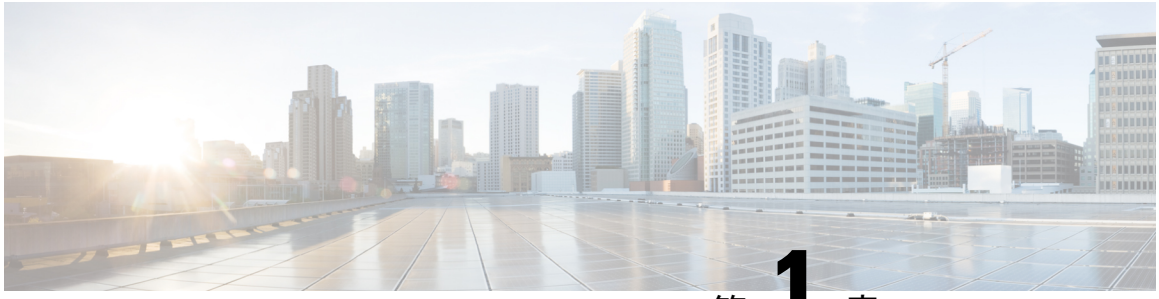
Cisco HyperFlex Systems ネットワークおよび外部ストレージ管理ガイド

初版：2018 年 4 月 13 日

最終更新：2021 年 1 月 6 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/

© 2018 –2021 Cisco Systems, Inc. All rights reserved.



第 1 章

新機能および変更された機能

-
- 新機能および変更された機能に関する情報 （1 ページ）

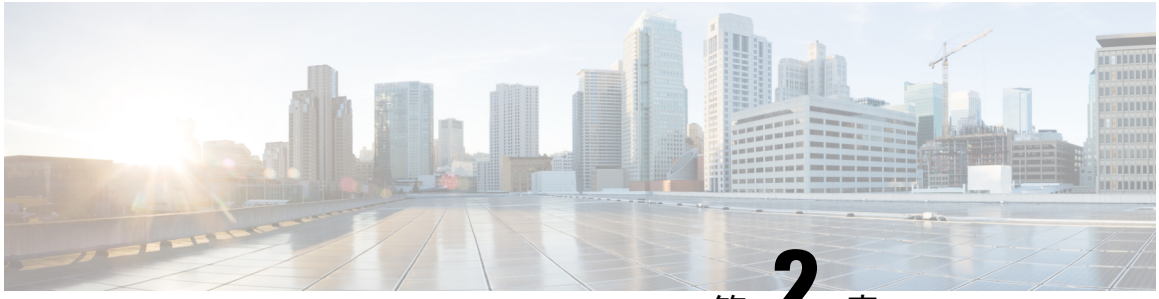
新機能および変更された機能に関する情報

次の表では、このガイドでの重要な変更点の概要を示します。テーブルは、このガイドに加えられたすべての変更のすべてを網羅したリストを提供しているわけではありません。

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

説明	追加日	参照先
[SAN Cloud (SAN クラウド)] タブで VSAN の作成について説明する注記が追加されました。	2019 年 7 月 12 日	ダイレクト アタッチド ストレージ （52 ページ）

新機能および変更された機能に関する情報



第 2 章

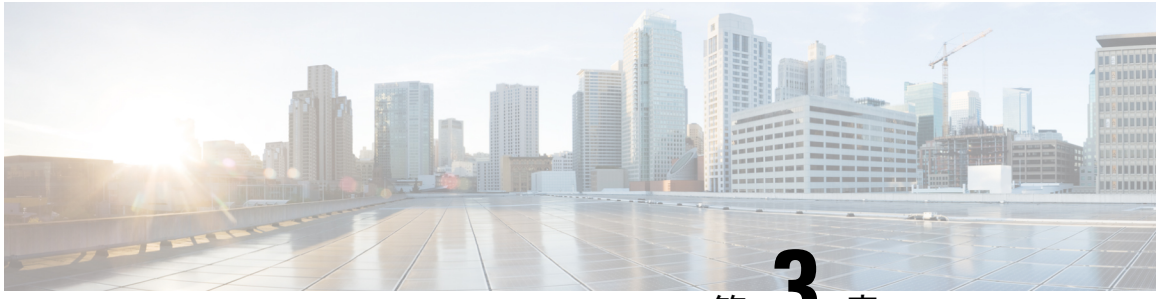
概要

- このマニュアルについて （3 ページ）

このマニュアルについて

このガイドでは、Cisco HyperFlex システムのネットワークと外部ストレージ アーキテクチャの概要について説明します。また、最初の HyperFlex クラスタの設定後に通常実行されるネットワークおよび外部管理手順についても説明します。

このガイドは、サポートされているすべての HX バージョンで使用されます。



第 3 章

ネットワーク管理

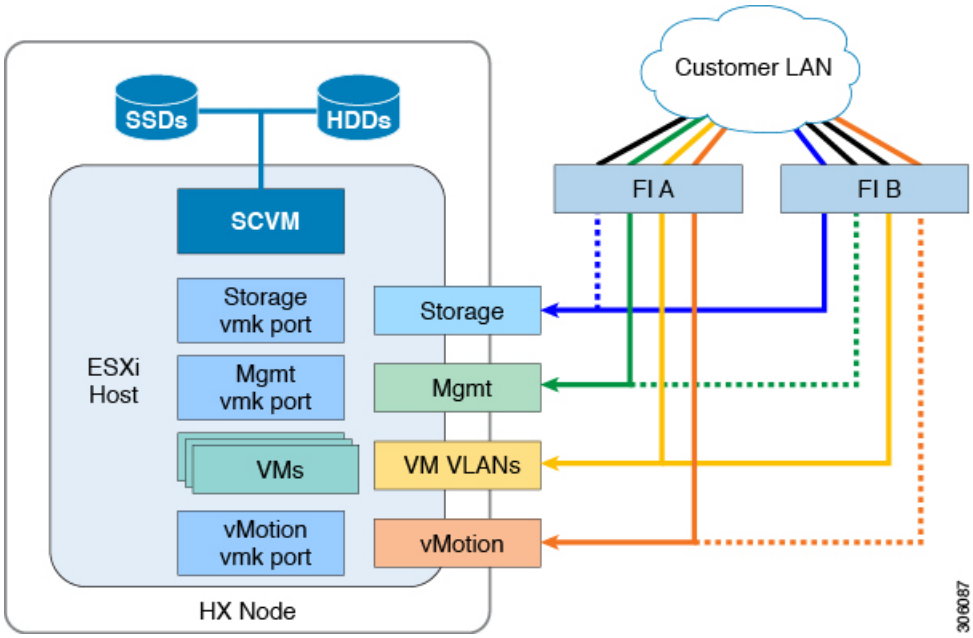
- 物理ネットワーク （5 ページ）
- VLAN とサブネット （7 ページ）
- ジャンボ フレーム （7 ページ）
- 論理ネットワーク （8 ページ）
- 仮想ネットワーク （9 ページ）

物理ネットワーク

Cisco UCS アップリンクの接続

Cisco UCS ネットワーク アップリンクは、UCS ファブリック インターコネクト (FIs) のペアからお客様のデータセンター内の LAN に「ノースバウンド」を接続します。すべての UCS アップリンクが、複数の 802.1Q VLAN ID をアップリングをまたいで伝送するトランクとして機能します。デフォルトでは、UCS ソフトウェアは、UCS 設定で定義されたすべての VLAN ID がすべての利用可能なアップリンクでトランクに適格であると想定しています。

図 *1:* 論理ネットワーク設計



Cisco FIs は、別のネットワーク スイッチではなく、エンドポイントの集合としてネットワーク上に出現します。内部的に、Cisco FIs はスパニング ツリー プロトコル（STP）ドメインに参加しません。また、レイヤ 2 イーサネット リンクで相互接続されないため、ネットワーク ループを形成できません。アップ ストリーム ルートブリッジは、STP を介してすべてのリンクアップ/ダウン決定を行います。

アップリンクは、両方の FIs から接続され、アクティブにされる必要があります。冗長性を確保するために、それぞれの FI 上で複数のアップリンクを 802.3ad Link Aggregation Control Protocol (LACP) ポート チャネルとして、または、個別のリンクを通して、複数のアップリンクを使用することができます。パフォーマンスと冗長性のレベルを最適化するために、仮想ポートチャネル (vPC) 機能を使用して、アップリンクを複数の上流に位置するシスコ スイッチへの LACP ポート チャネルとして構築します。vPC アップリンクを使用すれば、すべてのアップリンクをアクティブ通過データにすることができるうえ、個別のリンク障害や上流に位置するスイッチの故障から保護できます。他のアップリンク設定を冗長にすることはできますが、vPC を利用できない場合はスパニング ツリー プロトコル ループの回避によってリンクが無効になる可能性があります。

すべてのアップリンク接続方法で、トラフィックを FI 間で、つまり、ファブリック A からファブリック B へ転送できる必要があります。ケーブル、ポート、またはリンクの障害が発生して、通常は UCS ドメインから外に出ないトラフィックを強制的に UCS アップリンクに転送しなければならない場合があります。さらに、FI のファームウェア アップデート中など、トラフィック フロー パターンのメンテナンス手順を簡単に確認できますが、再起動が必要です。

VLAN とサブネット

Cisco HyperFlex システム構成では、アップストリーム LAN から複数の VLAN を UCS ドメインに伝送する必要があります。これらの VLAN は、UCS 設定で定義します。

表 *2 : HyperFlex* インストーラで作成された *VLAN*

VLAN 名	VLAN ID	目的
hx-inband-mgmt	ユーザが指定	ESXi ホスト管理インターフェイス HX ストレージ コントローラ VM 管理インターフェイス HX ストレージ クラスタ ローミング管理インターフェイス
hx-storage-data	ユーザが指定	ESXi ホスト ストレージ vmkernel インターフェイス HX ストレージ コントローラ ストレージ ネットワーク インターフェイス HX ストレージ クラスタ ローミング ストレージ インターフェイス
hx-vm-data	ユーザが指定	ゲスト VM ネットワーク インターフェイス
hx-vmotion	ユーザが指定	VMware ESXi ホスト vMotion vmkernel インターフェイス

