Cisco UCS Manager ストレージ管理ガイド（CLI 用）、リリース 4.2

初版：2021 年 6 月 25 日

最終更新：2023 年 1 月 6 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザーインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

目 次

はじめに

対象読者

このガイドは、次の 1 つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのような GUI 要素は、**[GUI 要素]** のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、`courier` フォントで示しています。

テキストのタイプ	説明
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、**this font**で示しています。 CLI コマンド内の変数は、このフォント で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

ワンポイント アドバイス 「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

Cisco UCS の関連資料

ドキュメント ロードマップ

すべての B シリーズ マニュアルの完全なリストについては、次の URL で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

すべての C-Series マニュアルの完全なリストについては、次の URL で入手可能な『『*Cisco UCS C-Series Servers Documentation Roadmap*』』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html

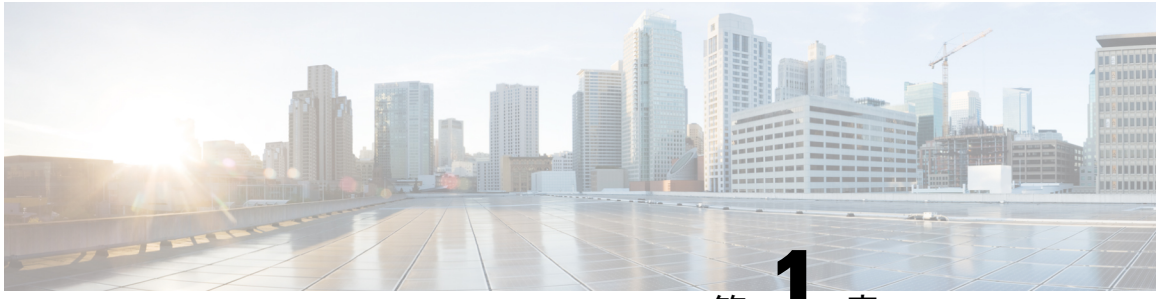
管理用の UCS Manager に統合されたラック サーバでサポートされるファームウェアと UCS Manager のバージョンについては、『Release Bundle Contents for Cisco UCS Software』[英語] を参照してください。

その他のマニュアル リソース

ドキュメントの更新通知を受け取るには、Cisco UCS Docs on Twitter をフォローしてください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載漏れに関する報告は、ucs-docfeedback@external.cisco.com に送信してください。ご協力をよろしくお願いいたします。



第 1 章

新機能と更新情報

新機能と更新情報

ここでは、Cisco UCS Manager、リリース 4.2 の新機能および変更された動作について説明します。

表 *1 : Cisco UCS Manager*、リリース *4.2(1i)* の新機能と変更された動作

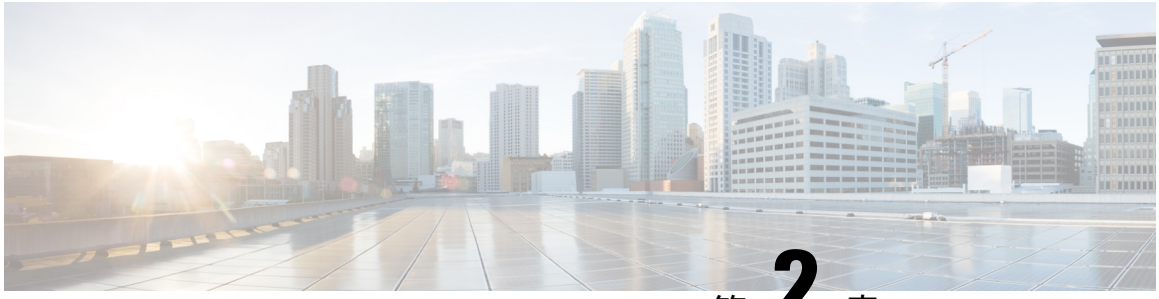
特長	説明	参照先
Cisco UCS M6 サーバー	Cisco UCS C245 M6サーバを次とともにサポートするようになりました： • UCS-M2-HWRAID • UCS C245 M6SX	Cisco ブート最適化 M.2 RAID コントローラ （142 ページ）

表 *2 : Cisco UCS Manager*、リリース *4.2(1f)* の新機能と変更された動作

特長	説明	参照先
ローカル ストレージの RAID レベルを無効にする	PCH SATA コントローラー（AHCI モード）をサポートするために、**ローカル ストレージ** RAID レベルの無効化を追加しました。	RAID レベル （145 ページ） および ストレージプロファイル PCH コントローラ定義の作成 （180 ページ）

表 *3 : Cisco UCS Manager*、リリース *4.2(1d)* の新機能と変更された動作

特長	説明	参照先
Cisco UCS M6 サーバー	Cisco UCS Manager は、Cisco UCS C220 M6 および UCS C240 M6 C シリーズ サーバーをサポートするようになりました。	Cisco ブート最適化 M.2 RAID コントローラ （142 ページ）
Cisco UCS M6 コントローラ	Cisco UCS Manager は、Cisco UCSC-C220-M6、UCSC-C240-M6、および UCSB-MRAID12G-M6 コントローラをサポートするようになりました。	コントローラの制限と制約事項 （152 ページ）
Aero コントローラの自動構成モード	Cisco UCS Manager は、Aero ストレージ コントローラを備えた M6 サーバー上のストレージ デバイスに自動構成オプションを使用するかどうかを選択できるようになりました。	ストレージ コントローラの自動構成モード （136 ページ）
セキュリティ プロトコルとデータ モデル（SPDM）	SPDM をストレージ コントローラでの認証に使用できるようになりました。ネイティブに使用することも、外部のセキュリティ証明書をアップロードして使用することもできます。	SPDM 認証 （130 ページ）



第 2 章

概要

概要

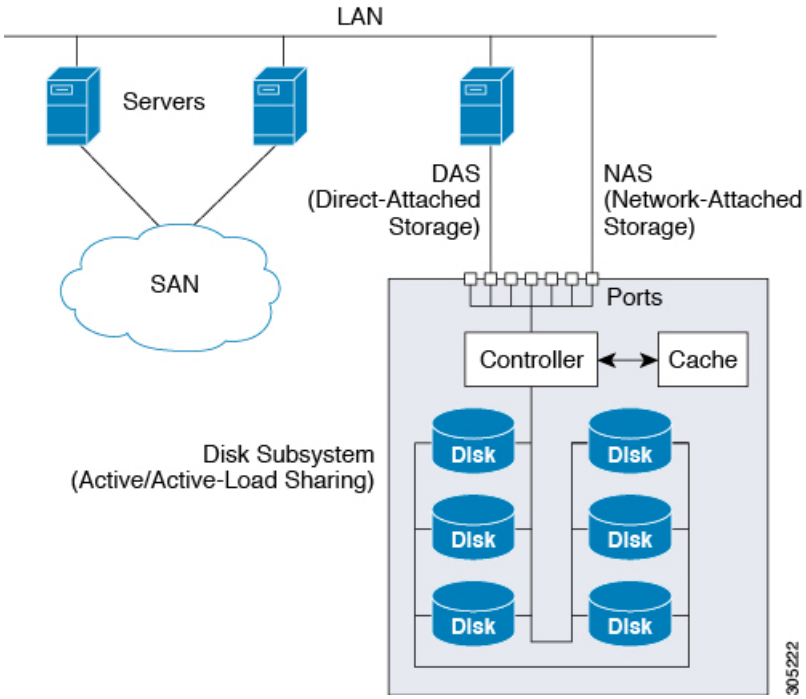
このガイドでは、次のようなストレージ管理タスクを設定する方法について説明します。

- ポートおよびポート チャネル
- ネームド VSAN
- SAN ピン グループ
- SAN アップリンク
- Pools
- FC ID の割り当て
- ストレージ関連ポリシー
- ストレージ プロファイル
- FlexFlash SD カードのサポート
- ダイレクト アタッチド ストレージ
- ストレージ インベントリ

ストレージ オプション

UCS Manager のストレージ オプションとそれぞれのオプションの利点について説明します。

図 *1 : Cisco UCS Manager* のストレージ オプション



- **ダイレクト アタッチド ストレージ（DAS）**：これはサーバ内で使用可能なストレージであり、並行 SCSI 実装内のマザーボード経由でシステムに直接接続されます。DAS は一般に、キャプティブ ストレージと呼ばれています。キャプティブ ストレージ トポロジ内のデバイスは、ストレージ ネットワークへのダイレクト アクセスが提供されておらず、ストレージの効率的な共有をサポートしていません。DAS のデータにアクセスするには、フロントエンド ネットワークを経由する必要があります。DAS デバイスは、他のサーバに対するモビリティがほとんどなく、拡張性も高くはありません。

  DAS デバイスではファイル共有に制限があり、実装と管理が複雑になることがあります。たとえば、DAS デバイスでデータのバックアップをサポートするには、ホスト上のリソースと、他のシステムが使用できないスペア ディスク システムが必要です。このストレージのコストとパフォーマンスは、サーバ内のディスクと RAID コントローラ カードによって決まります。DAS は安価で簡単に設定できますが、ハイエンド ストレージが備える拡張性、パフォーマンス、および高度な機能はありません。

- **ネットワーク アタッチド ストレージ（NAS）**：このストレージは通常、ファイル システムへのアクセスを提供するアプライアンスです。このストレージは、サーバで利用できるネットワーク ファイル システム（NFS）や Common Internet File System（CIFS）共有と同じくらいシンプルです。標準的な NAS デバイスは、コスト効率が高く、パフォーマンスはそれほど高くありませんが、容量は非常に大きく、信頼性を確保するための冗長性を備

えています。NASは通常、手頃な価格で簡単に設定することができ、一部の高度な機能も備えていますが、SAN が備える拡張性、パフォーマンス、および高度な機能はありません。

- **ストレージ エリア ネットワーク（SAN）**：SAN は、サーバとストレージ デバイスを接続することに特化した高速ネットワークです。SAN では、スイッチやディレクタなどの相互接続要素を使用したネットワーク全体のエニーツーエニー接続が可能になります。従来型のサーバとストレージの間の専用接続を排除し、サーバが事実上、ストレージデバイスを所有して管理するという概念もなくなります。また、サーバがアクセスできるデータ量の制約も解消されます。現在は、個々のサーバに接続されたストレージデバイスの数によってデータ量が制限されています。SAN を使用すると柔軟なネットワーク構築が可能となり、1 台のサーバまたは複数の異種サーバ間で共通のストレージユーティリティを共有できるようになります。ネットワークには、ディスク、テープ、光学式ストレージといった多数のストレージ デバイスを接続できます。さらに、ストレージ ユーティリティは、使用するサーバから離れた場所に配置することができます。このタイプのストレージは、最高レベルの信頼性、拡張性、パフォーマンスを提供します。SAN のコストは、その他のストレージ オプションと比較して非常に高くなります。

  SAN は、最も復元力が高く、スケーラブルでパフォーマンスの高いストレージですが、最も高価であり、管理も複雑です。

ストレージ設計の考慮事項

UCS ストレージの物理接続における設計上の考慮事項は、LAN の物理接続と比較するとわずかに異なります。SAN 接続に関する設計上の考慮事項を次に示します。

- ノースバウンドストレージの物理接続では、LAN 接続などの仮想ポート チャネル（vPC）がサポートされません。
- ポート チャネルまたはトランキングを利用して、複数のストレージ アップリンク ポートを結合して物理リンクの冗長性を確保することができます。
- ストレージ リソースの冗長性はストレージ自体で管理され、その方法はベンダーによって異なります。
- Nexus または MDS ファブリック スイッチのようなノースバウンドのシスコ ストレージ デバイスを介してストレージに接続します。
- ストレージを UCS ファブリック インターコネクトに直接接続することができます。この方法は、ファブリック インターコネクトの物理ポートを消費し、処理要件が増大するため、小規模な実装に推奨されます。
- ストレージ リソースへのアクセスを提供するには、VSAN やゾーン分割などのソフトウェア設定が必要です。

ストレージ設定の順序

ストレージ ネットワークを設定するには、次の推奨される順序に従ってください。

1. サーバ ポート、アップリンク ポート、および FC ポートを設定して有効化します。
2. 管理 IP アドレス プールを作成します（通常は、UCS Manager の管理者 IP アドレスと同じサブネット上に作成します）。
3. UUID プール、MAC プール、WWNN プール、WWPN プールを作成します（または対応する「デフォルト」プールを入力します）。ドメイン ID を埋め込みます。MAC および WWPN にはファブリック固有のプールを使用します（たとえば、Fabric-A、Fabric-B）。
4. SAN ブート用に、各ストレージ アレイのブート ターゲットに一意の「ブート ポリシー」を作成します。
5. VNIC テンプレート（たとえば、eth0-A、eth1-B）を作成します。これらはいずれも上記の MAC プールから取得され、それぞれ Fabric-A と Fabric-B に関連付けられます。
6. VHBA テンプレート（たとえば、fc0-A、fc1-B）を作成します。これらはいずれも上記の WWPN プールから取得され、それぞれ Fabric-A と Fabric-B に関連付けられます。
7. 必要に応じて、先に確立されたすべてのプール、ポリシー、およびテンプレートから取得されるサービス プロファイル テンプレートを作成します。
8. テンプレートからサービス プロファイルをインスタンス化してサービス プロファイルを特定のブレードに関連付けるか、またはサービス プロファイル テンプレートを特定のサーバ プールに関連付けるように設定します。

ストレージ プロトコル

ファイバ チャネル、iSCSI、および Fibre Channel over Ethernet は SAN 接続用のプロトコルです。

- **iSCSI**：プリンタ、スキャナ、テープ ドライブ、およびストレージデバイスといったさまざまな I/O 周辺機器を接続するための業界標準のプロトコルです。最も一般的な SCSI デバイスは、ディスクとテープ ライブラリです。

  SCSI は raw ハード ディスク ストレージをサーバに接続するための主要なプロトコルです。SCSI プロトコルを使用してリモート ストレージを制御するには、コマンドをカプセル化するラッパーとして、FC や iSCSI などのさまざまなテクノロジーが使用されます。

  ファイバ チャネル プロトコルは、SCSI トラフィックをカプセル化してコンピュータとストレージの間の接続を確立するためのインフラストラクチャを提供します。FC は、2、4、8、および 16 Gbps の速度で動作します。

- **ファイバ チャネル（FC）**は次の要素で構成されています。

- raw ストレージ容量を提供するハード ディスク アレイ。
- ハード ディスクを管理し、サーバに対してストレージ LUN およびマスキングを提供するストレージ プロセッサ。
- ストレージ プロセッサとサーバ HBA の間を接続するファイバ チャネル スイッチ（ファブリックとも呼ばれます）。
- ファイバ チャネル ホスト バス アダプタ：これらはコンピュータにインストールされ、SAN への接続を確立します。

ファイバチャネルは、ワールドワイド番号（WWN）でインフラストラクチャ コンポーネントを識別します。WWN は、FC デバイスを一意に識別する 64 ビットのアドレスです。MAC アドレスと同様に、ベンダーに割り当てられたビットが含まれており、それによってベンダーのデバイスを識別します。各エンド デバイス（HBA ポートなど）にはワールド ワイド ポート番号（WWPN）が与えられ、各接続デバイス（ファブリック スイッチなど）にはワールドワイド ノード番号（WWNN）が与えられます。

SAN への接続に使用されるファイバ チャネル HBA はイニシエータと呼ばれ、LUN としてディスクを提供するファイバ チャネル SAN はターゲットと呼ばれます。ファイバ チャネル プロトコルは、イーサネットや TCP/IP プロトコルとは異なります。

- **Fiber Channel over Ethernet（FCoE）**転送は、ファイバ チャネル配線を 10 ギガビット イーサネット ケーブルで置き換えるもので、ユニファイド I/O でのロスレス配信を実現します。イーサネットは、ネットワークで広く使用されています。イーサネットにデータセンター イーサネット（DCE）やプライオリティ フロー制御（PFC）などの拡張を加えて、データセンター向けに信頼性を高めることで、ファイバチャネルもイーサネット上に実装されるようになります。この実装を FCoE と呼びます。

UCS Manager の [SAN] タブ

UCS 管理者は、[SAN] タブから SAN（FC、iSCSI）やダイレクト アタッチド FC/FCoE、NAS アプライアンス、および通信に関連する設定要素を作成、変更、および削除できます。

このタブの主要なノードは次のとおりです。

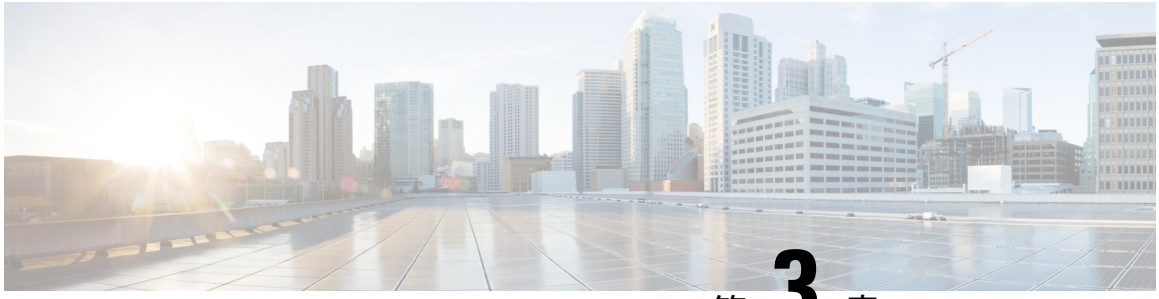
- [SAN Cloud]：このノードでは次の操作を実行できます。
  - SAN アップリンク（ストレージ ポート、ポート チャネル、SAN ピン グループなど）を設定します。
  - FC ID の割り当てを表示します。
  - WWN プール（WWPN、WWxN、および WWxN など）、iSCSI 修飾名（IQN）、プールを設定します。
  - 特定のエンド ポイントの FSM 詳細を表示してタスクが成功または失敗したかどうかを確認し、FSM を使用してエラーのトラブルシューティングを行います。

  - ストレージのイベントやエラーをモニタして状態を管理します。

- [Storage Cloud]：このノードでは次の操作を実行できます。
  - ストレージ FC リンクとストレージ FCoE インターフェイスを設定します（SAN ストレージ マネージャを使用）。
  - VSAN の設定を行います。
  - SAN クラウドのイベントをモニタして状態を管理します。

- **[Policies]**：このノードでは次の操作を実行できます。
  - しきい値のポリシー、クラス、およびプロパティを設定し、イベントをモニタします。
  - しきい値の組織およびサブ組織のストレージ ポリシー（デフォルト VHBA、動作、FC アダプタ、LACP、SAN 接続、SAN コネクタ、および VHBA テンプレートなど）を設定します。

- [Pools]：このノードでは、システムで定義されたプール（IQN、IQN サフィックス、WWNN、WWPN、および WWxN など）を設定できます。
- [Traffic Monitoring Sessions]：このノードでは、システムで定義されたポート トラフィック モニタリング セッションを設定できます。



第 3 章

SAN ポートおよびポート チャネル

ポート モード

ポートモードは、ファブリックインターコネクト上の統合ポートが、イーサネットまたはファイバ チャネル トラフィックを転送するかどうかを決定します。ポート モードを設定するには Cisco UCS Manager を使用します。ただし、ファブリック インターコネクトは自動的にポートモードを検出しません。

ポートモードを変更すると、既存のポート設定が削除され、新しい論理ポートに置き換えられます。VLANやVSANなど、そのポート設定に関連付けられているオブジェクトもすべて削除されます。ユニファイドポートでポートモードを変更できる回数に制限はありません。

ポート タイプ

ポート タイプは、統合ポート接続経由で転送されるトラフィックのタイプを定義します。

イーサネット ポート モードに変更されたユニファイド ポートは、デフォルトでアップリンク イーサネット ポート タイプに設定されます。ファイバ チャネル ポート モードに変更されたユニファイド ポートは、ファイバ チャネル アップリンク ポート タイプに設定されます。ファイバ チャネル ポートを設定解除することはできません。

ポート タイプ変更時のリブートは不要です。

イーサネット ポート モード

ポート モードを「イーサネット」に設定するときには、次のポート タイプを設定できます。

- サーバ ポート
- イーサネット アップリンク ポート
- イーサネット ポート チャネル メンバ
- FCoE ポート
- アプライアンス ポート
- アプライアンス ポート チャネル メンバ
- SPAN 宛先ポート
- SPAN 送信元ポート

（注） SPAN 送信元ポートでは、いずれかのポート タイプを設定した後、そのポートを SPAN 送信元として設定します。

ファイバ チャネル ポート モード

ポート モードを「ファイバ チャネル」に設定するときには、次のポート タイプを設定できます。

- ファイバ チャネル アップリンク ポート
- ファイバ チャネル ポート チャネル メンバ
- ファイバ チャネル ストレージ ポート
- SPAN 送信元ポート

（注） SPAN 送信元ポートでは、いずれかのポート タイプを設定した後、そのポートを SPAN 送信元として設定します。

ポート モード変更によるデータ トラフィックへの影響

ポート モードの変更は、Cisco UCS ドメイン へのデータ トラフィックの中断を引き起こす場合があります。中断の長さや影響を受けるトラフィックは、ポートモード変更を行ったモジュールおよび Cisco UCS ドメイン の設定に依存します。

ヒント システム変更中のトラフィックの中断を最小限にするには、固定と拡張モジュールにファイバ チャネル アップリンク ポートチャネルを形成します。

ポート モード変更の拡張モジュールへの影響

拡張モジュールのポートモードの変更後、モジュールを再起動します。拡張モジュールのポートを通過するすべてのトラフィックは、モジュールのリブート中に約 1 分間中断します。

ポート モード変更のクラスタ設定の固定モジュールへの影響

クラスタ設定には2個のファブリック インターコネクトがあります。固定モジュールへのポート変更を行った後、ファブリック インターコネクトはリブートします。データ トラフィックの影響は、1つのファブリック インターコネクトに障害が発生したときにもう一方にフェールオーバーするようサーバ vNIC を設定したかどうかに左右されます。

1 つのファブリック インターコネクトの拡張モジュール上のポート モードを変更し、第 2 のファブリック インターコネクトのポート モードを変更する前のリブートを待つ場合、次のことが発生します。

- サーバ vNIC のフェールオーバーでは、トラフィックは他のファブリック インターコネクトにフェールオーバーし、中断は発生しません。
- サーバ vNIC のフェールオーバーがない場合、ポートモードを変更したファブリック インターコネクトを通過するすべてのデータ トラフィックは、ファブリック インターコネクトがリブートする約 8 分間中断されます。

両方のファブリックインターコネクトの固定モジュールのポートモードを同時に変更すると、ファブリックインターコネクトによるすべてのデータ トラフィックが、ファブリックインターコネクトがリブートする約 8 分間中断されます。

ポート モード変更のスタンドアロン設定の固定モジュールへの影響

スタンドアロン設定にはファブリックインターコネクトが1つだけあります。固定モジュールへのポート変更を行った後、ファブリックインターコネクトはリブートします。ファブリックインターコネクトによるすべてのデータ トラフィックは、ファブリック インターコネクトがリブートする約 8 分間中断されます。

FC リンクの再調整

FC アップリンクは、FC ポート チャネルが使用されると自動的に調整されます。FC ポート チャネルを作成するには、ファイバ チャネル ポート チャネルの設定 （46 ページ） を参照してください。

ポート チャネルのメンバーでない FC アップリンク（個別の ISL）では、ロード バランシングは FC アップリンクのバランシング アルゴリズムに基づいて行われます。FC アップリンクのトランキングが無効の際に、ホストまたはサービス プロファイルの vHBA が使用可能な FC アップリンクを選択するには、アップリンクと vHBA が同一の VSAN に属している必要があります。

アルゴリズムは、vHBA ごとに、次の順序で FC アップリンクを探します。

1. 現在アップリンクにバインドされている vHBA の数に基づき、使用が最も少ない FC アップリンク。
2. FC アップリンクが均等にバランシングされている場合は、ラウンドロビンを使用します。

このプロセスを他のすべての vHBA についても行います。アルゴリズムは、pre-FIP、FIP アダプタと FLOGI 数などのその他のパラメータも考慮します。6 FLOGI に満たない場合、使用が最も少ないコンポーネントは表示されないことがあります。

ポート設定や他のアップリンクの状態の変更後、FC アップリンクを通過するトラフィックのバランスが崩れた場合、各アダプタの vHBA をリセットし、ロード バランシング アルゴリズムに FC アップリンクの現在の状態を評価させることでトラフィックを再度バランシングできます。

ポート モードの設定

⚠

注意 いずれかのモジュール のポート モードを変更すると、データ トラフィックが中断されることがあります。これは、固定モジュールを変更するとファブリック インターコネクトのリブートが必要となり、拡張モジュールを変更するとそのモジュール のリブートが必要となるためです。

Cisco UCS ドメインの中に、ハイ アベイラビリティ用に設定されたクラスタ構成が存在し、しかもフェールオーバー用に設定されたサービスプロファイルを持つサーバが存在する場合、固定モジュールのポート モードを変更しても、トラフィックはもう 1 つのファブリック インターコネクトにフェールオーバーし、データ トラフィックは中断されません。

Cisco UCS Manager CLI で、ユニファイド ポートをサポートする新しいコマンドはありません。代わりに、必要なポート タイプ用のモードにスコープしてから新しいインターフェイスを作成することで、ポート モードを変更します。設定済みのスロット ID およびポート ID に新しいインターフェイスを作成する場合、UCS Manager は、すでに設定されているインターフェイス

を削除し、新しく作成します。以前はイーサネット ポート モードで動作していたポートをファイバ チャネル ポート モードに設定するためにポート モードの変更が必要な場合、UCS Manager は変更を確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope** *port-type-mode*	次のいずれかのポート タイプの指定されたポート タイプ モードを開始します。 **eth-server** サーバ ポート設定用。 **eth-storage** イーサネット ストレージ ポートおよびイーサネット ストレージ ポート チャネルの設定用。 **eth-traffic-mon** イーサネット SPAN ポート設定用。 **eth-uplink** イーサネット アップリンク ポート設定用。 **fc-storage** ファイバ チャネル ストレージ ポート設定用。 **fc-traffic-mon** ファイバ チャネル SPAN ポート設定用。 **fc-uplink** ファイバ チャネル アップリンク ポートおよびファイバ チャネル アップリンク ポート チャネルの設定用。
ステップ 2	UCS-A /*port-type-mode* # **scope fabric** {**a** | **b**}	指定したファブリックの指定されたポート タイプ モードを開始します。
ステップ 3	UCS-A /*port-type-mode*/fabric # **create interface** *slot-id* *port-id*	指定されたポート タイプのインターフェイスを作成します。 ポート タイプをイーサネット ポート モードからファイバ チャネル ポート

	コマンドまたはアクション	目的
		モードに、またはその逆に変更すると、次の警告が表示されます。 `Warning: This operation will change the port mode (from Ethernet to FC or vice-versa). When committed, this change will require the module to restart.`
ステップ 4	イーサネットまたはファイバ チャネル ポート ブロックに属する他のポートの新しいインターフェイスを作成します。	イーサネットおよびファイバ チャネル ポートを固定または拡張モジュールに配置する方法を規定する、いくつかの制約事項があります。他の制約事項の範囲内で、2つのグループのポートを変更する必要があります。「ユニファイド ポートの設定に関するガイドライン」セクションに概説されている制約事項のいずれかに違反すると、エラーが発生します。
ステップ 5	UCS-A /*port-type-mode*/fabric/interface # **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。

ポート モードを設定したモジュールに応じて、Cisco UCS ドメインのデータ トラフィックが次のように中断されます。

- 固定モジュール：ファブリック インターコネクトがリブートします。そのファブリック インターコネクトを経由するすべてのデータ トラフィックが中断されます。ハイ アベイラビリティが提供され、フェールオーバー用に設定された vNIC があるサーバが含まれるクラスタ構成では、トラフィックは他のファブリック インターコネクトにフェールオーバーし、中断は発生しません。

  固定モジュールがリブートするまで約 8 分かかります。

- 拡張モジュール：モジュールがリブートします。そのモジュールのポートを経由するすべてのデータ トラフィックが中断されます。

  拡張モジュールがリブートするまでに約 1 分かかります。

例

次の例では、スロット 1 のポート 3 と 4 をイーサネット ポート モードのイーサネット アップリンク ポートからファイバ チャネル ポート モードのアップリンク ファイバ チャネル ポートに変更します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create interface 1 3
```

```
Warning: This operation will change the port mode (from Ethernet to FC or vice-versa).
When committed, this change will require the fixed module to restart.
UCS-A /fc-uplink/fabric/interface* # up
UCS-A /fc-uplink/fabric* #create interface 1 4
Warning: This operation will change the port mode (from Ethernet to FC or vice-versa).
When committed, this change will require the fixed module to restart.
UCS-A /fc-uplink/fabric/interface* #commit-buffer
```

ポート プロパティとファイバ チャネル統計の表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /fabric-interconnect # **connect nxos** {**a** | **b**	ファブリック インターコネクトの NX-OS モードを開始します。
ステップ 2	UCS-A(nxos) # **show interface fc** *slot-id*/*port-id*	ポートのプロパティとスループット レート、およびエラーなどのファイバ チャネルの統計情報が表示されます。 （注） UCS 6400 シリーズ ファブリック インターコネクトの **receive B2B credit remaining** が、そのピア スイッチの **transmit B2B credit remaining** と一致しません。フレームがリリースされると、クレジットが返されるため、**receive B2B credit remaining** パラメータは常に 64 になります。MDS ピアで、**transmit B2B credit remaining** パラメータは 0 に移動できます。この結果は、一致しません。これらのパラメータを比較するために、ピア スイッチで **show interface fc** *slot-id*/*port-id* コマンドを実行します。

例

次の例は、ポート プロパティおよび UCS 6400 シリーズ ファブリック インターコネクトをファイバ チャネルの統計情報を表示します。

```
UCS-A /fabric-interconnect # connect nxos a
UCS-A(nxos)# show interface fc 1/6
fc1/6 is trunking
    Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
    Port WWN is 20:06:00:de:fb:21:77:00
    Admin port mode is NP, trunk mode is on
    snmp link state traps are enabled
    Port mode is TNP
    Port vsan is 8
    Speed is 16 Gbps
    Transmit B2B Credit is 32
    Receive B2B Credit is 64
    Receive data field Size is 2112
    Beacon is turned off
    Belongs to san-port-channel 32
    Trunk vsans (admin allowed and active) (1,5,7-8,40,120)
    Trunk vsans (up)                       (1,5,7-8,40,120)
    Trunk vsans (isolated)                 ()
    Trunk vsans (initializing)             ()
    5 minutes input rate 497578904 bits/sec,62197363 bytes/sec, 30981 frames/sec
    5 minutes output rate 501679056 bits/sec,62709882 bytes/sec, 30319 frames/sec
      430000799 frames input,863205473268 bytes
        0 discards,0 errors
        0 invalid CRC/FCS,0 unknown class
        0 too long,0 too short
      423530360 frames output,876009587416 bytes
        0 discards,0 errors
      1 input OLS,1  LRR,9 NOS,0 loop inits
      1 output OLS,0 LRR, 8 NOS, 0 loop inits
      64 receive B2B credit remaining
      32 transmit B2B credit remaining
      0 low priority transmit B2B credit remaining
    Last clearing of "show interface" counters  :never
```

サーバ ポート

サーバ ポートの設定

リストされている全ポートタイプは、固定および拡張モジュールで構成可能です。これには、6100シリーズファブリック インターコネクトの拡張モジュールでは設定できないものの、6200シリーズ ファブリック インターコネクトの拡張モジュールでは設定できるサーバ ポートを含みます。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。

	Command or Action	Purpose
ステップ 3	UCS-A /eth-server/fabric # **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 4	UCS-A /eth-server/fabric # **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。

Example

次の例で、ファブリック B のスロット 1 にあるイーサネット サーバ ポート 4 のインターフェイスを作成し、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 eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # create interface 1 4
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

サーバ ポートの設定解除

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **delete interface** *slot-num* *port-num*	指定したイーサネット サーバ ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-server/fabric # **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。

Example

次に、ファブリック B のスロット 1 にあるイーサネット サーバ ポート 12 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric b
UCS-A /eth-server/fabric # delete interface 1 12
UCS-A /eth-server/fabric* # commit-buffer
UCS-A /eth-server/fabric #
```

統合ポート

ユニファイド ポートの設定に関するガイドライン

ユニファイドポートを設定する際は、次のガイドラインおよび制約事項を考慮してください。

ハードウェアおよびソフトウェアの要件

ユニファイド ポートは、次でサポートされます。

- Cisco UCS Manager リリース 4.1 および以降のリリースを使用している Cisco UCS 64108 ファブリック インターコネクト
- Cisco UCS Manager リリース 4.0 以降のリリースの Cisco UCS 6454 ファブリック インターコネクト
- Cisco UCS Manager リリース 3.1 以降のリリースの UCS 6300 シリーズ ファブリック インターコネクト
- Cisco UCS Manager リリース 2.0 以降のリリースの UCS 6200 シリーズ ファブリック インターコネクト
- Cisco UCS Manager リリース 3.0 以降のリリースの UCS 6324 シリーズ ファブリック インターコネクト

ユニファイド ポートは 6100 シリーズ ファブリック インターコネクトではサポートされません。それらで Cisco UCS Manager バージョン 2.0 が実行されている場合でも同様です。

ポート モードの配置

Cisco UCS Manager GUI インターフェイスは固定または拡張モジュールのユニファイド ポートのポート モードの設定に、スライダーを使用するため、ポート モードのユニファイド ポートへの割り当て方法を制限する次の制約事項が自動的に適用されます。Cisco UCS Manager CLI インターフェイスを使用する場合は、トランザクションをシステム設定にコミットするときに次の制約事項が適用されます。ポートモードの設定が次の制約事項のいずれかに違反している場合、Cisco UCS Manager CLI によってエラーが表示されます。

- イーサネット ポートはブロックにグループ化する必要があります。各モジュール（固定または拡張）において、イーサネット ポートブロックは、1 番目のポートから始まり、偶数番号のポートで終わる必要があります。
- ファイバ チャネル ポートがブロックにグループ化されていること。各モジュールについて（固定または拡張）、ファイバ チャネル ポート ブロックは、最後のイーサネット ポートの後ろにブロックの 1 番目のポートが続き、その後ろにモジュール内の残りのポートが含まれている必要があります。ファイバ チャネル ポートだけを含む設定では、ファイバ チャネルブロックは、固定または拡張モジュールの 1 番目のポートから開始する必要があります。

（注） Cisco UCS 6400 シリーズ ファブリック インターコネクト では、ユニファイド ポート機能が最初の 16 ポートに制限されます。ポート 1/1-1/16 のみ FC として設定できます。FC ポートは互いに連続している必要があり、その後に連続的なイーサーネット ポートが続く必要があります。

- Cisco UCS サーバーに接続されている Cisco UCS 6400 シリーズ ファブリック インターコネクト の場合、16 を超えるポートを接続するとエラーが発生します。
- イーサネット ポートとファイバ チャネル ポートの交替は、単一モジュール上ではサポートされない。

有効な設定例：固定モジュールのユニファイド ポート 1 ～ 16 がイーサネット ポート モードに設定され、ポート 17 ～ 32 がファイバ チャネル ポート モードに設定されている。拡張モジュールでは、ポート 1 ～ 4 をイーサネット ポート モードに設定し、ポート 5 ～ 16 をファイバ チャネル モードに設定できます。このポート割り当ては各個別モジュールの規則に準拠しているため、ポート タイプ（イーサネット ポートとファイバ チャネル ポート）の交替に関する規則に違反していません。

無効な設定例：ポート 16 から始まるファイバ チャネル ポートのブロックが含まれている。ポートの各ブロックは奇数ポートから開始する必要があるため、ポート 17 からブロックを開始しなければなりません。

（注） 各ファブリック インターコネクトで設定可能なアップリンク イーサネット ポートおよびアップリンク イーサネット ポート チャネル メンバの総数は、最大 31 に制限されています。この制限には、拡張モジュールで設定されるアップリンク イーサネット ポートおよびアップリンク イーサネット ポート チャネル メンバも含まれます。

ユニファイドアップリンクポートおよびユニファイドストレージポートの設定に関する注意およびガイドライン

以下は、ユニファイド アップリンク ポートとユニファイド ストレージ ポートを使用する際に従うべき注意事項とガイドラインです。

- ユニファイド アップリンク ポートでは、SPAN 送信元として 1 つのコンポーネントを有効にすると、他のコンポーネントが自動的に SPAN 送信元になります。

（注） イーサネット アップリンク ポートで SPAN 送信元が作成または削除されると、Cisco UCS Manager は自動的に FCoE アップリンク ポートで SPAN 送信元を作成または削除します。FCoE アップリンク ポートで SPAN 送信元を作成する場合も同じことが起こります。

- FCoE およびユニファイド アップリンク ポートでデフォルトでないネイティブ VLAN を設定する必要があります。この VLAN は、トラフィックには使用されません。Cisco UCS Manager はこの目的のために、既存の fcoe-storage-native-vlan を再利用します。この fcoe-storage-native-vlan は、FCoE およびユニファイドアップリンクでネイティブ VLAN として使用されます。
- ユニファイド アップリンク ポートでは、イーサネット アップリンク ポートにデフォルト以外の VLAN が指定されていない場合、fcoe-storage-native-vlan がユニファイド アップリンク ポートのネイティブ VLAN として割り当てられます。イーサネット ポートにネイティブ VLAN として指定されているデフォルトでないネイティブ VLAN がある場合、ユニファイド アップリンク ポートのネイティブ VLAN としてこれが割り当てられます。
- イーサネット ポート チャネル下でメンバ ポートを作成または削除すると、Cisco UCS Manager は FCoE ポート チャネル下で自動的にメンバ ポートを作成または削除します。FCoE ポート チャネルでメンバー ポートを作成または削除する場合も同じことが起こります。
- サーバ ポート、イーサネット アップリンク、FCoE アップリンクまたは FCoE ストレージなどのスタンドアロン ポートとしてイーサネット ポートを設定し、それをイーサネットまたは FCOE ポート チャネルのメンバ ポートにすると、Cisco UCS Manager は自動的にこのポートをイーサネットと FCoE ポート チャネル両方のメンバにします。
- サーバ アップリンク、イーサネット アップリンク、FCoE アップリンクまたは FCoE ストレージのメンバからメンバ ポートのメンバーシップを削除すると、Cisco UCS Manager はイーサネット ポート チャネルと FCoE ポート チャネルから対応するメンバ ポートを削除し、新しいスタンドアロン ポートを作成します。
- Cisco UCS Manager をリリース 2.1 から以前のリリースにダウングレードする場合は、ダウングレードが完了すると、すべてのユニファイド アップリンク ポートとポート チャネルがイーサネット ポートとイーサネット ポート チャネルに変換されます。同様に、すべてのユニファイド ストレージ ポートが、アプライアンス ポートに変換されます。
- ユニファイド アップリンク ポートとユニファイド ストレージ ポートの場合、2 つのインターフェイスを作成するときは、1 つだけライセンスがチェックされます。どちらかのインターフェイスが有効な限り、ライセンスはチェックされたままになります。両方のインターフェイスがユニファイド アップリンク ポートまたはユニファイド ストレージ ポートで無効の場合にのみライセンスが解放されます。
- Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチは、同一のダウンストリーム NPV スイッチ側の 1VF または 1VF-PO のみをサポートできます。

ユニファイド ポートのビーコン LED

6200 シリーズ ファブリック インターコネクトの各ポートには、対応するビーコン LED があります。[Beacon LED] プロパティが設定されている場合は、ビーコン LED が点灯し、特定のポート モードに設定されているポートが示されます。

[Beacon LED] プロパティは、特定のポートモード（イーサネットまたはファイバ チャネル）にグループ化されているポートを示すように設定できます。デフォルトでは、ビーコン LED プロパティは Off に設定されます。

（注） 拡張モジュールのユニファイド ポートの場合、[Beacon LED] プロパティは、拡張モジュールの再起動時にデフォルト値の [Off] にリセットされます。

ユニファイド ポートのビーコン LED の設定

ビーコン LED を設定する各モジュールについて次のタスクを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fabric-interconnect** {**a** | **b**}	指定したファブリックのファブリック インターコネクトモードを開始します。
ステップ 2	UCS-A /fabric # **scope card** *slot-id*	指定された固定または拡張モジュールのカード モードを開始します。
ステップ 3	UCS-A /fabric/card # **scope beacon-led**	ビーコン LED モードを開始します。
ステップ 4	UCS-A /fabric/card/beacon-led # **set admin-state** {**eth** | **fc** | **off**}	点灯ビーコン LED ライトが表すポートモードを指定します。 **eth** イーサネットモードで設定されたユニファイドポートすべてが点滅します。 **fc** ファイバ チャネル モードで設定されたユニファイドポートすべてが点滅します。 **off** モジュール上のすべてのポートのビーコン LED ライトが消えます。

