Cisco UCS Manager リリース 4.0 ストレージ管理ガイド

初版：2018 年 8 月 14 日

最終更新：2019 年 8 月 26 日

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

© 2018–2019 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに xiii

対象読者 xiii

表記法 xiii

関連 Cisco UCS 資料 xv

マニュアルに関するフィードバック xv

第 1 章

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

第 2 章

概要 3

概要 3

ストレージ オプション 4

ストレージ設計の考慮事項 5

ストレージ設定の順序 6

ストレージ プロトコル 6

UCS Manager の [SAN] タブ 7

第 3 章

SAN ポートおよびポート チャネル 9

ポート モード 9

ポート タイプ 10

サーバ ポート 11

サーバ ポートの設定 11

ファブリック インターコネクトのポートの再設定 11

ファブリック インターコネクトのポートのイネーブル化またはディセーブル化 12

ファブリック インターコネクトのポート設定解除 13
アプライアンス ポート 13
アプライアンス ポートの設定 13
アプライアンス ポートのプロパティの変更 15
FCoE およびファイバ チャネル ストレージ ポート 15
イーサネット ポートの FCoE ストレージ ポートとしての設定 15
ファイバ チャネル ストレージ ポートの設定 16
アップリンク ファイバ チャネル ポートの復元 17
FC リンクの再調整 17
FC アップリンク ポートの設定 18
FCoE アップリンク ポート 18
FCoE アップリンク ポートの設定 19
ユニファイド ストレージ ポート 20
アプライアンス ポートのユニファイド ストレージ ポートとしての設定 20
ユニファイド ストレージ ポートの設定解除 21
ユニファイド アップリンク ポート 22
ユニファイド アップリンク ポートの設定 22
ユニファイド アップリンク ポートの設定解除 23
ポリシーベースのポート エラー処理 23
エラーベース アクションの設定 24
ファイバ チャネル ポート チャネル 24
ファイバ チャネル ポート チャネルの作成 25
ファイバ チャネル ポート チャネルのイネーブル化 26
ファイバ チャネル ポート チャネルのディセーブル化 26
ファイバ チャネル ポート チャネルのポートの追加および削除 26
ファイバ チャネル ポート チャネルのプロパティの変更 27
ファイバ チャネル ポート チャネルの削除 28
FCoE ポート チャネル数 28
FCoE ポート チャネルの作成 28
FCoE ポート チャネルの削除 29
ユニファイド アップリンク ポート チャネル 29

第 4 章 ファイバ チャネルのゾーン分割 31

ファイバ チャネル ゾーン分割に関する情報 31

ゾーンに関する情報 31

ゾーン セットに関する情報 32

Cisco UCS Manager でのファイバ チャネル ゾーン分割のサポート 32

Cisco UCS Manager-ベースのファイバ チャネル ゾーン分割 33

vHBA イニシエータ グループ 33

ファイバ チャネル ストレージ接続ポリシー 34

ファイバ チャネル アクティブ ゾーン セット設定 34

スイッチベースのファイバ チャネル ゾーン分割 34

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 34

ファイバ チャネル ゾーン分割の設定 35

ファイバ チャネル ゾーン分割用の VSAN の作成 36

新しいファイバ チャネル ゾーン プロファイルの作成 39

ファイバ チャネル ゾーン プロファイルの削除 42

ファイバ チャネル ユーザ ゾーンの削除 42

ファイバ チャネル ストレージ接続ポリシー 43

ファイバ チャネル ストレージ接続ポリシーの削除 43

第 5 章 ネームド VSAN 45

ネームド VSAN 45

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 46

VSAN に関するガイドラインおよび推奨事項 46

ネームド VSAN の作成 48

ストレージ VSAN の作成 49

ネームド VSAN の削除 50

ストレージ VSAN の FCoE VLAN の VLAN ID の変更 51

ファイバ チャネル アップリンク トランキングのイネーブル化 51

ファイバ チャネル アップリンク トランキングのディセーブル化 52

第 6 章 SAN ピン グループ 53
SAN ピン グループ 53
SAN ピン グループの作成 54
SAN ピン グループの削除 54

第 7 章 FC ID の割り当て 55
ファイバ チャネル ID 55

第 8 章 WWN プール 57
WWN プール 57
WWNN プールの作成 58
WWNN プールへの WWN ブロックの追加 60
WWNN プールからの WWN ブロックの削除 61
WWNN プールへの WWNN イニシエータの追加 61
WWPN プールからの WWPN イニシエータの削除 62
WWNN プールの削除 62
WWPN プール 63
WWPN プールの作成 63
WWPN プールへの WWN ブロックの追加 65
WWPN プールからの WWN ブロックの削除 65
WWPN プールへの WWPN イニシエータの追加 66
WWPN プールからの WWPN イニシエータの削除 67
WWPN プールの削除 68
WWxN プール 68
WWxN プールの作成 68
WWxN プールへの WWN ブロックの追加 70
WWxN プールからの WWN ブロックの削除 71
WWxN プールの削除 71

第 9 章 ストレージ関連ポリシー 73

vHBA テンプレートについて 73
vHBA テンプレート 73
vHBA テンプレートの作成 73
vHBA テンプレートへの vHBA のバインディング 75
vHBA テンプレートからの vHBA のバインド解除 76
vHBA テンプレートの削除 76
ファイバ チャネル アダプタ ポリシー 77
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 77
ファイバ チャネル アダプタ ポリシーの作成 79
ファイバ チャネル アダプタ ポリシーの削除 85
デフォルトの vHBA 動作ポリシーについて 86
デフォルトの vHBA 動作ポリシー 86
デフォルトの vHBA 動作ポリシーの設定 86
SAN 接続ポリシー 87
LAN および SAN 接続ポリシーについて 87
LAN および SAN の接続ポリシーに必要な権限 87
サービス プロファイルと接続ポリシー間の相互作用 88
SAN 接続ポリシーの作成 88
SAN 接続ポリシー用の vHBA の作成 89
SAN 接続ポリシーからの vHBA の削除 90
SAN 接続ポリシー用のイニシエータ グループの作成 90
SAN 接続ポリシーからのイニシエータ グループの削除 91
SAN 接続ポリシーの削除 92

第 10 章 **SED セキュリティ ポリシー 93**
自己暗号化ドライブのセキュリティ ポリシー 93
コントローラとディスクのセキュリティ フラグ 94
ローカル セキュリティ ポリシーの管理 94
ローカル セキュリティ ポリシーの作成 94
ローカル セキュリティ ポリシーの変更 95

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 96
KMIP クライアント証明書ポリシー 96
グローバル KMIP クライアント証明書ポリシーの作成 97
サーバ用の KMIP クライアント証明書ポリシーの作成 98
リモート セキュリティ ポリシーの管理 99
リモート セキュリティ ポリシーの作成 99
リモート セキュリティ ポリシーの変更 100
リモート セキュリティ キーの変更 100
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 101
ディスクのセキュリティのイネーブル化とディセーブル化 101
コントローラのセキュリティのディセーブル化 102
ロックされたディスクのロックの解除 102
セキュア外部設定ディスクの消去 103

第 11 章 ストレージ プロファイル 105
ストレージ プロファイル 105
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 106
仮想ドライブ 106
ディスク グループ ポリシーの設定 108
RAID レベル 111
自動ディスク選択 113
サポートされている LUN の変更 114
サポートされていない LUN の変更 114
ディスク挿入の処理 115
非冗長仮想ドライブ 115
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 115
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 116
ホット スペア ドライブの交換 116
未使用スロットへの物理ドライブの挿入 117
仮想ドライブの命名 117

LUN の参照解除 117
コントローラの制限と制約事項 118
ストレージ プロファイル 118
ストレージ プロファイルの作成 118
特定のストレージ プロファイルの作成 119
ストレージ プロファイルの削除 120
ローカル LUN 120
ローカル LUN の設定 120
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 122
ローカル LUN の削除 123
PCH コントローラ定義 123
PCH SSD コントローラ定義 123
ストレージ プロファイル PCH コントローラ定義の作成 125
サービス プロファイル PCH コントローラ定義の変更 130
ストレージ プロファイル PCH コントローラ定義の削除 135
不良 M.2 ディスクの交換 136
ストレージ プロファイルと既存のサービス プロファイルとの関連付け 137
ストレージ プロファイルの設定 138
ブレード サーバの RAID コントローラの外部設定のインポート 138
ラック サーバの RAID コントローラの外部設定のインポート 138
ブレード サーバのローカル ディスク操作の設定 138
ラック サーバのローカル ディスク操作の設定 139
ローカル ディスクの設定操作 139
ローカル ストレージのブート ポリシー 141
組み込みのローカル LUN のブート ポリシーの設定 142
組み込みのローカル ディスクのブート ポリシーの設定 142
サービス プロファイル内のローカル LUN 操作 143
LUN 名の事前プロビジョニング 143
孤立した LUN の要求 144
LUN の展開および展開解除 144
サービス プロファイルで参照されている LUN の名前変更 145

第 12 章 ミニ ストレージ 147

ミニ ストレージ 147

ミニ ストレージ プロパティの表示 147

第 13 章 SD カード サポートの設定 149

FlexFlash Secure Digital Card Support 149

FlexFlash FX3S Support 151

FlexFlash SD カードのサポートのイネーブル化 152

FlexFlash SD カードのサポートのディセーブル化 152

自動同期のイネーブル化 153

Formatting the SD Cards 153

FlexFlash コントローラのリセット 154

FlexUtil セキュア デジタル カードのサポート 154

第 14 章 ダイレクト アタッチド ストレージ 155

ダイレクト アタッチド ストレージ 155

ファイバ チャネル スイッチング モード 155

ファイバ チャネル スイッチング モードの設定 157

ストレージ VSAN の作成 158

ファイバ チャネル ゾーン分割用の VSAN の作成 158

ファイバ チャネル ストレージ ポートの設定 161

ファイバ チャネル ゾーン分割の設定 162

ファイバ チャネル ストレージ接続ポリシーの作成 163

[Expert] ウィザードを使用したサービス プロファイルの作成 165

サービス プロファイルとサーバまたはサーバ プールの関連付け 167

ファイバ チャネル ゾーン分割設定の確認 168

ファイバ チャネル ゾーン分割設定のトラブルシューティング 168

第 15 章 ストレージ インベントリ 171

ローカル ディスク ロケータ LED のステータス 171

ローカル ディスク ロケータ LED のオンとオフの切り替え 172
NVMe の高度な VMD 搭載したカスタム LED のステータス 172
NVMe で最適化された M5 サーバ 176
MSwitch ディザスタ リカバリ 178
NVMe PCIe SSD インベントリ 178
NVMe PCIe SSD ストレージ インベントリの表示 178

第 16 章 **Cisco UCS S3260 システム ストレージ管理 181**
ストレージ サーバ機能およびコンポーネントの概要 181
Cisco UCS S3260 ストレージ管理操作 189
高可用性のためのディスクの共有 190
ディスク ゾーン分割ポリシー 190
ディスク ゾーン分割ポリシーの作成 191
ディスク スロットの作成と所有権の割り当て 194
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 195
ディスクの移行 196
ストレージ エンクロージャ操作 198
シャーシ レベルのストレージ エンクロージャの削除 198

はじめに

- 対象読者 （xiii ページ）
- 表記法 （xiii ページ）
- 関連 Cisco UCS 資料 （xv ページ）
- マニュアルに関するフィードバック （xv ページ）

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 ラベルなどの GUI 要素は、イタリック体（**italic**）で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルなどのメイン タイトルは、ボールド体（**bold**）で示しています。
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、イタリック体（*this font*）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 安全上の重要な注意事項

この警告マークは「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。機器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、一般的な事故防止対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存しておいてください

関連 Cisco UCS 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、以下の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

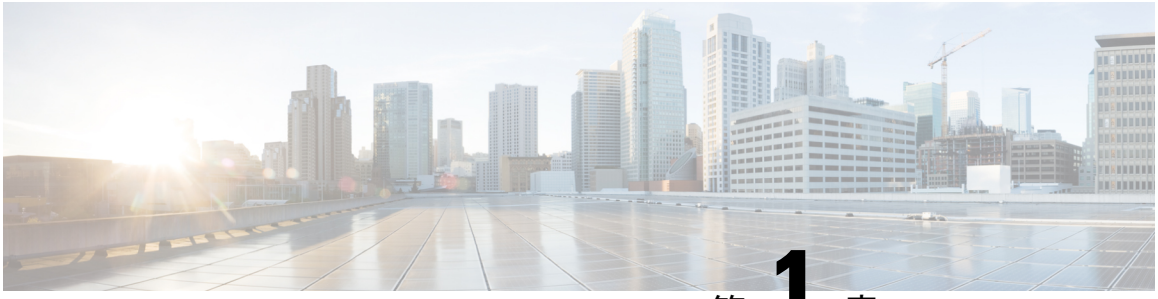
管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、「Release Bundle Contents for Cisco UCS Software」を参照してください。

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、または誤りや記載もれなどお気づきの点がございましたら、ucs-docfeedback@external.cisco.com までコメントをお送りください。ご協力をよろしくお願いいたします。



第 1 章

新機能および変更された機能に関する情報

• 新機能および変更された機能に関する情報 （1 ページ）

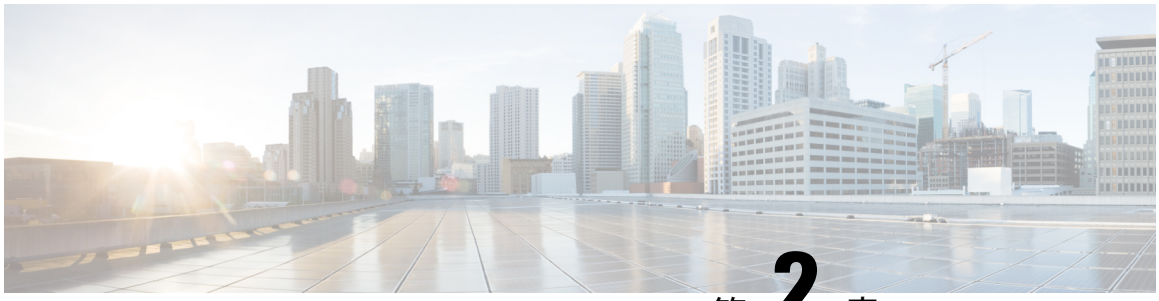
新機能および変更された機能に関する情報

ここでは、Cisco UCS Manager、リリース4.0(1a) 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 *4.0(1a)* の新機能と変更された動作

機能	説明	参照先
Cisco UCS 6454 Fabric Interconnect	このリリースでは、40/100ギガビットアップリンクポートを使用してファブリック内の10/25ギガビットポートをサポートするCisco UCS 6454 Fabric Interconnectが導入されました。	イーサネット ポートの FCoE ストレージ ポートとしての設定 （15 ページ）
Cisco UCS C125 M5 サーバ	Cisco UCS Managerは、Cisco UCS C125 M5 サーバの既存の機能すべてに対するサポートを拡張します。	PCH SSD コントローラ定義 （123 ページ）

新機能および変更された機能に関する情報



第 2 章

概要

- 概要 （3 ページ）
- ストレージ オプション （4 ページ）
- ストレージ設計の考慮事項 （5 ページ）
- ストレージ設定の順序 （6 ページ）
- ストレージ プロトコル （6 ページ）
- UCS Manager の [SAN] タブ （7 ページ）

概要

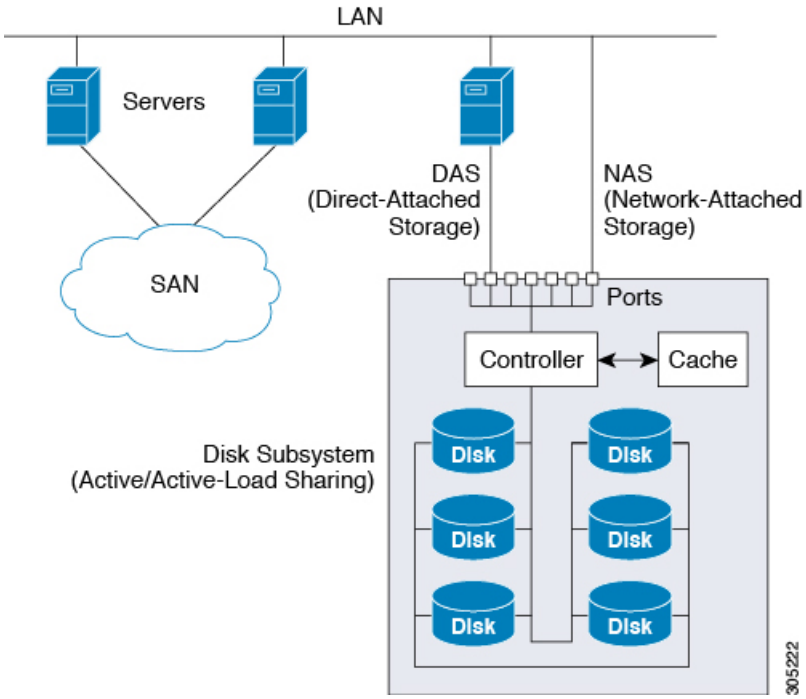
このガイドでは、次のようなストレージ管理タスクを設定する方法について説明します。

- 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。

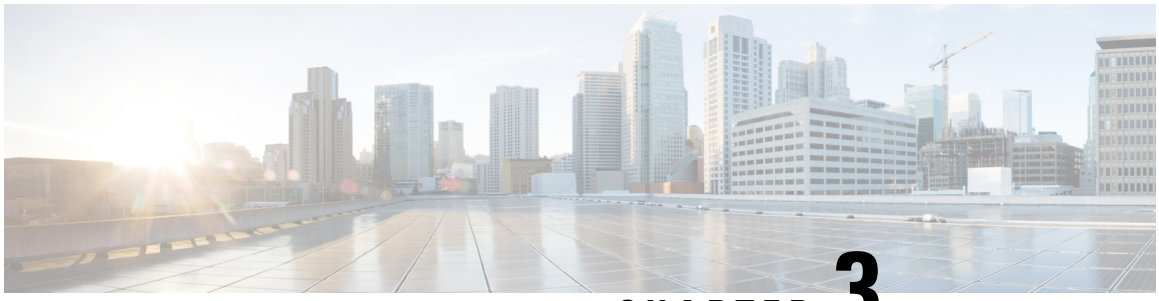
- [SAN Cloud]：このノードでは次の操作を実行できます。
  - SAN アップリンク（ストレージ ポート、ポート チャネル、SAN ピン グループなど）を設定します。
  - FC ID の割り当てを表示します。
  - WWN プール（WWPN、WWxN、および WWxN など）、iSCSI 修飾名（IQN）、プールを設定します。
  - 特定のエンド ポイントの FSM 詳細を表示してタスクが成功または失敗したかどうかを確認し、FSM を使用してエラーのトラブルシューティングを行います。

- 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。



CHAPTER 3

SAN ポートおよびポート チャネル

- ポート モード （9 ページ）
- ポート タイプ （10 ページ）
- サーバ ポート, on page 11
- ファブリック インターコネクトのポートの再設定, on page 11
- ファブリック インターコネクトのポートのイネーブル化またはディセーブル化 （12 ページ）
- ファブリック インターコネクトのポート設定解除, on page 13
- アプライアンス ポート （13 ページ）
- FCoE およびファイバ チャネル ストレージ ポート, on page 15
- FC リンクの再調整 （17 ページ）
- FC アップリンク ポートの設定 （18 ページ）
- FCoE アップリンク ポート （18 ページ）
- ユニファイド ストレージ ポート （20 ページ）
- ユニファイド アップリンク ポート （22 ページ）
- ポリシーベースのポート エラー処理 （23 ページ）
- ファイバ チャネル ポート チャネル （24 ページ）
- FCoE ポート チャネル数 （28 ページ）
- ユニファイド アップリンク ポート チャネル （29 ページ）

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 モードは Cisco UCS Manager で設定します。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 ポートのポート 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。

デフォルトでは、イーサネット ポート モードに変更されたユニファイド ポートはイーサネット 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 モードに変更された統合ポートは、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

イーサネットにポート モードを設定するときは、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 送信元ポートは、ポート タイプのいずれかを設定してから、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

ファイバ チャネルにポート モードを設定するときは、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
- FCoE アップリンク ポート
- SPAN 送信元ポート

（注） SPAN 送信元ポートは、ポート タイプのいずれかを設定してから、そのポートを SPAN 送信元として設定します。

サーバ ポート

サーバ ポートの設定

リストされているすべてのポート タイプは、サーバ ポートを含め、固定モジュールと拡張モジュールの両方で設定可能です。

このタスクでは、ポートの設定方法を1つだけ説明します。右クリック メニューから、または LAN アップリンク マネージャでも設定できます。

Procedure

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

ステップ 2 **[Equipment]** > **[Fabric Interconnects]** > **[*Fabric_Interconnect_Name*]** > **[Fixed Module]** > **[Ethernet Ports]** の順に展開します。

ステップ 3 [Ethernet Ports] ノードの下のポートをクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Reconfigure] をクリックします。

ステップ 6 ドロップダウン リストから [Configure as Server Port] を選択します。

ファブリック インターコネクトのポートの再設定

Procedure

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

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

ステップ 3 再設定するポートのノードを展開します。

ステップ 4 再設定するポートを 1 つ以上クリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Reconfigure] をクリックします。

ステップ 7 ドロップダウン リストからポートの再設定方法を選択します。

例：アップリンク イーサネット ポートをサーバ ポートとして再設定する

1. [Ethernet Ports] ノードを展開し、再設定するポートを選択します。
2. 上記のステップ 5 および 6 を実行します。
3. ドロップダウン リストから [Configure as Server Port] を選択します。

ファブリックインターコネクトのポートのイネーブル化またはディセーブル化

ファブリック インターコネクト上でポートを有効または無効にした後、1 分以上待ってからシャーシを再認識させます。シャーシを再認識させるのが早すぎると、シャーシからのサーバトラフィックのピン接続が、有効または無効にしたポートに対する変更を使用して更新されないことがあります。

ポートが設定されている場合にのみ、イネーブルまたはディセーブルにできます。ポートが未設定の場合は、イネーブルとディセーブルのオプションはアクティブではありません。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Fabric Interconnects]** > ***[Fabric_Interconnect_Name]*** の順に展開します。
ステップ 3 イネーブルまたはディセーブルにするポートのノードを展開します。
ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Enable Port] または [Disable Port] をクリックします。
ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 8 [OK] をクリックします。

ファブリック インターコネクトのポート設定解除

Procedure

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Fabric Interconnects]** > ***[Fabric_Interconnect_Name]*** の順に展開します。
ステップ 3 設定を解除するポートのノードを展開します。
ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Unconfigure] をクリックします。
ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 8 [OK] をクリックします。

