバおよび NTP サーバが設定されていること。
- SSO または Auto Support を使用している場合は、ノードが SSO および SMTP サービス用に確実に設定されていること。
- 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

ステップ 1 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。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 2 HX ノードが工場出荷時に準備されたノードであることを確認します。

(注) 工場でノードが準備されていない場合、HX サーバを手動で準備する場合は、『Cisco HyperFlex Systems インストールガイド (VMware ESXi 向け)』の「Cisco HyperFlex System のカスタマイズされたインストール方法」の項を参照してください。

既存のクラスターへのコンバージドノードの追加



- (注) RESTful API を使用してクラスター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。

- a) Web ブラウザで、HX Data Platform 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。
[Accept] または [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に表示される HX Data Platform インストーラ インストーラの [Build 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 : root

パスワード (デフォルト): Cisco123

- (注) 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。インストールを継続するには、ユーザー提供の新規パスワードを作成する必要があります。

- c) EULA を読んで、[I accept the terms and conditions] チェックボックスをオンにし、[Login] をクリックします。

ステップ 2 [Workflow] ページで [Cluster Expansion] を選択します。

ステップ 3 [Credentials] ページで、次のフィールドに値を入力します。

クラスター作成を実行するために、必要な設定データとともに *JSON configuration* ファイルをインポートすることもできます。次の 2 つの手順は、JSON ファイルをインポートする場合はオプションです。インポートしない場合には、データを必須フィールドに手動で入力できます。

- (注) 初めてのインストールでは、ファクトリ プレインストール JSON ファイルの調達についてシスコの担当者にお問い合わせください。

1. [Select a file] をクリックして、使用する JSON ファイルを選択して設定をロードします。
[Use Configuration] を選択します。
2. Cisco UCS Manager 用にインポートした値が異なる場合は、[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。

フィールド	説明
[UCS Manager Credentials]	

フィールド	説明
[UCS Manager Host Name]	UCS Manager FQDN または IP アドレス たとえば <i>10.193.211.120</i> と入力します。
[User Name]	<admin> ユーザ名。
[Password]	<admin> パスワード。
[vCenter Credentials]	
[vCenter Server]	vCenter Server の FQDN または IP アドレス。 たとえば <i>10.193.211.120</i> と入力します。 (注) <ul style="list-style-type: none"> • vCenter Server は、クラスタが動作可能になる前に必要です。 • vCenter アドレスとクレデンシャルは、vCenter へのルートレベルの管理者権限が必要です。 • vCenter Server 入力は、ネストされた vCenter を構築する場合には省略可能です。詳細については、『Nested vCenter TechNote』を参照してください。
[User Name]	<admin> ユーザ名。 例 : <i>administrator@vsphere.local</i> 。
[Admin Password]	<root> パスワード。
[Hypervisor Credentials]	
[Admin User Name]	<admin> ユーザ名。 これはファクトリ ノードの root です。
[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) システムは、デフォルトのパスワード [<i>Cisco123</i>] 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。インストールを継続するには、ユーザー提供の新規パスワードを作成する必要があります。

ステップ 4 [Continue] をクリックします。[Cluster Expand Configuration] ページが表示されます。展開する HX クラスタを選択します。

展開する 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、[Management IP Address] フィールドのクラスタ管理アドレスの IP を入力します。

ステップ 5 [Server Selection] ページには、[Unassociated] タブの下に関連付けされていない HX サーバのリストと、[Associated] タブの下に検出されたサーバのリストが表示されます。[Unassociated] タブからサーバを選択し、HyperFlex クラスタに含めます。

