



## Cisco UCS Manager リリース 4.2 ストレージ管理ガイド

初版：2021年6月25日

最終更新：2023年1月6日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（ [www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/) ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021–2023 Cisco Systems, Inc. All rights reserved.

【注意】シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。



(注)

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





## 目次

### Full Cisco Trademarks with Software License ?

### 偏向のないドキュメントに関する免責事項 ?

---

はじめに :

はじめに xvii

対象読者 xvii

表記法 xvii

Cisco UCS の関連資料 xix

マニュアルに関するフィードバック xix

---

第 1 章

新機能および変更された機能に関する情報 1

UCS マネージャ 4.2 の新機能および変更情報 1

---

第 2 章

概要 5

概要 5

Cisco UCS Manager ユーザ ドキュメント 6

ストレージ オプション 7

ストレージ設計の考慮事項 8

ストレージ設定の順序 9

ストレージ プロトコル 9

UCS Manager の [SAN] タブ 10

---

第 3 章

SAN ポートおよびポート チャネル 13

ポート モード 13

ポート タイプ 14

サーバポート	15
サーバポートの設定	15
ファブリック インターコネクットのポートの再設定	15
ファブリック インターコネクットのポートのイネーブル化またはディセーブル化	16
ファブリック インターコネクットのポート設定解除	16
アプライアンスポート	17
アプライアンスポートの設定	17
アプライアンスポートのプロパティの変更	19
FCoE およびファイバチャネルストレージポート	19
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	19
ファイバチャネルストレージポートの設定	20
アップリンクファイバチャネルポートの復元	21
FCリンクの再調整	21
FCストレージポートからFCアップリンクポートへの変換	22
FCoEアップリンクポート	22
FCoEアップリンクポートの設定	23
ユニファイドストレージポート	24
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	24
ユニファイドストレージポートの設定解除	25
ユニファイドアップリンクポート	26
ユニファイドアップリンクポートの設定	26
ユニファイドアップリンクポートの設定解除	27
ポリシーベースのポートエラー処理	27
エラーベースアクションの設定	28
ファイバチャネルポートチャネル	28
ファイバチャネルポートチャネルの作成	29
ファイバチャネルポートチャネルのイネーブル化	30
ファイバチャネルポートチャネルのディセーブル化	30
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	30
ファイバチャネルポートチャネルのプロパティの変更	31
ファイバチャネルポートチャネルの削除	32

FCoE ポート チャネル数	33
FCoE ポート チャネルの作成	33
FCoE ポート チャネルの削除	33
ユニファイドアップリンク ポート チャネル	34

---

**第 4 章**

<b>ファイバチャネルのゾーン分割</b>	<b>35</b>
ファイバチャネルゾーン分割に関する情報	35
ゾーンに関する情報	35
ゾーンセットに関する情報	36
Cisco UCS Manager でのファイバチャネルゾーン分割のサポート	36
Cisco UCS Manager-ベースのファイバチャネルゾーン分割	37
vHBA イニシエータグループ	37
ファイバチャネルストレージ接続ポリシー	38
ファイバチャネルアクティブゾーンセット設定	38
スイッチベースのファイバチャネルゾーン分割	38
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	38
ファイバチャネルゾーン分割の設定	39
ファイバチャネルゾーン分割用の VSAN の作成	40
新しいファイバチャネルゾーンプロファイルの作成	43
ファイバチャネルゾーンプロファイルの削除	46
ファイバチャネルユーザゾーンの削除	46
ファイバチャネルストレージ接続ポリシー	47
ファイバチャネルストレージ接続ポリシーの削除	47

---

**第 5 章**

<b>ネームド VSAN</b>	<b>49</b>
ネームド VSAN	49
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	50
VSAN に関するガイドラインおよび推奨事項	50
ネームド VSAN の作成	52
ストレージ VSAN の作成	53

ネームド VSAN の削除	54
ストレージ VSAN の FCoE VLAN の VLAN ID の変更	55
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	55
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	56

---

第 6 章           **SAN ピン グループ**   **57**

SAN ピン グループ	57
SAN ピン グループの作成	58
SAN ピン グループの削除	58

---

第 7 章           **FC ID の割り当て**   **59**

ファイバチャネル ID	59
-------------	----

---

第 8 章           **WWN プール**   **61**

WWN プール	61
WWNN プールの作成	62
WWNN プールへの WWN ブロックの追加	64
WWNN プールからの WWN ブロックの削除	65
WWNN プールへの WWNN イニシエータの追加	65
WWPN プールからの WWPN イニシエータの削除	66
WWNN プールの削除	66
WWPN プール	67
WWPN プールの作成	67
WWPN プールへの WWN ブロックの追加	69
WWPN プールからの WWN ブロックの削除	69
WWPN プールへの WWPN イニシエータの追加	70
WWPN プールからの WWPN イニシエータの削除	71
WWPN プールの削除	72
WWxN プール	72
WWxN プールの作成	72
WWxN プールへの WWN ブロックの追加	74



WWxN プールからの WWN ブロックの削除 75

WWxN プールの削除 75

## 第 9 章

### ストレージ関連ポリシー 77

vHBA テンプレートについて 77

vHBA テンプレート 77

vHBA テンプレートの作成 77

vHBA テンプレートへの vHBA のバインディング 79

vHBA テンプレートからの vHBA のバインド解除 80

vHBA テンプレートの削除 80

ファイバチャネルアダプタポリシー 81

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 81

ファイバチャネルアダプタポリシーの作成 85

ファイバチャネルアダプタポリシーの削除 91

デフォルトの vHBA 動作ポリシーについて 92

デフォルトの vHBA 動作ポリシー 92

デフォルトの vHBA 動作ポリシーの設定 92

SPDM セキュリティポリシー 93

SPDM セキュリティ 93

SPDM セキュリティポリシーの作成 94

セキュリティポリシーとサーバーの関連付け 95

障害アラート設定の表示 95

SAN 接続ポリシー 96

LANおよびSAN接続ポリシーの概要 96

LANおよびSANの接続ポリシーに必要な権限 96

サービスプロファイルと接続ポリシー間の相互作用 97

SAN 接続ポリシーの作成 97

SAN 接続ポリシー用の vHBA の作成 98

SAN 接続ポリシーからの vHBA の削除 99

SAN 接続ポリシー用のイニシエータグループの作成 99

SAN 接続ポリシーからのイニシエータグループの削除 100

SAN 接続ポリシーの削除	101
Intel® ボリューム管理デバイスの有効化	101
ボリューム管理デバイス (VMD) の設定	101
UCS Manager での VMD の有効化	102
パススルー モードでボリューム管理デバイス (VMD) 有効化	103
ボリューム管理デバイス (VMD) パススルーモード	103
VMD ドライバのダウンロード	104
Intel® ボリューム管理デバイス ドライバ	104
Linux VMD ドライバのダウンロード	105
Windows VMD ドライバのダウンロード	106
VMD パススルー ドライバのダウンロード	107
NVMe の高度な VMD 搭載したカスタム LED のステータス	108

## 第 10 章

**SED セキュリティ ポリシー 113**

自己暗号化ドライブのセキュリティ ポリシー	113
コントローラとディスクのセキュリティ フラグ	114
ローカルセキュリティ ポリシーの管理	115
ローカルセキュリティ ポリシーの作成	115
ローカルセキュリティ ポリシーの変更	115
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	116
KMIP クライアント証明書ポリシー	117
グローバル KMIP クライアント証明書ポリシーの作成	117
サーバ用の KMIP クライアント証明書ポリシーの作成	118
リモートセキュリティ ポリシーの管理	119
リモートセキュリティ ポリシーの作成	119
リモートセキュリティ ポリシーの変更	120
リモートセキュリティ キーの変更	121
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	121
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	121
コントローラのセキュリティのディセーブル化	122
ロックされたディスクのロックの解除	123

セキュア外部設定ディスクの消去 123

データを安全に削除する 124

## 第 11 章

### ストレージ プロファイル 125

ストレージ プロファイル 125

Cisco ブート最適化 M.2 RAID コントローラ 126

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 127

仮想ドライブ 127

ディスク グループ ポリシーの設定 129

RAID レベル 133

自動ディスク選択 135

サポートされている LUN の変更 136

サポートされていない LUN の変更 136

ディスク挿入の処理 137

非冗長仮想ドライブ 137

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 137

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 138

ホットスペアドライブの交換 138

未使用スロットへの物理ドライブの挿入 138

仮想ドライブの命名 139

LUN の参照解除 139

コントローラの制限と制約事項 140

ストレージプロファイル 143

ストレージプロファイルの作成 143

特定のストレージプロファイルの作成 144

ストレージプロファイルの削除 144

ローカル LUN 145

ローカル LUN の設定 145

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 147

ローカル LUN の削除 148

LUN の設定 148

LUN 設定	148
LUN 設定の作成	149
LUN セットの詳細の表示	151
LUN セットの削除	154
エアロ コントローラの構成	154
ストレージ コントローラの自動構成モード	154
自動構成ストレージプロファイルの作成	157
SPDM 認証	158
PCH コントローラ定義	158
PCH SSD コントローラ定義	158
ストレージプロファイル PCH コントローラ定義の作成	160
サービスプロファイル PCH コントローラ定義の変更	166
ストレージプロファイル PCH コントローラ定義の削除	170
M.2 モジュールの移行	172
不良 M.2 ディスクの交換	174
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	175
ストレージプロファイルの設定	176
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	176
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	177
ブレードサーバのローカルディスク操作の設定	177
ラックサーバのローカルディスク操作の設定	178
ローカルディスクの設定操作	179
ローカルストレージのブートポリシー	181
組み込みのローカル LUN のブートポリシーの設定	182
組み込みのローカルディスクのブートポリシーの設定	182
サービスプロファイル内のローカル LUN 操作	183
LUN 名の事前プロビジョニング	183
孤立した LUN の要求	184
LUN の展開および展開解除	184
サービスプロファイルで参照されている LUN の名前変更	185

---

**第 12 章****ミニストレージ 187**

ミニストレージ 187

ミニストレージ プロパティの表示 187

---

**第 13 章****SD カード サポートの設定 189**

FlexFlash セキュア デジタル カードのサポート 189

FlexFlash FX3S のサポート 191

FlexFlash SD カードのサポートのイネーブル化 192

FlexFlash SD カードのサポートのディセーブル化 193

自動同期のイネーブル化 193

SD カードのフォーマット 194

FlexFlash コントローラのリセット 194

FlexUtil セキュア デジタル カードのサポート 195

---

**第 14 章****ダイレクト アタッチドストレージ 197**

ダイレクト アタッチドストレージ 197

ファイバチャネル スイッチング モード 198

ファイバチャネル スイッチング モードの設定 199

ストレージ VSAN の作成 200

ファイバチャネル ゾーン分割用の VSAN の作成 200

ファイバチャネルストレージ ポートの設定 203

ファイバチャネルゾーン分割の設定 204

ファイバチャネルストレージ接続ポリシーの作成 205

[Expert] ウィザードを使用したサービス プロファイルの作成 207

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 209

ファイバチャネルゾーン分割設定の確認 210

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 210

---

**第 15 章****ストレージ インベントリ 213**

ローカル ディスク ロケータ LED のステータス 213

ローカルディスク ロケータ LED のオンとオフの切り替え	214
NVMe の高度な VMD 搭載したカスタム LED のステータス	214
NVMe で最適化された M5 サーバ	218
MSwitch ディザスタ リカバリ	220
NVMe PCIe SSD インベントリ	220
NVMe PCIe SSD ストレージ インベントリの表示	221
UCS ストレージのボリューム管理デバイスを有効にする	223
Intel® ボリューム管理デバイスの有効化	223
ボリューム管理デバイス (VMD) の設定	223
UCS Manager での VMD の有効化	223
パススルー モードでボリューム管理デバイス (VMD) 有効化	224
ボリューム管理デバイス (VMD) パススルーモード	224
VMD パススルーの設定	224
VMD ドライバのダウンロード	225
Intel® ボリューム管理デバイス ドライバ	225
Linux VMD ドライバのダウンロード	227
Windows VMD ドライバのダウンロード	228
VMD パススルー ドライバのダウンロード	229
NVMe の高度な VMD 搭載したカスタム LED のステータス	230

## 第 16 章

<b>Cisco UCS C3260 システム ストレージ管理</b>	<b>235</b>
ストレージ サーバ機能およびコンポーネントの概要	235
Cisco UCS C3260 ストレージ管理操作	245
高可用性のためのディスクの共有	246
ディスク ゾーン分割ポリシー	246
ディスク ゾーン分割ポリシーの作成	247
ディスク スロットの作成と所有権の割り当て	251
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	253
ディスクの移行	253
ストレージエンクロージャ操作	255
シャーシレベルのストレージエンクロージャの削除	255

SAS エクスパンダ設定ポリシー	256
SAS エクスパンダ設定ポリシーの作成	256
SAS エクスパンダ設定ポリシーの削除	257







## はじめに

- [対象読者](#) (xvii ページ)
- [表記法](#) (xvii ページ)
- [Cisco UCS の関連資料](#) (xix ページ)
- [マニュアルに関するフィードバック](#) (xix 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、フィールドのラベルのような GUI 要素は、 <b>[GUI 要素]</b> のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメインタイトルは、 <b>[メインタイトル]</b> のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体 ( <i>italic</i> ) 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、 <b>this font</b> で示しています。 CLI コマンド内の変数は、このフォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x y z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



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



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



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



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

**警告** 安全上の重要事項

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

これらの注意事項を保管しておいてください。

## Cisco UCS の関連資料

### ドキュメント ロードマップ

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

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

### その他のマニュアル リソース

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

## マニュアルに関するフィードバック

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





# 第 1 章

## 新機能および変更された機能に関する情報

- [UCS マネージャ 4.2 の新機能および変更情報 \(1 ページ\)](#)

### UCS マネージャ 4.2 の新機能および変更情報

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

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

特長	説明	参照先
Cisco UCS M6 コントローラ	Cisco UCS Managerは、Cisco UCS C225 M6サーバを次とともにサポートするようになりました: <ul style="list-style-type: none"><li>• C225-SFF の UCS C225 M6SX</li><li>• 直接接続された NVMe ドライブ</li></ul>	<ul style="list-style-type: none"><li>• <a href="#">Cisco ブート最適化 M.2 RAID コントローラ (126 ページ)</a></li><li>• <a href="#">コントローラの制限と制約事項 (140 ページ)</a></li></ul>

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

特長	説明	参照先
Cisco UCS M6 コントローラ	<p>Cisco UCS Managerは、Cisco UCS C245 M6サーバを次とともにサポートするようになりました:</p> <ul style="list-style-type: none"> <li>• UCS C245 M6SX SAS/SATA HDD</li> <li>• UCS-M2-HWRAID</li> <li>• 直接接続された NVMe ドライブ</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">Cisco ブート最適化 M.2 RAID コントローラ (126 ページ)</a></li> <li>• <a href="#">コントローラの制限と制約事項 (140 ページ)</a></li> </ul>

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

特長	説明	参照先
ローカルストレージの RAID レベルを無効にする	PCH SATA コントローラ (AHCI モード) をサポートするためのローカルストレージの無効化を追加しました。	<a href="#">ストレージプロファイル PCH コントローラ定義の作成 (160 ページ)</a> および <a href="#">サービスプロファイル PCH コントローラ定義の変更 (166 ページ)</a>

表 4: Cisco UCS Manager、リリース 4.2(1d) の新機能と変更された動作

特長	説明	参照先
Cisco UCS M6 サーバー	Cisco UCS Manager は、Cisco UCS C220 M6 および UCS C240 M6 C シリーズ サーバーをサポートするようになりました。	<a href="#">Cisco ブート最適化 M.2 RAID コントローラ (126 ページ)</a>
Cisco UCS M6 コントローラ	Cisco UCS Manager は、Cisco UCSC-C220-M6、UCSC-C240-M6、および UCSB-MRAID12G-M6 コントローラをサポートするようになりました。	<a href="#">コントローラの制限と制約事項 (140 ページ)</a>

特長	説明	参照先
Aero ストレージコントローラの自動構成モード	Cisco UCS Manager は、Aero PCIe SAS316 ポート ストレージコントローラを備えた Cisco UCS C220M6/C240M6 C シリーズ M6 サーバーに新しく挿入されたディスクの自動構成を有効にする、ストレージプロファイルの作成をサポートするようになりました。	<a href="#">ストレージコントローラの自動構成モード (154 ページ)</a>
セキュリティプロトコルとデータモデル (SPDM)	SPDM をストレージコントローラでの認証に使用できるようになりました。ネイティブに使用することも、外部のセキュリティ証明書をアップロードして使用することもできます。	<a href="#">SPDM 認証 (158 ページ)</a>







## 第 2 章

### 概要

---

- [概要 \(5 ページ\)](#)
- [Cisco UCS Manager ユーザ ドキュメント \(6 ページ\)](#)
- [ストレージ オプション \(7 ページ\)](#)
- [ストレージ設計の考慮事項 \(8 ページ\)](#)
- [ストレージ設定の順序 \(9 ページ\)](#)
- [ストレージプロトコル \(9 ページ\)](#)
- [UCS Manager の \[SAN\] タブ \(10 ページ\)](#)

### 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 チャンネル
- 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

# Cisco UCS Manager ユーザ ドキュメント

Cisco UCS Manager 次の表に記載する、細分化されたユースケース ベースの新しいドキュメントが用意されています。

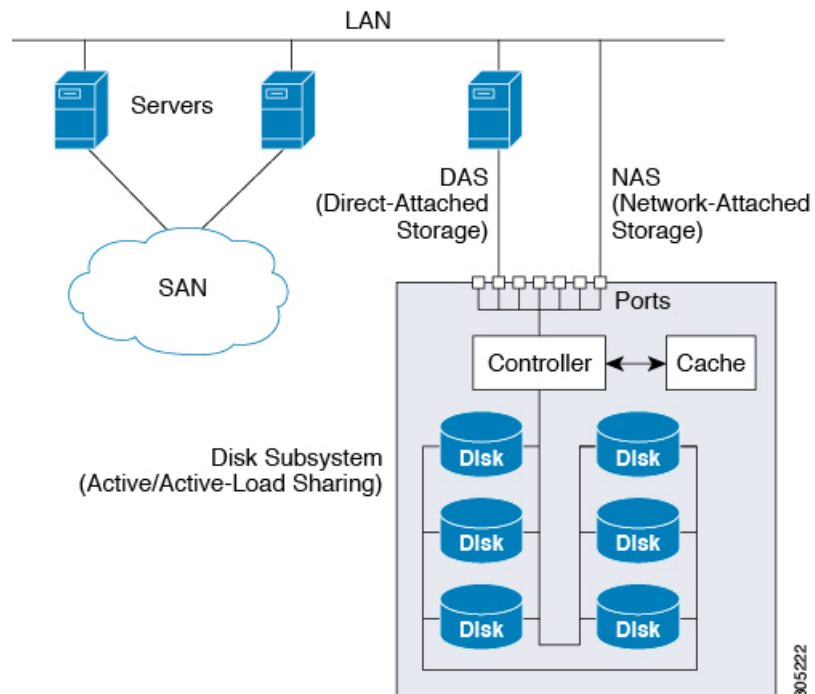
ガイド	説明
<a href="#">Cisco UCS Manager クイック スタート ガイド</a>	Cisco UCS のアーキテクチャと初回操作について説明しています。これにはCisco UCS Manager 初期構成と構成のベストプラクティスも含まれます。
<a href="#">Cisco UCS Manager アドミニストレーションガイド</a>	パスワード管理、ロールベースのアクセス構成、リモート認証、通信サービス、CIMC セッションの管理、組織、バックアップと復元、スケジュール設定オプションに、BIOS トークン、遅延導入について説明しています。
<a href="#">Cisco UCS Manager インフラストラクチャ管理ガイド</a>	Cisco UCS Manager で使用および管理される物理および仮想インフラストラクチャコンポーネントについて説明しています。
<a href="#">『Cisco UCS Manager Firmware Management Guide』</a>	自動インストールを使用したファームウェアのダウンロード、管理、アップグレード、サービスプロファイルを使用したファームウェアのアップグレード、ファームウェア自動同期を使用したエンドポイントでの直接ファームウェアアップグレード、機能カタログの管理、導入シナリオ、トラブルシューティングについて説明しています。
<a href="#">Cisco UCS Manager サーバ管理ガイド</a>	新しいランセンス、Cisco UCS Central への Cisco UCS ドメインの登録、パワーキャッピング、サーバブート、サーバプロファイル、サーバ関連のポリシーについて説明しています。
<a href="#">Cisco UCS Manager ストレージ管理ガイド</a>	Cisco UCS Manager での SUN、VSAN などのストレージ管理のすべての側面について説明しています。
<a href="#">Cisco UCS Manager ネットワーク管理ガイド</a>	Cisco UCS Manager での LAN、VLAN などのネットワーク管理のすべての側面について説明しています。

