



Cisco HyperFlex システム リリース 3.5 インストール ガイド (VMware ESXi 向け)

初版：2018年4月13日

最終更新：2020年6月3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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2018–2020 Cisco Systems, Inc. All rights reserved.



目次

第 1 章	HyperFlex 保留リリース 1
	HyperFlex 保留リリース 1

第 2 章	新機能および変更された機能に関する情報 3
	このリリースの新規情報および変更情報 3

第 3 章	概要 5
	Cisco HyperFlex HX シリーズ システム 5
	Cisco HyperFlex HX シリーズ システム コンポーネント 5
	Cisco HyperFlex HX シリーズ システム 設定オプション 7
	Cisco HyperFlex HX シリーズ システム 管理コンポーネント 8
	Cisco HyperFlex Connect ユーザ インターフェイスとオンライン ヘルプ 9
	[Dashboard] ページ 11
	[Operational Status] ダイアログボックス 13
	[Resiliency Health] ダイアログボックス 14

第 4 章	インストールの前提条件 17
	HyperFlex ソフトウェアのバージョン 17
	必要なハードウェア ケーブル 19
	ホスト要件 20
	ディスクの要件 20
	ブラウザの推奨事項 - 3.5(x) リリース 23
	ポート要件 24
	HyperFlex 外部接続 32

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	33
ネットワーク設定	35
VLAN および vSwitch の要件	37
Cisco UCS の要件	38
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 5 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 インターコネクットの設定	48
Cisco UCS Manager GUI を使用したプライマリ ファブリック インターコネクットの設定	49
Cisco UCS Manager GUI を使用したセカンダリ ファブリック インターコネクットの設定	51
CLI によるプライマリ ファブリック インターコネクットの設定	53
CLI による従属ファブリック インターコネクットの設定	54
コンソール設定の確認	55
Cisco UCS ファブリック インターコネクットへの HX シリーズ サーバの接続	57
概要	57
ファブリック インターコネクットへのコンバージド ノードの接続	57
直接接続モードのクラスタ セットアップの物理的な接続の図	59
ファブリック インターコネクットへのコンピューティング専用ノードの接続	60

第 6 章

Cisco HyperFlex Systems の設定	63
インストール ワークフロー	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	64
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	67

Syslog の設定	68
HyperFlex クラスタの設定と展開	69
HyperFlex GUI で使用される共通タスクの手順	69
HyperFlex サーバの関連付け	70
UCS Manager の設定	71
ハイパーバイザの設定	75
IP アドレスの設定	77
HyperFlex クラスタの設定	79
GPU を搭載した HyperFlex ノードの設置	83
HX データ プラットフォーム インストーラ ナビゲーション エイド ボタン	84
警告およびエラー メッセージ	84

 第 7 章

HyperFlex Data Platform でのライセンス設定 87

スマート ライセンスと HyperFlex	87
接続環境のライセンス管理	91
コントローラ VM を介してスマート ソフトウェア ライセンスとともにクラスタを登録する	91
スマート ライセンスからのクラスタの登録解除	92
スマート ライセンス承認の更新	93

 第 8 章

HyperFlex ハードウェア アクセラレーション カードの設定 95

HyperFlex ハードウェア アクセラレーション カードの概要	95
Install HyperFlex Hardware Acceleration Cards	96
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	97
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	99
HyperFlex クラスタの設定と展開	101
クレデンシャルの入力	101
HyperFlex サーバの関連付け	103
UCS Manager の設定	105
ハイパーバイザの設定	108
IP アドレスの設定	110

HyperFlex クラスタの設定	112
HyperFlex ハードウェア アクセラレーション カードの取り付けの確認	116
HyperFlex ハードウェア アクセラレーション カードのトラブルシューティング	117
HyperFlex ハードウェア アクセラレーション カードのに関する追加情報	117

第 9 章

クラスタ設定後のタスク	119
クラスタ設定後のガイドライン	119
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	120
インストール後のスクリプトの実行	121
ESXi ホストルート パスワードの変更	123
ストレージコントローラ パスワードの変更	124
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	124
ストレージクラスタでのデータストアの追加	125
HA ハートビートの設定	125
HyperFlex の Auto Support と Smart Call Home	126
HX Connect を使用した自動サポートの構成	128
CLI を使用した通知設定の構成	129
データ コレクションの Smart Call Home の構成	130
自己署名の証明書を CA 署名の証明書で置き換える	133
レプリケーション ペアリング	134
プライベート VLAN の追加	134
プライベート VLAN の概要	134
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	135
ESX ホストでのプライベート VLAN の設定	136
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	136
vSphere 標準スイッチでの VMNIC の削除	137
vSphere 分散スイッチの作成	137
vSphere 分散スイッチでのプライベート VLAN の作成	138
分散ポート グループでのプライベート VLAN の設定	138
分散型仮想スイッチと Cisco Nexus 1000v	139
HX Data Platform での vCenter のホスト	140

AMD GPU の展開 140

第 10 章

複数の HX クラスタの設定 143

複数のクラスタの設定 143

第 11 章

Cisco HyperFlex システム クラスタの展開 145

クラスタ展開のガイドライン 145

ESXi インストール ガイドライン 146

混合 M4/M5 クラスタを作成する場合の前提条件 146

混合クラスタ展開のガイドライン 147

混合クラスタ展開中の手順 148

コンバージド (HX220c/HX240c) ノードの追加に関する前提条件 149

コンバージド ノードの準備 150

既存のクラスタへのコンバージド ノードの追加 150

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 161

コンピューティング専用ノードの準備 162

HX データ プラットフォーム インストーラの確認 163

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 163

コンピューティング ノードへの VMware ESXi のインストール 163

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 165

クラスタ展開の障害の解決 173

ロジカルアベイラビリティ ゾーンの有効化 173

論理可用性ゾーンの要件および制限事項 174

ゾーンより小さいノードを含むクラスタの拡張 177

第 12 章

混在 CPU を伴うクラスタの設定 179

概要 179

混合 CPU を使用するための前提条件 179

EVC モードとの CPU 互換性 180

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 180

均一クラスタへの新世代サーバの追加 181

既存のクラスタへの混合または旧世代サーバの追加 181

第 13 章

Cisco HyperFlex Systems のカスタマイズされたインストール方法 185

概要 185

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 185

VMware ESXi をインストールします。 186

Cisco UCS Manager を使用した vMedia およびブート ポリシーの設定 187

リモート KVM コンソールのオープン 188

サーバの再起動 189

vMedia ポリシーおよびブート ポリシーの変更の取り消し 190

付録 A :

HX サーバ QoS システム クラスの設定 191

HX サーバ用の VLAN の作成 193

MAC アドレス プールの作成 194

QoS ポリシーの作成 196

HX サーバ用の vNIC テンプレートの作成 198

vSwitch の設定 203

仮想分散スイッチ (VDS) または Cisco Nexus 1000v (N1Kv) への vMotion ネットワークの移行 204

Stats Daemon のリセット 207

HyperFlex HX シリーズ サーバ ディスクの詳細 207

HyperFlex をインストールする際の有効性検査 208



第 1 章

HyperFlex 保留リリース

- [HyperFlex 保留リリース \(1 ページ\)](#)

HyperFlex 保留リリース

Cisco HyperFlex Data Platform リリース 3.5(2c) は、ダウンロードできなくなりました。[Cisco ソフトウェア ダウンロード](#) サイトで、3.5(2g) または最新の推奨リリースにアップグレードすることをお勧めします。

詳細については、『[CSCvp90129 のソフトウェア遅延通知](#)』を参照してください。



第 2 章

新機能および変更された機能に関する情報

- [このリリースの新規情報および変更情報 \(3 ページ\)](#)

このリリースの新規情報および変更情報

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

表 1: Cisco HX Data Platform の新機能と動作の変更点

機能	説明	リリースが追加されました	参照先
CSCvp90129 に対するソフトウェアの延期通知の発行	Cisco HyperFlex Data Platform リリース 3.5(2c) は、ダウンロードできなくなりました。	2020 年 1 月 14 日	HyperFlex 保留リリース (1 ページ)
ESXi 6.7 U2 サポート	VMware vSphere Hypervisor (ESXi) 6.7 U2 の HyperFlex Data Platform をインストールするためのサポートを提供します。	リリース 3.5 (2c)	HyperFlex ソフトウェアのバージョン

機能	説明	リリースが追加されました	参照先
ESXi 6.7 U1 サポート	VMware vSphere Hypervisor (ESXi) 6.7 U1 の HyperFlex Data Platform をインストールするためのサポートを提供します。	リリース 3.5 (2a)	HyperFlex ソフトウェアのバージョン
HX ハードウェアアクセラレーションカード	HyperFlex ノード上の HyperFlex ハードウェアアクセラレーションカードのインストール、ポストインストール、およびトラブルシューティングの詳細と、初期クラスタの設定について説明します。	リリース 3.5 (2a)	「 HyperFlex ハードウェアアクセラレーションカードの概要 」の章。



第 3 章

概要

この章では、Cisco HyperFlex システム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 \(5 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システム コンポーネント \(5 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システム 設定オプション \(7 ページ\)](#)
- [Cisco HyperFlex HX シリーズ システム 管理コンポーネント \(8 ページ\)](#)
- [Cisco HyperFlex Connect ユーザ インターフェイスとオンラインヘルプ \(9 ページ\)](#)

Cisco HyperFlex HX シリーズ システム

Cisco HyperFlex HX シリーズ システム は、完全内包型の仮想サーバプラットフォームを通じて、コンピューティング、ストレージ、ネットワークの 3 つのレイヤと強力な Cisco HX Data Platform ソフトウェア ツールを結合し、シングルポイント接続による簡素化された管理を実現します。Cisco HyperFlex HX 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 を設定するには、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。

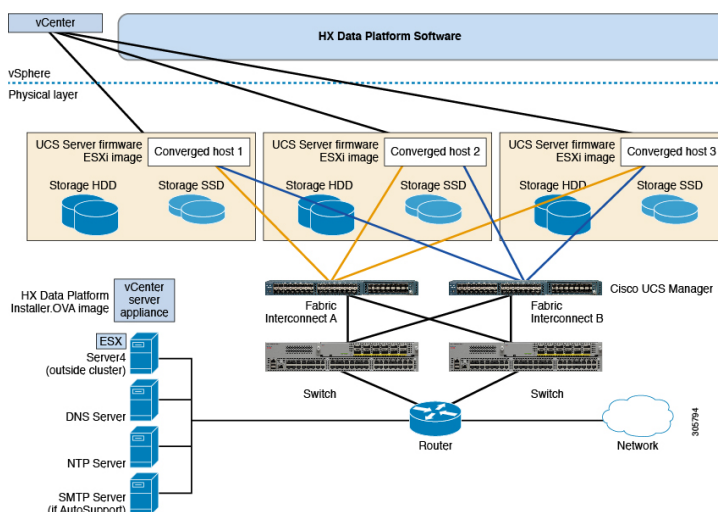
このドキュメントでは、購入して Cisco HyperFlex System の一部として導入された FI のことを **HX FI ドメイン**とも呼んでいます。サポートされているファブリック インターコネク トは次のとおりです。

- 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

3068304

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

3068308

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 を開くことです。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、一貫性のある設定が得られ、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ージドソフトウェアアプライアンスです。これにより、ネットワークストレージの必要性がなくなり、VMware vSphere およびその既存の管理アプリケーションと緊密に統合し、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ージ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、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 にも事前設定済みの vCenter Server からアクセスして、すべてのストレージのタスクを実行します。vCenter は、VMware vMotion、DRS、HA、および vSphere レプリケーションなどの主要なキー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 2: 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 (User)	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は、テーブルに表示される内容に影響を与える次の 3 つのフィールドのうち 1 つ以上を提供します。

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。HyperFlex (HX) Connect では、ほとんどのアクションの実行に管理者権限が必要です。

HX ストレージクラスタのステータスの概要が表示されます。これは Cisco HyperFlex Connect にログイン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>[情報 (Information)] ⓘ をクリックして、HX ストレージクラスタ名とステータスデータにアクセスします。</p>
[Cluster License Status (クラスターライセンスの状態)] セクション	<p>HX ストレージクラスタに初めてログインしたとき、または HX ストレージクラスタ ライセンスが登録されるまでに、次のリンクが表示されます。</p> <p>クラスタライセンスが登録されていないリンク : HX ストレージクラスタが登録されていない場合に表示されます。クラスタライセンスを登録するには、このリンクをクリックし、[Smart Software Licensing Product Registration (スマートソフトウェアライセンス製品登録)] 画面で製品インスタンス登録トークンを指定します。製品インスタンス登録トークンを取得する方法の詳細については、『Cisco HyperFlex システムインストールガイド』の「スマートライセンスへのクラスタの登録」セクションを参照してください。</p>
[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、復元力ステータスと、レプリケーションおよび障害データにアクセスします。</p>
[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	<p>クラスタのシステム日付および時刻。</p>

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は、テーブルに表示される内容に影響を与える次の3つのフィールドのうち1つ以上を提供します。

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、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 ストレージクラスの名前です。

UI 要素	基本情報
[Cluster Status] フィールド	<ul style="list-style-type: none"> • [オンライン (Online)] : クラスタの準備ができています。 • [オフライン (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。
[Data-at-rest encryption capable] フィールド	<ul style="list-style-type: none"> • 対応可 • [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。

[閉じる (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。

名前	説明
[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。

[閉じる (Close)] をクリックします。



第 4 章

インストールの前提条件

- [HyperFlex ソフトウェアのバージョン](#) (17 ページ)
- [必要なハードウェア ケーブル](#) (19 ページ)
- [ホスト要件](#) (20 ページ)
- [ディスクの要件](#) (20 ページ)
- [ブラウザの推奨事項 - 3.5\(x\) リリース](#) (23 ページ)
- [ポート要件](#) (24 ページ)
- [HyperFlex 外部接続](#) (32 ページ)
- [ファブリック インターコネクトのアップリンクのプロビジョニング](#) (33 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](#) (38 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)

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。

- HyperFlex は、UCS Manager および UCS Server Firmware バージョン 4.0(4a)、4.0(4b)、4.0(4c) をサポートしていません。



重要 これらのファームウェアバージョンにアップグレードしないでください。

これらの UCS Manager のバージョンにアップグレードしないでください。

- 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(3k)、3.2(3i)、または 4.0(2d) 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、推奨される UCS ファームウェアバージョンがインストールされていることを確認してください。



重要 複数の Nvidia GPU が存在する場合に Cisco UCS Manager 4.0 (2a) または 4.0 (2b) をアップグレードする場合は、GPU を削除してから、アップグレードと再インストールを実行してください。詳細については、[CSCvo13678](#)を参照してください。



重要 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)、B (ブレードサーバ) および C (ラックサーバ) パンドルが、すべての SED M4/M5 システムに対して Cisco UCS Manager バージョン 4.0(2b) 以降です。詳細については、[CSCvh04307](#)を参照してください。SED ベース HyperFlex システムでは、すべてのクラスタが HyperFlex リリース 3.5(2b) 以降であることも確認します。詳細については、[Field Notice \(70234\)](#) および [CSCvk17250](#) を参照してください。

- 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『[VMware ESXi 向け Cisco HyperFlex システム インストール ガイド](#)』を参照してください。
- 推奨される FI/サーバファームウェアの [リリース ノート](#)を確認してください。

表 3: M4/M5サーバ (SED 以外)の HyperFlex のソフトウェア バージョン

HyperFlex リリース	M4 推奨 FI/サーバファームウェア *(上記の重要な注意事項を必ず確認してください)	M5 推奨 FI/サーバファームウェア *(上記の重要な注意事項を必ず確認してください)
3.5 (2h)	4.0 (4h)	4.0 (4h)
3.5 (2g)	4.0 (4h)	4.0 (4h)
3.5(2f)	4.0 (4e)	4.0 (4e)
3.5(2e)	4.0 (4e)	4.0 (4e)
3.5 (2d)	4.0 (4e)	4.0 (4e)
3.5 (2c)	リリースの延期	
3.5 (2b)	4.0 (2d)、3.2 (3i)、3.1 (3k)	4.0(2d)
3.5(2a)	4.0(1c)、3.2(3i)、3.1(3k)	4.0(1c)
3.5(1a) - サポートされていない	4.0(1b)、3.2(3h)、3.1(3j)	4.0(1a)

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、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、サーバごとに最低 2 つの 40-GbE QSFP を使用します。
- ファブリック インターコネクト コンソール ケーブル (CAB-CONSOLE-RJ45) の一端に RJ-45 コネクタがあり、他端に DB9 コネクタがあること。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VLANID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。
- **VIC および NIC のサポート**: 詳細については、『[Cisco HyperFlex Systems: ネットワーキングトポロジ](#)』のマニュアルを参照してください。

ディスクの要件

ディスクの要件は、コンバイン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。

あるいはコンバイン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。

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 がインストールされた 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。

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

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

コンピューティング専用ノード

次の表に、コンピューティング専用機能に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。サーバに関連したポリシーについては、『[Cisco UCS Manager サーバ管理ガイド](#)』を参照してください。

サポートされ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。 <p>(注) HW RAID M.2 (UCS-M2-HWRAID および HX-M2-HWRAID) は、コンピューティング専用ノードではサポートされていません。</p>

ブラウザの推奨事項 - 3.5(x) リリース

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 4: 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	11 以上	11 以上
Google Chrome	14 以上	56 以上	56 以上
Mozilla Firefox	7 以上	52 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 プラグイン:**

Cisco HX Data Platform プラグイン は vSphere 内で動作します。VMware ホストのクライアントシステムブラウザの要件については、[VMwareのマニュアル](#)を参照してください。

Cisco HX Data Platform プラグインは vCenter HTML クライアントには表示されません。vCenter フラッシュ クライアントを使用する必要があります。

• **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 は VMware ESXi と VMware vCenter 用のポートを推奨します。

