



ストレージ関連ポリシー

- [vHBA テンプレートについて \(1 ページ\)](#)
- [ファイバチャネルアダプタ ポリシー \(6 ページ\)](#)
- [デフォルトの vHBA 動作ポリシーについて \(17 ページ\)](#)
- [SAN 接続ポリシー \(18 ページ\)](#)

vHBA テンプレートについて

vHBA テンプレート

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る必要があります。

vHBA 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 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

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。

2. [SAN] > [Policies] の順に展開します。
3. ポリシーを作成する組織のノードを展開します。
4. [vHBA Templates] ノードを右クリックし、[Create vHBA Template] を選択します。
5. [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。
6. [OK] をクリックします。

手順の詳細

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] > [Policies] の順に展開します。

ステップ3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ4 [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5 [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	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。- (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。任意の文字またはスペースを使用できます。ただし、` (アクセント記号)、\ (バックスラッシュ)、^ (キャラット)、" (二重引用符)、= (等号)、> (大なり)、< (小なり)、または' (一重引用符) は使用できません。
[Fabric ID] フィールド	このテンプレートで作成された vHBA が関連付けられているファブリック インターコネクトの名前。
[Select VSAN] ドロップダウンリスト	このテンプレートから作成された vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Template Type] フィールド	次のいずれかになります。 <ul style="list-style-type: none"> • [Initial Template] : テンプレートが変更されても、このテンプレートから作成された vHBA はアップデートされません。 • [Updating Template] : 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 がアップデートされます。

名前	説明
[Max Data Field Size] フィールド	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。 256 ~ 2112 の範囲の整数を入力します。デフォルトは 2048 です。
[WWPN Pool] ドロップダウンリスト	このテンプレートから作成された vHBA によって、WWPN アドレスを導出するために使用される WWPN プール。
[QoS Policy] ドロップダウンリスト	このテンプレートから作成された vHBA に関連付けられている Quality of Service (QoS) ポリシー。
[Pin Group] ドロップダウンリスト	このテンプレートから作成された vHBA に関連付けられている SAN ピングループ。
[Stats Threshold Policy] ドロップダウンリスト	このテンプレートから作成された vHBA に関連付けられている統計情報収集ポリシー。

ステップ 6 [OK] をクリックします。

次のタスク

vHBA テンプレートはサービス プロファイルにインクルードします。

vHBA テンプレートへの vHBA のバインディング

サービス プロファイルと関連付けられた vHBA を vHBA テンプレートにバインドすることができます。vHBA を vHBA テンプレートにバインドした場合、Cisco UCS Manager により、vHBA テンプレートに定義された値を使って vHBA が設定されます。既存の vHBA 設定が vHBA テンプレートに一致しない場合、Cisco UCS Manager により、vHBA が再設定されます。バインドされた vHBA の設定は、関連付けられた vHBA テンプレートを使用してのみ変更できます。vHBA をインクルードしているサービス プロファイルがすでにサービス プロファイル テンプレートにバインドされている場合、vHBA を vHBA テンプレートにバインドできません。



重要 再設定されている vHBA をテンプレートにバインドした場合、Cisco UCS Manager により、サービス プロファイルと関連付けられているサーバがリブートされます。

手順の概要

1. [Navigation] ペインで [Servers] をクリックします。
2. [Servers] > [Service Profiles] の順に展開します。
3. vHBA とバインドするサービスプロファイルが含まれている組織のノードを展開します。
4. [Service_Profile_Name] > [vHBAs] を展開します。

5. テンプレートにバインドする vHBA をクリックします。
6. [Work] ペインで、[General] タブをクリックします。
7. [Actions] 領域で、[Bind to a Template] をクリックします。
8. [Bind to a vHBA Template] ダイアログボックスで、次の手順を実行します。
9. 警告ダイアログボックスの [Yes] をクリックすることにより、バインディングによって vHBA の再設定が生じた場合に Cisco UCS Manager でサーバのリブートが必要になる場合があることを確認します。

手順の詳細

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

ステップ 2 [Servers] > [Service Profiles] の順に展開します。

ステップ 3 vHBA とバインドする サービスプロファイル が含まれている組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Service_Profile_Name] > [vHBAs] を展開します。

ステップ 5 テンプレートにバインドする vHBA をクリックします。

ステップ 6 [Work] ペインで、[General] タブをクリックします。

ステップ 7 [Actions] 領域で、[Bind to a Template] をクリックします。

ステップ 8 [Bind to a vHBA Template] ダイアログボックスで、次の手順を実行します。

- a) [vHBA Template] ドロップダウンリストから、vHBA をバインドするテンプレートを選択します。
- b) [OK] をクリックします。

ステップ 9 警告ダイアログボックスの [Yes] をクリックすることにより、バインディングによって vHBA の再設定が生じた場合に Cisco UCS Manager でサーバのリブートが必要になる場合があることを確認します。

vHBA テンプレートからの vHBA のバインド解除

手順の概要

1. [Navigation] ペインで [Servers] をクリックします。
2. [Servers] > [Service Profiles] の順に展開します。
3. バインドを解除する vHBA を備えた サービスプロファイル が含まれている組織のノードを展開します。
4. [Service_Profile_Name] > [vHBAs] を展開します。
5. テンプレートからバインドを解除する vHBA をクリックします。
6. [Work] ペインで、[General] タブをクリックします。
7. [Actions] 領域で [Unbind from a Template] をクリックします。
8. 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

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

ステップ2 [Servers] > [Service Profiles] の順に展開します。

ステップ3 バインドを解除する vHBA を備えた サービスプロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ4 [*Service_Profile_Name*] > [vHBAs] を展開します。

ステップ5 テンプレートからバインドを解除する vHBA をクリックします。

ステップ6 [Work] ペインで、[General] タブをクリックします。

ステップ7 [Actions] 領域で [Unbind from a Template] をクリックします。

ステップ8 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

vHBA テンプレートの削除

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] > [*Organization_Name*] の順に展開します。
3. [vHBA Templates] ノードを展開します。
4. 削除する vHBA テンプレートを右クリックし、[Delete] を選択します。
5. 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

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] > [Policies] > [*Organization_Name*] の順に展開します。

ステップ3 [vHBA Templates] ノードを展開します。

ステップ4 削除する vHBA テンプレートを右クリックし、[Delete] を選択します。

ステップ5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ファイバチャネルアダプタポリシー

イーサネットおよびファイバチャネルアダプタポリシー

このようなポリシーは、アダプタのトラフィック処理方法など、ホスト側のアダプタの動作を制御します。たとえば、このようなポリシーを使用して、次のデフォルト設定を変更できます。

- キュー
- 割り込み処理
- パフォーマンス拡張
- RSS ハッシュ
- 2つのファブリック インターコネクトがあるクラスタ構成におけるフェールオーバー

**Note**

ファイバチャネルアダプタ ポリシーの場合は、Cisco UCS Manager で表示される値が QLogic SANsurfer などのアプリケーションで表示される値と一致しない場合があります。たとえば、次の値は、SANsurfer と Cisco UCS Manager で明らかに異なる場合があります。