HX サーバがこの一覧に表示されていない場合、Cisco UCS Manager を調べてそれらが検出されていることを確認します。

サーバごとに、[Actions] ドロップダウン リストを使用して、以下を設定できます。

- [Launch KVM Console]—HX Data Platform 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。
- [Disassociate Server] : サービスプロファイルをそのサーバから削除するには、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.
```

[Configure Server Ports] ボタンを使用することで、新しいすべての HX ノードを検出できます。一般に、設定を開始する前に Cisco UCS Manager でサーバポートを設定します。

ステップ 6 [Continue] をクリックします。[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。この情報は、既存のクラスタ構成に一致している必要があります。

ステップ 7 [UCSM Configuration] ページで、ネットワークごとに次のフィールドに値を入力します。

フィールド	説明
[VLAN Configuration]	
(注) 次の各ネットワークにそれぞれ個別のサブネットと VLAN を使用します。	
[VLAN for Hypervisor and HyperFlex management]	
[VLAN Name]	名前 : hx-inband-mgmt
[VLAN ID]	デフォルトの VLAN ID : 3091
[VLAN for HyperFlex Storage traffic]	
[VLAN Name]	名前 : hx-storage-data
[VLAN ID]	デフォルトの VLAN ID : 3092

フィールド	説明
[VLAN for VM vMotion]	
[VLAN Name]	名前 : hx-vmotion
[VLAN ID]	デフォルトの VLAN ID : 3093
[VLAN for VM Network]	
[VLAN Name]	名前: vm-network
[VLAN ID]	デフォルトの VLAN ID : 3094 ゲスト VLAN のカンマ区切りリスト。
[MAC Pool]	
[MAC Pool Prefix]	さらに 2 つの 16 進文字 (0-F) を追加することで、MAC プールプレフィックスを設定します。 たとえば、00:25:B5:A0 などです。
['hx-ext-mgmt' IP Pool for Out-of-Band CIMC]	
[IP Blocks]	HyperFlex ノードに指定された IP アドレスの範囲。 これは、ゲスト VLAN の値のカンマ区切りリストにできます。 例えば、10.193.211.124-127, 10.193.211.158-163
[Subnet Mask]	IP アドレスを制限して制御するために、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 と指定します。
[Gateway]	IP アドレス。 たとえば、10.193.0.1 と指定します。
[iSCSI Storage]	
(注) 将来的に任意の時点で外部ストレージの利用を希望する場合は、これを事前に設定する必要があります。	
[Enable iSCSI Storage] チェックボックス	iSCSI ストレージを設定するには、オンにします。
[VLAN A Name]	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。
[VLAN A ID]	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。

フィールド	説明
[VLAN B Name]	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。
[VLAN B ID]	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。
[FC Storage]	(注) 将来的に任意の時点で外部ストレージの利用を希望する場合は、これを事前に設定する必要があります。
[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、オンにします。
[WWxN Pool]	WW ノード名および 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。
[VSAN A Name]	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。デフォルトでは、 <code>hx-ext-storage-fc-a</code> に設定されています。
[VSAN A ID]	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。 注意 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 ゾーニングを使用する既存の VSAN ID をインストーラに入力すると、その VSAN ID の既存の環境でゾーニングが無効になります。
[VSAN B Name]	下位のファブリック インターコネクト (FI-B) の VSAN の名前。デフォルトでは、 <code>hx-ext-storage-fc-b</code> に設定されています。
[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。 注意 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 ゾーニングを使用する既存の VSAN ID をインストーラに入力すると、その VSAN ID の既存の環境でゾーニングが無効になります。

フィールド	説明
[Advanced]	
[UCS Firmware Version]	ドロップダウンリストから HX サーバに関連付ける UCS 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 Cisco HX データプラットフォームのリリースノート を確認してください。 たとえば 3.2 (1日) と入力します。
[HyperFlex Cluster Name]	特定のクラスター内の HX サーバのグループに適用される名前。これはユーザ定義の名前です。HyperFlex クラスター名は、簡単に識別できるようにサービスプロファイルにラベルを追加します。
[Org Name]	一意の <i>Org Name</i> を指定します。これにより、残りの UCS ドメインからの HyperFlex 環境の分離が保証されます。

(注) [Configuration] ペインで VLAN、MAC プール、および IP アドレス プールの情報を確認します。これらの VLAN ID は、環境に応じて変更できます。デフォルトでは、インストーラによって VLAN が非ネイティブとして設定されます。トランク設定を適切に適用することで、非ネイティブ VLAN に対応するようにアップストリーム スイッチを設定する必要があります。

ステップ 8 [Continue] をクリックします。[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
[Configure Common Hypervisor Settings]	
[Subnet Mask]	IP アドレスを制限して制御するために、サブネットマスクを適切なレベルに設定します。 たとえば、255.255.0.0 と指定します。
[Gateway]	ゲートウェイの IP アドレス。 たとえば、10.193.0.1 と指定します。

フィールド	説明
[DNS Server(s)]	DNS サーバの IP アドレス。 DNS サーバがない場合は、HX データ プラットフォーム インストーラの [Cluster Configuration] ページのいずれ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 ホストに静的 IP アドレスとホスト名のみを使用します。 (注) 複数の DNS サーバを提供する場合は、両方の DNS サーバが正しく入力されていることを慎重に確認し、カンマで区切ってください。
[Hypervisor Settings]	IP アドレスを順番に並べるには、[Make IP Addresses and Hostnames Sequential] を選択してください。 (注) ドラッグ アンド ドロップを使用してサーバを並べ替えることができます。
[Name]	サーバ名。
[Serial]	サーバのシリアル番号。
[Static IP Address]	すべての ESXi ホストに静的 IP アドレスとホスト名を入力します。
[Hostname]	ホスト名フィールドを空欄のままにしないでください。

ステップ 9 [Continue] をクリックします。[IP Addresses] ページが表示されます。[Add Compute Server] または [Add Converged Server] 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。

