ストレージ関連ポリシー

vHBA テンプレートの設定

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 テンプレートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A /org # **create vhba-templ** *vhba-templ-name* [**fabric** {**a** | **b**}] [**fc-if** *vsan-name*]	vHBA テンプレートを作成し、組織 vHBA テンプレート モードを開始します。
ステップ 3	（任意） UCS-A /org/vhba-templ # **set descr** *description*	vHBA テンプレートの説明を指定します。

	コマンドまたはアクション	目的
ステップ 4	（任意） UCS-A /org/vhba-templ # **set fabric** {**a** | **b**}	vHBA に使用するファブリックを指定します。ステップ 2 で vHBA テンプレートを作成したときにファイブリックを指定しなかった場合、このコマンドでファブリックを指定するオプションを使用できます。
ステップ 5	（任意） UCS-A /org/vhba-templ # **set fc-if** *vsan-name*	vHBAテンプレートに使用する（VSANという名前の）ファイバチャネルインターフェイスを指定します。ステップ 2 で vHBA テンプレートを作成したときにファイバチャネルインターフェイスを指定しなかった場合、このコマンドでファイバチャネルインターフェイスを指定するオプションを使用できます。
ステップ 6	UCS-A /org/vhba-templ # **set max-field-size** *size-num*	vHBA がサポートするファイバ チャネル フレーム ペイロードの最大サイズ（バイト数）を指定します。
ステップ 7	UCS-A /org/vhba-templ # **set pin-group** *group-name*	vHBA テンプレートに対し使用するピン グループを指定します。
ステップ 8	UCS-A /org/vhba-templ # **set qos-policy** *mac-pool-name*	vHBAテンプレートに対し使用するQoSポリシーを指定します。
ステップ 9	UCS-A /org/vhba-templ # **set stats-policy** *policy-name*	vHBAテンプレートに対し使用するサーバおよびサーバコンポーネント統計情報しきい値ポリシーを指定します。
ステップ 10	UCS-A /org/vhba-templ # **set type** {**initial-template** | **updating-template**}	vHBA テンプレートのアップデート タイプを指定します。テンプレート更新時にこのテンプレートから作成される vHBA インスタンスが自動アップデートされないようにする場合、**initial-template** キーワードを使用します。その他の場合は **updating-template** キーワードを使用して、vHBA テンプレートの更新時にすべての vNIC インスタンスがアップデートされるようにします。
ステップ 11	UCS-A /org/vhba-templ # **set wwpn-pool** *pool-name*	vHBA テンプレートに対し使用する WWPN プールを指定します。

	コマンドまたはアクション	目的
ステップ 12	UCS-A /org/vhba-templ # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、vHBAテンプレートを設定し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org* # create vhba template VhbaTempFoo
UCS-A /org/vhba-templ* # set descr "This is a vHBA template example."
UCS-A /org/vhba-templ* # set fabric a
UCS-A /org/vhba-templ* # set fc-if accounting
UCS-A /org/vhba-templ* # set max-field-size 2112
UCS-A /org/vhba-templ* # set pin-group FcPinGroup12
UCS-A /org/vhba-templ* # set qos-policy policy34foo
UCS-A /org/vhba-templ* # set stats-policy ServStatsPolicy
UCS-A /org/vhba-templ* # set type updating-template
UCS-A /org/vhba-templ* # set wwpn-pool SanPool7
UCS-A /org/vhba-templ* # commit-buffer
UCS-A /org/vhba-templ #
```

vHBA テンプレートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **delete vhba-templ** *vhba-templ-name*	指定した vHBA テンプレートを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次に、VhbaTempFoo という名前の vHBA テンプレートを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope org /
UCS-A /org # delete vhba template VhbaTempFoo
UCS-A /org* # commit-buffer
UCS-A /org #
```