（注） データセンターでは、物理デバイスの管理に専用ネットワークまたはサブネットを使用することがよくあります。このシナリオでは、2 つの FI の mgmt0 インターフェイスを専用ネットワークまたはサブネットに接続する必要があります。HyperFlex のインストールでは、これを有効な構成と見なしますが、以下の注意点があります。次のサブネットへの IP 接続が可能な場所に HyperFlex インストーラを展開する必要があります。

- FI の mgmt0 インターフェイスのサブネット
- 前述の hx-inband-mgmt VLAN で使用されるサブネット

ジャンボ フレーム

ジャンボフレームを使用するように hx-storage-data VLAN およびサブネットを通過するすべての Cisco HyperFlex ストレージトラフィックを設定します。すべての通信が 9000 バイトの

Maximum Transmission Unit (MTU/最大伝送ユニット) サイズを持つ IP パケットを送信するように設定することを意味します。より大きな MTU 値を使用すると、送信される各 IP パケットのペイロードが大きくなるため、パケットごとにより多くのデータが送信され、結果的にデータの送受信が高速になります。この要件は、ジャンボフレームを渡すように Cisco UCS アップリンクを設定する必要があることも意味します。Cisco UCS アップリンク スイッチでジャンボ フレームを許可するように設定できなかった場合は、一部の障害シナリオで、特に、ケーブルやポートの障害によってストレージ トラフィックがノースバウンド Cisco UCS アップリンク スイッチを通過したときに、サービスの中断につながる可能性があります。

論理ネットワーク

Cisco HyperFlex システムは、以下の定義済みゾーンに分類される通信パスを備えています。

表 *3:* 定義された通信パスのゾーン

ゾーン	説明
管理ゾーン	物理ハードウェア、ハイパーバイザ ホスト、およびストレージ プラットフォーム コントローラ仮想マシン（SCVM）を制御するために必要な接続で構成されます。これらのインターフェイスと IP アドレスは、LAN/WAN 全体で HX システムを管理するすべてのスタッフが利用できるようにする必要があります。このゾーンは、ドメイン ネーム システム（DNS）と Network Time Protocol（NTP）へのアクセスを提供し、セキュア シェル（SSH）通信を可能にする必要があります。
VM ゾーン	HyperFlex ハイパーコンバージド システム内で動作するゲスト VM にネットワーク IO を提供するために必要な接続で構成されます。通常、このゾーンには、ネットワーク アップリンクを介して Cisco UCS ファブリック インターコネクト (FI) にトランキングされ、802.1Q VLAN ID でタグ付けされた複数の VLAN が含まれています。これらのインターフェイスと IP アドレスは、LAN/WAN 全体で HX システム内のゲスト VM と通信する必要があるすべてのスタッフおよびその他のコンピュータ エンドポイントが利用できるようにする必要があります。

ゾーン	説明
ストレージ ゾーン	Cisco HX Data Platform ソフトウェア、ESXi ホスト、およびストレージ コントローラ VM が HX 分散データ ファイルシステムに提供するために使用する接続で構成されます。適切に運用するためには、これらのインターフェイスと IP アドレスが相互に通信できる必要があります。通常の運用では、このトラフィックのすべてが Cisco UCS ドメイン内で発生しますが、このトラフィックが UCS ドメインのネットワーク ノースバウンドを通過する必要があるハードウェア障害シナリオがあります。そのため、HX ストレージ トラフィックに使用される VLAN は、FI B から FI A に、または、その逆方向に到達する UCS ドメインからのネットワーク アップリンクを通過できる必要があります。このゾーンは、主に、ジャンボ フレーム トラフィックを含むため、UCS アップリンク上でジャンボ フレームを有効にする必要があります。
vMotion ゾーン	ESXi ホストがゲスト VM の vMotion をホスト間で有効にするために使用する接続で構成されます。通常の運用では、このトラフィックのすべてが Cisco UCS ドメイン内で発生しますが、このトラフィックが Cisco UCS ドメインのネットワーク ノースバウンドを通過する必要があるハードウェア障害シナリオがあります。そのため、HX ストレージ トラフィックに使用される VLAN は、FI B から FI A に、または、その逆方向に到達する Cisco UCS ドメインからのネットワーク アップリンクを通過できる必要があります。

仮想ネットワーク

Cisco HyperFlex システムは、 ハイパーバイザ レベルで事前定義された仮想ネットワーク設計を備えています。HyperFlex インストーラは、4 つの異なる仮想スイッチ（vSwitches）を作成します。各スイッチでは、Cisco UCS サービス プロファイルで定義された vNIC によってそれぞれ処理された 2 つのアップリンクを使用します 。

図 *2 : ESXi* ネットワーク設計

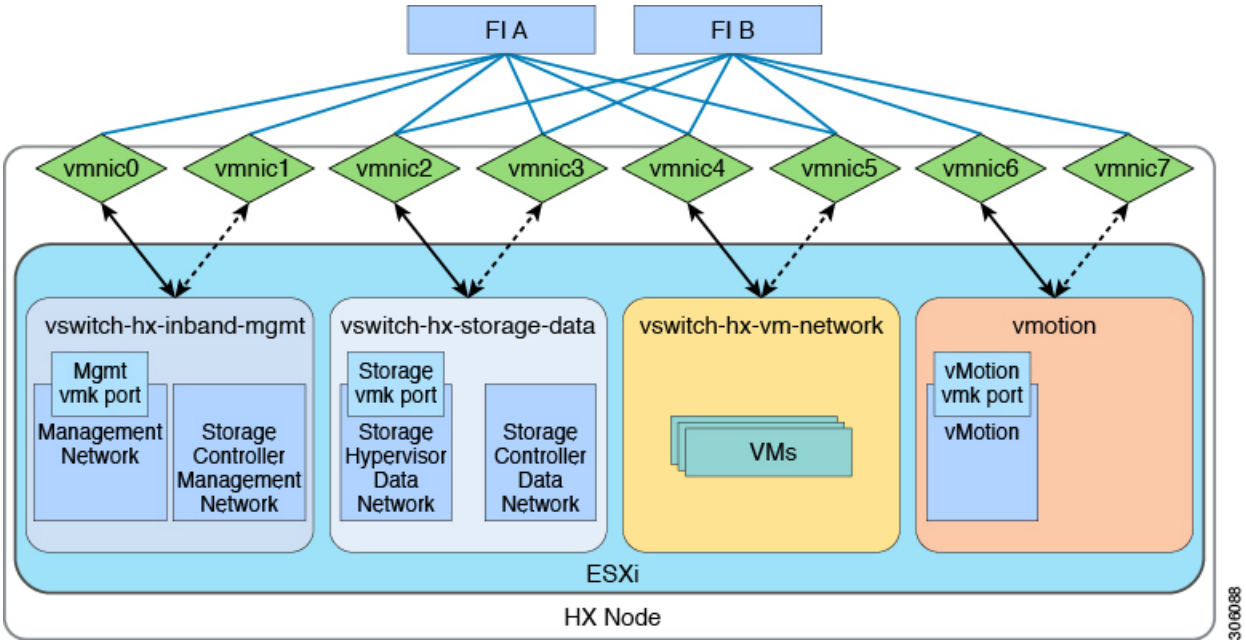
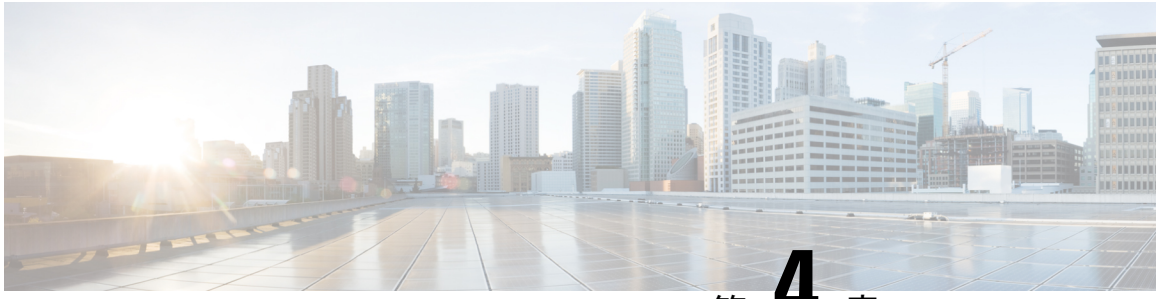


表 *4 :* インストーラ-作成された *vSwitches*

vSwitch	説明
vswitch-hx-inband-mgmt	デフォルトの vSwitch0。自動インストールの一部として、ESXi キックスタート ファイルで名前を変更します。インストーラは、標準の管理ネットワーク ポート グループで、デフォルトの vmkernel ポート vmk0 を設定します。スイッチは、ジャンボ フレームを含まない 2 つのアップリンク（ファブリック A 上のアクティブとファブリック B 上のスタンバイ）を使用します。インストーラは、ストレージ プラットフォーム コントローラ VM の 2 番目のポート グループを作成し、個々の管理インターフェイスに接続します。VLAN は、vNIC テンプレートに割り当てられるネイティブ VLAN ではないため、ESXi/vSphere で割り当てられます。
vswitch-hx-storage-data	自動インストールの一部として作成されています。インストーラは、ストレージ ハイパーバイザ データ ネットワーク ポート グループで、vmkernel ポート vmk1 を設定します。システムは、NFS を介した HX データストアへの接続のため、インターフェイスを使用します。スイッチは、ジャンボフレームを必要とする2つのアップリンク（ファブリック B 上のアクティブとファブリック A 上のスタンバイ）を使用します。インストーラは、ストレージ プラットフォーム コントローラ VM の 2 番目のポートを作成し、個々のストレージ インターフェイスに接続します。VLANは、vNICテンプレートに割り当てられるネイティブVLANではないため、ESXi/vSphere で割り当てられます。

vSwitch	説明
vswitch-hx-vm-network	自動インストールの一部として作成されています。スイッチは、ジャンボ フレームを含まない 2 つのアップリンク（ファブリック A および B の両方でアクティブ）を使用します。VLAN は、vNIC テンプレートに割り当てられるネイティブ VLAN ではないため、ESXi/vSphere で割り当てられます。
VMotion	自動インストールの一部として作成されています。スイッチは、ジャンボ フレームを必要とする 2 つのアップリンク（ファブリック A 上のアクティブとファブリック B 上のスタンバイ）を使用します。VLAN は、vNIC テンプレートに割り当てられるネイティブ VLAN ではないため、ESXi/vSphere で割り当てられます。



