



インストールの前提条件

- 必要なハードウェア ケーブル (1 ページ)
- ホスト要件 (2 ページ)
- ディスクの要件 (3 ページ)
- ポート要件 (5 ページ)
- HyperFlex 外部接続 (13 ページ)
- 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 (14 ページ)
- ネットワーク設定 (16 ページ)
- VLAN および vSwitch の要件 (18 ページ)
- Cisco UCS の要件 (19 ページ)
- ハイパーバイザ要件 (19 ページ)
- ストレージクラスタ要件 (20 ページ)
- vCenter 設定の要件 (22 ページ)
- システム サービス要件 (23 ページ)
- コントローラ VM 用 CPU リソース予約 (25 ページ)
- コントローラ仮想マシン用メモリ リソース予約 (25 ページ)
- 自動サポート 要件 (26 ページ)
- シングル サインオンの要件 (27 ページ)

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 6300 シリーズ ファブリック インターコネクト ハードウェア ガイド](#)』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 つのコンバージド 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、コンバージドノードとコンピューティング専用ノード間で異なります。使用可能な CPU およびメモリ容量を拡大するには、必要に応じてコンピューティング専用ノードを使用して既存のクラスタを拡張します。これらのコンピューティング専用ノードを使用すると、ストレージのパフォーマンスを向上させたり、ストレージ容量を拡大したりすることができます。

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

ソリッドステートディスク (SSD) のみが搭載されたサーバは、オールフラッシュサーバです。SSD とハードディスクドライブ (HDD) の両方が搭載されたサーバは、ハイブリッドサーバです。

以下は、HyperFlex クラスタ内のすべてのディスクに適用されます。

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



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

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

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、ESX 搭載の M.2 SATA SSD が内蔵されています。



- (注) サーバ上またはストレージクラス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) 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>

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

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

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

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

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

ポート番号	Service/Protocol	[Source]	ポート宛先	基本情報
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
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)	UCSM A/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 管理に必要なとされるすべてのポートを介して、Cisco UCS Manager から到達可能である必要があります。これにより、Cisco Intersight から ESXi 管理を展開できるようになります。 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タのアップリンクのプロビジョニング

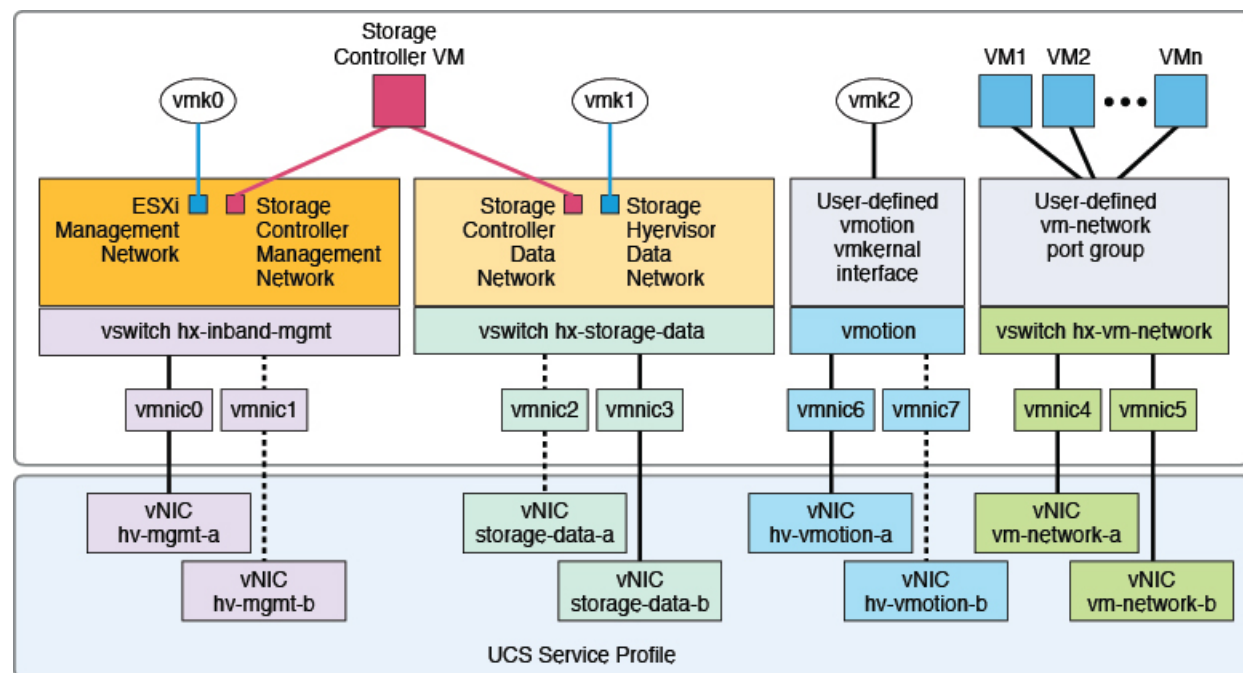
HyperFlex クラスタを設定する前に、ネットワークトラフィック管理を最適化するアップストリーム帯域幅容量を計画してください。これにより、コンポーネントで障害が発生したり、ネットワークが部分的に停止したりした場合でも、トラフィックフローを安定した状態に維持できます。