ファイバ チャネル アダプタ ポリシーの設定

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 ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **create fc-policy** *policy-name*	指定されたファイバチャネルアダプタ ポリシーを作成し、組織ファイバチャネル ポリシー モードを開始します。
ステップ 3	（任意） UCS-A /org/fc-policy # **set descr** *description*	ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 4	（任意） UCS-A /org/fc-policy # **set error-recovery** {**fcp-error-recovery** {**disabled** | **enabled**} | **link-down-timeout** *timeout-msec* | **port-down-io-retry-count** *retry-count* | **port-down-timeout** *timeout-msec*}	ファイバチャネルエラー回復を設定します。
ステップ 5	（任意） UCS-A /org/fc-policy # **set interrupt mode** {**intx** | **msi** | **msi-x**}}	ドライバ割り込みモードを設定します。
ステップ 6	（任意） UCS A/org/fc-policy # **set port** { **io-throttle-count** *throttle count* | **max-luns** *max-num*}	ファイバ チャネル ポートを設定します。 （注） **max-luns**オプションにのみ適用、**fc-initiator** vHBA のタイプ。

	コマンドまたはアクション	目的
ステップ 7	（任意） UCS-A /org/fc-policy # **set port-f-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	ファイバチャネルポートのファブリック ログイン（FLOGI）を設定します。
ステップ 8	（任意） UCS-A /org/fc-policy # **set port-p-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	ファイバチャネルのポートツーポート ログイン（PLOGI）を設定します。
ステップ 9	（任意） UCS A/org/fc-policy # **set recv-queue** { **count** *count*| **ring-size** *size-num*\\	ファイバチャネルの受信キューを設定します。
ステップ 10	（任意） UCS-A /org/fc-policy # **set scsi-io** {**count** *count* | **ring-size** *size-num*}	ファイバ チャネル I/O を設定します。
ステップ 11	（任意） UCS-A /org/fc-policy # **set trans-queue ring-size** *size-num*}	ファイバチャネルの送信キューを設定します。
ステップ 12	（任意） UCS-A /org/fc-policy # **set vhbatype mode** {**fc-initiator** | **fc-nvme-initiator** | **fc-nvme-target** | **fc-target**}	このポリシーで使用される vHBA タイプ。FC と FC-NVMe をサポートする vHBAs は、同じアダプタで作成できるようになりました。 （注） **fc-nvme-target** および **fc-target** は、技術プレビューオプションとして使用できます。
ステップ 13	UCS-A /org/fc-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、ファイバチャネルアダプタ ポリシーを設定し、トランザクションをコミットます。

```
UCS-A# scope org /
UCS-A /org* # create fc-policy FcPolicy42
UCS-A /org/fc-policy* # set descr "This is a Fibre Channel adapter policy example."
UCS-A /org/fc-policy* # set error-recovery error-detect-timeout 2500
UCS-A /org/fc-policy* # set port max-luns 4
UCS-A /org/fc-policy* # set port-f-logi retries 250
UCS-A /org/fc-policy* # set port-p-logi timeout 5000
UCS-A /org/fc-policy* # set recv-queue count 1
UCS-A /org/fc-policy* # set scsi-io ring-size 256
UCS-A /org/fc-policy* # set trans-queue ring-size 256
UCS-A /org/fc-policy* # commit-buffer
UCS-A /org/fc-policy #
```

次の例は、FC NVME イニシエータに vHBA タイプセットをファイバ チャネル アダプタ ポリシーを設定し、トランザクションをコミットます。

```
UCS-A# scope org /
UCS-A /org* # create fc-policy FcPolicy42
UCS-A /org/fc-policy* # set descr "This is a Fibre Channel adapter policy example."
UCS-A /org/fc-policy* # set error-recovery error-detect-timeout 2500
UCS-A /org/fc-policy* # set port-f-logi retries 250
UCS-A /org/fc-policy* # set port-p-logi timeout 5000
UCS-A /org/fc-policy* # set recv-queue count 1
UCS-A /org/fc-policy* # set scsi-io ring-size 256
UCS-A /org/fc-policy* # set trans-queue ring-size 256
UCS-A /org/fc-policy* # set vhbatype mode fc-nvme-initiator
UCS-A /org/fc-policy* # commit-buffer
UCS-A /org/fc-policy #
```