- 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。

Time Server

ポート番号	Service/Protocol	[Source]	ポート宛先	基本情報
123	NTP/UDP	各 ESXi ノード 各 SCVM ノード UCSM	Time Server	双方向

HX Data Platform インストーラ

ポート番号	Service/Protocol	[Source]	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 SCVM 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
			CIMC IP	
80	HTTP/TCP	HX Data Platform インストーラ	各 ESXi ノード	管理アドレス
			各 SCVM 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 SCVM 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	
			各 ESXi ノード	
なし	Ping/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	Service/Protocol	[Source]	ポート宛先	基本情報
25	SMTP/TCP	各 SCVM ノード CIP-M UCSM	メールサーバ (Mail Server)	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	Service/Protocol	[Source]	ポート宛先	基本情報
161	SNMP Poll/UDP	モニタリング サーバ	UCSM	オプション
162	SNMP トラップ/UDP	UCSM	モニタリング サーバ	任意

Name Server

ポート番号	Service/Protocol	[Source]	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	Name Server	管理アドレス
		各 SCVM ノード	Name Server	管理アドレス
		CIP-M	Name Server	クラスタ管理
		UCSM	Name Server	

vCenter

ポート番号	Service/Protocol	[Source]	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 SCVM ノード CIP-M	双方向
7444	HTTPS (VC SSO)/TCP	vCenter	各 ESXi ノード 各 SCVM ノード CIP-M	双方向

ポート番号	Service/Protocol	[Source]	ポート宛先	基本情報
9443	HTTPS (プラグイン)/TCP	vCenter	各 ESXi ノード 各 SCVM ノード CIP-M	双方向
5989	CIM サーバ/TCP	vCenter	各 ESXi ノード	
9080	CIM サーバ/TCP	vCenter	各 ESXi ノード	ESXi リリース 6.5 で導入されました
902	Heartbeat/TCP/UDP	vCenter	各 ESXi ノード	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	Service/Protocol	[Source]	ポート宛先	基本情報
22	SSH/TCP	User	各 ESXi ノード	管理アドレス
			各 SCVM 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	Service/Protocol	[Source]	ポート宛先	基本情報
80	HTTP/TCP	User	各 SCVM 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	User	各 SCVM 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	User	vCenter SSO Server	
9443	HTTPS (プラグイン)/TCP	User	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	Service/Protocol	[Source]	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	Service/Protocol	[Source]	ポート宛先	基本情報
2181 2888 3888	Zookeeper/TCP	ウィットネス	各 CVM ノード	双方向, 管理アドレス
8180	Exhibitor (Zookeeper lifecycle)/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	Service/Protocol	[Source]	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
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
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

ポート番号	Service/Protocol	[Source]	ポート宛先	基本情報
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

SED クラスタ

ポート番号	Service/Protocol	[Source]	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	各ノードからの CIMC	KVM サーバ	Key Exchange

UCSM

ポート番号	Service/Protocol	[Source]	ポート宛先	基本情報
443	暗号化など/TCP	各 CVM ノード	CIMC OOB	各 UCS ノードの双方向
81	KVM/HTTP	ユーザ	UCSM	OOB KVM
743	KVM/HTTP	ユーザ	UCSM	OOB KVM 暗号化

その他

ポート番号	Service/Protocol	[Source]	ポート宛先	基本情報
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
9097	CIP-M フェールオーバー/TCP	各 CVM ノード	各 CVM ノード	その他の CVM への各 CVM の双方向
111	RPC バインド/TCP	各 SCVM ノード	各 SCVM ノード	インストーラへの CVM アウトバウンド
8002	インストーラ/TCP	各 SCVM ノード	インストーラ	Service Location Protocol

ポート番号	Service/Protocol	[Source]	ポート宛先	基本情報
8080	Apache tomcat/TCP	各 SCVM ノード	各 SCVM ノード	stDeploy は 接続、uri/stdeploy の要求を行います
8082	認証サービス/TCP	各 SCVM ノード	各 SCVM ノード	Uri/auth/ を使用した要求
9335	hxRoboControl/TCP	各 SCVM ノード	各 SCVM ノード	Robo の導入
443	HTTPS/TCP	各 CVM 管理 IP (CIP を含む)	UCSMA/B および VIP	ポリシーの設定
5696	TLS/TCP	各ノードからの CIMC	KMS サーバ	Key Exchange
8125	UDP	各 SCVM ノード	各 SCVM ノード	Graphite
427	UDP	各 SCVM ノード	各 SCVM ノード	Service Location Protocol
32768 ~ 65535	UDP	各 SCVM ノード	各 SCVM ノード	SCVM のアウトバウンド通信



ヒント

標準設定がなく、異なるポート設定が必要な場合は、環境のカスタマイズについて、[表7ポートのリテラル値](#)を参照してください。

HyperFlex 外部接続

外部接続	説明	IP アドレス/FQDN/ポート/バージョン	基本情報
Intersight デバイス コネクタ	サポートされている HX システムは、各システムの管理コントローラに組み込まれているデバイスコネクタを介して Cisco Intersight に接続されます。	HTTPSポート番号 : 443 1.0.5-2084 以降 (Cisco Intersight によって自動的にアップグレード)	すべてのデバイスコネクタは、 svc.intersight.com を適切に解決でき、かつポート 443 のアウトバウンドで開始される HTTPS 接続を許可する必要があります。現在の HX インストーラでは、HTTP プロキシの使用がサポートされています。 ESXi 管理の IP アドレスは、インストーラから ESXi 管理に必要とされるすべてのポートを介して、Cisco UCS Manager から到達可能である必要があります。これにより、Cisco Intersight から ESXi 管理を展開できるようになります。 詳細については、Intersight ヘルプセンターの ネットワーク接続要件 を参照してください。
Auto Support	Auto Support (ASUP) は、HX Data Platform を通じて提供されるアラート通知サービスです。	SMTP ポート番号 : 25	Auto Support は、ノードのドライブ障害などのハードウェア問題が発生した際の診断に役立つハードウェアカウンタの履歴を提供するため、有効にすることを強く推奨します。

ファブリック インターコネクトのアップリンクのプロビジョニング

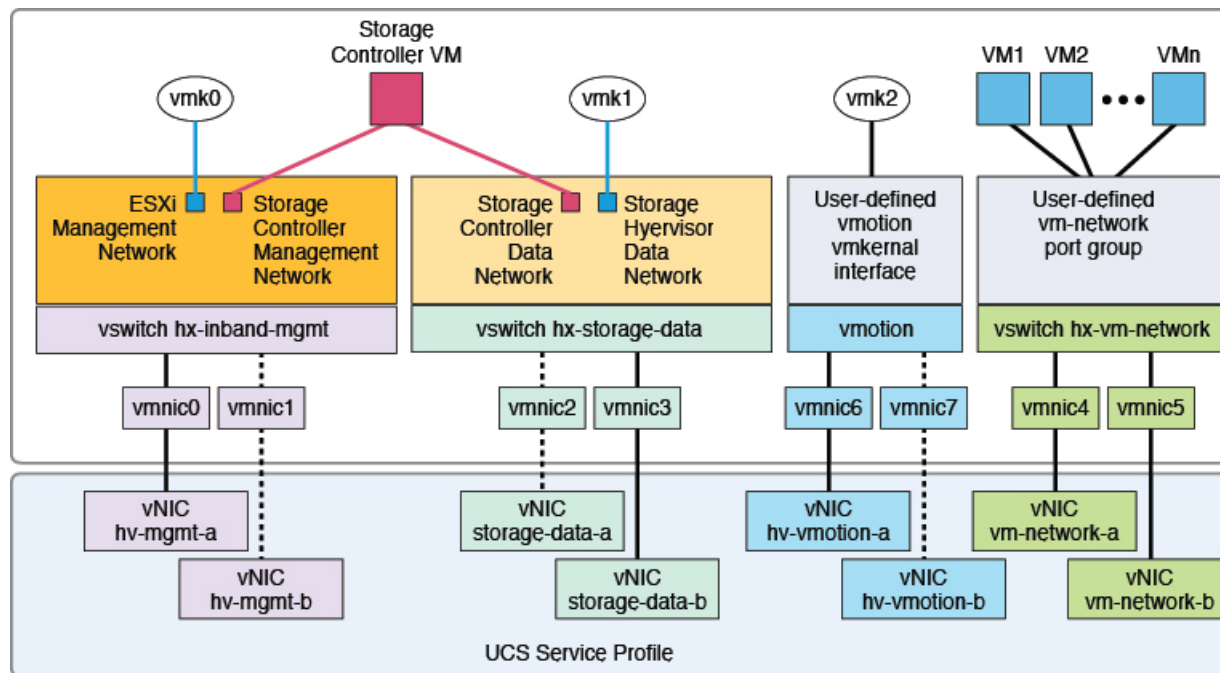
HyperFlex クラスタを設定する前に、ネットワーク トラフィック管理を最適化するアップストリーム帯域幅容量を計画してください。これにより、コンポーネントで障害が発生したり、ネットワークが部分的に停止したりした場合でも、トラフィックフローを安定した状態に維持できます。

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。



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

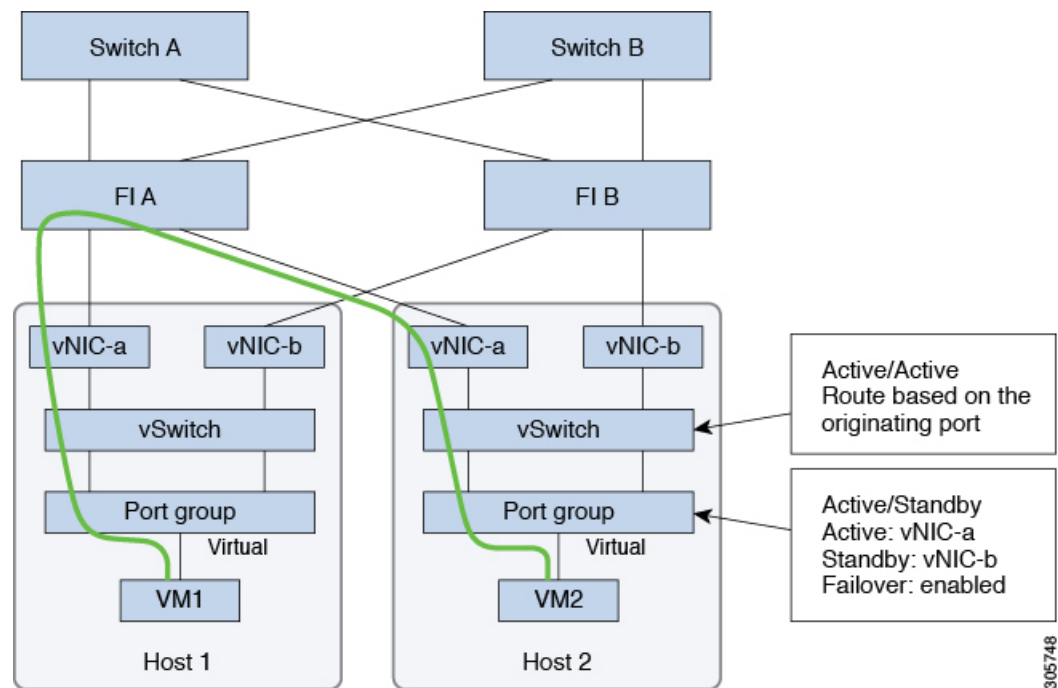
図 6: 単一ホストの *HyperFlex Data Platform* 接続



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

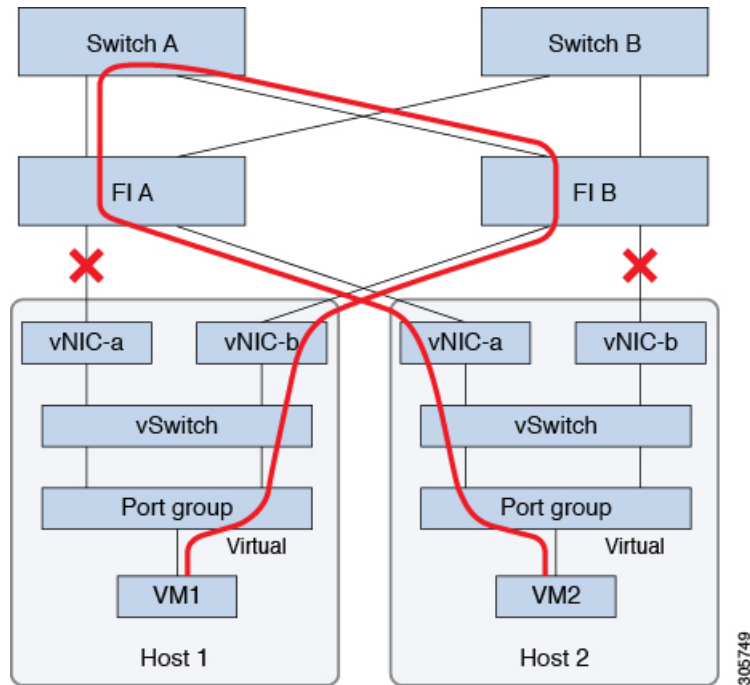
デフォルトの vSwitch NIC チューニング ポリシーとフェールオーバー ポリシーを [yes] に設定します。これにより、管理トラフィック、vMotion トラフィック、およびストレージトラフィックのすべてが、ローカルでファブリック インターコネクトに転送されるようになり、フローを安定した状態に維持できます。vNIC-a で障害が発生すると、ESXi がロード バランシングを計算し、すべての仮想ポートを vNIC-b に再ピンングします。vNIC-a がオンライン状態に戻った時点で、再びピンングが適用され、vNIC-a と vNIC-b の間で仮想ポートが元のように均等に分配されます。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

図 7: 安定した状態のトラフィック フロー



1つ以上のサーバ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 6300 Series Fabric Interconnect Hardware Guide—Deploy Layer 2 Disjoint Networks Upstream in End Host Mode](#)』というホワイトペーパーを参照してください。

ネットワーク設定



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

ベストプラクティス

- ネットワークごとに異なるサブネットとVLANを使用する必要があります。
- 10 Gbps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 Type	説明
(注)	次のネットワークごとに、異なるサブネットと VLAN を使用する必要があります。
VLAN ESXi および HyperFlex 管理トラフィック	VLAN 名 : 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。
- インバンド管理は、VLAN 2 または VLAN 3 ではサポートされていません。

Cisco UCS の要件

プロンプトが表示されたら、UCS ファブリック インターコネクトおよび 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
[名前 (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"> • データ複製ファクタ3: Hyperflex Edge を除くすべての環境で複製ファクタ3を強く推奨しています。複製ファクタ2では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。 <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すみませんが、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] (注) 既存のデータセンターオブジェクトを使用できます。データセンターが vCenter に存在しない場合は、作成されます。	vCenter データセンター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



注意

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。ネストされた DNS サーバは、DC 電源損失時など、クラスタ全体がシャットダウンした後にクラスタが起動しない可能性があります。

- NTP サーバ



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



- (注)
- ストレージクラスタを設定する前に、NTP サーバが動作していて、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。
 - アクティブ ディレクトリを NTP サーバとして使用している場合、NTP サーバが Microsoft ベスト プラクティスに従って設定されていることを確認してください。詳細については、『[Windows Time Service Tools and Settings](#)』を参照してください。NTP サーバが適切に設定されていない場合、同期が行われず、クライアント側で時間同期を修正する必要が発生する可能性があります。詳細については、『[Synchronizing ESXi/ESX time with a Microsoft Domain Controller](#)』を参照してください。

• Time Zone

フィールド	基本情報
[DNS Server(s)]	<p><IP address></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 address></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	Reservation	Limit
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	Yes

- 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 5 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 \(57 ページ\)](#)
- [概要 \(57 ページ\)](#)

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。

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

Cisco HyperFlex ノードのインストールの詳細については、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	

インストール先のノードのタイプ	参照先
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
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レーションおよびサービス 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レーションおよびサービス ガイド
Cisco UCS C480 M5 ノード	Cisco UCS C480 M5 サーバインストールレーションおよびサービス 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。

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

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

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

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

手順

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

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

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

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

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

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

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

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

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

手順

ステップ 1 コンソールポートに接続します。詳細については、[Cisco 6200 Series Fabric Interconnect Hardware Installation guide](#)を参照してください。

ステップ 2 ファブリック インターコネクタの電源を入れます。ファブリック インターコネクタが起動する際、電源オンセルフテストのメッセージが表示されます。

ステップ 3 インストール方式プロンプトに *gui* と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

- ファブリック インターコネクタの管理ポートの Ipv4 アドレス。
- ファブリック インターコネクタ上の管理ポートの Ipv4 サブネット マスク。
- ファブリック インターコネクタに割り当てられたデフォルト ゲートウェイの IPv4 アドレス。

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

ステップ 5 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。

ステップ 6 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager 起動ページに移動します。

ステップ 7 **[Express Setup (Express セットアップ)]** を選択します。

ステップ 8 **[Initial Setup (初期セットアップ)]** を選択し、**[Submit (送信)]** をクリックします。

ファブリック インターコネクタは、第 1 ファブリック インターコネクタの設定情報を検出します。

ステップ 9 **[Cluster and Fabric Setup (クラスタおよびファブリック セットアップ)]** 領域で、次のフィールドに値を入力します。

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

ステップ 10 **[System Setup (システム セットアップ)]** 領域の **[Admin Password of Master (マスターの管理者パスワード)]** フィールドに管理者アカウントのパスワードを入力します。**[Manager Initial Setup (Manager の初期セットアップ)]** 領域が表示されます。

ステップ 11 **[Manager Initial Setup (Manager の初期セットアップ)]** 領域で表示されるフィールドは、第 1 ファブリック インターコネクタを IPv4 のどちらの管理アドレスで設定したかによって異なります。次のように、設定に適したフィールドに入力します。

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

- ステップ 12 [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 インターコネクタの設定

手順

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

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

例

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

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

CLIによる従属ファブリック インターコネクタの設定

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



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

手順

- 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 インターコネクットの電源を入れます。
ファブリック インターコネクットが起動すると、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。