	コマンドまたはアクション	目的
ステップ 5	UCS-A /fabric/card/beacon-led # **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、イーサネット ポート モードのユニファイド ポートのビーコン ライトすべてを点滅させ、トランザクションをコミットします。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric # scope card 1
UCS-A /fabric/card # scope beacon-led
UCS-A /fabric/card/beacon-led # set admin-state eth
UCS-A /fabric/card/beacon-led* # commit-buffer
UCS-A /fabric/card/beacon-led #
```

ファブリック インターコネクトのユニファイド ポート

ユニファイド ポートは、イーサネットまたはファイバ チャネル トラフィックを伝送するように設定できるファブリック インターコネクトのポートです。これらのポートは予約されていません。Cisco UCS ドメイン はそれらを設定するまで、これらのポートを使用できません。

（注） ファブリック インターコネクトのポートを設定すると、管理状態が自動的にイネーブルに設定されます。ポートが他のデバイスに接続されている場合は、これによってトラフィックが中断されることがあります。ポートの設定後に、そのポートを無効にできます。

設定可能なビーコン LED は、選択したポート モードに設定されているユニファイド ポートを示します。

ユニファイド ストレージ ポート

ユニファイド ストレージでは、イーサネット ストレージ インターフェイスと FCoE ストレージ インターフェイスの両方として同じ物理ポートを設定する必要があります。ユニファイド ストレージ ポートとして、任意のアプライアンス ポートまたは FCoE ストレージ ポートを構成できます。ユニファイド ストレージ ポートを設定するには、ファブリック インターコネクトをファイバ チャネル スイッチング モードにする必要があります。

ユニファイド ストレージ ポートでは、個々の FCoE ストレージまたはアプライアンス インターフェイスをイネーブルまたはディセーブルにできます。

- ユニファイド ストレージ ポートでは、アプライアンス ポートにデフォルト以外の VLAN が指定されていない限り、fcoe-storage-native-vlan がユニファイド ストレージ ポートのネイティブ VLAN として割り当てられます。アプライアンス ポートにデフォルト以外のネ

イティブ VLAN がネイティブ VLAN として指定されている場合は、それがユニファイド ストレージ ポートのネイティブ VLAN として割り当てられます。

- アプライアンスインターフェイスをイネーブルまたはディセーブルにすると、対応する物理ポートがイネーブルまたはディセーブルになります。したがって、ユニファイド ストレージでアプライアンス インターフェイスをディセーブルにすると、FCoE ストレージが物理ポートとともにダウン状態になります（FCoE ストレージがイネーブルになっている場合でも同様です）。
- FCoE ストレージ インターフェイスをイネーブルまたはディセーブルにすると、対応する VFC がイネーブルまたはディセーブルになります。したがって、ユニファイド ストレージ ポートで FCoE ストレージ インターフェイスをディセーブルにした場合、アプライアンス インターフェイスは正常に動作し続けます。

ユニファイド ストレージ ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create interface** *slot-num port-num*	指定されたアプライアンス ポートのインターフェイスを作成します。
ステップ 4	UCS-A /eth-storage/fabric/interface* # **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。
ステップ 5	UCS-A /eth-storage/fabric/interface* # **scope fc-storage**	FC ストレージ モードを開始します。
ステップ 6	UCS-A /fc-storage* # **scope fabric**{**a** | **b**}	特定のアプライアンス ポートに対してイーサネット ストレージ モードを開始します。
ステップ 7	UCS-A /fc-storage/fabric # **create interface fcoe** *slot-num port-num*	アプライアンス ポート モードで FCoE ストレージ ポート モードを追加し、ユニファイド ストレージ ポートを作成します。

例

次の例では、ファブリック A のスロット 3 上のアプライアンス ポート 2 用のインターフェイスを作成し、同じポートに fc ストレージを追加してユニファイド ポートに変換し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # create interface 3 2
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric* # scope fc-storage
UCS-A /fc-storage*# scope fabric a
UCS-A /fc-storage/fabric* # create interface fcoe 3 2
UCS-A /fc-storage/fabric* # commit-buffer
UCS-A /fc-storage/fabric*
```

ユニファイド アップリンク ポート

同じ物理イーサネット ポート上にイーサネット アップリンクと FCoE アップリンクを設定した場合、そのポートはユニファイド アップリンク ポートと呼ばれます。FCoE またはイーサネット インターフェイスは個別にイネーブルまたはディセーブルにできます。

- FCoE アップリンクをイネーブルまたはディセーブルにすると、対応する VFC がイネーブルまたはディセーブルになります。
- イーサネット アップリンクをイネーブルまたはディセーブルにすると、対応する物理ポートがイネーブルまたはディセーブルになります。

イーサネット アップリンクをディセーブルにすると、ユニファイド アップリンクを構成している物理ポートがディセーブルになります。したがって、FCoE アップリンクもダウンします（FCoE アップリンクがイネーブルになっている場合でも同様です）。しかし、FCoE アップリンクをディセーブルにした場合は、VFC だけがダウンします。イーサネット アップリンクがイネーブルであれば、FCoE アップリンクは引き続きユニファイド アップリンク ポートで正常に動作することができます。

ユニファイド アップリンク ポートの設定

ユニファイド アップリンク ポートを設定するには、ユニファイド ポートとして既存の FCoE アップリンク ポートを変換します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク 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 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create interface** *15*	ユニファイド ポートとして FCoE アップリンク ポートを変換します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **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、既存の FCoE ポートでユニファイド アップリンク ポートを作成します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create interface 1 5
UCS-A /eth-uplink/fabric/interface* # commit-buffer
UCS-A /eth-uplink/interface #
```

ユニファイド アップリンク ポート チャネル

同じ ID でイーサネット ポート チャネルと FCoE ポート チャネルを作成した場合、それらはユニファイド ポート チャネルと呼ばれます。ユニファイド ポート チャネルが作成されると、指定されたメンバを持つファブリック インターコネクトで物理イーサネット ポート チャネルと VFC が作成されます。物理イーサネット ポート チャネルは、イーサネット トラフィックと FCoE トラフィックの両方を伝送するために使用されます。VFC は、FCoE トラフィックをイーサネット ポート チャネルにバインドします。

次のルールは、ユニファイドアップリンク ポートチャネルのメンバー ポートセットに適用されます。

- 同じ ID のイーサネット ポート チャネルと FCoE ポート チャネルは、同じメンバー ポート セットを持つ必要があります。
- イーサネットポートチャネルにメンバーポートチャネルを追加すると、Cisco UCS Manager は、FCoE ポート チャネルにも同じポート チャネルを追加します。同様に、FCoE ポート チャネルにメンバーを追加すると、イーサネット ポート チャネルにもそのメンバー ポートが追加されます。
- ポート チャネルの 1 つからメンバー ポートを削除すると、Cisco UCS Manager は他のポート チャネルから自動的にそのメンバー ポートを削除します。

イーサネットアップリンク ポートチャネルをディセーブルにすると、ユニファイドアップリンク ポートチャネルを構成している物理ポートチャネルがディセーブルになります。したがって、FCoE アップリンク ポート チャネルもダウンします（FCoE アップリンクがイネーブルに

なっている場合でも同様です）。FCoEアップリンク ポートチャネルをディセーブルにした場合は、VFC のみがダウンします。イーサネット アップリンク ポート チャネルがイネーブルであれば、FCoE アップリンク ポート チャネルは引き続きユニファイド アップリンク ポート チャネルで正常に動作することができます。

ユニファイド アップリンク ポート チャネルの設定

ユニファイドアップリンク ポートチャネルを設定するには、ユニファイドポートチャネルとして既存の FCoE アップリンク ポート チャネルを変換します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-uplink**	イーサネット アップリンク モードを開始します。
ステップ 2	UCS-A /eth-uplink # **scope fabric** {**a** | **b**}	指定されたファブリックのイーサネット アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /eth-uplink/fabric # **create port-channel** *ID*	指定したイーサネット アップリンク ポートのポートチャネルを作成します。
ステップ 4	UCS-A /eth-uplink/fabric/port-channel # **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、既存の FCoE ポート チャネルでユニファイド アップリンク ポート チャネルを作成します。

```
UCS-A# scope eth-uplink
UCS-A /eth-uplink # scope fabric b
UCS-A /eth-uplink/fabric # create port-channel 2
UCS-A /eth-uplink/fabric/port-channel* # commit-buffer
UCS-A /eth-uplink/fabric #
```

Cisco UCS Mini スケーラビリティ ポート

には4つのユニファイドポートに加えて、1つのスケーラビリティ ポートがあります。スケーラビリティ ポートは、適切に配線されている場合に、4 つの 1G または 10G SFP+ ポートをサポート可能な 40 GB QSFP+ ブレイクアウト ポートです。スケーラビリティ ポートは、サポート対象の Cisco UCS ラック サーバ、アプライアンス ポート、または FCoE ポート用のライセンス サーバ ポートとして使用できます。

Cisco UCS Manager GUI では、スケーラビリティ ポートは、**[Ethernet Ports]** ノードの下に **[Scalability Port 5]** と表示されます。個々のブレイクアウト ポートは、[Port 1] ～ [Port 4] と表示されます。

Cisco UCS Manager CLI では、スケーラビリティ ポートは表示されませんが、個々のブレークアウト ポートは **Br-Eth1/5/1** ～ **Br-Eth1/5/4** として表示されます。

スケーラビリティ ポートの設定

スケーラビリティ ポートにポート、ポート チャネル メンバー、または SPAN メンバーを設定するには、スケーラビリティ ポートに移動してから、標準ユニファイド ポート用の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **scope aggr-interface** *slot-num port-num*	スケーラビリティ ポートのイーサネット サーバ ファブリック集約インターフェイス モードを開始します。
ステップ 4	UCS-A /eth-server/fabric/aggr-interface # **show interface**	スケーラビリティ ポートのインターフェイスを表示します。
ステップ 5	UCS-A /eth-server/fabric/aggr-interface # **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 6	UCS-A /eth-server/fabric/aggr-interface # **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、ファブリック A スケーラビリティ ポートのイーサネット サーバ ポート 3 にインターフェイスを作成し、トランザクションをコミットする方法を示しています。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # scope aggr-interface 1 5
UCS-A /eth-server/fabric/aggr-interface # show interface
Interface:

Slot Id Aggr-Port ID Port Id  Admin State Oper State    State Reason
------- ------------ -------- ----------- ------------- ------------
```

```
      1            5        1 Enabled     Up
      1            5        2 Enabled     Up
      1            5        3 Enabled     Admin Down    Administratively Down
      1            5        4 Enabled     Admin Down    Administratively Down

UCS-A /eth-server/fabric/aggr-interface # create interface 1 3
UCS-A /eth-server/fabric/aggr-interface* # commit-buffer
UCS-A /eth-server/fabric/aggr-interface #
```

アプライアンス ポート

アプライアンス ポートは、直接接続された NFS ストレージにファブリック インターコネクトを接続する目的のみに使用されます。

（注） ダウンロードするファームウェア実行可能ファイルの名前。したがって、新しい VLAN に設定されたアプライアンス ポートは、ピン接続エラーにより、デフォルトで停止したままなります。これらのアプライアンス ポートを起動するには、同じ IEEE VLAN ID を使用して LAN クラウドで VLAN を設定する必要があります。

Cisco UCS Manager は、ファブリック インターコネクトごとに最大 4 つのアプライアンス ポートをサポートします。

アプライアンス ポートの設定

アプライアンス ポートは、固定モジュールと拡張モジュールのどちらでも設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create interface** *slot-num port-num*	指定されたアプライアンス ポートのインターフェイスを作成します。
ステップ 4	（任意） UCS-A /eth-storage/fabric/interface # **set portmode** {**access** | **trunk**}	ポート モードがアクセスとトランクのどちらであるかを指定します。デフォルトで、モードはトランクに設定されます。

	コマンドまたはアクション	目的
		（注） アプリケーション ポートでアップリンク ポートをトラバースする必要がある場合、LAN クラウドでこのポートによって使用される各 VLAN も定義する必要があります。たとえば、ストレージが他のサーバでも使用される場合や、プライマリ ファブリック インターコネクトのストレージ コントローラに障害が発生したときにトラフィックがセカンダリ ファブリック インターコネクトに確実にフェールオーバーされるようにする必要がある場合は、トラフィックでアップリンク ポートをトラバースする必要があります。
ステップ 5	（任意） UCS-A /eth-storage/fabric/interface # **set pingroupname** *pin-group name*	指定されたファブリックとポート、またはファブリックとポート チャネルへのアプライアンス ピン ターゲットを指定します。
ステップ 6	（任意） UCS-A /eth-storage/fabric/interface # **set prio** *sys-class-name*	アプライアンス ポートに QoS クラスを指定します。デフォルトでは、プライオリティは best-effort に設定されます。 sys-class-name 引数には、次のいずれかのクラス キーワードを指定できます。 • **[C]**：vHBA トラフィックのみを制御する QoS ポリシーにこのプライオリティを使用します。 • **[プラチナ（Platinum）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ゴールド（Gold）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。

	コマンドまたはアクション	目的
		• **[シルバー（Silver）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ブロンズ（Bronze）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ベストエフォート（Best Effort）]**：この優先順位は使用しないでください。ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当てて、別のシステム クラスを CoS 0 に設定した場合、Cisco UCS Managerはこのシステム クラスのデフォルトを使用しません。そのトラフィックに対しては、優先度がデフォルト（CoS 0）になります。
ステップ 7	（任意） UCS-A /eth-storage/fabric/interface # **set adminspeed** {**10gbps** | **1 gbps**}	インターフェイスの管理速度を指定します。デフォルトでは、管理速度は10gbpsに設定されます。
ステップ 8	UCS-A /eth-storage/fabric/interface # **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、ファブリック B のスロット 3 のアプライアンス ポート 2 にインターフェイスを作成し、ポート モードを access に設定し、アプライアンス ポートを pingroup1 と呼ばれるピン グループにピン接続し、QoS クラスを fc に設定し、管理速度を 10 Gbps に設定し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric b
UCS-A /eth-storage/fabric # create interface 3 2
UCS-A /eth-storage/fabric* # set portmode access
UCS-A /eth-storage/fabric* # set pingroupname pingroup1
UCS-A /eth-storage/fabric* # set prio fc
UCS-A /eth-storage/fabric* # set adminspeed 10gbps
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

次のタスク

アプライアンス ポートのターゲット MAC アドレスまたは VLAN を割り当てます。

アプライアンス ポートまたはアプライアンス ポート チャネルへの宛先 MAC アドレスの割り当て

次の手順は、アプライアンス ポートに宛先 MAC アドレスを割り当てます。アプライアンス ポート チャネルに宛先 MAC アドレスを割り当てるには、インターフェイスではなくポート チャネルにスコープを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric**{**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope interface** *slot-id port-id*	指定したインターフェイスのイーサネット インターフェイス モードを開始します。 （注） アプライアンス ポート チャネルに宛先 MAC アドレスを割り当てるには、 **scope port-channel** コマンドを **scope interface** の代わりに使用します。
ステップ 4	UCS-A /eth-storage/fabric/interface # **create eth-target** *eth-target name*	指定された MAC アドレス ターゲットの名前を指定します。
ステップ 5	UCS-A /eth-storage/fabric/interface/eth-target # **set mac-address** *mac-address*	MAC アドレスを nn:nn:nn:nn:nn:nn 形式で指定します。

例

次の例は、ファブリック B スロット 2 のポート 3 のアプライアンス デバイスに宛先 MAC アドレスを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage* # scope fabric b
UCS-A /eth-storage/fabric* # scope interface 2 3
UCS-A /eth-storage/fabric/interface* # create eth-target macname
```

```
UCS-A /eth-storage/fabric/interface* # set mac-address 01:23:45:67:89:ab
UCS-A /eth-storage/fabric/interface* # commit-buffer
UCS-A /eth-storage/fabric #
```

次の例は、ファブリック B のポート チャネル 13 のアプライアンス デバイスに宛先 MAC アドレスを割り当て、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage* # scope fabric b
UCS-A /eth-storage/fabric* # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel* # create eth-target macname
UCS-A /eth-storage/fabric/port-channel* # set mac-address 01:23:45:67:89:ab
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric #
```

アプライアンス ポートの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-storage# **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成し、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。
ステップ 3	UCS-A/eth-storage/vlan# **set sharing primary**	変更を保存します。
ステップ 4	UCS-A/eth-storage/vlan# **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。
ステップ 5	UCS-A/eth-storage# **create vlan** *vlan-name vlan-id*	ネームド VLAN を作成して、VLAN 名と VLAN ID を指定し、イーサネット ストレージ VLAN モードを開始します。
ステップ 6	UCS-A/eth-storage/vlan# **set sharing community**	作成しているセカンダリ VLAN にプライマリ VLAN を関連付けます。
ステップ 7	UCS-A/eth-storage/vlan# **set pubnwname** *primary vlan-name*	このセカンダリ VLAN に関連付けられているプライマリ VLAN を指定します。
ステップ 8	UCS-A/eth-storage/vlan# **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、アプライアンス ポートを作成します。

```
UCS-A# scope eth-storage
UCS-A/eth-storage# create vlan PRI600 600
UCS-A/eth-storage/vlan* # set sharing primary
UCS-A/eth-storage/vlan* # commit-buffer
UCS-A/eth-storage # create vlan COM602 602
UCS-A/eth-storage/vlan* # set sharing isolated
UCS-A/eth-storage/vlan* # set pubnwname PRI600
UCS-A/eth-storage/vlan* # commit-buffer
```

コミュニティ VLAN へのアプライアンス ポートのマッピング

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-storage# **scope fabric** {、|*b*}	指定したイーサネット ストレージ ファブリックインターコネクトのファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A/eth-storage/fabric# **create interface** *slot-num port-num*	指定されたイーサネット サーバ ポートのインターフェイスを作成します。
ステップ 4	UCS-A/eth-storage/fabric/interface# **exit**	インターフェイスを終了します。 （注） VLAN との関連付けの後、トランザクションをコミットすることを確認します。
ステップ 5	UCS-A/eth-storage/fabric# **exit**	ファブリックを終了します。
ステップ 6	UCS-A/eth-storage# **scope vlan** *vlan-name*	指定された VLAN を入力します。 （注） コミュニティ VLAN がアプライアンスのクラウドで作成されていることを確認します。
ステップ 7	UCS-A/eth-storage/vlan# **create member-port** *fabric slot-num port-num*	指定したファブリックのメンバ ポートを作成し、スロット番号、およびポート番号を割り当て、メンバ ポートの設定を開始します。
ステップ 8	UCS-A/eth-storage/vlan/member-port# **commit**	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、コミュニティ VLAN にアプライアンス ポートをマッピングします。

```
UCS-A# scope eth-storage
UCS-A/eth-storage# scope fabric a
UCS-A/eth-storage/fabric# create interface 1 22
UCS-A/eth-storage/fabric/interface*# exit
UCS-A/eth-storage/fabric*# exit
UCS-A/eth-storage*# scope vlan COM602
UCS-A/eth-storage/vlan*# create member-port a 1 22
UCS-A/eth-storage/vlan/member-port* commit
```

アプライアンス ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **delete eth-interface** *slot-num port-num*	指定したアプライアンス ポートのインターフェイスを削除します。
ステップ 4	UCS-A /eth-storage/fabric # **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、ファブリック B のスロット 2 のアプライアンス ポート 3 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric b
UCS-A /eth-storage/fabric # delete eth-interface 2 3
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

FCoE アップリンク ポート

FCoE アップリンク ポートは、FCoE トラフィックの伝送に使用される、ファブリック インターコネクトとアップストリーム イーサネット スイッチ間の物理イーサネット インターフェイス

です。このサポートにより、同じ物理イーサネット ポートで、イーサネット トラフィックとファイバ チャネル トラフィックの両方を伝送できます。

FCoE アップリンク ポートはファイバ チャネル トラフィック用の FCoE プロトコルを使用してアップストリーム イーサネット スイッチに接続します。これにより、ファイバ チャネル トラフィックとイーサネット トラフィックの両方が同じ物理イーサネット リンクに流れることができます。

（注） FCoE アップリンクとユニファイドアップリンクは、ユニファイドファブリックをディストリビューション レイヤ スイッチまで拡張することによりマルチホップ FCoE 機能を有効にします。

次のいずれかと同じイーサネット ポートを設定できます。

- [FCoE uplink port]：ファイバ チャネル トラフィック専用の FCoE アップリンク ポートとして。
- [Uplink port]：イーサネット トラフィック専用のイーサネット ポートとして。
- [Unified uplink port]：イーサネットとファイバ チャネル両方のトラフィックを伝送するユニファイド アップリンク ポートとして。

FCoE アップリンク ポートの設定

リストされている全ポートタイプは、固定および拡張モジュールで構成可能です。これには、6100 シリーズファブリック インターコネクトの拡張モジュールでは設定できないものの、6200 シリーズ ファブリック インターコネクトの拡張モジュールでは設定できるサーバ ポートを含みます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric**{**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create fcoeinterface** *slot-numberport-number*	指定した FCoE アップリンク ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **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、ファブリック A のスロット 8 で FCoE アップリンク ポート 1 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create fcoeinterface 1 8
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

FCoE アップリンク ポートの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **show fcoeinterface**	使用可能なインターフェイスを一覧表示します。

例

次に、ファブリック A で使用可能な FCoE アップリンク インターフェイスを表示する例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # show fcoeinterface
FCoE Interface:

Slot Id    Port Id    Admin State Operational State Operational State Reason  Li
c State            Grace Prd
---------- ---------- ----------- ----------------- ------------------------- --
------------------ ---------
         1         26 Enabled     Indeterminate                               Li
cense Ok                    0

Fcoe Member Port:

Port-channel Slot  Port  Oper State      State Reason
------------ ----- ----- --------------- ------------
1                1    10 Sfp Not Present Unknown
1                1     3 Sfp Not Present Unknown
1                1     4 Sfp Not Present Unknown
1                1     6 Sfp Not Present Unknown
1                1     8 Sfp Not Present Unknown
2                1     7 Sfp Not Present Unknown
UCS-A /fc-uplink/fabric #
```

FCoE アップリンク ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **delete fcoeinterface** *slot-numberport-number*	指定したインターフェイスを削除します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **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

以下に、ファブリック A のスロット 8 のポート 1 上の FCoE アップリンク インターフェイスを削除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # delete fcoeinterface 1 8
UCS-A /fc-uplink/fabric/fcoeinterface* # commit-buffer
UCS-A /fc-uplink/fabric/fcoeinterface #
```

FCoE およびファイバ チャネル ストレージ ポート

ファイバ チャネル ストレージまたは FCoE ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **create interface** {**fc** | **fcoe**} *slot-num port-num*	指定されたファイバ チャネル ストレージ ポートのインターフェイスを作成します。

	コマンドまたはアクション	目的
		Cisco UCS 6454 ファブリック インターコネクトでは、ポート 49 ～ 54 を FCoE ストレージ ポートとして設定することはできません。
ステップ 4	UCS-A /fc-storage/fabric # **commit-buffer**	トランザクションをコミットします。

例

次の例は、ファブリック A スロット 2 のファイバ チャネル ストレージ ポート 10 のインターフェイスを作成し、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
UCS-A /fc-storage/fabric* # create interface fc 2 10
UCS-A /fc-storage/fabric # commit-buffer
```

次のタスク

VSAN を割り当てます。

ファイバ チャネル ストレージまたは FCoE ポートの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **delete interface** {**fc** | **fcoe**} *slot-num port-num*	指定したファイバ チャネル ストレージ ポートまたは FCoE ストレージ ポートのインターフェイスを削除します。
ステップ 4	UCS-A /fc-storage/fabric # **commit-buffer**	トランザクションをコミットします。

例

次に、ファブリック A のスロット 2 のファイバ チャネル ストレージ ポート 10 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # scope fabric a
```

```
UCS-A /fc-storage/fabric* # delete interface fc 2 10
UCS-A /fc-storage/fabric # commit-buffer
```

アップリンク ファイバ チャネル ポートへのファイバ チャネル ストレージ ポートの復元

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックでファイバ チャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create interface** *slot-num port-num*	指定したファイバ チャネル アップリンク ポートのインターフェイスを作成します。
ステップ 4	UCS-A /fc-uplink/fabric # **commit-buffer**	トランザクションをコミットします。

例

次に、ファブリック A のスロット 2 でファイバ チャネル アップリンク ポート 10 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric* # create interface 2 10
UCS-A /fc-uplink/fabric # commit-buffer
```

アプライアンス ポート チャネル

アプライアンス ポート チャネルを使用すると、複数の物理的なアプライアンス ポートをグループ化して 1 つの論理的なイーサネット ストレージ リンクを作成し、耐障害性と高速接続を実現できます。Cisco UCS Manager において、先にポート チャネルを作成してから、そのポート チャネルにアプライアンス ポートを追加します。1 つのポート チャネルには、最大で 8 個のアプライアンス ポートを追加できます。

アプライアンス ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **create port-channel** ポート番号	指定されたイーサネット ストレージ ポートのポート チャネルを作成し、イーサネット ストレージ ファブリック ポート チャネル モードを開始します。
ステップ 4	（任意） UCS-A /eth-storage/fabric/port-channel # {**enable** | **disable**}	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	（任意） UCS-A /eth-storage/fabric/port-channel # **set name** *port-chan-name*	ポート チャネルの名前を指定します。
ステップ 6	（任意） UCS-A /eth-storage/fabric/port-channel # **set pingroupname** *pin-group name*	指定されたファブリックとポート、またはファブリックとポート チャネルへのアプライアンス ピン ターゲットを指定します。
ステップ 7	（任意） UCS-A /eth-storage/fabric/port-channel # **set portmode** {**access** | **trunk**}	ポート モードがアクセスとトランクのどちらであるかを指定します。デフォルトで、モードはトランクに設定されます。
ステップ 8	（任意） UCS-A /eth-storage/fabric/port-channel # **set prio** *sys-class-name*	アプライアンス ポートに QoS クラスを指定します。デフォルトでは、プライオリティは best-effort に設定されます。 sys-class-name 引数には、次のいずれかのクラス キーワードを指定できます。 • **[C]**：vHBA トラフィックのみを制御する QoS ポリシーにこのプライオリティを使用します。

	コマンドまたはアクション	目的
		• **[プラチナ（Platinum）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ゴールド（Gold）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[シルバー（Silver）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ブロンズ（Bronze）]**：vNIC トラフィックだけを制御する QoS ポリシーにこの優先順位を使用します。 • **[ベストエフォート（Best Effort）]**：この優先順位は使用しないでください。ベーシック イーサネット トラフィック レーンのために予約されています。この優先順位を QoS ポリシーに割り当てて、別のシステム クラスを CoS 0 に設定した場合、Cisco UCS Managerはこのシステム クラスのデフォルトを使用しません。そのトラフィックに対しては、優先度がデフォルト（CoS 0）になります。
ステップ 9	（任意） UCS-A /eth-storage/fabric/port-channel # **set speed** {**1gbps** | **2gbps** | **4gbps** | **8gbps** | **auto**}	ポート チャネルの速度を指定します。
ステップ 10	UCS-A /eth-storage/fabric/port-channel # **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、ファブリック A のポート 13 にポート チャネルを作成し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # create port-channel 13
UCS-A /eth-storage/fabric/port-channel* # enable
UCS-A /eth-storage/fabric/port-channel* # set name portchan13a
UCS-A /eth-storage/fabric/port-channel* # set pingroupname pingroup1
UCS-A /eth-storage/fabric/port-channel* # set portmode access
UCS-A /eth-storage/fabric/port-channel* # set prio fc
UCS-A /eth-storage/fabric/port-channel* # set speed 2gbps
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **delete port-channel** ポート番号	指定したイーサネット ストレージ ポートからポート チャネルを削除します。
ステップ 4	UCS-A /eth-storage/fabric # **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、ファブリック A のポート 13 のポート チャネルを設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # delete port-channel 13
UCS-A /eth-storage/fabric* # commit-buffer
UCS-A /eth-storage/fabric #
```

アプライアンス ポート チャネルのイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b** }	指定したファブリックのイーサネット ストレージ モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** *port-chan-name*	イーサネット ストレージ ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # {**enable** | **disable** }	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **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、ファブリック A のポート チャネル 13 を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel* # enable
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ 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 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** ポート番号	指定されたポートチャネルのイーサネット ストレージファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-storage/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、イーサネットストレージ ファブリック ポート チャネルのメンバ ポート モードを開始します。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **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、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート 13 のポート チャネルに追加し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel # create member-port 1 7
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

アプライアンス ポート チャネルからのメンバ ポートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-storage**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A /eth-storage # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット ストレージ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-storage/fabric # **scope port-channel** ポート番号	指定されたポートチャネルのイーサネット ストレージファブリック ポート チャネル 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 4	UCS-A /eth-storage/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。
ステップ 5	UCS-A /eth-storage/fabric/port-channel # **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、ファブリック A のポート 13 のポート チャネルからメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope eth-storage
UCS-A /eth-storage # scope fabric a
UCS-A /eth-storage/fabric # scope port-channel 13
UCS-A /eth-storage/fabric/port-channel # delete member-port 1 7
UCS-A /eth-storage/fabric/port-channel* # commit-buffer
UCS-A /eth-storage/fabric/port-channel #
```

ファイバ チャネル ポート チャネル

ファイバ チャネル ポート チャネルによって、複数の物理ファイバ チャネル ポートをグループ化して（リンク集約）、1 つの論理ファイバ チャネル リンクを作成し、耐障害性と高速接続性を提供することができます。Cisco UCS Manager では、先にポート チャネルを作成してから、そのポート チャネルにファイバ チャネル ポートを追加します。

（注） ファイバ チャネル ポートのチャネルは、シスコ以外のテクノロジーとの互換性がありません。

Cisco UCS 6200、6300、およびCisco UCS 6454 ファブリック インターコネクトシリーズファブリックインターコネクトでは、各 Cisco UCS ドメインに最大4つのファイバチャネルポートチャネルを作成できます。各ファイバ チャネル ポート チャネルには、最大 16 のアップリンク ファイバ チャネル ポートを含めることができます。

各 Cisco UCS ドメインには、Cisco UCS 6324 シリーズのファブリック インターコネクトを使用して、最大 2 つのファイバ チャネル ポートのチャネルを作成できます。各ファイバ チャネル ポート チャネルには、最大 4 つのアップリンク ファイバ チャネル ポートを含めることができます。

アップストリーム NPIV スイッチ上のファイバ チャネル ポート チャネルのチャネル モードが**アクティブ**に設定されていることを確認してください。メンバー ポートとピア ポートに同じチャネル モードが設定されていない場合、ポート チャネルはアップ状態になりません。チャネル モードが**アクティブ**に設定されている場合、ピア ポートのチャネル グループ モードに関係なく、メンバー ポートはピア ポートとのポート チャネル プロトコル ネゴシエーションを開

始します。チャネル グループで設定されているピア ポートがポート チャネル プロトコルをサポートしていない場合、またはネゴシエーション不可能なステータスを返す場合、デフォルトでオン モードの動作に設定されます。**アクティブ** ポート チャネル モードでは、各端でポート チャネル メンバー ポートを明示的にイネーブルおよびディセーブルに設定することなく自動リカバリが可能です。

この例は、チャネル モードをアクティブに設定する方法を示しています。

```
switch(config)# int po114
switch(config-if)# channel mode active
```

ファイバ チャネル ポート チャネルの設定

（注） 2 つのファイバ チャネル ポート チャネルに接続する場合、両方のポート チャネルの管理速度が、使用するリンクに一致している必要があります。いずれかまたは両方のファイバチャネル ポート チャネルの管理速度が auto に設定されている場合、Cisco UCS が管理速度を自動的に調整します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create port-channel** ポート番号	指定されたファイバ チャネル アップリンク ポートのポート チャネルを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	（任意） UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable**}	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	（任意） UCS-A /fc-uplink/fabric/port-channel # **set name** ポート チャネル名	ポート チャネルの名前を指定します。

	コマンドまたはアクション	目的
ステップ 6	（任意） UCS-A /fc-uplink/fabric/port-channel # **set speed** {**1gbps** | **2gbps** | **4gbps** | **8gbps** | **auto**}	ポート チャネルの速度を指定します。
ステップ 7	UCS-A /fc-uplink/fabric/port-channel # **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、ファブリック A にポート チャネル 13 を作成し、名前を portchan13a に設定し、管理状態を有効にし、速度を 2 Gbps の設定し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # set name portchan13a
UCS-A /fc-uplink/fabric/port-channel* # set speed 2gbps
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルの設定解除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **delete port-channel** ポート番号	指定したファイバ チャネル アップリンク ポートのポート チャネルを削除します。
ステップ 4	UCS-A /fc-uplink/fabric # **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、ファブリック A のポート チャネル 13 を設定解除し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # delete port-channel 13
UCS-A /fc-uplink/fabric* # commit-buffer
UCS-A /fc-uplink/fabric #
```

アップストリーム NPIV のファイバ チャネル ポート チャネルへのチャネル モード アクティブの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create port-channel** ポート番号	指定されたファイバ チャネル アップリンク ポートのポート チャネルを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	（任意） UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable**}	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。
ステップ 5	（任意） UCS-A /fc-uplink/fabric/port-channel # **set name** ポート チャネル名	ポート チャネルの名前を指定します。
ステップ 6	（任意） UCS-A /fc-uplink/fabric/port-channel # **scope** ポート チャネル名	ポート チャネルの名前を指定します。
ステップ 7	（任意） UCS-A /fc-uplink/fabric/port-channel # **channel mode** {**active**}	アップストリーム NPIV スイッチのチャネルモードを有効にします。
ステップ 8	UCS-A /fc-uplink/fabric/port-channel # **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、チャネルモードをアクティブにする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create port-channel 13
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # set name portchan13a
UCS-A /fc-uplink/fabric/port-channel* # channel mode active
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel # exit
UCS-A /fc-uplink/fabric/ # show port-channel database

portchan13a
    Administrative channel mode is active
    Operational channel mode is active

UCS-A /fc-uplink/fabric/ #
```

ファイバ チャネル ポート チャネルのイネーブル化またはディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックでファイバ チャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** ポート チャネル名	ファイバ チャネル アップリンク ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # {**enable** | **disable** }	ポート チャネルの管理状態をイネーブルまたはディセーブルにします。ポート チャネルは、デフォルトではディセーブルです。

例

次に、ファブリック A のポート チャネル 13 を有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
```

```
UCS-A /fc-uplink/fabric/port-channel* # enable
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** ポート番号	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **create member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを作成し、ファイバ チャネル アップリンク ファブリック ポート チャネル メンバ ポート モードを開始します。
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **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、スロット 1、ポート 7 のメンバ ポートをファブリック A のポート チャネル 13 に追加し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric # create member-port 1 7
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

ファイバ チャネル ポート チャネルからのメンバ ポートの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope port-channel** ポート番号	指定されたポート チャネルのファイバ チャネル アップリンク ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/port-channel # **delete member-port** *slot-num port-num*	ポート チャネルから指定されたメンバ ポートを削除します。
ステップ 5	UCS-A /fc-uplink/fabric/port-channel # **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、ファブリック A ポート チャネル 13 からメンバ ポートを削除し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope port-channel 13
UCS-A /fc-uplink/fabric # delete member-port 1 7
UCS-A /fc-uplink/fabric/port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/port-channel #
```

組織固有識別子の構成

Cisco Fibre Channel（FC）ポート チャネルは、ポート チャネルの両端にあるデバイスの組織固有識別子（OUI）に依存して設定されています。新しいデバイスがリリースされるか、OUI プールが枯渇したために新しいOUI範囲が既存のデバイスに割り当てられた場合、ポート チャネルを正常に設定するには、新しい OUI をそれぞれの OUI テーブルに追加する必要があります。

OUI の追加

新しい Cisco FC デバイスまたは新しく割り当てられた OUI 範囲を持つデバイスで FC ポート チャネルを確立するには、Cisco UCSM CLI から次のコマンドを使用して、OUI をデータベースに手動で追加します。

```
FI-A # sc fabric-interconnect {a|b}
FI-A /fabric-interconnect # sc oui-pool default
FI-A /fabric-interconnect/oui-pool # sh oui
FI-A /fabric-interconnect/oui-pool # create oui [oui-id]
FI-A /fabric-interconnect/oui-pool/oui* # commit-buffer
```

ここで、`oui-id` は、追加する必要があるデバイスの新しい OUI です。デバイス OUI は、8 桁の 16 進数である必要があります。OUI の有効範囲は 0x000000 ～ 0xffffff です。例えば 0xabcdef です。

OUI の表示

OUI のリストを表示するには、次のコマンドを実行します。

```
FI-A /fabric-interconnect/oui-pool# show oui
```

次の例は、`show oui` コマンドのサンプル出力を示しています。

```
FI-A /fabric-interconnect/oui-pool# show oui

OUI Entry:
Oui
---
0x0001ac
0x1b0000
0xaabbcc
0xddeeff
```

OUI の削除

OUI を削除するには、次のコマンドを実行します。

```
FI-A /fabric-interconnect/oui-pool# delete ouientry [oui-id]
```

ここで、oui-id は、削除する必要があるデバイスの OUI です。

FCoE ポート チャネル数

FCoE ポート チャネルでは、複数の物理 FCoE ポートをグループ化して 1 つの論理 FCoE ポート チャネルを作成できます。物理レベルでは、FCoE ポート チャネルは FCoE トラフィックをイーサネット ポート チャネル経由で転送します。したがって、一連のメンバから構成される FCoE ポート チャネルは基本的に同じメンバから構成されるイーサネット ポート チャネルです。このイーサネット ポート チャネルは、FCoE トラフィック用の物理トランスポートとして使用されます。

各 FCoE ポート チャネルに対し、 Cisco UCS Manager は VFC を内部的に作成し、イーサネット ポート チャネルにバインドします。ホストから受信した FCoE トラフィックは、FCoE トラフィックがファイバ チャネル アップリンク経由で送信されるのと同じ方法で、VFC 経由で送信されます。

FCoE ポート チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	特定のファブリックに対して FC - アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create fcoe-port-channel** *number*	指定した FCoE アップリンク ポートのポート チャネルを作成します。
ステップ 4	UCS-A /fc-uplink/fabric/fabricinterface # **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、ファブリック A のスロット 4 で FCoE アップリンク ポート 1 のインターフェイスを作成し、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create fcoe-port-channel 4
UCS-A /fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel #
```

FCoE アップリンク ポート チャネルへのメンバ ポートの追加

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックのファイバ チャネル アップリンク ファブリック モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope fcoe-port-channel** *ID*	指定したポート チャネルの FCoE アップリンク ポート チャネル モードを開始します。
ステップ 4	UCS-A /fc-uplink/fabric/fcoe-port-channel # **create member-port** スロット番号 ポート番号	ポート チャネルから指定されたメンバ ポートを作成し、FCoE アップリンク

	コマンドまたはアクション	目的
		ファブリック ポート チャネルのメンバ ポート モードを開始します。 （注） FCoE アップリンク ポート チャネルが、ユニファイド アップリンク ポート チャネルである場合、次のメッセージが表示されます。 警告: これがユニファイド ポート チャネルの場合、メンバは同じ ID のイーサネット ポート チャネルにも追加されます。
ステップ 5	UCS-A /fc-uplink/fabric/fcoe-port-channel # **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、スロット 1、ポート 7 のメンバ ポートをファブリック A の FCoE ポート チャネル 13 に追加し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope fcoe-port-channel 13
UCS-A /fc-uplink/fabric # create member-port 1 7
UCS-A /fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCS-A /fc-uplink/fabric/fcoe-port-channel #
```

アダプタ ポート チャネル

アダプタ ポート チャネルは、Cisco UCS 仮想インターフェイス カード（VIC）から I/O へのすべての物理リンクを 1 つの論理リンクにグループ化します。

アダプタ ポート チャネルは、正しいハードウェアの存在を検出したときに Cisco UCS Manager によって内部的に作成また管理されます。アダプタ ポート チャネルの手動設定はできません。アダプタ ポート チャネルは、Cisco UCS Manager GUI または Cisco UCS Manager CLI を使用して表示可能です。

アダプタ ポート チャネルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope iom** {**a b**}	指定した IOM でシャーシ IOM モードを開始します。
ステップ 3	UCS-A /chassis/iom # **scope port group**	指定したポート グループでポート グループ モードを開始します。
ステップ 4	UCS-A /chassis/iom/port group # **show host-port-channel** [**detail** |**expand**]	指定したシャーシのアダプタ ポート チャネルを表示します。

例

次に、ポート グループ モードでホスト ポート チャネルに関する情報を表示する例を示します。

```
UCS-A # scope chassis 1
UCS-A /chassis # scope iom a
UCS-A /chassis/iom # scope port group
UCS-A /chassis/iom/port group # show host-port-channel

Host Port channel:

  Port Channel Id Fabric ID Oper State       State Reason
    --------------- --------- ---------------- ------------
                1289 B         Up
                1290 B         Up
                1306 B         Up
                1307 B         Up
                1309 B         Up
                1315 B         Up

UCS-A /chassis/iom/port group #
```

イベント検出とアクション

Cisco UCS Manager は、I/O モジュール（IOM）からファブリック インターコネクトに接続されたネットワーク インターフェイスにエラーが発生した場合にアラームを監視およびトリガーする統計情報収集ポリシーを使用します。

ネットワーク インターフェイス ポートのエラー統計情報は NiErrStats と呼ばれ、次のエラーで構成されています。

NiErrStats のエラー名	説明
frameTx	TX_FRM_ERROR のカウンタ値を収集します。
tooLong	RX_TOOLONG のカウンタ値を収集します。
tooShort	RX_UNDERSIZE と RX_FRAGMENT のカウンタ値の合計を収集します。
Crc	RX_CRERR_NOT_STOMPED と RX_CRCERR_STOMPED のカウンタ値の合計を収集します。
inRange	RX_INRANGEERR のカウンタ値を収集します。

（注） ネットワーク インターフェイス ポートの統計情報はアクティブ ポートからのみ収集され、その統計情報は Cisco UCS Manager に送信されます。

ポリシーベースのポート エラー処理

Cisco UCS Manager がアクティブな NI ポートでエラーを検出し、エラー ディセーブル機能がイネーブルの場合、Cisco UCS Manager はエラーが発生した NI ポートに接続されているそれぞれの FI ポートを自動的にディセーブルにします。FI ポートがエラー ディセーブルになっているときは事実上シャットダウンし、トラフィックはポートで送受信されません。

エラー ディセーブル機能は、次の 2 つの目的で使用されます。

- どの FI ポートが error-disabled になっているかということと、接続されている NI ポートでエラーが発生したことを通知します。
- このポートが原因で同じシャーシ/FEX に接続された他のポートに障害が発生する可能性を削除します。このような障害は、NI ポートのエラーによって発生する可能性があり、最終的に重大なネットワーク上の問題を引き起こす可能性があります。エラーディセーブル機能は、この状況を回避するのに役立ちます。

しきい値定義の作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ 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 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **create class** クラス名	指定された統計情報しきい値ポリシー クラスを作成し、組織統計情報しきい値ポリシー クラス モードを開始します。使用可能なクラス名キーワードのリストを表示するには、 **create class ?** コマンドを組織しきい値ポリシー モードで入力します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **create property** プロパティ名	指定された統計情報しきい値ポリシー クラス プロパティを作成し、組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。使用可能なプロパティ名キーワードのリストを表示するには、 **create property ?** コマンドを組織しきい値ポリシー モードで入力します。
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set normal-value** 値	クラス プロパティに通常値を指定します。*value* の形式は、設定しているクラス プロパティによって異なる場合があります。必要な形式を確認するには、 **set normal-value ?** コマンドを組織統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property # **create threshold-value** {*above-normal* | *below-normal*} {*cleared* | *condition* | *critical* | *info* | *major* | *minor* | *warning*}	クラス プロパティに、指定したしきい値を作成し、組織統計情報しきい値ポリシー クラス プロパティしきい値モードを開始します。
ステップ 7	UCS-A/eth-server/stats-threshold-policy/class/property/threshold-value # **set** {**deescalating** | **escalating**} 値	降格および昇格のクラス プロパティしきい値を指定します。*value* の形式は、設定されているクラス プロパティしきい値によって異なる場合があります。必要な形式を確認するには、**set deescalating ?** または **set escalating ?** コマンドを組織統計情報しきい値ポリシー クラス プロパティ モードで入力します。
ステップ 8	UCS-A/eth-server/stats-threshold-policy/class/property/threshold-value # **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、しきい値定義を作成する例を示します。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # create class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class* # create property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property* # set normal-value 0
UCS-A /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal major
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set escalating
 5
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # set deescalating
 3
UCS-A /eth-server/stats-threshold-policy/class/property/threshold-value* # commit-buffer
```

ファブリック インターコネクト ポートにエラー無効を設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **scope class** クラス名	指定した統計情報しきい値ポリシー クラスの組織統計情報しきい値ポリシー クラス モードを開始します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **scope property** プロパティ名	指定した統計情報しきい値ポリシー クラス プロパティの組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set error-disable-fi-port** {**yes** | **no**}	クラス プロパティにエラー ディセーブル化ステータスを指定します。 クラス プロパティのエラー ディセーブル化を無効にするには、**no** オプションを使用します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property* # **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、FI ポートでエラー ディセーブル化を有効にする方法を示しています。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # scope class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class # scope property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property # set error-disable-fi-port yes
UCS-A /eth-server/stats-threshold-policy/class/property* # commit-buffer
```

