Cisco UCS Manager リリース 4.2 サーバ管理ガイド

初版：2021 年 6 月 24 日

最終更新：2023 年 7 月 12 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/

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

目 次

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

新機能および変更された機能に関する情報 1

第 2 章

サーバー管理の概要 7

サーバー管理の概要 7

Cisco UCS Manager ユーザ CLI ドキュメント 8

Cisco UCS Manager ユーザ ドキュメント 9

第 3 章

サーバー ライセンスの管理 11

ライセンス 11

C ダイレクト ラックのライセンスのサポート 12

ファブリック インターコネクトのホスト ID の入手方法 14

ライセンスの取得 15

ローカル ファイル システムからファブリック インターコネクトへのライセンスのダウンロード 16

リモート ロケーションからファブリック インターコネクトへのライセンスのダウンロード 17

ライセンスのインストール 18

ファブリック インターコネクトにインストールされているライセンスの表示 19

ポートまたは機能に使用できる猶予期間の決定 19
ライセンスの失効日の決定 20
ライセンスのアンインストール 20

第 4 章 Cisco UCS Central で Cisco UCS ドメイン を登録する 23
Cisco UCS ドメインの登録 23
Cisco UCS Manager と Cisco UCS Central 間のポリシー解決 24
Cisco UCS Central による Cisco UCS ドメイン の登録 25
Cisco UCS Central 間でのポリシー解決の設定 26
Cisco UCS Manager での Cisco UCS Central 登録プロパティの設定 27
Cisco UCS Central から Cisco UCS ドメイン を登録解除する 28

第 5 章 Cisco UCS での電力制限と電源管理 31
電力制限 Cisco UCS 31
電力ポリシーの設定 32
Cisco UCS サーバーの電源ポリシー 32
電源ポリシーの設定 33
電源の冗長性方式 34
ポリシー方式のシャーシ グループの電力制限の設定 34
ポリシー方式のシャーシ グループの電力制限 34
電力制御ポリシー 35
電力制御ポリシーの作成 36
電力制御ポリシーの削除 41
Power Saveモード 41
省電力モード ポリシー 41
電源節約ポリシーの作成 42
音響モード ファン プロファイル 43
音響モード ファン プロファイル 43
音響モードの構成 43
UCS Manager の電源グループ 47
電源グループの作成 49

電源グループへのシャーシの追加 51
電源グループからのシャーシの削除 51
電源グループの削除 51
ブレード レベルの電力制限 52
手動によるブレード レベルの電力制限 52
サーバーのブレード レベル電力制限の設定 52
ブレード レベル電力制限の表示 53
ファン制御ポリシーの構成 54
ファン制御ポリシー 54
ファン制御ポリシーの作成 54
グローバル電力プロファイリング ポリシーの設定 55
グローバル電力プロファイリング ポリシー 55
グローバル電力プロファイル ポリシーの設定 55
グローバル電力割り当てポリシーの設定 56
グローバル電力割り当てポリシー 56
グローバル電力割り当てポリシーの設定 56
電源投入操作時の電源管理 57
電源同期ポリシーの設定 58
電源同期ポリシー 58
電源同期の動作 58
電源同期ポリシーの作成 59
電源同期ポリシーの変更 61
電源同期ポリシーの削除 61
ラック サーバーの電源管理 62
UCS Mini 電源管理 62

第 6 章 ブレード サーバ ハードウェア管理 63
ブレード サーバー管理 64
ブレード サーバーの削除および解放に関するガイドライン 64
予期しないサーバー電力変更を回避するための推奨事項 65
ブレード サーバーのブート 66

サービス プロファイルからのラックマウント サーバのブート 66
ブレード サーバのブート順序の決定 67
ブレード サーバーのシャットダウン 68
サービス プロファイルからのサーバのシャットダウン 68
ブレード サーバのリセット 69
ブレード サーバの出荷時のデフォルト設定へのリセット 70
ブレード サーバの再確認 71
シャーシからのサーバーの削除 71
ブレード サーバからのインバンド設定の削除 72
ブレード サーバーの解放 73
存在しないブレード サーバ エントリの削除 73
ブレード サーバの再稼動 74
シャーシ内のサーバ スロットの再確認 74
存在しないブレード サーバの設定データベースからの削除 75
ブレード サーバのロケータ LED の切り替え 75
ブレード サーバのローカル ディスク ロケータ LED のオン/オフ切り替え 76
ブレード サーバーの CMOS のリセット 77
ブレード サーバーの CIMC のリセット 77
ブレード サーバーの TPM のクリア 78
ブレード サーバの POST 結果の表示 78
ブレード サーバーからの NMI の発行 79
ブレード サーバのヘルス イベントの表示 79
ヘルス LED アラーム 81
ヘルス LED アラームの表示 81
Smart SSD 82
SSD ヘルスのモニタリング 83

第 7 章 ラックマウント サーバ ハードウェア管理 85
ラックマウント サーバー管理 86
ラックエンクロージャ サーバー管理 86
ラックマウント サーバーの削除および解放に関するガイドライン 87

予期しないサーバー電力変更を回避するための推奨事項 88
ラックマウント サーバーのブート 89
サービス プロファイルからのラックマウント サーバのブート 90
ラックマウント サーバのブート順序の決定 90
ラックマウント サーバーのシャットダウン 91
サービス プロファイルからのサーバのシャットダウン 92
ラックマウント サーバのリセット 92
ラックマウント サーバーの出荷時のデフォルト設定へのリセット 93
永続メモリ スクラブ 94
ラックマウント サーバの再確認 95
ラックマウント サーバからのインバンド設定の削除 96
ラックマウント サーバーの解放 96
ラックマウント サーバの再稼動 97
ラックマウント サーバーの番号付け直し 97
存在しないラックマウント サーバの設定データベースからの削除 98
ラックマウント サーバのロケータ LED の切り替え 99
ラックマウント サーバのローカル ディスク ロケータ LED のオン/オフ切り替え 99
ラックマウント サーバーの CMOS のリセット 100
ラックマウント サーバーの CIMC のリセット 101
ラックマウント サーバーの TPM のクリア 101
ラックマウント サーバーからの NMI の発行 102
ラックマウント サーバのヘルス イベントの表示 103
ラックマウント サーバの POST 結果の表示 104
Power Transition Log の表示 105
Cisco UCS C125 M5 サーバスロット ID の表示 105

第 8 章 **S3X60 サーバ ノード ハードウェア管理 107**
Cisco UCS C3260 サーバー ノードの管理 108
Cisco UCS C3260 サーバ ノードのブート 108
サービス プロファイルからの Cisco UCS C3260 サーバのブート 108
Cisco UCS C3260 サーバ ノードのブート順序の決定 109

Cisco UCS C3260 サーバ ノードのシャットダウン 110
サービス プロファイルからの Cisco UCS C3260 サーバ ノードのシャットダウン 110
Cisco UCS C3260 サーバ ノードのリセット 111
Cisco UCS C3260 サーバー ノードの出荷時のデフォルト設定へのリセット 112
Cisco UCS C3260 サーバ ノードの再認識 113
シャーシからの Cisco UCS C3260 サーバ ノードの削除 114
Cisco UCS C3260 サーバ ノードからのインバンド設定の削除 114
Cisco UCS C3260 サーバ ノードの稼働停止 115
Cisco UCS C3260 サーバ ノードの再稼動 115
サーバ スロットの再認識 S3260 シャーシ 116
存在しない Cisco UCS C3260 サーバ ノードの設定データベースからの削除 116
Cisco UCS C3260 サーバ ノードのロケータ LED のオン/オフ切り替え 117
Cisco UCS C3260 サーバ ノードのローカル ディスク ロケータ LED のオン/オフ切り替え 118
Cisco UCS C3260 サーバ ノードの CIMC のリセット 118
Cisco UCS C3260 サーバ ノードの CMOS のリセット 119
S3X60 サーバーの BIOS パスワードのリセット 119
Cisco UCS C3260 サーバ ノードからの NMI の発行 120
Cisco UCS C3260 サーバ ノードの POST 結果の表示 120
Cisco UCS C3260 サーバ ノードのヘルス イベントの表示 121
ヘルス LED アラーム 123
ヘルス LED アラームの表示 123

第 9 章 サーバ プール 125
サーバ プールの設定 125
サーバ プール 125
サーバ プールの作成 125
サーバ プールの削除 126
サーバ プールへのサーバの追加 127
サーバ プールからのサーバの削除 127
UUID 接尾辞プールの設定 128
UUID 接尾辞プール 128

UUID 接尾辞プールの作成 128
UUID 接尾辞プールの削除 129
IP プールの設定 130
IP プール 130
IP プールの作成 131
IP プールへのブロックの追加 133
IP プールからのブロックの削除 134
IP プールの削除 134

第 10 章 サーバーのブート 137
ブート ポリシー 137
UEFI ブート モード 138
UEFI セキュア ブート 139
CIMC セキュア ブート 141
CIMCセキュア ブートのステータスの判別 142
ブート ポリシーの作成 142
SAN ブート 144
ブート ポリシー用 SAN ブート ポリシー設定 144
iSCSI ブート 145
iSCSI ブート プロセス 146
iSCSI ブートのガイドラインと前提条件 147
イニシエータ IQN の設定 149
Windows での MPIO のイネーブル化 149
iSCSI ブートの設定 150
iSCSI アダプタ ポリシーの作成 152
iSCSI アダプタ ポリシーの削除 154
iSCSI 認証プロファイルの作成 154
iSCSI 認証プロファイルの削除 155
iSCSI イニシエータ IP プールの作成 156
iSCSI ブート ポリシーの作成 157
サービス プロファイル用 iSCSI vNIC の作成 158

サービス プロファイルからの iSCSI vNIC の削除 160
サービス プロファイル レベルでのイニシエータ IQN の設定 160
サービス プロファイル レベルでのイニシエータ IQN の変更 161
iSCSI ブート パラメータの設定 161
iSCSI ブート パラメータの変更 166
IQN プール 170
IQN プールの作成 170
IQN プールへのブロックの追加 172
IQN プールからのブロックの削除 172
IQN プールの削除 173
LAN ブート 174
ブート ポリシー用 LAN ブート ポリシー設定 174
ローカル デバイス ブート 174
ブート ポリシー用ローカル ディスク ブートの設定 176
ブート ポリシー用仮想メディア ブートの設定 177
ブート ポリシー用 NVMe ブートの設定 179
vMedia サービス プロファイルへのブート ポリシーの追加 179
ブート ポリシーの削除 182
UEFI ブート パラメータ 182
UEFI ブート パラメータに関する注意事項と制約事項 182
UEFI ブート パラメータの設定 183
UEFI ブート パラメータの変更 184

第 11 章 サービス プロファイル 185
UCS Manager のサービス プロファイル 185
サーバー ID を上書きするサービス プロファイル 186
サーバー ID を継承するサービス プロファイル 187
サービス プロファイルに関するガイドラインおよび推奨事項 187
サービス プロファイルの作成方法 188
[Expert] ウィザードを使用したサービス プロファイルの作成 188
サーバ ID を継承するサービス プロファイルの作成 190

ブレード サーバのハードウェア ベースのサービス プロファイルの作成 191
ラックマウント サーバのハードウェア ベースのサービス プロファイルの作成 191
インバンド サービス プロファイル 192
サービス プロファイルからのインバンド設定の削除 192
サービス プロファイル タスク 193
サービス プロファイルの名前の変更 193
サービス プロファイルのクローン化 194
サービス プロファイルの UUID の変更 194
サービス プロファイルのブート順序の変更 196
サービス プロファイル用の vNIC の作成 198
サービス プロファイルからの vNIC の削除 199
サービス プロファイル用の vHBA の作成 199
vHBA に対する WWPN の変更 200
vHBA の永続的なバインディングのクリア 200
サービス プロファイルからの vHBA の削除 201
サービス プロファイルへの vHBA イニシエータ グループの追加 201
サービス プロファイルの削除 204
サービス プロファイルのアソシエーション 204
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 204
サービス プロファイルとサーバーまたはサーバー プールの関連付け解除 205
サービス プロファイル テンプレート 206
初期テンプレートと既存のテンプレート 206
サービス プロファイル テンプレートの作成 207
サービス プロファイル テンプレートから 1 つ以上のサービス プロファイルの作成 208
ブレード サーバのテンプレート ベースのサービス プロファイルの作成 209
ラックマウント サーバのテンプレート ベースのサービス プロファイルの作成 209
サービス プロファイルからのサービス プロファイル テンプレートの作成 210
サービス プロファイルのアセット タグの設定 211
サービス プロファイル テンプレート タスク 211
サービス プロファイル テンプレートへのサービス プロファイルのバインディング 211
サービス プロファイル テンプレートからのサービス プロファイルのバインド解除 212

サービス プロファイル テンプレートの UUID の変更 212
サービス プロファイルに割り当てられた UUID の、サービス プロファイル テンプレートのプールからのリセット 213
vNIC に割り当てられた MAC アドレスの、サービス プロファイル テンプレートのプールからのリセット 214
vHBA に割り当てられた WWPN の、サービス プロファイル テンプレートのプールからのリセット 215
サービス プロファイル テンプレートからのインバンド設定の削除 216
サービス プロファイルのアソシエーション 216
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 216
サービス プロファイル テンプレートとサーバ プールの関連付け 217
サービス プロファイルとサーバーまたはサーバー プールの関連付け解除 218
サーバ プールからのサービス プロファイル テンプレートの関連付け解除 219

第 12 章 サーバー関連ポリシー 221
BIOS 設定 222
サーバー BIOS 設定 222
サーバー BIOS 設定 222
BIOS ポリシー 341
デフォルトの BIOS 設定 341
BIOS ポリシーの作成 342
BIOS のデフォルトの修正 343
サーバの実際の BIOS 設定の表示 345
メモリ RAS 機能 345
Post-Package Repair (PPR) 345
Post Package Repair の有効化 345
提示されたメモリの制限 346
メモリ サイズの制限 346
部分メモリのミラーリング 347
部分メモリのミラーリングの有効化 348
トラステッド プラットフォーム モジュール 349
トラステッド プラットフォーム モジュール 349

Intel Trusted Execution Technology 349
トラステッド プラットフォームの設定 350
トラステッド プラットフォームの設定 350
TPM のプロパティの表示 351
SPDM セキュリティ 352
SPDM セキュリティ ポリシーの作成 353
セキュリティ ポリシーとサーバーの関連付け 354
障害アラート設定の表示 355
一貫したデバイスの命名 355
一貫したデバイスの命名の注意事項と制約事項（CDN） 355
BIOSポリシーでの一貫したデバイスの命名の設定 358
vNIC の CDN 名の設定 358
CIMC セキュリティ ポリシー 359
IPMI アクセス プロファイル 359
IPMI アクセス プロファイルの作成 360
IPMI アクセス プロファイルの削除 361
KVM 管理ポリシー 361
KVM 管理ポリシーの作成 362
グラフィックス カード ポリシー 363
グラフィックス カード ポリシーの作成 363
ローカル ディスク ポリシー 364
ローカル ディスク設定ポリシー 364
すべてのローカル ディスク設定ポリシーに関するガイドライン 365
RAID 用に設定されているローカル ディスク設定ポリシーに関するガイドライン 365
ローカル ディスク設定ポリシーの作成 367
ローカル ディスク設定ポリシーの変更 370
ローカル ディスク設定ポリシーの削除 371
FlexFlash のサポート 371
FlexFlash FX3S のサポート 374
FlexFlash SD カードを使用したブレード サーバの起動 375
FlexFlash SD カードのサポートのイネーブル化 376

自動同期のイネーブル化 377
SD カードのフォーマット 377
FlexFlash コントローラのリセット 377
永続メモリ モジュール 378
スクラブ ポリシー 378
スクラブ ポリシーの設定 378
スクラブ ポリシーの作成 381
スクラブ ポリシーの削除 383
DIMM エラー管理 383
DIMM の修正可能なエラー処理 383
メモリ エラーのリセット 384
DIMM のブラックリスト化 384
DIMM のブラックリストのイネーブル化 384
Serial over LAN ポリシー設定 385
Serial over LAN ポリシーの概要 385
Serial over LAN ポリシーの作成 386
Serial over LAN ポリシーの削除 387
サーバ自動構成ポリシー 387
サーバー自動構成ポリシーの概要 387
自動構成ポリシーの作成 388
自動構成ポリシーの削除 389
サーバ ディスカバリ ポリシー設定 390
サーバー ディスカバリ ポリシーの概要 390
サーバ ディスカバリ ポリシーの作成 391
サーバー ディスカバリ ポリシーの削除 392
ハードウェア変更検出ポリシー 392
ハードウェア変更検出ポリシーの設定 393
サーバ継承ポリシー設定 393
サーバー継承ポリシーの概要 393
サーバ継承ポリシーの作成 393
サーバー継承ポリシーの削除 394

サーバ プール ポリシー設定 395
サーバー プール ポリシーの概要 395
サーバ プール ポリシーの作成 395
サーバー プール ポリシーの削除 396
サーバ プール ポリシー資格情報設定 397
サーバー プール ポリシー資格情報の概要 397
サーバ プール ポリシーの資格情報の作成 397
サーバ プール ポリシーの資格情報の削除 403
サーバ プール ポリシーの資格情報からの資格の削除 403
vNIC/vHBA 配置ポリシー設定 403
vNIC/vHBA 配置ポリシー 403
vCon のアダプタへの配置 405
N20-B6620-2 および N20-B6625-2 ブレード サーバー用 405
vCon のアダプタへの配置（他のすべてのサポート対象サーバの場合） 406
vCon への vNIC/vHBA の割り当て 406
vNIC/vHBA 配置ポリシーの作成 409
vNIC/vHBA 配置ポリシーの削除 412
vCon への vNIC の明示的割り当て 413
vCon への vHBA の明示的割り当て 414
ダイナミック vNIC の前にスタティック vNIC を配置 416
vNIC/vHBA のホスト ポートの配置 418
ホスト ポート配置の設定 419
CIMC マウント vMedia 419
vMedia ポリシーの作成 420
サービス プロファイルへの vMedia ポリシーの追加 425
CIMC vMedia ポリシーの表示 428

第 13 章 ファームウェア アップグレード 429
ファームウェア アップグレード 429
コンポーネントのファームウェア バージョンの確認 429

第 14 章 診断の設定 431

Cisco UCS Manager 診断の概要 431

診断ポリシーの作成 432

ブレード サーバでの診断テスト 433

ブレード サーバでの診断テストの開始 433

ブレード サーバでの診断テストの停止 433

ラック サーバでの診断テスト 433

ラック サーバでの診断テストの開始 433

ラック サーバでの診断テストの停止 434

すべてのサーバでの診断テストの開始 434

すべてのサーバでの診断テストの停止 435

サーバ診断のステータス/結果の表示 435

診断のトラブルシューティング 437

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

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

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

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

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

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

警告　安全上の重要事項

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

これらの注意事項を保管しておいてください。

Cisco UCS の関連資料

ドキュメント ロードマップ

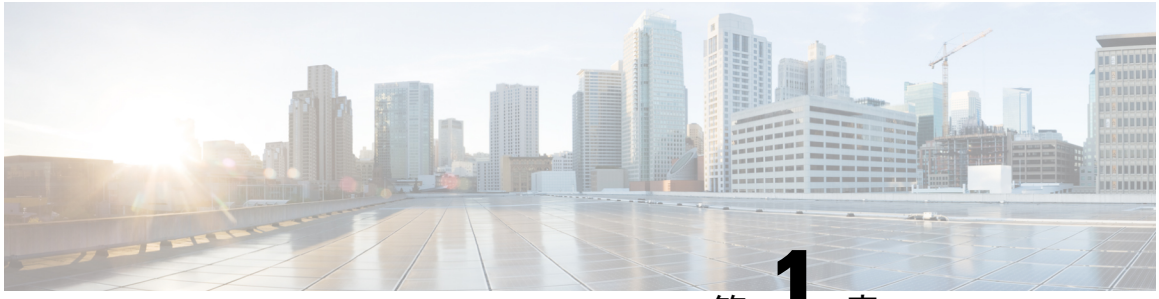
すべての B シリーズ マニュアルの完全なリストについては、次の URL で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

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

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

マニュアルに関するフィードバック

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



第 1 章

新機能および変更された機能に関する情報

• 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

ここでは、Cisco UCS Manager、リリース 4.2(2c) 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(2c)* の新機能と変更された動作

特長	説明	参照先
BIOS トークン	Cisco UCS Manager では、新しいBIOS トークンがサポートされるようになりました。	• トラステッド プラットフォーム BIOS 設定 （301 ページ）

ここでは、Cisco UCS Manager、リリース 4.2(1l) の新機能および変更された動作について説明します。

新機能および変更された機能に関する情報

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

特長	説明	参照先
Cisco UCS C225 M6サーバ のサポート	Cisco UCS Manager は Cisco UCS C225 M6サーバ をサポートするようになりました。	• 電力制限 Cisco UCS （31 ページ） • 電力制御ポリシー （35 ページ） • 音響モード ファン プロファイル （43 ページ） • 音響モードの構成 （43 ページ） • SPDM セキュリティ （352 ページ） • CIMC セキュア ブート （141 ページ）
BIOS トークン	Cisco UCS Manager には新しい BIOS トークンがあります。既存の BIOS トークンと値は変更されています。	• プロセッサのBIOS設定 （225 ページ） • RAS メモリの BIOS 設定 （273 ページ） • トラステッド プラットフォーム BIOS 設定 （301 ページ） • AMD 向け I/O BIOS 設定 （271 ページ）

ここでは、Cisco UCS Manager、リリース 4.2(1i) の新機能および変更された動作について説明します。

表 *3 : 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 C245 M6サーバ のサポート	Cisco UCS Manager は Cisco UCS C245 M6サーバ をサポートするようになりました。	• 電力制限 Cisco UCS （31 ページ） • 電力制御ポリシー （35 ページ） • 音響モード ファン プロファイル （43 ページ） • 音響モードの構成 （43 ページ） • SPDM セキュリティ （352 ページ） • CIMC セキュア ブート （141 ページ）
BIOS トークン	Cisco UCS Manager には新しい BIOS トークンがあります。既存の BIOS トークンと値は変更されています。	• プロセッサのBIOS設定 （225 ページ） • RAS メモリの BIOS 設定 （273 ページ） • トラステッド プラットフォーム BIOS 設定 （301 ページ） • AMD 向け I/O BIOS 設定 （271 ページ）

ここでは、Cisco UCS Manager、リリース 4.2(1f) の新機能および変更された動作について説明します。

新機能および変更された機能に関する情報

表 *4 : 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
BIOS トークン	Cisco UCS Manager には新しい BIOS トークンがあります。既存の BIOS トークンと値は変更されています。	• プロセッサのBIOS設定（225 ページ） • RAS メモリの BIOS 設定（273 ページ） • トラステッド プラットフォーム BIOS 設定 （301 ページ）

ここでは、Cisco UCS Manager、リリース 4.2(1d) の新機能および変更された動作について説明します。

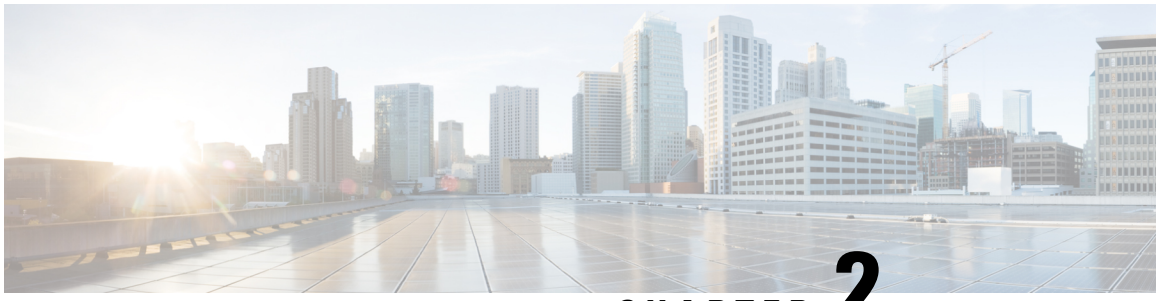
表 *5 : Cisco UCS Manager*、リリース *4.2(1d)* の新機能と変更された動作

特長	説明	参照先
Cisco UCS B200 M6、Cisco UCS C220 M6、および Cisco UCS C240 M6 サーバ	Cisco UCS Manager は以下のサーバーをサポートするようになりました。 • Cisco UCS B200 M6 • Cisco UCS C220 M6 • Cisco UCS C240 M6	—
BIOS トークン	Cisco UCS Manager には新しい BIOS トークンがあります。既存の BIOS トークンと値は変更されています。	• メイン BIOS 設定 （222 ページ） • プロセッサのBIOS設定（225 ページ） • RAS メモリの BIOS 設定（273 ページ） • Intel® OptaneTM DC 永続メモリ (DCPMM) BIOS トークン （287 ページ） • LOM および PCIe スロットの BIOS 設定 （303 ページ）

新機能および変更された機能に関する情報

特長	説明	参照先
セキュリティ プロトコルとデータ モデル（SPDM）	Cisco UCS Manager は SPDM ポリシーを介してアラート設定を構成できるようになりました。3 つのアラート レベルが利用可能です。	SPDM セキュリティ （352 ページ）
急速冷却	Cisco UCS Manager には、電力制御ポリシーのオプションとして利用可能な M6 サーバー用の急速冷却オプションがあります。	電力制御ポリシーの作成 （36 ページ）

新機能および変更された機能に関する情報



CHAPTER 2

サーバー管理の概要

- サーバー管理の概要 （7 ページ）
- Cisco UCS Manager ユーザ CLI ドキュメント （8 ページ）
- Cisco UCS Manager ユーザ ドキュメント （9 ページ）

サーバー管理の概要

Cisco UCS Manager 一般的なサーバー導入と複雑なサーバー導入を管理できます。たとえば、最初のシャーシで取得される、冗長なサーバー アクセス レイヤとなる 1 ペアのファブリック インターコネクト（FI）を用いた一般的な導入を管理でき、それらを最大 20 台のシャーシと 160 台の物理サーバーまで拡張することができます。これは、環境のワークロードをサポートするために、ブレード サーバーとラック マウント サーバーの組み合わせとなる場合があります。さらにサーバーを追加して、引き続き、サーバーのプロビジョニング、デバイス検出、インベントリ、設定、診断、監視、障害検出、監査を実行できます。

リリース 4.2（1）以降、Cisco UCS ManagerUCS Managerが次の Cisco UCS ハードウェアのサポートを導入します：

- Cisco UCS C220 M6サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C225 M6サーバ
- Cisco UCS C245 M6サーバ
- Cisco UCS B200 M6サーバ
- Cisco UCS VIC 1467（mLOM）
- Cisco UCS VIC 1477（mLOM）

、 Cisco UCS 6332 ファブリック インターコネクト、Cisco UCS Mini 6324 ファブリック インターコネクト と Cisco UCS 6200 シリーズ ファブリック インターコネクトには一元管理が含まれます。1 つのコンソールから同じドメイン内にある UCS ブレード サーバーとラックマウン

トサーバーを管理できます。また、Cisco UCS Manager から UCS Mini を管理することもできます。

最適なサーバーパフォーマンスを確保するために、サーバーに割り当てる電力量を設定できます。また、サーバーのブート ポリシー、サーバーの起動元となる場所、ブート デバイスの起動順序を設定できます。サービス プロファイルを作成し、サービス プロファイルをサーバーに割り当てることができます。サービス プロファイルでは、vNIC と vHBA の設定、BIOS 設定の有効化、ファームウェア ポリシーの適用、およびその他の設定を行うことができます。サービスプロファイルがサーバーに関連付けられると、構成済みの構成、ポリシー、および設定がサーバーにプッシュされます。

Cisco UCS Manager ユーザ CLI ドキュメント

Cisco UCS Manager 次の表に示す、使用例を基本とした従来よりもコンパクトなマニュアルが用意されています。

ガイド	説明
Cisco UCS Manager クイック スタート ガイド	Cisco UCS Manager の初期構成と構成のベストプラクティスを含め、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。
『Cisco UCS Manager アドミニストレーション ガイド』	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、BIOS トークン、遅延導入について説明しています。
Cisco UCS Manager インフラストラクチャ管理ガイド	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。
『Cisco UCS Manager Firmware Management Guide』	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。
Cisco UCS Manager サーバ管理ガイド	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。

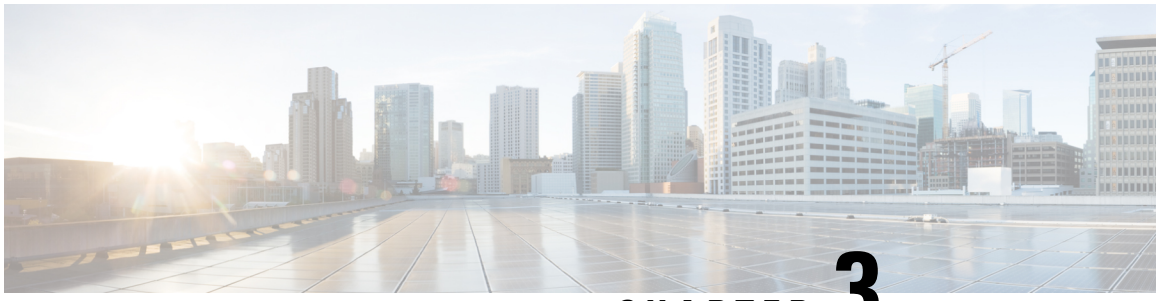
ガイド	説明
『Cisco UCS Manager Storage Management Guide』	SUN、VSAN など、Cisco UCS Managerでのストレージ管理のすべての側面について説明しています。
『Cisco UCS Manager Network Management Guide』	LAN 接続、VLAN 接続など、Cisco UCS Managerでのネットワーク管理のすべての側面について説明しています。
『Cisco UCS Manager System Monitoring Guide』	システム統計を含め、Cisco UCS Managerでのシステムおよびヘルス モニタリングのすべての側面について説明しています。
Cisco UCS S3260 サーバと Cisco UCS Manager との統合	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。

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
Cisco UCS Manager クイック スタート ガイド	Cisco UCS Manager の初期構成と構成のベストプラクティスを含め、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。
『Cisco UCS Manager アドミニストレーション ガイド』	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、BIOS トークン、遅延導入について説明しています。
Cisco UCS Manager インフラストラクチャ管理ガイド	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。

ガイド	説明
『Cisco UCS Manager Firmware Management Guide』	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。
Cisco UCS Manager サーバ管理ガイド	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。
『Cisco UCS Manager Storage Management Guide』	SUN、VSAN など、Cisco UCS Managerで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。
『Cisco UCS Manager Network Management Guide』	LAN 接続、VLAN 接続など、Cisco UCS Managerで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。
『Cisco UCS Manager System Monitoring Guide』	システム統計を含め、Cisco UCS Managerでのシステムおよびヘルス モニタリングのすべての側面について説明しています。
Cisco UCS S3260 サーバと Cisco UCS Manager との統合	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。



CHAPTER 3

サーバー ライセンスの管理

- ライセンス （11 ページ）
- C ダイレクト ラックのライセンスのサポート （12 ページ）
- ファブリック インターコネクトのホスト ID の入手方法 （14 ページ）
- ライセンスの取得 （15 ページ）
- ローカル ファイル システムからファブリック インターコネクトへのライセンスのダウンロード （16 ページ）
- リモート ロケーションからファブリック インターコネクトへのライセンスのダウンロード （17 ページ）
- ライセンスのインストール （18 ページ）
- ファブリック インターコネクトにインストールされているライセンスの表示 （19 ページ）
- ポートまたは機能に使用できる猶予期間の決定 （19 ページ）
- ライセンスの失効日の決定 （20 ページ）
- ライセンスのアンインストール （20 ページ）

ライセンス

各 Cisco UCS 6324 Fabric Interconnect にはポート ライセンスが付属します。このライセンスは工場でインストールされ、ハードウェアと共に出荷されます。C ダイレクト ポート ライセンスは猶予期間にプレインストールされ、ポートの初回の使用から開始され、Cisco UCS ラック サーバで使用できます。複数のポートが猶予期間内で動作している場合、ライセンスは猶予期間の終了が最も近いポートに移動されます。

猶予期間

ライセンスがインストールされていないポートを使用しようとすると、Cisco UCS は 120 日間の猶予期間を開始します。猶予期間は、最初にライセンスなしでポートを使用した時点から測定され、有効なライセンス ファイルがインストールされると一時停止されます。猶予期間中に使用された時間数はシステムに保存されます。

（注） 各物理ポートには固有の猶予期間があります。1 つのポートで猶予期間を開始しても、すべてのポートの猶予期間が開始するわけではありません。

ライセンスされているポートの設定を解除すると、そのライセンスは、猶予期間内で機能しているポートに移行されます。複数のポートが猶予期間内で動作している場合、ライセンスは猶予期間の終了が最も近いポートに移動されます。

ハイ アベイラビリティ コンフィギュレーション

フェールオーバー中の不整合を避けるため、クラスタ内の両方のファブリック インターコネクトに同数のライセンスされたポートを用意することを推奨します。均衡が保たれていない状態でフェールオーバーが発生すると、Cisco UCS は欠けているライセンスを有効化して、フェールオーバー ノードで使用される各ポートに対して猶予期間を開始します。

C ダイレクト ラックのライセンスのサポート

リリース 4.1(1a) 以降

リリース 4.1(1a) 以降の Cisco UCS 64108 ファブリック インターコネクト では、ポート 1 ～ 96 の C ダイレクト ポート ライセンスについて ETH_C_PORT_ACTIVATION_PKG 機能パックを使用します。ファブリック インターコネクトには、ETH_C_PORT_ACTIVATION_PKG ライセンスはデフォルトでは付属していません。必要に応じてこれらのライセンスを購入してください。

C ダイレクト サポートは、ラック サーバーに接続されたポートにのみ適用可能です。ETH_C_PORT_ACTIVATION_PKG は、既存のライセンス パッケージに、すべてのプロパティが既存のライセンス機能と同じように設定された状態で追加されます。[Subordinate Quantity] プロパティは、ラック サーバーに接続されたポートを追跡するために、ETH_PORT_ACTIVATION_PKG に追加されます。

Cisco UCS Manager GUI の [License] タブに、新しいライセンスとそのライセンスの [Subordinate Quantity] が表示されます。**scope license** の下で **show feature** コマンドおよび **show usage** コマンドを使用して、ライセンス機能、ベンダー バージョン タイプ、各ライセンスの猶予期間を表示することもできます。

リリース 4.0(1a) 以降

リリース 4.0(1a) 以降の Cisco UCS 6454 ファブリック インターコネクト では、ポート 1 ～ 48 の C ダイレクト ポート ライセンスについて ETH_C_PORT_ACTIVATION_PKG 機能パックを使用します。ファブリック インターコネクトには、ETH_C_PORT_ACTIVATION_PKG ライセンスはデフォルトでは付属していません。必要に応じてこれらのライセンスを購入してください。

C ダイレクト サポートは、ラック サーバーに接続されたポートにのみ適用可能です。ETH_C_PORT_ACTIVATION_PKG は、既存のライセンス パッケージに、すべてのプロパティ

が既存のライセンス機能と同じように設定された状態で追加されます。[Subordinate Quantity] プロパティは、ラック サーバーに接続されたポートを追跡するために、ETH_PORT_ACTIVATION_PKG に追加されます。

Cisco UCS Manager GUI の [License] タブに、新しいライセンスとそのライセンスの [Subordinate Quantity] が表示されます。**scope license** の下で **show feature** コマンドおよび **show usage** コマンドを使用して、ライセンス機能、ベンダー バージョン タイプ、各ライセンスの猶予期間を表示することもできます。

リリース 3.2(3o) 以前

各 Cisco UCS ファブリック インターコネクトは、デフォルトの数のポート ライセンスが工場で付与され、ハードウェアと一緒に出荷されます。C ダイレクト サポートは、ラック サーバーに接続されたポートにのみ適用可能です。10G_C_PORT_ACTIVATION_PKG および 40G_ETH_C_PORT_ACTIVATION _PKG は、既存のライセンス機能と同じプロパティがすべて設定された既存のライセンス パッケージに追加されます。[Subordinate Quantity] プロパティは、ラック サーバーに接続されたポートを追跡するために、10G_PORT_ACTIVATION_PKG および 40G_ETH_PORT_ACTIVATION_PKG に追加されます。

Cisco UCS Manager GUI の [License] タブに、新しいライセンスとそのライセンスの [Subordinate Quantity] が表示されます。**scope license** の下で **show feature** コマンドおよび **show usage** コマンドを使用して、ライセンス機能、ベンダー バージョン タイプ、各ライセンスの猶予期間を表示することもできます。

ラック サーバーに接続されたポートは、ライセンスが使用可能であるか、またはライセンスが使用中でない場合に、既存の 10G_PORT_ACTIVATION_PKG および 40G_ETH_PORT_ACTIVATION_PKG を使用できます。それ以外の場合は、10G_C_PORT_ACTIVATION_PKG および 40G_ETH_C_PORT_ACTIVATION_PKG を購入してライセンスの猶予期間を無効にする必要があります。

10 GB ポートでの変更はありません。10G_PORT_ACTIVATION_PKG および 10G_C_PORT_ACTIVATION_PKG ライセンス パッケージには、ETH_PORT_ACTIVATION_PKG および ETH_PORT_C_ACTIVATION_PKG ライセンス機能と同じプロパティがすべて含まれています。

設定と制約事項

- C ダイレクト ラック ライセンス機能は、CIMC ポートではなく、FI に直接接続されたラック サーバー ポートを構成します。10G_C_PORT_ACTIVATION_PKG および 40G_ETH_C_PORT_ACTIVATION_PKG のデフォルトの数量は常に 0 です。
- 40 GB ポートまたは 40 GB ブレークアウト ポート配下のブレークアウト ポートが接続なしで有効な場合、このポートには 40G_ETH_PORT_ACTIVATION_PKG（使用可能な場合）に基づいてライセンスが割り当てられます。このポートがタイムラグの後にダイレクト コネクト ラック サーバーに接続されると、ライセンスの完全な再割り当てがトリガーされ、このポートは、次のライセンス割り当てシナリオのいずれかで処理されます。

  40 GB ブレークアウト ポート配下のブレークアウト ポートが有効で、そのポートがダイレクト コネクト ラック サーバーに接続され、40G_C_PORT_ACTIVATION_PKG

ライセンス ファイルが FI にインストールされている場合は、次のライセンス割り当てが行われます。

- ブレークアウト ポート配下の他のポートがイネーブルでない場合は、40G_C_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられ、このライセンスの使用済み数量が増分されます。
- 他のポートが有効で、1 つ以上のポートがダイレクト コネクト ラック サーバーに接続されていない場合は、ポートが使用されていない場合でも、40G_ETH_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられ、このライセンスの使用済み数量が増分されます。

- 40 GB ブレークアウト ポート配下のブレークアウト ポートが有効で、そのポートがダイレクト コネクト ラック サーバーに接続され、40G_C_PORT_ACTIVATION_PKG ライセンス ファイルが FI にインストールされていない場合は、次のライセンス割り当てが行われます。
  - ブレークアウト ポート配下のポートがイネーブルでない場合は、40G_ETH_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられます。ライセンスが 40G_ETH_PORT_ACTIVATION_PKG で使用可能な場合は、下位の数量が増分されます。ライセンスが使用可能でない場合は、この機能の使用済み数量が増分され、ポート全体が猶予期間に入ります。
  - 他のポートが有効で、1つ以上のポートがダイレクトコネクトラックサーバーに接続されていない場合は、ポートが使用されていないときでも、40G_ETH_PORT_ACTIVATION_PKG に基づいて親の 40 GB ポートにライセンスが割り当てられ、このライセンスの使用済み数量が増分されます。

ファブリック インターコネクトのホスト ID の入手方法

ホスト ID はシリアル番号とも呼ばれます。

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]** > **[ファブリックインターコネクト]**を展開します。
ステップ 3 ホスト ID を取得するファブリック インターコネクト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 [Properties] 領域の [Serial Number (SN)] フィールドにホスト ID が表示されます。

次のタスク

シスコから必要なライセンスを入手します。

ライセンスの取得

（注） このプロセスは、このマニュアルのリリース後に変更される場合があります。このマニュアルの手順が1つ以上当てはまらない場合は、シスコの担当者にライセンス ファイルの入手方法をお問い合わせください。

始める前に

次を入手します。

- ファブリック インターコネクトのホスト ID またはシリアル番号
- ファブリック インターコネクトまたは拡張モジュールの権利証明書またはその他の購入証明書

手順

ステップ 1 権利証明書またはその他の購入証明書から、製品認証キー（PAK）を取得します。

ステップ 2 権利証明書またはその他の購入証明書で Web サイトの URL を確認します。

ステップ 3 ファブリック インターコネクトの Web サイト URL にアクセスし、シリアル番号と PAK を入力します。

シスコからライセンス ファイルが電子メールで送信されます。ライセンス ファイルは、要求されたファブリック インターコネクトでの使用だけを許可するようにデジタル署名されています。Cisco UCS Manager がライセンス ファイルにアクセスすると、要求された機能も有効になります。

次のタスク

ファブリック インターコネクトにライセンスをインストールします。

ローカル ファイル システムからファブリック インターコネクトへのライセンスのダウンロード

（注） クラスタ構成の場合、マッチングペアの両方のファブリックインターコネクトにライセンスをダウンロードしてインストールすることをお勧めします。個々のライセンスは、ダウンロードを開始するために使用するファブリック インターコネクトのみにダウンロードされます。

始める前に

シスコから必要なライセンスを入手します。

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 **[すべて]** > **[ライセンス管理]**を展開します。

ステップ 3 ライセンスをダウンロードするファブリック インターコネクトのノードをクリックします。

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

ステップ 5 [Download License] をクリックします。

ステップ 6 [Download License] ダイアログボックスで、[Location of the Image File] フィールドの [Local File System] オプション ボタンをクリックします。

ステップ 7 [Filename] フィールドに、ライセンス ファイルのフル パスと名前を入力します。

パス名またはファイル名にスペースを含めることはできません。たとえば、`c:\Path\Folder_Name\License.lic` は有効なパスですが、`c:\Path\Folder Name\License.lic` は「`Folder Name`」内にスペースがあるため無効です。

ライセンス ファイルが配置されているフォルダへの正確なパスがわからない場合は、[Browse] をクリックしてファイルに移動します。

ステップ 8 [OK] をクリックします。

Cisco UCS Manager GUI によってファブリック インターコネクトへのライセンスのダウンロードが開始されます。

ステップ 9 （任意） [Download Tasks] タブで、ダウンロードのステータスをモニタします。

（注） Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、**[パッケージ（Packages）]** タブで古いバンドルを削除して、領域を解放します。ブートフラッシュの空き領域を表示するには、ファブリック インターコネクトにナビゲートし、**[機器（Equipment）]** タブをクリックして、**[一般（General）]** タブの **[ローカル ストレージ情報（Local Storage Information）]** 領域を展開します。

ステップ 10 必要なライセンスがすべてファブリック インターコネクトにダウンロードされるまで、このタスクを繰り返します。

次のタスク

すべてのダウンロードタスクが完了した後、ライセンスをインストールします。

リモート ロケーションからファブリック インターコネクトへのライセンスのダウンロード

（注） クラスタ構成の場合、マッチングペアの両方のファブリックインターコネクトにライセンスをダウンロードしてインストールすることをお勧めします。個々のライセンスは、ダウンロードを開始するために使用するファブリック インターコネクトのみにダウンロードされます。

始める前に

シスコから必要なライセンスを入手します。

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 **[すべて]** > **[ライセンス管理]**を展開します。
ステップ 3 ライセンスをダウンロードするファブリック インターコネクトのノードをクリックします。
ステップ 4 [Work] ペインの [Download Tasks] タブをクリックします。
ステップ 5 [Download License] をクリックします。
ステップ 6 [Download License] ダイアログボックスで、[Location of the Image File] フィールドの [Remote File System] オプション ボタンをクリックします。
ステップ 7 プロトコルを指定し、必要な情報を入力します。

パス名またはファイル名にスペースを含めることはできません。たとえば、`c:\Path\Folder_Name\License.lic` は有効なパスですが、`c:\Path\Folder Name\License.lic` は「`Folder Name`」内にスペースがあるため無効です。

（注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメイン が Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン が Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

ステップ 8 [OK] をクリックします。

Cisco UCS Manager GUI によってファブリック インターコネクトへのライセンスのダウンロードが開始されます。

ステップ 9 （任意） [Download Tasks] タブで、ダウンロードのステータスをモニタします。

（注） Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、**[パッケージ（Packages）]** タブで古いバンドルを削除して、領域を解放します。ブートフラッシュの空き領域を表示するには、ファブリックインターコネクトにナビゲートし、**[機器（Equipment）]** タブをクリックして、**[一般（General）]** タブの **[ローカル ストレージ情報（Local Storage Information）]** 領域を展開します。

ステップ 10 必要なライセンスがすべてファブリックインターコネクトにダウンロードされるまで、このタスクを繰り返します。

次のタスク

すべてのダウンロードタスクが完了した後、ライセンスをインストールします。

ライセンスのインストール

始める前に

シスコから必要なライセンスを入手します。

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 **[すべて]** > **[ライセンス管理]**を展開します。

ステップ 3 [Work] ペインの [Downloaded License Files] タブをクリックします。

ステップ 4 テーブルからインストールするライセンスを選択します。

（注） 新しいポート ライセンスをインストールする場合、ダウンタイムは不要で、トラフィックへの影響はありません。

ステップ 5 [Install License] ボタンをクリックします。

ステップ 6 [Install License] ダイアログボックスで、[Yes] をクリックします。

Cisco UCS Manager GUIによってライセンスがインストールされ、未ライセンスのポートまたは機能がアクティブ化されます。

ファブリック インターコネクトにインストールされているライセンスの表示

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 **[すべて]** > **[ライセンス管理]**を展開します。

ステップ 3 [Work] ペインで、[Installed Licenses] タブをクリックし、ファブリック インターコネクトにインストールされているすべてのライセンスの詳細を表示します。

ステップ 4 表内のライセンスをクリックし、[Contents] タブにライセンスの詳細を表示します。

ファイル内の個々のライセンスの詳細を表示するには、ライセンス ファイルを展開する必要があります。

ポートまたは機能に使用できる猶予期間の決定

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 **[すべて]** > **[ライセンス管理]**を展開します。

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 動作状態、適用された猶予期間など機能の詳細を表示するには、テーブル中でその機能をクリックします。

ライセンスの失効日の決定

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 **[すべて]** > **[ライセンス管理]**を展開します。

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

ステップ 4 テーブル内のライセンスをクリックして、ライセンスの詳細を下の [Contents] タブに表示します。

ステップ 5 [Contents] タブでライセンス ファイルを展開して、ファイル内のすべてのライセンスを表示します。

ステップ 6 [Expiry] 列でライセンスの失効日を参照します。

ライセンスのアンインストール

（注） 使用中の永続ライセンスはアンインストールできません。未使用の永久ライセンスだけをアンインストールできます。使用中の永久ライセンスの削除を試みると、その要求は Cisco UCS Manager によって拒否され、エラー メッセージが表示されます。

始める前に

Cisco UCS Manager 設定をバックアップします。

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 **[すべて]** > **[ライセンス管理]**を展開します。

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

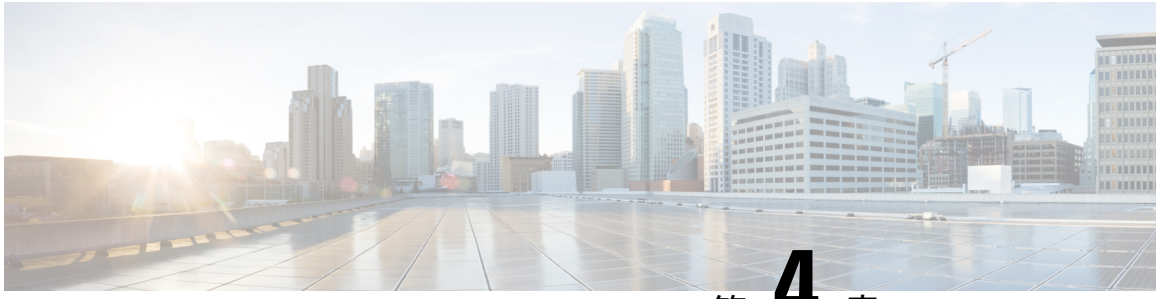
ステップ 4 テーブルからアンインストールするライセンスを選択します。

ステップ 5 [Clear License] ボタンをクリックします。

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。

Cisco UCS Manager はライセンスを非アクティブ化し、ライセンスのリストからそのライセンスを削除し、ファブリック インターコネクトからライセンスを削除します。ポートは、ライセ

ンスなしモードに移行します。クラスタ構成の場合は、他のファブリック インターコネクトからもライセンスをアンインストールする必要があります。



第 4 章

Cisco UCS Central で Cisco UCS ドメインを登録する

- Cisco UCS ドメインの登録 （23 ページ）
- Cisco UCS Manager と Cisco UCS Central 間のポリシー解決 （24 ページ）
- Cisco UCS Central による Cisco UCS ドメイン の登録 （25 ページ）
- Cisco UCS Central 間でのポリシー解決の設定 （26 ページ）
- Cisco UCS Manager での Cisco UCS Central 登録プロパティの設定 （27 ページ）
- Cisco UCS Central から Cisco UCS ドメイン を登録解除する （28 ページ）

Cisco UCS ドメインの登録

データセンター内の Cisco UCS ドメイン の一部またはすべてを Cisco UCS Central が管理するよう設定できます。

Cisco UCS Central に Cisco UCS ドメイン を管理させる場合は、そのドメインを登録する必要があります。登録するときには、 Cisco UCS Central と Cisco UCS Manager で管理するポリシーとその他の構成の種類を選択する必要があります。 Cisco UCS Centralは、登録されているすべての同じタイプのポリシーと構成を管理できますCisco UCS ドメイン。また、登録されている Cisco UCS ドメイン ごとに異なる設定を持つように選択することもできます。

Cisco UCS ドメイン を Cisco UCS Central に登録する前に以下のことを行います。

- Cisco UCS Manager と Cisco UCS Central の両方において NTP サーバーと正しいタイム ゾーンを設定し、それらが同期していることを確認します。Cisco UCS ドメインと Cisco UCS Central の日時が同期していないと、登録に失敗する可能性があります。
- Cisco UCS Central のホスト名または IP アドレスの入手
- Cisco UCS Central を導入したときに設定した共有秘密を入手します。

Cisco UCS Manager と Cisco UCS Central 間のポリシー解決

Cisco UCS Central に登録する各 Cisco UCS ドメインに対して、特定のポリシーや設定を管理するアプリケーションを選択できます。このポリシー解決は、同じ Cisco UCS Central に登録するすべての Cisco UCS ドメインで同じである必要はありません。

（注） Cisco UCS ドメインを Cisco UCS Central から登録解除すると、開かれているセッションはすべて終了します。

これらのポリシーおよび設定を解決するには、次のオプションを使用します。

- [Local]：ポリシーまたは設定は、Cisco UCS Manager によって決定および管理されます。
- [Global]：ポリシーまたは設定は、Cisco UCS Central によって決定および管理されます。

次の表に示すポリシーと設定は、Cisco UCS Manager または Cisco UCS Central のどちらで管理するかを選択できます。

名前	説明
[インフラストラクチャとカタログ ファームウェア（Infrastructure & Catalog Firmware）]	機能カタログとインフラストラクチャ ファームウェア ポリシーを、ローカルで定義するかまたは Cisco UCS Central から取得するかを決定します。
[タイムゾーン管理（Time Zone Management）]	日付と時刻を、ローカルで定義するかまたは Cisco UCS Central から取得するかを決定します。
[通信サービス（Communication Services）	HTTP、CIM XML、Telnet、SNMP、Web セッション制限、管理インターフェイス モニターリング ポリシー設定を、ローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[グローバル障害ポリシー（Global Fault Policy）]	グローバル障害ポリシーをローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[ユーザー管理（User Management）]	認証およびネイティブ ドメイン、LDAP、RADIUS、TACACS+、トラストポイント、ロケールおよびユーザー ロールを、ローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[DNS 管理（DNS Management）]	DNS サーバーをローカルまたは Cisco UCS Central のどちらで定義するかを決定します。

名前	説明
[バックアップおよびエクスポート ポリシー（Backup and Export Policies）]	Full State バックアップ ポリシーおよび All Configuration エクスポート ポリシーを、ローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[モニタリング（Monitoring）]	Call Home、Syslog、TFTP Core Exporter 設定を、ローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[SEL ポリシー（SEL Policy）]	管理対象エンドポイントをローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[電力割り当てポリシー（Power Allocation Policy）]	グローバル電力割り当てポリシーがローカルまたは Cisco UCS Centeral のいずれで定義されるかを決定します。
[電力拡張ポリシー（Powerextended Policy）]	電力拡張ポリシーがローカルまたは Cisco UCS Centeral のいずれで定義されるかを決定します。
[電力節約ポリシー（Powersave Policy）]	電力節約ポリシーがローカルまたは Cisco UCS Centeral のいずれで定義されるかを決定します。
[モジュラ シャーシ ファン制御ポリシー（Modular Chassis Fan Control Policy）]	モジュラ シャーシ ファン制御ポリシーをローカルで定義するか、Cisco UCS Central で定義するかを決定します。
[電力ポリシー（Power Policy）]	電力ポリシーがローカルまたは Cisco UCS Centeral のいずれで定義されるかを決定します。
[機器ポリシー（Equipment Policy]	機器グローバル、LAN クラウド、および SAN クラウドの各ポリシーが、ローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[Port Configuration]	ポート設定をローカルと Cisco UCS Central のどちらで定義するかを指定します。

Cisco UCS Central による Cisco UCS ドメイン の登録

始める前に

Cisco UCS Manager と Cisco UCS Central の両方において NTP サーバーと正しいタイム ゾーンを設定し、それらが同期していることを確認します。Cisco UCS ドメインと Cisco UCS Central の日時が同期していないと、登録に失敗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、[管理者]をクリックします。

ステップ 2 **[すべて]** > **[通信管理]**を展開します。

ステップ 3 [UCS Central] ノードをクリックします。

ステップ 4 [アクション（Actions）] 領域で、[UCS セントラル（UCS Central）] をクリックします。

ステップ 5 [Actions] 領域で、[Register With UCS Central] をクリックします。

ステップ 6 [Register with UCS Central] ダイアログボックスで、次の手順を実行します。

a) 次のフィールドに入力します。

名前	説明
[Hostname/IP Address] フィールド	Cisco UCS Central が展開されている仮想マシンのホスト名または IP アドレス。 （注） IPv4 や IPv6 アドレスではなくホスト名を使用する場合、DNS サーバを設定する必要があります。Cisco UCS ドメインが Cisco UCS Central に登録されていないか、または DNS 管理が [ローカル（local）] に設定されている場合は、Cisco UCS Managerで DNS サーバを設定します。Cisco UCS ドメインが Cisco UCS Central に登録されていて、DNS 管理が [グローバル（global）] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[Shared Secret] フィールド	Cisco UCS Central を導入したときに設定された共有秘密（またはパスワード）

b) [Policy Resolution Control] 領域の各フィールドで、次のいずれかのオプション ボタンをクリックします。

- [Local]：ポリシーまたは設定は、Cisco UCS Manager によって決定および管理されます。
- [Global]：ポリシーまたは設定は、Cisco UCS Central によって決定および管理されます。

c) [OK] をクリックします。

Cisco UCS Central 間でのポリシー解決の設定

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 **[すべて]** > **[通信管理]**を展開します。

ステップ 3 [UCS Central] ノードをクリックします。

ステップ 4 [アクション（Actions）] 領域で、[UCS セントラル（UCS Central）] をクリックします。

ステップ 5 [Policy Resolution Control] 領域の各フィールドで、次のいずれかのオプション ボタンをクリックします。

- [Local]：ポリシーまたは設定は、Cisco UCS Manager によって決定および管理されます。
- [Global]：ポリシーまたは設定は、Cisco UCS Central によって決定および管理されます。

ステップ 6 **[Save Changes]**をクリックします。

Cisco UCS Manager での Cisco UCS Central 登録プロパティの設定

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 **[すべて]** > **[通信管理]**を展開します。