第 4 章

クラスタ セットアップ後のネットワーク構成

- QoS ポリシーの作成, on page 13
- MAC アドレス プールの作成 （15 ページ）
- HX サーバ用の VLAN の作成 （16 ページ）
- プライベート VLAN の概要 （18 ページ）
- vSwitch の設定 （19 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 （20 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 （20 ページ）
- ESX ホストでのプライベート VLAN の設定 （21 ページ）
- vSphere 標準スイッチでの VMNIC の削除 （21 ページ）
- vSphere 分散スイッチの作成 （21 ページ）
- vSphere 分散スイッチでのプライベート VLAN の作成 （22 ページ）
- 分散ポート グループでのプライベート VLAN の設定 （22 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 （23 ページ）
- Stats Daemon のリセット （25 ページ）
- 既存のクラスタへの vNIC の追加 （26 ページ）

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。

次の表に示されるシステム クラスを設定できます。

Table 5: 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 を設定します。 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。
ファイバ チャネル	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 を設定します。 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。 **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。

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。

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 [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 [**QoS ポリシーの作成**] ダイアログ ボックスで、次の表に示すように、システム クラスのフィールドに入力します。

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。

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 のいずれかに設定します。「*A*」は、ファブリック インターコネクト (FI) 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。

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 [**MAC プールの作成**] ウィザードの [**名前と説明の定義**] ページで、以下の表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 アドレスが変更されると、ソフトウェアは ESXi を以前の設定方法に再設定します。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、設定されません。
- 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 プールを上にあるように設定します。
- 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。

HX サーバ用の VLAN の作成

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	
hx-inband-mgmt	次で使用されます。 • 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。 • 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。 • 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。 • 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。

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 （20 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 （20 ページ）。

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。

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。

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

ステップ 1 Cisco UCS Managerでプライベート VLAN を設定するには、『Cisco UCS Manager ネットワーク管理ガイド』を参照してください。

ステップ 2 上流に位置するスイッチでプライベート VLAN を設定するには、『Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』を参照してください。

ステップ 3 ESX ホストでプライベート VLAN を設定するには、ESX ホストでのプライベート VLAN の設定 （21 ページ） を参照してください。

既存の VM で VM ネットワークのプライベート VLAN を設定する

ステップ 1 Cisco UCS Managerでプライベート VLAN を設定するには、『Cisco UCS Manager ネットワーク管理ガイド』を参照してください。

ステップ 2 上流に位置するスイッチでプライベート VLAN を設定するには、『Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング設定ガイド』を参照してください。

ステップ 3 ESX ホストでプライベート VLAN を設定するには、以下を参照してください。ESX ホストでのプライベート VLAN の設定 （21 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。

ESX ホストでのプライベート VLAN の設定

ESX ホストでプライベート VLAN を設定するには、次の手順を実行します。

ステップ 1 VMware vSphere クライアントから vSphere 標準スイッチの VMNIC を削除します。

ステップ 2 前の手順で削除した VMNIC を使用して新しい vSphere 分散スイッチを作成します。

ステップ 3 無差別、独立、およびコミュニティ VLAN を作成します。

vSphere 標準スイッチでの VMNIC の削除

ステップ 1 VMware vSphere クライアントにログインします。

ステップ 2 [Home] > [Hosts and Clusters] を選択します。

ステップ 3 VMNIC を削除する ESX ホストを選択します。

ステップ 4 [Configuration] タブを開きます。

ステップ 5 [Networking] をクリックします。

ステップ 6 VMNIC を削除する**スイッチ**を選択します。

ステップ 7 [Manage the physical adapters connected to the selected switch] ボタンをクリックします。

ステップ 8 削除する **`vminc`** 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

ステップ 1 VMware vSphere クライアントにログオンします。

ステップ 2 [Home] > [Networking] を選択します。

ステップ 3 クラスタを右クリックして、[Distributed Switch] > [New Distributed Switch] を選択します。

ステップ 4 [Name and Location] ダイアログボックスに、分散スイッチの名前を入力します。

ステップ 5 [Select Version] ダイアログボックスで、バージョンと構成の要件に対応する分散スイッチ バージョンを選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Edit Settings] ダイアログボックスで、次のように指定します。

- [Number of uplink ports]
- [Network I/O Control] を**有効化**します。
- [Create a default port group] をオンにします。
- [Port Group Name] ボックスに、デフォルト ポート グループの**名前**を入力します。

ステップ 8 [Next] をクリックします。

ステップ 9 [Ready to Complete] ダイアログボックスで、設定した内容を確認します。

ステップ 10 [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

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。

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。

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。

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**

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。

既存のクラスタへの vNIC の追加

始める前に

iSCSI または NFS、または FC SAN を介して FlexPod などの他のストレージ システムに接続するには、HX クラスタの作成時に追加の vNIC を追加することをお勧めします。HyperFlex インストーラは、インストール時にオプションで追加の iSCSI vNIC または FC HBA を作成するように要求します。外部ストレージが必要な場合、または将来のある時点で設定する必要があります。

HyperFlex は、クラスタ作成後の vNIC の追加をサポートしています。既存のクラスタ にvNIC を追加するには、次の操作を実行します。

（注） ストレージクラスタがオフラインになる可能性があるため、これらのハードウェアの変更中に複数のノードを一度に再起動しないでください。後続のノードに移動する前に、各ホストと HX クラスタのヘルス状態を検証します。

（注） まれに、ESXi の vmnic が並べ替えられ、ネットワーク サービスを復元するために手動で再設定する必要があります。この手順を開始する前に、SSH を介してクラスタ内の**それぞれの** ESXi ホストで次のコマンドの出力を実行し、保存します。

```
esxcli network nic list
esxcli network vswitch standard list
esxcli network vswitch standard policy failover get -v vswitch-hx-inband-mgmt
esxcli network vswitch standard policy failover get -v vswitch-hx-storage-data
esxcli network vswitch standard policy failover get -v vmotion
esxcli network vswitch standard policy failover get -v vswitch-hx-vm-network
```

ステップ 1 UCSM にログインし、**[LAN]** タブをクリックして、**[ポリシー（Policies）]** > **ルート** > **[サブ組織（Sub-Organizations）]** > ***[このクラスタの Suborg の名前（Name of the Suborg for this Cluster）]*** > **[vNIC テンプレート（vNIC Templates）]**に移動します。**[vNIC テンプレート (vNIC Templates)]** ノードを右クリックし、選択します。

ステップ 2 **[LAN]** タブから、**[ポリシー（Policies）]** > **[root]** > **[サブ組織（Sub-Organizations）** > ***[このクラスタのサブ組織の名前（Name of the Suborg for this Cluster）]*** > **[LAN 接続ポリシー（LAN Connectivity Policies）]** > **[HyperFlex]**に移動します。ページ下部の **[追加（Add）]** をクリックします。名前を指定し、**[vNIC テンプレートの使用（Use vNIC Template）]** のチェックボックスをオンにして、**ステップ 1** で作成したテンプレートを選択します。最後に **[変更の保存（Save Changes）]** をクリックし、トリガーされる可能性のある警告を確認します。

vNIC テンプレートを LAN 接続ポリシーに追加すると、サーバは **[再起動の保留（Pending Reboot）]** 状態になり、新しいインターフェイスを追加するために再起動が必要になります。

（注） この時点では HX サーバを再起動しないでください。

ステップ 3 管理者特権を持つユーザとしてサーバにログインします。

ステップ 4 既存の HX ESXi ホストのいずれかを**メンテナンス モード**にします。

ステップ 5 ホストが**システム保守モード**に移行後に、関連付けられているノードを再起動して新しいハードウェアの追加を完了します。

ステップ 6 一部の設定では、ノードの再起動後に、HXDP ソフトウェアが DirectPath I/O 設定が変更されたことを検出し、再設定する必要があります。これにより、ノードの自動リブートが 1 回追加されます。

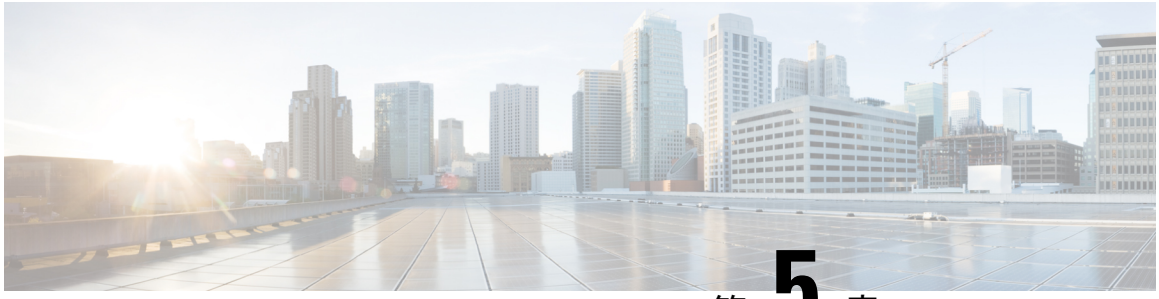
（注） 2 回目の再起動後、ESXi ホストをメンテナンス モードから終了すると、SCVM はエラーなしで自動的に起動します。

ステップ 7 クラスタのヘルス ステータスをチェックし、次のノードに進む前にクラスタが正常であることを確認します。クラスタのヘルス ステータスは、HyperFlex Connect で確認できます。

ステップ 8 すべてのノードがリブートされ、新しい vNIC が新しい vmnic インターフェイスとして ESXi に表示されるまで、必要に応じてクラスタの各ノードに対してステップ 3ー7 を繰り返します。

ステップ 9 新しい vSwitch を作成し、新しい vmnic をアップリンクとして割り当てます。既存の HyperFlex vSwitch または vmnic を変更しないでください。