ファイバ チャネル アダプタ ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **delete fc-policy** *policy-name*	指定されたファイバ チャネル アダプタ ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、FcPolicy42 という名前のファイバチャネルアダプタ ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete fc-policy FcPolicy42
UCS-A /org* # commit-buffer
UCS-A /org #
```

デフォルトの vHBA 動作ポリシーの設定

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org /**	ルート組織モードを開始します。
ステップ 2	UCS-A/org # **scope vhba-beh-policy**	デフォルトの vHBA 動作ポリシー モードを開始します。
ステップ 3	UCS-A/org/vhba-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	デフォルトの vHBA 動作ポリシーを指定します。次のいずれかになります。 • **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。

	コマンドまたはアクション	目的
		hw-inherit を指定する場合、vHBA テンプレートを指定して、vHBA を作成することもできます。 • **none**—Cisco UCS Manager はサービス プロファイルにデフォルトの vHBAs 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。
ステップ 4	UCS-A/org/vhba-beh-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、デフォルトの vNIC 動作ポリシーを **hw-inherit** に設定する方法を示します。

```
UCS-A # scope org /
UCS-A/org # scope vhba-beh-policy
UCS-A/org/vhba-beh-policy # set action hw-inherit
UCS-A/org/vhba-beh-policy* # commit-buffer
UCS-A/org/vhba-beh-policy #
```

SAN 接続ポリシーの設定

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **create san-connectivity-policy** *policy-name*	指定された SAN 接続ポリシーを作成を作成し、組織ネットワーク制御ポリシーモードを開始します。 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。
ステップ 3	（任意） UCS-A /org/lan-connectivity-policy # **set descr** ポリシー名	ポリシーに説明を追加します。どこでどのようにポリシーが使用されるかについての情報を含めることを推奨します。 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 4	UCS-A /org/service-profile # **set identity** {**dynamic-uuid** {*uuid* | **derived**} | **dynamic-wwnn** {*wwnn* | **derived**} | **uuid-pool** *pool-name* | **wwnn-pool** *pool-name*}	サーバーが UUID または WWNN を取得する方法を指定します。次のいずれかを実行できます。 • 一意の UUID を *nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn* 形式で作成します。 • 製造時にハードウェアに焼き付けられた UUID を取得する。 • UUID プールを使用する。

	コマンドまたはアクション	目的
		• 一意の WWNN を *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* の形式で作成します。 • 製造時にハードウェアに焼き付けられた WWNN を取得する。 • WWNN プールを使用する。
ステップ 5	UCS-A /org/lan-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、SanConnect242 という名前の SAN 接続ポリシーを作成し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # create san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy* # set descr "SAN connectivity policy"
UCS-A /org/san-connectivity-policy* # set identity wwnn-pool SanPool7
UCS-A /org/san-connectivity-policy* # commit-buffer
UCS-A /org/san-connectivity-policy #
```