ステップ 3 [UCS Central] ノードをクリックします。

ステップ 4 [アクション（Actions）] 領域で、[UCS セントラル（UCS Central）] をクリックします。

ステップ 5 [Status] 領域で、必要に応じて次を実行します。

a) 使用する [Cleanup Mode] のラジオ ボタンをクリックします。

次のいずれかになります。

- [Localize Global]：Cisco UCS ドメインを登録解除すると、その Cisco UCS ドメイン のすべてのグローバル ポリシーが Cisco UCS Manager 向けにローカライズされます。ポリシーは Cisco UCS ドメイン にとどまり、ポリシーの所有権は Cisco UCS Manager に対してローカルになり、Cisco UCS Manager の管理ユーザーが変更を実施できます。

  （注） Cisco UCS Central に Cisco UCS ドメイン を再登録すると、Cisco UCS Central と Cisco UCS Manager の両方にポリシーが存在するため、ポリシーの競合が発生することがあります。グローバル サービス プロファイルを作成して関連付ける前に、ローカル ポリシーを削除するか、ローカル ポリシーをグローバルに設定してください。

- [Deep Remove Global]：このオプションは、慎重に検討した後でのみ使用してください。Cisco UCS ドメイン の登録を解除すると、その Cisco UCS ドメイン 内のすべてのグローバル ポリシーが削除されます。グローバル サービス プロファイルがある場合、

それらは Cisco UCS Manager のローカル デフォルト ポリシーを参照するようになり、次のいずれかが発生します。

- デフォルトのローカル ポリシーが存在する場合は、サーバーがリブートします。
- デフォルトのローカル ポリシーがない場合は、設定エラーによってサービス プロファイルの関連付けに失敗します。

（注） [Deep Remove Global] クリーンアップ モードでは、Cisco UCS Central からの登録解除時にグローバル VSAN と VLAN は削除されません。必要に応じて、これらを手動で削除する必要があります。

b) （任意）[Suspend State] チェックボックスをオンにします。

オンにすると、Cisco UCS ドメイン が Cisco UCS Central から一時的に削除され、すべてのグローバル ポリシーはローカルの同等のものに戻ります。すべてのサービス プロファイルは、現在の ID が維持します。ただし、グローバル プールは表示されなくなり、新しいサービス プロファイルからアクセスできません。

c) （任意）[Acknowledge State] チェックボックスをオンにします。

Cisco UCS Manager と Cisco UCS Central の間の時間と整合性を表すイベント ID ストリームに差異や矛盾が生じると、Cisco UCS Manager は自身を停止状態にして、Cisco UCS Central から自身を切断します。

このチェックボックスをオンにすると、Cisco UCS Manager と Cisco UCS Central の間に不一致があることを認めた上で、引き続き Cisco UCS ドメインを Cisco UCS Central に再接続することになります。

ステップ 6 **[Save Changes]**をクリックします。

Cisco UCS Central から Cisco UCS ドメイン を登録解除する

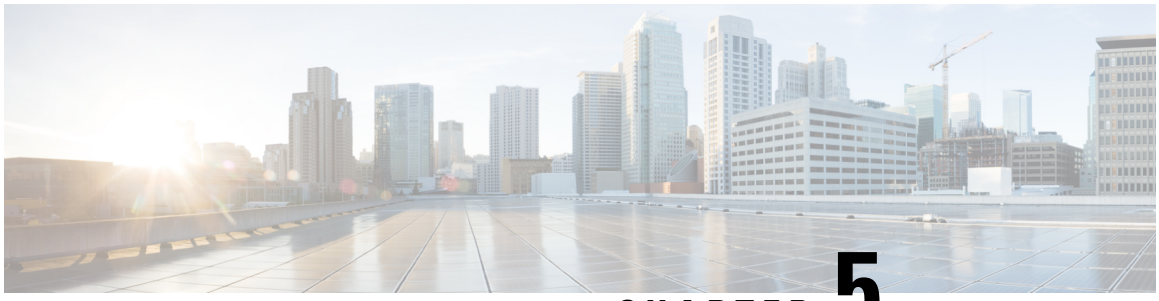
Cisco UCS ドメイン から Cisco UCS Central を登録解除すると、それ以降 Cisco UCS Manager はグローバル ポリシーの更新を受信しません。

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 **[すべて]** > **[通信管理]**を展開します。
ステップ 3 [UCS Central] ノードをクリックします。
ステップ 4 [アクション（Actions）] 領域で、[UCS セントラル（UCS Central）] をクリックします。
ステップ 5 [Actions] 領域で、[Unregister From UCS Central] 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。

ステップ 7 [OK] をクリックします。

Cisco UCS Central を使用して Cisco UCS ドメインを登録解除および登録した場合の影響の詳細については、「Policy Resolution between Cisco UCS Manager and Cisco UCS Central」を参照してください。



CHAPTER 5

Cisco UCS での電力制限と電源管理

- 電力制限 Cisco UCS （31 ページ）
- 電力ポリシーの設定, on page 32
- Cisco UCS サーバーの電源ポリシー （32 ページ）
- 電源ポリシーの設定 （33 ページ）
- 電源の冗長性方式 （34 ページ）
- ポリシー方式のシャーシ グループの電力制限の設定, on page 34
- ポリシー方式のシャーシ グループの電力制限 （34 ページ）
- 電力制御ポリシー （35 ページ）
- Power Saveモード, on page 41
- 音響モード ファン プロファイル, on page 43
- UCS Manager の電源グループ （47 ページ）
- ブレード レベルの電力制限, on page 52
- ファン制御ポリシーの構成, on page 54
- グローバル電力プロファイリング ポリシーの設定, on page 55
- グローバル電力割り当てポリシーの設定, on page 56
- 電源同期ポリシーの設定, on page 58
- ラック サーバーの電源管理 （62 ページ）
- UCS Mini 電源管理 （62 ページ）

電力制限 Cisco UCS

サーバーの最大消費電力は電力制限によって制御できます。また、Cisco UCS Manager での電力割り当ての管理については、ブレードサーバー、UCS C220、C240 M4/M5/M6、C480 M5/C480 M5 ML、C225 M6、 C245 M6 ラック サーバー、UCS Mini、ならびに UCS 混在ドメインでも行えます。

Cisco UCS Manager 以下のもので電力制限をサポートしています。

- UCS 6200 シリーズ Fabric Interconnect
- UCS 6300 シリーズ Fabric Interconnect

- UCS 6324 シリーズ ファブリック インターコネクト（Cisco UCS Mini）
- UCS 6400 シリーズ ファブリック インターコネクト

ポリシー方式のシャーシ グループ電力制限または手動でのブレード レベルの電力制限方式を使用して、シャーシ内のすべてのサーバーに適用される電源を割り当てることができます。

Cisco UCS Manager は、サーバーへの電力割り当てに役立つ次の電源管理ポリシーを提供しています。

電源管理ポリシー	説明
電源ポリシー	Cisco UCS ドメイン 内のすべてのシャーシに電源の冗長性を指定します。
電源制御ポリシー	シャーシ内の各ブレードの初期電源割り当てを計算するための優先順位を指定します。
省電力ポリシー	シャーシをグローバルに管理して、エネルギー効率または可用性を最大化します。
グローバル電力割り当てポリシー	シャーシ内のすべてのサーバーに適用されるポリシー方式のシャーシ グループの電力制限または手動でのブレード レベルの電力制限を指定します。
グローバル電力プロファイリング	サーバーの電力制限値を計算する方法を指定します。有効な場合、サーバーは、ベンチマークを通じて検出中にプロファイリングされます。このポリシーは、グローバル電力割り当てポリシーが Policy Driven Chassis Group Cap に設定されている場合に適用されます。

電力ポリシーの設定

Cisco UCS サーバーの電源ポリシー

電源ポリシーはグローバルで、Cisco UCS Manager インスタンスが管理するすべてのシャーシによって継承されます。サービス プロファイルに電源ポリシーを追加して、Cisco UCS ドメイン内のすべてのシャーシの電源に対して冗長性を指定することができます。このポリシーは PSU ポリシーとも呼ばれます。

電源の冗長性の詳細については、『*Cisco UCS 5108 Server Chassis Hardware Installation Guide*』を参照してください。

電源ポリシーの設定

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 [Global Policies] サブタブをクリックします。

ステップ 5 [Power Policy] 領域で、[Redundancy] フィールドの次のオプション ボタンのいずれかをクリックします。

- **[Non Redundant]**：Cisco UCS Manager は必要最小数の電源装置（PSU）をオンに設定し、それらの PSU 間のロード バランシングを行います。追加の PSU が設置されると、Cisco UCS Manager は追加された装置を「オフ」状態に設定します。いずれかの PSU への電源が切断されると、システムは Cisco UCS Manager が新しい PSU をアクティブ化して負荷の再調整ができるようになるまで、サービスの中断が発生することがあります。

  通常、非冗長動作のために Cisco UCS シャーシに少なくとも 2 台の PSU が必要です。小規模構成（必要電力 7500 ワット未満）の場合にのみ、単一 PSU で電力を供給できます。

- [N+1]：非冗長性を満たす合計数の PSU に加えて、冗長性を与える 1 台の追加 PSU がオンになり、シャーシの電力負荷が均等に分担されます。追加の PSU が設置されると、Cisco UCS Manager は追加された装置を「オフ」状態に設定します。いずれかの PSU への電源が切断されても、Cisco UCS Manager はサービスの中断なしでリカバリできます。

  一般に、N+1 動作のためには、1 つの Cisco UCS シャーシに、少なくとも 3 台の PSU が必要です。

- [Grid]：2 つの電源がオンにされます。そうでなければ、シャーシに N+1 よりも高い冗長性が要求されます。1 つの電源に障害が発生し、そのため 1 台または 2 台の PSU に電源障害が発生した場合、別の電源回路に接続され機能が存続している PSU がシャーシに電力を供給し続けます。

電源の冗長性の詳細については、『*Cisco UCS 5108 Server Chassis Hardware Installation Guide*』を参照してください。

電源の冗長性に加えて、**[省電力ポリシー（Power Save Policy）]** エリアから省電力ポリシーを有効にすることも選択できます。詳細については、省電力モード ポリシー （41 ページ）を参照してください。

ステップ 6 **[Save Changes]**をクリックします。

電源の冗長性方式

PSU 冗長性	最大電力 @ 240 V
グリッド	5000 ワット
N+1	7500 ワット
非冗長	8280 ワット

（注） シャーシ内に 4 つの PSU がインストール済みである場合、このテーブルは有効です。

ポリシー方式のシャーシ グループの電力制限の設定

ポリシー方式のシャーシ グループの電力制限

グローバル制限ポリシーで、ポリシー方式のシャーシ グループの電力制限を選択すると、Cisco UCS では、停電のリスクを負うことなく、サーバーのオーバーサブスクリプションを維持できます。オーバーサブスクリプションは、二重のプロセスによって実現できます。たとえば、Cisco UCS のシャーシ レベルでは、電源グループのメンバー間で使用可能な電力量を分割し、ブレード レベルでは、シャーシに割り当てられた電力量をプライオリティに基づいてブレード間で分割します。

サービス プロファイルの関連付けや関連付け解除が実行されるたびに、Cisco UCS Manager はシャーシ内の各ブレードサーバーへの電力割り当てを再計算します。必要に応じて、優先順位の低いサービス プロファイルの電力が優先順位の高いサービス プロファイルに再分配されます。

データセンターの回路ブレーカーを安全に保護するために、UCS 電源グループは 1 秒未満で電力をキャップします。ブレードは、シャーシの電力配分が最適化されるまで 20 秒間その上限にとどまる必要があります。これは、必要とされる一時的なスパイクに反応することがないよう、意図的によりゆっくりとしたタイムスケールで実行されます。

（注） システムは、各スロットのサーバーを起動するのに十分な電力をリザーブしています。これは、スロットが空の場合でも同様です。このリザーブ電力が、より多くの電力を必要とするサーバーで使用されることはありません。電力制限に準拠しないブレードはペナルティを課されます。

電力制御ポリシー

Cisco UCS は、電力制御ポリシーの優先順位設定をブレード タイプおよび設定とともに使用して、シャーシ内の各ブレードへの初期電力割り当てを計算します。通常の動作中、シャーシ内のアクティブなブレードは、同じシャーシ内のアイドルブレードから電力を借りることができます。すべてのブレードがアクティブで、電力制限に到達した場合は、優先順位が高い電力制御ポリシーを備えたサービスプロファイルが、優先順位の低い電力制御ポリシーを備えたサービス プロファイルよりも優先されます。

優先順位は 1 ～ 10 の段階にランク付けされており、1 が最も高い優先順位、10 が最も低い優先順位を表します。デフォルトのプライオリティは 5 です。

Cisco UCS Manager 3.2(2) 以降、シャーシの動的な電力調整メカニズムがデフォルトで有効になります。このメカニズムはブレードサーバーの電力使用量を継続的に監視し、それに応じて電力割り当てを調整します。シャーシの動的電力調整メカニズムは、Cisco UCS Manager によって設定された全体的なシャーシ電力予算内で動作します。この予算は、使用可能な PSU 電力とグループ電力から計算されます。

ミッションクリティカルなアプリケーションには、**no-cap** という特殊な優先順位も使用できます。優先順位を **no-cap** に設定しても、ブレード サーバーに最大電力が常に供給されるとは限りませんが、シャーシの動的電源調整の予算配分時には、他のサーバーよりもブレード サーバーが優先されます。

（注） すべてのブレード サーバーに no-cap 優先順位が設定されており、そのすべてが電力消費量の高い負荷を実行している場合は、動的な調整により実行された電力配分に基づいて、一部のブレード サーバーが高い電力使用量により制限を受ける可能性があります。

グローバル電力制御ポリシー オプションは、Cisco UCS Manager によって管理されるすべてのシャーシによって継承されます。

Cisco UCS Manager 4.1(3) 以降、省電力モードと呼ばれるグローバル ポリシーを使用できます。デフォルトでは無効になっています。つまり、電源冗長性ポリシーの選択に関係なく、存在するすべての PSU がアクティブなままです。ポリシーを有効にすると、以前の動作が復元されます。

Cisco UCS Manager 4.1(2) 以降、電力制御ポリシーは、静音性が求められる環境の Cisco UCS C220 M5 および C240 M5 ラックサーバのファンの調整にも使用されます。これらのファンの音響設定は、これらのサーバでのみ使用できます。C240 SD M5 ラック サーバでは、音響モードがデフォルトモードです。

Cisco UCS Manager 4.2(1) 以降、電力制御ポリシーは、高温になる可能性のある環境での冷却の調整にも使用されます。このオプションは、Cisco UCS C220 M6、C240 M6、C225 M6、および C245 M6 ラック サーバでのみ使用でき、任意のファン速度オプションで使用できます。

（注） 電力制御ポリシーはサービス プロファイルに含める必要があります。また、このサービス プロファイルをイネーブルにするには、サーバーに関連付ける必要があります。

電力制御ポリシーの作成

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 [Power Control Policies] を右クリックし、[Create Power Control Policy] を選択します。

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

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

名前	説明
[Fan Speed Policy] ドロップダウン	

名前	説明
	（注） Cisco UCS C125 M5 サーバでは、接続しているすべてのサーバに対して同じ**[Fan Speed Policy]**が選択されていることを確認します。Cisco UCS Managerは最後に関連付けるサーバの**[Fan Speed Policy]**を適用します。すべてのサーバに対して同じ **[Fan Speed Policy]** を選択することで、最後に関連付けるサーバに関係なく希望の **[Fan Speed Policy]** が選択されます。 ファン速度は、ラック サーバのみに対応します。次のいずれかになります。 • [低電力（Low Power）]：サーバを冷却し続けるのに必要な最小速度でファンが動作します。 • [Balanced]：ファンはサーバによって生じた熱に基づき、必要に応じてより高速で稼働します。 可能な場合、ファンは必要な最低速度に戻ります。 • [Performance]：ファンは、より高度なサーバ パフォーマンスに必要な速度で維持されます。 これにはより多くの電力が使用されますが、サーバが加熱し始めた場合にファンがすでに高速で稼働していることを意味しています。 （注） **[パフォーマンス（performance）]** オプションは、Cisco UCS C シリーズ M5 と M6 サーバーではサポートされていません。 • [High Power]：ファンは電力消費量よりパフォーマンスを重視した、より高い速度で維持されます。 • [最大電力（Max Power）]：ファン速度が常に最高速度に維持されます。このオプションは最大の冷却効果をもたらしますが、最大の電力を使用します。 •

名前	説明
	[音響 (Acoustic)]: 大きな音響が問題となる環境でのノイズレベルを減らすために、ファン速度を低下させます。他のモードのように、電力消費を調整して、コンポーネントのスロットリングを防止するものでありません。**[音響 (Acoustic)]** オプションを使用すると、短時間のスロットリングが発生しますが、ノイズレベルも低くなります。**[音響（Acoustic）]** モードは、Cisco UCS C220 M5 サーバ、Cisco UCS C240 M5 サーバ、Cisco UCS C240 SD M5 サーバ、Cisco UCS C220 M6サーバ、Cisco UCS C240 M6サーバ、Cisco UCS C225 M6 サーバ、および Cisco UCS C245 M6サーバでのみ利用可能です。 （注） C240 SD M5 、C220 M6、C240 M6、C225 M6、C245 M6 のサーバー上で**[音響（Acoustic）]** モードがデフォルトモードです。他のすべてのプラットフォームでは、**[低電力（Low Power）]** モードがデフォルト モードです。 • [任意（Any）] : サーバが最適なファン速度を決定します。
[急速冷却（Aggressive Cooling）] フィールド	潜在的に高温の熱環境向けのオプション設定です。急速冷却を有効にすると、より多くの電力が消費されますが、過熱の可能性を抑えられます。 **[急速冷却（Aggressive Cooling）]** は、 Cisco UCS C シリーズ M6 ラック サーバーのみサポートします。 2 つのオプションがあります。 • **無効（Disabled）**（デフォルト） • **有効（Enabled）** （注） **[急速冷却（Aggressive Cooling）]** オプションは、ファン速度の設定とは無関係です。

名前	説明
[Power Capping] フィールド	電源グループ内の電力需要が電源装置を超えた場合のサーバの挙動。次のいずれかになります。 • [No Cap]：電源グループ内の他のサーバの電力要求にかかわらず、サーバはフルキャパシティで動作します。 （注） Cisco UCS C-Series M5 、 M6 サーバーで、**[制限なし（No Cap)]** をこのフィールドで選択している場合には、**[パフォーマンス（Performance）]** を **[ファン速度ポリシー（Fan Speed Policy）]** フィールドで選択していないことを確認します。ファン速度ポリシーに **[Performance]** が選択され、パワーキャッピングに **[No Cap]** が選択されている場合、サーバとサービスプロファイルの関連付けが失敗します。 • [Cap]：サーバは、サーバグループ内での他のサーバとの相対的な優先順位に基づいて、最低限の電力容量を割り当てられます。より多くの電力が使用可能になると、Cisco UCS は制限されたサーバが元の割り当て量を超過することを許容します。電源グループで使用可能な総電力にドロップが発生したときのみ割り当てを減らします。 **[cap]** を選択する場合、Cisco UCS Manager GUI は **[Priority]** フィールドを表示します。
[Priority] フィールド	電力制限が有効になったときの、サーバの電力グループ内での優先順位。 1 ～ 10 の整数を入力し、1 が優先順位最高になります。

ステップ 6 [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。

電力制御ポリシーの削除

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。
ステップ 2 **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
ステップ 3 [Power Control 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。

Power Saveモード

省電力モード ポリシー

省電力モードは、中断せずにエネルギー効率（有効な場合）または可用性（無効な場合）のいずれかに重点を置ける、構成可能なシャーシ ポリシーです。デフォルトでは、省電力ポリシーは無効になっています。省電力モード ポリシーを無効にすると、電源冗長性の設定に関係なく、存在するすべてのPSUがアクティブなままになります。省電力ポリシーを有効にすると、電源冗長性ポリシーに従って PSU がアクティブに設定されます。

（注） 現在、要求された電力バジェットが利用可能な電力容量を下回ると、追加の PSU 容量は自動的に省電力モードになります。これにより、アクティブ PSU の効率が向上し、変換損失によるエネルギーの無駄が最小限に抑えられます。ただし、以下のようないくつかのユース ケースでは、このデフォルトの動作が停止につながる可能性があります。

1. 要求された電源ポリシー（グリッド）をサポートするために 2X PSU のみを必要とする軽負荷シャーシで、お客様が PSU 入力電源接続に関する設置ガイドの推奨に従わなかった場合。このシナリオでは、シャーシの 1 つのフィードには両方のアクティブな PSU が接続され、別のフィードには省電力モードの他の 2 つの PSU が接続されています。アクティブな PSU に接続されているフィードが失われると、シャーシ全体でサービスが中断されます。
2. 要求された電源ポリシー（N+1）をサポートするために 3X PSU を必要とする負荷の高いシャーシであり、顧客のラックがシャーシにデュアルフィードを提供している場合。このシナリオでは、3X PSU がアクティブで、1X PSU が省電力モードになっています。（計画的であれ、計画外であれ）アクティブな PSU の 2 つに接続されているフィードが失われ、残りのアクティブな PSU がサポートできるよりも負荷が大きい場合、電力不足が生じる可能性があります。

省電力モード ポリシーは、停止状況を回避するのに役立ちます。

電源ポリシーはグローバルで、Cisco UCS Manager が管理するすべてのシャーシによって継承されます。

電源節約ポリシーの作成

このプロセスを使用して、グローバルな省電力ポリシーを作成します。

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]** ノードをクリックします。
ステップ 3 [Work] ペインの [Policies] タブをクリックします。
ステップ 4 [Global Policies] サブタブをクリックします。
ステップ 5 グローバル省電力ポリシーを有効にするには、**[省電力ポリシー（Power Save Policy）]** 領域で、**[有効（Enable）]** チェックボックスをオンにします。
ステップ 6 **[Save Changes]**をクリックします。

音響モード ファン プロファイル

音響モード ファン プロファイル

音響モード ファン プロファイルはCisco UCS C220 M5 サーバ、C240 M5、C240 SD M5 、C220 M6、C240 M6、C225 M6と C245 M6 ラックサーバーで使用できます。

音響モードのファン ポリシーを設定すると、M5 および M6 ラック サーバーのノイズ レベルを低減できます。M5 および M6 サーバーの大容量ファンは、冷却能力を増やしますが、音響ノイズも大きくなります。M5 および M6 サーバーの標準ファンプロファイル（低電力、バランス、高電力、最大電力）は、エネルギー消費を最適化するためにサーバーを調整するように設計されています。これらのファン プロファイルの主な目的は、CPU と周辺機器のスロットリングを防ぐことです。

音響モードの目的は、ファンの速度を下げて、大きな音響が問題となる環境でのノイズ レベルを減らすことです。音響モードが選択されている場合、電力制限は効果がありません。

音響モードは、Cisco UCS Manager 4.1.1 以降でサポートされています。音響モードは C240 SD M5 、C220 M6、C240 M6、C225 M6 と C245 M6 サーバーのデフォルトモードで、このサーバーの GUI で自動的に選択されます。他のすべての M5 と M6 サーバーでは、デフォルトは低電力です。

音響モードの構成

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 [Power Control Policies] を右クリックし、[Create Power Control Policy] を選択します。これらの手順では [電源制御 (Power Control)] メニューを使用しますが、これらのメニューで管理されるファン ポリシーを作成します。

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

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

名前	説明
[Fan Speed Policy] ドロップダウン	ファン速度は、C シリーズ ラック サーバのみに対応します。音響モードは、Cisco UCS C220 M5、C240 M5、C240 SD M5 、C220 M6、C240 M6 、とC245 M6 ラック サーバーでのみ使用可能なファンポリシーです。 ファンの速度には次のいずれかを指定できます。 • **[音響 (Acoustic)]**: 大きな音響が問題となる環境でのノイズレベルを減らすために、ファン速度を低下させます。**[音響 (Acoustic)]** オプションを選択すると、ノイズ レベルを低下させるために短期的なスロットリングが行われることがあります。 （注） 音響モードを使用する Cisco UCS C シリーズ M5 および M6 サーバーでは、が **[電力制限（Power Capping）]フィールドで自動的に選択されます。音響モードは** C240 SD M5 、C220 M6、C240 M6、C225 M6、とC245 M6ラックサーバーのデフォルトのファン速度ポリシーです。 • [High Power]：ファンは電力消費量よりパフォーマンスを重視した、より高い速度で維持されます。 • [最大電力（Max Power）]：ファン速度が常に最高速度に維持されます。このオプションは最大の冷却効果をもたらしますが、最大の電力を使用します。 • [Any]：サーバが最適なファンの速度を決定します。 （注） **パフォーマンス** モードは、M5 および M6 サーバーでは使用できません。

名前	説明
[Power Capping] フィールド	電源グループ内の電力需要が電源装置を超えた場合に電力制限がかかります。音響モードを使用する Cisco UCS C シリーズ M5 および M6 サーバーでは、が **[電力制限（Power Capping）]** フィールドで自動的に選択されます。 （注） 音響モードは、 C240 SD M5 、C220 M6、C240 M6、C225 M6 と C245 M6 ラック サーバーのデフォルトファン速度ポリシーであり、**上限**オプションとともに自動的に選択されます。 • **制限なし**：音響モードが選択されている場合、サーバの電力スロットリングの優先順位を設定できます。 • **制限**：サーバは、電力スロットリングに必要な音響モードと、サーバ グループ内での他のサーバとの相対的な優先順位に基づいて、電力容量を割り当てられます。 **[制限 (cap)** が選択されると、Cisco UCS Manager GUI に **[優先度 (Priority)]** フィールドが表示されます。
[Priority] フィールド	電力制限が有効になったときの、サーバの電力グループ内での優先順位。 1 ～ 10 の整数を入力し、1 が優先順位最高になります。音響モードのデフォルトは5です。

ステップ 6 [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。

UCS Manager の電源グループ

電源グループは、すべてが同じ配電ユニット（PDU）から電源を得ているシャーシのセットです。Cisco UCS Manager では、1 つ以上のシャーシを含む電源グループを作成し、その電源グループに AC ワット単位でピーク電力キャップを設定することができます。

シャーシ レベルで電力制限を実装するには、以下が必要です。

- IOM、CIMC、および BIOS バージョン 1.4 以上
- 2 つの電源ユニット

ピーク電力キャップは、特定の電源グループ内のすべてのブレードサーバーで使用可能な最大電力を表すスタティック値です。電源グループにブレードを追加、または電源グループからブレードを除外し、手動でピーク電力値を変更しなかった場合、電源グループはピーク電力キャップを調整して、その電源グループ内のすべてのブレードの基本的な電源投入要件に適合させます。

最低 AC 890 ワットが各シャーシに設定されます。これは、空のシャーシに電源を供給するために必要な最低電力量である DC 電力 800 ワットに変換されます。ハーフ幅のブレードを関連付けるには、グループの制限値を AC 電力 1475 ワットに設定する必要があります。フル幅のブレードでは、AC 電力 2060 ワットに設定する必要があります。

シャーシが電源グループに追加されると、シャーシ内のブレードに関連付けられているすべてのサービスプロファイルが、その電源グループの一部になります。同様に、シャーシに新規ブレードを追加すると、そのブレードは、当然のこととして、シャーシの電源グループの一部になります。

（注） 電源グループの作成は、サーバープールの作成とは異なります。ただし、電源修飾子を作成してサーバー プール ポリシーに追加することで、サーバー プールに同じ電源グループのメンバを組み入れることができます。

シャーシを除外または削除すると、そのシャーシは電源グループから削除されます。

UCS Manager は明示的な電源グループと暗黙的な電源グループをサポートしています。

- [Explicit]：電源グループを作成し、シャーシとラックを追加し、グループに電力バジェットを割り当てることができます。
- [Implicit]：電力消費を安全限界内に制限することで、シャーシが常に保護されるようにします。デフォルトでは、明示的な電源グループに属さないすべてのシャーシがデフォルトグループに割り当てられ、適切な制限が設定されます。UCS Manager に接続する新しいシャーシは、別の電源グループに移動するまで、デフォルトの電源グループに追加されます。

次の表は、電源バジェットの割り当て時および電源グループとの連動時に、表示される可能性のあるエラー メッセージを示しています。

エラー メッセージ	Cause	推奨処置
電力グループ POWERGROUP_NAME のバジェットが不十分です（Insufficient budget for power group POWERGROUP_NAME） および/または Chassis N cannot be capped as group cap is low. Please consider raising the cap. および/または Admin committed insufficient for power group GROUP_NAME, using previous value N および/または Power cap application failed for chassis N	シャーシに電力制限を割り当てている状態で下限が満たされなかった場合、またはブレードの追加や電源ポリシーの変更のために電力要件が増えた場合に、これらのメッセージのいずれかが表示されます。	電力制限を、指定された電源グループの [Power Group] ページに表示された [Minimum Power Cap for Allowing Operations (W)] 値まで増やします。
Chassis N cannot be capped as the available PSU power is not enough for the chassis and the blades. Please correct the problem by checking input power or replace the PSU	シャーシの電力バジェット要件が使用可能な PSU 電力を上回っている場合に表示されます。	PSU 入力電力と冗長性ポリシーをチェックし、シャーシ用に十分な電力が使用可能であることを確認します。 PSUに障害がある場合は、PSUを交換します。
Power cap application failed for server N	サーバーが割り当てを超える電力を消費しており、制限できない場合、または電力が割り当てられていないサーバーに電源が投入されている場合に表示されます。	関連付けられていないサーバーの電源をオフにします。

エラー メッセージ	Cause	推奨処置
P-State lowered as consumption hit power cap for server	サーバーが、割り当てられた電力以下に電力消費を削減するよう制限されている場合に表示されます。	これは情報メッセージです。 サーバー電力を制限する必要がない場合は、サービス プロファイルの電力制御ポリシーの [Power Capping] フィールドの値を [no-cap] に設定します。
Chassis N has a mix of high-line and low-line PSU input power sources.	このエラーは、シャーシにハイラインとローラインの PSU 入力電源が混在して接続されている場合に発生します。	これは、サポートされていない設定です。PSU はすべて同様の電源に接続する必要があります。

電源グループの作成

始める前に

グローバル電力割り当てポリシーが [Global Policies] タブで [Policy Driven Chassis Group Cap] に設定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、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 [Power Groups] サブタブをクリックします。

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 Power Group] ウィザードの最初のページで、次のフィールドに値を入力します。

a) 電源グループの一意の名前および説明を入力します。

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

b) [Next] をクリックします。

ステップ 7 [Create Power Group] ウィザードの [Add Chassis Members] ページで、次の手順を実行します。

a) [Chassis] テーブルで、電源グループに含める 1 つ以上のシャーシを選択します。

b) 電源グループに含まれるすべてのシャーシを表示する [Selected Chassis] テーブルにシャーシを追加するには、[>>] ボタンをクリックします。

電源グループから 1 つ以上のシャーシを除外するには、[<<] ボタンを使用します。

c) [Next] をクリックします。

ステップ 8 [Create Power Group] ウィザードの [Add Rack Members] ページで、次の手順を実行します。

a) [Rack Unit] テーブルで、電源グループに含める 1 つ以上のラック ユニットを選択します。
b) 電源グループに含まれるすべてのラックを表示する [Selected Rack Unit] テーブルにラックを追加するには、[>>] ボタンをクリックします。

電源グループから 1 つ以上のラック ユニットを除外するには、[<<] ボタンを使用します。

c) [Next] をクリックします。

ステップ 9 [Create Power Group] ウィザードの [Add FEX Members] ページで、次の手順を実行します。

a) [FEX] テーブルで、電源グループに含める 1 つ以上の FEX を選択します。
b) 電源グループに含まれるすべての FEX を表示する [Selected FEX] テーブルにシャーシを追加するには、[>>] ボタンをクリックします。

電源グループから 1 つ以上の FEX を除外するには、[<<] ボタンを使用します。

c) [Next] をクリックします。

ステップ 10 [Create Power Group] ウィザードの [Add FI Members] ページで、次の手順を実行します。

a) [FI] テーブルで、電源グループに含める 1 つ以上の FI を選択します。
b) 電源グループに含まれるすべてのシャーシを表示する [Selected FI] テーブルに FI を追加するには、[>>] ボタンをクリックします。

電源グループから 1 つ以上の FI を除外するには、[<<] ボタンを使用します。

c) [Next] をクリックします。

ステップ 11 [Create Group Wizard] の [Power Group Attributes] ページで、次の手順を実行します。

a) 次のフィールドに入力します。

名前	説明
[Input Power(W)] フィールド	電源グループで使用可能な最大ピーク時電力（W）。 0 ～ 10000000 の整数を入力します。
[Recommended value for Input Power] フィールド	電源グループのすべてのメンバーに対する入力電力値の推奨範囲。

b) **[完了（Finish）]** をクリックします。

電源グループへのシャーシの追加

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]** ノードをクリックします。

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

ステップ 4 シャーシを追加する電源グループを右クリックし、[Add Chassis Members] を選択します。

ステップ 5 [Add Members Chassis] ダイアログ ボックスで、次のようにします。

a) [Chassis] テーブルで、電源グループに含める 1 つ以上のシャーシを選択します。

b) 電源グループに含まれるすべてのシャーシを表示する [Selected Chassis] テーブルにシャーシを追加するには、[>>] ボタンをクリックします。

電源グループから 1 つ以上のシャーシを除外するには、[<<] ボタンを使用します。

c) [OK] をクリックします。

電源グループからのシャーシの削除

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]** ノードをクリックします。

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

ステップ 4 シャーシを削除する電源グループを展開します。

ステップ 5 電源グループから削除するシャーシを右クリックし、[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。

電源グループの削除

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

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

ステップ 4 削除する電源グループを右クリックして、[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。

ブレード レベルの電力制限

手動によるブレード レベルの電力制限

手動によるブレード レベルの電力制限がグローバル制限ポリシーで設定されている場合は、Cisco UCS ドメインの各ブレード サーバーに対して電力制限を設定できます。

次の設定オプションを使用できます。

- [Watts] ：サーバーが一度に消費可能な最大電力量を指定できます。この最大値には、0 ～ 1300 W の任意の量を指定できます。

（注） 256GB DIMM を使用する B480 M5 システムには、1300 W の手動ブレード レベル 制限が必要です。

- [Unbounded] ：サーバーに対して電力使用制限を課しません。サーバーは、必要なだけ電力を使用できます。

サーバーの電力使用量の瞬間的な上昇がそのサーバーに設定された最大値以上になっても、Cisco UCS Manager によってサーバーが切断またはシャットダウンされることはありません。代わりに、サーバーで使用可能な量まで電力が Cisco UCS Manager によって削減されます。この削減により、サーバーの速度（CPU 速度など）が低下する可能性があります。

（注） 手動によるブレード レベル電力制限は、**[Equipment]** > **[Policies]** > **[Global Policies]** > **[Global Power Allocation Policy]**の順に設定します。電力制御ポリシーで設定された優先順位は関係ありません。

サーバーのブレード レベル電力制限の設定

始める前に

グローバル電力割り当てポリシーが [Global Policies] タブで [Manual Blade Level Cap] に設定されていることを確認してください。

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 電力使用量を設定するサーバを選択します。

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 [Power Budget] 領域で次の手順を実行します。

a) 見出しの右側の [Expand] アイコンをクリックしてフィールドを表示します。

b) 次のフィールドに入力します。

名前	説明
[Admin Status] フィールド	このサーバが電力制限されているかどうか。次のいずれかになります。 • [Unbounded]：どのような場合でもサーバは電力制限されません。 • **[Enabled]**：Cisco UCS Manager GUI は **[Watts]** フィールドを表示します。 （注） 手動ブレード レベルの電力制限は、シャーシで使用可能な電力に関係なく、単一システムの電力消費を制限します。
[Watts] フィールド	要求を満たす十分な電力がシャーシにない場合に、サーバが使用できる最大ワット数です。 値の範囲は 0 ～ 10000000 です。

ステップ 6 **[Save Changes]**をクリックします。

ブレード レベル電力制限の表示

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] > [シャーシ]**を展開します。

ステップ 3 サーバ電力使用量を表示するシャーシを選択します。

ステップ 4 次のいずれかを実行します。

- シャーシ内のすべてのサーバの電力使用量を表示するには、[Work] ペインの [Power] タブをクリックします。
- シャーシ内の 1 台のサーバの電力使用量を表示するには、シャーシを展開して目的のサーバをクリックします。その後、[Work] ペインの [Power] タブをクリックします。

ステップ 5 必要に応じて [Motherboards] ノードを展開し、電力カウンタを表示します。

ファン制御ポリシーの構成

ファン制御ポリシー

ファン制御ポリシーを使ってファンの速度を制御することにより、サーバの消費電力を削減し、ノイズ レベルを下げることができます。ファン制御ポリシーを導入すると、サーバー内のコンポーネントに基づき、そのサーバーに適したファン速度を決定できます。

ファン速度をグローバルに管理すると、一般的な冷却ニーズに基づいて、エンクロージャー内のすべての B シリーズ サーバー ファンに単一のポリシーを適用することで、電力管理に役立ちます。グローバル ポリシーでシャーシごとにファン速度を設定します。

ファン制御ポリシー オプションには次のものがあります。

- **[バランス（Balanced）]**：サーバーで生成された熱に基づき、必要に応じてファン速度を上げます。可能な場合、ファンは必要な最低速度に戻ります。これがデフォルトのオプションです。
- **[低電力（Low Power）]**：サーバーを冷却し続けるのに必要な最小速度でファンが動作します。

ファン制御ポリシーの作成

サーバー構成およびサーバー コンポーネントに基づいて、ファン制御ポリシーを作成し、適切なファン制御設定を決定できます。

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]** ノードをクリックします。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 **[ファン制御ポリシー（Fan Control Policy）]** エリアで、次のオプション ボタンのいずれかをクリックしてファン制御設定を決定します。

- **[バランス（Balanced）]**：この設定は、ほぼすべてのサーバー構成を冷却できます。これがデフォルトのオプションです。
- **[低電力（Low Power）]**：この設定は、最小構成のサーバーに最適です。

ステップ 5 **[Save Changes]**をクリックします。

グローバル電力プロファイリング ポリシーの設定

グローバル電力プロファイリング ポリシー

グローバル電力プロファイリング ポリシーは、電力割り当てをシャーシ内のすべてのサーバーにどのように適用するかを指定します。このポリシーは、グローバル電力割り当てポリシーを [Policy Driven Chassis Group Cap] に設定している場合に適用されます。グローバル電力プロファイリング ポリシーは次のいずれかに設定できます。

- [Disabled]：ブレードの最小/最大電力の制限値は、各コンポーネントの静的消費電力値に基づき算出されています。
- [Enabled]：ブレードの最小/最大電力の制限値は、サーバー ディスカバリの一部として測定されています。これらの値は、ブレードの実際の消費電力とほぼ同じです。

（注） グローバル電力プロファイリング ポリシーを有効にした後、最小/最大電力の上限値を取得するためにブレードを再認識させる必要があります。

グローバル電力プロファイル 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、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 [Global Policies] サブタブをクリックします。

ステップ 5 グローバル電力プロファイル ポリシーをイネーブルにするには、[Global Power Profile Policy] 領域で [Profile Power] チェックボックスをオンにします。

ステップ 6 **[Save Changes]**をクリックします。

グローバル電力割り当てポリシーの設定

グローバル電力割り当てポリシー

グローバル電力割り当てポリシーを使用すると、ポリシー方式のシャーシ グループ電力制限またはブレード レベルの手動電力制限のいずれかの電力割り当て方式をシャーシ内のサーバーに適用できます。

デフォルトのポリシー方式のシャーシ グループ電力制限による電力割り当て方式を適用することを推奨します。

重要 ブレード レベルの手動電力制限の設定に変更を加えると、ポリシー方式のシャーシ グループ電力制限に設定されたグループや設定オプションが失われる結果になります。

グローバル電力割り当てポリシーの設定

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。

ステップ 2 **[機器]** ノードをクリックします。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 [Global Policies] サブタブをクリックします。

ステップ 5 **[Global Power Allocation Policy]** 領域で、Cisco UCS ドメインで使用される電力制限管理モードを設定するために **[Allocation Method]** フィールド で次のラジオ ボタンのいずれかをクリックします。

- [Manual Blade Level Cap]：電力割り当ては、すべてのシャーシの個々のブレード サーバに設定されます。このオプションを選択した場合、電源グループは作成できません。
- [Policy Driven Chassis Group Cap]：電力割り当ては、関連付けられたサービス プロファイルに含まれる電力制御ポリシーによって、シャーシ レベルで設定されます。このオプションを選択すると、Cisco UCS ドメイン に 1 つ以上のシャーシを含む電源グループを作成できます。

デフォルトでは、電力割り当ては電力制御ポリシーによって各シャーシで実行されます。

ステップ 6 **[Save Changes]**をクリックします。

電源投入操作時の電源管理

電源投入時のブート調整

Cisco UCS Manager は、使用可能な電力量に基づいて、できるだけ多くのブレードをブートしようとします。ブレードをブートするために必要な電力が使用できない場合、Cisco UCS Manager は有限状態マシン（FSM）の CheckPowerAvailability ステージでのブートに切り替え、ブレードで「サーバー x/y に電源投入するために使用可能な電力が不足しています」とのエラーが表示されます。

必要な電力が使用可能になると、FSM はブレードの電源投入を続行します。ブレードの電源がオフになった後、割り当てられた電力バジェットは再利用されます。

（注） ブレードに割り当てられた電力バジェットが再利用されると、割り当てられた電力は 0 W として表示されます。

制限事項

Cisco UCS Manager 外でブレードの電源を入れた場合や、割り当てに使用できる電力が十分にない場合は、次の障害が発生します。

```
Power cap application failed for server x/y
```

サービス プロファイルの関連付け中の電力割り当て

サービスプロファイルの関連付け中にブレードに割り当てられる電力は、使用されている電力制御ポリシーと、電力グループから使用可能な電力によって決まります。正常なサービスプロファイルの関連付け中に電力がサーバーに割り当てられた後は、ブレードの最小電力制限が保証されます。電力制御ポリシーの優先度が no-cap に設定されている場合、ブレードには可能な最大電力制限が割り当てられ、表示されている測定済みの最大電力制限を上回る場合があります。

（注） 関連付けられたブレードの優先度が no-cap に変更され、最大電力制限を割り当てることができない場合は、次のいずれかのエラーが表示される場合があります。

- `PSU-insufficient`：PSU に使用可能な電力が不足しています。
- `Group-cap-insufficient`：グループの制限値がブレードには不足しています。

電源同期ポリシーの設定

電源同期ポリシー

Cisco UCS Manager には、関連するサービス プロファイルとサーバー間の電源同期の問題に対処するためにグローバルな（デフォルト）電源同期ポリシーが含まれています。サービスプロファイルの電源状態が、サーバーの実際の電源状態と異なる場合、電源同期ポリシーを使用すると、電源状態を同期することができます。このポリシーを使用すれば、サーバーの関連付けられたサービスプロファイル上の電源状態をいつ同期するかを制御することができます。電源同期ポリシーは他の電源関連ポリシーに影響しません。

電源同期ポリシーは、すべてのサービスプロファイルにデフォルトで適用されます。デフォルトの電源同期ポリシーを削除できませんが、デフォルトのポリシーは編集できます。独自の電源同期ポリシーを作成し、サービス プロファイルに適用できます。また、サービス プロファイルに固有の電源同期ポリシーを作成することもできます。作成したポリシーはデフォルトのポリシーよりも常に優先されます。

Cisco UCS Manager サービスプロファイルで参照されている電源同期ポリシーが存在しない場合、関連付けられたサービスプロファイルに障害を作成します。指定したサービスプロファイルの電源同期ポシリーを作成するか、サービスプロファイル内に存在するポリシーを参照先に変更すれば、Cisco UCS Manager は自動的に障害をクリアします。

電源同期の動作

Cisco UCS Manager は、サーバーの実際の電源状態がオフの場合のみ電源状態を同期します。現在の電源同期の動作は、シャローアソシエーションの後の実際の電源状態と望ましい電源状態に基づいています。

たとえば、次のイベントによりシャロー アソシエーションが行われます。

- ファブリック インターコネクト（FI）と IOM との接続切断。
- IOM のリセット
- FI の停電または再起動
- シャーシの再認識
- シャーシの停電
- サービス プロファイルの変更

次の表では、現在の電源同期動作について説明します。

イベント	望ましい電源状態	イベント前の実際の電源状態	イベント後の実際の電源状態
シャロー アソシエーション	ON	消灯	点灯
シャロー アソシエーション	消灯	消灯	消灯
シャロー アソシエーション	点灯	ON	ON
シャロー アソシエーション	オフ	点灯	ON

電源同期ポリシーの作成

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 [Power Sync Policies] を右クリックし、[Create Power Sync Policy] を選択します。

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

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

名前	説明
[説明（Description）] フィールド	ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Sync-Option] フィールド	物理サーバに関連付けられたサービスプロファイルの目的の電源状態を同期できるオプション。次のいずれかになります。 • [Default Sync]：最初のサーバーアソシエーション後に、設定変更または管理接続を行うと、サーバーの再アソシエーションをトリガーします。このオプションは、物理サーバーの電源状態がオフで、任意の電源状態がオンの場合、必要な電源状態を物理サーバーに同期します。これはデフォルトの動作です。 • [Always Sync]：最初のサーバ アソシエーションまたはサーバ再アソシエーションが行われると、このオプションは物理サーバの電源状態がオンで必要な電源状態がオフの場合であっても、必要な電源状態を物理電源状態に同期します。 • [Initial Only Sync]：このオプションは、サービス プロファイルがサーバに初めて関連付けられた時やサーバが再稼働する時にのみ電源状態をサーバに同期します。このオプションを設定すると、物理サーバ側から電源状態をリセットしてもサービス プロファイルの任意の電源状態には影響しません。

ステップ 6 [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。

電源同期ポリシーの変更

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]** > **[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 [root] ノードからサービス プロファイル ポリシーを選択します。

ステップ 5 [Work] ペインの [Policies] タブをクリックします。

ステップ 6 [Actions] 領域から [Change Power Sync Policy] をクリックします。

表示される情報は、[Select the Power Sync Policy] ドロップダウン リストの選択内容により異なります。次のオプションを選択できます。

- **[No Power Sync Policy]**：このオプションを選択すると、Cisco UCS Manager GUI は他の情報を一切表示しません。このオプションを選択すると、Cisco UCS Manager はデフォルトの電源同期ポリシーを暗黙的に使用します。Cisco UCS Manager はサービスプロファイル組織の下でデフォルトの電源同期ポリシーを検索します。該当するポリシーが見つからない場合、ルートにあるデフォルトの電源同期ポリシーを使用します。
- **[既存の Power Sync ポリシーを使用する（Use an Existing Power Sync Policy）]**：グローバル ポリシーを選択する場合。Cisco UCS Manager GUIは、既存のポリシーを選択できる **[電源同期ポリシー（Power Sync Policy）]** ドロップダウンリストを表示します。
- [Create a Local Power Sync Policy]：このサービス プロファイルでのみアクセス可能な電源同期ポリシーを作成するには、このオプションを選択します。また、[Power Sync Policy] 領域の [Create Power Sync Policy] リンクを使用して電源同期ポリシーを作成することもできます。

電源同期ポリシーの削除

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [Power Sync 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。

ラック サーバーの電源管理

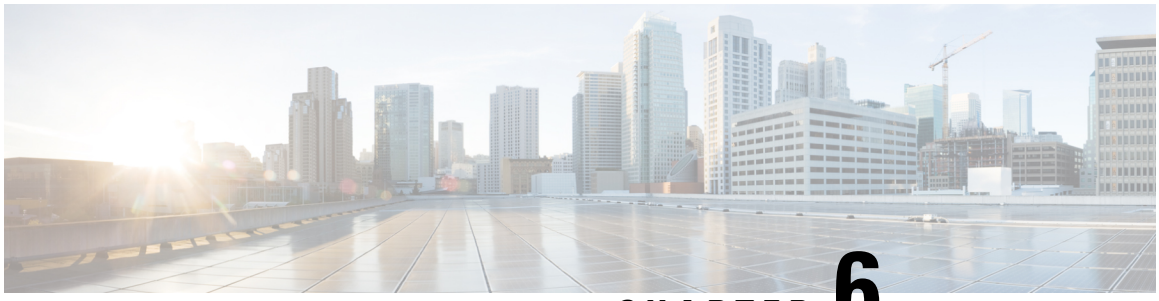
次のラック サーバーでは、パワー キャッピングがサポートされています。

- Cisco UCS C220 M4 サーバ
- Cisco UCS C240 M4 サーバ
- Cisco UCS C220 M5 サーバ
- Cisco UCS C240 M5 サーバ
- Cisco UCS C240 SD M5 サーバ
- Cisco UCS C480 M5 サーバ
- Cisco UCS C480 M5 ML サーバー
- Cisco UCS C220 M6サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C225 M6サーバ
- Cisco UCS C245 M6サーバ

パワーキャッピングは Cisco UCS C125 M5 サーバ ではサポートされません。

UCS Mini 電源管理

リモート オフィスとブランチ サイトに使用され、一部のサーバ導入用の Cisco UCS 6324 ファブリック インターコネクト (FI) でブレード サーバの電源を管理できます。UCS Manager は、Cisco UCS 6324 ファブリック インターコネクトとともに使用する場合に、デュアル ライン電源装置と 110 V をサポートします。110 V 電源はフル装備のシャーシに十分な電力を供給できない場合があるため、110 V 使用時の電力配賦を管理できます。デュアル電源は Cisco UCS Mini 6324 の AC-48V と DC-48V の両方の標準です。



CHAPTER 6

ブレード サーバ ハードウェア管理

- ブレード サーバー管理, on page 64
- ブレード サーバーのブート, on page 66
- サービス プロファイルからのラックマウント サーバのブート （66 ページ）
- ブレード サーバのブート順序の決定 （67 ページ）
- ブレード サーバーのシャットダウン, on page 68
- サービス プロファイルからのサーバのシャットダウン （68 ページ）
- ブレード サーバのリセット, on page 69
- ブレード サーバの出荷時のデフォルト設定へのリセット （70 ページ）
- ブレード サーバの再確認, on page 71
- シャーシからのサーバーの削除, on page 71
- ブレード サーバからのインバンド設定の削除 （72 ページ）
- ブレード サーバーの解放, on page 73
- 存在しないブレード サーバ エントリの削除 （73 ページ）
- ブレード サーバの再稼動 （74 ページ）
- シャーシ内のサーバ スロットの再確認, on page 74
- 存在しないブレード サーバの設定データベースからの削除, on page 75
- ブレード サーバのロケータ LED の切り替え, on page 75
- ブレード サーバのローカル ディスク ロケータ LED のオン/オフ切り替え （76 ページ）
- ブレード サーバーの CMOS のリセット, on page 77
- ブレード サーバーの CIMC のリセット, on page 77
- ブレード サーバーの TPM のクリア, on page 78
- ブレード サーバの POST 結果の表示, on page 78
- ブレード サーバーからの NMI の発行 （79 ページ）
- ブレード サーバのヘルス イベントの表示 （79 ページ）
- ヘルス LED アラーム （81 ページ）
- Smart SSD （82 ページ）

ブレード サーバー管理

Cisco UCS Manager によって、Cisco UCS ドメイン内のすべてのブレード サーバーを管理およびモニターできます。電源状態の変更など一部のブレードサーバー管理タスクは、サーバーおよびサービス プロファイルから実行できます。

残りの管理タスクは、サーバー上でのみ実行できます。

電源装置は、シャーシのブレードが2台以下の場合、省電力モードになります。3台目のブレードがシャーシに追加され、完全に検出されると、電源装置は通常のモードに戻ります。

シャーシ内のブレード サーバー スロットが空の場合、そのスロットに関する情報、エラー、および障害が Cisco UCS Manager から提供されます。サーバー ミスマッチ エラーを解決し、そのスロット内のブレードサーバーを Cisco UCS Manager で再検出するために、スロットを再認識させることもできます。

ブレード サーバーの削除および解放に関するガイドライン

Cisco UCS Manager を使ってブレード サーバーを削除するか解放するかを決定する場合は、次のガイドラインを考慮してください。

ブレード サーバーの解放

物理的に存在し接続されているブレードサーバーを一時的に解放するには、構成から一時的に削除します。サーバー情報の一部は、ブレードサーバーが再稼働する場合に備えて、将来使用するために Cisco UCS Manager によって保持されます。

ブレード サーバーの削除

削除は、ブレード サーバーをシャーシから接続解除して、Cisco UCS Manager から物理的に削除する（取り外す）場合に実行します。ブレードサーバーが物理的に存在し、シャーシに接続しているときは、Cisco UCS Manager から削除できません。ブレード サーバーの物理的な削除が完了すると、そのブレード サーバーの設定を Cisco UCS Manager で削除できます。

削除時、そのブレードサーバーへのアクティブ リンクは無効化され、すべてのエントリがデータベースから削除されます。サーバーは検出時に割り当てられたすべてのサーバー プールから自動的に削除されます。

（注） 自動的に削除されるのは、ディスカバリ中に自動的にサーバー プールへ追加されたサーバーのみです。サーバー プールに手動で追加したサーバーは手動で削除する必要があります。

削除したブレード サーバーを再び設定に追加するには、再び接続して検出する必要があります。Cisco UCS Manager に再導入したサーバーは新規サーバーとみなされ、詳細なディスカバリ プロセスが実施されます。このため、Cisco UCS Manager によって以前とは異なる新しい ID がサーバーに割り当てられることがあります。

予期しないサーバー電力変更を回避するための推奨事項

サーバーがサービス プロファイルに関連付けられていない場合は、サーバーの物理的な [Power] または [Reset] ボタンなど、サーバーの電源状態を変更するために使用可能な手段をすべて使用できます。

サーバーがサービス プロファイルに関連付けられているか、サービス プロファイルに割り当てられている場合は、サーバーの電源状態の変更は次の方法でのみ行う必要があります。

- Cisco UCS Manager GUI で、サーバーに関連付けられたサーバーまたはサービス プロファイルの [General] タブに移動し、[Actions] 領域で [Boot Server] または [Shutdown Server] を選択します。
- Cisco UCS Manager CLI で、サーバー、またはサーバーに関連付けられたサービス プロファイルに対して **power up** または **power down** コマンドを使用します。

重要 電源がオフになっている関連サーバーには、次のオプションのいずれも使用しないでください。

- GUI の [Reset]
- **cycle cycle-immediate**または CLI の**reset hard-reset-immediate**
- サーバーの物理的な [Power] または [Reset] ボタン

現在電源がオフになっているサーバーに対して、リセットまたはサイクルを実施するか、サーバーの物理的な [Power] ボタンを使用すると、サーバーの実際の電力状態がサービス プロファイルで必要とされる電源状態の設定と同期しなくなる可能性があります。サーバーと Cisco UCS Manager 間の通信が中断したり、サービス プロファイルの設定が変更されると、Cisco UCS Managerによって、必要とされる電源の状態がサービスプロファイルからサーバーに適用される場合があり、この結果予期しない電力変化が発生する可能性があります。

電源の同期に関する問題は、次に示すように予期しないサーバーの再起動につながる可能性があります。

サービス プロファイルで必要とされる電源状態	現在のサーバーの電源状態	通信が中断された後のサーバーの電源状態
アップ	電源オフ	[電源オン（Powered On）]

サービス プロファイルで必要とされる電源状態	現在のサーバーの電源状態	通信が中断された後のサーバーの電源状態
ダウン	電源オン	電源オン （注） 実行中のサーバーは、サービスプロファイルに必要とされる電源状態に関係なくシャットダウンされません。

ブレード サーバーのブート

[Actions] 領域で [Boot Server] リンクがグレー表示されている場合は、まず、サーバをシャットダウンする必要があります。

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 **[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 ブートするサーバを選択します。

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 [Actions] 領域の [Boot Server] 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。

サーバがブートされると、[General] タブの [Overall Status] フィールドに [OK] ステータスが表示されます。

サービス プロファイルからのラックマウント サーバのブート

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 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 関連付けられたサーバをブートする必要があるサービス プロファイルを選択します。