ガイド	説明
<a href="#">Cisco UCS Manager システム モニタリング ガイド</a>	Cisco UCS Manager でのシステム統計を含め、システムおよびヘルスマニタリングのすべての側面について説明しています。
<a href="#">Cisco UCS S3260 サーバと Cisco UCS Manager との統合</a>	Cisco UCS Manager による UCS S シリーズサーバ管理のすべての側面について説明しています。

## 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

スト、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。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クを利用して、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ต์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ต์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 \(13 ページ\)](#)
- [ポートタイプ \(14 ページ\)](#)
- [サーバポート, on page 15](#)
- [ファブリック インターコネクットのポートの再設定, on page 15](#)
- [ファブリック インターコネクットのポートのイネーブル化またはディセーブル化 \(16 ページ\)](#)
- [ファブリック インターコネクットのポート設定解除, on page 16](#)
- [アプライアンス ポート \(17 ページ\)](#)
- [FCoE およびファイバ チャネル ストレージ ポート, on page 19](#)
- [FC リンクの再調整 \(21 ページ\)](#)
- [FC ストレージ ポートから FC アップリンク ポートへの変換 \(22 ページ\)](#)
- [FCoE アップリンク ポート \(22 ページ\)](#)
- [ユニファイド ストレージ ポート \(24 ページ\)](#)
- [ユニファイド アップリンク ポート \(26 ページ\)](#)
- [ポリシーベースのポートエラー処理 \(27 ページ\)](#)
- [ファイバ チャネル ポート チャネル \(28 ページ\)](#)
- [FCoE ポート チャネル数 \(33 ページ\)](#)
- [ユニファイド アップリンク ポート チャネル \(34 ページ\)](#)

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

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

# ポートタイプ

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

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

ポートタイプ変更時のリブートは不要です。

## イーサネットポートモード

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

- サーバポート
- イーサネットアップリンクポート
- イーサネットポートチャンネルメンバ
- 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ンネルメンバ
- SPAN宛先ポート
- SPAN送信元ポート



---

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

---

## ファイバチャンネルポートモード

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

- ファイバチャンネルアップリンクポート
- ファイバチャンネルポートチャンネルメンバ
- ファイバチャンネルストレージポート
- SPAN送信元ポート



---

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

---

# 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 [ナビゲーション]ペインで、[機器]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 インターコネクットのポートの再設定

### Procedure

- 
- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクット (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 インターコネクッ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 インターコネクッ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 [ナビゲーション] ペインで、[機器] をクリックします。
  - ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクット (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、[はい] 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 インターコネクットのポート設定解除

### Procedure

- 
- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。

- ステップ2 [機器 (Equipment)] > [ファブリック インターコネクト (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、[はい] 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になります。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 [ナビゲーション] ペインで、[機器] をクリックします。

- ステップ 2 [機器 (Equipment) ]>[ファブリック インターコネクト (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、[はい] 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 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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でも設定できます。

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 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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。

Cisco UCS 6454 ファブリック インターコネクトS、49 54 のポートは、FCoE ストレージポートとして設定することはできません。

Cisco UCS 64108 ファブリック インターコネクト では、97-108 のポートは、FCoE ストレージポートとして設定することはできません。

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

**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** [ナビゲーション]ペインで、[機器]をクリックします。

**ステップ 2** [機器 (Equipment) ] > [ファブリック インターコネクト (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、[はい]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 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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、[はい]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 \(29 ページ\)](#) 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 トランッ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

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 ストレージポートから FC アップリンクポートへの変換

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。



**重要** Cisco UCS 6400 シリーズの場合、塗りつぶしパターンはグレー表示され、自動的に IDLE に設定されます。

### 手順

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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、[はい]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 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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] ノードの下で、[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、[はい] 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。アプライアンスポートまたは FCoE ストレージポートをユニファイドストレージポートとして構成できます。ユニファイドストレージポートを設定するには、ファブリックインターコネクタをファイバチャン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タがファイバチャン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 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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、[はい] 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 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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、**[はい]** 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** [ナビゲーション] ペインで、**[機器]** をクリックします。
- ステップ 2** **[機器 (Equipment)]** > **[ファブリック インターコネクト (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、[はい] 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 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネクト (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、[はい] 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ます。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 [ナビゲーション] ペインで、[管理者] 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、6400 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** [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ 2** [SAN] > [SANクラウド]を展開します。
- 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。  
**[Port Channel Admin Speed]** 1 Gbps および 2 Gbps は使用できませんCisco UCS 6400 シリーズファブリック インターコネクト。**[Port Channel Admin Speed]** 16 Gbps および 32 Gbps はCisco UCS 6400 シリーズファブリック インターコネクトに対してのみ使用可能です。
- ステップ 7** [終了] をクリックします。

## ファイバチャンネル ポート チャンネルのイネーブル化

### 手順

---

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
  - ステップ 2 [SAN] > [SAN クラウド (SAN Cloud)] > [ファブリック (Fabric)] > [FC ポート チャンネル (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 チャン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、[はい] をクリックします。
- 

## ファイバチャンネル ポート チャンネルのディセーブル化

### 手順

---

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
  - ステップ 2 [SAN] > [SAN クラウド (SAN Cloud)] > [ファブリック (Fabric)] > [FC ポート チャンネル (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 チャン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、[はい] をクリックします。
- 

## ファイバチャンネル ポート チャンネルのポートの追加および削除

### 手順

---

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] > [SAN クラウド (SAN Cloud)] > [ファブリック (Fabric)] > [FC ポート チャンネル (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 チャン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 auto に設定されている場合、Cisco UCS が管理速度を自動的に調整します。

### 手順

ステップ1 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ2 [SAN] > [SAN クラウド (SAN Cloud)] > [ファブリック (Fabric)] > [FC ポートチャネル (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 (Name)	説明
[名前 (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。

名前 (Name)	説明
[Port Channel Admin Speed] ドロップダウン リスト	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[1 Gbps]</b> <p>(注) Cisco UCS 6400 シリーズ ファブリック インターコネクタでは使用できません。</p> </li> <li>• <b>2 Gbps</b> <p>(注) Cisco UCS 6400 シリーズ ファブリック インターコネクタでは使用できません。</p> </li> <li>• <b>[4 Gbps]</b></li> <li>• <b>[8 Gbps]</b></li> <li>• <b>16 Gbps</b> <p>(注) Cisco UCS 6400 シリーズ ファブリック インターコネクタに対してのみ使用可能。</p> </li> <li>• <b>32 Gbps</b> <p>(注) Cisco UCS 6400 シリーズ ファブリック インターコネクタに対してのみ使用可能。</p> </li> <li>• <b>[auto]</b> <p>(注) Cisco UCS 6400 シリーズ ファブリック インターコネクタでは使用できません。</p> </li> </ul>

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 [ナビゲーション]ペインで、[LAN]をクリックします。

- ステップ2 [SAN]>[SANクラウド (SAN Cloud)]>[ファブリック (Fabric)]>[FCポートチャネル (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、[はい]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 [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ2 [SAN]>[SANクラウド]を展開します。
- 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 [終了] 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 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ2 [SAN] タブで、[SAN] > [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、[はい] 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 \(35 ページ\)](#)
- [Cisco UCS Manager でのファイバチャネルゾーン分割のサポート \(36 ページ\)](#)
- [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 \(38 ページ\)](#)
- [ファイバチャネルゾーン分割の設定 \(39 ページ\)](#)
- [ファイバチャネルゾーン分割用の VSAN の作成 \(40 ページ\)](#)
- [新しいファイバチャネルゾーンプロファイルの作成 \(43 ページ\)](#)
- [ファイバチャネルゾーンプロファイルの削除 \(46 ページ\)](#)
- [ファイバチャネルユーザゾーンの削除 \(46 ページ\)](#)
- [ファイバチャネルストレージ接続ポリシー \(47 ページ\)](#)

## 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ることで設定できません。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タに直接接続され、ゾーン分割は、Cisco UCS ローカルゾーン分割を使用して Cisco UCS Manager で実行されます。既存のファイバチャネルまたは FCoE のアップリンク接続を無効にする必要があります。現時点では、Cisco UCS は、UCS ローカルゾーン分割機能の利用において、現用系なファイバチャネル/FCoE アップリンク接続をサポートしていません。
- スイッチベースのファイバチャネルゾーン分割：この設定は、直接接続ストレージとアップリンクゾーン分割の組み合わせです。ファイバチャネルまたは FCoE のストレージはファブリックインターコネクタに直接接続され、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ต์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 インターコネクタ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 インターコネクタによるハイ 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 インターコネクタに同一の 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	まだ完了していない場合は、Cisco UCS ドメイン 内のファブリック インターコネクタの接続を、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 <b>clear-unmanaged-fc-zone-all</b> 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 インターコネクタ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。 <a href="#">ファイバチャネルスイッチングモードの設定 (199ページ)</a> 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。	<a href="#">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 (19ページ)</a> および <a href="#">ファイバチャネルストレージ</a>

	コマンドまたはアクション	目的
		ポートの設定 (20 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、SAN Uplinks Manager のファイバチャネルゾーンに組み込んで、共通/グローバル設定を使用して両方のファブリック インターコネクต์にアクセスできるように 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 (40 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 (40 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。 <ul style="list-style-type: none"> <li>• 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 (40 ページ) を参照してください。</li> <li>• 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 (207 ページ) を参照してください。</li> </ul>

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

手順

- ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ 2** [SAN] タブの [SAN] ノードをクリックします。
- ステップ 3** [Work] ペインの [SAN Uplinks] タブで、[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 アップリンク マネージャ (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、[すべて]サブタブを使用すると、設定済みのすべてのVSANがテーブルに表示されます。
- ステップ 5** テーブルの右側のアイコンバーで、[+] をクリックします。  
[+] アイコンが無効になっている場合、テーブルのいずれかのエントリをクリックして、有効にします。
- 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 (Name)	説明
[名前 (Name) ] フィールド	<p>ネットワークに割り当てられている名前。</p> <p>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。</p>
[FC Zoning] フィールド	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : 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。</li> <li>• <b>[Enabled]</b> : 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。</li> </ul> <p>(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。</p>

名前 (Name)	説明
[Type] オプション ボタン	<p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> <li>• [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。</li> <li>• [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。</li> </ul>
[VSAN ID] フィールド	<p>ネットワークに割り当てられている固有識別情報。</p> <p>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。</p>

名前 (Name)	説明
[FCoE VLAN] フィールド	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを（未使用の VLAN ID）4049 に変更することを検討します。</li> <li>• 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。</li> </ul> <p>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。</p>

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 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ 2 [SAN] タブで、[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
[名前 (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
[名前 (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	<p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> </ul>
(注)	<p>VSAN を選択するには、次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>• <b>Select VSAN</b></li> <li>• <b>VSAN の作成</b></li> <li>• <b>[Create Storage VSAN]</b></li> </ul>
[Select VSAN] ドロップダウン リスト	<p>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。</p> <p>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。</p>
[Create VSAN] リンク	<p>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、<a href="#">ファイバチャネルゾーン分割用の VSAN の作成 (40 ページ)</a> 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、チャンネルゾーンプロファイルの作成を続行できます。</p>
[Create Storage VSAN] リンク	<p>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、<a href="#">ファイバチャネルゾーン分割用の VSAN の作成 (40 ページ)</a> 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、チャンネルゾーンプロファイルの作成を続行できます。</p>

フィールド	説明
[Member WWPNs]	<p>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。</p> <p>このゾーンの WWPN を入力します。</p>

**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** [ナビゲーション] ペインで、[SAN] をクリックします。

**ステップ 2** [SAN] タブで、[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** [ナビゲーション] ペインで、[SAN] をクリックします。

**ステップ 2** [SAN] タブで、[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 [ナビゲーション]ペインで、[SAN]をクリックします。
  - ステップ2 [SAN] > [ポリシー (Policies)] > [Organization Name] の順に展開します。
  - ステップ3 [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、[はい]をクリックします。
-





## CHAPTER 5

# ネームド VSAN

- [ネームド VSAN, on page 49](#)
- [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 \(50 ページ\)](#)
- [VSAN に関するガイドラインおよび推奨事項 \(50 ページ\)](#)
- [ネームド VSAN の作成, on page 52](#)
- [ストレージ VSAN の作成 \(53 ページ\)](#)
- [ネームド VSAN の削除, on page 54](#)
- [ストレージ VSAN の FCoE VLAN の VLAN ID の変更 \(55 ページ\)](#)
- [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 \(55 ページ\)](#)
- [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 \(56 ページ\)](#)

## 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 インターコネクッ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 インターコネクッ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せん。

- 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ットのネームド 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ッ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 インターコネクットのすべてのファイバチャネルアップリンク ポートで、Cisco UCS ドメインのすべてのネームド VSAN が許可されます。

## VSAN に関するガイドラインおよび推奨事項

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

**VSAN 4079 は予約済み VSAN ID です。**

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

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

### FC スイッチ モードのネームド VSAN 用に予約された VSAN 範囲

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

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

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

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

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

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

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

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

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

### FC スイッチ モードのネームド VSAN ID の範囲に関する制約事項

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

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

## FCoE VLAN ID に関するガイドライン



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

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

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

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

### Procedure

- ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2** [SAN] > [SAN クラウド] 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 バーで、[+] をクリックします。

[+] アイコンが無効になっている場合、テーブルのいずれかのエントリをクリックして、有効にします。



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

### 手順

ステップ1 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ2 [SAN] タブで、[SAN] > [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で、[+] をクリックします。

[+] アイコンが無効になっている場合、テーブルのいずれかのエントリをクリックして、有効にします。

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ต์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ต์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** [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2** [SAN] タブで、[SAN] 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 キーや Ctrl キーを使用すると、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、[はい] 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 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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 インターコネクタがファイバチャネル エンドホスト モードに設定されている場合、ファイバチャネル アップリンク トランキング を有効にすると、ID が 3840 ~ 4079 の範囲にあるすべての VSAN が動作不能になります。



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

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

#### 手順

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] > [SANクラウド] を展開します。
- 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、[はい] 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 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] > [SANクラウド] を展開します。
- 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、[はい] 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 57

## 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 [ナビゲーション] ペインで、[SAN] をクリックします。
  - ステップ 2 [SAN] タブで、[SAN] > [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 グループの一意的な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 グループを vHBA テンプレートに含めます。

## SAN ピン グループの削除

### Procedure

---

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
  - ステップ 2 [SAN] タブで、[SAN] > [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、[はい] 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 \(59 ページ\)](#)

## 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、グローバルに一意的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 の各ポートに一意的な 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 61](#)
- [WWPN プール, on page 67](#)
- [WWxN プール, on page 72](#)

## WWN プール

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

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

WWN をブロック単位でプールに割り当てます。

### WWNN プール

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

### WWPN プール

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

### WWxN プール

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

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

- WWNN プールの場合、WWxN プールは [WWNN Assignment] ドロップダウン リストにオプションとして表示されます。
- WWPN プールの場合、[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 to 20:FF:00:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF. その他の WWN 範囲はすべて予約されています。ファイバ チャネル トラフィックが Cisco UCS インフラストラクチャを介して送信されると、送信元 WWPN は MAC アドレスに変換されます。送信元マルチキャスト MAC アドレスに変換可能な WWPN プールを使用することはできません。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX という形の WWN プレフィックスを使用することをお勧めします。

### Procedure

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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 (Name)	説明
[名前 (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。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (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。
[割り当て順序 (Assignment Order) ] フィールド	次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[デフォルト (Default) ]</b> : Cisco UCS Manager はプールからランダム ID を選択します。</li> <li>• <b>[シーケンシャル (Sequential) ]</b> : 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。</li> </ul>

- 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 (Name)	説明
[開始] 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 <i>ports-per-node</i> + 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 [終了] をクリックします。

### What to do next

WWNN プールをサービスプロファイルとテンプレートに含めます。

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

### 手順

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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 (Name)	説明
[開始] 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 <i>ports-per-node</i> + 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 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、Cisco UCS Manager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る。
- アドレスが割り当てられた vNIC または vHBA が削除される。
- vNIC または vHBA が異なるプールに割り当てられる。

### 手順

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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、[はい] 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 to 20:FF:00:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF. その他の WWN 範囲はすべて予約されています。ファイバチャネルトラフィックが Cisco UCS インフラストラクチャを介して送信されると、送信元 WWPN は MAC アドレスに変換されます。送信元マルチキャスト MAC アドレスに変換可能な WWPN プールを使用することはできません。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX という形の WWN プレフィックスを使用することをお勧めします。

### 手順

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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 (Name)	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。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (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 [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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、[はい]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、Cisco UCS Managerは、に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みアドレスは、次のいずれかが起きるまで、vNIC または vHBA に割り当てられた状態のままになります。

- 関連付けられたサービス プロファイルが削除される。

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

### Procedure

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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、[はい] 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 to 20:FF:00:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF. その他の WWN 範囲はすべて予約されています。ファイバチャネルトラフィックが Cisco UCS インフラストラクチャを介して送信されると、送信元 WWPN は MAC アドレスに変換されます。送信元マルチキャスト MAC アドレスに変換可能な WWPN プールを使用することはできません。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX という形の WWN プレフィックスを使用することをお勧めします。

### 手順

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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 (Name)	説明
[名前 (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。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (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。
[割り当て順序 (Assignment Order) ] フィールド	次のいずれかになります。  <ul style="list-style-type: none"> <li>• <b>[デフォルト (Default) ]</b> : Cisco UCS Manager はプールからランダム ID を選択します。</li> <li>• <b>[シーケンシャル (Sequential) ]</b> : 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。</li> </ul>

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 (Name)	説明
[開始] 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 <i>ports-per-node</i> + 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 [終了] をクリックします。

### 次のタスク

WWPN プールを vHBA テンプレートに含めます。



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

### 手順

- ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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 (Name)	説明
[開始] 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 <i>ports-per-node</i> + 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 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、Cisco UCS Manager 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る。
- アドレスが割り当てられた vNIC または vHBA が削除される。
- vNIC または vHBA が異なるプールに割り当てられる。

#### 手順

- 
- ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2** [SAN] タブで、[SAN] > [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、[はい] 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 to 20:FF:00:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF. その他の WWN 範囲はすべて予約されています。ファイバチャネルトラフィックが Cisco UCS インフラストラクチャを介して送信されると、送信元 WWPN は MAC アドレスに変換されます。送信元マルチキャスト MAC アドレスに変換可能な WWPN プールを使用することはできません。SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX という形の WWN プレフィックスを使用することをお勧めします。

---

#### 手順

- 
- ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2** [SAN] タブで、[SAN] > [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 (Name)	説明
[World Wide Name] フィールド	WWN。

名前 (Name)	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。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (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 (Name)	説明
[ブート ターゲット WWPN (Boot Target WWPN) ] フィールド	ブート イメージの場所に対応する WWPN。
[ブート ターゲット LUN (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 [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2 [SAN] タブで、[SAN] > [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、[はい] 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、Cisco UCS Managerは、に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みアドレスは、次のいずれかが起きるまで、vNIC または vHBA に割り当てられた状態のままになります。