（注） クラスタに追加された追加の vNIC には必ず新しい vSwitch を作成してください。



第 5 章

外部ストレージ管理

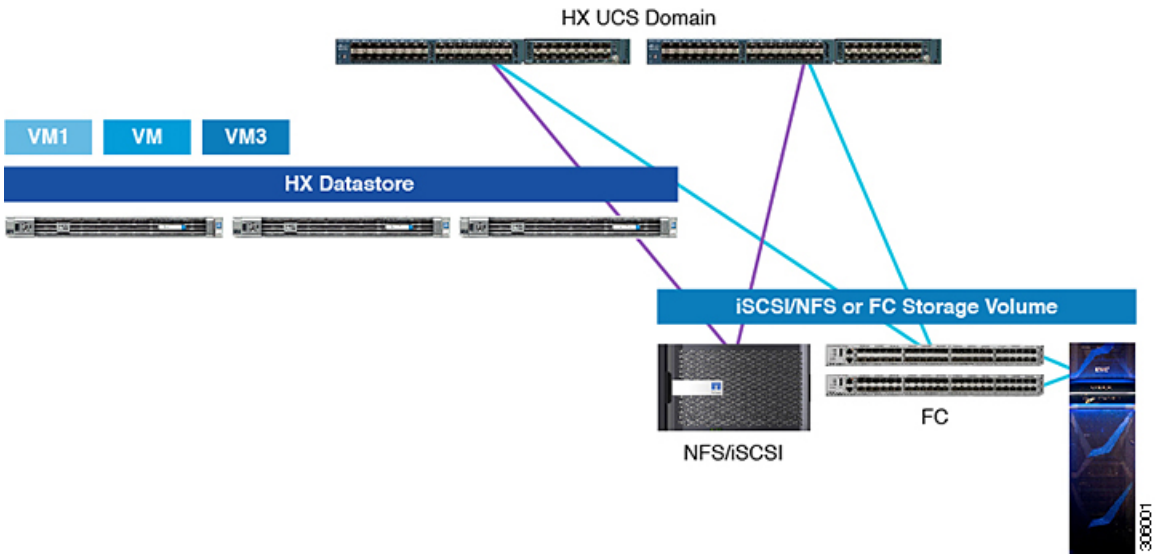
- 外部ストレージ管理の概要 （29 ページ）
- 外部ファイバ チャネル ストレージ （30 ページ）
- ストレージ設定の順序 （31 ページ）
- 外部 NFS ストレージへの Cisco HX サーバの接続 （47 ページ）
- ファイバ チャネルのゾーン分割 （49 ページ）
- ファイバ チャネルのゾーン分割 Cisco UCS Manager （50 ページ）
- ファイバ チャネル ゾーン分割の設定 （50 ページ）
- ダイレクト アタッチド ストレージ （52 ページ）
- ファイバ チャネル スイッチング モード （52 ページ）
- ファイバ チャネル スイッチング モードの設定 （53 ページ）

外部ストレージ管理の概要

Cisco HyperFlex System は、ユニファイド ファブリックを介して SAN ストレージとネットワーク アタッチド ストレージ（NAS）の両方への統合されたアクセスを提供します。ストレージ アクセスを統一することにより、Cisco Unified Computing System は、イーサネット、ファイバ チャネル、Fibre Channel over Ethernet（FCoE）、および iSCSI を介してストレージにアクセスできます。

次の図は、 Cisco HyperFlex System が外部ストレージと統合されていることを示しています。

図 *3*: 外部ストレージと *Cisco HyperFlex* システムの統合



外部ファイバ チャネル ストレージ

外部ファイバ チャネル ストレージへの HyperFlex ノードの接続

このドキュメントでは、Tier 1 外部ファイバ チャネル（FC）ストレージ アレイを HyperFlex ノードに接続する方法を詳しく説明します。外部FCストレージは、次のように、FCエンドホスト モードとイーサネット エンドホスト モードで HX ノードに接続できます。

- ファブリック接続 FC ストレージ
- ファブリック接続 FCoE ストレージ

ストレージ設計の考慮事項

HX SAN 接続の次の設計特性を考慮してください。

- ノースバウンドストレージの物理接続では、LAN接続などの仮想ポートチャネル（vPC）がサポートされません。
- ポート チャネルまたはトランキングはサポートされており、複数のストレージ アップリンク ポートを結合して物理リンクの冗長性を確保することができます。
- ストレージはストレージリソースの冗長性を管理します。これはベンダーによって異なります。
- 外部ストレージを HX ドメインに直接接続すると、追加の処理によりファブリック インターコネクトの物理ポートの使用量が増加します。

- ストレージリソースへのアクセスを提供するには、VSANやゾーン分割などのソフトウェア設定が必要です。
- 外部ストレージ接続を利用する場合は、2 つのクラスタ間で LAN 接続ポリシーが異なる可能性があるため、ストレージに接続する各クラスタを独自のドメイン内に置くことが不可欠です。
- HyperFlex を NetApp IP ストレージを備えた既存の UCS ドメインに統合する場合、デフォルトの QoS ゴールド クラスを 9216 バイトに変更します。これにより COS 4 でジャンボフレームが使用可能になります。詳細については「NetApp KB Article number 000003500」を参照してください。

ストレージ設定の順序

外部ストレージに HX を接続するには、次の手順に従います。

ステップ 1 管理レベルのクレデンシャルを使用して、HX データ プラットフォーム インストーラにログインします。

ステップ 2 最初のワークフローの選択で、[**操作内容を理解したうえでワークフローをカスタマイズする**] オプションをクリックします。

ステップ 3 [**UCSM 設定の実行**] および [**ESX 設定の実行**] のみを選択します。

ステップ 4 ウィザードに従って、設定を完了します。

このウィザードで作成する HX ポリシー、サービス プロファイル テンプレート、およびサービス プロファイルを、HX クラスタに関連付けることになります。

詳細な手順については、「HyperFlex 開始ガイド」の HX データ プラットフォームの設定の章を参照してください。

（注） クラスタがオンラインになったときは、vHBA はありません。

ステップ 5 以下のストレージ タイプのうち 1 つか両方を HX FI ドメインに接続します。

- ファイバ チャネル ストレージについては、「HX にファイバ チャネル ストレージを取り付ける 」を参照してください。
- ISCSI については、「HX へ iSCSI ストレージを取り付ける」を参照してください。

ステップ 6 HX インストーラに再度ログインし、[**開始**] をクリックします。

ステップ 7 最初のワークフローの選択で、[**操作内容を理解したうえでワークフローをカスタマイズする**] オプションをクリックします。

ステップ 8 [**HX ソフトウェアの展開**] を選択し、HX クラスタを作成するウィザードに従います。

HX にファイバ チャネル ストレージを取り付ける

この手順では、HX FI ドメインへファイバ チャネル（FC）ストレージを取り付ける高度な手順について説明します。

ステップ 1 Cisco UCS Manager GUI にログインします。

ステップ 2 ファイバ チャネル通信用の VSAN を作成します。詳細については、ファイバ チャネルの VSAN の作成 （32 ページ）を参照してください。

ステップ 3 HyperFlex の WWNN プールと WWNN ブロックを作成します。詳細については、WWNN プールの作成を参照してください。

ステップ 4 ファブリック固有の（hx-a および hx-b）WWNN プールと WWPN ブロックを作成します。詳細については、WWPN プールの作成 （34 ページ）を参照してください。

ステップ 5 ファブリック A とファブリック B にそれぞれ関連付けられている以前作成された WWPN プールを使用して、vHBA テンプレートのペアを作成します。

ステップ 6 HyperFlex SAN 接続ポリシーを作成します。詳細については、SAN 接続ポリシーの作成 （36 ページ）を参照してください。

ステップ 7 クラスタに使用する HX サービス プロファイル テンプレート（SPT）に HX SAN 接続ポリシーを割り当てます。このステップでは、変更された SPT から作成されたクラスタ内のすべてのノードで pending-ack が発生します。vHBA を使用してサービス プロファイルの再設定をトリガーするために、クラスタ内のすべてのサービス プロファイルのすべての pending-ack を確認します。

ファイバ チャネルの VSAN の作成

SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID は違っている必要があります。同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。ID が FCoE VLAN ID と重複しているすべての VLAN 上でイーサネット トラフィックがドロップされます。

ステップ 1 [Navigation] ペインで [SAN] をクリックします。

ステップ 2 [SAN Cloud] > [VSAN] ノードを選択します。

ステップ 3 [**VSAN**] ノードを右-クリックし、[**ストレージ VSAN の作成**] を選択します。

ステップ 4 [Create VSAN] 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
[Name] フィールド	ネットワークに割り当てられている名前。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

名前	説明
[**FC ゾーニング***] フィールド	FC エンドポイント -ホスト モードのファブリック インターコネクトの [**無効**] オプション ボタンが選択されていることを確認します。 （注） ファブリック インターコネクトがアップストリーム スイッチに接続されていないことを確認します。
設定	環境に応じて設定を選択します。 • VSAN がすべての使用可能なファブリック内で同じ VSAN ID にマッピングされるようにする場合は、[Common/Global] オプション ボタンをクリックします。 • ファブリック A とファブリック B で異なる ID を持つ 2 つの VSAN を作成する場合は、[Both Fabrics Configured Differently] オプション ボタンをクリックします。
[VSAN ID] フィールド	ネットワークに割り当てられている固有識別情報。FC エンドホスト モードの場合、3840 ～ 4079 も予約済みの VSAN ID 範囲です。
[FCoE VLAN] フィールド	ファイバ チャネル接続に使用される VLAN に割り当てられた固有識別情報。 VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Managerでは、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。

WWNN プールの作成

ワールド ワイド ノード名（WWNN）プールは、ワールド ワイド ノード名だけを含む World Wide Name（WWN）プールです。サービス プロファイルに WWNN のプールを含める場合、ソフトウェアは関連するサーバにそのプールから WWNN を割り当てます。

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。その他の WWN 範囲はすべて予約されています。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