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

ステップ 6 [Actions] 領域の [Boot Server] 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 [Boot Server] ダイアログボックスで [OK] をクリックします。

サーバがブートした後は、[General] タブの [Overall Status] フィールドに [ok] ステータスまたは [up] ステータスが表示されます。

ブレード サーバのブート順序の決定

ヒント　サーバに関連付けられているサービス プロファイルの [General] タブからもブート順序タブを表示できます。

手順

ステップ 1 [ナビゲーション]ペインで、[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 ブート順序を決定するサーバをクリックします。

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 [Boot Order Details] 領域が展開されていない場合は、見出しの右側の [Expand] アイコンをクリックします。

ステップ 6 サーバに割り当てられているブート順序を表示するには、[Configured Boot Order] タブをクリックします。

ステップ 7 物理サーバ構成内のさまざまなデバイスから何がブートされるかを表示するには、[Actual Boot Order] タブをクリックします。

（注）　[Actual Boot Order] では、[Internal EFI Shell] は常にブート順リストの最下部に表示されます。

ブレード サーバーのシャットダウン

この手順を使用して、インストールされているオペレーティング システムとともにサーバをシャットダウンした場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown Server] リンクがグレー表示されている場合、そのサーバは動作していません。

Note サービス プロファイルに関連付けられたブレード サーバをシャットダウンすると、VIF ダウン アラート F0283 および F0479 が自動的に制限されます。

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 **[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 シャットダウンするサーバを選択します。

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 [Actions] 領域で、[Shutdown Server] 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。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに電源オフ状態が表示されます。

サービス プロファイルからのサーバのシャットダウン

この手順を使用して、インストールされているオペレーティング システムとともにサーバをシャットダウンした場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown Server] リンクがグレー表示されている場合、そのサーバは動作していません。

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]**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 関連付けられたサーバをシャットダウンする必要があるサービスプロファイルを選択します。

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

ステップ 6 [Actions] 領域で、[Shutdown Server] 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。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに [down] ステータスまたは [power-off] ステータスが表示されます。

ブレード サーバのリセット

サーバをリセットすると、Cisco UCS Manager により、リセット ライン上にパルスが送信されます。オペレーティング システムのグレースフル シャットダウンを選択することができます。オペレーティング システムでグレースフル シャットダウンがサポートされていない場合、サーバ電源の再投入が行われます。サーバをリセットする前に Cisco UCS Manager にすべての管理操作を完了させるオプションの場合、それらの操作がサーバのリセット前に完了する保証はありません。

Note 電源切断状態からサーバをブートする場合は、**[リセット（Reset）]**を使用しないでください。

この手順を使用して電源投入を続けると、サーバの望ましい電源状態が実際の電源状態と同期しなくなり、サーバが後で予期せずシャットダウンすることがあります。選択したサーバを電源切断状態から安全にリブートするには、**[キャンセル（Cancel）]**をクリックし、**[ブート サーバ（Boot Server）]** アクションを選択します。

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 **[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 リセットするサーバを選択します。

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 [Actions] 領域で [Reset] をクリックします。

ステップ 6 [Reset Server] ダイアログボックスで、次の手順を実行します。

a) [Power Cycle] オプションをクリックします。

b) (Optional) このサーバの保留中の管理操作を Cisco UCS Manager によってすべて完了させる場合は、チェックボックスをオンにします。

c) [OK] をクリックします。

リセットが完了するまでに数分かかる場合があります。サーバがリセットされると、[General] タブの [Overall Status] フィールドに OK ステータスが表示されます。

ブレードサーバの出荷時のデフォルト設定へのリセット

ブレードサーバを出荷時の設定にリセットできるようになりました。デフォルトでは、出荷時へのリセット操作は、ストレージ ドライブおよび flexflash ドライブに影響しません。これはデータの損失を防止するためです。ただし、これらのデバイスを既知の状態にリセットすることもできます。

重要 ストレージ デバイスをリセットすると、データが失われる可能性があります。

サーバーを出荷時のデフォルト設定にリセットするには、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、[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 出荷時のデフォルト設定にリセットするサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [Reset to Factory Default] をクリックします。

b) [OK] をクリックします。

ステップ 7 表示される [Maintenance Server] ダイアログ ボックスから適切なオプションを選択します。

- すべてのストレージを削除するには、[Scrub Storage] チェックボックスを選択します。
- すべてのストレージを削除してからすべてのディスクを初期状態に戻すには、[Create Initial Volumes] チェックボックスを選択します。

  [Scrub Storage] チェックボックスを選択した場合のみ、このチェックボックスを選択できます。JBOD をサポートするサーバの場合、ディスクは JBOD 状態になります。JBOD をサポートしないサーバの場合、各ディスクはディスク内のすべての領域を占有する単一 R0 ボリュームで初期化されます。

重要 ストレージプロファイルを使用するには、[Create Initial Volumes] ボックスを選択しないでください。ストレージ プロファイルを使用しているときに初期ボリュームを作成すると、設定エラーが発生する可能性があります。

- すべての flexflash ストレージを削除するには、[Scrub FlexFlash] チェックボックスを選択します。

Cisco UCS Manager サーバを出荷時のデフォルト設定にリセットします。

ブレード サーバの再確認

サーバ、およびそのサーバのエンドポイントすべてを再検出するには、次の手順を実行します。たとえば、サーバがディスカバリ状態など、予期していなかった状態から抜け出せなくなっている場合に、この手順を使用します。

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 **[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 再確認するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Re-acknowledge] をクリックし、次に [OK] をクリックします。

Cisco UCS Manager はサーバを切断し、その後、サーバとシステム内の 1 つまたは複数のファブリック インターコネクトとの接続を確立します。確認が終了するまでに数分かかる場合があります。サーバが確認されると、[General] タブの [Overall Status] フィールドに OK ステータスが表示されます。

シャーシからのサーバーの削除

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）] > [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 シャーシから削除するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Decommission] をクリックし、[OK] をクリックします。

サーバが Cisco UCS構成から削除されます。

ステップ 7 シャーシの物理的な配置場所で、スロットからサーバー ハードウェアを取り外します。

サーバー ハードウェアの取り外し方法については、お使いのシャーシの『*Cisco UCS Hardware Installation Guide*』を参照してください。

What to do next

ブレード サーバを物理的に再設置する場合は、Cisco UCS Managerにそのサーバを再検出させるために、スロットの確認応答を再び行う必要があります。

詳細については、「シャーシ内のサーバ スロットの再確認, on page 74」を参照してください。

ブレード サーバからのインバンド設定の削除

この手順では、ブレード サーバからインバンド管理 IP アドレスの設定を削除します。このアクションがグレー表示されている場合、インバンド設定は完了していません。

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 **[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] > [*Server Name*]** の順に展開します。

ステップ 3 [作業（Work）] 領域の [インベントリ（Inventory）] タブをクリックします。

ステップ 4 [CIMC] サブタブをクリックします。

ステップ 5 [アクション（Actions）] 領域で、[インバンド構成の削除（Delete Inband Configuration）] をクリックします。

ステップ 6 [削除（Delete）] 確認ダイアログボックスで [はい（Yes）] をクリックします。

サーバのインバンド構成が削除されます。

（注） Cisco UCS Manager でインバンド サービス プロファイルがデフォルト VLAN とプール名を使って構成されている場合、ここでインバンド構成を削除した約 1 分後、サーバ CIMC が自動的にインバンド プロファイルからインバンド構成を取得します。

ブレード サーバーの解放

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）] > [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 稼働を停止するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [デコミッション（Decommission）] をクリックします。

b) [OK] をクリックします。

サーバが Cisco UCS構成から削除されます。

存在しないブレード サーバ エントリの削除

サーバを解放してサーバ ハードウェアを物理的に取り外したら、次の手順を実行します。この手順では、**[Decommissioned (デコミッション)]** タブからブレード サーバの既存の古いエントリを削除します。

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 [Work] ペインで [Decommissioned] タブをクリックします。

ステップ 3 リストから削除する各ブレード サーバの行で、[Recommission] カラムのチェックボックスをオンにしてから、[Save Changes] をクリックします。

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。

ブレード サーバの再稼動

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）]** ノードを展開します。

ステップ 3 **[Chassis]** ノードをクリックします。

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

ステップ 5 再稼動する各ブレードサーバの行で、[Recommission] カラムのチェックボックスをオンにしてから、[Save Changes] 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。

ステップ 7 （任意） サーバの再稼動と検出の進行状況を、そのサーバの [FSM] タブでモニタします。

シャーシ内のサーバ スロットの再確認

物理ハードウェアをシャーシから取り外さずにブレード サーバをデコミッションした場合、Cisco UCS Managerにサーバを再検出させて再稼働させるために、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、[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 スロットを再確認するサーバを選択します。

ステップ 4 Cisco UCS Managerに [Resolve Slot Issue] ダイアログボックスが表示された場合は、次のいずれかの手順を実行します。

オプション	説明
[Situation] 領域の [here] リンク	このリンクをクリックし、次に確認ダイアログボックスの **[はい（Yes）]** をクリックします。Cisco UCS Manager はスロットを再確認し、スロット内のサーバーを検出します。
OK	[General] タブに移動するには、このボタンをクリックします。[Actions] 領域の [Reacknowledge Slot] リンクを使用すると、Cisco UCS

オプション	説明
	Managerでスロットを再確認し、スロット内のサーバを検出できます。

存在しないブレードサーバの設定データベースからの削除

サーバを解放せずにサーバ ハードウェアを物理的に外した場合は、次の手順を実行します。サーバが物理的に存在する場合はこの手順を実行できません。

サーバを物理的に削除するには、シャーシからのサーバーの削除, on page 71 を参照してください。

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）] > [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 設定データベースから削除するサーバを選択します。

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 [Actions] 領域で、[Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Remove] をクリックし、[OK] をクリックします。

Cisco UCS Manager は、設定データベースからそのサーバに関するすべてのデータを削除します。サーバ スロットは、新しいサーバ ハードウェアの挿入に使用できます。

ブレード サーバのロケータ LED の切り替え

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）] > [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 ロケータ LED のオン/オフを切り替えるサーバを選択します。

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 [Actions] 領域で、次のいずれかをクリックします。

- [Turn on Locator LED]：選択したサーバの LED を点灯します。
- [Turn on Locator LED]：選択したサーバの LED を消灯します。
- **[Turn on Master Locator LED]**：Cisco UCS B460 M4 ブレード サーバで、マスター ノードの LED を点灯します。
- **[Turn off Master Locator LED]**：Cisco UCS M4 ブレード サーバで、マスター ノードの LED を消灯します。
- **[Turn on Slave Locator LED]**：Cisco UCS B460 M4 ブレード サーバで、スレーブ ノードの LED を点灯します。
- **[Turn off Locator LED]**：Cisco UCS B460 M4 ブレード サーバで、スレーブ ノードの LED を消灯します。

ブレード サーバのローカル ディスク ロケータ LED のオン/オフ切り替え

始める前に

- ディスクが配置されるサーバの電源が投入されていることを確認します。サーバがオフの場合、ローカル ディスクのロケータ LED のオン/オフを切り替えることはできません。

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 **[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 ディスクのロケータ LED のオン/オフを切り替えるサーバを選択します。

ステップ 4 [Work] ペインで、**[Inventory]** > **[Storage]** > **[Disks]** タブの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 5 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 6 [Details] 領域で、[Toggle Locator LED] をクリックします。
[Locator LED] の状態が [On] の場合は、[Off] に切り替わります。[Locator LED] の状態が [Off] の場合は、[On] に切り替わります。

ステップ 7 [Save Changes] をクリックします。

ブレード サーバーの CMOS のリセット

サーバのトラブルシューティングに CMOS のリセットが必要になることがあります。CMOS のリセットは、通常のサーバメンテナンスには含まれません。

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）] > [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 CMOS をリセットするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CMOS] をクリックし、[OK] をクリックします。

ブレード サーバーの CIMC のリセット

ファームウェアで、サーバのトラブルシューティングにCIMCのリセットが必要になることがあります。CIMCのリセットは、通常のサーバメンテナンスには含まれません。CIMCをリセットすると、CIMC はブレード サーバの管理コントローラを再起動します。

CIMCをリセットすると、CIMCがリブートするまで、Cisco UCSの電力モニタリング機能が短時間使用不能になります。通常、リセットは20秒しかかかりませんが、その間にピーク電力キャップを超える可能性はあります。低い電力制限が設定された環境で、設定された電力制限を超えないようにするには、CIMC のリブートまたはアクティブ化を交互に実施することを検討してください。

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）] > [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 CIMC をリセットするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CIMC (Server Controller)] をクリックし、[OK] をクリックします。

ブレード サーバーの TPM のクリア

TPM がサポートされている Cisco UCS M4 以降のブレード サーバーおよびラックマウント サーバーでのみ、TPM をクリアできます。

⚠

Caution TPM のクリアは危険性のある操作です。OS が起動を停止することがあります。また、データを損失する可能性もあります。

Before you begin

TPM が有効である必要があります。

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 **[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 TPM をクリアするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Clear TPM] をクリックし、[OK] をクリックします。

ブレード サーバの POST 結果の表示

サーバとそのアダプタに対する Power On Self-Test プロセスで収集された任意のエラーを表示できます。

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 **[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 POST の結果を表示するサーバを選択します。

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 [Actions] 領域で [View POST Results] をクリックします。

[POST Results] ダイアログボックスに、サーバとそのアダプタに対する POST の結果が一覧表示されます。

ステップ 6 (Optional) アダプタのプロパティを表示するには、[Affected Object] カラムをクリックします。

ステップ 7 [OK] をクリックして [POST Results] ダイアログボックスを閉じます。

ブレード サーバーからの NMI の発行

システムの無応答状態が続き、Cisco UCS Managerによって IMC から BIOS またはオペレーティング システムに NMI（マスク不能割り込み）を発行する必要がある場合には、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

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）] > [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 NMI を発行するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [Diagnostic Interrupt] をクリックします。

b) [OK] をクリックします。

Cisco UCS Manager BIOS またはオペレーティング システムに NMI を送信します。

ブレード サーバのヘルス イベントの表示

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 ヘルス イベントを表示するサーバを選択します。

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

このサーバでトリガーされたヘルス イベントが表示されます。このタブのフィールドは次のとおりです。

名前	説明
[Health Summary] 領域	
[Health Qualifier] フィールド	コンポーネントに対してトリガーされるすべてのヘルス イベントのカンマ区切りの名前。
[Health Severity] フィールド	コンポーネントに対してトリガーされるすべてのステータスイベントの最高シビラティ（重大度）。次のいずれかになります。 • **critical** • **major** • **minor** • **warning** • **info** • **cleared** （注） シビラティ（重大度）レベルが最高のものから順に記載されています。
[Health Details] 領域	
[Severity] カラム	ヘルス イベントのシビラティ（重大度）。次のいずれかになります。 • **critical** • **major** • **minor** • **warning** • **info** • **cleared** （注） シビラティ（重大度）レベルが最高のものから順に記載されています。
[Name] カラム	ヘルス イベントの名前。
[Description] カラム	ヘルス イベントの詳細。

名前	説明
[Value] カラム	ヘルス イベントの現在の値。
[Details] 領域	[Details] 領域には、[Health Details] 領域で選択するヘルス イベントの [Name] 、[Description] 、[Severity] および [Value] の詳細が表示されます。

ヘルス LED アラーム

ブレード ヘルス LED は各 Cisco UCS B シリーズ ブレード サーバーの前面にあります。Cisco UCS Manager を使用すると、ブレード ヘルス LED の色が緑からオレンジ、または点滅しているオレンジに変わるセンサーの障害を確認できます。

ヘルス LED アラームには次の情報が表示されます。

名前	説明
[Severity] カラム	アラームのシビラティ（重大度）。次のいずれかになります。 • [クリティカル（Critical）] : ブレード ヘルス LED がオレンジで点滅します。これは赤色のドットで示されます。 • [Minor] : ブレードヘルス LED がオレンジに点灯します。これはオレンジ色のドットで示されます。
[Description] カラム	アラームの簡単な説明。
[Sensor ID] カラム	アラームをトリガーしたセンサーの ID。
[Sensor Name] カラム	アラームをトリガーしたセンサーの名前。

ヘルス LED アラームの表示

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 ヘルス LED アラームを表示する対象のサーバをクリックします。

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、[View Health LED Alarms] をクリックします。

[View Health LED Alarms] ダイアログボックスに、選択したサーバのヘルス LED アラームが一覧表示されます。

ステップ 6 [OK] をクリックして、[View Health LED Alarms] ダイアログボックスを閉じます。

Smart SSD

Cisco UCS Manager リリース 3.1(3) から、SSD ヘルスのモニターリングがサポートされています。この機能は Smart SSD と呼ばれます。消耗ステータス（日数）、残り耐用期間のパーセンテージなどのプロパティに関する統計情報が表示されます。プロパティごとに最小値、最大値、平均値が記録され、表示されます。この機能では、プロパティのしきい値制限も表示されます。

（注） Smart SSD 機能は、一部の SSD でのみサポートされています。HDD ではサポートされていません。

サポートされる SSD の SATA レンジは次のとおりです。

- Intel
- Samsung
- Micron

サポートされる SSD の SAS レンジは次のとおりです。

- 東芝
- Sandisk
- Samsung
- Micron

（注）
- SAS SSD では [Power Cycle Count] は使用できません。
- スマート SSD 機能は、 M4 サーバー以降のみにサポートされいています。

SSD ヘルスのモニタリング

手順

ステップ 1 **[Equipment (機器)]** > **[Rack-Mounts (ラックマウント)]** > **[Servers (サーバ)]** > **[Server Number (サーバ番号)]** > **[Inventory (インベントリ)]** > **[Storage (ストレージ)]** に移動します。

ステップ 2 SSD ヘルスを表示するコントローラ コンポーネントをクリックします。

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

ステップ 4 ヘルス プロパティを表示する SSD をクリックします。

次の値を確認します。

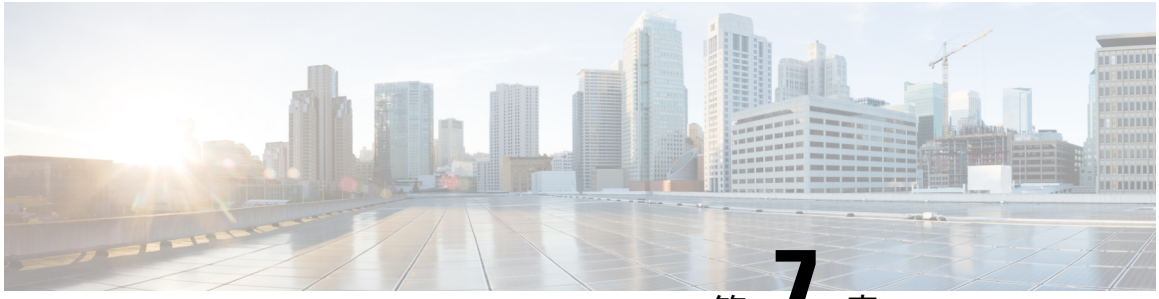
- [PercentageLifeLeft]：耐用期間を表示します。これにより、必要に応じてアクションを実行できます。
- [PowerCycleCount]：サーバのリブートで SSD の電源が再投入された回数を示します。
- [PowerOnHours]：SSD の電源がオンになっている期間を示します。要件に基づいて SSD を交換するか、またはオフにできます。

  （注） 他のプロパティが変化した場合は、更新後の [PowerOnHours] が表示されます。

- [WearStatusInDays]：特定の時点でのワークロード特性に基づいて、SSD の消耗状況に関するガイダンスが示されます。

  （注） これらの値は 1 時間ごとに更新されます。

  これらの値に対してしきい値制限を指定できます。これにより、値がそのしきい値制限に達するかまたは超過するとエラーとなります。Smart SSD 機能は温度を追跡します。温度がしきい値制限 (90°C) を超え、これが原因でディスクが劣化状態になり、劣化の理由が通知されると、エラーを示します。



第 7 章

ラックマウント サーバ ハードウェア管理

- ラックマウント サーバー管理 （86 ページ）
- ラックエンクロージャ サーバー管理 （86 ページ）
- ラックマウント サーバーの削除および解放に関するガイドライン （87 ページ）
- 予期しないサーバー電力変更を回避するための推奨事項 （88 ページ）
- ラックマウント サーバーのブート （89 ページ）
- サービス プロファイルからのラックマウント サーバのブート （90 ページ）
- ラックマウント サーバのブート順序の決定 （90 ページ）
- ラックマウント サーバーのシャットダウン （91 ページ）
- サービス プロファイルからのサーバのシャットダウン （92 ページ）
- ラックマウント サーバのリセット （92 ページ）
- ラックマウント サーバーの出荷時のデフォルト設定へのリセット （93 ページ）
- 永続メモリ スクラブ （94 ページ）
- ラックマウント サーバの再確認 （95 ページ）
- ラックマウント サーバからのインバンド設定の削除 （96 ページ）
- ラックマウント サーバーの解放 （96 ページ）
- ラックマウント サーバの再稼動 （97 ページ）
- ラックマウント サーバーの番号付け直し （97 ページ）
- 存在しないラックマウント サーバの設定データベースからの削除 （98 ページ）
- ラックマウント サーバのロケータ LED の切り替え, on page 99
- ラックマウント サーバのローカル ディスク ロケータ LED のオン/オフ切り替え （99 ページ）
- ラックマウント サーバーの CMOS のリセット （100 ページ）
- ラックマウント サーバーの CIMC のリセット （101 ページ）
- ラックマウント サーバーの TPM のクリア, on page 101
- ラックマウント サーバーからの NMI の発行 （102 ページ）
- ラックマウント サーバのヘルス イベントの表示 （103 ページ）
- ラックマウント サーバの POST 結果の表示 （104 ページ）
- Power Transition Log の表示 （105 ページ）
- Cisco UCS C125 M5 サーバスロット ID の表示 （105 ページ）

ラックマウント サーバー管理

Cisco UCS Manager を使用して、Cisco UCS ドメインに統合されているすべてのラックマウント サーバーを管理およびモニターすることができます。電力制限を除くすべての管理およびモニターリング機能がラックマウント サーバーでサポートされます。電源状態の変更など一部のラックマウント サーバー管理タスクは、サーバーとサービス プロファイルの両方から行うことができます。残りの管理タスクは、サーバー上でのみ実行できます。

Cisco UCS Manager は、検出された各ラックマウント サーバーに関する情報、エラー、および障害を提供します。

ヒント　サポートされる Cisco UCS ラックマウント サーバーと Cisco UCS Manager との統合方法については、ご使用の Cisco UCS Manager のリリースに応じた Cisco UCS C シリーズ サーバー統合ガイドまたは Cisco UCS S シリーズ サーバー統合ガイドを参照してください。

ラックエンクロージャ サーバー管理

このガイドで特に明記されていない限り、リリース4.0(1a)以降のCisco UCS ManagerではCisco UCS C125 M5 サーバの既存の機能すべてがサポートされます。

Cisco UCS C125 M5 サーバは Cisco UCS C4200 シリーズ ラック サーバ シャーシに収容されています。各 Cisco UCS C4200 シリーズ ラック サーバ シャーシは、2 ー 4個の Cisco UCS C125 M5 サーバノードをサポートします。Cisco UCS C125 M5 サーバノードを管理するため、Cisco UCS Managerは以下をサポートします。

- **ラック**：

  Cisco UCS ManagerGUI パス -**[Equipment]** > **[Rack-Mounts]** > **[Enclosures]**

  示Cisco UCS Managerにより管理されているすべての Cisco UCS C4200 シリーズ ラック サーバ シャーシのリストを表示します。

- **[Rack Enclosure]*rack_enclosure_number*:**

  Cisco UCS Manager GUI パス：**Equipment** > **Rack-Mounts** > **Enclosures** > **Rack Enclosure** ***rack_enclosure_number***

  各**[Rack Enclosure]**は、1 個の Cisco UCS C4200 シリーズ ラック サーバ シャーシであり、最大 4 つのCisco UCS C125 M5 サーバノード、4 つのファン ユニット、2 つの PSU を含むことができます。サーバのスロット ID については、Cisco UCS C125 M5 サーバスロット ID の表示 （105 ページ）を参照してください。

Cisco UCS C125 M5 サーバは、**[Rack Enclosure]*rack_enclosure_number***から他のラック サーバと同じ方法で管理できます。

（注） Cisco UCS C125 M5 サーバ では Cisco UCS 6400 シリーズ ファブリック インターコネクト および Fabric Interconnect 6300 シリーズをサポートします。

ラックマウントサーバーの削除および解放に関するガイドライン

Cisco UCS Manager を使ってラックマウント サーバーを削除するか解放するかを決定する場合は、次のガイドラインを考慮してください。

ラックマウント サーバーの解放

解放は、ラックマウントサーバーが物理的に存在し接続されているが、一時的に設定から削除する必要がある場合に実行します。解放されたラックマウントサーバーは最終的に再稼働することが予測されるので、サーバーの情報部分は、将来の使用に備え、Cisco UCS Managerによって保持されます。

ラックマウント サーバーの削除

削除は、ラックマウント サーバーをファブリック エクステンダから接続解除して、システムから物理的に削除する（取り外す）場合に実行します。ラックマウントサーバーが物理的に存在し、ファブリック エクステンダに接続しているときは、Cisco UCS Manager から削除できません。ラックマウント サーバーの接続を解除した後、その設定を Cisco UCS Manager から削除できます。

削除時、管理インターフェイスは接続解除され、すべてのエントリがデータベースから削除されます。サーバーは検出時に割り当てられたすべてのサーバープールから自動的に削除されます。

（注） 自動的に削除されるのは、検出時に自動的にサーバープールに追加されたサーバーのみです。サーバー プールに手動で追加したサーバーは手動で削除する必要があります。

削除したラックマウントサーバーを再び設定に追加する場合は、再接続して再度検出する必要があります。Cisco UCS Managerに再導入したサーバーは新規サーバーとみなされ、詳細なディスカバリ プロセスが実施されます。このため、Cisco UCS Manager によって以前とは異なる新しい ID がサーバーに割り当てられることがあります。

予期しないサーバー電力変更を回避するための推奨事項

サーバーがサービスプロファイルに関連付けられていない場合は、サーバーの物理的な [Power] または [Reset] ボタンなど、サーバーの電源状態を変更するために使用可能な手段をすべて使用できます。

サーバーがサービス プロファイルに関連付けられているか、サービス プロファイルに割り当てられている場合は、サーバーの電源状態の変更は次の方法でのみ行う必要があります。

- Cisco UCS Manager GUI で、サーバーに関連付けられたサーバーまたはサービス プロファイルの [General] タブに移動し、[Actions] 領域で [Boot Server] または [Shutdown Server] を選択します。
- Cisco UCS Manager CLI で、サーバー、またはサーバーに関連付けられたサービス プロファイルに対して **power up** または **power down** コマンドを使用します。

重要 電源がオフになっている関連サーバーには、次のオプションのいずれも使用しないでください。

- GUI の [Reset]
- **cycle cycle-immediate** または CLI の **reset hard-reset-immediate**
- サーバーの物理的な [Power] または [Reset] ボタン

現在電源がオフになっているサーバーに対して、リセットまたはサイクルを実施するか、サーバーの物理的な [Power] ボタンを使用すると、サーバーの実際の電力状態がサービス プロファイルで必要とされる電源状態の設定と同期しなくなる可能性があります。サーバーと Cisco UCS Manager 間の通信が中断したり、サービス プロファイルの設定が変更されると、Cisco UCS Managerによって、必要とされる電源の状態がサービスプロファイルからサーバーに適用される場合があり、この結果予期しない電力変化が発生する可能性があります。

電源の同期に関する問題は、次に示すように予期しないサーバーの再起動につながる可能性があります。

サービス プロファイルで必要とされる電源状態	現在のサーバーの電源状態	通信が中断された後のサーバーの電源状態
アップ	電源オフ	[電源オン（Powered On）]

サービス プロファイルで必要とされる電源状態	現在のサーバーの電源状態	通信が中断された後のサーバーの電源状態
ダウン	電源オン	電源オン （注） 実行中のサーバーは、サービスプロファイルに必要とされる電源状態に関係なくシャットダウンされません。

ラックマウント サーバーのブート

[Actions] 領域で [Boot Server] リンクがグレー表示されている場合は、まず、サーバをシャットダウン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、[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 ブートするサーバを選択します。

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 [Actions] 領域の [Boot Server] 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。

サーバがブートされると、[General] タブの [Overall Status] フィールドに [OK] ステータスが表示されます。

サービス プロファイルからのラックマウント サーバのブート

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 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 関連付けられたサーバをブートする必要があるサービス プロファイルを選択します。

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

ステップ 6 [Actions] 領域の [Boot Server] 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 [Boot Server] ダイアログボックスで [OK] をクリックします。

サーバがブートした後は、[General] タブの [Overall Status] フィールドに [ok] ステータスまたは [up] ステータスが表示されます。

ラックマウント サーバのブート順序の決定

ヒント　サーバに関連付けられているサービス プロファイルの [General] タブからもブート順序タブを表示できます。

手順

ステップ 1 [ナビゲーション]ペインで、[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 ブート順序を決定するサーバをクリックします。

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 [Boot Order Details] 領域が展開されていない場合は、見出しの右側の [Expand] アイコンをクリックします。

ステップ 6 サーバに割り当てられているブート順序を表示するには、[Configured Boot Order] タブをクリックします。

ステップ 7 物理サーバ構成内のさまざまなデバイスから何がブートされるかを表示するには、[Actual Boot Order] タブをクリックします。

（注） [Actual Boot Order] では、[Internal EFI Shell] は常にブート順リストの最下部に表示されます。

ラックマウント サーバーのシャットダウン

この手順を使用して、インストールされているオペレーティング システムとともにサーバをシャットダウンした場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown server] リンクがグレー表示されている場合、そのサーバは動作していません。

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]** > **[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 シャットダウンするサーバを選択します。

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 [Actions] 領域で、[Shutdown Server] 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。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに電源オフ状態が表示されます。

サービス プロファイルからのサーバのシャットダウン

この手順を使用して、インストールされているオペレーティング システムとともにサーバをシャットダウンした場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown Server] リンクがグレー表示されている場合、そのサーバは動作していません。

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]**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 関連付けられたサーバをシャットダウンする必要があるサービスプロファイルを選択します。

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

ステップ 6 [Actions] 領域で、[Shutdown Server] 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。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに [down] ステータスまたは [power-off] ステータスが表示されます。

ラックマウント サーバのリセット

サーバをリセットすると、Cisco UCS Manager により、リセット ライン上にパルスが送信されます。オペレーティング システムのグレースフル シャットダウンを選択することができます。オペレーティング システムでグレースフル シャットダウンがサポートされていない場合、サーバ電源の再投入が行われます。サーバをリセットする前に Cisco UCS Manager にすべての管理操作を完了させるオプションの場合、それらの操作がサーバのリセット前に完了する保証はありません。

（注） 電源切断状態からサーバをブートする場合は、**[リセット（Reset）]** を使用しないでください。

この手順を使用して電源投入を続けると、サーバの望ましい電源状態が実際の電源状態と同期しなくなり、サーバが後で予期せずシャットダウンすることがあります。選択したサーバを電源切断状態から安全にリブートするには、**[キャンセル（Cancel）]** をクリックし、**[ブート サーバ（Boot Server）]** アクションを選択します。

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]** > **[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 リセットするサーバを選択します。

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 [Actions] 領域で [Reset] をクリックします。

ステップ 6 [Reset Server] ダイアログボックスで、次の手順を実行します。

a) [Power Cycle] オプションをクリックします。

b) （任意） このサーバの保留中の管理操作を Cisco UCS Manager によってすべて完了させる場合は、チェックボックスをオンにします。

c) [OK] をクリックします。

リセットが完了するまでに数分かかる場合があります。サーバがリセットされると、[General] タブの [Overall Status] フィールドに OK ステータスが表示されます。

ラックマウントサーバーの出荷時のデフォルト設定へのリセット

ラックマウント サーバーを出荷時の設定にリセットできるようになりました。デフォルトでは、出荷時へのリセット操作は、ストレージ ドライブおよび flexflash ドライブなどのストレージに影響しません。これはデータの損失を防止するためです。ただし、これらのデバイスを既知の状態にリセットすることもできます。

重要 ストレージ デバイスをリセットすると、データが失われる可能性があります。

サーバーを出荷時のデフォルト設定にリセットするには、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、[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 出荷時のデフォルト設定にリセットするサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Reset to Factory Default] をクリックし、[OK] をクリックします。

ステップ 7 表示される [Maintenance Server] ダイアログ ボックスから適切なオプションを選択します。

- すべてのストレージを削除するには、[Scrub Storage] チェックボックスを選択します。
- すべてのストレージを削除してからすべてのディスクを初期状態に戻すには、[Create Initial Volumes] チェックボックスを選択します。

  [Scrub Storage] チェックボックスを選択した場合のみ、このチェックボックスを選択できます。JBOD をサポートするサーバの場合、ディスクは JBOD 状態になります。JBOD をサポートしないサーバの場合、各ディスクはディスク内のすべての領域を占有する単一 R0 ボリュームで初期化されます。

  重要 ストレージプロファイルを使用するには、[Create Initial Volumes] チェックボックスを選択しないでください。ストレージプロファイルを使用しているときに初期ボリュームを作成すると、設定エラーが発生する可能性があります。

- すべての flexflash ストレージを削除するには、[Scrub FlexFlash] チェックボックスを選択します。
- Persistent Memory ストレージをすべて削除するには、**[永続メモリ スクラブ（Persistent Memory Scrub）]** チェックボックスをオンにします。

Cisco UCS Manager サーバを出荷時のデフォルト設定にリセットします。

永続メモリ スクラブ

永続メモリ スクラブを使用すると、サーバの永続メモリ モジュールから永続メモリの設定とデータを削除することができます。

Cisco IMC では、永続メモリ モジュールを工場出荷時の初期状態にリセットすることにより、永続メモリをスクラブできます。

Cisco UCS Manager では、次の方法のいずれかを使用して永続メモリをスクラブできます。

- 永続メモリ スクラブ オプション設定が [yes (はい)] に設定されたサービス プロファイルおよびスクラブ ポリシーとの関連付け解除

- 永続メモリ スクラブ オプションが [yes (はい)] に設定されたサーバでの **工場出荷時のデフォルト動作へのリセット** の実行
- ゴールの削除

永続的メモリ スクラブが完了すると、次のことが発生します。

- すべての永続メモリ データが消去されます。
- 永続メモリの設定はが工場出荷時のデフォルト設定にリセットされます。

  B シリーズおよびC シリーズ サーバの場合、100% のメモリ モードが適用されます。S シリーズ サーバの場合、0% のメモリ モードとアプリケーションのダイレクト非インターリーブ タイプが に適用されます。
- 永続メモリ モジュールのセキュリティが無効になっています。

ラックマウント サーバの再確認

サーバ、およびそのサーバのエンドポイントすべてを再検出するには、次の手順を実行します。たとえば、サーバがディスカバリ状態など、予期していなかった状態から抜け出せなくなっている場合に、この手順を使用します。

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]** > **[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 再確認するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [Re-acknowledge] をクリックします。

b) [OK] をクリックします。

Cisco UCS Manager サーバを切断し、その後、サーバとシステム内の 1 つまたは複数のファブリック インターコネクトとの接続を確立します。確認が終了するまでに数分かかる場合があり

ます。サーバが認識されると、[General] タブの [Overall Status] フィールドに [OK] ステータスが表示されます。

ラックマウント サーバからのインバンド設定の削除

この手順では、ラック サーバからインバンド管理 IP アドレスの設定を削除します。このアクションがグレー表示されている場合、インバンド設定は設定されていません。

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 **[機器（Equipment）] > [ラックマウント（Rack Mounts）] > [サーバ（Servers）] > *[サーバ番号（Server Number）]*** の順に展開します。

ステップ 3 [作業（Work）] 領域の [インベントリ（Inventory）] タブをクリックします。

ステップ 4 [CIMC] サブタブをクリックします。

ステップ 5 [アクション（Actions）] 領域で、[インバンド構成の削除（Delete Inband Configuration）] をクリックします。

ステップ 6 [削除（Delete）] 確認ダイアログボックスで [はい（Yes）] をクリックします。

サーバのインバンド構成が削除されます。

（注） Cisco UCS Manager でインバンド サービス プロファイルがデフォルト VLAN とプール名で設定されている場合、ここでインバンド設定を削除してから約 1 分後に、サーバ CIMC が自動的にインバンド プロファイルからインバンド設定を取得します。

ラックマウント サーバーの解放

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 稼働を停止するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Decommission] をクリックし、[OK] をクリックします。

サーバが Cisco UCS構成から削除されます。

（注） **ラック エンクロージャ** から最後のCisco UCS C125 M5 サーバを使用停止にする場合、Cisco UCS Managerは [navigation] ペインからすべての **Rack Enclosure *rack_enclosure_number*** エントリを削除します。

ラックマウント サーバの再稼動

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 [Equipment] で、[Rack-Mounts] ノードを選択します。

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

ステップ 4 再稼動する各ラックマウント サーバーの行で、次の手順を実行します。

a) [Recommission] カラムでチェックボックスをオンにします。

b) [Save Changes] をクリックします

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。

ステップ 6 （任意） サーバの再稼動と検出の進行状況を、そのサーバの [FSM] タブでモニタします。

ラックマウント サーバーの番号付け直し

始める前に

サーバ間で ID を交換する場合は、まず両方のサーバを解放し、サーバ解放 FSM が完了するのを待ってから、番号の再設定手順に進みます。

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]** > **[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 [Servers] ノードを展開し、以下が含まれていないことを確認します。

- 番号を付け直すラックマウント サーバー
- 使用する番号を持つラックマウント サーバー

これらのサーバのいずれかが [Servers] ノードに表示されている場合は、それらのサーバを解放します。続行前に、解放 FSM が完了し、サーバがノードにリストされなくなるまで待機する必要があります。これには数分かかる場合があります。

ステップ 4 番号を付け直すラックマウント サーバを選択します。

ステップ 5 [Equipment] タブで [Rack-Mounts] ノードをクリックします。

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

ステップ 7 番号を付け直す各ラックマウント サーバの行で、次の手順を実行します。

a) [ID] フィールド内でダブルクリックし、ラックマウント サーバに割り当てる新しい番号を入力します。
b) [Recommission] カラムでチェックボックスをオンにします。
c) [Save Changes] 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 （任意） サーバの再稼動と検出の進行状況を、そのサーバの [FSM] タブでモニタします。

存在しないラックマウント サーバの設定データベースからの削除

サーバを解放せずにサーバ ハードウェアを物理的に外した場合は、次の手順を実行します。サーバが物理的に存在する場合はこの手順を実行できません。

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 **[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 設定データベースから削除するサーバを選択します。

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 [Actions] 領域で、[Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Remove] をクリックし、[OK] をクリックします。

Cisco UCS Manager は、設定データベースからそのサーバに関するすべてのデータを削除します。サーバ スロットは、新しいサーバ ハードウェアの挿入に使用できます。

ラックマウント サーバのロケータ LED の切り替え

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]** > **[ラックマウント]** > **[サーバ]**を展開します。

Note 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 ロケータ LED のオン/オフを切り替えるサーバを選択します。

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 [Actions] 領域で、次のいずれかをクリックします。

- **[Turn on Locator LED]**
- Turn off Locator LED

ラックマウントサーバのローカルディスク ロケータ LED のオン/オフ切り替え

始める前に

- ディスクが配置されるサーバの電源が投入されていることを確認します。サーバがオフの場合、ローカル ディスクのロケータ LED のオン/オフを切り替えることはできません。

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 **[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 ディスクのロケータ LED のオン/オフを切り替えるサーバを選択します。

ステップ 4 [Work] ペインで、**[Inventory]** > **[Storage]** > **[Disks]** タブの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 5 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 6 [Details] 領域で、[Toggle Locator LED] をクリックします。
[Locator LED] の状態が [On] の場合は、[Off] に切り替わります。[Locator LED] の状態が [Off] の場合は、[On] に切り替わります。

ステップ 7 [Save Changes] をクリックします。

ラックマウント サーバーの CMOS のリセット

サーバのトラブルシューティングに CMOS のリセットが必要になることがあります。CMOS のリセットは、通常のサーバメンテナンスには含まれません。

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]** > **[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 CMOS をリセットするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CMOS] をクリックし、[OK] をクリックします。

ラックマウント サーバーの CIMC のリセット

ファームウェアで、サーバのトラブルシューティングにCIMCのリセットが必要になることがあります。CIMCのリセットは、通常のサーバメンテナンスには含まれません。CIMCをリセットすると、CIMC はブレード サーバの管理コントローラを再起動します。

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]** > **[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 CIMC をリセットするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CIMC (Server Controller)] をクリックし、[OK] をクリックします。

ラックマウント サーバーの TPM のクリア

TPM がサポートされている Cisco UCS M4 以降のブレード サーバーおよびラックマウント サーバーでのみ、TPM をクリアできます。

⚠

Caution TPM のクリアは危険性のある操作です。OS が起動を停止することがあります。また、データを損失する可能性もあります。

Before you begin

TPM が有効である必要があります。

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

Note 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 TPM をクリアするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Clear TPM] をクリックし、[OK] をクリックします。

ラックマウント サーバーからの NMI の発行

システムの無応答状態が続き、Cisco UCS Managerによって IMC から BIOS またはオペレーティング システムに NMI（マスク不能割り込み）を発行する必要がある場合には、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

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]** > **[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 NMI を発行するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで [Diagnostic Interrupt] をクリックし、[OK] をクリックします。

Cisco UCS Manager BIOS またはオペレーティング システムに NMI を送信します。

ラックマウント サーバのヘルス イベントの表示

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 ヘルス イベントを表示するサーバを選択します。

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

このサーバでトリガーされたヘルスイベントが表示されます。このタブのフィールドは次のとおりです。

名前	説明
[Health Summary] 領域	
[Health Qualifier] フィールド	コンポーネントに対してトリガーされるすべてのヘルス イベントのカンマ区切りの名前。
[Health Severity] フィールド	コンポーネントに対してトリガーされるすべてのステータスイベントの最高シビラティ（重大度）。次のいずれかになります。 • **critical** • **major** • **minor** • **warning** • **info** • **cleared** （注） シビラティ（重大度）レベルが最高のものから順に記載されています。
[Health Details] 領域	

名前	説明
[Severity] カラム	ヘルス イベントのシビラティ（重大度）。次のいずれかになります。 • **critical** • **major** • **minor** • **warning** • **info** • **cleared** （注） シビラティ（重大度）レベルが最高のものから順に記載されています。
[Name] カラム	ヘルス イベントの名前。
[Description] カラム	ヘルス イベントの詳細。
[Value] カラム	ヘルス イベントの現在の値。
[Details] 領域	[Details] 領域には、[Health Details] 領域で選択するヘルス イベントの [Name] 、[Description] 、[Severity] および [Value] の詳細が表示されます。

ラックマウント サーバの POST 結果の表示

サーバとそのアダプタに対する Power On Self-Test プロセスで収集された任意のエラーを表示できます。

手順

ステップ 1 [ナビゲーション]ペインで、[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 POST の結果を表示するサーバを選択します。

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 [Actions] 領域で [View POST Results] をクリックします。

[POST Results] ダイアログボックスに、サーバとそのアダプタに対する POST の結果が一覧表示されます。

ステップ 6 （任意） アダプタのプロパティを表示するには、[Affected Object] カラムをクリックします。

ステップ 7 [OK] をクリックして [POST Results] ダイアログボックスを閉じます。

Power Transition Log の表示

Power Transition Log を確認できます。このログには、最後の 5 つのサーバの電力遷移が表示されます。表示される情報には、[Power Change Source] や [Timestamp] などがあります。

一意の電力遷移イベントだけが表示されます。UCSMにより開始された電力遷移の場合、電力遷移を引き起こした FSM が表示されます。

手順

ステップ 1 **[Equipment]** > **[Rack-Mounts]** > **[Servers]** を選択します。

ステップ 2 Power Transition Log を表示するサーバを選択します。

[General] タブに [Power Transition Log] が表示されます。

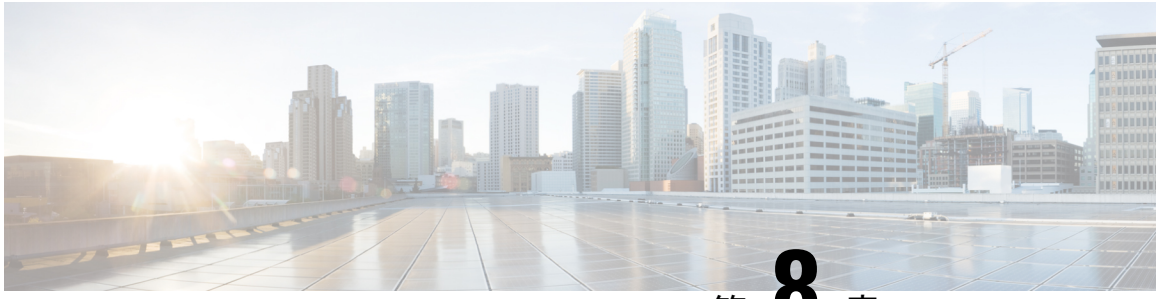
Cisco UCS C125 M5 サーバスロット ID の表示

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 **[Equipment]** > **[Rack Mounts]** > **[Enclosures]** > **[Rack Enclosure]*[rack_enclosure_number]*** の順に展開します。

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



第 8 章

S3X60 サーバ ノード ハードウェア管理

- Cisco UCS C3260 サーバー ノードの管理, on page 108
- Cisco UCS C3260 サーバ ノードのブート, on page 108
- サービス プロファイルからの Cisco UCS C3260 サーバのブート （108 ページ）
- Cisco UCS C3260 サーバ ノードのブート順序の決定 （109 ページ）
- Cisco UCS C3260 サーバ ノードのシャットダウン, on page 110
- サービス プロファイルからの Cisco UCS C3260 サーバ ノードのシャットダウン （110 ページ）
- Cisco UCS C3260 サーバ ノードのリセット, on page 111
- Cisco UCS C3260 サーバー ノードの出荷時のデフォルト設定へのリセット （112 ページ）
- Cisco UCS C3260 サーバ ノードの再認識, on page 113
- シャーシからの Cisco UCS C3260 サーバ ノードの削除, on page 114
- Cisco UCS C3260 サーバ ノードからのインバンド設定の削除 （114 ページ）
- Cisco UCS C3260 サーバ ノードの稼働停止, on page 115
- Cisco UCS C3260 サーバ ノードの再稼動 （115 ページ）
- サーバ スロットの再認識 S3260 シャーシ, on page 116
- 存在しない Cisco UCS C3260 サーバ ノードの設定データベースからの削除, on page 116
- Cisco UCS C3260 サーバ ノードのロケータ LED のオン/オフ切り替え, on page 117
- Cisco UCS C3260 サーバ ノードのローカル ディスク ロケータ LED のオン/オフ切り替え （118 ページ）
- Cisco UCS C3260 サーバ ノードの CIMC のリセット, on page 118
- Cisco UCS C3260 サーバ ノードの CMOS のリセット, on page 119
- S3X60 サーバーの BIOS パスワードのリセット （119 ページ）
- Cisco UCS C3260 サーバ ノードからの NMI の発行 （120 ページ）
- Cisco UCS C3260 サーバ ノードの POST 結果の表示, on page 120
- Cisco UCS C3260 サーバ ノードのヘルス イベントの表示 （121 ページ）
- ヘルス LED アラーム （123 ページ）

Cisco UCS C3260 サーバー ノードの管理

Cisco UCS Managerを使用して、Cisco UCS ドメインのCisco UCS C3260サーバー ノードすべてを管理およびモニターできます。電源状態の変更など一部のサーバー管理タスクは、サーバーおよびサービス プロファイルから実行できます。

残りの管理タスクは、サーバー上でのみ実行できます。

シャーシ内のサーバー スロットが空の場合、そのスロットに関する情報、エラー、および障害がCisco UCS Manager から提供されます。サーバー ミスマッチ エラーを解決し、そのスロット内のサーバーを再検出するために、スロットを再認識させることもできます。

Cisco UCS C3260 サーバ ノードのブート

[Actions] 領域で [Boot Server] リンクがグレー表示されている場合は、まず、サーバをシャットダウンする必要があります。

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 **[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 ブートするサーバを選択します。

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 [Actions] 領域の [Boot Server] 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。

サーバがブートされると、[General] タブの [Overall Status] フィールドに [OK] ステータスが表示されます。

サービス プロファイルからの Cisco UCS C3260 サーバのブート

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 サービス プロファイルを作成する組織、または適切なサービス 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 関連付けられたサーバをブートする必要があるサービス プロファイルを選択します。

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

ステップ 6 [Actions] 領域の [Boot Server] 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 [Boot Server] ダイアログボックスで [OK] をクリックします。

サーバがブートした後は、[General] タブの [Overall Status] フィールドに [ok] ステータスまたは [up] ステータスが表示されます。

Cisco UCS C3260 サーバ ノードのブート順序の決定

ヒント サーバに関連付けられているサービス プロファイルの [General] タブからもブート順序タブを表示できます。

手順

ステップ 1 [ナビゲーション]ペインで、[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 ブート順序を決定するサーバをクリックします。

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 [Boot Order Details] 領域が展開されていない場合は、見出しの右側の [Expand] アイコンをクリックします。

ステップ 6 サーバに割り当てられているブート順序を表示するには、[Configured Boot Order] タブをクリックします。

ステップ 7 物理サーバ構成内のさまざまなデバイスから何がブートされるかを表示するには、[Actual Boot Order] タブをクリックします。

Cisco UCS C3260 サーバ ノードのシャットダウン

この手順を使用して、インストールされているオペレーティング システムとともにサーバをシャットダウンした場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown Server] リンクがグレー表示されている場合、そのサーバは動作していません。

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）]** > **[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 シャットダウンするサーバを選択します。

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 [Actions] 領域で、[Shutdown Server] 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。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに電源オフ状態が表示されます。

サービス プロファイルからの Cisco UCS C3260 サーバ ノードのシャットダウン

この手順を使用して、インストールされているオペレーティング システムとともにサーバをシャットダウンした場合、Cisco UCS Manager により、この OS のグレースフル シャットダウン シーケンスがトリガーされます。

[Actions] 領域の [Shutdown Server] リンクがグレー表示されている場合、そのサーバは動作していません。

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]**を展開します。

ステップ 3 関連付けられているサービス プロファイルを含む組織のノードを展開します。

ステップ 4 シャットダウンするサーバと関連付けられたサービス プロファイルを選択します。

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

ステップ 6 [Actions] 領域で、[Shutdown Server] 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。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドに [down] ステータスまたは [power-off] ステータスが表示されます。

Cisco UCS C3260 サーバ ノードのリセット

サーバをリセットすると、Cisco UCS Manager により、リセット ライン上にパルスが送信されます。オペレーティング システムのグレースフル シャットダウンを選択することができます。オペレーティング システムでグレースフル シャットダウンがサポートされていない場合、サーバ電源の再投入が行われます。サーバをリセットする前に Cisco UCS Manager にすべての管理操作を完了させるオプションの場合、それらの操作がサーバのリセット前に完了する保証はありません。

Note 電源切断状態からサーバをブートする場合は、**[リセット（Reset）]** を使用しないでください。

この手順を使用して電源投入を続けると、サーバの望ましい電源状態が実際の電源状態と同期しなくなり、サーバが後で予期せずシャットダウンすることがあります。選択したサーバを電源切断状態から安全にリブートするには、**[キャンセル（Cancel）]** をクリックし、**[ブート サーバ（Boot Server）]** アクションを選択します。

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 **[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 リセットするサーバを選択します。

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 [Actions] 領域で [Reset] をクリックします。

ステップ 6 [Reset Server] ダイアログボックスで、次の手順を実行します。

a) [Power Cycle] オプションをクリックします。

b) (Optional) このサーバの保留中の管理操作を Cisco UCS Manager によってすべて完了させる場合は、チェックボックスをオンにします。

c) [OK] をクリックします。

リセットが完了するまでに数分かかる場合があります。サーバがリセットされると、[General] タブの [Overall Status] フィールドに OK ステータスが表示されます。

Cisco UCS C3260 サーバー ノードの出荷時のデフォルト設定へのリセット

Cisco UCS C3260 サーバー ノードを出荷時の設定にリセットできるようになりました。デフォルトでは、出荷時へのリセット操作は、ストレージ ドライブに影響しません。これはデータの損失を防止するためです。ただし、これらのデバイスを既知の状態にリセットすることもできます。

次のガイドラインは、スクラブ ポリシーを使用する場合に Cisco UCS C3260 サーバー ノードに適用されます。

- Cisco UCS C3260 サーバー ノードでは、スクラブ ポリシーを使用してストレージを削除することはできません。
- Cisco UCS C3260 サーバー ノードでは、FlexFlash ドライブはサポートされていません。
- Cisco UCS C3260 サーバー ノードで行える操作は、スクラブ ポリシーを使用した BIOS のリセットのみです。

重要 ストレージ デバイスをリセットすると、データが失われる可能性があります。

サーバーを出荷時のデフォルト設定にリセットするには、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、[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 出荷時のデフォルト設定にリセットするサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [Reset to Factory Default] をクリックします。

b) [OK] をクリックします。

ステップ 7 表示される [Maintenance Server] ダイアログ ボックスから適切なオプションを選択します。

- すべてのストレージを削除するには、[Scrub Storage] チェックボックスを選択します。

（注） Cisco UCS C3260 サーバ ノードでは、スクラブ ポリシーを使用してストレージを削除することはできません。

- すべてのストレージを削除してからすべてのディスクを初期状態に戻すには、[Create Initial Volumes] チェックボックスを選択します。

  [Scrub Storage] チェックボックスを選択した場合のみ、このチェックボックスを選択できます。JBOD をサポートするサーバの場合、ディスクは JBOD 状態になります。JBOD をサポートしないサーバの場合、各ディスクはディスク内のすべての領域を占有する単一 R0 ボリュームで初期化されます。

  重要 ストレージプロファイルを使用するには、[Create Initial Volumes] ボックスを選択しないでください。ストレージ プロファイルを使用しているときに初期ボリュームを作成すると、設定エラーが発生する可能性があります。

Cisco UCS Manager サーバを出荷時のデフォルト設定にリセットします。

Cisco UCS C3260 サーバ ノードの再認識

サーバ、およびそのサーバのエンドポイントすべてを再検出するには、次の手順を実行します。たとえば、サーバがディスカバリ状態など、予期していなかった状態から抜け出せなくなっている場合に、この手順を使用します。

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 **[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 再確認するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Re-acknowledge] をクリックし、次に [OK] をクリックします。

Cisco UCS Manager はサーバを切断し、その後、サーバとシステム内の 1 つまたは複数のファブリック インターコネクトとの接続を確立します。確認が終了するまでに数分かかる場合があります。サーバが確認されると、[General] タブの [Overall Status] フィールドに OK ステータスが表示されます。

シャーシからの Cisco UCS C3260 サーバ ノードの削除

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）] > [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 シャーシから削除するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Decommission] をクリックし、[OK] をクリックします。

サーバが Cisco UCS構成から削除されます。

ステップ 7 シャーシの物理的な配置場所で、スロットからサーバー ハードウェアを取り外します。

サーバー ハードウェアの取り外し方法については、お使いのシャーシの『*Cisco UCS Hardware Installation Guide*』を参照してください。

What to do next

サーバを物理的に取り付けなおす場合は、スロットを再認識して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

Cisco UCS C3260 サーバ ノードからのインバンド設定の削除

この手順では、ブレード サーバからインバンド管理 IP アドレスの設定を削除します。このアクションがグレー表示されている場合、インバンド設定は完了していません。

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 **[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] > [*Server Name*]** の順に展開します。

ステップ 3 [作業（Work）] 領域の [インベントリ（Inventory）] タブをクリックします。

ステップ 4 [CIMC] サブタブをクリックします。

ステップ 5 [アクション（Actions）] 領域で、[インバンド構成の削除（Delete Inband Configuration）] をクリックします。

ステップ 6 [削除（Delete）] 確認ダイアログボックスで [はい（Yes）] をクリックします。

サーバのインバンド構成が削除されます。

（注） Cisco UCS Manager でインバンド サービス プロファイルがデフォルト VLAN とプール名を使って構成されている場合、ここでインバンド構成を削除した約 1 分後、サーバ CIMC が自動的にインバンド プロファイルからインバンド構成を取得します。