ファブリック インターコネクト ポートに自動リカバリを設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope eth-server**	イーサネット ストレージ モードを開始します。
ステップ 2	UCS-A/eth-server # **scope stats-threshold-policy default**	統計情報しきい値ポリシー モードを開始します。
ステップ 3	UCSA/eth-server/stats-threshold-policy # **scope class** クラス名	指定した統計情報しきい値ポリシー クラスの組織統計情報しきい値ポリシー クラス モードを開始します。
ステップ 4	UCS-A/eth-server/stats-threshold-policy/class # **scope property** プロパティ名	指定した統計情報しきい値ポリシー クラス プロパティの組織統計情報しきい値ポリシー クラス プロパティ モードを開始します。
ステップ 5	UCS-A/eth-server/stats-threshold-policy/class/property # **set auto-recovery** {**enabled** | **disabled**}	クラス プロパティに自動リカバリ ステータスを指定します。 クラスプロパティの自動リカバリをディセーブルにするには、**disabled** オプションを使用します。
ステップ 6	UCS-A/eth-server/stats-threshold-policy/class/property* # **set auto-recovery-time** 時間	ポートが自動的に再びイネーブルになるまでの時間（分単位）を指定します。自動リカバリの時間は、0 ～ 4294967295 分の間で変更できます。
ステップ 7	UCS-A/eth-server/stats-threshold-policy/class/property* # **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、FI ポートに自動リカバリを設定する方法を示しています。

```
UCS-A # scope eth-server
UCS-A /eth-server # scope stats-threshold-policy default
UCS-A /eth-server/stats-threshold-policy # scope class ni-ether-error-stats
UCS-A /eth-server/stats-threshold-policy/class # scope property crc-delta
UCS-A /eth-server/stats-threshold-policy/class/property # set auto-recovery enabled
UCS-A /eth-server/stats-threshold-policy/class/property* # set auto-recovery-time 5
UCS-A /eth-server/stats-threshold-policy/class/property* # commit-buffer
```

ネットワーク インターフェイス ポートのエラー カウンタの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** シャーシ番号	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A/chassis # **scope iom** {**a** |**b**}	指定した IOM でシャーシ IOM モードを開始します。
ステップ 3	UCS-A/chassis/iom # **scope port-group fabric**	ネットワーク インターフェイス ポートを入力します。
ステップ 4	UCS-A/chassis/iom/port-group # **scope fabric-if** *fabric-if number*	指定されたネットワーク インターフェイスのポート番号を入力します。
ステップ 5	UCS-A/chassis/iom/port-group/fabric-if # **show stats**	ネットワーク インターフェイス ポートのエラー カウンタを表示します。

例

次の例は、ネットワーク インターフェイス ポートの統計情報を表示する方法を示しています。

```
UCS-A # scope chassis 1
UCS-A/chassis # scope iom a
UCS-A/chassis/iom # scope port-group fabric
UCS-A/chassis/iom/port-group # scope faric-if 1
UCS-A/chassis/iom/port-group/fabric-if # show stats
NI Ether Error Stats:
Time Collected: 2014-08-20T15:37:24:688
Monitored Object: sys/chassis-1/slot-1/fabric/port-1/ni-err-stats
Suspect: Yes
Crc (errors): 5000
Frame Tx (errors): 0
```

```
Too Long (errors): 0
Too Short (errors): 0
In Range (errors): 0
Thresholded: 0
```

ファブリック ポート チャネル

ファブリック ポート チャネルは、冗長性と帯域幅共有のため、IOM からファブリック インターコネクトへの複数の物理リンクを 1 個の論理リンクにグループ化できます。ファブリック ポート チャネル内の 1 個のリンクがアクティブである限り、ファブリック ポート チャネルは動作し続けます。

正しいハードウェアが接続されている場合、ファブリック ポート チャネルは Cisco UCS Manager で次のように作成されます。

- シャーシ ディスカバリ ポリシーで定義した設定に従って、シャーシを検出している最中に。
- 特定のシャーシのシャーシ接続ポリシーに設定された内容に従って、シャーシを検出した後に。

IOM のそれぞれに単一のファブリック ポート チャネルがあります。ファブリック インターコネクトに IOM を接続する各アップリンクは、個別リンクとして設定することもポート チャネルに含めることもできますが、1 つのアップリンクが複数のファブリック ポート チャネルに属することはできません。たとえば、2 つの IOM を持つシャーシが検出され、ファブリック ポート チャネルを作成するようにシャーシ ディスカバリ ポリシーが設定されている場合、Cisco UCS Manager は 2 つの独立したファブリック ポート チャネルを作成します。IOM-1 を接続するアップリンク用と、IOM-2 を接続するアップリンク用です。別のシャーシはこれらのファブリック ポート チャネルに加入できません。同様に、IOM-1 のファブリック ポート チャネルに属するアップリンクは、IOM-2 のファブリック ポート チャネルに加入できません。

ポート間のロード バランシング

IOM とファブリック インターコネクトの間にあるポート間のトラフィックに対するロード バランシングでは、ハッシュに次の基準を使用します。

- イーサネット トラフィックの場合：

  レイヤ 2 送信元アドレスおよび宛先アドレス

  レイヤ 3 送信元アドレスおよび宛先アドレス

  レイヤ 4 送信元ポートおよび宛先ポート

- FCoE トラフィックの場合：

  レイヤ 2 送信元アドレスおよび宛先アドレス

  送信元と宛先の ID（SID と DID）および Originator eXchange ID（OXID）

この例では、2200 シリーズ IOM モジュールは iom *X*（*X* はシャーシ番号）の接続によって確認されます。

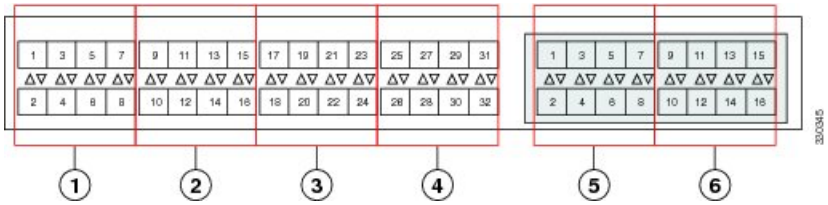
```
show platform software fwmctrl nifport
(....)
 Hash Parameters:
   l2_da: 1 l2_sa: 1 l2_vlan: 0
   l3_da: 1 l3_sa: 1
   l4_da: 1 l4_sa: 1
   FCoE l2_da: 1 l2_sa: 1 l2_vlan: 0
   FCoE l3_did: 1 l3_sid: 1 l3_oxid: 1
```

ファブリック ポート チャネルのケーブル接続の考慮事項

Cisco UCS 2200 シリーズ FEX と Cisco UCS 6200 シリーズ ファブリック インターコネクト間のリンクをファブリック ポート チャネル モードで設定する際、アダプタ上の使用可能な仮想インターフェイス（VIF）ネームスペースはその FEX のアップリンクがファブリック インターコネクト ポートに接続されている場所によって異なります。

6248 ファブリック インターコネクト内には、8 個の連続ポートが 6 セットあり、ポートのセットのそれぞれがシングル チップによって管理されます。FEX からのすべてのアップリンクが 1 つのチップによって管理される一連のポートに接続されると、Cisco UCS Managerはシャーシ内のブレードで展開されているサービス プロファイルで使用する VIF の数を最大化します。アップリンク接続が個別のチップで管理される複数のポートに分散している場合、VIF の数は少なくなります。

図 *2:* ファブリック ポート チャネルのポート グループ



注意 ファブリック ポート チャネルのポート グループに 2 番目のリンクを追加すると、混乱が生じ、VIF ネームスペースの使用可能な容量が、63 から 118 まで自動的に増加します。さらにリンクを追加しても混乱は生じないため、VIF ネームスペースは 118 のままになります。

注意 2 つのファブリック ポート チャネル ポート グループにシャーシをリンクしても、VIF ネームスペースは、手動で確認されないかぎり影響を受けません。その結果、VIF ネームスペースは 2 つのグループのうち、より小さいサイズのファブリック ポート チャネル ポート グループを使用するように自動的に設定されます（63 または 118 の VIF）。

ハイ アベイラビリティのクラスタ モード アプリケーションの場合、対称なケーブル設定を強く推奨します。ケーブル接続が非対称の場合、使用可能な VIF の最大数は 2 つのケーブル設定より小さくなります。

Cisco UCS 環境の VIF の最大数については、ご使用のハードウェアおよびソフトウェア設定用の設定制限についてのマニュアルを参照してください。

ファブリック ポート チャネルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **show fabric-port-channel** [**detail** | **expand**]	指定したファブリック インターコネクトのファブリック ポート チャネルを表示します。

例

次に、ファブリック インターコネクト A の設定済みファブリック ポート チャネルに関する情報を表示する例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # show fabric-port-channel
Fabric Port Channel:
    Port Channel Id Chassis Id Admin State Oper State       State Reason
    --------------- ---------- ----------- ---------------- ------------
               1025 1          Enabled     Failed           No operational members
               1026 2          Enabled     Up

UCS-A /eth-server/fabric #
```

ファブリック ポート チャネル メンバー ポートのイネーブル化またはディセーブル化

手順

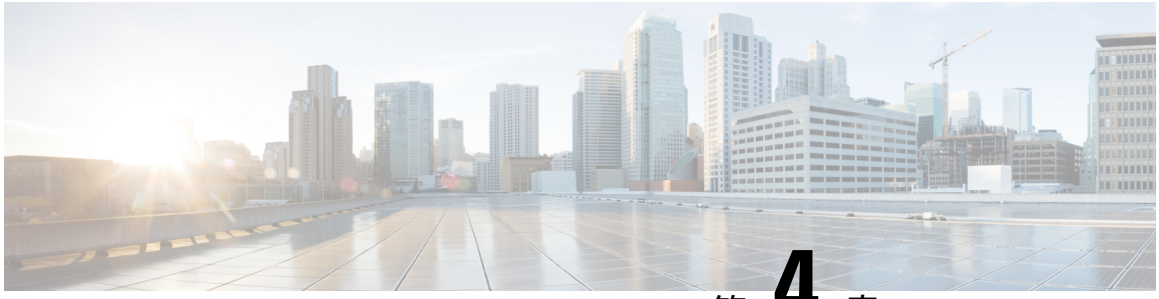
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope eth-server**	イーサネット サーバ モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /eth-server # **scope fabric** {**a** | **b**}	指定したファブリックのイーサネット サーバ ファブリック モードを開始します。
ステップ 3	UCS-A /eth-server/fabric # **scope fabric-port-channel** ポート チャネル *ID*	指定したファブリックでイーサネット サーバ ファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 4	UCS-A /eth-server/fabric/fabric-port-channel # **scope member-port** スロット *ID* ポート *ID*	指定したメンバー ポートでイーサネット サーバ ファブリック、ファブリック ポート チャネル モードを開始します。
ステップ 5	UCS-A /eth-server/fabric/fabric-port-channel # {**enable** | **disable**}	指定したメンバ ポートをイネーブルまたはディセーブルにします。
ステップ 6	UCS-A /eth-server/fabric/fabric-port-channel # **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、ファブリック ポート チャネル 1025 のファブリック チャネル メンバー ポート 1 31 をディセーブルにし、トランザクションをコミットする例を示します。

```
UCS-A# scope eth-server
UCS-A /eth-server # scope fabric a
UCS-A /eth-server/fabric # scope fabric-port-channel 1025
UCS-A /eth-server/fabric/fabric-port-channel # scope member-port 1 31
UCS-A /eth-server/fabric/fabric-port-channel/member-port # disable
UCS-A /eth-server/fabric/fabric-port-channel/member-port* # commit-buffer
UCS-A /eth-server/fabric/fabric-port-channel/member-port #
```



第 4 章

ファイバ チャネルのゾーン分割

ファイバ チャネル ゾーン分割に関する情報

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

（注） ファイバチャネルゾーニングは、次ではサポートされていません。 Cisco UCS 6454 ファブリック インターコネクト

ゾーン分割がもたらすアクセス制御とデータ トラフィック制御によって以下が可能になります。

- SAN ネットワーク セキュリティの強化

- データ損失や破損の防止
- パフォーマンス問題の軽減

ゾーンに関する情報

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

- ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
- ゾーンのサイズを変更できます。
- デバイスは複数のゾーンに所属できます。
- 1 つの物理ファブリックに最大 8,000 ゾーンを収容できます。

ゾーン セットに関する情報

各ゾーン セットは、1 つまたは複数のゾーンから構成されます。ゾーン セットを使用して、ファイバ チャネル ファブリック内でアクセス制御を実行することができます。また、ゾーン セットには次のような利点があります。

- アクティブにできるのは、常に 1 つのゾーン セットだけです。
- ゾーン セット内のすべてのゾーンは、ファブリック内のスイッチ全体で単一のエンティティとしてアクティブまたは非アクティブにできます。
- ゾーン セットへの変更は、ゾーン セットがアクティブになるまで適用されません。アクティブなゾーン セットに変更を加える場合は、変更を適用するためにそのゾーン セットを再アクティブ化する必要があります。
- 1 つのゾーンを 複数のゾーン セットのメンバにできます。
- ゾーン内の各スイッチは最大 500 のゾーン セットを持つことができます。

Cisco UCS Manager でのファイバ チャネル ゾーン分割のサポート

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

- Cisco UCS Manager-ベースのファイバ チャネル ゾーン分割：この設定は、直接接続ストレージとローカル ゾーン分割の組み合わせです。ファイバ チャネルまたは FCoE のスト

レージはファブリック インターコネクトに直接接続され、ゾーン分割は、Cisco UCS ローカル ゾーン分割を使用して Cisco UCS Manager で実行されます。既存のファイバ チャネルまたは FCoE のアップリンク接続を無効にする必要があります。現時点では、Cisco UCS は、UCS ローカルゾーン分割機能の利用において、現用系なファイバ チャネル/FCoE アップリンク接続をサポートしていません。

- スイッチベースのファイバチャネルゾーン分割：この設定は、直接接続ストレージとアップリンク ゾーン分割の組み合わせです。ファイバ チャネルまたは FCoE のストレージはファブリック インターコネクトに直接接続され、ゾーン分割は、MDS または Nexus 5000 スイッチを介して Cisco UCS ドメイン の外部から実行されます。この設定では、Cisco UCS ドメイン でのローカル ゾーン分割はサポートされません。

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

Cisco UCS Manager-ベースのファイバ チャネル ゾーン分割

With Cisco UCS Manager-ベースのゾーン分割の場合、Cisco UCS Managerは、このタイプのゾーン分割で設定されたすべての VSAN のゾーンの作成やアクティブ化など、Cisco UCS ドメインのファイバ チャネル ゾーン分割の設定を制御します。このタイプのゾーン分割は、ローカルゾーン分割、または直接接続ストレージとローカルゾーン分割の組み合わせとも呼ばれます。

（注） VSAN がアップストリーム スイッチの VSAN と通信するよう設定され、ファイバ チャネルポートまたは FCoE アップリンク ポートを含んでいる場合は、 Cisco UCS Manager-ベースのゾーン分割を実行できません。

サポートされているファイバ チャネル ゾーン分割モード

Cisco UCS Manager-ベースのゾーン分割は、次のタイプのゾーン分割をサポートしています。

- [Single initiator single target] :Cisco UCS Manager は、vHBA とストレージ ポートのペアごとに、ゾーンを 1 つ自動的に作成します。各ゾーンには 2 つのメンバが含まれます。ゾーンの数がサポートされている最大値を超えると予想される場合を除いて、このタイプのゾーン分割を設定することを推奨します。
- [Single initiator multiple targets]:Cisco UCS Manager は、vHBA ごとにゾーンを 1 つ自動的に作成します。ゾーンの数がサポートされている最大値に到達またはそれを超えると予想される場合は、このタイプのゾーン分割を設定することを推奨します。

vHBA イニシエータ グループ

vHBA イニシエータ グループによって、サービス プロファイル内のすべての vHBA のファイバ チャネル ゾーン分割設定を決定します。 Cisco UCS Manager には、デフォルトの vHBA イニシエータ グループは含まれていません。ゾーン内のサーバに割り当てるサービス プロファイルで vHBA イニシエータ グループを作成する必要があります。

vHBA イニシエータ グループでの設定により、以下が決定されます。

- イニシエータ グループに含める vHBA（vHBA イニシエータとも呼ばれる）。
- ファイバ チャネル ストレージ接続ポリシー。これには、関連する VSAN およびストレージ アレイ上のファイバ チャネル ターゲット ポートが含まれます。
- グループに含める vHBA に対して設定するファイバ チャネル ゾーン分割のタイプ。

ファイバ チャネル ストレージ接続ポリシー

ファイバ チャネル ストレージ接続ポリシーには、 Cisco UCS Managerベースのファイバ チャネル ゾーン分割の設定に使用される、ストレージ アレイ上の一連のターゲット ストレージ ポートが含まれています。このポリシーは、組織またはイニシエータ グループの下に作成できます。

これらのゾーン内のストレージ アレイは、ファブリック インターコネクトに直接接続される必要があります。ファイバチャネルストレージ接続ポリシーに組み込むこれらのアレイのターゲット ストレージ ポートには、ファイバ チャネル ストレージ ポートまたは FCoE ストレージ ポートを使用できます。ポートの WWN を使用して、ポートをポリシーに追加し、ファイバ チャネル ゾーンのポートを識別します。

（注） Cisco UCS Manager はデフォルトのファイバ チャネル ストレージを作成しません。

ファイバ チャネル アクティブ ゾーン セット設定

ファイバ チャネル ゾーン分割が有効になっている各 VSAN では、Cisco UCS Manager は自動的に 1 つのゾーン セットと複数のゾーンを設定します。ゾーン メンバーシップは、相互通信が許可されたイニシエータとターゲットのセットを指定します。Cisco UCS Managerは、自動的にそのゾーンセットをアクティブにします。

Cisco UCS Managerは、ユーザ設定の vHBA イニシエータ グループとそれらの関連したファイバ チャネル ストレージ接続ポリシーを処理し、ファイバ チャネル イニシエータとターゲット間の必要な接続を決定します。Cisco UCS Managerは、イニシエータとターゲット間のペアワイズ ゾーン メンバーシップを構築するために、次の情報を使用します。

- vHBA イニシエータのポート WWN は、vHBA イニシエータ グループから作成されます。
- ストレージ アレイのポート WWN は、ストレージ接続ポリシーから作成されます。

スイッチベースのファイバ チャネル ゾーン分割

スイッチベースのゾーン分割の場合、Cisco UCS ドメイン はアップストリーム スイッチからゾーン分割設定を継承します。Cisco UCS Manager では、ゾーン分割の設定に関する情報を設定したり表示したりできません。VSAN に対してスイッチベースのゾーン分割を適用するには、Cisco UCS Manager でその VSAN のゾーン分割を無効にする必要があります。

Cisco UCS Manager-ベースのファイバ チャネル ゾーン分割に関するガイドラインおよび推奨事項

ファイバ チャネル ゾーン分割の設定を計画する際は、次のガイドラインおよび推奨事項を考慮してください。

ファイバ チャネル スイッチング モードは Cisco UCS Manager 設定用のスイッチ モードでなければならない

Cisco UCS Manager にファイバ チャネル ゾーン分割を処理させる場合は、ファブリック インターコネクトがファイバ チャネル スイッチ モードである必要があります。エンドホスト モードではファイバ チャネル ゾーン分割を設定できません。

ハイ アベイラビリティのために対称構成を推奨

Cisco UCS ドメイン が 2 つのファブリック インターコネクトによるハイ アベイラビリティ構成である場合は、両方のファブリック インターコネクトに同一の VSAN セットを設定することを推奨します。

Cisco UCS Manager ファイバ チャネル ゾーン分割の設定

（注） この手順は、Cisco UCS Managerにより制御されるファイバ チャネル ゾーン分割に対し Cisco UCS ドメイン を設定するのに必要な手順の概要を示します。次のすべてのステップを完了する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	まだ完了してない場合は、 Cisco UCS ドメイン 内のファブリック インターコネクトの接続を、外付けファイバ チャネル スイッチ（MDS など）から切り離してください。	

	コマンドまたはアクション	目的
ステップ 2	Cisco UCS ドメインにまだ外部ファイバ チャネル スイッチによって管理されたゾーンが含まれる場合は、これらのゾーンを削除するために、影響を受けたすべての VSAN で **clear-unmanaged-fc-zone-all** コマンドを実行します。	この機能は現在、Cisco UCS Manager GUI では使用できません。このステップは、Cisco UCS Manager CLI で実行する必要があります。
ステップ 3	ファイバ チャネル スイッチ モードの両方のファブリック インターコネクトでファイバ チャネル スイッチング モードを設定します。	エンドホスト モードではファイバ チャネル ゾーン分割を設定できません。
ステップ 4	ファイバ チャネル ゾーンのトラフィック転送に必要なファイバ チャネルと FCoE ストレージ ポートを設定します。	
ステップ 5	1 つ以上の VSAN を作成し、ファイバ チャネル ゾーンのトラフィック転送に必要なすべての VSAN で、ファイバ チャネルのゾーン分割を有効にします。	クラスタの設定では、ファイバ チャネル ゾーンに含める予定の VSAN をファイバ チャネル ストレージ モードで作成し、それらが両方のファブリック インターコネクトにアクセスできるようにすることを推奨します。
ステップ 6	1 つ以上のファイバ チャネル ストレージ接続ポリシーを作成します。	必要に応じて、この手順を実行してサービス プロファイルにファイバ チャネル ゾーン分割を設定することができます。
ステップ 7	ファイバ チャネル ゾーン経由で通信する必要があるサーバに対してサービス プロファイルまたはサービス プロファイル テンプレートにゾーン分割を設定します。	この設定を完了するには、次の手順を完了します。 • VHBA に割り当てられた VSAN（複数の場合あり）のゾーン分割を有効にします。 • 1 つ以上の vHBA イニシエータ グループを設定します。

ファイバ チャネル ゾーン分割用の VSAN 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 fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink #**create vsan** {*VSAN_Name*} {*VSAN_ID*} {*FCoE_VLAN_ID*}	次を入力します。 • VSAN_Name：ネットワークに割り当てられている名前。この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。 • VSAN_ID：ネットワークに割り当てられている固有識別情報。IDは、1 ～ 4078 または 4080 ～ 4093 の間で設定できます。4079 は予約済み VSAN ID です。 • FCoE_VLAN_ID：ファイバ チャネル接続に使用される VLAN に割り当てられている固有識別情報。ID は、1 ～ 4029 または 4048 ～ 4093 の間で設定できます。VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Manager では、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLANは、デフォルトでVLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグ

	コマンドまたはアクション	目的
		レード前にVLAN 1を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを（未使用の VLAN ID）4049 に変更することを検討します。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージポート ネイティブ VLAN は VLAN 4049 を使用します。 Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの FIP 対応統合型ネットワーク アダプタの場合は、FCoE VLAN ID のネイティブ VLAN ではないネームドVLANを使ってネームドVSANを設定する必要があります。この設定により、FCoE トラフィックが確実にこれらのアダプタを通過できるようになります。
ステップ 3	UCS-A /fc-uplink #**commit-buffer**	

例

次の例では、TestVsan という名前の VSAN を作成して、システムの変更をコミットします。

```
UCS-A # scope fc-uplink
UCS-A /fc-uplink # create vsan TestVsan 2 30
UCS-A /fc-uplink/vsan* # commit-buffer
UCS-A /fc-uplink/vsan #
```

新しいファイバ チャネル ゾーン プロファイルの作成

新しいファイバ チャネル ゾーン プロファイルを作成するには、次の手順を実行します。

始める前に

VSAN がファイバ チャネル ゾーン分割用に作成されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **create fc-zone-profile** *Profile_Name*	指定した名前のファイバ チャネル プロファイルを作成します。
ステップ 3	UCS-A /fc-storage/fc-zone-profile * # **create fc-user-zone** *Zone_Name*	ファイバ チャネル ゾーンのプロファイル モードを開始し、指定したファイバ チャネル ゾーンを作成します。
ステップ 4	UCS-A /fc-storage/fc-zone-profile/fc-user-zone* # **set path** {**A** | **B**}	ファイバ チャネル ゾーンのパスを設定します。
ステップ 5	UCS-A /fc-storage/fc-zone-profile/fc-user-zone* # **set vsan** *VSAN_Name*	ファイバ チャネル ゾーンをネームド VSAN に設定します。
ステップ 6	UCS-A /fc-storage/fc-zone-profile/fc-user-zone* # **create member** *wwpn*	ファイバ チャネル ゾーン プロファイルの WWPN を作成します。
ステップ 7	UCS-A /fc-storage/fc-zone-profile/fc-user-zone* # **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、myProfilie という名前の FC ゾーン分割ポリシーを作成する例を示します。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # create fc-zone-profile myProfile
UCS-A /fc-storage/fc-zone-profile* # create fc-user-zone myZone
UCS-A /fc-storage/fc-zone-profile/fc-user-zone* # set path A
UCS-A /fc-storage/fc-zone-profile/fc-user-zone* # set vsan test
UCS-A /fc-storage/fc-zone-profile/fc-user-zone* # create member 20:c2:11:25:b5:00:00:7f
UCS-A /fc-storage/fc-zone-profile/fc-user-zone/member* # commit-buffer
```

ファイバ チャネル ゾーン プロファイルの削除

ファイバ チャネル ゾーン プロファイルを削除するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **delete fc-zone-profile** *Profile_Name*	指定した名前のファイバ チャネル プロファイルを削除します。
ステップ 3	UCS-A /fc-storage* # **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、myProfile という名前の FC ゾーン プロファイルを削除する例を示します。

```
UCS-A # scope fc-storage
UCS-A /fc-storage # delete fc-zone-profile myProfile
UCS-A /fc-storage* # commit-buffer
UCS-A /fc-storage #
```

ファイバ チャネル ユーザ ゾーンの削除

ファイバ チャネル ユーザ ゾーンを削除するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fc-zone-profile** *Profile_Name*	指定したファイバ チャネル プロファイルに移動します。
ステップ 3	UCS-A /fc-storage/fc-zone-profile # **delete fc-user-zone** *Userzone_Name*	指定したファイバ チャネル ユーザ ゾーンを削除します。
ステップ 4	UCS-A /fc-storage/fc-zone-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。

例

次に、myZone という名前の FC ユーザ ゾーン プロファイルを削除する例を示します。

```
UCS-A # scope fc-storage
UCS-A /fc-storage # scope fc-zone-profile myProfile
```

```
UCS-A /fc-storage/fc-zone-profile # delete fc-user-zone myZone
UCS-A /fc-storage/fc-zone-profile* # commit-buffer
UCS-A /fc-storage #
```

両方のファブリック インターコネクトにアクセス可能な VSAN からの管理対象外ゾーンの削除

外部ファイバ チャネル スイッチを切断した後、そのスイッチによって管理されていたファイバ チャネル ゾーンが Cisco UCS ドメイン からクリアされていない場合があります。この手順では、Cisco UCS ドメイン ドメインの各 VSAN からこれらのゾーンを削除して、ファイバ チャネル ゾーン分割を Cisco UCS に設定できます。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクトのファイバ チャネル アップリンク モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **scope vsan** *vsan-name*	指定されたネームド VSAN の VSAN モードが開始されます。
ステップ 4	UCS-A /fc-uplink/fabric/vsan # **clear-unmanaged-fc-zones-all**	指定されたネームド VSAN からすべての管理対象外ファイバ チャネル ゾーンをクリアします。 必要に応じて、ステップ 2 から 4 を繰り返し、バッファをコミットする前に、指定したファブリック インターコネクトにアクセス可能なすべての VSAN から管理対象外のゾーンを削除することができます。
ステップ 5	UCS-A /fc-uplink/fabric/vsan # **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、管理対象外のゾーンをファブリック インターコネクト A にアクセス可能なネームド VSAN 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 fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # scope vsan finance
UCS-A /fc-uplink/fabric/vsan # clear-unmanaged-fc-zones-all
UCS-A /fc-uplink/fabric/vsan* # commit-buffer
UCS-A /fc-uplink #
```

1 つのファブリック インターコネクトにアクセス可能な VSAN からの管理対象外ゾーンの削除

外部ファイバ チャネル スイッチを切断した後、そのスイッチによって管理されていたファイバ チャネル ゾーンが Cisco UCS ドメイン からクリアされていない場合があります。この手順では、Cisco UCS ドメイン ドメインの各 VSAN からこれらのゾーンを削除して、ファイバ チャネル ゾーン分割を Cisco UCS に設定できます。

始める前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope vsan** *vsan-name*	指定されたネームド VSAN の VSAN モードが開始されます。
ステップ 3	UCS-A /fc-uplink/vsan # **clear-unmanaged-fc-zones-all**	指定されたネームド VSAN からすべての管理対象外ファイバ チャネル ゾーンをクリアします。 必要に応じて、ステップ 2 と 3 を繰り返し、バッファをコミットする前に、両方のファブリック インターコネクトにアクセス可能なすべての VSAN から管理対象外のゾーンを削除することができます。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /fc-uplink/vsan # **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、管理対象外のゾーンをネームド VSAN 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 fc-uplink
UCS-A /fc-uplink # scope vsan finance
UCS-A /fc-uplink/vsan # clear-unmanaged-fc-zones-all
UCS-A /fc-uplink/vsan* # commit-buffer
UCS-A /fc-uplink #
```

ファイバ チャネル ストレージ接続ポリシーの設定

ファイバ チャネル ストレージ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 storage-connection-policy** *policy-name*	ストレージ接続ポリシーを指定されたポリシー名で作成し、組織ストレージ接続ポリシー モードを開始します。
ステップ 3	UCS-A /org # **set zoning-type** {**none** | **simt** | **sist**}	• **[None]**:Cisco UCS Manager ファイバ チャネル ゾーニングは設定されていません。 • **[Single Initiator Single Target]**：Cisco UCS Manager は、vHBA とストレージポートのペアごとに、ゾーンを 1 つ自動的に作成します。各ゾーンには2つのメンバが含まれます。ゾーンの数がサポートされている最大値を超えると予想される場合を除いて、このタイプのゾーン分割を設定することを推奨します。

	コマンドまたはアクション	目的
		• **[Single Initiator Multiple Targets]**：Cisco UCS Manager は、vHBA ごとにゾーンを 1 つ自動的に作成します。ゾーンの数がサポートされている最大値に到達またはそれを超えると予想される場合は、このタイプのゾーン分割を設定することを推奨します。
ステップ 4	UCS-A /org/storage-connection-policy # **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 5	UCS-A /org/storage-connection-policy/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 6	UCS-A /org/storage-connection-policy/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。
ステップ 7	UCS-A /org/storage-connection-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、ファブリック インターコネクト A とデフォルト VSAN を使用して scPolicyZone1 という名前のルート組織でファイバ チャネル ストレージ接続ポリシーを設定し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org* # create storage-connection-policy scPolicyZone1
UCS-A /org/storage-connection-policy* set zoning-type sist
UCS-A /org/storage-connection-policy* # create storage-target 20:10:20:30:40:50:60:70
UCS-A /org/storage-connection-policy/storage-target* # set target-path a
UCS-A /org/storage-connection-policy/storage-target* # set target-vsan default
UCS-A /org/storage-connection-policy* # commit-buffer
UCS-A /org/storage-connection-policy #
```

ファイバ チャネル ストレージ接続ポリシーの削除

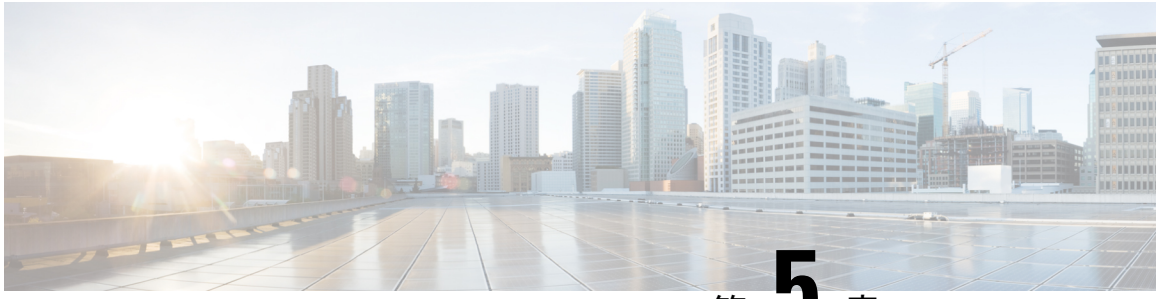
手順

	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* として / を入力します。
ステップ 2	UCS-A /org # **delete storage-connection-policy** *policy-name*	指定されたストレージ接続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

次の例では、ルート組織から scPolicyZone1 という名前のストレージ接続ポリシーを削除し、トランザクションをコミットします。

```
UCS-A# scope org /
UCS-A /org # delete san-connectivity-policy scPolicyZone1
UCS-A /org* # commit-buffer
UCS-A /org #
```



第 5 章

ネームド VSAN

ネームド VSAN

ネームド VSAN は、所定の外部 SAN への接続を作成します。VSAN は、ブロードキャスト トラフィックを含む、その外部 SAN へのトラフィックを切り離します。1 つのネームド VSAN のトラフィックは、別のネームドVSANにトラフィックが存在していることを認識しますが、そのトラフィックの読み取りまたはアクセスはできません。

ネームド VLAN と同様、VSAN ID に名前を割り当てると、抽象レイヤが追加されます。これにより、ネームド VSAN を使用するサービス プロファイルに関連付けられたすべてのサーバをグローバルにアップデートすることができます。外部SANとの通信を維持するために、サーバを個別に再設定する必要はありません。同じ VSAN ID を使用して、複数のネームド VSAN を作成できます。

クラスタ構成内のネームド VSAN

クラスタ構成では、1 つのファブリック インターコネクトのファイバ チャネル アップリンク ポート、または両方のファブリック インターコネクトのファイバ チャネル アップリンク ポートにアクセスできるように、ネームド VSAN を設定できます。

ネームド VSAN と FCoE VLAN ID

それぞれのネームド VSAN に FCoE VLAN ID を設定する必要があります。このプロパティによって、VSAN とそのファイバ チャネル パケットの送信に使用する VLAN を指定します。

Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの FIP 対応統合型ネットワーク アダプタの場合は、FCoE VLAN ID のネイティブ VLAN ではないネームド VLAN を使ってネームド VSAN を設定する必要があります。この設定により、FCoE トラフィックが確実にこれらのアダプタを通過できるようになります。

次の設定例では、ファブリック A にマッピングされた vNIC および vHBA を含むサービス プロファイルが、FIP 対応の統合型ネットワーク アダプタを搭載したサーバに関連付けられます。

- vNIC は VLAN 10 を使用するように設定されています。
- VLAN 10 は、vNIC のネイティブ VLAN として指定されています。
- vHBA は VSAN 2 を使用するように設定されています。
- したがって、VLAN 10 を FCoE VLAN ID として VSAN 2 に設定することはできません。VSAN 2 はファブリック A に設定されている他の VLAN にマッピングできます。

ネームド VSAN のファイバ チャネル アップリンク トランキング

各ファブリック インターコネクトのネームド VSAN にファイバ チャネル アップリンク トランキングを設定できます。ファブリック インターコネクトのトランキングをイネーブルにした場合、そのファブリック インターコネクトのすべてのファイバ チャネル アップリンク ポートで、 Cisco UCS ドメイン のすべてのネームド VSAN が許可されます。

VSAN に関するガイドラインおよび推奨事項

次のガイドラインと推奨事項は、ストレージ VSAN を含め、すべてのネームド VSAN に適用されます。

VSAN 4079 は予約済み VSAN ID です。

VSAN を 4079 に設定しないでください。この VSAN は予約されており、FC スイッチ モードや FC エンドホスト モードでは使用できません。

ID 4079 でネームド VSAN を作成すると、Cisco UCS Manager はエラーをマークし、VSAN 障害を生成します。

FC スイッチ モードのネームド VSAN 用に予約された VSAN 範囲

Cisco UCS ドメインで FC スイッチ モードを使用する予定の場合は、ID が 3040 ～ 4078 の範囲にある VSAN を設定しないでください。

ファブリック インターコネクトが FC スイッチ モードで動作するように設定されている場合、その範囲内の VSAN は動作しません。Cisco UCS Manager は、その VSAN に エラーのマークを付け、障害を発生させます。

FC エンドホスト モードのネームド VSAN 用に予約された VSAN 範囲

Cisco UCS ドメインで FC エンドホスト モードを使用する予定の場合、ID が 3840 ～ 4079 の範囲にある VSAN を設定しないでください。

Cisco UCS ドメイン内に次の状況が存在する場合、その範囲内の VSAN は動作しません。

- ファブリック インターコネクトが FC エンドホスト モードで動作するように設定されている。
- Cisco UCS ドメイン は、ファイバ チャネル トランキングまたは SAN ポート チャネルで設定されます。

これらの設定が存在する場合、Cisco UCS Manager は次の操作を実行します。

1. 3840 ～ 4079 の ID を持つすべての VSAN を使用不能にします。
2. 動作しない VSAN に対して障害を生成します。
3. デフォルトの VSAN にすべての非動作 VSAN を転送します。
4. 非動作 VSAN に関連付けられたすべての vHBA をデフォルトの VSAN に転送します。

ファイバ チャネル トランキングをディセーブルにし、既存の SAN ポート チャネルのいずれかを削除する場合、Cisco UCS Manager は 3840 ～ 4078 の範囲の VSAN を動作状態に戻し、関連付けられた vHBA をそれらの VSAN に復元します。

FC スイッチ モードのネームド VSAN ID の範囲に関する制約事項

Cisco UCS ドメインで FC スイッチ モードを使用する計画の場合、3040 ～ 4078 の範囲の VSAN を設定しないでください。

FC スイッチ モードで動作するファブリック インターコネクトがアップストリーム スイッチとして MDS に接続されている場合、Cisco UCS Manager で 3040 ～ 4078 の範囲に設定されポート VSAN として割り当てられた VSAN を MDS に作成できません。この設定では、ポート VSAN の不一致が発生する可能性があります。

FCoE VLAN ID に関するガイドライン

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN上でイーサネットトラフィックがドロップされます。

VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Managerでは、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。

- Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを （未使用の VLAN ID）4049 に変更することを検討します。
- Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。

両方のファブリック インターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル アップリンク モード）

Note SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN上でイーサネットトラフィックがドロップされます。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。

	Command or Action	Purpose
ステップ 2	UCS-A /fc-uplink # **create vsan** *vsan-name vsan-id fcoe-id*	指定された VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル アップリンク VSAN モードを開始します。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージ ポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを （未使用の VLAN ID）4049 に変更することを検討します。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 3	UCS-A /fc-uplink/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバ チャネル ゾーン分割を設定します。 • disabled：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。 • enabled：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 4	UCS-A /fc-uplink/vsan # **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。

Example

次の例では、両方のファブリック インターコネクト用のネームド VSAN を作成し、VSAN に accounting という名前を付け、VSAN ID 2112 を割り当て、FCoE VLAN ID

4021 を割り当て、Cisco UCS Manager-based ファイバ チャネル ゾーン分割について VSAN をイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink* # create vsan accounting 2112 4021
UCS-A /fc-uplink/vsan # set fc-zoning enabled
UCS-A /fc-uplink/vsan* # commit-buffer
UCS-A /fc-uplink/vsan #
```

両方のファブリック インターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル ストレージ モード）

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN上でイーサネットトラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **create vsan** *vsan-name vsan-id fcoe-id*	指定された VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル ストレージ VSAN モードを開始します。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを （未使用の VLAN ID）4049 に変更することを検討します。

	コマンドまたはアクション	目的
		• Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 3	UCS-A /fc-storage/vsan # **create member-port** {**fc** | **fcoe**} {**a** | **b**} *slot-id port-id*	メンバ ポートを作成し、ポート タイプ、ファブリック、スロット ID およびポート ID かを指定します。
ステップ 4	UCS-A /fc-storage/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバ チャネル ゾーン分割を設定します。 • disabled：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。 • enabled：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 5	UCS-A /fc-storage/vsan # **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、ネームド VSAN を作成し、VSAN に finance という名前を付け、VSAN ID 3955 を割り当て、FCoE VLAN ID 4021 を割り当て、メンバ ポートを作成してメンバ ポート A、スロット 1 ポート 40 に割り当て、Cisco UCS Manager-based ファイバ チャネル ゾーン分割について VSAN をイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage/ # create VSAN finance 3955 4021
UCS-A /fc-storage/vsan # create member-port fcoe a 1 40
UCS-A /fc-storage/vsan # set fc-zoning enabled
UCS-A /fc-storage/vsan/member-port* # commit-buffer
UCS-A /fc-storage/vsan/member-port #
```

1 つのファブリック インターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル アップリンク モード）

Note SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN上でイーサネットトラフィックがドロップされます。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクト（A または B）のファイバ チャネル アップリンク ファブリック インターコネクト モードを開始します。
ステップ 3	UCS-A /fc-uplink/fabric # **create vsan** *vsan-name vsan-id fcoe-id*	指定された VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル アップリンク VSAN モードを開始します。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを （未使用の VLAN ID）4049 に変更することを検討します。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで

	Command or Action	Purpose
		VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 4	UCS-A /fc-uplink/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバ チャネル ゾーン分割を設定します。 • disabled：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。 • enabled：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 5	UCS-A /fc-uplink/fabric/vsan # **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。

Example

次の例では、ファブリック インターコネクト A 用のネームド VSAN を作成し、VSAN に finance という名前を付け、VSAN ID 3955 を割り当て、FCoE VLAN ID 2221 を割り当て、Cisco UCS Manager-based ファイバ チャネル ゾーン分割について VSAN をイネーブルにし、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # create vsan finance 3955 2221
UCS-A /fc-uplink/vsan # set fc-zoning enabled
UCS-A /fc-uplink/fabric/vsan* # commit-buffer
UCS-A /fc-uplink/fabric/vsan #
```