[Make IP Addresses Sequential] を選択して、IP アドレスを連続させます。IP アドレスの場合は、属するデータ ネットワークまたは管理ネットワークを指定します。

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 アドレスの次のフィールドに値を入力します。

フィールド	説明
[Management Hypervisor]	ESXi ホストとストレージクラスタ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。

フィールド	説明
[Management Storage Controller]	ストレージコントローラ VM とストレージクラスタ間の HX データ プラットフォーム 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クラスタ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静的 IP アドレスを入力します。
[Data Storage Controller]	ストレージコントローラ VM とストレージクラスタ間の HX データ プラットフォーム 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>[Hypervisor]、[Storage Controller VM (Management)]、[Hypervisor (Data)]、および [Storage Controller VM (Data)] 列の最初の行に IP アドレスを入力すると、HX Data Platform 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、[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
<p>[Controller VM Password]</p>	<p>デフォルトの管理者ユーザ名とパスワードがコントローラ VM に適用されます。VM は、コンバージドとコンピューティング専用のすべてのノードにインストールされています。</p> <p>重要</p> <ul style="list-style-type: none"> • 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は変更できません。 • 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 文字になる複合パスワードを指定してください。 • 作成するコントローラ VM および HX クラスタにユーザ定義のパスワードを指定できます。パスワードの文字と形式の制限事項については、『Cisco HX Data Platform Management Guide』の「Guidelines for HX Data Platform Special Characters」の項を参照してください。
<p>[Advanced Configuration]</p>	
<p>[Jumbo frames]</p> <p>[Enable Jumbo Frames] チェックボックス</p>	<p>ホスト vSwitch と vNIC、および各ストレージコントローラ VM 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にオンにします。</p> <p>デフォルト値は 9000 です。</p> <p>(注) MTU サイズを 9000 以外の値に設定するには、Cisco TAC にお問い合わせください。</p>

フィールド	説明
[Disk Partitions] [Clean up Disk Partitions] チェックボックス	<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、バックアップする必要があります。</p> <p>重要 工場出荷時のシステムにはこのオプションを選択しないでください。工場出荷時の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は、このオプションを選択して既存のデータとパーティションを削除します。</p>

ステップ 10 [Start] をクリックします。[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。
- ホストを vSphere Web Client の vCenter クラスタに追加します。
- HX Data Platform インストーラ で、[Retry Deploy] をクリックします。

ステップ 11 クラスタ展開が完了したら、[Launch HyperFlex Connect] をクリックしてストレージクラスタの管理を開始します。

(注) 既存のストレージクラスタにノードを追加する場合、スケジュールされた時間に自動再調整が行われるまで、クラスタには引き続き元のストレージクラスタと同じ HA 復元力があります。

再調整は通常、24 時間中にスケジュールされ、ノードの障害発生後の 2 時間、またはストレージクラスタの領域がなくなった場合に行われます。

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を再調整する必要がある場合は、次に示すストレージクラスタの再調整コマンドを手動で実行します。

ストレージクラスタ コントローラ VM コマンドラインから、次のコマンドを実行します。

1. # stcli rebalance start --force
2. 再調整のステータスをモニタするには
stcli rebalance status

ステップ 12 新しいノードがストレージクラスタに追加された後、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) vSphere 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] 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、vSphere HA に対し [Reconfigure] を選択します。

コンピューティング専用ノードの追加に関する前提条件

コンピューティング専用ノードは、HyperFlex クラスタの作成後にクラスタに追加できます。このノードは、追加のコンピューティングリソースを提供するために追加されます。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続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。
- 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。
- サービスプロファイルの関連付け後、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。この設定には、VLAN ID、スイッチタイプ (vSwitch かどうか)、外部スイッチ VLAN タギング (EST) を使用する VLAN タギング、仮想スイッチ タギング (VST) を使用する VLAN タギング、仮想分散スイッチ (vDS) があります。



(注) ストレージクラスタが領域不足の状態にある場合に、新しいノードを追加すると、システムは自動的にストレージクラスタを再調整します。これは、24時間ごとに実行される再調整に加えて行われるものです。

- 追加する新しいノードが HX クラスタですでに使用されているものとは異なる CPU ファミリを搭載している場合には、EVC を有効にしてください。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バージョンが、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。ソフトウェアのバージョンを確認するには、vCenter の [ストレージクラスタ概要] タブに移動し、上部のセクションで HX データプラットフォームのバージョンを確認します。必要に応じてアップグレードします。

- 新しいノードに 1 つ以上の有効な DNS サーバおよび NTP サーバが設定されていること。
- SSO または Auto Support を使用している場合は、ノードが SSO および SMTP サービス用に確実に設定されていること。
- ESXi インストールは、HX M4 コンピューティング専用 ノードの SD カードまたはフロントアクセス対応 SSD でサポートされています。USB フラッシュまたはフロントアクセス対応 SSD またはフロントアクセス対応 HDD に ESXi をインストールすると、再起動中にコントローラ VM を削除します。

コンピューティング専用ノードの準備

ステップ 1 サーバがサポート対象の HX サーバで、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。

- a) 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 インターコネクタ用の Cisco UCS Manager アドレスを入力します。