- ターゲットごとの最大 LUN : SANsurfer の最大 LUN は 256 であり、この数値を超える値は表示されません。Cisco UCS Manager では、より大きな最大 LUN の値をサポートしています。このパラメータは、FC イニシエータにのみ適用されます。
- リンク ダウン タイムアウト : SANsurfer では、リンク ダウンのタイムアウトしきい値を秒単位で設定します。Cisco UCS Manager では、この値をミリ秒で設定します。したがって、Cisco UCS Manager で 5500 ミリ秒と設定された値は、SANsurfer では 5 秒として表示されます。
- 最大データフィールドサイズ : SANsurfer で許可された最大値は 512、1024、および 2048 です。Cisco UCS Manager では、任意のサイズの値を設定できます。したがって、Cisco UCS Manager で 900 と設定された値は、SANsurfer では 512 として表示されます。
- LUN Queue Depth : LUN キュー デプス設定は Windows システムの FC アダプタ ポリシーで使用できます。キュー デプスとは、HBA が 1 回の伝送で送受信できる LUN ごとのコマンドの数です。Windows Storport ドライバは、これに対するデフォルト値として、物理ミニポートに 20、仮想ミニポートに 250 を設定します。この設定により、アダプタのすべての LUN の初期キュー デプスを調整します。この値の有効範囲は 1 ~ 254 です。デフォルトの LUN キュー デプスは 20 です。この機能は、Cisco UCS Manager バージョン 3.1(2) 以降でのみ使用できます。このパラメータは、FC イニシエータにのみ適用されます。
- IO TimeOut Retry : 指定されたタイムアウト時間内にターゲット デバイスが I/O 要求に回答しない場合、FC アダプタは、タイマーの期限が切れると、保留中のコマンドを破棄して同じ IO を再送信します。この値に対する FC アダプタの有効範囲は 1 ~ 59 秒です。デフォルトの IO リトライ タイムアウトは 5 秒です。この機能は、Cisco UCS Manager バージョン 3.1(2) 以降でのみ使用できます。

オペレーティング システム固有のアダプタ ポリシー

デフォルトでは、Cisco UCS は、イーサネット アダプタ ポリシーとファイバチャネルアダプタ ポリシーのセットを提供します。これらのポリシーには、サポートされている各サーバオペレーティング システムにおける推奨設定が含まれています。オペレーティング システムはこれらのポリシーに影響されます。通常、ストレージベンダーはデフォルト以外のアダプタ設定を要求します。ベンダーが提供しているサポートリストで必須設定の詳細を確認できます。

**Important**

該当するオペレーティングシステムには、これらのポリシーの値を使用することを推奨します。シスコのテクニカルサポートで指示されない限り、デフォルトのポリシーの値は変更しないでください。

ただし、（デフォルトのアダプタポリシーを使用する代わりに）OSのイーサネットアダプタポリシーを作成する場合は、次の式を使用してそのOSで動作する値を計算する必要があります。

UCSファームウェアに応じて、ドライバの割り込み計算は異なる可能性があります。新しいUCSファームウェアは、以前のバージョンとは異なる計算を使用します。Linuxオペレーティングシステムの後のドライバリリースバージョンでは、割り込みカウントを計算するために別の式が使用されるようになってきていることに注意してください。この式で、割り込みカウントは送信キューまたは受信キューのどちらかの最大数+2になります。

Linux アダプタ ポリシーの割り込みカウント

Linuxオペレーティングシステムのドライバは、異なる計算式を使用して、eNICドライババージョンに基づき割り込みカウントを計算します。UCS 3.2 リリースは、それぞれ8～256までeNICドライバのTxとRxキューの数を増加しました。

ドライバのバージョンに応じて、次の戦略のいずれかを使用します。

UCS 3.2ファームウェアリリースより前のLinuxドライバは、次の計算式を使用して、割り込みカウントを計算します。

$$\text{完了キュー} = \text{送信キュー} + \text{受信キュー}$$

$$\text{割り込み回数} = (\text{完了キュー} + 2) \text{ 以上である } 2 \text{ のべき乗の最小値}$$

たとえば、送信キューが1で受信キューが8の場合、

$$\text{完了キュー} = 1 + 8 = 9$$

$$\text{割り込み回数} = (9 + 2) \text{ 以上の } 2 \text{ のべき乗の最小値} = 16$$

UCSファームウェアリリース3.2以上のドライバでは、Linux eNICドライバは次の計算式を使用して、割り込みカウントを計算します。

$$\text{Interrupt Count} = (\#Tx \text{ or } Rx \text{ Queues}) + 2$$

次に例を示します。

$$\text{割り込みカウント } wq = 32, rq = 32, cq = 64 - \text{割り込みカウント} = \text{最大}(32, 32) + 2 = 34$$

$$\text{割り込みカウント } wq = 64, rq = 8, cq = 72 - \text{割り込みカウント} = \text{最大}(64, 8) + 2 = 66$$

$$\text{割り込みカウント } wq = 1, rq = 16, cq = 17 - \text{割り込みカウント} = \text{最大}(1, 16) + 2 = 18$$

ファイバチャネルを使用したファブリック上のNVMe

NVM Express (NVMe) インターフェイスは、不揮発性メモリサブシステムとの通信にホストソフトウェアを使用できます。このインターフェイスは、PCI Express (PCIe) インターフェイスに

は通常、登録レベルインターフェイスとして添付されているエンタープライズ不揮発性ストレージが最適化されます。

ファイバチャネル (FC-NVMe) を使用したファブリック上の NVMe では、ファイバチャネル NVMe インターフェイスに適用するためのマッピングプロトコルを定義します。このプロトコルは、ファイバチャネルファブリック NVMe によって定義されたサービスを実行するファイバチャネルサービスと指定した情報単位 (IUs) を使用する方法を定義します。NVMe イニシエータにアクセスでき、ファイバチャネル経由で情報を NVMe ターゲットに転送します。

FC NVMe では、ファイバチャネルおよび NVMe の利点を組み合わせた。柔軟性と NVMe のパフォーマンスが向上し、共有ストレージアーキテクチャのスケラビリティを取得します。Cisco UCS Manager リリース 4.0(2) には、UCS VIC 14xx アダプタのファイバチャネルを使用したファブリック上の NVMe がサポートされています。

Cisco UCS Manager では、事前設定されているアダプタポリシーのリストで、推奨される FcNVMe アダプタポリシーを提供します。新しい FcNVMe アダプタポリシーを作成するには、ファイバチャネルアダプタポリシーの作成]セクションの手順に従います。

RDMA を使用したファブリック上の NVMe

ファブリック上の NVMe (NVMeoF) は、あるコンピュータが別のコンピュータで使用可能な NVMe ネームスペースにアクセスできる通信プロトコルです。NVMeoF は NVMe に似ていますが、NVMeoF ストレージデバイスの使用に関連するネットワーク関連の手順が異なります。NVMeoF ストレージデバイスを検出、接続、および接続解除するためのコマンドは、Linux に記載されている `nvme` ユーティリティに統合されています。

Cisco がサポートする NVMeoF は、コンバージドイーサネットバージョン 2 (RoCEv2) 上の RDMA です。RoCEv2 は、UDP を介して動作するファブリックプロトコルです。ドロップなしポリシーが必要です。

eNIC RDMA ドライバは eNIC ドライバと連携して動作します。これは、NVMeoF を設定するときに最初にロードする必要があります。

Cisco UCS Manager には、NVMe RoCEv2 インターフェイスを作成するためのデフォルトの Linux NVMe-RoCE アダプタポリシーが用意されています。デフォルトの Linux アダプタポリシーは使用しないでください。NVMeoF の RoCEv2 の設定の詳細については、コンバージドイーサネット (RoCE) v2 上の RDMA 向け Cisco UCS Manager 設定ガイドを参照してください。

RDMA を使用する NVMeoF は、Cisco UCS VIC 1400 シリーズアダプタを搭載した M5 B シリーズまたは C シリーズサーバでサポートされています。