1 つのファブリック インターコネクトにアクセス可能なネームド VSAN の作成（ファイバ チャネル ストレージ モード）

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN上でイーサネットトラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **scope fabric** {**a** | **b**}	指定したファブリック インターコネクトのファイバ チャネル ストレージ モードを開始します。
ステップ 3	UCS-A /fc-storage/fabric # **create vsan** *vsan-name vsan-id fcoe-id*	指定された VSAN を作成し、VSAN の名前、VSAN ID および FCoE VLAN ID を指定し、ファイバ チャネル ストレージ VSAN モードを開始します。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを （未使用の VLAN ID）4049 に変更することを検討します。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで

	コマンドまたはアクション	目的
		VLAN 4048 を使用します。FCoE ストレージ ポート ネイティブ VLAN は VLAN 4049 を使用します。
ステップ 4	UCS-A /fc-storage/fabric/vsan # **create member-port** {**fc** | **fcoe**} {**a** | **b**} *slot-id port-id*	指定された VSAN のメンバ ポートを作成します。
ステップ 5	UCS-A /fc-storage/vsan # **set fc-zoning** {**disabled** | **enabled**}	次のように、VSAN に対するファイバ チャネル ゾーン分割を設定します。 • disabled：アップストリーム スイッチがファイバ チャネル ゾーン分割を設定および制御します。または、ファイバ チャネル ゾーン分割がこの VSAN で実行されません。 • enabled：Cisco UCS Manager がファイバ チャネル ゾーン分割を設定し、制御します。
ステップ 6	UCS-A /fc-storage/fabric/vsan # **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、ファブリック A にネームド VSAN を作成し、VSAN に finance という名前を付け、VSAN ID 3955 を割り当て、FCoE VLAN ID 2221 を割り当て、メンバ ポートを作成してメンバ ポート A、スロット 1 ポート 40 に割り当て、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage/ # scope fabric a
UCS-A /fc-storage/fabric # create VSAN finance 3955 2221
UCS-A /fc-storage/fabric/vsan # create member-port a 1 40
UCS-A /fc-storage/fabric/vsan # set fc-zoning enabled
UCS-A /fc-storage/fabric/vsan/member-port* # commit-buffer
UCS-A /fc-storage/fabric/vsan/member-port #
```

ネームド VSAN の削除

Cisco UCS Manager に、削除するものと同じ VSAN ID を持つネームド VSAN が含まれている場合、この ID を持つネームド VSAN がすべて削除されるまで、この VSAN はファブリック インターコネクト設定から削除されません。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **delete vsan** *vsan-name*	指定されたネームド VSAN を削除します。
ステップ 3	UCS-A /fc-uplink # **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。

Example

次に、ネームド VSAN 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 fc-uplink
UCS-A /fc-uplink # delete vsan finance
UCS-A /fc-uplink* # commit-buffer
UCS-A /fc-uplink #
```

ネームド VSAN の FCoE ネイティブ VLAN の VLAN ID の変更

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN上でイーサネットトラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope vsan** *vsan-name*	指定されたネームド VSAN の VSAN モードが開始されます。
ステップ 3	UCS-A /fc-uplink/vsan # **set fcoe-vlan** *fcoe-vlan-id*	ファイバ チャネル接続に使用される VLANに割り当てられた固有識別情報を設定します。

	コマンドまたはアクション	目的
ステップ 4	UCS-A /fc-uplink/vsan # **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、finance というネームド VSAN の FCoE ネイティブ VLAN の VLAN ID を 4000 に変更し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope vsan finance
UCS-A /fc-uplink/vsan # set fcoe-vlan 4000
UCS-A /fc-uplink/vsan* # commit-buffer
UCS-A /fc-uplink/vsan #
```

ストレージ VSAN の FCoE ネイティブ VLAN の VLAN ID の変更

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN上でイーサネットトラフィックがドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-storage**	ファイバ チャネル ストレージ モードを開始します。
ステップ 2	UCS-A /fc-storage # **set fcoe-storage-native-vlan** *fcoe-id*	ファイバ チャネル接続に使用される VLANに割り当てられた固有識別情報を設定します。
ステップ 3	UCS-A /fc-storage # **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、finance というストレージ VSAN の FCoE ネイティブ VLAN の VLAN ID を 4000 に変更し、トランザクションをコミットします。

```
UCS-A# scope fc-storage
UCS-A /fc-storage # set fcoe-storage-native-vlan 4000
UCS-A /fc-storage* # commit-buffer
UCS-A /fc-storage #
```

ファイバチャネルアップリンクのトランキングのイネーブル化またはディセーブル化

（注） ファブリック インターコネクトがファイバ チャネル エンドホスト モードに設定されている場合、ファイバ チャネル アップリンク トランキングを有効にすると、ID が 3840 ～ 4079 の範囲にあるすべての VSAN が動作不能になります。

（注） ファブリック インターコネクトで VSAN トランキングを有効にする前に、すべてのホスト OS ストレージ パスの冗長性が機能していることを確認してください。ファイバ チャネル パスが回復されたことをモニタリングおよび確認する手順の詳細については、[データ パスの準備ができていることの確認（Verification that the Data Path is Ready）]セクションを参照してください。ファイバ チャネル アップリンクへのすべてのパスを回避するには、これに従う必要があります。

確認後、セカンダリ ファブリック インターコネクトでファイバチャネルアップリンク トランキングを有効にし、セカンダリ ファイバ チャネル VIF パスが回復するまで待ちます。次に、データ パスを検証した後、プライマリ ファブリック インターコネクト ファイバ チャネル トランキングをイネーブル化に移行します。

手順

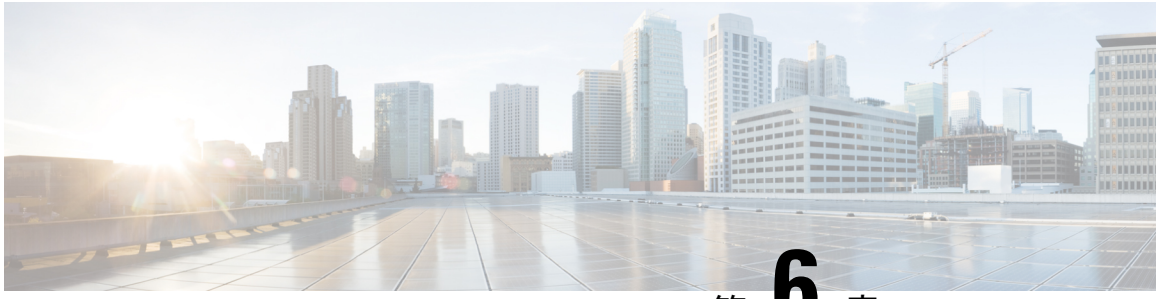
	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **scope fabric** {**a** | **b** }	指定したファブリックでファイバ チャネル アップリンク モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /fc-uplink/fabric # **set uplink-trunking** {**enabled** | **disabled** }	アップリンクのトランキングをイネーブルまたはディセーブルにします。
ステップ 4	UCS-A /fc-uplink/fabric # **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、ファブリック A のファイバチャネルアップリンクのトランキングを有効にし、トランザクションをコミットする例を示します。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # scope fabric a
UCS-A /fc-uplink/fabric # set uplink-trunking enabled
UCS-A /fc-uplink/fabric* # commit-buffer
UCS-A /fc-uplink/fabric #
```



第 6 章

SAN ピン グループ

SAN ピン グループ

Cisco UCS では、SAN ピン グループを使用して、サーバ上の vHBA からのファイバ チャネル トラフィックがファブリック インターコネクト上のアップリンク ファイバ チャネル ポートへピン接続されます。このピン接続を使用して、サーバからのトラフィックの分散を管理できます。

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

ピン接続をサーバに設定するには、SAN ピン グループを vHBA ポリシーに含める必要があります。その後、vHBA ポリシーは、そのサーバに割り当てられたサービス プロファイルに取り込まれます。vHBA からのすべてのトラフィックは、I/O モジュールを経由して、指定されたアップリンク ファイバ チャネルへ移動します。

同じピン グループを複数の vHBA ポリシーに割り当てられます。したがって、vHBA ごとに手動でトラフィックをピン接続する必要はありません。

Important 既存の SAN ピン グループのターゲット インターフェイスを変更すると、そのピン グループを使用するすべての vHBA のトラフィックが中断されます。ファイバ チャネル プロトコルでトラフィックを再びピン接続するために、ファブリック インターコネクトからログインとログアウトが実行されます。

SAN ピン グループの設定

2つのファブリック インターコネクトを持つシステムでピン グループとの関連付けができるのは、1つのファブリック インターコネクト、または両方のファブリック インターコネクトだけです。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope fc-uplink**	ファイバ チャネル アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **create pin-group** *pin-group-name*	ファイバ チャネル（SAN）のピン グループを指定された名前で作成し、ファイバ チャネル アップリンクのピン グループ モードを開始します。
ステップ 3	(Optional) UCS-A /fc-uplink/pin-group # **set descr** *description*	ピン グループに説明を加えます。 **Note** 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	(Optional) UCS-A /fc-uplink/pin-group # **set target** {**a** | **b** | **dual**} **port** *slot-num* / *port-num*	指定したファブリックとポートにファイバ チャネル ピン ターゲットを設定します。
ステップ 5	UCS-A /fc-uplink/pin-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

Example

次の例は、fcpingroup12 という名前の SAN ピン グループを作成し、ピン グループに説明を加え、スロット 2 のポート 1 にピン グループのターゲットを設定し、トランザクションをコミットします。

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # create pin-group fcpingroup12
UCS-A /fc-uplink/pin-group* # set descr "This is my pin group #12"
UCS-A /fc-uplink/pin-group* # set target a port 2/1
UCS-A /fc-uplink/pin-group* # commit-buffer
UCS-A /fc-uplink/pin-group #
```

What to do next

ピン グループを vHBA テンプレートに含めます。

FCoE ピン グループの設定

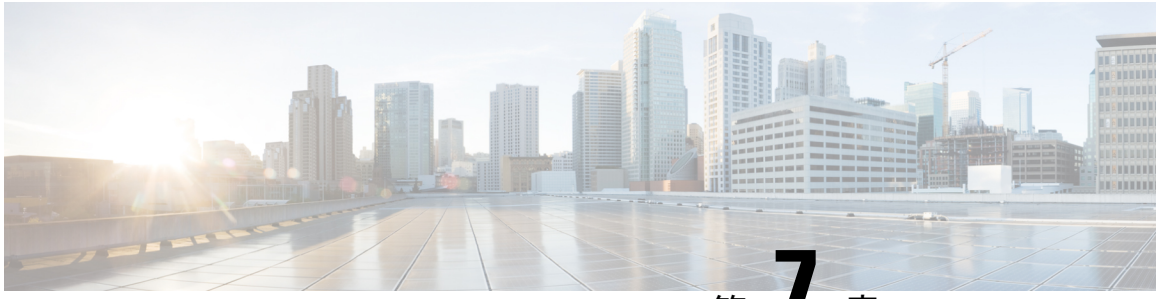
FCoE ピン グループを作成して、ピン グループ ターゲットとして FCoE アップリンク ポートを指定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope fc-uplink**	FC アップリンク モードを開始します。
ステップ 2	UCS-A /fc-uplink # **create pin-group fcoepingroup**	FCoE ピン グループを指定された名前で作成し、FCoE アップリンクのピン グループ モードを開始します。
ステップ 3	UCS-A /fc-uplink/pin-group # **set target a fcoe-port 1/8**	このピン グループのターゲットとして FCoE ポート 1/8 を設定します。
ステップ 4	UCS-A /fc-uplink/pin-group # **commit-buffer**	トランザクションをシステム設定にコミットします。

例

```
UCS-A# scope fc-uplink
UCS-A /fc-uplink # create pin-group fcoepingroup
UCS-A /fc-uplink/pin-group* #set target a fcoe-port 1/8
UCS-A /fc-uplink/pin-group* # commit-buffer
UCS-A /fc-uplink/pin-group #
```



第 7 章

FC ID の割り当て

ファイバ チャネル ID

ファイバ チャネルのノードおよびポートには、グローバルに一意なワールド ワイド番号（WWN）が必須です。Cisco UCS では、WWN は ID プールとして作成されます。ファイバ チャネル ノード（サーバ全体、ストレージアレイ）にはワールドワイドノード名（WWNN）が必須で、ファイバ チャネル ポートにはワールド ワイド ポート名（WWPN）が必須です。WWNN と WWPN はいずれも物理エンティティであるため、64 ビットのアドレスが割り当てられています。

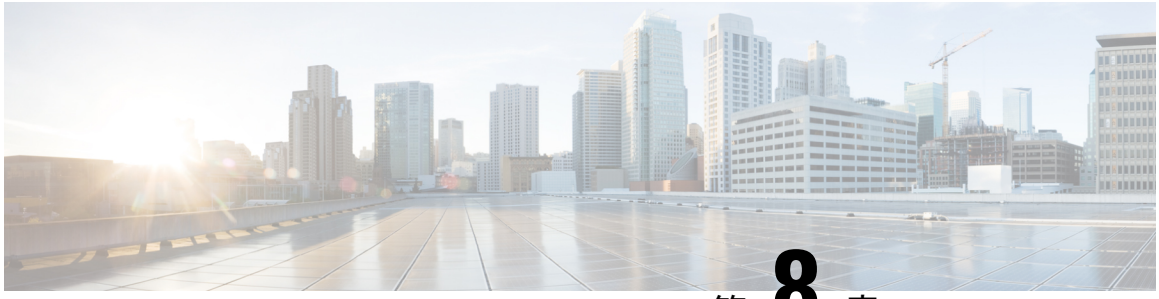
WWNN プールは、Cisco UCS ドメインに対する 1 つの大きなプールとして作成されます。Cisco UCS Manager の [SAN] タブでは、デフォルト プールを使用できます。ただし、その UCS ドメインではカスタムの WWNN プールを作成することを推奨します。

通信デバイスはノードです。サーバのホスト バス アダプタはファイバ チャネル ノードを構成します。サーバとホストでは、WWNN は各ホスト バス アダプタ（HBA）で一意です。SAN スイッチでは、WWNN はシャーシに共通です。ミッドレンジ ストレージでは、WWNN は各コントローラ ユニットで共通です。エンタープライズ ストレージでは、WWNN はアレイ全体で一意です。

各サーバには、HBA の各ポートに一意の WWPN が割り当てられます。SAN スイッチでは、WWPN はシャーシの各ポートで使用できます。ストレージでは、各ポートに個別の番号が割り当てられます。

Cisco UCS Manager の [FC Identity] タブには、Cisco UCS ドメイン SAN クラウドに含まれるデバイスの FC ID が、次のような情報と共に表示されます。

- 選択されたデバイスの WWNN または WWPN 識別子
- 識別子が vHBA に割り当てられているかどうか
- 識別子が割り当てられた vHBA



第 8 章

WWW プール

WWN プール

ワールド ワイド名（WWN）のプールは、Cisco UCS ドメインCisco UCS ドメイン内のファイバ チャネル vHBA で使用される WWN の集合です。次の独立したプールを作成します。

- vHBA に割り当てられる WW ノード名
- vHBA に割り当てられる WW ポート名
- WW ノード名と WW ポート名の両方

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:00:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF:FF. その他の WWN 範囲はすべて予約されています。ファイバ チャネル トラフィックが Cisco UCS インフラストラクチャを介して送信されると、送信元 WWPN は MAC アドレスに変換されます。送信元マルチキャスト MAC アドレスに変換可能な WWPN プールを使用することはできません。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX という形の WWN プレフィックスを使用することをお勧めします。

サービス プロファイルで WWN プールを使用する場合は、サービス プロファイルに関連付けられたサーバで使用される WWN を手動で設定する必要はありません。複数のテナントを実装するシステムでは、WWN プールを使用して、各組織で使用される WWN を制御できます。

WWN をブロック単位でプールに割り当てます。

WWNN プール

WWNN プールは、WW ノード名だけを含む WWN プールです。サービス プロファイルに WWNN のプールを含める場合、関連付けられたサーバには、そのプールから WWNN が割り当てられます。

WWPN プール

WWPN プールは、WW ポート名だけを含む WWN プールです。サービス プロファイルに WWPN のプールを含めると、関連付けられているサーバの各 vHBA のポートに、そのプールから WWPN が割り当てられます。

WWxN プール

WWxN プールは、WW ノード名と WW ポート名の両方を含む WWN プールです。ノードごとに WWxN プールで作成されるポート数を指定できます。プール サイズは、*ports-per-node* + 1 の倍数である必要があります。たとえば、ノードごとに 7 つのポートを指定する場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 のポートを指定する場合、プール サイズは 64 の倍数である必要があります。

WWNN または WWPN プールを選択するたびに WWxN プールを使用できます。WWxN プールを割り当てるには、その前に WWxN プールを作成する必要があります。

- WWNN プールの場合、WWxN プールは [WWNN Assignment] ドロップダウン リストにオプションとして表示されます。
- WWPN プールの場合は、[WWPN Assignment] ドロップダウン リストから [Derived] を選択します。

WWN プールの作成

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:00:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF:FF. その他の WWN 範囲はすべて予約されています。ファイバ チャネル トラフィックが Cisco UCS インフラストラクチャを介して送信されると、送信元 WWPN は MAC アドレスに変換されます。送信元マルチキャスト MAC アドレスに変換可能な WWPN プールを使用することはできません。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX という形の WWN プレフィックスを使用することをお勧めします。

Procedure

	Command or Action	Purpose
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 wwn-pool** *wwn-pool-name* {**node-and-port-wwn-assignment** | **node-wwn-assignment** | **port-wwn-assignment**}	指定された名前と目的で WWN プールを作成し、組織 WWN プール モードを開始します。次のいずれかになります。 • **node-and-port-wwn-assignment**：ワールド ワイド ノード名（WWNN）およびワールド ワイド ポート名（WWPN）の両方を含む WWxN プールを作成します。 • **node-wwn-assignment**：WWNN のみを含む WWNN プールを作成します。 • **port-wwn-assignment**：WWPN のみを含む WWPN プールを作成します。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
ステップ 3	(Optional) UCS-A /org/wwn-pool # **set descr** *description*	WWN プールの説明を記入します。 **Note** 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	UCS A/org/wwn-pool # **set assignmentorder** {**default** |**sequential**}	次のいずれかになります。 • **default**：Cisco UCS Manager はプールからランダム ID を選択します。

	Command or Action	Purpose
		• **sequential**：Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。
ステップ 5	UCS A/org/wwn-pool # **set max-ports-per-node** {**15-ports-per-node** | **3-ports-per-node** | **31-ports-per-node** |**63-ports-per-node** |**7-ports-per-node**}	WWxN プールの場合、このプール内の各ノード名に割り当てることができるポートの最大数。デフォルト値は **3-ports-per-node** です。 **Note** WWxN プールのプール サイズは、ノードごとのポートに 1 を加えた数の倍数である必要があります。たとえば、**7-ports-per-node** を指定する場合、プール サイズは 8 の倍数である必要があります。**63-ports-per-node** を指定する場合、プール サイズは 64 の倍数である必要があります。
ステップ 6	UCS-A /org/wwn-pool # **create block** *first-wwn last-wwn*	WWN ブロック（範囲）を作成し、組織 WWN プール ブロック モードを開始します。ブロックの最初と最後の WWN を *nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn* 形式で指定する必要があります。WWN 間はスペースで区切ります。 **Note** WWN プールには、複数の WWN ブロックを含めることができます。複数の WWN ブロックを作成するには、組織 WWN プール モードから複数の **create block** コマンドを入力します。
ステップ 7	UCS-A /org/wwn-pool/block # **exit**	組織 WWN プール ブロック モードを終了します。
ステップ 8	UCS-A /org/wwn-pool # **create initiator** *wwn wwn*	WWNN または WWPN プール用の単一イニシエータを作成し、組織 WWN プール イニシエータ モードを開始します。イニシエータを *nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn* 形式を使用して指定する必要があります。

	Command or Action	Purpose
		Note WWNN または WWPN プールは複数のイニシエータを含むことができます。複数のイニシエータを作成するには、組織 WWN プールモードから複数の **create initiator** コマンドを入力します。
ステップ 9	UCS-A /org/wwn-pool/initiator # **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。

Example

次に、sanpool という名前の WWNN プールを作成し、プールの説明を記入し、プールに使用される WWN とイニシエータのブロックを指定し、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 wwn-pool sanpool node-wwn-assignment
UCS-A /org/wwn-pool* # set descr "This is my WWNN pool"
UCS-A /org/wwn-pool* # create block 20:00:00:25:B5:00:00:00 20:00:00:25:B5:00:00:01
UCS-A /org/wwn-pool/block* # exit
UCS-A /org/wwn-pool* # create initiator 23:00:00:05:AD:1E:02:00
UCS-A /org/wwn-pool/initiator* # commit-buffer
UCS-A /org/wwn-pool/initiator #
```

次に、sanpool という名前の WWxN プールを作成し、プールの説明を記入し、ノードあたりのポート数を 7 を指定し、プールに使用される 8 個の WWN からなるブロックを指定し、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 wwn-pool sanpool node-and-port-wwn-assignment
UCS-A /org/wwn-pool* # set descr "This is my WWxN pool"
UCS-A /org/wwn-pool* # set max-ports-per-node 7-ports-per-node
UCS-A /org/wwn-pool* # create block 20:00:00:25:B5:00:00:00 20:00:00:25:B5:00:00:08
UCS-A /org/wwn-pool/block* # commit-buffer
UCS-A /org/wwn-pool/block #
```

What to do next

- WWPN プールを vHBA テンプレートに含めます。
- WWNN プールをサービスプロファイルとテンプレートに含めます。
- WWxN プールをサービスプロファイルとテンプレートに含めます。

WWN プールの削除

プールを削除した場合、Cisco UCS Managerは、 に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みアドレスは、次のいずれかが起きるまで、vNIC または vHBA に割り当てられた状態のままになります。

- 関連付けられたサービス プロファイルが削除される。
- アドレスが割り当てられた vNIC または vHBA が削除される。
- vNIC または vHBA が異なるプールに割り当てられる。

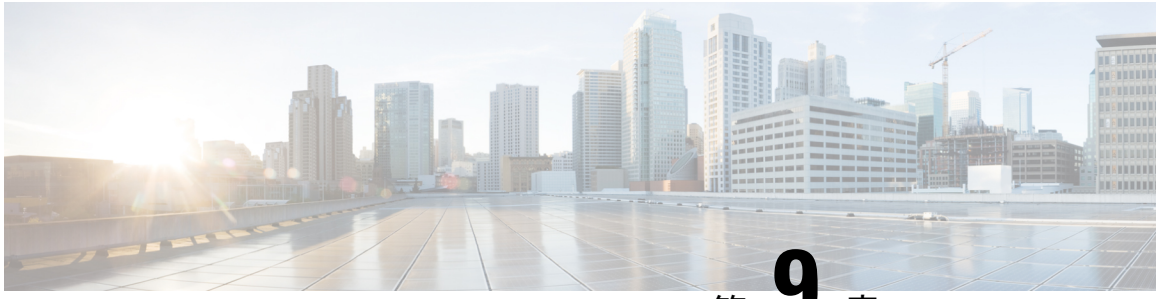
手順

	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 wwn-pool** *pool-name*	指定された WWN プールを削除します。
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、pool4 という名前の WWN プールを削除し、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 wwn-pool pool4
UCS-A /org* # commit-buffer
UCS-A /org #
```



第 9 章

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** ー 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（122 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 （122 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設定にコミットします。

第 10 章

ストレージ プロファイル

ストレージ プロファイル

ストレージプロファイルを作成して使用することで、ストレージディスクの数、これらのディスクのロールと用途、およびその他のストレージパラメータを柔軟に定義できます。ストレージプロファイルには、1つ以上のサービスプロファイルのストレージ要件がカプセル化されます。ストレージ プロファイルで設定された LUN は、ブート LUN またはデータ LUN として使用でき、また特定のサーバ専用にすることができます。さらに、ローカル LUN をブート デバイスとして指定することも可能です。ただし、LUNのサイズ変更はサポートされていません。ストレージ プロファイルを導入すると、次の利点があります。

- 複数の仮想ドライブを設定し、仮想ドライブによって使用される物理ドライブを選択できます。仮想ドライブのストレージ容量も設定できます。
- ディスク グループに含まれるディスクの数、タイプ、ロールを設定できます。
- ストレージ プロファイルをサービス プロファイルに関連付けることができます。

ストレージ プロファイルは、組織レベルでも、サービス プロファイル レベルでも作成できます。サービス プロファイルには、専用ストレージ プロファイルおよび組織レベルのストレージ プロファイルを関連付けることができます。

Cisco ブート最適化 M.2 RAID コントローラ

4.0(4a) 以降、Cisco UCS ManagerはMarvell ® 88SE92xx PCIe から SATA 6Gb/s コントローラを搭載した Cisco ブート最適化 M.2 コントローラ (UCS-M2-HWRAID) をサポートしています。これは、次のサーバでサポートされています。

- Cisco UCS C245 M6サーバ
- Cisco UCS C220 M6サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ

次の 2 つのドライブは、Cisco ブート最適化 M. 2 RAID コントローラによって管理されます。

- 240GB M.2 6G SATA SSD
- 960GB M.2 6G SATA SSD

Cisco ブート最適化 M. 2 RAID コントローラは、RAID1/JBOD (デフォルト-JBOD) モードと UEFI ブート モードのみをサポートします。

Cisco ブート最適化 M.2 Raid コントローラの制限

- 既存の LUN の移行はサポートされていません。
- **ローカル ディスク設定**ポリシーはサポートされていません。
- 1 つの LUN を作成するとディスク容量をすべて使用するため、作成できる LUN の数は 1 つに制限されます。
- Lun は、ストレージ プロファイルの下の **[Local LUN (ローカル LUN)]** タブ (を参照) を使用して作成され、コントローラ定義を使用しません。
- 異なる容量の 2 台のドライブを混在させることはできません。
- ブレードまたはラック サーバー上の孤立した仮想ドライブの名前を変更することはできません。

ディスク グループおよびディスク グループ設定ポリシー

ストレージに使用するディスクを選択して設定できます。これらの物理ディスクの論理集合は「ディスク グループ」と呼ばれます。ディスク グループを使用すれば、ローカル ディスクを整理できます。ストレージ コントローラは、ディスク グループの作成と設定を制御します。

ディスク グループ設定ポリシーは、ディスク グループの作成方法と設定方法を定義したものです。このポリシーで、ディスク グループに使用するRAIDレベルを指定します。また、ディスク グループのディスクの手動選択または自動選択とディスクのロールも指定します。1つのディスク グループ ポリシーを使用して、複数のディスク グループを管理できます。ただし、1つのディスク グループを複数のディスク グループ ポリシーで管理することはできません。

ホット スペアとは、ディスク グループに含まれるディスクで障害が発生した場合にディスク グループで使用できる、未使用の予備ディスクのことです。ホット スペアを使用できるのは、フォールトトラレント RAID レベルをサポートするディスク グループのみです。

仮想ドライブ

1つのディスク グループは、複数の仮想ドライブにパーティション分割できます。その場合、オペレーティング システムには各仮想ドライブが個別の物理デバイスとして表されます。

ディスク グループのすべての仮想ドライブは、同じ1つのディスク グループ ポリシーを使用して管理する必要があります。

設定状態

[設定状態（Configuration States）]には、仮想ドライブの設定状態が示されます。仮想ドライブの設定状態は次のいずれかになります。

- [適用中（Applying）]：仮想ドライブを作成中です。
- [適用済み（Applied）]：仮想ドライブの作成が完了したか、仮想ディスク ポリシーの変更が設定されて正常に適用されました。
- [適用失敗（Failed to apply）]：基礎となるストレージ サブシステムで発生したエラーにより、仮想ドライブの作成、削除、または名前変更が失敗しました。
- [Orphaned]：この仮想ドライブを含むサービス プロファイルが削除されたか、サービス プロファイルとストレージ プロファイルとの関連付けが解除されています。

（注） 孤立したLUNは、OSの起動に使用できません。これらのLUNにイメージをインストールすることはできますが、これらのドライブからの起動は失敗します。特定の孤立したLUNを使用するには、ストレージ プロファイルを再度関連付ける必要があります。これにより、「装備済み」プレゼンス状態に戻ります。

- [Not in use]：この仮想ドライブが含まれていたサービス プロファイルが何にも関連付けられていない状態になっています。

展開状態

[展開状態（Deployment States）] には、仮想ドライブで実行中のアクションが示されます。仮想ドライブの展開状態は次のいずれかになります。

- [アクションなし（No action）]：仮想ドライブに対して保留中の作業項目はありません。
- [作成中（Creating）]：仮想ドライブを作成中です。
- [削除中（Deleting）]：仮想ドライブを削除中です。
- [変更中（Modifying）]：仮想ドライブを変更中です。
- [適用失敗（Apply-Failed）]：仮想ドライブの作成または変更が失敗しました。

動作状態

[動作状態（Operability States）] には、仮想ドライブの動作状態が示されます。仮想ドライブの動作状態は次のいずれかになります。

- [最適（Optimal）]：仮想ドライブの動作状態は正常です。設定されているすべてのドライブがオンラインです。
- [縮退（Degraded）]：仮想ドライブの動作状態は最適ではありません。設定されたドライブのいずれかに障害が発生したか、オフラインの状態です。
- [Cache-degraded]：仮想ドライブは write back モードの書き込みポリシーを使用して作成されましたが、BBU に障害が発生したか、BBU がありません。

（注） always write back モードを選択した場合は、この状態になりません。

- [Partially degraded]：RAID 6 仮想ドライブの動作状態が最適ではありません。設定されたドライブのいずれかに障害が発生したか、オフラインの状態です。RAID 6 は、最大 2 件のドライブ障害を許容できます。
- [オフライン（Offline）]：仮想ドライブが、RAID コントローラで使用できません。これは実質的に障害状態です。
- [不明（Unknown）]：仮想ドライブの状態は不明です。

プレゼンス状態

[プレゼンス状態（Presence States）] には、仮想ドライブ コンポーネントのプレゼンスが示されます。仮想ドライブのプレゼンス状態は次のいずれになります。

- [実装済み（Equipped）]：仮想ドライブを利用できます。
- [不一致（Mismatched）]：仮想ドライブの展開状態が、その仮想ドライブに設定されている状態と異なります。
- [欠落（Missing）]：仮想ドライブがありません。

RAID レベル

ディスク グループの RAID レベルは、可用性、データの冗長性、および I/O パフォーマンスの確保を目的とした、ディスク グループでのデータの編成方法を表します。

RAID により、次の機能が提供されます。

- ストライピング：複数の物理デバイスでデータをセグメント化します。これにより、デバイスの同時アクセスが可能になり、スループットが向上するため、パフォーマンスが向上します。
- ミラーリング：同じデータを複数のデバイスに書き込むことで、データの冗長性を確保します。
- パリティ：デバイスで障害が発生した場合にエラーを修正できるよう、追加のデバイスに冗長データを保管します。パリティによって完全な冗長性が実現されることはありませんが、シナリオによってはエラー リカバリが可能になります。
- スパニング：複数のドライブを 1 つの大容量ドライブとして使用できます。たとえば、4 台の 20 GB ドライブを結合して、1 台の 80 GB ドライブのように扱うことができます。

サポートされている RAID レベルは次のとおりです。

- [ローカル ストレージを無効にする（Disable Local Storag）]：(PCH SSD コントローラ定義でサポート) このディスク ポリシー モードは、SATA AHCI コントローラを無効にします。このモードは、SATA AHCI コントローラの下にディスクが存在しない場合にのみ設定できます。このコントローラを再度有効にして、コントローラをデフォルト値（AHCI）に戻すには、[RAID なし（No RAID）] または [ローカル ストレージなし（No Local Storage）] モードを選択できます。
- [No Local Storage]：（PCH SSD コントローラ定義でサポート）ディスクレス サーバまたは SAN 専用の設定で使用します。このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0 Striped]：（PCH SSD コントローラ定義でサポート）データはアレイ内のすべてのディスクにストライプ化され、高速スループットを提供します。データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- [RAID 1 Mirrored]：（PCH SSD コントローラ定義でサポート）データは 2 つのディスクに書き込まれ、1つのディスクで障害が発生した場合でも完全なデータ冗長性を提供します。最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。

- [Any Configuration]：（PCH SSD コントローラ定義でサポート）変更なしにローカル ディスク 設定を転送するサーバ設定の場合。
- [No RAID]：（PCH SSD コントローラ定義でサポート）JBOD ディスクと同様にすべてのディスクが相互依存関係なく個別に使用できます。[No RAID] を選択し、RAID ストレージが設定されているオペレーティング システムをすでに持っているサーバにこのポリシーを適用する場合、システムはディスクのコンテンツを削除しません。したがって、No RAID モードを適用した後でサーバに目に見える違いがない場合があります。このことは、ポリシーの RAID 設定とサーバの [インベントリ (Inventory)] > [ストレージ (Storage)] タブで表示される実際のディスク設定の間の不一致を生じさせる可能性があります。以前の RAID 情報がディスクから削除されたことを確認するには、No RAID 設定モードを適用した後で、すべてのディスク情報を削除するスクラブ ポリシーを適用します。
- [RAID 5 Striped Parity]：（PCH SSD コントローラ定義ではサポート対象外）アレイ内のすべてのディスクにデータがストライプ化されます。各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。

  RAID 5 は、RAID-5 グループに属する複数のディスクにパリティ データ ブロックを配分します。RAID 5 には、3 台以上のディスクが必要です。
- [RAID 6 Striped Dual Parity]:（PCH SSD コントローラ定義ではサポート対象外）アレイ内のすべてのディスクにデータがストライプ化され、2 つのパリティ データを使用して最大 2 つの物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。

  2 つ目のパリティ ブロックが追加される点を除けば、RAID 6 は RAID 5 と同じ機能です。RAID 6 には 4 台以上のディスクが必要です。
- [RAID 10 Mirrored and Striped]：（PCH SSD コントローラ定義ではサポート対象外）RAID 10 がミラー化されたディスク ペアを使用して、ブロックレベル ストライプ化を通じて完全なデータ冗長性と高いスループット レートを提供します。RAID 10 は、パリティおよびブロック レベルのストライピングを使用しないミラーリングを行います。RAID 10 には 4 台以上のディスクが必要です。
- [RAID 50 Striped Parity and Striped]：（PCH SSD コントローラ定義ではサポート対象外）複数のストライプ化されたパリティ ディスク セットにデータがストライプ化され、高いスループットと複数のディスク障害耐性を提供します。
- [RAID 60 Striped Dual Parity and Striped]：（PCH SSD コントローラ定義ではサポート対象外）複数のストライプ化されたデュアル パリティ ディスク セットにデータがストライプ化され、高いスループットと優れたディスク障害耐性を提供します。

（注） 一部の Cisco UCS サーバでは、特定の RAID 設定オプションにライセンスが必要です。Cisco UCS Manager で、このローカル ディスク ポリシーを含むサービス プロファイルをサーバに関連付けると、選択された RAID オプションに適切なライセンスが備わっているかが Cisco UCS Managerによって確認されます。問題がある場合は、サービスプロファイルを関連付ける際に Cisco UCS Manager に設定エラーが表示されます。特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『Hardware Installation Guide』を参照してください。

自動ディスク選択

ディスク グループ構成を指定して、そのディスク グループに含まれるローカル ディスクを指定しないと、Cisco UCS Manager はディスク グループ構成ポリシーで指定された基準に従って、使用するディスクを決定します。この場合、Cisco UCS Manager は複数の方法でディスクを選択できます。

一連のディスクのすべての修飾子が一致すると、それらのディスクはスロット番号に従って順番に選択されます。通常のディスクおよび専用ホット スペアは、スロット番号が小さい順に選択されます。

ディスク選択プロセスは次のとおりです。

1. 新しい仮想ドライブの作成が必要なすべてのローカル LUN について処理が繰り返されます。繰り返し処理は、次の基準に、記載する順で従います。
   1. ディスクの種類
   2. 降順の最小ディスク サイズ
   3. 降順のスペース要件
   4. アルファベット順のディスク グループ修飾子名
   5. アルファベット順のローカル LUN 名
2. 最小ディスク数および最小ディスク サイズに応じて、通常のディスクを選択します。検索基準を満たすディスクのうち、スロット番号が最も小さい順にディスクが選択されます。

（注） ドライブ タイプとして [Any] を指定すると、使用可能な最初のドライブが選択されます。最初のドライブが選択されると、以降のドライブはそのドライブと互換性のあるタイプになります。たとえば、最初のドライブが SATA である場合、後続のすべてのドライブも SATA となります。Cisco UCS Manager リリース 2.5 でサポートされているのは SATA と SAS のみです。

Cisco UCS Manager リリース 2.5 では RAID のマイグレーションをサポートしていません。

3. 専用ホット スペアの選択方法も、通常のディスクを選択する場合と同じです。[Unconfigured Good] 状態のディスクのみが選択されます。
4. プロビジョニング済み LUN に、展開済み仮想ドライブと同じディスク グループ ポリシーが設定されている場合は、同じディスク グループへの新しい仮想ドライブの展開を試みます。そうでない場合は、展開する新しいディスクの検索を試みます。

サポートされている LUN の変更

LUN が関連付けられたサーバにすでに展開されているとしても、LUN 設定に対する一部の変更はサポートされます。

次のタイプの変更を行うことができます。

- 新しい仮想ドライブの作成。
- 孤立した状態にある既存の仮想ドライブの削除。
- 既存の仮想ドライブに対する、再構成を伴わない変更。次の変更は、データ損失やパフォーマンスの低下を伴わずに既存の仮想ドライブに対して行うことができます。
  - ポリシー変更。たとえば、キャッシュ書き込みポリシーを変更するなどです。
  - ブート パラメータの変更。

LUN を削除すると、警告が表示されます。データ損失を回避するための措置を取ってください。

サポートされていない LUN の変更

既存の LUN に対する変更の中には、元の仮想ドライブを破棄して新しい仮想ドライブ作成しなければ適用できない変更があります。その場合はすべてのデータが失われるため、そのような変更はサポートされていません。

再構成を伴う既存の仮想ドライブに対する変更はサポートされていません。サポートされていない、再構成を伴う変更は次のとおりです。

- 再構成を通して可能となる、サポートされている任意の RAID レベルの変更。たとえば、RAID0 から RAID1 への変更。
- 再構成を通した仮想ドライブのサイズ増加。
- 再構成を通したディスクの追加および削除。

破壊的変更もサポートされていません。サポートされていない破壊的変更は次のとおりです。

- 再構成をサポートしない RAID レベルの変更。たとえば、RAID5 から RAID1 への変更。
- 仮想ドライブのサイズ縮小。

- 同じドライブ グループに他の仮想ドライブが存在する状況における、再構成をサポートする RAID レベルの変更。
- ディスク グループに仮想ドライブを収容するだけのスペースが残っていない場合のディスクの削除。
- 仮想ドライブで使用しているディスク セットの明示的変更。

ディスク挿入の処理

次の一連のイベントが発生する場合があります。

1. LUN が、次のいずれかの方法で作成されます。
   1. ユーザがローカル ディスク参照を使用して、明示的にスロットを指定します。
   2. ユーザが指定した基準に従って、システムがスロットを選択します。
2. LUN が正常に展開されます。つまり、そのスロットを使用する仮想ドライブが作成されます。
3. ディスクをスロットから取り外します（おそらくディスクで障害が発生したため）。
4. 同じスロットに新しい有効なディスクを挿入します。

次のシナリオが可能です。

- 非冗長仮想ドライブ （149 ページ）
- ホット スペア ドライブが割り当てられていない冗長仮想ドライブ （150 ページ）
- ホット スペア ドライブが割り当てられた冗長仮想ドライブ （150 ページ）
- ホット スペア ドライブの交換 （150 ページ）
- 未使用スロットへの物理ドライブの挿入 （151 ページ）

非冗長仮想ドライブ

非冗長仮想ドライブ（RAID0）は、物理ドライブが除去されると [Inoperable] 状態になります。新しい有効なドライブが挿入されると、新しい物理ドライブは [Unconfigured Good] 状態になります。

非冗長仮想ドライブの場合、仮想ドライブの回復手段はありません。仮想ドライブを削除してから再作成する必要があります。

ホット スペア ドライブが割り当てられていない冗長仮想ドライブ

冗長仮想ドライブ（RAID 1、RAID 5、RAID 6、RAID 10、RAID 50、RAID 60）にホット スペア ドライブが割り当てられていないと、古い物理ドライブを取り除いたスロットに有効な物理ドライブを挿入するまでは、仮想ドライブの不一致、仮想ドライブのメンバ欠如、ローカル ディスクの欠如といった障害状態になります。

物理ドライブのサイズが古いドライブのサイズ以上である場合、ストレージコントローラは自動的にその新しいドライブを仮想ドライブ用に使用します。新しいドライブは [Rebuilding] 状態になります。再ビルドが完了すると、仮想ドライブは [Online] 状態に戻ります。

ホット スペア ドライブが割り当てられた冗長仮想ドライブ

冗長仮想ドライブ（RAID 1、RAID 5、RAID 6、RAID 10、RAID 50、RAID 60）にホット スペア ドライブが割り当てられている場合、ドライブで障害が発生したり、ドライブを取り除いたりすると、仮想ドライブが [Degraded] 状態になった時点で、専用ホット スペア ドライブ（使用可能な場合）が [Rebuilding] 状態になります。再ビルドが完了すると、そのドライブが [Online] 状態になります。

仮想ドライブが運用可能であっても、仮想ドライブは Cisco UCSM が期待する物理設定と一致しないため、ディスク欠如および仮想ドライブ不一致の障害が発生します。

ディスクが欠如しているスロットに新しいディスクを挿入すると、前のホット スペア ディスクから、新しく挿入されたディスクへの自動コピー バックが開始されます。コピー バックの後、ホット スペア ディスクが復元されます。復元された時点で、すべてのエラーがクリアされます。

自動コピー バックが開始されず、新しく挿入したディスクの状態が [Unconfigured Good]、[JBOD] または [Foreign Configuration] のままになっている場合は、新しいディスクをスロットから取り除き、前のホット スペア ディスクをスロットに再挿入して、外部設定をインポートしてください。これにより再ビルドプロセスが開始され、ドライブの状態が [Online] になります。その時点で、新しいディスクをホット スペア スロットに挿入し、ホット スペアとしてマークして、Cisco UCSM で使用可能な情報と完全に一致させます。

ホット スペア ドライブの交換

ホット スペア ドライブを交換すると、新しいホット スペア ドライブは [Unconfigured Good]、[Unconfigured Bad]、[JBOD]、または [Foreign Configuration] 状態になります。