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にも設定できます。

このタスクでは、アプライアンス ポートの設定方法を 1 つだけ説明します。[General] タブからアプライアンス ポートを設定することもできます。

（注） アップリンク ポートがダウンしているときにアプライアンスを設定すると、Cisco UCS Manager はアプライアンス ポートに障害が発生していることを通知するエラー メッセージを表示する場合があります。このメッセージは、関連するネットワーク制御ポリシーの [Action on Uplink Fail] オプションで制御されます。

手順

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

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

ステップ 3 設定するポートのノードを展開します。

ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。

サーバ ポート、アップリンク イーサネット ポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Reconfigure] をクリックします。

ステップ 7 ドロップダウン リストから、[Configure as Appliance Port] をクリックします。

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

ステップ 9 [Configure as Appliance Port] ダイアログ ボックスで、必須フィールドに入力します。

ステップ 10 [VLANs] 領域で、次の手順を実行します。

a) フィールド で、次のオプション ボタンの 1 つをクリックしてポート チャネルで使用するモードを選択します。

- **[Trunk]**：Cisco UCS Manager GUI に VLAN テーブルが表示され、使用する VLAN を選択することができます。
- **[Access]**：Cisco UCS Manager GUIに **[Select VLAN]**ドロップダウン リストが表示され、このポートまたはポート チャネルに関連付ける VLAN を選択できます。

いずれかのモードで、[Create VLAN] リンクをクリックして、新しい VLAN を作成できます。

（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。

b) [Trunk] オプション ボタンをクリックした場合は、VLAN テーブルの必須フィールドに入力します。
c) [Access] オプション ボタンをクリックした場合は、**[Select VLAN]**ドロップダウン リストから VLAN を選択します。

ステップ 11 （任意） エンドポイントを追加する場合は、[Ethernet Target Endpoint] チェックボックスをオンにし、名前と MAC アドレスを指定します。

ステップ 12 [OK] をクリックします。

アプライアンス ポートのプロパティの変更

手順

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

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

ステップ 3 変更するアプライアンス ポートのノードを展開します。

ステップ 4 [Ethernet Ports] を展開します。

ステップ 5 プロパティを変更するアプライアンス ポートをクリックします。

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

ステップ 7 [Actions] 領域で、[Show Interface] をクリックします。

すべてのフィールドを表示するには、ペインを展開するか、[Properties] ダイアログ ボックスのスクロール バーを使用することが必要になる場合があります。

ステップ 8 [Properties] ダイアログボックスで、必要に応じて値を変更します。

ステップ 9 [OK] をクリックします。

FCoE およびファイバ チャネル ストレージ ポート

イーサネット ポートの FCoE ストレージ ポートとしての設定

FCoE ストレージ ポートは、固定モジュールと拡張モジュールのどちらにも設定できます。

このタスクでは、FCoE ストレージ ポートの設定方法を 1 種類だけ説明します。ポートの[General] タブから FCoE ストレージ ポートを設定することもできます。

始める前に

これらのポートが有効になるためには、ファイバ チャネル スイッチング モードが [Switching] に設定されている必要があります。ストレージ ポートは、エンドホスト モードでは動作しません。

手順

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

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

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- **[Fixed Module]**
- **Expansion Module**

ステップ 4 [Ethernet Ports] ノード以下の 1 つ以上のポートをクリックします。

アップリンク イーサネット ポート、サーバ ポート、またはアプライアンス ポートを再設定する場合は、適切なノードを展開します。

ステップ 5 選択したポートを右クリックし、[Configure as FCoE Storage Port] を選択します。

ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 7 [OK] をクリックします。

ファイバ チャネル ストレージ ポートの設定

このタスクでは、FC ストレージ ポートの設定方法を 1 種類だけ説明します。そのポートの [General] タブから FC ストレージ ポートを設定することもできます。

始める前に

これらのポートが有効になるためには、ファイバ チャネル スイッチング モードが [Switching] に設定されている必要があります。ストレージ ポートは、エンドホスト モードでは動作しません。

手順

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

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

ステップ 3 [Expansion Module] ノードを展開します。

ステップ 4 [FC Ports] ノード以下の 1 つ以上のポートをクリックします。

ステップ 5 選択したポートを右クリックし、[Configure as FC Storage Port] を選択します。

ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 7 [OK] をクリックします。

アップリンク ファイバ チャネル ポートの復元

このタスクでは、アップリンク FC ポートとして動作する FC ストレージ ポートを復元する方法を 1 つだけ説明します。そのポートの [General] タブから FC ストレージ ポートを再設定することもできます。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Fabric Interconnects]** > ***[Fabric_Interconnect_Name]*** の順に展開します。
ステップ 3 [Expansion Module] ノードを展開します。
ステップ 4 [FC Ports] ノード以下の 1 つ以上のポートをクリックします。
ステップ 5 選択した 1 つ以上のポートを右クリックし、[Configure as Uplink Port] を選択します。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 7 [OK] をクリックします。

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 チャネルの作成 （25 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。

FC アップリンク ポートの設定

固定モジュールまたは拡張モジュールのいずれかに FC アップリンク ポートを設定できます。

このタスクでは、FC アップリンク ポートの設定方法を 1 つだけ説明します。FC アップリンク ポートは、ポートの右クリック メニューから設定することもできます。

手順

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

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

ステップ 3 設定するポートのノードを展開します。

ステップ 4 [FC Ports] ノードで、任意の**ストレージ** ポートを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域から、[Configure as Uplink Port] を選択します。

ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 Cisco UCS Manager GUI が成功のメッセージを表示します。

[Actions] 領域で、[Configure as Uplink Port] がグレーアウトして、[Configure as FC Storage Port] がアクティブになります。

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

固定モジュールまたは拡張モジュールに FCoE アップリンク ポートを設定できます。

このタスクでは、FCoE アップリンク ポートの設定方法を 1 つだけ説明します。アップリンク イーサネット ポートは、右クリックメニュー、またはポートの [General] タブから設定することもできます。

手順

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

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

ステップ 3 設定するポートのノードを展開します。

ステップ 4 [Ethernet Ports] ノードの下の、[Unconfigured] ポートを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Reconfigure] をクリックします。

ステップ 7 ドロップ ダウン オプションから、[Configure as FCoE Uplink Port] を選択します。

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

ステップ 9 Cisco UCS Manager GUI が成功のメッセージを表示します。

[Properties] 領域で、[Role] が [FCoE Uplink] に変わります。

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。固定モジュールまたは拡張モジュールのユニファイド 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 ポートを設定できます。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。

アプライアンス ポートのユニファイド ストレージ ポートとしての設定

アプライアンス ポートまたは FCoE ストレージ ポートからユニファイド ストレージ ポートを設定できます。未設定のポートからユニファイド ストレージ ポートを設定することもできます。未設定ポートから開始する場合、アプライアンスの設定または FCoE ストレージの設定をポートに割り当てた後に、ユニファイド ストレージ ポートとしてイネーブルにするために別の設定を追加します。

重要 ファブリック インターコネクトがファイバ チャネル スイッチング モードであることを確認します。

手順

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

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

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- **[Fixed Module]**
- **Expansion Module**

ステップ 4 [Ethernet Ports] ノードの下で、すでにアプライアンス ポートとして設定されているポートを選択します。

[Work (作業)] ペインの **[General (全般)]** タブの **[Properties (プロパティ)]** 領域で、**[Role (役割)]** が **[Appliance Storage (アプライアンス ストレージ)]** として表示されます。

ステップ 5 [Actions] 領域で、[Reconfigure] をクリックします。

ステップ 6 ポップアップ メニューから、[Configure as FCoE Storage] ポートを選択します。

ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 Cisco UCS Manager GUI に成功メッセージが表示されます。[Properties] 領域で、[Role] の表示が [Unified Storage] に変わります。

ユニファイド ストレージ ポートの設定解除

ユニファイド接続ポートから両方の設定を解除して削除できます。または、いずれか一方を設定解除し、もう一方をポートに保持することができます。

手順

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

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

ステップ 3 設定を解除するポートのノードを展開します。

ステップ 4 [Ethernet Ports] ノードで、設定を解除するポートを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Unconfigure] をクリックします。次のオプションが表示されます。

- **[Unconfigure FCoE Storage Port]**
- **[Unconfigure Appliance Port]**
- **[Unconfigure both]**

ステップ 7 設定解除オプションのいずれか 1 つを選択します。

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

ステップ 9 Cisco UCS Manager GUI に成功メッセージが表示されます。選択した設定解除オプションに基づいて、[Properties] 領域の [Role] が変更されます。

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

次のいずれかから、ユニファイド アップリンク ポートを設定できます。

- 既存の FCoE アップリンク ポートまたはイーサネット アップリンク ポートから
- 未設定のアップリンク ポートから

固定モジュールまたは拡張モジュールのユニファイド アップリンク ポートを設定できます。

手順

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

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

ステップ 3 設定するポートのノードを展開します。

ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Properties] 領域で、[Role] が [FCoE Uplink] として表示されていることを確認します。

ステップ 7 [Actions] 領域で、[Reconfigure] をクリックします。

ステップ 8 ドロップダウン オプションから、[Configure as Uplink Port] を選択します。

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

ステップ 10 Cisco UCS Manager GUI が成功のメッセージを表示します。

[Properties] 領域で、[Role] が [Unified Uplink] に変わります。

ユニファイド アップリンク ポートの設定解除

ユニファイド アップリンク ポートから両方の設定を解除して削除できます。または、FCoE ポート設定またはイーサネット ポート設定のいずれか一方を設定解除し、もう一方をポートに保持することができます。

手順

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

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

ステップ 3 設定を解除するポートのノードを展開します。

ステップ 4 [Ethernet Ports] ノードで、設定を解除するポートを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Unconfigure] をクリックします。次のオプションのいずれかを選択します。

- **[Unconfigure FCoE Uplink Port]**
- **[Unconfigure Uplink Port]**
- **[Unconfigure both]**

ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 Cisco UCS Manager GUI に成功メッセージが表示されます。選択した設定解除オプションに基づいて、[Properties] 領域の [Role] が変更されます。

ステップ 9 [Save Changes] をクリックします。

ポリシーベースのポート エラー処理

Cisco UCS Manager がアクティブなネットワーク インターフェイス（NI）ポートでエラーを検出し、エラー ディセーブル機能が実装されている場合、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ファブリック インターコネクト ポートを自動的にディセーブルにします。ファブリック インターコネクト 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。

- ファブリック インターコネクト ポートが error-disabled になっているポート、および接続されている NI ポートでエラーが発生したことを通知します。
- このポートは同じ Chassis/FEX に接続されている他のポートの障害になる可能性がなくなります。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。

エラーベース アクションの設定

手順

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

ステップ 2 **[Admin]** > **[All]** > **[Stats Management]** > **[fabric]** > **[Internal LAN]** > **[thr-policy-default]** > **[etherNiErrStats]** の順に展開します。

ステップ 3 デルタ プロパティを選択します。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 ファブリック インターコネクト ポートでエラー ディセーブル状態を実装するには、[Disable FI port when fault is raised] チェックボックスをオンにします。

ステップ 6 自動リカバリをイネーブルにするには、[Enable Auto Recovery] フィールドで、[Enable] を選択します。

ステップ 7 ポートを自動的に再度イネーブルにできるようになるまでの時間を指定するには、[Time (in minutes)] フィールドに必要な値を入力します。

ステップ 8 [Save Changes] をクリックします。

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 シリーズ ファブリック インターコネクトを搭載した各 Cisco UCS ドメイン で、最大 4 個のファイバ チャネル ポート チャン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 チャネルの作成

手順

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

ステップ 2 **[SAN]** > **[SAN Cloud]** の順に展開します。

ステップ 3 ポート チャネルを作成するファブリックのノードを展開します。

ステップ 4 [FC Port Channels] ノードを右クリックし、[Create Port Channel] を選択します。

ステップ 5 [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。

ステップ 6 [Add Ports] パネルで、ポート チャネルの管理速度を指定し、ポート チャネルにポートを追加します。

ステップ 7 [完了（Finish）] をクリックします。

ファイバ チャネル ポート チャネルのイネーブル化

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 **[SAN]** > **[SAN Cloud]** > ***[Fabric]*** > **[FC Port Channels]** の順に展開します。
ステップ 3 イネーブルにするポート チャネルをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Actions] 領域で、[Enable Port Channel] をクリックします。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ファイバ チャネル ポート チャネルのディセーブル化

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 **[SAN]** > **[SAN Cloud]** > ***[Fabric]*** > **[FC Port Channels]** の順に展開します。
ステップ 3 ディセーブルにするポート チャネルをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Actions] 領域の [Disable Port Channel] をクリックします。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ファイバ チャネル ポート チャネルのポートの追加および削除

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 **[SAN]** > **[SAN Cloud]** > ***[Fabric]*** > **[FC Port Channels]** の順に展開します。
ステップ 3 ポートを追加または削除するポート チャネルをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Actions] 領域で、[Add Ports] をクリックします。
ステップ 6 [Add Ports] ダイアログ ボックスで、次のいずれかを実行します。

- ポートを追加するには、**[Ports]** テーブル で 1 つ以上のポートを選択し、**[>>]** ボタン をクリックして **[Ports in the port channel]** テーブル にポートを追加します。

- ポートを削除するには、**[Ports in the port channel]** テーブル で 1 つ以上のポートを選択し、**[<<]** ボタン をクリックしてポート チャネルからポートを削除して **[Ports]** テーブル に追加します。

ステップ 7 [OK] をクリックします。

ファイバ チャネル ポート チャネルのプロパティの変更

（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自動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

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

ステップ 2 **[SAN]** > **[SAN Cloud]** > ***[Fabric]*** > **[FC Port Channels]** の順に展開します。

ステップ 3 変更するポート チャネルをクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [Properties] 領域で、次の 1 つ以上のフィールドの値を変更します。

名前	説明
[Name] フィールド	ポート チャネルに対して指定されたユーザ定義名。この名前には、1 ～ 16 文字の英数字を使用できます。
[VSAN] ドロップダウン リスト	ポート チャネルに関連付けられた VSAN。
[Port Channel Admin Speed] ドロップダウン リスト	ポート チャネルの管理スピード。ここに表示される値は次のとおりです。 • **[1 Gbps]** • **2 Gbps** • **[4 Gbps]** • **[8 Gbps]** • **[auto]**

ステップ 6 [Save Changes] をクリックします。

ファイバ チャネル ポート チャネルの削除

手順

ステップ 1 [Navigation] ペインで [LAN] をクリックします。
ステップ 2 **[SAN]** > **[SAN Cloud]** > ***[Fabric]*** > **[FC Port Channels]** の順に展開します。
ステップ 3 削除するポート チャネルを右クリックし、[Delete] を選択します。
ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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 チャネルの作成

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 **[SAN]** > **[SAN Cloud]** の順に展開します。
ステップ 3 ポート チャネルを作成するファブリックのノードを展開します。
ステップ 4 [FCoE Port Channels] ノードを右クリックし、[Create FCoE Port Channel] を選択します。
ステップ 5 [Create FCoE Port Channel] ウィザードの [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。
ステップ 6 [Create FCoE Port Channel] ウィザードの [Add Ports] パネルで、追加するポートを指定します。

ステップ 7 [完了（Finish）] をクリックします。

FCoE ポート チャネルの削除

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[SAN Cloud]** > **[*Fabric*]** > **[FCoE Port Channels]** の順に展開します。
ステップ 3 削除するポート チャネルを右クリックし、[Delete] を選択します。
ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

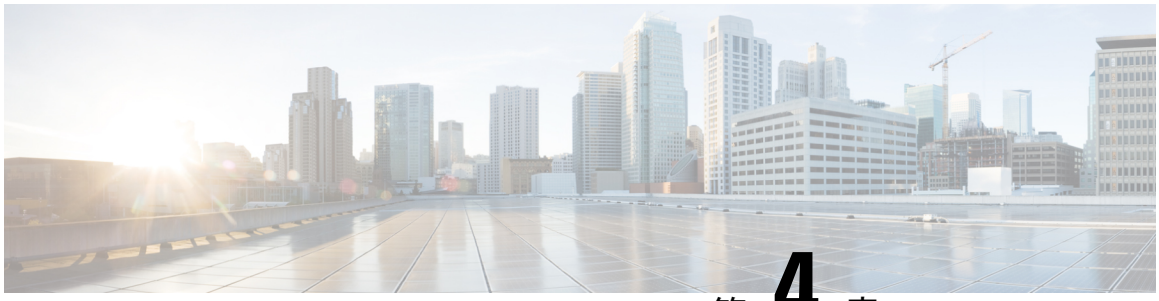
ユニファイド アップリンク ポート チャネル

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。



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 （31 ページ）
- Cisco UCS Manager でのファイバ チャネル ゾーン分割のサポート （32 ページ）
- 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 （34 ページ）
- ファイバ チャネル ゾーン分割の設定 （35 ページ）
- ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ）
- 新しいファイバ チャネル ゾーン プロファイルの作成 （39 ページ）
- ファイバ チャネル ゾーン プロファイルの削除 （42 ページ）
- ファイバ チャネル ユーザ ゾーンの削除 （42 ページ）
- ファイバ チャネル ストレージ接続ポリシー （43 ページ）

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。

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 アップリンク接続を無効にする必要があります。 Cisco UCS は、UCS ローカル ゾーン分割機能の使用と共存するアクティブなファイバ チャネルまたは FCoE アップリンク接続を現在サポートしていません。
- スイッチベースのファイバチャネル 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。

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。	
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。ファイバ チャネル スイッチング モードの設定（157 ページ）を参照してください。
ステップ 4	ファイバ チャネル ゾーンのトラフィック転送に必要なファイバ チャネルと FCoE ストレージ ポートを設定します。	イーサネット ポートの FCoE ストレージ ポートとしての設定 （15 ページ）およびファイバ チャネル ストレージ

	コマンドまたはアクション	目的
		ポートの設定 （16 ページ） を参照してください。
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。	クラスタ設定では、 VSAN を作成することをお勧めします。ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ） を参照してください。
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。ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ） を参照してください。
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。ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ） を参照してください。 • 1 つ以上の vHBA イニシエータ グループを設定します。[Expert] ウィザードを使用したサービスプロファイルの作成 （165 ページ） を参照してください。

ファイバ チャネル ゾーン分割用の VSAN の作成

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID は違っている必要があります。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 と重なる ID が設定されたすべての 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

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

ステップ 2 [SAN] タブの [SAN] ノードをクリックします。

ステップ 3 [Work] ペインの [SAN Uplinks] タブの [SAN Uplinks Manager] リンクをクリックします。

別のウィンドウに [SAN Uplinks Manager] が開きます。

ステップ 4 [SAN Uplinks Manager] で [VSAN] タブをクリックします。

VSANは、どのサブタブでも作成できます。ただし、[All]サブタブを使用すれば、設定済みのすべての VSAN をテーブルに表示できます。

ステップ 5 テーブルの右側のアイコン バーの [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 6 [Create VSAN] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ネットワークに割り当てられている名前。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[FC Zoning] フィールド	Cisco UCS Manager が Cisco UCS ドメインに対してファイバ チャネル ゾーン分割を設定するかどうかを決定するためのオプション ボタンをクリックします。次のいずれかになります。 • **[Disabled]**：アップストリーム スイッチがファイバ チャネル ゾーン分割を処理します。またはファイバチャネルゾーン分割は、Cisco UCS ドメインに対して実行されません。 Cisco UCS Manager はファイバチャネルゾーニングを設定しません。 • **[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 Cisco UCS ドメイン。 （注） Cisco UCS Managerを介してファイバ チャネル ゾーン分割をイネーブルにする場合は、ファイバチャネル ゾーン分割に使用されている VSAN でアップストリーム スイッチを設定しないでください。

名前	説明
[Type] オプション ボタン	オプション ボタンをクリックして、VSAN の設定方法を決定します。次のいずれかになります。 • [Common/Global]：VSAN は、すべての使用可能なファブリック内で同じ VSAN ID にマッピングされます。 • [Fabric A]：VSAN は、ファブリック A にだけ存在する VSAN ID にマッピングされます。 • [Fabric B]：VSAN は、ファブリック B にだけ存在する VSAN ID にマッピングされます。 • [Both Fabrics Configured Differently]：VSAN は、使用可能なファブリックごとに異なる VSAN ID にマッピングされます。このオプションを選択すると、 Cisco UCS Manager GUI に、各ファブリックの**[VSAN ID]** フィールドと **[FCoE VLAN]** フィールドが表示されます。
[VSAN ID] フィールド	ネットワークに割り当てられている固有識別情報。 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。また、FC エンドホスト モードを使用する場合は、3840 ～ 4079 も予約済みの VSAN ID 範囲です。

名前	説明
[FCoE VLAN] フィールド	ファイバ チャネル接続に使用される VLAN に割り当てられた固有識別情報。 VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Managerでは、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。 • 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、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。 • 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 7 [OK] をクリックします。

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

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

ステップ 2 [SAN] タブで、[Storage Cloud] をクリックします。

ステップ 3 [FC Zone Profiles] を右クリックして、[Create FC Zone Profile] を選択します。

ステップ 4 [Create FC Zone Profile] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Name] フィールド	プロファイルの名前。 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。
[Description] フィールド	このフィールドは任意です。ゾーン プロファイルについての簡単な説明を入力します。
[FC Zoning] オプション ボタン	ゾーン プロファイルの必要な状態を選択します。
[FC User Zones]	FC ユーザ ゾーンを作成するには、テーブルの右側にある [+] アイコンをクリックします。[Create FC User Zone] ウィンドウが表示されます。FC ユーザ ゾーンを作成するための詳細について次の手順を続行します。 （注） [+] アイコンが無効の場合、テーブルのエントリをクリックして、有効にします。

ステップ 5 [Create FC User Zone] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Name] フィールド	FC ゾーンの名前です。 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。

フィールド	説明
[Path] オプション ボタン	オプション ボタンをクリックして、VSAN の設定方法を決定します。次のオプションから選択できます。 • [Path A]：ファブリック A にだけ存在する VSAN ID への VSAN パスです。 • [Path B]：ファブリック B にだけ存在する VSAN ID への VSAN パスです。
（注） VSAN を選択するには、次のいずれかを実行します。 • **Select VSAN** • **VSAN の作成** • **[Create Storage VSAN]**	
[Select VSAN] ドロップダウン リスト	ネットワークにすでに存在する VSAN に割り当てられる固有識別子です。 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。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。
[Create VSAN] リンク	新しいウィンドウに新しい VSAN を作成するには、[+]アイコンをクリックします。これにより、ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ） で同じタスクを実行することができます。VSAN を作成したら、ここに戻り、チャネル ゾーン プロファイルの作成を続行できます。
[Create Storage VSAN] リンク	新しいウィンドウに新しいストレージ VSAN を作成するには、[+]アイコンをクリックします。これにより、ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ） で同じタスクを実行することができます。VSAN を作成したら、ここに戻り、チャネル ゾーン プロファイルの作成を続行できます。