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

### 手順

- 
- ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。
  - ステップ 2 [SAN] タブで、[SAN] > [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、[はい]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 という形の WWN プレフィックスを使用することをお勧めします。

---

### 手順

- 
- ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。
  - ステップ 2 [SAN] タブで、[SAN] > [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 (Name)	説明
[名前 (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。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (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。
[割り当て順序 (Assignment Order) ] フィールド	次のいずれかになります。 <ul style="list-style-type: none"> <li>• <b>[デフォルト (Default) ]</b> : Cisco UCS Manager はプールからランダム ID を選択します。</li> <li>• <b>[シーケンシャル (Sequential) ]</b> : 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。</li> </ul>

- 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 (Name)	説明
[開始] フィールド	ブロック内の最初の WWN。

名前 (Name)	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 <i>ports-per-node</i> + 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 [終了] をクリックします。

#### 次のタスク

WWxN プールをサービスプロファイルとテンプレートに含めます。

## 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 to 20:FF:00:FF:FF:FF:FF or from 50:00:00:00:00:00:00 to 5F:FF:00: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 WWPNS を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX という形の WWN プレフィックスを使用することをお勧めします。

#### 手順

ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ 2 [SAN] タブで、[SAN] > [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 (Name)	説明
[開始] フィールド	ブロック内の最初の WWN。

名前 (Name)	説明
[Size] フィールド	<p>ブロック内の WWN の数。</p> <p>WWxN プールの場合、プールサイズは <i>ports-per-node</i> + 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 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。</p>

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、Cisco UCS Manager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る。
- アドレスが割り当てられた vNIC または vHBA が削除される。
- vNIC または vHBA が異なるプールに割り当てられる。

### 手順

ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ 2 [SAN] タブで、[SAN] > [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、[はい] 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、Cisco UCS Managerは、に割り当てられたアドレスを再割り当てしません。削除されたプールのすべての割り当て済みアドレスは、次のいずれかが起きるまで、vNIC または vHBA に割り当てられた状態のままになります。

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

- vNIC または vHBA が異なるプールに割り当てられる。

### Procedure

---

- ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。
  - ステップ 2 [SAN] タブで、[SAN] > [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、[はい]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 \(77 ページ\)](#)
- [ファイバチャネルアダプタ ポリシー \(81 ページ\)](#)
- [デフォルトの vHBA 動作ポリシーについて \(92 ページ\)](#)
- [SPDM セキュリティ ポリシー \(93 ページ\)](#)
- [SAN 接続ポリシー \(96 ページ\)](#)

## 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としています。

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

## 手順

**ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。

**ステップ 2** [SAN] > [ポリシー]を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

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

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

名前 (Name)	説明
[名前 (Name) ] フィールド	仮想ホストバス アダプタ (vHBA) テンプレートの名前。 この名前には、1～16文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[Description] フィールド	テンプレートのユーザー定義による説明。 256文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、> (大なり)、< (小なり)、または' (一重引用符) は使用できません。
[Fabric ID] フィールド	このテンプレートで作成された vHBA が関連付けられているファブリック インターコネクタの名前。
[Select VSAN] ドロップダウン リスト	このテンプレートから作成された vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Template Type] フィールド	次のいずれかになります。 <ul style="list-style-type: none"> <li>• [Initial Template] : テンプレートが変更されても、このテンプレートから作成された vHBA はアップデートされません。</li> <li>• [Updating Template] : テンプレートが変更されると、このテンプレートから作成された vHBA がアップデートされます。</li> </ul>

名前 (Name)	説明
[Max Data Field Size] フィールド	vHBA がサポートするファイバチャネルフレームのペイロードバイトの最大サイズ。  256 ~ 2112 の範囲の整数を入力します。デフォルトは 2048 です。
[WWPN Pool] ドロップダウンリスト	このテンプレートから作成された vHBA によって、WWPN アドレスを導出するために使用される WWPN プール。
[QoS Policy] ドロップダウンリスト	このテンプレートから作成された vHBA に関連付けられている Quality of Service (QoS) ポリシー。
[Pin Group] ドロップダウンリスト	このテンプレートから作成された vHBA に関連付けられている SAN ピングループ。
[Stats Threshold Policy] ドロップダウンリスト	このテンプレートから作成された vHBA に関連付けられている統計情報収集ポリシー。

ステップ 6 [OK] をクリックします。

#### 次のタスク

vHBA テンプレートをサービス プロファイルに含めます。

## vHBA テンプレートへの vHBA のバインディング

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



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

#### 手順

ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ 2 [サーバ] > [サービス プロファイル] を展開します。

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

**ステップ 4** [Service\_Profile\_Name] > [vHBAs] を展開します。

**ステップ 5** テンプレートにバインドする vHBA をクリックします。

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

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

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

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

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

---

## vHBA テンプレートからの vHBA のバインド解除

### 手順

---

**ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。

**ステップ 2** [サーバ]>[サービスプロファイル]を展開します。

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

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

**ステップ 4** [Service\_Profile\_Name] > [vHBAs] を展開します。

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

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

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

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

---

## vHBA テンプレートの削除

### 手順

---

**ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。

- ステップ2 [SAN]>[ポリシー (Policies)]>[*Organization\_Name*]の順に展開します。
- ステップ3 [vHBA Templates] ノードを展開します。
- ステップ4 削除する vHBA テンプレートを右クリックし、[Delete] を選択します。
- ステップ5 確認ダイアログボックスが表示されたら、[はい]をクリックします。

## ファイバチャネルアダプタ ポリシー

### イーサネットおよびファイバチャネルアダプタ ポリシー

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

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



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

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

### オペレーティング システム固有のアダプタ ポリシー

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



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

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

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

### Linux アダプタ ポリシーの割り込みカウント

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

ドライバのバージョンに応じて、次のストラテジーのいずれかを使用します。

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

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

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

たとえば、送信キューが 1 で受信キューが 8 の場合、

$$\text{完了キュー} = 1 + 8 = 9$$

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

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

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

次に例を示します。

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

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

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

### Windows アダプタでの割り込みカウント ポリシー

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

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

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

VIC 1200 および VIC 1300 シリーズアダプタの例:

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

VIC 1400 シリーズ以降のアダプタの例 :

Tx=1、Rx=4、CQ=5、割り込み=512、RSS を有効にする

### ファイバチャネルを使用したファブリック上の NVMe

NVM Express (NVMe) インターフェイスは、不揮発性メモリサブシステムとの通信にホストソフトウェアを使用できます。このインターフェイスは、PCI Express (PCIe) インターフェイスには通常、登録レベルインターフェイスとして添付されているエンタープライズ不揮発性ストレージが最適化されます。

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

FC NVMe では、ファイバチャネルおよび NVMe の利点を組み合わせた。柔軟性と NVMe のパフォーマンスが向上し、共有ストレージアーキテクチャのスケラビリティを取得します。Cisco UCS マネージャ リリース 4.0 (2) には、UCS VIC 1400 シリーズアダプタのファイバチャネルを使用したファブリック上の NVMe がサポートされています。

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

### RDMA を使用したファブリック上の NVMe

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

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

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



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

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

## ファイバチャネルアダプタ ポリシーの作成



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

### 手順

**ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。

**ステップ 2** [サーバ] > [ポリシー]を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

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

**ステップ 5** 次のフィールドに、ポリシーの名前および説明を入力します。

表 5:

名前 (Name)	説明
[名前 (Name) ] フィールド	<p>ポリシーの名前。</p> <p>この名前には、1～16 文字の英数字を使用できます。 - (ハイフン)、_ (アンダースコア)、: (コロン)、および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。</p>
[説明 (Description) ] フィールド	<p>ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。</p> <p>256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。 ` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、&gt; (大なり)、&lt; (小なり)、または' (一重引用符) は使用できません。</p>

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

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

**ステップ7** (任意) [Options] 領域で、次の値を調整します。

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

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

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

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

名前 (Name)	説明
[vHBA Type] ラジオ ボタン	<p>このポリシーで使用される vHBA タイプ。サポートされている FC と FC NVMe Vhba は、同じアダプタでここで作成できます。このポリシーで使用される vHBA タイプには、次のいずれかを指定できます。</p> <ul style="list-style-type: none"> <li>• FC イニシエータ]: レガシー SCSI FC vHBA イニシエータ</li> <li>• FC ターゲット: SCSI FC ターゲット機能をサポートする vHBA</li> </ul> <p>(注) このオプションは、Tech Preview として利用できます。</p> <ul style="list-style-type: none"> <li>• FC NVME イニシエータ-、FC NVME イニシエータ、FC NVME ターゲットを検出し、それらに接続するは vHBA</li> <li>• FC NVME ターゲット: FC NVME ターゲットとして機能し、NVME ストレージへの接続を提供する vHBA</li> </ul> <p>(注) このオプションは、技術プレビューとして使用可能です。</p> <p>vHBA タイプは、UCS VIC 1400 アダプタ でのみサポートされています。</p>

ステップ 8 [OK] をクリックします。

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

## ファイバチャネルアダプタ ポリシーの削除

### 手順

ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。

ステップ 2 [SAN] > [ポリシー (Policies)] > [Organization\_Name] の順に展開します。

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

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

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

# デフォルトの vHBA 動作ポリシーについて

## デフォルトの vHBA 動作ポリシー

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

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

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



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

## デフォルトの vHBA 動作ポリシーの設定

### 手順

**ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。

**ステップ 2** [SAN] > [ポリシー] を展開します。

**ステップ 3** [root] ノードを展開します。

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

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

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

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



ステップ 6 [Save Changes]をクリックします。

## SPDM セキュリティ ポリシー

### SPDM セキュリティ

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



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

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

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

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

- フルセキュリティ :

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

- 部分的なセキュリティ (デフォルト):

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

- No Security

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

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

証明書は、システムのすべてのユーザー インターフェイスに一覧表示されます。

## SPDM セキュリティ ポリシーの作成

この手順では、SPDM ポリシーを作成します。



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

### 手順

- ステップ 1** [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2** [ポリシー (Policies)] に移動します。[root] ノードを展開します。
- ステップ 3** [SPDM 証明書ポリシー (SPDM Certificate Policies)] を右クリックして [SPDM ポリシー (SPDM Policies の作成)] を選択します。
- ステップ 4** このポリシーの名前を入力し、セキュリティ レベルとして [障害アラート設定 (Fault Alert Setting)] を選択します：これは [無効 (Disabled)]、[一部 (Partial)]、または [完全 (Full)] のいずれかです。  
デフォルトは [一部 (Partial)] です。
- ステップ 5** [追加 (Add)] ([ポリシーの作成 (Create Policy)] ウィンドウ) をクリックします。[SPDM 証明書の追加 (Add SPDM Certificate)] ウィンドウが開きます。
- ステップ 6** 証明書に名前を付けます。  
UCS Manager は、Pem 証明書のみをサポートします。
- ステップ 7** [証明書 (Certificate)] フィールドに証明書の内容を貼り付けます。
- ステップ 8** [OK] をクリックして証明書を追加し、[SPDM ポリシーの作成 (Create SPDM Policy)] ウィンドウに戻ります。  
最大 40 件の証明書を追加できます。

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

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

---

#### 次のタスク

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

## セキュリティ ポリシーとサーバーの関連付け

#### 始める前に

SPDM セキュリティ ポリシーの作成

#### 手順

---

ステップ1 [ナビゲーション] ペインで、[サーバ] をクリックします。

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

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

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

ステップ4 [OK] をクリックします。

SPDM ポリシーがこのサービス プロファイルに関連付けられます。

---

#### 次のタスク

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

## 障害アラート設定の表示

特定のシャーシに関連付けられている障害アラート設定を表示できます。

#### 始める前に

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

## 手順

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

**ステップ2** ラックマウント サーバーを選択します。

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

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

# SAN 接続ポリシー

## LANおよびSAN接続ポリシーの概要

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



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

## LAN および SAN の接続ポリシーに必要な権限

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

### 接続ポリシーの作成に必要な権限

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

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

### 接続ポリシーをサービス プロファイルに追加するために必要な権限

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

## サービス プロファイルと接続ポリシー間の相互作用

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

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

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

## SAN 接続ポリシーの作成

### 手順

- ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2** [SAN] > [ポリシー] を展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** [SAN Connectivity Policies] を右クリックし、[Create SAN Connectivity Policy] を選択します。
- ステップ 5** [Create SAN Connectivity Policy] ダイアログボックスで、名前と任意の説明を入力します。
- ステップ 6** [World Wide Node Name] 領域の [WWNN Assignment] ドロップダウン リストから次のいずれかを選択します。
  - デフォルトの WWN プールを使用するには、 を選択します。
  - [Manual Using OUI] に一覧表示されるオプションのいずれかを選択し、[World Wide Node Name] フィールドに WWN を入力します。

WWNN は、20:00:00:00:00:00:00:00 ~ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ~ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。[here] リンクをクリックして、指定した WWNN が使用可能であることを確認できます。

- 指定したプールから WWN を割り当てるには、リストから WWN プール名を選択します。各プール名の後には、プール内で利用可能な WWN の数および WWN の合計数を示す、括弧に囲まれた 2 つの数字が表示されます。

- ステップ 7** [vHBAs] テーブルで、[Add] をクリックします。
- ステップ 8** [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。
- ステップ 9** [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。  
この領域から VSAN または SAN ピン グループを作成することもできます。
- ステップ 10** [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
- ステップ 11** [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。  
この領域からファイバチャネルアダプタ ポリシーまたは QoS ポリシーを作成することもできます。
- ステップ 12** ポリシーに必要なすべての vHBA を作成したら、[OK] をクリックします。

### 次のタスク

ポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに含めます。

## SAN 接続ポリシー用の vHBA の作成

### 手順

- ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。
- ステップ 2** [SAN] タブで、[SAN] > [Policies] > [Organization\_Name] > [San Connectivity Policies] の順に展開します。
- ステップ 3** vHBA を作成するポリシーを選択します。
- ステップ 4** [Work] ペインで、[General] タブをクリックします。
- ステップ 5** テーブル アイコン バーの [+] ボタンをクリックします。
- ステップ 6** [Create vHBAs] ダイアログボックスで、名前と説明（オプション）を入力します。
- ステップ 7** [Fabric ID]、[Select VSAN]、[Pin Group]、[Persistent Binding]、[Max Data] の順に選択します。  
この領域から VSAN または SAN ピン グループを作成することもできます。
- ステップ 8** [Operational Parameters] 領域で、[Stats Threshold Policy] を選択します。
- ステップ 9** [Adapter Performance Profile] 領域で、[Adapter Policy] と [QoS Policy] を選択します。

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

ステップ 10 [Save Changes]をクリックします。

## SAN 接続ポリシーからの vHBA の削除

### 手順

- ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ 2 [SAN] > [ポリシー (Policies)] > [Organization Name] の順に展開します。
- ステップ 3 vHBA を削除するポリシーを選択します。
- ステップ 4 [Work] ペインで、[General] タブをクリックします。
- ステップ 5 [vHBAs] テーブルで、次の手順を実行します。
  - a) 削除する vHBA をクリックします。
  - b) アイコンバーで [Delete] をクリックします。
- ステップ 6 確認ダイアログボックスが表示されたら、[はい]をクリックします。

## SAN 接続ポリシー用のイニシエータ グループの作成

### 手順

- ステップ 1 [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ 2 [SAN] > [ポリシー (Policies)] > [Organization Name] の順に展開します。
- ステップ 3 イニシエータ グループを作成するポリシーを選択します。
- ステップ 4 [Work] ペインで、[vHBA Initiator Groups] タブをクリックします。
- ステップ 5 テーブルアイコンバーの [+] ボタンをクリックします。
- ステップ 6 [Create vHBA Initiator Group] ダイアログボックスで、次のフィールドに値を入力します。

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

名前 (Name)	説明
[Description] フィールド	<p>グループの説明。</p> <p>256文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、&gt; (大なり)、&lt; (小なり)、または' (一重引用符) は使用できません。</p>
[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	<p>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</p> <ul style="list-style-type: none"> <li>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、<b>[Global Storage Connection Policy]</b> 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。</li> </ul> <p>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、<b>[Create Storage Connection Policy]</b> リンクをクリックします。</p> <ul style="list-style-type: none"> <li>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、<b>[Specific Storage Connection Policy]</b> オプションを選択します。Cisco UCS Manager GUI に表示される<b>[Specific Storage Connection Policy]</b> 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。</li> </ul>
[Create Storage Connection Policy] リンク	すべてのサービス プロファイルとサービス プロファイル テンプレートで使用可能な新しいストレージ接続ポリシーを作成するには、このリンクをクリックします。

ステップ7 [OK] をクリックします。

## SAN 接続ポリシーからのイニシエータ グループの削除

### 手順

ステップ1 [ナビゲーション]ペインで、[SAN]をクリックします。

ステップ2 [SAN] > [ポリシー (Policies)] > [Organization\_Name] の順に展開します。



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

## SAN 接続ポリシーの削除

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

### 手順

- ステップ1** [ナビゲーション]ペインで、[SAN]をクリックします。
- ステップ2** [SAN] > [ポリシー (Policies)] > [Organization Name] の順に展開します。
- ステップ3** [SAN Connectivity Policies] ノードを展開します。
- ステップ4** 削除するポリシーを右クリックし、[Delete] を選択します。
- ステップ5** 確認ダイアログボックスが表示されたら、[はい]をクリックします。

## Intel® ボリューム管理デバイスの有効化

### ボリューム管理デバイス (VMD) の設定

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

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

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

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

## UCS Manager での VMD の有効化

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



(注) OS をインストールする前に、VMD を有効にする必要があります。

### 手順

- ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ 2 ポリシーを作成する組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 3 VMD の BIOS ポリシーの設定：サービス プロファイルを選択し、[ポリシー (Policies)] タブに移動します。[ポリシー (Policies)] セクションで、BIOS セクションを右クリックして、ポップアップから [BIOSポリシーの作成 (Create BIOS Policy)] を選択します。[BIOS ポリシー (BIOS Policy)] フォームに名前と説明(任意)を入力します。[OK] をクリックしてポリシーを作成します。
- ステップ 4 [ポリシー (Policies)] > [ルート (Root)] > [BIOS ポリシー (BIOS Policies):] に移動し、新しいポリシーを選択します。
- ステップ 5 [BIOS ポリシー (BIOS Policies)] を展開し、サブメニューから [アドバンスド (Advanced)] および [LOM および PCIe スロット (LOM and PCIe Slots)] を選択します。
- ステップ 6 [VMD の有効化 (VMD enable)] まで下にスクロールし、[有効 (enable)] を選択します。
- ステップ 7 [保存を変更 (Save Changes)] をクリックして、VMD 機能を有効にします。
- ステップ 8 [ブート ポリシー (Boot Policy)] タブで、ローカルブートポリシーを作成します。ブートモードとして [Uefi] を選択し、[ローカル デバイス (Local Devices)] メニューから NVMe を追加します。[変更の保存 (Save Changes)] をクリックし、ポリシーの変更内容を保存します。

# パススルー モードでボリューム管理デバイス (VMD) 有効化

## ボリューム管理デバイス (VMD) パススルーモード

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

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



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

## VMD パススルーの設定

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

### 手順

- ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2 ポリシーを作成する組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 3 VMD の BIOS ポリシーの設定：サービス プロファイルを選択し、[ポリシー (Policies)] タブに移動します。[ポリシー (Policies)] セクションで、BIOS セクションを右クリックして、ポップアップから [BIOS ポリシーの作成 (Create BIOS Policy)] を選択します。[BIOS ポリシー (BIOS Policy)] フォームに名前と説明 (任意) を入力します。[OK] をクリックしてポリシーを作成します。
- ステップ 4 [ポリシー (Policies)] > [ルート (Root)] > [BIOS ポリシー (BIOS Policies):] に移動し、新しいポリシーを選択します。
- ステップ 5 [BIOS ポリシー (BIOS Policies)] を展開し、サブメニューから [アドバンスド (Advanced)] および [LOM および PCIe スロット (LOM and PCIe Slots)] を選択します。
- ステップ 6 [VMD の有効化 (VMD enable)] まで下にスクロールし、[有効 (enable)] を選択します。
- ステップ 7 [保存を変更 (Save Changes)] をクリックして、VMD 機能を有効にします。