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

- ステップ 4** **y** と入力して、従属ファブリック インターコネクットをクラスタに追加します。
- ステップ 5** ピア ファブリック インターコネクットの管理パスワードを入力します。
- ステップ 6** 従属ファブリック インターコネクット上の管理ポートの IP アドレスを入力します。
- ステップ 7** 設定の概要を確認し、**yes** と入力して設定を保存および適用するか、**no** と入力して設定ウィザードを初めからやり直して設定を一部変更します。

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

例

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

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

コンソール設定の確認

SSH を介してファブリック インターコネクットにログインすることで、両方のファブリック インターコネクット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 5:

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の両方のファブリック インターコネクットの動作状態およびリーダーシップ ロールを表示します。	次の例の表示では、両方のファブリック インターコネク트가 Up 状態、HA が Ready 状態、ファブリック インターコネク트가 A がプライマリ ロール、ファブリック インターコネク트가 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 0x2e95deaccd0f11e2-0x8ff35147e84f3de2Start 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-9133-89fa154e3fa1, state: active

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

概要

Cisco HX220c および HX240c サーバはファブリック インターコネクトに直接接続します。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 インターコネクトに接続した後、そのサーバが検出された時点で、UCS Manager 設定フォームを使用して、Cisco UCS Manager で使用可能な C シリーズ ソフトウェア バンドルを更新します。

直接接続モードを使用する場合は、すべての Cisco UCS 管理対象アダプタを、ファブリック インターコネクト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 インターコネクトと互換性がありません。
 - Cisco UCS の設定に関する一般的な制限事項：[Cisco UCS 6200、6332 および 6324 シリーズ Cisco UCS Manager コンフィギュレーション上限値ガイド](#)を参照してください。

ファブリック インターコネクトへのコンバージド 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。
- 近い将来に FC ストレージを接続する必要がない場合は、ポート 1 ~ 16 のみを使用します。
- Cisco UCS FI 63xx および64xx では、ポート 1 ~ 6 を FC ポートとして設定することだけがサポートされています。今後 FC ストレージを接続する必要がある場合は、ポート 1 ~ 6 を FC に変換します。



(注) 変換により、HX の展開が中断される場合があります。

- CIMC サーバを接続する前に、Cisco VIC 1227 が HXc240 の PCIe スロット 2 または HXc220 のライザ 1 スロット 1 に装着されており、Cisco UCS Manager と統合できることを確認します。カードが正しいスロットに装着されていない場合、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。

手順

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、サーバポー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。

直接接続モードのクラスタ セットアップの物理的な接続の図

次の図は、C-Series Rack-Mount Server と Cisco UCS Domain、Cisco UCS Manager リリース 3.1 以降との直接接続モードの物理接続の例を示しています。次の図は、UCS Manager と C-Series ラックマウントサーバを統合する場合の配線構成を示しています。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

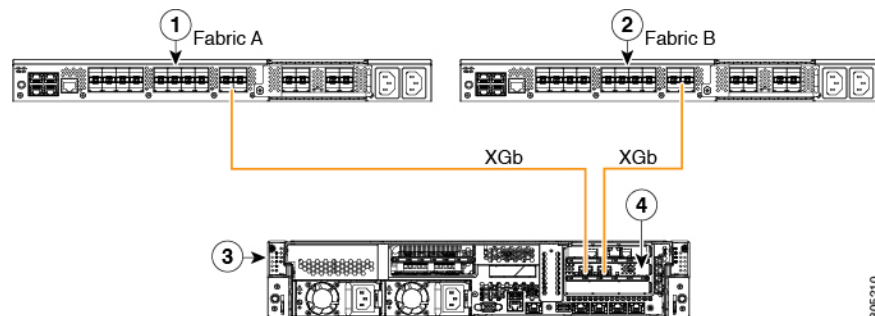
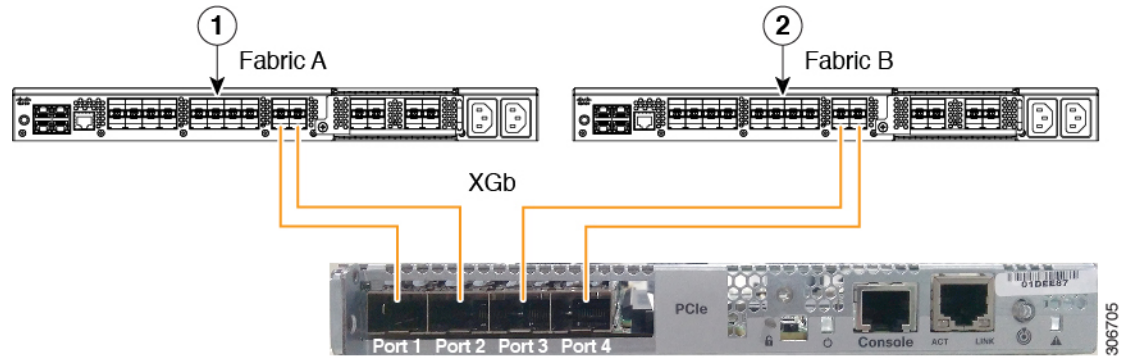


図 10: Cisco VIC 1455 との直接接続の配線構成



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

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

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

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 \(165 ページ\)](#)を参照してください。



第 6 章

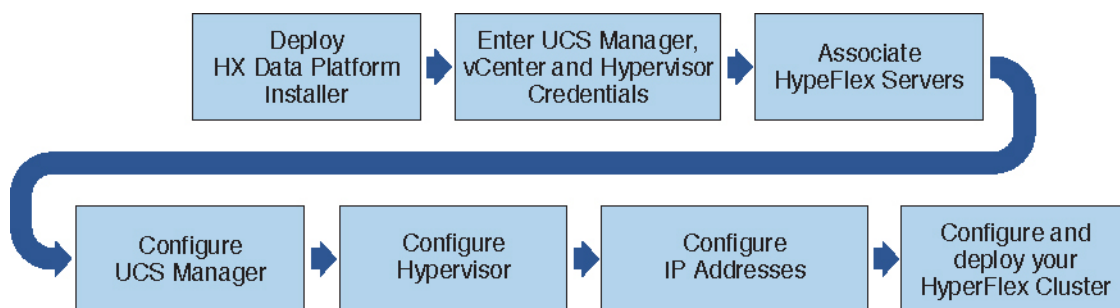
Cisco HyperFlex Systems の設定

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。

- [インストール ワークフロー](#) (63 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](#) (64 ページ)
- [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](#) (67 ページ)
- [Syslog の設定](#) (68 ページ)
- [HyperFlex クラスタの設定と展開](#) (69 ページ)
- [GPU を搭載した HyperFlex ノードの設置](#) (83 ページ)
- [HX データ プラットフォーム インストーラ ナビゲーション エイド ボタン](#) (84 ページ)
- [警告およびエラー メッセージ](#) (84 ページ)

インストール ワークフロー

次のインストールワークフローは、HX Data Platform インストーラ を使用して標準クラスタを作成する場合に、関連する手順をまとめています。



インストール時に次のワークフローに従ってください。

1. vSphere Web Client を使用して HX データ プラットフォーム インストーラ OVA を展開します。ハイパーバイザ ウィザードが新しい VM に IP アドレスを割り当てる際の DHCP に対してデフォルトの場合、静的 IP アドレスを持つ HX データ プラットフォーム インストーラ OVA を展開します。詳細については、[vSphere Web クライアントを使用した HX Data](#)

[Platform インストーラ OVA の展開 \(64 ページ\)](#) または [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 \(67 ページ\)](#) を参照してください。

2. Syslog を設定して、syslog の一元的なリポジトリにすべてのログ情報を送信します。詳細については、[Syslog の設定 \(68 ページ\)](#) を参照してください。
3. UCS Manager、vCenter、およびハイパーバイザのクレデンシャルを入力します。
4. サーバポートを設定し、HyperFlex サーバを関連付けます。詳細については、[HyperFlex サーバの関連付け \(70 ページ\)](#) を参照してください。
5. アウトオブバンド CIMC、iSCSi ストレージ、および FC ストレージの VLAN、MAC プール、'hx-ext-mgmt' IPPool を設定します。詳細については、[UCS Manager の設定 \(71 ページ\)](#) を参照してください。
6. ハイパーバイザを設定します。詳細については、[ハイパーバイザの設定 \(75 ページ\)](#) を参照してください。



(注) ESXi ネットワーキングが完了している場合は、再インストールの際にハイパーバイザの設定をスキップできます。

7. IP アドレスを設定します。詳細については、[IP アドレスの設定 \(77 ページ\)](#) を参照してください。
8. HyperFlex クラスタを設定し展開します。詳細については、「[HyperFlex クラスタの設定 \(79 ページ\)](#)」を参照してください。

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。

手順

- 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。

- 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。
- 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、ユーザーレディ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 インベントリ リスト (vCenter Inventory list) > ホスト (Host) > Host (Host) > OVA を展開 (Deploy OVA) を展開します

- ステップ 3** HX Data Platform インストーラ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 (67 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 (コンマ区切り)。 DHCP が必要な場合は空白のままにしてください。
[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。
Root パスワード	ルート ユーザー パスワード。 このフィールドは必須フィールドです。

ステップ 5 [Next] をクリックします。リストされたオプションが正しいかどうかを確認し、**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 4 GB のメモリです。これらの設定を小さくすると、CPU の使用率が 100% になり、ホスト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。

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。

手順

- 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.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1
--prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8
--prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco
--prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5
--prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36
--prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0
--prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova
vi://root:password@esx_server
```

このコマンドでは、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.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1	適切なゲートウェイ IP アドレスを指定します。
prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8	適切な DNS IP アドレスを指定します。
prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco	適切なドメインを指定します。
prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5	適切な NTP IP アドレスを指定します。
prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36	適切なインストーラの静的 IP アドレスを指定します。
prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0	適切なネットマスクアドレスを指定します。
prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword	root ユーザー パスワードを指定します。
/opt/ovf/frfsi_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ャルを含めます。

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



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

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

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

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

手順

ステップ 1 syslog サーバが稼動していることと、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 クラスタの設定と展開

HyperFlex GUI で使用される共通タスクの手順

Procedure

ステップ 1 HX Data Platform インストーラに、root ユーザのログイン情報でログインします。最初にログインしたとき、初期設定のデフォルトのパスワードを変更するよう求められます。

- 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。
- 次のログイン資格情報を入力します。

- ユーザ名 : root
- パスワード : Cisco123

c) EULA を読んで、**[I accept the terms and conditions (利用規約に同意します)]** セレクトボックスをオンにし、**[Login (ログイン)]** をクリックします。

ステップ 2 **[Change factory default password (初期のデフォルトパスワードの変更)]** 画面で、次のフィールドに値を入力し、**[Change password & Login (パスワードとログインの変更)]** をクリックします。

フィールド	説明
New password	ハイパーバイザの新しいパスワードを入力してください。
新しいパスワードをもう一度入力してください	ハイパーバイザの新しいパスワードを再度入力します。

HyperFlex サーバの関連付け

[サーバの選択] ページで、右の [設定] ページに使用するクレデンシャルの詳細なリストが表示されます。[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。

フィールド	説明
ロケータ LED (Locator LED)	サーバーの検索をオンにします。
サーバ名 (Server Name)	サーバに割り当てられた名前。
Status (ステータス)	<ul style="list-style-type: none"> • アクセス不可
モデル (Model)	サーバモデルが表示されます。
シリアル (Serial)	サーバのシリアル番号を表示します。
関連付けのステータス (Assoc State)	<ul style="list-style-type: none"> • 関連付け • [関連付け解除]
サービスプロファイル (Service Profile) (関連付けられたサーバに対してのみ)	サーバに割り当てられているサービスプロファイル。

フィールド	説明
アクション (Actions)	<ul style="list-style-type: none"> • [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。

始める前に

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

手順

ステップ 1 **[Configure Server Ports]** ボタンをクリックして、新しいすべての HX ノードを検出します。**[サーバーポートの構成 (Configure Server Ports)]** ダイアログボックスで、サーバポートとして構成するすべてのポートを一覧表示します。**[Configure]** をクリックします。

(注) 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 2 **[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。

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

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

ステップ 3 **[続行]** をクリックして UCS マネージャーを設定します。「[UCS Manager の設定 \(71 ページ\)](#)」を参照してください。

UCS Manager の設定

[UCSM 設定] ページで、アウトオブバンド CIMC、iSCSi ストレージ、および FC ストレージの VLAN、MAC プール、'hx-ext-mgmt' IP プールを設定します。

始める前に

HyperFlex クラスタにサーバを関連付けます。[HyperFlex サーバの関連付け \(70 ページ\)](#) を参照してください。

手順

ステップ1 [VLAN 設定] セクションで、次のフィールドを入力します。

(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。

フィールド	説明
[VLAN for Hypervisor and HyperFlex management]	
[VLAN Name]	hx-inband-mgmt
VLAN ID (Admin. VLAN ID)	デフォルト—3091
[VLAN for HyperFlex Storage traffic]	
[VLAN Name]	hx-storage-data
VLAN ID (Admin. VLAN ID)	デフォルト—3092
[VLAN for VM vMotion]	
[VLAN Name]	hx-vmotion
VLAN ID (Admin. VLAN ID)	デフォルト—3093
[VLAN for VM Network]	
[VLAN Name]	vm-network
VLAN ID	デフォルト—3094 ゲスト VLAN のカンマ区切りリスト。

ステップ2 [MAC プール] セクションで、2つ以上の16進文字 (0~F) を追加し [MAC プールプレフィックス] を設定します。

(注) すべてのUCSドメイン間で他のMACアドレスプールに使用されていないプレフィックスを選択します。

Example:
00:25:B5:A0:

ステップ3 [アウトオブバンド CIMC の hx-ext-mgmt' IP プール] セクションで、次のフィールドを入力します。

フィールド	説明
[IP Blocks]	HyperFlex ノードに指定された IP アドレスの範囲。IP アドレスは、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 などです。
[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 アドレスを入力します。 たとえば、10.193.0.1 と指定します。

ステップ 4 外部ストレージを追加する場合は、以下のフィールドに記入して **iSCSI ストレージ** を設定します。

フィールド	説明
[iSCSI ストレージの有効化] チェックボックス	チェックボックスをオンにして iSCSI ストレージを設定します。
VLAN A 名 (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。
VLAN B 名 (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。

ステップ 5 外部ストレージを追加する場合は、以下のフィールドに記入して **FC ストレージ** を設定します。

フィールド	説明
[FC ストレージの有効化] チェックボックス	FC ストレージを有効にするには、チェックボックスをオンにします、

フィールド	説明
[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ต์に対し、WWPN および WWNN 用の WWxN プールが作成されます。
VSAN A 名 (VSAN A Name)	プライマリ ファブリック インターコネクต์ (FI-A) の VSAN の名前。 デフォルト—hx-ext-storage-fc-a。
VSAN A ID	プライマリ ファブリック インターコネクต์ (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 ゾーニングを使用してインストーラで既存の VSAN ID を入力する場合、ゾーニングは VSAN ID の既存の環境で無効になります。
[VSAN B Name]	下位のファブリック インターコネクต์ (FI-B) の VSAN の名前。 デフォルト—hx-ext-storage-fc-b。
VSAN B ID	下位のファブリック インターコネクต์ (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 ゾーニングを使用してインストーラで既存の VSAN ID を入力する場合、ゾーニングは VSAN ID の既存の環境で無効になります。

ステップ 6 [詳細] セクションで、次の手順を実行します。

フィールド	説明
UCS サーバファームウェアバージョン (UCS Server Firmware Version)	ドロップダウンリストから HX サーバに関連付ける 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(1d)。
[HyperFlex Cluster Name]	ユーザー定義名を指定します。HyperFlex クラスタ名は、特定のクラスタ内の HX サーバのグループに適用されます。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。
[Org Name]	一意組織名を指定して、UCS ドメインの残りの部分から HyperFlex 環境の分離を確認します。

ステップ 7 [続行] をクリックして HyperFlex を設定します。「[ハイパーバイザの設定 \(75 ページ\)](#)」を参照してください。

ハイパーバイザの設定



(注) [ハイパーバイザの設定 (Hypervisor Configuration)] ページの [設定 (Configuration)] ペインで、VLAN、MAC プール、および IP アドレスプール情報を確認します。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、HX Data Platform 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。



注目 ESXi ネットワーキングが完了している場合は、再インストールの際にハイパーバイザの設定をスキップできます。

始める前に

アウトオブバンド CIMC の VLAN、MAC プール、および 'hx-ext-mgmt' IP プールを設定します。外部ストレージを追加する場合は、iSCSI ストレージと FC ストレージを設定します。UCS

サーバのファームウェアバージョンを選択し、HyperFlexクラスタの名前を割り当てます。 [UCS Manager の設定 \(71 ページ\)](#) を参照してください。

手順

ステップ 1 [一般的なハイパーバイザ設定を設定する(Configure Common Hypervisor Settings)] セクションで、次のフィールドに入力します。

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。 (注) <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 [クラスタ設定 (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。 • 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、コンマで区切ってください。

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

(注) ドラッグアンドドロップを使用してサーバを並べ替えることができます。

フィールド	説明
[名前 (Name)]	サーバに割り当てられた名前。
ロケータ LED (Locator LED)	サーバの検索をオンにします。

フィールド	説明
シリアル (Serial)	サーバのシリアル番号を表示します。
[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 3 [続行] をクリックして IP アドレスを設定します。「[IP アドレスの設定 \(77 ページ\)](#)」を参照してください。

IP アドレスの設定

始める前に

[[ハイパーバイザ設定](#)] ページでハイパーバイザの設定が完了していることを確認します。[ハイパーバイザの設定 \(75 ページ\)](#) を参照してください。

手順

- ステップ 1** [IP アドレス] ページで [IP アドレスを連続させる] を選択して、IP アドレスを連続させます。
- ステップ 2** ハイパーバイザ、ストレージコントローラ (管理) とハイパーバイザ、ストレージコントローラ (データ) カラムの最初の行に IP アドレスを入力するとき、HX Data Platform インストーラで残りのノードについてもノード情報を段階的に自動入力します。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。

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

各 HX ノードについては、ハイパーバイザ、ストレージコントローラ、管理、データ IP アドレスを入力します。IP アドレスについては、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しているかを指定します。

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。

ステップ 3 ここで指定した 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。

次の IP アドレスを提供します。

フィールド	説明
管理クラスタ データの IP アドレス (Management Cluster Data IP Address)	HX データプラットフォームストレージクラスタの管理ネットワーク IP アドレスを入力します。
データ クラスタ データ IP アドレス (Data Cluster Data IP Address)	HX Data Platform ストレージクラスタのデータネットワークの IP アドレスを入力します。
[Management Subnet Mask]	VLAN と vSwitch についてのサブネット情報を入力します。 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。
[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。
[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、10.193.0.1 と指定します。

ステップ 4 [続行] をクリックして HyperFlex クラスタを設定します。「[HyperFlex クラスタの設定 \(79 ページ\)](#)」を参照してください。

HyperFlex クラスタの設定

[クラスタ設定 (Cluster Configuration)] ページで、Cisco HX ストレージクラスタの場合、次のフィールドを入力して HyperFlex クラスタの展開を開始します。

始める前に

[IP アドレス] ページで IP アドレスの設定が完了していることを確認します。[IP アドレスの設定 \(77 ページ\)](#) を参照してください。

手順

ステップ 1 [Cisco HX Cluster] セクションで、次のフィールドに入力します。

フィールド	説明
クラスタ名 (Cluster Name)	HX データ プラットフォーム ストレージクラスタの名前を指定します。
レプリケーション ファクタ (Replication Factor)	<p>ストレージクラスタ間のデータの冗長レプリカの数指定します。レプリケーションファクタを 2 つまたは 3 つの冗長レプリカに設定します。</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。 Hyperflex Edge を除くすべての環境で複製ファクタ 3 を強く推奨しています。複製ファクタ 2 では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。

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

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。

- 重要**
- コントローラ VM またはコントローラ VM のデータストアの名前は変更できません。
 - 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つの小文字、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。

ステップ 3 [vCenter 構成 (vCenter Configuration)] セクションで、次のフィールドに入力します。

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

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

DNS サーバ (DNS Server(s))	各 DNS サーバの IP アドレスのカンマ区切りリスト。
NTP サーバ (NTP Server(s))	各 NTP サーバの IP アドレスのカンマ区切りリスト。 (注) ストレージコントローラ VM と ESXi ホストで動作するサービス間のクロック同期のために、すべてのホストが同じ NTP サーバを使用する必要があります。
DNS ドメイン名 (DNS Domain Name)	DNS FQDN または IP アドレスが無効です
タイムゾーン (Time Zone)	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。

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

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

ステップ 6 [高度な設定 (Advanced Configuration)] セクションで、次の手順を実行します。

フィールド	説明
ジャンボ フレーム ジャンボ フレームを有効化 (Enable Jumbo Frames)	ホスト 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 ディスク パーティションのクリーン アップ (Clean up Disk Partitions)	手動で準備されたサーバの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。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。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。 注目 工場で準備されたシステムにはこのオプションを選択しないでください。工場で準備されたシステムのディスクパーティションは正しく設定されています。

フィールド	説明
Virtual Desktop (VDI)	<p>VDI のみの環境でオンにします。</p> <p>(注) ストレージクラスタの作成後に VDI 設定を変更するには、リソースをシャットダウンまたは移動し、変更を加え (下の手順に記載)、クラスタを再起動します。</p> <p>デフォルトでは、HyperFlex クラスタは VSI ワークロード用にパフォーマンス調整されるように設定されています。</p> <p>このパフォーマンスのカスタマイズは、Hyperflex Data Platform クラスタで次の手順を実行することによって変更できます。HyperFlex クラスタを VDI から VSI ワークロード (またはその逆) に変更するには、次のようにします。</p> <p>警告: メンテナンスウィンドウが必要です。これにより、クラスタがオフラインの間はデータが使用できなくなります。</p> <ol style="list-style-type: none"> 1. <code>~#stcli cluster shutdown</code> を実行してクラスタをシャットダウンします。 2. すべてのコントローラ VM の <code>storfs cfg</code> を編集し、<code>workloadType</code> を <code>Vsi</code> または <code>Vdi</code> に変更します。 3. クラスタの作成後に、クラスタを起動し (<code>stcli cluster start</code>)、調整の変更を有効にします。
(オプション) vCenter Server のシングルサインオン (vCenter Single-Sign-On Server)	<p>この情報は、SSO URL が到達可能でない場合のみ必要です。</p> <p>(注) このフィールドは使用しないでください。これはレガシー展開に使用されます。</p> <p>[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。</p>

ステップ7 [開始(Start)] をクリックして、HyperFlex クラスタの展開を開始します。[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] のセクション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。導入されたクラスタのステータスは、[オンライン (Online)] および [ヘルシー (Healthy)] として表示されます。
- [HyperFlex Connect の起動 (Launch HyperFlex Connect)] をクリックし、データストアを作成してクラスタを管理します。

GPU 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、4GB 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、4GB 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。

HX データ プラットフォーム インストーラ ナビゲーション エイド ボタン

- 設定のエクスポート (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。
- ワークフロー情報—情報アイコンの上にカーソルを合わせると、現在のワークフローが表示されます。HyperFlex クラスタの作成の場合、ワークフロー情報は **Create Workflow = Esx** です。
- [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。
- 設定 (Settings) : 歯車のアイコンをクリックすると、[(やり直し (Start over))] または [ログアウト (Log Out)] を実行できます。

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 7 章

HyperFlex Data Platform でのライセンス設定

- [スマートライセンスと HyperFlex \(87 ページ\)](#)
- [接続環境のライセンス管理 \(91 ページ\)](#)

スマートライセンスと HyperFlex

概要

シスコスマートソフトウェアライセンシング (スマートライセンス) はインテリジェントなソフトウェアライセンス管理システムで、組織全体でライセンスを調達、導入、管理するなど、時間のかかる手動のライセンスタスクを自動化します。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。



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

HX ストレージクラスタを登録した後、Cisco Smart Software Manager または Smart Software Manager サテライトに対して HyperFlex を特定するために使われる証明書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

Registration Status	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。

Registration Status	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るにはライセンスの購入または更新が必要です。</p>

Registration Status	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。

Registration Status	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。

接続環境のライセンス管理

接続環境のライセンスを管理するには、次の手順を実行します。

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

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

手順

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 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 4 HX ストレージクラスタが登録されていることを確認します。