次のタスク

この SAN 接続ポリシーに 1 つ以上の vHBA および（または）イニシエータ グループを追加します。

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **delete san-connectivity-policy** *policy-name*	指定された SAN 接続ポリシーを削除します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例では、SanConnect52 という名前の SAN 接続ポリシーをルート組織から削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # delete san-connectivity-policy SanConnect52
UCS-A /org* # commit-buffer
UCS-A /org #
```

SAN 接続ポリシー用の vHBA の作成

SAN 接続ポリシーの作成 （14 ページ） から続行した場合、ステップ 3 でこの手順を開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/san-connectivity-policy # **create vhba** *vhba-name* [**fabric** {**a** | **b**}] [**fc-if** *fc-if-name*]	指定した SAN 接続ポリシー用の vHBA を作成し、vHBA モードを開始します。 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。
ステップ 4	UCS-A /org/lan-connectivity-policy # **set adapter-policy** ポリシー名	vHBA に対し使用するアダプタ ポリシーを指定します。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /org/san-connectivity-policy/vhba # **set identity** {**dynamic-wwpn** {*wwpn* | **derived**} | **wwpn-pool** *wwn-pool-name*}	vHBA の WWPN を指定します。 次のいずれかのオプションを使用してストレージ ID を設定できます。 • 一意の WWPN を *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh* 形式で作成します。 WWPN 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。 WWPN に Cisco MDS ファイバ チャネル スイッチと互換性を持たせる場合は、WWPN テンプレート **20:00:00:25:B5:XX:XX:XX** を使用します。 • 製造時にハードウェアに焼き付けられた WWPN から WWPN 取得する。 • WWN プールから WWPN を割り当てる。
ステップ 6	UCS-A /org/san-connectivity-policy/vhba # **set max-field-size** *size-num*	vHBA がサポートするファイバ チャネル フレーム ペイロードの最大サイズ（バイト数）を指定します。 256 ～ 2112 の範囲の整数を入力します。デフォルトは 2048 です。
ステップ 7	UCS-A /org/san-connectivity-policy/vhba # **set order** {*order-num* | **unspecified**}	vHBA の PCI スキャン順序を指定します。
ステップ 8	UCS-A /org/san-connectivity-policy/vhba # **set pers-bind** {**disabled** | **enabled**}	ファイバチャネルターゲットに対する永続的なバインディングをディセーブルまたはイネーブルにします。
ステップ 9	UCS-A /org/san-connectivity-policy/vhba # **set pin-group** *group-name*	vHBA に使用する SAN ピン グループを指定します。
ステップ 10	UCS-A /org/san-connectivity-policy/vhba # **set qos-policy** *policy-name*	vHBA に対し使用する QoS ポリシーを指定します。

	コマンドまたはアクション	目的
ステップ 11	UCS-A /org/san-connectivity-policy/vhba # **set stats-policy** *policy-name*	vHBA に使用する統計情報しきい値ポリシーを指定します。
ステップ 12	UCS-A /org/san-connectivity-policy/vhba # **set template-name** *policy-name*	vHBA に使用する vHBA テンプレートを指定します。vHBA に vHBA テンプレートを使用する場合は、手順4、7、および 8 などの vHBA テンプレートに含まれていないすべての設定を完了する必要があります。
ステップ 13	UCS-A /org/san-connectivity-policy/vhba # **set vcon** {**1** | **2** | **3** | **4** | **any**}	vHBA を 1 つまたはすべての仮想ネットワーク インターフェイス接続に割り当てます。
ステップ 14	UCS-A /org/san-connectivity-policy/vhba # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、SanConnect242 という名前の SAN 接続ポリシー用の vHBA を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy* # create vhba vhba3 fabric a
UCS-A /org/san-connectivity-policy/vhba* # set adapter-policy AdaptPol2
UCS-A /org/san-connectivity-policy/vhba* # set identity wwpn-pool SanPool7
UCS-A /org/san-connectivity-policy/vhba* # set max-field-size 2112
UCS-A /org/san-connectivity-policy/vhba* # set order 0
UCS-A /org/san-connectivity-policy/vhba* # set pers-bind enabled
UCS-A /org/san-connectivity-policy/vhba* # set pin-group FcPinGroup12
UCS-A /org/san-connectivity-policy/vhba* # set qos-policy QosPol5
UCS-A /org/san-connectivity-policy/vhba* # set stats-policy StatsPol2
UCS-A /org/san-connectivity-policy/vhba* # set template-name SanConnPol3
UCS-A /org/san-connectivity-policy/vhba* # set vcon any
UCS-A /org/san-connectivity-policy/vhba* # commit-buffer
UCS-A /org/san-connectivity-policy/vhba #
```

次のタスク

必要に応じて、SAN 接続ポリシーに別の vHBA またはイニシエータ グループを追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