- ステップ 8** VMD パススルーモードの有効化を完了するには、サブメニューから **[アドバンスド (Advanced)]** および **[Intel Directed IO]** を選択し、**[Intel VT Directed IO]** までスクロールダウンします。ドロップダウンが **[有効 (Enabled)]** に設定されていることを確認します。そうでない場合は、設定します。
- ステップ 9** **[変更を保存 (Save Changes)]** をクリックして、VMD パススルー ポリシーを有効にします。
- ステップ 10** **[ブートポリシー (Boot Policy)]** タブで、ローカルブートポリシーを作成します。**[ブートモード (Boot Mode)]** の **[Uefi]** を選択します。**[OK]** をクリックしてポリシーを作成します。

## VMD ドライバのダウンロード

### Intel® ボリューム管理デバイス ドライバ

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

- Linux
- Windows 2016、2019
- VMWare



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

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

- Red Hat Linux
- Ubuntu

Intel VMD の機能を使用するには、次のことを行う必要があります。

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



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

- 適切な VMD NVMe ドライバをインストールします。

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

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

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

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

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

Intel VRoC を使用するには、次のことを行う必要があります。

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

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

## Linux VMD ドライバのダウンロード

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

### 始める前に

BIOS 設定で VMD が有効になっていることを確認してください。



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

### 手順

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

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

### 次のタスク

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

## Windows VMD ドライバのダウンロード

ドライババンドルをダウンロードするには、次の手順を実行します。

### 始める前に

BIOS 設定で VMD が有効になっていることを確認してください。



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

### 手順

- ステップ 1** Web ブラウザで、<https://software.cisco.com/download/home>を開きます。
- ステップ 2** プラットフォームに応じて、**UCS B シリーズ ブレードサーバソフトウェア**または**UCS C シリーズ ラックマウント UCS 管理対象サーバソフトウェア**を検索します。

- ステップ 3** ソフトウェア タイプの選択から UCS ドライバを選択します。ユニファイド コンピューティング システム (UCS) ドライバ。
- ステップ 4** 左のパネルの最新リリースをクリックします。  
VMD の ISO イメージは、4.0 (4f) リリース以降で使用できます。
- ステップ 5** [UCS 関連の windows ドライバの ISO イメージのみ (ISO image of UCS-related windows drivers only)] をクリックして、ドライババンドルをダウンロードします。
- ステップ 6** ドライババンドルがダウンロードされたら、それを開き、[ストレージ (Storage)] > [Intel] > [VMD] > [KIT\_x\_x\_x\_xxxx] を選択します。
- ステップ 7** フォルダのコンテンツを展開します。
- ステップ 8** キットと [キット (KIT)] > [インストール (Install)] のエントリをクリックします。
- ステップ 9** このフォルダには、ドライバパッケージと関連資料の両方が含まれています。  
**VROC\_x\_x\_x\_xxxxInstall** の zip ファイルを展開します。
- ステップ 10** ドライバとともにパッケージ化されたインストール手順に従います。

---

#### 次のタスク

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

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

## VMD パススルー ドライバのダウンロード

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



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

#### 始める前に



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

## 手順

- 
- ステップ 1** Web ブラウザで、<https://software.cisco.com/download/home>を開きます。
- ステップ 2** サーバ・ユニファイド コンピューティングの検索
- ステップ 3** プラットフォームに応じて、**UCS B シリーズ ブレード サーバ ソフトウェア**または **UCS C シリーズ ラックマウント UCS 管理対象サーバ ソフトウェア**を検索します。
- ステップ 4** ソフトウェア タイプの選択から UCS ユーティリティを選択します。ユニファイド コンピューティング システム (UCS) ユーティリティ。
- ステップ 5** 左のパネルの最新リリースをクリックします。

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

- ステップ 6** [UCS 関連の vmware ユーティリティの ISO イメージのみ (ISO image of UCS-related vmware utilities only)] をクリックして、ユーティリティバンドルをダウンロードします。
- ステップ 7** ドライババンドルがダウンロードされたら、それを開き、[ストレージ (Storage)] > [Intel] > [VMD] を選択します。

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

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

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

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

## 次のタスク

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

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

## NVMe の高度な VMD 搭載したカスタム LED のステータス

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



## LED の点滅

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

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

### ドライブ ホットプラグ時の LED の動作

NVMe を持つ VMD は、突然のホットプラグをサポートします。ディスクがホット解除され、同じスロットに再装着されると、障害 LED が 10 秒間点滅します。これは予期される動作です。ドライブが取り外されたときに、スロットの LED が障害状態を示されますが、バックプレーンでは LED が点滅可能になるように、ドライブがスロットに存在する必要があります。したがって、障害状態はドライブが取り外された後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 6: 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。	<p>障害パターンは、次の場合に表示されます。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul> <p>デフォルト = オプション 1</p>
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。	<p>デフォルト = 有効</p> <p>次のように設定できます。</p> <ol style="list-style-type: none"> <li>1. 無効 (1 台のドライブのみ)</li> <li>2. 有効 (すべてのドライブ)</li> </ol>
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 7: 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 <b>BLACKLIST</b>	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 <b>BLINK_ON_INIT</b>	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) <b>REBUILD_BLINK_ON_ALL</b>	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 <b>BLINK_ON_MIGR</b>	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 <b>log_level</b>	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 <b>RAID_MEMBERS_ONLY</b>	フラグが ledmon (true) に設定されている場合、RAID メンバであるドライブにのみモニタリングを制限します。	1. False/ (すべての RAID メンバと PT) 2. True/(RAID メンバのみ) デフォルト = False
特定のコントローラのみ限定されたスキャン <b>WHITELIST</b>	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 8: 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。



## 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 \(113 ページ\)](#)
- [コントローラとディスクのセキュリティ フラグ \(114 ページ\)](#)
- [ローカルセキュリティ ポリシーの管理 \(115 ページ\)](#)
- [KMIP クライアント証明書ポリシー \(117 ページ\)](#)
- [リモートセキュリティ ポリシーの管理 \(119 ページ\)](#)
- [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 \(121 ページ\)](#)
- [コントローラのセキュリティのディセーブル化 \(122 ページ\)](#)
- [ロックされたディスクのロックの解除 \(123 ページ\)](#)
- [セキュア外部設定ディスクの消去 \(123 ページ\)](#)
- [データを安全に削除する \(124 ページ\)](#)

## 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 シリーズと B-シリーズ M5 サーバ、および S シリーズのサーバの SED セキュリティ ポリシーをサポートしています。

SED は、セキュリティ キーを指定してロックしなければなりません。このセキュリティ キーはキー暗号化キーまたは認証パスフレーズとも呼ばれ、メディア暗号化キーの暗号化に使用されます。ディスクがロックされていない場合は、データの取得にキーは必要ありません。

Cisco UCS Manager では、セキュリティ キーをローカルでも、リモートからでも設定できます。ローカルでキーを設定した場合、そのキーを覚えておく必要があります。キーを忘れた場合、それを取得することはできず、データが失われます。キー管理サーバ (KMIP サーバとも呼ばれる) を使用すると、リモートでキーを設定できます。この方法により、ローカル管理でのキーの保管と取得に伴う問題に対処することができます。

SEDの暗号化と復号化はハードウェアを介して行われます。したがって、システムの全体的なパフォーマンスには影響がありません。SEDは、瞬間的な暗号化消去によってディスクの廃止コストや再配置コストを削減します。暗号化消去は、メディア暗号キーを変更することによって実行されます。ディスクのメディア暗号キーが変更されると、そのディスク上のデータは復号不能になるので、ただちにデータが使用不可になります。Cisco UCS Manager リリース 3.1(3) では、SED は C シリーズ サーバと S シリーズ サーバにディスク盗難防止機能を提供します。HX サーバについては、SED はノード盗難防止機能を提供します。Cisco UCS Manager リリース 4.0(2) では、UCS B シリーズ M5 サーバに SED セキュリティ ポリシーを拡張します。

## コントローラとディスクのセキュリティ フラグ

セキュリティ フラグは、ストレージ コントローラとディスクの現在のセキュリティ ステータスを示します。

ストレージ コントローラとディスクには、次のセキュリティ フラグがあります。

- **Security Capable** : コントローラまたはディスクが SED 管理をサポートできることを示します。
- **Security Enable** : コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティがデバイス上で有効であることを示します。このフラグは、セキュリティ ポリシーを設定してサーバに関連付け、コントローラとディスクを保護しているときに設定されます。HX デバイスでは、このフラグは設定されません。
- **Secured** : コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティが HX デバイス上で有効であることを示します。

次のセキュリティ フラグは、ストレージ ディスクにのみ適用されます。

- **Locked** : ディスク キーがコントローラ上のキーと一致していないことを示します。これは、異なるキーでプログラムされたサーバ間でディスクを移動すると発生します。ロックされたディスク上のデータにはアクセスできないため、オペレーティングシステムがディスクを使用できません。このディスクを使用するには、ディスクのロックを解除するか、または外部設定を安全に消去します。
- **Foreign Secured** : セキュア ディスクは外部設定になっていることを示します。正しいキーでロックされたディスクのロックを解除しても、ディスクが外部設定状態になっており、そのディスク上のデータが暗号化されているとこのようになります。このディスクを使用するには、外部設定をインポートするか、または外部設定をクリアします。

# 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** [ナビゲーション]ペインで、[機器]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 (Name)	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。

名前 (Name)	説明
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 文字以下で入力します。
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 文字以下で入力します。
組織名	証明書を要求している組織。 32 文字以下で入力します。
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 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 の C シリーズおよび S シリーズ サーバでは、展開機器 > ラック マウント > サーバの > サーバの ID。
- ステップ 3 B シリーズ サーバ展開機器 > シャーシ > シャーシ ID > サーバ > サーバ ID
- 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 [Security] サブタブをクリックします。
- ステップ 6 [Create KMIP Client Cert Policy] をクリックします。
- ステップ 7 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 (Name)	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 文字以下で入力します。
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 文字以下で入力します。
組織名	証明書を要求している組織。 32 文字以下で入力します。
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 8 [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 の C シリーズおよび S シリーズ サーバでは、展開機器 > ラック マウント > サーバの > サーバの ID。

ステップ 3 B シリーズ サーバ展開機器 > シャーシ > シャーシ ID > サーバ > サーバ ID

ステップ 4 [Work] 領域の [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 [Controllers] タブで、SAS コントローラを選択します。

ステップ 7 [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** の C シリーズおよび S シリーズ サーバでは、展開機器 > ラック マウント > サーバの > サーバの ID。
- ステップ 3** B シリーズ サーバ展開機器 > シャーシ > シャーシ ID > サーバ > サーバ ID
- ステップ 4** [Work] 領域の [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** [Disks] タブで、ディスクを選択します。
- ステップ 7** [Details] 領域で、[Enable Encryption] をクリックします。
- ステップ 8** 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** の C シリーズおよび S シリーズ サーバでは、展開機器 > ラック マウント > サーバの > サーバの ID。
- ステップ 3** B シリーズ サーバ展開機器 > シャーシ > シャーシ ID > サーバ > サーバ ID
- ステップ 4** [Work] 領域の [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** [Controllers] タブで、SAS コントローラを選択します。
- ステップ 7** [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 の C シリーズおよび S シリーズ サーバでは、展開機器 > ラック マウント > サーバの > サーバの ID。

ステップ3 B シリーズ サーバ展開機器 > シャーシ > シャーシ ID > サーバ > サーバ ID

ステップ4 [Work] 領域の [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 [Disks] タブで、ディスクを選択します。

ステップ7 [General] タブで、[Secure Erase Foreign Configuration] をクリックします。

## データを安全に削除する

委員会規制 (EU) 2019/424 は、データを安全に処分することを要求しています。

データの安全な廃棄は、Cisco UCS サーバのさまざまなドライブ、メモリ、およびストレージからデータを消去し、工場出荷時の設定にリセットするための、一般的なツールを使用することによって可能になります。

委員会規制 (EU) 2019/424 に準拠するためのデータの安全な削除は、次の Cisco UCS サーバでサポートされています。

- Cisco UCS B200
- Cisco UCS B480
- Cisco UCS C125
- Cisco UCS C220
- Cisco UCS C240
- Cisco UCS C480
- Cisco UCS S3260

安全にデータを削除するため、UCS サーバに取り付けられているデバイスについて十分に理解し、適切なツールを実行する必要があります。場合によっては、複数のツールを実行する必要がある場合があります。

データを安全に消去する方法の詳細については、<https://www.cisco.com/web/dofc/18794277.pdf> を参照してください。





## 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 \(125 ページ\)](#)
- [Cisco ブート最適化 M.2 RAID コントローラ \(126 ページ\)](#)
- [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 \(127 ページ\)](#)
- [RAID レベル \(133 ページ\)](#)
- [自動ディスク 選択 \(135 ページ\)](#)
- [サポートされている LUN の変更 \(136 ページ\)](#)
- [サポートされていない LUN の変更 \(136 ページ\)](#)
- [ディスク 挿入の処理 \(137 ページ\)](#)
- [仮想ドライブの命名 \(139 ページ\)](#)
- [LUN の参照解除 \(139 ページ\)](#)
- [コントローラの制限と制約事項 \(140 ページ\)](#)
- [ストレージ プロファイル \(143 ページ\)](#)
- [ストレージ プロファイルの設定 \(176 ページ\)](#)

## 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。

## Cisco ブート最適化 M.2 RAID コントローラ

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

- Cisco UCS C225 M6サーバ
- Cisco UCS C245 M6サーバ
- Cisco UCS C220 M6サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS B200 M5 サーバ
- Cisco UCS B480 M5 サーバ

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

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

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

### Cisco ブート最適化 M.2 Raid コントローラの制限

- 既存の LUN の移行はサポートされていません。
- ローカル ディスク設定ポリシーはサポートされていません。
- 1つの LUN を作成するとディスク容量をすべて使用するため、作成できる LUN の数は1つに制限されます。
- Lun は、ストレージ プロファイルの下での **[Local LUN (ローカル LUN)]** タブ (**ローカル LUN の設定 (145 ページ)** を参照) を使用して作成され、コントローラ定義を使用しません。
- 異なる容量の2台のドライブを混在させることはできません。

- ブレードまたはラック サーバー上の孤立した仮想ドライブの名前を変更することはできません。

## ディスク グループおよびディスク グループ設定ポリシー

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は「ディスク グループ」と呼ばれます。ディスク グループを使用すれば、ローカルディスクを整理できます。ストレージ コントローラは、ディスク グループの作成と設定を制御します。

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

ホット スペアとは、ディスク グループに含まれるディスクで障害が発生した場合にディスク グループで使用できる、未使用の予備ディスクのことです。ホットスペアを使用できるのは、フォールトトレラント 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

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

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



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

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

### 展開状態

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

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

### 動作状態

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

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



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

- [Partially degraded] : RAID 6 仮想ドライブの動作状態が最適ではありません。設定されたドライブのいずれかに障害が発生したか、オフラインの状態です。RAID 6 は、最大 2 件のドライブ障害を許容できます。

- [オフライン (Offline)] : 仮想ドライブが、RAID コントローラで使用できません。これは実質的に障害状態です。
- [不明 (Unknown)] : 仮想ドライブの状態は不明です。

### プレゼンス状態

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

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

## 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** [ナビゲーション (Navigation)] ペインで、[ストレージ (Storage)] をクリックします。
- ステップ 2** [ストレージ (Storage)] > [ストレージ プロビジョニング (Storage Provisioning)] > [ストレージ ポリシー (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 (Name)	説明
[名前 (Name)] フィールド	ポリシーの名前  この名前には、1～16 文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、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)、^ (caret)、" (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。

名前 (Name)	説明
[RAID Level] ドロップダウンリスト	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>[RAID 0 Striped]</b></li> <li>• <b>[RAID 1 Mirrored]</b></li> </ul> <p><b>Note</b> Cisco ブート最適化 M. 2 RAID コントローラ (UCS-M2-HWRAID) は、RAID1 のみをサポートしません。</p> <ul style="list-style-type: none"> <li>• <b>[RAID 5 Striped Parity]</b></li> <li>• <b>[RAID 6 Striped Dual Parity]</b></li> <li>• <b>RAID 10 Mirrored and Striped</b></li> </ul> <p><b>Note</b> RAID1 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。</p>

**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。

**Note** Cisco ブート最適化 M. 2 Raid コントローラ (HWRAID) を設定している場合は、[ステップ 7, on page 131](#) に進みます。

名前 (Name)	説明
[Number of drives] フィールド	<p>ディスク グループのドライブの数を指定します。</p> <p>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。</p>
[Drive Type] フィールド	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>HDD</b></li> <li>• <b>SSD</b></li> <li>• <b>[Unspecified]</b></li> </ul> <p>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。</p>

名前 (Name)	説明
[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。

- テーブル右側のアイコン バーにある [+] をクリックします。
- [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 (Name)	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。 <b>Note</b> M.2 ドライブには通常スロット ID = 253、254があります。 さらに、[Equipment (機器)] > [Server (サーバ)]/[servernumber (サーバ番号)] > ([Inventory (インベントリ)] > [Storage (ストレージ)] > [Disks (ディスク)] に移動して、スロット ID を確認します。
[Role] フィールド	<b>Note</b> Cisco ブート最適化 M.2 Raid コントローラ (UCS-M2-HWRAID) を設定している場合は、[Normal (標準)] を選択します (デフォルト)。他の値を選択すると、設定エラーになります。 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。 <ul style="list-style-type: none"> <li>標準</li> <li>[Dedicated Hot Spare]</li> <li>グローバル ホット スペア</li> </ul>

名前 (Name)	説明
[Span ID] フィールド	<p><b>Note</b> Cisco ブート最適化 M. 2 Raid コントローラ (UCS-M2-HWRAID) を設定している場合は、このフィールドは適用されません。  <b>[SPAN ID (範囲 ID)]</b> フィールドは <b>[unspecified (未指定)]</b> のままにします。いずれかの値を選択すると、設定エラーになります。</p> <p>ディスクが属しているスパングループの ID を指定します。単一のスパングループに属している複数のディスクは、大容量の単一ディスクとして扱うことができます。値の範囲は 0 ~ 8 です。RAID-10、RAID-50、および RAID-60 の場合、最小 2 スパンが必要で、最大 8 スパンがサポートされません。スパニング情報が必要ない場合は、スパン識別子を <b>Unspecified</b> として設定することもできます。</p>

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

- Note** Cisco ブート最適化 M. 2 Raid コントローラ (HWRAID) を設定している場合は、次のようになります。
- 作成できる仮想ドライブは 1 つのみです。
  - **ストリップ サイズ (KB)** には、**64 KB** または **32KB** を選択します。他の値を選択すると、設定エラーになります。
  - **アクセスポリシー、読み取りポリシー、書き込みキャッシュポリシー、IO ポリシー、およびドライブキャッシュ** の場合は、**[Platform Default (プラットフォームデフォルト)]** を選択します。他の値を選択すると、設定エラーになります。

名前 (Name)	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。 <ul style="list-style-type: none"> <li>• <b>Platform Default</b></li> <li>• <b>[Read Write]</b></li> <li>• <b>[Read Only]</b></li> <li>• <b>ブロック</b></li> </ul>
[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。 <ul style="list-style-type: none"> <li>• <b>Platform Default</b></li> <li>• <b>[Read Ahead]</b></li> <li>• <b>[Normal]</b></li> </ul>



名前 (Name)	説明
[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。 <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [Write Through]</li> <li>• [Write Back Good Bbu]</li> <li>• [Always Write Back]</li> </ul>
[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。 <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• 直接</li> <li>• Cached</li> </ul>
[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。 <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [No Change]</li> <li>• 有効化</li> <li>• 無効化</li> </ul>