フィールド	説明
[Member WWPNs]	ワールドワイドポート名（WWPN）を作成するには、テーブルの右側にある [+] アイコンをクリックします。[Create FC Zone Member] ウィンドウが表示されます。 このゾーンの WWPN を入力します。

ステップ 6 [Create FC Zone Member] ウィンドウの [OK] をクリックします。

ステップ 7 [Create FC User Zone] ウィンドウの [OK] をクリックします。

ステップ 8 [Create FC Zone Profile] ウィンドウの [OK] をクリックします。

新しく作成されたファイバ チャネル ゾーン プロファイルは、[FC Zone Profiles] の下に表示されます。

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

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

ステップ 2 [SAN] タブで、[Storage Cloud] をクリックします。

ステップ 3 [FC Zone Profiles] をクリックします。

ステップ 4 [Work] ペインで、削除するゾーン プロファイルの名前を右クリックします。

ステップ 5 [Delete] を選択し、確認のために [Yes] をクリックします。

ゾーン プロファイルは、システムから削除されます。

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

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

ステップ 2 [SAN] タブで、[Storage Cloud] をクリックします。

ステップ 3 [FC Zone Profiles] をクリックします。
ステップ 4 [Work] ペインで、ゾーン プロファイルを選択します。
ステップ 5 FC ユーザ ゾーンに移動します。
ステップ 6 削除するユーザ ゾーンの名前を右クリックします。
ステップ 7 [Delete] を選択し、確認のために [Yes] をクリックします。

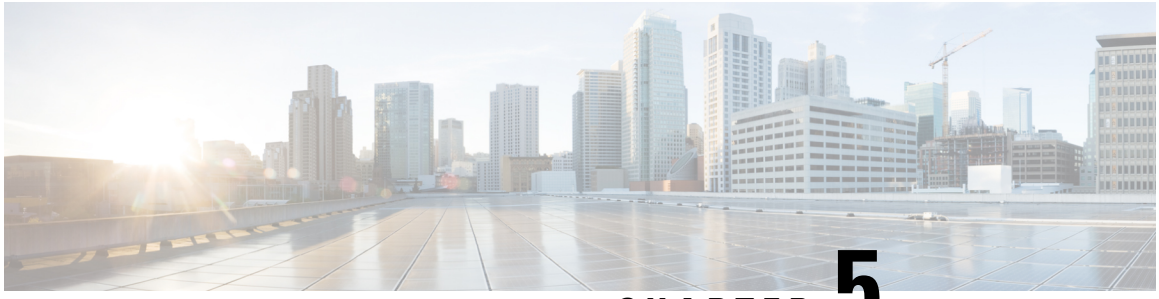
ユーザ ゾーンがシステムから削除されます。

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の削除

手順

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



CHAPTER 5

ネームド VSAN

- ネームド VSAN, on page 45
- 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 （46 ページ）
- VSAN に関するガイドラインおよび推奨事項 （46 ページ）
- ネームド VSAN の作成, on page 48
- ストレージ VSAN の作成 （49 ページ）
- ネームド VSAN の削除, on page 50
- ストレージ VSAN の FCoE VLAN の VLAN ID の変更 （51 ページ）
- ファイバ チャネル アップリンク トランキングのイネーブル化 （51 ページ）
- ファイバ チャネル アップリンク トランキングのディセーブル化 （52 ページ）

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。

この範囲の VSAN は、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は動作しません。 Cisco UCS Manager はその VSAN を エラーとしてマークし、障害を生成します。

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 は違っている必要があります。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 と重なる ID が設定されたすべての 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、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。
- 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。

ネームド VSAN の作成

Note SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID は違っている必要があります。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 と重なる ID が設定されたすべての 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

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

ステップ 2 **[SAN]** > **[SAN Cloud]** の順に展開します。

ステップ 3 [Work] ペインで、[VSANs] タブをクリックします。

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create VSAN] ダイアログボックスで、必須情報を入力します。

ステップ 6 [OK] をクリックします。

Cisco UCS Manager GUI で、次の [VSANs] ノードの 1 つに VSAN が追加されます。

- 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ストレージ VSAN の場合は、**[SAN Cloud]** > **[VSANs]** ノード。
- 1 つのファブリック インターコネクトのみにアクセス可能な VSAN の場合は、**[SAN Cloud]** > **[*Fabric_Name*]** > **[VSANs]** ノード。

ストレージ VSAN の作成

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID は違っている必要があります。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 と重なる ID が設定されたすべての 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

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Storage Cloud]** を展開します。

ステップ 3 [Work] ペインで、[VSANs] タブをクリックします。

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create VSAN] ダイアログボックスで、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

Cisco UCS Manager GUI で、次の [VSANs] ノードの 1 つに VSAN が追加されます。

- 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ストレージ VSAN の場合は、**[Storage Cloud]** > **[VSANs]** ノード
- 1 つのファブリック インターコネクトのみにアクセス可能な VSAN の場合は、**[Storage Cloud]** > **[*Fabric_Name*]** > **[VSANs]** ノード

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

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

ステップ 2 [SAN] タブで、[SAN] ノードをクリックします。

ステップ 3 [Work] ペインで、[VSANs] タブをクリックします。

ステップ 4 削除する VSAN のタイプに応じて、次のサブタブのいずれかをクリックします。

サブタブ	説明
すべて	Cisco UCS ドメインのすべての VSAN を表示します。
Dual Mode	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 VSAN を表示します。
[Switch A]	ファブリック インターコネクト A だけにアクセスできる VSAN を表示します。
[Switch B]	ファブリック インターコネクト B だけにアクセスできる VSAN を表示します。

ステップ 5 テーブルで、削除する VSAN をクリックします。

Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 6 強調表示された VSAN を右クリックし、[Delete] を選択します。

ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ストレージ VSAN の FCoE VLAN の VLAN ID の変更

注意 ストレージ VSAN の FCoE VLAN の VLAN ID を変更すると、トラフィックが短時間中断します。SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID は違っている必要があります。VSAN 内の FCoE 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 NIC 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します。FCoE VLAN ID と重なる ID が設定されたすべての VLAN 上でイーサネット トラフィックがドロップされます。

グローバル ポリシーでデフォルト VSAN または設定済み VSAN の FCoE VLAN を変更すると、ストレージの切断や完全シャットダウンが発生する可能性があります。

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[Storage Cloud]** > **[VSANs]** を展開します。
ステップ 3 FCoE VLAN ID を変更する VSAN を選択します。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [FCoE VLAN] フィールドで、目的の VLAN ID を入力します。
ステップ 6 [Save Changes] をクリックします。

ファイバ チャネル アップリンク トランキングのイネーブル化

（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 トランキングをイネーブルにすると、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。

手順

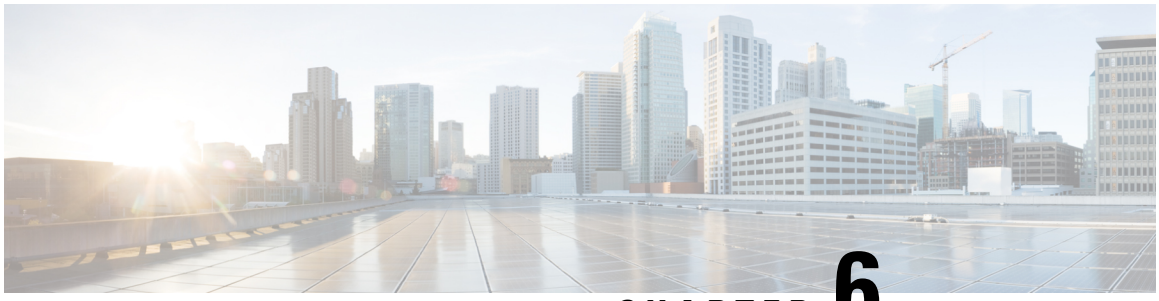
ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 **[SAN]** > **[SAN Cloud]** の順に展開します。
ステップ 3 FC アップリンク トランキングをイネーブルにするファブリックのノードをクリックします。

ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Actions] 領域で、[Enable FC Uplink Trunking] をクリックします。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ファイバチャネルアップリンクトランキングのディセーブル化

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 **[SAN]** > **[SAN Cloud]** の順に展開します。
ステップ 3 ファイバ チャネル アップリンク トランキングをディセーブルにするファブリックのノードをクリックします。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Actions] 領域の [Disable FC Uplink Trunking] をクリックします。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。



CHAPTER 6

SAN ピン グループ

• SAN ピン グループ, on page 53

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 グループの作成

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

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

ステップ 2 [SAN] タブで、**[SAN]** > **[SAN Cloud]** を展開します。

ステップ 3 [SAN Pin Groups] を右クリックし、[Create SAN Pin Group] を選択します。

ステップ 4 ピン グループの一意の名前および説明を入力します。

ステップ 5 ファブリック インターコネクト A のトラフィックをピン接続するには、[Targets] 領域で次の手順を実行します。

a) [Fabric A] チェックボックスをオンにします。

b) [Interface] フィールドでドロップダウン矢印をクリックし、ツリー形式のブラウザを移動して、ピン グループに関連付けるアップリンク ファイバ チャネル ポートを選択します。

ステップ 6 ファブリック インターコネクト B のトラフィックをピン接続するには、[Targets] 領域で次の手順を実行します。

a) [Fabric B] チェックボックスをオンにします。

b) [Interface] フィールドでドロップダウン矢印をクリックし、ツリー形式のブラウザを移動して、ピン グループに関連付けるアップリンク ファイバ チャネル ポートを選択します。

ステップ 7 [OK] をクリックします。

What to do next

ピン グループは、vHBA テンプレートにインクルードします。

SAN ピン グループの削除

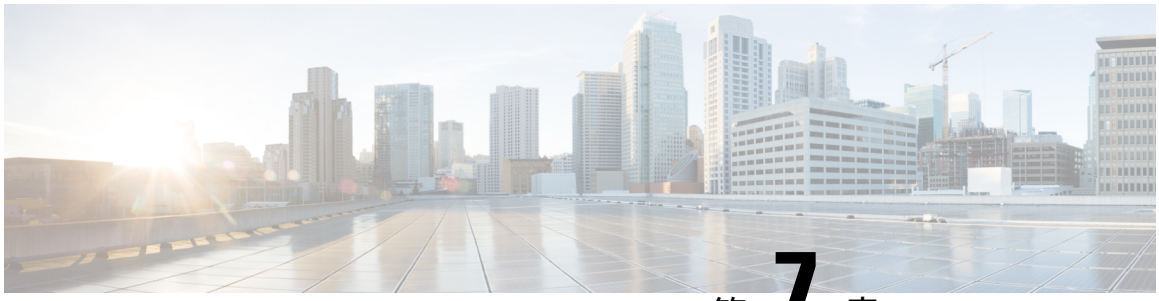
Procedure

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

ステップ 2 [SAN] タブで、**[SAN]** > **[SAN Cloud]** > **[SAN Pin Groups]** を展開します。

ステップ 3 削除する SAN ピン グループを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。



第 7 章

FC ID の割り当て

• ファイバ チャネル ID （55 ページ）

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。

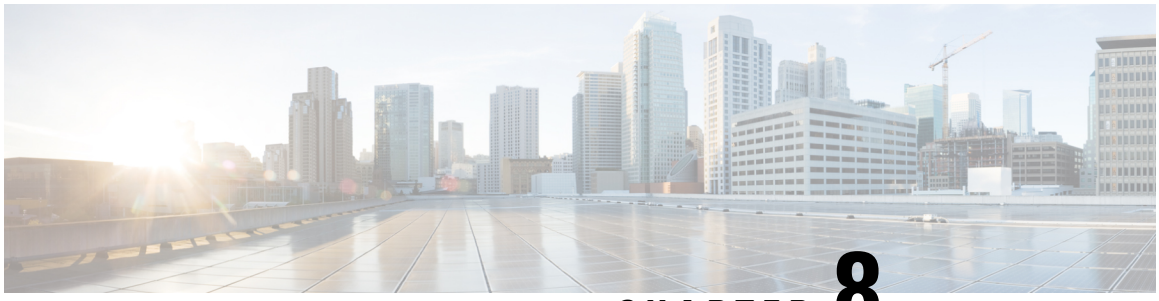
WWNN プールは、Cisco UCS ドメインに対する 1 つの大きなプールとして作成されます。Cisco UCS Manager の [SAN] タブでは、デフォルト プールを使用できます。ただし、その UCS ドメインではカスタムの WWNN プールを作成することを推奨します。

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



CHAPTER 8

WWN プール

- WWN プール, on page 57
- WWPN プール, on page 63
- WWxN プール, on page 68

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 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。

WWNN 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 の WWN プレフィックスを使用することをお勧めします。

Procedure

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** を展開します。

ステップ 3 プールを作成する組織のノードを展開します。

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

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

ステップ 5 [Create WWNN Pool] ウィザードの [Define Name and Description] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ワールド ワイド ノード名プールの名前。 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。
[Description] フィールド	プールの説明。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Assignment Order] フィールド	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。 • **[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 6 [Next] をクリックします。

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

ステップ 8 [Create WWN Block] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、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つのポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 9 [OK] をクリックします。

ステップ 10 [完了（Finish）] をクリックします。

What to do next

WWNN プールはサービス プロファイルとテンプレートに含めます。

WWNN プールへの WWN ブロックの追加

重要 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 の WWN プレフィックスを使用することをお勧めします。

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [WWNN Pools] ノードを展開します。

ステップ 4 WWN ブロックを追加する WWNN プールを右クリックして、[Create WWN Block] を選択します。

ステップ 5 [Create WWN Block] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、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 つのポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWNN プールからの WWN ブロックの削除

プールからアドレス ブロックを削除すると、 はそのブロックの中の vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたブロックのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** > **[WWNN Pools]** > **[*WWNN_Pool_Name*]** を展開します。

ステップ 3 削除する WWN ブロックを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

WWNN プールへの WWNN イニシエータの追加

重要 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 の WWN プレフィックスを使用することをお勧めします。

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [WWNN Pools] ノードを展開します。

ステップ 4 WWNN イニシエータを追加する WWNN プールを右クリックして、**[Create WWNN Initiator (WWNN イニシエータの作成)]** を選択します。

ステップ 5 [Create WWNN Initiator] ダイアログボックスで、次のフィールドに情報を入力します。

名前	説明
[World Wide Name] フィールド	WWN。
[Name] フィールド	WWNN イニシエータの名前。 この名前には、1～16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	WWNN イニシエータのユーザ定義による説明。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 6 [OK] をクリックします。

WWPN プールからの WWPN イニシエータの削除

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。
ステップ 3 [WWPN Pools] ノードを展開します。
ステップ 4 WWPN イニシエータを削除する WWPN プールを選択します。
ステップ 5 [Work] ペインで [Initiators] タブをクリックします。
ステップ 6 削除するイニシエータを右クリックし、[Delete] を選択します。
ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

WWNN プールの削除

プールを削除した場合、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ブロックは、次のいずれかが起きるまで、割り当てられたvNICまたは vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合

- アドレスが割り当てられた vNIC または vHBA が削除された場合
- vNIC または vHBA が異なるプールに割り当てられた場合

Procedure

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。
ステップ 3 [WWNN Pools] ノードを展開します。
ステップ 4 削除する WWNN プールを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

WWPN プール

WWPN プールの作成

重要 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 の WWN プレフィックスを使用することをお勧めします。

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** を展開します。
ステップ 3 プールを作成する組織のノードを展開します。

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

ステップ 4 [WWPN Pools] を右クリックし、[Create WWPN Pool] を選択します。
ステップ 5 [Create WWPN Pool] ウィザードの [Define Name and Description] ページで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ワールド ワイド ポート名（WWPN）プールの名前。 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。
[Description] フィールド	プールの説明。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Assignment Order] フィールド	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。 • **[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 6 [Next] をクリックします。

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

ステップ 8 [Create WWN Block] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、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つのポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 9 [OK] をクリックします。

ステップ 10 [完了（Finish）] をクリックします。

次のタスク

WWPN プールは、vHBA テンプレートにインクルードします。

WWPN プールへの WWN ブロックの追加

重要 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 の WWN プレフィックスを使用することをお勧めします。

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [WWPN Pools] ノードを展開します。

ステップ 4 WWN ブロックを追加する WWPN プールを右クリックして、[Create WWN Block] を選択します。

ステップ 5 [Create WWN Block] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、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 つのポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWPN プールからの WWN ブロックの削除

プールからアドレス ブロックを削除すると、 はそのブロックの中の vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたブロックのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

- 関連付けられたサービス プロファイルが削除された場合

- アドレスが割り当てられた vNIC または vHBA が削除された場合
- vNIC または vHBA が異なるプールに割り当てられた場合

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** > **[WWPN Pools]** > **[*WWPN_Pool_Name*]** を展開します。

ステップ 3 削除する WWN ブロックを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

WWPN プールへの WWPN イニシエータの追加

重要 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 の WWN プレフィックスを使用することをお勧めします。

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [WWPN Pools] ノードを展開します。

ステップ 4 WWPN イニシエータを追加する WWPN プールを右クリックして、[Create WWPN Initiator] を選択します。

ステップ 5 [Create WWPN Initiator] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[World Wide Name] フィールド	WWN。

名前	説明
[Name] フィールド	WWPN イニシエータの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	WWPN イニシエータのユーザ定義による説明。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 6 SAN ブート ターゲットを追加する場合は、[Boot Target] 領域を展開し、次のフィールドに値を入力します。

名前	説明
[Boot Target WWPN] フィールド	ブート イメージの場所に対応する WWPN。
[Boot Target LUN] フィールド	ブート イメージの場所に対応する LUN。

ステップ 7 [OK] をクリックします。

WWPN プールからの WWPN イニシエータの削除

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。
ステップ 3 [WWPN Pools] ノードを展開します。
ステップ 4 WWPN イニシエータを削除する WWPN プールを選択します。
ステップ 5 [Work] ペインで [Initiators] タブをクリックします。
ステップ 6 削除するイニシエータを右クリックし、[Delete] を選択します。
ステップ 7 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

WWPN プールの削除

プールを削除した場合、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ブロックは、次のいずれかが起きるまで、割り当てられたvNICまたは vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。
ステップ 3 [WWPN Pools] ノードを展開します。
ステップ 4 削除する WWPN プールを右クリックし、[Delete] を選択します。
ステップ 5 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

WWxN プール

WWxN プールの作成

重要 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 の WWN プレフィックスを使用することをお勧めします。

手順

ステップ 1 [Navigation] ペインで [SAN] をクリックします。
ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** を展開します。

ステップ 3 プールを作成する組織のノードを展開します。

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

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

ステップ 5 [Create WWxN Pool] ウィザードの [Define Name and Description] ページで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ワールド ワイド ポート名（WWPN）プールの名前。 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。
[Description] フィールド	プールの説明。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Max Ports per Node] フィールド	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。 オブジェクトの保存後は、この値を変更できません。
[Assignment Order] フィールド	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。 • **[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 6 [Next] をクリックします。

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

ステップ 8 [Create WWN Block] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。

名前	説明
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、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 つのポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 9 [OK] をクリックします。

ステップ 10 [完了（Finish）] をクリックします。

次のタスク

WWxN プールはサービス プロファイルとテンプレートに含めます。

WWxN プールへの WWN ブロックの追加

重要 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 の WWN プレフィックスを使用することをお勧めします。

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [WWxN Pools] ノードを展開します。

ステップ 4 WWN ブロックを追加する WWxN プールを右クリックして、[Create WWN Block] を選択します。

ステップ 5 [Create WWN Block] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。

名前	説明
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、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つのポートがある場合、プール サイズは 8 の倍数である必要があります。ノードごとに 63 個のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWxN プールからの WWN ブロックの削除

プールからアドレス ブロックを削除すると、 はそのブロックの中の vNIC または vHBA に割り当てられたアドレスを再割り当てしません。削除されたブロックのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** > **[WWxN Pools]** > **[*WWxN_Pool_Name*]** を展開します。

ステップ 3 削除する WWN ブロックを右クリックし、[Delete] を選択します。

ステップ 4 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

WWxN プールの削除

プールを削除した場合、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ブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

Procedure

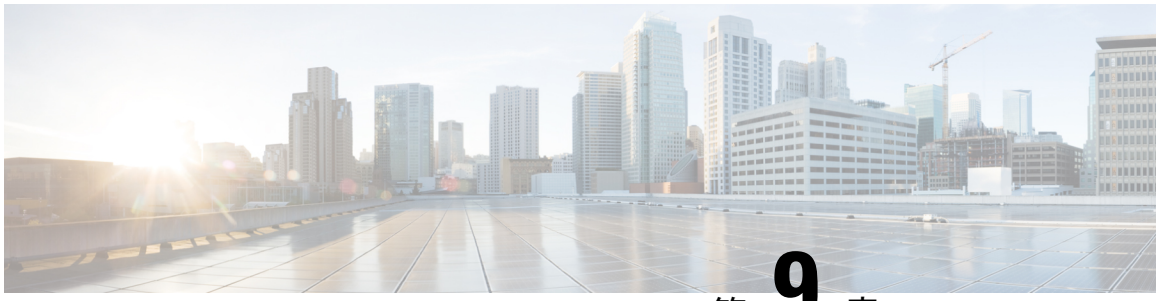
ステップ 1 [Navigation] ペインで [SAN] をクリックします。

ステップ 2 [SAN] タブで、**[SAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [WWxN Pools] ノードを展開します。

ステップ 4 削除する WWxN プールを右クリックし、[Delete] を選択します。

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



第 9 章

ストレージ関連ポリシー

- vHBA テンプレートについて （73 ページ）
- ファイバ チャネル アダプタ ポリシー （77 ページ）
- デフォルトの vHBA 動作ポリシーについて （86 ページ）
- SAN 接続ポリシー （87 ページ）

vHBA テンプレートについて

vHBA テンプレート

このテンプレートは、サーバ上の vHBA による SAN への接続方法を定義するポリシーです。これは、vHBA SAN 接続テンプレートとも呼ばれます。

このポリシーを有効にするには、このポリシーをサービス プロファイルに含める必要があります。

vHBA テンプレートの作成

始める前に

このポリシーは、次のリソースの 1 つ以上がシステムにすでに存在していることを前提にしています。

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

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

ステップ 4 [vHBA Templates] ノードを右クリックし、[Create vHBA Template] を選択します。

ステップ 5 [Create vHBA Template] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
Name field	The name of the virtual HBA template. この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
Description field	A user-defined description of the template. 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
Fabric ID field	The name of the fabric interconnect that vHBAs created with this template are associated with.
[Select VSAN] ドロップダウンリスト	このテンプレートから作成された vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
Template Type field	This can be one of the following: • **Initial Template**—vHBAs created from this template are not updated if the template changes. • **Updating Template**—vHBAs created from this template are updated if the template changes.
Max Data Field Size field	The maximum size of the Fibre Channel frame payload bytes that the vHBA supports. Enter an integer between 256 and 2112. The default is 2048.

