ストレージ関連ポリシー

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

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー]**を展開します。

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
[名前（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ー定義による説明。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（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。 • [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 テンプレートをサービス プロファイルに含めます。

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 を含むサービス 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

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サーバ]** > **[サービスプロファイル]**を展開します。

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

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サーバ]** > **[サービスプロファイル]**を展開します。

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、**[はい]**をクリックします。

vHBA テンプレートの削除

手順

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー（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、**[はい]**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 要求に応答しない場合、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、次のストラテジー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。

完了キュー = 送信キュー + 受信キュー
割り込み回数 = (完了キュー + 2) 以上である 2 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、

完了キュー = 1 + 8 = 9
割り込み回数 = (9 + 2) 以上の 2 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。

Interrupt Count = (#Tx or Rx Queues) + 2

次に例を示します。

割り込みカウント wq = 32、rq = 32、cq = 64 - 割り込みカウント = 最大(32、 32) + 2 = 34
割り込みカウント wq = 64、rq = 8、cq = 72 – 割り込みカウント = 最大(64, 8) + 2 = 66
割り込みカウント wq = 1、rq = 16、cq = 17 - 割り込みカウント = 最大(1、16) + 2 = 18

Windows アダプタでの割り込みカウント ポリシー

Windows OS の場合、VIC 1400 シリーズ以降のアダプタの UCS Manager で推奨されるアダプタ ポリシーは Win-HPN であり、RDMA が使用されている場合、推奨されるポリシーは

Win-HPN-SMB です。VIC 1400 シリーズ以降のアダプタの場合、推奨される割り込み値の設定は 512 であり、Windows VIC ドライバが必要な数の割り込みを割り当てます。

VIC 1300 および VIC 1200 シリーズ アダプタの場合、推奨される UCS Manager アダプタ ポリシーは Windows であり、割り込みは TX + RX + 2 で、最も近い 2 の累乗に丸められます。サポートされる Windows キューの最大数は、Rx キューの場合は 8、Tx キューの場合は 1 です。

VIC 1200 および VIC 1300 シリーズ アダプタの例:

Tx = 1、Rx = 4、CQ = 5、割り込み = 8 (1 + 4 は最も近い 2 のべき乗に丸められます)、RSS を有効にする

VIC 1400 シリーズ以降のアダプタの例：

Tx = 1、Rx = 4、CQ = 5、割り込み = 512、RSS を有効にする

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ー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 1400 シリーズ 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 FC-NVMe アダプタ ポリシーを提供します。新しい FC-NVMe 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

ステップ 1　[ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2　**[サーバ]** > **[ポリシー]**を展開します。

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
[名前（Name）] フィールド	ポリシーの名前。 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。
[説明（Description）] フィールド	ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（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。

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 技術情報の数。 1 ～ 16 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	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。 • [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。 （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。
[Flogi Retries] フィールド	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。 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 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。 （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。
[Flogi Timeout (ms)] フィールド	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。 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 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。 （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。 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。

名前	説明
[Plogi Retries] フィールド	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。 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。 （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。
[Plogi Timeout (ms)] フィールド	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。 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。 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。 （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。 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。
[Port Down Timeout (ms)] フィールド	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 ドライバ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。 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。 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。 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。 （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。

名前	説明
IO リトライ タイムアウト（秒）	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。 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。
[Port Down IO Retry] フィールド	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。 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。 （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。
[Link Down Timeout (ms)] フィールド	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。 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。 （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。
[IO Throttle Count] フィールド	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。 （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。 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。

名前	説明
[Max LUNs Per Target] フィールド	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、サーバーで実行されている OS により管理されます。 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。 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。 （注） • 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す。
[LUN Queue Depth] フィールド	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。 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。 （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。
[Interrupt Mode] オプション ボタン	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。 • [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。 （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。