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。

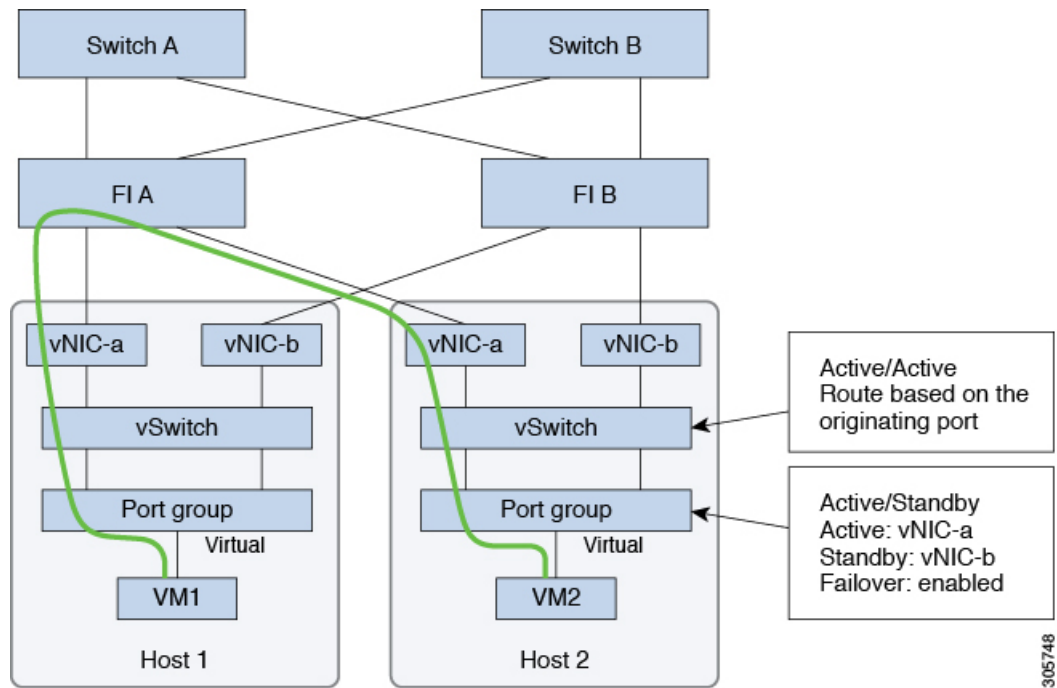
図 1: 単一ホストの *HyperFlex Data Platform* 接続



- 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.

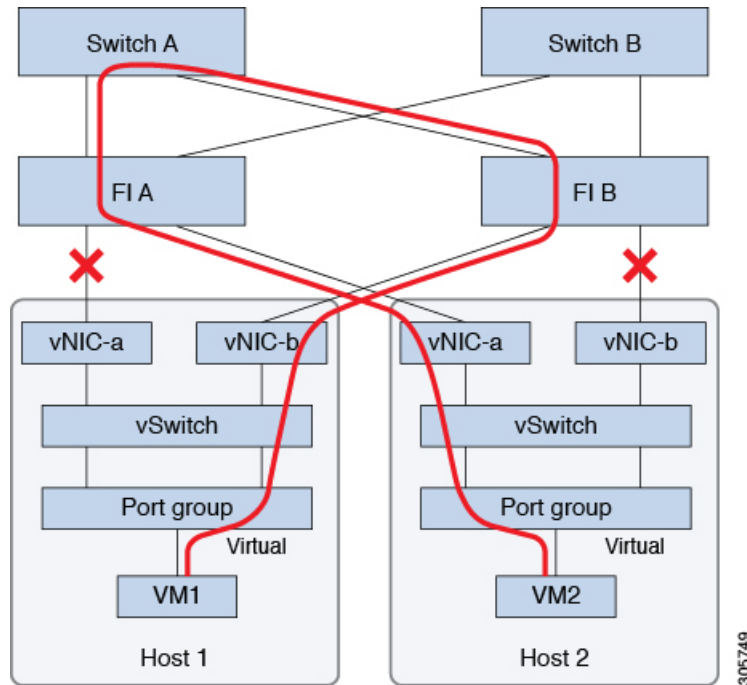
デフォルトの vSwitch NIC チューニング ポリシーとフェールオーバー ポリシーを [yes] に設定します。これにより、管理トラフィック、vMotion トラフィック、およびストレージトラフィックのすべてが、ローカルでファブリック インターコネクトに転送されるようになり、フローを安定した状態に維持できます。vNIC-a で障害が発生すると、ESXi がロード バランシングを計算し、すべての仮想ポートを vNIC-b に再ピンングします。vNIC-a がオンライン状態に戻った時点で、再びピンングが適用され、vNIC-a と vNIC-b の間で仮想ポートが元のように均等に分配されます。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 2: 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 3: 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性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	48 GB	○
HXAF220C-M4/M5s	72 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。