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むことで、データの冗長性を確保します。
- パリティ：デバイスで障害が発生した場合にエラーを修正できるよう、追加のデバイスに冗長データを保管します。パリティによって完全な冗長性が実現されることはありませんが、シナリオによってはエラー リカバリが可能になります。
- スパニング：複数のドライブを1つの大容量ドライブとして使用できます。たとえば、4台の20 GB ドライブを結合して、1台の80 GB ドライブのように扱うことができます。

サポートされている RAID レベルは次のとおりです。

- RAID 0 ストライピング：データはアレイのすべてのディスクにストライピングされ、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 デュアルパリティ付きストライピング：データをアレイのすべてのディスクにストライピングし、2つのパリティデータセットを使用することで、最大2台の物理ディスクを障害から保護します。データブロックの各行に、2セットのパリティデータが格納されます。

2つ目のパリティブロックが追加される点を除けば、RAID 6はRAID 5と同じ機能です。RAID 6には4台以上のディスクが必要です。

- RAID 10 ミラーリングおよびストライピング：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いスループット 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 データ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 グループ構成を指定して、そのディスク グループに含まれるローカル ディスクを指定しないと、Cisco UCS Manager はディスク グループ構成ポリシーで指定された基準に従って、使用するディスクを決定します。この場合、Cisco UCS Manager は複数の方法でディスクを選択できます。

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

ディスク選択プロセスは次のとおりです。

1. 新しい仮想ドライブの作成が必要なすべてのローカル LUN について処理が繰り返されません。繰り返し処理は、次の基準に、記載する順に従います。
  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せん。そうでない場合は、展開する新しいディスクの検索を試みます。

## サポートされている LUN の変更

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

次のタイプの変更を行うことができます。

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

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

## サポートされていない LUN の変更

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

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

- 再構成を通して可能となる、サポートされている任意の RAID レベルの変更。たとえば、RAID0 から RAID1 への変更。
- 再構成を通じた仮想ドライブのサイズ増加。
- 再構成を通じ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。
- 仮想ドライブのサイズ縮小。
- 同じドライブグループに他の仮想ドライブが存在する状況における、再構成をサポートする RAID レベルの変更。
- ディスク グループに仮想ドライブを収容するだけのスペースが残っていない場合のディスクの削除。

- 仮想ドライブで使用しているディスク セットの明示的変更。

## ディスク挿入の処理

次の一連のイベントが発生する場合があります。

1. LUN が、次のいずれかの方法で作成されます。
  1. ユーザがローカル ディスク参照を使用して、明示的にスロットを指定します。
  2. ユーザが指定した基準に従って、システムがスロットを選択します。
2. LUNが正常に展開されます。つまり、そのスロットを使用する仮想ドライブが作成されま
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 \(137 ページ\)](#)
- [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 \(137 ページ\)](#)
- [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 \(138 ページ\)](#)
- [ホット スペア ドライブの交換 \(138 ページ\)](#)
- [未使用スロットへの物理ドライブの挿入 \(138 ページ\)](#)

## 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せん。

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、ブレードまたはラックサーバの孤立した仮想ドライブの名前は、変更することができます。



---

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

---

## LUN の参照解除

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

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

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

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

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

## コントローラの制限と制約事項

- 次の表は、サーバーでサポートされる最大仮想ドライブ数を示しています。

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



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

- 次の表は、次の Cisco UCS C225 M6サーバーでサポートされるストレージコントローラの最大数を示しています。



表 9: サポートされるストレージコントローラの最大数: Cisco UCS C225 M6サーバ

サーバー/ストレージコントローラ	最大仮想ドライブ数
Cisco UCS C225 M6サーバ	<ul style="list-style-type: none"> <li>• C225-SFF の UCS C225 M6SX および UCS C245 M6SX (10 前面 SAS/SATA ドライブ)</li> <li>• UCS-M2-HWRAID 上の 2 台の M.2 2280 ドライブ</li> <li>• 直接接続された NVMe ドライブ (前面に 10 台の NVMe ドライブ)</li> </ul>

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

表 10: サポートされるストレージコントローラの最大数: Cisco UCS C245 M6サーバ

サーバー/ストレージコントローラ	最大仮想ドライブ数
Cisco UCS C245 M6サーバ	<ul style="list-style-type: none"> <li>• デュアル UCS C245 M6 SX 16 SAS/SATA HDD</li> <li>• UCS C245 M6SX プラス 28 SAS/SATA HDD</li> <li>• UCS-M2-HWRAID 上の 2 台の M.2 2280 ドライブ</li> <li>• リア ライザーに直接接続された NVMe (最大 4 台の NVMe SSD)</li> </ul>

- 次の表は、Cisco UCS C225 M6サーバのストレージドライブでサポートされているコントローラとドライバの構成を示しています。

	ストレージコントローラ	フロント ケージ サポート			シングル CPU
		NVMe ドライブの台数	NVMe ドライブの接続		
C225-SFF (10 フロント)	C225-SFF の UCS C225 M6SX または UCS C245 M6SX	最大 10	最大 4	PCIe Gen4 x2	10 SAS

	ストレージコントローラ	フロント ケージ サポート			シングル CPU
C225-NVMe (10 フロント)	CPU へ直接接続	未サポート	最大 10	PCIe Gen4 x2	10 NVMe

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

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

- Cisco UCS Manager リリース 2.2(4) では、ブロック サイズが 4K のドライブはブレードサーバではサポートされませんが、ラックマウントサーバではサポートされます。ブロック サイズが 4K のドライブをブレードサーバに挿入した場合、検出に失敗し、「Unable to get Scsi Device Information from the system」というエラーメッセージが表示されます。
- Cisco UCS Manager リリース 3.1(2) 以降のリリースでは、C240 M4、M5、および M6 サーバでアウト オブ バンド インベントリ (OOB) をサポートしていない RAID コントローラの場合、動作状態として NA、ドライブ状態として Unknown が表示されます。

# ストレージ プロファイル

## 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 [ナビゲーション (Navigation) ] ペインで、[ストレージ (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 145](#)」を参照してください。
- ステップ 7 (Optional) [LUN Set] 領域で、[LUN Set] を作成し、このストレージ プロファイルにそれらを追加します。  
詳細については、「[LUN 設定の作成, on page 149](#)」を参照してください。
- ステップ 8 [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 160](#)」を参照してください。
- ステップ 9 [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 115](#)および[リモートセキュリティ ポリシーの作成, on page 119](#)を参照してください。

**ステップ 10** [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** [サーバ] > [サービスプロファイル] を展開します。
- 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、[はい] 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** [ナビゲーション (Navigation) ] ペインで、[ストレージ (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 [ナビゲーション (Navigation) ] ペインで、[ストレージ (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 (Name)	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	<p>ローカル LUN の名前。</p> <p>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。</p> <p><b>Note</b>      <b>ローカル LUN 要求の準備 (Prepare Claim Local LUN)</b> で指定された名前が要求される名前と異なる場合、この LUN 名と LUN プロパティに表示される仮想ドライブ名は異なります。</p>

名前 (Name)	説明
[Size (GB)] フィールド	この LUN のサイズ (GB 単位)。  <b>Note</b> 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。  <b>Note</b> Cisco ブート最適化 M. 2 Raid コントローラを使用したセットアップでは、このフィールドはグレー表示されません。ただし、このフィールドに入力する必要はありません。システムは、指定されたサイズに関係なく、フルディスク容量を使用して LUN を作成します。
[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。  • <b>[Auto Deploy]</b> : ローカル LUN を自動展開します。  • <b>[No Auto Deploy]</b> : 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 [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2 [サーバ] > [サービス プロファイル] を展開します。
- ステップ 3 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 [作業 (Work)] ペインで、[ストレージ (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。
  - [Applied] : 管理状態は [Online] です。LUN はサーバに関連付けられていて、仮想ドライブが作成されました。
  - [Apply Failed] : 管理状態は [Online] です。LUN はサーバに関連付けられていますが、仮想ドライブの作成が失敗しました。
  - [Not Applied] : LUN がサーバに関連付けられていないか、サーバに関連付けられていても、管理状態が [Undeployed] になっています。
- [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 [ナビゲーション (Navigation) ] ペインで、[ストレージ (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 [はい (Yes) ] をクリックします。
- 

## LUN の設定

### LUN 設定

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

LUN 設定の作成中には次のガイドラインを考慮する必要があります。

- ディスクの唯一の SSD および HDD タイプを使用できます。
- 最大 60 ディスクを 1 つの範囲内で使用できます。
- 2 つの異なる LUN の設定の構成での範囲内でのディスクの同じセットを追加することはできません。
- ディスク スロットの範囲の LUN 設定のディスクが設定されているかどうかは、同じストレージポリシーでローカル LUN 設定で設定された同じディスクを設定することはできません。同様に、ローカル LUN 設定では、ディスクが設定されている場合は、同じディスクで、ディスク スロットの範囲の LUN セットを使用できません。
- LUN の設定が設定されている、サーバは、OOB ストレージの操作をサポートする必要があります。



- 同じサービス プロファイルのストレージポリシーとローカルディスク ポリシーを設定することはできません。
- ローカル LUN および LUN の設定に同じ名前を持つことはできません。
- S シリーズ サーバ PCH コントローラでスロット 201 および 202 はサポートされません LUN の設定。

### LUN セットの制限事項

Cisco UCS Manager LUN の設定を次の制限があります。

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

## LUN 設定の作成

[Navigation] ペインの [Storage] タブからストレージ プロファイル ポリシーに LUN 設定を作成できます。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 LUN 設定を作成することもできます。

### Before you begin

LUN の設定の作成に使用するしようとしているディスクのセットが **UnConfigured Good** または **JBOD** ドライブの状態であることを確認します。



**Note** ディスク ドライブの状態を **JBOD** 状態の場合は、スロットの範囲内で同じディスクを使用するかどうかデータ損失を発生可能性があります。

### Procedure

- ステップ 1 [ナビゲーション (Navigation) ] ペインで、[ストレージ (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 LUN 設定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 LUN Set] をクリックします。
- ステップ 6 [Create LUN Set] ダイアログボックスで、以下のフィールドに入力します。

名前 (Name)	説明
[名前 (Name) ] フィールド	LUN 設定の名前。 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。
RAID レベルオプション	現在Cisco UCS Manager <b>RAID 0</b> ストライピングオプションのみをサポートしています。
ディスク スロット範囲() フィールド	ディスクのスロット範囲。
[Strip Size (KB)] ドロップダウンリスト	ストライプ仮想ドライブの場合は、各物理ディスクにあるストライプデータセグメントの部分。  <ul style="list-style-type: none"> <li>• [Platform Default]</li> <li>• 8 KB</li> <li>• 16 KB</li> <li>• 32KB</li> <li>• 64 KB</li> <li>• 128 KB</li> <li>• 256 KB</li> <li>• 512 KB</li> <li>• 1024 KB</li> </ul>
[Access Policy] オプション	許可されたアクセスのタイプ。次のいずれかになります。  <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [Read Write]</li> <li>• 読み取り専用</li> <li>• ブロック</li> </ul>

名前 (Name)	説明
読み取りポリシーオプション	<p>先行読み出しキャッシュ モード。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [Read Ahead]</li> <li>• [Normal]</li> </ul>
[Write Cache Policy] オプション	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [Write Through]</li> <li>• [Write Back Good Bbu]</li> <li>• [Always Write Back]</li> </ul>
IO ポリシーオプション	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• 直接</li> <li>• Cached</li> </ul>
ドライブ キャッシュオプション	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [No Change]</li> <li>• 有効</li> <li>• 無効</li> </ul>
[Security] チェックボックス	<p>仮想ドライブを保護するには、このチェックボックスをオンにします。</p>

ステップ 7 [OK] をクリックします。

## LUN セットの詳細の表示

### 手順

ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。

ステップ 2 [サーバ] > [サービスプロファイル] を展開します。

- ステップ 3** 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** [作業 (Work) ] ペインで、[ストレージ (Storage) ] タブをクリックします。
- ステップ 6** ストレージ プロファイル] サブタブをクリックし、 **LUN の設定]** 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 LUN 設定に関する次の詳細情報が表示されます。

表 11: LUN 設定

名前 (Name)	説明
[Name] カラム	LUN 設定の名前。
<b>RAID</b> レベルオプション	現在Cisco UCS Manager <b>RAID 0</b> ストライピングオプションのみをサポートしています。
ディスク スロット範囲() フィールド	ディスクのスロット範囲。

名前 (Name)	説明
[名前 (Name) ] フィールド	LUN 設定の名前。  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。
<b>RAID</b> レベルオプション	現在Cisco UCS Manager <b>RAID 0</b> ストライピングオプションのみをサポートしています。
ディスク スロット範囲() フィールド	ディスクのスロット範囲。

名前 (Name)	説明
[Strip Size (KB)] ドロップダウンリスト	<p>ストライプ仮想ドライブの場合は、各物理ディスクにあるストライプデータセグメントの部分。</p> <ul style="list-style-type: none"> <li>• [Platform Default]</li> <li>• 8 KB</li> <li>• 16 KB</li> <li>• 32KB</li> <li>• 64 KB</li> <li>• 128 KB</li> <li>• 256 KB</li> <li>• 512 KB</li> <li>• 1024 KB</li> </ul>
[Access Policy] オプション	<p>許可されたアクセスのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [Read Write]</li> <li>• 読み取り専用</li> <li>• ブロック</li> </ul>
読み取りポリシーオプション	<p>先行読み出しキャッシュ モード。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [Read Ahead]</li> <li>• [Normal]</li> </ul>
[Write Cache Policy] オプション	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [Write Through]</li> <li>• [Write Back Good Bbu]</li> <li>• [Always Write Back]</li> </ul>

名前 (Name)	説明
IO ポリシーオプション	次のいずれかになります。 <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• 直接</li> <li>• Cached</li> </ul>
ドライブ キャッシュオプション	次のいずれかになります。 <ul style="list-style-type: none"> <li>• Platform Default</li> <li>• [No Change]</li> <li>• 有効</li> <li>• 無効</li> </ul>
[Security] チェックボックス	仮想ドライブを保護するには、このチェックボックスをオンにします。

## LUN セットの削除

### 手順

- ステップ 1 [ナビゲーション (Navigation) ] ペインで、[ストレージ (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 LUN 設定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 [LUN Set] を展開し、削除する LUN 設定を選択します。
- ステップ 5 削除する LUN 設定を右クリックして、[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 [はい (Yes) ] をクリックします。

## エアロ コントローラの構成

### ストレージコントローラの自動構成モード

Cisco UCS C220M6/C240M6 C シリーズ M6 サーバーは、ダイレクトアタッチドストレージ用の PCIe SAS316 ポートストレージコントローラをサポートします。コントローラは、新しく

挿入されたディスクの状態を自動的に Unconfigured-Good の状態に移行する自動構成モードをサポートしています。

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

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

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

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

コントローラは次のモデルをサポートします。

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

以下の表は、さまざまなシナリオでの自動構成の動作を示しています。

自動構成モード	再起動/OCR	ホットプラグ	ユーザアクション
Unconfigured-Good (オフ)	<ul style="list-style-type: none"> <li>• すべての Unconfigured-Good ドライブは、Unconfigured-Good のままです。</li> <li>• 以前に構成されたすべての JBOD は JBOD のままです。</li> </ul>	<ul style="list-style-type: none"> <li>• 挿入されたドライブは Unconfigured-Good のままです。</li> <li>• 別のサーバーからの JBOD は、このコントローラで Unconfigured-Good のままです。</li> </ul>	<p>自動構成を無効にしても、既存の構成には影響しません</p> <p>すべての JBOD デバイスは、コントローラの起動後も JBOD のままです。</p> <p>Unconfigured-Good は、コントローラの起動後も unconfiguredgood のままです。</p>

自動構成モード	再起動/OCR	ホットプラグ	ユーザアクション
JBOD	<ul style="list-style-type: none"> <li>すべての Unconfigured-Good は JBOD に変換されます。</li> </ul>	新しく挿入された未構成のデバイスは、JBOD に変換されます。	<p>コントローラ上のすべての Unconfigured-Good のドライブ（ユーザーが作成したものではない）は、JBOD に変換されます。</p> <p>ユーザーが作成した Unconfigured-Good ドライブは、次の再起動まで Unconfigured-Good のままです。再起動中に、Unconfigured-Good は JBOD に変換されます。</p>
RAID0 (RAID0 ライトバック)	<ul style="list-style-type: none"> <li>すべての Unconfigured-Good は、RAID0 書き戻しに変換されます。</li> </ul>	新しく挿入された未構成のデバイスは、RAID0 書き戻しに変換されます。	<p>コントローラ上のすべての Unconfigured-Good のドライブ（ユーザーが作成したものではない）は、RAID0 書き戻しに変換されます。</p> <p>ユーザーが作成した Unconfigured-Good は、コントローラの再起動後も Unconfigured-Good のままです。</p> <p>すべての RAID0 書き戻しデバイスは、コントローラの再起動後も RAID0 書き戻しとして残ります。</p>

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



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

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

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

## 自動構成ストレージ プロファイルの作成

ストレージの自動構成 (自動構成) モード オプションは、Aero コントローラを備えた Cisco UCS M6 サーバーでのみ使用できます。

### 手順

- 
- ステップ 1** [ナビゲーション (Navigation) ] ペインで、[ストレージ (Storage) ] をクリックします。
- ステップ 2** [プロファイル (Profiles) ] に移動します。[root] ノードを展開します。
- ステップ 3** [ストレージ (Storage) ] を右クリックします。
- ステップ 4** [ストレージ プロファイルの作成 (Create Storage Profile) ] メニューで、プロファイルに名前を付けます。メニューには、[未指定 (Unspecified) ] としてマークされた自動構成モードが表示されます。
- ステップ 5** 再起動時に特定の状態を保持する自動構成モード オプションを有効にするには、[未指定 (Unspecified) ] の選択を解除し、目的の状態 ([未構成良好 (Unconfigured Good) ]、[JBOD]、または [RAID 0]) を選択します。システムの再起動時に、選択した状態が BMC にプッシュされます。
- 自動構成が [未指定 (Unspecified) ] のままになっている場合、再起動前に構成されていた状態が保持されます。
- (注) Aero コントローラが存在しない場合、サービス プロファイルの関連付けは失敗します。
- ステップ 6** [OK] をクリックします。
-

## SPDM 認証

セキュリティ プロトコルおよびデータ モデル (SPDM) は、ストレージ コントローラでの認証のために BMC によって使用されます。これには、ストレージ コントローラ ファームウェアがセキュア ブートされていることと、Slot0 に Broadcom 証明書チェーンがインストールされていることが必要です。ファームウェアの更新中、Broadcom ファームウェアは、OCR またはホストが再起動するまで、ストレージ ファームウェアの古い測定値を保持します。デバイス認証が失敗した場合、ファームウェアはインベントリ関連のコマンドのみを許可します。設定操作は実行できません。

## 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 NORAIID には適用されません。  
『UCS Manager Server Management Guide』をご覧ください。
- 内蔵 SSD ドライブでのファームウェア アップグレードのサポート。
  - M4 以前のサーバの場合、ディスク ファームウェアのアップグレードは PCH コントローラが SWRAID モードの場合にのみサポートされます。AHCI モードではサポートされていません。

- M5以降のサーバの場合、ディスクファームウェアのアップグレードはSWRAIDモードと AHCI モードの両方でサポートされます（ただしCisco UCS C125 M5 サーバ、AHCI モードのみをサポートする場合を除く）。

ストレージプロファイルポリシーで PCH コントローラの SSD を設定できます。サービスプロファイルの関連付けが解除された後でも、LUN 設定を保存する保護設定を有効または無効にすることができます。コントローラモードを選択します。PCH コントローラ コンフィギュレーションでは、RAID0 と RAID1 の2つの RAID オプションのみをサポートしています。コントローラに接続されたすべてのディスクが JBOD ディスクとして構成された AHCI モードでは、[NoRAID]設定オプションを使用してください。設定の導入は、ストレージプロファイルをサービスプロファイルへ関連付けるプロセスの一環として実行されます。

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

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

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

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



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

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

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

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

## FCH コントローラの設定

Fusion Controller Hub (FCH) SSD コントローラ定義は、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