ホット スペア ドライブの状態が Cisco UCSM で設定されている状態と異なることから、仮想ドライブの不一致または仮想ドライブ メンバの不一致による障害が発生します。

このエラーは、手動でクリアする必要があります。それには、次の操作を実行します。

1. 新しく挿入されたドライブの状態を [Unconfigured Good] に戻します。
2. 新しく挿入されたドライブを、Cisco UCSM が期待するホット スペア ドライブとなるように設定します。

未使用スロットへの物理ドライブの挿入

未使用のスロットに新しい物理ドライブを挿入した場合、そのドライブが [Unconfigured Good] 状態であっても、正常な物理ドライブが欠如している仮想ドライブがあると、ストレージコントローラも Cisco UCSM もその新しいドライブを利用しません。

その場合、ドライブは [Unconfigured Good] 状態になるだけです。新しいドライブを利用するには、新しく挿入されたドライブを参照するように LUN を変更するか、そのドライブを参照する LUN を作成する必要があります。

仮想ドライブの命名

UCSM を使用して仮想ドライブを作成すると、UCSM がその仮想ドライブに固有 ID を割り当てます。以降の操作では、この ID を使用して確実に仮想ドライブを識別できます。UCSM では、サービスプロファイルを関連付ける時点で仮想ドライブに柔軟に名前を付けられるようにもなっています。サービスプロファイルまたはサーバによって参照されていない仮想ドライブは、いずれも孤立した仮想ドライブとしてマークされます。

固有 ID に加え、名前がドライブに割り当てられます。名前は、次の 2 つの方法で割り当てられます。

- 仮想ドライブを設定する際に、ストレージプロファイルで参照できる名前を、ユーザが明示的に割り当てることができます。
- ユーザが仮想ドライブの名前をプロビジョニングしなかった場合、UCSM が仮想ドライブの一意の名前を生成します。

サービスプロファイルまたはサーバーによって参照されていない、ブレードまたはラックサーバーの孤立した仮想ドライブの名前は、変更することができます。

（注） 孤立した仮想ドライブの名前変更は、Cisco ブート最適化 M.2 Raid コントローラ（UCS-M2-HWRAID）ではサポートされていません。

LUN の参照解除

LUN を使用するサービス プロファイルがなくなると、LUN の参照は解除されます。LUN の参照解除は、次のシナリオの一環として行われる場合があります。

- LUN がストレージ プロファイルから参照されなくなった。
- ストレージ プロファイルがサービス プロファイルから参照されなくなった。
- サーバの関連付けがサービス プロファイルから解除された。
- サーバが稼働停止された。

LUN が参照されなくなっても、サーバがまだ関連付けられている場合は、再関連付けが行われます。

LUN が含まれていたサービス プロファイルの関連付けが解除されると、LUN の状態は [Not in use] に変更されます。

LUN が含まれていたサービス プロファイルが削除されると、LUN の状態は [Orphaned] に変更されます。

コントローラの制限と制約事項

- 次の表は、サーバーでサポートされる最大仮想ドライブ数を示しています。

サーバー/ストレージ コントローラ	最大仮想ドライブ数
UCSB-MRAID12G-M6	16
UCSC-C220-M6、UCSC-C240-M6、UCSC-C225-M6、UCSC-C245-M6	32
UCSC-C240-M5、UCSC-C480-M5	32
UCS-S3260-M5、UCSC-C3X60-M4、UCSC-C3K-M4	64
UCSC-C240-M4、UCSC-C240-M3、UCSC-C24-M3	24
UCSB-MRAID12G	16
UCS-M2-HWRAID	2
他のすべてのサーバーの場合。	18

（注）

- ストレージ コントローラは、check max 機能をサポートします。
- サーバーに、同じストレージプロファイルによって管理されている複数のストレージコントローラがある場合、最大仮想ドライブはサーバーでサポートされる最大値に制限されます。
- UCS-MSTOR-M2 および UCS-MSTOR-SD コントローラは、M6 サーバーではサポートされていません。

- 次の表は、Cisco UCS C245 M6サーバ でサポートされるストレージ コントローラの最大数を示しています。

表 *4*：サポートされるストレージ コントローラの最大数：*Cisco UCS C245 M6*サーバ

サーバー/ストレージ コントローラ	最大仮想ドライブ数
Cisco UCS C245 M6サーバ	• デュアル UCS C245 M6 SX 16 SAS/SATA HDD • UCS C245 M6SX プラス 28 SAS/SATA HDD • UCS-M2-HWRAID 上の 2 台の M.2 2280 ドライブ • リア ライザーに直接接続された NVMe (最大 4 台の NVMe SSD)

- 次の表に、Cisco UCS C245 M6サーバ でサポートされる最大ストレージ ドライブを示します。

サーバー/ストレージ コントローラ	最大仮想ドライブ数
UCS Cisco UCS C245 M6 x 28 HDD/SDD バックプレーン 最大 24 台の 2.5 インチ 12 Gbps フロントロード HDD または SSD と 4 台の背面ホットスワップ可能な 2.5 インチ NVMe ドライブ、最大 8 台（4 フロント + 4 リア）	デュアル UCS C245 M6 SX 12 SAS3 ドライブ (コントローラあたり 12)
Cisco UCS C245 M6 x 24 HDD/SDD バックプレーン	UCS C245 M6SX プラス 24 SAS3 ドライブ
RAID 1 をサポートする UCS-M2-HWRAID M.2 モジュール	1
UCS-M2-HWRAID M.2 モジュールのみが、4 台の前面 NVMe ドライブと 4 台の背面 NVMe ドライブでサポートされます。	1

- Cisco UCS Manager リリース 2.2(4) では、ブロック サイズが 4K のドライブはブレード サーバではサポートされませんが、ラックマウント サーバではサポートされます。ブロック サイズが 4K のドライブをブレード サーバに挿入した場合、検出に失敗し、「`Unable to get Scsi Device Information from the system`」というエラー メッセージが表示されます。

- Cisco UCS Manager リリース 3.1(2) 以降のリリースでは、C240 M4、M5、および M6 サーバーでアウト オブ バンド インベントリ（OOB）をサポートしていない RAID コントローラの場合、動作状態として `NA` 、ドライブ状態として `Unknown` が表示されます。

ストレージ プロファイルの設定

ディスク グループ ポリシーの設定

ディスク グループ ポリシーの設定は、自動または手動でディスクを選択することにより行います。ディスク グループの設定には、次の操作が必要です。

1. RAID レベルの設定 （154 ページ）
2. ディスク グループ内のディスクの自動設定 （155 ページ） または ディスク グループ内のディスクの手動設定 （158 ページ）

（注） Cisco ブート最適化 M. 2 Raid コントローラ (HWRAID) をセットアップしている場合は、 ディスクのみを手動で構成することができます。

3. 仮想ドライブ プロパティの設定 （160 ページ）

RAID レベルの設定

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* として / を入力します。
ステップ 2	UCS A/org# **create disk-group-config-policy** ディスク グループ名	指定された名前でディスク グループ設定ポリシーを作成して、ディスク グループ設定ポリシー モードを開始します。
ステップ 3	UCS-A /org/disk-group-config-policy* # **set raid-level** *raid-level*	ディスク グループ設定ポリシーの RAID レベルを指定します。指定可能な RAID レベルを以下に示します。 • raid-0-striped • raid-1-mirrored • raid-10-mirrored-and-striped • raid-5-striped-parity • raid-6-striped-dual-parity • raid-50-striped-parity-and-striped

	コマンドまたはアクション	目的
		• raid-60-striped-dual-parity-and-striped （注） Cisco ブート最適化 M. 2 RAID コントローラ (UCS-M2-HWRAID) は、RAID1 のみをサポートします。
ステップ 4	UCS-A /org/disk-group-config-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

次に、ディスク グループ設定ポリシーの RAID レベルを設定する例を示します。

```
UCS-A# scope org
UCS-A /org # create disk-group-config-policy raid5policy
UCS-A /org/disk-group-config-policy* # set raid-level raid-5-striped-parity
UCS-A /org/disk-group-config-policy* # commit-buffer
```

次のタスク

ディスク グループ設定ポリシーの一部としてディスクを自動または手動で設定します。

ディスク グループ内のディスクの自動設定

UCSM により、ディスク グループ内のディスクを自動的に選択し、設定することができます。

RAID 1 ポリシーを使用するディスク グループを作成して、そのグループに 4 つのディスクを設定すると、ストレージ コントローラによって RAID1E 構成が内部的に作成されます。

Cisco ブート最適化 M. 2 Raid コントローラ（HWRAID）をセットアップした場合は、ディスク グループ内のディスクの手動設定 （158 ページ） に進みます。

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# **enter disk-group-config-policy** *disk-group-name*	指定されたディスク グループ名のディスク グループ設定ポリシー 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/disk-group-config-policy* # **enter disk-group-qual**	ディスク グループ認定モードを開始します。このモードでは、UCSM が、自動的に、指定されたディスク グループの一部としてディスクを設定します。
ステップ 4	UCS-A /org/disk-group-config-policy/disk-group-qual* # **set drive-type** *drive-type*	ディスク グループのドライブ タイプを指定します。次のオプションを選択できます。 • HDD • SSD • Unspecified （注） ドライブのタイプとして **Unspecified** を指定した場合は、最初の使用可能なドライブが選択されます。最初のドライブが選択されると、以降のドライブはそのドライブと互換性のあるタイプになります。たとえば、最初のドライブが SSD の場合、以降のすべてのドライブが SSD になります。
ステップ 5	UCS-A /org/disk-group-config-policy/disk-group-qual* # **set min-drive-size** *drive-size*	ディスク グループの最小ドライブ サイズを指定します。この基準を満たすディスク以外は選択できません。 最小ドライブ サイズの範囲は 0 ～ 10240 GB です。最小ドライブ サイズを **Unspecified** に設定することもできます。最小ドライブ サイズを **Unspecified** に設定した場合は、すべてのサイズのドライブが選択可能になります。
ステップ 6	UCS-A /org/disk-group-config-policy/disk-group-qual* # **set num-ded-hot-spares** *hot-spare-num*	ディスク グループの専用ホット スペアの数を指定します。 専用ホット スペア数の範囲は 0 ～ 24 です。専用ホット スペアの数を **Unspecified** に設定することもできます。専用ホット スペアの数を **Unspecified** に設定した場合は、ディス

	コマンドまたはアクション	目的
		ク選択プロセスに従ってホット スペアが選択されます。
ステップ 7	UCS-A /org/disk-group-config-policy/disk-group-qual* # **set num-drives** *drive-num*	ディスク グループのドライブの数を指定します。 Cisco UCS C240、C220、C24、および C22 サーバの場合、ドライブの範囲は 0 ～ 24 です。他のすべてのサーバの場合、1 サーバ当たりの制限は最大 16 ドライブです。。ドライブの数を **Unspecified** に設定することもできます。ドライブの数を **Unspecified** に設定した場合は、ドライブの数がディスク選択プロセスに従って選択されます。
ステップ 8	UCS-A /org/disk-group-config-policy/disk-group-qual* # **set num-glob-hot-spares** *hot-spare-num*	ディスク グループのグローバル ホット スペアの数を指定します。 グローバル ホット スペアの数の範囲は 0 ～ 24 です。グローバル ホット スペアの数を **Unspecified** に設定することもできます。グローバル ホット スペアの数を **Unspecified** に設定した場合は、ディスク選択プロセスに従ってグローバル ホット スペアが選択されます。
ステップ 9	UCS-A /org/disk-group-config-policy/disk-group-qual* # **set use-remaining-disks** {**no** | **yes**}	ディスク グループ ポリシーの残りのディスクが使用されるかどうかを指定します。 このコマンドのデフォルト値は **no** です。
ステップ 10	UCS-A /org/disk-group-config-policy/disk-group-qual* # **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、ディスク グループ設定ポリシーに対してディスクを自動的に設定する例を示します。

```
UCS-A# scope org
UCS-A /org # enter disk-group-config-policy raid5policy
UCS-A /org/disk-group-config-policy* # enter disk-group-qual
UCS-A /org/disk-group-config-policy/disk-group-qual* # set drive-type hdd
UCS-A /org/disk-group-config-policy/disk-group-qual* # set min-drive-size 1000
```

```
UCS-A /org/disk-group-config-policy/disk-group-qual* # set num-ded-hot-spares 2
UCS-A /org/disk-group-config-policy/disk-group-qual* # set num-drives 7
UCS-A /org/disk-group-config-policy/disk-group-qual* # set num-glob-hot-spares 2
UCS-A /org/disk-group-config-policy/disk-group-qual* # set use-remaining-disks no
UCS-A /org/disk-group-config-policy/disk-group-qual* # commit-buffer
```

```
UCS-A# scope org
UCS-A /org # enter disk-group-config-policy raid5policy
UCS-A /org/disk-group-config-policy* # enter disk-group-qual
UCS-A /org/disk-group-config-policy/disk-group-qual* # set drive-type ssd
UCS-A /org/disk-group-config-policy/disk-group-qual* # set min-drive-size 1000
UCS-A /org/disk-group-config-policy/disk-group-qual* # set num-ded-hot-spares 2
UCS-A /org/disk-group-config-policy/disk-group-qual* # set num-drives 7
UCS-A /org/disk-group-config-policy/disk-group-qual* # commit-buffer
```

次のタスク

仮想ドライブを設定します。

ディスク グループ内のディスクの手動設定

ディスク グループのディスクを手動で設定することができます。

RAID 1 ポリシーを使用してディスク グループを作成し、そのグループに 4 つのディスクを設定すると、ストレージ コントローラによって RAID 1E 構成が内部的に作成されます。

Cisco ブート最適化 M. 2 RAID コントローラ（UCS-M2-HWRAID）は、RAID1 のみをサポートします。

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# **enter disk-group-config-policy** *disk-group-name*	指定されたディスク グループ名のディスク グループ設定ポリシー モードを開始します。
ステップ 3	UCS-A /org/disk-group-config-policy* # **create local-disk-config-ref** *slot-num*	指定されたスロットのローカル ディスク設定参照を作成して、ローカル ディスク設定参照モードを開始します。 （注） M.2 ドライブには通常スロット ID = 253、254があります。
ステップ 4	UCS-A /org/disk-group-config-policy/local-disk-config-ref *# **set role** *role*	ディスク グループ内のローカル ディスクのロールを指定します。次のオプションを選択できます。

	コマンドまたはアクション	目的
		• ded-hot-spare：専用のホット スペア • Glob-hot-spare：グローバル ホット スペア • normal （注） Cisco ブート最適化 M. 2 Raid コントローラ（UCS-M2-HWRAID）をセットアップしている場合は、標準（normal）を選択します 。他の値を選択すると、設定エラーになります。
ステップ 5	UCS-A /org/disk-group-config-policy/local-disk-config-ref *# **set span-id** *span-id*	ディスクが属しているスパン グループの ID を指定します。単一のスパン グループに属している複数のディスクは、大容量の単一ディスクとして扱うことができます。値の範囲は 0 ～ 8 です。RAID-10、RAID-50、および RAID-60 の場合、最小 2 スパンが必要で、最大 8 スパンがサポートされます。スパニング情報が必要ない場合は、スパン ID を **Unspecified** として設定することもできます。 （注） • Cisco UCS リリース 2.5 では、最大 4 つのスパン グループを作成できます。 • Cisco ブート最適化 M. 2 Raid コントローラ (UCS-M2-HWRAID) を設定している場合は、このフィールドは適用されません。[範囲 ID（SPAN ID）] フィールドは **[未指定（Unspecified）]** のままにします。いずれかの値を選択すると、設定エラーになります。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/disk-group-config-policy/local-disk-config-ref *# **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、ディスク グループ設定ポリシーに対してディスクを手動で設定する例を示します。

```
UCS-A# scope org
UCS-A /org # enter disk-group-config-policy raid5policy
UCS-A /org/disk-group-config-policy* # create local-disk-config-ref 1
UCS-A /org/disk-group-config-policy/local-disk-config-ref *# set role ded-hot-spare
UCS-A /org/disk-group-config-policy/local-disk-config-ref* # set span-id 1
UCS-A /org/disk-group-config-policy/local-disk-config-ref *# commit-buffer
```

次のタスク

仮想ドライブ プロパティを設定します。

仮想ドライブ プロパティの設定

1 つのディスク グループ内のすべての仮想ドライブを単一のディスク グループ ポリシーを使用して管理する必要があります。

これらのプロパティをサポートしないサーバに関連付けようとすると、設定エラーが生成されます。

次のストレージ コントローラだけがこれらのプロパティをサポートします。

- LSI 6G MegaRAID SAS 9266-8i
- LSI 6G MegaRAID SAS 9271-8i
- LSI 6G MegaRAID 9265-8i
- LSI MegaRAID SAS 2208 ROMB
- LSI MegaRAID SAS 9361-8i

LSI MegaRAID SAS 2208 ROMB コントローラの場合、これらのプロパティは、B420-M3 ブレードサーバだけでサポートされます。他のコントローラでは、これらのプロパティは複数のラック サーバでサポートされます。

（注） Cisco ブート最適化 M. 2 Raid コントローラ (HWRAID) を設定している場合は、 次のようになります。

- 作成できる仮想ドライブは 1 つのみです。
- **ストリップ サイズ** には、**64 KB** または **32KB** を選択します。他の値を選択すると、設定エラーになります。
- **access-policy**、**read-policy**、**write-cache-policy**、**io-policy**、および **drive-cache** には、**platform-default** を選択します。他の値を選択すると、設定エラーになります。

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 disk-group-config-policy** *disk-group-name*	指定されたディスク グループ名のディスク グループ設定ポリシーモードを開始します。
ステップ 3	UCS-A /org/disk-group-config-policy* # **create virtual-drive-def**	仮想ドライブ定義を作成して、仮想ドライブ定義モードを開始します。
ステップ 4	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set access-policy** *policy-type*	アクセスポリシーを指定します。次のいずれかになります。 • blocked • platform-default • read-only: • read-write
ステップ 5	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set drive-cache** *state*	ドライブ キャッシュの状態を指定します。次のいずれかになります。 • 有効化 • 無効化 • no-change • platform-default

	コマンドまたはアクション	目的
		重要 Cisco UCS リリース 2.5 では、ドライブ キャッシュの状態を変更できません。選択されたドライブ キャッシュの状態に関係なく、**platform-default** のまま変化しません。
ステップ 6	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set io-policy** *policy-type*	I/O ポリシーを指定します。次のいずれかになります。 • cached • direct • platform-default
ステップ 7	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set read-policy** *policy-type*	読み取りポリシーを指定します。次のいずれかになります。 • normal • platform-default • read-ahead
ステップ 8	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set strip-size** *strip-size*	ストリップサイズを指定します。次のいずれかになります。 • 64 KB • 128 KB • 256 KB • 512 KB • 1024 KB • platform-default
ステップ 9	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set write-cache-policy** *policy-type*	書き込みキャッシュ ポリシーを指定します。次のいずれかになります。 • always-write-back • platform-default • write-back-good-bbu • write-through

	コマンドまたはアクション	目的
ステップ 10	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **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。
ステップ 11	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **show**	設定された仮想ドライブ プロパティを表示します。

例

次に、仮想ディスク プロパティを設定する例を示します。

```
UCS-A# scope org
UCS-A /org # scope disk-group-config-policy raid0policy
UCS-A /org/disk-group-config-policy # create virtual-drive-def
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set access-policy read-write
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set drive-cache enable
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set io-policy cached
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set read-policy normal
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set strip-size 1024
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set write-cache-policy
write-through
UCS-A /org/disk-group-config-policy/virtual-drive-def* # commit-buffer
UCS-A /org/disk-group-config-policy/virtual-drive-def # show

Virtual Drive Def:
    Strip Size (KB): 1024KB
    Access Policy: Read Write
    Read Policy: Normal
    Configured Write Cache Policy: Write Through
    IO Policy: Cached
    Drive Cache: Enable
UCS-A /org/disk-group-config-policy/virtual-drive-def #
```

次のタスク

ストレージ プロファイルの作成

ストレージ プロファイルの作成

ストレージ プロファイルは、組織レベルとサービス プロファイル レベルで作成できます。

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* として **/** を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **create storage-profile** *storage-profile-name*	指定された名前を持つストレージ プロファイルを組織レベルで作成し、ストレージ プロファイル設定モードを開始します。
ステップ 3	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。
ステップ 4	（任意） UCS-A /org* # **enter service-profile** *service-profile-name*	指定されたサービス プロファイルを入力します。
ステップ 5	（任意） UCS-A /org/service-profile* # **create storage-profile-def**	ストレージ プロファイルをサービス プロファイル レベルで作成します。
ステップ 6	UCS-A /org/service-profile/storage-profile-def* # **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、ストレージ プロファイルを組織レベルで作成する例を示します。

```
UCS-A# scope org
UCS-A /org # create storage-profile stp2
UCS-A /org/storage-profile* # commit-buffer
```

次に、ストレージ プロファイルをサービス プロファイル レベルで作成する例を示します。

```
UCS-A# scope org
UCS-A /org* # enter service-profile sp1
UCS-A /org/service-profile* # create storage-profile-def
UCS-A /org/service-profile/storage-profile-def* # commit-buffer
```

次のタスク

ローカル LUN の作成

ストレージ プロファイルの削除

組織レベルまたはサービス プロファイル レベルで作成されたストレージ プロファイルを削除できます。

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* として **/** を入力します。
ステップ 2	UCS-A /org # **delete storage-profile** *storage-profile-name*	組織レベルで、指定された名前を持つストレージ プロファイルを削除します。
ステップ 3	（任意） UCS-A /org # **scope service-profile** *service-profile-name*	指定されたサービス プロファイルを入力します。
ステップ 4	（任意） UCS-A /org/service-profile # **delete storage-profile-def**	サービス プロファイル レベルの専用ストレージ プロファイルを削除します。

例

次に、組織レベルのストレージ プロファイルを削除する例を示します。

```
UCS-A # scope org
UCS-A /org #  delete storage-profile stor1
```

次に、サービス プロファイル レベルのストレージ プロファイルを削除する例を示します。

```
UCS-A # scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # delete storage-profile-def
```

ローカル LUN

ローカル LUN の作成

ローカル LUN は、組織レベルのストレージプロファイル内に作成することも、サービス プロファイル レベルの専用ストレージ プロファイル内に作成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 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。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **enter storage-profile** *storage-profile-name*	指定されたストレージ プロファイルのストレージ プロファイル モードを開始します。
ステップ 3	UCS-A /org/storage-profile* # **create local-lun** *lun-name*	指定された名前を持つローカル LUN を作成します。
ステップ 4	UCS-A /org/storage-profile/local-lun* # **set auto-deploy** {**auto-deploy** | **no-auto-deploy**}	LUN を自動展開にするかどうかを指定します。
ステップ 5	UCS-A /org/storage-profile/local-lun* # **set disk-policy-name** *disk-policy-name*	この LUN のディスク ポリシー名を指定します。
ステップ 6	UCS-A /org/storage-profile/local-lun* # **set order** *order-num*	この LUN の順序を指定します。順序に有効な値の範囲は 1 ～ 64 です。また、順序値を **lowest-available** にして、使用可能な最小の順序値が自動的に LUN に割り当てられるように指定することもできます。 ストレージ プロファイルから参照される複数の LUN に、一意の名前と一意の順序を割り当てる必要があります。
ステップ 7	UCS-A /org/storage-profile/local-lun* # **set expand-to-avail** {**no** | **yes**}	LUN を使用可能なすべてのディスク グループに展開するかどうかを指定します。 各サービス プロファイルでは、1 つの LUN のみをこのオプションを使用するように設定できます。
ステップ 8	UCS-A /org/storage-profile/local-lun* # **set size** *size*	この LUN のサイズを GB 単位で指定します。 （注） Cisco ブート最適化 M.2 Raid コントローラを使用したセットアップでは、サイズを指定する必要はありません。システムは、指定されたサイズに関係なく、フルディスク容量を使用して LUN を作成します。

	コマンドまたはアクション	目的
		（注） 孤立したLUNを要求する際にLUNサイズを指定する必要はありません。
ステップ 9	UCS-A /org/storage-profile/local-lun* # **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、組織レベルのストレージ プロファイル内にローカル LUN を設定する例を示します。

```
UCS-A# scope org
UCS-A /org # enter storage-profile stp2
UCS-A /org/storage-profile* # create local-lun lun2
UCS-A /org/storage-profile/local-lun* # set disk-policy-name dpn2
UCS-A /org/storage-profile/local-lun* # set order 2
UCS-A /org/storage-profile/local-lun* # set size 1000
UCS-A /org/storage-profile/local-lun* # commit-buffer
```

```
UCS-A# scope org
UCS-A /org # enter storage-profile stp2
UCS-A /org/storage-profile* # create local-lun lun2
UCS-A /org/storage-profile/local-lun* # set auto-deploy no-auto-deploy
UCS-A /org/storage-profile/local-lun* # set disk-policy-name dpn2
UCS-A /org/storage-profile/local-lun* # set expand-to-avail yes
UCS-A /org/storage-profile/local-lun* # set size 1000
UCS-A /org/storage-profile/local-lun* # commit-buffer
```

次に、サービス プロファイル レベルの専用ストレージプロファイル内にローカルLUNを設定する例を示します。

```
UCS-A# scope org
UCS-A /org* # enter service-profile stp1
UCS-A /org/service-profile* # enter storage-profile-def
UCS-A /org/service-profile/storage-profile-def # create local-lun lun1
UCS-A /org/service-profile/storage-profile-def/local-lun* # set disk-policy-name dpn1
UCS-A /org/service-profile/storage-profile-def/local-lun* # set order 1
UCS-A /org/service-profile/storage-profile-def/local-lun* # set size 1000
UCS-A /org/service-profile/storage-profile-def/local-lun* # commit-buffer
```

```
UCS-A# scope org
UCS-A /org # enter service-profile sp1
UCS-A /org/service-profile* # enter storage-profile-def
UCS-A /org/service-profile/storage-profile-def # create local-lun lun1
UCS-A /org/service-profile/storage-profile-def/local-lun* # set auto-deploy no-auto-deploy
UCS-A /org/service-profile/storage-profile-def/local-lun* # set disk-policy-name dpn1
UCS-A /org/service-profile/storage-profile-def/local-lun* # set expand-to-avail yes
UCS-A /org/service-profile/storage-profile-def/local-lun* # set size 1000
UCS-A /org/service-profile/storage-profile-def/local-lun* # commit-buffer
```

次のタスク

サービス プロファイルとストレージ プロファイルの関連付け

ストレージ プロファイル内のローカル LUN の順序変更

set order コマンドを使用して、サーバに対するローカル LUN の表示順序を変更することができます。この操作によって、サーバがリブートされます。

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 # **enter storage-profile** *storage-profile-name*	指定されたストレージ プロファイルのストレージ プロファイル モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **enter local-lun** *lun-name*	指定されたローカル LUN のローカル LUN モードを開始します。
ステップ 4	UCS-A /org/storage-profile/local-lun* # **set disk-policy-name** *disk-policy-name*	この LUN のディスク ポリシー名を指定します。
ステップ 5	UCS-A /org/storage-profile/local-lun # **set order** *order-num*	この LUN の順序を指定します。順序に有効な値の範囲は 1 ～ 64 です。また、順序値を **lowest-available** にして、使用可能な最小の順序値が自動的に LUN に割り当てられるように指定することもできます。
ステップ 6	UCS-A /org/storage-profile/local-lun* # **set size** *size*	この LUN のサイズを GB 単位で指定します。
ステップ 7	UCS-A /org/storage-profile/local-lun* # **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、組織レベルのストレージ プロファイル内のローカル LUN の順序を変更する例を示します。

```
UCS-A# scope org
UCS-A /org # enter storage-profile stp1
UCS-A /org/storage-profile* # enter local-lun lun1
UCS-A /org/storage-profile/local-lun* # set disk-policy-name dpn1
UCS-A /org/storage-profile/local-lun* # set order 1
```

```
UCS-A /org/storage-profile/local-lun* # set size 10
UCS-A /org/storage-profile/local-lun* # exit
UCS-A /org/storage-profile* # enter local-lun lun2
UCS-A /org/storage-profile/local-lun* # set disk-policy-name dpn2
UCS-A /org/storage-profile/local-lun* # set order 2
UCS-A /org/storage-profile/local-lun* # set size 10
UCS-A /org/storage-profile/local-lun* # exit
UCS-A /org/storage-profile* # commit-buffer

UCS-A /org/storage-profile # show configuration

 enter storage-profile stp1
     enter local-lun lun1
         set auto-deploy auto-deploy
         set disk-policy-name dpn1
         set order 1
         set size 10
     exit
     enter local-lun lun2
         set auto-deploy auto-deploy
         set disk-policy-name dpn2
         set order 2
         set size 10
     exit
     set descr ""
 exit

UCS-A /org/storage-profile # enter local-lun lun1
UCS-A /org/storage-profile/local-lun # set order 2
UCS-A /org/storage-profile/local-lun* # exit
UCS-A /org/storage-profile* # enter local-lun lun2
UCS-A /org/storage-profile/local-lun* # set order 1
UCS-A /org/storage-profile/local-lun* # exit
UCS-A /org/storage-profile* # commit-buffer
UCS-A /org/storage-profile # show configuration

 enter storage-profile stp1
     enter local-lun lun1
         set auto-deploy auto-deploy
         set disk-policy-name dpn1
         set order 2
         set size 10
     exit
     enter local-lun lun2
         set auto-deploy auto-deploy
         set disk-policy-name dpn2
         set order 1
         set size 10
     exit
     set descr ""
 exit
```

ストレージ プロファイル内のローカル LUN の削除

LUN を削除すると、サーバから仮想ドライブ参照が削除された後、対応する仮想ドライブが孤立としてマークされます。

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 # **enter storage-profile** *storage-profile-name*	指定されたストレージ プロファイルのストレージ プロファイル モードを開始します。
ステップ 3	（任意） UCS-A /org/storage-profile* # **show local-lun**	指定されたストレージ プロファイル内のローカル LUN を表示します。
ステップ 4	UCS-A /org/storage-profile* # **delete local-lun** *lun-name*	指定された LUN を削除します。
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。

例

次に、ストレージ プロファイル内の LUN を削除する例を示します。

```
UCS-A # scope org
UCS-A /org # enter storage-profile stp2
UCS-A /org/storage-profile # show local-lun


Local SCSI LUN:

    LUN Name   Size (GB)   Order            Disk Policy Name Auto Deploy

    ---------- ----------- ---------------- ---------------- -----------

    luna       1           2                raid0            Auto Deploy

    lunb       1           1                raid0            Auto Deploy

UCS-A /org/storage-profile # delete local-lun luna
UCS-A /org/storage-profile* # commit-buffer
UCS-A /org/storage-profile* # show local-lun


Local SCSI LUN:

    LUN Name   Size (GB)   Order            Disk Policy Name Auto Deploy

    ---------- ----------- ---------------- ---------------- -----------

    lunb       1           1                raid0            Auto Deploy
```

LUN の設定

LUN 設定

リリースで始まる4.0(2a)、 Cisco UCS Manager LUN の設定オプションを使用した個々 の raid 0 Lun にディスク スロットの範囲を設定する機能を提供します。

LUN 設定の作成中には次のガイドラインを考慮する必要があります。

- ディスクの唯一の SSD および HDD タイプを使用できます。
- 最大 60 ディスクを 1 つの範囲内で使用できます。
- 2 つの異なる LUN の設定の構成での範囲内でのディスクの同じセットを追加することはできません。
- ディスク スロットの範囲の LUN 設定のディスクが設定されているかどうかは、同じストレージ ポリシーでローカル LUN 設定で設定された同じディスクを設定することはできません。同様に、ローカル LUN 設定では、ディスクが設定されている場合は、同じディスクで、ディスク スロットの範囲の LUN セットを使用できません。
- LUN の設定が設定されている、サーバは、OOB ストレージの操作をサポートする必要があります。
- 同じサービス プロファイルのストレージ ポリシーとローカル ディスク ポリシーを設定することはできません。
- ローカル LUN および LUN の設定に同じ名前を持つことはできません。
- S シリーズ サーバ PCH コントローラでスロット 201 および 202 はサポートされません LUN の設定。

LUN セットの制限事項

Cisco UCS ManagerLUN の設定を次の制限があります。

- LUN の設定に孤立状態のローカル Lun を要求することはできません。
- 作成されると、LUN の設定を変更することはできません。削除し、必要なパラメータを新しい LUN 設定を作成する必要があります。
- LUN の設定からは、OS ブートはサポートされていません。

LUN 設定の作成

LUN 設定は、組織レベルのストレージ プロファイル内に作成することも、サービス プロファイル レベルの専用ストレージ プロファイル内に作成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 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 # **enter storage-profile** *storage-profile-name*	指定されたストレージプロファイルのストレージプロファイルモードを開始します。
ステップ 3	UCS-A /org/storage-profile* # **create lun-set** *lun-set-name*	指定した名前の LUN 設定を作成します。
ステップ 4	UCS A/org/storage-profile/lun-set * # **set disk-slot-range** *disk-slot-range*	ディスクのスロット範囲を指定します。
ステップ 5	UCS A/org/storage-profile/lun-set * # **create virtual-drive-def**	仮想ドライブ設定コマンドモードを開始します。
ステップ 6	UCS A/org/storage-profile/lun-set/virtual-drive-def * # **set access-policy** {**blocked** |**platform-default** |**read-only** |**read-write**}	許可されたアクセスのタイプを指定します。
ステップ 7	UCS A/org/storage-profile/lun-set/virtual-drive-def * # **set drive-cache** {**disable** |**enable** |**no-change** |**platform-default**}	ドライブ キャッシュのタイプを指定します。
ステップ 8	UCS A/org/storage-profile/lun-set/virtual-drive-def * # **set io-policy** {**cached** |**direct** |**platform-default**}	入力/出力ポリシーのタイプを指定します。
ステップ 9	UCS A/org/storage-profile/lun-set/virtual-drive-def * # **set read-policy** {**normal** |**platform-default** |**read-ahead**}	先行読み出しキャッシュ モードを指定します。
ステップ 10	UCS A/org/storage-profile/lun-set/virtual-drive-def * # **set security** {**no** |**yes**}	仮想ドライブを保護するには、このオプションを設定します。
ステップ 11	UCS A/org/storage-profile/lun-set/virtual-drive-def * # **set strip-size** {**1024kb** |**128kb** |**16kb** |**256kb** |**32kb** |**512kb** |**64kb** |**8kb** |**platform-default**}	各物理ディスクにあるストライプデータ セグメントの部分を指定します。
ステップ 12	UCS A/org/storage-profile/lun-set/virtual-drive-def * # **set write-cache-policy**	書き込みポリシーのタイプを指定します。

	コマンドまたはアクション	目的
	{**always-write-back** |**platform-default** |**write-back-good-bbu** |**write-through**}	
ステップ 13	UCS A/org/storage-profile/lun-set/virtual-drive-def * #**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、LUN 設定を作成し、仮想ドライブを設定します。

```
UCS-A# scope org
UCS-A/org # enter storage-profile stroageprofile1
UCS-A/org/storage-profile # create lun-set lunset1
UCS-A/org/storage-profile/lun-set* # set disk-slot-range 2
UCS-A/org/storage-profile/lun-set* # create virtual-drive-def
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # set access-policy read-write
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # set drive-cache enable
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # set io-policy direct
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # set read-policy read-ahead
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # set security yes
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # set strip-size 512kb
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # set write-cache-policy
platform-default
UCS-A/org/storage-profile/lun-set/virtual-drive-def* # commit-buffer
```

次のタスク

サービス プロファイルとストレージ プロファイルを関連付けます

LUN セットの削除

LUN 設定は、組織レベルのストレージ プロファイル内に作成することも、サービス プロファイル レベルの専用ストレージ プロファイル内に削除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 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 # **enter storage-profile** *storage-profile-name*	指定されたストレージ プロファイルのストレージ プロファイル モードを開始します。
ステップ 3	UCS-A /org/storage-profile* # **delete lun-set** *lun-set-name*	指定した名前で LUN 設定を削除します。

	コマンドまたはアクション	目的
ステップ 4	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。

例

次の例では、LUN 設定を削除します。

```
UCS-A# scope org
UCS-A/org # enter storage-profile stroageprofile1
UCS-A/org/storage-profile # delete lun-set lunset1
UCS-A/org/storage-profile* # commit-buffer
```

Aero コントローラの構成

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設定にコミットします。

PCH コントローラ定義

PCH SSD コントローラ定義

Cisco UCS Manager プラットフォーム コントローラ ハブ（PCH）ソリッド ステート ドライブ（SSD）コントローラ定義によって提供されるストレージプロファイル内のローカルストレー

ジ設定で、単一 RAID または JBOD ディスク アレイ内にあるすべてのディスクを設定できます。

（注） PCH コントローラによって管理されているディスクを取り外したり挿入したりする場合は、サーバを再確認してください。

PCH コントローラ定義を設定することで、次の機能がサポートされます。

- オンボード PCH コントローラに接続された 2 台の内蔵 SSD 間で単一の LUN RAID を構成する機能
- コントローラを AHCI（JBOD）および SWRAID（RAID）の 2 つのモードで構成する方法
- 組み込みのローカル LUN および組み込みのローカル ディスク ブート ポリシーで PCH ストレージデバイスを構成する機能。これにより、サーバ内にその他のブート可能なローカル ストレージ デバイスが存在していても、ブート順序を正確に制御できます。ローカル LUN またはローカル JBOD オプションを使用して PCH ディスクから起動しないでください。
- 内蔵 SSD ドライブでのスクラブ ポリシーのサポート。これは SWRAID モードにのみ適用されます。これは PCH コントローラ モードの AHCI と NORAID には適用されません。『*UCS Manager Server Management Guide*』をご覧ください。
- 内蔵 SSD ドライブでのファームウェア アップグレードのサポート。
  - M4 以前のサーバの場合、ディスク ファームウェアのアップグレードは PCH コントローラが SWRAID モードの場合にのみサポートされます。AHCI モードではサポートされていません。
  - M5 以降のサーバの場合、ディスク ファームウェアのアップグレードは SWRAID モードと AHCI モードの両方でサポートされます（ただしCisco UCS C125 M5 サーバ、AHCI モードのみをサポートする場合を除く）。

ストレージ プロファイル ポリシーで PCH コントローラの SSD を設定できます。サービス プロファイルの関連付けが解除された後でも、LUN 設定を保存する保護設定を有効または無効にすることができます。コントローラ モードを選択します。PCH コントローラ コンフィギュレーションでは、RAID0 と RAID1 の 2 つの RAID オプションのみをサポートしています。コントローラに接続されたすべてのディスクが JBOD ディスクとして構成された AHCI モードでは、[No RAID] 設定オプションを使用してください。設定の導入は、ストレージプロファイルをサービス プロファイルへ関連付けるプロセスの一環として実行されます。

Cisco UCS Manager は、次の M4 サーバで PCH の管理対象内部 SSD をサポートします。

- UCSC-C240-M4L
- UCSC-C240-M4SX

Cisco UCS Manager は、すべての M5 および M6 サーバー（Cisco UCS C125 M5 サーバ を除く）で、以下のM.2 カード上の PCH 管理 SSD をサポートします。

- 240GB M.2 6G SATA SSD
- 960GB M.2 6G SATA SSD

（注） M5およびM6サーバーでは、コントローラ定義でのソフトウェアRAID設定とブート ポリシーでのレガシーブートモード設定を一緒に行うことはできません。コントローラ定義では、UEFIブートモードのみがソフトウェアRAID設定でサポートされています。この条件は、ドライブがブート ドライブとして使用されていない場合にも適用されます。

Cisco UCS Manager のブート ポリシーで PCH コントローラ定義を設定するために、PCH LUN および PCH Disk という 2 つの新しいデバイスを選択できます。**EmbeddedLocalLun** は SWRAID モードのブート デバイスを表し、**EmbeddedLocalDisk** は AHCI モードのブート デバイスを表します。

システムは、サポートされている SSD のスクラビング処理を行うために同じスクラブ ポリシーを使用します。スクラブが Yes の場合、設定された LUN は関連付けの解除または再検出の一環として破棄されます。スクラブが No の場合、設定された LUN は関連付けの解除および再検出の間に保存されます。

Cisco UCS Manager は、PCH コントローラが SWRAID モードの場合にのみ、内蔵 SSD のファームウェア アップグレードをサポートします。AHCI モードではサポートされていません。

FCH コントローラの設定

Fusion Controller Hub (FCH) SSD コントローラー定義は、AMD ベースのCisco UCS C125 M5 サーバストレージ プロファイルにローカル ストレージ構成を提供します。AMD プロセッサ ベースのサーバの場合、PCH コントローラは FCH コントローラと呼ばれます。コントローラ タイプは Cisco UCS Manager GUI の PCH として残ります。

FCH コントローラは、次の相違点を除く PCH コントローラと同じようにで動作します。

- FCH は、AHCI (JBOD) モードのみです。

（注） Cisco UCS Manager GUIは **RAID 0**、**RAID 1**としてRAIDサポートを表示しますが、Cisco UCS C125 M5 サーバは AHCI モードのみをサポートします。

（注） PCH コントローラによって管理されているディスクを取り外したり挿入したりする場合は、サーバを再確認してください。

- 2 つの FCH コントローラがあります。
  - 最初の PCH コントローラがフロント パネルの SATA ディスクを管理します (別の PCIe ストレージ コントローラがない場合)

• 2 台目の PCH コントローラが M.2 SSD を管理

（注） Cisco UCS C125 M5 サーバの場合、PCH ID は 3 と 4 です。

（注） このドキュメントの PCH コントローラに関する詳細情報と手順は、Intel ベースと AMD ベースの両方のサーバに適用できます。

ストレージ プロファイル PCH コントローラ定義の作成

ストレージ プロファイル下の組織レベルまたはサービス プロファイル レベルで PCH コントローラ定義を作成できます。

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* として */* を入力します。 （注） このタスクでは、ストレージ プロファイルが組織レベルにあることを想定しています。ストレージ プロファイルがサービス プロファイル レベルの場合に、サービス プロファイル下のストレージ プロファイル定義にスコープ設定する手順については、次の例を参照してください。
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	選択したストレージ プロファイルのストレージ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **create controller-def** *controller-definition-name*	PCH コントローラ定義を指定された名前で作成し、コントローラ定義コンフィギュレーション モードを開始します。
ステップ 4	UCS-A /org/storage-profile/controller-def* # **create controller-mode-config**	PCH コントローラ コンフィギュレーションを作成し、コントローラ モード