ファイバチャネルアダプタポリシーの作成



ヒント この領域のフィールドが表示されない場合は、見出しの右側の展開アイコンをクリックします。

手順の概要

1. [Navigation] ペインで [Servers] をクリックします。
2. [Servers] > [Policies] の順に展開します。
3. ポリシーを作成する組織のノードを展開します。
4. [Adapter Policies] を右クリックし、[Create Fibre Channel Adapter Policy] を選択します。
5. 次のフィールドに、ポリシーの名前および説明を入力します。
6. (任意) [Resources] 領域で、次の値を調整します。
7. (任意) [Options] 領域で、次の値を調整します。
8. [OK] をクリックします。
9. 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Adapter Policies] を右クリックし、[Create Fibre Channel Adapter Policy] を選択します。

ステップ 5 次のフィールドに、ポリシーの名前および説明を入力します。

表 1:

名前	説明
[Name] フィールド	<p>ポリシーの名前。</p> <p>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。</p>
[Description] フィールド	<p>ポリシーの説明。ポリシーを使用する場所とタイミングについての情報を含めることを推奨します。</p> <p>256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、` (アクセント記号)、\ (バックスラッシュ)、^ (キャラット)、" (二重引用符)、= (等号)、> (大なり)、< (小なり)、または ' (一重引用符) は使用できません。</p>

ステップ 6 (任意) [Resources] 領域で、次の値を調整します。

名前	説明
[Transmit Queues] フィールド	割り当てる送信キュー リソースの数。 この値は変更できません。
[Ring Size] フィールド	各送信キュー内の記述子の数。このパラメータは、汎用サービスの Extended Link Services (ELS) および Common Transport (CT) ファイバチャネルフレームに適用されます。アダプタのパフォーマンスには影響しません。 64 ~ 128 の整数を入力します。デフォルトは 64 です。
[Receive Queues] フィールド	割り当てる受信キュー リソースの数。 この値は変更できません。
[Ring Size] フィールド	各受信キュー内の記述子の数。このパラメータは、汎用サービスの Extended Link Services (ELS) および Common Transport (CT) ファイバチャネルフレームに適用されます。アダプタのパフォーマンスには影響しません。 64 ~ 2048 の整数を入力します。デフォルトは 64 です。
[I/O Queues] フィールド	システムで割り当てる IO キュー リソースの数。 1 ~ 64 の整数を入力します。デフォルトは 16 です。
[Ring Size] フィールド	各 I/O キュー内の記述子の数。 64 ~ 512 の整数を入力します。デフォルトは 512 です。 (注) 記述子の数はアダプタのパフォーマンスに影響を与える可能性があるため、デフォルト値を変更しないことを推奨します。

ステップ7 (任意) [Options] 領域で、次の値を調整します。

名前	説明
[FCP Error Recovery] フィールド	<p>テープデバイスによるシーケンスレベルエラーの修復に FCP Sequence Level Error Recovery (FC-TAPE) プロトコルを使用するかどうかを選択します。これにより、VIC ファームウェアの Read Exchange Concise (REC) および Sequence Retransmission Request (SRR) 機能を有効または無効にできます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : デフォルトです。 • [Enabled] : システムが 1 つ以上のテープ ドライブ ライブラリに接続している場合は、このオプションを選択します。 <p>(注) このパラメータは、Virtual Interface Card (VIC) アダプタを搭載したサーバにのみ適用されます。</p>
[Flogi Retries] フィールド	<p>システムがファブリックへのログインを最初に失敗してから再試行する回数。</p> <p>任意の整数を入力します。システムが無限に試行し続けるように指定するには、このフィールドに「infinite」と入力します。ストレージレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>(注) このパラメータは、VIC アダプタまたはコンバージド ネットワーク アダプタを搭載したサーバにのみ適用されます。</p>
[Flogi Timeout (ms)] フィールド	<p>システムがログインを再試行する前に待機するミリ秒数。</p> <p>1000 ~ 255000 の整数を入力します。デフォルト値は 4,000 です。ストレージレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>(注) このパラメータは、VIC アダプタまたは統合型ネットワークアダプタを搭載したサーバにのみ適用されます。</p> <p>ブート vHBA で Flogi タイムアウト値を 20 秒以上に設定すると、アダプタが最初の Flogi に対する承認を受信しなかった場合に SAN ブート障害が発生する可能性があります。ブート可能な vHBA の場合、推奨されるタイムアウト値は 5 秒以下です。</p>

名前	説明
[Plogi Retries] フィールド	<p>システムがポートへのログインを最初に失敗してから再試行する回数。</p> <p>0 ～ 255 の整数を入力します。デフォルト値は 8 です。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>(注) このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。</p>
[Plogi Timeout (ms)] フィールド	<p>システムがログインを再試行する前に待機するミリ秒数。</p> <p>1000 ～ 255000 の整数を入力します。デフォルト値は 20,000 です。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>SAN から Windows OS をブートするために使用される HBA の場合、このフィールドの推奨値は 4,000 ミリ秒です。</p> <p>(注) このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。</p> <p>ブート vHBA で Plogi タイムアウト値を 20 秒以上に設定すると、アダプタが最初の Plogi に対する承認を受信しなかった場合に SAN ブート障害が発生する可能性があります。ブート可能な vHBA の場合、推奨されるタイムアウト値は 5 秒以下です。</p>
[Port Down Timeout (ms)] フィールド	<p>リモート ファイバチャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。このパラメータはホスト マルチパス ドライブにとって重要であり、エラー処理に使用される主要指標の 1 つとなります。</p> <p>0 ～ 240000 の整数を入力します。デフォルト値は 30,000 です。ESX を実行している VIC アダプタ搭載のサーバの場合、推奨値は 10,000 です。</p> <p>SAN から Windows OS をブートするために使用されるポートがあるサーバの場合、このフィールドの推奨値は 5,000 ミリ秒です。</p> <p>ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>(注) このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。</p>

名前	説明
IO リトライ タイムアウト (秒)	<p>保留中のコマンドを破棄して同じIOを再送信するまでにFCアダプタが待機する秒数です。これは、ネットワークデバイスが、指定された時間内の I/O 要求に応答しないと発生します。</p> <p>0～59の整数を入力します。デフォルトのIOリトライタイムアウトは5秒です。</p>
[Port Down IO Retry] フィールド	<p>ポートが使用不可能であるとシステムが判断する前に、そのポートへのIO要求がビジー状態を理由に戻される回数。</p> <p>0～255の整数を入力します。デフォルト値は8です。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>(注) このパラメータは、Windows を実行している VIC アダプタ搭載のサーバにのみ適用されます。</p>
[Link Down Timeout (ms)] フィールド	<p>アップリンクポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンクポートがオフラインになっていなければならないミリ秒数。</p> <p>0～240000の整数を入力します。デフォルト値は30,000です。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>(注) このパラメータは、Windows を実行している VIC アダプタ搭載のサーバにのみ適用されます。</p>
[IO Throttle Count] フィールド	<p>vHBA 内で同時に保留可能なデータまたは制御 I/O 操作の最大数。この値を超えると、保留中の I/O 操作の数が減り、追加の操作が処理できるようになるまで、キューで I/O 操作が待機します。</p> <p>(注) このパラメータは、LUN キューの長さと同じではありません。LUN キューの長さは、サーバにインストールされている OS に基づいて、Cisco UCS Managerにより管理されます。</p> <p>256～1024の整数を入力します。デフォルトは256です。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p>