SAN 接続ポリシーからの vHBA の削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/san-connectivity-policy # **delete vHBA** *vhba-name*	SAN 接続ポリシーから指定された vHBA を削除します。
ステップ 4	UCS-A /org/san-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、vHBA3 という名前の vHBA を SanConnect242 という名前の SAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy # delete vHBA vHBA3
UCS-A /org/san-connectivity-policy* # commit-buffer
UCS-A /org/san-connectivity-policy #
```

SAN 接続ポリシー用のイニシエータ グループの作成

SAN 接続ポリシーの作成 （14 ページ） から続行した場合、ステップ 3 でこの手順を開始します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として / を入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシー モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/san-connectivity-policy # **create initiator-group** *group-name* **fc**	ファイバ チャネル ゾーン分割の指定イニシエータ グループを作成し、イニシエータ グループ モードを開始します。 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。
ステップ 4	UCS-A /org/san-connectivity-policy/initiator-group # **create initiator** *vhba-name*	イニシエータ グループの指定 vHBA イニシエータを作成します。 必要に応じて、この手順を繰り返しグループに 2 番めの vHBA を追加します。
ステップ 5	UCS-A /org/san-connectivity-policy/initiator-group # **set storage-connection-policy** *policy-name*	SAN 接続ポリシーに指定したストレージ接続ポリシーを関連付けます。 （注） この手順は、SAN 接続ポリシーに関連付ける既存のストレージ接続ポリシーを関連付けると仮定しています。行うには、ステップ 10 に進みます。代わりに、このポリシーのローカル ストレージ定義を作成する場合は、ステップ 6 に進みます。
ステップ 6	UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def # **create storage-target** *wwpn*	指定された WWPN を持つストレージ ターゲット エンドポイントを作成し、ストレージ ターゲット モードを開始します。
ステップ 7	UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target # **set target-path** {**a** | **b**}	ターゲット エンドポイントとの通信に使用するファブリック インターコネクトを指定します。
ステップ 8	UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target # **set target-vsan** *vsan*	ターゲット エンドポイントとの通信に使用する VSAN を指定します。

	コマンドまたはアクション	目的
ステップ 9	UCS-A /org/san-connectivity-policy/initiator-group # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、SanConnect242 という名前の SAN 接続ポリシーに対し 2 つのイニシエータを持つ initGroupZone1 という名前のイニシエータ グループを設定し、scPolicyZone1 という名前のローカル ストレージ接続ポリシー定義を設定し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org* # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy # create initiator-group initGroupZone1 fc
UCS-A /org/san-connectivity-policy/initiator-group* # set zoning-type sist
UCS-A /org/san-connectivity-policy/initiator-group* # create initiator vhba1
UCS-A /org/san-connectivity-policy/initiator-group* # create initiator vhba2
UCS-A /org/san-connectivity-policy/initiator-group* # create storage-connection-def
scPolicyZone1
UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def* # create
storage-target
20:10:20:30:40:50:60:70
UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target*
 # set
target-path a
UCS-A /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target*
 # set
target-vsan default
UCS-A /org/san-connectivity-policy/initiator-group* # commit-buffer
UCS-A /org/san-connectivity-policy/initiator-group #
```

次のタスク

必要に応じて、SAN 接続ポリシーに他のイニシエータ グループまたは vHBA を追加します。そうでない場合は、サービス プロファイルまたはサービス プロファイル テンプレートにポリシーをインクルードします。

SPDM セキュリティ ポリシーの作成

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 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 認証

セキュリティ プロトコルおよびデータ モデル（SPDM）は、ストレージ コントローラでの認証のためにBMCによって使用されます。これには、ストレージコントローラ ファームウェアがセキュア ブートされていることと、Slot0 に Broadcom 証明書チェーンがインストールされ

ていることが必要です。ファームウェアの更新中、Broadcom ファームウェアは、OCR またはホストが再起動するまで、ストレージファームウェアの古い測定値を保持します。デバイス認証が失敗した場合、ファームウェアはインベントリ関連のコマンドのみを許可します。設定操作は実行できません。

SPDM セキュリティ ポリシーの作成

セキュリティプロトコルおよびデータモデル（SPDM）ポリシーを作成して、認証のためにセキュリティ アラート レベルと証明書の内容を BMC に提示できます。

- UCS-A# **scope org**

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に **/** を入力します。
ステップ 2	UCS-A /org # **create spdm-certificate-policy** *policy-name*	新しい SPDM セキュリティ証明書ポリシーを指定されたポリシー名で作成し、組織 SPDM 証明書ポリシー モードを開始します。
ステップ 3	UCS-A /org/spdm-certificate-policy* # **set fault-alert** {**full** | **partial** | **no**}	このポリシーの障害アラート レベルを構成します。
ステップ 4	（任意） UCS-A /org/spdm-certificate-policy* # **set descr** *description*	SPDMセキュリティ証明書ポリシーの説明を記します。 （注） 説明にスペース、特殊文字、または句読点が含まれている場合、説明を引用符で括る必要があります。引用符は、**show** コマンド出力の説明フィールドには表示されません。
ステップ 5	UCS-A /org/spdm-certificate-policy # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、「部分的なセキュリティ」アラート レベル（エンドポイント認証またはファームウェア測定エラーが検出されたときに生成されるエラー）を使用して、「test」