- b) [UCS Manager の起動 (Launch UCS Manager)] ボタンをクリックします。
- c) プロンプトが表示された場合は、Java をダウンロードして、インストールし、受け入れます。
- d) 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: `admin`

パスワード: `<admin password>`

ステップ 3 サーバを検索して、サーバがストレージクラスタと同じ FI ドメインに追加されており、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 リリース ノート](#)』を確認してください。

HX データ プラットフォーム インストーラの確認

ステップ 1 ストレージクラスタのすべてのノードと、ストレージクラスタに追加されてコンピューティング ノードと通信できるノードに、HX データ プラットフォーム 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 データ プラットフォーム インストーラがインストールされていない場合は、「**HX データ プラットフォーム 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専用ノードへの HX プロファイルの適用

Cisco UCS Manager では、ネットワーク ポリシーは 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する必要があります。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。

Cisco HX Data Platform サポート対象のバージョンの ESXi 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されている場合、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が関連付けを終了していることを確認します。

ステップ 1 Cisco HyperFlex の [cisco.com](#) ダウンロード サイトから ESXi の HX カスタム イメージをダウンロードします。「[ソフトウェアをダウンロードする](#)」を参照してください。

Cisco UCS Manager を通じてアクセスできるネットワーク 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、**[Servers] > [Service Profiles] > [Sub-Organizations] > [hx-cluster]** をクリックします。
- [hx-cluster]** を右クリックして、**[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、**[Virtual Media] > [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。
- [Virtual Media] > [Activate Virtual Devices]** の順に選択します。
これはポップアップ ウィンドウで開きます。
 - [Accept the session] > [Apply]** の順にクリックします。
- ステップ 6** [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。
 - [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 が含まれています。
- 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 [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。
 - [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** を押します。
 - [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。
 - Enter** キーを押して、選択します。
- 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。短い待機期間後に自動的に消える警告が表示されても問題はありません。 **ESXi DCUI** が完全に表示され、インストールの終了がシグナリングされるのを待機します。
- 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、[Continue] をクリックします。[Retry Hypervisor Configuration] をクリックして、クラスタ展開の残りを完了します。
-

既存のクラスターへのコンピューティング専用ノードの追加

既存の HyperFlex システム クラスターに 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ー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。

- a) Web ブラウザで、HX Data Platform 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。
[Accept] または [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に表示される HX Data Platform インストーラ インストーラの [Build 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 : root

パスワード (デフォルト): Cisco123

(注) 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。インストールを継続するには、ユーザー提供の新規パスワードを作成する必要があります。

- c) EULA を読んで、[I accept the terms and conditions] チェックボックスをオンにし、[Login] をクリックします。

ステップ 2 [Workflow] ページで [Cluster Expansion] を選択します。

ステップ 3 [Credentials] ページで、次のフィールドに値を入力します。

クラスター作成を実行するために、必要な設定データとともに *JSON configuration* ファイルをインポートすることもできます。次の 2 つの手順は、JSON ファイルをインポートする場合はオプションです。インポートしない場合には、データを必須フィールドに手動で入力できます。

(注) 初めてのインストールでは、ファクトリ プレインストール JSON ファイルの調達についてシスコの担当者にお問い合わせください。

1. [Select a file] をクリックして、使用する JSON ファイルを選択して設定をロードします。
[Use Configuration] を選択します。
2. Cisco UCS Manager 用にインポートした値が異なる場合は、[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。

フィールド	説明
[UCS Manager Credentials]	
[UCS Manager Host Name]	UCS Manager FQDN または IP アドレス たとえば <i>10.193.211.120</i> と入力します。
[User Name]	<admin> ユーザ名。
[Password]	<admin> パスワード。
[vCenter Credentials]	
[vCenter Server]	vCenter Server の FQDN または IP アドレス。 たとえば <i>10.193.211.120</i> と入力します。 (注) <ul style="list-style-type: none"> • vCenter Server は、クラスタが動作可能になる前に必要です。 • vCenter アドレスとクレデンシヤルは、vCenter へのルートレベルの管理者権限が必要です。 • vCenter Server 入力は、ネストされた vCenter を構築する場合には省略可能です。詳細については、『Nested vCenter TechNote』を参照してください。
[User Name]	<admin> ユーザ名。 例 : <i>administrator@vsphere.local</i> 。
[Admin Password]	<root> パスワード。
[Hypervisor Credentials]	
[Admin User Name]	<admin> ユーザ名。 これはファクトリ ノードの root です。

フィールド	説明
[Admin Password]	<p><root> パスワード。</p> <p>デフォルトのパスワードは、ファクトリ ノードの Cisco123 です。</p> <p>(注) 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。インストールを継続するには、ユーザー提供の新規パスワードを作成する必要があります。</p>