	コマンドまたはアクション	目的
		コンフィギュレーション モードを開始します。
ステップ 5	UCS-A /org/storage-profile/controller-def/controller-mode-config* # **set protect-config** {**yes**|**no**}	サーバは、サービス プロファイルとの関連付けが解除されても、PCH コントローラ内の設定を保持するかどうかを指定します。
ステップ 6	UCS-A /org/storage-profile/controller-def/controller-mode-config* # **set raid-mode** {**any-configuration** | **disable-local-storage** |**no-local-storage** | **no-raid** | **raid-0-striped** | **raid-1-mirrored** | **raid-5-striped-parity** | **raid-50--striped-parity-and-striped** | **raid-6-striped-dual-parity** | **raid-60-striped-dual-parity-and-striped** | **raid-10-mirrored-and-striped**}	PCH コントローラの RAID モードを指定します。
ステップ 7	UCS-A /org/storage-profile/controller-def/controller-mode-config* # **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

この例では、「storage-profile-A」という名前の組織レベル ストレージ プロファイルに、RAID モードが RAID 1 に設定されミラーリングされている、「raid1-controller」と呼ばれる PCH コントローラ定義を追加する方法を示します。

```
UCS-A# scope org /
UCS-A /org # scope storage-profile storage-profile-A
UCS-A /org/storage-profile # create controller-def raid1-controller
UCS-A /org/storage-profile/controller-def* # create controller-mode-config
UCS-A /org/storage-profile/controller-def/controller-mode-config* # set protect-config
yes
UCS-A /org/storage-profile/controller-def/controller-mode-config* # set raid-mode
raid-1-mirrored
UCS-A /org/storage-profile/controller-def/controller-mode-config* # commit buffer
```

この例では、「Service-Profile1」と呼ばれるサービス プロファイルにスコープし、ストレージ プロファイルを作成し、その後そのストレージ プロファイル内で「Raid60Ctrlr」と呼ばれる PCH コントローラ定義を作成する方法を示します。コントローラ定義の保護モードはオフになっており、RAID 60 ストライピング デュアル パリティとストライピングを使用します。

```
UCS-A /org/service-profile # scope org /
UCS-A /org # scope service-profile Service-Profile1
UCS-A /org/service-profile # create storage-profile-def
UCS-A /org/service-profile/storage-profile-def* # create controller-def Raid60Ctrlr
UCS-A /org/service-profile/storage-profile-def/controller-def* # create
controller-mode-config
```

```
UCS-A /org/service-profile/storage-profile-def/controller-def/controller-mode-config* #
 set protect-config no
UCS-A /org/service-profile/storage-profile-def/controller-def/controller-mode-config* #
 set raid-mode raid-60-striped-dual-parity-and-striped
UCS-A /org/service-profile/storage-profile-def/controller-def/controller-mode-config* #
 commit-buffer
```

ストレージ プロファイル PCH コントローラ定義の削除

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。 （注） このタスクでは、ストレージ プロファイルが組織レベルにあることを想定しています。ストレージ プロファイルがサービス プロファイル レベルの場合に、サービス プロファイル下のストレージ プロファイル定義にスコープ設定する手順については、次の例を参照してください。
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	選択したストレージ プロファイルのストレージ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **delete controller-def** *controller-definition-name*	PCH コントローラ定義を指定された名前で削除します。
ステップ 4	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。

例

この例では、「storage-profile-A」という名前の組織レベル ストレージプロファイルから「raid1-controller」と呼ばれる PCH コントローラ定義を削除する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope storage-profile storage-profile-A
```

```
UCS-A /org/storage-profile # delete controller-def raid1-controller
UCS-A /org/storage-profile* # commit-buffer
```

M.2 モジュールの移行

SWRAID での M.2 モジュールの移行

次の手順を実行して、SWRAID モードの M.2 モジュールを宛先サーバに移行します。

始める前に

コントローラ定義では、UEFI ブート モードのみがソフトウェア RAID 設定でサポートされています。この条件は、ドライブがブート ドライブとして使用されていない場合にも適用されます。ソース サーバと宛先サーバのブート モードがUEFIに設定されており、コントローラ定義がSWRAIDと同じ（R0/R1）に設定されていることを確認します。

手順

ステップ 1 サーバを正常にシャット ダウンします。

ステップ 2 M.2 モジュールを物理的に取り外します。

ソース サーバの SWRAID M.2 コントローラ設定でのソース サーバのブート モードは UEFI であることが必要です。組み込み型ディスクで UEFI ブート パラメータを使用し、宛先サーバのブート ポリシーを設定します。

ステップ 3 宛先サーバの M.2 モジュールにディスクを挿入します。

ステップ 4 サーバの電源をオンにします。

ステップ 5 サーバを再認識します。

AHCI モードでの M.2 モジュールの移行

次の手順を実行して、NORAID モードの M.2 モジュールを宛先サーバに移行します。

始める前に

- ソース サーバがレガシー ブート モード状態の場合、宛先サーバもレガシー ブート モードであり、コントローラ定義が [NORAID] で設定されていることを確認します。
- ソース サーバが UEFI ブート モード状態の場合、宛先サーバも UEFI ブート モードであり、コントローラ定義が [NORAID] で設定されていることを確認します。

手順

ステップ 1 サーバを正常にシャット ダウンします。

ステップ 2 M.2 モジュールを物理的に取り外します。

ステップ 3 次のいずれかを実行します。

- M.2 コントローラのディスクがソース サーバで UEFI のブート モードであった場合は、宛先サーバのブート ポリシーを UEFI ブート パラメータを使用して設定します。
- M.2 コントローラのディスクが、ソース サーバでレガシーのブート モードの場合、宛先サーバのブート ポリシーをレガシー モードに設定します。

ステップ 4 宛先サーバに M.2 モジュールを挿入します。

ステップ 5 サーバの電源をオンにします。

ステップ 6 サーバを再認識します。

（注） ディスクが不良である場合、サーバはディスク ステータスに [Not Detected] と表示します。「不良 M.2 ディスクの交換 （185 ページ）」を実行して、不良ディスクを交換します。

SWRAID ディスクの移行

次の手順を実行して、SWRAID モードの M.2 ディスクを宛先サーバに移行します。

始める前に

コントローラ定義では、UEFI ブート モードのみがソフトウェア RAID 設定でサポートされています。この条件は、ドライブがブート ドライブとして使用されていない場合にも適用されます。ソース サーバと宛先サーバのブート モードが UEFI に設定されており、コントローラ定義がSWRAIDと同じ（R0/R1）に設定されていることを確認します。

手順

ステップ 1 サーバを正常にシャット ダウンします。

ステップ 2 物理的に M.2 モジュールを取り外し、ディスクを取り出します。

ソース サーバでディスクを SWRAID として使用している場合、ブート モードは UEFI にする必要があり、組み込み型ディスクでUEFIブートパラメータを使用し、宛先サーバのブート ポリシーを設定します。

ステップ 3 宛先サーバの M.2 モジュールにディスクを挿入します。

ステップ 4 サーバの電源をオンにします。

ステップ 5 サーバを再認識します。

（注） ディスクの [Drive State] に [Online] と表示されている必要があります。ディスクが不良である場合、サーバはディスクを検出できないか、または [Drive State] に [Online] ではなく、[BAD]（または [FAILED]）と表示されます。「不良 M.2 ディスクの交換 （185 ページ）」を実行して、不良ディスクを交換します。

AHCI モードでの JBOD ディスクの移行

次の手順を実行して、NORAID モードの JBOD ディスクを宛先サーバに移行します。

始める前に

- ソース サーバがレガシー ブート モード状態の場合、宛先サーバもレガシー ブート モードであり、コントローラ定義が [NORAID] で設定されていることを確認します。
- ソース サーバが UEFI ブート モード状態の場合、宛先サーバも UEFI ブート モードであり、コントローラ定義が [NORAID] で設定されていることを確認します。

手順

ステップ 1 サーバのグレースフル シャット ダウンを実行します。

ステップ 2 物理的にモジュールを取り外し、M.2 ハード ディスクを取り出します。

ステップ 3 次のいずれかを実行します。

- M.2 コントローラのディスクがソース サーバで UEFI のブート モードであった場合は、宛先サーバのブート ポリシーを UEFI ブート パラメータを使用して設定します。
- M.2 コントローラのディスクが、ソース サーバでレガシーのブート モードの場合、宛先サーバのブート ポリシーをレガシー モードに設定します。

ステップ 4 宛先サーバの M.2 モジュールに M.2 ディスクを挿入します。

ステップ 5 サーバの電源をオンにします。

ステップ 6 サーバを再認識します。

不良 M.2 ディスクの交換

次の手順を実行して、不良 M.2 ディスクを交換します。

始める前に

SWRAID コント ローラの定義が設定されており、交換ディスクによって空ドライブがフォーマットされたことを確認します。

手順

ステップ 1 正常にサーバの電源を切ります。

ステップ 2 不良 M.2 ドライブを物理的に取り外します。**シリアル番号**と**ディスク スロット**を使用して不良ディスクを識別します。

ステップ 3 交換 M.2 ドライブを挿入します。

ステップ 4 サーバの電源をオンにします。

ステップ 5 ディスクが再構築されるまで待機してから、サーバを再確認します。

（注） SWRAID の再構築には、ディスク サイズ、ディスク速度、OS コンテンツ、およびその他のパラメータに応じて 35 ～ 75 分かかる場合があります。

AHCI は NORAID 設定であるため、再構築は適用されません。

（注） 障害のある M.2 ドライブを交換すると、もう一方のスロットにあるドライブの動作状態とドライブ状態は「低下」に、そして「再構築」に変わります。ドライブを通常の状態に戻すには、ブレードを停止して再稼働します。

ストレージ プロファイルとサービス プロファイルの関連付け

組織レベルで作成されたストレージ プロファイルは複数のサービス プロファイルから参照できるため、そのストレージプロファイルをサービスプロファイルと関連付けるためには、サービス プロファイル内での名前参照が必要となります。

重要 ストレージ プロファイルは組織レベルで定義することも、サービス プロファイルで（専用ストレージ プロファイルとして）定義することもできます。したがって、組織のストレージ プロファイルと専用ストレージ プロファイルの両方がある場合、サービス プロファイルはその両方から有効なローカル LUN を継承します。サービス プロファイルは、最大 2 つのローカル LUN を継承できます。

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* として / を入力します。
ステップ 2	UCS-A /org # **scope service-profile** *service-profile-name*	指定されたサービス プロファイル 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/service-profile # **set storage-profile-name** *storage-profile-name*	指定されたストレージ プロファイルとサービスプロファイルを関連付けます。 （注） ストレージ プロファイルからサービス プロファイルの関連付けを解除するには、**set storage-profile-name** コマンドを使用し、ストレージ プロファイル名として "" を指定します。
ステップ 4	UCS-A /org/service-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。

例

次に、ストレージプロファイルとサービスプロファイルを関連付ける例を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # set storage-profile-name stp2
```

次に、ストレージプロファイルからサービスプロファイルの関連付けを解除する例を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile # set storage-profile-name ""
```

サービス プロファイルに継承されたすべてのローカルLUNの詳細の表示

ストレージ プロファイルは、組織レベルで定義することも、サービス プロファイルの専用ストレージ プロファイルとして定義することもできます。したがって、組織のストレージ プロファイルと専用ストレージ プロファイルの両方がある場合、サービス プロファイルはその両方から有効なローカル LUN を継承します。サービス プロファイルは、最大 2 つのローカル LUN を継承できます。次のコマンドを使用することで、サービス プロファイルに継承されたすべてのローカル LUN の詳細を表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A /org/service-profile # **show local-lun-ref**	指定したサービス プロファイルに継承されたすべてのローカル LUN に関する次の詳細情報が表示されます。 • [Name]：ストレージ プロファイルでの LUN の名前。 • [Admin State]：ローカル LUN が展開されるかどうかを指定します。管理状態は、**Online**または**Undeployed** の場合があります。 ローカル LUN がサービス プロファイルによって参照されている場合、auto-deploy ステータスが **no-auto-deploy** であれば、管理状態は **Undeployed** になり、そうでない場合は、**Online** になります。ローカル LUN がサービス プロファイルで参照された後、そのローカルLUN の自動展開のステータスが変更されたとしても、サービス プロファイルに継承された LUN の管理状態には反映されません。 • [RAID Level]：使用されているディスク グループの RAID レベルの要約。 • [Provisioned Size (GB)]：ストレージ プロファイルに指定されている LUN のサイズ（GB 単位）。 • [Assigned Size (MB)]：UCSM によって割り当てられたサイズ（MB 単位）。 • [Config State]：LUN 設定の状態。状態は次のいずれかになります。 • [Applying]：管理状態は [Online] です。LUN はサーバに関連付けられていて、仮想ドライブが作成されているところです。

	コマンドまたはアクション	目的

		• [Applied]：管理状態は [Online] です。LUN はサーバに関連付けられていて、仮想ドライブが作成されました。
		• [Apply Failed]：管理状態は [Online] です。LUN はサーバに関連付けられていますが、仮想ドライブの作成が失敗しました。
		• [Not Applied]：LUN がサーバに関連付けられていないか、サーバに関連付けられていても、管理状態が [Undeployed] になっています。
		• [Not In Use]：サービス プロファイルは仮想ドライブを使用していますが、その仮想ドライブはサーバと関連付けられていません。
		
		• **Reference LUN**：事前プロビジョニングされた仮想ドライブ名または UCSM が生成した仮想デバイス名。
		• **Deploy Name**：展開後の仮想ドライブ名。
		• **ID**：仮想ドライブ ID。
		• [Drive State]：仮想ドライブの状態。以下の状態があります。
		  • 不明
		  • **Optimal**
		  • **Degraded**
		  • **Inoperable**
		  • **Partially Degraded**

例

```
UCS-A /org/service-profile # show local-lun-ref


Local LUN Ref:

    Profile LUN Name Admin State RAID Level             Provisioned Size (GB)  Assigned
 Size (MB)   Config State Referenced Lun Deploy Name ID          Drive State

    ---------------- ----------- ---------------------- ----------------------
-------------------- ------------ -------------- ----------- ----------- -----------

    luna             Online      RAID 0 Striped         1
        1024 Applied      luna-1         luna-1      1003        Optimal

    lunb             Online      RAID 0 Striped         1
        1024 Applied      lunb-1         lunb-1      1004        Optimal

UCS-A /org/service-profile #




Local LUN Ref:
    Name             Admin State RAID Level             Provisioned Size (GB)  Assigned
 Size (MB)   Config State Referenced Lun Deploy Name ID          Drive State
    ---------------- ----------- ---------------------- ----------------------
-------------------- ------------ -------------- ----------- ----------- -----------
    lun111           Online      RAID 0 Striped         30                     30720
             Applied      lun111-1       lun111-1    1001        Optimal
    lun201           Online      Unspecified            1                      0
             Not Applied
```

RAID コントローラの外部設定のインポート

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}	RAID コントローラ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/raid-controller # **set admin-state import-foreign-configuration**	Foreign Configuration 状態にあるローカル ディスクからの設定のインポートを可能にします。

例

次に、Foreign Configuration 状態にあるローカルディスクから外部設定をインポートする例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # set admin-state import-foreign-configuration
UCS-A /chassis/raid-controller* #
```

ローカル ディスクの設定操作

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}	RAID コントローラ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します。
ステップ 4	UCS A/chassis/raid-controller/local-disk # **set admin-state** {**clear-foreign-configuration** |**dedicated-hot-spare** [*admin vd id*] |**prepare-for-removal** |**remove-hot-spare** |**unconfigured-good** |**undo-prepare-for-removal**}	ローカル ディスクを次の状態のいずれかに設定します。 • **clear-foreign-configuration**：新しい設定に導入された時点でローカルディスク内に存在する外部設定を消去します。 • **dedicated-hot-spare**：ローカルディスクを専用ホット スペアとして指定します。割り当てることが可能な管理仮想ドライブ ID の範囲は 0 ～ 4294967295 です。 • **prepare-for-removal**：ローカルディスクをシャーシから削除する対象としてマークするように指定します。 • **remove-hot-spare**：ローカルディスクがホット スペアではなくなるように指定します。これは、不一致エ

	コマンドまたはアクション	目的
		ラーを解消するためだけに使用してください。 • **unconfigured-good**：ローカル ディスクが設定可能になるように指定します。 • **undo-prepare-for-removal**：ローカル ディスクをシャーシから削除する対象としてマークしないように指定します。

例

次に、ローカル ディスクから外部設定を消去する例を示します。

```
UCS-A /chassis/raid-controller/local-disk # set admin-state clear-foreign-configuration
```

次に、ローカル ディスクを専用ホット スペアとして指定する例を示します。

```
UCS-A /chassis/raid-controller/local-disk* # set admin-state dedicated-hot-spare 1001
```

次に、ローカルディスクをシャーシから削除する対象としてマークするように指定する例を示します。

```
UCS-A /chassis/raid-controller/local-disk* # set admin-state prepare-for-removal
```

次に、ローカルディスクをホットスペアとして削除する対象としてマークするように指定する例を示します。

```
UCS-A /chassis/raid-controller/local-disk* # set admin-state remove-hot-spare
```

次に、ローカルディスクが有効であるが使用のための設定がされていない状態になるように指定する例を示します。

```
UCS-A /chassis/raid-controller/local-disk* # set admin-state unconfigured-good
```

次に、ローカルディスクをシャーシから削除する対象としてマークしないように指定する例を示します。

```
UCS-A /chassis/raid-controller/local-disk* # set admin-state undo-prepare-for-removal
```

仮想ドライブ プロパティの設定

1 つのディスク グループ内のすべての仮想ドライブを単一のディスク グループ ポリシーを使用して管理する必要があります。

これらのプロパティをサポートしないサーバに関連付けようとすると、設定エラーが生成されます。

次のストレージ コントローラだけがこれらのプロパティをサポートします。

- LSI 6G MegaRAID SAS 9266-8i
- LSI 6G MegaRAID SAS 9271-8i
- LSI 6G MegaRAID 9265-8i
- LSI MegaRAID SAS 2208 ROMB
- LSI MegaRAID SAS 9361-8i

LSI MegaRAID SAS 2208 ROMB コントローラの場合、これらのプロパティは、B420-M3 ブレードサーバだけでサポートされます。他のコントローラでは、これらのプロパティは複数のラック サーバでサポートされます。

（注） Cisco ブート最適化 M. 2 Raid コントローラ (HWRAID) を設定している場合は、 次のようになります。

- 作成できる仮想ドライブは 1 つのみです。
- **ストリップ サイズ** には、**64 KB** または **32KB** を選択します。他の値を選択すると、設定エラーになります。
- **access-policy**、**read-policy**、**write-cache-policy**、**io-policy**、および **drive-cache** には、**platform-default** を選択します。他の値を選択すると、設定エラーになります。

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 disk-group-config-policy** *disk-group-name*	指定されたディスク グループ名のディスク グループ設定ポリシーモードを開始します。
ステップ 3	UCS-A /org/disk-group-config-policy* # **create virtual-drive-def**	仮想ドライブ定義を作成して、仮想ドライブ定義モードを開始します。
ステップ 4	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set access-policy** *policy-type*	アクセスポリシーを指定します。次のいずれかになります。 • blocked • platform-default

	コマンドまたはアクション	目的
		• read-only: • read-write
ステップ 5	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set drive-cache** *state*	ドライブ キャッシュの状態を指定します。次のいずれかになります。 • 有効化 • 無効化 • no-change • platform-default 重要　Cisco UCS リリース 2.5 では、ドライブ キャッシュの状態を変更できません。選択されたドライブ キャッシュの状態に関係なく、**platform-default** のまま変化しません。
ステップ 6	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set io-policy** *policy-type*	I/O ポリシーを指定します。次のいずれかになります。 • cached • direct • platform-default
ステップ 7	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set read-policy** *policy-type*	読み取りポリシーを指定します。次のいずれかになります。 • normal • platform-default • read-ahead
ステップ 8	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set strip-size** *strip-size*	ストリップ サイズを指定します。次のいずれかになります。 • 64 KB • 128 KB • 256 KB • 512 KB • 1024 KB

	コマンドまたはアクション	目的
		• platform-default
ステップ 9	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **set write-cache-policy** *policy-type*	書き込みキャッシュ ポリシーを指定します。次のいずれかになります。 • always-write-back • platform-default • write-back-good-bbu • write-through
ステップ 10	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **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。
ステップ 11	UCS-A /org/disk-group-config-policy/virtual-drive-def* # **show**	設定された仮想ドライブ プロパティを表示します。

例

次に、仮想ディスク プロパティを設定する例を示します。

```
UCS-A# scope org
UCS-A /org # scope disk-group-config-policy raid0policy
UCS-A /org/disk-group-config-policy # create virtual-drive-def
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set access-policy read-write
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set drive-cache enable
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set io-policy cached
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set read-policy normal
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set strip-size 1024
UCS-A /org/disk-group-config-policy/virtual-drive-def* # set write-cache-policy
write-through
UCS-A /org/disk-group-config-policy/virtual-drive-def* # commit-buffer
UCS-A /org/disk-group-config-policy/virtual-drive-def # show

Virtual Drive Def:
    Strip Size (KB): 1024KB
    Access Policy: Read Write
    Read Policy: Normal
    Configured Write Cache Policy: Write Through
    IO Policy: Cached
    Drive Cache: Enable
UCS-A /org/disk-group-config-policy/virtual-drive-def #
```

次のタスク

ストレージ プロファイルの作成

孤立仮想ドライブの削除

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}	RAID コントローラ シャーシ モードを開始します。
ステップ 3	（任意） UCS-A /chassis/raid-controller # **delete virtual-drive id** *virtual-drive-id*	指定された仮想ドライブ ID を持つ孤立仮想ドライブを削除します。
ステップ 4	（任意） UCS-A /chassis/raid-controller # **delete virtual-drive name** *virtual-drive-id*	指定された仮想ドライブ名を持つ孤立仮想ドライブを削除します。
ステップ 5	（任意） UCS-A /chassis/raid-controller # **scope virtual-drive** *virtual-drive-id*	指定された孤立仮想ドライブの仮想ドライブ モードを開始します。
ステップ 6	UCS-A /chassis/raid-controller/virtual-drive # **set admin-state delete**	孤立仮想ドライブを削除します。
ステップ 7	UCS-A /chassis/raid-controller/virtual-drive # **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、仮想ドライブ ID を指定して孤立仮想ドライブを削除する例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # show virtual-drive

Virtual Drive:
    ID: 1001
    Name: lun111-1
    Block Size: 512
    Blocks: 62914560
    Size (MB): 30720
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 0
    Change Qualifier: No Change
    Config State: Applied
    Deploy Action: No Action

    ID: 1002
    Name: luna-1
    Block Size: 512
    Blocks: 2097152
    Size (MB): 1024
    Operability: Operable
    Presence: Equipped
```

```
    Oper Device ID: 1
    Change Qualifier: No Change
    Config State: Orphaned
    Deploy Action: No Action

    ID: 1003
    Name: lunb-1
    Block Size: 512
    Blocks: 2097152
    Size (MB): 1024
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 2
    Change Qualifier: No Change
    Config State: Orphaned
    Deploy Action: No Action

    ID: 1004
    Name: lunb-2
    Block Size: 512
    Blocks: 2097152
    Size (MB): 1024
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 3
    Change Qualifier: No Change
    Config State: Orphaned
    Deploy Action: No Action

    ID: 1005
    Name: luna-2
    Block Size: 512
    Blocks: 2097152
    Size (MB): 1024
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 4
    Change Qualifier: No Change
    Config State: Orphaned
    Deploy Action: No Action

...

UCS-A /chassis/raid-controller # delete virtual-drive id 1002
Warning: When committed, the virtual drive will be deleted, which may result in data
loss.

UCS-A /chassis/raid-controller # commit-buffer
```

次に、仮想ドライブ名を指定して孤立仮想ドライブを削除する例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # show virtual-drive

Virtual Drive:
    ID: 1001
    Name: lun111-1
    Block Size: 512
    Blocks: 62914560
    Size (MB): 30720
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 0
```

```
    Change Qualifier: No Change
    Config State: Applied
    Deploy Action: No Action

    ID: 1003
    Name: lunb-1
    Block Size: 512
    Blocks: 2097152
    Size (MB): 1024
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 2
    Change Qualifier: No Change
    Config State: Orphaned
    Deploy Action: No Action

    ID: 1004
    Name: lunb-2
    Block Size: 512
    Blocks: 2097152
    Size (MB): 1024
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 3
    Change Qualifier: No Change
    Config State: Orphaned
    Deploy Action: No Action

    ID: 1005
    Name: luna-2
    Block Size: 512
    Blocks: 2097152
    Size (MB): 1024
    Operability: Operable
    Presence: Equipped
    Oper Device ID: 4
    Change Qualifier: No Change
    Config State: Orphaned
    Deploy Action: No Action

...

UCS-A /chassis/raid-controller # delete virtual-drive name lunb-1
Warning: When committed, the virtual drive will be deleted, which may result in data
loss.

UCS-A /chassis/raid-controller # commit-buffer
```

次に、管理状態を設定して孤立仮想ドライブを削除する例を示します。

```
UCS-A# scope chassis 1
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # scope virtual-drive 1004
UCS-A /chassis/raid-controller/virtual-drive # set admin-state delete

Warning: When committed, the virtual drive will be deleted, which may result in data
loss.

UCS-A /chassis/raid-controller/virtual-drive # commit-buffer
```

孤立仮想ドライブの名前変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope chassis** *chassis-num*	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **scope raid-controller** *raid-contr-id* {**sas** | **sata**}	RAID コントローラ シャーシ モードを開始します。
ステップ 3	UCS-A /chassis/raid-controller # **scope virtual-drive** *virtual-drive-id*	指定された仮想ドライブの仮想ドライブ モードを開始します。
ステップ 4	UCS-A /chassis/raid-controller/virtual-drive # **set name** *virtual-drive-name*	孤立仮想ドライブの名前を指定します。
ステップ 5	UCS-A /chassis/raid-controller/virtual-drive # **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、孤立仮想ドライブの名前を指定する例を示します。

```
UCS-A /chassis # scope raid-controller 1 sas
UCS-A /chassis/raid-controller # scope virtual-drive 1060
UCS-A /chassis/raid-controller/virtual-drive* # set name vd1
UCS-A /chassis/raid-controller/virtual-drive* # commit-buffer
```

ローカル ストレージのブート ポリシー

ストレージ コントローラのプライマリ ブート デバイスを、ローカル LUN または JBOD ディスクとして指定できます。各ストレージ コントローラには、1 つのプライマリ ブート デバイスを設定できます。ただし、ストレージ プロファイルでは、プライマリ ブート LUN として 1 つのデバイスのみを設定できます。

4.0(4a) 以降、Cisco UCS Manager は Marvell 88SE92xx PCIe から SATA 6Gb/s コントローラ (UCS-M2-HWRAID) を搭載した Cisco ブート最適化 M.2 コントローラをサポートしています。コントローラは UEFI ブート モードのみをサポートします。

ブート ポリシーのローカル ストレージ オプションは、Cisco ブート最適化 M. 2 Raid コントローラの SATA ドライブからのブートをサポートします。

また、ブート ポリシーの組み込みローカル ストレージ オプションは、Cisco ブート最適化 M. 2 Raid コントローラの SATA ドライブからのブートをサポートします。プライマリおよびセカンダ リタイプは、特に 2 台の SATA ドライブから起動します。

（注） Cisco UCS C3260 M3 サーバでは、Cisco UCS Manager GUI を使用したブート ポリシーへのローカル LUN の追加時に [Local LUN Image Path] のオプションとして [Any] はサポートされていません。Cisco UCS Manager CLIでは Cisco UCS C3260 コマンド オプションは **local-any**M3 サーバノードでサポートされていません。

ローカル LUN のブート ポリシーの設定

（注） Cisco UCS Manager リリース 2.5 では、JBOD をブート デバイスとして設定できません。

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 boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy # **create storage**	ブート ポリシーのストレージ ブートを作成し、組織ブート ポリシー ストレージ モードを開始します。
ステップ 4	UCS-A /org/boot-policy/storage # **create local**	ローカルストレージ場所を作成し、ブート ポリシーのローカル ストレージ モードを開始します。
ステップ 5	UCS-A /org/boot-policy/storage/local/ # **create local-lun**	ローカル ハード ディスク ドライブをローカルストレージとして指定します。
ステップ 6	UCS-A /org/boot-policy/storage/local/local-lun # **create local-lun-image-path** {**primary** | **secondary**}	指定した LUN のブート順序を指定します。 **重要** Cisco UCS Manager リリース 2.2(4) は **secondary** ブート順序をサポートしていません。
ステップ 7	UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path # **set lunname** *lun_name*	ブートを開始する LUN の名前を指定します。

	コマンドまたはアクション	目的
ステップ 8	UCS-A /org/boot-policy/storage/local/*local-storage-device* # **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、lab1-boot-policy という名前のブート ポリシーを作成して、そのポリシー用のローカル ハード ディスク ドライブ ブートを作成し、ブート順序とブートを開始する LUN を指定して、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* # scope boot-policy lab1-boot-policy
UCS-A /org/boot-policy* # create storage
UCS-A /org/boot-policy/storage* # create local
UCS-A /org/boot-policy/storage/local* # create local-lun
UCS-A /org/boot-policy/storage/local/local-lun # create local-lun-image-path primary
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path # set lunname luna
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path # commit-buffer
UCS-A /org/boot-policy/storage/local/local-lun/local-lun-image-path #
```

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

ローカル JBOD ディスクのブート 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 # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy # **create storage**	ブート ポリシーのストレージ ブートを作成し、組織ブート ポリシー ストレージ モードを開始します。
ステップ 4	UCS-A /org/boot-policy/storage # **create local**	ローカルストレージ場所を作成し、ブート ポリシーのローカル ストレージ モードを開始します。
ステップ 5	UCS-A /org/boot-policy/storage/local/ # **create local-jbod**	ローカル JBOD ディスクをローカル ストレージとして指定します。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /org/boot-policy/storage/local/local-jbod # **create local-lun-image-path***{primary | secondary}*	
ステップ 7	UCS-A /org/boot-policy/storage/local/local-jbod/local-disk-image-path # **set slotnumber** *slotnumber*	
ステップ 8	UCS-A /org/boot-policy/storage/local/local-jbod/local-disk-image-path* # **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、lab1-boot-policy という名前のブート ポリシーを作成して、そのポリシー用のローカル JBOD ディスク ドライブ ブートを作成し、ブート順序とブートを開始する JBOD を指定して、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* # scope boot-policy lab1-boot-policy
UCS-A /org/boot-policy* # create storage
UCS-A /org/boot-policy/storage* # create local
UCS-A /org/boot-policy/storage/local/ # create local-jbod
UCS-A /org/boot-policy/storage/local/local-jbod* # create local-disk-image-path primary
UCS-A /org/boot-policy/storage/local/local-jbod/local-disk-image-path # set slotnumber
1
UCS-A /org/boot-policy/storage/local/local-jbod/local-disk-image-path* # commit-buffer
UCS-A /org/boot-policy/storage/local/local-jbod/local-disk-image-path #
```

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

組み込みのローカル LUN のブート ポリシーの設定

（注） 1 つのブート可能 LUN をプライマリまたはセカンダリ ブート デバイスとして指定します。ブート可能 LUN をプライマリとセカンダリの両方の起動デバイスとして指定すると、起動ポリシーによってサービス プロファイル設定エラーが発生します。

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] に / を入力します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy # **create storage**	ブート ポリシーのストレージ ブートを作成し、組織ブート ポリシー ストレージ モードを開始します。
ステップ 4	UCS-A /org/boot-policy/storage # **create local**	ローカルストレージ場所を作成し、ブート ポリシーのローカル ストレージ モードを開始します。
ステップ 5	UCS-A /org/boot-policy/storage/local/ # **create embedded-local-lun**	埋め込まれたローカル LUN をローカル ストレージとして指定します。
ステップ 6	UCS A/org/boot-policy/storage/local/embedded-local-lun * # **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、lab1-boot-policy という名前のブート ポリシーを作成して、そのポリシー用の埋め込み LUN ブートを作成し、ブート順序とブートを開始する LUN を指定して、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* # scope boot-policy lab1-boot-policy
UCS-A /org/boot-policy* # create storage
UCS-A /org/boot-policy/storage* # create local
UCS-A /org/boot-policy/storage/local/ # create embedded-local-lun
UCS-A /org/boot-policy/storage/local/embedded-local-lun* # commit-buffer
UCS-A /org/boot-policy/storage/local/embedded-local-lun #
```

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

組み込みのローカル ディスクのブート ポリシーの設定

（注） Cisco UCS C125 M5 サーバ の場合、独立した PCIe ストレージ コントローラがない場合は、内蔵ローカル ディスクの起動ポリシーを設定してはいけません。代わりに、**[Add Local Disk]**オプションを使用します。

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] に / を入力します。
ステップ 2	UCS-A /org # **scope boot-policy** *policy-name*	指定されたブート ポリシーの組織ブート ポリシー モードを開始します。
ステップ 3	UCS-A /org/boot-policy # **create storage**	ブート ポリシーのストレージ ブートを作成し、組織ブート ポリシー ストレージ モードを開始します。
ステップ 4	UCS-A /org/boot-policy/storage # **create local**	ローカルストレージ場所を作成し、ブート ポリシーのローカル ストレージ モードを開始します。
ステップ 5	UCS-A /org/boot-policy/storage/local/ # **create embedded-local-jbod**	埋め込まれたローカル JBOD をローカル ストレージとして指定します。
ステップ 6	UCS A/org/boot-policy/storage/local/embedded-local-jbod * # **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、lab1-boot-policy という名前のブート ポリシーを作成して、そのポリシー用の埋め込まれた JBOD ディスク ドライブ ブートを作成し、ブート順序とブートを開始する JBOD を指定して、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* # scope boot-policy lab1-boot-policy
UCS-A /org/boot-policy* # create storage
UCS-A /org/boot-policy/storage* # create local
UCS-A /org/boot-policy/storage/local/ # create embedded-local-jbod
UCS-A /org/boot-policy/storage/local/embedded-local-jbod* # commit-buffer
UCS-A /org/boot-policy/storage/local/embedded-local-jbod #
```

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

サービス プロファイル内のローカル LUN 操作

サービス プロファイルはサービス プロファイル テンプレートから作成されますが、次の操作は個別のサービス プロファイル レベルでローカル LUN ごとに実行できます。

- LUN 名の事前プロビジョニングまたは孤立 LUN の要求 （205 ページ）

- LUN の展開および展開解除 （206 ページ）
- サービス プロファイルで参照されている LUN の名前変更 （207 ページ）

（注） LUN名の事前プロビジョニング、孤立LUNの要求、およびLUNの展開または展開解除後は、サーバがリブートされます。

LUN 名の事前プロビジョニングまたは孤立 LUN の要求

set ref-name コマンドを使用して、LUN 名を事前プロビジョニングしたり、孤立 LUN を要求したりできます。LUN 名の事前プロビジョニングや孤立 LUN の要求は、LUN の管理状態が **Undeployed** の場合にだけ実行できます。 また、LUN の管理状態を手動で **Undeployed** に変更し、孤立 LUN を要求することもできます。

重要 この操作によって、サーバがリブートされます。

LUN 名が空の場合は、要求する前に LUN 名を設定します。

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 service-profile** *service-profile-name*	指定されたサービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile# **enter local-lun-ref** *lun-name*	指定された LUN を入力します。
ステップ 4	UCS-A /org/service-profile/local-lun-ref# **set ref-name** *ref-lun-name*	参照 LUN 名を設定します。 事前プロビジョニングする LUN 名がすでに存在し、その LUN が孤立している場合、その LUN はサービス プロファイルによって要求されます。名前を事前にプロビジョニングする LUN が存在しない場合、指定した名前の LUN が新規に作成されます。

- LUN が存在していて、孤立していない場合は、設定エラーが発生します。

- LUN がすでに参照されている場合に、参照名を変更すると、古い LUN が解放され、その参照名で LUN が要求または作成されます。古い LUN は、サーバから LUN 参照が削除された段階で孤立としてマークされます。

例

次に、LUN 名を事前プロビジョニングする例を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile* # enter local-lun-ref lun1
UCS-A /org/service-profile/local-lun-ref* # set ref-name lun2
```

LUN の展開および展開解除

admin-state コマンドを使用して、LUN を展開または展開解除することができます。ローカル LUN の管理状態が [Undeployed] の場合、LUN の参照は削除されていて、LUN は展開されていません。

重要 この操作によって、サーバがリブートされます。

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# **scope service-profile** *service-profile-name*	指定されたサービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile# **enter local-lun-ref** *lun-name*	指定された LUN を入力します。
ステップ 4	UCS-A /org/service-profile/local-lun-ref# **set admin-state** {**online** | **undeployed**}	指定された LUN の管理状態を **online** または **undeployed** に設定します。 LUN がすでに参照済みで、その管理状態が **undeployed** に設定されている場合は、古い LUN が解放されます。古い LUN は、LUN 参照がサーバから削除された後に孤立としてマークされます。

例

次に、LUN を展開する例を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile* # enter local-lun-ref lun1
UCS-A /org/service-profile/local-lun-ref* # set admin-state online
```

次に、LUN を展開解除する例を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile* # enter local-lun-ref lun1
UCS-A /org/service-profile/local-lun-ref* # set admin-state undeployed
```

サービス プロファイルで参照されている LUN の名前変更

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 service-profile** *service-profile-name*	指定されたサービス プロファイル モードを開始します。
ステップ 3	UCS-A /org/service-profile# **enter local-lun-ref** *lun-name*	指定された LUN を入力します。
ステップ 4	UCS-A /org/service-profile/local-lun-ref# **set name**	参照 LUN の名前を変更します。

例

次に、サービス プロファイルから参照される LUN の名前を変更する例を示します。

```
UCS-A# scope org
UCS-A /org # scope service-profile sp1
UCS-A /org/service-profile* # enter local-lun-ref lun1
UCS-A /org/service-profile/local-lun-ref* # set name lun11
```

第 11 章

SD カード サポートの設定

この章は、次の内容で構成されています。

FlexFlash セキュア デジタル カードのサポート

概要

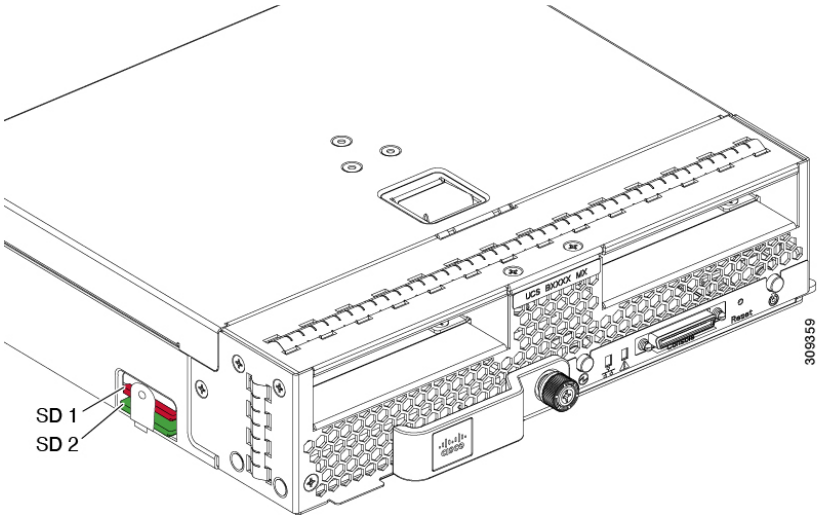
Cisco UCSB シリーズ、C シリーズ M4 以降、および S シリーズ M4 サーバーは、内部セキュア デジタル（SD）メモリ カードをサポートしています。SD カードは、Cisco Flexible Flash ストレージ コントローラ（SD カード用スロットが 2 つある PCI ベースのコントローラ）によってホストされます。カードには、HV と呼ばれる単一のパーティションが含まれます。FlexFlash が有効な場合、Cisco UCS Manager では、BIOS とホスト ホスト オペレーティング システムのどちらに対しても、HV パーティションを USB ドライブとして表示します。

提供される一方または両方の SD カード スロットを装着できます。SD カードが 2 つ装着されている場合は、ミラー化モードで使用できます。

（注） サーバー内で異なる容量のカードを混在させないでください。

SD カードはオペレーティング システムのブート イメージやその他の情報を保存するために使用できます。次の図に、SD カード スロットを示します。

図 *3: SD* カード スロット



FlexFlash はデフォルトでディセーブルになっています。サービス プロファイルで使用されるローカル ディスク ポリシーで FlexFlash をイネーブルにできます。FlexFlash がローカル ディスク ポリシーで有効と定義され、サーバーが SD カードをサポートしている場合、FlexFlash コントローラはサービス プロファイルを関連付ける際に有効になります。サーバーが SD カードをサポートしていない場合や CIMC バージョンが古い場合は、構成エラー メッセージが表示されます。

サポートされるサーバーの FlexFlash を無効にすると、ハイパーバイザまたは HV パーティションはホストからすぐに切断されます。FlexFlash コントローラは、関連サービス プロファイルの関連付け解除の一環としてもディセーブルになります。

FlexFlash コントローラはデュアル SD カード用の RAID-1 をサポートします。FlexFlash スクラブ ポリシーは、両方のカードの HV パーティションを削除し、そのカードを正常な RAID 状態にすることができます。

RAID ペアの新しい SD カードを設定し、次の方法のいずれかを使用してそれらをフォーマットすることができます。

- SD カードをフォーマットします。詳細な情報については
- 関連付けられているサーバーの場合、FlexFlash スクラブ ポリシーを作成し、サーバーからサービス プロファイルの関連付けを解除します。関連付けられていないサーバーの場合、FlexFlash スクラブ ポリシーを作成し、デフォルトのスクラブのポリシーを変更した後でサーバーを再認識させます。

  『*Cisco UCS Manager Server Management Guide*』の「*Scrub Policy Settings*」セクションには、スクラブ ポリシーの使用方法に関する詳細情報が記載されています。

（注） ペアリングが完了したらすぐにスクラブ ポリシーをディセーブルにします。

HV パーティションから起動するには、SD カードがサービス プロファイルで使用されるブート ポリシーで定義されている必要があります。

FlexFlash ファームウェア管理

FlexFlash コントローラ ファームウェアは、CIMC イメージの一部としてバンドルされます。CIMC をアップグレードする際に、最新のファームウェア バージョンが FlexFlash コントローラで使用可能な場合、コントローラは管理されなくなり、FlexFlashインベントリには、[Controller State] が [Waiting For User Action] として、[Controller Health] が [Old Firmware Running] として表示されます。FlexFlash コントローラのファームウェアをアップグレードするには、ボード コントローラの更新を行う必要があります。詳細については、該当する『 *Cisco UCS B-Series Firmware Management Guide*』、次の URL で入手できます。
http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html を参照してください。

Cisco Flexible Flash ストレージ コントローラの制約事項：

- Cisco Flexible Flash ストレージ コントローラは 16 GB、32 GB および 64 GB の SD カードのみをサポートしています。
- ラック サーバーの SD カードをブレード サーバーで使用したり、ブレード サーバーの SD カードをラック サーバーで使用することは推奨されません。サーバー タイプ間での SD カードの交換は SD カードのデータ損失につながる可能性があります。
- 一部のCisco UCS C シリーズ ラックマウント サーバーには、4 つのパーティション（HV、HUU、SCU、ドライバ）を持つ SD カードが搭載されています。Cisco UCS Managerでは HV パーティションのみが表示されます。FlexFlash スクラブ ポリシーを使用して、4 つのパーティションを持つ SD カードを単一 HV パーティション カードに移行できます。
- FlexFlash コントローラは RAID-1 同期（ミラー再構築）をサポートしません。SD カードがRAIDデグレード状態である場合、あるいはメタデータエラーがコントローラによって報告された場合は、FlexFlash スクラブ ポリシーを実行して RAID のためのカードを組み合わせる必要があります。FlexFlash のスクラブ ポリシーの詳細については、「サーバー関連ポリシー」を参照してください。次の条件によってRAIDデグレードやメタデータエラーが引き起こされる可能性があります。
  - サーバーの 1 つのスロットにすでに SD カードが装着されているときに、別のスロットに新しいまたは使用されていた SD カードを挿入する。
  - 異なるサーバーの 2 つの SD カードを挿入する。
- サーバーのファームウェア バージョンは、2.2(1a) 以上が必要です。

FlexUtil セキュア デジタル カードのサポート

C シリーズ M5 ラックマウント サーバは、ストレージ用のマイクロ SD (FlexUtil) メモリ カードをサポートします。ただし、UCS Manager は、MICRO-SD カードの管理サポートを提供していません。

第 12 章

ミニストレージ

ミニストレージ

ミニストレージスロットは、Cisco UCS M5 ブレードおよびラック サーバにある新しいスロットです。このスロットは空でも、SD ストレージ モジュールまたは M.2 SATA モジュールを装着してもかまいません。

（注） Cisco UCS Manager は、Micro-SD カードをサポートしていません。

ミニストレージ SD モジュールは、内蔵 SD コントローラと 2 つの SD カード スロットから構成されています。これらのカードには、RAID 1 の機能が備わっています。

ミニ M.2 SATA モジュールは、2 つの SATA スロットから構成されています。サーバ上にある PCH コントローラは、このモジュール上の SATA ドライブを制御します。

4.0(4a) 以降、Cisco UCS Manager は ミニ ストレージの Marvell 88SE92xx PCIe から SATA 6Gb/s コントローラ (UCS-M2-HWRAID) を搭載した Cisco ブート最適化 M.2 コントローラをサポートしています。

Cisco UCS Manager を使用してミニ ストレージ モジュールのインベントリ登録および管理を行うことができます。

ミニストレージ プロパティの表示

ミニ ストレージ モジュールは、M5 以降のサーバでのみサポートされています。

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** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **show mini-storage** [**detail**]	指定したサーバのミニ ストレージ モジュールに関する詳細情報を表示します。

例

この例では、サーバ 6 のミニ ストレージ モジュールに関する詳細情報が表示されます。