```
# stcli license show summary
```

別の方法として、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。[コントローラ VM を介してスマートソフトウェアライセンスとともにクラスタを登録する \(91 ページ\)](#) 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
```

手順

ステップ1 コントローラ VM にログインします。

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

```
# stcli license deregister
```

ステップ3 HX ストレージクラスタが登録解除されたことを確認します。

```
# stcli license show summary
```

スマートライセンス承認の更新

始める前に

- 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
```

手順

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
```



第 8 章

HyperFlex ハードウェア アクセラレーションカードの設定

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

- [HyperFlex ハードウェア アクセラレーションカードの概要 \(95 ページ\)](#)
- [Install HyperFlex Hardware Acceleration Cards \(96 ページ\)](#)
- [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 \(97 ページ\)](#)
- [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 \(99 ページ\)](#)
- [HyperFlex クラスタの設定と展開 \(101 ページ\)](#)
- [HyperFlex ハードウェア アクセラレーションカードの取り付けの確認 \(116 ページ\)](#)
- [HyperFlex ハードウェア アクセラレーションカードのトラブルシューティング \(117 ページ\)](#)
- [HyperFlex ハードウェア アクセラレーションカードのに関する追加情報 \(117 ページ\)](#)

HyperFlex ハードウェア アクセラレーションカードの概要

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



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

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

Install HyperFlex Hardware Acceleration Cards

始める前に

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

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



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

- クラスタ タイプは、すべてフラッシュ/ハイブリッド ESXi である必要があります。
- インストールは、HX 240 M5 サーバでのみサポートされています。
- ハードウェア アクセラレーション カードは、Cisco HX データ複製では動作しません。

手順

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

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

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

- HX クラスタの設定と展開

vSphere Web 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。

手順

- 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。

- 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。
- 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、ユーザー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 インベントリ リスト (vCenter Inventory list) > ホスト (Host) > Host (Host) > OVA を展開 (Deploy OVA)を展開します

ステップ 3 HX Data Platform インストーラ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 \(67 ページ\)](#) 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 (コンマ区切り)。 DHCP が必要な場合は空白のままにしてください。
[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。
Root パスワード	ルート ユーザー パスワード。 このフィールドは必須フィールドです。

ステップ 5 [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 4 GB のメモリです。これらの設定を小さくすると、CPU の使用率が 100% になり、ホスト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。

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。

手順

- 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。

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

```

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

```

このコマンドでは、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.3gateway.Cisco_HX_Installer_Appliance=10.64.8.1	適切なゲートウェイ IP アドレスを指定します。
prop:hx.4DNS.Cisco_HX_Installer_Appliance=10.64.1.8	適切な DNS IP アドレスを指定します。
prop:hx.5domain.Cisco_HX_Installer_Appliance=cisco	適切なドメインを指定します。
prop:hx.6NTP.Cisco_HX_Installer_Appliance=10.64.8.5	適切な NTP IP アドレスを指定します。
prop:hx.1ip0.Cisco_HX_Installer_Appliance=10.64.8.36	適切なインストーラの静的 IP アドレスを指定します。
prop:hx.2netmask0.Cisco_HX_Installer_Appliance=255.255.248.0	適切なネットマスクアドレスを指定します。
prop:hx.7root_password.Cisco_HX_Installer_Appliance=mypassword	root ユーザー パスワードを指定します。
/opt/ovf/rfsi_test/Cisco-HX-Data-Platform-Installer-v1.7.1-14786.ova	HX 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。

コマンド	説明
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ャルを含めます。

HyperFlex クラスタの設定と展開

クレデンシャルの入力

[クレデンシャル] ページで、JSON ファイルまたは入力データから、必要なフィールドに手動で必要な設定データをインポートするように選択できます。



(注) HyperFlex クラスタの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。

クラスタ作成を実行するには、JSON 設定 ファイルから設定データをインポートし、次の操作を行います。

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データをロードします。[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。

手順

ステップ 1 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 ログイン ページで、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 **Build ID**] を確認します。

ステップ 2 ログイン ページで、次のクレデンシャルを入力します。

ユーザ名 : root

パスワード (デフォルト): Cisco123

注目 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。ユーザーが入力した新しいパスワードを指定しない限り、インストールを続行できません。

- ステップ 3** [利用規約に同意します (I accept the terms and conditions)] チェック ボックスをオンにして、[ログイン (Login)] をクリックします。
- ステップ 4** [ワークフローの選択] ページで、[クラスタの作成] ドロップダウン リストから、[標準クラスタ] を選択します。
- ステップ 5** [クレデンシャル] ページで、次の設定データを入力します。

フィールド	説明
UCS Manager のホスト名 (UCS Manager Host Name)	UCS Manager FQDN または IP アドレスを入力します。 たとえば <i>10.193.211.120</i> と入力します。
UCS Manager のユーザ名 (UCS Manager User Name)	[administrative username] を入力します。
パスワード (Password)	管理者パスワードを入力します。

vCenter クレデンシャル (vCenter Credentials)

フィールド	説明
vCenter サーバ (vCenter Server)	vCenter サーバ FQDN または IP アドレスを入力します。 たとえば <i>10.193.211.120</i> と入力します。 (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]	[administrative username] を入力します。 例 : <i>administrator@vsphere.local</i> 。
[Admin Password]	管理者パスワードを入力します。

- ステップ 6** [ハイパーバイザの設定 (Hypervisor Configuration)] ページで、次の設定データを入力します。
ハイパーバイザのクレデンシャル

フィールド	説明
管理者ユーザ名 (Admin User Name)	[administrative username] を入力します。 ユーザ名は、ファクトリーノードの root です。
新しいパスワード (New Password)	重要 ハイパーバイザの工場出荷時パスワードを変更する必要があります。 次のガイドラインを使用してハイパーバイザの新しいパスワードを作成します。 <ul style="list-style-type: none"> • 長さは 6～80 字である必要があります。 • 1 個の大文字、1 個の小文字、1 個の数字、1 個の特殊文字が必要です。 • パスワードが大文字で始まる場合、2 個の大文字が必要です。 • パスワードが数字で終わる場合、2 桁の数字が必要です。
新しいパスワードの確認 (Confirm New Password)	ハイパーバイザの新しいパスワードを再度入力します。

ステップ 7 [続行] をクリックして、HyperFlex サーバへの関連付けを開始します。「[HyperFlex サーバの関連付け \(70 ページ\)](#)」を参照してください。

HyperFlex サーバの関連付け

[サーバの選択] ページで、右の [設定] ページに使用するクレデンシャルの詳細なリストが表示されます。[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。

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

フィールド	説明
関連付けのステータス (Assoc State)	<ul style="list-style-type: none"> • 関連付け • [関連付け解除]
サービスプロファイル (Service Profile) (関連付けられたサーバに対してのみ)	サーバに割り当てられているサービスプロファイル。
アクション (Actions)	<ul style="list-style-type: none"> • [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。

始める前に

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

手順

ステップ 1 **[Configure Server Ports]** ボタンをクリックして、新しいすべての HX ノードを検出します。**[サーバポートの構成 (Configure Server Ports)]** ダイアログ ボックスで、サーバポートとして構成するすべてのポートを一覧表示します。**[Configure]** をクリックします。

(注) 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 2 **[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。

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

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

ステップ 3 **[続行]** をクリックして UCS マネージャーを設定します。「[UCS Manager の設定 \(71 ページ\)](#)」を参照してください。

UCS Manager の設定

[UCSM 設定] ページで、アウトオブバンド CIMC、iSCSi ストレージ、および FC ストレージの VLAN、MAC プール、'hx-ext-mgmt' IP プールを設定します。

始める前に

HyperFlex クラスタにサーバを関連付けます。[HyperFlex サーバの関連付け \(70 ページ\)](#) を参照してください。

手順

ステップ 1 [VLAN 設定] セクションで、次のフィールドを入力します。

(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。

フィールド	説明
[VLAN for Hypervisor and HyperFlex management]	
[VLAN Name]	hx-inband-mgmt
VLAN ID (Admin. VLAN ID)	デフォルト—3091
[VLAN for HyperFlex Storage traffic]	
[VLAN Name]	hx-storage-data
VLAN ID (Admin. VLAN ID)	デフォルト—3092
[VLAN for VM vMotion]	
[VLAN Name]	hx-vmotion
VLAN ID (Admin. VLAN ID)	デフォルト—3093
[VLAN for VM Network]	
[VLAN Name]	vm-network
VLAN ID	デフォルト—3094 ゲスト VLAN のカンマ区切りリスト。

ステップ 2 [MAC プール] セクションで、2つ以上の 16 進文字 (0~F) を追加し [MAC プール プレフィックス] を設定します。

(注) すべての UCS ドメイン間で他の MAC アドレスプールに使用されていないプレフィックスを選択します。

Example:
00:25:B5:A0:

ステップ 3 [アウトオブバンド CIMC の hx-ext-mgmt' IP プール] セクションで、次のフィールドを入力します。

フィールド	説明
[IP Blocks]	HyperFlex ノードに指定された IP アドレスの範囲。IP アドレスは、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 などです。
[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 アドレスを入力します。 たとえば、10.193.0.1 と指定します。

ステップ 4 外部ストレージを追加する場合は、以下のフィールドに記入して **iSCSI ストレージ** を設定します。

フィールド	説明
[iSCSI ストレージの有効化] チェックボックス	チェックボックスをオンにして iSCSI ストレージを設定します。
VLAN A 名 (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。
VLAN B 名 (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。

ステップ 5 外部ストレージを追加する場合は、以下のフィールドに記入して **FC ストレージ** を設定します。

フィールド	説明
[FC ストレージの有効化] チェックボックス	FC ストレージを有効にするには、チェックボックスをオンにします、
[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 名 (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—hx-ext-storage-fc-a。
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 ゾーニングを使用してインストーラで既存の VSANID を入力する場合、ゾーニングは VSAN ID の既存の環境で無効になります。
[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—hx-ext-storage-fc-b。
VSAN B ID	下位のファブリック インターコネクタ (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 ゾーニングを使用してインストーラで既存の VSANID を入力する場合、ゾーニングは VSAN ID の既存の環境で無効になります。

ステップ 6 [詳細] セクションで、次の手順を実行します。

フィールド	説明
UCS サーバファームウェアバージョン (UCS Server Firmware Version)	ドロップダウン リストから HX サーバに関連付ける 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(1d)。
[HyperFlex Cluster Name]	ユーザー定義名を指定します。HyperFlex クラスタ名は、特定のクラスタ内の HX サーバのグループに適用されます。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。
[Org Name]	一意組織名を指定して、UCS ドメインの残りの部分から HyperFlex 環境の分離を確認します。

ステップ 7 [続行] をクリックして HyperFlex を設定します。「[ハイパーバイザの設定 \(75 ページ\)](#)」を参照してください。

ハイパーバイザの設定



(注) [ハイパーバイザの設定 (Hypervisor Configuration)] ページの [設定 (Configuration)] ペインで、VLAN、MAC プール、および IP アドレスプール情報を確認します。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、HX Data Platform 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。



注目 ESXi ネットワーキングが完了している場合は、再インストールの際にハイパーバイザの設定をスキップできます。

始める前に

アウトオブバンド CIMC の VLAN、MAC プール、および 'hx-ext-mgmt' IP プールを設定します。外部ストレージを追加する場合は、iSCSI ストレージと FC ストレージを設定します。UCS