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 (Name)	説明
[名前 (Name) ] フィールド	<p>ストレージ コントローラの名前。</p> <p>(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。</p> <p>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。</p>
[Protect Configuration] チェックボックス	<p>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。</p> <p>(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。</p>

名前 (Name)	説明
[RAID Level] ドロップダウン リスト	

名前 (Name)	説明
	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[ローカルストレージを無効にする (Disable Local Storage)]</b> : (PCH SSD コントローラ定義でサポート) このディスク ポリシー モードは、SATA AHCI コントローラを無効にします。このモードは、SATA AHCI コントローラの下にディスクが存在しない場合にのみ設定できます。このコントローラを再度有効にして、コントローラをデフォルト値(AHCI)に戻すには、<b>[RAID なし (No RAID)]</b> または <b>[ローカルストレージなし (No Local Storage)]</b> モードを選択できます。</li> <li>• <b>[No Local Storage]</b> : (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。</li> <li>• <b>[RAID 0 Striped]</b> : (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。</li> <li>• <b>[RAID 1 Mirrored]</b> : (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。</li> <li>• <b>[Any Configuration]</b> : (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。</li> <li>• <b>[No RAID]</b> : (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。<b>[No RAID]</b> 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、<b>[No RAID]</b> 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 <b>[Inventory] &gt; [Storage]</b> 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。</li> </ul> <p>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、<b>[No RAID]</b> コンフィギュレーション モードの適用</p>

名前 (Name)	説明
	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[RAID 5 Striped Parity]</b> : (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。</li> <li>• <b>[0RAID 6 Striped Dual Parity]</b>: (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。</li> <li>• <b>[RAID 10 Mirrored and Striped]</b> : (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。</li> <li>• <b>[RAID 50 Striped Parity and Striped]</b> : (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。</li> </ul>



名前 (Name)	説明
	<ul style="list-style-type: none"> <li>• [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。</li> </ul> <p>(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に関連付ける際に Cisco UCS Manager に設定エラーが表示されます。</p> <p>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。</p>

**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
- 『[Cisco UCS C220 M5 Server Installation and Service Guide](#)』の「*Installing LSI MegaSR Drivers For Windows and Linux*」セクション
- 『[Cisco UCS C240 M5 Server Installation and Service Guide](#)』の「*Installing LSI MegaSR Drivers For Windows and Linux*」セクション
- 『[Cisco UCS C480 M5 Server Installation and Service Guide](#)』の「*Installing LSI MegaSR Drivers For Windows and Linux*」セクション



(注) Cisco UCS B200 M5 サーバおよび Cisco UCS B480 M5 サーバのソフトウェア RAID ドライバのインストールについては、上記のいずれかの M5 サーバと同じ手順に従います。

## 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 (Name)	説明
[名前 (Name) ] フィールド	<p>ストレージコントローラの名前。</p> <p>(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。</p> <p>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。</p>
[Protect Configuration] チェックボックス	<p>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。</p> <p>(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。</p>

名前 (Name)	説明
[RAID Level] ドロップダウン リスト	

名前 (Name)	説明
	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[ローカル ストレージを無効にする (Disable Local Storage)]</b> : (PCH SSD コントローラ定義でサポート) このディスク ポリシー モードは、SATA AHCI コントローラを無効にします。このモードは、SATA AHCI コントローラの下にディスクが存在しない場合にのみ設定できます。このコントローラを再度有効にして、コントローラをデフォルト値(AHCI)に戻すには、<b>[RAID なし (No RAID)]</b> または <b>[ローカル ストレージなし (No Local Storage)]</b> モードを選択できます。</li> <li>• <b>[No Local Storage]</b> : (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。</li> <li>• <b>[RAID 0 Striped]</b> : (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。</li> <li>• <b>[RAID 1 Mirrored]</b> : (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。</li> <li>• <b>[Any Configuration]</b> : (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。</li> <li>• <b>[No RAID]</b> : (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。<b>[No RAID]</b> 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、<b>[No RAID]</b> 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 <b>[Inventory] &gt; [Storage]</b> 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。</li> </ul> <p>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、<b>[No RAID]</b> コンフィギュレーションモードの適用</p>

名前 (Name)	説明
	<p>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。</p> <ul style="list-style-type: none"><li>• <b>[RAID 5 Striped Parity]</b> : (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。</li><li>• <b>[0RAID 6 Striped Dual Parity]</b>: (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。</li><li>• <b>[RAID 10 Mirrored and Striped]</b> : (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。</li><li>• <b>[RAID 50 Striped Parity and Striped]</b> : (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。</li></ul>

名前 (Name)	説明
	<ul style="list-style-type: none"> <li>• [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。</li> </ul> <p>(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に関連付ける際に Cisco UCS Manager に設定エラーが表示されます。</p> <p>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。</p>

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 \(171 ページ\)](#)

**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。

## M.2 モジュールの移行

### SWRAID での M.2 モジュールの移行

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

#### 始める前に

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

#### 手順

---

**ステップ 1** サーバを正常にシャット ダウンします。

**ステップ 2** M.2 モジュールを物理的に取り外します。

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

**ステップ 3** 宛先サーバの M.2 モジュールにディスクを挿入します。

**ステップ 4** サーバの電源をオンにします。

**ステップ 5** サーバを再認識します。

---

### AHCI モードでの M.2 モジュールの移行

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

#### 始める前に

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



## 手順

---

**ステップ 1** サーバを正常にシャットダウンします。

**ステップ 2** M.2 モジュールを物理的に取り外します。

**ステップ 3** 次のいずれかを実行します。

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

**ステップ 4** 宛先サーバに M.2 モジュールを挿入します。

**ステップ 5** サーバの電源をオンにします。

**ステップ 6** サーバを再認識します。

(注) ディスクが不良である場合、サーバはディスクステータスに [Not Detected] と表示します。「[不良 M.2 ディスクの交換 \(174 ページ\)](#)」を実行して、不良ディスクを交換します。

---

## SWRAID ディスクの移行

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

### 始める前に

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

## 手順

---

**ステップ 1** サーバを正常にシャットダウンします。

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

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

**ステップ 3** 宛先サーバの M.2 モジュールにディスクを挿入します。

**ステップ 4** サーバの電源をオンにします。

**ステップ 5** サーバを再認識します。

- (注) ディスクの [Drive State] に [Online] と表示されている必要があります。ディスクが不良である場合、サーバはディスクを検出できないか、または [Drive State] に [Online] ではなく、[BAD] (または [FAILED]) と表示されます。「[不良 M.2 ディスクの交換 \(174 ページ\)](#)」を実行して、不良ディスクを交換します。

---

## AHCI モードでの JBOD ディスクの移行

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

### 始める前に

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

### 手順

**ステップ 1** サーバのグレースフルシャットダウンを実行します。

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

**ステップ 3** 次のいずれかを実行します。

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

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

**ステップ 5** サーバの電源をオンにします。

**ステップ 6** サーバを再認識します。

---

## 不良 M.2 ディスクの交換

次の手順を実行して、不良 M.2 ディスクを交換します。

### 始める前に

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

## 手順

- ステップ 1 正常にサーバの電源を切ります。
- ステップ 2 不良 M.2 ドライブを物理的に取り外します。シリアル番号とディスク スロットを使用して不良ディスクを識別します。
- ステップ 3 交換 M.2 ドライブを挿入します。
- ステップ 4 サーバの電源をオンにします。
- ステップ 5 ディスクが再構築されるまで待機してから、サーバを再確認します。

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

AHCI は NORAIID 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 \(207 ページ\)](#) を参照してください。

## 手順

- ステップ 1 [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2 [サーバ] > [サービス プロファイル] を展開します。
- ステップ 3 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 [作業 (Work) ] ペインで、[ストレージ (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に関連付けるには、[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、[ストレージ プロファイルを作成 (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。新しいストレージプロファイルの作成方法については、[ストレージプロファイルの作成 \(143 ページ\)](#) で詳しく説明しています。
- 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

#### 始める前に

Cisco ブート最適化 M.2 RAID コントローラでセットアップする場合、Cisco UCS Manager は異なる外部設定を持つ 2 個のドライブを接続する場合、インポートの設定を認識しません。HII メニューを使用して 1 個のドライブで最初に設定を消去する必要があります。HII メニューを使用して設定を消去する方法については、『[Configuration Guides](#)』を参照してください。

#### 手順

---

- ステップ 1** [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2** [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [サーバ (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

### 始める前に

Cisco ブート最適化 M.2 RAID コントローラでセットアップする場合、Cisco UCS Manager は異なる外部設定を持つ2個のドライブを接続する場合、インポートの設定を認識しません。HII メニューを使用して1個のドライブで最初に設定を消去する必要があります。HII メニューを使用して設定を消去する方法については、『[Configuration Guides](#)』を参照してください。

### 手順

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

**ステップ 2** [機器]>[ラックマウント]>[サーバ]を展開します。

(注) Cisco UCS C125 M5 サーバでは、[機器 (Equipment)]>[ラックマウント (Rack Mounts)]>[エンクロージャ (Enclosures)]>[ラック エンクロージャ *rack\_enclosure\_number* (Rack Enclosure *rack\_enclosure\_number*)]>[サーバ (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。

## 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** [ナビゲーション]ペインで、[機器]をクリックします。

**ステップ 2** [機器 (Equipment)]>[シャーシ (Chassis)]>[シャーシ番号 (*Chassis Number*)]>[サーバ (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** [ナビゲーション] ペインで、[機器] をクリックします。

**ステップ 2** [機器] > [ラックマウント] > [サーバ] を展開します。

(注) Cisco UCS C125 M5 サーバでは、[機器 (Equipment)] > [ラックマウント (Rack Mounts)] > [エンクロージャ (Enclosures)] > [ラック エンクロージャ *rack\_enclosure\_number* (Rack Enclosure *rack\_enclosure\_number*)] > [サーバ (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 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] の順に展開します
  - ステップ 3 [作業 (Work)] ペインで、[ストレージ (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 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] の順に展開します
  - ステップ 3 [作業 (Work)] ペインで、[ストレージ (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 [はい (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 [ナビゲーション] ペインで、[機器] をクリックします。

ステップ 2 [機器] > [ラックマウント] > [サーバ] を展開します。

(注) Cisco UCS C125 M5 サーバでは、[機器 (Equipment)] > [ラックマウント (Rack Mounts)] > [エンクロージャ (Enclosures)] > [ラック エンクロージャ rack\_enclosure\_number (Rack Enclosure rack\_enclosure\_number)] > [サーバ (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 [はい (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 [ナビゲーション] ペインで、[機器] をクリックします。

ステップ 2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [サーバ (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 [ナビゲーション] ペインで、[機器] をクリックします。

ステップ 2 [機器] > [ラックマウント] > [サーバ] を展開します。

(注) Cisco UCS C125 M5 サーバ では、[機器 (Equipment)] > [ラックマウント (Rack Mounts)] > [エンクロージャ (Enclosures)] > [ラック エンクロージャ *rack\_enclosure\_number* (Rack Enclosure *rack\_enclosure\_number*)] > [サーバ (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。

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

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

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



(注) Cisco UCS C3260 M3 サーバでは、Cisco UCS Manager GUI を使用したブート ポリシーへのローカル LUN の追加時に [Local LUN Image Path] のオプションとして [Any] はサポートされていません。Cisco UCS Manager CLI では Cisco UCS C3260 コマンド オプションは **local-anyM3** 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 C3260 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。
  - 1つのブート可能 LUN をプライマリまたはセカンダリ ブート デバイスとして指定します。ブート可能 LUN をプライマリとセカンダリの両方の起動デバイスとして指定すると、起動ポリシーによってサービス プロファイル設定エラーが発生します。

### 手順

- ステップ 1** [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2** [サーバ] > [ポリシー] を展開します。
- ステップ 3** ポリシーを作成する組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 4** 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** [ナビゲーション] ペインで、[サーバ] をクリックします。

**ステップ 2** [サーバ] > [ポリシー] を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

**ステップ 4** 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
- Cisco UCS C220 M6 ラックマウント サーバー
- Cisco UCS C240 M6 ラックマウント サーバー

**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 [ナビゲーション] ペインで、[サーバ] をクリックします。
  - ステップ 2 [サーバ] > [サービス プロファイル] > [Service\_Profile\_Name] を展開します。
  - ステップ 3 [作業 (Work)] ペインで、[ストレージ (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 [ナビゲーション] ペインで、[サーバ] をクリックします。
  - ステップ 2 [サーバ] > [サービス プロファイル] > [Service\_Profile\_Name] を展開します。
  - ステップ 3 [作業 (Work)] ペインで、[ストレージ (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 [ナビゲーション] ペインで、[サーバ] をクリックします。
  - ステップ 2 [サーバ] > [サービス プロファイル] > [Service\_Profile\_Name] を展開します。
  - ステップ 3 [作業 (Work)] ペインで、[ストレージ (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 [ナビゲーション] ペインで、[サーバ] をクリックします。
  - ステップ 2 [サーバ] > [サービス プロファイル] > [Service\_Profile\_Name] を展開します。
  - ステップ 3 [作業 (Work)] ペインで、[ストレージ (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。
-

■ サービス プロファイルで参照されている LUN の名前変更



## 第 12 章

# ミニストレージ

- [ミニストレージ \(187 ページ\)](#)
- [ミニストレージプロパティの表示 \(187 ページ\)](#)

## 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。

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

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

## ミニストレージプロパティの表示

ミニストレージモジュールは、M5 以降のサーバでのみサポートされています。

## 手順

---

- ステップ 1 [ナビゲーション] ペインで、[機器] をクリックします。
  - ステップ 2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [サーバ (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 セキュア デジタル カードのサポート \(189 ページ\)](#)
- [FlexUtil セキュア デジタル カードのサポート \(195 ページ\)](#)

## FlexFlash セキュア デジタル カードのサポート

### 概要

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

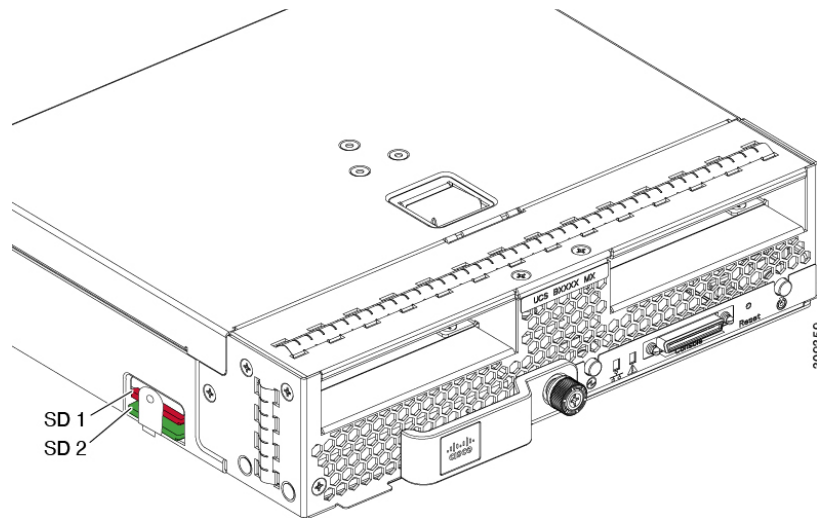
提供される一方または両方の SD カード スロットを装着できます。SD カードが 2 つ装着されている場合は、ミラー化モードで使用できます。



(注) サーバー内で異なる容量のカードを混在させないでください。

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

図 2: SD カード スロット



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

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

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

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

- SD カードをフォーマットします。詳細な情報については [SD カードのフォーマット \(194 ページ\)](#) を参照してください。
- 関連付けられているサーバーの場合、FlexFlash スクラブ ポリシーを作成し、サーバーからサービス プロファイルの関連付けを解除します。関連付けられていないサーバーの場合、FlexFlash スクラブ ポリシーを作成し、デフォルトのスクラブのポリシーを変更した後でサーバーを再認識させます。

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



(注) ペ어링が完了したらすぐにスクラブ ポリシーをディセーブルにします。

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

### FlexFlash ファームウェア管理

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

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

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

## FlexFlash FX3S のサポート

リリース 2.2(3)以降、Cisco UCS Manager では FX3S コントローラによる追加の FlexFlash サポートが可能になりました。FX3S コントローラは次のサーバー上に存在します。

- Cisco UCSB200 M4および M5ブレード サーバー
- Cisco UCSC220 M4および M5ラック サーバー
- Cisco UCS C240 M4 および M5 ラック サーバ
- C480 M5 ラック サーバー
- C480 M5 ML ブレード サーバー
- B480 M5 ブレード サーバー
- Cisco UCS C125 M5 サーバ

FX3S 制御を使用した FlexFlash 操作は、Cisco Flexible Flash ストレージ コントローラでの操作と同じです。FlexFlash はデフォルトでは無効で、ローカル ディスク ポリシーを使用して有効化されます。また、コントローラをリセットし、SD カードをフォーマットして、一对の SD カードを自動同期させることもできます。

FX3S コントローラの SD カードには、ハイパーバイザと呼ばれる単一のパーティションが含まれています。

#### Cisco FX3S コントローラの制約事項：

- FX3S コントローラは、32 GB および 64 GB の SD カードのみをサポートします。16 GB のカードはサポートされません。
- FX3S コントローラは、M5 以上のブレードで 128 GB のカードをサポートします。
- ラック サーバーの SD カードをブレードサーバーで使用したり、ブレードサーバーの SD カードをラック サーバーで使用することは推奨されません。サーバー タイプ間での SD カードの交換は SD カードのデータ損失につながる可能性があります。
- サーバーのファームウェアバージョンは、2.2(3a) 以上が必要です。

## FlexFlash SD カードのサポートのイネーブル化

### 手順

**ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。

**ステップ 2** [サーバ]>[ポリシー]を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

**ステップ 4** [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 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [サーバ (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。
- 

## SD カードのフォーマット

### 手順

---

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [サーバ (Servers)] の順に展開します。
  - ステップ 3 SD カードをフォーマ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 [Format SD Cards] をクリックします。
  - ステップ 7 [Yes] をクリックして、SD カードをフォーマットします。
- 

## FlexFlash コントローラのリセット

### 手順

---

- ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
  - ステップ 2 [機器 (Equipment)] > [シャーシ (Chassis)] > [シャーシ番号 (Chassis Number)] > [サーバ (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 \(197 ページ\)](#)
- [ファイバ チャネル スイッチング モード \(198 ページ\)](#)
- [ファイバ チャネル スイッチング モードの設定 \(199 ページ\)](#)
- [ストレージ VSAN の作成 \(200 ページ\)](#)
- [ファイバ チャネル ゾーン分割用の VSAN の作成 \(200 ページ\)](#)
- [ファイバ チャネル ストレージ ポートの設定 \(203 ページ\)](#)
- [ファイバ チャネル ゾーン分割の設定 \(204 ページ\)](#)

## 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 つのポー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 インターコネクタ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。

Cisco UCS 6400 シリーズ ファブリック インターコネクタは、フィルパターンが IDLE に設定されていない 8 Gbps 直接接続 FC 接続 (FC アップリンク ポートまたは FC ストレージ ポート) をサポートしません。次のいずれかを実行して、Cisco UCS 6200 シリーズ ファブリック インターコネクタから Cisco UCS 6400 シリーズ ファブリック インターコネクタに移行できます。

- 6400 シリーズ ファブリック インターコネクタと 8 GB FC 接続のストレージ アレイの間に SAN スイッチを使用します。
- ストレージ アレイを 16 GB または 32 GB FC 接続にアップグレードします。

# 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트가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、Cisco UCS Manager が両方のファブリック インターコネク트가同時に再起動します。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트의再ロードが順次行われます。Cisco UCS Manager リリース 3.1(3) 以降では、スイッチングモードの変更により、最初に従属ファブリック インターコネク트가リブートします。プライマリ ファブリック インターコネク트는、[保留中のアクティビティ (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트가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트가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 [ナビゲーション] ペインで、[機器] をクリックします。
- ステップ 2 [機器 (Equipment)] > [ファブリック インターコネク트가 (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트가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 が同じであってはなりません。VSAN 内の FCoE VLAN と VLAN で同じ ID を使用すると、その FCoE VLAN を使用しているすべての vNIC とアップリンク ポートで重大な障害が発生し、トラフィックが中断されます。FCoE VLAN ID と ID が重複するすべての VLAN 上でイーサネットトラフィックがドロップされます。