ステップ 1 [Navigation] ペインで [SAN] をクリックします。

ステップ 2 **[SAN]** > **[Pools]** > **[root]** > **[Sub-Organizations]** > **[hx-cluster]** の順に展開します。

ステップ 3 プールを作成する [hx-cluster] サブ組織を展開します。

ステップ 4 [WWNN Pools] を右クリックし、[Create WWNN Pool] を選択します。

ステップ 5 [Create WWNN Pool] ウィザードの [Define Name and Description] ダイアログボックスで、[HyperFlex] と入力します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Create WWNN Pool] ウィザードの [Add WWN Blocks] ページで、[Add] をクリックします。

ステップ 8 [Create WWN Block] 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。

[**フォーム**] フィールド：ブロック内の最初の WWN。

[**サイズ**] フィールド：ブロックに含める WWN の数。

WWN プールの場合、プール サイズは ports-per-node + 1 の倍数にする必要があります。たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 9 [**OK**] をクリックします。

ステップ 10 [完了（Finish）] をクリックします。

次のタスク

WWPN プールを作成します。

WWPN プールの作成

WWWPN プールを作成するには、次の手順を実行します。

ステップ 1 [Navigation] ペインで [SAN] をクリックします。

ステップ 2 **[SAN]** > **[Pools]** > **[root]** > **[Sub-Organizations]** > **[hx-cluster]** の順に展開します。

ステップ 3 [WWPN Pools] を右クリックし、[Create WWPN Pool] を選択します。

ステップ 4 [Create WWPN Pool] ウィザードの [Define Name and Description] ダイアログボックスで、[hx-a] と入力します。

ステップ 5 [Next] をクリックします。

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

ステップ 7 [Create WWN Block] 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。

[**フォーム**] フィールド：ブロック内の最初の WWN。

[**サイズ**] フィールド：ブロックに含める WWN の数。

WWN プールの場合、プール サイズは ports-per-node + 1 の倍数にする必要があります。たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

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。

次のタスク

WWPN プール [hx-b] を作成します。上記の手順に従ってください。

vHBA テンプレートの作成

このテンプレートは、サーバ上の vHBA による SAN への接続方法を定義するポリシーです。これは、vHBA SAN 接続テンプレートとも呼ばれます。このポリシーを有効にするには、このポリシーをサービス プロファイルに含めます。

始める前に

vHBA テンプレート ポリシーを作成する前に、次のリソースの 1 つまたは複数がシステムに存在することを確認します。

- ネームド VSAN
- WWNN プール、または WWPN プール
- SAN ピン グループ
- 統計情報しきい値ポリシー

ステップ 1 [Navigation] ペインで [SAN] をクリックします。

ステップ 2 [SAN] > [ポリシー] > [ルート] > [サブ組織] > [hx クラスタ] の順に展開します。

ステップ 3 [vHBA Templates] ノードを右クリックし、[Create vHBA Template] を選択します。

ステップ 4 [Create vHBA Template] 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
[Name] フィールド	[vhba-a] と入力します。 仮想ホスト バス アダプタ（vHBA）テンプレートの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。スペース、またはハイフン（-）、アンダースコア（_）、ピリオド（.）およびコロン（:）以外の特殊文字は使用できません。この名前は、オブジェクトの保存後には変更できません。
[Description] フィールド	256 文字以下で入力します。 テンプレートのユーザ定義による説明。
[Fabric ID] フィールド	[A] を選択します。

名前	説明
[Select VSAN] ドロップダウン リスト	ファブリック A に選択した VSAN を選択して、この vHBA に関連付けます。
[Template Type] フィールド	[Updating Template] を選択します。 このテンプレートが変更されると、このテンプレートから作成された vHBA が更新されます。
[Max Data Field Size] フィールド	デフォルト：2048 vHBA がサポートするファイバチャネルフレームのペイロード バイトの最大サイズ。
[WWPN Pool] ドロップダウン リスト	[hx-a] を割り当てます。
[QoS Policy] ドロップダウン リスト	<設定しない>
[Pin Group] ドロップダウン リスト	<設定しない>
[Stats Threshold Policy] ドロップダウン リスト	<設定しない>

ステップ 5 [OK] をクリックします。

SAN 接続ポリシー

接続ポリシーは、ネットワーク内のサーバと SAN の間の接続およびネットワーク通信リソースを決定します。これらのポリシーは、プールを使用してサーバに MAC アドレス、WWN、および WWPN を割り当て、サーバがネットワークとの通信に使用する vNIC および vHBA を識別します。

（注） これらの接続ポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートに含まれるため、静的 ID を接続ポリシーで使用することはお勧めしません。接続ポリシーは、複数のサーバを設定するためにも使用できます。

SAN 接続ポリシーの作成

ステップ 1 [Navigation] ペインで [SAN] をクリックします。

ステップ 2 [SAN] > [ポリシー] > [ルート] > [サブ組織] > [hx クラスタ] の順に展開します。

ステップ 3 [SAN Connectivity Policies] を右クリックし、[Create SAN Connectivity Policy] を選択します。

ステップ 4 [Create SAN Connectivity Policy] ダイアログボックスで、[Name] として **`Hyperflex`** と入力し、オプションで [Description] に説明を入力します。

ステップ 5 [WWNN の割り当て（WWNN Assignment）] ドロップダウンから、[Hyperflex] プールを選択します。

各プール名の後には、プール内で利用可能な WWN の数および WWN の合計数を示す、括弧に囲まれた 2 つの数字が表示されます。

ステップ 6 [Add] をクリックします。

ステップ 7 [Create vHBAs] ダイアログボックスで、名前として **vhba-a** と入力します。

ステップ 8 [vHBA テンプレートの使用（Use vHBA template）] をクリックします。

ステップ 9 **[vHBA template (vHBA テンプレート)]** ドロップダウン リストから **[vhba-a]** を選択します。

ステップ 10 **[Adapter Policy (アダプタ ポリシー)]** ドロップダウン リストから **[VMware]** を選択します。

ステップ 11 [OK] をクリックします。

ステップ 12 ステップ 7 から 12 を繰り返して、vHBA **vhba-b** を作成し、**vhba-b** テンプレートを割り当てます。

次のタスク

HX ノード サービス プロファイル テンプレートに SAN 接続ポリシーを統合します。

HX ノード サービス プロファイル テンプレートへの SAN 接続ポリシーの統合

このプロシージャにより、この SPT に関連付けられているサービス プロファイルがユーザの確認をとってから HX ノードをリブートします。

ステップ 1 [Navigation] ペインで [Server] をクリックします。

ステップ 2 [Servers] > [Service Profile Template] > [root] > [Sub-Organizations] > [hx-cluster] の順に展開します。

ステップ 3 [Service Template hx-nodes] を選択し、[vHBA] を選択します。

ステップ 4 作業ペインの [Storage] タブで、[SAN Connectivity Policy] セクションにあるドロップダウン リストから [HyperFlex] を選択します。

ステップ 5 **[保存 (Save)]** をクリックします。

---

vNIC または vHBA を導入済み HyperFlex クラスタへ追加

HyperFlex クラスタをインストールした後で FlexPod などの追加のストレージを追加するには、次の手順に従ってください。これらのハードウェアを変更した後は、一度に複数のノードを再起動しないでください。後続のノードで再起動または手順を実行する前に、各ノードのヘルス状態を確認します。

仮想ネットワーク インターフェイス コントローラ（vNIC）または仮想ホスト バス アダプタ（vHBA）を導入済み HyperFlex クラスタに追加するには、次の手順を完了します。

ステップ 1 HyperFlex のサービス プロファイル テンプレートに vHBA を追加します。詳細については、vHBA テンプレートの作成 （35 ページ）を参照してください。

重要 vHBA をサービス プロファイル テンプレートに追加した後、HX サーバに再起動が必要と表示されます。この時点では HX サーバを再起動しないでください。

ステップ 2 vSphere Web Clientを使用して HX ESXi サーバの 1 つをメンテナンス モードにします。

a) vSphere Web クライアント ナビゲータから、**[Hosts and Clusters]** > **[Datacenter]** > **[HX Cluster]** > ***[node]*** の順に選択します。

b) ノードを右クリックし、**[Cisco HX Maintenance Mode]** > **[Enter HX Maintenance Mode]** の順に選択します。

ステップ 3 システム保守モードに移行後に、Cisco UCS Manager の関連付けられているノードを再起動して新しいハードウェアの追加を完了します。

ステップ 4 ESXi サーバのパススルーを設定します:

a) vSphere Web Client ナビゲータから、**[vCenter Inventory]** > **[Resources]** > **[Hosts]** > **[ESX host]** > **[Manage]** > **[Settings]** > **[Hardware]** > **[PCI Devices]** > **[Edit]** の順に選択します。

b) ハードウェアに移動し、[advanced settings] を選択します。

c) [Configure Passthrough] を選択します。

d) パススルーにする [LSI card] を選択して [OK] をクリックします。

ステップ 5 ESXi ホストをリブートします。

ステップ 6 ESXi ホストが再起動したら、[詳細設定] 画面でパススルーデバイスが利用可能になっていることを確認します。

ステップ 7 HX メンテナンス モードを終了します。

a) vSphere Web クライアント ナビゲータから、**[Hosts and Clusters]** > **[Datacenter]** > **[HX Cluster]** > ***[node]*** の順に選択します。

b) ノードを右クリックし、**[Cisco HX Maintenance Mode]** > **[Exit HX Maintenance Mode]** の順に選択します。

ステップ 8 HX コントローラを再設定する:

a) システムを右クリックして、[Edit Settings] を選択します。[OK] をクリックします。

b) [Hardware] タブで、PCI デバイスが利用不可と表示されます。デバイスを強調表示して [Remove] をクリックします。

c) [Add] をクリックします。[PCI device] を選択して、[Next] をクリックします。

d) PCI デバイスがドロップダウン リストで強調表示されている必要があります。[Next] をクリックします。

e) [Finish] を選択します。[OK] をクリックします。

ステップ 9 HX コントローラを右クリックして電源オンにします。

ステップ 10 HyperFlex クラスタのヘルス ステータスをチェックし、次のノードに進む前にクラスタが正常であることを確認します。

```
# stcli cluster info|grep -i health
```

```
Sample output:
healthstate : healthy
state: healthy
storage cluster is healthy
```