サーバのファームウェアバージョンを選択し、HyperFlexクラスタの名前を割り当てます。UCS Manager の設定 (71 ページ) を参照してください。

手順

ステップ 1 [一般的なハイパーバイザ設定を設定する(Configure Common Hypervisor Settings)] セクションで、次のフィールドに入力します。

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。 (注) <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 [クラスタ設定 (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。 • 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、コンマで区切ってください。

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

(注) ドラッグ アンド ドロップを使用してサーバを並べ替えることができます。

フィールド	説明
[名前 (Name)]	サーバに割り当てられた名前。
ロケータ LED (Locator LED)	サーバの検索をオンにします。

フィールド	説明
シリアル (Serial)	サーバのシリアル番号を表示します。
[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 3 [続行] をクリックして IP アドレスを設定します。「[IP アドレスの設定 \(77 ページ\)](#)」を参照してください。

IP アドレス の 設定

始める前に

[[ハイパーバイザ設定](#)] ページでハイパーバイザの設定が完了していることを確認します。[ハイパーバイザの設定 \(75 ページ\)](#) を参照してください。

手順

ステップ 1 [IP アドレス] ページで [IP アドレスを連続させる] を選択して、IP アドレスを連続させます。

ステップ 2 ハイパーバイザ、ストレージコントローラ (管理) とハイパーバイザ、ストレージコントローラ (データ) カラムの最初の行に IP アドレスを入力するとき、HX Data Platform インストーラで残りのノードについてもノード情報を段階的に自動入力します。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。

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

各 HX ノードについては、ハイパーバイザ、ストレージコントローラ、管理、データ IP アドレスを入力します。IP アドレスについては、ネットワークがデータ ネットワークまたは管理 ネットワークに属しているかを指定します。

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。

ステップ 3 ここで指定した 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。

次の IP アドレスを提供します。

フィールド	説明
管理クラスタ データの IP アドレス (Management Cluster Data IP Address)	HX データ プラットフォーム ストレージクラスタの管理ネットワーク IP アドレスを入力します。
データ クラスタ データ IP アドレス (Data Cluster Data IP Address)	HX Data Platform ストレージクラスタのデータネットワークの IP アドレスを入力します。
[Management Subnet Mask]	VLAN と vSwitch についてのサブネット情報を入力します。 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。
[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。
[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、10.193.0.1 と指定します。

ステップ 4 [続行] をクリックして HyperFlex クラスタ を設定します。「[HyperFlex クラスタ の 設定 \(79 ページ\)](#)」を参照してください。

HyperFlex クラスタ の 設定

[クラスタ設定 (Cluster Configuration)] ページで、Cisco HX ストレージ クラスタ の場合、次のフィールドを入力して HyperFlex クラスタ の展開を開始します。

始める前に

[IP アドレス] ページで IP アドレス の設定が完了していることを確認します。[IP アドレス の 設定 \(77 ページ\)](#) を参照してください。

手順

ステップ 1 [Cisco HX Cluster] セクションで、次のフィールドに入力します。

フィールド	説明
クラスタ名 (Cluster Name)	HX データ プラットフォーム ストレージ クラスタ の名前を指定します。
レプリケーション ファクタ (Replication Factor)	<p>ストレージ クラスタ 間 のデータ の冗長レプリカ の数を指定します。レプリケーション ファクタ を 2 つまたは 3 つ の冗長レプリカ に設定します。</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。 Hyperflex Edge を除くすべての環境で複製ファクタ 3 を強く推奨しています。複製ファクタ 2 では、可用性と復元性のレベルが低くなります。コンポーネントまたはノードの障害による停電のリスクは、アクティブかつ定期的なバックアップを作成することにより軽減されます。

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

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。

- 重要**
- コントローラ VM またはコントローラ VM のデータストアの名前は変更できません。
 - 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 つの小文字、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。

ステップ 3 [vCenter 構成 (vCenter Configuration)] セクションで、次のフィールドに入力します。

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

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

DNS サーバ (DNS Server(s))	各 DNS サーバの IP アドレスのカンマ区切りリスト。
NTP サーバ (NTP Server(s))	各 NTP サーバの IP アドレスのカンマ区切りリスト。 (注) ストレージコントローラ VM と ESXi ホストで動作するサービス間のクロック同期のために、すべてのホストが同じ NTP サーバを使用する必要があります。
DNS ドメイン名 (DNS Domain Name)	DNS FQDN または IP アドレスが無効です
タイムゾーン (Time Zone)	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。

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

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

ステップ 6 [高度な設定 (Advanced Configuration)] セクションで、次の手順を実行します。

フィールド	説明
ジャンボ フレーム ジャンボ フレームを有効化 (Enable Jumbo Frames)	ホスト 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 ディスク パーティションのクリーン アップ (Clean up Disk Partitions)	手動で準備されたサーバの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。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。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。 注目 工場準備されたシステムにはこのオプションを選択しないでください。工場準備されたシステムのディスクパーティションは正しく設定されています。

フィールド	説明
Virtual Desktop (VDI)	<p>VDI のみの環境でオンにします。</p> <p>(注) ストレージクラスタの作成後に VDI 設定を変更するには、リソースをシャットダウンまたは移動し、変更を加え (下の手順に記載)、クラスタを再起動します。</p> <p>デフォルトでは、HyperFlex クラスタは VSI ワークロード用にパフォーマンス調整されるように設定されています。</p> <p>このパフォーマンスのカスタマイズは、Hyperflex Data Platform クラスタで次の手順を実行することによって変更できます。HyperFlex クラスタを VDI から VSI ワークロード (またはその逆) に変更するには、次のようにします。</p> <p>警告: メンテナンスウィンドウが必要です。これにより、クラスタがオフラインの間はデータが使用できなくなります。</p> <ol style="list-style-type: none"> 1. <code>~#stcli cluster shutdown</code> を実行してクラスタをシャットダウンします。 2. すべてのコントローラ VM の <code>storfs cfg</code> を編集し、<code>workloadType</code> を <code>Vsi</code> または <code>Vdi</code> に変更します。 3. クラスタの作成後に、クラスタを起動し (<code>stcli cluster start</code>)、調整の変更を有効にします。
(オプション) vCenter Server のシングルサインオン (vCenter Single-Sign-On Server)	<p>この情報は、SSO URL が到達可能でない場合のみ必要です。</p> <p>(注) このフィールドは使用しないでください。これはレガシー展開に使用されます。</p> <p>[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。</p>

ステップ 7 [開始(Start)] をクリックして、HyperFlex クラスターの展開を開始します。[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] のセクション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。導入されたクラスターのステータスは、[オンライン (Online)] および [ヘルシー (Healthy)] として表示されます。
- [HyperFlex Connect の起動 (Launch HyperFlex Connect)] をクリックし、データストアを作成してクラスターを管理します。

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

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

手順

ステップ 1 コントローラ VM にログインします。

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

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

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

手順

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

症状	回避策
クラスタは動作していますが、vCenter と HX Connect UI で汎用アラートに注意するようにしてください。	サポートについては、Cisco の営業担当者にご連絡ください。
NR ペ어링が試行されると、クラスタはペ어링 エラーを報告します。	3.5.2 を実行しているクラスタでは、NR ペ어링は他のリリース (2.6、3.0.1、3.5.1、3.5.2) では許可されず、HX ハードウェア アクセラレーション カードによって有効にされたクラスタでは許可されません。
カードがオフラインになり、UI と vCenter でイベントがスローされると、インストール中にエラーが検出されます。	TAC に問い合わせサポートを受けてください。

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

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

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



第 9 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](#) (119 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](#) (120 ページ)
- [インストール後のスクリプトの実行](#) (121 ページ)
- [ESXi ホストルートパスワードの変更](#) (123 ページ)
- [ストレージコントローラパスワードの変更](#) (124 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](#) (124 ページ)
- [ストレージクラスタでのデータストアの追加](#) (125 ページ)
- [HA ハートビートの設定](#) (125 ページ)
- [HyperFlex の Auto Support と Smart Call Home](#) (126 ページ)
- [自己署名の証明書を CA 署名の証明書で置き換える](#) (133 ページ)
- [レプリケーション ペアリング](#) (134 ページ)
- [プライベート VLAN の追加](#) (134 ページ)
- [分散型仮想スイッチと Cisco Nexus 1000v](#) (139 ページ)
- [HX Data Platform での vCenter のホスト](#) (140 ページ)
- [AMD GPU の展開](#) (140 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。

手順

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

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

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

```
# pciPassthru.64bitMMIOSizeGB = "64"
```



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

インストール後のスクリプトの実行

インストーラ 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。



重要

- 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。

1. インストーラ VM でシェルに接続するには、SSH クライアントを使用します。
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 とシェルの警告を抑制します。
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。

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
Select post_install workflow-

1. New/Existing Cluster
2. Expanded Cluster
3. Generate Certificate

Note: Workflow No.3 is mandatory to have unique SSL certificate in the cluster.
By Generating this certificate, it will replace your current certificate.
If you're performing cluster expansion, then this option is not required.

Selection: 3
Certificate generation workflow selected

Logging in to controller 10.20.1.64
HX CVM admin password:
Getting ESX hosts from HX cluster...

Select Certificate Generation Workflow-

1. With vCenter
2. Without vCenter

Selection: 1
vCenter URL: 10.33.16.40
Enter vCenter username (user@domain): administrator@vsphere.local
vCenter Password:
Starting certificate generation and re-registration.
Trying to retrieve vCenterDatacenter information ....
Trying to retrieve vCenterCluster information ....
Certificate generated successfully.
Cluster re-registration in progress ....
Cluster re-registered successfully.
root@HyperFlex-Installer:~#

```

サンプルのネットワーク エラー

```

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

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

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

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

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

Cluster:
Version - 1.8.1a-19499
Model - HX220C-M4S
Health - HEALTHY
Access policy - LENIENT

```

```
ASUP enabled - False
SMTP server - smtp.cisco.com
```

ESXi ホスト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。

手順

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。

手順

ステップ1 ストレージコントローラ VM にログインします。

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

```
# stcli security password set
```

このコマンドによって、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。

手順

- 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、[vSphere Web Client にログイン (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。

手順

- 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。

手順

ステップ 1 vSphere にログインします。

ステップ 2 DRS が有効になっていることを確認します。

vSphere の[ホーム (Home)] > [ホストとクラスタ (Hosts and Clusters)] > 、[クラスタ (cluster)] > [設定 (Configure)]、[サービス (Services)]を選択します。[vSphere DRS] をクリックします。

ステップ 3 [Edit] ボタンをクリックします。[vSphere HA] をクリックします。[Edit] をクリックします。

ステップ 4 選択されていない場合は、[vSphere HA をオンにする (Turn on vSphere HA)] を選択します。

ステップ 5 ドロップダウンメニューから [アドミッション コントロール (Admission Control)] > [フェールオーバー容量の定義 (Define Failover capacity by)] > [クラスタ リソース割合 (Cluster resource percentage)] を展開します。デフォルト値を使用することも、[Override calculated failover capacity] を有効にしてパーセンテージを入力することもできます。

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

ステップ 7 [OK] をクリックします。

HyperFlex の 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。



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

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 (128 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 (129 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 \(130 ページ\)](#) 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

一般に、Auto Support (ASUP) はHXストレージクラスタの作成中に設定されます。設定されなかった場合、HX Connect ユーザ 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。

手順

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。
[Terms and Conditions (使用条件)] チェック ボックス	エンドユーザー使用契約。自動サポート機能を使用するには、このチェック ボックスをオンにする必要があります。
[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。

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。

手順

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 を使用するには次の必要があります。

- 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

手順

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問い合わせてください。

```
root@ucs-stct1vm-554-1:/tmp# asupcli post --type alert
/bin/sh: 1: ansible: not found
Failed to post - not enough arguments for format string
root@ucs-stct1vm-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。

オプション	必須またはオプション	説明
<code>--portal-url PORTALURL</code>	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)。
<code>--proxy-url PROXYURL</code>	オプション。	HTTP プロキシの URL を指定します (該当する場合)。
<code>--proxy-port PROXYPORT</code>	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)。
<code>--proxy-user PROXYUSER</code>	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。

自己署名の証明書を CA 署名の証明書で置き換える

CA 証明書のインポートは、シェルスクリプトによって自動化されています。任意の CVM、できれば CIP ノードから CSR（証明書署名要求）を生成します。各 CVM は同じ証明書でインストールする必要があるため、クラスタに必要な CSR は 1 つだけです。CSR を生成するとき、管理 CIP に割り当てられたホスト名をサブジェクトの識別名の共通名として入力する必要があります。

次に例を示します。

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:HyperFlex
Common Name (e.g. server FQDN or YOUR name) []:<hostname-cluster-management-IP>
Email Address []:support@cisco.com
```

CA 証明書を取得したら、自動スクリプトを使用して証明書をインポートします。スクリプトは、その CVM の証明書のみを更新します。



- (注) クラスタ拡張の場合は、証明書をインポートするために、同じ証明書とキーファイルを使用して、拡張されたノード CVM でスクリプトを再度実行する必要があります。

手順

ステップ 1 CVM でのスクリプトの場所は、`/usr/share/springpath/storfs-misc/hx-scripts/` です。

```
certificate_import_input.sh
run stcli cluster reregister
```

ステップ 2 コントローラ VM (CIP を指す) で、このコマンドを実行して CSR 要求を生成します。

```
openssl req -nodes -newkey rsa:2048 -keyout /etc/ssl/private/<Host Name of the CVM>.key
-out /etc/ssl/certs/<Host Name of the CVM>.csr
cat /etc/ssl/certs/<host name mapped to the management CIP>.csr - Copy the request
to any notepad.
Send the request to CA to generate the certificate
```

ステップ 3 CA (.crt ファイル) から証明書を受信したら、証明書とキーを各 CVM にコピーします。

ステップ 4 各 CVM で、`./certificate_import_input.sh` スクリプトを使用して証明書をインポートします。