### 手順

**ステップ 1** [ナビゲーション] ペインで、[SAN] をクリックします。

**ステップ 2** [SAN] タブで、[SAN] > [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で、[+] をクリックします。

[+] アイコンが無効になっている場合、テーブルのいずれかのエントリをクリックして、有効にします。

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

手順

**ステップ 1** [ナビゲーション]ペインで、[SAN]をクリックします。

**ステップ 2** [SAN] タブの [SAN] ノードをクリックします。

**ステップ 3** [Work] ペインの [SAN Uplinks] タブで、[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 アップリンク マネージャ (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、[すべて]サブタブを使用すると、設定済みのすべてのVSANがテーブルに表示されます。

**ステップ 5** テーブルの右側のアイコンバーで、[+] をクリックします。

[+] アイコンが無効になっている場合、テーブルのいずれかのエントリをクリックして、有効にします。

**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 (Name)	説明
[名前 (Name) ] フィールド	<p>ネットワークに割り当てられている名前。</p> <p>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。</p>
[FC Zoning] フィールド	<p>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。</p> <ul style="list-style-type: none"> <li>• <b>[Disabled]</b> : 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。</li> <li>• <b>[Enabled]</b> : 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。</li> </ul> <p>(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。</p>

名前 (Name)	説明
[Type] オプション ボタン	<p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> <li>• [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。</li> <li>• [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。</li> </ul>
[VSAN ID] フィールド	<p>ネットワークに割り当てられている固有識別情報。</p> <p>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。</p>

名前 (Name)	説明
[FCoE VLAN] フィールド	<p>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。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、未使用または未予約の VLAN ID に変更する必要があります。たとえば、デフォルトを（未使用の VLAN ID）4049 に変更することを検討します。</li> <li>• 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。</li> </ul> <p>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。</p>

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 [ナビゲーション]ペインで、[機器]をクリックします。
- ステップ2 [機器 (Equipment)] > [ファブリック インターコネクト (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、[はい]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	まだ完了していない場合は、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 <b>clear-unmanaged-fc-zone-all</b> 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。 <a href="#">ファイバチャネルスイッチングモードの設定 (199ページ)</a> 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	ファイバチャンネルゾーンのトラフィック転送に必要なファイバチャンネルと 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 (19 ページ) およびファイバチャンネルストレージポートの設定 (20 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、ファイバチャンネルゾーンのトラフィック転送に必要なすべての VSAN で、ファイバチャンネルのゾーン分割を有効にします。	クラスタ設定では、SAN Uplinks Manager のファイバチャンネルゾーンに組み込んで、共通/グローバル設定を使用して両方のファブリック インターコネクต์にアクセスできるように VSAN を作成することをお勧めします。ファイバチャンネルゾーン分割用の VSAN の作成 (40 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ン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ンネルゾーン分割を設定することができます。ファイバチャンネルゾーン分割用の VSAN の作成 (40 ページ) を参照してください。
ステップ 7	ファイバチャン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。 <ul style="list-style-type: none"> <li>• 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。ファイバチャンネルゾーン分割用の VSAN の作成 (40 ページ) を参照してください。</li> <li>• 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 (207 ページ) を参照してください。</li> </ul>

## ファイバチャンネルストレージ接続ポリシーの作成

### 手順

ステップ 1 [ナビゲーション] ペインで、[SAN] をクリックします。

**ステップ 2** [SAN] > [ポリシー] を展開します。

**ステップ 3** ポリシーを作成する組織のノードを展開します。

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

**ステップ 4** [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 (Name)	説明
[名前 (Name) ] フィールド	<p>ポリシーの名前。</p> <p>この名前には、1 ~ 16 文字の英数字を使用できます。 - (ハイフン) 、 _ (アンダースコア) 、 : (コロン) 、 および . (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。</p>
[説明 (Description) ] フィールド	<p>ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。</p> <p>256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。 ` (アクセント記号) 、 \ (円記号) 、 ^ (カラット) 、 " (二重引用符) 、 = (等号) 、 &gt; (大なり) 、 &lt; (小なり) 、 または ' (一重引用符) は使用できません。</p>

**ステップ 6** [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 (Name)	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。
[説明 (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。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ ( caret)、" (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** [ナビゲーション] ペインで、[サーバ] をクリックします。
- ステップ 2** [サーバ] > [サービスプロファイル] を展開します。
- ステップ 3** 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、名前を指定した後で **[終了 (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 プロファイルをブレード サーバまたはサーバ プールと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 [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ 2 [サーバ]>[サービスプロファイル]を展開します。
- ステップ 3 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で、サービス プロファイルにこのプールのサーバーが割り当てられます。 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) [ServerId] 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** サーバに関連付けた後のサービスプロファイルの移行を制限する場合は、[移行の制限]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。両方のサーバのハードウェアが類似していない場合、アソシエーション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 (213 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 (214 ページ)
- NVMe の高度な VMD 搭載したカスタム LED のステータス (214 ページ)
- NVMe で最適化された M5 サーバ (218 ページ)
- NVMe PCIe SSD インベントリ (220 ページ)
- NVMe PCIe SSD ストレージ インベントリの表示 (221 ページ)
- UCS ストレージのボリューム管理デバイスを有効にする (223 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。
- 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。
  - 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ブ 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 12: 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。	<p>障害パターンは、次の場合に表示されます。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul> <p>デフォルト = オプション 1</p>
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。	<p>デフォルト = 有効</p> <p>次のように設定できます。</p> <ol style="list-style-type: none"> <li>1. 無効 (1 台のドライブのみ)</li> <li>2. 有効 (すべてのドライブ)</li> </ol>
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 13: 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 <b>BLACKLIST</b>	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 <b>BLINK_ON_INIT</b>	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) <b>REBUILD_BLINK_ON_ALL</b>	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 <b>BLINK_ON_MIGR</b>	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 <b>log_level</b>	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 <b>RAID_MEMBERS_ONLY</b>	フラグが ledmon (true) に設定されている場合、RAIDメンバであるドライブにのみモニタリングを制限します。	1. False/(すべてのRAIDメンバとPT) 2. True/(RAIDメンバのみ) デフォルト = False
特定のコントローラのみ限定されたスキャン <b>WHITELIST</b>	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 14: 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 MSwitch 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。各ケースには、MSwitch を含むインタポータカードがあります。各サーバは、最大 24 台の NVMe ドライブ (3 個の NVMe ドライブ ケージ x 8 個の NVMe ドライブ) をサポートできます。サーバは背面 PCIe Aux ドライブ ケージもサポートしています。これには、PCIe スロット 10 に配置された MSwitch によって管理される最大 8 台の NVMe ドライブを搭載できます。

このセットアップでは次の機能はサポートされていません。

- NVMe ドライブ ケージと HDD ドライブ ケージの組み合わせ
- 背面補助ドライブ ケージに関係なく、Cisco 12G 9460-8i RAID コントローラと NVMe ドライブ ケージの組み合わせ



(注) UCS C480 M5 PID は、以前のリリースと同じです。



(注) B200 および B480 M5 ブレード サーバでは、NVMe ドライブを SAS コントローラで直接使用することはできません。代わりに LSTOR-PT パススルー コントローラを使用してください。

NVMe 最適化 M5 サーバでは、次の MSwitch カードがサポートされています。

- UCS-C480-M5 HDD Ext NVMe カード (UCSC-C480-8NVME)—PCIe MSwitch を含む、インタポータ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、各ケースは最大 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 [ナビゲーション] ペインで、[機器] 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 (Name)	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。

名前 (Name)	説明
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。
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。

# UCS ストレージのボリューム管理デバイスを有効にする

## Intel® ボリューム管理デバイスの有効化

### ボリューム管理デバイス (VMD) の設定

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

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

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

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

### UCS Manager での VMD の有効化

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



(注) OS をインストールする前に、VMD を有効にする必要があります。

#### 手順

**ステップ 1** [ナビゲーション] ペインで、[サーバ] をクリックします。

**ステップ 2** ポリシーを作成する組織のノードを展開します。

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

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

## パススルーモードでボリューム管理デバイス (VMD) 有効化

### ボリューム管理デバイス (VMD) パススルーモード

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

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



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

### VMD パススルーの設定

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

## 手順

- 
- ステップ 1** [ナビゲーション]ペインで、[サーバ]をクリックします。
- ステップ 2** ポリシーを作成する組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ 3** VMD の BIOS ポリシーの設定：サービス プロファイルを選択し、[ポリシー (Policies)] タブに移動します。[ポリシー (Policies)] セクションで、BIOS セクションを右クリックして、ポップアップから [BIOS ポリシーの作成 (Create BIOS Policy)] を選択します。[BIOS ポリシー (BIOS Policy)] フォームに名前と説明 (任意) を入力します。[OK] をクリックしてポリシーを作成します。
- ステップ 4** [ポリシー (Policies)] > [ルート (Root)] > [BIOS ポリシー (BIOS Policies):] に移動し、新しいポリシーを選択します。
- ステップ 5** [BIOS ポリシー (BIOS Policies)] を展開し、サブメニューから [アドバンスド (Advanced)] および [LOM および PCIe スロット (LOM and PCIe Slots)] を選択します。
- ステップ 6** [VMD の有効化 (VMD enable)] まで下にスクロールし、[有効 (enable)] を選択します。
- ステップ 7** [保存を変更 (Save Changes)] をクリックして、VMD 機能を有効にします。
- ステップ 8** VMD パススルーモードの有効化を完了するには、サブメニューから [アドバンスド (Advanced)] および [Intel Directed IO] を選択し、[Intel VT Directed IO] までスクロールダウンします。ドロップダウンが [有効 (Enabled)] に設定されていることを確認します。そうでない場合は、設定します。
- ステップ 9** [変更を保存 (Save Changes)] をクリックして、VMD パススルー ポリシーを有効にします。
- ステップ 10** [ブートポリシー (Boot Policy)] タブで、ローカルブートポリシーを作成します。[ブートモード (Boot Mode)] の [Uefi] を選択します。[OK] をクリックしてポリシーを作成します。
- 

## VMD ドライバのダウンロード

### Intel® ボリューム管理デバイス ドライバ

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

- Linux
- Windows 2016、2019
- VMWare



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

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

- Red Hat Linux
- Ubuntu

Intel VMD の機能を使用するには、次のことを行う必要があります。

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



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

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

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

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

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

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

Intel VRoC を使用するには、次のことを行う必要があります。

- BIOS 設定で VMD を有効にする
- UEFI ブート モードを使用する

- ボリュームを作成するのに十分なドライブ リソースがある
- [BIOS HII] オプションを使用して、VRoC を設定し、設定します。

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

## Linux VMD ドライバのダウンロード

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

### 始める前に

BIOS 設定で VMD が有効になっていることを確認してください。



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

### 手順

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

### 次のタスク

CPU (VRoC) の Intel® 仮想 RAID Linux ソフトウェア ユーザー ガイドは、<https://www.intel.com/content/www/us/en/support/articles/000030445/memory-and-storage/>

[ssd-software.html?productId=122484&localeCode=us\\_en](https://software.cisco.com/download/home) のユーザー マニュアルに記載されています。これは、ブート前環境での BIOS HII VRoC 設定の実行に関する情報と、プログラム可能な LED ユーティリティのインストールと使用方法について説明します。

## Windows VMD ドライバのダウンロード

ドライババンドルをダウンロードするには、次の手順を実行します。

### 始める前に

BIOS 設定で VMD が有効になっていることを確認してください。



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

### 手順

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

### 次のタスク

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



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

## VMD パススルー ドライバのダウンロード

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



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

### 始める前に



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

### 手順

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

**ステップ 2** サーバ-ユニファイド コンピューティングの検索

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

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

**ステップ 5** 左のパネルの最新リリースをクリックします。

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

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

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

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

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

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

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

### 次のタスク

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

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

## NVMe の高度な VMD 搭載したカスタム LED のステータス

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

### LED の点滅

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

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

### ドライブ ホットプラグ時の LED の動作

NVMe を持つ VMD は、突然のホットプラグをサポートします。ディスクがホット解除され、同じスロットに再装着されると、障害 LED が 10 秒間点滅します。これは予期される動作です。ドライブが取り外されたときに、スロットの LED が障害状態を示されますが、バックプレーンでは LED が点滅可能になるように、ドライブがスロットに存在する必要があります。したがって、障害状態はドライブが取り外された後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 15: 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、エンクローチャ内の特定のデバイスを識別します。	1 ~ 3600 秒。この範囲外の値は、デフォルトで 12 秒に設定されています。 デフォルトは 12 秒です。
ドライブの障害	デバイスのステータス LED を、定義された障害パターンで点灯することによって、縮退状態または障害状態のドライブを示します。	障害パターンは、次の場合に表示されます。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul> デフォルト = オプション 1

ステータス LED	動作	オプション
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。
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 16: 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 <b>BLACKLIST</b>	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 <b>BLINK_ON_INIT</b>	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

ステータス LED	動作	オプション
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) <b>REBUILD_BLINK_ON_ALL</b>	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 <b>BLINK_ON_MIGR</b>	RAID ボリューム内のすべてのドライブでパターンを再構築します (移行が完了するまで)。	1. True/有効 (すべてのドライブ上) 2. False/無効 (ドライブなし) デフォルト = True/有効
ledmon デバッグ レベルの設定 <b>log_level</b>	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 <b>RAID_MEMBERS_ONLY</b>	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 <b>WHITELIST</b>	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 17: 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。

ステータス LED	動作	オプション
「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。



# CHAPTER 16

## Cisco UCS C3260 システムストレージ管理

- [ストレージサーバ機能およびコンポーネントの概要 \(235 ページ\)](#)
- [Cisco UCS C3260 ストレージ管理操作 \(245 ページ\)](#)
- [高可用性のためのディスクの共有, on page 246](#)
- [ストレージエンクロージャ操作, on page 255](#)
- [SAS エクスパンダ設定ポリシー, on page 256](#)

### ストレージサーバ機能およびコンポーネントの概要

#### ストレージサーバ機能

次の表に、Cisco UCS C3260 システムの機能の概要を示します。

表 18: Cisco UCS C3260 システムの機能

特長	説明
シャーシ	4 ラック ユニット (4RU) シャーシ
プロセッサ	<ul style="list-style-type: none"><li>• Cisco UCS C3260 M3 サーバノード: 各サーバノード内の 2 つの Intel Xeon E5-2600 v2 シリーズプロセッサ。</li><li>• Cisco UCS C3260 M4 サーバノード: 各サーバノード内の 2 つの Intel Xeon E5-2600 v4 シリーズプロセッサ。</li><li>• Cisco UCS C3260 M3 サーバノード: 各サーバノード内の 2 つの Skylake 2S-EP プロセッサ。</li></ul>
メモリ	各サーバノード内で最大 16 個の DIMM。

特長	説明
マルチビット エラー保護	このシステムは、マルチビット エラー保護をサポートします。
ストレージ	<p>システムには次のストレージ オプションがあります。</p> <ul style="list-style-type: none"> <li>• 最大 56 台のトップ ローディング 3.5 インチ ドライブ</li> <li>• オプションのドライブ エクспанダ モジュール内に最大 4 台の 3.5 インチ、リア ローディング ドライブ</li> <li>• 最大 4 台の 2.5 インチ、リア ローディング SAS ソリッドステート ドライブ (SSD)</li> <li>• サーバ ノード内部の 1 台の 2.5 インチ NVMe ドライブ <ul style="list-style-type: none"> <li>(注) これは S3260 M4 サーバにのみ適用されます。</li> </ul> </li> <li>• サーバ ノード内に 2 台の 7 mm NVMe ドライブ <ul style="list-style-type: none"> <li>(注) これは、S3260 M5 サーバのみに適用されます。</li> </ul> </li> <li>• IO エクспанダのサポートされている 2 つの 15 mm NVMe ドライブ</li> </ul>
ディスク管理	<p>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。</p> <ul style="list-style-type: none"> <li>• 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</li> </ul>
RAID バックアップ	supercap 電源モジュール (SCPM) は、RAID コントローラ カードにマウントされます。

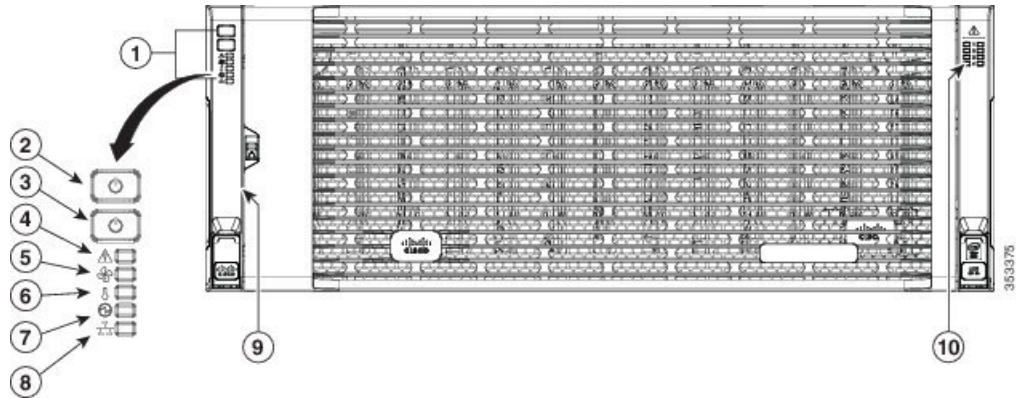


特長	説明
PCIe I/O	<p>オプションの I/O エクスパンダは、8x Gen 3 PCIe 拡張スロットを 2 つ提供します。</p> <p>リリース 3.2(3) 以降では、S3260 M5 サーバで次をサポートしています。</p> <ul style="list-style-type: none"> <li>• Intel X550 デュアルポート 10GBase-T</li> <li>• Qlogic QLE2692 デュアルポート 16G ファイバチャネル HBA</li> <li>• N2XX-AIPCI01 Intel X520 デュアルポート 10 Gb SFP+ アダプタ</li> </ul>
ネットワークおよび管理 I/O	<p>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。</p> <ul style="list-style-type: none"> <li>• SIOC ごとに 2 つの SFP+ 40 Gb ポート</li> <li>• SIOC ごとに 1 つの 10/100/1000 イーサネット専用管理ポート</li> </ul> <p>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。</p>
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	<p>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。</p> <p>さらに、各電源にはファンが 1 個あります。</p>

### 前面パネルの機能

次の図に、Cisco UCS C3260 システムの前面パネルの機能を示します。

図 3: 前面パネルの機能

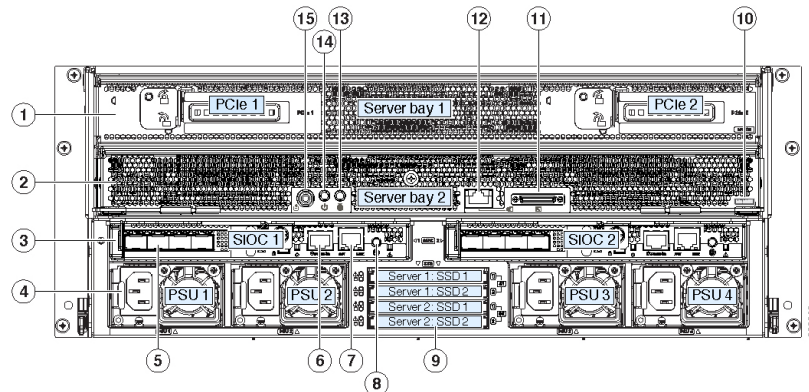


1	操作パネル	6	温度ステータス LED
2	システム電源ボタン/LED	7	電源装置ステータス LED
3	システムユニット識別ボタン/LED	8	ネットワークリンクアクティビティ LED
4	システムステータス LED	9	引き出し型の資産タグ (前面ベゼルの下に表示されない)
5	ファンステータス LED	10	内蔵ドライブのステータス LED