名前	説明
[Max LUNs Per Target] フィールド	<p>ファイバチャネルドライバがエクスポートまたは表示する LUN の最大数。LUN の最大数は、通常、サーバで実行されている OS により管理されます。</p> <p>1 ～ 1024 の整数を入力します。デフォルト値は 256 です。ESX または Linux を実行しているサーバの場合、推奨値は 1024 です。</p> <p>オペレーティングシステムのドキュメントでこのパラメータの最適な値を確認することをお勧めします。</p> <p>(注)</p> <ul style="list-style-type: none"> • このパラメータは、VIC アダプタまたはネットワークアダプタを搭載したサーバにのみ適用されます。 • このパラメータは、FC イニシエータにのみ適用されません。
[LUN Queue Depth] フィールド	<p>HBA が 1 回の伝送で送受信できる LUN ごとのコマンドの数です。</p> <p>1 ～ 254 の整数を入力します。デフォルトの LUN キュー デプスは 20 です。</p> <p>(注) このパラメータは、FC イニシエータにのみ適用されます。</p>
[Interrupt Mode] オプション ボタン	<p>ドライバからオペレーティングシステムに割り込みを送信する方法。次のいずれかになります。</p> <ul style="list-style-type: none"> • [MSI-X] : 機能拡張された Message Signaled Interrupts (MSI) 。サーバのオペレーティングシステムがこれに対応している場合には、このオプションを選択することをお勧めします。 • [MSI] : MSI だけ。 • [INTx] : PCI INTx 割り込み。 <p>(注) このパラメータは、VIC アダプタを搭載しているサーバや、Window 以外の OS を実行しているネットワークアダプタ搭載のサーバにのみ適用されます。Windows OS では、このパラメータは無視されます。</p>

名前	説明
[vHBA Type] ラジオ ボタン	<p>このポリシーで使用される vHBA タイプ。サポートされている FC と FC NVMe Vhba は、同じアダプタでここで作成できます。このポリシーで使用される vHBA タイプには、次のいずれかを指定できます。</p> <ul style="list-style-type: none"> • FC イニシエータ]: レガシー SCSI FC vHBA イニシエータ • FC ターゲット: SCSI FC ターゲット機能をサポートする vHBA <p>(注) このオプションは、Tech Preview として利用できます。</p> <ul style="list-style-type: none"> • FC NVME イニシエータ-、FC NVME イニシエータ、FC NVME ターゲットを検出し、それらに接続するは vHBA • FCNVME ターゲット: FCNVME ターゲットとして機能し、NVME ストレージへの接続を提供する vHBA <p>(注) このオプションは、技術プレビューとして使用可能で す。</p> <p>vHBA タイプは、UCS VIC 14xx アダプタでのみサポートされています。</p>

ステップ 8 [OK] をクリックします。

ステップ 9 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ファイバチャネルアダプタポリシーの削除

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] > [Organization_Name] の順に展開します。
3. [Fibre Channel Policies] ノードを展開します。
4. 削除するポリシーを右クリックし、[Delete] を選択します。
5. 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

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] > [Policies] > [Organization_Name] の順に展開します。

ステップ 3 [Fibre Channel Policies] ノードを展開します。

ステップ 4 削除するポリシーを右クリックし、[Delete] を選択します。

ステップ5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

デフォルトの vHBA 動作ポリシーについて

デフォルトの vHBA 動作ポリシー

デフォルトの vHBA 動作ポリシーにより、サービス プロファイルに対する vHBA の作成方法を設定できます。vHBA を手動で作成するか、自動的に作成されるようにするかを選択できます。

デフォルトの vHBA 動作ポリシーを設定して、vHBA の作成方法を定義することができます。次のいずれかになります。

- [None] : Cisco UCS Manager サービス プロファイルにデフォルトの vHBA を作成しません。すべての vHBA を明示的に作成する必要があります。
- [HW Inherit] : サービス プロファイルが vHBA を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vHBA を作成します。



(注) vHBA のデフォルト動作ポリシーを指定しない場合、[none] がデフォルトで使用されます。

デフォルトの vHBA 動作ポリシーの設定

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] の順に展開します。
3. [root] ノードを展開します。
4. [Default vHBA Behavior] をクリックします。
5. [General] タブの、[Properties] 領域で、[Action] フィールドにある次のオプション ボタンの内の1つをクリックします。
6. [Save Changes] をクリックします。

手順の詳細

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] > [Policies] の順に展開します。

ステップ3 [root] ノードを展開します。

ルート組織内のデフォルトの vHBA 動作ポリシーのみを設定できます。サブ組織内のデフォルトの vHBA 動作ポリシーは設定できません。

ステップ 4 [Default vHBA Behavior] をクリックします。

ステップ 5 [General] タブの、[Properties] 領域で、[Action] フィールドにある次のオプションボタンの内の1つをクリックします。

- [None] : Cisco UCS Manager サービス プロファイルにデフォルトの vHBA を作成しません。すべての vHBA を明示的に作成する必要があります。
- [HW Inherit] : サービス プロファイルが vHBA を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vHBA を作成します。

ステップ 6 [Save Changes] をクリックします。

SAN 接続ポリシー

LAN および SAN 接続ポリシーについて

接続ポリシーは、ネットワーク上のサーバと LAN または SAN 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) 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められ、複数のサーバの設定に使用される可能性があるため、接続ポリシーでは静的 ID を使用しないことをお勧めします。

LAN および SAN の接続ポリシーに必要な権限

接続ポリシーを使用すると、ネットワーク権限またはストレージ権限のないユーザが、ネットワーク接続とストレージ接続を備えたサービス プロファイルやサービス プロファイルテンプレートを作成したり変更したりできるようになります。ただし、接続ポリシーを作成するには、適切なネットワーク権限とストレージ権限が必要です。

接続ポリシーの作成に必要な権限

接続ポリシーは、他のネットワークやストレージの設定と同じ権限を必要とします。たとえば、接続ポリシーを作成するには、次の権限の少なくとも1つを有している必要があります。

- admin : LAN および SAN 接続ポリシーを作成できます
- ls-server : LAN および SAN 接続ポリシーを作成できます
- ls-network : LAN 接続ポリシーを作成できます
- ls-storage : SAN 接続ポリシーを作成できます

接続ポリシーをサービス プロファイルに追加するために必要な権限

接続ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイルテンプレートに組み込むことができます。ただし、ls-compute 権限しかないユーザは接続ポリシーを作成できません。

サービス プロファイルと接続ポリシー間の相互作用

次のいずれかの方法により、サービス プロファイルに LAN および SAN の接続を設定できます。

- サービス プロファイルで参照される LAN および SAN 接続ポリシー
- サービス プロファイルで作成されるローカル vNIC および vHBA
- ローカル vNIC および SAN 接続ポリシー
- ローカル vHBA および LAN 接続ポリシー

Cisco UCS では、サービス プロファイルのローカル vNIC および vHBA 設定と接続ポリシー間の相互排他性が維持されます。接続ポリシーとローカルに作成した vNIC または vHBA を組み合わせて使用することはできません。サービス プロファイルに LAN 接続ポリシーを含めると、既存の vNIC 設定がすべて消去されます。SAN 接続ポリシーを含めた場合は、そのサービス プロファイル内の既存の vHBA 設定がすべて消去されます。

SAN 接続ポリシーの作成

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] の順に展開します。
3. ポリシーを作成する組織のノードを展開します。
4. [SAN Connectivity Policies] を右クリックし、[Create SAN Connectivity Policy] を選択します。
5. [Create SAN Connectivity Policy] ダイアログボックスで、名前と任意の説明を入力します。
6. [World Wide Node Name] 領域の [WWNN Assignment] ドロップダウンリストから次のいずれかを選択します。
7. [vHBAs] テーブルで、[Add] をクリックします。
8. [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。

9. [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。
10. [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
11. [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。
12. ポリシーに必要なすべての vHBA を作成したら、[OK] をクリックします。