Cisco UCS C3260 サーバ ノードの稼働停止

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）] > [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 稼働を停止するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [デコミッション（Decommission）] をクリックします。

b) [OK] をクリックします。

サーバが Cisco UCS構成から削除されます。

What to do next

- サーバーを物理的に取り付けなおす場合は、Cisco UCS Manager にスロットを再認識させ、そのサーバーを再検出させる必要があります。

Cisco UCS C3260 サーバ ノードの再稼動

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]** ノードをクリックします。

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

ステップ 4 再稼動する各サーバの行で、[Recommission] カラムのチェックボックスをオンにしてから、[Save Changes] をクリックします。

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。

ステップ 6 （任意） サーバの再稼動と検出の進行状況を、そのサーバの [FSM] タブでモニタします。

サーバ スロットの再認識 S3260 シャーシ

物理ハードウェアをシャーシから取り外さずにサーバの稼働を中止した場合、Cisco UCS Manager にサーバを再検出させ、再認識させるには、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、[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 スロットを再確認するサーバを選択します。

ステップ 4 Cisco UCS Managerに [Resolve Slot Issue] ダイアログボックスが表示された場合は、次のいずれかの手順を実行します。

オプション	説明
[Situation] 領域の [here] リンク	このリンクをクリックし、次に確認ダイアログボックスの **[はい（Yes）]** をクリックします。Cisco UCS Manager はスロットを再確認し、スロット内のサーバーを検出します。
OK	[General] タブに移動するには、このボタンをクリックします。[Actions] 領域の [Reacknowledge Slot] リンクを使用すると、Cisco UCS Managerでスロットを再確認し、スロット内のサーバを検出できます。

存在しない Cisco UCS C3260 サーバ ノードの設定データベースからの削除

サーバを解放せずにサーバ ハードウェアを物理的に外した場合は、次の手順を実行します。サーバが物理的に存在する場合はこの手順を実行できません。

サーバを物理的に削除するには、シャーシからの Cisco UCS C3260 サーバ ノードの削除, on page 114 を参照してください。

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）] > [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 設定データベースから削除するサーバを選択します。

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 [Actions] 領域で、[Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、[Remove] をクリックし、[OK] をクリックします。

Cisco UCS Manager は、設定データベースからそのサーバに関するすべてのデータを削除します。サーバ スロットは、新しいサーバ ハードウェアの挿入に使用できます。

Cisco UCS C3260 サーバ ノードのロケータ LED のオン/オフ切り替え

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）] > [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 ロケータ LED のオン/オフを切り替えるサーバを選択します。

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 [Actions] 領域で、次のいずれかをクリックします。

- [Turn on Locator LED]：選択したサーバの LED を点灯します。
- [Turn on Locator LED]：選択したサーバの LED を消灯します。

Cisco UCS C3260 サーバ ノードのローカル ディスク ロケータ LED のオン/オフ切り替え

始める前に

- ディスクがゾーン分割されていることを確認します。ゾーン分割されていないディスクでは、ロケータ LED のオンおよびオフはできません。
- ディスクが配置されるサーバの電源が投入されていることを確認します。サーバがオフの場合、ローカル ディスクのロケータ LED のオン/オフを切り替えることはできません。

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 **[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 ディスクのロケータ LED のオン/オフを切り替えるサーバを選択します。

ステップ 4 [Work] ペインで、**[Inventory] > [Storage] > [Disks]** タブの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 5 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 6 [Details] 領域で、[Toggle Locator LED] をクリックします。
[Locator LED] の状態が [On] の場合は、[Off] に切り替わります。[Locator LED] の状態が [Off] の場合は、[On] に切り替わります。

ステップ 7 [Save Changes] をクリックします。

Cisco UCS C3260 サーバ ノードの CIMC のリセット

ファームウェアで、サーバのトラブルシューティングにCIMCのリセットが必要になることがあります。CIMCのリセットは、通常のサーバメンテナンスには含まれません。CIMCをリセットすると、CIMC はブレード サーバの管理コントローラを再起動します。

CIMCをリセットすると、CIMCがリブートするまで、Cisco UCSの電力モニタリング機能が短時間使用不能になります。通常、リセットは20秒しかかかりませんが、その間にピーク電力キャップを超える可能性はあります。低い電力制限が設定された環境で、設定された電力制限を超えないようにするには、CIMC のリブートまたはアクティブ化を交互に実施することを検討してください。

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）] > [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 CIMC をリセットするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CIMC (Server Controller)] をクリックし、[OK] をクリックします。

Cisco UCS C3260 サーバ ノードの CMOS のリセット

サーバのトラブルシューティングに CMOS のリセットが必要になることがあります。CMOS のリセットは、通常のサーバメンテナンスには含まれません。

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）] > [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 CMOS をリセットするサーバを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 [Recover Server] ダイアログボックスで、[Reset CMOS] をクリックし、[OK] をクリックします。

S3X60 サーバーの BIOS パスワードのリセット

このオプションを使用すると、F2 BIOS 構成プロンプトを使用せずに BIOS パスワードをリセットできます。BIOS パスワードのリセットは、通常のサーバー メンテナンスには含まれません。BIOS パスワードのリセット後、サーバーはすぐに再起動され、新しい BIOS パスワードが更新されます。

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）] > [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 BIOS パスワードをリセットするサーバーを選択します。

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 [Actions] 領域の [Recover Server] をクリックします。

ステップ 6 **[サーバーの回復（Recover Server）]** ダイアログボックスで、**[BIOS パスワードのリセット（Reset BIOS Password）]** をクリックし、**[OK]** をクリックします。

Cisco UCS C3260 サーバ ノードからの NMI の発行

システムの無応答状態が続き、Cisco UCS Managerによって IMC から BIOS またはオペレーティング システムに NMI（マスク不能割り込み）を発行する必要がある場合には、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

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）] > [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 NMI を発行するサーバを選択します。

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 [Actions] 領域の [Server Maintenance] をクリックします。

ステップ 6 [Maintenance] ダイアログボックスで、次の手順を実行します。

a) [Diagnostic Interrupt] をクリックします。

b) [OK] をクリックします。

Cisco UCS Manager BIOS またはオペレーティング システムに NMI を送信します。

Cisco UCS C3260 サーバ ノードの POST 結果の表示

サーバとそのアダプタに対する Power On Self-Test プロセスで収集された任意のエラーを表示できます。

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 **[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 POST の結果を表示するサーバを選択します。

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 [Actions] 領域で [View POST Results] をクリックします。

[POST Results] ダイアログボックスに、サーバとそのアダプタに対する POST の結果が一覧表示されます。

ステップ 6 (Optional) アダプタのプロパティを表示するには、[Affected Object] カラムをクリックします。

ステップ 7 [OK] をクリックして [POST Results] ダイアログボックスを閉じます。

Cisco UCS C3260 サーバ ノードのヘルス イベントの表示

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 ヘルス イベントを表示するサーバを選択します。

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

このサーバでトリガーされたヘルスイベントが表示されます。このタブのフィールドは次のとおりです。

名前	説明
[Health Summary] 領域	
[Health Qualifier] フィールド	コンポーネントに対してトリガーされるすべてのヘルス イベントのカンマ区切りの名前。

名前	説明
[Health Severity] フィールド	コンポーネントに対してトリガーされるすべてのステータスイベントの最高シビラティ（重大度）。次のいずれかになります。 • **critical** • **major** • **minor** • **warning** • **info** • **cleared** （注） シビラティ（重大度）レベルが最高のものから順に記載されています。
[Health Details] 領域	
[Severity] カラム	ヘルス イベントのシビラティ（重大度）。次のいずれかになります。 • **critical** • **major** • **minor** • **warning** • **info** • **cleared** （注） シビラティ（重大度）レベルが最高のものから順に記載されています。
[Name] カラム	ヘルス イベントの名前。
[Description] カラム	ヘルス イベントの詳細。
[Value] カラム	ヘルス イベントの現在の値。

名前	説明
[Details] 領域	[Details] 領域には、[Health Details] 領域で選択するヘルス イベントの [Name] 、[Description] 、[Severity] および [Value] の詳細が表示されます。

ヘルス LED アラーム

サーバー正常性 LED は、各サーバーの前面にあります。Cisco UCS Manager では、センサー故障が発生すると、ブレード正常性 LED が緑色からオレンジ色またはオレンジ色の点滅に変化します。

ヘルス LED アラームには次の情報が表示されます。

名前	説明
[Severity] カラム	アラームのシビラティ（重大度）。次のいずれかになります。 • [Critical]：サーバー ヘルス LED がオレンジの点滅になっています。これは赤色のドットで示されます。 • [Minor]：サーバー ヘルス LED がオレンジになっています。これはオレンジ色のドットで示されます。
[Description] カラム	アラームの簡単な説明。
[センサー ID（Sensor ID）] カラム	アラームをトリガーしたセンサーの ID。
[Sensor Name] カラム	アラームをトリガーしたセンサーの名前。

ヘルス LED アラームの表示

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。

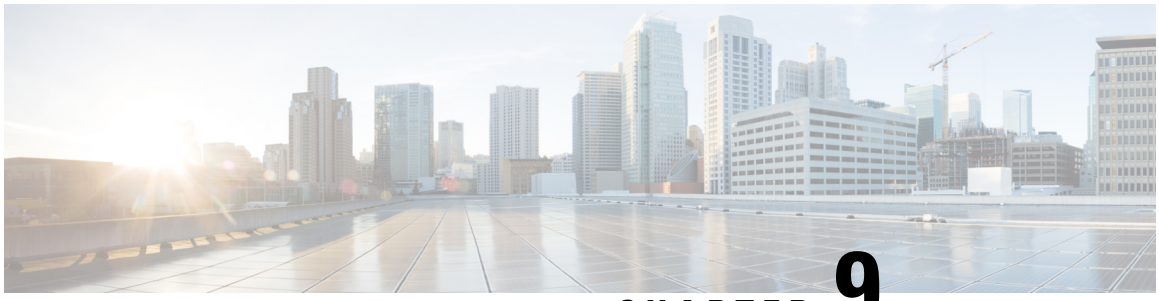
ステップ 3 ヘルス LED アラームを表示する対象のサーバをクリックします。

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、[View Health LED Alarms] をクリックします。

[View Health LED Alarms] ダイアログボックスに、選択したサーバのヘルス LED アラームが一覧表示されます。

ステップ 6 [OK] をクリックして、[View Health LED Alarms] ダイアログボックスを閉じます。



CHAPTER 9

サーバ プール

- サーバ プールの設定, on page 125
- UUID 接尾辞プールの設定, on page 128
- IP プールの設定, on page 130

サーバ プールの設定

サーバ プール

サーバプールは複数のサーバで構成されています。これらのサーバは通常、同じ特性を持ちます。それらの特性は、シャーシ内の位置であったり、サーバ タイプ、メモリ量、ローカル ストレージ、CPU のタイプ、ローカル ドライブ構成などの属性だったりします。サーバを手動でサーバプールに割り当てることも、サーバプール ポリシーとサーバプール ポリシー資格情報を使用して割り当てを自動化することもできます。

システムが組織を通じて、マルチテナント機能を実装している場合、特定の組織で使用されるサーバ プールを 1 つ以上、指定できます。たとえば、CPU を 2 個搭載したサーバをすべて含むプールをマーケティング組織に割り当て、メモリのサイズが 64GB のサーバをすべて、財務組織に割り当てることができます。

サーバプールには、システム内のどのシャーシにあるサーバでも入れることができます。1 つのサーバは複数のサーバ プールに属することができます。

サーバ プールの作成

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]** > **[プール]**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 [Server Pools] ノードを右クリックし、[Create Server Pool] を選択します。

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

名前	説明
[名前（Name）] フィールド	サーバ 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	サーバ プール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）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 6 [Next] をクリックします。

ステップ 7 [Create Server Pool] ウィザードの [Add Servers] ページで、次の手順を実行します。

a) [Available Servers] テーブルで、1 つ以上のサーバを選択します。
b) [>>] ボタンをクリックして、サーバ プールにサーバを追加します。
c) 適切なサーバをすべてプールに追加したら、[Finish] をクリックします。

サーバ プールの削除

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（Servers）]** > **[プール（Pools）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [Server Pools] ノードを展開します。

ステップ 4 削除する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。

サーバ プールへのサーバの追加

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（Servers）]** > **[プール（Pools）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 1 つまたは複数のサーバを追加するプールを右クリックして、[Add Servers to Server Pool] を選択します。

ステップ 4 [Add Servers to Server Pool] ダイアログボックスで、次の手順を実行します。

a) **[Servers]** テーブル で、サーバ プールに追加するサーバを選択します。

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。

b) **[>>]** ボタン をクリックして、それらのサーバを **[Pooled Servers]** テーブル に移動し、サーバ プールに追加します。

c) [OK] をクリックします。

サーバ プールからのサーバの削除

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（Servers）]** > **[プール（Pools）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 1 つまたは複数のサーバを削除するプールを右クリックし、[Add Servers to Server Pool] を選択します。

ステップ 4 [Add Servers to Server Pool] ダイアログボックスで、次の手順を実行します。

a) **[Pooled Servers]** テーブルで、サーバ プールから削除するサーバを選択します。

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。

b) **[<<]** ボタンをクリックして、選択したサーバを**[Servers]** テーブルに移動し、サーバ プールから削除します。

c) [OK] をクリックします。

UUID 接尾辞プールの設定

UUID 接尾辞プール

UUID接尾辞プールは、サーバへの割り当てに使用できるSMBIOS UUIDの集まりです。UUIDの接頭辞を構成する先頭の桁の数字は固定です。残りの桁で構成されるUUID接尾辞は変数です。UUID接尾辞プールは、特定のプールを使用するサービスプロファイルに関連づけられた各サーバについて、これらの変数が一意であることを保証して競合を回避します。

サービス プロファイルで UUID 接尾辞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の UUID を手動で設定する必要はありません。

UUID 接尾辞プールの作成

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 **[サーバ]** > **[プール]**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 [UUID Suffix Pools] を右クリックし、[Create UUID Suffix Pool] を選択します。

ステップ 5 [UUID サフィックス プールの作成（Create UUID Suffix Pool）] ウィザードの [名前と説明の定義（Define Name and Description）] ページで、次のフィールドを入力します。

名前	説明
[名前（Name）] フィールド	UUID 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）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

名前	説明
[Prefix] フィールド	次のいずれかになります。 • [Derived]：システムによって接尾辞が作成されます。 • [other]：任意の接尾辞を指定します。 このオプションを選択すると、任意の接尾辞を *XXXXXXXX-XXXX-XXXX* の形式で入力できるテキスト フィールドが Cisco UCS Manager GUI に表示されます。
[割り当て順序（Assignment Order）] フィールド	次のいずれかになります。 • **[デフォルト（Default）]**：Cisco UCS Manager はプールからランダム ID を選択します。 • **[シーケンシャル（Sequential）]**：Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。

ステップ 6 [Next] をクリックします。

ステップ 7 [UUID サフィックス プールの作成（Create UUID Suffix Pool）] ウィザードの [UUID ブロックの追加（Add UUID Blocks）] ページで、[追加（Add）] をクリックします。

ステップ 8 [UUID サフィックスのブロックの作成（Create a Block of UUID Suffixes）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[開始] フィールド	ブロック内の最初の UUID。
[Size] フィールド	ブロック内の UUID の数。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックして、ウィザードを終了します。

次のタスク

UUID接尾辞プールをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

UUID 接尾辞プールの削除

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、[サーバ]をクリックします。
ステップ 2 **[サーバ（Servers）]** > **[プール（Pools）]** > ***[Organization_Name]*** の順に展開します。
ステップ 3 [UUID Suffix Pools] ノードを展開します。
ステップ 4 削除する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。

IP プールの設定

IP プール

IP プールは、用途が初期設定されていない IP アドレスの集合です。IPv4 または IPv6 アドレスのプールを作成するCisco UCS Manager以下を実行します。

- サービス プロファイルが関連付けられているサーバーのデフォルトの管理 IP プール **ext-mgmt** の置き換え。Cisco UCS Manager は、サーバーの Cisco Integrated Management Controller（CIMC）で終端する外部アクセスのために、IP プールに IP アドレスの各ブロックを予約しています。サービスプロファイルが関連付けられていない場合は、CIMC 用の **ext-mgmt** IP プールを使用して IP アドレスを取得する必要があります。
- CIMC 用の管理インバンドまたはアウトオブバンド IP アドレスの置き換え。

（注） Cisco UCS Manager では iSCSI ブート IPv6 プールを作成できません。

IPv4 アドレスのプールを作成する Cisco UCS Manager 以下を実行します。

- デフォルトの iSCSI ブート IP プール **iscsi-initiator-pool** の置き換え。Cisco UCS Manager は、指定された IP プールの各 IP アドレス ブロックを予約します。
- 管理 IP アドレスと iSCSI ブート IP アドレス両方の置き換え。

（注） サーバまたはサービスプロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、IP プールに含まれていてはなりません。

IP プールの作成

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 [LAN] タブで、**[LAN]** > **[Pools]** > **[*Organization_Name*]** を展開します。

ステップ 3 [IP Pools] を右クリックし、[Create IP Pool] を選択します。

ステップ 4 [Create IP Pool] ウィザードの [Define Name and Description] ページで、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	IP アドレス 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	ユーザ定義による IP アドレス 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）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[割り当て順序（Assignment Order）] フィールド	次のいずれかになります。 • **[デフォルト（Default）]**：Cisco UCS Manager はプールからランダム ID を選択します。 • **[シーケンシャル（Sequential）]**：Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。

ステップ 5 [Next] をクリックします。

ステップ 6 [Create IP Pool] ウィザードの [Add IPv4 Blocks] ページで、[Add] をクリックします。

ステップ 7 [IPv4 アドレス ブロックの作成（Create a Block of IPv4 Addresses）] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[開始] フィールド	ブロック内の最初の IPv4 アドレス。
[Size] フィールド	プール内の IP アドレスの数。

名前	説明
[Subnet Mask] フィールド	ブロック内の IPv4 アドレスと関連付けられたサブネット マスク。
[Default Gateway] フィールド	ブロック内の IPv4 アドレスに関連付けられたデフォルト ゲートウェイ。
[Primary DNS] フィールド	この IPv4 アドレスのブロックがアクセスするプライマリ DNS サーバ。
[Secondary DNS] フィールド	この IPv4 アドレスのブロックがアクセスするセカンダリ DNS サーバ。

ステップ 8

ステップ 9 [Next] をクリックします。

ステップ 10 [Create IP Pool] ウィザードの [Add IPv6 Blocks] ページで、[Add] をクリックします。

ステップ 11 [Create a Block of IPv6 Addresses] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[開始] フィールド	ブロック内の最初の IPv6 アドレス。
[Size] フィールド	プール内の IP アドレスの数。
Prefix	ブロック内の IPv6 アドレスに関連付けられたネットワーク アドレス プレフィクス。
[Default Gateway] フィールド	ブロック内の IPv6 アドレスに関連付けられたデフォルト ゲートウェイ。
[Primary DNS] フィールド	この IPv6 アドレスのブロックがアクセスするプライマリ DNS サーバ。
[Secondary DNS] フィールド	この IPv6 アドレスのブロックがアクセスするセカンダリ DNS サーバ。

ステップ 12 **[OK]** をクリックします。

ステップ 13 [Finish] をクリックして、ウィザードを終了します。

次のタスク

IP 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。

IP プールへのブロックの追加

IP プールに IPv4 または IPv6 のアドレスのブロックを追加できます。

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 [LAN] タブで、**[LAN]** > **[プール（Pools）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [IP プール（IP Pools）] ノードを展開します。

ステップ 4 目的の IP プールを右クリックし、次のうちの 1 つを選択します。

- **[Create Block of IPv4 Addresses]**
- **[Create Block of IPv6 Addresses]**

ステップ 5 適切なダイアログ ボックスのフィールドに入力します。

a) [Create a Block of IPv4 Addresses] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[名前（Name）] カラム	ブロックに割り当てる IPv4 アドレスの範囲。
[開始（From）] カラム	ブロック内の最初の IPv4 アドレス。
[終了（To）] カラム	ブロック内の最後の IPv4 アドレス。
[サブネット（Subnet）] カラム	ブロック内の IPv4 アドレスと関連付けられたサブネット マスク。
[デフォルト ゲートウェイ（Default Gateway）] カラム	ブロック内の IPv4 アドレスに関連付けられたデフォルト ゲートウェイ。
[プライマリ DSN（Primary DNS）] カラム	この IPv4 アドレスのブロックがアクセスするプライマリ DNS サーバ。
[セカンダリ DNS（Secondary DNS）] カラム	この IPv4 アドレスのブロックがアクセスするセカンダリ DNS サーバ。

b) [Create a Block of IPv6 Addresses] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Name] カラム	ブロックに割り当てられている IPv6 アドレスの範囲。
[From] カラム	ブロック内の最初の IPv6 アドレス。
[To] カラム	ブロック内の最後の IPv6 アドレス。
[Prefix] カラム	ブロック内の IPv6 アドレスに関連付けられたネットワーク アドレス プレフィクス。

名前	説明
[Default Gateway] カラム	ブロック内の IPv6 アドレスに関連付けられたデフォルト ゲートウェイ。
[Primary DNS] カラム	この IPv6 アドレスのブロックがアクセスするプライマリ DNS サーバ。
[Secondary DNS] カラム	この IPv6 アドレスのブロックがアクセスするセカンダリ DNS サーバ。

ステップ 6 [OK] をクリックします。

IP プールからのブロックの削除

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 [LAN] タブで、**[LAN]** > **[Pools]** > **[Root]** を展開します。
ステップ 3 [IP Pools] ノードを展開します。
ステップ 4 IP アドレスのブロックを削除するプールを展開します。
ステップ 5 削除する IP アドレス ブロックを右クリックし、[削除（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。

IP 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

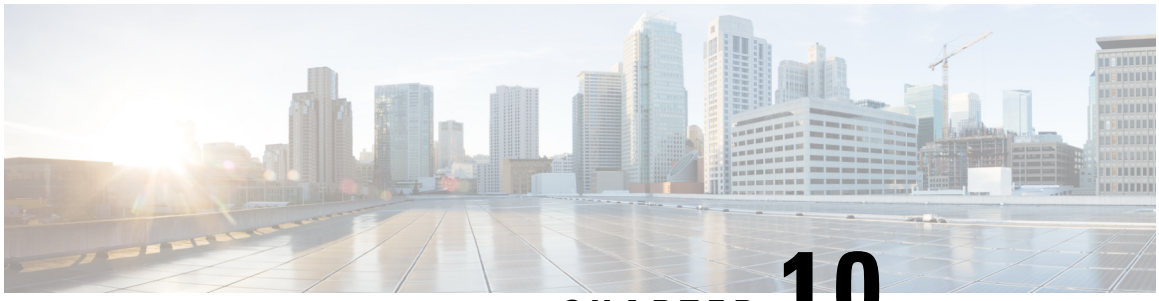
ステップ 1 [ナビゲーション]ペインで、[LAN]をクリックします。
ステップ 2 [LAN] タブで、**[LAN]** > **[プール（Pools）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [IP プール（IP Pools）] ノードを展開します。

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

Note デフォルト プールである [ext-mgmt] および [iscsi-initiator-pool] は削除できません。

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 10

サーバーのブート

- ブート ポリシー, on page 137
- UEFI ブート モード （138 ページ）
- UEFI セキュア ブート （139 ページ）
- CIMC セキュア ブート （141 ページ）
- ブート ポリシーの作成, on page 142
- SAN ブート （144 ページ）
- iSCSI ブート （145 ページ）
- LAN ブート （174 ページ）
- ローカル デバイス ブート （174 ページ）
- ブート ポリシーの削除, on page 182
- UEFI ブート パラメータ （182 ページ）

ブート ポリシー

Cisco UCS Manager では、ブレード サーバーとラック サーバーのブート ポリシーを作成できます。

Cisco UCS Manager ブート ポリシーは、BIOS 設定メニューのブート順序をオーバーライドし、次のことを決定します。

- ブート デバイスの選択
- サーバのブート元
- ブート デバイスの起動順序

たとえば、関連付けられたサーバーをローカルディスクやCD-ROM（仮想メディア（VMedia））などのローカル デバイスからブートしたり、SAN ブートや LAN（PXE）ブートを選択したりすることができます。

1 つ以上のサービス プロファイルに関連付ける名前付きブート ポリシーを作成するか、または特定のサービス プロファイルに対するブート ポリシーを作成できます。ブート ポリシーを有効にするには、ブート ポリシーをサービス プロファイルに含め、このサービス プロファイル

をサーバーに関連付ける必要があります。サービス プロファイルにブート ポリシーを含めない場合、Cisco UCS Manager によってデフォルトのブート ポリシーが適用されます。

Note ブート ポリシーに対する変更は、そのブート ポリシーを含んでいる、更新中のサービス プロファイル テンプレートを使って作成されたすべてのサーバーに伝播されます。BIOS にブート順序情報を再書き込みするためのサービスプロファイルとサーバーとの再関連付けは自動的にトリガーされます。

また、ブート ポリシーに次を指定することもできます。

- ローカル LUN の名前指定された名前は、展開される名前ではなく、ストレージ プロファイル内の論理名です。プライマリ名のみを指定します。セカンダリ名を指定すると、設定エラーが発生します。
- JBOD ディスクからブートするための特定の JBOD ディスク番号。
- 下位互換性のための任意の LUN。ただし、これは非推奨です。その他のデバイスでは、正常なブートを確保するために、ブート可能なイメージを保持している必要はありません。

UEFI ブート モード

Unified Extensible Firmware Interface（UEFI）は、オペレーティング システムとプラットフォーム ファームウェア間のソフトウェア インターフェイスを定義する仕様です。Cisco UCS Manager では、BIOS ファームウェア インターフェイスの代わりに UEFI が使用されます。これにより、BIOS はレガシー サポートを提供する一方で UEFI で動作できるようになります。

ブート ポリシーを作成する際は、レガシー ブート モードまたは UEFI ブート モードのいずれかを選択できます。レガシー ブート モードは、Cisco UCS C125 M5 サーバ 以外のすべての Cisco UCS サーバでサポートされます。UEFI ブート モードは M4 以降のサーバーでのみサポートされ、このモードで UEFI セキュア ブート モードを有効にできます。Cisco UCS C125 M5 サーバ は UEFI ブート モードのみサポートしています。

UEFI PXE ブートは、Cisco UCS Manager リリース 2.2(4) 以降と統合された Cisco UCS ラック サーバー上のすべての Cisco VIC アダプタでサポートされています。Cisco UCS Manager リリース 2.2(1) 以降では、すべての Cisco ブレード サーバーで UEFI PXE ブートがサポートされます。

次の制限は、UEFI ブート モードに適用されます。

- UEFI ブート モードは、次の組み合わせではサポートされません。
  - Cisco UCS Manager と統合された Cisco UCS ブレード サーバーおよびラック サーバー上の Gen-3 Emulex アダプタと QLogic アダプタ。
  - Cisco UCS Manager と統合された Cisco UCS ラック サーバー上の Broadcom アダプタに対する iSCSI ブート。

- 2 つの iSCSI LUN で UEFI ブート モードを使用する場合は、Cisco UCS Manager に IQN 接尾辞プールからの名前の選択を許可するのではなく、基礎となる両方の iSCSI eNIC に適用されるサービス プロファイルに共通の iSCSI イニシエータ名を手動で指定する必要があります。共通の名前を指定しない場合、Cisco UCS Manager は 2 番目の iSCSI LUN を検出できません。
- 同じサーバーで UEFI とレガシー ブート モードを混在させることはできません。
- ブート ポリシーに設定されているブート デバイスに UEFI 対応オペレーティング システムがインストールされている場合にのみ、サーバーは UEFI モードで正常に起動します。互換性のある OS が存在しない場合、ブート デバイスは [Boot Order Details] 領域の [Actual Boot Order] タブに表示されません。
- ごくまれですが、UEFI ブート マネージャ エントリが BIOS NVRAM に正しく保存されなかったため、UEFI ブートが成功しない場合があります。UEFI シェルを使用すると、UEFI ブート マネージャ エントリを手動で入力することができます。この状況は、以下の場合に発生する可能性があります。
  - UEFI ブート モードが有効なブレード サーバーがサービス プロファイルから関連付けを解除され、[Equipment] タブまたは前面パネルを使用してブレードの電源を手動でオンにする場合。
  - UEFI ブート モードが有効なブレード サーバーがサービス プロファイルから関連付けを解除され、直接の VIC ファームウェア アップグレードが試行される場合。
  - UEFI ブート モードが有効なブレード サーバーまたはラック サーバーが SAN LUN からブートされ、サービス プロファイルが移行される場合。

Cisco UCS Manager で UEFI ブート パラメータを作成できます。詳細については「UEFI ブート パラメータ （182 ページ）」を参照してください。

UEFI セキュア ブート

Cisco UCS Manager は、Cisco UCS B シリーズ M4 以降のブレード サーバー、 Cisco UCS C シリーズ M4 以降のラック サーバー 、および Cisco UCS S シリーズ M4 ラック サーバー、 および Cisco UCS C125 M5 サーバで UEFI セキュア ブートをサポートしています。 Linux セキュア ブートは、リリース 4.0 (4a) 以降の SLES 15、SLES 13 SP4、Red Hat Linux 7.6 オペレーティング システムでサポートされています。UEFI セキュア ブートがイネーブルの場合、すべての実行可能ファイル（ブート ローダ、アダプタ ドライバなど）はロードされる前に BIOS によって認証されます。認証されるには、そのイメージに Cisco 認証局（CA）または Microsoft CA による署名が必要です。

UEFI セキュア ブートには次の制限が適用されます。

- UEFI ブート モードは、ブート ポリシーで有効にする必要があります。
- UEFI ブート モードは、ドライブでのみ使用可能です。

- Cisco UCS Manager ソフトウェアと BIOS ファームウェアは、リリース 2.2 以上である必要があります。

（注） UEFI ブート モードは、リリース 2.2(3a) 以降の Cisco UCS C シリーズおよび S シリーズ ラック サーバーでサポートされます。

- ユーザー生成された暗号キーはサポートされません。
- UEFI セキュア ブートは、Cisco UCS Manager でのみ制御できます。
- サーバーがセキュア ブート モードのときに Cisco UCS Manager を以前のバージョンにダウングレードする場合は、ダウングレードする前に、サーバーの関連付けを解除し、再び関連付ける必要があります。これを行わないと、サーバー ディスカバリは失敗します。
- Cisco UCS Manager リリース 4.0 では、次のオペレーティング システムで UEFI セキュア ブートがサポートされています。
  - Cisco UCS Manager リリース 4.0(1) では、windows 2016 および Windows 2012 R2 でのみ UEFI セキュア ブートがサポートされています。
  - Cisco UCS Manager リリース 4.0(1) では、windows 2016 および Windows 2019 でのみ UEFI セキュア ブートがサポートされています。
  - Cisco UCS Manager リリース 4.0 では、次で UEFI セキュア ブートがサポートされています。

表 *6 : Linux* オペレーティング システム

Linux OS	eNIC/nENIC	fNIC
RHEL 7.5	3.2.210.18.738.12	1.6.0.50
RHEL 7.6	3.2.210.18.738.12	2.0.0.37
Centos 7.5	3.2.210.18.738.12	1.6.0.50
CentOS 7.6	3.2.210.18.738.12	1.6.0.50
SLES 12.4	3.2.210.18.738.12	2.0.0.32
SLES 15	3.2.210.18.738.12	2.0.0.39-71.0
ESXi	受信トレイの動作	受信トレイの動作

（注）
- ESXi の場合、受信トレイのドライバは署名され、機能します。非同期ドライバは署名されておらず、機能しません。
- Oracle OS は IPv6 をサポートしていません。
- XEN OS は IPv6 をサポートしていません。

表 *7: Windows* オペレーティング システム

Windows OS	neNIC	Nfsd Nic
Windows 2016	5.3.25.4	3.2.0.3
Windows 2019	5.3.25.4	3.2.0.3

CIMC セキュア ブート

CIMC セキュア ブートでは、署名済みのシスコ ファームウェア イメージのみをサーバーにインストールし、実行できます。CIMC が更新されると、イメージは、ファームウェアがフラッシュされる前に認証されます。認証に失敗すると、ファームウェアはフラッシュされません。これにより、CIMC ファームウェアへの不正アクセスを防止します。

CIMC セキュア ブートの注意事項と制約事項

- CIMC セキュア ブートは、Cisco UCS M4、M5 と M6 ラック サーバーでサポートされています。

（注） CIMC セキュア ブートはCisco UCS C220 M4/M5/M6、C240 M4/M5/M6、C480 M5/C480 M5 ML、C225 M6と C245 M6ラック サーバーではデフォルトで有効になっており、Cisco UCS C460 M4 ラック サーバーでは CIMC ファームウェア リリース 2.2(3) 以降へのアップグレード後に自動的に有効になります。

- CIMCセキュアブートがイネーブルになると、それをディセーブルにすることはできません。
- CIMC セキュア ブートがサーバー上で有効になると、2.1(3) より前の CIMC ファームウェア イメージにダウングレードすることはできません。

CIMCセキュア ブートのステータスの判別

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 **[Equipment** > **Rack-Mounts]** > **[Servers]** > **[*Server Name*]** の順に展開します。

ステップ 3 [作業（Work）] 領域の [インベントリ（Inventory）] タブをクリックします。

ステップ 4 [CIMC] サブタブをクリックします。

ステップ 5 [CIMC] 領域の [Secure Boot Operational State] フィールドをメモします。

次のいずれかになります。

- [Unsupported]：CIMC セキュア ブートはサーバーでサポートされていません。
- [Disabled]：CIMCセキュアブートはサーバーでサポートされていますが、無効になっています。
- [Enabling]：CIMC セキュア ブートはイネーブルで、操作は進行中です。
- [Enabled]：CIMC セキュア ブートはサーバでイネーブルになっています。

ブート ポリシーの作成

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

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]** > **[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 [Boot Policies] を右クリックし、[Create Boot Policy] を選択します。

[Create Boot Policy] ウィザードが表示されます。

ステップ 5 ポリシーの一意の名前と説明を入力します。

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

ステップ 6 (Optional) ブート順序に変更を加えた後、**[Reboot on Boot Order Change]** チェック ボックス を確認して、このブート ポリシーを使用するすべてのサーバを再起動します。

シスコ以外の VIC アダプタがあるサーバに適用されるブート ポリシーの場合、[Reboot on Boot Order Change] チェックボックスがオフでも、SAN デバイスが追加、削除または順序の変更がなされると、ブート ポリシーの変更の保存時にサーバは常にリブートします。

ステップ 7 (Optional) 必要に応じて、**[Enforce vNIC/vHBA/iSCSI Name]** チェック ボックスをオンにします。

- オンにした場合、Cisco UCS Manager は設定エラーと、**[Boot Order]** テーブルにリストされた 1 つ以上の vNIC、vHBA、iSCSI vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかのレポートとを表示します。
- オフにした場合は、Cisco UCS Manager がサービス プロファイルから（ブート オプションに応じて）vNIC または vHBA を使用します。

ステップ 8 [Boot Mode] フィールドで [Legacy] または [UEFI] オプション ボタンをオンにします。

Note Cisco UCS C125 M5 サーバ は UEFI ブート モードのみをサポートします。

ステップ 9 [UEFI] を選択した場合、UEFI ブート セキュリティを有効にするには [ブート セキュリティ（Boot Security）] チェックボックスをオンにします。

ステップ 10 次の 1 つ以上のオプションをブート ポリシーに設定し、ブート順序を設定します。

- [Local Devices boot]：サーバのローカル ディスクなどのローカル デバイスから、仮想メディアまたはリモート仮想ディスクを起動するには、ブート ポリシー用ローカル ディスク ブートの設定, on page 176 に進みます。
- [SAN boot]：SAN のオペレーティング システム イメージから起動するには、ブート ポリシー用 SAN ブート ポリシー設定, on page 144 に進みます。

  プライマリおよびセカンダリ SAN ブートを指定できます。プライマリ ブートが失敗した場合、サーバーはセカンダリからのブートを試行します。
- [LAN boot]：集中型プロビジョニング サーバから起動するには、ブート ポリシー用 LAN ブート ポリシー設定, on page 174 に進みます。
- [iSCSI ブート（iSCSI boot）]：iSCSI LUN から起動するには、iSCSI ブート ポリシーの作成, on page 157 に進みます。

What to do next

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられると、サーバの [General] タブの [Boot Order Details] 領域でブート順序を確認できます。

SAN ブート

SAN 上のオペレーティング システム イメージから 1 つ以上のサーバーがブートするように、ブート ポリシーを設定できます。ブート ポリシーにはプライマリとセカンダリの SAN ブートを含めることができます。プライマリ ブートが失敗した場合、サーバーはセカンダリからのブートを試行します。

シスコでは、システム内で最高のサービス プロファイル モビリティを提供する SAN ブートの使用を推奨しています。SANからブートした場合、あるサーバーから別のサーバーにサービス プロファイルを移動すると、新しいサーバーは、同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、新しいサーバーは同じサーバーと認識されます。

SAN ブートを使用するには、次の項目が設定されていることを確認してください。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージ デバイスと通信できること。
- オペレーティング システム イメージが置かれているデバイス上のブート ターゲット LUN（論理ユニット番号）。

（注） SAN ブートは、Cisco UCS ブレードおよびラック サーバー上の Gen-3 Emulex アダプタではサポートされていません。

ブート ポリシー用 SAN ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

Tip ローカル ディスクと SAN LUN の両方がブート順序のストレージ タイプに設定されていて、オペレーティング システムまたは論理ボリューム マネージャ（LVM）の設定が誤っている場合、サーバが SAN LUN ではなくローカル ディスクからブートする場合があります。

たとえば、Red Hat Linux がインストールされているサーバで、LVM にデフォルトの LVM が設定されていて、ブート順序に SAN LUN とローカル ディスクが設定されている場合、Linux は同じ名前の LV が 2 つあるという通知を生成し、SCSI ID の値が最も小さい LV（ローカル ディスクの可能性があります）からブートします。

この手順は、ブート ポリシーの作成, on page 142 から直接続いています。

Procedure

ステップ 1 下矢印をクリックして [vHBAs] 領域を展開します。

ステップ 2 [Add SAN Boot] リンクをクリックします。

ステップ 3 [Add San Boot] ダイアログ ボックスで、vHBA とタイプを指定して、[OK] をクリックします。

[Primary] または [Secondary] の SAN ブートを指定できます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。[Any] オプションは、SAN ストレージデバイスに直接接続し、UCS Manager をバイパスしているサポート対象外のアダプタに使用します。UCSM が管理するサポート対象の一連のアダプタの場合の SAN ブートには [Any] を使用しないでください。サポート対象外のアダプタについては、ベンダーの指示に従ってブート用のアダプタを設定します。

ステップ 4 この vHBA がブート可能な SAN イメージを参照する場合は、[Add SAN Boot Target] リンクをクリックし、[Add SAN Boot Target] ダイアログボックスで、ブート ターゲット LUN、ブート ターゲット WWPN、およびタイプを指定して、[OK] をクリックします。

ステップ 5 次のどちらかを実行します。

- **[Boot Order]** テーブルに別のブート デバイスを追加します。
- [OK] をクリックして終了します。

What to do next

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

iSCSI ブート

iSCSI ブートを利用すると、サーバーはネットワークにリモートに配置されている iSCSI ターゲット マシンからオペレーティング システムを起動できます。

iSCSI ブートは次の Cisco UCS VIC アダプタでサポートされます：

- Cisco UCS VIC 1200 シリーズ
- Cisco UCS VIC 1300 シリーズ
- Cisco UCS VIC 1400 シリーズ

iSCSI ブートを設定する前に満たさなければならない前提条件があります。これらの前提条件のリストについては、iSCSI ブートのガイドラインと前提条件 （147 ページ） を参照してください。

iSCSI ブートを実装するための手順の概要については、iSCSI ブートの設定 （150 ページ）を参照してください。

iSCSI ブート プロセス

Cisco UCS Manager は、サーバーにあるアダプタをプログラムするための関連付けプロセスで、サービス プロファイル用に作成された iSCSI vNIC と iSCSI のブート情報を使用します。アダプタのプログラミング後に、サーバーは最新のサービス プロファイル値で再起動します。電源投入時セルフ テスト（POST）の後、アダプタは、それらのサービス プロファイル値を使用して初期化を試みます。値を使用して指定されたターゲットにログインできる場合、アダプタは iSCSI ブート ファームウェア テーブル（iBFT）を初期化してホスト メモリにポスト紙、有効なブート可能 LUN をシステム BIOS にポストします。ホスト メモリにポストされる iBFT には、プライマリ iSCSI VNIC にプログラミングされた、イニシエータとターゲットの設定が含まれています。

（注） 以前は、ホストは LUN 検出が最初に終了したパスに応じて、設定されたブート パスのうち 1 つだけを参照し、そのパスから起動していました。現在は、設定された iSCSI ブート vNIC が 2 つある場合、ホストは両方のブート パスを参照するようになりました。そのため、マルチパス構成では、両方のブート vNIC に単一の IQN を設定する必要があります。ホスト上のブート vNIC に設定された異なる IQN が存在する場合、ホストは PCI 順序が低いブート vNIC に設定された IQN を使用して起動します。

次の手順であるオペレーティング システム（OS）のインストールでは、iBFT 対応の OS が必要です。OS のインストール時に、OS インストーラは iBFT テーブルのホストのメモリをスキャンし、iBFT テーブルの情報を使用してブート デバイスの検出とターゲット LUN への iSCSI パス作成を行います。OS によっては、このパスを完了するために NIC ドライバが必要です。このステップが成功した場合、OS インストーラが OS をインストールする iSCSI ターゲット LUN を検出します。

（注） iBFT は OS インストールのソフトウェア レベルで動作し、HBA モード（別名 TCP オフロード）では動作しない場合があります。iBFT が HBA モードで動作するかどうかは、インストール中の OS の機能によって異なります。また、Cisco UCS M51KR-B Broadcom BCM57711 アダプタを含むサーバーについては、iBFT は MTU ジャンボ設定に関係なく、最大伝送単位（MTU）サイズ 1500 で正常に動作します。OS が HBA モードをサポートする場合、iSCSI インストール プロセスの後に HBA モード、デュアル ファブリックのサポートおよびジャンボ MTU サイズの設定が必要な場合があります。

iSCSI ブートのガイドラインと前提条件

iSCSI ブートを設定する前に、これらのガイドラインと前提条件を満たす必要があります。

- iSCSI ブート ポリシーの作成後、ls-compute 権限を持つユーザーは、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ーは iSCSI ブート ポリシーを作成できません。
- セカンド vNIC（フェールオーバー vNIC）が iSCSI LUN から起動する必要がある Windows 2008 サーバーからの iSCSI ブートを設定するには、Microsoft Knowledge Base Article 976042 を参照してください。Microsoft には、ネットワーキング ハードウェアが変更されたときに、Windows が iSCSI ドライブからの起動に失敗するか、bugcheck エラーが発生する可能性がある、という既知の問題があります。この問題を回避するには、Microsoft が推奨する解決方法に従ってください。
- ストレージ アレイは、iSCSI ブートのライセンスが付与され、アレイ サイド LUN マスキングが正しく設定されている必要があります。
- 各 iSCSI イニシエータに 1 つずつ、2 つの IP アドレスを決定する必要があります。IP アドレスは、ストレージアレイと同じサブネット上にある必要があります（可能な場合）。IP アドレスは、Dynamic Host Configuration Protocol（DHCP）を使用して静的または動的に割り当てられます。
- グローバル ブート ポリシーのブート パラメータは設定できません。代わりに、ブート パラメータを設定した後、ブート ポリシーを適切なサービス プロファイルに含めます。
- オペレーティング システム（OS）は iSCSI Boot Firmware Table（iBFT）互換である必要があります。
  - RHEL 7.x の場合は、インストールの前にカーネル パラメータ「rd.iscsi.ibft=1」が必須となります。パラメータを入力しないと、iSCSI ブートに失敗することがあります。
  - SLES 12.x の場合は、次のガイドラインに従う必要があります。
    - カーネルをロードする前に、インストール ディスクで「e」を押し、linuxefi (EFI を使用している場合) またはカーネル (レガシーを使用している場合) を編集して、カーネル パラメータ「rd.iscsi.ibft=1 rd.iscsi.firmware=1 rd.neednet=1」を追加します。パラメータを入力しないと、iSCSI ブートに失敗することがあります。
    - ISCSI を使用する既存のシステムで、/etc/iscsi/iscsid.conf has node.startup=automatic (manual ではない) であることを確認します。このパラメータを /etc/default/grub/ に追加してから、grub2-mkconfig -o /boot/grub2/grub.cfg を実行して grub 設定を再構築します。
- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタの場合：
  - iSCSI ブートを使用するサーバーは、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタを含んでいる必要があります。アダプタ カードの取り付け方法や交換方法については、『*Cisco UCS B250 Extended Memory Blade Server Installation and Service Note*』 を参照してください。サービス ノートは、

http://www.cisco.com/go/unifiedcomputing/b-series-doc の 『*Cisco UCS B-Series Servers Documentation Roadmap*』 からアクセスできます。

- iSCSI デバイスの MAC アドレスを設定します。
- DHCP Vendor ID（オプション 43）を使用している場合は、iSCSI デバイスの MAC アドレスを /etc/dhcpd.conf に設定します。
- HBA モード（別名 TCP オフロード）および Boot to Target 設定がサポートされます。ただし、インストール中の HBA モードは Windows OS だけがサポートします。
- OS をインストールする前に、iSCSI のアダプタ ポリシーで Boot to Target 設定を無効にし、OS をインストールした後で、Boot to Target 設定を再度有効にします。

（注） アダプタ ポリシーの設定を変更するたびに、アダプタはリブートして新しい設定を適用します。

- iSCSI ターゲットに OS をインストールするときは、iSCSI ターゲットの順番を OS イメージが存在するデバイスよりも前にしておく必要があります。たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に iSCSI ターゲット、その後 CD とする必要があります。
- サーバーが iSCSI ブートされた後は、イニシエータ名、ターゲット名、LUN、iSCSI デバイス IP、ネット マスクやゲートウェイを Broadcom ツールで変更しないでください。
- POST（電源投入時自己診断テスト）プロセスを中断しないでください。中断すると、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタは初期化に失敗します。

- Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合：

  Cisco UCS VIC-1240 仮想インターフェイス カードの場合：

  - iSCSI デバイスの MAC アドレスを設定しないでください。
  - HBA モードおよび Boot to Target 設定はサポートされていません。
  - iSCSI ターゲットに OS をインストールするときは、iSCSI ターゲットの順番を OS イメージが存在するデバイスよりも後にしておく必要があります。たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に CD、その後 iSCSI ターゲットとする必要があります。
  - DHCP Vendor ID（オプション 43）を使用している場合、オーバーレイ vNIC の MAC アドレスを /etc/dhcpd.conf に設定する必要があります。
  - サーバーの iSCSI ブート後は、オーバーレイ vNIC の IP 詳細を変更しないでください。

- VMware ESX/ESXi オペレーティング システムは、iSCSI ブート ターゲット LUN へのコア ダンプ ファイルの保存をサポートしていません。ダンプ ファイルはローカル ディスクに書き込む必要があります。

イニシエータ IQN の設定

Cisco UCS は、サービス プロファイルが物理サーバーに関連付けられた時点で、以下のルールを使用してアダプタ iSCSI vNIC のイニシエータ IQN を決定します。

- サービス プロファイル レベルのイニシエータ IQN と iSCSI vNIC レベルのイニシエータ IQN を、1 つのサービス プロファイルで一緒に使用することはできません。
- イニシエータ IQN をサービス プロファイル レベルで指定すると、DHCP オプション 43 の場合（イニシエータ IQN はアダプタ iSCSI vNIC で空に設定される）を除き、すべてのアダプタ iSCSI vNIC が同じイニシエータ IQN を使用するように設定されます。
- イニシエータ IQN を iSCSI vNIC レベルで設定すると、サービス プロファイル レベルのイニシエータ IQN は削除されます（存在する場合）。
- サービス プロファイルに 2 つの iSCSI vNIC があり、一方にだけイニシエータ IQN が設定されている場合、もう一方にはデフォルトの IQN プールが設定されます。この設定は後で変更できます。唯一の例外は、DHCP オプション 43 が設定されている場合です。その場合、もう一方の iSCSI vNIC のイニシエータ IQN は、サービス プロファイルを関連付けるときに削除されます。

（注） ベンダー ID を設定して、DHCP オプション 43 を使用するように iSCSI vNIC を変更した場合、サービス プロファイル レベルで設定したイニシエータ IQN は削除されません。サービス プロファイル レベルのイニシエータ IQN は、DHCP オプション 43 を使用しない別の iSCSI vNIC で使用できます。

Windows での MPIO のイネーブル化

ストレージ アレイで接続を最適化するには、MPIOをイネーブルにします。

（注） ネットワーク ハードウェアを変更すると、Windows が iSCSI ドライブからの起動に失敗する場合があります。詳細については、『Microsoft support Article ID: 976042』を参照してください。

始める前に

Microsoft Multipath I/O（MPIO）を有効化するサーバーには、Cisco VIC ドライバが必要です。

ブート LUN に設定されたパスが複数ある場合、LUN がインストールされるときにイネーブルにするパスは 1 つのみです。

手順

ステップ 1 サーバーに関連付けられたサービス プロファイルで、プライマリ iSCSI vNIC を設定します。

詳細については、サービス プロファイル用 iSCSI vNIC の作成 （158 ページ）を参照してください。

ステップ 2 プライマリ iSCSI vNIC を使用して、iSCSI ターゲット LUN に Windows オペレーティング システムをインストールします。

ステップ 3 Windows のインストールが完了したら、ホスト上で MPIO をイネーブルにします。

ステップ 4 サーバーに関連付けられたサービス プロファイルで、ブート ポリシーにセカンダリ iSCSI vNIC を追加します。

詳細については、iSCSI ブート ポリシーの作成 （157 ページ） を参照してください。

iSCSI ブートの設定

LUN ターゲットから iSCSI ブートするよう Cisco UCS でアダプタまたはブレードを設定する場合、次のすべてのステップを完了します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） iSCSI ブートのアダプタ ポリシーを設定します。	詳細については、iSCSI ブート ポリシーの作成 （157 ページ）を参照してください。
ステップ 2	（任意） イニシエータとターゲットの認証プロファイルを設定します。	詳細については、iSCSI 認証プロファイルの作成 （154 ページ）を参照してください。
ステップ 3	（任意） IP アドレス プールの IP アドレスを使用するよう iSCSI イニシエータを設定するには、iSCSI イニシエータ プールに IP アドレスのブロックを追加します。	詳細については、iSCSI イニシエータ IP プールの作成 （156 ページ）を参照してください。
ステップ 4	すべてのサービス プロファイルで使用できるブート ポリシーを作成します。または、特定のサービス ポリシーに対してのみローカル ブート ポリシーを作	すべてのサービス プロファイルで使用できるブート ポリシーの作成の詳細については、iSCSI ブート ポリシーの作成（157ページ）を参照してください。

	コマンドまたはアクション	目的
	成できます。ただし、複数のサービスプロファイルと共有できるブートポリシーを作成することを推奨します。	
ステップ 5	すべてのサービスプロファイルで使用できるブートポリシーを作成した場合は、それをサービスプロファイルに割り当てます。それ以外の場合は、次のステップに進みます。	ステップ 7 において、サービス プロファイルで iSCSI ブートおよび vNIC パラメータを設定するときに、サービスプロファイルにブートポリシーを割り当てることができます。
ステップ 6	サービス プロファイルで iSCSI vNIC を作成します。	詳細については、サービスプロファイル用 iSCSI vNIC の作成 （158 ページ）を参照してください。
ステップ 7	expert モードでサービス プロファイルにおいて、またはサービスプロファイル テンプレートにおいて、iSCSI ブート パラメータ（iSCSI 修飾子名（IQN）、イニシエータ、ターゲット インターフェイスなど）および iSCSI vNIC パラメータを設定します。	詳細については、[Expert] ウィザードを使用したサービスプロファイルの作成（188 ページ）またはサービスプロファイルテンプレートの作成（207 ページ）を参照してください。
ステップ 8	iSCSI ブート動作を確認します。	詳細については、「*Verifying iSCSI Boot*」を参照してください。
ステップ 9	OS をインストールする前に、OS が iSCSI ブート ファームウェア テーブル (iBFT) と互換性があることを確認します。 • RHEL 7.x の場合は、OS をインストールする前にカーネルパラメータ「rd.iscsi.ibft=1」が必須となります。 • SLES 12.x については、カーネルをロードする前に、インストールディスクで「e」を押し、linuxefi (EFI を使用している場合) またはカーネル(レガシーを使用している場合) を編集して、カーネル パラメータ「rd.iscsi.ibft=1 rd.iscsi.firmware=1 rd.neednet=1」を追加します。	適切なパラメータを入力しないと、iSCSI ブート操作に失敗することがあります。
ステップ 10	サーバーに OS をインストールします。	詳細については、次のいずれかのドキュメントを参照してください。

	コマンドまたはアクション	目的
		• 『*Cisco UCS B* シリーズ ブレード サーバー *VMware* インストレーション ガイド』 • 『*Cisco UCS B* シリーズ ブレード サーバー *Linux* インストレーション ガイド』 • 『*Cisco UCS B* シリーズ ブレード サーバー *Windows* インストレーション ガイド』
ステップ 11	サーバーをブートします。	

iSCSI アダプタ ポリシーの作成

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]** > **[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 iSCSI Adapter Policy] を選択します。

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

名前	説明
[名前（Name）] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[Connection Timeout] フィールド	Cisco UCS が、最初のログインに失敗し、iSCSI アダプタが使用できないと見なすまで待機する秒数。 0 ～ 255 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアの値セットを使用します（デフォルト：15 秒）。

名前	説明
[LUN Busy Retry Count] フィールド	iSCSI LUN 検出中にエラーが発生した場合に接続を再試行する回数。 0 ～ 60 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアの値セットを使用します（デフォルト：15 秒）。
[DHCP Timeout] フィールド	イニシエータが DHCP サーバーが使用できないと判断するまでに待機する秒数。 60 ～ 300 の整数を入力します（デフォルト：60 秒）。
[Enable TCP Timestamp] チェックボックス	TCP タイムスタンプを使用する場合は、このボックスをオンにします。この設定では、必要に応じてパケットのラウンドトリップ時間を計算できるように、送信パケットにはパケット送信時のタイムスタンプが付きます。 **Note** このオプションは、Cisco UCS NIC M51KR-B アダプタを備えたサーバーだけに適用されます。
[HBA Mode] チェックボックス	HBA モード（別名 TCP オフロード）をイネーブルにするには、このボックスをオンにします。 **Important** このオプションは、Windows オペレーティング システムを実行する Cisco UCS NIC M51KR-B アダプタがあるサーバーに対してのみ有効にするようにします。
[Boot to Target] チェックボックス	iSCSI ターゲットから起動する場合は、このボックスをオンにします。 **Note** このオプションは、Cisco UCS NIC M51KR-B アダプタを備えたサーバーだけに適用されます。このオプションは、サーバにオペレーティング システムをインストールするまで無効にしておく必要があります。

名前	説明
[Owner] フィールド	次のいずれかになります。 • [ローカル（Local）]：このポリシーは、この Cisco UCS ドメイン内のサービス プロファイルとサービス プロファイル テンプレートでのみ使用できます。 • [グローバル移行中（Pending Global）]：このポリシーの制御は、Cisco UCS Centralに移行中です。移行が完了すると、このポリシーは（Cisco UCS Centralに登録されている）すべての Cisco UCS ドメインで使用可能になります。 • [グルーバル（Global）]：このポリシーは Cisco UCS Central で管理されます。このポリシーを変更する場合は、必ず Cisco UCS Central を使用してください。