ステップ 4 [Continue] をクリックします。[Cluster Expand Configuration] ページが表示されます。展開する HX クラスターを選択します。

展開する HX クラスターが見つからない場合、もしくはクラスターのロードに時間がかかる場合、[管理 IP アドレス フィールド] のクラスター管理アドレスの IP を入力します。

ステップ 5 [Continue] をクリックします。[Server Selection] ページが表示されます。[Server Selection] ページの [Associated] タブに、接続済みのすべての HX サーバが一覧されます。これらのサーバは選択しないでください。[Unassociated] タブで、クラスターに追加するサーバを選択します。

ステップ 6 [Continue] をクリックします。[UCS Manager 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、必須フィールドには、既存の HX クラスターからインポートした設定データが取り込まれているはずですが、クラスターに追加する対象のサーバがアソシエートされていない場合は、それらのサーバを選択して [Continue] をクリックします。
 - 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。このページで適切な設定を使用することを確認します。

各ネットワークに以下の情報を入力します:

フィールド	情報
[VLAN for ESXi and HyperFlex management]	
[VLAN Name]	名前 : hx-inband-mgmt
[VLAN ID]	デフォルトの VLAN ID : 3091
[VLAN for HyperFlex Storage traffic]	
[VLAN Name]	名前 : hx-storage-data
[VLAN ID]	デフォルトの VLAN ID : 3092
[VLAN for VM vMotion]	

フィールド	情報
[VLAN Name] [VLAN ID]	名前 : hx-vmotion デフォルトの VLAN ID : 3093
[VLAN for VM Network]	
[VLAN Name] [VLAN ID]	名前 : hx-vm-network デフォルトの VLAN ID : 3094
[MAC Pool]	
[MAC Pool Prefix]	たとえば、00:25:B5:99 などとします (99 はデフォルトです。この値はユーザ環境に応じて設定できます)。
hx-ext-mgmt IP Pool for Out-of-Band CIMC	
[IP Blocks]	HyperFlex ノードに指定された IP アドレスの範囲。これは、ゲスト VLAN の値のカンマ区切りリストにできます。 たとえば、10.193.211.124-127、10.193.211.158-163、255.255.255.0 などです。 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 と指定します。
[Subnet]	IP アドレスを制限して制御するために、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 と指定します。
[Default gateway]	IP アドレス。 たとえば、10.193.0.1 と指定します。
[Advanced]	
[UCS 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 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 Cisco HX データ プラットフォームのリリースノート を確認してください。 たとえば 3.2 (1d) と入力します。

フィールド	情報
[HyperFlex Cluster Name]	特定のクラスター内の HX サーバのグループに適用される名前。これはユーザ定義の名前です。HyperFlex クラスター名は、ラベルを識別しやすいようにサービス プロファイルに追加します。

(注) [Configuration] ペインで VLAN、MAC プール、ANDIP アドレス プールの情報を確認します。これらの VLANID は、環境に応じて変更できます。デフォルトでは、インストーラによって VLAN が非ネイティブとして設定されます。トランク設定を適切に適用することで、非ネイティブ VLAN に対応するようにアップストリーム スイッチを設定する必要があります。

ステップ 7 [Continue] をクリックします。[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
[Configure Common Hypervisor Settings]	
[Subnet Mask]	IP アドレスを制限して制御するために、サブネット マスクを適切なレベルに設定します。 たとえば、255.255.0.0 と指定します。
[Gateway]	ゲートウェイの IP アドレス。 たとえば、10.193.0.1 と指定します。
[DNS Server(s)]	DNS サーバの IP アドレス。 DNS サーバがない場合は、HX データ プラットフォーム インストーラの [Cluster Configuration] ページのいずれ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 ホストに静的 IP アドレスとホスト名のみを使用します。 (注) 複数の DNS サーバを提供する場合は、両方の DNS サーバが正しく入力されていることを慎重に確認し、カンマで区切ってください。
[Hypervisor Settings]	
IP アドレスを順番に並べるには、[Make IP Addresses and Hostnames Sequential] を選択してください。 (注) ドラッグ アンド ドロップを使用してサーバを並べ替えることができます。	
[Name]	サーバ名。

フィールド	説明
[Serial]	サーバのシリアル番号。
[Static IP Address]	すべての ESXi ホストに静的 IP アドレスとホスト名を入力します。
[Hostname]	ホスト名フィールドを空欄のままにしないでください。

ステップ 8 [Continue] をクリックします。[IP Addresses] ページが表示されます。[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、[Make IP Addresses Sequential] を選択します。

フィールド	情報
[Management Hypervisor]	ESXi ホストとストレージクラスタ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。
[Management Storage Controller]	なし。
[Data Hypervisor]	ESXi ホストとストレージクラスタ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静的 IP アドレスを入力します。
[Data Storage Controller]	なし。
Controller VM	コントローラ VM が既存の HX クラスタにインストールされている場合、それらのコントローラ 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。 (注) コントローラ VM 名は変更できません。既存のクラスタ パスワードを使用してください。

ステップ 9 [Start] をクリックします。[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 Data Platform 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. [General] タブで、[Unbind from the Template] をクリックします。

3. 作業中のウィンドウで、[Storage] タブをクリックします。[Local Disk Configuration Policy] サブ タブをクリックします。
4. [Actions] 領域で、次のように選択します。[Change Local Disk Configuration Policy] > [Create Local Disk Configuration Policy]。
5. [Create Local Disk Configuration Policy] で、ポリシーの名前を入力し、デフォルトとして残りの部分を保持します。[OK] をクリックします。
6. [Actions] 領域の [Change Local Disk Configuration Policy] 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 Data Platform インストーラ UI に戻り、[Retry UCSM Configuration] をクリックします。

(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、「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。