手順の詳細

-
- 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] > [Policies] の順に展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** [SAN Connectivity Policies] を右クリックし、[Create SAN Connectivity Policy] を選択します。
- ステップ 5** [Create SAN Connectivity Policy] ダイアログボックスで、名前と任意の説明を入力します。
- ステップ 6** [World Wide Node Name] 領域の [WWNN Assignment] ドロップダウン リストから次のいずれかを選択します。
- デフォルトの WWN プールを使用するには、 を選択します。
 - [Manual Using OUI] に一覧表示されるオプションのいずれかを選択し、[World Wide Node Name] フィールドに WWN を入力します。

WWNN 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 の範囲内で指定できます。[here] リンクをクリックして、指定した WWNN が使用可能であることを確認できます。
 - 指定したプールから WWN を割り当てるには、リストから WWN プール名を選択します。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 7** [vHBAs] テーブルで、[Add] をクリックします。
- ステップ 8** [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。
- ステップ 9** [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。
この領域から VSAN または SAN ピン グループを作成することもできます。
- ステップ 10** [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
- ステップ 11** [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。
この領域からファイバチャネルアダプタ ポリシーまたは QoS ポリシーを作成することもできます。
- ステップ 12** ポリシーに必要なすべての vHBA を作成したら、[OK] をクリックします。
-

次のタスク

ポリシーはサービス プロファイルまたはサービス プロファイル テンプレートにインクルードします。

SAN 接続ポリシー用の vHBA の作成

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] タブで、[SAN] > [Policies] > [Organization_Name] > [San Connectivity Policies] の順に展開します。
3. vHBA を作成するポリシーを選択します。
4. [Work] ペインで、[General] タブをクリックします。
5. テーブル アイコン バーの [+] ボタンをクリックします。
6. [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。
7. [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。
8. [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
9. [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。
10. [Save Changes] をクリックします。

手順の詳細

-
- 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] タブで、[SAN] > [Policies] > [Organization_Name] > [San Connectivity Policies] の順に展開します。
- ステップ 3** vHBA を作成するポリシーを選択します。
- ステップ 4** [Work] ペインで、[General] タブをクリックします。
- ステップ 5** テーブル アイコン バーの [+] ボタンをクリックします。
- ステップ 6** [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。
- ステップ 7** [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。
この領域から VSAN または SAN ピン グループを作成することもできます。
- ステップ 8** [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
- ステップ 9** [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。
この領域からファイバ チャネル アダプタ ポリシーまたは QoS ポリシーを作成することもできます。
- ステップ 10** [Save Changes] をクリックします。
-

SAN 接続ポリシーからの vHBA の削除

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] > [Organization_Name] の順に展開します。
3. vHBA を削除するポリシーを選択します。
4. [Work] ペインで、[General] タブをクリックします。
5. [vHBAs] テーブルで、次の手順を実行します。
6. 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

-
- 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] > [Policies] > [Organization_Name] の順に展開します。
 - ステップ 3 vHBA を削除するポリシーを選択します。
 - ステップ 4 [Work] ペインで、[General] タブをクリックします。
 - ステップ 5 [vHBAs] テーブルで、次の手順を実行します。
 - a) 削除する vHBA をクリックします。
 - b) アイコンバーで [Delete] をクリックします。
 - ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
-

SAN 接続ポリシー用のイニシエータ グループの作成

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] > [Organization_Name] の順に展開します。
3. イニシエータ グループを作成するポリシーを選択します。
4. [Work] ペインで、[vHBA Initiator Groups] タブをクリックします。
5. テーブル アイコン バーの [+] ボタンをクリックします。
6. [Create vHBA Initiator Group] 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。
7. [OK] をクリックします。

手順の詳細

-
- 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] > [Policies] > [Organization_Name] の順に展開します。

- ステップ3** イニシエータ グループを作成するポリシーを選択します。
- ステップ4** [Work] ペインで、[vHBA Initiator Groups] タブをクリックします。
- ステップ5** テーブル アイコンバーの [+] ボタンをクリックします。
- ステップ6** [Create vHBA Initiator Group] 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 イニシエータ グループの名前。 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	グループの説明。 256文字以下で入力します。任意の文字またはスペースを使用できます。ただし、` (アクセント記号)、\ (バックスラッシュ)、^ (キャラット)、" (二重引用符)、= (等号)、> (大なり)、< (小なり)、または' (一重引用符) は使用できません。
[Select vHBA Initiators] テーブル	使用する各 vHBA に対応する、[Select] カラムのチェックボックスをオンにします。
[Storage Connection Policy] ドロップダウン リスト	この vHBA イニシエータ グループに関連付けられているストレージ接続ポリシー項目 <ul style="list-style-type: none"> 既存のストレージ接続ポリシーを使用して、ドロップダウンリストからそのポリシーを選択します。Cisco UCS Manager GUIでは、[Global Storage Connection Policy] 領域に、ポリシーとその FC ターゲット エンドポイントに関する情報が表示されます。 グローバルに利用できる新しいストレージ接続ポリシーを作成し、[Create Storage Connection Policy] リンクをクリックします。 この vHBA イニシエータ グループでのみ利用できるローカルストレージ接続ポリシーを作成し、[Specific Storage Connection Policy] オプションを選択します。Cisco UCS Manager GUI に表示される [Specific Storage Connection Policy] 領域を使って、ローカルストレージ接続ポリシーを設定できます。
[Create Storage Connection Policy] リンク	すべてのサービス プロファイルとサービス プロファイル テンプレートで使用可能な新しいストレージ接続ポリシーを作成するには、このリンクをクリックします。

- ステップ7** [OK] をクリックします。

SAN 接続ポリシーからのイニシエータ グループの削除

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] > [Organization_Name] の順に展開します。
3. イニシエータ グループを削除するポリシーを選択します。
4. [Work] ペインで、[vHBA Initiator Groups] タブをクリックします。
5. テーブルで、次の手順を実行します
6. 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

-
- 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] > [Policies] > [Organization_Name] の順に展開します。
 - ステップ 3 イニシエータ グループを削除するポリシーを選択します。
 - ステップ 4 [Work] ペインで、[vHBA Initiator Groups] タブをクリックします。
 - ステップ 5 テーブルで、次の手順を実行します
 - a) 削除するイニシエータ グループをクリックします。
 - b) アイコンバーで [Delete] をクリックします。
 - ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
-

SAN 接続ポリシーの削除

サービス プロファイルに含まれる SAN 接続ポリシーを削除する場合、すべての vHBA もそのサービス プロファイルから削除し、そのサービス プロファイルに関連付けられているサーバの SAN データ トラフィックを中断します。

手順の概要

1. [Navigation] ペインで [SAN] をクリックします。
2. [SAN] > [Policies] > [Organization_Name] の順に展開します。
3. [SAN Connectivity Policies] ノードを展開します。
4. 削除するポリシーを右クリックし、[Delete] を選択します。
5. 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手順の詳細

-
- 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] > [Policies] > [Organization_Name] の順に展開します。
- ステップ3 [SAN Connectivity Policies] ノードを展開します。
- ステップ4 削除するポリシーを右クリックし、[Delete] を選択します。
- ステップ5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

Intel® ボリューム管理デバイスの有効化

ボリューム管理デバイス (VMD) の設定

Intel® ボリューム管理デバイス (VMD) は、VMD 対応ドメインに接続された PCIe ソリッドステートドライブを管理するための NVMe ドライバを提供するツールです。これには、PCIe ドライブの Surprise ホットプラグと、ステータスを報告するための点滅パターンの設定が含まれます。PCIe ソリッドステートドライブ (SSD) ストレージには、デバイスのステータスを示すために LED を点滅させる標準化された方法がありません。VMD を使用すると、単純なコマンドラインツールを使用して、直接接続された PCIe ストレージとスイッチに接続された PCIe ストレージの両方の LED インジケータを制御できます。