名前	説明
WWPN Pool drop-down list	The WWPN pool that a vHBA created from this template uses to derive its WWPN address.
QoS Policy drop-down list	The QoS policy that is associated with vHBAs created from this template.
Pin Group drop-down list	The SAN pin group that is associated with vHBAs created from this template.
Stats Threshold Policy drop-down list	The statistics collection policy that is associated with vHBAs created from this template.

ステップ 6 [OK] をクリックします。

次のタスク

vHBA テンプレートはサービス プロファイルにインクルードします。

vHBA テンプレートへの vHBA のバインディング

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

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

手順

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

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

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

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

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

ステップ 5 テンプレートにバインドする vHBA をクリックします。

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

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

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

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

b) [OK] をクリックします。

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

vHBA テンプレートからの vHBA のバインド解除

手順

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

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

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

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

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

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

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

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

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

vHBA テンプレートの削除

手順

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

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

ステップ 3 [vHBA Templates] ノードを展開します。

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

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

ファイバ チャネル アダプタ ポリシー

イーサネットおよびファイバ チャネル アダプタ ポリシー

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

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

Note ファイバ チャネル アダプタ ポリシーの場合は、 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 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。 では、より大きな最大 LUN の値をサポートしています。
- 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。 では、この値をミリ秒で設定します。したがって、 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。 では、任意のサイズの値を設定できます。したがって、 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。
- 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。

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

ファイバ チャネル アダプタ ポリシーの作成

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

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。
ステップ 2 **[Servers]** > **[Policies]** の順に展開します。
ステップ 3 ポリシーを作成する組織のノードを展開します。

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

ステップ 4 **[Adapter Policies]** を右クリックし、**[Create Fibre Channel Adapter Policy]** を選択します。
ステップ 5 次のフィールドに、ポリシーの名前および説明を入力します。

表 *2:*

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーを使用する場所とタイミングについての情報を含めることを推奨します。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

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

名前	説明
[Transmit Queues] フィールド	割り当てる送信キュー リソースの数。 この値は変更できません。
[Ring Size] フィールド	各送信キュー内の記述子の数。このパラメータは、汎用サービスの Extended Link Services（ELS）および Common Transport（CT）ファイバ チャネル フレームに適用されます。アダプタのパフォーマンスには影響しません。 64 ～ 128 の整数を入力します。デフォルトは 64 です。
[Receive Queues] フィールド	割り当てる受信キュー リソースの数。 この値は変更できません。
[Ring Size] フィールド	各受信キュー内の記述子の数。このパラメータは、汎用サービスの Extended Link Services（ELS）および Common Transport（CT）ファイバ チャネル フレームに適用されます。アダプタのパフォーマンスには影響しません。 64 ～ 2048 の整数を入力します。デフォルトは 64 です。
[I/O Queues] フィールド	システムで割り当てる SCSI IO キュー リソースの数。 1 ～ 16 の整数を入力します。デフォルトは 16 です。

名前	説明
[Ring Size] フィールド	各 SCSI I/O キュー内の記述子の数。 64 ～ 512 の整数を入力します。デフォルトは 512 です。 （注） 記述子の数はアダプタのパフォーマンスに影響を与える可能性があるため、デフォルト値を変更しないことを推奨します。

ステップ 7 （任意） [Options] 領域で、次の値を調整します。

名前	説明
[FCP Error Recovery] フィールド	テープデバイスによるシーケンス レベル エラーの修復に FCP Sequence Level Error Recovery（FC-TAPE）プロトコルを使用するかどうかを選択します。これにより、VIC ファームウェアの Read Exchange Concise（REC）および Sequence Retransmission Request（SRR）機能を有効または無効にできます。次のいずれかになります。 • [Disabled]：デフォルトです。 • [Enabled]：システムが 1 つ以上のテープ ドライブ ライブラリに接続している場合は、このオプションを選択します。 （注） このパラメータは、Virtual Interface Card (VIC) アダプタを搭載したサーバにのみ適用されます。
[Flogi Retries] フィールド	システムがファブリックへのログインを最初に失敗してから再試行する回数。 任意の整数を入力します。システムが無限に試行し続けるように指定するには、このフィールドに「**infinite**」と入力します。ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタまたはコンバージド ネットワーク アダプタを搭載したサーバにのみ適用されます。

名前	説明
[Flogi Timeout (ms)] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1000 ～ 255000 の整数を入力します。デフォルト値は 4,000 です。ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタまたは統合型ネットワーク アダプタを搭載したサーバにのみ適用されます。 ブート vHBA で Flogi タイムアウト値を 20 秒以上に設定すると、アダプタが最初の Flogi に対する承認を受信しなかった場合に SAN ブート障害が発生する可能性があります。ブート可能な vHBA の場合、推奨されるタイムアウト値は 5 秒以下です。
[Plogi Retries] フィールド	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。デフォルト値は 8 です。ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。
[Plogi Timeout (ms)] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1000 ～ 255000 の整数を入力します。デフォルト値は 20,000 です。ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 SAN から Windows OS をブートするために使用される HBA の場合、このフィールドの推奨値は 4,000 ミリ秒です。 （注） このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。 ブート vHBA で Plogi タイムアウト値を 20 秒以上に設定すると、アダプタが最初の Plogi に対する承認を受信しなかった場合に SAN ブート障害が発生する可能性があります。ブート可能な vHBA の場合、推奨されるタイムアウト値は 5 秒以下です。

名前	説明
[Port Down Timeout (ms)] フィールド	リモート ファイバ チャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。このパラメータはホスト マルチパス ドライバにとって重要であり、エラー処理に使用される主要指標の 1 つとなります。 0 ～ 240000 の整数を入力します。デフォルト値は 30,000 です。ESX を実行している VIC アダプタ搭載のサーバの場合、推奨値は 10,000 です。 SAN から Windows OS をブートするために使用されるポートがあるサーバの場合、このフィールドの推奨値は 5,000 ミリ秒です。 ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。
IO リトライ タイムアウト（秒）	保留中のコマンドを破棄して同じ IO を再送信するまでに FC アダプタが待機する秒数です。これは、ネットワーク デバイスが、指定された時間内の I/O 要求に応答しないと発生します。 0 ～ 59 の整数を入力します。デフォルトの IO リトライ タイムアウトは 5 秒です。
[Port Down IO Retry] フィールド	ポートが使用不可能であるとシステムが判断する前に、そのポートへの IO 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。デフォルト値は 8 です。ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、Windows を実行している VIC アダプタ搭載のサーバにのみ適用されます。
[Link Down Timeout (ms)] フィールド	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0 ～ 240000 の整数を入力します。デフォルト値は 30,000 です。ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、Windows を実行している VIC アダプタ搭載のサーバにのみ適用されます。

名前	説明
[IO Throttle Count] フィールド	vHBA 内で同時に保留可能なデータまたは制御 I/O 操作の最大数。この値を超えると、保留中の I/O 操作の数が減り、追加の操作が処理できるようになるまで、キューで I/O 操作が待機します。 （注） このパラメータは、LUN キューの長さと同じではありません。LUN キューの長さは、サーバにインストールされている OS に基づいて、Cisco UCS Manager により管理されます。 256 ～ 1024 の整数を入力します。デフォルトは 256 です。ストレージ アレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。
[Max LUNs Per Target] フィールド	ファイバ チャネル ドライバがエクスポートまたは表示する LUN の最大数。LUN の最大数は、通常、サーバで実行されている OS により管理されます。 1 ～ 1024 の整数を入力します。デフォルト値は 256 です。ESX または Linux を実行しているサーバの場合、推奨値は 1024 です。 オペレーティングシステムのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） • このパラメータは、VIC アダプタまたはネットワーク アダプタを搭載したサーバにのみ適用されます。
[LUN Queue Depth] フィールド	HBA が 1 回の伝送で送受信できる LUN ごとのコマンドの数です。 1 ～ 254 の整数を入力します。デフォルトの LUN キュー デプスは 20 です。

名前	説明
[Interrupt Mode] オプション ボタン	ドライバからオペレーティング システムに割り込みを送信する方法。次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。サーバのオペレーティングシステムがこれに対応している場合には、このオプションを選択することをお勧めします。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。 （注） このパラメータは、VIC アダプタを搭載しているサーバや、Window 以外の OS を実行しているネットワーク アダプタ搭載のサーバにのみ適用されます。Windows OS では、このパラメータは無視されます。

ステップ 8 [OK] をクリックします。

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

ファイバ チャネル アダプタ ポリシーの削除

手順

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

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

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

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

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

デフォルトの vHBA 動作ポリシーについて

デフォルトの vHBA 動作ポリシー

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

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

- [None]： 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、 はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vHBA を作成します。

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

デフォルトの vHBA 動作ポリシーの設定

手順

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

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

ステップ 3 [root] ノードを展開します。

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

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

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

- [None]： 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、 はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて必要な vHBA を作成します。

ステップ 6 [Save Changes] をクリックします。

SAN 接続ポリシー

LAN および SAN 接続ポリシーについて

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

（注） 接続ポリシーはサービスプロファイルおよびサービスプロファイルテンプレートに含められ、複数のサーバの設定に使用される可能性があるため、接続ポリシーでは静的 ID を使用しないことをお勧めします。

LAN および SAN の接続ポリシーに必要な権限

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

接続ポリシーの作成に必要な権限

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

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

接続ポリシーをサービス プロファイルに追加するために必要な権限

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

サービス プロファイルと接続ポリシー間の相互作用

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

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

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

SAN 接続ポリシーの作成

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

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

ステップ 5 [Create SAN Connectivity Policy] ダイアログボックスで、名前と任意の説明を入力します。

ステップ 6 **[World Wide Node Name]** 領域の**[WWNN Assignment]** ドロップダウン リストから次のいずれかを選択します。

- デフォルトの WWN プールを使用するには、 を選択します。
- [Manual Using OUI] に一覧表示されるオプションのいずれかを選択し、[World Wide Node Name] フィールドに WWN を入力します。

  WWNN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 [here] リンクをクリックして、指定した WWNN が使用可能であることを確認できます。
- 指定したプールから WWN を割り当てるには、リストから WWN プール名を選択します。各プール名の後には、プール内で利用可能な WWN の数および WWN の合計数を示す、括弧に囲まれた 2 つの数字が表示されます。

ステップ 7 [vHBAs] テーブルで、[Add] をクリックします。

ステップ 8 [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。

ステップ 9 [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。

この領域から VSAN または SAN ピン グループを作成することもできます。

ステップ 10 [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。

ステップ 11 [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。

この領域からファイバ チャネル アダプタ ポリシーまたは QoS ポリシーを作成することもできます。

ステップ 12 ポリシーに必要なすべての vHBA を作成したら、[OK] をクリックします。

次のタスク

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

SAN 接続ポリシー用の vHBA の作成

手順

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Policies]** > **[*Organization_Name*]** > **[San Connectivity Policies]** の順に展開します。

ステップ 3 vHBA を作成するポリシーを選択します。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 テーブル アイコン バーの [+] ボタンをクリックします。

ステップ 6 [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。

ステップ 7 [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。

この領域から VSAN または SAN ピン グループを作成することもできます。

ステップ 8 [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。

ステップ 9 [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。

この領域からファイバ チャネル アダプタ ポリシーまたは QoS ポリシーを作成することもできます。

ステップ 10 [Save Changes] をクリックします。

SAN 接続ポリシーからの vHBA の削除

手順

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

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

ステップ 3 vHBA を削除するポリシーを選択します。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [vHBAs] テーブルで、次の手順を実行します。

a) 削除する vHBA をクリックします。

b) アイコン バーで [Delete] をクリックします。

ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

SAN 接続ポリシー用のイニシエータ グループの作成

手順

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

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

ステップ 3 イニシエータ グループを作成するポリシーを選択します。

ステップ 4 [Work] ペインで、[vHBA Initiator Groups] タブをクリックします。

ステップ 5 テーブル アイコン バーの [+] ボタンをクリックします。

ステップ 6 [Create vHBA Initiator Group] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	vHBA イニシエータ グループの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。

名前	説明
[Description] フィールド	グループの説明。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Select vHBA Initiators] テーブル	使用する各 vHBA に対応する、[Select] カラムのチェックボックスをオンにします。
[Storage Connection Policy] ドロップダウン リスト	この vHBA イニシエータ グループに関連付けられているストレージ接続ポリシー項目 • 既存のストレージ接続ポリシーを使用して、ドロップダウン リストからそのポリシーを選択します。Cisco UCS Manager GUI では、 **[Global Storage Connection Policy]** 領域に、ポリシーとその FC ターゲット エンドポイントに関する情報が表示されます。 グローバルに利用できる新しいストレージ接続ポリシーを作成し、[Create Storage Connection Policy] リンクをクリックします。 • この vHBA イニシエータ グループでのみ利用できるローカル ストレージ接続ポリシーを作成し、[Specific Storage Connection Policy] オプションを選択します。Cisco UCS Manager GUI に表示される**[Specific Storage Connection Policy]** 領域を使って、ローカル ストレージ接続ポリシーを設定できます。
[Create Storage Connection Policy] リンク	すべてのサービス プロファイルとサービス プロファイル テンプレートで使用可能な新しいストレージ接続ポリシーを作成するには、このリンクをクリックします。

ステップ 7 [OK] をクリックします。

SAN 接続ポリシーからのイニシエータ グループの削除

手順

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

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

ステップ 3 イニシエータ グループを削除するポリシーを選択します。

ステップ 4 [Work] ペインで、[vHBA Initiator Groups] タブをクリックします。

ステップ 5 テーブルで、次の手順を実行します

a) 削除するイニシエータ グループをクリックします。

b) アイコン バーで [Delete] をクリックします。

ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

SAN 接続ポリシーの削除

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

手順

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

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

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

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

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

第 10 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 （93 ページ）
- コントローラとディスクのセキュリティ フラグ （94 ページ）
- ローカル セキュリティ ポリシーの管理 （94 ページ）
- KMIP クライアント証明書ポリシー （96 ページ）
- リモート セキュリティ ポリシーの管理 （99 ページ）
- ディスクのセキュリティのイネーブル化とディセーブル化 （101 ページ）
- コントローラのセキュリティのディセーブル化 （102 ページ）
- ロックされたディスクのロックの解除 （102 ページ）
- セキュア外部設定ディスクの消去 （103 ページ）

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）を使用して、キーをリモートから設定できます。この方法で、ローカル管理でのキーの保管と取得に関する問題に対処します。

SED の暗号化と復号化は、ハードウェアを通じて実行されます。したがって、全体的なシステム パフォーマンスに影響しません。SED は瞬時に暗号を消去することで、ディスクの使用停止や再展開のコストを削減します。メディア暗号化キーを変更することで、暗号消去が実行されます。ディスクのメディア暗号化キーを変更すると、そのディスク上のデータは復号化でき

ず、すぐに使用できない状態になります。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。

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。

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

始める前に

新しいストレージ プロファイルまたは既存のストレージ プロファイルにローカル ポリシーを作成できます。

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 ポリシーを作成するストレージ プロファイルを選択します。

ステップ 3 **[Security Policy]** タブをクリックし、次に **[Create Security Policy]** をクリックするかまたは **[storage profile]** を右クリックして [Create Security Policy] を選択します。

ステップ 4 [Local Policy] オプションをクリックします。

a) [Key] に入力します。

キーには 32 個の英数字を使用する必要があります。

b) [OK] をクリックします。

次のタスク

こうして作成されたキーは、そのサーバのストレージプロファイルに関連付けられ、ストレージ コントローラの下に展開されます。これを確認するには、**[Server ID]** > **Inventory]** > **[Storage]** > **[Controller]** に進み、SAS ストレージ コントローラを選択します。**[General]** タブに移動し、**[Security]** フィールドが **[drive security enable]** として表示されているかどうかを確認します。

ローカル セキュリティ ポリシーの変更

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 ポリシーを作成したストレージ プロファイルを選択します。

ステップ 3 [Security Policy] タブをクリックします。

ステップ 4 （任意） ローカル ポリシーのキーを変更するには、[Local Policy] 領域で次の手順を実行します。

a) [Key] フィールドにデータベースの新しいセキュリティ キーを入力します。

b) [Deployed Key] フィールドにデータベースの現在のセキュリティ キーを入力します。

ステップ 5 （任意）セキュリティ ポリシーを **ローカル ポリシー**から**リモート ポリシー**に変更するには、次の手順を実行します。

a) [Remote Policy] オプションをクリックします。

b) [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。

c) （任意） [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。

d) （任意） [Deployed Key] フィールドにデータベースの現在のセキュリティ キーを入力します。

e) （任意） [Port] フィールドに、サーバのポート番号を入力します。

f) [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。
g) （任意） [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。

ステップ 6 [Save Changes] をクリックします。

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

グローバル KMIP クライアント証明書ポリシーを作成することができます。

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

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

ステップ 2 [Work] ペインの [Policies] タブをクリックします。

ステップ 3 [Security] サブタブをクリックします。

ステップ 4 [Create KMIP Client Cert Policy] をクリックします。

ステップ 5 表示された [Create KMIP Client Cert Policy] ダイアログボックスで、次の情報を入力します。

名前	説明
Country Code	会社所在国の国コード。 アルファベット2文字を大文字で入力します。
状態	証明書を要求している会社の本社が存在する州または行政区分。 32 文字まで入力します。
地名	証明書を要求している会社の本社が存在する市または町。 32 文字まで入力します。
組織名	証明書を要求している組織。 32 文字まで入力します。
部署名	組織ユニット 最大 64 文字まで入力できます。
Email	要求に関連付けられている電子メール アドレス。
Validity	証明書の有効期間。

ステップ 6 [OK] をクリックします。

サーバ用の KMIP クライアント証明書ポリシーの作成

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

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

ステップ 2 展開**機器** > **ラック マウント** > **サーバ** > **サーバの ID**。

ステップ 3 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。

ステップ 4 [Security] サブタブをクリックします。

ステップ 5 [Create KMIP Client Cert Policy] をクリックします。

ステップ 6 表示された [Create KMIP Client Cert Policy] ダイアログボックスで、次の情報を入力します。

名前	説明
Country Code	会社所在国の国コード。 アルファベット2文字を大文字で入力します。
状態	証明書を要求している会社の本社が存在する州または行政区分。 32 文字まで入力します。
地名	証明書を要求している会社の本社が存在する市または町。 32 文字まで入力します。
組織名	証明書を要求している組織。 32 文字まで入力します。
部署名	組織ユニット 最大 64 文字まで入力できます。
Email	要求に関連付けられている電子メール アドレス。
Validity	証明書の有効期間。

ステップ 7 [OK] をクリックします。

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

新規ストレージ プロファイルまたは既存のストレージ プロファイルにリモート ポリシーを作成できます。

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

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 ポリシーを作成するストレージ プロファイルを選択します。

ステップ 3 **[Security Policy]** タブをクリックし、次に **[Create Security Policy]** をクリックするかまたは **[storage profile]** を右クリックして [Create Security Policy] を選択します。

ステップ 4 [Remote Policy] オプションをクリックします。

a) [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。
b) （任意） [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。
c) （任意） [Port] フィールドに、サーバのポート番号を入力します。
d) [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。
e) （任意） [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。
f) [OK] をクリックします。

ポリシーが正常に作成されたというメッセージが表示されます。

次のタスク

こうして作成されたキーは、そのサーバのストレージプロファイルに関連付けられ、ストレージコントローラの下に展開されます。これを確認するには、**[Server ID]** > **Inventory]** > **[Storage]** > **[Controller]** に進み、SAS ストレージ コントローラを選択します。**[General]** タブに移動し、**[Security]** フィールドが **[drive security enable]** として表示されているかどうかを確認します。

リモート セキュリティ ポリシーの変更

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 ポリシーを作成したストレージ プロファイルを選択します。

ステップ 3 [Security Policy] タブをクリックします。

ステップ 4 リモート ポリシーを変更するには、[Remote Policy] 領域で次の手順を実行します。

a) [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。

b) （任意） [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。

c) （任意） [Port] フィールドに、サーバのポート番号を入力します。

d) [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。

この証明書をブラウザから Base 64 形式で保存します。

e) （任意） [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。

ステップ 5 セキュリティ ポリシーを **リモート ポリシー**から**ローカル ポリシー**に変更するには、次の手順を実行します。

a) [Local Policy] オプションをクリックします。

b) [Key] フィールドにコントローラの新しいセキュリティ キーを入力します。

ステップ 6 [Save Changes] をクリックします。

リモート セキュリティ キーの変更

手順

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

ステップ 2 展開**機器** > **ラック マウント** > **サーバ** > **サーバの ID**。

ステップ 3 [Work] 領域の [Inventory] タブをクリックします。

ステップ 4 [Storage] サブタブをクリックします。

ステップ 5 [Controllers] タブで、SAS コントローラを選択します。

ステップ 6 [General] タブで、[Modify Remote Key] をクリックします。

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。

ディスクのセキュリティのイネーブル化とディセーブル化

始める前に

- ディスクのセキュリティを有効にするには、ディスクが JBOD であることを確認します。
- ディスクをセキュアに消去するには、そのディスクが未設定で良好な状態になっている必要があります。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 展開**機器** > **ラック マウント** > **サーバ** > **サーバの ID**。
ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
ステップ 4 [Storage] サブタブをクリックします。
ステップ 5 [Disks] タブで、ディスクを選択します。
ステップ 6 [Details] 領域で、[Enable Encryption] をクリックします。
ステップ 7 セキュア ディスクを無効にするには、[Secure Erase] をクリックします。

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

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 展開**機器** > **ラック マウント** > **サーバ** > **サーバの ID**。
ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
ステップ 4 [Storage] サブタブをクリックします。
ステップ 5 [Controllers] タブで、SAS コントローラを選択します。
ステップ 6 [General] タブで、[Disable Security] をクリックします。

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。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Rack-Mounts]** > **[Servers]** > **[Server Number]** の順に展開します。
ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
ステップ 4 [Storage] サブタブをクリックします。
ステップ 5 [Controller] タブで、SAS コントローラを選択します。
ステップ 6 ローカル セキュリティ ポリシーで保護されているディスクのロックを解除するには、次の手順を実行します。
a) [General] タブで、[Unlock Disk] をクリックします。
b) [Key] テキスト ボックスに、そのディスクをロックするのに使用したキーを入力します。
c) [OK] をクリックします。

ステップ 7 リモート KMIP サーバで保護されているディスクのロックを解除するには、[General] タブで [Unlock For Remote] をクリックします。