ステップ 11 必要に応じて、クラスタ内の各ノードにプロセスを繰り返します。

HX へ iSCSI ストレージを取り付ける

この手順では、HX FI ドメインへ iSCSIストレージを取り付ける高度な手順について説明します。

ステップ 1 Cisco UCS Manager GUIにログインします。

ステップ 2 VLAN を作成します。

ステップ 3 iSCSI ストレージの MAC プール アドレスを作成します。詳細については、外部ストレージの MAC アドレス プールの作成 （42 ページ）を参照してください。

ステップ 4 ファブリック A とファブリック B にそれぞれ関連付けられている vNIC テンプレートのペアを作成します。詳しくは、iSCSI ストレージの vNIC テンプレートの作成 （43 ページ）を参照してください。

ステップ 5 HyperFlex LAN 接続ポリシーを作成します。詳しくは、LAN 接続ポリシーの作成 （44 ページ）を参照してください。

ステップ 6 クラスタに使用する HX サービス プロファイル テンプレート（SPT）に HX LAN 接続ポリシーを割り当てます。これにより、変更された SPT から作成されたクラスタ内のすべてのノードで pending-ack が発生します。vNIC を使用してサービス プロファイルの再設定をトリガーするために、クラスタ内のすべてのサービス プロファイルのすべての pending-ack を確認します。詳細な手順については、LAN 接続ポリシーの作成 （44 ページ）を参照してください。

ステップ 7 ネットワークおよびストレージ アダプタを追加します。詳しくは、ネットワーク アダプタの追加 （45 ページ）を参照してください。

iSCSI SAN の概念

iSCSI SAN はコンピュータ システム間またはホスト サーバ間でイーサネット接続を使用する、ハイパフォーマンスのストレージ サブシステムです。SAN のコンポーネントには、ストレージ トラフィックを転送するホスト サーバ、スイッチ、ルータ内の iSCSI ホスト バス アダプタ（HBA）またはネットワーク インターフェイス カード（NIC）、ケーブル、ストレージ プロセッサ、およびストレージ ディスク システムがあります。

iSCSI SAN は、クライアント/サーバ アーキテクチャを使用します。iSCSI イニシエータと呼ばれるクライアントは、ホスト上で稼働します。iSCSI プロトコルを使用してカプセル化した状態で、iSCSI コマンドを発行し送信することで、クライアントは iSCSI セッションを開始します。iSCSI ターゲットと呼ばれるサーバは、ネットワーク上の物理ストレージ システムを表します。また、たとえば仮想マシンで稼働する iSCSI ターゲット エミュレータなどの iSCSI ターゲットを仮想 iSCSI SAN で提供することもできます。iSCSI ターゲットは必要な iSCSI データを送信して、イニシエータからのコマンドに応答します。

検出、認証、およびアクセス制御

ストレージを検出し、そのストレージへのアクセスを制限するには、いくつかのメカニズムを使用できます。ストレージ アクセス制御ポリシーをサポートするように、ホストとインターネット SCSI（iSCSI）を設定する必要があります。

仮想マシンが iSCSI SAN 上のデータにアクセスする方法

ESXi は、SAN ストレージデバイス上にある VMFS データストア内の仮想マシンから、ディスク ファイルを保管します。仮想マシンのゲスト オペレーティング システムが自身の仮想ディスクに対して iSCSI コマンドを発行すると、SCSI 仮想化層により、コマンドが VMFS ファイル操作に変換されます。iSCSI イニシエータがネットワーク接続に使用するポートに応じて、イーサネット スイッチとルータは、ホストがアクセス対象とするストレージ デバイスにリクエストを伝送します。

iSCSI SAN での ESXi の使用

SAN と併せて ESXi を使用することで、ストレージが統合されて信頼性が向上するとともに、ディザスタ リカバリにも役立ちます。iSCSI SAN ストレージ システムを使用するように ESXi ホストをセットアップする場合は、いくつかの特殊な考慮事項があることに注意してください。

iSCSI ストレージに関するベスト プラクティス

iSCSI SAN と併せて ESXi を使用する際は、VMware が提示している問題回避のためのベストプラクティスに従ってください。

ストレージ システムがストレージ API（アレイ統合ハードウェア アクセラレーション機能）をサポートしている場合は、ストレージ予約を確認します。また、ストレージ システム側でハードウェア アクセラレーション サポートを有効にする方法について、ベンダーのドキュメントで確認する必要があります。

iSCSI SAN の問題の回避

SAN と併せて ESXi を使用する際は、SAN 設定で問題が発生しないよう、以下の特定のガイドラインに従ってください。

- 各 LUN に配置する VMFS データストアは 1 つだけにしてください。LUN 上に複数の VMFS データストアを配置することは推奨されません。
- システムが設定するパスポリシーは、それを変更することによってどのような影響があるかを理解していない限り、変更しないでください。
- 設定、アクセス制御、ストレージ、スイッチ、サーバ、iSCSI HBA 設定、ソフトウェアおよびファームウェアのバージョン、ストレージの配線計画を含め、すべての情報を文書化してください。
- 障害時に備えた計画を立てます。トポロジマップの複数のコピーを作成します。各要素について、その要素で障害が発生した場合に SAN に与える影響を検討してください。

- 極めて重要な障害点を見逃さないよう、設計に記載されている各種のリンク、スイッチ、HBA、およびその他の要素のそれぞれをチェックするごとに線を引いて消します。
- スロットとバス速度に基づき、iSCSI HBA が ESXi ホストの正しいスロットに設置されていることを確認します。サーバで使用可能なバスの間で PCI バスの負荷を分散します。
- ESXi パフォーマンス グラフ、イーサネット スイッチ統計情報、およびストレージパフォーマンス統計情報を含め、あらゆる可視の情報で、ストレージネットワーク内のさまざまなモニタ ポイントを十分に理解します。
- ホストが使用する VMFS データストアが配置されている LUN の ID を変更する際は注意してください。ID が変更されると、VMFS データストアで実行中の仮想マシンで障害が発生します。VMFS データストアで実行中の仮想マシンがないとしても、LUN の ID を変更した後は、ホスト上で再スキャンを行って ID をリセットする必要があります。再スキャンを使用する方法の詳細については、「`Storage Refresh and Rescan Operations`」を参照してください。
- iSCSI アダプタのデフォルト名を変更する必要がある場合は、使用する名前が世界レベルで一意であり、適切な形式になっていることを確認します。ストレージアクセスに問題が発生しないよう、それぞれ異なるホスト上にあるアダプタであっても、決して複数のアダプタに同じ iSCSI 名前を割り当てないでください。
- iSCSI トラフィックとアップリンクがそれぞれに専用の vSwitch で隔離されるようにしてください。

HX FI ドメインに iSCSI ストレージを追加するための VLAN の作成

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 以下の表に示すように、右クリックして [**VLAN の作成**] 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-extstorage-iscsi	外部ストレージの接続を追加するために使用されます	HyperFlex	4201

（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。
- 共有タイプは、[None] に設定されます。

ステップ 4 [OK] をクリックします。

次のタスク

外部ストレージの MAC プールを作成します。

外部ストレージの MAC アドレス プールの作成

すでに存在する 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します。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 (FI) 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。

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 [**MAC プールの作成**] ウィザードの [**名前と説明の定義**] ページで、以下の表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**
hx-extstorage-a	HyperFlex システムに外部ストレージを追加するための MAC プール	Sequential	00:25:B5:XX:1:01-63

（注） MACアドレスの最後のブロックを確認し、次の順序のブロックを使用して、両方のファブリックに新しい MAC プールを作成してください。

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。

次のタスク

手順を繰り返して、ファブリック インターコネクト b に MAC プール **hx-extstorage-b** を作成します。

iSCSI ストレージの vNIC テンプレートの作成

このテンプレートは、サーバ上の vNIC と LAN の接続方法を定義するポリシーです。これは、vNIC LAN 接続テンプレートとも呼ばれます。このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

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
- Jumbo MTU
- QoS ポリシー

ステップ 1 Cisco UCS Manager で、[LAN] タブ > [Policies] > [root] > [Sub-Organization] > [Hyperflex] > [vNIC Templates] に移動します。

ステップ 2 [vNIC Templates] ノードを右クリックし、[Create vNIC Template] を選択します。

ステップ 3 [Create vNIC Template] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Name] フィールド	**extstorage_iscsi-a** を入力します この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	テンプレートのユーザ定義による説明。 256 文字以下で入力します。
[Fabric ID] フィールド	[A] を選択します

名前	説明
[Redundancy] ドロップダウン リスト	Primary
Target	アダプタ
[Template Type] フィールド	[Updating Template] を選択します。 このテンプレートが変更されると、このテンプレートから作成された vNIC が更新されます。
[VLAN] フィールド	hx-extstorage-iscsi（上記で作成したもの）
[CDN Source]	vNIC 名
[MTU] ドロップダウン リスト	**9000**
[MAC Pool]	**hx-extstorage-a**（以前に作成済み）
[QoS Policy] ドロップダウン リスト	**Bronze**
Connection	**Dynamic**

ステップ 4 [OK] をクリックします。

次のタスク

FI B の vNIC テンプレートを作成します。

LAN 接続ポリシー

接続ポリシーは、ネットワーク内のサーバと LAN の間の接続およびネットワーク通信リソースを決定します。このポリシーは、プールを使用して MAC アドレスをサーバに割り当て、サーバがネットワークとの通信に使用する vNIC を識別します。

（注） これらのポリシーはサービス プロファイルとサービス プロファイル テンプレートに含まれているため、接続ポリシーで静的 ID を使用しないことをお勧めします。接続ポリシーは、複数のサーバを設定するためにも使用できます。

LAN 接続ポリシーの作成

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Sub-Org] > [hx-cluster] > [LAN Connectivity Policies] > [HyperFlex] を展開します。

ステップ 3 [**vNIC の追加（Add vNICs）**] をクリックします。

ステップ 4 [**vNIC を作成 (Create vNIC)**] ダイアログボックスで、名前を入力します。**vNIC テンプレート**と**冗長ペアの使用をチェックしてください。**