VMD を使用するには、最初に UCS Manager BIOS ポリシーを使用して VMD を有効にして、UEFI ブート オプションを設定する必要があります。VMD を有効にすると、ルートポートに接続されている PCIe SSD ストレージに対して、Surprise ホットプラグとオプションの LED ステータス管理が提供されます。VMD パススルーモードは、ゲスト VM 上のドライブを管理する機能を提供します。

また、VMD を有効にすると、intel® Xeon® スケーラブルプロセッサのハイブリッド RAID アーキテクチャである CPU 上の Intel® 仮想 RAID (VRoC) の設定も可能になります。VRoC の使用および設定に関するマニュアルは、Intel の Web サイトを参照してください。

重要： VMD は、オペレーティングシステムをインストールする前に、UCS Manager BIOS 設定で有効にする必要があります。OS のインストール後に有効にすると、サーバの起動に失敗します。この制限は、標準の VMD および VMD パススルーの両方に適用されます。同様に有効にすると、システム機能を失わずに VMD を無効にすることはできません。

UCS Manager での VMD の有効化

UCS Manager で VMD の BIOS およびローカルブートポリシーを設定するには、次の手順を実行します。VMD プラットフォームのデフォルトは無効になっています。



(注) OS をインストールする前に、VMD を有効にする必要があります。

- ステップ1 [Navigation] ペインで [Servers] をクリックします。
- ステップ2 ポリシーを作成する組織のノードを展開します。

システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

- ステップ 3** VMD の BIOS ポリシーの設定：サービスプロファイルを選択し、[ポリシー (Policies)] タブに移動します。[ポリシー (Policies)] セクションで、BIOS セクションを右クリックして、ポップアップから **[BIOS ポリシーの作成 (Create BIOS Policy)]** を選択します。[BIOS ポリシー (BIOS Policy)] フォームに名前と説明 (任意) を入力します。[OK] をクリックしてポリシーを作成します。
- ステップ 4** [ポリシー (Policies)] > [ルート (Root)] > **[BIOS ポリシー (BIOS Policies):]** に移動し、新しいポリシーを選択します。
- ステップ 5** **[BIOS ポリシー (BIOS Policies)]** を展開し、サブメニューから **[アドバンスド (Advanced)]** および **[LOM および PCIe スロット (LOM and PCIe Slots)]** を選択します。
- ステップ 6** **[VMD の有効化 (VMD enable)]** まで下にスクロールし、**[有効 (enable)]** を選択します。
- ステップ 7** **[保存を変更 (Save Changes)]** をクリックして、VMD 機能を有効にします。
- ステップ 8** **[ブート ポリシー (Boot Policy)]** タブで、ローカルブートポリシーを作成します。ブートモードとして **[Uefi]** を選択し、**[ローカル デバイス (Local Devices)]** メニューから **NVMe** を追加します。[変更の保存 (Save Changes)] をクリックし、ポリシーの変更内容を保存します。

パススルーモードでボリューム管理デバイス (VMD) 有効化

ボリューム管理デバイス (VMD) パススルーモード

直接デバイス割り当て用の Intel® ボリューム管理デバイス (VMD) ドライバリリースパッケージには、VMware ESXi ハイパーバイザの直接割り当て (PCIe パススルー) 用の Intel VMD UEFI ドライババージョンが含まれています。7 Intel VMD NVMe ドライバは、CPU に接続された Intel PCIe NVMe SSD の管理に役立ちます。

サポートされているゲスト VM からの VMD 物理アドレスの直接割り当てと検出を有効にするには、Intel VMD ドライバが必要です。ドライバは、Red Hat Linux または Ubuntu の ESXi サポートのパススルーモードに対してのみ提供されます。VMD パススルーは、オペレーティングシステムをロードする前に UCS Manager BIOS ポリシーを設定することで有効になります。オペレーティングシステムがロードされると、VMD パススルーオプションを有効または無効にすることはできません。



- (注) パススルーモードはデフォルトで有効になっていますが、続行する前に有効になっていることを常に確認する必要があります。

VMD パススルーの設定

パススルーモードは、Red Hat Linux または Ubuntu ゲストオペレーティングシステムの ESXi ドライバでのみサポートされています。

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

- ステップ 2** ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 3** VMD の BIOS ポリシーの設定：サービス プロファイルを選択し、[ポリシー (Policies)] タブに移動します。[ポリシー (Policies)] セクションで、BIOS セクションを右クリックして、ポップアップから [BIOS ポリシーの作成 (Create BIOS Policy)] を選択します。[BIOS ポリシー (BIOS Policy)] フォームに名前と説明 (任意) を入力します。[OK] をクリックしてポリシーを作成します。
- ステップ 4** [ポリシー (Policies)] > [ルート (Root)] > [BIOS ポリシー (BIOS Policies):] に移動し、新しいポリシーを選択します。
- ステップ 5** [BIOS ポリシー (BIOS Policies)] を展開し、サブメニューから [アドバンスド (Advanced)] および [LOM および PCIe スロット (LOM and PCIe Slots)] を選択します。
- ステップ 6** [VMD の有効化 (VMD enable)] まで下にスクロールし、[有効 (enable)] を選択します。
- ステップ 7** [保存を変更 (Save Changes)] をクリックして、VMD 機能を有効にします。
- ステップ 8** VMD パススルー モードの有効化を完了するには、サブメニューから [アドバンスド (Advanced)] および [Intel Directed IO] を選択し、[Intel VT Directed IO] までスクロールダウンします。ドロップダウンが [有効 (Enabled)] に設定されていることを確認します。そうでない場合は、設定します。
- ステップ 9** [変更を保存 (Save Changes)] をクリックして、VMD パススルー ポリシーを有効にします。
- ステップ 10** [ブート ポリシー (Boot Policy)] タブで、ローカル ブート ポリシーを作成します。[ブート モード (Boot Mode)] の [Uefi] を選択します。[OK] をクリックしてポリシーを作成します。

VMD ドライバのダウンロード

Intel® ボリューム管理デバイス ドライバ

NVMe 用 Intel® ボリューム管理デバイス (VMD) は、Intel Xeon プロセッサ内のハードウェア ロジックを使用してドライブ管理オプションを有効にします。特定のドライバは、次のオペレーティング システムで使用できます。

- Linux
- Windows 2016、2019
- VMWare



(注) 最新の VMWare ドライバは、VMWare サイトから直接入手できます。Cisco のダウンロードサイトで VMWare ドライバをダウンロード可能な次のリンクでは、VMWare のログインページに直接移動します。

ESXi 上のゲストオペレーティングシステムの場合は、VMD パススルーモードを使用します。VMD パススルーでサポートされているオペレーティングシステムは次のとおりです。

VMD を搭載している CPU (VRoC) の Intel® 仮想 RAID

- Red Hat Linux
- Ubuntu

Intel VMD の機能を使用するには、次のことを行う必要があります。

- UCS Manager で BIOS ポリシーを作成して、VMD を有効にします。



(注) OS のインストール後に VMD が有効または無効になっている場合、システムの起動に失敗します。OS のインストール後に BIOS 設定を変更しないでください。