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。

次のタスク

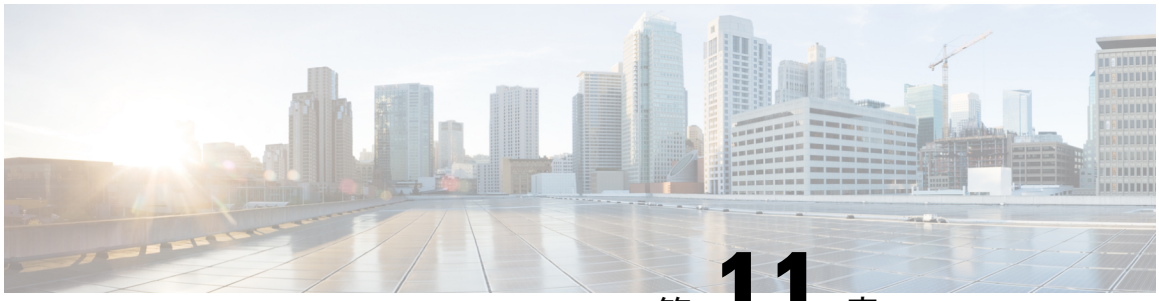
外部設定をインポートするか、またはクリアします。

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

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 展開**機器** > **ラック マウント** > **サーバ** > **サーバの ID**。
ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
ステップ 4 [Storage] サブタブをクリックします。
ステップ 5 [Disks] タブで、ディスクを選択します。
ステップ 6 [General] タブで、[Secure Erase Foreign Configuration] をクリックします。



第 11 章

ストレージ プロファイル

- ストレージ プロファイル （105 ページ）
- 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 （106 ページ）
- RAID レベル （111 ページ）
- 自動ディスク選択 （113 ページ）
- サポートされている LUN の変更 （114 ページ）
- サポートされていない LUN の変更 （114 ページ）
- ディスク挿入の処理 （115 ページ）
- 仮想ドライブの命名 （117 ページ）
- LUN の参照解除 （117 ページ）
- コントローラの制限と制約事項 （118 ページ）
- ストレージ プロファイル （118 ページ）
- ストレージ プロファイルの設定 （138 ページ）

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。

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

シャーシ内のサーバは、そのシャーシ内で集中管理されたストレージを使用することができます。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をディスク グループと言います。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 コントローラがディスク 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、およびディスクのロールを手動で選択するか、自動で選択するかどうかも指定します。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。さらに、ディスクをグローバル ホット スペアとして割り当てることができ、ディスク グループで使用できます。

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

[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。

- [Applying]：仮想ドライブを作成中です。
- [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。
- [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。

- [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

[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。

- [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。
- [Creating]：仮想ドライブを作成中です。
- [Deleting]：仮想ドライブを削除中です。
- [Modifying]：仮想ドライブを変更中です。
- [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

[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。

- [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。
- [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 つのドライブ障害を許容できます。
- [Offline]：仮想ドライブが、RAID コントローラで使用できません。これは基本的に障害状態です。
- [Unknown]：仮想ドライブの状態は不明です。

プレゼンス ステータス

[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 ステータスは次のいずれになります。

- [Equipped]：仮想ドライブを利用できます。
- [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。
- [Missing]：仮想ドライブがありません。

ディスク グループ ポリシーの設定

ディスク グループ ポリシーに、自動または手動でディスクを設定できます。

Procedure

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

ステップ 2 **[Storage]** > **[Storage Provisioning]** > **[Storage Policies]** の順に展開します

ステップ 3 ディスク グループ ポリシーを作成する組織のノードを展開します。

ステップ 4 組織の [Disk Group Policies] を右クリックし、[Create Disk Group Policy] を選択します。

ステップ 5 [Create Disk Group Policy] ダイアログボックスで、次の情報を指定します。

名前	説明
[Name] フィールド	ポリシーの名前 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーが使用される場所と条件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。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（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。
[RAID Level] ドロップダウン リスト	次のいずれかになります。 • **[RAID 0 Striped]** • **[RAID 1 Mirrored]** • **[RAID 5 Striped Parity]** • **[RAID 6 Striped Dual Parity]** • **RAID 10 Mirrored and Striped**

名前	説明
	Note RAID 1 ポリシーでディスク グループを作成し、このグループに 4 つのディスクを設定すると、ストレージ コントローラにより、内部で RAID 1E 構成が作成されます。

ステップ 6 ディスク グループ ポリシーに自動的にディスクを設定するには、[Disk Group Configuration (Automatic)] を選択し、次の情報を指定します。

名前	説明
[Number of drives] フィールド	ディスク グループのドライブの数を指定します。 ドライブ数の範囲は 0 ～ 24 です。デフォルトのドライブ数は、[Unspecified] です。ドライブ数を [Unspecified] として選択すると、ディスクの選択プロセスに応じたディスク数が選択されます。
[Drive Type] フィールド	ディスク グループのドライブのタイプ。次のオプションを選択できます。 • **HDD** • **SSD** • **[Unspecified]** デフォルトのドライブ タイプは [Unspecified] です。ドライブ タイプとして [Unspecified] を選択すると、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 SSD の場合、以降のすべてのドライブが SSD になります。
[Number of Hot Spares] フィールド	ディスク グループの専用ホット スペアの数。 専用ホット スペア数の範囲は 0 ～ 24 です。デフォルトの専用ホット スペア数は [Unspecified] です。専用ホット スペア数を [Unspecified] として選択すると、ディスクの選択プロセスに応じたホット スペア数が選択されます。
[Min Drive Size] フィールド	ディスク グループの最小ドライブ サイズ。この基準を満たすディスクのみが選択可能になります。 最小ドライブ サイズの範囲は 0 ～ 10240 GB です。デフォルトの最小ドライブ サイズは [Unspecified] です。最小ドライブ サイズを [Unspecified] として選択すると、すべてのサイズのディスクが選択可能になります。

ステップ 7 ディスク グループ ポリシーに手動でディスクを設定するには、[Disk Group Configuration (Manual)] を選択してから、次の手順に従います。

a) テーブル右側のアイコン バーにある [+] をクリックします。

b) [Create Local Disk Configuration Reference] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Slot] フィールド	ローカル ディスク参照を設定するスロット。
[Role] フィールド	ディスク グループでのローカル ディスクのロール。次のオプションを選択できます。 • **標準** • **[Dedicated Hot Spare]** • **グローバル ホット スペア**
[Span ID] フィールド	ローカル ディスクのスパン ID。値の範囲は 0 ～ 8 です。 ローカル ディスクのデフォルト スパン ID は [Unspecified] です。これは、スパニング情報が必要でない場合にのみ使用してください。

ステップ 8 [Virtual Drive Configuration] 領域に、次の情報を指定します。

名前	説明
[Strip Size (KB)] フィールド	仮想ドライブのストライプ サイズ。許容される値は [Platform Default] のみです。
[Access Policy] フィールド	仮想ドライブのアクセス ポリシー。次のいずれかになります。 • **Platform Default** • **[Read Write]** • **[Read Only]** • **ブロック**
[Read Policy] フィールド	仮想ドライブの読み取りポリシー。次のいずれかになります。 • **Platform Default** • **[Read Ahead]** • **[Normal]**
[Write Cache Policy] フィールド	仮想ドライブのキャッシュ書き込みポリシー。次のいずれかになります。 • **Platform Default** • **[Write Through]** • **[Write Back Good Bbu]**

名前	説明
	• **[Always Write Back]**
[IO Policy] フィールド	仮想ドライブの I/O ポリシー。次のいずれかになります。 • **Platform Default** • **直接** • **Cached**
[Drive Cache] フィールド	ドライブ キャッシュの状態。次のいずれかになります。 • **Platform Default** • **[No Change]** • **[Enable]** • **[Disable]**

ディスク グループ内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。

ステップ 9 [OK] をクリックします。

Note 仮想ドライブ（VD）のデフォルト値を受け入れて、ディスク グループ ポリシーをサービス プロファイルに関連付けると、サービス プロファイルに関連付けられた後に VD の設定を変更できます。デフォルト以外の値を使用するように WebBIOS から VD のデフォルト値を変更すると、変更された値を確認するためのプロパティ エラーは生成されません。

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んで、データの冗長性を実現します。

- 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：複数のドライブが1つの大きなドライブであるかのように機能できます。たとえば、4 台の 20 GB ドライブを結合して、1 台の 80 GB ドライブのようにすることができます。

サポートされている RAID レベルは次のとおりです。

- RAID 0 Striped：データはアレイ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：データが 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に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。
- RAID 5 Striped Parity：データはアレイのすべてのディスクに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：アレイのすべてのディスクにデータをストライプ化し、2 つのパリティ データ セットを使用して、最大 2 台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：RAID 10 はミラーリングされたディスクのペアを使用して完全なデータ冗長性を提供し、ブロック レベルのストライピングによって高度なスループット レートを実現します。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：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。
- RAID 60 Striped Dual Parity and Striped：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。

自動ディスク選択

ディスク グループ設定を指定して、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 グループ設定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。 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。
  - ポリシーの変更。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を作成しなければ適用できない変更があります。その場合、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 への変更です。
- 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。
- [Expand To Available] オプションは、既に導入されている LUN ではサポートされません。

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 への変更です。
- 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 ドライブ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 （115 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 （115 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 （116 ページ）
- ホット スペア ドライブの交換 （116 ページ）
- 未使用スロットへの物理ドライブの挿入 （117 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

Cisco UCS Manager を使用して仮想ドライブを作成すると、Cisco UCS Manager 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。Cisco UCS Manager 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、Cisco UCS Manager 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によって参照されていない仮想ドライブの名前は変更することができます。

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

- Cisco UCS C240、C220、C24、および C22 サーバの場合、各ストレージ コントローラは 24 台の仮想ドライブをサポートします。 他のすべてのサーバの場合、各ストレージ コントローラは 16 台の仮想ドライブをサポートします。
- 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 サーバのアウト 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] が、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

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 ポリシーは、[Navigation] ペインの [Storage] タブで作成できます。さらに、[Servers] タブで、サービス プロファイルに固有のデフォルト ストレージ プロファイルを設定することもできます。

Caution 以前のリリースの UCS Manager からのデフォルトのローカル ディスク設定がサービス プロファイルやサービス プロファイル テンプレートにある Cisco UCS ブレード サーバまたはラック サーバで、3.1 以降のリリースにアップグレードする場合は、ローカル ディスク設定のデフォルトのポリシーを、ローカル ディスク ポリシーの RAID レベルのオプションではなく、[Any Configuration] に変更すると、同じサービス プロファイルやサービス プロファイル テンプレート内のローカル LUN を使用してストレージ プロファイルを正常に作成できます。レガシー LUN は、その後、ストレージ インベントリの一部になります。

Procedure

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

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

ステップ 3 ストレージ プロファイルを作成する組織のノードを展開します。

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

ステップ 4 組織を右クリックし、[Create Storage Profile] を選択します。

ステップ 5 [Create Storage Profile] ダイアログボックスで、ストレージ プロファイルの名前を指定します。[Description] に、このストレージ プロファイルの説明を任意で入力できます。

ステップ 6 (Optional) **[LUNs]**領域で、 **[Local LUNs]** を作成し、このストレージ プロファイルに追加します。

詳細については、「ローカル LUN の設定, on page 120」を参照してください。

ステップ 7 **[LUNs]** 領域で、**[Controller Definitions]**を作成し、このストレージプロファイルに追加します。

詳細については、「ストレージプロファイル PCH コントローラ定義の作成, on page 125」を参照してください。

ステップ 8 **[LUNs]** 領域で、**[Security Policy]**を作成し、このストレージ プロファイルに追加します。

詳細については、ローカル セキュリティ ポリシーの作成, on page 94およびリモート セキュリティ ポリシーの作成, on page 99を参照してください。

ステップ 9 [OK] をクリックします。

特定のストレージ プロファイルの作成

手順

ステップ 1 **[Servers]** > **[Service Profiles]** の順に展開します。

ステップ 2 特定のストレージ プロファイルを作成するサービス プロファイルが含まれる組織のノードを展開します。

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

ステップ 3 特定のストレージ プロファイルを作成するサービス プロファイルを選択します。

ステップ 4 [Work] ペインで、**[Storage]** > **[LUN Configuration]** タブをクリックします。

ステップ 5 [Actions] 領域で、[Modify Storage Profile] をクリックします。

ステップ 6 [Modify Storage Profile] ダイアログボックスで、[Specific Storage Profile] タブをクリックします。

ステップ 7 [Create Specific Storage Profile] をクリックします。

ステップ 8 （任意） [Specific Storage Profile] 領域で、[Description] フィールドに入力して、ストレージ プロファイルの説明を設定します。

各サービス プロファイルには、特定のストレージ プロファイルを 1 つだけ含めることができます。そのため、このストレージ プロファイルの名前はデフォルトで提供されます。

ステップ 9 [Storage Items] 領域で、ローカル LUN を作成し、このストレージプロファイルに追加します。

ステップ 10 [OK] をクリックします。

ステップ 11 確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ストレージ プロファイルの削除

手順

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

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

ステップ 3 削除するストレージ プロファイルが含まれる組織のノードを展開します。

ステップ 4 削除するストレージ プロファイルを右クリックし、[Delete] を選択します。

ステップ 5 表示される確認ダイアログで、[Yes] をクリックします。

ローカル LUN

ローカル LUN の設定

[Navigation] ペインの [Storage] タブで、ストレージ プロファイル ポリシーに含めるローカル LUN を作成できます。さらに、[Servers] タブで、サービス プロファイルに固有のデフォルト ストレージ プロファイルに含めるローカル LUN を作成することもできます。

Procedure

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

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

ステップ 3 ローカル LUN を作成する対象のストレージ プロファイルが含まれる組織のノードを展開します。

ステップ 4 [Work] ペインで、[General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Create Local LUN] をクリックします。

ステップ 6 [Create Local LUN] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Create Local LUN] オプション	（ローカル LUN の作成時に表示されます）ローカル LUN を作成するときにデフォルトで選択されます。
[Prepare Claim Local LUN] オプション	（ローカル LUN の作成時に表示されます）孤立した LUN を要求する場合に選択します。
[Name] フィールド	ローカル LUN の名前。 この名前には、1 ～ 10 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で、この名前を変更することはできません。
[Size (GB)] フィールド	この LUN のサイズ（GB 単位）。サイズの許容範囲は 1 ～ 10240 GB です。 **Note** 孤立した LUN を要求する場合は、LUN サイズを指定する必要はありません。
[Fractional Size (MB)]フィールド	この LUN の分数サイズ（MB）。
[Auto Deploy] オプション ボタン	ローカル LUN を自動的に展開するかどうかを指定します。次のいずれかになります。 • **[Auto Deploy]** ：ローカル LUN を自動展開します。 • **[No Auto Deploy]** ：ローカル LUN を自動展開しません。
[Expand To Available] チェックボックス	（ラック サーバとブレード サーバのみで使用可能）この LUN を使用可能なディスク グループ全体を使用するように展開できることを指定します。 サービス プロファイルごとに、このオプションを使用できる LUN は 1 つだけです。 [Expand To Available] オプションは、既に導入されている LUN ではサポートされません。
[Select Disk Group Configuration] ドロップダウン リスト	このローカル LUN に適用されるディスク グループ設定をドロップダウン リストから選択します。
[Create Disk Group Policy] リンク	新しいディスク グループを作成する [Create Disk Group Policy] ダイアログボックスを表示します。

ステップ 7 (Optional) このローカル LUN に新しいディスク グループ ポリシーを作成する場合は、[Create Disk Group Policy] をクリックします。

ステップ 8 [OK] をクリックします。

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

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

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

ステップ 3 表示対象のサービス プロファイルが含まれる組織のノードを展開します。

ステップ 4 継承されたローカル LUN を表示するサービス プロファイルを選択します。

ステップ 5 [Work] ペインで、[Storage] タブをクリックします。

ステップ 6 **[Storage Configuration]** サブタブをクリックし、**[Local LUNs]** タブをクリックします。

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。
- [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。
- **サイズ (MB)**:、mb ですが、ストレージ プロファイルで指定された LUN のサイズ。
- [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。
  - [Applyed]：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。
- [Deploy Name]：展開後の仮想ドライブの名前。

- **LUN ID**—LUN 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**

ローカル LUN の削除

手順

ステップ 1 [Navigation] ペインで [Storage] をクリックします。
ステップ 2 **[Storage]** > **[Storage Profiles]** の順に展開します。
ステップ 3 ローカル LUN を削除するストレージ プロファイルが含まれる組織のノードを展開します。
ステップ 4 目的のストレージ プロファイルの [Local LUNs] を展開し、削除するローカル LUN を選択します。
ステップ 5 削除する LUN を右クリックして、[Delete] を選択します。
確認用のダイアログボックスが表示されます。
ステップ 6 [Yes] をクリックします。

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。

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 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

PCH コントローラ定義によって提供されるストレージ プロファイル内のストレージ設定で、PCH コントローラに接続された内蔵 SSD を設定できます。コントローラ定義の名前を作成し、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が解除された場合でもストレージ プロファイルで設定を保持するかどうかを指定し、RAID レベルを選択してコントローラ モードを指定します。

手順

ステップ 1 [Navigation] ペインで、**[Storage]** > **[Storage Profiles]** の順に展開します。

ステップ 2 コントローラの定義を作成するストレージ プロファイルを選択します。

ステップ 3 **[Controller Definitions]** タブをクリックし、パネル下の **[Add]** をクリックするか、または [storage profile] を右クリックし **[Create Controller Definition]** を選択します。

ステップ 4 **[Create Controller Definition]** ダイアログ ボックスで、次の情報を設定します。

名前	説明
[Name] フィールド	ストレージ コントローラの名前。 （注） PCH コントローラ定義を保存すると、[General Tab Properties] 領域から名前を変更することはできません。 最大 16 文字まで入力できます。任意の英数字を使用できます。特殊文字と空白はサポートされていません。
[Protect Configuration] チェックボックス	オンにすると、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が解除されても、ストレージ プロファイルの設定が保持されます。 （注） このオプションが有効な状態で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を解除した後、そのストレージプロファイルに新しいサービスプロファイルを関連付け、そのサービスプロファイル内のローカルディスク設定ポリシーに前とは異なるプロパティが含まれていると、サーバから設定不一致のエラーが返され、関連付けは失敗します。

名前	説明
[RAID Level] ドロップダウン リスト	

名前	説明
	次のいずれかのディスク ポリシー 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、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。そのため、[No RAID] モードの適用後にサーバ上で違いがわからないことがあります。これにより、ポリシーの RAID 設定と、サーバの [Inventory] > [Storage] タブに表示される実際のディスク設定が一致しない場合があります。 以前のすべての RAID 設定情報をディスクから削除するには、[No RAID] コンフィギュレーション モードの適用後に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。

名前	説明
	• **[0RAID 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 ディスクを使用して最大 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。 • [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、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 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。

ステップ 5 [OK] をクリックします。
新しい PCH コントローラ定義が、ナビゲーション ウィンドウに表示されます。

次のタスク

特定のオペレーティングシステムのソフトウェアRAIDドライバのインストール手順については、次を参照してください。

- 『*Cisco UCS C240 M4 Server Installation and Service Guide*』の「Installing LSI MegaSR Drivers for Windows and Linux」セクション

サービス プロファイル PCH コントローラ定義の変更

始める前に

RAID レベルを [RAID 0 Striped] または [RAID 1 Mirrored] から [NO RAID] へ変更する場合は、その手順を開始する前に、次の手順を実行します。

1. 関連付けられているサービスプロファイルにスクラブ ポリシーがあることを確認します。『*Cisco UCS Manager Server Management Guide*』の「*Creating a Service Profile with the Expert Wizard*」を参照してください。
2. サービス プロファイルからサーバの関連付けを解除します。『*Cisco UCS Manager Server Management Guide*』の「*Disassociating a Service Profile from a Server or Server Pool*」を参照してください。

手順

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

ステップ 2 [Storage Profiles] を展開して、特定のストレージ プロファイル名を選択します。

ステップ 3 [Controller Definitions] を展開して、特定のコントローラ定義をクリックします。

ステップ 4 [General] タブで、次の情報を変更します。

名前	説明
[Name] フィールド	ストレージ コントローラの名前。 （注） PCH コントローラ定義を保存すると、[General Tab Properties] 領域から名前を変更することはできません。 最大 16 文字まで入力できます。任意の英数字を使用できます。特殊文字と空白はサポートされていません。

名前	説明
[Protect Configuration] チェックボックス	オンにすると、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が解除されても、ストレージ プロファイルの設定が保持されます。 （注） このオプションが有効な状態で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を解除した後、そのストレージプロファイルに新しいサービスプロファイルを関連付け、そのサービスプロファイル内のローカルディスク設定ポリシーに前とは異なるプロパティが含まれていると、サーバから設定不一致のエラーが返され、関連付けは失敗します。

名前	説明
[RAID Level] ドロップダウン リスト	

名前	説明
	次のいずれかのディスク ポリシー 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、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。そのため、[No RAID] モードの適用後にサーバ上で違いがわからないことがあります。これにより、ポリシーの RAID 設定と、サーバの [Inventory] > [Storage] タブに表示される実際のディスク設定が一致しない場合があります。 以前のすべての RAID 設定情報をディスクから削除するには、[No RAID] コンフィギュレーション モードの適用後に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。

名前	説明
	• **[0RAID 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 ディスクを使用して最大 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。 • [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、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 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。

ステップ 5 [OK] をクリックします。

変更した PCH コントローラ定義が正常に保存されたかどうかが表示されます。

次のタスク

サービス プロファイルからサーバの関連付けを解除して、RAID レベルを [RAID 0 Striped] または [RAID 1 Mirrored] から [NO RAID] に変更した場合は、次の手順を実行します。

1. M4 サーバの場合は、そのサーバを再認識させます。『*Cisco UCS Manager Server Management Guide*』の「*Reacknowledging a Rack-Mount Server*」を参照してください。
2. サービス プロファイルをサーバに関連付けます。『*Cisco UCS Manager Server Management Guide*』の「*Associating a Service Profile with a Server or Server Pool*」を参照してください。

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

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

ステップ 2 [Storage Profiles] を展開します。

ステップ 3 [PCH Controller Definitions] を展開します。

ステップ 4 **[Navigation (ナビゲーション)]** ペインで、削除する特定の**コントローラ定義**をクリックします。

ステップ 5 [General] タブの [Actions] 領域で、[Delete] をクリックします。

ステップ 6 定義を削除するかどうかを確認します。

定義が正常に削除されたかどうかが表示されます。削除されない場合は次を参照してください： PCH コントローラ定義の設定のトラブルシューティング （135 ページ）