```
root@SpringpathControllerVUFSTDS58L:/usr/share/springpath/storfs-misc/hx-scripts#
./certificate_import_input.sh
```

ステップ5 キーのパスとして、`/etc/ssl/private/<CVMのホスト名>.key`を入力します。

ステップ6 <CAへのパス.crtファイル>という証明書形式で証明書のパスを入力します。

(注) すべての入力を入力した後、インポートプロセスが完了するまでにいくらか時間がかかります。

ステップ7 CIPをポイントしているCVMから`stcli reregister`コマンドを実行して、クラスタをvCenterに再登録します。証明書をインポートしたら、クラスタを再登録する必要があります。

レプリケーションペアリング

レプリケーションクラスタペアの作成は、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 6: 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 \(135 ページ\)](#)。
- [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 \(136 ページ\)](#)。

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

手順

- 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 \(136 ページ\)](#) 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。

手順

- 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

手順

- 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 \(136 ページ\)](#)
- 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。
 - a) 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。
 - b) 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。
 - c) [Next] をクリックします。
 - d) 移行する**仮想マシン**を選択します。
 - e) [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。
 - a) vCenter 仮想マシンを右クリックして、[Edit Settings] をクリックします。
 - b) [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

手順

-
- 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 [閉じる (Close)] をクリックします。
-

vSphere 分散スイッチの作成

手順

-
- 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 [完了 (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

手順

- 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 を右クリックします。
- ステップ 3 [Edit Settings] をクリックします。
- ステップ 4 [Private VLAN] タブを選択します。
- ステップ 5 [Primary private VLAN ID] タブで、プライベート VLAN ID を入力します。
- ステップ 6 [Secondary private VLAN ID] タブで、プライベート VLAN ID を入力します。
- ステップ 7 [Type] ドロップダウン リストから、VLAN のタイプを選択します。有効な値は次のとおりです。

- [Isolated]
- [Community]
- 無差別(デフォルト)

ステップ 8 [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。

手順

- 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。

手順	操作	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
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 10 章

複数の HX クラスタの設定

- [複数のクラスタの設定 \(143 ページ\)](#)

複数のクラスタの設定

複数の HyperFlex クラスタを同じ UCS ドメイン (ファブリック インターコネクットのペア) の下に共存させることができます。次のガイドラインに従い、ドメインに接続されているすべての機器に対して、スムーズに運用できるようにする必要があります。



- (注) 2つの異なる HX 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

- 標準 HXDP ライセンスを使用する場合、コンピューティング専用ノードの数は、コンバージドノードの数以下にする必要があります。エンタープライズ HXDP ライセンスでは、コンバージドノードに対して、最大 2:1 比のコンピューティングを使用できます。
- 新しい HyperFlex クラスタを作成するには、第 2 章に示されている要件をすべて満たしていることを確認してください。また、第 4 章に示されているプロセスに従ってください。
- 展開については、HX Data Platform インストーラを使用します。
- HX クラスタのすべてのノードは、同じポリシーとサービスプロファイルを参照する必要があります。
- 各 HX クラスタの一意的な名前を割り当てます。
- 各 HX クラスタは、インストールの一部として固有のサブ組織に作成されます。この階層は、固有のポリシーがクラスタごとに作成されるようにするため、変更しないでください。

- 各クラスタは、固有のストレージデータ VLAN を使用して、すべてのストレージトラフィックを分離しておく必要があります。複数のクラスタにわたってこの VLAN を再利用することは推奨されません。
- VLAN (管理およびゲストトラフィック VLAN など) を再利用する場合は、UCSM にすでに存在していても、VLAN ごとに新しい固有の VLAN 名を作成します。これにより、そのドメイン内の他のクラスタやサーバが中断されることはなくなります。
- 互換性のある Cisco UCS Manager と Cisco HyperFlex 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。

- 同じ Cisco HX データ プラットフォーム インストーラを使用して別の vCenter に 2 番目のクラスタを設定する前に、ブラウザのキャッシュをクリアしてください。これにより、古いクラスタの IP アドレスがキャッシュされ展開が失敗するなどの問題が回避されます。



(注) トラフィックに応じて、さらにアップリンクポートを追加する必要がある場合があります。



(注) ファブリックインターコネクトの同じペアに接続されている複数のクラスタ間で、同じ VLAN を使用することができます (管理、vMotion、VM ゲスト VLAN など)。これは、IP が重複しない限り可能です。ただし、ストレージトラフィックが安全に分離されるように、クラスタごとに HX ストレージ VLAN を異なる状態に保つことを推奨します。ベストプラクティスに対してストレージ VLAN を再利用する場合は、IP の重複を避けるために細心の注意をしてください。重複 IP があると、別のクラスタの既存のストレージトラフィックが中断される可能性があります。

手順

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 11 章

Cisco HyperFlex システム クラスタの展開

- クラスタ展開のガイドライン (145 ページ)
- 混合 M4/M5 クラスタを作成する場合の前提条件 (146 ページ)
- 混合クラスタ展開のガイドライン (147 ページ)
- 混合クラスタ展開中の手順 (148 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 (149 ページ)
- コンバージド ノードの準備 (150 ページ)
- 既存のクラスタへのコンバージド ノードの追加 (150 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 (161 ページ)
- コンピューティング専用ノードの準備 (162 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 (165 ページ)
- クラスタ展開の障害の解決 (173 ページ)
- ロジカル アベイラビリティ ゾーンの有効化 (173 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。



(注) HW RAID M.2 (UCS-M2-HWRAID および HX-M2-HWRAID) は、コンピューティング専用ノードではサポートされていません。

- 検出されたクラスタをクリックして、3.5x またはそれ以前のリリースの標準 ESX クラスタの拡張を続行します。そうしないとエラーになります。
- 拡張ワークフローの中でコントローラ VM の管理クレデンシャルのみを使用します。管理以外の他のクレデンシャルを使用すると、拡張に失敗する可能性があります。

ESXi インストール ガイドライン

1. コンピューティング ノードのブート ポリシーを変更します。
M5 サーバの HyperFlex ストレッチ クラスタ コンピューティング専用ノードのテンプレートおよびブート ポリシーを変更するには:
 1. テンプレートの複製
 2. コンピューティング M5 ノードにフラッシュカードがない場合、ローカルブートポリシーから Flex flash のチェックを外します。
 3. 適切な WWPN で SAN ブートをブート順序に追加します。
2. DPI 拡張ワークフローを開始します。
3. プロンプトされる場合、ISO イメージを使用して ESXi をインストールします。
4. DPI 拡張ワークフローに戻り、ESXi インストール ワークフローを完了します。



(注) Hypervisor 設定が失敗し、SOL ロギングの障害メッセージが表示される場合、ルートおよびデフォルト パスワードを使用して SSH でインストーラ CLI にアクセスし、ESXi ハイパーバイザを設定します。そして、高度なインストーラを実行し、**[HX Storage Software (HX ストレージ ソフトウェア)]** および **[Expand Cluster (クラスタの拡張)]** チェック ボックスをチェックして、ESXi インストール プロセスを続行します。

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。

- **Hypercheck ヘルス チェック ユーティリティ:** アップグレードする前に、Hypercheck クラスタでこの予防的ヘルス チェック ユーティリティを実行することを推奨します。これらのチェックにより、注意が必要なエリアがすぐに見やすくなり、シームレスなアップグレードエクスペリエンスを保証します。Hypercheck のインストールと実行方法の完全な

手順の詳細については、『[Hyperflex 健全性および事前アップグレードチェック ツール](#)』を参照してください。

- 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。

混合クラスタ展開のガイドライン

- 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。ドライブの互換性については、『[Cisco Hyperflex Drive Compatibility](#)』ドキュメントを参照してください。
 - 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。
- HX Edge、SED、LFF、Hyper-v、およびストレッチ クラスタは、混合 M4 および M5 クラスタをサポートしていません。

リリース 3.5 向け混合クラスタ拡張のガイドライン

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。

混合クラスタ展開中の手順

- 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ー ノードと一致すること。
- HyperFlex クラスターですでに使用されているものとは異なる CPU ファミリを持つノードを追加するには、EVC を有効にします。詳細については、『Cisco HyperFlex Systems インストールガイド (VMware ESXi 向け)』の「混在 CPU を伴うクラスターの設定」の項を参照してください。
- ノードのソフトウェアバージョンが、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) クラスターをアップグレードする場合は、クラスターで実行されている 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

手順

-
- 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。
- 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) 取り外したコンバージドノードやディスクは、元のクラスタで再利用しないでください。
-

既存のクラスタ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。
-

手順

-
- ステップ 1** Cisco HX Data Platform インストーラ を起動します。
- Web ブラウザで、HX 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。
 - 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。ユーザーが入力した新しいパスワードを指定しない限り、インストールを続行できません。

- 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問い合わせてください。

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]	

フィールド	説明
[vCenter Server]	vCenter Server の FQDN または IP アドレス。 たとえば <code>10.193.211.120</code> と入力します。 (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 : <code>administrator@vsphere.local</code> 。
[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 ノードのルートです。
[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 <code>Cisco123</code> です。 (注) システムは、デフォルトのパスワード [<code>Cisco123</code>] 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。ユーザーが入力した新しいパスワードを指定しない限り、インストールを続行できません。

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 (Admin. 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 (Admin. VLAN ID)	デフォルトの VLAN ID : 3092
[VLAN for VM vMotion]	
[VLAN Name]	名前 : hx-vmotion
VLAN ID (Admin. VLAN ID)	デフォルトの VLAN ID : 3093

フィールド	説明
[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、hx-ext-storage-fc-a 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 ゾーニングを使用してインストーラで既存の VSAN ID を入力する場合、ゾーニングは VSAN ID の既存の環境で無効になります。
[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、hx-ext-storage-fc-b 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 ゾーニングを使用してインストーラで既存の VSAN ID を入力する場合、ゾーニングは VSAN ID の既存の環境で無効になります。</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(1d)。</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>クラスタの固有の組織名を表示して、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]	
[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、 <i>255.255.0.0</i> と指定します。
[Gateway]	ゲートウェイの IP アドレス。 たとえば、 <i>10.193.0.1</i> 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、コ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。
[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、『<i>Cisco HX Data Platform Management Guide</i>』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 工場で準備されたシステムにはこのオプションを選択しないでください。工場で準備されたシステムのディスクパーティションは正しく設定されています。手動で準備されたサーバでは、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) 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 クラスターの作成後にクラスターに追加できます。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、クラスター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。

- 追加する新しいノードが HX クラスターですでに使用されているものとは異なる CPU ファミリ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 を伴うクラスターの設定」の項を参照してください。

- ノードのソフトウェアバージョンが、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、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。



(注) HW RAID M.2 (UCS-M2-HWRAID および HX-M2-HWRAID) は、コンピューティング専用ノードではサポートされていません。

コンピューティング専用ノードの準備

手順

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。

- 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。
- [UCS Manager の起動 (Launch UCS Manager)] ボタンをクリックします。
- プロンプトが表示された場合は、Java をダウンロードして、インストールし、受け入れます。
- 管理者クレデンシャルを使用してログインします。

ユーザ名: **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

手順

- 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。

手順

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。

手順

-
- 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、[サーバ (Servers)] > [サービス プロファイル (Service Profiles)] > [サブ組織 (Sub-Organizations)] > [hx-cluster] をクリックします。
 - [hx-cluster] を右クリックして、[KVM 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。

- b) [Enter boot selection] メニューから、矢印キーを使用して **Cisco vKVM-Mapped vDVD1.22** オプションを強調表示します。
- c) **Enter** キーを押して、選択します。

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。**ESXiDCUI** 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。



- (注) 既存のクラスタにコンピューティング専用ノードを追加した後、vmotion の vmk2 インターフェイスを手動で設定する必要があります。

手順

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。ユーザーが入力した新しいパスワードを指定しない限り、インストールを続行できません。

- 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問い合わせてください。

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]	

フィールド	説明
[vCenter Server]	vCenter Server の FQDN または IP アドレス。 たとえば <code>10.193.211.120</code> と入力します。 (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 : <code>administrator@vsphere.local</code> 。
[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 ノードのルートです。
[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 <code>Cisco123</code> です。 (注) システムは、デフォルトのパスワード [<code>Cisco123</code>] 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。ユーザーが入力した新しいパスワードを指定しない限り、インストールを続行できません。

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、[管理 IP アドレス 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 [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。クラスタ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 (Admin. 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]	
[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 : hx-vm-network
[VLAN ID]	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	

フィールド	情報
[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、 <i>10.193.211.124-127</i> 、 <i>10.193.211.158-163</i> 、 <i>255.255.255.0</i> 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、 <i>10.193.0.1</i> 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、 <i>255.255.0.0</i> と指定します。
[Default gateway]	IP アドレス。 たとえば、 <i>10.193.0.1</i> 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、 <i>3.2(1d)</i> 。
[HyperFlex Cluster Name]	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。

(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 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 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、 <i>255.255.0.0</i> と指定します。
[Gateway]	ゲートウェイの IP アドレス。 たとえば、 <i>10.193.0.1</i> 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、コ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 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	<p>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。</p> <p>(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。</p>

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。[ローカルディスクの設定ポリシー] 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. [ローカルディスク設定ポリシーの作成] 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、**[Continue (続行)]** をクリックして、**[Retry UCSM Configuration (UCSM 構成の再試行)]** をクリックします。

Compute Node Expansion - ESXi Installation Required

ESXi must be installed on all nodes being added at this point using the HX ESXi ISO on [cisco.com](https://www.cisco.com)

Using an existing installation of ESXi will cause installation to fail. Other ESXi ISOs other than the one posted on Cisco are not supported.

Once ESXi is installed, select Continue and then Retry to continue installation.
Full instructions can be found below.

If ESXi is already installed using the HX ESXi ISO wait for it to boot and then select Continue and Retry to continue installation.

 Instructions

 Launch UCS Manager

Continue

(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、「ホストは手動で vCenter に追加する必要があります (The host needs to be manually added to vCenter)」というメッセージが出されます。展開操作を正常に実行するには、次のようにします。

- vSphere クライアントに追加する ESXi ホストにログインします。
- コントローラ VM の電源をオフにします。
- ホストを vSphere Web Client の vCenter クラスタに追加します。
- 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。

- VMware vSphere クライアントにログインします。
- [Home] > [Hosts and Clusters] > [Datacenter] > [Cluster] > [Host]** の順に選択します。
- 新規ノードを選択します。
- 右クリックして **[Reconfigure for vSphere HA]** を選択します。

ステップ 12 既存のクラスタにコンピューティング専用ノードを追加した後、vmotion の vmk2 インターフェイスを手動で設定する必要があります。

クラスタ展開の障害の解決

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。

手順

- 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** [初めからやり直す (Start Over)] : 進捗テーブル エントリを消去することで、適用した設定を無効にし、[Cluster Configuration] ページに戻って新しい展開を再度開始できます。テクニカル アシスタンス センター (TAC) を参照してください。
- ステップ 3** [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のみ選択します。

HyperFlex の再展開を目的としたノードのクリーンアップの詳細については、『[HyperFlex Customer Cleanup Guides for FI and Edge](#)』を参照してください。

ロジカル アベイラビリティ ゾーンの有効化

HyperFlex クラスタ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、クラスタ内の複数のノード間で大規模なデータ移動が行われる場合があります。これにより、クラスタ内の IO パフォーマンスが低下する可能性があります。
<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>

論理可用性ゾーンの要件および制限事項

論理可用性ゾーン (LAZ) には次の要件や制限事項が適用されます。

- インストール処理中に論理可用性ゾーンを設定できるのは、8 ノード以上の HyperFlex クラスタのみです。
- 論理可用性ゾーンは、HyperFlex クラスタのインストール中に有効にするか、または後でコマンドラインインターフェイスから有効にすることができます。クラスタ全体のデータの大規模な移行と再編成を避けるため、この機能はインストール中に有効にするをお勧めします。データの大規模な移行と再編成では、すでにデータが含まれているクラスタで LAZ を有効にしている場合、データ分散規則に従う必要があります。
- ゾーンの数は、手動で 3、4、5 に指定するか、またはインストーラを通じて自動的に選択するようにできます (推奨設定)。インストーラでゾーン数を決定する場合、ゾーン数はクラスタのノード数に基づいて決定されます。

3 としての RF を引き受けるノード数と結果として生じるゾーン数のマッピング表がここにあります

クラスターのハイパーコンバージドノードの数	クラスターのゾーンの数
8	4
9	3
10	5
11	3
12	3
13	3
14	7
15	3
16	4
17	3
18	3
19	3
20	4
21	3
22	11
23	3
24	3
25	5
26	13
27	3
28	4
29	3
30	3
31	3
32	4

[HyperFlex Connect] > [System information (システム情報)]、[HyperFlex Connect] > [Dashboard (ダッシュボード)] にそれぞれアクセスして、LAZ ステータスを表示し、どのノードがどのゾーンにあるかチェックします。

また、CLI を使用して LAZ の詳細を表示するには、次のコマンドを実行します。

```
stcli cluster get-zone

zones:
-----
pNodes:
-----
state: ready
name: 10.10.18.61
-----
state: ready
name: 10.10.18.59
-----
zoneId: 0000000057eebaab:00000000000000003
numNodes: 2
-----
pNodes:
-----
state: ready
name: 10.10.18.64
-----
state: ready
name: 10.10.18.65
-----
zoneId: 0000000057eebaab:00000000000000001
numNodes: 2
-----
pNodes:
-----
state: ready
name: 10.10.18.60
-----
state: ready
name: 10.10.18.63
-----
zoneId: 0000000057eebaab:00000000000000004
numNodes: 2
-----
pNodes:
-----
state: ready
name: 10.10.18.58
-----
state: ready
name: 10.10.18.62
-----
zoneId: 0000000057eebaab:00000000000000002
numNodes: 2
-----
isClusterZoneCompliant: True
zoneType: logical
isZoneEnabled: True
numZones: 4
AboutCluster Time : 08/22/2019 2:31:39 PM PDT
```

- HyperFlex クラスタによって各ゾーンにどのノードが参加するかが決定されます。この設定は変更できません。

- 容量の利用とデータの分散を最もバランス良く保つため、クラスタ内のノード数を3、4、5、または7の倍数にすることをお勧めします。たとえば、8ノードは2台のサーバによる4つのゾーンに均等に分割され、9ノードは3台のサーバによる3つのゾーンに均等に分割されます。11ノードでは、ゾーン間でノード数のバランスが悪くなり、ノードにおける容量の利用のバランスが悪くなります。
- LAZを有効にしてクラスタを動作させている場合は、クラスタの拡張をゾーン数の倍数で行ってください。そのように拡張することで、各ノードでノード数の一致が保たれ、容量の利用のバランスが悪くなるのを防ぎます。たとえば、3つのゾーンがあるクラスタは、さらに3つのノードを追加して拡張します。これは、1つまたは2つのノードしか追加しないとバランスが悪くなるからです。4つのノードを追加しても同様です。

ゾーンより小さいノードを含むクラスタの拡張

クラスタ内での論理可用性ゾーン(LAZ)の設定には、いくつかの要件とガイドラインがあります。[論理可用性ゾーンの要件および制限事項 \(174ページ\)](#) を参照してください。これらの要件を無視する場合、次の手順でクラスタを展開できます。

手順

ステップ1 LAZを無効にします。

```
stcli cluster set-zone --zone 0
```

数分待機すると、およそ5分ほどでLAZが無効になります。

ステップ2 クラスタにノードを追加します。

ステップ3 ノードがクラスタに追加された後、LAZを有効にします。

```
stcli cluster set-zone --zone 1
```

ゾーン数が明示的に設定されていない場合、デフォルトで4ゾーンが作成されます。

ステップ4 クラスタ内で再バランシングを開始します。

```
stcli rebalance start
```

- (注)
- ノードの再バランシングにより、クラスタのパフォーマンスが30%～40%ほど低下する可能性があります。
 - クラスタ内のノードの再バランシングにかかる時間は、クラスタのサイズとクラスタ内のデータによって異なります。`stcli rebalance status` コマンドを使用して、再バランシング アクティビティの進捗を確認できます。

ステップ5 クラスタ設定を確認し、クラスタがゾーンに準拠するか判断します。