ステップ 6 [OK] をクリックします。

What to do next

アダプタ ポリシーをサービス プロファイルとテンプレートに含めます。

iSCSI 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、[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] ノードを展開します。

ステップ 5 アダプタ 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。

iSCSI 認証プロファイルの作成

iSCSI ブートの場合、イニシエータおよびターゲットの iSCSI 認証プロファイルを作成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 **[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 [iSCSI Authentication Profiles] を右クリックし、[iSCSI Authentication Profile] を選択します。

ステップ 5 [Create Authentication 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。

名前	説明
[名前（Name）] フィールド	認証プロファイルの名前。 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。
[ユーザ ID（User ID）] フィールド	このプロファイルに関連付けられたユーザ ID。 1 ～ 128 文字の文字、スペース、特殊文字を入力します。
[Password] フィールド	このプロファイルに関連付けられたパスワード。 12 ～ 16 文字（特殊文字を含む）を入力します。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

ステップ 6 [OK] をクリックします。

次のタスク

認証プロファイルをサービス プロファイルとテンプレートに含めます。

iSCSI 認証プロファイルの削除

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]** > **[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 [iSCSI Authentication Profiles] ノードを展開します。

ステップ 5 削除する IP プールを右クリックし、[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。

iSCSI イニシエータ IP プールの作成

iSCSI ブートに使用する IP アドレスのグループを作成できます。Cisco UCS Manager は指定した IPv4 アドレスのブロックを予約します。

サーバまたはサービスプロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、IP プールに含まれていてはなりません。

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 **[LAN]** > **[プール]**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 [IP Pools] ノードを展開します。

ステップ 5 [IP Pool iscsi-initiator-pool] を右クリックし、[Create Block of IPv4 Addresses] を選択します。

ステップ 6 [Create a Block of IPv4 Addresses] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[名前（Name）] カラム	ブロックに割り当てる IPv4 アドレスの範囲。
[開始（From）] カラム	ブロック内の最初の IPv4 アドレス。
[終了（To）] カラム	ブロック内の最後の IPv4 アドレス。
[サブネット（Subnet）] カラム	ブロック内の IPv4 アドレスと関連付けられたサブネットマスク。
[デフォルト ゲートウェイ（Default Gateway）] カラム	ブロック内の IPv4 アドレスに関連付けられたデフォルト ゲートウェイ。
[プライマリ DSN（Primary DNS）] カラム	この IPv4 アドレスのブロックがアクセスするプライマリ DNS サーバ。
[セカンダリ DNS（Secondary DNS）] カラム	この IPv4 アドレスのブロックがアクセスするセカンダリ DNS サーバ。

ステップ 7 [OK] をクリックします。

次のタスク

1 つ以上のサービス プロファイルまたはサービス プロファイル テンプレートを設定し、iSCSI イニシエータ IP プールから iSCSI イニシエータ IP アドレスを取得します。

iSCSI ブート ポリシーの作成

ブート ポリシーあたり最大 2 つの iSCSI vNIC を追加できます。一方の vNIC はプライマリ iSCSI ブート ソースとして動作し、もう一方はセカンダリ iSCSI ブート ソースとして動作します。

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 [Boot Policies] を右クリックし、[Create Boot Policy] を選択します。

[Create Boot Policy] ウィザードが表示されます。

ステップ 5 ポリシーの一意の名前と説明を入力します。

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

ステップ 6 （任意） ブート順序の変更後にこのブート ポリシーを使用するサーバをリブートするには、**[Reboot on Boot Order Change]** チェック ボックス をオンにします。

Cisco UCS Manager GUI で、ブート ポリシーの [順序を変更したときにリブートする（Reboot on Boot Order Change] チェックボックスがオンになっていて、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスを削除または追加してもブート順序には直接影響せず、サーバは再起動しません。

（注） これは、標準のブート順序を使用しているサーバにのみ適用されます。

ステップ 7 （任意） 必要に応じて、**[Enforce vNIC/vHBA/iSCSI Name]** チェック ボックスをオンにします。

- オンにした場合、Cisco UCS Manager は設定エラーと、**[Boot Order]** テーブルにリストされた 1 つ以上の vNIC、vHBA、iSCSI vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかのレポートとを表示します。

- オフにした場合は、Cisco UCS Manager がサービス プロファイルから（ブート オプションに応じて）vNIC または vHBA を使用します。

ステップ 8 iSCSI ブートをブート ポリシーに追加するには、次の手順を実行します。

a) 下矢印をクリックして [iSCSI vNICs] 領域を展開します。
b) [Add iSCSI Boot] リンクをクリックします。
c) [Add iSCSI Boot] ダイアログボックスで、iSCSI vNIC の名前を入力し、[OK] をクリックします。
d) 別の iSCSI vNIC を作成するには、ステップ b、c を繰り返します。

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの **[一般（General）]** タブの **[ブート順序の詳細（Boot Order Details）]** 領域で実際のブート順序を確認できます。

サービス プロファイル用 iSCSI vNIC 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 **[サーバ]** > **[サービスプロファイル]**を展開します。
ステップ 3 iSCSI vNIC を作成するサービス 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。
ステップ 4 iSCSI vNIC を作成するサービス プロファイルを展開します。
ステップ 5 [iSCSI vNICs] ノードを右クリックし、[Create vNICs] を選択します。
ステップ 6 [Create iSCSI vNIC] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	iSCSI vNIC 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。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC に関連付けられた LAN vNIC（存在する場合）。

名前	説明
[iSCSI Adapter Policy] ドロップダウン リスト	この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー（存在する場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI アダプタを作成するには、このリンクをクリックします。
[MAC Address] フィールド	この iSCSI vNIC に関連付けられた MAC アドレス（存在する場合）。MAC アドレスが設定されていない場合、Cisco UCS Manager GUI は **[Derived]** と表示します。
[MAC Pool] フィールド	この iSCSI vNIC に関連付けられた MAC プール（存在する場合）。
[VLAN] ドロップダウン リスト	この iSCSI vNIC に関連付けられた仮想 LAN。デフォルトの VLAN は [default] です。 （注） Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合、指定する VLAN はオーバーレイ vNIC のネイティブ VLAN と同じである必要があります。 Cisco UCS M51KR-B Broadcom BCM57711 アダプタの場合、指定した VLAN は、オーバーレイ vNIC に割り当てられたどの VLAN でも設定できます。

ステップ 7 [iSCSI MAC Address] 領域の [MAC Address Assignment] ドロップダウン リストで、次のいずれかを選択します。

- MAC アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。このサービス プロファイルに関連付けられるサーバが Cisco UCS M81KR 仮想インターフェイス カード アダプタまたは Cisco UCS VIC-1240 仮想インターフェイス カードを含む場合、このオプションを選択します。

  重要 このサービス プロファイルに関連付けられたサーバに Cisco UCS NIC M51KR-B アダプタが含まれる場合、MAC アドレスを指定する必要があります。

- 特定の MAC アドレスを使用する場合は、[00:25:B5:XX:XX:XX] を選択し、アドレスを [MAC Address] フィールドに入力します。このアドレスが使用可能であることを確認するには、対応するリンクをクリックします。
- プール内の MAC アドレスを使用する場合は、リストからプール名を選択します。各プール名の後には、数字のペアが括弧で囲まれています。最初の数字はそのプール内の使用可能な MAC アドレスの数であり、2 番めの数字はそのプール内の MAC アドレスの合計数です。

この Cisco UCS ドメインが Cisco UCS Central に登録されている場合は、プール カテゴリが 2 つ存在することがあります。**[ドメイン プール（Domain Pools）]** は Cisco UCS ドメイン でローカルに定義され、**[グローバル プール（Global Pools）]** は Cisco UCS Central で定義されます。

ステップ 8 （任意）すべてのサービス プロファイルで使用できる MAC プールを作成する場合は、[Create MAC Pool] をクリックし、[Create MAC Pool] ウィザードでフィールドに値を入力します。

詳細については、『』『*Cisco UCS Manager Network Management Guide, Release 3.2*』の「*Creating a MAC Pool*」セクションを参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 （任意） イニシエータ名を設定または変更する場合は、[iSCSI vNIC（iSCSI vNICs）] タブから [イニシエータ名のリセット（Reset Initiator Name）] または [イニシエータ名の変更（Change Initiator Name）] をクリックし、[イニシエータ名の変更（Change Initiator Name）] ダイアログ ボックスのフィールドを入力するかクリックします。詳細については、「サービス プロファイル レベルでのイニシエータ IQN の設定 （160 ページ）」を参照してください。

サービス プロファイルからの iSCSI vNIC の削除

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 iSCSI vNIC を削除するサービス 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。

ステップ 4 iSCSI vNIC を削除するサービス プロファイルを展開します。

ステップ 5 [iSCSI vNICs] ノードを展開します。

ステップ 6 削除する iSCSI vNIC 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。

サービス プロファイル レベルでのイニシエータ IQN の設定

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 編成の対象となるノードを展開します。

ステップ 4 変更する iSCSI vNIC のサービス プロファイルをクリックします。
ステップ 5 [作業（Work）] ペインで、[iSCSI vNIC（iSCSI vNICs）] タブをクリックします。
ステップ 6 [Reset Initiator Name] 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。

サービス プロファイル レベルでのイニシエータ IQN の変更

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]**を展開します。
ステップ 3 編成の対象となるノードを展開します。
ステップ 4 変更する iSCSI vNIC のサービス プロファイルをクリックします。
ステップ 5 [作業（Work）] ペインで、[iSCSI vNIC（iSCSI vNICs）] タブをクリックします。
ステップ 6 [アクション（Actions）] エリアで、[イニシエータ名の変更（Change Initiator Name）] をクリックします。
ステップ 7 [Change Initiator Name] ダイアログボックスで、次のフィールドの値を変更します。

名前	説明
[イニシエータ名の割り当て（Initiator Name Assignment）] ドロップダウン リスト	ドロップダウン リストから、使用する IQN イニシエータ名を選択します。
[イニシエータ名] フィールド	手動によるイニシエータ名の割り当てを選択した場合は、イニシエータ名を入力します。
[IQN サフィックス プールの作成（Create IQN Suffix Pool）] リンク	これをクリックして、新しい IQN 接尾辞プールを作成します。

ステップ 8 [OK] をクリックします。

iSCSI ブート パラメータの設定

iSCSI vNIC のブート順序、ブート ポリシー、iSCSI 認証プロファイル、イニシエータ インターフェイス、ターゲット インターフェイスなど、iSCSI ブート パラメータを設定できます。

手順

ステップ 1 [ナビゲーション]ペインで、[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 iSCSIブート パラメータを作成するサービスプロファイ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 iSCSI ブート パラメータを作成するサービス プロファイルをクリックします。

ステップ 5 [Boot Order] タブをクリックします。

ステップ 6 [Specific Boot Policy] 領域で、下矢印をクリックして [iSCSI vNICs] 領域を展開します。

ステップ 7 [iSCSI vNICs] 領域で、サーバのブート元の iSCSI vNIC をダブルクリックしてそれらを [Boot Order] テーブルに追加します。

ステップ 8 [iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。

2 つの iSCSI vNIC がある場合は、ブート パラメータを設定する方を選択します。

ステップ 9 [Set iSCSI Boot Parameters] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ブート パラメータを設定している iSCSI vNIC の名前。
[認証プロファイル（Authentication Profile）] ドロップダウン リスト	関連する iSCSI 認証プロファイルの名前。
[認証プロファイルの作成（Create Authentication Profile）] リンク	このリンクをクリックして、すべての iSCSI vNIC で使用可能となる新しい iSCSI 認証プロファイルを作成します。

ステップ 10 [Initiator Name] 領域で、次のフィールドに入力します。

名前	説明
[イニシエータ名の割り当て（Initiator Name Assignment）] ドロップダウン リスト	iSCSI ブート イニシエータ名の割り当て方法を選択します。次の方法の中から 1 つを選択してください。 • [手動（Manual）]：[イニシエータ名（Initiator Name）] フィールドに名前を入力します。イニシエータ名は最大 223 文字です。 • [Pools]：IQN 接尾辞プールを選択します。このプールから名前が割り当てられます。 （注） [iSCSI ブート パラメータの設定（Set iSCSI Boot Parameters）] ダイアログボックスでイニシエータ名を設定すると、サービス プロファイル レベルではなく、iSCSI vNIC レベルでイニシエータ IQN が設定されます。複数のパスが設定されている場合は、[iSCSI vNICs] タブから、またはサービス プロファイルの作成時に、イニシエータ IQN を設定する必要があります。 必要に応じて、イニシエータ名を変更またはリセットできます。詳細については、サービス プロファイル レベルでのイニシエータ IQN の変更 （161 ページ）を参照してください。
[IQN サフィックス プールの作成（Create IQN Suffix Pool）] リンク	すべての iSCSI vNIC で使用可能な新しい IQN 接尾辞プールを作成するには、このリンクをクリックします。
]Initiator Name] フィールド	iSCSI イニシエータ名を定義する正規表現。 任意の英数字および次の特殊文字を入力できます。 • .（ピリオド） • :（コロン） • -（ダッシュ）

ステップ 11 [Initiator IP Address Policy] ドロップダウン リストで、次のいずれかを選択します。

オプション	説明
[Select (DHCP used by default)]	システムが DHCP を使用してインターフェイスを自動的に選択します。 ステップ 13 に進みます。
Static	スタティック IPv4 アドレスが、この領域に入力された情報に基づいて iSCSI ブート vNIC に割り当てられます。

オプション	説明
	ステップ 12 に進みます。
Pool	IPv4 アドレスが管理 IP アドレス プールから iSCSI ブート vNIC に割り当てられます。 ステップ 13 に進みます。

ステップ 12 [Initiator IP Address Policy] ドロップダウン リストから [Static] を選択した場合は、次のフィールドに値を入力します。

名前	説明
[IPv4 Address] フィールド	iSCSI ブート vNIC に割り当てられた IPv4 アドレス。 このアドレスを指定する場合は、[Initiator IP Address Policy] ドロップダウン リストで [Static] を選択する必要があります。
[Subnet Mask] フィールド	IPv4 アドレスに関連付けられたサブネット マスク。
[デフォルト ゲートウェイ（Default Gateway）] フィールド	IPv4 アドレスに関連付けられたデフォルト ゲートウェイ。
[プライマリ DNS（Primary DNS）] フィールド	プライマリ DNS サーバーのアドレス。
[セカンダリ DNS（Secondary DNS）] フィールド	セカンダリ DNS サーバー アドレス。

ステップ 13 iSCSI ターゲット インターフェイスでは、次のいずれかのオプション ボタンを選択します。

オプション	説明
[iSCSI Static Target Interface]	システムにより、設定する必要があるスタティック ターゲット インターフェイスが作成されます。 ステップ 14 に進みます。
[iSCSI Auto Target Interface]	システムにより、自動ターゲット インターフェイスが作成されます。自動ターゲットがイニシエータと DHCP ベンダー ID のどちらを使用するか指定する必要があります。 ステップ 16 に進みます。

ステップ 14 [iSCSI Static Target Interface] を選択した場合、[Static Target Interface] テーブルで [Add] をクリックします。

ステップ 15 [Create iSCSI Static Target] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[iSCSI Target Name] フィールド	iSCSI ターゲットの iSCSI 修飾名（IQN）または拡張固有識別子（EUI）の名前を定義する正規表現。 任意の英数字および次の特殊文字を入力することができます。 • .（ピリオド） • :（コロン） • -（ダッシュ） **重要** この名前は、標準の IQN または EUI のガイドラインに従って適切な形式にする必要があります。 以下に、正しい形式の iSCSI ターゲット名の例を示します。 • iqn.2001-04.com.example • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 • iqn.2001-04.com.example:storage.tape1.sys1.xyz • iqn.2001-04.com.example:storage.disk2.sys1.xyz • eui.02004567A425678D
[Priority] フィールド	システムによって iSCSI ターゲットに割り当てられたプライオリティ。
[Port] フィールド	iSCSI ターゲットに関連付けられたポート。 1 ～ 65535 の整数を入力します。デフォルトは 3260 です。
[認証プロファイル（Authentication Profile）] ドロップダウン リスト	関連する iSCSI 認証プロファイルの名前。
[iSCSI 認証プロファイルの作成（Create iSCSI Authentication Profile）] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。
[IPv4 Address] フィールド	iSCSI ターゲットに割り当てられた IPv4 アドレス。
[LUN Id] フィールド	iSCSI ターゲットの LUN 識別子です。

ステップ 16 [iSCSI Auto Target Interface] を選択した場合、[DHCP Vendor Id] フィールドにイニシエータ名またはDHCPベンダーIDを入力します。イニシエータがすでに設定済みである必要があります。ベンダー ID には、最大 32 文字の英数字を指定できます。

ステップ 17 [OK] をクリックします。

iSCSI ブート パラメータの変更

iSCSI vNIC のブート順序、ブート ポリシー、iSCSI 認証プロファイル、イニシエータ インターフェイス、ターゲット インターフェイスなど、iSCSI ブート パラメータを変更できます。

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 iSCSIブートパラメータを変更するサービスプロファイ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 iSCSI ブート パラメータを変更するサービス プロファイルをクリックします。

ステップ 5 [Boot Order] タブをクリックします。

ステップ 6 [Specific Boot Policy] 領域で、下矢印をクリックして [iSCSI vNICs] 領域を展開します。

ステップ 7 ブート順序の iSCSI vNIC を追加または削除する、またはブート順序を変更するには、次のいずれかを実行します。

- iSCSI vNIC を追加するには、[iSCSI vNICs] 領域で、iSCSI vNIC をダブルクリックして [Boot Order] テーブルに追加します。
- ブート順序から iSCSI vNIC を削除するには、[Boot Order] テーブルで、iSCSI vNIC を選択して [Delete] をクリックします。
- iSCSI vNIC のブート順序を変更するには、[Boot Order] テーブルで、iSCSI vNIC を選択して [Move Up] または [Move Down] をクリックします。

ステップ 8 ブート パラメータを変更するには、[iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。

2 つの iSCSI vNIC がある場合は、ブート パラメータを変更する方を選択します。

ステップ 9 [Set iSCSI Boot Parameters] ダイアログボックスで、次のいずれかのフィールドの値を変更します。

名前	説明
[名前（Name）] フィールド	ブート パラメータを設定している iSCSI vNIC の名前。
[認証プロファイル（Authentication Profile）] ドロップダウン リスト	関連する iSCSI 認証プロファイルの名前。
[認証プロファイルの作成（Create Authentication Profile）] リンク	このリンクをクリックして、すべての iSCSI vNIC で使用可能となる新しい iSCSI 認証プロファイルを作成します。

ステップ 10 [Initiator Name] 領域で、次のフィールドに入力します。

名前	説明
[イニシエータ名の割り当て（Initiator Name Assignment）] ドロップダウン リスト	iSCSI ブート イニシエータ名の割り当て方法を選択します。次の方法の中から 1 つを選択してください。 • [手動（Manual）]：[イニシエータ名（Initiator Name）] フィールドに名前を入力します。イニシエータ名は最大 223 文字です。 • [Pools]：IQN 接尾辞プールを選択します。このプールから名前が割り当てられます。 （注） [iSCSI ブート パラメータの設定（Set iSCSI Boot Parameters）] ダイアログボックスでイニシエータ名を設定すると、サービス プロファイル レベルではなく、iSCSI vNIC レベルでイニシエータ IQN が設定されます。複数のパスが設定されている場合は、[iSCSI vNICs] タブから、またはサービス プロファイルの作成時に、イニシエータ IQN を設定する必要があります。 必要に応じて、イニシエータ名を変更またはリセットできます。詳細については、サービス プロファイル レベルでのイニシエータ IQN の変更 （161 ページ）を参照してください。
[IQN サフィックス プールの作成（Create IQN Suffix Pool）] リンク	すべての iSCSI vNIC で使用可能な新しい IQN 接尾辞プールを作成するには、このリンクをクリックします。
]Initiator Name] フィールド	iSCSI イニシエータ名を定義する正規表現。 任意の英数字および次の特殊文字を入力できます。 • .（ピリオド） • :（コロン） • -（ダッシュ）

ステップ 11 [Initiator IP Address Policy] ドロップダウン リストの選択を、次のいずれかに変更します。

オプション	説明
[Select (DHCP used by default)]	システムが DHCP を使用してインターフェイスを自動的に選択します。 ステップ 13 に進みます。
Static	スタティック IPv4 アドレスが、この領域に入力された情報に基づいて iSCSI ブート vNIC に割り当てられます。

オプション	説明
	ステップ 12 に進みます。
Pool	IPv4 アドレスが管理 IP アドレス プールから iSCSI ブート vNIC に割り当てられます。 ステップ 13 に進みます。

ステップ 12 [Initiator IP Address Policy] ドロップダウン リストで [Static] を選択した場合、次のフィールドを入力するか変更してください。

名前	説明
[IPv4 Address] フィールド	iSCSI ブート vNIC に割り当てられた IPv4 アドレス。 このアドレスを指定する場合は、[Initiator IP Address Policy] ドロップダウン リストで [Static] を選択する必要があります。
[Subnet Mask] フィールド	IPv4 アドレスに関連付けられたサブネット マスク。
[デフォルト ゲートウェイ（Default Gateway）] フィールド	IPv4アドレスに関連付けられたデフォルト ゲートウェイ。
[プライマリ DNS（Primary DNS）] フィールド	プライマリ DNS サーバーのアドレス。
[セカンダリDNS（Secondary DNS）] フィールド	セカンダリ DNS サーバー アドレス。

ステップ 13 iSCSI ターゲット インターフェイスでは、次のいずれかのオプション ボタンを選択します。

オプション	説明
[iSCSI Static Target Interface]	システムにより、設定する必要があるスタティック ターゲット インターフェイスが作成されます。 ステップ 14 に進みます。
[iSCSI Auto Target Interface]	システムにより、自動ターゲット インターフェイスが作成されます。自動ターゲットがイニシエータと DHCP ベンダー ID のどちらを使用するか指定する必要があります。 ステップ 15 に進みます。

ステップ 14 [iSCSI Static Target Interface] を選択した場合は、[Static Target Interface] テーブルで次のいずれかを実行します。

- iSCSI スタティック ターゲット インターフェイスを追加するには、[Add] をクリックします。iSCSI ターゲット インターフェイスを変更するには、変更する iSCSI ターゲット イン

ターフェイスを選択して [Modify] をクリックします。次に、[Create iSCSI Static Target] ダイアログボックスで、次のフィールドを入力または変更します。

名前	説明
[iSCSI Target Name] フィールド	iSCSI ターゲットの iSCSI 修飾名（IQN）または拡張固有識別子（EUI）の名前を定義する正規表現。 任意の英数字および次の特殊文字を入力することができます。 • .（ピリオド） • :（コロン） • -（ダッシュ） **重要** この名前は、標準の IQN または EUI のガイドラインに従って適切な形式にする必要があります。 以下に、正しい形式の iSCSI ターゲット名の例を示します。 • iqn.2001-04.com.example • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 • iqn.2001-04.com.example:storage.tape1.sys1.xyz • iqn.2001-04.com.example:storage.disk2.sys1.xyz • eui.02004567A425678D
[Priority] フィールド	システムによって iSCSI ターゲットに割り当てられたプライオリティ。
[Port] フィールド	iSCSI ターゲットに関連付けられたポート。 1 ～ 65535 の整数を入力します。デフォルトは 3260 です。
[認証プロファイル（Authentication Profile）] ドロップダウン リスト	関連する iSCSI 認証プロファイルの名前。
[iSCSI 認証プロファイルの作成（Create iSCSI Authentication Profile）] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。
[IPv4 Address] フィールド	iSCSI ターゲットに割り当てられた IPv4 アドレス。
[LUN Id] フィールド	iSCSI ターゲットの LUN 識別子です。

- iSCSI ターゲット インターフェイスを削除するには、削除する iSCSI ターゲット インターフェイスを選択して [Delete] をクリックします。

（注） 2 つの iSCSI スタティック ターゲットがあり、優先順位 1 位のターゲットを削除すると、優先順位 2 位のターゲットが優先順位 1 位のターゲットになります。ただし、このターゲットは、Cisco UCS Manager では、引き続き優先順位 2 位のターゲットとして表示されます。

ステップ 15 [iSCSI Auto Target Interface] を選択した場合、[DHCP Vendor Id] フィールドのエントリをイニシエータ名または DHCP ベンダー ID に変更します。イニシエータがすでに設定済みである必要があります。ベンダー ID には、最大 32 文字の英数字を指定できます。

ステップ 16 [OK] をクリックします。

IQN プール

IQN プールは、Cisco UCS ドメイン内の iSCSI vNIC によって発信側 ID として使用される iSCSI 修飾名（IQN）の集合です。

IQN プールのメンバは、プレフィックス**:**サフィックス**:**数字の形式になります。これで、プレフィックス、サフィックス、および数字のブロック（範囲）を指定することができます。

IQN プールには、番号の範囲やサフィックスが異なる（ただし、プレフィックスは共通している）複数の IQN ブロックを含めることができます。

IQN プールの作成

（注） ほとんどの場合、最大 IQN サイズ（プレフィックス + サフィックス + 追加文字）は 223 文字です。Cisco UCS NIC M51KR-B アダプタを使用する場合、IQN サイズを 128 文字に制限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、[SAN]をクリックします。

ステップ 2 **[SAN]** > **[プール]**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 [IQN Pools] を右クリックし、[Create IQN Suffix Pool] を選択します。

ステップ 5 [Create IQN Suffix 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。

フィールド	説明
名前	iSCSI 修飾名（IQN）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]	プール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）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
Prefix	このプール用に作成された任意の IQN ブロックのプレフィクス。 1 ～ 150 文字を入力します。任意の文字や数字、および次の特殊文字を使用できます：（ピリオド）、:（コロン）、-（ハイフン）。たとえば、**`iqn1.alpha.com`** を使用できます。
[割り当て順序（Assignment Order）] フィールド	次のいずれかになります。 • **[デフォルト（Default）]**：Cisco UCS Manager はプールからランダム ID を選択します。 • **[シーケンシャル（Sequential）]**：Cisco UCS Manager はプールから最も小さい使用可能な ID を選択します。

ステップ 6 [Next] をクリックします。

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

ステップ 8 [Create a Block of IQN Suffixes] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Suffix] フィールド	iSCSI 修飾名（IQN）のこのブロックの接尾辞。 1 ～ 64 文字を入力します。任意の文字や数字、および次の特殊文字を使用できます：（ピリオド）、:（コロン）、-（ハイフン）。たとえば、**`alphadc-1`** を使用できます。
[From] フィールド	ブロック内の最初の接尾辞番号。
[Size] フィールド	ブロック内の接尾辞の数。

ステップ 9 **[OK]** をクリックします。

ステップ 10 [Finish] をクリックして、ウィザードを終了します。

次のタスク

IQN サフィックス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。

IQN プールへのブロックの追加

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]** > **[プール]**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 [IQN Pools] ノードを展開します。

ステップ 5 目的の IQN プールを右クリックし、[Create a Block of IQN Suffixes] を選択します。

ステップ 6 [Create a Block of IQN Suffixes] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Suffix] フィールド	iSCSI 修飾名（IQN）のこのブロックの接尾辞。 1 ～ 64 文字を入力します。任意の文字や数字、および次の特殊文字を使用できます：.（ピリオド）、:（コロン）、-（ハイフン）。たとえば、**alphadc-1** を使用できます。
[From] フィールド	ブロック内の最初の接尾辞番号。
[Size] フィールド	ブロック内の接尾辞の数。

ステップ 7 **[OK]** をクリックします。

IQN プールからのブロックの削除

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]** > **[プール]**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 [IQN Pools] ノードを展開します。
ステップ 5 IQN 接尾辞のブロックを削除する IQN プールを選択します。
ステップ 6 [Work] ペインで、[IQN Blocks] タブをクリックします。
ステップ 7 削除するブロックを右クリックし、[Delete] を選択します。
ステップ 8 **[はい (Yes)]** をクリックして削除を確認します。
ステップ 9 **[Save Changes]**をクリックします。

IQN 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]** > **[プール]**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 [IQN Pools] ノードを展開します。
ステップ 5 削除するプールを右クリックして、[削除]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。

LAN ブート

LAN の集中プロビジョニング サーバーから 1 つまたは複数のサーバーをブートするブート ポリシーを設定できます。LAN（またはPXE）ブートは、そのLANサーバーからサーバーにOSをインストールする際に頻繁に使用されます。

LAN ブート ポリシーには、複数のタイプのブート デバイスを追加できます。たとえば、ローカル ディスクや仮想メディア ブートをセカンダリ ブート デバイスとして追加できます。

ブート ポリシー用 LAN ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。たとえば、セカンダリ ブート デバイスとしてローカル ディスクや仮想メディアのブートを追加できます。

この手順は、ブート ポリシーの作成 （142 ページ） から直接続いています。

手順

ステップ 1 下矢印をクリックして [vNICs] 領域を展開します。

ステップ 2 **[Add LAN Boot]** リンクをクリックします。

ステップ 3 **[Add LAN Boot]** ダイアログボックスで、LAN ブートに使用する vNIC の名前を [vNIC] フィールドに入力して、[OK] をクリックします。

ステップ 4 次のどちらかを実行します。

- **[Boot Order]** テーブルに別のブート デバイスを追加します。
- [OK] をクリックして終了します。

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ローカル デバイス ブート

Cisco UCS Manager 異なるローカル デバイスから起動することができます。

（注） 拡張ブート順序を使用している Cisco UCS M4 以降のブレード サーバーとラック サーバーの場合、トップレベルと第 2 レベルのどちらのブート デバイスも選択できます。

（注） 同じコントローラで複数のブート オプションが提供されている場合、ブート オプションは、Cisco UCS Manager で設定されたブート順序ではなく、次のように扱われます。

- OS がインストールまたはブートされると、UEFI ブートの場合、インストールされた OS は、Cisco UCS Manager で設定されているブート オプションに関係なく、ブート オプションを 0 優先度（最優先） にプッシュします。
- 起動順序は、BIOS によって設定された起動デバイスの列挙と、コントローラがデバイスをホストに公開する方法 (または Cisco UCS Manager で提供) に基づいています。

ローカル ディスク ブート

サーバーにローカル ドライブがある場合、ブート ポリシーを設定して、トップレベルのローカルディスク デバイスまたは第2 レベルのデバイスのいずれかからサーバーを起動できます。

- [Local LUN]：ローカル ディスクまたはローカル LUN からの起動を有効にします。
- [Local JBOD]：ブート可能な JBOD からの起動を有効にします。
- [SD card]：SD カードからの起動を有効にします。
- [Internal USB]：内部 USB からの起動を有効にします。
- [External USB]：外部 USB からの起動を有効にします。
- [内蔵ローカル LUN（Embedded Local LUN）]：すべての Cisco UCS M4、M5 、および M6 サーバー上の内蔵ローカル LUN からの起動を有効にします。
- [内蔵ローカル ディスク（Embedded Local Disk）]：すべての Cisco UCS M4、M5、および M6 サーバー上の内蔵ローカル ディスクからの起動を有効にします。

（注） Cisco UCS C125 M5 サーバでは、別の PCIe ストレージ コントローラがない場合、このオプションを使用しないでください。代わりに、**[Add Local Disk]**オプションを使用します。

（注） 第 2 レベルのデバイスは、拡張ブート順序を使用している Cisco UCS M4 以降のブレード サーバーとラック サーバーでのみ使用できます。

仮想メディア ブート

ブート ポリシーを設定して、サーバーからアクセスできる仮想メディア デバイスから 1 つ以上のサーバーを起動できます。仮想メディア デバイスは、物理 CD/DVD ディスク（読み取り専用）またはフロッピーディスク（読み取りと書き込み）のサーバーへの挿入を疑似的に実行します。このタイプのサーバー ブートは、通常、サーバーに手動でオペレーティング システムをインストールするために使用されます。

（注） 第 2 レベルのデバイスは、拡張ブート順序を使用している Cisco UCS M4 以降のブレード サーバーとラック サーバーでのみ使用できます。

リモート仮想ドライブのブート

ブート ポリシーを設定して、サーバーからアクセスできるリモート仮想ドライブから 1 つ以上のサーバーを起動できます。

NVMe のブート

リリース 3.2(1) 以降、Cisco UCS Manager には NVMe デバイスを M5 および M6 ブレード サーバーやラック サーバーのブート ポリシーに追加するオプションが備わっています。BIOS は、存在する NVMe デバイスを列挙し、UEFI 対応 OS がインストールされている最初の NVMe デバイスで起動します。

Cisco ブート最適化 M.2 RAID コントローラ

4.0(4a) 以降、Cisco UCS Manager は Marvell 88SE92xx PCIe から SATA 6Gb/s コントローラ (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。BIOS は、このコントローラにインストールされている M.2 SATA ドライブを列挙し、その後前面パネルの SATA ドライブが UEFI 対応 OS がインストールされている最初の SATA デバイスから起動します。

ブート ポリシー用ローカル ディスク ブートの設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。たとえば、セカンダリ ブート デバイスとして SD カードのブートを追加できます。

この手順は、ブート ポリシーの作成 （142 ページ） から直接続いています。

手順

ステップ 1 **[ローカル デバイス (Local Devices)]** 領域を展開します。

ステップ 2 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- [ローカル ディスクの追加（Add Local Disk）] または
  - **[Add Local LUN]**
  - **[Add Local JBOD (ローカル JBOD の追加)]**
  - **[Add SD Card]**
  - **[Add Internal USB]**
  - **[Add External USB]**
  - **[Add Embedded Local LUN (内蔵ローカルLUNの追加)]**
  - **[Add Embedded Local Disk (内蔵ローカルディスクの追加)]**

    重要 Cisco Boot 最適化 M. 2 RAID コントローラ (HWRAID) が設定されている場合は、**[Add Embedded Local Disk (組み込みローカル ディスクを追加)]** ダイアログ ボックスで、**[いずれか (Any)]** を選択してディスクを追加します。**[プライマリ (Primary)]** または **[セカンダリ (Secondary)]** を選択しないでください。

（注） 拡張ブート順序を使用している Cisco UCS M4 以降のブレード サーバーとラック サーバーの場合、トップレベルと第2 レベルのどちらのブート デバイスも選択できます。

ステップ 3 次のどちらかを実行します。

- **[Boot Order]** テーブルに別のブート デバイスを追加します。
- [OK] をクリックして終了します。

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ブート ポリシー用仮想メディア ブートの設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービ

ス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。ローカル ディスク ブートをセカンダリ ブート デバイスとして追加できます。

（注） 仮想メディアでは、USB を有効にする必要があります。USB の機能に影響する BIOS 設定を変更した場合は、仮想メディアにも影響します。したがって、最適なパフォーマンスを実現するためには、次の USB BIOS をデフォルト設定のままにしておくことをお勧めします。

- [デバイスをブート不可能にする（Make Device Non Bootable）]：**[無効（disabled）]** に設定します。
- [USB アイドル電源最適化設定（USB Idle Power Optimizing Setting）]：**[ハイパフォーマンス（high-performance）]** に設定します。

この手順は、ブート ポリシーの作成 （142 ページ） から直接続いています。

手順

ステップ 1 下矢印をクリックして [Local Devices] 領域を展開します。

ステップ 2 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- **[Add CD/DVD]** または
  - **[Add Local CD/DVD]**
  - **[Add Remote CD/DVD]**（ラック サーバの KVM CD/DVD 用）

    M5 ブレード サーバを使用した設定で、ISO を KVM コンソールにマッピングしている場合は、**ブート順序**には **[Remote CD/DVD]** のみを使用してください。
- **[Add Floppy]** または
  - **[Add Local Floppy]**
  - **[Add Remote Floppy]**
- **[Add Remote Virtual Drive]**

（注） 拡張ブート順序を使用している Cisco UCS M4 以降のブレード サーバーとラック サーバーの場合、トップレベルと第 2 レベルのどちらのブート デバイスも選択できます。

ステップ 3 次のどちらかを実行します。

- **[Boot Order]** テーブルに別のブート デバイスを追加します。

- [OK] をクリックして終了します。

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ブート ポリシー用 NVMe ブートの設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。たとえば、セカンダリ ブート デバイスとして SD カードのブートを追加できます。

この手順は、ブート ポリシーの作成 （142 ページ） から直接続いています。

手順

ステップ 1 下矢印をクリックして [Local Devices] 領域を展開します。

ステップ 2 [Add NVMe] をクリックし、デバイスを [Boot Order] テーブルに追加します。

（注） NVMe ブート ポリシーは、**[Uefi]** ブート モードでのみ使用できます。

ステップ 3 次のどちらかを実行します。

- **[Boot Order]** テーブルに別のブート デバイスを追加します。
- [OK] をクリックして終了します。

次のタスク

ブート ポリシーをサービス プロファイルとテンプレートに含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

vMedia サービス プロファイルへのブート ポリシーの追加

この手順では、[Create Service Profile (expert)] ウィザードの [Server Boot Order] ページで、vMedia のブート ポリシーのオプションを設定する方法について説明します。

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]**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。
[Unified Computing System Manager] ペインが表示されます。

ステップ 5 [名前（Name）] フィールドに、サービス プロファイルの識別に使用できる一意の名前を入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

この名前は、サービスプロファイルを作成する組織またはサブ組織内で一意である必要があります。

ステップ 6 **[UUID Assignment]** ドロップダウン リストで、次のいずれかの手順を実行します。

オプション	説明
Select (pool default used by default)	デフォルトの UUID 接尾辞プールから UUID を割り当てます。 ステップ 8 に進みます。
	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUID はサービス プロファイルがサーバと関連付けられるまで割り当てられません。この時点で、UUIDは製造元によってサーバに割り当てられた UUID 値に設定されます。サービス プロファイルを後で別のサーバに移動すると、UUIDは新しいサーバに一致するように変更されます。 ステップ 8 に進みます。
	手動で割り当てる UUID を使用します。 ステップ 7 に進みます。
Pools ***Pool_Name***	ドロップダウン リストの下部のリストから選択する UUID 接尾辞プールから UUID を割り当てます。 各プール名の後には、プール内で利用可能な UUID の数および UUID 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。 既存のプールを使用するのではなく、すべてのサービス プロファイルがアクセスできるプールを作成する場合は、ステップ 4 に進みます。それ以外の場合はステップ 8 に進みます。

ステップ 7 （任意） オプションを選択した場合は、次の手順を実行します。

a) [UUID] フィールドに、このサービス プロファイルを使用するサーバに割り当てる有効な UUID を入力します。

ステップ 8 （任意） このサービス プロファイルで使用する新しい UUID サフィックス プールを作成する場合は、[Create UUID Suffix Pool] をクリックし、[Create UUID Suffix Pool] ウィザードのフィールドに値を入力します。

詳細については、UUID 接尾辞プールの作成 （128 ページ）を参照してください。

ステップ 9 （任意） テキスト ボックスに、このサービス プロファイルの説明を入力します。

このサービス プロファイル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）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 10 [Next] をクリックします。

ステップ 11 [Create Service Profile (expert)] に移動し、[Server Boot Order] をクリックします。
[Boot Policy] ペインが表示されます。

ステップ 12 [Boot Policy] ドロップダウン リストから、次のいずれかを選択します。

オプション	説明
Select Boot Policy to use	このサービスプロファイルにデフォルトのブート ポリシーを割り当てます。 ステップ 13 に進みます。
[特定のブート ポリシーを作成（Create a Specific Boot Policy）]	このサービスプロファイルテンプレートだけがアクセスできるローカル ブート ポリシーを作成できます。
Boot Policies ***Policy_Name***	サービス プロファイルに既存のブート ポリシーを割り当てます。このオプションを選択した場合、Cisco UCS Manager でポリシーの詳細が表示されます。 既存のポリシーを使用するのではなく、すべてのサービス プロファイルがアクセスできるポリシーを作成する場合は、[Create Boot Policy] をクリックします。それ以外の場合は、リストでポリシーを選択し、ステップ 13 に進みます。

ステップ 13 すべてのサービス プロファイルおよびテンプレートにアクセスできる新しいブート ポリシーを作成したら、[Boot Policy] ドロップダウン リストからそのポリシーを選択します。

ステップ 14 [Next] をクリックします。

次のタスク

サービス プロファイルを Cisco UCS サーバに関連付けます。

ブート ポリシーの削除

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（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
ステップ 3 [Boot 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。

UEFI ブート パラメータ

サーバーの UEFI ブート モードは、プラットフォーム ハードウェアに保存されている情報によって決まります。UEFI OS ブート ローダに関する情報を含むブート エントリは、サーバーの BIOS フラッシュに保存されます。2.2(4) より前の Cisco UCS Manager リリースでは、サービス プロファイルがあるサーバーから別のサーバーに移行されると、ブートローダ情報は宛先サーバーで使用できなくなります。そのため、BIOS は、サーバーを UEFI ブート モードでブートするためのブート ローダ情報をロードできません。

Cisco UCSM リリース 2.2(4) では、宛先サーバー上の UEFI OS ブート ローダの位置に関する情報を BIOS に提供する UEFI ブート パラメータが導入され、BIOS はその位置からブート ローダをロードできます。サーバーは、そのブートローダ情報を使用して、UEFI ブート モードでブートできます。

UEFI ブート パラメータに関する注意事項と制約事項

- ブート モードが UEFI の場合のみ、UEFI ブート パラメータを設定できます。
- Cisco UCS Manager をリリース 2.2(4) 以降にアップグレードする場合は、サービス プロファイルの移行中に UEFI ブートが失敗しても自動的に処理されません。UEFI 対応 OS で正常にブートするには、ターゲット デバイスで UEFI ブート パラメータを明示的に作成しておく必要があります。
- UEFI ブート パラメータは、セカンドレベルのブート順序をサポートする、M4 以降のすべてのサーバーでサポートされています。
- 次のデバイス タイプの UEFI ブート パラメータを指定できます。

- SAN LUN
- ISCSI LUN
- ローカル LUN

- UEFI ブート パラメータは各オペレーティング システム固有のパラメータです。次のオペレーティング システムの UEFI ブート パラメータを指定できます。
  - VMware ESX
  - SUSE Linux
  - Microsoft Windows
  - Red Hat Enterprise Linux 7

UEFI ブート パラメータの設定

始める前に

ブート ポリシーの [Boot Mode] が [Uefi] 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、[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 [Boot Policies] を展開し、UEFI ブート パラメータを設定するブート 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 LUN の UEFI ブート パラメータを設定するには、[Boot Order] 領域の LUN を選択し、[Set Uefi Boot Parameters] をクリックします。

重要 ローカル LUN、SAN LUN、iSCSI LUN に対してのみ UEFI ブート パラメータを設定できます。

ステップ 6 **[Set Uefi Boot Parameters]** ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Boot Loader Name]	ブートローダの名前を指定します。これは必須フィールドです。 例：grub.efi
[Boot Loader Path]	ブートローダがある場所のパスを指定します。これは必須フィールドです。ブート ローダの名前をこのフィールドに入力しないでください。パスだけを指定する必要があります。 例：\EFI\RedHat

フィールド	説明
[Boot Loader Description]	ブート ローダの詳細です。これは、F6ブート メニューに表示される可読形式の名前です。

ステップ 7 [OK] をクリックします。

ステップ 8 **[Save Changes]**をクリックします。

UEFI ブート パラメータの変更

始める前に

ブート ポリシーの [Boot Mode] が [Uefi] 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、[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 [Boot Policies] を展開し、UEFI ブート パラメータを変更するブート 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 UEFI ブート パラメータを使用して、LUN の UEFI ブート パラメータを変更するには、[Boot Order] 領域で LUN を選択し、[Modify Uefi Boot Parameters] をクリックします。

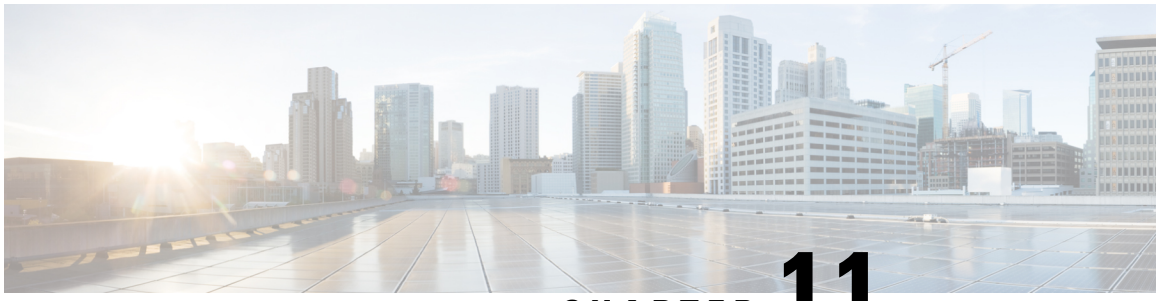
重要 ローカル LUN、SAN LUN、および iSCSI LUN に対してのみ UEFI ブート パラメータを設定できます。

ステップ 6 **[Modify Uefi Boot Parameters]** ダイアログボックスで、次の情報を入力します。

フィールド	説明
[Boot Loader Name]	ブート ローダの名前を指定します。これは必須フィールドです。
[Boot Loader Path]	ブート ローダがある場所のパスを指定します。これは必須フィールドです。
[Boot Loader Description]	ブート ローダの詳細です。

ステップ 7 [OK] をクリックします。

ステップ 8 **[Save Changes]**をクリックします。



CHAPTER 11

サービス プロファイル

- UCS Manager のサービス プロファイル （185 ページ）
- サーバー ID を上書きするサービス プロファイル, on page 186
- サーバー ID を継承するサービス プロファイル, on page 187
- サービス プロファイルに関するガイドラインおよび推奨事項 （187 ページ）
- サービス プロファイルの作成方法, on page 188
- インバンド サービス プロファイル, on page 192
- サービス プロファイル タスク, on page 193
- サービス プロファイルのアソシエーション, on page 204
- サービス プロファイル テンプレート, on page 206
- サービス プロファイル テンプレート タスク, on page 211
- サービス プロファイルのアソシエーション, on page 216

UCS Manager のサービス プロファイル

サービスプロファイルは、単一のサーバーおよびそのストレージとネットワークの特性を定義します。Cisco UCS Manager および UCS Mini のサービス プロファイルを作成できます。サービス プロファイルがサーバーに導入されると、UCS Manager は、サービス プロファイルで指定された設定に一致するよう、サーバー、アダプタ、ファブリック エクステンダ、ファブリック インターコネクトを自動的に設定します。

サービス プロファイルには、次の 4 種類の情報が含まれています。

- [Server definition]：プロファイルに適用するために必要なリソース（特定のシャーシに挿入された特定のサーバーやブレード）を定義します。
- [Identity information]：UUID、各仮想 NIC（vNIC）の MAC アドレス、各 HBA の WWN 仕様が含まれます。
- [Firmware revision specifications]：特定のテスト済みのファームウェア リビジョンをインストールする必要がある場合、またはその他の理由で特定のファームウェアを使用する必要がある場合に使用します。

- [Connectivity definition]：ネットワーク アダプタ、ファブリック エクステンダ、および親インターコネクトを設定します。ただし、この情報には各ネットワーク コンポーネントの設定方法の詳細が含まれていないため抽象的です。

UCS システムは、サーバー ID を継承するサービス プロファイルとサーバー ID をオーバーライドするサービス プロファイルの 2 つのタイプのサービス プロファイルを提供しています。

（注） サーバーは、そのプロパティの一部として**サーバー パーソナリティ**のフィールドを表示することもあります。Cisco UCS M6 サーバーでは、サーバーのパーソナリティが HX サーバーに設定されている場合に、このフィールドが表示されます。サーバー パーソナリティが設定されていない場合、このフィールドは表示されません。サーバー パーソナリティは情報提供のみを目的としており、UCS マネージャーの GUI ではリセットできません。ただし、UCS マネージャーの CLI には、サーバを「パーソナリティなし」の状態に戻すためのコマンド ライン オプションが用意されています。

サーバー ID を上書きするサービス プロファイル

このタイプのサービス プロファイルにより、柔軟性と制御性が最大化されます。このプロファイルでは、アソシエーション時にサーバーに設定されていた ID 値を上書きし、Cisco UCS Manager で設定されたリソース プールとポリシーを使用して一部の管理タスクを自動化できます。

このサービス プロファイルは、あるサーバーとの関連付けを解除して、別のサーバーに関連付けることができます。この再アソシエーションは手動で行うこともできますし、自動サーバー プール ポリシーを通じて行うこともできます。UUID や MAC アドレスなど、新しいサーバーの工場出荷時の設定は、サービス プロファイルでの設定で上書きされます。その結果、サーバーでの変更はネットワークに対して透過的です。新しいサーバーの使用を開始するために、ネットワークでコンポーネントやアプリケーションを再設定する必要はありません。

このプロファイルにより、次のようなリソース プールやポリシーを通じて、システム リソースを利用し、管理できるようになります。

- MAC アドレスのプール、WWN アドレス、UUID などの仮想 ID 情報
- イーサネットおよびファイバ チャネル アダプタ プロファイル ポリシー
- ファームウェア パッケージ ポリシー
- オペレーティング システム ブート順序ポリシー

サービス プロファイルに電源管理ポリシー、サーバー プール資格情報ポリシー、または特定のハードウェア設定が必要な別のポリシーが含まれていない場合は、そのサービス プロファイルを Cisco UCS ドメインのどのタイプのサーバーにも使用できます。

これらのサービス プロファイルは、ラックマウント サーバーまたはブレード サーバーのどちらかに関連付けることができます。サービスプロファイルの移行の可否は、サービスプロファイルの移行制限を選択するかどうかによって決まります。

Note 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。

サーバー ID を継承するサービス プロファイル

このハードウェアベースのサービスプロファイルは使用も作成も簡単です。このプロファイルは、サーバーのデフォルト値を使用して、ラックマウント型サーバーの管理を模倣します。これは特定のサーバーに関連付けられているため、別のサーバーへの移動や移行はできません。

このサービスプロファイルを使用するために、プールや設定ポリシーを作成する必要はありません。

このサービス プロファイルは、アソシエーション時に存在する次のような ID 情報および設定情報を継承し、適用します。

- 2 つの NIC の MAC アドレス
- 統合ネットワーク アダプタまたは仮想インターフェイス カードについては、2 つの HBA の WWN アドレス
- BIOS バージョン
- サーバーの UUID

Important このプロファイルをサーバーに関連付ける前に、製造元でサーバーのハードウェアに設定された値が変更された場合、このサービス プロファイルを通じて継承されたサーバーの ID および設定情報は、この値とは異なる可能性があります。

サービス プロファイルに関するガイドラインおよび推奨事項

サービス プロファイルまたはサービス プロファイル テンプレートに含まれるポリシー（ローカルディスク設定ポリシーなど）やプールに固有のガイドラインと推奨事項に加え、サービス プロファイルとサーバーを関連付ける機能に影響する以下のガイドラインと推奨事項も順守してください。

ラックマウント サーバーで設定できる vNIC 数の制限

Cisco UCS Manager と統合されているラックマウント サーバーでは、Cisco UCS P81E 仮想インターフェイスカード（N2XX-ACPCI01）などのサポート対象のアダプタごとに最大 56 の vNIC を設定できます。

ラックマウント サーバーの電力制限はサポート対象外

電力制限はラック サーバーではサポートされません。ラックマウント サーバーに関連付けられているサービスプロファイルに電力制御ポリシーを含めた場合、そのポリシーは実行されません。

vNIC に関する QoS ポリシーのガイドライン

QoS ポリシーのプライオリティ設定が **fc**（ファイバ チャネル システム クラス）ではない場合にのみ、そのポリシーを vNIC に割り当てることができます。QoS ポリシーのプライオリティに他のシステム クラスを設定できます。

vHBA に関する QoS ポリシーのガイドライン

QoS ポリシーのプライオリティ設定が **fc**（ファイバ チャネル システム クラス）である場合にのみ、そのポリシーを vHBA に割り当てることができます。

QoS ポリシーのホスト制御設定は vNIC にのみ適用されます。vHBA には影響しません。

サービス プロファイルの作成方法

[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。

Note LAN 接続ポリシーに対応する vNIC を作成する場合、ダイナミック vNIC、usNIC および VMQ はサポートされません。イーサネット アダプタ ポリシーを設定する場合は、RoCE、VXLAN、NvGRE はサポートされません。

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。

Note ストレージ ポリシーに従って vHBA を設定する場合は、FC vNIC はサポートされません。

ステップ 8 (オプション)**[ゾーニング (Zoning)]** パネルで、必要なゾーン分割情報を指定して **[次へ (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] パネルで、配置方法と PCI 順序を指定して [Next] 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。

サーバ ID を継承するサービス プロファイルの作成

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] を選択します。

ステップ 5 [Create Service Profile] ダイアログボックスの [Naming] 領域で、次のフィールドに値を入力します。

a) [名前（Name）] フィールドに、サービス プロファイルの識別に使用できる一意の名前を入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

b) **[Description]** フィールドに、このサービス プロファイルの説明を入力します。

ステップ 6 [Create Service Profile] ダイアログボックスの [vNICs] 領域で、プライマリおよびセカンダリの vNIC を選択します。

ステップ 7 [Create Service Profile] ダイアログボックスの [vHBAs] 領域で、プライマリおよびセカンダリの vHBA を選択します。

ステップ 8 [Create Service Profile] ダイアログボックスの [Boot Order] 領域で、プライマリおよびセカンダリのブート デバイスを選択します。

ステップ 9 （任意） [Server Association (optional)] 領域の [Select] カラムで、サーバのオプション ボタンをクリックして、このサービスとこのサーバを関連付けます。

ステップ 10 **[OK]** をクリックします。

ブレード サーバのハードウェア ベースのサービス プロファイルの作成

ハードウェア ベースの サービス プロファイルを別のサーバに移動することはできません。

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）] > [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 ハードウェア ベースのサービス プロファイルを作成するサーバを選択します。

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 [Actions] 領域で [Create Service Profile] をクリックします。

ステップ 6 [Create Service Profile for Server] ダイアログボックスで、次の手順を実行します。

a) [Create Service Profile in Organization] ドロップダウン リスト から、サービス プロファイルを作成する組織を選択します。

b) ラジオ ボタンをクリックします。

c) [Name] フィールドに、サービス プロファイルの一意の名前を入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

d) Cisco UCS Manager でサービス プロファイルの vNIC を作成する場合、[Create Default vNICs] チェックボックスをオンにします。

e) Cisco UCS Manager でサービス プロファイルの vHBA を作成する場合、[Create Default vHBAs] チェックボックスをオンにします。

f) [OK] をクリックします。

Cisco UCS Manager がサーバの ID および設定情報を継承して自動的に適用し、サービス プロファイルを作成してから、それをサーバに関連付けます。

ラックマウント サーバのハードウェア ベースのサービス プロファイルの作成

ハードウェア ベースの サービス プロファイルを別のサーバに移動することはできません。

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 **[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 ハードウェア ベースのサービス プロファイルを作成するサーバを選択します。

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 [Actions] 領域で [Create Service Profile] をクリックします。

ステップ 6 [Create Service Profile for Server] ダイアログボックスで、次の手順を実行します。

a) [Create Service Profile in Organization] ドロップダウン リスト から、サービス プロファイルを作成する組織を選択します。

b) ラジオ ボタンをクリックします。

c) [Name] フィールドに、サービス プロファイルの一意の名前を入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

d) Cisco UCS Manager でサービス プロファイルの vNIC を作成する場合、[Create Default vNICs] チェックボックスをオンにします。

e) Cisco UCS Manager でサービス プロファイルの vHBA を作成する場合、[Create Default vHBAs] チェックボックスをオンにします。

f) [OK] をクリックします。

Cisco UCS Manager がサーバの ID および設定情報を継承して自動的に適用し、サービス プロファイルを作成してから、それをサーバに関連付けます。

インバンド サービス プロファイル

サービス プロファイルからのインバンド設定の削除

この手順では、サービス プロファイルからインバンド管理 IP アドレスの設定を削除します。このアクションがグレー表示されている場合、インバンド設定は設定されていません。

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 [Work] ペインで、[General] タブをクリックします。