ステップ 7 正常に削除されたら、[OK] をクリックします。

PCH コントローラ定義の設定のトラブルシューティング

PCH コントローラ定義の作成

次のような状況では、PCH コントローラ定義の設定に失敗します。

- サポートされていないサーバ モデルのコントローラ定義を設定しようとする
- レガシーのローカルディスク設定ポリシーを使用して、ストレージプロファイル内の PCH ストレージを設定しようとする
- ストレージ プロファイル コントローラ定義とストレージ プロファイル ローカル LUN 設定インターフェイスを使用して、同じコントローラを設定しようとする
- [Protect Configuration] チェックボックスがオンになっており、SWRAID モードで展開された設定とは異なる RAID タイプを設定した場合
- [Protect Configuration] チェックボックスがオンになっており、RAID タイプが現在のコントローラ モードと一致しない場合

警告 すでに関連付けられたサーバの PCH ストレージ設定を変更すると（コントローラ モードの変更、RAID レベルの変更、コントローラ修飾子の変更など）、PNUOS ブートがトリガーされて、ホスト OS のダウンタイムが発生します。

ブート ポリシー

次のいずれかの場合に設定エラーが発生します。

- ブート ポリシーで PCH Disk を選択しましたが、プライマリまたはセカンダリ ターゲット パスのスロット番号が、格納されている内蔵 SSD スロット番号のいずれにも一致しませんでした。
- ブート ポリシーで PCH LUN と PCH Disk の両方を同時に選択しました。

ファームウェア

互換性のないソフトウェアの組み合わせに対しては、関連付けを行うときに設定エラーは発生しません。ただし、サポート対象のソフトウェアの組み合わせを使用していない場合、関連付けの実行中に PCH SSD コントローラのストレージ設定が失敗したり、展開されなかったりすることがあります。また、互換性のないソフトウェアの組み合わせに対する関連付けの最後に PCH SSD コントローラからブートすると、内蔵 SSD で障害が発生することがあります。

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 プロファイルと既存のサービス プロファイルとの関連付け

ストレージ プロファイルを既存または新規のサービス プロファイルに関連付けることができます。[Expert] ウィザードを使用したサービス プロファイルの作成 （165 ページ）を参照してください。

手順

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

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

ステップ 3 ストレージ プロファイルに関連付けるサービス プロファイルが含まれる組織のノードを展開します。

ステップ 4 ストレージ プロファイルに関連付けるサービス プロファイルを選択します。

ステップ 5 [Work] ペインで、[Storage] タブをクリックします。

ステップ 6 [LUN Configuration] サブタブをクリックします。

ステップ 7 [Actions] 領域で、[Modify Storage Profile] をクリックします。[Modify Storage Profile] ダイアログボックスが表示されます。

ステップ 8 [Storage Profile Policy] タブをクリックします。

ステップ 9 このサービス プロファイルに既存のストレージプロファイルを関連付けるには、[Storage Profile] ドロップダウンリストから関連付けるストレージ プロファイルを選択し、[OK] をクリックします。[Storage Items] 領域に、ストレージ プロファイルの詳細が表示されます。

ステップ 10 新しいストレージを作成して、そのストレージをこのサービス プロファイルに関連付けるには、**[Create Storage Profile]**をクリックし、必須フィールドに入力してから **[OK]**をクリックします。 ストレージ プロファイルの作成 （118 ページ）は、新しいストレージ プロファイルの作成に関する詳細情報を提供します。

ステップ 11 （任意） ストレージ プロファイルとサービス プロファイルとの関連付けを解除するには、[Storage Profile] ドロップダウンリストから [No Storage Profile] を選択し、[OK] をクリックします。

ストレージ プロファイルの設定

ブレード サーバの RAID コントローラの外部設定のインポート

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。
ステップ 3 外部設定をインポートする RAID コントローラが搭載されたサーバを選択します。
ステップ 4 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。
ステップ 5 [Controller] サブタブをクリックします。
ステップ 6 [Actions] 領域で、[Import Foreign Configuration] をクリックします。

ラック サーバの RAID コントローラの外部設定のインポート

ブレード サーバのローカル ディスク操作の設定

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。
ステップ 3 ローカル ディスク操作を設定するサーバを選択します。
ステップ 4 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。
ステップ 5 [Disks] サブタブをクリックします。
ステップ 6 目的のディスクを右クリックし、次のいずれかの操作を選択します。

- [Clear Foreign Configuration State]：新しい設定へのローカルディスクの導入時に、そのローカル ディスクに存在する外部設定をクリアします。
- [Set Unconfigured Good]：ローカル ディスクを設定可能として指定します。
- [Set Prepare For Removal]：ローカルディスクをシャーシから除去する対象として指定します。
- [Set Undo Prepare For Removal]：ローカルディスクがシャーシから除去する対象でなくなったことを指定します。
- [Mark as 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。使用可能なドライブの中から仮想ドライブを選択できます。

- [Remove Hot Spare]：ローカル ディスクがホット スペアでなくなったことを指定します。
- [Set JBOD to Unconfigured Good]：新しいローカル ディスクを [Unconfigured Good] としてマークして、設定可能にすることを指定します。

ラック サーバのローカル ディスク操作の設定

手順

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

ステップ 2 **[Equipment]** > **[Rack Mounts]** > **[Servers]** の順に展開します。

ステップ 3 ローカル ディスク操作を設定するサーバを選択します。

ステップ 4 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。

ステップ 5 [Disks] サブタブをクリックします。

ステップ 6 目的のディスクを右クリックし、次のいずれかの操作を選択します。

- [Clear Foreign Configuration State]：新しい設定へのローカル ディスクの導入時に、そのローカル ディスクに存在する外部設定をクリアします。
- [Set Unconfigured Good]：ローカル ディスクを設定可能として指定します。
- [Set Prepare For Removal]：ローカル ディスクを除去する対象として指定します。
- [Set Undo Prepare For Removal]：ローカル ディスクが除去する対象でなくなったことを指定します。
- [Mark as 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。使用可能なドライブの中から仮想ドライブを選択できます。
- [Remove Hot Spare]：ローカル ディスクがホット スペアでなくなったことを指定します。
- [Set JBOD to Unconfigured Good]：新しいローカル ディスクを [Unconfigured Good] としてマークして、設定可能にすることを指定します。

ローカル ディスクの設定操作

手順

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

ステップ 2 **[Equipment]** > **[Chassis]** > **[Chassis *Number*]** の順に展開します

ステップ 3 [Work] ペインで、[Storage] タブをクリックします。

ステップ 4 [Disks] サブタブをクリックします。

ステップ 5 目的のディスクを右クリックし、次のいずれかの操作を選択します。

- [Clear Foreign Configuration State]：新しい設定へのローカルディスクの導入時に、そのローカル ディスクに存在する外部設定をクリアします。
- [Set Unconfigured Good]：ローカル ディスクを設定可能として指定します。
- [Set Prepare For Removal]：ローカルディスクをシャーシから除去する対象として指定します。
- [Set Undo Prepare For Removal]：ローカルディスクがシャーシから除去する対象でなくなったことを指定します。
- [Mark as 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。使用可能なドライブの中から仮想ドライブを選択できます。
- [Remove Hot Spare]：ローカル ディスクがホット スペアでなくなったことを指定します。
- [Set JBOD to Unconfigured Good]：新しいローカル ディスクを [Unconfigured Good] としてマークして、設定可能にすることを指定します。

孤立した仮想ドライブの削除

手順

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

ステップ 2 **[Equipment]** > **[Chassis]** > **[Chassis *Number*]** の順に展開します

ステップ 3 [Work] ペインで、[Storage] タブをクリックします。

ステップ 4 [LUNs] サブタブをクリックします。

ステップ 5 目的の仮想ドライブを右クリックし、[Delete Orphaned LUN] を選択します。

確認用のダイアログボックスが表示されます。

ステップ 6 [Yes] をクリックします。

ラック サーバの孤立した仮想ドライブの削除

手順

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

ステップ 2 **[Equipment]** > **[Rack Mounts]** > **[Servers] の順に展開します。**

ステップ 3 孤立した仮想ドライブを削除するサーバを選択します。

ステップ 4 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。

ステップ 5 [LUNs] サブタブをクリックします。

ステップ 6 目的の仮想ドライブを右クリックし、[Delete Orphaned LUN] を選択します。

確認用のダイアログボックスが表示されます。

ステップ 7 [Yes] をクリックします。

ブレード サーバの孤立した仮想ドライブの名前変更

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。
ステップ 3 孤立した仮想ドライブの名前を変更するサーバを選択します。
ステップ 4 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。
ステップ 5 [LUNs] サブタブをクリックします。
ステップ 6 目的の仮想ドライブを右クリックし、[Rename Referenced LUN] を選択します。
ステップ 7 表示される [Rename Referenced LUN] ダイアログボックスで、新しい LUN 名を入力します。
ステップ 8 [OK] をクリックします。

ラック サーバの孤立した仮想ドライブの名前変更

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Rack Mounts]** > **[Servers] の順に展開します。**
ステップ 3 孤立した仮想ドライブの名前を変更するサーバを選択します。
ステップ 4 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。
ステップ 5 [LUNs] サブタブをクリックします。
ステップ 6 目的の仮想ドライブを右クリックし、[Rename Referenced LUN] を選択します。
ステップ 7 表示される [Rename Referenced LUN] ダイアログボックスで、新しい LUN 名を入力します。
ステップ 8 [OK] をクリックします。

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。

（注） Cisco UCS S3260 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 S3260 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。

組み込みのローカル LUN のブート ポリシーの設定

（注） Cisco UCS S3260 M3 サーバ ノードでは、ローカル LUN または JBOD から組み込みのローカル LUN またはディスクにブート ポリシーを移行する前に、ローカル ストレージ設定を削除し、関連付けが完了するまで待機してから、最後に新しいローカル ストレージ設定を追加する必要があります。これは、PCH ディスクまたは LUN からブート処理をイネーブルにします。

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

ステップ 4 設定するブート ポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 下矢印をクリックして、[Local Devices] 領域を展開します。

ステップ 7 [Add Embedded Local LUN] をクリックして、ローカル LUN のブート順序を設定します。

ステップ 8 ローカル LUN をプライマリ ブート デバイスとして設定するには、[Primary] を選択します。

ステップ 9 [LUN Name] フィールドに、プライマリ ブート デバイスとして設定する LUN の名前を入力します。

ステップ 10 [OK] をクリックします。

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） UCSC-C125 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

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

ステップ 4 設定するブート ポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 下矢印をクリックして、[Local Devices] 領域を展開します。

ステップ 7 **[Add Embedded Local Disk]** をクリックして、ローカル JBOD デバイスをプライマリ ブート デバイスとして設定します。

BOD は次のサーバでのみサポートされます。

- Cisco UCS B200 M3 ブレード サーバ
- Cisco UCS B260 M4 ブレード サーバ
- Cisco UCS B460 M4 ブレード サーバ
- Cisco UCS B200 M4 ブレード サーバ
- Cisco UCS C220 M4 ラックマウント サーバ
- Cisco UCS C240 M4 ラックマウント サーバ
- Cisco UCS C460 M4 ラックマウント サーバ
- すべての Cisco UCS M5 サーバ
- Cisco UCS S3260 M4 および M5 サーバ

ステップ 8 **[Disk Slot Number]** フィールドに、プライマリ ブート デバイスとして設定する JBOD ディスクのスロット番号を入力します。

ステップ 9 [OK] をクリックします。

サービス プロファイル内のローカル LUN 操作

LUN 名の事前プロビジョニング

LUN 名を事前にプロビジョニングできるのは、LUN の管理状態が [Undeployed] となっている場合のみです。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。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。
ステップ 2 **[Servers]** > **[Service Profiles]** > **[Service_Profile_Name]** の順に展開します。
ステップ 3 [Work] ペインで、[Storage] タブをクリックします。
ステップ 4 [LUN Configuration] タブをクリックします。
ステップ 5 [Local LUNs] サブタブで、LUN 名を事前プロビジョニングする LUN を右クリックし、[Pre-Provision LUN Name] を選択します。
ステップ 6 [Set Pre-Provision LUN Name] ダイアログボックスで、LUN の名前を入力します。
ステップ 7 [OK] をクリックします。

孤立した LUN の要求

孤立した LUN を要求できるのは、LUN の管理状態が [Undeployed] となっている場合のみです。 LUN の管理状態を明示的に **[Undeployed]** に変更すると、孤立した LUN を要求できます。

LUN 名が空の場合は、要求する前に LUN 名を設定します。

手順

ステップ 1 [Navigation] ペインで [Servers] をクリックします。
ステップ 2 **[Servers]** > **[Service Profiles]** > **[Service_Profile_Name]** の順に展開します。
ステップ 3 [Work] ペインで、[Storage] タブをクリックします。
ステップ 4 [LUN Configuration] タブをクリックします。
ステップ 5 [Local LUNs] サブタブで、要求する LUN を右クリックし、[Claim Orphan LUN] を選択します。
ステップ 6 [Claim Orphan LUN] ダイアログボックスで、所有権を要求する対象とする孤立した LUN を選択します。
ステップ 7 LUN を右クリックし、[Set Admin State] を選択します。
ステップ 8 表示される [Set Admin State] ダイアログボックスで [Undeployed] を選択して、LUN を展開解除し、所有者を要求します。
ステップ 9 [OK] をクリックします。

LUN の展開および展開解除

LUN を展開または展開解除できます。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。

手順

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

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

ステップ 3 [Work] ペインで、[Storage] タブをクリックします。

ステップ 4 [LUN Configuration] タブをクリックします。

ステップ 5 [Local LUNs] サブタブで、展開または展開解除する LUN を右クリックし、[Set Admin State] を選択します。

ステップ 6 表示される [Set Admin State] ダイアログボックスで、LUN を展開する場合は [Online] を選択し、LUN を展開解除する場合は [Undeployed] を選択します。

ステップ 7 [OK] をクリックします。

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

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

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

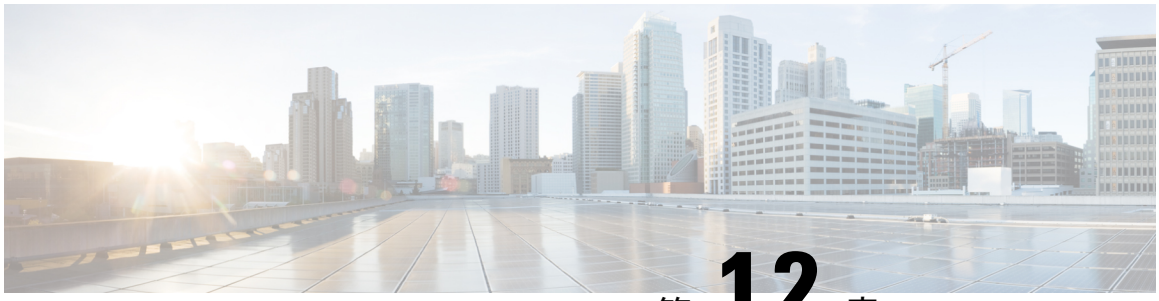
ステップ 3 [Work] ペインで、[Storage] タブをクリックします。

ステップ 4 [LUN Configuration] タブをクリックします。

ステップ 5 [Local LUNs] サブタブで、参照されている LUN の名前を変更する LUN を右クリックし、[Rename Referenced LUN] を選択します。

ステップ 6 [Rename Referenced LUN] ダイアログボックスで、参照されている LUN の新しい名前を入力します。

ステップ 7 [OK] をクリックします。



第 12 章

ミニ ストレージ

- ミニ ストレージ （147 ページ）
- ミニ ストレージ プロパティの表示 （147 ページ）

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。

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

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

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

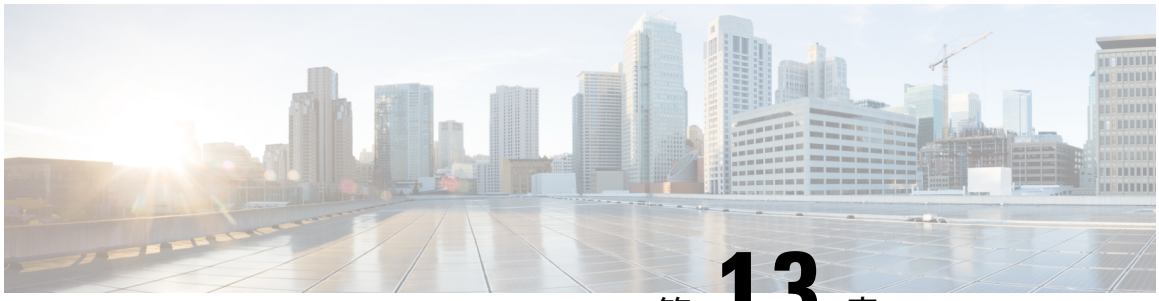
ステップ 3 ミニ ストレージのプロパティを表示するサーバを選択します。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [Motherboard] サブタブをクリックします。

ステップ 6 [Mini Storage] 領域で、[Expand] アイコンをクリックしてその領域を展開します。

ミニ ストレージのプロパティが表示されます。



第 13 章

SD カード サポートの設定

- FlexFlash Secure Digital Card Support, on page 149
- FlexUtil セキュア デジタル カードのサポート （154 ページ）

FlexFlash Secure Digital Card Support

Overview

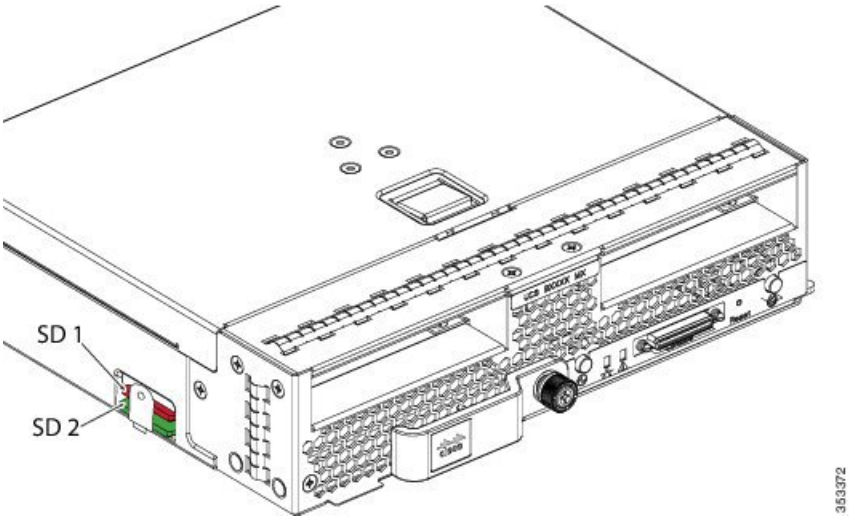
Cisco UCS B-Series, C-Series M3 and higher, and S-Series M4 servers support internal Secure Digital (SD) memory cards. The SD cards are hosted by the Cisco Flexible Flash storage controller, a PCI-based controller which has two slots for SD cards. The cards contain a single partition called HV. When FlexFlash is enabled, Cisco UCS Manager displays the HV partition as a USB drive to both the BIOS and the host operating system.

You can populate one or both the SD card slots that are provided. If two SD cards are populated, you can use them in a mirrored mode.

Note Do not mix different capacity cards in the same server.

The SD cards can be used to store operating system boot images or other information. The following figure illustrates the SD card slots.

Figure 2: SD Card Slots



FlexFlash is disabled by default. You can enable FlexFlash in a local disk policy used in a service profile. When FlexFlash is enabled in a local disk policy, and the server is capable of supporting SD cards, the FlexFlash controller is enabled during service profile association. If a server is not capable of supporting SD cards or has an older CIMC version, a config failure message is displayed.

If you disable FlexFlash in a supported server, the Hypervisor or HV partition is immediately disconnected from the host. The FlexFlash controller will also be disabled as part of a related service profile disassociation.

The FlexFlash controller supports RAID-1 for dual SD cards. The FlexFlash scrub policy erases the HV partition in both cards, and brings the cards to a healthy RAID state.

You can configure new SD cards in a RAID pair and format them using one of the following methods:

- Format the SD cards.
- For an associated server, create a FlexFlash scrub policy and disassociate the service profile from the server. For an unassociated server, create a FlexFlash scrub policy and reacknowledge the server after modifying the default scrub policy.

  The *Scrub Policy Settings* section in the *Cisco UCS Manager Server Management Guide* provides more details about the usage of the scrub policy.

Note Disable the scrub policy as soon as the pairing is complete.

To boot from the HV partition, the SD card must be present in the boot policy used in the service profile.

FlexFlash Firmware Management

The FlexFlash controller firmware is bundled as part of the CIMC image. When you upgrade the CIMC, if a newer firmware version is available for the FlexFlash controller, the controller can no longer be managed, and the FlexFlash inventory displays the **Controller State** as **Waiting For User Action** and the **Controller Health** as **Old Firmware Running**. To upgrade the FlexFlash controller firmware, you need to perform a board controller update. For more information, see the appropriate *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.

Limitations for the Cisco Flexible Flash Storage Controller:

- The Cisco Flexible Flash storage controller only supports 16 GB, 32 GB, and 64 GB SD cards.

  Note 16 GB and 32 GB cards are supported only on the B200-M3 blade servers, and the 64 GB SD cards are supported only on the B200-M4 blade servers.

- We do not recommend using an SD card from a rack server in a blade server, or using an SD card from a blade server in a rack server. Switching SD cards between server types might result in data loss from the SD card.
- Some Cisco UCS C-Series rack-mount servers have SD cards with four partitions: HV, HUU, SCU, and Drivers. Only the HV partition is visible in Cisco UCS Manager. You can migrate a four-partition SD card to a single HV partition card with a FlexFlash scrub policy.
- The FlexFlash controller does not support RAID-1 sync (mirror rebuild). If the SD cards are in a degraded RAID state, or if any metadata errors are reported by the controller, you must run the FlexFlash scrub policy to pair the cards for RAID. For more information about the FlexFlash scrub policy, see Server-Related Policies. The following conditions might result in degraded RAID or metadata errors:
  - Inserting a new or used SD card in one slot, when the server already has an SD card populated in the second slot.
  - Inserting two SD cards from different servers.
- The server firmware version must be at 2.2(1a) or higher.

FlexFlash FX3S Support

Beginning with Release 2.2(3), Cisco UCS Manager allows additional FlexFlash support with the FX3S controller. The FX3S controller is present on the following servers:

- Cisco UCS B200 M4 blade server
- Cisco UCS C220 M4 rack server
- Cisco UCS C240 M4, rack server

FlexFlash operations with the FX3S control are similar to those with the Cisco Flexible Flash storage controller. FlexFlash is disabled by default, and is enabled using a local disk policy. You can also reset the controller, format the SD cards, and enable automatic synchronization of your paired SD cards.

The SD cards for the FX3S controller contain a single partition called Hypervisor.

Limitations for the Cisco FX3S Controller:

- The FX3S controller supports only 32 GB and 64 GB SD cards. 16 GB cards are not supported.