```
stcli cluster get-zone
```




第 12 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 \(179 ページ\)](#)
- [混合 CPU を使用するための前提条件 \(179 ページ\)](#)
- [EVC モードとの CPU 互換性 \(180 ページ\)](#)
- [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 \(180 ページ\)](#)

概要

HyperFlex は、同じファブリック インターコネクトで 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。

新世代のサーバを追加する統一クラスタ、そしてサーバの世代が混合した既存のクラスタという考慮すべき 2 つのパスがあります。

均一クラスタへの新世代サーバの追加

クラスタが現在均一で、新世代サーバをクラスタに追加する場合は、VC で現在の世代の EVC モードを選択することで、EVC オンラインを中断せずに有効にすることができます。次に、拡張を使用して通常どおりに続行します(コンバージドまたはコンピューティングのみ)。拡張が試行される前に、EVC モードが設定されていることが必須です。

クラスタ拡張を実行する前に、均一クラスタで EVC モードを有効にするには、次の手順を実行します。

手順

ステップ 1 HX クラスタで vMotion との拡張された互換性 (EVC) を有効にする

- a) vSphere Web Client ナビゲータから、[Hosts and Cluster] > [Datacenter] > [HX Cluster] を選択します。
- b) 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。
- c) [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 2 HyperFlex インストーラを使用したコンピューティングのみまたはコンバージド ノードの展開を続行します。

既存のクラスタへの混合または旧世代サーバの追加

クラスタにはすでにサーバの世代が混在しているか、既存のクラスタに旧世代のサーバを追加する必要があります(コンピューティング専用ノード)。



- (注) 新しいノードを持つクラスタ拡張ワークフロー中に EVC モードが有効になっていない場合は、これらの手順に従ってください。

旧世代サーバを既存のクラスタに追加するには、次の手順を実行します。

手順

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。

- 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。
- controller_vm** を右クリックするか、[Actions] メニューから [Power] > [Shut Down Guest OS] を選択します。

ステップ 5 各 HX ホストをメンテナンス モードにします。

- vSphere Web Client ナビゲータから、[ホストとクラスタ (Hosts and Clusters)] > [データセンター (Datacenter)] > [HX Cluster クラスタ (HX Cluster)] > [ノード (node)] の順に選択します。
- ノードを右クリックし、[Maintenance Mode] > [Enter Maintenance Mode] の順に選択します。

(注) この操作に Cisco HX メンテナンス モード (Cisco HX Maintenance Mode) メニューを使用しないでください。

ステップ 6 HX クラスタで vMotion との拡張された互換性 (EVC) を有効にする

- 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。

- c) [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。

- a) vSphere Web Client ナビゲータから、[ホストとクラスタ (Hosts and Clusters)] > [データセンター (Datacenter)] > [HX Cluster クラスタ (HX Cluster)] > [ノード (node)] の順に選択します。
- b) ノードを右クリックし、[Maintenance Mode] > [Exit Maintenance Mode] の順に選択します。

(注) この操作に Cisco HX メンテナンス モード (Cisco HX Maintenance Mode) メニューを使用しないでください。

ステップ 8 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。

- a) 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。
- b) [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。

ステップ 12 HyperFlex インストーラを使用したコンピューティングのみの展開を続行します。



第 13 章

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

- [概要 \(185 ページ\)](#)
- [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 \(185 ページ\)](#)
- [VMware ESXi をインストールします。 \(186 ページ\)](#)

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 の再導入。

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。

手順

-
- 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。
- [Customized Workflow] を選択します。
 - [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。
『VMware ESXi の Cisco HyperFlex システム インストール ガイド』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。
- [Customized Workflow] を選択します。
 - [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。

手順

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。

手順

- 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ーをクリックします。
- ステップ 20 [Boot Order] リストで [CIMC Mounted CD/DVD] エントリーを選択し、[Move Up] ボタンを何度かクリックして [CIMC Mounted CD/DVD] エントリー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。

手順

- 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 [サーバ (Servers)] > [サービス プロファイル (Service Profiles)] > [ルート (Root)] > [サブ組織 (Sub-Organizations)] > [HX クラスタ (hx-cluster)] > [ラック ユニット番号 (rack-unit-number)] の順に展開します。
- ステップ 3 [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。

手順

- 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。

手順

- 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。



APPENDIX **A**

HX サーバ QoS システム クラスの設定

Cisco UCS は、DCE（Data Center Ethernet）を使用して、Cisco UCS ドメイン内のすべてのトラフィックを処理します。イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が 8 つの仮想レーンに分割されています。内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。それ以外の 6 つの仮想レーンの Quality of Service（QoS）を設定できます。Cisco UCS ドメイン全体にわたり、これら 6 つの仮想レーンで DCE 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

各システム クラスは特定のタイプのトラフィック用に帯域幅の特定のセグメントを予約します。これにより、過度に使用されるシステムでも、ある程度のトラフィック管理が提供されます。たとえば、ファイバチャネルプライオリティ システム クラスを設定して、FCoE トラフィックに割り当てられる DCE 帯域幅の割合を決定することができます。

UCS Manager で QoS システム クラスを設定するには、次の手順を実行します。

Procedure

- ステップ 1** Web ブラウザを開き、Cisco UCS Manager の IP アドレスを入力します。ログイン クレデンシャルを入力します。
- ステップ 2** Cisco UCS Manager で、[LAN] タブに移動します。
- ステップ 3** [LAN] タブで、[LAN] > [LAN Cloud] を展開します。
- ステップ 4** [QoS System Class] ノードを選択します。
- ステップ 5** [Work] ペインで、[General] タブをクリックします。
- ステップ 6** システムのトラフィック管理ニーズを満たすために設定するシステムクラスの次のプロパティを更新します。

Priority	イネーブル	QoS	パケット損失	重量	[MTU]	マルチキャストの最適化
----------	-------	-----	--------	----	-------	-------------

Platinum	有効にするシステムのチェックボックスをオンにします。	5	いいえ	4	9216	いいえ
Gold		4	対応	4	normal	いいえ
Silver		2	はい	ベストエフォート	normal	はい
Bronze		1	はい	ベストエフォート	9216	いいえ
ベストエフォート		いずれか	はい	ベストエフォート	normal	いいえ
fibre Channel		3	なし	5	fc	該当なし

Note 新しい Cisco UCS ドメイン設定で Platinum および Bronze システム クラスの MTU 値を変更すると、以下の警告メッセージを受信する場合があります。

- Validating MTU change for QoS system class: 'platinum'. Failed: Cannot change MTU from '1500' to '9216' since it is currently in use by '0' service profile(s).
- Validating MTU change for QoS system class: 'bronze'. Failed: Cannot change MTU from '1500' to '9216' since it is currently in use by '0' service profile(s).

ステップ 7 [Save Changes] をクリックします。

- [HX サーバ用の VLAN の作成 \(193 ページ\)](#)
- [MAC アドレス プールの作成 \(194 ページ\)](#)
- [QoS ポリシーの作成, on page 196](#)
- [HX サーバ用の vNIC テンプレートの作成 \(198 ページ\)](#)
- [vSwitch の設定 \(203 ページ\)](#)
- [仮想分散スイッチ \(VDS\) または Cisco Nexus 1000v \(N1Kv\) への vMotion ネットワークの移行 \(204 ページ\)](#)
- [Stats Daemon のリセット \(207 ページ\)](#)
- [HyperFlex HX シリーズ サーバ ディスクの詳細 \(207 ページ\)](#)
- [HyperFlex をインストールする際の有効性検査 \(208 ページ\)](#)

HX サーバ用の VLAN の作成

手順

ステップ 1 Web ブラウザを開き、Cisco UCS Manager の IP アドレスを入力します。ログインクレデンシャルを入力します。

ステップ 2 [LAN] タブ > [LAN] > [LAN Cloud] > [VLANS] に移動します。

ステップ 3 次の表に示すように、右クリックして [Create VLANs] を選択します。

VLAN 名	説明	マルチキャスト ポリシー名	VLAN ID (デフォルト)
hx-inband-mgmt	次で使用されます。 <ul style="list-style-type: none"> • ESX 管理 • ストレージコントローラ VM への SSH • HX クラスタ管理 IP : マルチキャストトラフィックを使用 • HX データプラットフォームプラグイン用の HyperFlex VM への vCenter 接続 	HyperFlex	3091
hx-storage-data	次で使用されます。 <ul style="list-style-type: none"> • ESX NFS クライアント (IOvisor) • HyperFlex レプリケーション/クラスタ • クラスタ データ VIP 	HyperFlex	3092
hx-vmotion	次で使用されます。 <ul style="list-style-type: none"> • VM およびストレージ vMotion、FT、iSCSI 	HyperFlex	3093
insert existing vlan name	次で使用されます。 <ul style="list-style-type: none"> • VM データ トラフィック 	HyperFlex	任意*

(注)

- 設定オプションは [Common/Global] です。これは、両方のファブリックに適用され、いずれの状況でも同じ設定パラメータが使用されます。
- *VM データ VLAN に関する特別な推奨事項はありません。VM データ トラフィック用の独自の VLAN を作成できます。デフォルトでは、HXDP インストーラは VM データ トラフィック用の VLAN を作成しません。
- 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。

MAC アドレス プールの作成

すでに存在する可能性がある MAC アドレスの重複を避けるために、デフォルトの MAC アドレスのブロックを変更できます。各ブロックには、デフォルトで 100 個の MAC アドレスが含まれており、UCS システムごとに最大 100 の HX サーバを展開できます。トラブルシューティングを容易にするために、vNIC ごとに 1 つの MAC プールを使用することを推奨します。



- (注) 8 桁目は A または B に設定します。「A」は、ファブリック インターコネクト A にピン接続された vNIC で設定されます。「B」は、ファブリック インターコネクト B にピン接続された vNIC で設定されます。

手順

- ステップ 1** Web ブラウザを開き、Cisco UCS Manager の IP アドレスを入力します。ログインクレデンシャルを入力します。
- ステップ 2** Cisco UCS Manager で、[LAN tab] > [Pools] > [root] > [Sub-org] > [hx-cluster] > [MAC Pools] に移動します。
- ステップ 3** [MAC Pools] を右クリックし、[Create MAC Pool] を選択します。
- ステップ 4** [Create MAC Pool] ウィザードの [Define Name and Description] ページで、次に示すように必須フィールドに入力します。

MAC プール名	説明	割り当て順序	MAC アドレス ブロック
hv-mgmt-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:01:01-64
hv-mgmt-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:02:01-64

storage-data-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:03:01-64
storage-data-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:04:01-64
vm-network-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:05:01-64
vm-network-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:06:01-64
hv-vmotion-a	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:07:01-64
hv-vmotion-b	HyperFlex システム用 MAC プール	Sequential	00:25:B5:XX:08:01-64

ステップ 5 [Next] をクリックします。

ステップ 6 [Create MAC Pool] ウィザードの [Add MAC Addresses] ページで、[Add] をクリックします。

ステップ 7 [Create a Block of MAC Addresses] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[First MAC Address] フィールド	ブロック内の最初の MAC アドレス。
[Size] フィールド	ブロック内の MAC アドレス数。

ステップ 8 [OK] をクリックします。

ステップ 9 [完了 (Finish)] をクリックします。

MAC アドレスの変更後、以前に設定されたように ESXi が再設定されます。しかし、管理 IP には DHCP が割り当てられたため、IP が変わります。

MAC アドレス変更に対する製造プロセスの影響

- 特に顧客が UCS ファブリック インターコネクトがない HyperFlex サーバを発注する場合、製造プロセスと顧客サイトの間で MAC アドレスが変わります。
- MAC アドレスは、サービスプロファイルの関連付けの際に設定されます。サービスプロファイルの関連付けの解除の間は、設定されせん。
- 製造プロセスの最後で、サービスプロファイルの関連付けが解除されます。つまり、MAC アドレスが未設定になります。
- HyperFlex サーバを導入する場合は、MAC アドレス プールを上記のように設定します。

- VMWare は Consistent Device Naming (CDN) をサポートしていますが、5.5.SR が公開されて以来、問題が報告されています。

QoS ポリシーの作成

Quality Of Service (QoS) ポリシーは、vNIC または vHBA に向けた発信トラフィックにシステムクラスを割り当てます。このシステムクラスにより、このトラフィックに対する Quality Of Service が決定されます。

vNIC ポリシー、または vHBA ポリシーに QoS ポリシーをインクルードし、その後、このポリシーをサービス プロファイルにインクルードして、vNIC または vHBA を設定する必要があります。

次の表は、設定可能なシステム クラスをまとめたものです。

Table 7: システム クラス

システム クラス	説明
プラチナ Gold Silver ブロンズ	サービスプロファイルの QoS ポリシーに含めることができる設定可能なシステム クラスのセット。各システム クラスはトラフィック レーンを 1 つ管理します。 これらのシステム クラスのプロパティはすべて、カスタム 設定やポリシーを割り当てるために使用できます。
ベスト エフォート	ベーシック イーサネット トラフィックのために予約されたレーンに対する QoS を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップ ポリシーがあります。このシステム クラスをディセーブルにはできません。

システム クラス	説明
ファイバ チャンネル	<p>Fibre Channel over Ethernet トラフィックのために予約されたレーンに対する Quality Of Service を設定するシステム クラス。</p> <p>このシステムクラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。たとえば、このクラスには、データパケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。このシステムクラスをディセーブルにはできません。</p> <p>Note FCoE トラフィックには、他のタイプのトラフィックで使用できない、予約された QoS システムクラスがあります。他のタイプのトラフィックに FCoE で使用される CoS 値がある場合、その値は 0 にリマークされます。</p>

UCS Manager で QoS ポリシーを作成するには、次の手順を実行します。

Procedure

- ステップ 1 Web ブラウザを開き、Cisco UCS Manager の IP アドレスを入力します。ログインクレデンシヤルを入力します。
- ステップ 2 [Navigation] ペインで [LAN] をクリックします。
- ステップ 3 [LAN] タブで [LAN] > [Policies] を展開します。
- ステップ 4 [root] ノード > [Sub-org] > [hx-cluster] の順に展開します
- ステップ 5 [QoS Policy] を右クリックし、[Create QoS Policy] を選択します。
- ステップ 6 [Create QoS Policy] ダイアログボックスで、次の表に示すように必要なフィールドに値を入力します。

QoS ポリシー名	QoS クラス	Burst Size	レート	ホストコントロール
Platinum	Platinum	10240	ライン レート	none
Gold	Gold	10240	ライン レート	none
Silver	Silver	10240	ライン レート	none
Bronze	Bronze	10240	ライン レート	none
ベストエフォート	ベストエフォート	10240	ライン レート	none

- ステップ 7 [OK] をクリックします。

What to do next

QoS ポリシーは、vNIC または vHBA テンプレートにインクルードします。

HX サーバ用の vNIC テンプレートの作成

始める前に

このポリシーは、次のリソースの1つ以上がシステムにすでに存在していることを前提にしています。

- ネームド VLAN
- MAC プール
- QoS ポリシー
- LAN ピン グループ
- 統計情報しきい値ポリシー

このプロシージャでは、合計 8 つの vNIC テンプレートを作成します。FI (A) と、同じセットを FI (B) のそれぞれに、トラフィック管理、ストレージ管理、ネットワーク管理、および VMotion 用のテンプレートを 1 つずつ割り当てます。

手順

- ステップ 1** Cisco UCS Manager では、[LAN tab] > [Policies] > [root] > [Sub-Organization] > [Hyperflex] > [vNIC Templates] に移動します。
- ステップ 2** [vNIC テンプレート (vNIC Templates)] ノードを右クリックし、[vNIC テンプレートを作成 (Create vNIC Template)] を選択します。
- ステップ 3** [Create Network Policy] ダイアログボックスで、次のように必要なフィールドに値を入力します。

vNIC テンプレート名	ファブリック ID	VLAN	ネイティブ VLAN	MAC アドレスプール	MTU	QoS ポリシー	ネットワーク制御ポリシー	説明
hv-mgmt-a	A	h1a	なし	hv-mgmt-a	1500	Silver	ネットワーク制御ポリシー： hyperflex-infra	<p>次で使用されます。</p> <ul style="list-style-type: none"> • ESX 管理 • ストレージコントローラ VM への SSH • クラスタ管理 IP • HXDP プラグイン用の HX コントローラ VM への vCenter 接続。 • hv-mgmt-a と hv-mgmt-b は、vCenter で仮想スイッチ vswitch-hx-inband-mgmt のアップリンクとして使用されます。
hv-mgmt-b	B	h1b	なし	hv-mgmt-b				

vNIC テンプレート名	ファブリック ID	VLAN	ネイティブ VLAN	MAC アドレスプール	MTU	QoS ポリシー	ネットワーク制御ポリシー	説明
storage-data-a	A	storage-data	なし	storage-data-a	9000	Platinum	ネットワーク制御ポリシー： hyperflex-infra	<p>次で使用されます。</p> <ul style="list-style-type: none"> • ESXi NFS クライアント (IOSvisor) • HXDP レプリケーション/クラスタ • クラスタ データ VIP • storage-data-a と storage-data-b は、vCenter で仮想スイッチ vswitch-lx-storage-data のアップリンクとして使用されます。 • NFS トラフィックは、セキュリティと QoS を考慮して、専用の vNIC および VLAN 上にある必要があります。
storage-data-b	B	storage-data	なし	storage-data-b				
vm-network-a	A	(カスタマー vlan 名)	なし	vm-network-a	1500	Gold	ネットワーク制御ポリシー： hyperflex-vm	<p>次で使用されます。</p> <ul style="list-style-type: none"> • VM データ トラフィック (VDI、データベースなど) • vm-network-a と vm-network-b は、vCenter で仮想スイッチ vswitch-lx-vm-network のアップリンクとして使用されます。
vm-network-b	B	(カスタマー VLAN 名)	なし	vm-network-b				

vNIC テンプレート名	ファブリック ID	VLAN	ネイティブ VLAN	MAC アドレスプール	MTU	QoS ポリシー	ネットワーク制御ポリシー	説明
hv-vmotion-a	A	hv-vmotion-a	なし	hv-vmotion-a	9000	Bronze	ネットワーク制御ポリシー： hyperflex-infra	次で使用されます。 <ul style="list-style-type: none"> VM とストレージ vMotion、FT hv-vmotion-a と hv-vmotion-b は、vCenter で仮想スイッチ vmotion のアップリンクとして使用されます。
hv-vmotion-b	B	hv-vmotion-b	なし	hv-vmotion-a				

[General] 領域で、次の参照テーブルに従って、8 つすべての vNIC にすべてのプロパティを設定します。

フェールオーバー	無効
Target	アダプタ
Template Type	更新
PIN グループ	not set
Stats Threshold Policy	デフォルト
ダイナミック vNIC 接続ポリシー	not set
VLANs	各 vNIC テンプレートについて、以下の表に示すように設定されました。

表 8: vNIC テンプレートに設定された VLAN

vNIC 名	VLANs	注
hv-mgmt-a hv-mgmt-b	hx-inband-mgmt	<p>HXDP インストーラは、次のように UCSM LCP vNIC に単一の VLAN を設定します。</p> <ul style="list-style-type: none"> • VLAN 名を「hx-inband-mgmt」に設定します • デフォルトでは VLAN ID を 3091 に設定します。 <p>(注) HXDP インストーラで VLAN ID を変更できません。</p> <ul style="list-style-type: none"> • HXDP のインストール後、UCSM を開き、追加の VLAN を作成して、「hv-mgmt-a」および「hv-mgmt-b」vNIC テンプレートに追加できます。 <p>(注) これらの追加の VLAN を使用して、NetApp NFS/ISCSI ファイラーなどの外部システムにアクセスすることができます。</p> <ul style="list-style-type: none"> • ポートグループ名は、VLAN の [hx-inband-mgmt] でサポートされる [Storage Controller, Management Network] に設定されている値です。
storage-data-a storage-data-b	hx-storage-data	<p>HXDP インストーラは、次のように単一 VLAN を設定します。</p> <ul style="list-style-type: none"> • VLAN 名を「hx-storage-data」に設定します • ネイティブ VLAN として設定します • デフォルトでは VLAN ID を 3092 に設定します <p>(注) HXDP インストーラで VLAN ID を変更できませんが、hx-inband-mgmt と同じにすることはできません。さもないと、ESXi ルーティングが混乱します。</p> <ul style="list-style-type: none"> • ポートグループ名は次のとおりです。 <ul style="list-style-type: none"> • 「Storage Controller Data Network」の後ろに VLAN 「hx-storage-data」が続きます。 • VMK 「Storage Hypervisor Data Network」の後ろに VLAN 「hx-storage-data」が続きます • サブネット 10

vNIC 名	VLANs	注
vm-network-a	ユーザが作成した VLAN	<ul style="list-style-type: none"> UCSM で 1 つ以上の VLAN を手動で作成します ポート グループを手動で作成します。その際、ユーザが作成した VLAN を後ろに続けます UCSM でさらに多くの VLAN を作成し、それらを VM トラフィック用に「vm-network-a」および「vm-network-b」vNIC テンプレートに割り当てることができます。 <p>(注) HXDP インストーラは VLAN またはポート グループを設定しません。</p>
vm-network-b		
hv-vmotion-a	hx-vmotion	<p>HXDP インストーラは、次のように単一 VLAN を設定します。</p> <ul style="list-style-type: none"> VMotion: VLAN hx-vmotion VLAN ID を設定します ネイティブ VLAN として設定します デフォルトの VLAN ID は 3093 です サブネット 10
hv-vmotion-b		

ステップ 4 完了したら、[OK] をクリックします。

vSwitch の設定

VMware ESX および ESXi ホストの両方で、GUI またはコマンドラインから vSwitch を設定できます。

CLI 設定は、複数の ESX サーバをインストールして、vSwitch 設定のスクリプトを構築する際に非常に便利です。

ESX のインストール後、次の手順で ESX ホストの vSwitch を設定します。

手順

ステップ 1 各 ESX サーバのコマンドラインにログインします。

ステップ 2 リストされた名前を使用して、各 ESX サーバで 3 つの vSwitch を作成します。

- **vswitch-hx-storage-data**

スイッチで MTU を 9000 に設定します。

- **vmotion**

スイッチで MTU を 9000 に設定します。

- **vswitch-hx-vm-network**

ステップ 3 次の CLI コマンドを使用して、3 つの新しい vSwitch を作成します。