## 背面パネルの機能

次の図に、Cisco UCS C3260 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	<p>サーバー ベイ 1</p> <ul style="list-style-type: none"> <li>• (オプション) I/O エクスパンダ (図を参照) (Cisco UCS C3260 M4および M5サーバノードのみに搭載)</li> <li>• (オプション) サーバノード</li> <li>• (オプション) ドライブ拡張モジュール</li> </ul>	8	現時点ではサポートされていません。
2	<p>サーバー ベイ 2</p> <ul style="list-style-type: none"> <li>• (オプション) サーバノード (Cisco UCS C3260 M4および M5に表示)</li> <li>• (オプション) ドライブ拡張モジュール</li> </ul>	9	現時点ではサポートされていません。

3	<p>システム I/O コントローラ (SIOC)</p> <ul style="list-style-type: none"> <li>• サーバ ベイ 1 にサーバ ノードがある場合、SIOC 1 が必要</li> <li>• 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</li> </ul>	10	<p>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)</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• 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</li> </ul>
4	電源装置 (4、2+2 として冗長)	11	<p>Cisco UCS C3260 M4 サーバノードのラベル (M4 SVRN)</p> <p>(注) このラベルは、Cisco UCS C3260 M4 および M5サーバノードを識別します。Cisco UCS C3260 M3 サーバノードにはラベルがありません。</p>
5	40 Gb SFP+ ポート (SIOC ごとに 2 つ)	12	<p>KVM コンソール コネクタ (サーバノードごとに 1 つ)</p> <p>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</p>

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

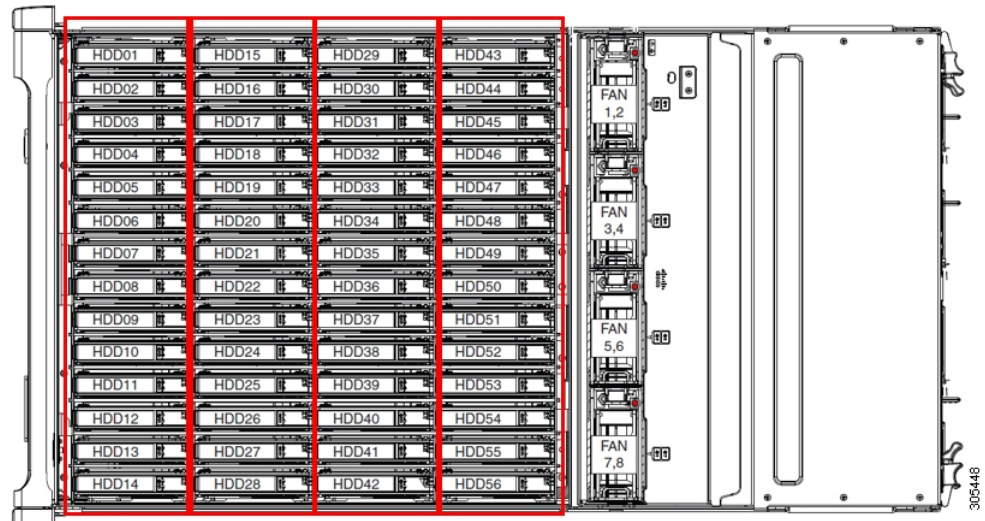
Cisco UCS C3260 システムは、1つまたは2つのノードから構成されています。各ノードには2つのCPU、128 GB、256 GB、または512 GBのDIMMメモリ、最大4GBのキャッシュのRAIDカードまたはパススルーコントローラが備わっています。サーバノードは次のいずれかです。

- Cisco UCS C3260 M3 サーバノード
- Cisco UCS C3260 M4 サーバノード：このノードに、サーバノードの上部に接続するオプションのI/O エクスパンダが含まれる場合があります。
- Cisco UCS C3260 M5 サーバノード：このノードに、サーバノードの上部に接続するオプションのI/O エクスパンダが含まれる場合があります。

### ディスクスロット

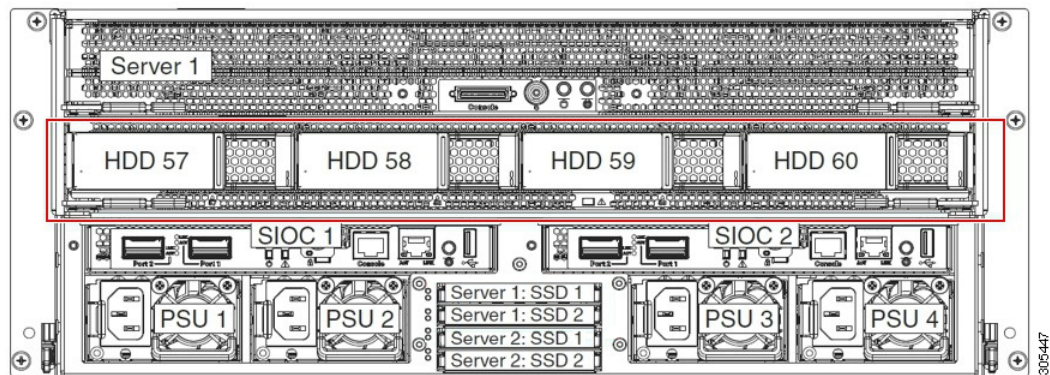
Cisco UCS S3260 シャーシのHDDマザーボードに14ディスクスロットが4行と、HDD拡張トレイに追加の4ディスクスロットがあります。次の図は、上面からアクセス可能でホットスワップ可能な56台の3.5インチの6TBまたは4TB 7200 rpm NL-SAS HDDドライブのディスクの配置を示しています。ディスクスロットに2つのSASポートがあり、それぞれがシャーシのSASエクスパンダに接続されます。

図 5: Cisco UCS C3260 上面図



次の図は、HDD 拡張トレイに 4 つの追加ディスク スロットを備えた Cisco UCS S3260 シャーシを示しています。

図 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 C3260 システムでは Server SIOC Connectivity 機能がサポートされています。シャーシに単一サーバとデュアル SIOC が装着されている場合、この機能を使用して、プライマリ SIOC および補助 SIOC の両方を經由するデータパスを設定できます。

### SAS エクスパンダ

Cisco UCS C3260 システムには、冗長モードで実行し、シャーシレベルのディスクをサーバのストレージコントローラに接続する2つのSASエクспанダがあります。SASエクспанダは、ストレージコントローラのために2つのパスを提供するため、可用性が向上します。それらには、次の利点があります。

- ハードドライブのプールを管理します。
- サーバのストレージコントローラへのハードドライブのディスクのゾーン設定。

リリース 3.2(3a)以降、Cisco UCS Manager は、ディスクスロットごとに単一のDiskPortを設定することによって、ディスクへの単一パスアクセスを有効にすることができます。これにより、サーバは単一のデバイスのみを検出し、マルチパス設定を避けることができます。

次の表に、各SASエクспан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спанダ間のSASのアップリンクの数は、サーバに搭載されているコントローラのタイプによって異なることがあります。

### ストレージエンクロージャ

Cisco UCS C3260には、次のタイプのストレージエンクロージャが備わっています。

#### シャーシレベルのストレージエンクロージャ

- **HDD motherboard enclosure** : シャーシの56のデュアルポートディスクスロットは、HDDマザーボードエンクロージャで構成されています。
- **HDD 拡張トレイ** : Cisco UCS C3260 システムに追加された4つのデュアルディスクスロットでHDD拡張トレイを構成しています。



- (注) HDD拡張トレイは現場交換可能ユニット (FRU) です。ディスクは挿入時は未割り当てのままであり、ストレージコントローラに割り当てることができます。ディスクゾーン分割の実行方法の詳細については、次を参照してください。 [ディスクゾーン分割ポリシー \(246 ページ\)](#)

### サーバレベルのストレージエンクロージャ

サーバレベルのストレージエンクロージャは、サーバに事前に割り当てられた専用のエンクロージャです。次のいずれかになります。

- **背面ブート SSD エンクロージャ**：このエンクロージャには、Cisco UCS C3260 システムの背面パネル上の2つの2.5インチディスクスロットが含まれています。各サーバは2つの専用ディスクスロットを備えています。これらのディスクスロットはSATA SSDをサポートします。
- **Server board NVMe enclosure**：このエンクロージャには1つのPCIe NVMe コントローラが搭載されています。



(注) Cisco UCS C3260 システムでは、上記2種類のエンクロージャに物理的にディスクが存在することもできますが、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 19:

ストレージコントローラのタイプ	ファームウェアのタイプ	モード	共有	OOB サポート
UCSC-S3X60-R1GB	メガ RAID	HW RAID、JBOD	いいえ	はい
UCS-C3K-M4RAID	メガ RAID	HW RAID、JBOD	いいえ	はい
UCSC-S3X60-HBA	イニシエータターゲット	パススルー	はい	はい
UCS-S3260-DHBA	イニシエータターゲット	パススルー	はい	はい
UCS-S3260-DRAID	メガ RAID	HW RAID、JBOD	いいえ	はい

### その他のストレージコントローラ

**SW RAID コントローラ**：Cisco UCS C3260 システム内のサーバは、SW RAID コントローラに接続しているPCIeライザーに組み込まれた、2つの専用内部SSDをサポートします。このコントローラは、Cisco C3000 M3 サーバでサポートされます。

**NVMe コントローラ**：Cisco UCS C3260 システム内のサーバによって、NVMe ディスクのインベントリとファームウェアアップデートにこのコントローラが使用されます。



さまざまなサーバノードでサポートされているストレージコントローラに関する詳細は、関連するサービス ノートを参照してください。

- [Cisco UCS S3260 ストレージ サーバ サービス ノート用 Cisco UCS C3X60 M3 サーバ ノード](#)
- [Cisco UCS S3260 ストレージ サーバ サービス ノート用 Cisco UCS C3X60 M4 サーバ ノード](#)
- [Cisco UCS S3260 ストレージ サーバ用 Cisco UCS S3260 M5 サーバ ノードのサービス ノート](#)

## Cisco UCS C3260 ストレージ管理操作

次の表に、Cisco UCS Manager 統合 Cisco UCS C3260 システムで、実行できるさまざまなストレージ管理操作を示します。

動作	説明	次を参照してください。
高可用性のためのディスクの共有	<p>Cisco UCS C3260 システムの SAS エクспанダは、ドライブのプールをシャール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。</p> <ol style="list-style-type: none"> <li>1. ディスク ゾーン分割ポリシーを作成します。</li> <li>2. ディスクのスロットを作成し、所有権を割り当てます。</li> <li>3. シャールプロファイルにディスクを関連付けます。</li> </ol>	このガイドの「ディスク ゾーン分割ポリシー」セクション。

動作	説明	次を参照してください。
ストレージプロファイル、ディスクグループおよびディスクグループ設定ポリシー	Cisco UCS C3260 システムでストレージディスクの定義、ディスクの割り当て、および管理を行うには、Cisco UCS Manager のストレージプロファイルとディスクグループポリシーを利用できます。	『Cisco UCS Manager Storage Management Guide, Release 3.1(2)』の「Storage Profiles」セクション。Cisco UCS Manager リリース 3.2 ストレージ管理ガイド
ストレージエンクロージャ操作	サーバで、HDD 拡張トレイを交換するか、以前に挿入したトレイを取り外します。	このガイドの「シャードレベルのストレージエンクロージャの削除」セクション。

## 高可用性のためのディスクの共有

### ディスク ゾーン分割ポリシー

ディスク ゾーン分割を使用してサーバノードにドライブを割り当てることができます。ディスクゾーン分割は、同一サーバのコントローラまたは異なるサーバのコントローラで実行することができます。ディスクの所有権は次のいずれかになります。

#### 未割り当て

未割り当てのディスクとは、サーバノードに表示されていないものを指します。

#### 専用

このオプションを選択すると、**[Server]** および **[Controller][Server]**、**[Controller]**、**[Drive Path]**、およびディスク スロットの **[Slot Range]** の値を設定する必要があります。



(注) ディスクは割り当てられたコントローラにのみ表示されます。

リリース 3.2(3a)以降、Cisco UCS S 3260 M 5 以降のサーバでは、Cisco UCS Manager は、ディスク スロットごとに単一の DiskPort を設定することによって、ディスクへの単一パスアクセスを有効にすることができます。1つのパスの設定により、サーバが設定で選択されたドライブが1つパスでのみディスクドライブを検出します。シングルパスアクセスは、**Cisco UCS S3260 デュアルパススルーコントローラ (UCS-S3260-DHBA)** でのみサポートされています。

シングルパスアクセスが有効になると、3.2(3a)より前のリリースにダウングレードすることはできません。ダウングレードするには、ディスクゾーニングポリシーでディスク

スロットのディスク パスを**Path Both**に設定して、この機能を無効にし、すべてのディスク スロットを両方のディスク ポートに割り当てます。

#### 共有

共有ディスクとは、複数のコントローラに割り当てられるものを指します。これらは、サーバがクラスタ構成で動作し、各サーバにHBA モードのストレージコントローラがある場合に絞って使用されます。



(注) デュアル HBA コントローラを使用する場合は、特定の条件下では共有モードを使用できません。

#### シャーシのグローバル ホット スペア

このオプションを選択すると、ディスクの[Slot Range]の値を設定する必要があります。



**重要** ディスクの移行と孤立した LUN の要求：サーバ（サーバ 1）へゾーン分割されたディスクを別のサーバ（サーバ 2）に移行するには、仮想ドライブ（LUN）を転送準備完了としてマークするか、仮想ドライブを非表示にする処理を実行します。次に、そのディスクに割り当てるディスク ゾーン分割ポリシーを変更できます。仮想ドライブ管理の詳細については、『[Cisco UCS Manager Storage Management Guide](#)』の「*Disk Groups and Disk Configuration Policies*」のセクションを参照してください。

## ディスク ゾーン分割ポリシーの作成

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

名前 (Name)	説明
[説明 (Description) ] フィールド	<p>ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。</p> <p>256文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、&gt; (大なり)、&lt; (小なり)、または' (一重引用符) は使用できません。</p>
[Preserve Config] チェックボックス	<p>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。</p> <p>(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。</p>

[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	

名前	フィールド
	<p>スロットの所有権の値。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>Unassigned</b> : 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。</li> <li>• <b>Dedicated</b>—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 [Drive Path]、および [Slot Range] の値を設定する必要があります。</li> </ul> <p>リリース 3.2(3a)以降、Cisco UCS Manager は、ディスクスロットごとに単一の DiskPort を設定することによって、ディスクへの単一バスアクセスを有効にすることができます。これにより、サーバは単一のデバイスのみを検出し、マルチパス設定を避けることができます。</p> <p>ドライブのパスのオプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>両方のパス(デフォルト)</b>- ドライブパスは両方の SAS エクспанダにゾーニングされます。</li> <li>• <b>パス 0</b> - ドライブパスは、SAS エクспанダ 1 にゾーニングされます。</li> <li>• <b>パス 1</b> - ドライブパスは、SAS エクспанダ 2 にゾーニングされます。</li> </ul> <ul style="list-style-type: none"> <li>• <b>Shared</b> : 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。</li> </ul> <p>(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、<a href="#">表 20: デュアル HBA コントローラ</a></p>

名前	フィールド
	<p>の共有モードの制約事項 (251 ページ) を参照してください。</p> <ul style="list-style-type: none"> <li>• 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。</li> </ul>
[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	<p>ディスクが割り当てられているコントローラの ID。</p> <p>(注) デュアル RAID セットアップで、最初のコントローラから 2 番目のディスクにディスクを移行するには、<b>[Assigned to Controller]</b> をセカンドコントローラに変更します。</p>
[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 20: デュアル HBA コントローラの共有モードの制約事項

サーバ	HDD トレイ	コントローラ	共有モードのサポート
Cisco UCS C3260	非対応	デュアル HBA	未サポート
Cisco UCS C3260	HDD トレイ	デュアル HBA	未サポート
事前プロビジョニング	HDD トレイ	デュアル HBA	サポート対象外

## 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 (Name)	説明
[Ownership] チェックボックス	<p>ディスク スロットの所有権。次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• <b>Unassigned</b> : 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。</li> <li>• <b>Dedicated</b> : 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。</li> <li>• <b>Shared</b> : 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。</li> </ul> <p>(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、<a href="#">表 20: デュアル HBA コントローラの共有モードの制約事項 (251 ページ)</a> を参照してください。</p> <ul style="list-style-type: none"> <li>• <b>Chassis Global Hot Spare</b> : 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。</li> </ul>

- 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 [ナビゲーション] ペインで [シャーシ] をクリックします。
- ステップ 2 [シャーシ] > [シャーシプロファイル] を展開します。
- 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 [終了] 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、『Cisco UCS Manager Storage Management Guide, Release 3.1』、『Cisco UCS Manager リリース 3.2 ストレージ管理ガイド』の「仮想ドライブ」セクションを参照してください。



- (注) デュアルRAIDセットアップで、ディスクをファーストコントローラからセカンドに移行するには、ディスクゾーニングポリシーの [Assigned to Controller] をセカンドコントローラに変更します。ディスクゾーン分割ポリシーの作成 (247 ページ) 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 (Name)	説明
<b>Rename</b>	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。
<b>Set Transportation Ready</b>	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。
<b>Clear Transportation Ready</b>	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。

名前 (Name)	説明
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。
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** [ナビゲーション]ペインで、[機器]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。

## SAS エクスパンダ設定ポリシー

### SAS エクスパンダ設定ポリシーの作成

#### 手順

- ステップ1 [ナビゲーション] ペインで [シャーシ] をクリックします。
- ステップ2 [シャーシ] > [ポリシー] を展開します。
- ステップ3 ポリシーを作成する組織のノードを展開します。  
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
- ステップ4 [Sas Expander Configuration Policies] を右クリックし、[Create Sas Expander Configuration Policy] を選択します。
- ステップ5 [Create Sas Expander Configuration 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 (Name)	説明
[名前 (Name) ] フィールド	<p>ポリシーの名前。</p> <p>この名前には、1～16文字の英数字を使用できます。- (ハイフン)、_ (アンダースコア)、: (コロン)、および. (ピリオド) は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。</p>
[説明 (Description) ] フィールド	<p>ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。</p> <p>256文字以下で入力します。次を除く任意の文字またはスペースを使用できます。` (アクセント記号)、\ (円記号)、^ (caret)、" (二重引用符)、= (等号)、&gt; (大なり)、&lt; (小なり)、または' (一重引用符) は使用できません。</p>

名前 (Name)	説明
[6G-12G Mixed Mode] フィールド	<p>次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• [Disabled] : このポリシーでは接続管理が無効になっているため、12G が使用可能でも SAS エクスパンダは 6G の速度のみを使用します。</li> <li>• [Enabled] : このポリシーでは接続管理が有効になっており、可用性に基づいて 6G と 12G 間で速度をインテリジェントに切り替えます。</li> </ul> <p><b>[6G-12G Mixed Mode]</b>を有効にした後は、3.2(3a)より前のリリースにダウングレードすることはできません。ダウングレードするには、このモードを無効にします。</p> <ul style="list-style-type: none"> <li>• [No Change] (デフォルト) : 事前の設定が保持されます。</li> </ul> <p>(注) <b>[6G-12G Mixed Mode]</b>モードを有効または無効にするには、システムが再起動します。</p> <p><b>[6G-12G Mixed Mode]</b>フィールドは、Cisco UCS S3260 M5 以降のサーバでのみ使用可能です。</p>

ステップ 6 [OK] をクリックします。

## SAS エクスパンダ設定ポリシーの削除

### 手順

ステップ 1 [ナビゲーション] ペインで [シャーシ] をクリックします。

ステップ 2 [シャーシ] > [ポリシー] を展開します。

ステップ 3 プールを含む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 [Sas Expander Configuration Policies] を展開します。

ステップ 5 削除する SAS エクスパンダ ポリシーを右クリックし、[Delete] 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、[はい] をクリックします。



## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。