- We do not recommend using an SD card from a rack server in a blade server, or using an SD card from a blade server in a rack server. Switching SD cards between server types might result in data loss from the SD card.
- The server firmware version must be at 2.2(3a) or higher.

FlexFlash SD カードのサポートのイネーブル化

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

ステップ 4 [Local Disk Config Policies] を展開し、FlexFlash サポートをイネーブルにするローカル ディスク設定ポリシーを選択します。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [FlexFlash State] フィールドで、[Enable] オプション ボタンをクリックします。

ステップ 7 **[FlexFlash Removable State]** フィールドで、[removable] 状態を選択します。Flex Flash SDカードを [removable] として定義する必要がある場合は、 **[Yes]**オプションをクリックします。ハイパーバイザ要件を調べて、[removable] 状態の設定を確認してください。

- **[No Change]**(デフォルト) - ハイパーバイザが SD カードの [preset] 状態を必要としない場合は、このオプションを使用してください。
- **[No]** - ハイパーバイザが SD カードの [non-removable] 状態を必要とする場合は、このオプションを使用してください。

ステップ 8 [Save Changes] をクリックします。

FlexFlash SD カードのサポートのディセーブル化

この手順では、ローカル ディスク ポリシー内の FlexFlash 機能をディセーブルにする方法について説明します。

手順

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

ステップ 2 [Filter] ドロップダウン リストから [Policies] を選択します。

ステップ 3 [Local Disk Config Policies] ツリーを展開します。

ステップ 4 FlexFlash をディセーブルにするポリシーを強調表示します。

ステップ 5 タスク ペインの [Events] タブをクリックし、[FlexFlash State] の隣にある [Disable] オプション ボタンを選択します。

ステップ 6 FlexFlash SD カードを交換する必要がある場合は、[FlexFlash Removable State] フィールドの [Yes] ラジオ ボタンを選択します。FlexFlash の削除可能状態を変更する前に、SD カードが使用中でないことを確認します。

ステップ 7 [Save Changes] をクリックします。

自動同期のイネーブル化

手順

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

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 自動同期を有効にするサーバをクリックします。

ステップ 4 [Work] ペインの [Inventory] タブをクリックします。

ステップ 5 [Storage] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Enable Auto-sync] をクリックします。

ステップ 7 [Enable Auto-sync] ダイアログボックスで、プライマリとして使用するSDカードの [Admin Slot Number] を選択します。

ステップ 8 [OK] をクリックします。

Formatting the SD Cards

Procedure

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

ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。

ステップ 3 Click the server for which you want to format the SD cards.

ステップ 4 In the **Work** pane, click the **Inventory** tab.

ステップ 5 Click the **Storage** subtab.

ステップ 6 In the **Actions** area, click **Format SD Cards**.

ステップ 7 Click **Yes** to format the SD cards.

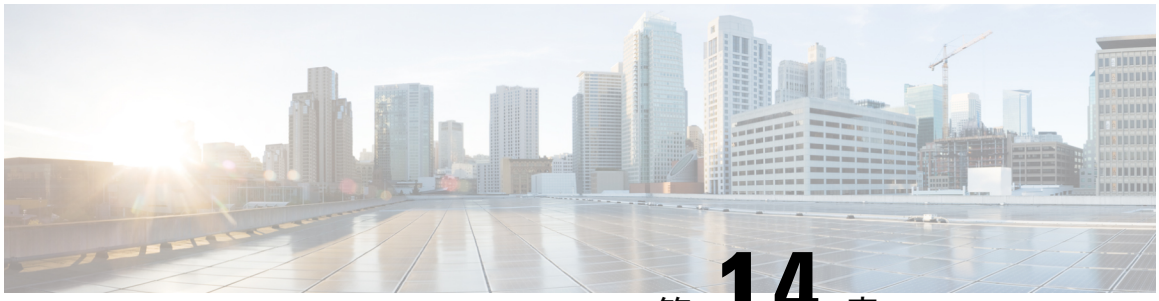
FlexFlash コントローラのリセット

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Chassis]** > ***[Chassis Number]*** > **[Servers]** の順に展開します。
ステップ 3 FlexFlash コントローラをリセットするサーバをクリックします。
ステップ 4 [Work] ペインの [Inventory] タブをクリックします。
ステップ 5 [Storage] サブタブをクリックします。
ステップ 6 [Actions] 領域で [Reset FlexFlash Controller] をクリックします。
ステップ 7 FlexFlash コントローラをリセットするには [Yes] をクリックします。

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 14 章

ダイレクト アタッチド ストレージ

- ダイレクト アタッチド ストレージ （155 ページ）
- ファイバ チャネル スイッチング モード （155 ページ）
- ファイバ チャネル スイッチング モードの設定 （157 ページ）
- ストレージ VSAN の作成 （158 ページ）
- ファイバ チャネル ゾーン分割用の VSAN の作成 （158 ページ）
- ファイバ チャネル ストレージ ポートの設定 （161 ページ）
- ファイバ チャネル ゾーン分割の設定 （162 ページ）

ダイレクト アタッチド ストレージ

標準的なダイレクト アタッチド ストレージ（DAS）システムは、データ ストレージ デバイスで構成されています（たとえば、ラックに設置された多数のハード ディスク ドライブがホスト バス アダプタ（HBA）を介してコンピュータに直接接続されています）。これら 2 つのポイント間にはネットワーク デバイス（スイッチやルータなど）がありません。

DAS 接続に使用される主要なプロトコルは、ATA、SATA、eSATA、SCSI、SAS、USB、USB 3.0、IEEE 1394、およびファイバ チャネルです。

Cisco UCS Manager では、SAN スイッチでゾーン分割設定をプッシュしなくても DAS を使用できます。

ここで説明されている DAS の構成では、ストレージ アレイ ポートとファブリック インターコネクトの間に物理ケーブルが接続済みであることが想定されています。

ファイバ チャネル スイッチング モード

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

エンドホスト モード

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

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

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

Switch Mode

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

スイッチ モードはデフォルトのファイバ チャネル スイッチング モードではありません。

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

ファイバ チャネル スイッチング モードの設定

重要 ファイバ チャネル スイッチング モードを変更すると、Cisco UCS Managerによりログアウトされ、ファブリック インターコネクトが再起動されます。クラスタ設定の場合、Cisco UCS Manager リリース 3.1(1) 以前のリリースでは、Cisco UCS Managerにより両方のファブリック インターコネクトが同時に再起動されます。Cisco UCS Manager リリース 3.1 (2) では、ファイバ チャネル スイッチング モードを変更すると、UCS ファブリック インターコネクトが順次リロードします。Cisco UCS Manager リリース 3.1(3) では、スイッチング モードを変更した結果として、従属ファブリック インターコネクトが初めて再起動されます。プライマリ ファブリック インターコネクトは、[Pending Activities] で確認された後にのみ再起動します。プライマリ ファブリック インターコネクトがファイバ チャネル スイッチング モードに変更され、システムが使用できるようになるまでには数分間かかります。

（注） ファブリック インターコネクトがリロードすると、約 10 ～ 15 分のダウンタイムがシステム全体で発生します。

手順

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

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

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

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

- **[Set Fibre Channel Switching Mode]**
- **[Set Fibre Channel End-Host Mode]**

現在のモードのリンクはグレー表示されます。

ステップ 5 ダイアログボックスで、[Yes] をクリックします。

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

ストレージ VSAN の作成

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID は違っている必要があります。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 と重なる ID が設定されたすべての 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

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

ステップ 2 [SAN] タブで、**[SAN]** > **[Storage Cloud]** を展開します。

ステップ 3 [Work] ペインで、[VSANs] タブをクリックします。

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create VSAN] ダイアログボックスで、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

Cisco UCS Manager GUI で、次の [VSANs] ノードの 1 つに VSAN が追加されます。

- 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ストレージ VSAN の場合は、**[Storage Cloud]** > **[VSANs]** ノード
- 1 つのファブリック インターコネクトのみにアクセス可能な VSAN の場合は、**[Storage Cloud]** > **[*Fabric_Name*]** > **[VSANs]** ノード

ファイバ チャネル ゾーン分割用の VSAN の作成

（注） SAN クラウドの FCoE VLAN と LAN クラウドの VLAN の ID は違っている必要があります。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 と重なる ID が設定されたすべての 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

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

ステップ 2 [SAN] タブの [SAN] ノードをクリックします。

ステップ 3 [Work] ペインの [SAN Uplinks] タブの [SAN Uplinks Manager] リンクをクリックします。

別のウィンドウに [SAN Uplinks Manager] が開きます。

ステップ 4 [SAN Uplinks Manager] で [VSAN] タブをクリックします。

VSANは、どのサブタブでも作成できます。ただし、[All]サブタブを使用すれば、設定済みのすべての VSAN をテーブルに表示できます。

ステップ 5 テーブルの右側のアイコン バーの [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 6 [Create VSAN] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ネットワークに割り当てられている名前。 この名前には、1 ～ 32 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[FC Zoning] フィールド	Cisco UCS Manager が Cisco UCS ドメインに対してファイバ チャネル ゾーン分割を設定するかどうかを決定するためのオプション ボタンをクリックします。次のいずれかになります。 • **[Disabled]**：アップストリーム スイッチがファイバ チャネル ゾーン分割を処理します。またはファイバチャネル ゾーン分割は、Cisco UCS ドメインに対して実行されません。 Cisco UCS Manager はファイバチャネルゾーニングを設定しません。 • **[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 Cisco UCS ドメイン。 （注） Cisco UCS Managerを介してファイバ チャネル ゾーン分割をイネーブルにする場合は、ファイバチャネル ゾーン分割に使用されている VSAN でアップストリーム スイッチを設定しないでください。

名前	説明
[Type] オプション ボタン	オプション ボタンをクリックして、VSAN の設定方法を決定します。次のいずれかになります。 • [Common/Global]：VSAN は、すべての使用可能なファブリック内で同じ VSAN ID にマッピングされます。 • [Fabric A]：VSAN は、ファブリック A にだけ存在する VSAN ID にマッピングされます。 • [Fabric B]：VSAN は、ファブリック B にだけ存在する VSAN ID にマッピングされます。 • [Both Fabrics Configured Differently]：VSAN は、使用可能なファブリックごとに異なる VSAN ID にマッピングされます。このオプションを選択すると、 Cisco UCS Manager GUI に、各ファブリックの**[VSAN ID]** フィールドと **[FCoE VLAN]** フィールドが表示されます。
[VSAN ID] フィールド	ネットワークに割り当てられている固有識別情報。 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。また、FC エンドホスト モードを使用する場合は、3840 ～ 4079 も予約済みの VSAN ID 範囲です。

名前	説明
[FCoE VLAN] フィールド	ファイバ チャネル接続に使用される VLAN に割り当てられた固有識別情報。 VLAN 4048 はユーザが設定可能です。ただし、Cisco UCS Managerでは、VLAN 4048 が次のデフォルト値に使用されます。4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。 • 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、使用または予約されていない VLAN ID に変更する必要があります。たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。 • 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 7 [OK] をクリックします。

ファイバ チャネル ストレージ ポートの設定

このタスクでは、FC ストレージ ポートの設定方法を 1 種類だけ説明します。そのポートの [General] タブから FC ストレージ ポートを設定することもできます。

始める前に

これらのポートが有効になるためには、ファイバ チャネル スイッチング モードが [Switching] に設定されている必要があります。ストレージ ポートは、エンドホスト モードでは動作しません。

手順

ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
ステップ 2 **[Equipment]** > **[Fabric Interconnects]** > ***[Fabric_Interconnect_Name]*** の順に展開します。
ステップ 3 [Expansion Module] ノードを展開します。
ステップ 4 [FC Ports] ノード以下の 1 つ以上のポートをクリックします。
ステップ 5 選択したポートを右クリックし、[Configure as FC Storage Port] を選択します。
ステップ 6 確認ダイアログボックスが表示されたら、[Yes] をクリックします。
ステップ 7 [OK] をクリックします。

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。	
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。ファイバ チャネル スイッチング モードの設定 （157 ページ）を参照してください。

	コマンドまたはアクション	目的
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。	イーサネット ポートの FCoE ストレージ ポートとしての設定 （15 ページ）およびファイバ チャネル ストレージ ポートの設定 （16 ページ） を参照してください。
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。	クラスタ設定では、 VSAN を作成することをお勧めします。ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ）を参照してください。
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。ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ） を参照してください。
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。ファイバ チャネル ゾーン分割用の VSAN の作成 （36 ページ）を参照してください。 • 1 つ以上の vHBA イニシエータ グループを設定します。[Expert] ウィザードを使用したサービスプロファイルの作成 （165 ページ） を参照してください。

ファイバ チャネル ストレージ接続ポリシーの作成

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。

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

ステップ 4 [Storage Connection Policies] ノードを右クリックし、[Create Storage Connection Policy] を選択します。

ステップ 5 [Create Storage Connection Policy] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーを使用する場所とタイミングについての情報を含めることを推奨します。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 6 **[Zoning Type]** フィールドで、次のオプション ボタンのいずれかをクリックします。

- **[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。
- **[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 7 **[FC Target Endpoints]** テーブル で、テーブルの右側にあるアイコン バーで [+] をクリックします。

[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 8 [Create FC Target Endpoint] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

名前	説明
[WWPN] フィールド	ファイバ チャネルまたは FCoE ストレージ アレイ上の物理ターゲット ポートに割り当てられた WWPN（WWN）です。サーバは、この WWPN（WWN）を使用して、ストレージ アレイに設定された LUN にアクセスします。
[Description] フィールド	ターゲット エンドポイントの説明。ターゲット エンドポイントが接続するポート、LUN、またはストレージ アレイに関する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。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Path] フィールド	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。
[Select VSAN] ドロップダウン リスト	ターゲット エンドポイントとの通信に使用する VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。

ポリシーの対象となるすべてのターゲット エンドポイントを作成するまでこの手順を繰り返します。

ステップ 9 ポリシーの対象となるすべてのターゲット エンドポイントを作成したら、[OK] をクリックします。

[Expert] ウィザードを使用したサービス プロファイルの作成

Procedure

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

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

ステップ 3 サービス プロファイルを作成する組織のノードを展開します。

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

ステップ 4 組織を右クリックし、[Create Service Profile (expert)] を選択します。

ステップ 5 [Identify Service Profile] パネルで、サービス プロファイルの [Name]、[UUID assignment] を指定して、[Next] をクリックします。

任意で、このサービスプロファイルの説明を設定できます。UUIDが使用できない場合、このパネルからUUID サフィックス プールを作成することもできます。

Note サービス プロファイルをすばやく作成するには、名前を指定した後に **[Finish]** をクリックします。 Cisco UCS Managerは、指定された名前とすべてのシステム デフォルト値を使用して新しいサービス プロファイルを作成します。

ステップ 6 （オプション）[Networking] パネルで、[Dynamic vNIC Connection Policy] と [LAN Connectivity] のセクションに必要な情報を指定して、[Next] をクリックします。

このパネルからダイナミック vNIC 接続ポリシーおよびLAN 接続ポリシーを作成できます。

ステップ 7 （オプション）[Storage] パネルで、[Local Storage Policy]、[SAN Connectivity]、[WWNN]、[VSAN] などの、SAN 構成情報を指定して、[Next] をクリックします。

このパネルからローカル ディスク設定ポリシーおよびSAN 接続ポリシーを作成できます。

ステップ 8 （任意）[Zoning] パネルで、必要なゾーン分割情報を指定して [Next] をクリックします。

このパネルから vHBA イニシエータ グループを作成できます。

ステップ 9 (オプション)**[vNIC/vHBA Placement (vNIC/vHBA 配置)]**パネルで、配置方法と PCI 順序を指定して **[Next (次へ)]** をクリックします。

このパネルから配置ポリシーを作成できます。

ステップ 10 （オプション）[Server Boot Order] パネルで、ドロップダウン リストから [Boot Policy] を指定して [Next] をクリックします。

このパネルからブート ポリシーを作成できます。

ステップ 11 （任意）[Maintenance Policy] パネルで、メンテナンス ポリシーを指定して [Next] をクリックします。

このパネルから、新しいメンテナンス ポリシーを作成してメンテナンス スケジュールを指定できます。

ステップ 12 （オプション）[Server Assignment] パネルで、[Server Assignment] をドロップダウン リストから選択して指定し、サーバ割り当てに適用する電源状態を指定して [Next] をクリックします。

このパネルからサーバ プールまたはホスト ファームウェア パッケージを作成できます。

ステップ 13 （オプション）[Operational Policies] パネルで、[BIOS Configuration]、[External IPMI Management Configuration]、[Management IP Address]、[Monitoring Configuration(Thresholds)]、[Power Control Policy Configuration]、[Scrub Policy] などのシステムの動作情報を指定して [Finish] をクリックします。

Note アウトバンド IPv4 アドレス、またはインバンド IPv4 または IPv6 アドレスをセットアップするには、それぞれのタブをクリックして、必須フィールドに入力します。

これらの各設定に必要なポリシーが見つからない場合は、このパネルで作成できます。

サービス プロファイルとサーバまたはサーバ プールの関連付け

作成時にサービス プロファイルとブレード サーバまたはサーバ プールを関連付けなかった場合、またはサービス プロファイルを関連付けるブレード サーバまたはサーバ プールを変更する場合には、次の手順を実行します。

Procedure

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

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

ステップ 3 新しいサーバまたはサーバ プールに関連付けるサービス プロファイルが含まれている組織のノードを展開します。

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

ステップ 4 サーバに関連付けるサービス プロファイルを右クリックし、[Associate Service Profile] を選択します。

ステップ 5 [Associate Service Profile] ダイアログボックスで、次のいずれかのオプションを選択します。

オプション	説明
サーバ プール	ドロップダウン リストからサーバ プールを選択します。 Cisco UCS Managerは、このプールから取得したサーバをサービス プロファイルに割り当てます。 ステップ 7 に進みます。
[サーバ（Server）]	ナビゲーション ツリーで適切な使用可能サーバに移動し、サービス プロファイルに割り当てるサーバを選択します。 ステップ 7 に進みます。
[Custom Server]	サービス プロファイルに割り当てられるサーバが含まれるシャーシおよびスロットを指定します。サーバがスロット内に存在しない場合、またはそれ以外の理由で使用できない場合、サービス プロファイルは、サーバが使用できるようになったらサーバに関連付けられます。 ステップ 6 に進みます。

ステップ 6 [Custom Server] を選択した場合は、次の手順を実行します。

a) [Chassis Id] フィールドに、選択したサーバが配置されるシャーシの番号を入力します。

b) [Server Id] フィールドで、選択したサーバが配置されているスロットの番号を入力します。

ステップ 7 サーバに関連付けられた後にサービス プロファイルの移行を制限する場合は、[Restrict Migration] チェックボックスをオンにします。

移行を制限しない場合、既存のサービス プロファイルを移行する前に、Cisco UCS Manager による新規サーバの互換性チェックは実行されません。両方のハードウェアが似ていない場合、関連付けが失敗することがあります。

ステップ 8 [OK] をクリックします。

ファイバ チャネル ゾーン分割設定の確認

ゾーン設定およびゾーン セットのアクティブ化が正しく機能することを確認します。

手順

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

ステップ 2 [Servers] タブの **[Servers]** > **[Service Profiles]** を展開します。

ステップ 3 以前に作成したサービス プロファイルに移動してクリックします。

ステップ 4 右側のペインで [FC Zones] タブをクリックします。

以下を確認します。

- イニシエータおよびターゲットの WWPN が同じゾーンにあります。
- ゾーンの [Admin State] が [Applied] になっています。
- [Oper State] が [Active] になっています。

（注） UCS Manager はゾーン名を自動的に作成します。ゾーンの命名規則は ClusterName_FabricID_ZoneID_ServiceProfileName_InitiatorName です。

ファイバ チャネル ゾーン分割設定のトラブルシューティング

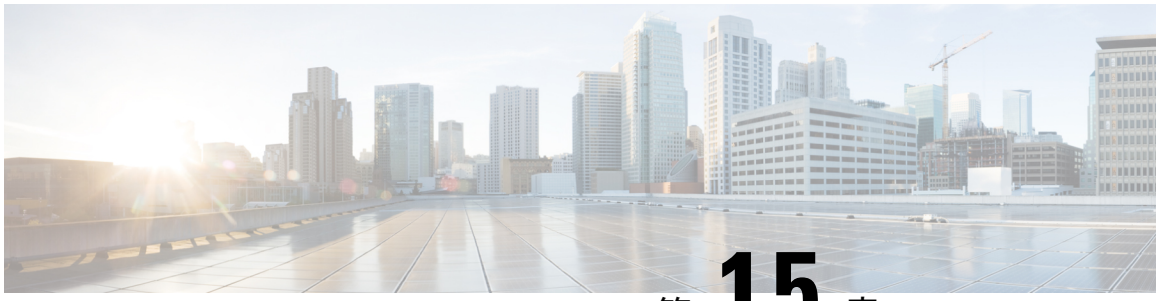
サービス プロファイルを作成しても、[FC Zones] タブにゾーンが表示されない場合は、このトラブルシューティング チェックリストを使用してください。

- 対象の VSAN でゾーン分割がイネーブルになっていますか。
- サービス プロファイルは関連付けられていますか。

  ゾーンは、サービス プロファイルがサーバに関連付けられている場合にのみ作成されます。

- vHBA イニシエータ グループで正しいストレージ接続ポリシーが選択されていますか。
- 正しい vHBA が正しい vHBA イニシエータ グループに追加されていますか。
- vHBA で正しい VSAN が選択されていますか。

- ストレージ接続ポリシーで正しい VSAN およびファブリックが選択されていますか。



第 15 章

ストレージ インベントリ

- ローカル ディスク ロケータ LED のステータス （171 ページ）
- ローカル ディスク ロケータ LED のオンとオフの切り替え （172 ページ）
- NVMe の高度な VMD 搭載したカスタム LED のステータス （172 ページ）
- NVMe で最適化された M5 サーバ （176 ページ）
- NVMe PCIe SSD インベントリ （178 ページ）
- NVMe PCIe SSD ストレージ インベントリの表示 （178 ページ）

ローカル ディスク ロケータ LED のステータス

ローカル ディスクのロケータ LED は、ローカル ディスクを挿入するスロットにあります。この LED は、特定のディスクがブレード サーバまたはラック サーバに挿入されている場所を示します。サーバ内の多数のディスクの中から、メンテナンスのために特定のディスクを削除する必要がある場合に、ロケータ LED が役立ちます。

次の場合に、ローカル ディスク ロケータ LED を正常にオンまたはオフにできます。

- サーバの電源がオンになっている。サーバの電源がオフになっているときに、ロケータ LED をオンまたはオフにしようとすると、UCS Manager はエラーを生成します。
- CIMC バージョンが UCS Manager 3.1 以降。
- RAID コントローラがアウトオブバンド（OOB）ストレージインターフェイスをサポートする。