というポリシーを作成する方法を示しています。デフォルトのポリシー所有者はローカルです。

```
UCS-A-FI-A /org #create spdm-certificate-policy test
UCS-A-FI-A /org /spdm-certificate-policy* # set?
fault-alert - Configure fault alert setting
desc - Description of policy
policy-owner  - Change ownership of policies
UCS-A-FI-A /org /spdm-certificate-policy* # set fault-alert partial
UCS-A-FI-A /org/spdm-certificate-policy* #commit-buffer
UCS-A-FI-A /org/spdm-certificate-policy# show details

SPDM Certificate Profile:
Name: test
Fault Alert Setting: partial
Description:
Policy Owner: Local
```

次のタスク

必要に応じて、外部のセキュリティ証明書を割り当てます。

外部 SPDM セキュリティ証明書ポリシーのロード

SPDM を使用すると、外部のセキュリティ証明書をダウンロードできます。

始める前に

SPDM セキュリティ証明書ポリシーを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /org # **scope spdm-certificate-policy**	SPDMセキュリティ証明書ポリシーモードを開始します。
ステップ 2	UCS-A org/spdm-certificate-policy# **create spdm-cert** *Certificate name*	指定された外部証明書の SPDM セキュリティ証明書ポリシーを作成します。
ステップ 3	UCS-A /org/spdm-certificate-policy* # **set** {*certificate* }	証明書を指定すると、外部証明書の内容を求めるプロンプトが表示されます。サポートされている証明書の種類は pem のみです。
ステップ 4	UCS-A /org/spdm-certificate-policy # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

次の例は、PEM タイプの Broadcom の証明書をロードする方法を示しています。

例

```
UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert?
Name - Certificate name

UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert Broadcom
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set?
certificate - Certificate content

UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set certificate
{enter certificate content}
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # commit-buffer
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert# show detail
SPDM Certificate:
Name: Broadcom
Certificate Type: pem
Certificate Content:
```

セキュリティ ポリシー違反警告レベルの表示

ポリシーを作成したら、SPDM ポリシーのアラート レベルを確認できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /org/spdm-certificate-policy # **show fault-alert** 例： `UCS-A /server/cimc/spdm-certificate #show fault-alert`	返された結果は、この SPDM ポリシーの設定がデフォルトである [部分（Partial）] であることを示しています。 `SPDM Fault Alert Setting: Partial`

証明書インベントリの表示

アップロードされたSPDM証明書を表示し、指定された証明書の詳細を要求することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server*	
ステップ 2	UCS-A/server # **scope cimc** *server*	
ステップ 3	UCS-A/server/cimc # **scope spdm** *server*	
ステップ 4	UCS-A/server/cimc/spdm # **show certificate**	返される結果は、証明書のインベントリを示しています。

	コマンドまたはアクション	目的

ステップ 5	UCS-A/server/cimc/spdm # **show certificate** *certificate-id***detail**
	例：
	`UCS-A /server/cimc/spdm-certificate #show certificate 3 detail`
	`Certificate Information`
	`Certificate Id : 3`
	`Subject Country Code (C) : US`
	`Subject State (ST) : Colorado`
	`Subject Organization (O) : Broadcom Inc.`
	`Subject Organization Unit(OU) : NA`
	`Subject Common Name (CN) : NA`
	`Issuer Country Code (C) : US`
	`Issuer State (ST) : Colorado`
	`Issuer City (L) : Colorado Springs`
	`Issuer Organization (O) : Broadcom Inc.`
	`Issuer Organization Unit(OU) : NA`
	`Issuer Common Name (CN) : NA`
	`Valid From : Oct 23 00:25:13 2019 GMT`
	`Valid To : Apr 8 10:36:14 2021 GMT`
	`UserUploaded : Yes`
	`Certificate Content : <Certificate String>`
	`Certificate Type : PEM`
		返される結果は、証明書 ID、識別子、および有効期限を示しています。