1. vSphere クライアントに追加する ESXi ホストにログインします。
2. コントローラ VM の電源をオフにします。
3. ホストを vSphere Web Client の vCenter クラスターに追加します。
4. HX インストーラで、[Retry Deploy] をクリックします。

ステップ 10 インストールが完了したら、[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 11 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、HA が追加されたノードを認識できるようになります。

- a) VMware vSphere クライアントにログインします。
- b) [Home] > [Hosts and Clusters] > [Datacenter] > [Cluster] > [Host] の順に選択します。
- 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。

クラスター展開の障害の解決

エラー ダイアログボックスを受信し、ストレージクラスターの展開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 [Edit Configuration] : [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ます。

ステップ 2 [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 [Continue] : エラーが発生している障害を無視して、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) [Continue] ボタンは、障害について把握していて、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選択します。

ロジカルアベイラビリティゾーンの有効化

HyperFlex クラスターを正常に設定したら、以下のコマンドを参照してロジカルアベイラビリティゾーン (LAZ) を有効化または無効化してください。



重要 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。

クラスターのフレッシュインストールの場合、最良の結果を得るために、クラスターの作成中は LAZ を有効にしておくことをお勧めします。

コマンド	説明
<code>stcli cluster get-zone</code>	ゾーンが有効になっているかどうか確認します。
<code>stcli cluster set-zone --zone 0</code>	ゾーンを無効にします。

コマンド	説明
<pre>stcli cluster set-zone --zone 1 stcli rebalance start</pre>	<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>重要</p> <ul style="list-style-type: none"> ゾーン分割を有効化せずに作成されたクラスターは、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。 ゾーンを有効化して作成したら、rebalance start コマンドを実行する必要があります。 再調整アクティビティをトリガーすると、クラスター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、クラスター内の IO パフォーマンスが低下する可能性があります。
<pre>stcli cluster set-zone --zone 1 --numzones <integer-value> 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>重要 ゾーンを有効化および作成したら、rebalance start コマンドを実行する必要があります。</p>



第 11 章

混在 CPU を伴うクラスタの設定

この章では、異なる Intel CPU バージョンを使用する複数の HX ノードを同じ FI に追加する方法を説明します。

- [概要 \(147 ページ\)](#)
- [混合 CPU を使用するための前提条件 \(147 ページ\)](#)
- [EVC モードとの CPU 互換性 \(148 ページ\)](#)
- [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 \(148 ページ\)](#)

概要

HyperFlex は、同じファブリック インターコネクタで Intel v3 および Intel v4 CPU をサポートします。Intel v3 および Intel v4 CPU 間で仮想マシンを移行するには、VMware Enhanced vMotion Compatibility (EVC) を有効にします。EVC を有効にした後、下位モデルの CPU の機能が基準となるように、HyperFlex クラスタ内のすべてのホストを設定します。仮想マシンがどのホスト上で実行されているかに関わらず、すべての仮想マシンに同一の CPU 機能が公開されるため、仮想マシンを HyperFlex クラスタ内のホスト間で移行できます。これにより、ホストの基になるハードウェアが異なる場合でも、vMotion の CPU 互換性が確保されます。

混合 CPU を使用するための前提条件

- CPU が EVC 対応のクラスタ内の単一のベンダーからのみ使用できること。この場合、別のベンダーによるホストを EVC 対応のクラスタに追加することはできません。
- EVC 対応のクラスタで、異なるリビジョン番号 (v2、v3、または v4) の Xeon E3 または Xeon E5 ファミリの Intel プロセッサが使用されていること。この場合、EVC ベースラインが必要になります。
- BIOS で高度な仮想化 CPU 機能が有効であること (利用できる場合)。有効にしないと、EVC を有効にする際に、EVC 互換性チェックで特定の CPU に存在すると想定される機能を検出できないため、問題が発生することがあります。

- 以下のシナリオでは、仮想マシンが EVC クラスタに含まれているとしても、vMotion を使用した仮想マシンの移行が失敗する場合があります。
 - 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。
 - 仮想マシンがソース ホストとターゲット ホストで共有されるストレージに存在しない場合。

EVC モードとの CPU 互換性

CPU との互換性がある EVC (Enhanced vMotion Compatibility) モードを判別するには、『[VMware Compatibility Guide](#)』を参照してください。サーバモデルまたは CPU ファミリを検索し、[CPU Series] 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、同じ名前を持つプロセッサで利用できる機能と密接に対応します。

vSphere Web クライアントの使用

1. vSphere Web Client ナビゲータから、[Hosts and Clusters] > [HX Cluster] > [Summary] を選択します。[Summary] タブでは、EVC が有効になっているかどうかが表示され、有効になっている場合はホストの現在の EVC モードが表示されます。
2. EVC モードの横にある青いアイコンをクリックすると、そのホストでサポートされるすべての EVC モードの一覧が表示されます。

VMware 共有ユーティリティ ツールの使用

VMware には、互換性のある EVC モードおよびその他の CPU 機能を表示する、無料の CPU 識別ユーティリティが用意されています。このユーティリティを[共有ユーティリティ](#)からダウンロードして、ISO イメージからホストをブートすることができます。

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

EVC を有効にして、クラスタ内のホスト間で vMotion による移行が可能になるよう確認します。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。EVC モードは、クラスタの拡張中でも中断することなく有効にできます。



- (注)
- EVC はデフォルトで無効になっています。VMware EVC のクラスタ設定で 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。さらに詳細については、VMware KB の記事「[EVC and CPU Compatibility FAQ \(1005764\)](#)」を参照してください。

ここでは、コンピューティング ノード内の古い CPU を既存の HyperFlex クラスタに追加する場合に必要な手順について説明します。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。

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。

応答の例：