```
# esxcli network vswitch standard add -v vswitch-hx-storage-data
# esxcli network vswitch standard set -v vswitch-hx-storage-data -mtu= 9000
# esxcli network vswitch standard add -v vswitch-vmotion
# esxcli network vswitch standard set -v vswitch-vmotion -mtu=9000
# esxcli network vswitch standard add -v vswitch-hx-vm-network
```

ステップ 4 ESXi のインストール時に作成されるデフォルトの vSwitch **vSwitch0** は、Hx データ プラットフォーム ノードのセットアップ スクリプトが機能するように、「**vswitch-hx-inband-mgmt**」に名前を変更する必要があります。次のコマンドを使用してスイッチの名前を変更してから、**vmkernel** がコンフィギュレーション ファイルを再度読み取り、新しい名前を使用するように、ホストを再起動します。

```
# sed -i 's/vSwitch0/vswitch-hx-inband-mgmt/g' /etc/vmware/esx.conf
# reboot
```

ステップ 5 次のコマンドを使用して、ホストの再起動後に、vSwitch の作成と名前の変更が確認できます。

```
# esxcli network vswitch standard list
```

前述の 4 つの vSwitch がコマンド出力に表示されていることを確認します。switch-hx-inband-mgmt vSwitch だけがアップリンクおよびポート グループをリストアップします。HX Data Platform インストーラ スクリプトは、残りのネットワーク構成を実行します。

仮想分散スイッチ (VDS) または Cisco Nexus 1000v (N1Kv) への vMotion ネットワークの移行



- (注)
- HX に依存しない以下の特定のネットワークでは、VMware DVS または Cisco Nexus 1000v を使用して HX Data Platform を設定できます。
 - vMotion ネットワーク
 - 仮想マシン ネットワーク
 - 詳細については、[Cisco Nexus 1000v のドキュメント](#)を参照してください。

HX に依存しない vSwitch と関連するポート グループを DVS ネットワークまたは N1Kv ネットワークに移行するには、次の手順を実行します。

手順

ステップ 1 vCenter から、DVS スイッチおよびポート グループを作成します。

- a) **[vCenter Inventory Lists] > [Datacenters] > [datacenter] > [Related Objects] > [Distributed Switches]** の順に選択します。[Add Distributed Switch] アイコンをクリックします。
- b) **[New Distributed Switch]** ウィザードを完了します。2 つのアップリンクを使用して各 DVS スイッチを作成します。

例 : VM ネットワークと vmotion pg

- DVSwitch-VMNetwork : DVPortGroup-VMNetwork
- DVSwitch-Vmotion : DVPortGroup-Vmotion

ステップ 2 vSwitch、VMNetwork を移行します。VMNetwork を、従来の vSwitch から DVS に移行するには、次の手順を実行します。

- a) **[vCenter Inventory Lists] > [Datacenters] > [datacenter] > [Related Objects] > [Distributed Switches]** の順に選択します。
- b) **[DVSwitch-VMNetwork vSwitch]** を選択します。[Add and Manage Hosts] アイコンをクリックします。**[Add and Manage Hosts (ホストの追加と管理)]** ウィザードが起動します。
- c) **[Select task]** ページで、**[Add Hosts]** を選択します。**[Next]** をクリックします。
- d) **[Select hosts]** ページで、**[Add New Hosts]** をクリックします。クラスタ内のすべてのホストを選択します。**[Next]** をクリックします。
- e) **[Select network adapter tasks]** ページで、**[Manage physical adapters]** と **[Migrate virtual machine networking]** を選択します。**[Next]** をクリックします。
- f) **[Manage physical network adapters]** ページで、**vswitch-hx-vm-network : VM ネットワークの一部である物理アダプタが DVSwitch-VMNetwork に割り当てられます。**
- g) **[On other switches/unclaimed list (他のスイッチ/要求解除リスト)]** で、スイッチで使用中の **vswitch-hx-vm-network** に対応する **vmnic** を選択します。
- h) **[Assign (割り当て)]** アップリンクをクリックします。
- i) **[自動割り当て]** を選択します。
- j) **[OK]** をクリックします。ページが更新され、新しく割り当てられた **vmnic** が **[On this switch]** にリストされます。
- k) **[Analyze impact]** ページに、この移行による影響が表示されます。影響がすべてグリーンであることを確認します。**[Next]** をクリックします。
- l) **[Migrate VM networking]** ページで、新しいネットワーク **DVPortGroup-VMNetwork** に移行する VM を選択します。

Next

すべてのホストから、コントローラ VM、stCtlVM を除くすべての VM を選択します。**[DVPortGroup-VMNetwork]** を選択します。**[Next]** をクリックします。

(注) 各ホストの VM のリストには、コントローラ VM を含むすべての VM が含まれています。コントローラ VM は選択しないでください。コントローラ VM を移行すると、ストレージクラスタが中断されます。

m) [Ready to complete] ページで、移行の概要を確認します。[Finish] をクリックします。

(注) 移行後のシステムによって、複数のネットワーク関連のアラームが生成されます。アラームを確認し、クリアします。

ステップ 3 vmotion pg に vSwitch を移行します。vmotion pg を、従来の vSwitch から DVS に移行するには、次の手順を実行します。

- a) [vCenter Inventory Lists] > [Datacenters] > [datacenter] > [Related Objects] > [Distributed Switches] の順に選択します。
- b) [DVSwitch-Vmotion vSwitch] を選択します。[Add and Manage Hosts] アイコンをクリックします。[Add and Manage Hosts (ホストの追加と管理)] ウィザードが起動します。
- c) [Select task] ページで、[Add Hosts] を選択します。[Next] をクリックします。
- d) [Select hosts] ページで、[Add New Hosts] をクリックします。クラスタ内のすべてのホストを選択します。[Next] をクリックします。
- e) [Select network adapter tasks] ページで、タスク [Manage physical adapters] と [Manage VMkernel adapters] を選択します。[Next] をクリックします。
- f) [Manage physical network adapters (物理ネットワーク アダプタの管理)] ページで、vmotion:vmotion pg の物理アダプタ部分が DVSwitch-Vmotion に割り当てられます。

[On other switches/unclaimed (他のスイッチ/要求解除)] リストで、スイッチで使用中の vmotion に対応する vmnic を選択します。[Assign uplink] をクリックし、[Auto-assign] を選択して [OK] をクリックします。ページが更新され、新しく割り当てられた vmnic が [On this switch] にリストされます。[Next] をクリックします。

- g) [Manage VMkernel network adapters (VMkernel ネットワーク アダプタの管理)] ページで、VMkernel アダプタをポート グループ DVPortGroup-Vmotion に移行します。

各ホストに対し、[On other switches (他のスイッチ)] で、スイッチで使用中の vmotion に対応する VMkernel アダプタを選択します。[Assign port group] をクリックします。宛先ポートグループ、DVPortGroup-Vmotion を選択します。[OK] をクリックします。ページが更新され、VMkernel ネットワーク アダプタが再度割り当てられ、送信元ポートグループと宛先ポートグループがリストされます。

- h) 新しいネットワーク、DVPortGroup-Vmotion に移行するホストを選択します。[Next] をクリックします。
- i) [Ready to complete] ページで、移行の概要を確認し、[Finish] をクリックします。

ステップ 4 移行後の手順：IO、ネットワークの接続性、および VM の移行について、VM に影響がないことを確認します。

Stats Daemon のリセット

Description

ネットワーク デーモンは、UDP または TCP 経由で送信されるカウンタやタイマーなどの統計情報をリッスンし、1 つ以上の着脱可能なバックエンド サービスに集計を送信します。

手動で HX Data Platform サーバに ESX を再インストールした後、パフォーマンス統計情報が正しく表示されるように、stats daemon をリセットします。

アクション : stats daemon の再起動

手順

ステップ 1 ESX ホストのコントローラ VM のコマンドラインにログインします。

ステップ 2 restart コマンドを実行します。

```
# /etc/init.d/statsd restart
```

ステップ 3 ストレージクラスタのすべての ESX ホストのコントローラ VM で手順 1 および手順 2 を繰り返します。

HyperFlex HX シリーズ サーバ ディスクの詳細



(注) 発注ツールにおいて、特定の PID で利用可能なディスク（およびサーバ）のみがサポートされます。

すべての HX シリーズサーバは、クラスタ内で同じタイプにする必要があります、ディスクの数も同じでなければなりません。

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。

すべての SSD は TRIM をサポートする必要があります、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。

HX220c	HX240c	Hybrid
Cisco 220c M4 （以下を搭載）： 2 X 2.5GHz E5-2680 v3 24 X 16GB DDR4 RAM 1 X Cisco 12GBps SAS RAID コントローラ 2 X 64 GB SD FlexFlash カード 1 X 120 GB SATA SSD 1 X 480 GB SATA SSD 6 X 1.2 TB、12 GBps SAS 10k RPM HDD VIC 1227 MLOM（2 X 10Gb ポート）	Cisco 240c M4 （以下を搭載）： 2 X 2.5 GHz E5-2680 v3 24 X 16GB DDR4 RAM 1 X 120GB 背面 SSD 1 X Cisco 12GBps SAS RAID コントローラ 1 X 120 GB SATA SSD 1 X 1.6TB 前面 SATA SSD 最大 23 X 1.2 TB SAS 10k RPM HDD（データ用） VIC 1227 MLOM	Cisco B200 M4 (+ HX240c) ： 2 X 2.5GHz E5-2680 v3 24 X 16GB DDR4 RAM 2 X 64GB SD FlexFlash カード VIC 1340

HyperFlex をインストールする際の有効性検査

リリース 1.7.1-14835 のハードウェアの新機能

HyperFlex インストーラは、HX システムを設定する前に、以下の有効性検査を行います。

1. ファームウェア
2. ハードウェア
3. QoS
4. VLAN

有効性検査の結果は、次のいずれかの重大度レベルになります。

- [OK]：検査に合格しました。
- [Warning]：検査に合格しませんでした。理想的には問題を修正すべきですが、インストールを続行することはできます。
- [Error]：検査できませんでした。エラーが修正されるまで、インストールを続行することはできません。

1. ファームウェアの有効性検査

コンフィギュレーション ファイル：firmware_support.json

- **バージョンの互換性**：HyperFlex のバージョンに UCS バージョンとの互換性があることが確認されます。バージョンの互換性に関する最新情報については、Cisco HyperFlex HCL のドキュメントを参照してください。

重大度：Error

設定：[Advanced] -> [firmware_support] -> [ucs_version]

- **ディスク領域**：インストーラ VM に、UCS A、B、C バンドルと ESXi イメージをダウンロードするのに十分なディスク領域があることが確認されます。現在、約 3 GB の空き領域が要件となっています。

重大度：Error

2. ハードウェアの有効性検査

これらの有効性検査では、HX システムに必要なハードウェア設定が確認されます。サーバの特定のモデルでサポートされるハードウェア設定の詳細については、サーバ仕様書で確認できます。

コンフィギュレーション ファイル：hardware_support.json

- **FI 接続**：HX サーバは両方のファブリック インターコネクタに接続できるはずです。

重大度：エラー

- **対称 FI 接続**：HX サーバが両方のファブリック インターコネクタで同じポートに接続されることが確認されます。

重大度：警告

- **FlexFlash コントローラ**：HX サーバに SD カード FlexFlash コントローラがあることが確認されます。

重大度：Error

- **FlexFlash コントローラ エラー**：SD カード FlexFlash コントローラにエラーがないことが確認されます。

重大度：Error

- **SD カード**：HX サーバに 2 つの SD カードがあることが確認されます。

重大度：Error

- **SAS コントローラ**：HX サーバの SAS コントローラがサポート対象であることが確認されます。

重大度：Error

設定：[Advanced] -> [hardware_support] -> [<ServerModel>] -> [sas_ctrl_supp_pid]

- **ディスク**：HX サーバのディスクがサポート対象であることが確認されます。

重大度：Error

ディスクは 3 種類の機能に使用されるため、ディスクごとに以下の 3 つの設定があります。

- SDS ログ SSD

設定 : [Advanced] -> [hardware_support] -> [<ServerModel>] -> [ssd_sds_logs_supp_pid]

- キャッシング SSD

設定 : [Advanced] -> [hardware_support] -> [<ServerModel>] -> [ssd_caching_supp_pid]

- データ HDD

設定 : [Advanced] -> [hardware_support] -> [<ServerModel>] -> [hdd_supp_pid]

- **SDS ログ SSD :**

HX サーバの SAS コントローラがサポート対象であることが確認されます。

また、HX240C_M4SX サーバの SDS ログ SSD が PCH コントローラ (サポート SSD) に接続されていることも確認されます。

重大度 : Error

- **キャッシング SSD :** HX サーバのキャッシングが SAS コントローラに接続されていることが確認されます。

重大度 : Error

- **同一データ ディスク :** HX サーバのすべてのデータ ディスクが同じ PID であることが確認されます。

重大度 : Error

- **データ ディスクのセクター サイズ :** HX サーバのすべてのデータ ディスクのセクター サイズが 512 バイトであることが確認されます。

重大度 : Error

設定 : [Advanced] -> [hardware_support] -> [<ServerModel>] -> [hdd_sector_size]

- **最小データ ディスク :** HX サーバの 3 つ以上のデータ ディスクがあることが確認されます。

重大度 : 警告

設定 : [Advanced] -> [hardware_support] -> [<ServerModel>] -> [hdd_min_req]

3. QoS の有効性検査

QoS の有効性検査では、必要とされる QoS 設定を適用できるかどうかを確認されます。以下の表に、HyperFlex トラフィックのシステム QoS クラスで必要とされる MTU を記載します。

QoS クラス	HyperFlex トラフィック	必要な MTU
Platinum	ストレージ データ	9216

Gold	VM データ	1500
Silver	管理トラフィック	1500
Bronze	VMotion トラフィック	9216
Best Effort	なし	1500

- **MTU の競合** : インストーラは上記の QoS クラスの MTU を設定しようと試みます。ただし、上記の QoS クラスのいずれか 1 つでも関連するサービス プロファイルで使用されている場合、インストーラはすべての HyperFlex トラフィックにベストエフォート QoS クラスを設定しようと試みます。

重大度 : 警告

- **ベストエフォート MTU** : HyperFlex トラフィックにベストエフォート QoS クラスを使用する必要がある場合、ベストエフォート MTU が標準 (1500) またはジャンボ (9000) であることが確認されます。

重大度 : Error

- **QoS パラメータの変更** : 以下のいずれかの QoS パラメータを変更する必要があるかどうかを確認されます。

- admin_state
- weight
- multicast_optimize
- cos
- drop

重大度 : 警告

4. VLAN の有効性検査

- **ストレージ/管理の競合** : [storage-data] と [hv-mgmt] の vNIC に同じ VLAN が設定されていないことが確認されます。

重大度 : 警告

- **ストレージ/vMotion** : [storage-data] と [hv-vmotion] の vNIC に同じ VLAN が設定されていないことが確認されます。

重大度 : 警告

- **管理/vMotion** : [hv-mgmt] と [hv-vmotion] の vNIC に同じ VLAN が設定されていないことが確認されます。

重大度 : 警告

- **ストレージ VLAN** : [storage-data] の vNIC で使用中の VLAN が指定されていないことが確認されます。

重大度 : 警告