ステップ 6	UCS-A /org/spdm-certificate-policy/certificate # **show**
	例：
	`SPDM Certificate:`
	`Name SPDM Certificate Type`
	`----------`
	`----------`
	`cert1 Pem`
	例：
	`UCS-A /server/cimc/spdm-certificate/certificate #up`
	`UCS-A /server/cimc/spdm-certificate #show`
	`SPDM Certificate Policy:`
	`Name Fault Alert Setting`
	`----------`
	`----------`
	`Broadcom Full`
		返される結果は、証明書の詳細の種類を示しています。
		返される結果は、障害アラートの設定を示しています。

SPDM ポリシーの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、org-name に / と入力します。
ステップ 2	UCS-A /org # **delete spdm-certificate-policy** *policy-name*	指定された SPDM 制御ポリシーを削除します。
ステップ 3	UCS-A /org # **commit-buffer**	トランザクションをシステムの設定に対して確定します。

例

次の例は、VendorPolicy2 という名前の電力制御ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete spdm-certificate-policy VendorPolicy2
UCS-A /org* # commit-buffer
UCS-A /org #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、*org-name* として **/** を入力します。
ステップ 2	UCS-A /org # **scope san-connectivity-policy** *policy-name*	指定した SAN 接続ポリシーの SAN 接続ポリシー モードを開始します。
ステップ 3	UCS-A /org/san-connectivity-policy # **delete initiator-group** *group-name*	SAN 接続ポリシーから指定されたイニシエータ グループを削除します。
ステップ 4	UCS-A /org/san-connectivity-policy # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例では、initGroup3 という名前のイニシエータ グループを SanConnect242 という名前の SAN 接続ポリシーから削除し、トランザクションをコミットする方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope san-connectivity-policy SanConnect242
UCS-A /org/san-connectivity-policy # delete initiator-group initGroup3
UCS-A /org/san-connectivity-policy* # commit-buffer
UCS-A /org/san-connectivity-policy #
```

Aero コントローラー ストレージ プロファイルの構成

ストレージ コントローラの自動構成モード

Cisco UCS C220M6/C240M6 C シリーズ M6 サーバーは、ダイレクト アタッチド ストレージ用の PCIe SAS316 ポート ストレージ コントローラをサポートします。コントローラは、新しく挿入されたディスクの状態を自動的に Unconfigured-Good の状態に移行する自動構成モードをサポートしています。

このため、ストレージプロファイルを作成してサーバーに関連付けることで、自動構成を使用するかどうかを選択できます。デフォルトでは、自動構成機能は無効になっており、サーバーの再起動時にドライブの状態が保持されます。

自動構成を使用する場合は、次のいずれかからドライブの状態を選択する必要があります。

- Unconfigured-Good
- JBOD
- RAID0（RAID0 ライトバック）

これは、コントローラ ファームウェアが systemPD の動作を EPD-PT に変更するためです。EPD-PT は、内部的にはドライブ DDF メタデータのない RAID0 ボリュームです。コントローラには、RAID0 ボリュームとして識別するためのメタデータが格納されます。EPD-PT ドライブは JBOD ドライブと見なされるため、ドライブのステータスは JBOD およびオンラインとして報告されます。

コントローラは次のモデルをサポートします。

- UCSC-RAID-M6T
- UCSC-RAID-M6HD
- UCSC-RAID-M6SD
- UCSX-X10C-RAIDF

以下の表は、さまざまなシナリオでの自動構成の動作を示しています。

自動構成モード	再起動/OCR	ホットプラグ	ユーザアクション