ステップ 4 [アクション（Actions）] 領域で、[インバンド構成の削除（Delete Inband Configuration）] をクリックします。

ステップ 5 [削除（Delete）] 確認ダイアログボックスで [はい（Yes）] をクリックします。

サービス プロファイルのインバンド管理 IP アドレスの設定が削除されます。

サービス プロファイル タスク

サービス プロファイルの名前の変更

サービス プロファイルの名前を変更すると、次のことが起こります。

- サービス プロファイルの以前の名前を参照するイベント ログと監査ログは、その名前のまま保持されます。
- 名前変更の操作を記録する、新しい監査データが作成されます。
- サービス プロファイルの以前の名前で生じたすべての障害データは、新しいサービス プロファイル名に転送されます。

（注） 保留中の変更があるサービス プロファイルの名前は変更できません。

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]**を展開します。

ステップ 3 名前を変更するサービス プロファイ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 名前を変更するサービス プロファイルをクリックします。

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、[Rename Service Profile] をクリックします。

ステップ 7 **[Rename Service Profile]** ダイアログ ボックスで、**[New Name]** フィールドフィールドにサービス プロファイルの新しい名前を入力します。

この名前には、2～32 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

ステップ 8 [OK] をクリックします。

サービス プロファイルのクローン化

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 クローンするサービス プロファイルを右クリックし、[Create a Clone] を選択します。

ステップ 5 [Create Clone From Service Profile] ダイアログボックスで次の作業を行います。

a) 新しいプロファイルに使用する名前を [Clone Name] フィールドに入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

この名前は、サービスプロファイルを作成する組織またはサブ組織内で一意である必要があります。

b) [OK] をクリックします。

ステップ 6 作成したサービス プロファイルに移動し、すべてのオプションが正しいことを確認します。

サービス プロファイルの UUID の変更

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]**を展開します。

ステップ 3 UUID を変更したいサービス プロファイ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 関連付けられたサーバの UUID を変更する必要のあるサービス プロファイルを選択します。

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

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

ステップ 7 **[UUID Assignment]** ドロップダウン リストで、次のいずれかの手順を実行します。

オプション	説明
[Select (pool default used by default)]	デフォルトの UUID 接尾辞プールから UUID を割り当てます。 ステップ 9 に進みます。
[Hardware Default]	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUID はサービス プロファイルがサーバと関連付けられるまで割り当てられません。この時点で、UUID は製造元によってサーバに割り当てられた UUID 値に設定されます。サービス プロファイルを後で別のサーバに移動すると、UUID は新しいサーバに一致するように変更されます。 ステップ 9 に進みます。
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX	手動で割り当てる UUID を使用します。 ステップ 8 に進みます。
Pools ***Pool_Name***	ドロップダウン リストの下部のリストから選択する UUID 接尾辞プールから UUID を割り当てます。 各プール名の後には、プール内で利用可能な UUID の数および UUID 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 9 に進みます。

ステップ 8 （任意） オプションを選択した場合は、次の手順を実行します。

a) [UUID] フィールドに、このサービス プロファイルを使用するサーバに割り当てる有効な UUID を入力します。

b) 選択した UUID が使用可能であることを確認するには、[here] リンクをクリックします。

ステップ 9 **[OK]** をクリックします。

サービス プロファイルのブート順序の変更

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]**を展開します。

ステップ 3 ブート順序を変更するサービス プロファイ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 ブート順序を変更するサービス プロファイルをクリックします。

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

ステップ 6 [Modify Boot Policy] をクリックして既存のブート ポリシーを変更します。

ステップ 7 [Modify Boot Policy] ダイアログボックスで、[Boot Policy] ドロップダウン リストから次のいずれかを選択します。

オプション	説明
Select Boot Policy to use	このサービス プロファイルにデフォルトのブート ポリシーを割り当てます。 ステップ 14 に進みます。
[特定のブート ポリシーを作成（Create a Specific Boot Policy）]	このサービス プロファイル テンプレートだけがアクセスできるローカル ブート ポリシーを作成できます。 ステップ 8 に進みます。
Boot Policies ***Policy_Name***	サービス プロファイルに既存のブート ポリシーを割り当てます。このオプションを選択した場合、Cisco UCS Manager でポリシーの詳細が表示されます。 既存のポリシーを使用するのではなく、すべてのサービス プロファイルがアクセスできるポリシーを作成する場合は、[Create Boot Policy] をクリックし、ステップ 2 に進みます。それ以外の場合はステップ 14 に進みます。

ステップ 8 ブート ポリシーの作成を選択した場合は、[Create Boot Policy] ダイアログボックスにポリシーの一意の名前と説明を入力します。

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

ステップ 9 （任意） ブート順序の変更後にこのブート ポリシーを使用するすべてのサーバをリブートするには、**[Reboot on Boot Order Change]** チェック ボックスをオンにします。

Cisco UCS Manager GUI で、ブート ポリシーの [順序を変更したときにリブートする（Reboot on Boot Order Change] チェックボックスがオンになっていて、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスを削除または追加してもブート順序には直接影響せず、サーバは再起動しません。

ステップ 10 （任意） 必要に応じて、**[Enforce vNIC/vHBA/iSCSI Name]** チェック ボックスをオンにします。

- オンにした場合、Cisco UCS Manager は設定エラーと、**[Boot Order]** テーブルにリストされた 1 つ以上の vNIC、vHBA、iSCSI vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかのレポートとを表示します。
- オフにした場合は、Cisco UCS Manager がサービス プロファイルから（ブート オプションに応じて）vNIC または vHBA を使用します。

ステップ 11 ローカル ディスク、仮想 CD-ROM、または仮想フロッピーをブート順序に追加するには、次の手順を実行します。

a) 下矢印をクリックして [Local Devices] 領域を展開します。

b) 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- [ローカル ディスクの追加（Add Local Disk）] または
  - **[Add Local LUN]**
  - **[Add Local JBOD (ローカル JBOD の追加)]**
  - **[Add SD Card]**
  - **[Add Internal USB]**
  - **[Add External USB]**
  - **[Add Embedded Local LUN (内蔵ローカルLUNの追加)]**
  - **[Add Embedded Local Disk (内蔵ローカルディスクの追加)]**
- **[Add CD/DVD]** または
  - **[Add Local CD/DVD]**
  - **[Add Local Remote CD/DVD]**

    M5 ブレード サーバを使用した設定で、ISO を KVM コンソールにマッピングしている場合は、**ブート順序**には **[Remote CD/DVD]** のみを使用してください。

c) 別のブート デバイスを [Boot Order] テーブルに追加するか、[OK] をクリックして作業を終了します。

ステップ 12 LAN ブートをブート順序に追加するには、次の手順を実行します。

a) 下矢印をクリックして [vNICs] 領域を展開します。
b) **[Add LAN Boot]** リンクをクリックします。
c) **[Add LAN Boot]** ダイアログボックスで、LAN ブートに使用する vNIC の名前を [vNIC] フィールドに入力して、[OK] をクリックします。
d) 別のデバイスを [Boot Order] テーブルに追加するか、[OK] をクリックして作業を終了します。

ステップ 13 SAN ブートをブート順序に追加するには、次の手順を実行します。

a) 下矢印をクリックして [vHBAs] 領域を展開します。
b) [Add SAN Boot] リンクをクリックします。
c) [Add San Boot] ダイアログ ボックスで、vHBA とタイプを指定して、[OK] をクリックします。
d) この vHBA がブート可能な SAN イメージを参照する場合は [Add SAN Boot Target] リンクをクリックし、[Add SAN Boot Target] ダイアログボックス で、ブート ターゲット LUN、ブート ターゲット WWPN、およびタイプを指定して、[OK] をクリックします。
e) 別のブート デバイスを [Boot Order] テーブルに追加するか、[OK] をクリックして作業を終了します。

ステップ 14 [OK] をクリックします。

サービス プロファイル用の vNIC 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 **[サーバ]** > **[サービスプロファイル]**を展開します。

ステップ 3 vNIC 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。

ステップ 4 vNIC を作成するサービス プロファイルを展開します。

ステップ 5 [vNICs] ノードを右クリックし、[Create vNICs] を選択します。

ステップ 6 既存の vNIC テンプレートを使用するには、[vNIC の作成（Create vNIC）] ダイアログボックスで名前を入力し、[MAC アドレスの割り当て（MAC Address Assignment）] を選択して [vNIC テンプレートの使用（Use vNIC Template）] チェックボックスをオンにします。

この領域では MAC プールを作成することもできます。

ステップ 7 **ファブリック ID** を選択し、使用する **VLAN** を選択してから、**CDN 名** と **MTU** を選択し、**ピン グループ** を選択します。

この領域から VLAN および LAN 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]、[QoS Policy]、および [Network Control Policy] を選択します。

この領域では、イーサネット アダプタ ポリシー、QoS ポリシー、ネットワーク制御ポリシーも作成できます。

ステップ 10 [Connection Policy] 領域で、[Dynamic vNIC]、[usNIC] または [VMQ] ラジオ ボタンを選択して、対応するポリシーを選択します。

この領域では、ダイナミック vNIC、usNIC、または VMQ の接続ポリシーも作成できます。

ステップ 11 [OK] をクリックします。

サービス プロファイルからの vNIC の削除

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 vNIC を削除するサービス プロファイルが含まれる組織のノードを展開します。

ステップ 4 vNIC を削除するサービス プロファイルを展開します。

ステップ 5 **vNIC** ノードを展開します。

ステップ 6 削除する vNIC 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。

サービス プロファイル用の vHBA 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 **[サーバ]** > **[サービスプロファイル]**を展開します。

ステップ 3 vHBA 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。

ステップ 4 vHBA を作成するサービス プロファイルを展開します。

ステップ 5 [vHBAs] ノードを右クリックし、[Create vHBAs] を選択します。

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 [OK] をクリックします。

vHBA に対する WWPN の変更

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]**を展開します。

ステップ 3 WWPN を変更する サービス プロファイル を含む組織の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 WWPN を変更する 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、[Change World Wide Name] をクリックします。

ステップ 8 [Change World Wide Port Name] 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 9 [OK] をクリックします。

vHBA の永続的なバインディングのクリア

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 を変更する サービス プロファイル を含む組織の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 永続的なバインディングをクリアする 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、[Clear Persistent Binding] 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。

サービス プロファイルからの vHBA の削除

手順

ステップ 1 [ナビゲーション]ペインで、[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 を削除するサービス プロファイルが含まれる組織のノードを展開します。
ステップ 4 vHBA を削除するサービス プロファイルを展開します。
ステップ 5 [vHBAs] ノードを展開します。
ステップ 6 削除する vHBA 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。

サービス プロファイルへの vHBA イニシエータ グループの追加

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 vHBA イニシエータ グループを追加するサービス プロファイ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 3 vHBA イニシエータ グループを追加するサービス プロファイルを選択します。
ステップ 4 [Work] ペインで、**[Storage]** > **[vHBA Initiator Groups]** をクリックします。
ステップ 5 テーブル の右にあるアイコン バーの **[+]** 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、名前と説明を設定するには、次のフィールドに入力します。

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

名前	説明
[Description] フィールド	グループの説明。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 7 **[Select vHBA Initiators]** テーブル で、vHBA イニシエータ グループに含める各 vHBA の **[Select]** 列のチェック ボックスをオンにします。

ステップ 8 イニシエータ グループにストレージ接続ポリシーを追加するには、次のオプションの 1 つを選択します。

- [Storage Connection Policy] ドロップダウン リスト から既存のストレージ接続ポリシーを選択します。ステップ 10 に進みます。
- Cisco UCS ドメイン 内の他の vHBA のイニシエータ グループ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場合は、リンク をクリックします。詳細については、「Creating a Fibre Channel Storage Connection Policy」を参照してください。ストレージ接続ポリシーを作成した後、ステップ 10 に進みます。
- この vHBA のイニシエータ グループにのみ利用可能なストレージ接続ポリシーを作成するには、 オプション を選択します。ステップ 9 に進みます。

ステップ 9 この vHBA のイニシエータ グループにのみ利用可能なストレージ接続ポリシーを作成するには、**[Specific Storage Connection Policy]** 領域 で、次のフィールドを入力します。

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

名前	説明
[Zoning Type] フィールド	次のいずれかになります。 • **[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。
[FC Target Endpoints] テーブル	このポリシーに関連付けられたファイバチャネルターゲットエンドポイントこのテーブルには、次のカラムとボタンがあります。 • [WWPN] カラム：エンドポイントに関連付けられたワールド ワイド ポート名。 • [Path] カラム：エンドポイントへのパス。 • [VSAN] カラム：エンドポイントに関連付けられた VSAN。 • [Add] ボタン：新しい FC ターゲット エンドポイントを作成します。 • [Delete] ボタン：選択したエンドポイントを削除します。 • [Properties] ボタン：選択したエンドポイントのすべてのプロパティを表示します。

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。

サービス プロファイルの削除

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 **[Servers]** > **[Service Profiles]** > ***[Organization_Name]*** を展開します.

ステップ 3 削除するサービス プロファイルを右クリックし、[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。

ステップ 5 **[OK]** をクリックします。

サービス プロファイルのアソシエーション

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。

オプション	説明
	ステップ 7 に進みます。
[Custom Server]	サービス プロファイルに割り当てられるサーバが含まれるシャーシおよびスロットを指定します。サーバがスロット内に存在しない場合、またはそれ以外の理由で使用できない場合、サービス プロファイルは、サーバが使用できるようになったらサーバに関連付けられます。 ステップ 6 に進みます。

ステップ 6 [Custom Server] を選択した場合は、次の手順を実行します。

a) [Chassis Id] フィールドに、選択したサーバが配置されるシャーシの番号を入力します。

b) [Server Id] フィールドで、選択したサーバが配置されているスロットの番号を入力します。

ステップ 7 サーバに関連付け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。

サービス プロファイルとサーバーまたはサーバー プールの関連付け解除

サービスプロファイルの関連付けを解除すると、Cisco UCS Managerにより、サーバのオペレーティング システムのシャットダウンが試みられます。適度な時間が経過してもオペレーティング システムがシャットダウンされない場合は、Cisco UCS Managerにより、サーバが強制的にシャットダウンされます。

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 サーバまたはサーバ プールとの関連付けを解除するサービス 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 4 サーバとの関連付けを解除するサービス プロファイルを右クリックし、[Disassociate Service Profile] を選択します。

ステップ 5 [Disassociate Service Profile] ダイアログボックスで、[Yes] をクリックしてサービス プロファイルの関連付けを解除することを確認します。

ステップ 6 (Optional) サーバのステータスおよび有限状態マシン（FSM）をモニタして、アソシエーションの解除が完了したことを確認します。

サービス プロファイル テンプレート

初期テンプレートと既存のテンプレート

サービス プロファイル テンプレートを使用して、vNIC や vHBA の個数などの同じ基本パラメータ、および同じプールから取得された ID 情報を使ってすばやく複数のサービス プロファイルを作成できます。

Tip 既存のサービス プロファイルに類似した値を持つ 1 つのサービス プロファイルだけが必要な場合は、Cisco UCS Manager GUI でサービス プロファイルを複製できます。

たとえば、データベース ソフトウェアをホストするサーバーの設定に、類似した値を持つ数個のサービスプロファイルが必要である場合、手動、または既存のサービスプロファイルから、サービスプロファイルテンプレートを作成できます。その後、このテンプレートを使用して、サービス プロファイルを作成します。

Cisco UCS は、次のタイプのサービス プロファイル テンプレートをサポートしています。

初期テンプレート

初期テンプレートから作成されたサービスプロファイルはテンプレートのプロパティをすべて継承します。初期のサービス プロファイル テンプレートから作成されたサービス プロファイルはテンプレートにバインドされます。ただし、初期のテンプレートに対して行われた変更は、バインドされたサービスプロファイルに自動的に伝播されません。バインドされたサービス プロファイルに変更を伝播したい場合は、そのサービス プロファイルをアンバインドしてから、再び初期テンプレートにバインドします。

アップデート テンプレート

アップデート テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承し、そのテンプレートへの接続をそのまま保持します。アップデート テンプレートを変更すると、このテンプレートから作成されたサービスプロファイルが自動的にアップデートされます。

Note 初期テンプレートと標準のサービス プロファイルから作成されたサービス プロファイルは、**[リセット (Reset)]** がクリックされると、順次プール内で使用可能な最小の ID を取得します。

アップデート テンプレートから作成されたサービス プロファイルは、**[リセット (Reset)]** がクリックされると、順次プール内のより小さい ID が未使用の場合でも、同じ ID を保持します。

サービス プロファイル テンプレートの作成

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 **[サーバ]** > **[サービスプロファイルテンプレート]**を展開します。

ステップ 3 サービス プロファイル テンプレート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 Template] を選択します。

ステップ 5 [Identify Service Profile Template] パネルで、サービス プロファイルの [Name]、[Type]、[UUID Assignment] を指定し、[Next] をクリックします。

このサービス プロファイル テンプレートの説明（任意）を入力できます。

（注） サービス プロファイル テンプレートをすばやく作成するには、名前を指定した後で **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 テンプレートを作成します。

ステップ 6 （任意）[Networking] パネルで、[Dynamic vNIC Connection Policy] と [LAN Connectivity] 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 （任意）[Storage] パネルで、SAN 設定情報（[Local Storage Policy]、[SAN Connectivity]、[WWNN]、[vHBAs] など）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] パネルで、配置方法と PCI 順序を指定して [Next] 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 （任意）[Server Assignment] パネルで、ドロップダウン リストの [Pool Assignment] と、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。

（注） 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 テンプレートから 1 つ以上のサービス 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テンプレート]**を展開します。

ステップ 3 サービス プロファイルのベースとして使用するサービス プロファイル テンプレート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 プロファイルの作成元となるサービス プロファイル テンプレートを右クリックし、[Create Service Profiles From Template] を選択します。

ステップ 5 [Create Service Profiles From Template] ダイアログボックスで、必要な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。

ブレード サーバのテンプレート ベースのサービス プロファイルの作成

始める前に

Cisco UCS Manager には、適切な値の設定された正規のサービス プロファイル テンプレートが存在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、[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 テンプレート ベースのサービス プロファイルを作成するサーバを選択します。

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 [Actions] 領域で [Create Service Profile] をクリックします。

ステップ 6 [Create Service Profile for Server] ダイアログボックスで、次の手順を実行します。

a) ラジオ ボタンをクリックします。

b) [Name] フィールドに、サービス プロファイルの一意の名前を入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

c) ドロップダウンリストで、このサーバに関連付けるサービス プロファイルの作成元となるテンプレートを選択します。

（注） ドロップダウン リストには、選択したブレード サーバと互換性のあるサービス プロファイル テンプレートだけが表示されます。

d) [OK] をクリックします。

ラックマウント サーバのテンプレート ベースのサービス プロファイルの作成

始める前に

Cisco UCS Manager には、適切な値の設定された正規のサービス プロファイル テンプレートが存在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、[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 テンプレート ベースのサービス プロファイルを作成するサーバを選択します。

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 [Actions] 領域で [Create Service Profile] をクリックします。

ステップ 6 [Create Service Profile for Server] ダイアログボックスで、次の手順を実行します。

a) ラジオ ボタンをクリックします。

b) [Name] フィールドに、サービス プロファイルの一意の名前を入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

c) ドロップダウンリストで、このサーバに関連付けるサービス プロファイルの作成元となるテンプレートを選択します。

d) [OK] をクリックします。

サービス プロファイルからのサービス プロファイル テンプレートの作成

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 **[サーバ]** > **[サービスプロファイル]**を展開します。

ステップ 3 テンプレートのベースとして使用するサービス 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 4 テンプレートの作成元となるサービス プロファイルを右クリックし、[Create a Service Profile Template] を選択します。

ステップ 5 [Create Template From Service Profile] 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。

サービス プロファイルのアセット タグの設定

手順

ステップ 1 **[Servers]** > **[Service Profiles]** を選択します。

ステップ 2 アセット タグを作成する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わっていない場合は、[root] ノードを展開します。

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

ステップ 4 [Asset Tag] フィールドに、サーバを識別する名前を入力します。

この名前には 2 ～ 32 文字の英数字を使用できます。次を除く任意の特殊文字またはスペースを使用できます。`（アクセント記号）、\（バックスラッシュ）、^（キャラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 変更を反映するため、サーバを手動でリブートします。

サービス プロファイル テンプレート タスク

サービス プロファイル テンプレートへのサービス プロファイルのバインディング

サービスプロファイルをサービスプロファイルテンプレートにバインドすることができます。サービス プロファイル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 テンプレートに定義された値を使って、サービス プロファイルが設定されます。既存のサービス プロファイル設定がサービス プロファイル テンプレートに一致しない場合、Cisco UCS Manager により、サービス プロファイルが再設定されます。バインドされたサービスプロファイルの設定は、関連付けられたテンプレートを使用してのみ変更できます。

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 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 バインドする サービス プロファイル をクリックします。

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、[Bind to a Template] をクリックします。

ステップ 7 [Bind to a Service Profile Template] ダイアログボックスで、次の手順を実行します。

a) [Service Profile Template] ドロップダウン リストから、サービス プロファイル に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。

サービス プロファイル テンプレートからのサービス プロファイルのバインド解除

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 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 バインドを解除する サービス プロファイル をクリックします。

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 [Unbind from the Template] 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。

サービス プロファイル テンプレートの UUID の変更

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テンプレート]**を展開します。

ステップ 3 UUID を変更するサービス プロファイル テンプレート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 UUID 割り当てを変更するサービス プロファイル テンプレートを選択します。

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、[Change UUID] をクリックします。

ステップ 7 **[UUID 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。

オプション	説明
Select (pool default used by default)	デフォルトの UUID 接尾辞プールから UUID を割り当てます。
	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUIDはサービスプロファイルがサーバと関連付けられるまで割り当てられません。この時点で、UUIDは製造元によってサーバに割り当てられた UUID 値に設定されます。サービスプロファイルを後で別のサーバに移動すると、UUIDは新しいサーバに一致するように変更されます。
Pools ***Pool_Name***	ドロップダウン リストの下部のリストから選択する UUID 接尾辞プールから UUID を割り当てます。 各プール名の後には、プール内で利用可能な UUID の数および UUID 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 8 **[OK]** をクリックします。

サービス プロファイルに割り当てられた UUID の、サービス プロファイル テンプレートのプールからのリセット

更新中のサービス プロファイル テンプレートに割り当てられている UUID サフィックス プールを変更しても、そのテンプレートで作成されたサービスプロファイルに割り当てられている UUID は Cisco UCS Manager によって変更されません。Cisco UCS Manager を使用して、新しくサービスプロファイルに割り当てられたプールからUUIDを割り当て、関連付けられたサーバに反映させるには、UUIDをリセットする必要があります。サービスプロファイルおよび関連付けられたサーバに割り当てられている UUID は、次の状況でのみリセットできます。

- サービス プロファイルが更新中のサービス プロファイル テンプレートから作成されていて、UUID 接尾辞プールから割り当てられた UUID が含まれている。
- UUID接尾辞プール名がサービス プロファイルで指定されている。たとえば、プール名が空でない場合です。

- UUID の値が 0 でない（サーバ ハードウェアに由来しない）。

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 UUIDをリセットするサービスプロファイルがインクルードされた組織に対応する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 関連付けられたサーバのUUIDを別のUUID接尾辞プールにリセットする必要があるサービスプロファイルを選択します。

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

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

この処理が表示されない場合、そのサービスプロファイルのUUID設定はUUIDのリセット要件を満たしていません。

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。

vNIC に割り当てられた MAC アドレスの、サービス プロファイル テンプレートのプールからのリセット

更新中のサービス プロファイル テンプレートに割り当てられている MAC プールを変更しても、そのテンプレートで作成されたサービス プロファイルに割り当てられているMACアドレスはCisco UCS Managerによって変更されません。Cisco UCS Managerを使用して、新しくサービス プロファイルに割り当てられたプールから MAC アドレスを割り当て、関連付けられたサーバに反映させるには、MAC アドレスをリセットする必要があります。サービス プロファイルおよび関連付けられたサーバに割り当てられている MAC アドレスは、次の状況でのみリセットできます。

- サービス プロファイルが更新中のサービス プロファイル テンプレートから作成されていて、MAC プールから MAC アドレスが割り当てられている。
- MAC プール名がサービス プロファイルで指定されている。たとえば、プール名が空でない場合です。
- MAC アドレスの値が 0 でない（サーバ ハードウェアに由来しない）。

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 MAC アドレスをリセットするサービス プロファイル がインクルードされた組織に対応する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]*** > **[vNICs]** を展開します。

ステップ 5 リセットする MAC アドレスに対応する vNIC 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 [Reset MAC Address] 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 [OK] をクリックします。

vHBA に割り当てられた WWPN の、サービス プロファイル テンプレートのプールからのリセット

更新中のサービス プロファイル テンプレートに割り当てられている WWPN プールを変更しても、そのテンプレートで作成されたサービス プロファイルに割り当てられている WWPN は Cisco UCS Manager によって変更されません。Cisco UCS Manager を使用して、新しくサービス プロファイルに割り当てられたプールから WWPN を割り当て、関連付けられたサーバに反映させるには、WWPN をリセットする必要があります。サービス プロファイルおよび関連付けられたサーバに割り当てられている WWPN は、次の状況でのみリセットできます。

- サービス プロファイルが更新中のサービス プロファイル テンプレートから作成されていて、WWPN プールから WWPN が割り当てられている。
- WWPN プール名がサービス プロファイルで指定されている。たとえば、プール名が空でない場合です。
- WWPN の値が 0 でない（サーバ ハードウェアに由来しない）。

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 WWPN をリセットするサービス プロファイルがインクルードされた組織に対応する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 リセットする WWPN に対応する 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 [Reset WWPN] 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 [OK] をクリックします。

サービス プロファイル テンプレートからのインバンド設定の削除

この手順では、サービス プロファイル テンプレートからインバンド管理 IP アドレスの設定を削除します。このアクションがグレー表示されている場合、インバンド設定は設定されていません。

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 **[Servers] > [Service Profile Template] > [*Service_Profile_Template_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 [アクション（Actions）] 領域で、[インバンド構成の削除（Delete Inband Configuration）] をクリックします。
ステップ 5 [削除（Delete）] 確認ダイアログボックスで [はい（Yes）] をクリックします。

サービス プロファイル テンプレートのインバンド管理 IP アドレスの設定が削除されます。

サービス プロファイルのアソシエーション

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) [Server Id] フィールドで、選択したサーバが配置されているスロットの番号を入力します。

ステップ 7 サーバに関連付け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。

サービス プロファイル テンプレートとサーバ プールの関連付け

作成時にサービス プロファイル テンプレートをサーバ プールに関連付けなかった場合、またはこのテンプレートから作成されたサービス プロファイルに関連付けるサーバ プールを変更する場合には、次の手順を実行します。

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テンプレート]**を展開します。

ステップ 3 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 プールに関連付けるサービス プロファイル テンプレートを右クリックして、[Associate with Server Pool] を選択します。

[Associate with Server Pool] ダイアログボックスが開きます。

ステップ 5 [Pool Assignment] ドロップダウン リストの [Server Pool] セクションから、サーバ プールを選択します。

[Assign Later] を選択すると、サービス プロファイル テンプレートはサーバ プールに関連付けられません。

ステップ 6 （任意） [Select Qualification] ドロップダウン リストから、このテンプレートで作成したサービス プロファイルに関連付けられているサーバに適用するサーバ プール ポリシー資格情報を選択します。

ステップ 7 **[OK]** をクリックします。

サービス プロファイルとサーバーまたはサーバー プールの関連付け解除

サービスプロファイルの関連付けを解除すると、Cisco UCS Managerにより、サーバのオペレーティングシステムのシャットダウンが試みられます。適度な時間が経過してもオペレーティング システムがシャットダウンされない場合は、Cisco UCS Managerにより、サーバが強制的にシャットダウンされます。

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 サーバまたはサーバ プールとの関連付けを解除するサービス 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 4 サーバとの関連付けを解除するサービス プロファイルを右クリックし、[Disassociate Service Profile] を選択します。

ステップ 5 [Disassociate Service Profile] ダイアログボックスで、[Yes] をクリックしてサービス プロファイルの関連付けを解除することを確認します。

ステップ 6 (Optional) サーバのステータスおよび有限状態マシン（FSM）をモニタして、アソシエーションの解除が完了したことを確認します。

サーバ プールからのサービス プロファイル テンプレートの関連付け解除

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テンプレート]**を展開します。

ステップ 3 サーバ プールとの関連付けを解除するサービス 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 4 サーバ プールとの関連付けを解除するサービス プロファイル テンプレートを右クリックし、[Disassociate Template] 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 12

サーバー関連ポリシー

- BIOS 設定, on page 222
- トラステッド プラットフォーム モジュール, on page 349
- SPDM セキュリティ （352 ページ）
- SPDM セキュリティ ポリシーの作成 （353 ページ）
- セキュリティ ポリシーとサーバーの関連付け （354 ページ）
- 障害アラート設定の表示 （355 ページ）
- 一貫したデバイスの命名 （355 ページ）
- CIMC セキュリティ ポリシー （359 ページ）
- グラフィックス カード ポリシー （363 ページ）
- ローカル ディスク ポリシー, on page 364
- 永続メモリ モジュール （378 ページ）
- スクラブ ポリシー, on page 378
- DIMM エラー管理, on page 383
- Serial over LAN ポリシー設定, on page 385
- サーバ自動構成ポリシー, on page 387
- サーバ ディスカバリ ポリシー設定, on page 390
- サーバ継承ポリシー設定, on page 393
- サーバ プール ポリシー設定, on page 395
- サーバ プール ポリシー資格情報設定, on page 397
- vNIC/vHBA 配置ポリシー設定, on page 403
- CIMC マウント vMedia （419 ページ）

BIOS 設定

サーバー BIOS 設定

サーバー BIOS 設定

Cisco UCS では、Cisco UCS ドメイン 内のサーバー上の BIOS 設定をグローバルに変更する方法が 2 つ用意されています。サーバーまたはサーバーの集合のニーズに合う特定の BIOS 設定グループを含む BIOS ポリシーを 1 つ以上作成するか、特定のサーバー プラットフォームに対するデフォルトの BIOS 設定を使用できます。

BIOS ポリシーおよびサーバー プラットフォームのデフォルトの BIOS 設定のどちらででも、Cisco UCS Manager によって管理されるサーバーの BIOS 設定を微調整できます。

データセンターのニーズに応じて、一部のサービス プロファイルについては BIOS ポリシーを設定し、同じ Cisco UCS ドメイン 内の他のサービス プロファイルについては BIOS のデフォルトを使用したり、そのいずれかのみを使用したりできます。また、Cisco UCS Manager を使用して、サーバーの実際の BIOS 設定を表示し、それらが現在のニーズを満たしているかどうかを確認できます。

（注） Cisco UCS Manager は、BIOS ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。これらの変更はバッファ内にとどまり、サーバーがリブートされるまでは有効になりません。

設定するサーバーで BIOS 設定のサポートを確認することをお勧めします。RAS メモリのミラーリング モードなどの一部の設定は、すべての Cisco UCS サーバーでサポートされているわけではありません。

メイン BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるメイン サーバの BIOS 設定を示しています。

名前	説明
Properties	

名前	説明
[Reboot on BIOS Settings Change]	1 つ以上の BIOS 設定を変更した後、サーバーをリブートするタイミング。 この設定を有効にした場合、サーバーのサービス プロファイルのメンテナンス ポリシーに従ってサーバーがリブートされます。たとえば、メンテナンス ポリシーでユーザーの確認応答が必要な場合、サーバーはリブートされず、ユーザーが保留中のアクティビティを確認するまで BIOS の変更は適用されません。 この設定を有効にしない場合、BIOS の変更は、別のサーバー設定変更の結果であれ手動リブートであれ、次回のサーバーのリブート時まで適用されません。
BIOS 設定	
[Quiet Boot]	BIOS が Power On Self-Test（POST）中に表示する内容。次のいずれかになります。 • [disabled][Disabled]：BIOSはブート中にすべてのメッセージとオプションROM情報を表示します。 • [enabled][Enabled]：BIOSはロゴ画面を表示しますが、ブート中にメッセージやオプション ROM 情報を表示しません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[POST error pause]	POST 中にサーバーで重大なエラーが発生した場合の処理。次のいずれかになります。 • [disabled][Disabled]：BIOSはサーバーのブートを続行します。 • [enabled][Enabled]：POST中に重大なエラーが発生した場合、BIOS はサーバーのブートを一時停止し、Error Manager を開きます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Resume on AC power loss]	予期しない電力損失後に電力が復帰したときにサーバーがどのように動作するかを決定します。次のいずれかになります。 • [stay-off][StayOff]：手動で電源をオンにするまでサーバーの電源がオフのままになります。 • [last-state][LastState]：サーバーの電源がオンになり、システムが最後の状態を復元しようとします。 • [reset][Reset]：サーバーの電源がオンになり、自動的にリセットされます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Front panel lockout]	前面パネルの電源ボタンとリセット ボタンがサーバーによって無視されるかどうかを決定します。次のいずれかになります。 • [disabled][Disabled]：前面パネルの電源ボタンとリセットボタンはアクティブであり、サーバーに影響を与えるために使用できます。 • [enabled][Enabled]：電源ボタンとリセットボタンはロック アウトされます。サーバーをリセットしたり、電源をオンにしたりできるのは、CIMC GUI からのみです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[CDN Control]	一貫したデバイスの命名によって、一貫した方法でイーサネット インターフェイスに名前を付けることができます。これによりイーサネット インターフェイスの名前は、より統一され、識別しやすくなり、アダプタや他の設定に変更が加えられても永続的に保持されます。 一貫したデバイスの命名をイネーブルにするかどうか。次のいずれかになります。 • [disabled][Disabled]：一貫したデバイスの命名はBIOSポリシーでディセーブルになっています。 • [enabled][Enabled]：一貫したデバイスの命名はBIOSポリシーでイネーブルになっています。これにより、イーサネット インターフェイスに一貫した方法で命名できます。これがデフォルトのオプションです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
PCIe Slots CDN コントロール	PCIe スロットの Consistent Device Naming（CDN）制御により、PCIe スロットに一貫した方法で名前を付けることができます。これにより PCIe スロットの名前は、より統一され、識別しやすくなり、構成に変更が加えられても永続的に保持されます。次のいずれかになります。 • **ディセーブル化** — Consistent Device Naming（CDN）はディセーブル化されています。これがデフォルトのオプションです。 • **イネーブル化** — Consistent Device Naming（CDN）はイネーブル化されています。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

プロセッサのBIOS設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるプロセッサの BIOS 設定を示しています。

名前	説明
[Intel Turbo Boost Tech]	プロセッサでインテルターボブーストテクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [disabled][Disabled]：プロセッサの周波数は自動的には上がりません。 • [enabled][Enabled]：必要に応じてプロセッサでTurbo Boost Technology が利用されます。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Enhanced Intel SpeedStep Tech]	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [disabled][Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [enabled][Enabled]：プロセッサでEnhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Intel HyperThreading Tech]	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [disabled][Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [enabled][Enabled]：プロセッサでの複数スレッドの並列実行を許可します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Intel Speed Select（Intel の速度選択）]	Intel Speed Select テクノロジーを使用して CPU のパフォーマンスを向上させ、論理プロセッサ コア、頻度、および TDP スレッド設定の数に基づいて、3 つの動作プロファイルのいずれかで実行する CPU を調整し、基本プラットフォームのデフォルト設定でパフォーマンスを向上させます。これらのプロファイルは、高、中、および低のコア設定に対応しており、次のいずれかになります。 • **Base**：プロセッサは Base を使用します。 • **Config 1**：プロセッサは Config 1 を使用します。 • **Config 2**：プロセッサは Config 2 を使用します。 • **Config 3**：プロセッサは Config 3 を使用します。 • **Config 4**：プロセッサは Config 4 を使用します。： （注） 値 **Config 1** および **Config 2** は、Cicso UCS M6 サーバーではサポートされていません。 （注） Cisco UCS M6 および Cisco UCS M7 サーバーの場合、 **Config 3** および **Config 4** （第 4 世代 Intel Xeon Scalable プロセッサおよび第 5 世代 Intel Xeon Scalable プロセッサ）の値は、 **Config 1** および **Config 2** の値 （第 3 世代 Interl Xeon スケーラブル プロセッサ）と同等です。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 を参照してください。

名前	説明
[コア多重処理（Core Multi Processing）]	パッケージ内のCPUごとの論理プロセッサ コアの状態を設定します。この設定を無効にすると、Intelハイパースレッディング テクノロジーも無効になります。次のいずれかになります。 • [all]：すべての論理プロセッサ コアの多重処理を有効にします。 • [1～***n***]:Sサーバで実行可能なCPUあたりの論理プロセッサコアの数を指定します。マルチプロセッシングを無効にして、サーバーで動作するCPUごとの論理プロセッサ コアを1つのみにするには、[1]を選択します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Execute Disable Bit]	サーバーのメモリ領域を分類し、アプリケーション コードを実行可能な場所を指定します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効化します。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [disabled][Disabled]：プロセッサがメモリ領域を分類しません。 • [enabled][Enabled]：プロセッサがメモリ領域を分類します。 • [Platform Default][platform-default]：BIOSは、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Intel Virtualization Technology]	プロセッサで Intel Virtualization Technology を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [disabled][Disabled]：プロセッサでの仮想化を禁止します。 • [enabled][Enabled]：プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 （注） このオプションを変更した場合は、設定を有効にするためにサーバーの電源を再投入する必要があります。
[Hardware Prefetcher]	プロセッサで、インテルハードウェアプリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [disabled][Disabled]：ハードウェア プリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェアプリフェッチャを使用します。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 （注） この値を指定するには、**[CPU Performance]** を [Custom] に設定する必要があります。[Custom] 以外の値の場合は、このオプションよりも、選択されたCPUパフォーマンスプロファイルの設定が優先されます。

名前	説明
[Adjacent Cache Line Prefetcher]	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサで必要な行のみを取得します。 • [enabled][Enabled]：プロセッサで必要な行およびペアの行の両方を取得します。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 （注） この値を指定するには、[CPU Performance] を [Custom] に設定する必要があります。[Custom] 以外の値の場合は、このオプションよりも、選択されたCPUパフォーマンスプロファイルの設定が優先されます。
[DCU Streamer Prefetch]	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [disabled][Disabled]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [enabled][Enabled]：DCUPrefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[DCU IP Prefetcher]	プロセッサで DCU IP プリフェッチ メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュデータをプリロードしません。 • [enabled][Enabled]：DCUIP Prefetcher で最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[KTU プリフェッチ（KTI Prefetch）]	KTI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュデータをプリロードしません。 • [enabled][Enabled]：KTIPrefetcher で最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[LLC プリフェッチ（LLC Prefetch）]	プロセッサがLLCプリフェッチメカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサでキャッシュデータをプリロードしません。 • [enabled][Enabled]：LLCPrefetcher で最も関連性が高いと判断されたデータを含むL1 キャッシュをプリロードします。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[XPT プリフェッチ（XPT Prefetch）	XPT プリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPUは XPT Prefetch オプションを使用しません。 • [enabled][Enabled]：CPUは XPT Prefetcher オプションを有効にします。 • **自動化**：CPU 自動化では XPT Prefetcher オプションを有効にします。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Direct Cache Access]	プロセッサで、データをI/Oデバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュミスを減らすのに役立ちます。次のいずれかになります。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：データはI/O デバイスから直接プロセッサ キャッシュには入れられません。 • [enabled][Enabled]：データはI/O デバイスから直接プロセッサ キャッシュに入れられます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Processor C State]	アイドル期間中にシステムが省電力モードに入ることができるかどうか。次のいずれかになります。 • [disabled][Disabled]：システムは、アイドル時にも高パフォーマンス状態を維持します。 • [enabled][Enabled]：システムはDIMM や CPU などのシステム コンポーネントへの電力を低減できます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Processor C1E]	C1 に入ってプロセッサが最低周波数に遷移できるようにします。この設定は、サーバをリブートするまで有効になりません。次のいずれかになります。 • [disabled][Disabled]：CPUは C1 状態でも引き続き最大周波数で動作します。 • [enabled][Enabled]：CPUは最小周波数に移行します。 このオプションでは、C1 状態での最大電力量が削減されます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Processor C3 Report]	プロセッサからオペレーティング システムにC3 レポートを送信するかどうか。次のいずれかになります。 • [enabled][Enabled]：プロセッサからC3 レポートをOS に送信します。 • [disabled][Disabled]：プロセッサからC3 レポートを送信しません。 • [acpi-c2][ACPI C2]：プロセッサからAdvanced Configuration and Power Interface（ACPI）C2 フォーマットを使用して C3 レポートを送信します。 • [acpi-c3][ACPI C3]：プロセッサからACPI C3 フォーマットを使用して C3 レポートを送信します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 Cisco UCS B440 Server の場合、[BIOS Setup] メニューでこれらのオプションに対して [enabled] と [disabled] が使用されます。[acpi-c2] または [acpi-c2] を指定すると、このサーバーではそのオプションの BIOS 値に [enabled] が設定されます。
[Processor C6 Report]	プロセッサからオペレーティング システムにC6 レポートを送信するかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサからC6 レポートを送信しません。 • [enabled][Enabled]：プロセッサからC6 レポートを送信します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[プロセッサ C7 レポート（Processor C7 Report）]	プロセッサからオペレーティングシステムにC7 レポートを送信するかどうか。次のいずれかになります。 • [c7][C7]：プロセッサからC7 フォーマットを使用してレポートを送信します。 • [c7s][C7s]：プロセッサからC7s フォーマットを使用してレポートを送信します。 • [disabled][Disabled]：プロセッサからC7 レポートを送信しません。 • [enabled][Enabled]：プロセッサからC7 レポートを送信します。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[プロセッサCMCI（Processor CMCI）]	CMCI の生成を有効にします。次のいずれかになります。 • [disabled][Disabled]：プロセッサはCMCI を無効にします。 • [enabled][Enabled]：プロセッサはCMCI を有効にします。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[CPU Performance]	サーバーのCPUパフォーマンス プロファイルを設定します。次のいずれかになります。 • [カスタム（Custom）]：パフォーマンス プロファイルのすべてのオプションをサーバーのBIOSセットアップから設定できます。また、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。 • **[企業（Enterprise）]**：M4 以降のサーバーに対して、すべてのプリフェッチャとデータの再利用が有効になります。 • [high-throughput][High Throughput]：データの再利用とDCU IPプリフェッチャはイネーブルになり、他のすべてのプリフェッチャはディセーブルになります。 • [hpc][HPC]：プリフェッチャはすべてイネーブルになり、データの再利用はディセーブルになります。この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Max Variable MTRR Setting]	平均修復時間（MTRR）変数の数を選択できます。次のいずれかになります。 • [auto-max][AutoMax]：BIOSはプロセッサのデフォルト値を使用します。 • **8**：BIOS は MTRR 変数に指定された数を使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Local X2 APIC]	Application Policy Infrastructure Controller（APIC）アーキテクチャ タイプを設定できます。次のいずれかになります。 • [disabled][Disabled]：プロセッサがローカルX2 APICを無効にします。 • [enabled][Enabled]：プロセッサがローカルX2 APICを有効にします。 • [xapic][XAPIC]：標準のxAPICアーキテクチャを使用します。 • [x2apic][X2APIC]：拡張x2APIC アーキテクチャを使用してプロセッサの32ビットアドレス指定能力をサポートします。 • [auto][Auto]：検出されたxAPIC アーキテクチャを自動的に使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Power Technology]	次のオプションのCPU電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [disabled][Disabled]：サーバーでCPU電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • **[Energy Efficient]**：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。 • [performance][Performance]：サーバーは前述のBIOSパラメータのパフォーマンスを自動的に最適化します。 • [custom][Custom]：サーバーは前述のBIOSパラメータの個々の設定を使用します。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Energy Performance]	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • [performance][Performance]：サーバーでは、すべてのサーバーコンポーネントに全電力を常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [balanced-performance][BalancedPerformance]：サーバーは、すべてのサーバー コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [balanced-energy][BalancedEnergy]：サーバーは、すべてのサーバー コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [energy-efficient][EnergyEfficient]：サーバーは、すべてのサーバー コンポーネントに提供する電力を少なくし、電力消費を抑えます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[Frequency Floor Override]	アイドル時に、CPU がターボを除く最大周波数よりも低い周波数にできるようにするかどうか。次のいずれかになります。 • [disabled][Disabled]：アイドル中にCPU をターボを除く最大周波数よりも低くできます。このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [enabled][Enabled]：アイドル状態のときにCPU を最大非ターボ周波数よりも低くできません。このオプションではシステム パフォーマンスが向上しますが、消費電力が増加することがあります。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[P STATE Coordination]	BIOS がオペレーティング システムに P-state サポートモデルを伝達する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様では、次の 3 つのモデルが定義されています。 • [hw-all][HWALL]：プロセッサ ハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [sw-all][SWALL]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [sw-any][SWANY]：OS Power Manager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 （注） [Power Technology][CPUPowerManagement] を [Custom] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

名前	説明
[DRAM Clock Throttling]	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [auto][Auto]：CPUがDRAMクロック スロットリング設定を決定します。 • [balanced][Balanced]：DRAMクロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [performance][Performance]：DRAMクロック スロットリングはディセーブルです。追加の電力をかけてメモリ帯域幅を増やします。 • [Energy Efficient]：DRAMのクロックスロットリングを上げてエネルギー効率を向上させます。 • [Platform Default][platform-default]：BIOSは、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[External SSC enable] ドロップダウンリスト	このオプションでは、外部クロック ジェネレータのクロック拡散スペクトルを有効または無効にすることができます。 Cisco Bシリーズサーバおよび Sシリーズ M5 および M6サーバの場合、このオプションはデフォルトで無効になっています。Cisco Cシリーズラック サーバでは、デフォルトで有効になっています。 • [無効 (Disabled)][無効 (Disabled)]—クロック拡散スペクトルのサポートは使用できません。 • enabled Enabled：クロックスペクトラム拡散サポートは常に使用可能です。 • [Platform Default][platform-default]：BIOSは、サーバタイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Channel Interleaving]	CPUがメモリブロックを分割して、インターリーブされたチャネル間にデータの連続部分を分散し、同時読み取り動作を有効にするかどうか。次のいずれかになります。 • [auto][Auto]：実行するインターリーブはCPUによって決定されます。 • **[1 Way]**： • [2-way][2Way]： • [3-way][3Way]： • [4-way][4-way]：最大量のチャネルインターリーブが使用されます。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Rank Interleaving]ドロップダウン リスト	1つのランクを更新中に別のランクにアクセスできるよう、CPU がメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [auto][Auto]：実行するインターリーブはCPUによって決定されます。 • **[1 Way]**： • [2-way][2Way]： • [4-way][4-way] • [8-way][8Way]：最大量のランク インターリーブが使用されます。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[サブ NUMA クラスタリング（Sub NUMA Clustering）]	CPU がサブ NUMA クラスタリングをサポートするかどうか。そのクラスタリングでは、タグ ディレクトリとメモリ チャネルは常に同じ領域にあります。次のいずれかになります。 • **[自動（Auto）]** — BIOS かサブ NUMA のクラスタリングされるかが決まります。 • [disabled][Disabled]：サブNUMA クラスタリングは発生しません。これがデフォルトのオプションです。 • [enabled][Enabled]：サブNUMA クラスタリングが発生します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[IMC インターリーブ（IMC Interleaving）]	この BIOS オプションは、Integrated Memory Controller（IMC）間のインターリーブを制御します。 • [1-way Interleave]：インターリーブはありません。 • [2-way Interleave]：2 つの IMC 間でアドレスがインターリーブされます。 • [Auto]：CPU が IMC のインターリーブ モードを決定します。 • [Platform Default]：BIOS は、サーバー タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Memory Interleaving]	メモリの更新中に別のメモリにアクセスできるように、CPU が物理メモリをインターリーブするかどうか設定します。このオプションは、ファブリック レベルでメモリのインターリーブを制御します。チャネル、ダイ、ソケットの要件はメモリによって異なるため、選択したオプションがメモリでサポートされない場合これらは無視されます。次のいずれかになります。 • **[なし（None）]** • **[Channel（チャネル）]** • **[死亡する（Die）]** • **[ソケット（Socket）]** • **Auto**： これはデフォルトのオプションです。 • **[プラットフォームのデフォルト（Platform Default）]**：BIOS は、サーバ タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[Demand Scrub]	CPU または I/O から読み取り要求があった時に発生したシングル ビット メモリ エラーを、システムで修正するかどうか。次のいずれかになります。 • [disabled][Disabled]：1ビット メモリ エラーは修正されません。 • [enabled][Enabled]：1ビット メモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求への応答として設定されます。 • [Platform Default][platform-default]：BIOS は、サーバ タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Patrol Scrub]	システムがサーバー上のメモリの未使用部分でも単一ビットメモリエラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [disabled][Disabled]：CPUがメモリアドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [enabled][Enabled]：システムは定期的にメモリを読み書きしてECC エラーを探します。エラーが見つかると、システムは修復を試みます。このオプションにより、単一ビットエラーは複数ビットエラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[DCPMM Firmware Downgrade（DCPMM ファームウェアのダウングレード）]	次のいずれかになります。 • **[無効]**：サポートは無効になります。 • **[有効]**：サポートは有効になります。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[設定可能な TDP コントロール（Configurable TDP Control）]	Thermal Design Power (TDP) のカスタマイズされた値を設定できます。次のいずれかになります。 • **自動**：プロセッサの定格 TDP 値を使用します。 • **手動**：TDP 値をカスタマイズできます。

名前	説明
[Altitude]	物理サーバーがインストールされている地点のおよその海抜（m 単位）。次のいずれかになります。 • [auto][Auto]：物理的な高度をCPU が決定します。 • [300-m][300M]：サーバーは、海抜約 300 m です。 • [900-m][900M]：サーバーは、海抜約 900 m です。 • [1500-m][1500M]：サーバーは、海抜約 1500 m です。 • [3000-m][3000M]：サーバーは、海抜約 3000 m です。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[パッケージの C ステート（Package C State）]	アイドル時にサーバー コンポーネントが使用できる電力量。次のいずれかになります。 （注） C220 M4、C240 M4、C460 M4、および S3260 M4 サーバの場合は、**パッケージ C の状態制限**を**制限なし**、または**プラットフォームのデフォルト**に設定することを推奨します。 **パッケージ C の状態制限**制限なしに変更する場合は、**パワー テクノロジー**が**カスタム**に設定されていることを確認します。
[CPU ハードウェア電源管理（CPU Hardware Power Management）]	プロセッサの Hardware Power Management（HWPM）をイネーブルにします。次のいずれかになります。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 • [disabled][Disabled]：HWPMがディセーブルになります。 • [hwpm-native-mode][HWPM Native Mode]：HWPM ネイティブ モードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB Mode]：HWPMアウトオブボックス モードがイネーブルになります。 • [Native Mode with no Legacy]（GUI のみ）

名前	説明
[エネルギーパフォーマンスの調整（Energy Performance Tuning）]	BIOS またはOS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。 • **[BIOS]**： • **[OS]**： • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[ワークロード設定（Workload Configuration）]	この機能を使用すると、ワークロードを最適化できます。オプションは [Balanced] と [I/O Sensitive] です。 • **[バランス（Balanced）]** • **[IO感度（IO Sensitive）]**— これはデフォルトのオプションです。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 [Balanced] を使用することを推奨します。
[コア パフォーマンス ブースト（Core Performance Boost）]	AMDプロセッサがアイドル状態（ほとんど使用されていない状態）のときにコアの周波数を上げるかどうかを指定します。次のいずれかになります。 • **[Auto]**：パフォーマンスをブーストする方法をCPUで自動的に決定します。 • **[Disabled]**：CPUにより自動的にブースト パフォーマンスが決定されます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[非コア周波数スケーリング（Uncore Frequency Scaling）]	プロセッサの非コア部分の周波数のスケーリングを設定できます。次のいずれかになります。 • **[Enabled]**：プロセッサの非コア部分の周波数を、負荷に応じて上下します。(デフォルト) • **[Disabled]**：プロセッサの非コア部分の周波数を固定します。 • [Platform Default][platform-default]：BIOS は、サーバタイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。 [非コア周波数スケーリング（Uncore Frequency Scaling）]の固定の上限値と下限値については、『Intel® Dear Customer Letter（DCL）』を参照してください。
[TDP の設定（Config TDP）]	プロセッサの温度設計電力 (TDP) 値の調整を可能にします。プロセッサの動作とパフォーマンス レベルを変更することにより、プロセッサの消費電力と TDP を同時に調整できます。したがって、プロセッサは、使用可能な冷却容量と望ましい消費電力に応じて、パフォーマンス レベルが高いまたは低い方で動作します。 次のいずれかになります。 • **[Normal]**：CPUは通常のパフォーマンスレベルで動作します。(デフォルト) • **[Level 1]** • **[Level 2]** （注） TDP レベルの値については、『Intel Dear Customer Letter（DCL）』を参照してください。

名前	説明
[UPI リンク速度（UPIH Link Speed）]	複数のソケット間での Intel Ultra Path Interconnect (UPI) リンク速度の設定を可能にします。次のいずれかになります。 • **[Auto]**：最適なリンク速度を自動的に設定します。（デフォルト） • **9.6GT/s (ギガ転送/秒)**：最適なリンク速度を 9.6GT/秒に設定します。 • **[10.4GT/s]**：最適なリンク速度を 10.4GT/秒に設定します。 • **[11.2GT/s]**：最適なリンク速度 11.2GT/秒に設定します。 • リンクごとの設定を使用 （注） **リンクごとの設定の使用**は、UCS M6 サーバーではサポートされていません。
[グローバル C ステート制御（Global C-state Control）]	AMD プロセッサが IO ベースの C ステート ジェネレーションおよび DF C ステートを制御するかどうかです。次のいずれかになります。 • **[Auto]**：CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • **[Disabled]**：グローバル C ステートの制御が無効になります。 • **[Enabled]**：グローバル C ステートの制御が有効になります。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[L1 ストリーム HW プリフェッチャ（L1 Stream HW Prefetcher）]	プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、L1 キャッシュに入れることを許可するかどうか。次のいずれかになります。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサキャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェア プリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェアプリフェッチャを使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[L2 ストリーム HW プリフェッチャ（L2 Stream HW Prefetcher）]	プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。 • [auto][Auto]：CPUは、I/Oデバイスからプロセッサキャッシュにデータを配置する方法を決定します。 • [disabled][Disabled]：ハードウェア プリフェッチャは使用しません。 • [enabled][Enabled]：プロセッサで、キャッシュの問題が検出されたときにハードウェアプリフェッチャを使用します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[AMD メモリ インターリービング サイズ（AMD Memory Interleaving Size）]	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10、11）も指定します。次のいずれかになります。 • 1 KB • 2 KB • 256 バイト • 512 バイト • **自動**: CPU、メモリ ブロックのサイズを決定します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[チップセレクト インターリービング（Chipselect Interleaving）]	ノード 0 に選択する DRAM チップ経由でメモリ ブロックがインターリーブされるかどうか。次のいずれかになります。 • **[Auto]**：CPU でチップ セレクトのインタリーブの方法を自動的に決定します。 • **[Disabled]**：チップの選択は、メモリ コントローラ内でインターリーブされません。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[バンク グループ スワップ（Bank Group Swap）]	物理アドレスをアプリケーションに割り当てる方法を決定します。次のいずれかになります。 • **[Auto]**：アプリケーションへの物理アドレスの割り当て方法を CPU で自動的に決定します。 • **[Disabled]**：バンク グループ スワップは使用されません。 • **[Enabled]**：バンク グループ スワップによりアプリケーションのパフォーマンスを向上させます。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[決定論的スライダ（Determinism Slider）]	AMDプロセッサにより動作方法を決定できます。次のいずれかになります。 • **[Auto[**：CPU はデフォルトの決定論的な電源設定を自動で使用します。 • **[Performance]**：プロセッサは、最適なパフォーマンスかつ一貫した方法で動作します。 • **[Power]**：プロセッサは、ダイごとに許容される最大のパフォーマンスで動作します。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[IOMMU]	出入力メモリ管理ユニット（IOMMU） により、AMDプロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。次のいずれかになります。 • **[Auto]**：これらのアドレスのマッピング方法をCPUで決定します。 • **[Disabled]**：IOMMU は使用されません。 • **[Enabled]**：IOMMU によりアドレス マッピングを行います。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。
[SVM モード（SVM Mode）]	プロセッサが AMD セキュア仮想マシン テクノロジを使用するかどうか。次のいずれかを選択できます。 • **[Disabled]**：プロセッサで SVM テクノロジーを使用しません。 • **[Enabled]**：プロセッサで SVM テクノロジーを使用します。これがデフォルトのオプションです。 • [Platform Default][platform-default]：BIOS は、サーバータイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SMEE]	プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable（SMEE）機能を使用するかどうかを指定します。次のいずれかになります。 • **Auto**： これはデフォルトのオプションです。 • **[Disabled]**：プロセッサで SMEE 機能を使用しません。 • **[Enabled]**：プロセッサで SMEE 機能を使用します。 • **[プラットフォームのデフォルト（Platform Default）]**：BIOS は、サーバ タイプとベンダーを決める際に、BIOS デフォルト値に含まれるこの属性の値を使用します。
[UPI プリフェッチ（UPI Prefetch）]	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [有効（enabled）][有効（Enabled）]：UPIプリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。 • [disabled][Disabled]：プロセッサでキャッシュデータをプリロードしません。 • **自動**：プロセッサは UPI プリフェッチャ オプションを有効にします。
[SGX 自動 MP レジストレーション エージェント（SGX Auto MP Registration Agent）]	レジストレーション エージェント サービスがプラットフォーム キーを保存できるようにします。次のいずれかになります。 • **[有効]**：サポートは有効になります。 • **[無効]**：サポートは無効になります。
[SProcessor エポック（SProcessor Epoch）] ***n***	n で指定された EPOCH 番号の SGX EPOCH 所有者値を定義できます。
[SGX ファクトリー リセット（SGX Factory Reset）]	その後の起動時にシステムが SGX の工場出荷時リセットを実行できるようにします。これにより、すべての登録データが削除されます。次のいずれかになります。 • **[有効]**：サポートは有効になります。 • **[無効]**：サポートは無効になります。