NVMe の Intel Volume Management Device (VMD) が有効になっている場合は、NVMe 管理対象デバイスの LED の点滅パターンを設定してドライブ ステータスを表示することもできます。障害 ID 点滅パターンによって識別された VMD 対応ドライブは、システムをシャットダウンせずにホットプラグできます。

ローカル ディスク ロケータ LED のオンとオフの切り替え

始める前に

オンとオフ

- ディスクが配置されているサーバの電源がオンになっていることを確認します。サーバの電源がオフの場合、ローカル ディスク ロケータ LED をオンまたはオフにすることはできません。

手順

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

ステップ 2 [Equipment] タブの **[Equipment]** > **[Rack Mounts]** > **[Servers]** > **[*Server Number*]** を展開します。

a) ラックマウントサーバの場合は、**[Rack Mounts (ラック マウント)][Server (サーバ)] *[Server Number (サーバ番号)]*** に移動します。

b) ブレード サーバの場合は、> **[Sensor (センサー)]**> **[Storage (ストレージ)]***[Server Number (サーバ番号)]* に移動します。

ステップ 3 [Work] 領域で、[Inventory] > [Storage] > [Disks] タブを順にクリックします。
ストレージ コントローラ インベントリが表示されます。

ステップ 4 ディスクをクリックします。
ディスクの詳細が表示されます。

ステップ 5 [Actions] 領域で、[Turn on Locator LED] または [Turn off Locator LED] をクリックします。
[Locator LED] の状態が、[Properties] 領域に表示されます。

ステップ 6 [Save Changes] をクリックします。

NVMe の高度な VMD 搭載したカスタム LED のステータス

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

LED の点滅

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

ステータス LED です。VMD は、アクティビティ LED ではなく、ステータス LED のみを管理します。

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

ドライブ ホットプラグ時の LED の動作

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

カスタム点滅パターン

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

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

表 3 : LED 点滅パターン: Windows

ステータス LED	動作	オプション
「アクティブ LED」	指定されたパターンでそのドライブのステータス LED を点滅させることにより、エンクロージャ内の特定のデバイスを識別します。	1 ～ 3600 秒。この範囲外の値は、デフォルトで 12 秒に設定されています。 デフォルトは 12 秒です。

ステータス LED	動作	オプション
ドライブの障害	デバイスのステータス LED を、定義された障害パターンで点灯することによって、縮退状態または障害状態のドライブを示します。	障害パターンは、次の場合に表示されます。 • 1. 物理的に取り外された場合。 または 障害が発生したドライブを含む RAID ボリュームは、削除されるか、物理的に取り外されます。 • 2. RAID ボリュームの一部である障害が発生していないドライブが取り外された時点、または障害が発生したドライブが識別され取り外された時点から。新しいドライブが同じスロットに挿入されるか、またはプラットフォームがリブートされるまで、障害状態のままになります。 デフォルト = オプション 1
RAID ボリュームの初期化または確認と修復のプロセス	RAID ボリュームが再構築状態になると、再構築されている特定のドライブまたは再構築されている RAID ボリューム全体のいずれかで、定義された再構築パターンでステータス LED が点滅します。	デフォルト = 有効 次のように設定できます。 1. 無効 (1 台のドライブのみ) 2. 有効 (すべてのドライブ)
管理対象の取り外し	管理対象のホットプラグでは、ドライブが物理的に取り出されるまで、管理対象ドライブのステータス LED が、定義された検出パターンで点滅します。	なし。デフォルトでは、イネーブルです。

ステータス LED	動作	オプション
RAIDボリュームが移行中です	RAIDボリュームの移行中は、プロセスが完了するまで、すべてのドライブで定義されている再構築パターンでステータス LED が点滅します。	デフォルト = 有効 次のように設定できます。 1. 無効 (ステータス LED は点滅しません) 2. 有効 (ステータス LED を点滅)
Rebuild	移行中のドライブのみが点滅します。	デフォルト = 無効

表 *4 : LED* 点滅パターン*: Linux*

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

ステータス LED	動作	オプション
ledmon デバッグ レベルの設定 **log_level**	対応–ログレベル `ledmon` からのフラグ。	指定できる値は、quiet、error、warning、info、debug、all (0 は「quiet」)、5は「all」を意味します) です。 デフォルト = 2
1 個の RAID メンバまたはすべての RAID の管理設定 **RAID_MEMBRES_ONLY**	フラグが `ledmon` (true) に設定されている場合、RAID メンバであるドライブにのみモニタリングを制限します。	1. False/ (すべての RAID メンバと PT) 2. True/(RAID メンバのみ) デフォルト = False
特定のコントローラのみに限定されたスキャン **WHITELIST**	`ledmon` では、LED 状態の変更を、ホワイトリストにリストされているコントローラに制限します。	ホワイトリスト コントローラの LED の状態の変更を制限します。 デフォルトでは、制限はありません。

表 5: LED 点滅パターン: ESXi

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

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MRAIDPCIe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。

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。

Note 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。

Procedure

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

ステップ 2 **[Rack-Mounts (ラックマウント)]** > **[Servers (サーバ)]** を展開します。

ステップ 3 MSwitch を含むのサーバを展開します。

ステップ 4 **[Work (作業)]** ペインで、**[Inventory (インベントリ)]** > **[Storage (ストレージ)]** > **[Disks (ディスク)]** タブの順にクリックします。

ステップ 5 回復する MSwitch を選択します。

ステップ 6 **[General (全般)]** タブで、**[Disaster Recovery (障害復旧)]** をクリックします。

Note 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。

ステップ 7 FSM からリカバリ ステータスをモニタできます。

NVMe PCIe SSD インベントリ

Cisco UCS Manager GUI は、Non-Volatile Memory Express（NVMe）Peripheral Component Interconnect Express（PCIe）SSD ストレージ デバイスのインベントリを検出、識別、および表示します。サーバ内のストレージ デバイスの状態を表示できます。NVMe 対応 PCIe SSD ストレージ デバイスは、SAS または SATA の SSD と比較して、遅延を短縮し、1 秒あたりの入出力操作数（IOPS）を増加させ、電力消費を削減できます。

NVMe PCIe SSD ストレージ インベントリの表示

手順

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

ステップ 2 [Equipment] タブの **[Equipment]** > **[Rack Mounts]** > **[Servers]** の順に展開します。

ステップ 3 [Inventory] タブをクリックします。

ステップ 4 次のいずれかを実行します。

a) [Storage] タブをクリックします。

[Storage Controller NVME ID number] という名前の NVMe PCIe SSD ストレージ デバイスの一覧が表示されます。名前、サイズ、シリアル番号、動作ステータス、状態、その他の詳細が表示されます。

b) NVMe PCIe SSD ストレージ デバイスをクリックします。

次のインベントリ詳細が表示されます。

名前	説明
ID	サーバで設定されている NVMe PCIe SSD ストレージ デバイス。
Model	NVMe PCIe SSD ストレージ デバイスのモデル。
Revision	NVMe PCIe SSD ストレージ デバイスのリビジョン。
RAID Support	NVMe PCIe SSD ストレージ デバイスが RAID 対応かどうか。
OOB Interface Support	NVMe PCIe SSD ストレージ デバイスがアウトオブバンド管理をサポートしているかどうか。
PCIe Address	仮想インターフェイス カード（VIC）上の NVMe PCIe SSD ストレージ デバイス。 （注） NVMe カードのホット挿入時に PCIe アドレスは表示されません。この情報を表示するには、サーバを再認識させます。
Number of Local Disks	NVMe PCIe SSD ストレージ デバイスに含まれているディスク数。

名前	説明
Rebuild Rate	NVMe PCIe SSD ストレージ デバイスには適用されません。
ベンダー	NVMe PCIe SSD ストレージ デバイスを製造したベンダー。
PID	NVMe PCIe SSD ストレージ デバイスの製品ID（製品名、モデル名、製品番号とも呼ばれます）。
シリアル（Serial）	ストレージ デバイスのシリアル番号。

CHAPTER 16

Cisco UCS S3260 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 （181 ページ）
- Cisco UCS S3260 ストレージ管理操作 （189 ページ）
- 高可用性のためのディスクの共有, on page 190
- ストレージ エンクロージャ操作, on page 198

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 S3260 システムの機能の概要を示します。

表 *6 : Cisco UCS S3260* システムの機能

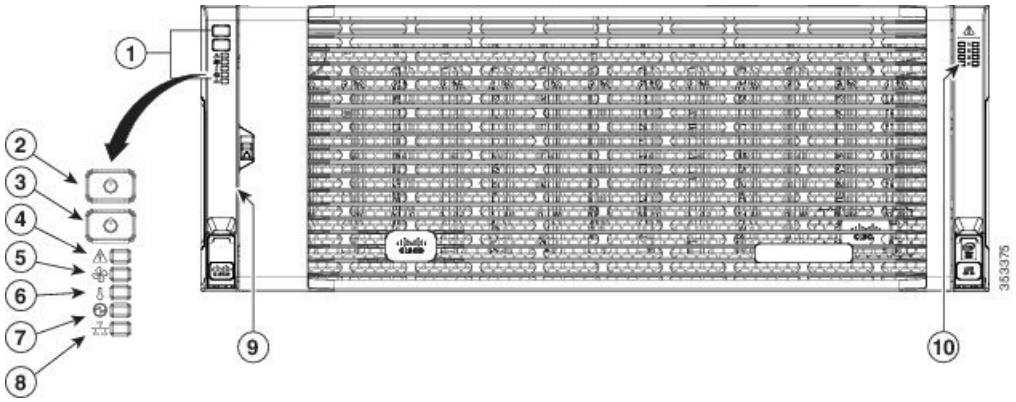
機能	説明
シャーシ	4 ラック ユニット（4RU）シャーシ
プロセッサ	• Cisco UCS S3260 M3 サーバ ノード：各サーバ ノード内の 2 つの Intel Xeon E5-2600 v2 シリーズ プロセッサ。 • Cisco UCS S3260 M4 サーバ ノード：各サーバ ノード内の 2 つの Intel Xeon E5-2600 v4 シリーズ プロセッサ。
メモリ	各サーバ ノード内で最大 16 個の DIMM。
マルチビット エラー保護	このシステムは、マルチビット エラー保護をサポートします。
ストレージ	システムには次のストレージ オプションがあります。

機能	説明
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。
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。
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 S3260 システムの前面パネルの機能を示します。

図 *3 :* 前面パネルの機能

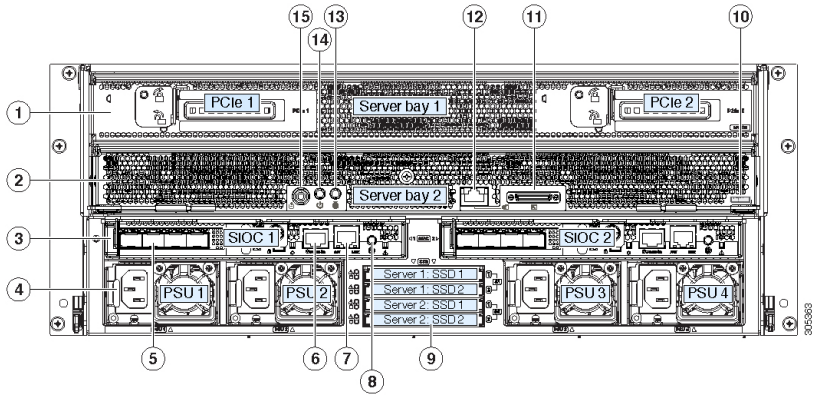


1	操作パネル	6	温度ステータス LED
2	システム電源ボタン/LED	7	電源装置ステータス LED
3	システム ユニット識別ボタン/LED	8	ネットワーク リンク アクティビティ LED
4	システム ステータス LED	9	引き出し型の資産タグ（前面ベゼルの下に表示されない）
5	ファン ステータス LED	10	内蔵ドライブのステータス LED

背面パネルの機能

次の図に、 Cisco UCS S3260 システムの背面パネルの機能を示します。

図 *4 :* 前面パネルの機能



ディスク スロット

1	サーバ ベイ 1 • （オプション）I/O エクスパンダ（図を参照）（Cisco UCS S3260 M4 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 ベイ 2 • （オプション）サーバ ノード (Cisco UCS S3260 M4 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 ベイ 1 にサーバ ノードがある場合は 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 S3260 M4 サーバ ノードのラベル（M4 SVRN） （注） このラベルは、Cisco UCS S3260 M4サーバ ノードを識別します。Cisco UCS S3260 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 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 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

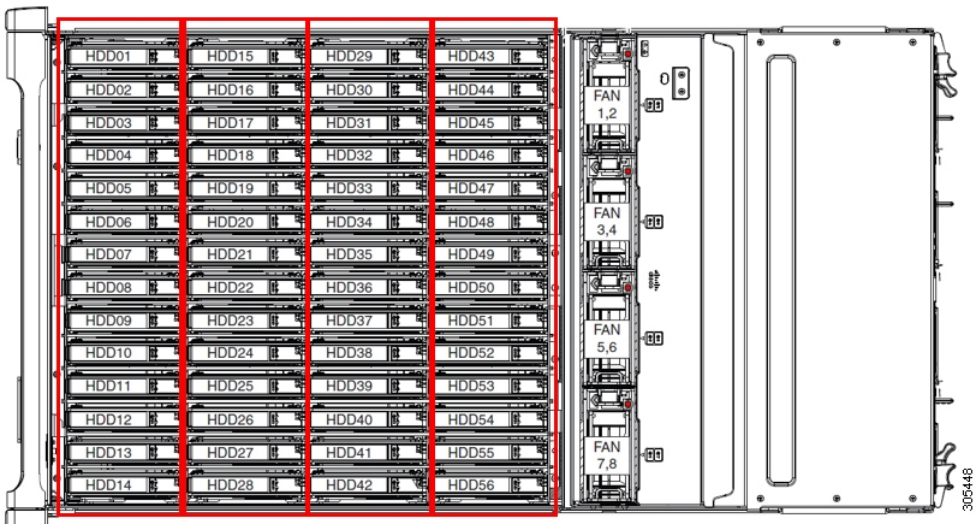
Cisco UCS S3260 システムは、1 つまたは 2 つのノードから構成されています。各ノードには 2 つの CPU、128 GB、256 GB、または 512 GB の DIMM メモリ、最大 4 GB のキャッシュの RAID カードまたはパススルー コントローラが備わっています。サーバ ノードは次のいずれかです。

- Cisco UCS S3260 M3 サーバ ノード
- Cisco UCS S3260 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。

ディスク スロット

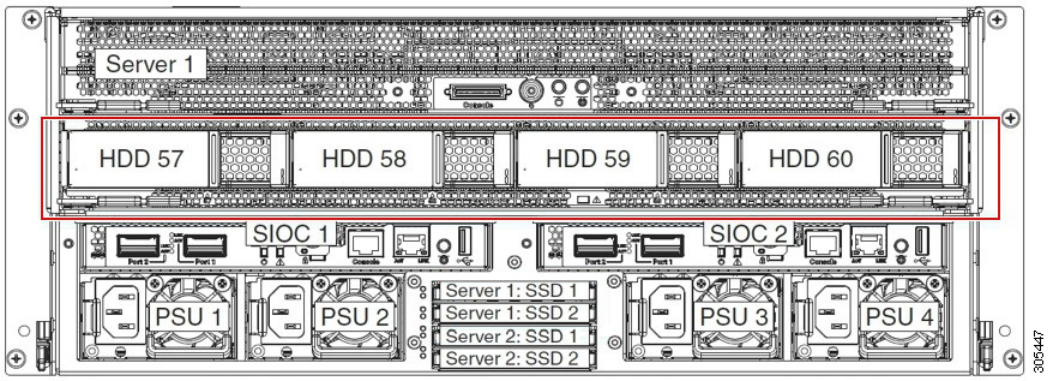
Cisco UCS S3260 シャーシ の HDD マザーボードに 14 ディスク スロットが 4 行と、HDD 拡張トレイに追加の 4 ディスク スロットがあります。次の図は、上面からアクセス可能でホットスワップ可能な 56 台の 3.5 インチの 6 TB または 4 TB 7200 rpm NL-SAS HDD ドライブのディスクの配置を示しています。ディスク スロットに 2 つの SAS ポートがあり、それぞれがシャーシの SAS エクスパンダに接続されます。

図 *5 : Cisco UCS S3260* 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 *6 : 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 S3260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 S3260 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。

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 S3260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 S3260 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 （190 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 S3260 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 S3260 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 7:

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	なし	対応
UCS-C3K-M4RAID	メガ RAID	HW RAID、JBOD	なし	対応
UCSC-S3X60-HBA	イニシエータ ターゲット	パススルー	対応	対応
UCS-S3260-DHBA	イニシエータ ターゲット	パススルー	対応	対応

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 S3260 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 S3260 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 ストレージ管理操作

次の表に、Cisco UCS Manager 統合 Cisco UCS S3260 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 S3260 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。
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 S3260 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。
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、 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。

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

手順

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

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

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

ステップ 4 [Create Disk Zoning Policy] ダイアログボックスで、次を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後にこの名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーを使用する場所とタイミングについての情報を含めることを推奨します。 256 文字以下で入力します。任意の文字またはスペースを使用できます。ただし、`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Preserve Config] チェックボックス	このチェックボックスをオンにすると、スロット番号、所有権、割り当てられたサーバ、割り当てられたコントローラとコントローラのタイプなどのディスクに関するすべての設定関連情報を維持します。 （注） デフォルトでは、[Preserve Config] チェックボックスはオフになっています。

[Disk Zoning Information] 領域で、次を入力します。

名前	フィールド
[Name] カラム	ディスク スロットの名前。
[Slot Number] カラム	ディスクのスロット番号。

名前	フィールド
[**Ownership**] カラム	スロットの所有権の値。次のいずれかになります。 • Unassigned：このオプションは、デフォルトで選択されます。 [Slot Range] フィールドにスロット番号を設定できます。 • **Dedicated**—このオプションを選択すると **[Server]**、**[Controller]**、およびディスクスロットの および **[Slot Range]** の値を設定する必要があります。 • Shared：このオプションを選択すると、ディスク スロットに対する、[Slot Range] と、割り当てられているサーバ、割り当てられているコントローラ、コントローラのタイプなどのコントローラ情報の値を設定する必要があります。 （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。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、表 8 : デュアル HBA コントローラの共有モードの制約事項 （194 ページ）を参照してください。 • Chassis Global Hot Spare ：このオプションを選択すると、ディスク スロットに対する [Slot Range] の値を設定する必要があります。
[Assigned to Server] 列	ディスクが割り当てられているサーバの ID。
[Assigned to Controller] 列	ディスクが割り当てられているコントローラの ID。
[Controller Type] 列	コントローラのタイプ。ディスクが専用または共有のいずれでも、コントローラ タイプは常に SAS です。

表 *8:* 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 S3260	非対応	デュアル HBA	未サポート
Cisco UCS S3260	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

ディスク スロットの作成と所有権の割り当て

ディスク ゾーン分割ポリシーの作成後、ディスク スロットを作成し、所有権を割り当てる必要があります。

手順

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

ステップ 2 **[Policies]** > **[root]** > **[Disk Zoning Policies]** の順に展開して、ディスク スロットを追加するディスク ゾーン分割ポリシーを選択します。

ステップ 3 [Work] ペインで、[Actions] の下の [Add Slots to Policy] をクリックします。

ステップ 4 [Add Slots to Policy] ダイアログボックスで、次のように入力します。

名前	説明
[Ownership] チェックボックス	ディスク スロットの所有権。次のいずれかになります。 • Unassigned：このオプションは、デフォルトで選択されます。[Slot Range] フィールドにスロット番号を設定できます。 • Dedicated：このオプションを選択すると、[Server]、[Controller]、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。 • Shared：このオプションを選択すると、ディスク スロットに対する、[Slot Range] と、割り当てられているサーバ、割り当てられているコントローラ、コントローラのタイプなどのコントローラ情報の値を設定する必要があります。 （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。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、表 8 : デュアル HBA コントローラの共有モードの制約事項 （194 ページ）を参照してください。 • Chassis Global Hot Spare ：このオプションを選択すると、ディスク スロットに対する [Slot Range] の値を設定する必要があります。

ステップ 5 [OK] をクリックします。

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

手順

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

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

ステップ 3 シャーシ プロファイルを作成する組織のノードを展開します。

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

ステップ 4 組織を右クリックし、[Create Chassis Profile] を選択します。

ステップ 5 [Identify Chassis Profile] ページで、シャーシ プロファイルの名前を指定し、[Next] をクリックします。

ステップ 6 （任意）[Maintenance Policy] ページで、メンテナンス ポリシーの名前を指定して [Next] をクリックします。

ステップ 7 [Chassis Assignment] ページで、[Chassis Assignment] の下の [Select existing Chassis] を選択し、このシャーシプロファイルに関連付けるシャーシを選択します。[Next] をクリックします。

ステップ 8 [Disk Zoning] ページで、このシャーシプロファイルに関連付けるディスクのゾーン分割に関するポリシーを指定します。

ステップ 9 [完了（Finish）] をクリックします。

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「仮想ドライブ」セクションを参照してください。

手順

ステップ 1 [Navigation] ペインで、**[Equipment]** > **[Chassis]** > **[Servers]** の順にクリックします。

ステップ 2 ディスクの移行を実行するサーバを選択します。

ステップ 3 [Work (作業)] ペインで、**[Inventory (インベントリ)]** タブをクリックします。

ステップ 4 [Storage] サブタブをクリックします。

ステップ 5 [LUNs] サブタブをクリックします。

ステップ 6 別のサーバに移行するための仮想ドライブを準備するストレージコントローラを選択します。

ステップ 7 移行するディスクを選択します。

ステップ 8 [Actions] 領域で、次のいずれかを選択します。

名前	説明
Rename	ディスクの名前を変更するには、このリンクをクリックします。
[削除（Delete）]	ディスクを削除するには、このリンクをクリックします。

名前	説明
Set Transportation 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移行するには、このリンクをクリックします。 （注） 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。
ClearTransportation Ready	仮想ドライブの状態の転送準備完了をクリアするには、このリンクをクリックします。
Hide Virtual Drive	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、このオプションをクリックします。 （注） 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。

名前	説明
Unhide Virtual Drive	仮想ドライブを表示して入出力処理を有効にするには、このリンクをクリックします。

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。

手順

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

ステップ 2 **[Chassis (シャーシ)]** > **[Servers (サービス)]** > **[Storage Enclosures (ストレージ エンクロージャ)]** の順に展開します。

ステップ 3 削除するストレージ エンクロージャを選択します。

ステップ 4 [Actions] 領域で [Remove Enclosure] をクリックします。