- 適切な VMD NVMe ドライバをインストールします。
- ドライバパッケージに適切な管理ツールをインストールします。
- UEFI から起動します。

VMD を搭載している CPU (VRoC) の Intel® 仮想 RAID

CPU (VRoC) の Intel® 仮想 RAID サポートでは、Intel Xeon プロセッサ内部の VMD 対応 Intel NVMe SSD ドライブの BIOS 内で RAID ボリュームを作成および管理できます。Intel VRoC の詳細については、<https://www.intel.com/content/www/us/en/support/products/122484/memory-and-storage/ssd-software/intel-virtual-raid-on-cpu-intel-vroc.html> を参照してください。

Intel VRoC のユーザー ガイドには、次のリンク先から直接アクセスできます。
https://www.intel.com/content/www/us/en/support/articles/000030445/memory-and-storage/ssd-software.html?productId=122484&localeCode=us_en

Windows および Linux ユーザー マニュアルには、事前ブート環境での Intel VRoC の設定方法についても記載されています。VRoC での RAID ボリュームの作成は、HII インターフェイスを介して実行されます。Windows のマニュアルでは、[BIOS HII] オプションを使用して VRoC で RAID ボリュームを設定する方法について説明します。

Intel VRoC を使用するには、次のことを行う必要があります。

- BIOS 設定で VMD を有効にする
- UEFI ブート モードを使用する
- ボリュームを作成するのに十分なドライブ リソースがある
- [BIOS HII] オプションを使用して、VRoC を設定し、設定します。

Cisco の Intel VRoC の実装では、RAID 0 (ストライピング)、RAID 1 (ミラーリング)、RAID 5 (パリティ付きストライピング)、および RAID 10 (ミラーリングとストライピングの組み合わせ) がサポートされています。

Linux VMD ドライバのダウンロード

ドライババンドルをダウンロードしてインストールするには、次の手順を実行します。

始める前に

BIOS 設定で VMD が有効になっていることを確認してください。



(注) OS のインストール後に VMD が有効または無効になっている場合、システムの起動に失敗します。OS のインストール後に BIOS 設定を変更しないでください。

ステップ 1 Web ブラウザで、<https://software.cisco.com/download/home>を開きます。

ステップ 2 プラットフォームに応じて、**UCS B シリーズ ブレード サーバソフトウェア**または **UCS C シリーズ ラックマウント UCS 管理対象サーバソフトウェア**を検索します。

ステップ 3 ソフトウェア タイプの選択から UCS ドライバを選択します。ユニファイド コンピューティング システム (UCS) ドライバ。

ステップ 4 左のパネルの最新リリースをクリックします。

(注) ブレードサーバの VMD の ISO イメージは、4.0 (4f) リリース以降で使用できます。

ステップ 5 [UCS 関連の linux ドライバの ISO イメージのみ (ISO image of UCS-related linux drivers only)] をクリックして、ドライババンドルをダウンロードします。

ステップ 6 ドライババンドルがダウンロードされたら、それを開き、[ストレージ (Storage)] > [Intel] > > [RHEL]/x.x/を選択します。

ステップ 7 インストールする Red Hat Linux のバージョンをクリックします。

ステップ 8 フォルダのコンテンツを展開します。このフォルダには、ドライバパッケージと関連資料の両方が含まれています。ドライバとともにパッケージ化されたインストール手順に従います。

次のタスク

CPU (VRoC) の Intel® 仮想 RAID Linux ソフトウェア ユーザー ガイドは、https://www.intel.com/content/www/us/en/support/articles/000030445/memory-and-storage/ssd-software.html?productId=122484&localeCode=us_en のユーザー マニュアルに記載されています。これは、ブート前環境での BIOS HII VRoC 設定の実行に関する情報と、プログラム可能な LED ユーティリティのインストールと使用方法について説明します。

Windows VMD ドライバのダウンロード

ドライババンドルをダウンロードするには、次の手順を実行します。

始める前に

BIOS 設定で VMD が有効になっていることを確認してください。



(注) OS のインストール後に VMD が有効または無効になっている場合、システムの起動に失敗します。OS のインストール後に BIOS 設定を変更しないでください。

- ステップ 1** Web ブラウザで、<https://software.cisco.com/download/home>を開きます。
- ステップ 2** プラットフォームに応じて、**UCS B シリーズ ブレードサーバソフトウェア**または**UCS C シリーズ ラックマウント UCS 管理対象サーバソフトウェア**を検索します。
- ステップ 3** ソフトウェア タイプの選択から UCS ドライバを選択します。ユニファイド コンピューティング システム (UCS) ドライバ。
- ステップ 4** 左のパネルの最新リリースをクリックします。
- VMD の ISO イメージは、4.0 (4f) リリース以降で使用できます。
- ステップ 5** **[UCS 関連の windows ドライバの ISO イメージのみ (ISO image of UCS-related windows drivers only)]** をクリックして、ドライババンドルをダウンロードします。
- ステップ 6** ドライババンドルがダウンロードされたら、それを開き、**[ストレージ (Storage)] > [Intel] > [VMD] > [KIT_x_x_x_xxxx]** を選択します。
- ステップ 7** フォルダのコンテンツを展開します。
- ステップ 8** キットと **[キット (KIT)] > [インストール (Install)]** のエントリをクリックします。
- ステップ 9** このフォルダには、ドライバパッケージと関連資料の両方が含まれています。**VROC_x_x_x_xxxxInstall** の zip ファイルを展開します。
- ステップ 10** ドライバとともにパッケージ化されたインストール手順に従います。

次のタスク

CPU (VRoC) の Intel®仮想 RAID の設定については、<https://www.intel.com/content/www/us/en/support/products/122484/memory-and-storage/ssd-software/intel-virtual-raid-on-cpu-intel-vroc.html> のオンライン手順を参照してください。

VRoC RAID の機能と管理に関する情報については、https://www.intel.com/content/dam/support/us/en/documents/memory-and-storage/ssd-software/Windows_VROC_User_Guide.pdf の『CPU ソフトウェア ユーザー ガイドの Windows Intel 仮想 RAID』を参照してください。

VMD パススルー ドライバのダウンロード

VMD パススルーモードのドライババンドルをダウンロードしてインストールするには、次の手順を実行します。



(注) VMD パススルー ドライババンドルには、ESXi と Ubuntu の両方のパッケージが含まれていません。

始める前に



(注) OS のインストール後に VMD が有効または無効になっている場合、システムの起動に失敗します。OS のインストール後に BIOS 設定を変更しないでください。

ステップ 1 Web ブラウザで、<https://software.cisco.com/download/home>を開きます。

ステップ 2 サーバ - ユニファイド コンピューティングの検索

ステップ 3 プラットフォームに応じて、**UCS B シリーズ ブレード サーバソフトウェア**または **UCS C シリーズ ラックマウント UCS 管理対象サーバソフトウェア**を検索します。

ステップ 4 ソフトウェア タイプの選択から UCS ユーティリティを選択します。ユニファイド コンピューティングシステム (UCS) ユーティリティ。

ステップ 5 左のパネルの最新リリースをクリックします。

(注) VMD の ISO イメージは、UCSM 4.0 (4f) リリース以降で使用できます。

ステップ 6 [UCS 関連の vmware ユーティリティの ISO イメージのみ (ISO image of UCS-related vmware utilities only)] をクリックして、ユーティリティバンドルをダウンロードします。

ステップ 7 ドライババンドルがダウンロードされたら、それを開き、[ストレージ (Storage)] > [Intel] > [VMD] を選択します。

バンドルには、目的のバージョンの ESXi または VMD Direct Assign with Ubuntu、パススルー モード、および署名付き LED オフラインバンドルの両方のドライバインストールパッケージが用意されています。また、ESXi で Ubuntu 仮想マシンを設定する手順を提供する pdf も含まれています。