例*: iscsi-A*

ステップ 5 **ピア名**を入力します。

例*: iscsi-B*

ステップ 6 **[vNIC Template (vNIC テンプレート)]**の名前として、ドロップダウン リストから *[iscsi-A]* を選択します。[OK] をクリックします。

ステップ 7 ステップ 3 から 6 を繰り返して、vNIC *iscsi-B* を作成し、*vNIC-b* テンプレートを割り当てます。

ステップ 8 [Save Changes] をクリックします。表示される [変更の保存 (Save Changes)] ボックスで、[**はい (Yes)**]をクリックして変更を受け入れます。
HX ノード サービス プロファイル テンプレートに LAN 接続ポリシーを統合します。

HX ノード サービス プロファイル テンプレートへの LAN 接続ポリシーの統合

ステップ 1 **[Server (サーバ)]** タブに移動し、**[root] > [Sub-Org] > [hx-cluster] > [Service Template hx-nodes]** の順に展開します。

ステップ 2 作業ペインの **[Network (ネットワーク)]** タブで、**[LAN Connectivity Policy (LAN 接続ポリシー)]** セクションにあるドロップダウン リストから **`[HyperFlex]`** を選択します。

ステップ 3 [Modify vNIC/HBA Placement] をクリックします。iscsi vNIC が適切な順序かどうかを確認します。それらがその順序で最後になっていることを確認します。必要に応じて配置し直します。

（注） FC と iSCSI の両方のストレージを追加する場合は、vHBA の順序が vNIC の順序に先行します。

ステップ 4 **[Save（保存）]** をクリックします。

このプロシージャにより、この SPT に関連付けられているサービス プロファイルがユーザの確認をとってから HX ノードをリブートします。

ネットワーク アダプタの追加

ステップ 1 VMware vCenter に進みます。

ステップ 2 [HX ノード（HX node）] を選択します。

ステップ 3 [Configuration] > [Hardware] に移動します。

ステップ 4 [ネットワーク アダプタ（Network Adapters）] をクリックします。

ステップ 5 作成した iSCSI vmnic が [Network Adapters] に表示されていることを確認します。[Networking] をクリックします。

ステップ 6 [Create vSphere Standard Switch] を選択し、新しい vSwitch を作成して、前に追加した 2 つの vNIC を選択します。

ステップ 7 [Next] をクリックします。

ステップ 8 ポート グループを作成し、接続タイプを [VMkernel] に設定します。[Port Group Properties] セクションで、[Network Label]、[VLAN ID]、および [Network Type] に値を入力します。

ステップ 9 [**次へ**] をクリックし、[**IP Address**] に iSCSI イニシエータの IP アドレスを入力します。

ステップ 10 [Finish] をクリックします。vswitch が作成され、1 つの vmkernel ポート グループが割り当てられます。

注目 マルチパスを設定する場合は、作成した vswitch の [Properties] をクリックし、[Add] をクリックして別の vmkernel ポリシーを追加します。上記のステップ 8 および 9 を実行します。[Finish] をクリックします。

2 つの vmkernel ポートを使用してマルチパスを設定した場合は、NIC チーミング ポリシーを設定します。

最初の vmkernel ポートをクリックして [**編集] をクリックし、[NIC チーミング** チェックボックスをオンにしてスイッチ フェールオーバー順序をオーバーライドします。一方の vnic アダプタをアクティブにしてもう一方を未使用の状態にします。2 番目の vmkernel ポートについて、以上の逆の設定を行います。

ストレージ アダプタの追加

ステップ 1 VMware vCenter に進みます。

ステップ 2 [HX ノード（HX node）] を選択します。

ステップ 3 [Configuration] > [Hardware] に移動します。

ステップ 4 [ストレージ アダプタ（Storage Adapters）] をクリックします。

ステップ 5 [USB Storage Controller] を選択します。

ステップ 6 [Add] をクリックします。

ステップ 7 [Add iSCSI Software Adapter] をクリックします。

ステップ 8 [OK] をクリックします。

ステップ 9 新しい [Software iSCSI adapter] が [Storage Adapter] リストに追加されます。追加された [Software iSCSI Adapter] をリストから選択します。

ステップ 10 [Properties] > [Network Configuration] タブの順にクリックします。

ステップ 11 [Add] をクリックします。

ステップ 12 *vNIC 10* と *vNIC 11* が表示されているはずです。この両方を選択して、[OK] をクリックします。

ステップ 13 [Dynamic Discovery] タブに移動します。

ブランクで表示されます。

ステップ 14 [Add the iSCSI target IP against the iSCSI adapter] をクリックします。デフォルト ポートとして使用します。

ステップ 15 [OK] をクリックします。

ターゲットが取り込まれます。2 番目の IP マルチパスに対して、上記の手順を繰り返します。

（注） ソフトウェアは、再スキャンを要求してきます。[Yes] をクリックします。iSCSI LUN が割り当て済みの場合は、ソフトウェアの **[Configuration (設定)]** でデバイスの下にその iSCSI LUN が表示されます (シック クライアント)。

ステップ 16 [Storage] に移動します。

ステップ 17 [Configuration] タブで、[Add Storage] をクリックします。

ステップ 18 [Storage Type] として [Disk] または [LUN] を選択します。[Next] をクリックします。

ステップ 19 LUN が表示されます。それを選択してから、[Next] をクリックします。

ステップ 20 [Datastore Name] にデータストア名を入力し、[Finish] をクリックします。

外部 NFS ストレージへの Cisco HX サーバの接続

Network File System

ESXi に統合された NFS クライアントは、ネットワーク ファイル システム（NFS）プロトコルを使用して、NAS サーバ上にある指定の NFS ボリュームに TCP/IP でアクセスします。ESXi ホストにはボリュームをマウントすることができ、そのボリュームでストレージニーズに対応します。

ESXi は、ほとんどの NFS ボリュームで以下のストレージ機能をサポートします。

- VMotion および Storage vMotion
- ハイ アベイラビリティ（HA）
- 分散リソース スケジューラ（DRS）

NFS に関する注意事項と要件

NFS ストレージを使用する際は、設定、ネットワーク、NFS データストアに関する以下の注意事項に従ってください。

NFS サーバ設定時の注意事項

- 使用する NFS サーバが VMware HCL に記載されていることを確認します。サーバ ファームウェアに適切なバージョンを使用する必要があります。
- NFS ストレージを設定する際は、ストレージ ベンダーの推奨事項に従います。
- NFS ボリュームは NFS を使用して TCP でエクスポートされるようにする必要があります。

- ホストのそれぞれにボリュームへのルートアクセス権限が割り当てられるようにします。NAS サーバがルート アクセス権限を付与しないとしても、ホスト上に NFS データストアをマウントすることはできます。ただし、そのデータストアで仮想マシンを作成することはできません。
- NFS サーバが 1 つの共有に対して両方のプロトコル バージョンを指定していないことを確認します。
- ファイルを保管する基礎の NFS ボリュームが読み取り専用となっている場合は、NFS サーバがそのボリュームを読み取り専用としてエクスポートすることを確認してください。そうでない場合は、ESXi ホスト上でそのボリュームを読み取り専用データストアとして設定する必要があります。このようしないと、ホストがそのデータストアを読み取り/書き込みに対応すると見なし、ファイルを開けなくなります。

NFS ネットワークに関する注意事項

- ネットワーク接続を可能にするには、ホストに標準ネットワーク アダプタが必要です。
- ESXi はレイヤ 2 およびレイヤ 3 のネットワーク スイッチをサポートします。レイヤ 3 スイッチを使用する場合は、ESXi ホストと NFS ストレージ アレイをそれぞれ別のサブネットに配置して、ネットワーク スイッチでルーティング情報を処理する必要があります。
- NFS トラフィックとアップリンクがそれぞれに専用の vSwitch で隔離されるようにしてください。
- NFS ストレージには VMkernel ポート グループが必要です。新しい仮想スイッチ（vSwitch）上に、IP ストレージの VMkernel ポート グループを追加してください。vSwitch スイッチとしては、vSphere 標準スイッチ（VSS）または vSphere 分散スイッチ（VDS）を使用できます。
- 複数のポートで NFS トラフィックに対応する場合は、それに応じて適切に仮想スイッチと物理スイッチが設定されていることを確認します。詳細については、vSphere ネットワークに関するドキュメントを参照してください。

（注） NFS ストレージの設定の詳細については、ストレージ ベンダーのドキュメントを参照してください。

NFS ストレージの vSwitch、アダプタ、およびポート グループの作成

ステップ 1 vCenter Web クライアントで、[**インベントリ**] > [**ホストとクラスタ**] > [**DC**] > [**ホスト**] に移動し、以下の手順を実行します。

a) [Configuration] タブで、[Networking] > [Add Networking] の順にクリックします。

b) ウィザード ボックスで、[**VMkernel**] を選択し、[**次へ**] をクリックします。

ステップ 2 [Create vSphere Standard switch] を選択し、使用可能な vmnic を選択します。[Next] をクリックします。

ステップ 3 ポート グループの名前を入力します。例：NFS

環境にネイティブ VLAN がある場合、VLAN ID をデフォルトのままにします。。

ステップ 4 **IP 設定** 情報を入力し、[**次へ**] をクリックし、[**終了**] をクリックします。

NFS ストレージ環境の設定

ステップ 1 NFS サーバで、NFS ボリュームを設定し、そのボリュームをマウント先の ESXi ホストにエクスポートします。NFS サーバの IP アドレスまたは DNS 名および絶対パス、あるいは NFS 共有フォルダ名に注意してください。

（注） このデータストアをマウントする各ホストが、Active Directory ドメインの一部になっていること、およびホストごとに NFS 認証クレデンシャルが設定されていることを確認します。

ステップ 2 vCenter シック クライアントで、[Storage] に移動します。[Configuration] タブで、[Add Storage] をクリックします。ウィザード ボックスで、[Network File System (NFS)] を選択します。[Next] をクリックします。