名前	説明
[vHBA Type] ラジオ ボタン	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。 • 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 （注） このオプションは、Tech Preview として利用できます。 • 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 • FC NVME ターゲット: FC NVME 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 （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。 vHBA タイプは、UCS VIC 1400 アダプタ でのみサポートされています。

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、**[はい]**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

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー（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、**[はい]**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

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー]**を展開します。

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。

SPDM セキュリティ ポリシー

SPDM セキュリティ

Cisco UCS M6 サーバーには、デバイス自体に対する攻撃のベクトルを提供したり、デバイスを使用してシステム内の別のデバイスを攻撃したりする可能性のある可変コンポーネントが含まれている場合があります。これらの攻撃を防御するために、セキュリティ プロトコルおよびデータ モデル （SPDM）仕様では、デバイスがその ID と変更可能なコンポーネント構成の正確さを証明するように要求する安全なトランスポートの実装が可能になっています。この機能は、Cisco UCS Manager リリース 4.2(1d) 以降の Cisco UCS C220 および C240 M6 サーバーでサポートされています。

（注） SPDM は現在、Cisco UCS C225 M6サーバ および Cisco UCS C245 M6サーバ ではサポートされていません。

SPDMは、さまざまなトランスポートおよび物理メディアを介してデバイス間でメッセージ交換を実行するためのメッセージ、データ オブジェクト、およびシーケンスを定義します。これは、管理コンポーネント トランスポート プロトコル（MCTP）を介したベースボード管理コントローラ（BMC）とエンドポイント デバイス間のメッセージ交換を調整します。メッセージ交換には、BMC にアクセスするハードウェア ID の認証が含まれます。SPDM は、デバイス認証、ファームウェア測定、および証明書管理の管理レベルを指定することにより、低レベルのセキュリティ機能と操作へのアクセスを可能にします。エンドポイントデバイスは、認証を提供するように求められます。 BMC はエンドポイントを認証し、信頼できるエンティティのアクセスのみを許可します。

UCS Manager では、オプションで外部セキュリティ証明書を BMC にアップロードできます。ネイティブの内部証明書を含め、最大 40 の SPDM 証明書が許可されます。制限に達すると、証明書をアップロードできなくなります。ユーザーがアップロードした証明書は削除できますが、内部/デフォルトの証明書は削除できません。

SPDM セキュリティ ポリシーでは、3 つのセキュリティ レベル設定のいずれかを指定できます。セキュリティは、次の 3 つのレベルのいずれかで設定できます。

- フル セキュリティ：

  これは、最高のMCTPセキュリティ設定です。この設定を選択した場合、エンドポイントの認証またはファームウェアの測定が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証またはファームウェア測定がサポートされていない場合にも、障害が生成されます。

- 部分的なセキュリティ (デフォルト):

この設定を選択した場合、エンドポイントの認証またはファームウェアの測定が失敗すると、障害が生成されます。エンドポイントのいずれかでエンドポイント認証またはファームウェア測定がサポートされていない場合には、障害が生成されません。

- No Security

  この設定を選択した場合（エンドポイント測定やファームウェア測定が失敗しても）障害は発生しません。

1 つ以上の外部/デバイス証明書のコンテンツを BMC にアップロードすることもできます。SPDM ポリシーを使用すると、必要に応じてセキュリティ証明書または設定を変更または削除できます。証明書は、不要になったときに削除または置き換えることができます。

証明書は、システムのすべてのユーザー インターフェイスに一覧表示されます。

SPDM セキュリティ ポリシーの作成

この手順では、SPDM ポリシーを作成します。

（注） 最大 40 の SPDM 証明書 (ネイティブ証明書を含む) をアップロードできます。

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[ポリシー（Policies）]** に移動します。[root] ノードを展開します。

ステップ 3 **[SPDM 証明書ポリシー（SPDM Certificate Policies）]** を右クリックして **[SPDM ポリシー（SPDM Policies の作成）]** を選択します。