```
UCS-A# scope server 1/6
UCS-A /chassis/server # show mini-storage detail

Mini Storage Module:
    ID: 1
    Type: M2
    Model: UCS-MSTOR-M2
    Vendor: Cisco Systems Inc
    HW Rev: 0
    Serial: FCH2050JDHM
    VID: V00
    Part Number: 73-17926-04
    Product Name: Cisco UCS Mini-Storage Carrier for M.2
    Caption: Cisco UCS Mini-Storage Carrier for M.2 (holds up to 2)
    Description: Dual M.2 Mini-Storage Carrier (holds up to 2 M.2 modules)
```

ミニ ストレージのストレージ コントローラの表示

ミニ ストレージ モジュールは、M5 以降のサーバでのみサポートされています。

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** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **scope mini-storage** *id* **m2** | **sd**	指定されたサーバおよびミニ メモリカードの種類のミニ ストレージ モードを開始します。
ステップ 3	UCS-A /chassis/server/mini-storage # **show referenced-controller** [**detail**]	指定したサーバのミニ ストレージ モジュールで参照されるストレージ コントローラに関する情報を表示します。

例

この例では、サーバ 6 で M.2 ミニ メモリ カードのストレージ コントローラに関する情報が表示されます。

```
UCS-A# scope server 1/6
UCS-A /chassis/server # scope mini-storage 1 m2
UCS-A /chassis/server/mini-storage # show referenced-controller detail

Referenced Controller:
    ID: 1
    Type: PCH
```

この例では、サーバ 3 で SD ミニ メモリ カードのストレージ コントローラに関する情報が表示されます。

```
UCS-A# scope server 1/3
UCS-A /chassis/server # scope mini-storage 1 sd
UCS-A /chassis/server/mini-storage # show referenced-controller detail

Referenced Controller:
    ID: 1
    Type: PCH
```

第 13 章

SED セキュリティ ポリシー

自己暗号化ドライブのセキュリティ ポリシー

自己暗号化ドライブ（SED）には、リアルタイムで着信データを暗号化し、送信データを復号化する特殊なハードウェアが搭載されています。ディスク上のデータは常にディスクで暗号化され、暗号化された形式で格納されます。暗号化されたデータはディスクから読み出す際に常に復号化されます。メディア暗号化キーがこの暗号化と復号化を制御します。このキーはプロセッサやメモリには保存されません。 Cisco UCS Manager は、Cisco UCS C シリーズと B-シリーズ M5 サーバ、および S シリーズのサーバの SED セキュリティ ポリシーをサポートしています。

SED は、セキュリティ キーを指定してロックしなければなりません。このセキュリティ キーはキー暗号化キーまたは認証パスフレーズとも呼ばれ、メディア暗号化キーの暗号化に使用されます。ディスクがロックされていない場合は、データの取得にキーは必要ありません。

Cisco UCS Manager では、セキュリティ キーをローカルででも、リモートからでも設定できます。ローカルでキーを設定した場合、そのキーを覚えておく必要があります。キーを忘れた場合、それを取得することはできず、データが失われます。キー管理サーバ (KMIP サーバとも呼ばれる) を使用すると、リモートでキーを設定できます。この方法により、ローカル管理でのキーの保管と取得に伴なう問題に対処することができます。

SED の暗号化と復号化はハードウェアを介して行われます。したがって、システムの全体的なパフォーマンスには影響がありません。SED は、瞬間的な暗号化消去によってディスクの廃止コストや再配置コストを削減します。暗号化消去は、メディア暗号キーを変更することによって実行されます。ディスクのメディア暗号キーが変更されると、そのディスク上のデータは復号不能になるので、ただちにデータが使用不可になります。Cisco UCS Manager リリース 3.1(3) では、SED は C シリーズ サーバと S シリーズ サーバにディスク盗難防止機能を提供します。HX サーバについては、SED はノード盗難防止機能を提供します。Cisco UCS Manager リリース 4.0(2) では、UCS B シリーズ M5 サーバに SED セキュリティ ポリシーを拡張します。

コントローラとディスクのセキュリティ フラグ

セキュリティ フラグは、ストレージ コントローラとディスクの現在のセキュリティ ステータスを示します。

ストレージ コントローラとディスクには、次のセキュリティ フラグがあります。

- Security Capable：コントローラまたはディスクが SED 管理をサポートできることを示します。
- Security Enable：コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティがデバイス上で有効であることを示します。このフラグは、セキュリティポリシーを設定してサーバに関連付け、コントローラとディスクを保護しているときに設定されます。HX デバイスでは、このフラグは設定されません。
- Secured：コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティが HX デバイス上で有効であることを示します。

次のセキュリティ フラグは、ストレージ ディスクにのみ適用されます。

- Locked：ディスク キーがコントローラ上のキーと一致していないことを示します。これは、異なるキーでプログラムされたサーバ間でディスクを移動すると発生します。ロックされたディスク上のデータにはアクセスできないため、オペレーティング システムがディスクを使用できません。このディスクを使用するには、ディスクのロックを解除するか、または外部設定を安全に消去します。
- Foreign Secured：セキュア ディスクは外部設定になっていることを示します。正しいキーでロックされたディスクのロックを解除しても、ディスクが外部設定状態になっており、そのディスク上のデータが暗号化されているとこのようになります。このディスクを使用するには、外部設定をインポートするか、または外部設定をクリアします。

データを安全に削除する

委員会規制 (EU) 2019/424 は、データを安全に処分することを要求しています。

データの安全な廃棄は、Cisco UCS サーバのさまざまなドライブ、メモリ、およびストレージからデータを消去し、工場出荷時の設定にリセットするための、一般的なツールを使用することによって可能になります。

委員会規制 (EU) 2019/424 に準拠するためのデータの安全な削除は、次の Cisco UCS サーバでサポートされています。

- Cisco UCS B200
- Cisco UCS B480
- Cisco UCS C125
- Cisco UCS C220
- Cisco UCS C240
- Cisco UCS C480
- Cisco UCS S3260

安全にデータを削除するため、UCS サーバに取り付けられているデバイスについて十分に理解し、適切なツールを実行する必要があります。場合によっては、複数のツールを実行する必要がある場合があります。

データを安全に消去する方法の詳細については、https://www.cisco.com/web/dofc/18794277.pdf を参照してください。

ローカル セキュリティ ポリシーの管理

ローカル セキュリティ 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**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create storage-profile** *storage-profile-name*	指定された名前を持つストレージ プロファイルを組織レベルで作成し、ストレージ プロファイル設定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/storage-profile* # **create security**	指定されたストレージ プロファイルのセキュリティポリシーを作成し、セキュリティ ポリシー モードを開始します。
ステップ 4	UCS-A /org/storage-profile/security* # **create drive-security**	指定されたストレージ プロファイルのセキュリティのドライブ セキュリティ ポリシーを作成し、ドライブ セキュリティ ポリシー モードを開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-セキュリティ * # **create local**	指定されたストレージ プロファイルのローカル セキュリティ ポリシーを作成し、ローカル ポリシー モードを開始します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security/local* # **set security-key** *security-key*	ローカル ポリシーの指定されたセキュリティ キーを設定します。セキュリティ キーには、32 文字がなければなりません。
ステップ 7	UCS-A /org/storage-profile/security/drive-security/local* # **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

この例では、セキュリティ キーをもつローカル セキュリティ ポリシーの作成方法を示します。

```
UCS-A# scope org
UCS-A /org # create storage-profile stp-demo
UCS-A /org/storage-profile* # create security
UCS-A /org/storage-profile/security* # create drive-security
UCS-A /org/storage-profile/security/drive-security* # create local
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

ローカル セキュリティ ポリシーのセキュリティ キーの変更

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。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	指定されたストレージ プロファイルのストレージ プロファイル設定モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **scope security**	指定されたストレージ プロファイルのセキュリティ ポリシー モードを開始します。
ステップ 4	UCS A/org/storage-profile/security # **scope drive-security**	指定されたストレージ プロファイル セキュリティのドライブ セキュリティ ポリシー モードを開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-security # **scope local**	指定されたストレージ プロファイルのローカル ポリシー モードを開始します。
ステップ 6	UCS A/org/storage-profile/security/drive-security/local # **set deployed-security-key** *existing-security-key*	新しいキーを設定するために、サーバで展開される既存のキーを指定します。
ステップ 7	UCS-A /org/storage-profile/security/drive-security/local* # **set security-key** *new-security-key*	ローカルポリシーの新しいセキュリティキーを設定します。
ステップ 8	UCS-A /org/storage-profile/security/drive-security/local* # **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

この例では、ローカル セキュリティ ポリシーのセキュリティ キーを変更する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # scope local
UCS-A /org/storage-profile/security/drive-security/local # set deployed-security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisnewkey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

ローカルからリモートへのセキュリティ ポリシーの変更

始める前に

KMIP クライアント証明書ポリシーを作成したことを確認します。

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**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	選択したストレージプロファイルのストレージ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **scope security**	指定されたストレージプロファイルのセキュリティ ポリシーモードを開始します。
ステップ 4	UCS A/org/storage-profile/security # **scope drive-security**	指定されたストレージプロファイルセキュリティのドライブ セキュリティ ポリシー モードを開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-security # **create remote**	リモートポリシーモードを作成し、開始します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security/remote* # **set deployed-security-key** *existing-security-key*	サーバで展開された既存のキーを指定します。
ステップ 7	UCS-A /org/storage-profile/security/drive-security/remote* # **set primary-server** *primary-server-name*	プライマリ サーバ ホスト名または IP サーバを設定します。
ステップ 8	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set secondary-server** *secondary-server-name*	セカンダリ サーバ ホスト名または IP サーバを設定します。
ステップ 9	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set port** *kmip-server-port-number*	KMIP サーバのポート番号を設定します。KMIP サーバ ポート番号は、1024 から 65535 の範囲を設定できます。
ステップ 10	UCS-A /org/storage-profile/security/drive-security/remote* # **set server-certificate**	リモート セキュリティ ポリシーに KMIP 証明書を設定します。

	コマンドまたはアクション	目的
ステップ 11	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set timeout** *timeout-seconds*	ストレージと KMIP サーバの間の通信がタイム アウトする秒数を設定します。タイムアウトは 5 秒 ～ 20 秒の範囲となる場合があります。
ステップ 12	UCS-A /org/storage-profile/security/drive-security/remote* # **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。
ステップ 13	UCS A/org/storage-profile/security/drive-security/remote #**exit**	ドライブ セキュリティ ポリシー モードを開始します。
ステップ 14	UCS-A /org/storage-profile/security/drive-security # **delete local**	既存のローカルセキュリティ ポリシーを削除します。
ステップ 15	UCS-A /org/storage-profile/security/drive-security* # **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

この例では、ローカルからリモートへのセキュリティ ポリシーを変更する方法を示します。

```
UCS-A # scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # create remote
UCS-A /org/storage-profile/security/drive-security/remote* # set deployed-security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/remote* # set primary-server 10.10.10.1
UCS-A /org/storage-profile/security/drive-security/remote* # set secondary-server
10.10.10.2
UCS-A /org/storage-profile/security/drive-security/remote* # set port 5696
UCS-A /org/storage-profile/security/drive-security/remote* # set server-certificate
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Certificate:
>-----BEGIN CERTIFICATE-----
    MIIEEDCCAvigAwIBAgIGALOfZVDsMA0GCSqGSIb3DQEBCwUAMIGQMSowKAYDVQQD
    EyFDRyBDQSBTIG9uIHZvcm1ldHJpY2RzbS5jaXNjby5jb20xFTATBgNVBAsTDFNh
    dmJ1U3RvcmRldjEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczERMA8GA1UEBxMIU2Fu
    IEpvc2UxEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XDTE2MDkw
    NzE5MzMwMVoXDTI2MDkwOTE5MzMwMVowgZAxKjAoBgNVBAMTIUNHIENBIFMgb24g
    dm9ybWV0cmljZHNtLmNpc2NvLmNvbTEVMBMGA1UECxMMU2F2YnVTdG9yZGV2MRYw
    FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMREwDwYDVQQHEwhTYW4gSm9zZTETMB>EGA1UE
    CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
    DwAwggEKAoIBAQDhX2UdIV>TQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
    Xwj7yzArflrZ2kWvQCm4f6AdLOFUWzbuo+Fxd3rurd>w6BhJXdLj8Piq8094PqCLp
    qdUF83SsRVVbCXHxOqdk9jsSQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
    LeKFC8DUEm0GlGQACwiJ3s9O4+P2CI/d4P/>EyWwqABf3YJmAI1EQyUnoTwrg6EgY
    ZvcpHsmjXnbBZrL+ON7FBcbrTanvjyJxE6tFf5cRPGhymfna7Fd3lfVwZCcGIoR+
```

```
    EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbj>BsMBIGA1UdEwEB/wQI
    MAYBAf8CAQAwDgYDVR0PAQH/>>>>>>>>>>BAQDAgEGMB0GA1UdDgQWBBRnYyFiAK2lEDZJNC0Y
    VlIqMgiUJDAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDs
    MA0GCSqGSIb3DQEBCwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
    mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aeSAddQUOCy8fhiPoaMFrlTgs1hdS0p
    NJvfxV6QCun2UMRSuxWfG>0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KEsvWW
    5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
    +U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdns16uprmvWa3VBk3
    OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF>
    -----END CERTIFICATE-----

UCS-A /org/storage-profile/security/drive-security/remote* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/remote # exit
UCS-A /org/storage-profile/security/drive-security # delete local
UCS-A /org/storage-profile/security/drive-security* # commit-buffer
UCS-A /org/storage-profile/security/drive-security #
```

ローカル セキュリティ ポリシーを使用しているサーバへのセキュアなディスクの挿入

サーバにセキュアなディスクを挿入すると、次のいずれかが行われます。

- ドライブ上のセキュリティキーが、サーバのセキュリティキーと一致し、自動的にロックが解除されます。
- ディスク上のセキュリティキーとサーバ上のセキュリティキーが異なっています。ディスクはロックされたディスクとして表示されます。ロックされたディスク上で次のいずれかを実行できます。
  - セキュアな外部設定を消去してディスク上のすべてのデータを削除します。
  - ディスクの正しいキーを提供してディスクのロックを解除します。ディスクのロックを解除すると、ディスクはForeign Securedの状態になります。これらのディスクの外部設定は、すぐにインポートするか、またはクリアする必要があります。

（注） 現在の一連のディスクの外部設定をインポートする前に別の一連のディスクのロックを解除すると、現在の一連のディスクは再度ロックされ、Lockedの状態になります。

KMIP クライアント証明書ポリシー

KMIPサーバとも呼ばれているキー管理サーバを使用して、キーをリモートから設定できます。リモートポリシーを作成する前に、KMIPクライアント証明書ポリシーを作成する必要があります。証明書の生成に使用するホスト名はKMIP サーバのシリアル番号です。

証明書ポリシーは、2 つの独立した範囲から作成できます。

- グローバルスコープ：最初にこの範囲でグローバル証明書ポリシーを作成できます。この範囲で証明書を変更しても、証明書は再生成されません。
- サーバスコープ：この範囲で証明書ポリシーを作成または変更できます。作成または変更すると、証明書が再生成されます。このような証明書はそのサーバに固有であり、そのサーバについてグローバル証明書がオーバーライドされます。

KMIP クライアント証明書ポリシーを作成したら、次のいずれかを実行します。

- KMIP サーバに生成された証明書をコピーします。
- 生成された証明書署名要求を使用して CA 署名付き証明書を取得します。この CA 署名付き証明書を CIMC にコピーします。

グローバル KMIP クライアント証明書ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **create kmip-client-cert-policy**	KMIP 証明書ポリシーを作成し、KMIP クライアント証明書ポリシーモードを開始します。
ステップ 3	UCS-A /security/kmip-client-cert-policy* # **set country** *country-code*	KMIP 証明書ポリシーの国コードを指定します。国コードは大文字で 2 文字を含まなければなりません。
ステップ 4	UCS-A /security/kmip-client-cert-policy* # **set locality** *locality-code*	ローカリティの名前またはKMIP 証明書ポリシーの都市を指定します。ローカリティの名前として最大32 文字までを入力します。
ステップ 5	UCS-A /security/kmip-client-cert-policy* # **set org-name** *org-name*	KMIP 証明書ポリシーを要求する組織名を指定します。組織名として最大32 文字を入力します。
ステップ 6	UCS-A /security/kmip-client-cert-policy* # **set org-unit-name** *unit-name*	KMIP 証明書ポリシーを要求する組織ユニット名を指定します。組織ユニット名として最大64 文字を入力します。
ステップ 7	UCS-A /security/kmip-client-cert-policy* # **set state** *state-code*	KMIP 証明書ポリシーの州、地域、または郡の名前を指定します。州の名前として最大で 32 文字を入力します。

	コマンドまたはアクション	目的
ステップ 8	（任意） UCS-A /security/kmip-client-cert-policy* # **set email** *email-address*	リクエストに関連付けられた電子メール アドレスを指定します。
ステップ 9	（任意） UCS-A /security/kmip-client-cert-policy* # **set validity** *days*	証明書の有効期間を日数で指定します。有効期間は 365 日から 3650 日間です。
ステップ 10	UCS-A /security/kmip-client-cert-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。
ステップ 11	UCS A/security/kmip-client-cert-policy # **show**	KMIP 証明書ポリシーの詳細を表示します。

例

この例では、KMIP 証明書のポリシーを作成する方法を示します。

```
UCS-A# scope security
UCS-A /security # create kmip-client-cert-policy
UCS-A /security/kmip-client-cert-policy* # set country IN
UCS-A /security/kmip-client-cert-policy* # set locality BLR
UCS-A /security/kmip-client-cert-policy* # set org-name XYZ
UCS-A /security/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A /security/kmip-client-cert-policy* # set state KA
UCS-A /security/kmip-client-cert-policy* # commit-buffer
UCS-A /security/kmip-client-cert-policy # show

KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /security/kmip-client-cert-policy #
```

サーバ用の KMIP クライアント証明書の作成

サーバ用の KMIP クライアント証明書ポリシーを作成できます。この証明書は、特定のサーバにのみ適用され、グローバル KMIP クライアント証明書をオーバーライドします。

このポリシーを使用しているときに証明書の作成に使用するホスト名はサーバのシリアル番号です。

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-number*	指定したサーバのサーバ設定モードを開始します。
ステップ 2	UCS-A /server # **create kmip-client-cert-policy**	KMIP 証明書ポリシーを作成し、KMIP クライアント証明書ポリシーモードを開始します。
ステップ 3	UCS A/server/kmip-client-cert-ポリシー * # **set country** *country-code*	KMIP 証明書ポリシーの国コードを指定します。国コードは大文字で 2 文字を含まなければなりません。
ステップ 4	UCS A/server/kmip-client-cert-ポリシー * # **set locality** *locality-code*	ローカリティの名前またはKMIP 証明書ポリシーの都市を指定します。ローカリティの名前として最大32 文字までを入力します。
ステップ 5	UCS-A /server/kmip-client-cert-policy* # **set org-name** *org-name*	KMIP 証明書ポリシーを要求する組織名を指定します。組織名として最大32 文字を入力します。
ステップ 6	UCS-A /server/kmip-client-cert-policy* # **set org-unit-name** *unit-name*	KMIP 証明書ポリシーを要求する組織ユニット名を指定します。組織ユニット名として最大64 文字を入力します。
ステップ 7	UCS-A /server/kmip-client-cert-policy* # **set state** *state-code*	KMIP 証明書ポリシーの州、地域、または郡の名前を指定します。州の名前として最大で 32 文字を入力します。
ステップ 8	（任意） UCS A/server/kmip-client-cert-ポリシー * # **set email** *email-address*	リクエストに関連付けられた電子メール アドレスを指定します。
ステップ 9	（任意） UCS-A /server/kmip-client-cert-policy* # **set validity** *days*	証明書の有効期間を日数で指定します。有効期間は365 日から3650 日間です。
ステップ 10	UCS-A /server/kmip-client-cert-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。
ステップ 11	UCS A/server/kmip-client-cert-policy # **show**	KMIP 証明書の詳細を表示します。

例

この例では、rack-mount サーバで KMIP 証明書を作成する方法を示します。

```
UCS-A# scope server 5
UCS-A /server # create kmip-client-cert-policy
UCS-A /server/kmip-client-cert-policy* # set country IN
UCS-A /server/kmip-client-cert-policy* # set locality BLR
UCS-A /server/kmip-client-cert-policy* # set org-name XYZ
UCS-A /server/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A /server/kmip-client-cert-policy* # set state KA
UCS-A /server/kmip-client-cert-policy* # commit-buffer
UCS-A /server/kmip-client-cert-policy* # show

KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /server/kmip-client-cert-policy #
```

この例では、ブレード サーバで KMIP 証明書を作成する方法を示します。

```
UCS-A# scope server 1/5
UCS-A chassis/server # create kmip-client-cert-policy
UCS-A chassis/server/kmip-client-cert-policy* # set country IN
UCS-A chassis/server/kmip-client-cert-policy* # set locality BLR
UCS-A chassis/server/kmip-client-cert-policy* # set org-name XYZ
UCS-A chassis/server/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A chassis/server/kmip-client-cert-policy* # set state KA
UCS-A chassis/server/kmip-client-cert-policy* # commit-buffer
UCS-A chassis/server/kmip-client-cert-policy* # show

KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /server/kmip-client-cert-policy #
```

リモート セキュリティ ポリシーの管理

リモート セキュリティ ポリシーの作成

始める前に

KMIP クライアント証明書ポリシーを作成したことを確認します。

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**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	選択したストレージプロファイルのストレージ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **create security**	セキュリティモードを作成し、開始します。
ステップ 4	UCS-A /org/storage-profile/security* # **create drive-security**	ドライブ セキュリティ モードを作成し、開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-セキュリティ * # **create remote**	リモートポリシーモードを作成し、開始します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security/remote* # **set primary-server** *primary-server-name*	プライマリ サーバ ホスト名または IP サーバを設定します。
ステップ 7	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set secondary-server** *secondary-server-name*	セカンダリ サーバ ホスト名または IP サーバを設定します。
ステップ 8	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set port** *kmip-server-port-number*	KMIP サーバのポート番号を設定します。KMIP サーバ ポート番号は、1024 から 65535 の範囲を設定できます。
ステップ 9	UCS-A /org/storage-profile/security/drive-security/remote* # **set server-certificate**	リモート セキュリティ ポリシーに KMIP 証明書を設定します。
ステップ 10	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set timeout** *timeout-seconds*	ストレージと KMIP サーバの間の通信がタイム アウトする秒数を設定します。タイムアウトは 5 秒 ～ 20 秒の範囲となる場合があります。
ステップ 11	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **create login**	KMIP サーバのログインの詳細を作成し、ログイン モードを開始します。
ステップ 12	（任意） UCS-A /org/storage-profile/security/drive-security/remote/login* # **set username** *username*	KMIP サーバにログインするためのユーザ名を設定します。
ステップ 13	（任意） UCS-A /org/storage-profile/security/drive-security/remote/login* # **set password** *password*	KMIP サーバにログインするためのパスワードを設定します。

	コマンドまたはアクション	目的
ステップ 14	UCS-A /org/storage-profile/security/drive-security/remote/login* # **commit-buffer**	トランザクションをシステム設定にコミットします。

例

```
UCS-A # scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # create security
UCS-A /org/storage-profile/security* # create drive-security
UCS-A /org/storage-profile/security/drive-security* # create remote
UCS-A /org/storage-profile/security/drive-security/remote* # set primary-server 10.10.10.1
UCS-A /org/storage-profile/security/drive-security/remote* # set secondary-server
10.10.10.2
UCS-A /org/storage-profile/security/drive-security/remote* # set port 5696
UCS-A /org/storage-profile/security/drive-security/remote* # set server-certificate
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Certificate:
>-----BEGIN CERTIFICATE-----
    MIIEEDCCAvigAwIBAgIGALOfZVDsMA0GCSqGSIb3DQEBCwUAMIGQMSowKAYDVQQD
    EyFDRyBDQSBTIG9uIHZvcm1ldHJpY2RzbS5jaXNjby5jb20xFTATBgNVBAsTDFNh
    dmJ1U3RvcmRldjEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczERMA8GA1UEBxMIU2Fu
    IEpvc2UxEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XDTE2MDkw
    NzE5MzMwMVoXDTI2MDkwOTE5MzMwMVowgZAxKjAoBgNVBAMTIUNHIENBIFMgb24g
    dm9ybWV0cmljZHNtLmNpc2NvLmNvbTEVMBMGA1UECxMMU2F2YnVTdG9yZGV2MRYw
    FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMREwDwYDVQQHEwhTYW4gSm9zZTETMB>EGA1UE
    CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
    DwAwggEKAoIBAQDhX2UdIV>TQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
    Xwj7yzArflrZ2kWvQCm4f6AdLOFUWzbuo+Fxd3rurd>w6BhJXdLj8Piq8094PqCLp
    qdUF83SsRVVbCXHxOqdk9jsSQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
    LeKFC8DUEm0GlGQACwiJ3s9O4+P2CI/d4P/>EyWwqABf3YJmAI1EQyUnoTwrg6EgY
    ZvcpHsmjXnbBZrL+ON7FBcbrTanvjyJxE6tFf5cRPGhymfna7Fd3lfVwZCcGIoR+
>   EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbj>BsMBIGA1UdEwEB/wQI
    MAYBAf8CAQAwDgYDVR0PAQH/>>>>>>>>>BAQDAgEGMB0GA1UdDgQWBBRnYyFiAK2lEDZJNC0Y
    VlIqMgiUJDAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDs
    MA0GCSqGSIb3DQEBCwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
    mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aeSAddQUOCy8fhiPoaMFrlTgs1hdS0p
    NJvfxV6QCun2UMRSuxWfG>0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KEsvWW
    5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
    +U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdns16uprmvWa3VBk3
    OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF>
    -----END CERTIFICATE-----

UCS-A /org/storage-profile/security/drive-security/remote* # create login
UCS-A /org/storage-profile/security/drive-security/remote/login* # set username user1
UCS-A /org/storage-profile/security/drive-security/remote/login* # set password Password
UCS-A /org/storage-profile/security/drive-security/remote/login* # exit
UCS-A /org/storage-profile/security/drive-security/remote # exit
UCS-A /org/storage-profile/security/drive-security # show detail expand

Drive Security:
    Remote:
        Primary Server Name: 10.10.10.1
        Secondary Server Name:10.10.10.2
        KMIP Server Port: 5696
        Deployed Security Key:
        KMIP Server Certificate: -----BEGIN CERTIFICATE-----
```

```
MIIEEDCCAvigAwIBAgIGALOfZVDsMA0GCSqGSIb3DQEBCwUAMIGQMSowKAYDVQQD
EyFDRyBDQSBTIG9uIHZvcm1ldHJpY2RzbS5jaXNjby5jb20xFTATBgNVBAsTDFNh
dmJ1U3RvcmRldjEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczERMA8GA1UEBxMIU2Fu
IEpvc2UxEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XDTE2MDkw
NzE5MzMwMVoXDTI2MDkwOTE5MzMwMVowgZAxKjAoBgNVBAMTIUNHIENBIFMgb24g
dm9ybWV0cmljZHNtLmNpc2NvLmNvbTEVMBMGA1UECxMMU2F2YnVTdG9yZGV2MRYw
FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMREwDwYDVQQHEwhTYW4gSm9zZTETMBEGA1UE
CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDhX2UdIVTQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
Xwj7yzArflrZ2kWvQCm4f6AdLOFUWzbuo+Fxd3rurdw6BhJXdLj8Piq8094PqCLp
qdUF83SsRVVbCXHxOqdk9jsSQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
LeKFC8DUEm0GlGQACwiJ3s9O4+P2CI/d4P/EyWwqABf3YJmAI1EQyUnoTwrg6EgY
ZvcpHsmjXnbBZrL+ON7FBcbrTanvjyJxE6tFf5cRPGhymfna7Fd3lfVwZCcGIoR+
EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbjBsMBIGA1UdEwEB/wQI
MAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRnYyFiAK2lEDZJNC0Y
VlIqMgiUJDAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDs
MA0GCSqGSIb3DQEBCwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aeSAddQUOCy8fhiPoaMFrlTgs1hdS0p
NJvfxV6QCun2UMRSuxWfG0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KEsvWW
5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
+U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdns16uprmvWa3VBk3
OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF
-----END CERTIFICATE-----
```


リモート セキュリティ キーの変更

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-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。現在、Cisco UCS Manager は SAS コントローラでのみ SED をサポートします。
ステップ 3	UCS-A /server/raid-controller # **set admin-state modify-remote-key**	リモートのセキュリティ ポリシーのセキュリティ キーを変更します。
ステップ 4	UCS-A /server/raid-controller # **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

この例では、ラックマウント サーバ用のコントローラのリモートのセキュリティ キーを変更する方法を示します。

```
UCS-A# scope server 3
UCS-A /server # scope raid-controller 1 sas
UCS-A /server/raid-controller # set admin-state modify-remote-key
```

```
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、ブレードサーバ用のコントローラのリモートのセキュリティキーを変更する方法を示します。

```
UCS-A# scope server 1/3
UCS-A chassis/server # scope raid-controller 1 sas
UCS-A chassis/server/raid-controller # set admin-state modify-remote-key
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

リモートからローカルへのセキュリティ ポリシーの変更

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 storage-profile** *storage-profile-name*	指定されたストレージプロファイルのストレージプロファイル設定モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **scope security**	指定されたストレージプロファイルのセキュリティポリシーモードを開始します。
ステップ 4	UCS A/org/storage-profile/security # **scope drive-security**	指定されたストレージプロファイルセキュリティのドライブセキュリティポリシー モードを開始します。
ステップ 5	UCS-A /org/storage-profile/security/drive-security # **delete remote**	既存のリモートのセキュリティ ポリシーを削除します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security* # **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。
ステップ 7	UCS A/org/storage-profile/security/drive-security # **create local**	ローカルポリシーモードを作成し、開始します。
ステップ 8	UCS-A /org/storage-profile/security/drive-security/local* # **set security-key** *security-key*	ローカルポリシーのセキュリティキーを設定します。

	コマンドまたはアクション	目的
ステップ 9	UCS-A /org/storage-profile/security/drive-security/local* # **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。
ステップ 10		

例

この例では、ローカルにリモートからセキュリティ ポリシーを変更する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # delete remote
UCS-A /org/storage-profile/security/drive-security* # commit-buffer
UCS-A /org/storage-profile/security/drive-security # create local
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

リモート セキュリティ ポリシーを使用しているサーバへのセキュアなディスクの挿入

リモート セキュリティ ポリシーを使用しているサーバにセキュアなディスクを挿入すると、ストレージ ディスクはロックされたディスクとして表示されます。次のいずれかを実行します。

- 以前にローカル キーを使用してディスクがロックされていた場合は、そのローカル キーを使用してディスクのロックを手動で解除します。
- リモート KMIP サーバを使用してロックを解除します。

セキュアなディスクをローカル セキュリティ ポリシーを使用しているサーバからリモート セキュリティ ポリシーを使用しているサーバに移動すると、ディスクはロックされた状態として表示されます。ローカル キーを使用してディスクのロックを手動で解除します。

既存の仮想ドライバの保護

始める前に

- コントローラは、セキュアでなければなりません。

- 仮想ドライブは、**孤立**状態である必要があります。

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-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server# **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller# **scope virtual-drive** *virtual-drive-id*	指定された孤立仮想ドライブの仮想ドライブ モードを開始します。
ステップ 4	UCS-A /server/raid-controller/virtual-drive# **set admin-state secure-drive-group**	既存の仮想ドライブを保護します。
ステップ 5	UCS-A /server/raid-controller/virtual-drive*# **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

この例では、ラックマウント サーバ の既存の仮想ドライブ を保護する方法を示します。

```
UCS-A# scope server 1
UCS-A /server# scope raid-controller 3 sas
UCS-A /server/raid-controller# scope virtual-drive 1000
UCS-A /server/raid-controller/virtual-drive # set admin-state secure-drive-group
UCS-A /server/raid-controller/virtual-drive*# commit-buffer
UCS-A /server/raid-controller/virtual-drive#
```

この例は、ブレード サーバの既存の仮想ドライブを保護する方法を示します。

```
UCS-A# scope server 1/4
UCS-A chassis/server# scope raid-controller 3 sas
UCS-A chassis/server/raid-controller# scope virtual-drive 1000
UCS-A chassis/server/raid-controller/virtual-drive # set admin-state secure-drive-group

UCS-A chassis/server/raid-controller/virtual-drive*# commit-buffer
UCS-A chassis/server/raid-controller/virtual-drive#
```

ディスクのセキュリティの有効化

始める前に

ディスクが JBOD であることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS A/server/raid-controller/local-disk # **set admin-state enable-security**	JBOD でセキュリティを有効にします。
ステップ 5	UCS A/server/raid-controller/local-ディスク * # **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

この例では、ラックマウント サーバの JBOD のセキュリティを有効にする方法を示します。

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state enable-security
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

この例では、ブレード サーバの JBOD のセキュリティを有効にする方法を示します。

```
UCS-A# scope server 1/3
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # set admin-state enable-security
```

```
UCS-A chassis/server/raid-controller/local-disk* # commit-buffer
UCS-A chassis/server/raid-controller/local-disk #
```

セキュア ディスクの消去

始める前に

ディスクが **Unconfigured Good** 状態であることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS-A /server/raid-controller/local-disk # **set admin-state clear secure-drive**	セキュアなディスクを消去し、ディスクのセキュリティをクリアします。
ステップ 5	UCS A/server/raid-controller/local-ディスク * # **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

この例は、ラック マウント サーバのセキュア ディスクを消去する方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state clear secure-drive
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

この例は、ブレード サーバのセキュア ディスクを消去する方法を示します。

```
UCS-A # scope server 1/3
UCS-A chassis/server # scope raid-controller 3 sas
```

```
UCS-A chassis/server/raid-controller # scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # set admin-state clear secure-drive
UCS-A chassis/server/raid-controller/local-disk* # commit-buffer
UCS-A chassis/server/raid-controller/local-disk #
```

コントローラのセキュリティのディセーブル化

始める前に

SAS コントローラ上でのみ、セキュリティを無効にすることができます。コントローラ上のセキュリティを無効にするには、まずすべてのセキュアディスク上のセキュリティを無効にしてから、コントローラのすべてのセキュア仮想ドライブを削除します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **set admin-state disable-security**	コントローラのセキュリティ キーを無効にします。
ステップ 4	UCS-A /server/raid-controller # **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

この例では、ラックマウント サーバの コントローラ のセキュリティを無効にする方法を示します。

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state disable-security
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、ブレード サーバのコントローラのセキュリティを無効にする方法を示します。

```
UCS-A# scope server 1/3
```

```
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # set admin-state disable-security
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

ロックされたディスクのロックの解除

SED のキーがコントローラ上のキーと一致していない場合、そのディスクは [Locked, Foreign Secure] と表示されます。そのディスクのセキュリティキーを提供するか、またはリモート KMIP サーバを使用して、ディスクのロックを解除します。ディスクのロックを解除した後、外部設定をインポートするか、またはクリアします。

ロックされたディスクのロックを解除すると、そのディスクのセキュリティ ステータスは [Foreign Secure] と表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。現在、Cisco UCS Manager は SAS コントローラでのみ SED をサポートします。
ステップ 3	UCS-A /server/raid-controller # **set admin-state unlock-disk** [*security-key*]	ロックされたディスクのロックを解除します。 セキュリティキーが設定される場合、このキーは、ロックされた状態にあるディスクをロック解除するために使用されます。 セキュリティキーが設定されない場合、Cisco UCS Manager は KMIP サーバを使用してディスクをロック解除しようとします。リモート セキュリティがサーバに設定される場合のみ、セキュリティキーの設定はオプションです。
ステップ 4	UCS-A/server/raid-controller * # **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

この例では、ローカル セキュリティ ポリシーが設定されたラックマウント サーバでロックされたディスクのロックをセキュリティキーを使用して解除する方法を説明します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state unlock-disk thisisastring
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、リモート セキュリティ ポリシーが設定されたラックマウント サーバでロックされたディスクのロックをKMIPサーバを使用して解除する方法を説明します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state unlock-disk
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、ローカル セキュリティ ポリシーが設定されたブレード サーバでロックされたディスクをセキュリティ キーを使用して解除する方法を説明します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # set admin-state unlock-disk thisisastring
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

この例では、リモート セキュリティ ポリシーが設定されたブレード サーバでロックされたディスクのロックを KMIP サーバを使用して解除する方法を説明します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # set admin-state unlock-disk
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

セキュア外部設定ディスクの消去

ロックされた状態のディスクがあり、そのディスクを既存のデータにアクセスせずに使用する場合は、セキュアな外部設定ディスクを消去できます。

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-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS-A /server/raid-controller/local-disk # **set admin-state clear secure-foreign-config-drive**	セキュアな外部設定ドライブをクリアします。
ステップ 5	UCS A/server/raid-controller/local-ディスク * # **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

この例は、ラック マウント サーバの外部設定ディスクをクリアする方法を示します。

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state clear
secure-foreign-config-drive
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

この例は、ブレード サーバの外部設定ディスクをクリアする方法を示します。

```
UCS-A# scope server 1/3
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # set admin-state clear
secure-foreign-config-drive
UCS-A chassis/server/raid-controller/local-disk* # commit-buffer
UCS-A chassis/server/raid-controller/local-disk #
```

コントローラのセキュリティ フラグの表示

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-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **show detail**	RAID コントローラの詳細を表示します。

例

この例では、ラックマウント サーバの コントローラ のセキュリティ フラグが有効になっているか、チェックする方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # show detail

RAID Controller:
    ID: 3
    Type: SAS
    PCI Addr: 03:00.0
    Vendor: LSI Corp.
    Model: LSI MegaRAID SAS 3108
    Serial: SV55346948
    HW Rev: C0
    Raid Support: RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
    OOB Interface Supported: Yes
    Mode: RAID
    Rebuild Rate: 30
    Controller Status: Optimal
    Config State: Applied
    Pinned Cache Status: Disabled
    Sub OEM ID: 0
    Supported Strip Sizes: 1MB,64KB,256KB,512KB,128KB
    Default Strip Size: 64KB
    PCI Slot: HBA
    Controller Flags: Drive Security Capable
```

この例では、ブレード サーバの コントローラ のセキュリティ フラグが有効になっているか、チェックする方法を示します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # show detail

RAID Controller:
    ID: 3
    Type: SAS
    PCI Addr: 03:00.0
    Vendor: LSI Corp.
    Model: LSI MegaRAID SAS 3108
    Serial: SV55346948
    HW Rev: C0
    Raid Support: RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
    OOB Interface Supported: Yes
    Mode: RAID
    Rebuild Rate: 30
    Controller Status: Optimal
    Config State: Applied
    Pinned Cache Status: Disabled
    Sub OEM ID: 0
    Supported Strip Sizes: 1MB,64KB,256KB,512KB,128KB
    Default Strip Size: 64KB
    PCI Slot: HBA
    Controller Flags: Drive Security Capable
```

ローカル ディスクのセキュリティ フラグの表示

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-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS-A /server/raid-controller/local-disk # **show detail**	ローカルディスクの詳細を表示します。

例

この例では、ラックマウント サーバの ローカルディスク のセキュリティ フラグを表示する方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller #scope local-disk 2
UCS-A /server/raid-controller/local-disk # show detail

Local Disk:
    ID: 4
    Block Size: 512
    Physical Block Size: 4096
    Blocks: 1560545280
    Raw Size: 763097
    Size: 761985
    Technology: SSD
    Operability: Operable
    Oper Qualifier Reason: N/A
    Presence: Equipped
    Connection Protocol: SAS
    Product Variant: default
    Product Name: 800GB Enterprise performance SAS SED SSD (10 FWPD) - MTFDJAK800MBS
    PID: UCS-SD800GBEK9
    VID: V01
    Vendor: MICRON
    Model: S650DC-800FIPS
    Vendor Description: Micron
    Serial: ZAZ090VD0000822150Z3
    HW Rev: 0
    Running-Vers: MB13
    Average Seek Time (R/W): N/A
    Track to Track Seek Time (R/W): 115ms
    Part Number: 16-100911-01
    SKU: UCS-SD800GBEK9
    Drive State: Online
    Power State: Active
    Link Speed: 12 Gbps
    Enclosure Association Type: Direct Attached
    Device Version: MB13
    Drive Security Flags: Secured,Security Enabled,Security Capable
```