```
Operational Status: Online
Resiliency Status: Healthy
```

• **コントローラ VM の使用方法**

コントローラ VM で、`#stcli cluster info` コマンドを実行します。

応答の例：

```
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切ります。

ステップ 3 1 台のストレージ 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機します。

ステップ 4 全ストレージ コントローラ VM をシャットダウンします。

- a) vSphere Web Client ナビゲータから、[VMs and Templates]>[vCenter server]>[Datacenter]>[Discovered virtual machine]>[Virtual Machines]>[controller_vm] を選択します。
- b) **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。

- a) vSphere Web Client ナビゲータから、[Hosts and Clusters]>[Datacenter]>[HX Cluster]>[node] の順に選択します。
- b) 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 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
- vSphere Web Client ナビゲータから、**[Hosts and Cluster] > [Datacenter] > [HX Cluster]** を選択します。
 - EVC を有効にするクラスタを選択します。[Work] ペインで、[Manage] または [Configure] タブをクリックします。[VMware EVC] を選択します。
 - [Edit] ボタンをクリックし、希望の EVC モードを選択します。[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。
- vSphere Web Client ナビゲータから、**[Hosts and Clusters] > [Datacenter] > [HX Cluster] > [node]** の順に選択します。
 - 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 Maintenance Mode] メニューを使用しないでください。
- ステップ 8** コントローラ VM は、ホストがメンテナンス モードになった後、自動的に電源が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。
- vSphere Web Client ナビゲータから、**[VMs and Templates] > [vCenter server] > [Datacenter] > [ESXi Agents] > [Virtual Machines] > [controller_vm]** を選択します。
 - [controller_vm] を右クリックするか、[Actions] メニューから選択します。**[Power] > [Power On or Power] > [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ます。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。
-



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 \(151 ページ\)](#)
- [Cisco HyperFlex Systems が事前設定されていない場合のインストールおよび設定のワークフロー \(151 ページ\)](#)
- [VMware ESXi をインストールします。 \(152 ページ\)](#)

概要

この章では、インストール手順に進む前に、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は、次のシナリオで使用できます。

- コンピューティング専用ノードを HyperFlex クラスタに追加する。
- Cisco HyperFlex System を再導入する。

実行するタスクは、事前設定された HyperFlex Systems を導入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な新しいタスクは、VMware ESXi のインストールです。