名前	説明
[SGX PBUKEY ハッシュ（SGX PBUKEY HASH）]*n*	ソフトウェアガード拡張（SGX）の値を設定できます。この値の設定範囲は、以下のとおりです。 • SGX PUBKEY HASH0 — 7 ～ 0 の間 • SGX PUBKEY HASH1 — 15 ～ 8 の間 • SGX PUBKEY HASH2 — 23 ～ 16 の間 • SGX PUBKEY HASH3 — 31 ～ 24 の間
[SGX 書き込み有効（SGX Write Enable）]	SGX 書き込み機能を有効にすることができます。次のいずれかになります。 • **[有効]**：サポートは有効になります。 • **[無効]**：サポートは無効になります。
[SGX パッケージ情報インバンド アクセス（SGX Pkg info In-Band Access）]	SGX パッケージ情報インバンドアクセスを有効にすることができます。次のいずれかになります。 • **[有効]**：サポートは有効になります。 • **[無効]**：サポートは無効になります。
[SGX QoS]	SGX QoS を有効にすることができます。次のいずれかになります。 • **[有効]**：サポートは有効になります。 • **[無効]**：サポートは無効になります。
[Intel Dynamic Speed Select（Intel ダイナミック速度選択）]	Intel ダイナミック速度選択モードでは、ユーザーは自動モードで異なる速度とコアを使用して CPU を動作させることができます。次のいずれかになります。 • **有効**：Intel ダイナミック速度選択が有効になっています。 • **無効**：Intel ダイナミック速度選択が無効になっています。

名前	説明
[IIO eDPC サポート（IIO eDPC Support）]	eDPC を使用すると、修正不可能なエラーの後にダウンストリーム リンクを無効にすることができるため、制御された堅牢な方法で回復することが可能になります。次のいずれかになります。 • **[無効]**：eDPC サポートは無効になります。 • **致命的なエラーの場合**：eDPC は致命的なエラーの場合にのみ有効になります。 • **致命的および非致命的エラー**：eDPC は、致命的および非致命的エラーの両方に対して有効になっています。
[マルチキー トータル メモリ暗号化（Multikey Total Memory Encryption、MK-TME）	MK-TME を使用すると、独自のキーを持つ 1 つの暗号化ドメインを複数持つことができます。異なるメモリページを異なるキーで暗号化できます。次のいずれかになります。 • **[有効]**：サポートは有効になります。これがデフォルトのオプションです。 • **[無効]**：サポートは無効になります。
[SWガード拡張（SW Guard Extensions、SGX）	ソフトウェア ガード拡張（SGX）機能を有効にすることができます。次のいずれかになります。 • **[有効]**：サポートは有効になります。 • **[無効]**：サポートは無効になります。
[トータル メモリ暗号化（Total Memory Encryption、TME）	システムの物理メモリ全体を暗号化する機能を提供します。次のいずれかになります。 • **[有効]**：サポートは有効になります。これがデフォルトのオプションです。 • **[無効]**：サポートは無効になります。

名前	説明
[所有者 EPOCH入力タイプ選択（Select Owner EPOCH input type）]	作成され、ロックされたメモリ領域に使用されるセキュリティ キーのシードを変更できます。次のいずれかになります。 • **SGX 所有者エポック有効化**：現在の入力タイプを変更しません。 • **新しいランダム所有者エポックに変更**：エポックをシステムが生成したランダムな数値に変更します。 • **手動ユーザー定義所有者エポック**：エポック シードをユーザーが入力した 16 進値に変更します。

[強化 CPU パフォーマンス（Enhanced CPU Performance）]	サーバー設定を自動的に調整することにより、CPU パフォーマンスを向上させます。次のいずれかになります。
	• **[無効]**：プロセッサでこの機能を使用しません。これがデフォルトのオプションです。
	• **[自動]**：サーバー設定を調整して、プロセッサのパフォーマンスを向上させることができます。
	（注）
	• この機能を有効にすると、消費電力が増加する可能性があります。
	• この機能を使用するには、サーバーが次の要件を満たしている必要があります。
	  • サーバーが、Barlow Pass DIMM を使用していないこと。
	  • Cisco UCS C220 M6 サーバーの DIMM モジュール サイズは 64 GB 未満であり、Cisco UCS C240 M6 サーバーでは 256 GB 未満であること。
	  • サーバーに GPU カードが搭載されていないこと。

名前	説明
[UPI リンク有効化（UPI Link Enablement）]	プロセッサが必要とする数のウルトラパスインターコネクト（UPI）リンクを有効にします。次のいずれかになります。 • **[自動]**：これはデフォルトのオプションです。 • **1** • **2**
[UPI 電力管理（UPI Power Manangement）]	UPI 電力管理は、サーバーの電力を節約するために使用できます。次のいずれかになります。 • **有効**：プロセッサがこの機能をサポートできるようにします。 • **無効**：プロセッサのこの機能をサポートを無効にします。これがデフォルトのオプションです。
[C1 自動降格解除（C1 Auto UnDemotion）]	プロセッサがC1降格状態から自動的に解除できるようにするかどうかを選択します。次のいずれかになります。 • **Auto** これがデフォルトのオプションです。 • **有効**：プロセッサがこの機能をサポートできるようにします。 • **無効**：この機能をサポートするプロセッサを無効にします。
[C1 自動降格（C1 Auto Demotion）]	有効にすると、CPU は非コア自動降格情報に基づいてC1状態に自動的に降格します。次のいずれかになります。 • **Auto** これがデフォルトのオプションです。 • **有効**：プロセッサがこの機能をサポートできるようにします。 • **無効**：この機能をサポートするプロセッサを無効にします。

名前	説明
[CPU ダウンコア制御 7xx3（CPU Downcore control 7xx3）	1 つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。次のいずれかになります。 • **[Auto]**：有効化する必要のあるコアの数を CPU で判断します。これはデフォルトのオプションです。 • **ONE (1+0)**：1 つの CPU コンプレックスで 1 つのコアを有効にします。 • **Two (2+0)**：1 つの CPU コンプレックスで 2 つのコアを有効にします。 • **Three (3+0)**：1 つの CPU コンプレックスで 3 つのコアを有効にします。 • **Four (4+0)**：1 つの CPU コンプレックスで 4 つのコアを有効にします。 • **Five (5+0)**：1 つの CPU コンプレックスで 5 つのコアを有効にします。 • **Six (6+0)**：1 つの CPU コンプレックスで 6 つのコアを有効にします。 • **Seven (7+0)**：1 つの CPU コンプレックスで 7 つのコアを有効にします。 （注） このトークンは、7xx3 モデルのプロセッサを搭載したサーバーにのみ適用されます。

名前	説明
[固定 SOC P ステート（Fixed SOC P-State）]	このオプションは、APBDIS（アルゴリズム パフォーマンス ブースト（APB）無効化）が設定されている場合のターゲットPステートを定義します。**P-x**は、取り付けられているプロセッサの有効な P ステートを指定します。次のいずれかになります。 • **自動**：プロセッサに適した有効な P ステートを設定します。これがデフォルトのオプションです。 • **P0**：最高のパフォーマンスを発揮する SOC P ステートです。 • **P1**：次にパフォーマンスの高い SOC P ステートです。 • **P2**：次にパフォーマンスの高い SOC P ステートです。 • **P3**：最小の SOC 出力 P ステートです。
[APBDIS]	SMU の APBDIS（アルゴリズム パフォーマンス ブースト（APB）無効化）値を選択できます。次のいずれかになります。 • **自動**：SMU の自動 ApbDis を設定します。これがデフォルトのオプションです。 • **0**：SMU への ApbDis をクリアします。 • **1**：SMU への ApbDis をセットします。
[CCD 制御（CCD Control）]	システムで有効にしたい電荷結合デバイス CCD の数を指定できます。次のいずれかになります。 • **自動**：プロセッサによって提供される最大数の CCD が有効になります。これがデフォルトのオプションです。 • **2 CCDS** • **3 CCDS** • **4 CCDS** • **6 CCDS**

名前	説明
[Cisco xGMI 最大速度（Cisco xGMI Max Speed）]	このオプションは、18 Gbps XGMI リンク速度を有効にします。次のいずれかになります。 • **無効**：機能を無効にします。これがデフォルトのオプションです。 • **有効**：機能を有効にします。
[NUMAドメインとしてのACPI SRAT L3キャッシュ（ACPI SRAT L3 Cache As NUMA Domain）]	各 CCX がそのオン ドメインにあると宣言されている物理ドメインの上に仮想ドメインのレイヤーを作成します。次のいずれかになります。 • **自動**：自動モードに設定します。これがデフォルトのオプションです。 • **無効**：ドメイン構成に NPS 設定を使用します。 • **有効**：各CCXを独自のドメインにあると宣言します。
[ストリーミング ストア制御（Streaming Stores Control）]	ストリーミング ストア機能を有効にします。次のいずれかになります。 • **自動**：自動モードに設定します。これがデフォルトのオプションです。 • **無効**：機能は無効です。 • **有効**：機能は有効です。
[DF C ステート（DF C-States）]	システムで長時間のアイドル状態が予想される場合、この制御により、システムは、システムをさらに低電力状態に設定できるDF Cステートに移行できます。次のいずれかになります。 • **自動**：自動モードに設定します。これがデフォルトのオプションです。 • **無効**：このオプションはオフです。長時間のアイドル状態は予想されないため、省電力は実現されません。 • **有効**：このオプションはアクティブです。システムがアイドル状態のときに電力を節約します。

名前	説明
[SEV-SNP サポート（SEV-SNP Support）]	セキュア ネスティッドページング機能を有効にできます。次のいずれかになります。 • **無効**：プロセッサで SEV-SNP 機能を使用しません。これがデフォルトのオプションです。 • **有効**：プロセッサでSEV-SNP機能を使用します。
[効率モード有効（Efficiency Mode Enable）]	効率に基づいて消費電力を設定できます。次のいずれかになります。 • **自動**：CPU はデフォルトの設定を自動で使用します。これがデフォルトのオプションです。 • **有効**：効率モードは有効です。
[SNP メモリ カバレッジ（SNP Memory Coverage）]	SNP メモリ カバレッジを設定できます。次のいずれかになります。 • **自動**：システムがメモリ カバレッジを決定します。これがデフォルトのオプションです。 • **無効**：プロセッサはこの機能を使用しません。 • **有効**：この機能は有効です。 • **カスタム**：カスタム サイズは、カバーする SNP メモリ サイズで定義できます。
[カバーする SNP メモリ サイズ、MB 単位（SNP Memory Size to Cover in MB）]	SNP メモリ サイズを設定できます。 値の範囲は 0 ～ 1048576 です。0 がデフォルトのオプションです。
[SMT モード（SMT Mode）]	プロセッサで AMD Simultaneous MultiThreading テクノロジーを使用するかどうかを指定します。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • **[Auto]**：プロセッサは、マルチスレッドの並列実行を許可します。 • **有効**：プロセッサはマルチスレッドを許可します。これがデフォルトのオプションです。 • **無効**：プロセッサはマルチスレッドを許可しませんん。

名前	説明
[CPCC]	コラボレーティブプロセッサパフォーマンス制御を設定できます。次のいずれかになります。 • **自動**：CPU はデフォルトの CPPC 設定を自動で使用します。これがデフォルトのオプションです。 • **無効**：機能は無効です。 • **有効**：コラボレーティブプロセッサパフォーマンスが有効になっています。
[ダウンコア制御 7xx2（Downcore control 7xx2）]	1 つ以上のコアの動作を停止する機能を提供します。シリコン回路でサポートされています。OS の制限、またはシステムの電力削減要件により、コア数を減らすことが望ましい場合があります。この項目により、実行中のコアの数を制御できます。この設定では、プロセッサで使用可能なコアの数を減らすことしかできません。次のいずれかになります。 • **[Auto]**：有効化する必要のあるコアの数を CPU で判断します。これがデフォルトのオプションです。 • **Two (1+1)**：片方の CPU コンプレックスで 2 つのコアを有効にします。 • **Four (2+2)**：片方の CPU コンプレックスで 4 つのコアを有効にします。 • **Six (3+3)**：片方の CPU コンプレックスで 6 つのコアを有効にします。
[プロセッサ EPP プロファイル（Processor EPP Profile）]	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • **[パフォーマンス（Performance）]** • **[バランスのとれたパフォーマンス（Balanced Performance）]**— これは、デフォルト オプションです。 • **[バランスのとれた電力（Balanced power）]** • **[電力（Power）]**

名前	説明
[自律コア C 状態（Autonomous Core C-state）]	HALT 命令を MWAIT 命令に変換する CPU Autonomous C-State を有効にします。次のいずれかになります。 • **Disabled**：これはデフォルトのオプションです。 • [enabled][Enabled]
[エネルギー効率ターボ（Energy Efficient Turbo）]	エネルギー効率の高いターボが有効になっている場合、CPU の最適なターボ周波数は、CPU 使用率に基づいてダイナミックになります。パワー/パフォーマンスのバイアス設定も、エネルギー効率の高いターボに影響します。次のいずれかになります。 • **Disabled**：これはデフォルトのオプションです。 • [enabled][Enabled]
[ハードウェア P 状態（Hardware P-States）]	プロセッサ ハードウェアの P ステートを有効にします。次のいずれかになります。 • [disabled][Disabled]：HWPMがディセーブルになります。 • **[hwpm ネイティブ モード（HWPM Native Mode）]** — HWPM ネイティブ モードがイネーブルになります。これがデフォルトのオプションです。 • **[HWPM OOB モード（HWPM OOB Mode）]** — HWPM アウトオブボックス モードがイネーブルになります。 • **[レガシーのないネイティブ モード（Native Mode with no Legacy）]**

名前	説明
[エネルギー/パフォーマンスの BIOS 構成（Energy/Performance BIOS Config）]	システム パフォーマンスまたはエネルギー効率がこのサーバーで重要かどうかを判断できます。次のいずれかになります。 • **[パフォーマンス（Performance）]** — サーバーでは、すべてのサーバー コンポーネントに全電力を常時提供します。 このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • **[バランスのとれたパフォーマンス（Balanced Performance）]** — サーバーは、すべてのサーバーコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。これがデフォルトのオプションです。 • **[バランスのとれた電力（Balanced power）]** — サーバーは、すべてのサーバー コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（power）] **[電力（Power）]** — サーバーは、すべてのサーバーコンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。
[電力パフォーマンスの調整（Power Performance Tuning）]]	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。次のいずれかになります。 • **BIOS** — エネルギー効率の調整のために BIOS を選択します。 • **OS** — エネルギーパフォーマンスの調整にOSを選択します。これがデフォルトのオプションです。 • **PECI** — 効率を調整する場合は、 PECI を選択します。

名前	説明
[コアは、イネーブル化されました（Cores Enabled）]	サーバー上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • **[全て（All）]**—すべての物理コアをイネーブルにします。これにより、関連付けられている論理プロセッサ コアで Hyper Threading もイネーブルになります。 • **[1] ～ [48]** — サーバーで実行できる物理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。
[ハイパースレッディング [すべて]（Hyper-Threading [All]）]	プロセッサでインテル ハイパースレッディング テクノロジーを使用するかどうか。このテクノロジーでは、マルチスレッド ソフトウェア アプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [disabled][Disabled]：プロセッサでのハイパースレッディングを禁止します。 • [enabled][Enabled]：プロセッサでの複数スレッドの並列実行を許可します。
[SpeedStep（Pstates）]	プロセッサで拡張版 Intel SpeedStep テクノロジーを使用するかどうか設定します。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [disabled][Disabled]：プロセッサの電圧または周波数を動的に調整しません。 • [enabled][Enabled]：プロセッサでEnhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。

名前	説明
[ブートパフォーマンスモード（Boot Performance Mode）]	オペレーティング システムのハンドオフ前に設定されている BIOS のパフォーマンス状態をユーザが選択できるようになります。次のいずれかになります。 • **[最大パフォーマンス（Max Performance）]** — プロセッサの P-state の比率が最大です。 • **[最大効率（Max Efficient）]** —プロセッサの P-state の比率が最小です。 • **[インテル nm によって設定されています（Set by Intel NM）]** —プロセッサの P-state 比は Intel によって設定されます。
[EIST PSD 関数（EIST PSD Function）]	EIST は、電圧と周波数のペア（P 状態）の変更に固有の遅延を短縮するため、これらの遷移がより頻繁に発生するようになります。これにより、より詳細なデマンド ベースのスイッチングが可能になり、アプリケーションの要求に基づいて電力とパフォーマンスのバランスを最適化できます。次のいずれかになります。 • **[Hw 全て（Hw All）]** — プロセッサは、論理プロセッサの依存関係間の P 状態を調整します。OS は、すべての論理プロセッサで P-state 要求を最新の状態に保ちます。これがデフォルトのオプションです。 • **[Sw 全て（Sw All）]** — OS Power Manager によって、依存関係にある論理プロセッサ間の P-state を調整します。すべての論理プロセッサで遷移を開始します。
[ターボ モード（Turbo Mode）]	プロセッサでインテル ターボ ブースト テクノロジーを使用するかどうか。このテクノロジーでは、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にそのプロセッサの周波数が上がります。次のいずれかになります。 • [disabled][Disabled]：プロセッサの周波数は自動的には上がりません。 • **[有効（Enabled）]** — 必要に応じてプロセッサでターボ ブースト テクノのジーが利用されます。これがデフォルトのオプションです。

名前	説明
[拡張APIC]	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • **Disabled**：これはデフォルトのオプションです。 • **[有効（Enabled）]**。
[メモリ インターリービング サイズ（Memory Interleaving Size）]	インターリーブされるメモリ ブロックのサイズを決定します。また、インターリーブの開始アドレス（ビット 8、9、10または、11）も指定します。次のいずれかになります。 • 1 KB • 2 KB • 4 KB • 256 バイト • 512 バイト • **自動**: CPU、メモリ ブロックのサイズを決定します。 • [Platform Default][platform-default]：BIOS は、サーバー タイプとベンダーを決める際に、BIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[UPI リンク周波数選択 (UPI Link Frequency Select)]	拡張 APIC サポートをイネーブルまたはディセーブルにできます。次のいずれかになります。 • **[自動 (Auto)]** — このオプションは、最適なリンク速度を自動的に設定します。これがデフォルトのオプションです。 • **9.6GT/S** — このオプションは、最適なリンク速度として 9.6GT/s を使用します。 • **10.4GT/S**— このオプションは、最適なリンク速度として 10.4GT/s を使用します。 • **11.2GT/S**— このオプションは、最適なリンク速度として 10.4GT/s を使用します。 • **12.8GT/S**：このオプションは、最適なリンク速度として 12.8GT/s を使用します。 • **14.4gt/s**：このオプションは、最適なリンク速度として 14.4GT/s を使用します。 • **16.0GT/S**：このオプションは、最適なリンク速度として 16.0GT/s を使用します。 • **20.0GT/S**：このオプションは、最適なリンク速度として 20.0GT/s を使用します。

Intel 向け I/O BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる Intel Directed I/O の BIOS 設定を示しています。

名前	説明
[Intel VT for Directed IO]	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサで仮想化テクノロジーを使用しません。 • [enabled][Enabled]：プロセッサで仮想化テクノロジーを使用します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） 他の Intel Directed I/O BIOS 設定を変更する場合は、このオプションをイネーブルにする必要があります。
[Intel VTD interrupt Remapping]	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサがリマッピングをサポートしません。 • [enabled][Enabled]：プロセッサが必要に応じてVT-d Interrupt Remapping を使用します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Intel VTD coherency support]	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサがコヒーレンシをサポートしません。 • [enabled][Enabled]：プロセッサが必要に応じてVT-d Coherency を使用します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Intel VTD ATS support]	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサがATS をサポートしません。 • [enabled][Enabled]：プロセッサが必要に応じてVT-d ATS を使用します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Intel VTD pass through DMA support]	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。次のいずれかになります。 • [disabled][Disabled]：プロセッサがパススルーDMA をサポートしません。 • [enabled][Enabled]：プロセッサが必要に応じてVT-d パススルー DMA を使用します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

AMD 向け I/O BIOS 設定

次の表に、AMD 向けの BIOS ポリシーを介して構成できる入出力 BIOS 設定の一覧を示します。

名前	説明
[PCIe ARI サポート (PCIe ARI Support)]	PCIe の代替ルーティング ID（ARI）解釈機能は、8 個以上の機能を有効にする PCIe ヘッダーのデバイス番号フィールドを再解釈する ARI の実装を通じて、より多くの仮想機能をサポートします。次のいずれかになります。 • **Disabled**：サポートは使用できません。 • **Enabled**：PCIe ARIサポートを使用できます。 • **Auto**—PCIe ARI Support is in auto mode. これがデフォルトのオプションです。

名前	説明
[IPv4 PXE サポート（IPv4 PXE Support）]	PXE の IPv4 サポートを有効または無効にします。次のいずれかになります。 • **[無効(Disabled)]** : PV6 PXE のサポートは利用できません。 • **[有効（Enabled）]** : IPv6 PXE サポートを利用できます。これがデフォルトのオプションです。
IPv4 HTTP Support	HTTP の IPv4 サポートを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]** : IPv4 HTTP サポートは使用できません。 • **[有効（Enabled）]** : IPv4 PXE サポートを利用できます。これがデフォルトのオプションです。
[IPv6 PXE サポート（IPv6 PXE Support）]	HTTP の IPv6 サポートを有効または無効にします。次のいずれかになります。 • **[無効（Disabled）]** : IPv6 HTTP サポートは使用できません。 • **[有効（Enabled）]** : IPv6 PXE サポートを利用できます。これがデフォルトのオプションです。

名前	説明
[Network Stack (ネットワーク スタック)]	このオプションでは、IPv6 と IPv4 をモニタできます。次のいずれかになります • **[無効 (Disabled)]**: ネットワーク スタックのサポートは使用できません。 （注） 無効にすると、 **IPV4 PXE サポート**に設定された値はシステムに影響しません。 • **[Enabled (有効)]**: ネットワーク スタックのサポートを利用できます。これがデフォルトのオプションです。 （注） Network Stack トークンの値が [無効（Disabled）] の場合、以下のトークンとその値も設定されます • IPV4PXE - 無効 • IPV4HTTP - 無効 • IPV6HTTP - 無効
[SR-IOVサポート（SR-IOV Support）]	サーバー上で SR-IOV（Single Root I/O Virtualization）を有効にするか無効にするか。次のいずれかになります。 • **イネーブル化**—SR-IOV はイネーブル化されます。これがデフォルトのオプションです。 • **ディセーブル化** — SR-IOV はディセーブル化されます。

RAS メモリの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して設定できる RAS メモリの BIOS 設定の一覧を示します。

名前	説明
[部分的なキャッシュ行の節約（Partial Cache Line Sparing）]	パーシャル キャッシュ ライン スペアリング (PCLS) は、メモリ コントローラーのエラー防止メカニズムです。PCLSは、メモリアクセス中に置換できるように、ビットの欠陥のあるニブルの場所を、対応するデータコンテンツとともにスペア ディレクトリに静的にエンコードします。次のいずれかになります。 • **[無効（Disabled）]**：サポートは無効になります。 • **[有効（Enabled）]**：サポートは有効になります。
UMA	UMA設定を設定できます。次のいずれかになります。 • **[無効-All-2All（Disable-All-2All）]** • **[半球-2-クラスタ（Hemisphere-2-clusters）]**
[メモリサーマルスロットリングモード（Memory Thermal Throttling Mode）]	メモリの温度が制限内にあることを保証する保護メカニズムを提供します。温度が最高しきい値を超えると、メモリ アクセス レートが下げられ、Baseboard Management Controller（BMC）がファンを調整してメモリを冷却し、過熱による DIMM の損傷を防ぎます。次のいずれかになります。 • **CLTT with PECI**：プラットフォーム環境制御インターフェイスを使用してクローズドループサーマル スロットリングを有効にします。これがデフォルトのオプションです。 • **Disabled**。 （注） この設定は、デフォルトの **CLTT with PECI** のままにすることを推奨します

名前	説明
[拡張メモリ テスト（Enhanced Memory Test）]	システムの起動中に拡張メモリテストを有効にします。メモリ量に応じて起動時間は長くなります。次のいずれかになります。 • **Auto**： これはデフォルトのオプションです。 （注） この設定は、デフォルト状態の **Auto** のままにしておくことをお勧めします。 • [enabled][Enabled] • [disabled][Disabled] （注） • この BIOS トークン名は、M6 サーバーの **Advanced Memory Test** から **Enhanced Memory Test** に変更されました。
[透過的セキュアメモリ暗号化（Transparent Secure Memory Encryption、TSME）	システム メモリに格納されているすべてのデータの透過的なハードウェア メモリ暗号化を提供します。次のいずれかになります。 • [enabled][Enabled] • [disabled][Disabled] • **Auto**： これはデフォルトのオプションです。 （注） Rowhammer スタイルの攻撃を軽減するために、この設定は **Auto** のデフォルト状態のままにすることを推奨します。
[セキュア暗号仮想化（Secure Encrypted Virtualization、SEV）	VM のコードとデータが分離された、暗号化仮想マシン（VM）の実行を有効にします。次のいずれかになります。 • **253 ASIDs** • **509 ASIDs** • **Auto**： これはデフォルトのオプションです。 （注） Rowhammer スタイルの攻撃を軽減するために、この設定は **Auto** のデフォルト状態のままにすることを推奨します。

名前	説明
[DRAM SW サーマル スロットリング（DRAM SW Thermal Throttling）]	ソフトウェアが温度制限内で機能することを保証する保護メカニズムを提供します。温度が最大しきい値を超えると、パフォーマンスを低下させ、最小しきい値まで冷却します。次のいずれかになります。 • [enabled][Enabled] • **Disabled**：これはデフォルトのオプションです。 （注） Rowhammer スタイルの攻撃を軽減するために、この設定は **Auto** のデフォルト状態のままにすることを推奨します。
[メモリ リフレッシュ レート（Memory Refresh Rate）]	メモリ コントローラのリフレッシュ レートを制御し、メモリ構成とワークロードに応じて、メモリのパフォーマンスと電力に影響を及ぼせるようにします。次のいずれかになります。 • **1x Refresh** • **2x Refresh**：これはデフォルトのオプションです。
[パニックと高水準点（Panic and High Watermark）]	メモリ コントローラの遅延リフレッシュ機能を制御します。次のいずれかになります。 • **[高（High）]**：メモリ コントローラは、最大 8 つのリフレッシュ コマンドを延期できます。メモリ コントローラは、延期されたすべてのリフレッシュをリフレッシュ間隔内で実行します。9番目のリフレッシュ コマンドについては、リフレッシュの優先順位を**パニック**にします。メモリ コントローラは、延期されたすべてのリフレッシュ コマンドが実行されるまで、通常のメモリ トランザクションを一時停止します。 • **[低（Low）]**：これはデフォルトのオプションです。メモリ コントローラは、リフレッシュ コマンドを延期することはできません。 （注） Rowhammer スタイルの攻撃を軽減するために、この設定はデフォルト状態（**[低（Low）]**）のままにすることを推奨します。

名前	説明
[メモリ RAS 設定（Memory RAS configuration）]	

名前	説明
	サーバーに対するメモリの信頼性、可用性および機密性（RAS）の設定方法。次のいずれかになります。 • **Maximum Performance**：システム パフォーマンスを最適化し、すべての高度な RAS 機能を無効にします。 • [mirroring][Mirroring]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。 このモードは UCS M4 以前のブレード サーバーに使用します。 • [lockstep][Lockstep]：サーバー内のDIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップ モードを有効にして、メモリ アクセス遅延の最小化およびパフォーマンスの向上を実現できます。B440 サーバーでは [lockstep] がデフォルトで有効になっています。 • [Mirror Mode 1LM]：ミラー モード 1LM は、ミラーリングされるシステム内の 1LM メモリ全体を設定し、結果的にメモリ容量を半減させます。このモードは UCS M5 および M6 ブレード サーバーに使用します。 • **[部分的なミラー モード 1LM (Partial Mirror Mode 1LM)]**：部分的なミラー モード 1LM は、ミラーリングされるシステム内の 1LM メモリの一部全体を設定し、結果的にメモリ容量を半減させます。このモードは UCS M5 および M6 ブレード サーバーに使用します。 • [sparing][Sparing]：システムの信頼性は、他のDIMM が故障した場合に使用できるように、メモリを予備に保持することによって最適化されます。このモードは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。 • **ADDDC Sparing**：システムの信頼性は、他の DIMM が故障した場合に使用できるように、メモリを予備に保持することによって最適化されます。このモードは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含ま

名前	説明
	れるこの属性の値を使用します。
[NUMA 最適化（NUMA optimized）]	BIOS で NUMA をサポートするかどうか。次のいずれかになります。 • [disabled][Disabled]：BIOSで NUMA をサポートしません。 • [enabled][Enabled]：NUMAに対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションをイネーブルにした場合は、一部のプラットフォームでシステムのソケット間メモリ インターリーブをディセーブルにする必要があります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[ポストパッケージ修復（Post Package Repair）]	Post Package Repair (PPR) は、スペア セルに置き換えて、障害のあるメモリ セルを修復する機能を提供します。次のいずれかになります。 • **Disabled**：BIOS で PPR タイプの選択をサポートしません。 • **Hard PPR**：これにより、破損したストレージセルが永続的に再マッピングされることになります。これがデフォルトのオプションです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[メモリ サイズ制限（GB）（Memory Size Limit in GB）]	部分的なメモリのミラー モードの容量を、合計メモリ容量の 50% に制限します。メモリサイズは、0 GB ~ 65535 GB の範囲で 1 GB ずつ増加します。

名前	説明
[ミラーリング モード（Mirroring Mode）]	メモリのミラーリングは、メモリに 2 つの同じデータイメージを保存することにより、システムの信頼性を向上させます。 このオプションは、[Memory RAS Config] で [mirroring] オプションを選択したときのみ使用可能です。次のいずれかを指定できます。 • [inter-socket][Inter-Socket]：メモリは、CPUソケットをまたいで 2 台の Integrated Memory Controller（IMC）間でミラーリングされます。 • [intra-socket][Intra-Socket]：1台の IMC が同じソケットの別の IMC とミラーリングされます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[スペアリング モード（Sparing Mode）]	スペアリングはメモリを予備に保持することで信頼性を最適化し、別の DIMM の障害発生時に使用できるようにします。このオプションは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。使用可能なスペアリング モードは、現在のメモリ容量によって異なります。 このオプションは、[Memory RAS Config] で [sparing] オプションを選択したときのみ使用可能です。次のいずれかを指定できます。 • [dimm-sparing][DIMM Sparing]：1枚の DIMM が予備に保持されます。DIMM に障害が発生すると、その DIMM の内容はスペア DIMM に移されます。 • [rank-sparing][Rank Sparing]：DIMMのスペア ランクが予備に保持されます。あるランクの DIMM に障害が発生した場合、そのランクの内容がスペアランクに移されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[LV DDR モード（LV DDR Mode）]	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [auto][Auto]：CPUが、低電圧メモリ動作または高周波メモリ動作のどちらを優先するかを決定します。 • [power-saving-mode][PowerSaving Mode]：低電圧メモリ動作が高周波メモリ動作よりも優先されます。このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [performance-mode][Performance Mode]：高周波動作が低電圧動作よりも優先されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[DRAM リフレッシュ レート（DRAM Refresh rate）]	内部メモリ用の更新間隔レート。次のいずれかになります。 • **[1x]** • **[2x]** • **[3x]** • **[4x]** • [auto][Auto] • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[DDR3 電圧選択（DDR3 Voltage Selection）]	デュアル電圧 RAM に使用される電圧。次のいずれかになります。 • **DDR3 1500mv** • **DDR3 1350mv** • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Partial Memory Mirror Mode（部分メモリ ミラー モード）]	部分的なメモリ ミラーリングを使用すると、GB 単位またはメモリ容量の割合によって部分的にミラーリングすることができます。ここで選択したオプションに応じて、使用可能なフィールドで、部分的なミラーの割合または部分的なミラー容量を GB 単位で定義できます。メモリ容量の最大 50% を部分的にミラーリングできます。次のいずれかを設定できます。 • **無効**: 部分的なメモリ ミラーが無効になります。これがデフォルトのオプションです。 • **容量**：部分メモリ モードでミラーリングされるメモリの量は、合計メモリの割合として定義されます。 • **値 (GB)**: 部分的なメモリ モードでミラーリングされるメモリの合計は GB で定義されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） **部分的なメモリ ミラー モード**は標準の**ミラーリング モード**に対して相互に排他的です。 部分的なミラー 1 ~ 4 は、関連オプションで GB または割合で設定されている容量制限を超えない限り、任意の数または設定で使用できます。
[部分的なミラー割合（Partial Mirror percentage）]	使用可能なメモリの総量を、合計メモリの割合として制限します。これは、0.000.01 %から 50.00 % まで、0.01 % 単位で増加させられます。
[部分ミラー 1 サイズ（GB）（Partial Mirror1 Size in GB）]	部分的な Mirror1 のメモリの量を GB 単位で制限します。これは、0 GB ~ 65535 GB の範囲で 1 GB ずつ増加します。
[部分ミラー 2 サイズ（GB）（Partial Mirror2 Size in GB）]	部分的な Mirror2 のメモリの量を GB 単位で制限します。これは、0 GB ~ 65535 GB の範囲で 1 GB ずつ増加します。
[部分ミラー 3 サイズ（GB）（Partial Mirror3 Size in GB）]	部分的な Mirror3 のメモリの量を GB 単位で制限します。これは、0 GB ~ 65535 GB の範囲で 1 GB ずつ増加します。

名前	説明
[部分ミラー4サイズ（GB）（Partial Mirror4 Size in GB）]	部分的な Mirror4 のメモリの量を GB 単位で制限します。これは、0 GB ~ 65535 GB の範囲で 1 GB ずつ増加します。
揮発性メモリ モード	メモリ モードの構成を許可します。次のいずれかが考えられます。 • **1LM**：1 層メモリ（1LM）を構成します。 • **2LM**：2 層メモリ（2LM）を構成します。
[メモリ帯域幅ブースト（Memory Bandwidth Boost）]	メモリ帯域幅を増やすことができます。次のいずれかになります。 • [enabled][Enabled] • [disabled][Disabled]
[バーストおよび遅延リフレッシュ（Burst and Postponed Refresh）]	メモリがアクティブで、指定されたウィンドウ内でリフレッシュを実行するときに、メモリ コントローラがリフレッシュ サイクルを延期できるようにします。遅延リフレッシュ サイクルは、複数のリフレッシュ サイクルのバーストで実行される場合があります。次のいずれかになります。 • [enabled][Enabled] • **Disabled**：これはデフォルトのオプションです。 （注） Rowhammer スタイルの攻撃を軽減するために、この設定は **Auto** のデフォルト状態のままにすることを推奨します。

名前	説明
[LLC デッドライン（LLC Dead Line）]	CPU の非包括的キャッシュ スキームでは、中間レベル キャッシュ（MLC）から削除された内容が最終レベル キャッシュ（LLC）に書き込まれます。行を MLC から削除する際、コアはそれらにデッドとしてフラグを立てることがあります（再度読み取られる可能性が小さい場合）。LLC には、デッドラインを削除し、LLC に書き込まないオプションがあります。次のいずれかになります。 • **Enabled**：使用可能な空きスペースがある場合、デッド ラインを LLC に書き込むことを LLC に許可します。これがデフォルトのオプションです。 • **Disabled**：デッドラインは常に削除されます。LLC に書き込まれることはありません。 • **Auto**：CPU が LLC のデッド ラインの割り当てを決定します
[XPT リモート プリフェッチ（XPT Remote Prefetch）	この機能は、LLC 要求を複製し、最近の LLC 履歴に基づいてリモート マシンの適切なメモリ コントローラに送信して、待ち時間を減らします。次のいずれかになります。 • [enabled][Enabled] • [disabled][Disabled] • **Auto**：CPU が機能を決定します。これがデフォルトのオプションです。
[仮想 NUMA（Virtual NUMA）]	仮想 NUMA（仮想非均一メモリ アクセス）は、VMware 仮想マシン（VM）のメモリ アクセス最適化方法であり、メモリ帯域幅のボトルネックを防ぐのに役立ちます。次のいずれかになります。 • **Enabled**：機能が有効になっています。 • **Disabled**：機能が無効になっています。これがデフォルトのオプションです。

名前	説明
[4 G 以上の復号化（Above 4G Decoding）]	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • **Enabled**：サーバーは、64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。これがデフォルトのオプションです。 • **Disabled**：サーバーは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。
[ソケットごとの NUMA ノード（NUMA Nodes per Socket）]	ソケットごとにメモリ NUMA ドメインを構成できます。次のいずれかになります。 • **Auto**：チャネル数を自動に設定します。これがデフォルトのオプションです。 • **NPS0**：ソケットごとの NUMA ノード数を 0 にします。 • **NPS1**：ソケットごとの NUMA ノード数を 1 にします。 • **NPS2**：ソケットごとの NUMA ノード数を 2 にし、SoC の左半分と右半分に 1 つずつにします。. • **NPS4**：ソケットごとの NUMA ノード数を 4 にし、クワドラントごとに 1 つにします。
[ディスク タイプの選択 (Select Disk Type)]	指定された障害のある行から指定されたスペア行へのアクセスを永続的に再マッピングする、**[ハード PPR (Hard PPR)]**をサポートしています。 • **[ハード PPR (hard PPR)]**：サポートは有効になっています。これがデフォルトのオプションです。 （注） ハード PPR は、**[メモリ RAS 設定 (Memory RAS Configuration)]**が**[ADDDC スペア (ADDDC Sparing)]**に設定されている場合にのみ使用できます。他の RA の選択では、この設定を **Disabled** に設定する必要があります。 • **[無効]**：サポートは無効になります。

名前	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）]	サーバーに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • **[ミラー モード 1LM（Mirror Mode 1LM）]** — システム メモリの半分をバックアップとして使用し、システムの信頼性を最適化します。 • **[ADDDC のスペアリング（ADDDC sparing）]** — 適応可能な仮想ロックステップは、ADDDC モードをサポートするためにハードウェアおよびファームウェアで実装されるアルゴリズムです。選択すると、アルゴリズムがアクティブになるまでシステムのパフォーマンスが最適化されます。このアルゴリズムは、DRAM デバイスで障害が発生した場合にアクティブになります。アルゴリズムがアクティブになると、仮想ロックステップ リージョンがアクティブになり、実行時に障害が発生したリージョンが動的にマッピングされ、パフォーマンスへの影響はリージョン レベルで制限されます。これがデフォルトのオプションです。 • **[部分的なミラー モード 1LM（Partial Mirror Mode 1LM）]** — 部分的な DIMM ミラーリングによって完全なミラー コピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なミラーリングでは、部分的なミラーコピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。 • **[最大パフォーマンス（Maximum Performance）]**：システムのパフォーマンスが最適化されます。
NUMA	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • **[有効]**：サポートは有効になります。 • **[無効]**：サポートは無効になります。

名前	説明
[操作 モード（Operation Mode）]	操作モードを設定できます。次のいずれかになります。 • **[テストのみ（Test Only）]** — サポートが有効になっています。 • **[テストと修復（Test and Repair）]** — サポートは無効になっています。

Intel® Optane™ DC 永続メモリ (DCPMM) BIOS トークン

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる Intel® Optane™ DC メモリの BIOS 設定の一覧を示します。

名前	説明
[NVM パフォーマンス設定 (NVM Performance Setting)]	**NVM パフォーマンス設定**により、DDR チャネル上の DDR と DDRT トランザクション間の効率的なメジャーモード調停が可能になり、チャネル BW と DRAM の遅延が最適化されます。 すべての M5 および M6 サーバーに適用されます。 次のいずれかの値を指定できます。 • **BW 最適化**：DDR および DDRT BW 用に最適化されています。これがデフォルトのオプションです。 • **遅延最適化**：DDRT BW が存在する場合 DDR 遅延が改善します。 • **バランシング プロファイル**：メモリ モード用に最適化されています。

名前	説明
[CR QoS]	同時DCPMM BW飽和スレッドの存在下でのDRAMおよびシステム全体のBWドロップを防止し、同種のDDRTのみの使用への影響を最小限に抑えます。マルチテナントの使用例、VMなどに適していますが、メモリモードも向上します。「ワーストケース」の低下をターゲットにします。 すべての M5 および M6 サーバーに適用されます。 次のいずれかの値を指定できます。 • **[無効（Disabled）]**：機能は無効です。これがデフォルトのオプションです。 • **[レシピ 1（Recipe 1）**：6 モジュール、最適化されたソケットあたり 4 モジュール • **[レシピ 2（Recipe 2）**：最適化されたソケットあたり 2 モジュール • **[レシピ 3（Recipe 3）**：最適化されたソケットあたり 1 モジュール • **モード 0 - PMem QoS 機能を無効にします** • **モード 1 - M2M QoS 有効化、CHA QoS 無効化** • **モード 2 - M2M QoS 有効化、CHA QoS 有効化** （注） 値**無効**、**レシピ 1**、**レシピ 2**、、**レシピ 3**、は UCS M6 サーバーではサポートされていません。

名前	説明
[CR Fastgo Config]	**CR FastGo Config** は、FastGO が無効になっている場合の DDRT 非一時書き込み帯域幅を改善します。FastGO を有効にすると、アンコアへの NT 書き込みのフローが高速になります。FastGO を無効にすると、CPU アンコアの NT 書き込みキューが減少し、DCPMM で連続して改善され、帯域幅が向上します。 すべての Cisco UCS M5 および Cisco UCS M6 サーバーに適用されます。 次のいずれかの値を指定できます。 • **[自動（Auto）]**：オプション 1 と同じです。FastGO を無効にします。DDRT に推奨されます。これが default のオプションです (Default とは区別してください)。 • **[デフォルト（Default）]**：FastGO を有効にします。 • **[オプション 1（Option 1）]**：FastGO を無効にします。 • **オプション 2、オプション 3、オプション 4、オプション 5**：該当なし。 • **[最適化を有効にする（Enable Optimization）** • **[最適化を無効にする（Disable Optimization）]** （注） 値**最適化を有効にする**、**最適化を無効にする**、および**自動**は、Cisco UCS M6 サーバーでサポートされます。

名前	説明
[AD の Snoopy モード (Snoopy mode for AD)]	すべてのDRAMアクセスでディレクトリを維持しながら、DCPMM アクセスのスヌーピング モードを有効にします。スヌープは、ソケット間のキャッシュの一貫性を維持します。ディレクトリは、リモート ノード情報をローカル（メモリ内）に保持することでスヌープを削減します。ディレクトリのルックアップと更新により、メモリ トラフィックが追加されます。 ディレクトリは、DRAMには適していますが、DCPMMには必ずしも適していません。非NUMAワークロードの場合、この機能を有効にすると、DCPMM に対するディレクトリの更新が排除されるため、DDRT の帯域幅が制限されたワークロードに役立ちます。ディレクトリは AD へのアクセスに対して無効になり、代わりにリモート ソケットをスヌーピングして所有権を確認します。ディレクトリはDRAMアクセスにのみ使用されます。 • **有効** • **無効** これはデフォルトのオプションです。
[2LM の Snoopy モード (Snoopy mode for 2LM)]	すべてのDRAMアクセスでディレクトリを維持しながら、DCPMM アクセスのスヌーピング モードを有効にします。スヌープは、ソケット間のキャッシュの一貫性を維持します。ディレクトリは、リモート ノード情報をローカル（メモリ内）に保持することでスヌープを削減します。ディレクトリのルックアップと更新により、メモリ トラフィックが追加されます。 ディレクトリは、DRAMには適していますが、DCPMMには必ずしも適していません。非NUMAワークロードの場合、この機能を有効にすると、DCPMM に対するディレクトリの更新が排除されるため、DDRT の帯域幅が制限されたワークロードに役立ちます。ディレクトリは、ファーメモリ アクセスに対して無効になっており、代わりにリモート ソケットをスヌーピングして所有権を確認します。ディレクトリは DRAM (メモリの近く) にのみ使用されます。 • **有効** • **無効** これはデフォルトのオプションです。

名前	説明
[eADR サポート（eADR Support）]	拡張非同期 DRAM リフレッシュ (eADR) により、データを含むCPUキャッシュ ラインが適切なタイミング、必要な順序でフラッシュされます。**電源障害から保護されたドメイン**にも含まれます。次のいずれかが考えられます。 • **有効** • [disabled][Disabled] • **Auto**： これはデフォルトのオプションです。

シリアル ポートの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるシリアル ポートの BIOS 設定の一覧を示します。

名前	説明
[Serial port A enable]	シリアル ポート A を有効にするか無効にするか。次のいずれかになります。 • [disabled][Disabled]：シリアルポートはディセーブルです。 • [enabled][Enabled]：シリアルポートはイネーブルです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

USB BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる USB BIOS 設定の一覧を示します。

名前	説明
[Make Device Non Bootable]	サーバーがUSBデバイスからブートできるかどうか。次のいずれかになります。 • [disabled][Disabled]：サーバーはUSBデバイスからブートできます。 • [enabled][Enabled]：サーバーはUSBデバイスからブートできません。 • **[Platform Default]**[platform-default]：BIOSは、サーバタイプとベンダーのBIOSデフォルト値に含まれるこの属性の値を使用します。
[Legacy USB Support]	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [disabled][Disabled]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [enabled][Enabled]：レガシーUSBのサポートは常に使用できます。 • [auto][Auto]：USBデバイスが接続されていない場合、レガシーUSBのサポートがディセーブルになります。 • **[Platform Default]**[platform-default]：BIOSは、サーバタイプとベンダーのBIOSデフォルト値に含まれるこの属性の値を使用します。

名前	説明
[USB Idle Power Optimizing Setting]	USB EHCI のアイドル時電力消費を減らすために USB アイドル時電力最適化設定を使用するかどうか。この設定で選択した値によって、パフォーマンスが影響を受けることがあります。次のいずれかになります。 • [high-performance][High Performance]：最適なパフォーマンスを電力節約より優先するため、USB システムのアイドル時電力最適化設定はディセーブルにされます。 このオプションを選択すると、パフォーマンスが大幅に向上します。サイトにサーバーの電源制限がない場合はこのオプションを選択することを推奨します。 • [lower-idle-power][Lower Idle Power]：電力節約を最適なパフォーマンスより優先するため、USB システムのアイドル時電力最適化設定はイネーブルにされます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB Front Panel Access Lock]	USB 前面パネル アクセス ロックは、USB ポートへの前面パネル アクセスをイネーブルまたはディセーブルにするために設定されます。次のいずれかになります。 • [disabled][Disabled] • [enabled][Enabled] • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Port 60/64 Emulation]	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [disabled][Disabled]：60h/64エミュレーションはサポートされません。 • [enabled][Enabled]：60h/64エミュレーションはサポートされます。 サーバーでUSB非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB Port Front]	前面パネルの USB デバイスを有効にするか無効にするか。次のいずれかになります。 • [disabled][Disabled]：前面パネルのUSB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [enabled][Enabled]：前面パネルのUSB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[USB Port Internal]	内部 USB デバイスを有効にするか無効にするか。次のいずれかになります。 • [disabled][Disabled]：内部USB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [enabled][Enabled]：内部USB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOSおよびオペレーティング システムによって検出されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB Port KVM]	vKVM ポートが有効か無効か。次のいずれかになります。 • [disabled][Disabled]：KVMキーボードとマウス デバイスをディセーブルにします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • [enabled][Enabled]：KVMキーボードとマウス デバイスをイネーブルにします。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB Port Rear]	背面パネルの USB デバイスを有効にするか無効にするか。次のいずれかになります。 • [disabled][Disabled]：背面パネルのUSB ポートをディセーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [enabled][Enabled]：背面パネルのUSB ポートをイネーブルにします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[USB Port SD Card]	SD カード ドライブを有効にするか無効にするか。次のいずれかになります。 • [disabled][Disabled]：SDカード ドライブをディセーブルにします。SD カード ドライブは、BIOS およびオペレーティング システムによって検出されません。 • [enabled][Enabled]：SDカード ドライブをイネーブルにします。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[USB Port VMedia]	仮想メディア デバイスを有効にするか無効にするか。次のいずれかになります。 • [disabled][Disabled]：vMediaデバイスをディセーブルにします。 • [enabled][Enabled]：vMediaデバイスをイネーブルにします。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[All USB Devices]	すべての物理および仮想USBデバイスを有効にするか無効にするか。次のいずれかになります。 • [disabled][Disabled]：すべてのUSBデバイスがディセーブルです。 • [enabled][Enabled]：すべてのUSBデバイスがイネーブルです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[xHCI Mode]	xHCI モードを有効または無効にします。次のいずれかになります。 • [disabled][Disabled]：xHCIモードは無効になります。 • [enabled][Enabled]：xHCIモードは有効です。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
USB Port:M.2 Storage	USB ポート:M.2 ストレージが有効か無効か。次のいずれかになります。 • **無効** — USB ポート:M.2 ストレージを無効にします。 • **有効** — USB ポート:M.2 ストレージを有効にします。これがデフォルトのオプションです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

PCI 設定の BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる PCI 設定の BIOS 設定を示しています。

名前	説明
[Maximum memory below 4GB]	PAE サポートなしで動作しているオペレーティング システムのメモリ使用率を、BIOS がシステム設定に応じて 4GB 以下で最大化するかどうか。次のいずれかになります。 • [disabled][Disabled]：メモリ使用率を最大化しません。 PAE をサポートするオペレーティング システムすべてにこのオプションを選択します。 • [enabled][Enabled]：PAEをサポートしないオペレーティング システムについて 4GB 以下でメモリ使用率を最大化します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Memory mapped IO above 4GB]	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O を有効または無効にします。レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。次のいずれかになります。 • [disabled][Disabled]：64ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [enabled][Enabled]：64 ビットPCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[VGA Priority]	システムに複数の VGA デバイスがある場合は、VGA グラフィックス デバイスの優先順位を設定できます。次のいずれかになります。 • [onboard][Onboard]：プライオリティがオンボード VGA デバイスに与えられます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [offboard][Offboard]：プライオリティがPCIE グラフィックス アダプタに与えられます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [onboard-vga-disabled][Onboard VGA Disabled]：PCIE グラフィックアダプタが優先され、オンボード VGA デバイスが無効になります。 （注） オンボード VGA がディセーブルの場合、vKVM は機能しません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） オンボード VGA デバイスのみが Cisco UCS B シリーズ サーバーでサポートされます。

名前	説明
[ASPM Support]	BIOS での ASPM（アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [disabled][Disabled]：ASPMサポートは、BIOS でディセーブルです。 • [auto][Auto]：電力状態をCPU が決定します。 • [forcel0][ForceL0]：すべてのリンクを強制的にL0 スタンバイ（L0s）状態にします。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[BME DMA Mitigation Support]	不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。 • **[Disabled]**：PCI BME ビットは BIOS で無効になっています。 • **[Enabled]**：PCI BME ビットは BIOS で有効になっています。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

QPI の BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる QPI の BIOS 設定を示しています。

名前	説明
[QPI Link Frequency Select]	Intel QuickPath Interconnect（QPI）リンク周波数（ギガトランスファー/秒（MT/s）単位）。次のいずれかになります。 • **20.0GT/s** • **16.0GT/s** • **14.4GT/s** • **12.8GT/s** • [6400][6.4GT/s] • [7200][7.2GT/s] • [8000][8.0GT/s] • [9600][9.6GT/s] • [auto][Auto]：QPIリンク周波数が CPU によって決定されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[QPI Snoop Mode]	次のいずれかになります。 • [home-snoop][HomeSnoop]：スヌープは、常に、メモリ コントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多いですが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • [cluster-on-die][ClusterOn Die]：このモードは、コアが 10 以上のプロセッサでのみ使用できます。高度にNUMA最適化されたワークロードに最適なモードです。 • [home-directory-snoop-with-osb][HomeDirectory Snoop with OSB] • [early-snoop][EarlySnoop]：分散キャッシュ リング停止で、別のキャッシングエージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードやNUMA最適化されていないワークロードに最適です。 • [auto][Auto]：QPIスヌープ モードは CPU によって決定されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

トラステッド プラットフォーム BIOS 設定

次の表に、BIOSポリシーまたはデフォルトBIOS設定を介して実行できるトラステッドプラットフォーム BIOS 設定の一覧を示します。

名前	説明
[トラステッド プラットフォーム モジュール サポート（TPM）（Trusted Platform Module Support (TPM)）]	サーバーの認証に使用するアーティファクトを安全に保存するコンポーネントであるトラステッド プラットフォーム モジュール（TPM）の有効と無効を切り替えます。次のいずれかになります。 • **無効**：TPM を無効にします。 • **有効**：TPM を有効にします。 • **プラットフォームデフォルト**：TPM を有効にします。

名前	説明
[インテル Trusted Execution Technology（TXT）サポート（Intel Trusted Execution Technology (TXT) Support）]	ビジネス サーバー上で使用され、保管される情報の保護機能を強化する、Intel Trusted Execution Technology（TXT）の有効と無効を切り替えます。次のいずれかになります。 • **無効**：TXTを無効にします。これがデフォルトのオプションです。 • **有効**：TXT を有効にします。 • **プラットフォームデフォルト**：TXT を有効にします。 TXT のみを有効にした場合でも、暗黙的に TPM、VT、および VT-d も有効になります。
[SHA-1 PCR バンク（SHA-1 PCR Bank）]	プラットフォーム構成レジスタ（PCR）は、TPM 内のメモリ位置です。複数の PCR をまとめて PCR バンクと呼びます。セキュア ハッシュ アルゴリズム 1 または SHA-1 PCR バンクでは、TPM セキュリティを有効または無効にすることができます。次のいずれかになります。 • **無効**：SHA-1 PCR バンクを無効にします。 • **有効**：SHA-1 PCR バンクを有効にします。これがデフォルトのオプションです。
[SHA-256 PCR バンク（SHA-256 PCR Bank）]	プラットフォーム構成レジスタ（PCR）は、TPM 内のメモリ位置です。複数の PCR をまとめて PCR バンクと呼びます。セキュア ハッシュ アルゴリズム 256 ビットまたは SHA-256 PCR バンクでは、TPM セキュリティを有効または無効にすることができます。次のいずれかになります。 • **無効**：SHA-256 PCR バンクを無効にします。 • **有効**：SHA-256 PCR バンクを有効にします。これがデフォルトのオプションです。
[トラステッド プラットフォーム モジュール状態（Trusted Platform Module State）]	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかになります。 • **[無効（Disabled）]** — サーバーは TPM を使用しません。 • **[有効（Enabled）]** — サーバーは TPM を使用します。これがデフォルトのオプションです。