ステップ 4 このポリシーの名前を入力し、セキュリティ レベルとして **[障害アラート設定（Fault Alert Setting）]** を選択します：これは **[無効（Disabled）]**、**[一部（Partial）]**、または **[完全（Full）]** のいずれかです。

デフォルトは **[一部（Partial）]** です。

ステップ 5 **[追加（Add）]**（**[ポリシーの作成（Create Policy）]** ウィンドウ）をクリックします。**[SPDM 証明書の追加（Add SPDM Certificate)]** ウィンドウが開きます。

ステップ 6 証明書に名前を付けます。

UCS Manager は、**Pem** 証明書のみをサポートします。

ステップ 7 [証明書（Certificate）] フィールドに証明書の内容を貼り付けます。

ステップ 8 **[OK]** をクリックして証明書を追加し、**[SPDM ポリシーの作成（Create SPDM Policy）]** ウィンドウに戻ります。

最大 40 件の証明書を追加できます。

ステップ 9 **[SPDM ポリシーの作成（Create SPDM Policy）]** メニューで、**[OK]** をクリックします。

SPDMポリシーを作成してから、サーバールートポリシーの下で**SPDM証明書ポリシー（SPDM Certificate Policy）]** を選択すると、アラート設定とともにすぐにリストに表示されます。

次のタスク

証明書をサービス プロファイルに割り当てます。サービス プロファイルを有効にするには、サービス プロファイルをサーバーに関連付ける必要があります。

セキュリティ ポリシーとサーバーの関連付け

始める前に

SPDM セキュリティ ポリシーの作成

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サービス プロファイル（Service Profiles）]** に移動します。[root] ノードを展開します。

ステップ 3 作成したポリシーに関連付けるサービス プロファイルを選択します。

a) **[ポリシー（Policies）]** タブで、下にスクロールして **[SPDM 証明書ポリシー（SPDM Certificate Policy）]**を展開します。**[SPDM 証明書ポリシー（SPDM Certificate Policy）]** ドロップダウンで、このサービスプロファイルに関連付ける目的のポリシーを選択します。

ステップ 4 [OK] をクリックします。

SPDM ポリシーがこのサービス プロファイルに関連付けられます。

次のタスク

障害アラート レベルをチェックして、目的の設定に設定されていることを確認します。

障害アラート設定の表示

特定のシャーシに関連付けられている障害アラート設定を表示できます。

始める前に

ポリシーを作成して、それとサービス プロファイルを関連付けることができます。

手順

ステップ 1 **[ナビゲーション（Navigation）]** ペインで **[機器（Equipment）]** をクリックします。

ステップ 2 ラックマウント サーバーを選択します。

ステップ 3 **[インベントリ（Inventory）]** タブで **[CIMC]** を選択します。.

ユーザーがアップロードした証明書が一覧表示され、特定の証明書の情報を選択して表示できます。

SAN 接続ポリシー

LANおよびSAN接続ポリシーの概要

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

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー]**を展開します。

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 テンプレートに含めます。

SAN 接続ポリシー用の vHBA の作成

手順

ステップ 1 [ナビゲーション]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

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー（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、**[はい]**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

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー（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
[名前（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。

名前	説明
[Description] フィールド	グループの説明。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（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 • 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

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー（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、**[はい]**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され、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は中断されます。

手順

ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[ポリシー（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、**[はい]**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。

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]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 **[アドバンスト (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。

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]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 **[アドバンスト (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**[アドバンスト (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 (E1nabled)]**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。

- 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。

手順

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。

手順

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す。

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。

手順

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 Asssign 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。

ステータス LED	動作	オプション
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。 • 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。 1. 無効 (1 台のドライブのみ) 2. 有効 (すべてのドライブ)
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。

ステータス LED	動作	オプション
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
RAIDボリュームが以降中です **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

ステータス LED	動作	オプション
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_MEMBRES_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に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。

翻訳について
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。