ステップ 3 [Local NFS] ウィザードが表示されます。ターゲット サーバの IP アドレスと、そのアドレスに対応するパスを入力します。データストアに名前を付けます。[Next] と [Finish] をクリックします。

（注） 注：サービスプロファイルテンプレート、サービスプロファイル、およびポリシーに関して Cisco UCS Manager で行う必要がある変更はありません。詳細については、**vSphere ネットワークに関するドキュメント**を参照してください。

ファイバ チャネルのゾーン分割

ファイバ チャネル（FC）ゾーン分割によって、FC ファブリックを 1 つ以上のゾーンに区切ることができます。各ゾーンでは、VSAN で相互通信できる FC イニシエータと FC ターゲットのセットが定義されます。ゾーン分割により、ホストとストレージ デバイスまたはユーザ グループ間のアクセス制御を設定することができます。

ゾーンに関する情報

ゾーンは複数のゾーン メンバから構成されており、次のような特性を備えています。

- ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
- ゾーンのサイズを変更できます。
- デバイスは複数のゾーンに所属できます。

1 つの物理ファブリックに最大 8,000 ゾーンを収容できます。

ファイバ チャネルのゾーン分割 Cisco UCS Manager

Cisco UCS Manager は、スイッチベースの ファイバ チャネル (FC) ゾーン分割と Cisco UCS Manager ベースの FC ゾーン分割をサポートしています。同じ Cisco UCS ドメイン 内ではゾーン分割タイプを組み合わせて設定できません。次のゾーン分割タイプのいずれかを使って Cisco UCS ドメイン を設定できます。

- Cisco UCS Managerベース FC 分割：ローカルのゾーン分割と直接接続ストレージを組み合わせます。FC または FCoE ストレージは、ファブリック インターコネクト (FI) に直接接続します。Cisco UCS ローカル ゾーン分割を使用して Cisco UCS Manager のゾーン分割を実行します。既存の FC または FCoE アップリンク接続を無効にします。Cisco UCS は、Cisco UCS ローカル ゾーン分割機能の使用と共存するアクティブな FC チャネルまたは FCoE アップリンク接続を現在サポートしていません。
- スイッチ ベースの FC ゾーン分割 — ダイレクト アタッチド ストレージとアップリンク ゾーン分割を組み合わせます。FC または FCoE ストレージは、FI に直接接続します。MDS または Nexus 5000 スイッチを使用して、Cisco UCS ドメイン ドメインの外部でゾーン分割を実行します。この設定では、Cisco UCS ドメイン でのローカル ゾーン分割はサポートされません。スイッチベースのゾーン分割の場合、Cisco UCS ドメイン はアップストリーム スイッチからゾーン分割設定を継承します。

（注） ゾーン分割は VSAN 単位で設定されます。ファブリック レベルでゾーン分割を有効にすることはできません。

推奨事項

- Cisco UCS Manager で FC ゾーン分割を処理する場合、FI をファイバ チャネル スイッチ モードにする必要があります。エンドホスト モードでは FC ゾーン分割を設定できません。
- Cisco UCS ドメイン ドメインが 2 つの FI で高可用性に設定されている場合は、両方の FI を同じ VSAN セットで設定することを推奨します。

ファイバ チャネル ゾーン分割の設定

手順の概要

1. まだ完了してない場合は、Cisco UCS ドメイン内のファブリック インターコネクトの接続を、外部ファイバ チャネル スイッチ（MDS など）から切り離します。

2. 外部ファイバ チャネル スイッチによって管理されたゾーンが Cisco UCS ドメイン 含まれる場合は、これらのゾーンを削除するために、影響を受けたすべての VSAN で `clear-unmanaged-fc-zone-all` コマンドを実行します。
3. ファイバ チャネル スイッチ モードの両方のファブリック インターコネクトでファイバ チャネル スイッチング モードを設定します。
4. ファイバチャネルゾーンのトラフィック転送に必要なファイバチャネルと FCoE ストレージ ポートを設定します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	まだ完了してない場合は、Cisco UCS ドメイン内のファブリック インターコネクトの接続を、外部ファイバ チャネル スイッチ（MDS など）から切り離します。	
ステップ 2	外部ファイバ チャネル スイッチによって管理されたゾーンが Cisco UCS ドメイン 含まれる場合は、これらのゾーンを削除するために、影響を受けたすべての VSAN で `clear-unmanaged-fc-zone-all` コマンドを実行します。	この機能は現在、Cisco UCS Manager GUI では使用できません。この手順は、Cisco UCS Manager CLI で実行する必要があります。
ステップ 3	ファイバ チャネル スイッチ モードの両方のファブリック インターコネクトでファイバチャネル スイッチング モードを設定します。	エンドホスト モードではファイバ チャネル ゾーン分割を設定できません。http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/3-1/b_UCSM_GUI_Storage_Management_Guide_3_1/b_UCSM_GUI_Storage_Management_Guide_3_1_chapter_01110.html#task_B6E0C2A15FE84D498503ADC19CDB160Bを参照してください。
ステップ 4	ファイバ チャネル ゾーンのトラフィック転送に必要なファイバチャネルと FCoE ストレージ ポートを設定します。	「Configuring an Ethernet Port as an FCoE Storage Port」および「Configuring a Fiber Channel Storage Port」を参照してください。次のリンクを参照してください。 http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Storage-Mgmt/3-1/b_UCSM_GUI_Storage_Management_Guide_3_1/b_UCSM_GUI_Storage_Management_Guide_3_1_chapter_01100.html#task_A33D13CA58924EB1AD35EBA473B92625

ダイレクト アタッチド ストレージ

標準的なダイレクトアタッチドストレージ（DAS）システムは、ホストバスアダプタ（HBA）を介してコンピュータに直接接続されているデータ ストレージデバイスで構成されています。これら2つのポイント間にはネットワーク デバイス（スイッチやルータなど）がありません。DAS 接続に使用される主要なプロトコルは、ATA、SATA、eSATA、SCSI、SAS、USB、USB 3.0、IEEE 1394、およびファイバ チャネルです。

Cisco UCS Manager では、SAN スイッチでゾーン分割設定をプッシュしなくても DAS を使用できます。ここで説明されている DAS の構成では、ストレージ アレイ ポートとファブリック インターコネクトの間に物理ケーブルが接続済みであることが想定されています。

（注） ストレージが直接接続されている場合でも、[SAN Cloud (SAN クラウド)] タブに VSAN が作成されます。

ファイバ チャネル スイッチング モード

ファイバ チャネル スイッチング モードは、サーバとストレージデバイス間のスイッチング装置としてファブリック インターコネクトがどのように動作するかを決定します。ファブリック インターコネクトは、次のファイバ チャネル スイッチング モードのいずれかで動作します。

エンドホスト モード

エンドホスト モードを使用すると、ファブリック インターコネクトは、仮想ホスト バス アダプタ（vHBA）を介して接続されているすべてのサーバ（ホスト）に代わって、接続されているファイバ チャネル ネットワークに対するエンド ホストとして動作することができます。この動作は、vHBA をファイバ チャネル ポート アダプタにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ファイバチャネルポートはファブリックの残りの部分に対してサーバ ポート（N ポート）となります。エンドホスト モードの場合、ファブリック インターコネクトは、アップリンク ポートがトラフィックを相互に転送するのを拒否することでループを回避します。

エンドホスト モードは N ポート仮想化（NPV）モードと同義です。このモードは、デフォルトのファイバ チャネル スイッチング モードです。

（注） エンドホスト モードを有効にした場合、vHBA がアップリンク ファイバ チャネル ポートに固定ピン接続されていて、このアップリンク ポートがダウンすると、システムはその vHBA をピン接続し直すことはできず、その vHBA はダウンしたままになります。

Switch Mode

スイッチ モードは従来のファイバ チャネル スイッチング モードです。スイッチ モードを使用して、ファブリック インターコネクトをストレージデバイスに直接接続することができます。ファイバ チャネル スイッチ モードの有効化は、SAN が存在しない（たとえば、ストレージに直接接続された 1 つの Cisco UCS ドメイン）ポッド モデル、または SAN が存在する（アップストリーム MDS を使用）ポッド モデルで役に立ちます。スイッチ モードはデフォルトのファイバ チャネル スイッチング モードではありません。

（注） ファイバ チャネル スイッチ モードでは、SAN ピン グループは不適切です。既存の SAN ピン グループはすべて無視されます。

ファイバ チャネル スイッチング モードの設定

重要 ファイバ チャネル スイッチング モードを変更する場合、Cisco UCS Manager の動作はバージョンによって異なります。

UCS Manager バージョン 3.1(1) 以前のリリースで、Cisco UCS Manager は同時にファブリック インターコネクトを同時に再起動します。

ファイバ チャネル スイッチング モードを変更すると、両方の Cisco UCS ファブリック インターコネクトが同時にリロードします。ファブリック インターコネクトがリロードすると、約 10 ～ 15 分のダウンタイムがシステム全体で発生します。

UCS Manager バージョン 3.1(2) では、ファイバ チャネル スイッチング モードが変更されると、UCS ファブリック インターコネクトが順次リロードされ、2 番目のファブリック インターコネクトがファイバ チャネル スイッチング モードの変更を完了してシステムの準備が整うまでに数分かかることがあります。

UCS Manager Release 3.1(3) では、スイッチング モードを変更した結果として、従属ファブリック インターコネクトが初めて再起動されます。プライマリ ファブリック インターコネクトは、[Pending Activities] で確認された後にのみ再起動します。プライマリ ファブリック インターコネクトがファイバ チャネル スイッチング モードに変更され、システムが使用できるようになるまでには数分間かかります。

詳細については、『Cisco UCS Manager Firmware Management Guide』を参照してください。

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。

ステップ 2 [Equipment] > [Fabric Interconnects] > [Fabric_Interconnect_Name] の順に展開します。

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

ステップ 4 [General] タブの [Actions] 領域で、次のリンクのいずれかをクリックします。

- **[Set FC Switching Mode]**
- **[Set FC End-Host Mode]**

  現在のモードのリンクはグレー表示されます。

ステップ 5 ダイアログボックスで、[Yes] をクリックします。

Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager GUI との接続を解除します。

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。

リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。

あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。