Unconfigured-Good（オフ）	• すべてのUnconfigured-Goodドライブは、Unconfigured-Goodのままです。 • 以前に構成されたすべてのJBODはJBODのままです。	• 挿入されたドライブはUnconfigured-Goodのままです。 • 別のサーバーからのJBODは、このコントローラでUnconfigured-Goodのままです。	自動構成を無効にしても、既存の構成には影響しません すべてのJBODデバイスは、コントローラの起動後もJBODのままです。 Unconfigured-Goodは、コントローラーの起動後もunconfiguredgoodのままです。
JBOD	• すべてのUnconfigured-GoodはJBODに変換されます。	新しく挿入された未構成のデバイスは、JBODに変換されます。	コントローラー上のすべてのUnconfigured-Goodのドライブ（ユーザーが作成したものではない）は、JBODに変換されます。 ユーザーが作成したUnconfigured-Goodドライブは、次回の再起動までUnconfigured-Goodのままです。再起動中に、Unconfigured-GoodはJBODに変換されます。

自動構成モード	再起動/OCR	ホットプラグ	ユーザアクション
RAID0（RAID0 ライトバック）	• すべての Unconfigured-Good は、RAID0 書き戻しに変換されます。	新しく挿入された未構成のデバイスは、RAID0 書き戻しに変換されます。	コントローラー上のすべての Unconfigured-Good のドライブ（ユーザーが作成したものではない）は、RAID0 書き戻しに変換されます。 ユーザーが作成した Unconfigured-Good は、コントローラの再起動後も Unconfigured-Good のままです。 すべての RAID0 書き戻しデバイスは、コントローラの再起動後も RAID0 書き戻しとして残ります。

EPD-PT（JBOD）をデフォルト構成として選択すると、ホストの再起動後、Unconfigured-Good の状態は保持されません。ドライブの状態は、自動構成機能を無効にすることで保持できます。自動構成オプションが使用されている場合、デフォルトの自動構成は常にドライブを Unconfigured-Good としてマークします。

自動構成を選択すると、ドライブは目的のドライブ状態に構成されます。JBOD および構成されていないドライブは、次のコントローラ ブートまたは OCR でそれに応じてドライブの状態が設定されます。

次の表は、さまざまな自動構成シナリオのサンプル ユース ケースを示しています。

ユースケースのシナリオ	自動構成オプション
サーバーを JBOD のみに使用する (例: ハイパーコンバージド、Hadoop データノードなど)	JBOD
サーバーを RAID ボリュームに使用する (例: SAP HANA データベース)	未構成良好
JBOD と RAID ボリュームが混在するサーバーの使用	未構成良好
ドライブの RAID0 書き戻しごとにサーバーを使用する（例：Hadoop データ ノード）	RAID0 ライトバック

自動構成プロファイルの作成

ストレージプロファイルにストレージの自動構成(自動構成)モードオプションを含めること、そして不要になったら構成を解除することができます。変更は、次回のシステムブート時に有効になります。ストレージの自動構成は、Aero コントローラーを備えた Cisco UCS M6 サーバーでのみ使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope org** *org-name*	指定した組織の組織モードを開始します。ルート組織モードを開始するには、[org-name] に / を入力します。
ステップ 2	UCS-A/org# **scope storage-profile** *profile-name*	指定されたプロファイルのストレージプロファイルに入ります。
ステップ 3	UCS-A/org/storage-profile# **show detail expand**	ストレージ プロファイルの詳細ビューを表示します。このストレージプロファイルに対して自動構成モードが有効になっていない場合、または Aero コントローラーが存在しない場合、自動構成モードのエントリは表示されません。自動構成が構成されていない場合、挿入されたデバイスはシステムの再起動時にその状態を保持します。
ステップ 4	UCS-A/org/storage-profile# **set auto-config-mode** jbod | raid-0 | unconfigured-good | unspecified	自動構成モードを有効にし、ディスク構成モードを目的の状態に設定します。追加のパラメータが指定されていない場合、挿入されたすべてのデバイスは、再起動時に未構成良好としてタグ付けされます。自動構成モードを無効にする場合は、unconfigured と入力します。
ステップ 5	UCS-A/org/storage-profile# **commit-buffer**	トランザクションをシステムの設定にコミットします。

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。