ステップ 8 インストールする ESXi のバージョンまたは Ubuntu 用の zip ファイルのいずれかをクリックします。

ESXi バージョンの場合は、**ESXi_x > Direct Assign** をクリックして、目的の zip ファイルを選択します。

ステップ 9 フォルダのコンテンツを展開します。ドライバソフトウェアとともにパッケージ化されたインストール手順に従います。

次のタスク

LED 管理ツール zip ファイルを解凍します。ドライバパッケージに記載されている手順に従って、管理ツールをインストールします。

コマンドライン ツールを使用する前に、ESXi コマンドラインシェルを、vSphere クライアントまたは ESXi ホストシステムの直接コンソールのいずれかから有効にする必要があります。

NVMe の高度な VMD 搭載したカスタム LED のステータス

VMD を設定したら、PCIe NVMe ドライブの LED 点滅パターンをカスタマイズできます。LED のカスタマイズに関する情報については、ドライバパッケージに含まれているユーザーガイドを参照してください。

LED の点滅

PCIe SSD ドライブは、ドライブのステータスと健全性を示す LED を管理するための標準的な方法はありません。これがない場合、誤ったドライブを削除するリスクが生じ、結果としてデータが失われます。SSD ドライブには2つのインジケータがあり、最初は緑色のアクティビティ LED で信号が SSD から直接到着します。2 番目はバックプレーンから信号が送信されるステータス LED です。VMD は、アクティビティ LED ではなく、ステータス LED のみを管理します。

LED 管理は、NVMe または SATA ドライブにのみ適用されます。I/O ケーブル、PCIe アドインカードのいずれか、またはマザーボードに直接接続されているドライブはサポートされません。

ドライブホットプラグ時の LED の動作

NVMe を持つ VMD は、突然のホットプラグをサポートします。ディスクがホット解除され、同じスロットに再装着されると、障害 LED が 10 秒間点滅します。これは予期される動作です。ドライブが取り外されたときに、スロットの LED が障害状態を示されますが、バックプレーンでは LED が点滅可能になるように、ドライブがスロットに存在する必要があります。したがって、障害状態はドライブが取り外された後にも発生していますが、新しいドライブが挿入されて検出されたときにのみ LED が点滅します。ホットプラグイベントが処理されると、LED は通常の状態に戻ります。

カスタム点滅パターン

VMD を搭載した VRoC では、互換性のあるバックプレーンのステータス LED の基本 LED 管理設定を行うことができます。VMD NVMe ドライバがインストールされたら、VMD LED 管理ツールをインストールできます。これにより、コマンドラインインターフェイスで LED を管理できます。VMD を使用すると、障害が発生したドライブを識別しやすくするために、PCIe NVMe ドライブの LED 点滅パターンをカスタマイズできます。

次の表に、さまざまなプラットフォームでカスタマイズされた点滅に関する簡単なガイドラインを示します。独自のパターンがプログラム可能であるため、これらの表には代表的なガイドラインのみが記載されています。

表 2: LED 点滅パターン: Windows

ステータス LED	動作	オプション
「アクティブ LED」	指定されたパターンでそのドライブのステータス LED を点滅させることにより、エンクロージャ内の特定のデバイスを識別します。	1 ~ 3600 秒。この範囲外の値は、デフォルトで 12 秒に設定されています。 デフォルトは 12 秒です。
ドライブの障害	デバイスのステータス LED を、定義された障害パターンで点灯することによって、縮退状態または障害状態のドライブを示します。	障害パターンは、次の場合に表示されます。 <ul style="list-style-type: none"> 1. 物理的に取り外された場合。 または 障害が発生したドライブを含む RAID ボリュームは、削除されるか、物理的に取り外されます。 2. RAID ボリュームの一部である障害が発生していないドライブが取り外された時点、または障害が発生したドライブが識別され取り外された時点から。新しいドライブが同じスロットに挿入されるか、またはプラットフォームがリブートされるまで、障害状態のままになります。 デフォルト = オプション 1
RAID ボリュームの初期化または確認と修復のプロセス	RAID ボリュームが再構築状態になると、再構築されている特定のドライブまたは再構築されている RAID ボリューム全体のいずれかで、定義された再構築パターンでステータス LED が点滅します。	デフォルト = 有効 次のように設定できます。 <ol style="list-style-type: none"> 1. 無効 (1 台のドライブのみ) 2. 有効 (すべてのドライブ)

ステータス LED	動作	オプション
管理対象の取り外し	管理対象のホットプラグでは、ドライブが物理的に取り出されるまで、管理対象ドライブのステータス LED が、定義された検出パターンで点滅します。	なし。デフォルトでは、イネーブルです。
RAID ボリュームが移行中です	RAID ボリュームの移行中は、プロセスが完了するまで、すべてのドライブで定義されている再構築パターンでステータス LED が点滅します。	デフォルト = 有効 次のように設定できます。 1. 無効 (ステータス LED は点滅しません) 2. 有効 (ステータス LED を点滅)
Rebuild	移行中のドライブのみが点滅します。	デフォルト = 無効

表 3: LED 点滅パターン: Linux

ステータス LED	動作	オプション
コントローラのスキップ/除外 BLACKLIST	ledmon はブラックリストにリストされているスキャンコントローラを除外します。設定ファイルでホワイトリストも設定されている場合、ブラックリストは無視されます。	ブラックリストのコントローラを除外します。 デフォルト = すべてのコントローラをサポート
RAID ボリュームの初期化、検証、または検証と修正 BLINK_ON_INIT	RAID ボリューム内のすべてのドライブでパターンを再構築します (初期化、検証、または検証および修正が完了するまで)。	1. True/有効 (すべてのドライブ上) 2. False/無効 (ドライブなし) デフォルト = True/有効
ledmon スキャン間隔の設定 間隔	ledmon sysfs スキャン間の時間間隔を定義します。 値は秒単位です。	10s (最大 5s) デフォルトは 10 秒です。
RAID ボリュームの再構築 (RAID 再構築) REBUILD_BLINK_ON_ALL	RAID ボリュームが再構築される単一ドライブ上でパターンを再構築	1. False/無効 (1 台のドライブ) 2. True/有効 (すべてのドライブ上) デフォルト = False/無効

ステータス LED	動作	オプション
RAID ボリュームが以降中で BLINK_ON_MIGR	RAID ボリューム内のすべてのドライブでパターンを再構築します(移行が完了するまで)。	1. True/有効(すべてのドライブ上) 2. False/無効(ドライブなし) デフォルト = True/有効
ledmon デバッグ レベルの設定 log_level	対応-ログレベル ledmon からのフラグ。	指定できる値は、quiet、error、warning、info、debug、all (0 は「quiet」)、5 は「all」を意味します) です。 デフォルト = 2
1 個の RAID メンバまたはすべての RAID の管理設定 RAID_MEMBERS_ONLY	フラグが ledmon (true) に設定されている場合、RAID メンバであるドライブにのみモニタリングを制限します。	1. False/(すべての RAID メンバと PT) 2. True/(RAID メンバのみ) デフォルト = False
特定のコントローラのみ限定されたスキャン WHITELIST	ledmon では、LED 状態の変更を、ホワイトリストにリストされているコントローラに制限します。	ホワイトリスト コントローラの LED の状態の変更を制限します。 デフォルトでは、制限はありません。

表 4: LED 点滅パターン: ESXi

ステータス LED	動作	オプション
「識別」	定義された検索パターンでそのドライブのステータス LED を点滅させることにより、エンクロージャ内の特定のデバイスを識別する機能。	なし。デフォルトはオフです。
「オフ」	ラック内の特定のデバイスが配置されたら、「識別」 LED をオフにする機能があります。	なし。デフォルトはオフです。