Cisco HyperFlex Systems が事前設定されていない場合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 Systems 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。

VMware ESXi をインストールします。

ステップ 1 vCenter でクラスタを削除して、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 データ プラットフォーム 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 Cisco HX Data Platform インストーラ を起動してサインインします。

- a) [Customized Workflow] を選択します。
- b) [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 インストール ガイド (VMware ESXi 向け)』の「Configuring Cisco UCS Manager and HX Data Platform」の項に記載されている手順に従います。

ステップ 4 vMedia メソッドを使用して、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 インストーラ によって、ESXi サーバに静的 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 Cisco HX Data Platform インストーラ を再度起動します。

- a) [Customized Workflow] を選択します。
- b) [Run ESX Configuration]、[Deploy HX Software]、および [Create HX Cluster] を選択します。

ウィザードで必ず [Delete Existing Partitions] を選択してください。

VMware ESXi をインストールします。

サーバには、サポート対象バージョンの VMware ESXi が必要です。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。

VMware ESXi イメージを Cisco HyperFlex Data Platform の [ソフトウェア ダウンロード](#) ページからダウンロードします。Cisco UCS Manager を通じてアクセスできるネットワーク 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。

次に例を示します。

HX-Vmware-ESXi-60U2-4192238-Cisco-Custom-6.0.2.3.iso

次のタスク

- Cisco UCS Manager 経由で vMedia およびブート ポリシーを設定します。
- 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 経由で vMedia およびブート ポリシーの変更を元に戻します。

Cisco UCS Manager を使用した 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

Cisco 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、標準クラスタに [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 [Navigation] ペインで、[Servers] タブをクリックします。
- ステップ 2 [Servers] > [Policies] > [root] > [Sub-Organizations] > [hx-cluster] > [vMedia Policies] の順に展開します。
- ステップ 3 [vMedia Policy HyperFlex] をクリックします。
- ステップ 4 設定ペインで [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 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 [Image Variable Name] として [None] を選択します。
- ステップ 10 [Remote File] 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 [Remote Path] に **/images/** と入力します。
- ステップ 12 [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、[Servers] > [Service Profile Templates] > [root] > [Sub-Organizations] > [hx-cluster] > [Service Template hx-nodes] の順に選択します。

- ステップ 14 [vMedia Policy] タブをクリックします。
- ステップ 15 [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 Policy] を選択して、[OK] を 2 回クリックします。
- ステップ 17 [Servers] > [Policies] > [root] > [Sub-Organizations] > [hx-cluster] > [Boot Policy HyperFlex] の順に選択します。
- ステップ 18 ナビゲーション ペインで、[CIMC Mounted vMedia] というセクションを展開します。
- ステップ 19 [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 [Boot Order] リストで [CIMC Mounted CD/DVD] エントリを選択し、[Move Up] ボタンを何度かクリックして [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 [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 コンソールのオープン

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 [Navigation] ペインで [Servers] をクリックします。
- ステップ 2 [Servers] > [Service Profiles] > [Root] > [Sub-Organizations] > [hx-cluster] > [rack-unit-number] を展開します。
- ステップ 3 [Work] ペインで、[General] タブをクリックします。
- ステップ 4 [Actions] 領域の [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 [Continue] をクリックします。間もなくしてリモートの [KVM Console] ウィンドウが表示され、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追加のサーバごとに、ステップ 2 ~ 4 を繰り返します。

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ためにサーバを再起動します。

サーバを再起動するには、以下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 [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Equipment] > [Rack Mounts] > [Servers] の順に展開します。

ステップ 3 [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 右クリックして [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 [Power Cycle] を選択し、[OK] をクリックします。

これで、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、無視しても問題ありません。

vMedia ポリシーおよびブート ポリシーの変更の取り消し

サーバがブートループに陥ったり、インストール用の ISO ファイルから常に起動したりしないようにするには、ブート ポリシーへ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 ファイルから起動し、インストールプロセスが開始されていることを確認します。

ステップ 1 Cisco UCS Manager の [Navigation] ペインで [Servers] をクリックします。

ステップ 2 [Servers] > [Policies] > [Root] > [Sub-Organizations] > [hx-cluster_name] > [Boot Policies] > [Boot Policy HyperFlex] の順に展開します。

ステップ 3 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [Actions] 領域で、[CIMC Mounted CD/DVD] をクリックします。

ステップ 5 [Boot Order] リストから [CIMC Mounted CD/DVD] エントリを選択し、[Delete] をクリックします。

ステップ 6 [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

以前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 クラスタを展開してください。詳細については、「[クラスタ展開のガイドライン](#)」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の一部になっていて、何かを修正するためにイメージが再作成された場合は、Cisco TAC に連絡して指示を受けてください。