この例では、ブレード サーバの ローカル ディスク のセキュリティ フラグを表示する方法を示します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller #scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # show detail

Local Disk:
    ID: 4
    Block Size: 512
    Physical Block Size: 4096
    Blocks: 1560545280
    Raw Size: 763097
```

```
Size: 761985
Technology: SSD
Operability: Operable
Oper Qualifier Reason: N/A
Presence: Equipped
Connection Protocol: SAS
Product Variant: default
Product Name: 800GB Enterprise performance SAS SED SSD (10 FWPD) - MTFDJAK800MBS
PID: UCS-SD800GBEK9
VID: V01
Vendor: MICRON
Model: S650DC-800FIPS
Vendor Description: Micron
Serial: ZAZ090VD0000822150Z3
HW Rev: 0
Running-Vers: MB13
Average Seek Time (R/W): N/A
Track to Track Seek Time (R/W): 115ms
Part Number: 16-100911-01
SKU: UCS-SD800GBEK9
Drive State: Online
Power State: Active
Link Speed: 12 Gbps
Enclosure Association Type: Direct Attached
Device Version: MB13
Drive Security Flags: Secured,Security Enabled,Security Capable
```

仮想ドライブのセキュリティ フラグの表示

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-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope virtual-drive** *virtual-drive-id*	仮想ドライブ モードを開始します。
ステップ 4	UCS-A /server/raid-controller/virtual-drive # **show detail**	仮想デバイスの詳細を表示します。

例

この例では、ラックマウント サーバの仮想ディスク のセキュリティ フラグを表示する方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope virtual-drive 1000
UCS-A /server/raid-controller/virtual-drive # show detail

Virtual Drive:
    ID: 1000
    Name: luna
    Block Size: 512
    Blocks: 20971520
    Size: 10240
    Operability: Operable
    Presence: Equipped
    Lifecycle: Allocated
    Drive State: Optimal
    Type: RAID 0 Striped
    Strip Size (KB): 64
    Access Policy: Read Write
    Read Policy: Normal
    Configured Write Cache Policy: Write Through
    Actual Write Cache Policy: Write Through
    IO Policy: Direct
    Drive Cache: No Change
    Bootable: False
    Oper Device ID: 0
    Change Qualifier: No Change
    Config State: Applied
    Deploy Action: No Action
    Service Profile Lun Reference: org-root/ls-sp1/vdrive-ref-lun-1
    Assigned To Server: sys/rack-unit-1
    Available Size on Disk Group (MB): 751745
    Unique Identifier: 90ae6ea0-6a39-49e1-9c0d-0f3e2e9ecfce
    Vendor Unique Identifier: 678da6e7-15b2-9c20-2011-c4f60c40e57a
    Security Flags: Drive Security Enable,Drive Security Capable
```

この例は、ブレードサーバの仮想ディスクのセキュリティフラグを表示する方法を示しています。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # scope virtual-drive 1000
UCS-A chassis/server/raid-controller/virtual-drive # show detail

Virtual Drive:
    ID: 1000
    Name: luna
    Block Size: 512
    Blocks: 20971520
    Size: 10240
    Operability: Operable
    Presence: Equipped
    Lifecycle: Allocated
    Drive State: Optimal
    Type: RAID 0 Striped
    Strip Size (KB): 64
    Access Policy: Read Write
    Read Policy: Normal
    Configured Write Cache Policy: Write Through
    Actual Write Cache Policy: Write Through
```

```
IO Policy: Direct
Drive Cache: No Change
Bootable: False
Oper Device ID: 0
Change Qualifier: No Change
Config State: Applied
Deploy Action: No Action
Service Profile Lun Reference: org-root/ls-sp1/vdrive-ref-lun-1
Assigned To Server: sys/rack-unit-1
Available Size on Disk Group (MB): 751745
Unique Identifier: 90ae6ea0-6a39-49e1-9c0d-0f3e2e9ecfce
Vendor Unique Identifier: 678da6e7-15b2-9c20-2011-c4f60c40e57a
Security Flags: Drive Security Enable,Drive Security Capable
```

第 14 章

ストレージ インベントリ

NVMe で最適化された M5 サーバ

3.2(3a) 以降では、Cisco UCS Manager は次の NVMe 最適化 M5 サーバをサポートしています。

- UCSC-C220-M5SN— PCIe MSwitch は、UCS C220 M5 サーバ用の専用 PCIe MSwirch スロットに配置されます。このセットアップでは、最大 10 台の NVMe ドライブがサポートされます。最初の 2 台のドライブは、ライザーを介して直接接続されています。残りの 8 台のドライブは、MSwitch によって接続および管理されます。このセットアップでは、SAS/SATA ドライブの組み合わせはサポートされていません。

- UCSC-C240-M5SN—PCIe MSwitch は、UCS C240 M5 サーバのスロット 4 のライザー 2 に配置されます。サーバは最大 24 台のドライブをサポートします。スロット1 ～ 8 は、MSwitch によって接続および管理される NVMe ドライブです。また、サーバは背面で最大 2 台の NVMe ドライブをサポートし、ライザーを介して直接接続されます。この設定では、スロット 9 ～ 24 の SAS/SATA ドライブと SAS/SATA の組み合わせがサポートされています。これらのドライブは、専用の MRAID PCIe スロットに配置された SAS コントローラによって管理されます。

- UCS-C480-M5—UCS C480 M5 サーバは最大 3 個の NVMe ドライブをサポートし、それぞれ最大 8 台の NVMe ドライブをサポートします。各ケージには、MSwitch を含むインタポーザ カードがあります。各サーバは、最大 24 台の NVMe ドライブ (3 個の NVMe ドライブ ケージ x 8 個の NVMe ドライブ) をサポートできます。サーバは背面 PCIe Aux ドライブ ケージもサポートしています。これには、PCIe スロット 10 に配置された MSwitch によって管理される最大 8 台の NVMe ドライブを搭載できます。

  このセットアップでは次の機能はサポートされていません。

  - NVMe ドライブ ケージと HDD ドライブ ケージの組み合わせ
  - 背面補助ドライブ ケージに関係なく、Cisco 12G 9460-8i RAID コントローラと NVMe ドライブ ケージの組み合わせ

（注） UCS C480 M5 PID は、以前のリリースと同じです。

（注） B200 および B480 M5 ブレード サーバーでは、NVMe ドライブを SAS コントローラで直接使用することはできません。代わりにLSTOR-PT パススルー コントローラを使用してください。

NVMe 最適化 M5 サーバでは、次の MSwitch カードがサポートされています。

- UCS-C480-M5 HDD Ext NVMe カード (UCSC-C480-8NVME)—PCIe MSwitch を含む、インタポーザカードを接続した前面NVMe ドライブケージ。各サーバは最大3 個の前面NVMe ドライブ ケージをサポートし、各ケージは最大8 台のNVMe ドライブをサポートします。各サーバは、最大 24 台の NVMe ドライブ (3 個の NVMe ドライブ ケージ x 8 個の NVMe ドライブ) をサポートできます。
- C480 M5 PCIe NVMe スイッチ カード (UCSC NVME-SC)—PCIe スロット10 に挿入された背面補助ドライブ ケージで最大 8 台の NVMe ドライブをサポートする PCIe MSwitch カード。

（注） Cisco C480 M5 サーバは、最大 32 台の NVMe ドライブ (背面補助ドライブケージの前面の 24 NVMe ドライブ + 8 台の NVMe ドライブ) をサポートします。

- UCSC-C220-M5SN および UCSC-C240-M5SN には、個別の MSwitch PID はありません。これらのサーバの MSwitch カードは、対応する NVMe 最適化サーバの一部です。

MSwitch ディザスタ リカバリ

破損したMSwitch を回復し、以前動作していたファームウェアにロールバックすることができます。

（注） Cisco UCS C480 M5 サーバ を使用して設定した場合、mswitch 障害復旧プロセスは、一度に 1 個の MSwitch でのみ実行できます。障害復旧プロセスが 1 個の MSwitch ですでに実行されている場合は、完了するまで待機します。FSM からリカバリ ステータスをモニタできます。

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** [*chassis-num*/*server-num* | *dynamic-uuid*]	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope nvme-swtich** *nvme_switch*	指定されたNVMeスイッチに入ります。
ステップ 3	UCS-A /server/nvme-switch # **set recover-nvme-switch**	指定した名前で LUN 設定を削除します。
ステップ 4	UCS-A /server/nvme-switch* # **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。
ステップ 5	UCS-A /server/nvme-switch # **exit**	MSwitch モードを終了します。
ステップ 6	UCS-A /server # **ack-nvme-switch-recovery acknowledge**	MSwitch リカバリを確認します。
ステップ 7	UCS-A /server* # **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。 （注） 障害復旧プロセス中は、サーバをリセットしないでください。

例

次の例では、server1 の MSwitch を復旧します。

```
UCS-A# scope server 1
UCS-A/server # scope nvme-switch 1
UCS-A/server/nvme-switch # set recover-nvme-switch
UCS-A/server/nvme-switch* # commit-buffer
UCS-A/server/nvme-switch # exit
UCS-A/server # ack-nvme-switch-recovery acknowledge
UCS-A/server* # commit-buffer
```

B200 M6 サーバーの NVMe 交換に関する考慮事項

システムの電源がオフのときにCisco B200 M6 サーバーの NVMe ストレージ デバイスをスワップまたは交換すると、、エラー状態が発生する可能性があります。このエラーの発生を回避するため、次の予防措置を講じてください。

- サーバーの電源を切らずに、NVMe SSD ストレージ デバイスを交換またはホットスワップします。

- サーバーの電源を切った状態でNVMeストレージを交換する必要がある場合は、サーバーをデコミッションし、ハードウェアを取り外すか、交換してから、サーバーを再起動します。これにより、サーバーは再コミッションされ、NVMeストレージは正しく検出されます。

システムの電源がオフになっているときにNVMeストレージを交換すると、そのコントローラは応答なしとしてマークされます。この問題を回復するには、サーバーを再認識させます。

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。

CHAPTER 15

Cisco UCS C3260 システム ストレージ管理

ストレージ サーバ機能およびコンポーネントの概要

ストレージ サーバ機能

次の表に、 Cisco UCS C3260 システムの機能の概要を示します。

表 *5 : Cisco UCS C3260* システムの機能

特長	説明
シャーシ	4 ラック ユニット（4RU）シャーシ
プロセッサ	• Cisco UCS C3260 M3 サーバ ノード：各サーバ ノード内の 2 つの Intel Xeon E5-2600 v2 シリーズ プロセッサ。 • Cisco UCS C3260 M4 サーバ ノード：各サーバ ノード内の 2 つの Intel Xeon E5-2600 v4 シリーズ プロセッサ。 • Cisco UCS C3260 M3 サーバ ノード：各サーバ ノード内の 2 つの Skylake 2S-EP プロセッサ。
メモリ	各サーバ ノード内で最大 16 個の DIMM。

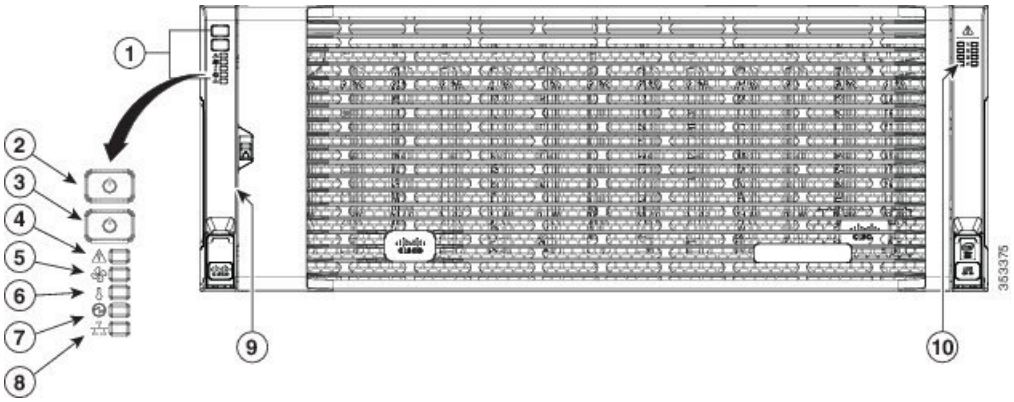
特長	説明
マルチビット エラー保護	このシステムは、マルチビット エラー保護をサポートします。
ストレージ	システムには次のストレージ オプションがあります。 • 最大 56 台のトップ ローディング 3.5 インチ ドライブ • オプションのドライブ エクスパンダ モジュール内に最大 4 台の 3.5 インチ、リア ローディング ドライブ • 最大 4 台の 2.5 インチ、リア ローディング SAS ソリッド ステート ドライブ（SSD） • サーバ ノード内部の 1 台の 2.5 インチ NVMe ドライブ （注） これは S3260 M4 サーバにのみ適用されます。 • サーバ ノード内に 2 台の 7 mm NVMe ドライブ （注） これは、S3260 M5 サーバのみに適用されます。 • IO エクスパンダのサポートされている 2 つの 15 mm NVMe ドライブ
ディスク管理	このシステムは、最大 2 台のストレージ コントローラをサポートしています。 • 各サーバ ノード内に Cisco ストレージ コントローラ カード用の専用メザニン形式ソケット 1 基
RAID バックアップ	supercap 電源モジュール（SCPM）は、RAID コントローラ カードにマウントされます。

特長	説明
PCIe I/O	オプションの I/O エクスパンダは、8x Gen 3 PCIe 拡張スロットを 2 つ提供します。 リリース 3.2(3) 以降では、S3260 M5 サーバで次をサポートしています。 • Intel X550 デュアルポート 10GBase-T • Qlogic QLE2692 デュアル ポート 16G ファイバ チャネル HBA • N2XX-AIPCI01 Intel X520 デュアル ポート 10 Gb SFP+ アダプタ
ネットワークおよび管理 I/O	システムには、システム I/O コントローラ（SIOC）を 1 つまたは 2 つ搭載できます。それにより、背面パネル管理とデータ接続が可能になります。 • SIOC ごとに 2 つの SFP+ 40 Gb ポート • SIOC ごとに 1 つの 10/100/1000 イーサネット専用管理ポート サーバ ノードごとに、KVM ケーブルで 2 つの USB を接続できる 1 つの背面パネル KVM コネクタ、1 つの VGA DB-15 コネクタ、1 つのシリアル DB-9 コネクタがあります。
電源	2 台または 4 台の電源装置、各 1050 W（ホットスワップ可能で 2+2 冗長）。
冷却	前面から背面に冷却を引き出す4つの内蔵ファン モジュール、ホットスワップ可能。各ファン モジュールには 2 つのファンが内蔵されています。 さらに、各電源にはファンが 1 個あります。

前面パネルの機能

次の図に、Cisco UCS C3260 システムの前面パネルの機能を示します。

図 *4:* 前面パネルの機能

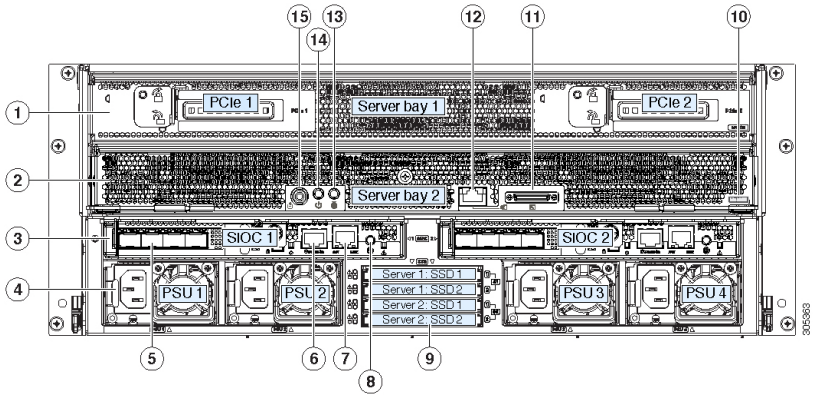


1	操作パネル	6	温度ステータス LED
2	システム電源ボタン/LED	7	電源装置ステータス LED
3	システム ユニット識別ボタン/LED	8	ネットワーク リンク アクティビティ LED
4	システム ステータス LED	9	引き出し型の資産タグ（前面ベゼルの下に表示されない）
5	ファン ステータス LED	10	内蔵ドライブのステータス LED

背面パネルの機能

次の図に、 Cisco UCS C3260 システムの背面パネルの機能を示します。

図 *5:* 前面パネルの機能



ディスク スロット

1	サーバー ベイ 1 • （オプション）I/O エクスパンダ（図を参照）（Cisco UCS C3260 M4および M5サーバ ノードのみに搭載） • （オプション）サーバ ノード • （オプション）ドライブ拡張モジュール	8	現時点ではサポートされていません。
2	サーバー ベイ 2 • （オプション）サーバ ノード (Cisco UCS C3260 M4およびM5に表示) （オプション）ドライブ拡張モジュール	9	現時点ではサポートされていません。

3	システム I/O コントローラ（SIOC） • サーバー ベイ 1 にサーバー ノードがある場合、SIOC 1 が必要 • サーバ ベイ 2 にサーバ ノードがある場合は SIOC 2 が必要です	10	ソリッド ステート ドライブ ベイ（最大で 4 つの 2.5 インチ SAS SSD） • ベイ 1 および 2 の SSD には、サーバ ベイ 1 のサーバ ノードが必要です • ベイ 3 および 4 の SSD には、サーバ ベイ 2 のサーバ ノードが必要です
4	電源装置（4、2+2 として冗長）	11	Cisco UCS C3260 M4 サーバ ノードのラベル（M4 SVRN） （注） このラベルは、 Cisco UCS C3260 M4 および M5サーバ ノードを識別します。Cisco UCS C3260 M3 サーバ ノードにはラベルがありません。
5	40 Gb SFP+ ポート（SIOC ごとに 2 つ）	12	KVM コンソール コネクタ（サーバ ノードごとに 1 つ） USB 2 個、VGA 1 個、シリアル コネクタ 1 個を装備した KVM ケーブルで使用

6	Chassis Management Controller（CMS）のデバッグ ファームウェア ユーティリティ ポート（SIOC ごとに 1 つ）	13	サーバー ノードのユニット識別ボタン/LED
7	10/100/1000 専用管理ポート、RJ-45 コネクタ（SIOC ごとに 1 つ）	14	サーバー ノードの電源ボタン
		15	サーバ ノードのリセット ボタン（サーバ ノードのチップセットをリセット）

ストレージ サーバ コンポーネント

サーバ ノード

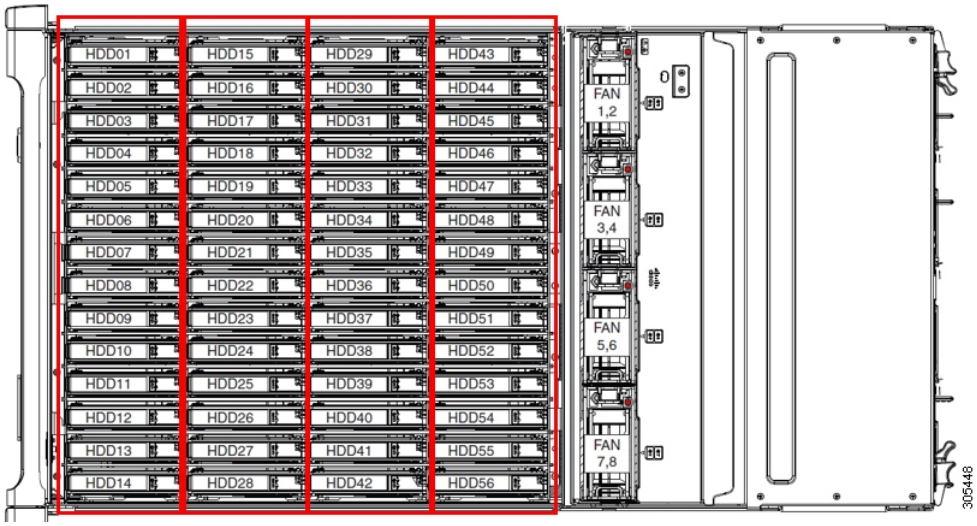
Cisco UCS C3260 システムは、1 つまたは 2 つのノードから構成されています。各ノードには 2 つの CPU、128 GB、256 GB、または 512 GB の DIMM メモリ、最大 4 GB のキャッシュの RAID カードまたはパススルー コントローラが備わっています。サーバ ノードは次のいずれかです。

- Cisco UCS C3260 M3 サーバ ノード
- Cisco UCS C3260 M4 サーバ ノード：このノードに、サーバ ノードの上部に接続するオプションの I/O エクスパンダが含まれる場合があります。
- Cisco UCS C3260 M5 サーバ ノード：このノードに、サーバ ノードの上部に接続するオプションの I/O エクスパンダが含まれる場合があります。

ディスク スロット

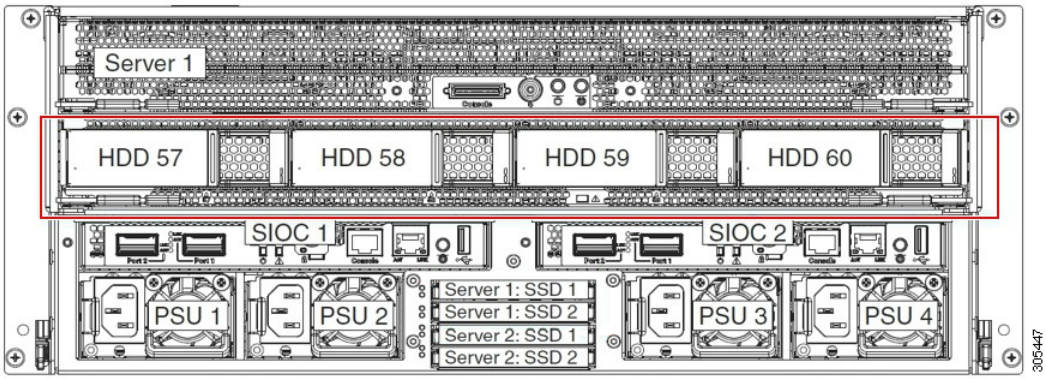
Cisco UCS S3260 シャーシ の HDD マザーボードに 14 ディスク スロットが 4 行と、HDD 拡張トレイに追加の 4 ディスク スロットがあります。次の図は、上面からアクセス可能でホットスワップ可能な 56 台の 3.5 インチの 6 TB または 4 TB 7200 rpm NL-SAS HDD ドライブのディスクの配置を示しています。ディスク スロットに 2 つの SAS ポートがあり、それぞれがシャーシの SAS エクスパンダに接続されます。

図 *6 : Cisco UCS C3260* 上面図



次の図は、HDD 拡張トレイに 4 つの追加ディスク スロットを備えた Cisco UCS S3260 シャーシ を示しています。

図 *7 : HDD* 拡張トレイを搭載した *Cisco UCS 3260*（背面図）



2 つのサーバ ノードと 2 つの SIOC がある場合、次の機能を使用できます。

1. 上のサーバ ノードは左の SIOC（サーバ スロット 1、SIOC1）を使用します。
2. 下のサーバは右の SIOC（サーバ スロット 2、SIOC2）を使用します。

2 つの SIOC を搭載した 1 つのサーバ ノードがある場合、Server SIOC Connectivity 機能を有効にできます。リリース 3.1(3) から、Cisco UCS C3260システムでは Server SIOC Connectivity 機能がサポートされています。シャーシに単一サーバとデュアル SIOC が装着されている場合、この機能を使用して、プライマリ SIOC および補助 SIOC の両方を経由するデータ パスを設定できます。

SAS エクスパンダ

Cisco UCS C3260 システムには、冗長モードで実行し、シャーシ レベルのディスクをサーバのストレージ コントローラに接続する 2 つの SAS エクスパンダがあります。SAS エクスパンダは、ストレージコントローラの間に2つのパスを提供するため、可用性が向上します。それらには、次の利点があります。

- ハード ドライブのプールを管理します。
- サーバのストレージ コントローラへのハード ドライブのディスクのゾーン設定。

リリース 3.2(3a) 以降、Cisco UCS Manager は、ディスク スロットごとに単一の DiskPort を設定することによって、ディスクへの単一パス アクセスを有効にすることができます。これにより、サーバは単一のデバイスのみを検出し、マルチパス設定を避けることができます。

次の表に、各 SAS エクスパンダのポートの、導入の種類に基づくディスクへの接続方法について示します。

Port range	Connectivity
1 ～ 56	上面からアクセス可能なディスク
57 ～ 60	HDD 拡張トレイのディスク。

（注） ストレージ コントローラと SAS エクスパンダ間の SAS のアップリンクの数は、サーバに搭載されているコントローラのタイプによって異なることがあります。

ストレージ エンクロージャ

Cisco UCS C3260には、次のタイプのストレージ エンクロージャが備わっています。

シャーシ レベルのストレージ エンクロージャ

- HDD motherboard enclosure：シャーシの 56 のデュアル ポート ディスク スロットは、HDD マザーボード エンクロージャで構成されています。
- **HDD 拡張トレイ**：Cisco UCS C3260 システムに追加された 4 つのデュアル ディスク スロットで HDD 拡張トレイを構成しています。

（注） HDD拡張トレイは現場交換可能ユニット（FRU）です。ディスクは挿入時は未割り当てのままであり、ストレージコントローラに割り当てることができます。ディスク ゾーン分割の実行方法の詳細については、次を参照してください。 ディスク ゾーン分割ポリシー （262 ページ）

サーバ レベルのストレージ エンクロージャ

サーバ レベルのストレージ エンクロージャは、サーバに事前に割り当てられた専用のエンクロージャです。次のいずれかになります。

- **背面ブート SSD エンクロージャ**：このエンクロージャには、Cisco UCS C3260 システムの背面パネル上の 2 つの 2.5 インチ ディスク スロットが含まれています。各サーバは 2 つの専用ディスク スロットを備えています。これらのディスク スロットは SATA SSD をサポートします。
- Server board NVMe enclosure：このエンクロージャには 1 つの PCIe NVMe コントローラが搭載されています。

（注） Cisco UCS C3260 システムでは、上記 2 種類のエンクロージャに物理的にディスクが存在することができても、ホスト OS からは、すべてのディスクが SCSI エンクロージャの一部として見なされます。これらは単一 SES エンクロージャとして動作するように設定された SAS エクスパンダに接続されます。

ストレージ コントローラ

メザニン ストレージ コントローラ

次の表に、さまざまなストレージコントローラのタイプ、ファームウェアのタイプ、モード、共有および OOB サポートを示します。

表 *6*：

ストレージ コントローラのタイプ	ファームウェアのタイプ	モード	共有	OOB サポート
UCSC-S3X60-R1GB	メガ RAID	HW RAID、JBOD	いいえ	○
UCS-C3K-M4RAID	メガ RAID	HW RAID、JBOD	いいえ	○
UCSC-S3X60-HBA	イニシエータ ターゲット	パススルー	はい	はい
UCS-S3260-DHBA	イニシエータ ターゲット	パススルー	はい	はい
UCS-S3260-DRAID	メガ RAID	HW RAID、JBOD	いいえ	○

その他のストレージ コントローラ

SW RAID コントローラ：Cisco UCS C3260 システム内のサーバは、SW RAID コントローラに接続している PCIe ライザーに組み込まれた、2 つの専用内部 SSD をサポートします。このコントローラは、Cisco C3000 M3 サーバでサポートされます。

NVMe コントローラ： Cisco UCS C3260 システム内のサーバによって、NVMe ディスクのインベントリとファームウェア アップデートにこのコントローラが使用されます。

さまざまなサーバ ノードでサポートされているストレージ コントローラに関する詳細は、関連するサービス ノートを参照してください。

- Cisco UCS S3260 ストレージ サーバ サービス ノート用 Cisco UCS C3X60 M3 サーバ ノード
- Cisco UCS S3260 ストレージ サーバ サービス ノート用 Cisco UCS C3X60 M4 サーバ ノード
- Cisco UCS S3260 ストレージ サーバ用 Cisco UCS S3260 M5 サーバ ノードのサービス ノート

Cisco UCS C3260 ストレージ管理操作

次の表に、Cisco UCS Manager 統合 Cisco UCS C3260 システムで、実行できるさまざまなストレージ管理操作を示します。

動作	説明	次を参照してください。
高可用性のためのディスクの共有	Cisco UCS C3260 システムの SAS エクスパンダは、ドライブのプールをシャーシ レベルで管理できます。高可用性のためにディスクを共有するには、次の手順を実行してください。 **1.** ディスク ゾーン分割ポリシーを作成します。 **2.** ディスクのスロットを作成し、所有権を割り当てます。 **3.** シャーシ プロファイルにディスクを関連付けます。	このガイドの「ディスク ゾーン分割ポリシー」セクション。

動作	説明	次を参照してください。
ストレージ プロファイル、ディスク グループおよびディスク グループ設定ポリシー	Cisco UCS C3260 システムでストレージ ディスクの定義、ディスクの割り当て、および管理を行うには、Cisco UCS Manager のストレージ プロファイルとディスク グループ ポリシーを利用できます。	『』の「Storage Profiles」セクション。*Cisco UCS Manager* リリース *3.2* ストレージ管理ガイド
ストレージ エンクロージャ操作	サーバで、HDD 拡張トレイを交換するか、以前に挿入したトレイを取り外します。	このガイドの「シャーシ レベルのストレージ エンクロージャの削除」セクション。

高可用性のためのディスクの共有

ディスク ゾーン分割ポリシー

ディスク ゾーン分割を使用してサーバ ノードにドライブを割り当てることができます。ディスク ゾーン分割は、同一サーバのコントローラまたは異なるサーバのコントローラで実行することができます。ディスクの所有権は次のいずれかになります。

未割り当て

未割り当てのディスクとは、サーバ ノードに表示されていないものを指します。

専用

このオプションを選択すると、 **[Server]**、 **[Controller]**、 **[Drive Path]**、およびディスク スロットの **[Slot Range]** の値を設定する必要があります。

（注） ディスクは割り当てられたコントローラにのみ表示されます。

リリース 3.2(3a)以降、Cisco UCS S 3260 M 5 以降のサーバでは、 Cisco UCS Manager は、ディスク スロットごとに単一の DiskPort を設定することによって、ディスクへの単一パス アクセスを有効にすることができます。1 つのパスの設定により、サーバが設定で選択されたドライブが 1 つパスでのみディスク ドライブを検出します。シングルパスアクセスは、**Cisco UCS S3260 デュアル パス スルー コントローラ** (UCS-S3260-DHBA) でのみサポートされています。

シングル パス アクセスが有効になると、3.2(3a)より前のリリースにダウングレードすることはできません。ダウングレードするには、ディスク ゾーニング ポリシーでディスク

スロットのディスク パスを**Path Both**に設定して、この機能を無効にし、すべてのディスク スロットを両方のディスク ポートに割り当てます。

共有

共有ディスクとは、複数のコントローラに割り当てられるものを指します。これらは、サーバがクラスタ構成で動作し、各サーバに HBA モードのストレージ コントローラがある場合に絞って使用されます。

（注） デュアル HBA コントローラを使用する場合は、特定の条件下では共有モードを使用できません。

シャーシのグローバル ホット スペア

このオプションを選択すると、ディスクの**[Slot Range]**の値を設定する必要があります。

重要 ディスクの移行と孤立した LUN の要求：サーバ（サーバ 1）へゾーン分割されたディスクを別のサーバ（サーバ 2）に移行するには、仮想ドライブ（LUN）を転送準備完了としてマークするか、仮想ドライブを非表示にする処理を実行します。次に、そのディスクに割り当てるディスク ゾーン分割ポリシーを変更できます。仮想ドライブ管理の詳細については、『Cisco UCS Manager Storage Management Guide』の「*Disk Groups and Disk Configuration Policies*」のセクションを参照してください。

ディスク ゾーン分割ポリシーの作成

Procedure

	Command or Action	Purpose
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 disk-zoning-policy** *diskzoning policy-name*	指定した名前のディスク ゾーン分割ポリシーを作成します。
ステップ 3	UCS-A /org/disk-zoning-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。

Example

次の例では、dzp1 ディスク ゾーン分割ポリシーを作成します。

```
UCS-A# scope org
```

```
UCS-A /org # create disk-zoning-policy dzp1
UCS-A /org/disk-zoning-policy*# commit-buffer
UCS-A /org/disk-zoning-policy#
```

ディスク スロットの作成と所有権の割り当て

Procedure

	Command or Action	Purpose
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/ # **disk-zoning-policy** *disk-zoning-policy-name*	ディスク ゾーン分割ポリシーに移動します。
ステップ 3	UCS-A org/disk-zoning-policy # **create disk-slot** *slot-id*	指定したスロット番号のディスク スロットを作成します。
ステップ 4	UCS-A org/disk-zoning-policy/disk-slot* # **set ownership** *ownership-type {chassis-global-host-spare\dedicated\shared\unassigned}*	ディスクの所有権を次のいずれかに指定します: • **chassis-global-hot-spare**：シャーシ グローバル ホット スペア • **dedicated**：専用 リリース 3.2(3a) 以降、Cisco UCS Manager は、ディスク スロットごとに単一の DiskPort を設定することによって、ディスクへの単一パス アクセスを有効にすることができます。これにより、サーバは単一のデバイスのみを検出し、マルチパス設定を避けることができます。 ドライブのパスのオプションは次のとおりです。 • **path-both (デフォルト)** - ドライブ パスは両方の SAS エクスパンダにゾーニングされます。 • **path-0** - ドライブ パスは、SAS エクスパンダ 1 にゾーニングされます。

	Command or Action	Purpose
		• **path-1** - ドライブ パスは、SAS エクスパンダ 2 にゾーニングされます。 drivepath を設定するのには、次のコマンドを使用します。 **`set drivepath`** ***`drivepath{path-0/path-1/path-both}`*** • **shared**：共有 **Note** デュアル HBA コントローラを使用する場合は、特定の条件下では共有モードを使用できません。デュアル HBA コントローラの**共有**モードの条件を確認するには、Table 7: デュアル HBA コントローラの共有モードの制約事項, on page 265を参照してください。 • **unassigned**：未割り当て
ステップ 5	UCS-A org/disk-zoning-policy/disk-slot* # **create controller-ref** *server-id* **sas** *controller-id*	指定したサーバ スロットのコントローラ参照を作成します。
ステップ 6	UCS-A org/disk-zoning-policy/disk-slot # **commit-buffer**	トランザクションをコミットします。

Table 7: デュアル ***HBA*** コントローラの共有モードの制約事項

サーバ	HDD トレイ	コントローラ	共有モードのサポート
Cisco UCS C3260	非対応	デュアル HBA	未サポート
Cisco UCS C3260	HDD トレイ	デュアル HBA	未サポート
事前プロビジョニング	HDD トレイ	デュアル HBA	未サポート

Example

次の例では、ディスク スロット 1 を作成して所有権を共有に設定し、サーバ スロット 1 のコントローラ参照を作成してトランザクションをコミットします。

```
UCS-A# scope org
UCS-A /org # scope disk-zoning-policy test
UCS-A /org/disk-zoning-policy* # create disk-slot 1
UCS-A /org/disk-zoning-policy/disk-slot* # set ownership shared
UCS-A /org/disk-zoning-policy/disk-slot* # create controller-ref 1 sas 1
UCS-A /org/disk-zoning-policy/disk-slot* # create controller-ref 2 sas 1
UCS-A /org/disk-zoning-policy/disk-slot* #commit-buffer
UCS-A /org/disk-zoning-policy/disk-slot #
```

シャーシ プロファイルへのディスク ゾーン分割ポリシーの関連付け

Procedure

	Command or Action	Purpose
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 chassis-profile** *chassis-profile-name*	指定した名前でシャーシ プロファイルを作成します。
ステップ 3	UCS-A org/chassis-profile* # **set disk-zoning-policy** *disk-zoning-policy*	指定したディスク ゾーン分割ポリシーを設定します。
ステップ 4	UCS-A org/chassis-profile* # **commit-buffer**	トランザクションをコミットします。
ステップ 5	UCS-A org/chassis-profile # **associate chassis** *chassis-id*	ディスク ゾーン分割ポリシーに含まれるディスクを、指定したシャーシ番号のシャーシに関連付けます。

Example

次の例では、ch1 シャーシ プロファイルを作成してディスク ゾーン分割ポリシー all56shared を設定し、トランザクションをコミットして all56shared ポリシーに含まれるディスクをシャーシ 3 に関連付けます。

```
UCS-A# scope org
UCS-A /org # create chassis-profile ch1
UCS-A /org/chassis-profile* # set disk-zoning-policy all56shared
UCS-A /org/chassis-profile* # commit-buffer
UCS-A /org/chassis-profile # associate chassis 3
UCS-A /org/fw-chassis-pack/pack-image #
```

ディスクの移行

1 つのサーバから別のサーバへゾーン分割されているディスクを移行する前に、転送準備完了として仮想ドライブ（LUN）をマークするか、または仮想ドライブの非表示操作を実行する必要があります。これにより、サービスプロファイルからのすべての参照がディスクの移行前に削除されたことを確認します。仮想ドライブの詳細については、『』の「virtual drives」セクションを参照してくださいCisco UCS Manager リリース 3.2 ストレージ管理ガイド

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A# **scope chassis** シャーシ番号	指定したシャーシのシャーシ モードを開始します。
ステップ 2	UCS-A /chassis# **scope virtual-drive-container** *virtual-drive-container-num*	指定した番号の仮想ドライブ コンテナに移動します。
ステップ 3	UCS-A /chassis/virtual-drive-container# **scope virtual-drive** *virtual-drive--num*	指定した仮想ドライブ コンテナの仮想ドライブに移動します。
ステップ 4	UCS-A /chassis/virtual-drive-container/virtual-drive# **scope virtual-drive** *virtual-drive--num* **set admin-state** *admin-state*	仮想ドライブの管理状態として、次のいずれかを指定します。 • **clear-transport-ready**：仮想ドライブをトランスポート可能でなくなった状態として設定します。 • **delete**：仮想ドライブを削除します。 • **hide**：1 つのサーバから別のサーバへ仮想ドライブを安全に移行するには、このオプションを選択します。 **Note** ディスク グループのすべての仮想ドライブは、移行またはサーバノードから割り当て解除される前に、非表示としてマークされている必要があります。 • **transport-ready**：1 つのサーバから別のサーバへ仮想ドライブを安全に

	Command or Action	Purpose
		移行するには、このオプションを選択します。 **Note** 仮想ドライブはトランスポート可能としてマークされると、ストレージ コントローラによって、そのドライブ上でのすべてのIO操作がディセーブルになります。さらに、仮想ドライブのゾーン分割と外部構成のインポートが完了した後、仮想ドライブが動作可能になります。
ステップ 5	UCS-A /chassis/virtual-drive-container/virtual-drive# **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。

Example

次の例では、仮想ドライブ コンテナ 1 の仮想ドライブ 1001 の状態をトランスポート可能として設定します。

```
UCS-A# scope chassis
UCS-A /chassis# scope virtual-drive-container 1
UCS-A /chassis/virtual-drive-container# scope virtual-drive 1001
UCS-A /chassis/virtual-drive-container/virtual-drive# set admin-state transport-ready
UCS-A /chassis/virtual-drive-container/virtual-drive# commit-buffer
```

ストレージ エンクロージャ操作

シャーシ レベルのストレージ エンクロージャの削除

物理的に取り外した後で、Cisco UCS ManagerのHDD拡張トレイに対応するストレージエンクロージャを削除できます。サーバ レベルまたは他のシャーシ レベルのストレージ エンクロージャは削除できません。

Procedure

	Command or Action	Purpose
ステップ 1	UCS-A # **scope chassis** *chassis-id*	指定したシャーシでシャーシ モードを開始します。
ステップ 2	UCS-A /chassis # **remove storage-enclosure** *storage-enclosure-name*	指定した名前のシャーシ レベルのストレージ エンクロージャを削除します。

Example

次に、シャーシ 2 からストレージ エンクロージャ 25 を削除する例を示します。

```
UCS-A# scope chassis 2
UCS-A /chassis# remove storage-enclosure 25
UCS-A /chassis#
```

SAS エクスパンダ設定ポリシー

SAS エクスパンダ設定ポリシーの作成

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] に / を入力します。
ステップ 2	UCS-A org/ # **create sas-expander-configuration-policy** *sas-expander-configuration-policy-name*	指定されたポリシー名で SAS エクスパンダ設定ポリシーを作成します。
ステップ 3	（任意） UCS-A /org/sas-expander-configuration-policy* # **set descr** *description*	ポリシーの説明を記します。
ステップ 4	（任意） UCS-A /org/sas-expander-configuration-policy* # **set 6g-12g-mixed-mode** *disabled|enabled|no-change*	（注） [6G-12G Mixed Mode]モードを有効または無効にするには、システムが再起動します。 • [Disabled]：このポリシーでは接続管理が無効になっているため、12G

	コマンドまたはアクション	目的
		が使用可能でも SAS エクスパンダは 6G の速度のみを使用します。 • [Enabled]：このポリシーでは接続管理が有効になっており、可用性に基づいて 6G と 12G 間で速度をインテリジェントに切り替えます。 • [No Change]（デフォルト）：事前の設定が保持されます。
ステップ 5	UCS-A /org/sas-expander-configuration-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、secp1 SAS エクスパンダ設定ポリシーを作成します。

```
UCS-A# scope org
UCS-A /org # create sas-expander-configuration-policy secp1
UCS-A /org/sas-expander-configuration-policy*# set 6g-12g-mixed-mode enabled
UCS-A /org/sas-expander-configuration-policy*# commit-buffer
UCS-A /org/sas-expander-configuration-policy#
```

SAS エクスパンダ設定ポリシーの削除

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 sas-expander-configuration-policy** *sas-expander-configuration-policy-name*	指定されたポリシー名と SAS エクスパンダ設定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コミットします。

例

次の例では、secp1 SAS エクスパンダ設定ポリシーを削除します。

```
UCS-A# scope org
UCS-A /org # delete create sas-expander-configuration-policy secp1
UCS-A /org*# commit-buffer
UCS-A /org/#
```

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。