名前	説明
[TPM 保留中の操作（TPM Pending Operation）]	トラステッド プラットフォーム モジュール（TPM）Pending Operation オプションを使用すると、保留中の操作のステータスを制御できます。次のいずれかになります。 • **[なし（None）]** — アクションはありません。これがデフォルトのオプションです。 • **TPMClear** — 保留中の操作をクリアします。

LOM および PCIe スロットの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる USB BIOS 設定の一覧を示します。

名前	説明
[PCIe Slot SAS OptionROM]	オプション ROM が SAS ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCIe Slot *n* Link Speed]	このオプションを使用すると、PCIe スロット ***n*** に装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe Slot *n* OptionROM]	オプション ROM がポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe Slot HBA OptionROM]	オプション ROM が HBA ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCIe Slot MLOM OptionROM]	オプション ROM が MLOM ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe Slot N*x* OptionROM]	オプション ROM がポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe 10G LOM 2 Link]	オプション ROM が 10G LOM ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[PCI ROM CLP]	PCI ROM Command Line Protocol（CLP）は、カード上の iSCSI や PxE などのさまざまなオプション ROM の実行を制御します。デフォルト設定は、ディセーブルです。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SIOC1 Option ROM]	システム I/O コントローラ 1（SIOC1）のオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SIOC2 Option ROM]	システム I/O コントローラ 2（SIOC2）のオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SBMezz1 Option ROM]	SBMezz1 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SBMezz2 Option ROM]	SBMezz2 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[IOESlot1 OptionROM] ドロップダウン リスト	オプション ROM が IOE スロット 1 で有効かどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[IOEMEZZ 1 OptionROM]	オプション ROM が IOE Mezz1 で有効かどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[IOE Slot2 Option ROM]	オプション ROM が IOE スロット 2 で有効かどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[IOEMEZZ 1 OptionROM]	オプション ROM が IOE NVMe1 で有効かどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[IOEMEZZ 2 OptionROM]	オプション ROM が IOE NVMe2 で有効かどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SBNVME1 Option ROM]	SBNVMe1 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
PCIe Slot MRAID-*n* OptionROM	オプション ROM が MRAID ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
PCIe Slot RAID OptionROM	オプション ROM が RAID ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
Rear NVME *n* Link Speed	このオプションでは、リア PCIe スロット *n* に取り付けられた NVME カードの最高速度を制限することができます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [enabled][Enabled]：最大速度が制限されます。 （注） • 背面 *NVME 1* リンク速度と背面 *NVME 2* リンク速度の場合、**有効**になっている値は Cisco UCS M6 サーバーではサポートされていません。 • 背面 *NVME 3* リンク スピードと背面 *NVME 4* リンク スピードの場合、**有効**になっている値を使用できますが、選択した場合、BIOS レベルでは効果がありません。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[前面 NVME *n*リンク速度（Front NVME n Link Speed）]	このオプションでは、フロントPCIeスロットに取り付けられたNVMEカードの最高速度を制限することができます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 これがデフォルトのオプションです。 • [enabled][Enabled]：最大速度が制限されます。 （注） 前面 *NVME 1* リンク速度と前面 *NVME 2* リンク速度の場合、**有効**になっている値は Cisco UCS M6 サーバーでは利用可能ですがサポートされていません。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） 前面 *Nvme 13* リンク速度から前面 *Nvme 24* リンク速度までの場合、BIOS トークンと値は使用可能ですが、選択されている場合、BIOS レベルでは効果がありません。
HBA リンク速度	このオプションでは、HBA カードの最高速度を制限することができます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
MLOM リンク速度	このオプションを使用すると MLOM アダプタの最大速度を制限できます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。 • [enabled][Enabled]：最大速度が制限されます。 （注） 値 **Enabled** は、Cisco UCS M6 サーバーではサポートされていません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
MRAID Link Speed	このオプションでは、MRAIDの最高速度を制限することができます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 • **有効** — 最大速度は、制限されていません。 （注） 値 **有効** は、Cisco UCS M6 サーバーではサポートされていません。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
RAID-*n* Link Speed	このオプションを使用すると RAID の最大速度を制限できます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[すべてのオンボード LOM（All Onboard LOM）]	すべてのオンボード LOM ポートがイネーブルであるか、ディセーブルであるか。次のいずれかになります。 • [enabled][Enabled]：すべてのオンボードLOM がイネーブルです。 • [disabled][Disabled]：すべてのオンボードLOM がディセーブルです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
LOM Port 1 OptionRom	オプション ROM が LOM ポート 1 で使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
LOM Port 2 OptionRom	オプション ROM が LOM ポート 2 で使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[Slot *n* State]	PCIe スロット *n* に取り付けられているアダプタ カードの状態。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • [uefi-only][UEFI Only]：拡張スロットはUEFI でのみ使用できます。 • [legacy-only][Legacy Only]：レガシーの場合にのみ拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SBNVMe1 OptionROM]	SBNVMe1 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SBNVMe2 OptionROM]	SBNVMe2 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SIOCNVMe1 OptionROM] リスト	SIOCNVMe1 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SIOCNVMe2 OptionROM]	SIOCNVMe2 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SBLom1 OptionROM]	SBLom1 コントローラのオプション ROM をサーバーが使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SBNVMe*n* Link Speed]	SBNVMe スロット ***n*** のリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [enabled][Enabled]：最大速度が制限されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SIOCNVMe*n* Link Speed]	SIOCNVMe スロット ***n*** のリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [enabled][Enabled]：最大速度が制限されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SIOC*n* Link Speed]	SIOC スロット ***n*** のリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [enabled][Enabled]：最大速度が制限されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SBMezz*n* Link Speed]	SBMezz スロット ***n*** のリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [enabled][Enabled]：最大速度が制限されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[IOESlot*n* Link Speed]	IOE スロット ***n*** のリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [enabled][Enabled]：最大速度が制限されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[IOEMezz*n* Link Speed]	IOEMezz スロット ***n*** のリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [enabled][Enabled]：最大速度が制限されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[IOENVMe*n* Link Speed]	IOENVMe スロット ***n*** のリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [enabled][Enabled]：最大速度が制限されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[CDN Support for LOMs]	イーサネット ネットワーキング識別子の命名規則を、Consistent Device Naming（CDN）と従来の命名規則のどちらに準拠させるかを指定します。次のいずれかになります。 • **有効**：OS イーサネット ネットワーク識別子に、LOM ポート 0 や LOM ポート 1 のように、物理的な LAN on Motherboard（LOM）のポート番号付けに基づく Consistent Device Naming（CDN）規則で名前を付けます。 • **[Disabled]**：OS イーサネット ネットワーキング識別子に、デフォルトの規則に従ってETH0、ETH1 などの名前を付けます。デフォルトで、CDN オプションはディセーブルになっています。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[VMD Enable]	PCIe バスに接続されている NVMe SSD をスワップできるかどうかを指定します。この設定により、これらのドライブの LED ステータス ライトも標準化されます。LED ステータス ライトは、特定の障害インジケータ パターンを表示するようにオプションでプログラムできます。 次のいずれかになります。 • **[Enabled]**：PCIe バスに接続されている NVMe SSD のホット スワップを許可します。 • **[Disabled]**：PCIe バスに接続されている NVMe SSD のホット スワップを禁止します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
ACS 制御 SLOT-*n* n = 11 ~ 14	アクセス コントロール サービス (ACS) を使用すると、プロセッサでは制御スロット *n* の複数のデバイス間のピアツーピア通信を有効または無効にすることができます。次のいずれかになります。 • **有効**: 制御スロット *n* の複数のデバイス間のピアツーピア通信を有効にします。 • **無効**: 制御スロット *n* の複数のデバイス間のピアツーピア通信を無効にします。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
PCIe スロット GPU*n* OptionROM 次の場合のみ Cisco UCS C480 M5 ML サーバー	GPU スロット *n* のオプション ROM が有効かどうか。*n* は、1 ~ 8 のスロット番号です。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
ACS 制御 GPU-*n* n = 1 ~ 8	アクセス コントロール サービス (ACS) を使用すると、プロセッサでは GPU の複数のデバイス間のピアツーピア通信を有効または無効にすることができます。次のいずれかになります。 • **無効**: GPU の複数のデバイス間のピアツーピア通信を有効にします。 • **有効**: GPU の複数のデバイス間のピアツーピア通信を無効にします。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[PCIe PLL SSC]ドロップダウンリスト	クロックを 0.5% ダウンスプレッドすることで EMI 干渉を低減します。 拡散せずにクロックを集中化するには、この機能を無効にします。 すべての Cisco UCS M5 と M6 サーバーの場合、このオプションはデフォルトで無効になっています。 • **無効**：クロックは拡散せずに集中化されます。 • **自動**：EMI干渉は自動調整されます。 • **ZeroPointFive**：クロックを0.5%ダウンスプレッドすることでEMI干渉を低減します。 • **プラットフォームのデフォルト**—BIOSは、サーバータイプおよびベンダーの BIOS デフォルトに含まれるこの属性の値を使用します。
Front Nvme*n* OptionROM	このオプションでは、SSD:NVMeスロット*n*に接続されたPCIeアダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • **[有効]** — これは、デフォルト オプションです。 • [disabled][Disabled]

名前	説明
[PCIe スロット n リンク速度（PCIe Slot*n* Link Speed）]	スロット *n* で指定された PCIe スロットのリンク速度。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。
MSTOR-RAID リンクスピード	このオプションを使用すると MSTOR アダプタの最大速度を制限できます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。 （注） この BIOS 設定 *MSTOR-RAID* リンク速度では、トークンと値を使用できますが、選択しても BIOS レベルには影響しません。
MSTOR-RAID OptionROM	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかが考えられます。 • **無効** — オプション ROM は使用できません。 • **有効** — Option ROM これがデフォルトのオプションです。
MLOM OptionROM	オプション ROM が MLOM ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。

名前	説明
MRAID OptionROM	オプション ROM が MRAID ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。
Rear Nvme *n* OptionRom	オプション ROM が背面 NVME*n* ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
PCIe slot MSTOR Link Speed	このオプションを使用すると MSTOR アダプタの最大速度を制限できます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 これがデフォルトのオプションです。 • [disabled][Disabled]：最大速度は制限されません。
PCIe Slot MSTOR RAID OptionROM	サーバが PCIe MSTOR RAID のオプション ROM を使用するかどうか。次のいずれかが考えられます。 • **無効** — オプション ROM は使用できません。 • **有効** — Option ROM これがデフォルトのオプションです。
PCIe RAS Support	PCIe RAS サポートが PCIe スロットで使用可能かどうか。次のいずれかになります。 • **無効** — PCIe RAS はスロットで使用可能です。 • **有効** — PCIe RAS はスロットで使用できません。これがデフォルトのオプションです。

名前	説明
MRAID*n* Link Speed	このオプションでは、MRAIDの最高速度を制限することができます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • **Gen 4** — 最大 16GT/s までの速度が許可されます。 • [auto][Auto]：最大速度は自動的に設定されます。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
MRAID*n* OptionROM	オプション ROM が MRAID ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。
NVME-*n* OptionROM	オプション NVME がポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。

名前	説明
PCIe スロット OCP リンク速度	このオプションを使用すると OCP の最大速度を制限できます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [auto][Auto]：最大速度は自動的に設定されます。 これがデフォルトのオプションです。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
RAID*n* OptionROM	オプション ROM が RAID ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。
IOENVMe*n* OptionROM	オプション ROM が IOENVMe ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。
GPU*n* OptionRom	オプション ROM が GPU ポートで使用できるかどうか。次のいずれかになります。 • [disabled][Disabled]：拡張スロットを使用できません。 • [enabled][Enabled]：拡張スロットを使用できます。 これがデフォルトのオプションです。

名前	説明
RAID リンク速度	このオプションを使用すると RAID の最大速度を制限できます。次のいずれかになります。 • [gen1][Gen 1]：最大速度が2.5 GT/s（ギガ転送/秒）になります。 • [gen2][Gen 2]：最大速度が5 GT/s になります。 • [gen3][Gen 3]：最大速度が8 GT/s になります。 • [auto][Auto]：最大速度は自動的に設定されます。 これがデフォルトのオプションです。 • **有効** — 最大速度は、制限されていません。 （注） 値 **有効** は、Cisco UCS M6 サーバーではサポートされていません。 • [disabled][Disabled]：最大速度は制限されません。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

グラフィック設定の BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるグラフィック設定の BIOS 設定の一覧を示します。

名前	説明
[Integrated Graphics]	統合グラフィックスをイネーブルにします。次のいずれかになります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
Integrated Graphics Aperture Size	統合グラフィックス コントローラのマップド メモリのサイズを設定できます。次のいずれかになります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
Onboard Graphics	オンボードグラフィックス（KVM）をイネーブルにします。次のいずれかになります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

ブート オプションの BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるブート オプションの BIOS 設定を示しています。

名前	説明
[ブート オプションの再試行（Boot Option Retry）]	BIOS でユーザー入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。次のいずれかになります。 • [ディセーブル]: ユーザ入力を待機してから非EFIベースのブートオプションを再試行します。これがデフォルトのオプションです。 • [イネーブル]: ユーザ入力を待機せずに非EFIベースのブートオプションを継続的に再試行します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[SAS RAID]	Intel SAS Entry RAID モジュールがイネーブルかどうか。次のいずれかになります。 • [ディセーブル]: Intel SAS Entry RAIDモジュールはディセーブルです。 • [イネーブル]: Intel SAS Entry RAIDモジュールはイネーブルです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[SAS RAID module]	Intel SAS Entry RAID モジュールがどのように設定されるか。次のいずれかになります。 • [it-ir-raid]：Intel IT/IR RAID を使用するよう RAID モジュールを設定します。 • [intel-esrtii]：Intel Embedded Server RAID Technology II を使用するよう RAID モジュールを設定します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[オンボード SCU ストレージ サポート（Onboard SCU Storage Support）] ドロップダウンリスト	オンボード ソフトウェア RAID コントローラをサーバーで使用できるかどうか。次のいずれかになります。 • [ディセーブル]: ソフトウェアRAIDコントローラを使用できません。 • [イネーブル]: ソフトウェアRAIDコントローラを使用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[冷却時間(秒)（Cool Down Time (sec)）]	次のブート試行までの待機時間（秒単位）。次のいずれかになります。 • [15]：次のブートを試行するまで、システムは 15 秒間待機します。 • [45]：次のブートを試行するまで、システムは 45 秒間待機します。 • **[90]** — 次のブートを試行するまで、システムは 90 秒間待機します。これがデフォルトのオプションです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 このトークンは、[Boot Option Retry] トークンがイネーブルになっている場合にのみ有効になります。

名前	説明
[再試行数（Number of Retries）]	ブートの試行回数。次のいずれかになります。 • **[無制限（Infinite）]** — システムは起動のすべてのオプションを試行します。 • [13]：システムは起動を 13 回試みます。これがデフォルトのオプションです。 • **[5]** — システムは起動を 5 回試みます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[P-SATA モード (P-SATA Mode)]	このオプションでは、P-SATA モードを選択できます。次のいずれかになります。 • [disabled][Disabled]：P-SATAモードは無効になります。 • [lsi-sw-raid][LSI SW RAID]：LSI SW RAID の場合、SATA コントローラと sSATA コントローラの両方を RAID モードに設定します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[電源オン パスワード（Power On Password）]	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、BIOS 関数（IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへのブート）にアクセスする前にパスワードの検証が必要になります。次のいずれかを指定できます。 • [disabled][Disabled]：電源オンパスワードは無効になります。 • [enabled][Enabled]：電源オン パスワードが有効になります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[IPV6 PXE サポート（IPV6 PXE Support）]	PXE の IPv6 サポートを有効または無効にします。次のいずれかになります • [無効（disabled）][無効（Disabled）]：IPV6PXE のサポートは利用できません。 • [enabled][Enabled]：IPV6PXE のサポートを常に利用できます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[アダプティブ メモリ トレーニング（Adaptive Memory Training）]	このトークンが有効になっているときに、BIOS はCPU/メモリ設定情報と共にメモリ トレーニング結果(最適化されたタイミング/電圧値) を保存し、それらをその後のリブートに再使用して、ブート時間を短縮します。保存済みメモリのトレーニング結果は、最後の保存操作後の 24 時間以内に、リブートが発生した場合にのみ使用されます。次のいずれかになります。 • **無効になっています**:**適応型のメモリ トレーニング**が無効になっています。 • **Enabled**—**適応型のメモリ トレーニング**が有効になっています。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
BIOS Tech メッセージ レベルのコントロール(C125 M5)	このトークンを有効にするには、出力レベルより細かく制御が BIOS Tech ログが使用できます。これにより、冗長であるか、あまり使用しない BIOS Tech ログ メッセージの数が減少します。次のいずれかになります。 • **Disabled**—**BIOS Techlog レベル**が無効になっています。 • **Enabled**—**BIOS Techlog レベル**が有効になっています。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[OptionROM起動最適化（OptionROM Launch Optimization）]	オプション ROM の起動は PCI スロット レベルで管理されます。デフォルトで有効になっています。多数のネットワーク コントローラおよびオプション ROM をもつストレージHBA から成る設定では、すべてのオプション ROM は、PCI スロットのオプション ROM コントロールがすべてに対して有効になっている場合に起動できます。ただし、ブートプロセスでは、コントローラのサブセットのみを使用できます。このトークンが有効になっているときに、ブート ポリシーに存在するこれらのコントローラでのみ、オプション ROM が起動されます。次のいずれかになります。 • **Disabled—OptionROM 起動最適化** が無効です。 • **Enabled—OptionROM 起動最適化**が有効になっています。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[BIOS Techlog レベル（BIOS Techlog Level）]	このオプションは、**BIOS tech ログファイル**のメッセージのタイプを示します。ログファイルには、次のタイプのいずれかを指定できます。 • **[最小（Minimum）]**：Critical messages will be displayed in the log file.重要なメッセージがログファイルに表示されます。これがデフォルトのオプションです。 • **[標準（Normal）]**：警告およびロード メッセージがログファイルに表示されます。. • **[最大（Maximum）]**：標準に加え、情報関連のメッセージがログファイルに表示されます。

名前	説明
[P-SATA OptionROM]	このオプションでは、P-SATA モードを選択できます。次のいずれかになります。 • [lsi-sw-raid][LSI SW RAID]：LSI SW RAID の場合、SATA コントローラと sSATA コントローラの両方を RAID モードに設定します。これがデフォルトのオプションです。 • [disabled][Disabled]：P-SATAモードは無効になります。 • **AHCI** — コントローラを AHCI モードに設定します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[M.2 SATA OptionROM]	このオプションでは、P-SATA モードを選択できます。次のいずれかになります。 • [lsi-sw-raid][LSI SW RAID]：LSI SW RAID の場合、SATA コントローラと sSATA コントローラの両方を RAID モードに設定します。これがデフォルトのオプションです。 • [disabled][Disabled]：P-SATAモードは無効になります。 • **AHCI** — コントローラを AHCI モードに設定します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[UEFI ブート モード（UEFI Boot Mode）]	このオプションでは、UEFI ブート モードを選択できます。次のいずれかになります。 • **[無効（Disabled）]** — UEFI ブートモードが無効になっています。 • **[有効（Enabled）]** — UEFI ブートモードが有効になっています。

（注） Cisco UCS Manager の BIOS パラメータ仮想化機能により、統合された一連のサービス プロファイルの BIOS 設定を実際の BIOS サポート パラメータにマッピングします。ただし、すべての BIOS 設定項目がすべてのサーバー モデルやプラットフォームに適用できるわけではありません。カスタム BIOS ポリシーを作成し、**[ブート オプション再試行（Boot Option Retry）]** を選択したときに、ブート可能なオプションがない場合は、Cisco UCS B420 M4 サーバーのリブートは失敗し、Cisco UCS Manager は次のメッセージを表示します：*[Reboot and Select proper Boot device or Insert Boot Media in selected Boot device and press a key*（再起動して適切な起動デバイスを選択するか、選択した起動デバイスに起動メディアを挿入して、キーを押してください）*]*。ブート パスを修正した後には、手動でブート オプションを設定して、サーバーが停電の後にリブートできるようにしておく必要があります。BIOS デフォルト サーバーのポリシー、および BIOS オプションとそのデフォルト設定の詳細については、BIOS ポリシー （341 ページ）およびサーバー BIOS 設定 （222 ページ）を参照してください。

サーバー管理 BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できるサーバー管理 BIOS 設定の一覧を示します。

一般設定

名前	説明
[Assert NMI on SERR]	システム エラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。次のいずれかになります。 • **[Disabled]**：SERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • **[Enabled]**：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。[Assert NMI on PERR] を有効にする場合は、この設定を有効にする必要があります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Assert NMI on PERR]	プロセッサバスパリティエラー（PERR）の発生時に、BIOSがマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。次のいずれかになります。 • **[Disabled]**：PERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • **[Enabled]**：PERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。この設定を使用するには、[Assert NMI on SERR] をイネーブルにする必要があります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[OS Boot Watchdog Timer Policy]	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • [power-off][Power Off]：OS ブート中にウォッチドッグ タイマーが期限切れになった場合、サーバーは電源オフになります。 • [reset][Reset]：OSのブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にだけ利用できます。

名前	説明
[OS Boot Watchdog Timer Timeout]	BIOS でウォッチドッグ タイマーの設定に使用されるタイムアウト値。次のいずれかになります。 • [5-minutes]：ウォッチドッグ タイマーはOSブート開始から 5 分後に期限切れになります。 • [10-minutes]：ウォッチドッグ タイマーは OS ブート開始から 10 分後に期限切れになります。 • [15-minutes]：ウォッチドッグ タイマーは OS ブート開始から 15 分後に期限切れになります。 • [20 分（20-minutes）]：ウォッチドッグ タイマーはOSブート開始から20分後に期限切れになります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にだけ利用できます。
[FRB-2 タイマー（FRB-2 Timer）]	POST 中にシステムがハングした場合に、システムを回復するために FRB-2 タイマーが使用されるかどうか。次のいずれかになります。 • **[Disabled]**：FRB-2 タイマーは使用されません。 • **[Enabled]**：POST 中に FRB-2 タイマーが開始され、必要に応じてシステムの回復に使用されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

コンソール リダイレクション設定

名前	説明
[Console redirection]	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションで使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションの関連性はなくなり、無効になります。次のいずれかになります。 • **[Disabled]**：POST 中にコンソール リダイレクションは発生しません。 • **COM 0**：POST 中にコンソール リダイレクション陽のシリアルポートを有効にします。このオプションは M6 ブレード サーバーおよびラックマウント サーバーに対してのみ有効です。 （注） 値 **serial-port-a** は、M6 サーバーではサポートされていません。 • **[serial-port-b]** または **[COM 1]**：POST 中のコンソール リダイレクション用にシリアル ポート B を有効にし、サーバー管理タスク実行を許可します。このオプションは、ラックマウント サーバーでのみ有効です。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） このオプションを有効にする場合は、POST 中に表示される Quiet Boot のロゴ画面を無効にします。

名前	説明
[Flow Control]	フロー制御にハンドシェイク プロトコルを使用するかどうかを設定します。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレーム コリジョンを減らすことができます。次のいずれかになります。 • **[None]**：フロー制御は使用されません。 • **RTS-CTS**：RTS/CTS がフロー制御に使用されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[Baud rate]	シリアル ポートの伝送速度として使用されるボー レート。[Console Redirection] を無効にする場合は、このオプションを使用できません。次のいずれかになります。 • **[9.6k]**：9600 ボー レートが使用されます。 • **[19.2k]**：19200 ボー レートが使用されます。 • **[38.4k]**：38400 ボー レートが使用されます。 • **[57.6k]**：57600 ボー レートが使用されます。 • **[115.2k]**：115200 ボー レートが使用されます。これがデフォルトのオプションです。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[Terminal type]	コンソール リダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 • **[PC-ANSI]**：PC-ANSI 端末フォントが使用されます。 • **[VT100]**：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • **[VT100-PLUS]**：サポートされている vt100-plu ビデオ端末とその文字セットが使用されます。 • **[VT-UTF8]**：UTF-8 文字セットのビデオ端末が使用されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[Legacy OS redirection]	シリアル ポートでレガシーなオペレーティング システム（DOS など）からのリダイレクションを有効にするかどうか。次のいずれかになります。 • **[Disabled]**：コンソール リダイレクションがイネーブルになっているシリアル ポートは、レガシーなオペレーティング システムから認識されません。 • **[Enabled]**：コンソール リダイレクションがイネーブルになっているシリアル ポートはレガシー オペレーティング システムに表示されます。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Putty KeyPad] **set console-redir-config putty-function-keypad**	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • **[VT100]**：ファンクション キーによって **ESC OP** ～ **ESC O[** を生成します。 • **[LINUX]**：Linux 仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は **ESC [[A** ～ **ESC [[E** を生成します。 • **[XTERMR6]**：ファンクション キー F5 ～ F12 がデフォルトモードと同様に動作します。ファンクション キー F1 ～ F4 によって ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • **[SCO]**：ファンクション キー F1 ～ F12 が **ESC [M** ～ **ESC [X** を生成します。ファンクション キーと Shift キーによって **ESC [Y** ～ **ESC [j** を生成します。Ctrl キーとファンクション キーによって **ESC [k** ～ **ESC [v** を生成します。Shift、Ctrl およびファンクション キーによって **ESC [w** ～ **ESC [{** を生成します。 • [escn][ESCN]：デフォルトモードです。 ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーによって **ESC [11~** や **ESC [12~** などのシーケンスを生成します。 • **[VT400]**：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーによって **ESC OP** ～ **ESC OS** を生成します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[アウトオブバンド管理（Out of Band Management）]	Windows の Special Administration Control（SAC）で使用。このオプションを使用すると、Windows 緊急管理サービスに使用できる COM ポート 0 を設定できます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [disabled][Disabled]：Windows オペレーティング システムで使用する汎用ポートとして COM ポート 0 を設定します。 • [enabled][Enabled]：Windows 緊急管理サービスのリモート管理ポートとして COM ポート 0 を設定します。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[BIOS POST 後のリダイレクション（Redirection After BIOS POST）]	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • [always_enable][Always Enable]：OS ブート時と実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [bootloader][Bootloader]：OS ブート ローダに制御が渡される前に BIOS レガシー コンソール リダイレクションが無効になります。 • **[Platform Default]**[platform-default]：BIOS は、サーバ タイプとベンダーの BIOS デフォルト値に含まれるこの属性の値を使用します。
[OS ウォッチドッグ タイマー ポリシー（OS Watchdog Timer Policy）]	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。 • **Power_Off**：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバーの電源がオフになります。これがデフォルトのオプションです。 • [reset][Reset]：OSのブート中にウォッチドッグ タイマーが切れた場合、サーバーはリセットされます。

名前	説明
[FRB-2 タイマー（FRB 2 Timer）]	POST 中にシステムがハングアップした場合に、システムを回復するために FRB2 タイマーを使用するかどうかを指定します。次のいずれかになります。 • **Disabled**：FRB-2 タイマーは使用しません。 • **Enabled**：POST 中に FRB-2 タイマーが開始され、必要に応じてシステムの回復に使用されます。これがデフォルトのオプションです。
OS ウォッチドッグ タイマー	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [disabled][Disabled]：サーバーのブートにかかる時間のトラッキングにウォッチドッグ タイマーは使用されません。これがデフォルトのオプションです。 • [enabled][Enabled]：サーバーのブートにかかる時間をウォッチドッグタイマーでトラッキングします。これがデフォルトのオプションです。
OSウォッチドッグタイマータイムアウト	OSが指定された時間内にブートしない場合、OSウォッチドッグ タイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。次のいずれかになります。 • **5 Minutes**—OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • **10 Minutes**—OS ウォッチドッグ タイマーは、ブートが開始されてから10分後に期限が切れます。これがデフォルトのオプションです。 • **15 Minutes**—OS ウォッチドッグ タイマーは、ブートが開始されてから 15 分後に期限が切れます。 • **20 Minutes**—OS ウォッチドッグ タイマーは、ブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは、OS ウォッチドッグ タイマーをイネーブル化した場合にのみ適用されます。

BIOS ポリシー

BIOS ポリシーは、サーバーまたはサーバー グループに対する BIOS 設定の設定を自動化するポリシーです。ルート組織内のすべてのサーバーに対して使用可能なグローバル BIOS ポリシーを作成するか、サブ組織の階層に対してのみ使用可能な BIOS ポリシーを作成できます。

BIOS ポリシーを使用するには、次の手順を実行します。

1. Cisco UCS Manager で BIOS ポリシーを作成します。
2. BIOS ポリシーを 1 つ以上のサービス プロファイルに割り当てます。
3. サービス プロファイルをサーバーと関連付けます。

サービス プロファイルの関連付け時に、Cisco UCS Manager はサーバー上の BIOS 設定を BIOS ポリシー内の設定と一致するように変更します。BIOS ポリシーを作成せず、BIOS ポリシーをサービス プロファイルに割り当てていない場合は、サーバーの BIOS 設定にそのサーバー プラットフォームのデフォルトが使用されます。

デフォルトの BIOS 設定

Cisco UCS Manager には、Cisco UCS がサポートするサーバーの各タイプのためのデフォルト BIOS 設定が含まれています。デフォルト BIOS 設定は、ルート組織だけで使用でき、グローバルです。Cisco UCS でサポートされている各サーバー プラットフォームには、1 セットの BIOS 設定のみを適用できます。デフォルト BIOS 設定は変更できますが、デフォルト BIOS 設定の追加セットの作成はできません。

デフォルト BIOS 設定の各セットは、サポートされているサーバーの特定のタイプに合わせて設計されており、サービス プロファイルに BIOS ポリシーが含まれていない、特定のタイプのすべてのサーバーに適用されます。

サーバー固有の設定が満たされない特定の要件が Cisco UCS 実装にあるのでない限り、Cisco UCS ドメイン内のサーバーの各タイプ用に設計されたデフォルト BIOS 設定を使用することをお勧めします。

Cisco UCS Manager により、これらのサーバー プラットフォーム固有の BIOS 設定が次のように適用されます。

- サーバーに関連付けられたサービス プロファイルには、BIOS ポリシーは含まれません。
- BIOS ポリシーには、特定の設定に対するプラットフォーム デフォルトのオプションが設定されます。

Cisco UCS Manager によって提供されるデフォルト BIOS 設定は変更できます。ただし、デフォルトの BIOS 設定に対する変更は、その特定のタイプまたはプラットフォームのすべてのサーバーに適用されます。特定のサーバーの BIOS 設定のみを変更する場合は、BIOS ポリシーを使用することを推奨します。

M5 サーバー以降の BIOS トークンは読み取り専用であり、変更することはできません。BIOS トークン、デフォルト値、および値の完全な最新リストについては、[Cisco UCS M5 Server BIOS Tokens] を参照してください。

M6 サーバー以降の BIOS トークンは読み取り専用であり、変更することはできません。BIOS トークン、デフォルト値、および値の完全な最新リストについては、「Cisco UCS M6 Server BIOS Tokens」を参照してください。

BIOS ポリシーの作成

（注） Cisco UCS Manager は、BIOS ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。これらの変更はバッファ内にとどまり、サーバーがリブートされるまでは有効になりません。

設定するサーバーで BIOS 設定のサポートを確認することをお勧めします。RAS メモリのミラーリング モードなどの一部の設定は、すべての Cisco UCS サーバーでサポートされているわけではありません。

手順

ステップ 1 [ナビゲーション]ペインで、[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 [BIOS Policies] を右クリックして [Create BIOS Policy] を選択します。

ステップ 5 [Create BIOS Policy] ウィザードの [Main] ページで [名前（Name）] フィールドに BIOS ポリシーの名前を入力します。

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

ステップ 6 [BIOS ポリシーの作成（Create BIOS Policy）] ウィザードで、次の手順を実行して BIOS 設定を実行します。

a) BIOS 設定を変更する場合は、該当するオプション ボタンをクリックするか、ドロップダウン リストから適切な項目を選択します。

各 BIOS 設定のオプションに関する説明および情報については、次のトピックを参照してください。

- **[Main]** ページ：メイン BIOS 設定 （222 ページ）
- **[詳細（Advanced）]** ページ：メイン BIOS 設定 （222 ページ）
- **[Processor]** ページ：プロセッサのBIOS設定 （225 ページ）

- **[Intel 向け I/O BIOS（IO BIOS for Intel）]** ページ： Intel 向け I/O BIOS 設定 （269 ページ）
- **[AMD 向け I/O BIOS（IO BIOS for AMD）]** ページ：AMD 向け I/O BIOS 設定 （271 ページ）
- **RAS Memory** ページ：RAS メモリの BIOS 設定 （273 ページ）
- **[Serial Port]** ページ：シリアル ポートの BIOS 設定 （291 ページ）
- **[USB]** ページ：USB BIOS 設定 （291 ページ）
- **[PCI Configuration]** ページ：PCI 設定の BIOS 設定 （297 ページ）
- **[QPI]** ページ：QPI の BIOS 設定 （299 ページ）
- **[LOM および PCIe スロット（LOM and PCIe Slots）]** サブタブ：LOM および PCIe スロットの BIOS 設定 （303 ページ）
- **[トラステッド プライバシー（Trusted Platform）]** サブタブ：トラステッド プラットフォーム BIOS 設定 （301 ページ）
- **[グラフィックス構成（Graphics Configuration）]** サブタブ：グラフィック設定の BIOS 設定 （325 ページ）
- **[Boot Options]** ページ：ブート オプションの BIOS 設定 （326 ページ）
- **[Server Management]** ページ：サーバー管理 BIOS 設定 （332 ページ）

b) 各ページの後に [Next] をクリックします。

ステップ 7 ポリシーの BIOS 設定がすべて完了したら、[Finish] をクリックします。

BIOS のデフォルトの修正

設定するサーバーで BIOS 設定のサポートを確認することをお勧めします。RAS メモリのミラーリング モードなどの一部の設定は、すべての Cisco UCS サーバーでサポートされているわけではありません。

サーバー固有の設定が満たされない特定の要件が Cisco UCS 実装にあるのでない限り、Cisco UCS ドメイン内のサーバーの各タイプ用に設計されたデフォルト BIOS 設定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、[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 [BIOS Defaults] を展開して、デフォルトの BIOS 設定を変更するサーバのモデル番号または希望のポリシーを選択します。

ステップ 5 [Work] ペインで該当するタブをクリックしてから、必要なオプション ボタンをクリックするか、ドロップダウン リストから選択してデフォルトの BIOS 設定を変更します。

各 BIOS 設定のオプションに関する説明および情報については、次のトピックを参照してください。すべての BIOS 設定がサーバの各タイプに使用できるわけではありません。

- **[Main]** タブ：メイン BIOS 設定 （222 ページ）
- [Advanced] タブ：
  - **[Processor]** サブタブ：プロセッサのBIOS設定 （225 ページ）
  - **[Intel 向け I/O BIOS（IO BIOS for Intel）]** サブタブ： Intel 向け I/O BIOS 設定 （269 ページ）
  - **[AMD 向け I/O BIOS（IO BIOS for AMD）]** ページ：AMD 向け I/O BIOS 設定 （271 ページ）
  - **[RAS Memory]** サブタブ：RAS メモリの BIOS 設定 （273 ページ）
  - **[Serial Port]** サブタブ：シリアル ポートの BIOS 設定 （291 ページ）
  - **[USB]** サブタブ：USB BIOS 設定 （291 ページ）
  - **[PCI Configuration]** サブタブ：PCI 設定の BIOS 設定 （297 ページ）
  - QPI サブタブ: QPI の BIOS 設定 （299 ページ）
  - **[LOM および PCIe スロット（LOM and PCIe Slots）]** サブタブ：LOM および PCIe スロットの BIOS 設定 （303 ページ）
  - **[トラステッド プライバシー（Trusted Platform）]** サブタブ：トラステッド プラットフォーム BIOS 設定 （301 ページ）
  - **[グラフィックス構成（Graphics Configuration）]** サブタブ：グラフィック設定の BIOS 設定 （325 ページ）
- **[Boot Options]** タブ：ブート オプションの BIOS 設定 （326 ページ） ブート オプションの BIOS 設定 （326 ページ）
- **[Server Management]** タブ：サーバー管理 BIOS 設定 （332 ページ） サーバー管理 BIOS 設定 （332 ページ）

ステップ 6 **[Save Changes]**をクリックします。

サーバの実際の BIOS 設定の表示

サーバーの実際の BIOS 設定を表示するには、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、[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 実際の BIOS 設定を表示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 [BIOS Settings] 領域で、見出しの右側にある [Expand] アイコンをクリックして領域を開きます。

[BIOS Settings] 領域の各タブに、そのサーバ プラットフォームの設定が表示されます。いくつかのタブには追加情報を含むサブタブがあります。

メモリ RAS 機能

Intel® Xeon®プロセッサは、BIOS 経由で追加の RAS メモリ機能をサポートします。これらの機能は、メモリ DIMM のパフォーマンスと信頼性を向上させるために、プロセッサの機能を拡張します。

Post-Package Repair (PPR)

Post Package Repair (PPR) を使用すると、システムのブート時に検出された障害のある行を、DDR4 DRAM 内のスペアの行で置き換えることができます。Cisco UCS M5 および M6 プラットフォームはハード PPR を適用します。ハード PPR では、修復は永続的です。障害が発生した行への再マッピングを元に戻すことはできません。再マッピングは、電源の取り外し後も維持されます。PPR イベントが発生した場合、プラットフォーム ファームウェアは、修復を有効にするためにシステムの再起動が行われるよう、障害が発生したことを顧客に知らせます。

DRAM バンクのスペアの行の数は、DIMM の製造会社およびモデルによって異なります。PPR イベントの実行後に使用可能なスペア行は、プラットフォーム ファームウェアには表示されません。これにより、プラットフォーム ファームウェアの可視性で使用可能なすべてのスペア行が使用されると、修復が有効にならず、同じ DIMM でメモリエラーが発生する可能性があります。

Post Package Repair の有効化

有効にすると、修復プロセスは取消不能になります。

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 **[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 [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 5 **[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 6 メインの作業ペインで、**[アドバンスト (Advanced)]** タブを選択し、**[RAS メモリ (RAS Memory)]** タブを選択します。

ステップ 7 システム ブート中に検出された障害のあるセル領域の自動修復を有効にするには、**[PPR タイプ設定の選択 (Select PPR Type Configuration)]** で **[Hard PPR]** を選択します。

ステップ 8 **[Save Changes]**をクリックします。

提示されたメモリの制限

ユーザーに表示されるメモリの量は、BIOS で制限できます。システムに高容量DIMMモジュールが完全に装着されている場合は、実際に使用されるメモリ量を減らすことが望ましい場合があります。

メモリ制限は、取り付けられている使用可能なすべての DIMM で可能な限り均等に適用されます。指定できる提供メモリの最小量は 1 GB です。次のパラメータが適用されます。

0 = 制限なし。取り付けられているメモリの量がすべて表示されます。

1 ~ 2^{31} -1 = 提示されたメモリのサイズ (GB)

実際に提示されるメモリ サイズは、常に指定されたメモリ サイズに等しいか、それよりも小さくなります。

メモリ サイズの制限

実際に提示されるメモリ サイズは、常に指定されたメモリ サイズに等しいか、それよりも小さくなります。

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 **[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 [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 5 **[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 6 メインの作業ペインで、**[アドバンスト (Advanced)]** タブを選択し、**[RAS メモリ (RAS Memory)]** タブを選択します。

ステップ 7 ミラーリングする提供メモリの量を制限するには、[**Memory Size limit**] (gb) に移動し、ユーザに提示する必要があるメモリ量の値 (gb) を入力します。

ステップ 8 **[Save Changes]**をクリックします。

部分メモリのミラーリング

DIMM がアドバンスト RAS 機能の場合は、部分的なメモリ ミラーリング。ゴールドおよびプラチナナム SKU CPU のみがこの機能をサポートしています

部分的な DIMM ミラーリングによって完全なミラー コピーを保持するのではなく、メモリ セルの特定の領域のミラーコピーが作成されます。部分的なメモリのミラーリングは、BIOS ポリシーのセットアップ メニューまたは Linux オペレーティング システムから実行できます。部分的なミラーリングでは、部分的なミラーコピーの属性を使用して、メモリ マップにミラー領域が作成されます。最大 4 個の部分的なミラーを使用して、合計メモリ容量の最大 50% をミラーリングできます。

ミラーリングの場合、各 IMC に少なくとも 2 個の DDR チャネルを装着する必要があります。部分的なミラーリングでは、最大 4 個のミラー リージョンを持つ、IMC あたり 1 個の DDR4 ミラー リージョンがサポートされます。

双方向チャネル インターリーブでは、2 個のチャネルが各 IMC に入力されます。3 方向チャネル インターリーブでは、3 個のチャネルが各 IMC に入力されます。

部分的なミラーリングは、ランクのスペアリングと ADDDC との互換性がありません。

部分的なミラーリングには、次のルールが適用されます。

- DIMM の装着は、ミラーリングされたチャネルで同一である必要があります。
- ミラー ペアは、IMC DDR チャネル内の同じ M2M 内にある必要があります。
- 1 個の iMC 内の DDR4 部分的なミラー リージョンは、双方向チャネルのインターリーフまたは 3 方向チャネル インターリーブのいずれかである必要があります。2 および 3 方向チャネルのインターリーフを混在させることはできません。ミラー リージョンが iMCs をまたがる場合、チャネルのインターリーフは同じである必要があります。

部分メモリのミラーリングの有効化

部分的な DIMM メモリ ミラーリングの量は、使用可能なメモリ リソースまたはギガバイト単位のいずれかの割合で設定できます。

始める前に

（注） 部分的なメモリ ミラー モードは、標準のミラーリング モードとは相互に排他的です。

部分的なミラーリングは、ランクのスペアリングと ADDDC との互換性がありません。これらが選択されていないことを確認します。

手順

ステップ 1 [ナビゲーション]ペインで、[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 [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 5 **[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 6 メインの作業ペインで、**[アドバンスト (Advanced)]** タブを選択し、**[RAS メモリ (RAS Memory)]** タブを選択します。

ステップ 7 **[メモリ RAS 設定 (MEMORY RAS Configuration)]** に移動し、ドロップダウン リストから **[部分的なミラー モード 1LM (Partial Mirror Mode 1LM)]** を選択します。

ステップ 8 部分的なミラーを割合で設定するには、**[部分的なメモリ ミラー モード (Partial Memory Mirror Mode)]**に移動し、ドロップダウンから **[割合 (Percentage)]** を選択します。

ステップ 9 **[部分的なミラーの割合 (Partial Mirror percentage)]** に移動し、ミラーリングするメモリの目的の割合を表す 0.01 ~ 50.00 の値を入力します。

ステップ 10 部分的なミラーをギガバイトで設定するには、**[部分的なメモリ ミラー モード (Partial Memory Mirror Mode)]**に移動し、ドロップダウンから **[GB の値 (Value in GB)]** を選択します。

ステップ 11 **[部分的なミラー 1 (Partial Mirror 1)]** の [制限 (limit)] フィールドに表示されるメモリの 1 ~ GB の範囲の値を入力します。

ステップ 12 必要に応じて、追加の値を **[部分的なミラー 2 (Partial Mirror 2)]**、**[部分的なミラー 3 (Partial Mirror 3)]**、および **[部分的なミラー 4 (Partial Mirror 4)]** に入力します。これらのミラーに入力された合計値は、使用可能な合計メモリを超えることはできません。

ステップ 13 **[Save Changes]**をクリックします。

次のタスク

システムをリブートします。

トラステッド プラットフォーム モジュール

トラステッド プラットフォーム モジュール

トラステッド プラットフォーム モジュール（TPM）は、サーバーの認証に使用するアーティファクトを安全に保存できるコンポーネントです。これらのアーティファクトには、パスワード、証明書、または暗号キーを収録できます。プラットフォームが信頼性を維持していることを確認するうえで効果的なプラットフォームの尺度の保存でも、TPM を使用できます。すべての環境で安全なコンピューティングを実現するうえで、認証（プラットフォームがその表明どおりのものであることを証明すること）および立証（プラットフォームが信頼でき、セキュリティを維持していることを証明するプロセス）は必須の手順です。これは Intel の Trusted Execution Technology（TXT）セキュリティ機能の要件であり、TPM を搭載したサーバーの BIOS 設定で有効にする必要があります。Cisco UCS M4 以降のブレード サーバーとラックマウント サーバは TPM をサポートしています。TPM はこれらのサーバーでデフォルトで有効になっています。

重要

- Cisco UCS Manager をリリース 2.2(4) 以降にアップグレードすると、TPM が有効になります。
- TPM が有効な状態で Cisco UCS Manager をリリース 2.2(4) からダウングレードすると、TPM が無効になります。

Intel Trusted Execution Technology

Intel Trusted Execution Technology（TXT）を使用すると、ビジネス サーバー上で使用および保管される情報の保護機能が強化されます。この保護の主要な特徴は、隔離された実行環境および付随メモリ領域の提供にあり、機密データに対する操作をシステムの他の部分から見えない状態で実行することが可能になります。Intel TXT は、暗号キーなどの機密データを保管できる封印されたストレージ領域を提供し、悪意のあるコードからの攻撃時に機密データが漏洩するのを防ぐために利用できます。Cisco UCS M4 以降のブレード サーバとラックマウント サーバは TXT をサポートしています。TXT はこれらのサーバーでデフォルトで無効になっています。

TXT は、[TMP]、[Intel Virtualization Technology (VT)]、および [Intel Virtualization Technology for Directed I/O (VT-d)] を有効にした後でのみ、有効にすることができます。TXT のみを有効にすると、暗黙的に TPM、VT、および VT-d も有効になります。

トラステッド プラットフォームの設定

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 TPM を設定する組織のノードを展開します。

ステップ 4 [BIOS Policies] を展開し、TPM を設定する BIOS ポリシーを選択します。

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

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

ステップ 7 TPM を設定するには、次のいずれかをクリックします。

オプション	説明
[disabled]	TPM を無効にする
[enabled]	TPM を有効にする
[Platform Default]	TPM を有効にする

ステップ 8 TPM を設定するには、次のいずれかをクリックします。

オプション	説明
[disabled]	TXT を無効にする
[enabled]	TXT を有効にする
[Platform Default]	TXT を無効にする

ステップ 9 **[Save Changes]**をクリックします。

トラステッド プラットフォームの設定

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 TPM を設定する組織のノードを展開します。

ステップ 4 [BIOS Policies] を展開し、TPM を設定する BIOS ポリシーを選択します。

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

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

ステップ 7 TPM を設定するには、次のいずれかをクリックします。

オプション	説明
[disabled]	TPM を無効にする
enable	TPM を有効にする
[Platform Default]	TPM を有効にする

ステップ 8 TPM を設定するには、次のいずれかをクリックします。

オプション	説明
[disabled]	TXT を無効にする
enable	TXT を有効にする
[Platform Default]	TXT を無効にする

ステップ 9 **[Save Changes]**をクリックします。

TPM のプロパティの表示

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*）]** > **[カートリッジ（Cartridges）]** > **[カートリッジ番号（Cartridge *Number*）]** > **[サーバ（Servers）]** の順に展開します

ステップ 3 TPM 設定を表示するサーバを選択します。

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

ステップ 5 [Motherboard] サブタブをクリックします。

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。

完全（Full）：このオプションを選択した場合、サポートされているエンドポイントとサポートされていないエンドポイントの両方の認証が失敗すると、障害が生成されます。

部分的（Partial）：このオプションを選択した場合、サポートされているエンドポイントにのみ認証が失敗すると、障害が生成されます。エンドポイントで認証がサポートされていないときは、障害は発生しません。

無効化（Disabled）：このオプションを選択した場合、サポートされているエンドポイントとサポートされていないエンドポイントの両方の認証に対して障害が生成されません。

デフォルトは **[一部（Partial）]** です。

（注） SPDM再認証を実行して障害を更新するには、関連付けられたプロファイルの障害アラート値が変更されたときに、Cisco IMC の再起動またはホストの再起動が必要です。

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。

一貫したデバイスの命名

オペレーティング システムが一貫した方法でイーサネット インターフェイスに命名できるメカニズムがない場合は、サーバーの構成が変更されたネットワーク接続の管理は困難になります。Cisco UCS Manager リリース 2.2(4) で導入された一貫したデバイスの命名（CDN）を使用すると、イーサネットインターフェイスに一貫した方法で名前を付けることができます。これにより、アダプタまたは他の設定が変更された場合でも、イーサネットインターフェイスの名前がより永続的になります。

vNIC の CDN を設定するには、次の手順を実行します。

- BIOS ポリシーで一貫したデバイスの命名を有効にします。
- BIOS ポリシーとサービス プロファイルを関連付けます。
- vNIC の一貫した命名を設定します。

一貫したデバイスの命名の注意事項と制約事項（CDN）

- CDN は次のオペレーティング システムでサポートされています。
  - Windows 2016 以降の Windows リリース
  - Windows Server 2019
  - Red Hat Enterprise Linux (RHEL) 6.x および 7.x

- SLES 12 SP3、SLES 12 SP4、および SLES 15 (4.0 (4a) 以降)
- ESXi 6.7

- CDN は、 M4 以降のすべてのブレード サーバーとラックマウント サーバーでサポートされます。
- CDN をサポートするには、BIOS とアダプタ ファームウェアがリリース 2.2(4) 以降のバンドルに組み込まれている必要があります。
- RHEL オペレーティング システムがサーバにインストールされている場合、「**sysfs label**」としてコマンド「**biosdevname -d**」を実行すると、CDN が表示されます。CDN によってカーネル名が変更されることはありません。
- CDN は vNIC テンプレートでサポートされています。
- 同じサービス プロファイル内の複数の vNIC に同じ CDN 名を指定することはできません。
- CDN 名が vNIC に指定されていない場合は、vNIC 名が CDN 名として使用されます。
- vNIC に設定する CDN 名は、[Admin CDN Name] として表示されます。vNIC に最後に適用された CDN 名前は、[Oper CDN Name] として表示されます。たとえば、「vnic0」という名前の vNIC の [管理者 CDN 名（Admin CDN Name）] が cdn0 の場合、この vNIC の [オペレータ CDN 名（Oper CDN Name）] は cdn0 になりますが、同じ vNIC でも [管理者 CDN 名（Admin CDN Name）] が指定されていない場合は [オペレータ CDN 名（Oper CDN Name）] は vnic0 になります。
- Cisco UCS Manager リリース 3.1 とそれより古いリリースでは、CDN 対応の BIOS ポリシーがサーバーに割り当てられている場合、アダプタ ファームウェアのダウングレードは禁止されています。
- Cisco UCS Manager リリース 2.2（4）では、CDN のイネーブル化がされた BIOS ポリシーが関連付けられたサーバー プロファイル上に割り当てられた場合、Cisco UCS Managerまたは BIOS のダウングレードは禁止されています。
- 適用された BIOS ポリシーが CDN 非対応から CDN 対応に、または CDN 対応から CDN 非対応に変更された場合は、BIOS 更新プログラムのリブートが有効かどうかに関係なく、警告が表示されホストがリブートします。
- Windows オペレーティング システムをインストールする前に、BIOS ポリシーで CDN を有効にし、vNIC に CDN 名を追加しておくことを推奨します。
- Windows オペレーティング システムがすでにサーバーにインストールされ、CDN が BIOS ポリシーで有効な場合は、次の手順を実行します。
  1. ネットワーク ドライバをアンインストールします。
  2. システムで非表示のデバイスをスキャンし、それらをアンインストールします。
  3. システムで新しいハードウェアを再スキャンし、ネットワーク ドライバを再インストールします。

（注） これを行わないと、vNIC が設定された CDN 名で認識されません。

- サービス プロファイルで、適用された BIOS ポリシーが CDN 非対応から CDN 対応に、または CDN 対応から CDN 非対応に変更された場合は、次の手順を実行します。
  1. ネットワーク ドライバをアンインストールします。
  2. システムで非表示のデバイスをスキャンし、それらを削除します。
  3. システムで新しいハードウェアを再スキャンし、ネットワーク ドライバを再インストールします。

（注） BIOS ポリシーが CDN 対応から CDN 非対応に変更された場合は、CDN 名がシステム上のすべての vNIC から削除されたことを確認します。

- vNIC に変更が加えられた場合、システム上のすべてのデバイスの BDF も変更されます。次に、システムに存在するすべての vNIC の BDF の変更をトリガするいくつかのシナリオを示します。
  - vNIC が追加または削除された場合
  - vNIC がシステム上のあるアダプタからシステム上の別のアダプタに移動された場合

  これらの変更がシステムに加えられた場合は、次の手順を実行します。
  1. 存在するすべてのネットワーク インターフェイスからネットワーク ドライバをアンインストールします。
  2. システムで非表示のデバイスをスキャンし、それらをアンインストールします。
  3. システムで新しいハードウェアを再スキャンし、ネットワーク コントローラにネットワーク ドライバを再インストールします。

  非表示のデバイスが削除されないと、ネットワーク アダプタの CDN 名は Cisco UCS Manager に設定されたとおりに表示されません。

各種アダプタが混在する場合の CDN

CDN 名が CDN がサポートされているアダプタと CDN がサポートされていないアダプタが混在するシステム内の vNIC に設定されると、システム配置において、CDN が設定された vNIC が CDN をサポートするアダプタに配置されない場合があります。

CDN が BIOS ポリシーで有効であり、システム配置によって、CDN が設定された vNIC（Admin CDN 設定済み）が CDN をサポートしていないアダプタに配置された場合は、情報エラーが発生しますが、サービス プロファイルの設定問題は無視されます。

CDN が BIOS ポリシーで有効であり、システム配置によって、vNIC（Admin CDN 未設定）が CDN をサポートしていないアダプタに配置された場合は、情報エラーが発生しますが、サービス プロファイルの設定問題は無視されます。この場合、[Oper CDN Name] は空になり、vNIC 名から派生されません。

CDN 名をサーバーのホスト ネットワーク インターフェイス名として展開する場合は、サポートされるアダプタに手動で vNIC を配置する必要があります。

BIOSポリシーでの一貫したデバイスの命名の設定

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 [root] を展開します。

ステップ 4 [BIOS Policies] を展開します。

ステップ 5 CDN を設定する BIOS ポリシーを選択します。

（注） デフォルトの BIOS ポリシーは CDN 値を B200 M6 サーバーに保存しないため、UCS Manager はカスタム CDN 値を vNIC にプッシュしません。BIOS ポリシーの CDN 値を設定するには、CDN 値を含む必要な値を使用して BIOS ポリシーを作成します。

ステップ 6 [Main] タブの [Consistent Device Naming] フィールドで次のいずれかをクリックして、CDN を設定します。

オプション	説明
[disabled]	BIOS ポリシーで CDN を無効にします。
enabled	BIOS ポリシーで CDN を有効にします。
Platform Default	BIOS は、サーバ タイプとベンダーに関する BIOS のデフォルト設定に含まれるこの属性の値を使用します。

ステップ 7 **[Save Changes]**をクリックします。

vNIC の CDN 名の設定

CDN 名が vNIC に指定されていない場合は、vNIC 名が CDN 名として使用されます。

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 CDN 名を設定する vNIC を含む組織のノードを展開します。

ステップ 4 CDN 名を設定する vNIC を含むサービス プロファイルと [vNICs] ノードを展開します。

ステップ 5 vNIC を選択します。

ステップ 6 [General] タブをクリックします。

ステップ 7 [Properties] 領域で [CDN Source] として [User Defined] を選択します。

ステップ 8 vNIC の CDN 名を **[CDN 名 (CDN Name)]** フィールドに入力します。

（注） vNIC に設定する CDN 名は [CDN Name] として表示されます。vNIC に最後に適用された CDN 名は、[Oper CDN Name] として表示されます。たとえば、「vnic0」という名前の vNIC の [CDN Name] が cdn0 の場合、この vNIC の [Oper CDN Name] は cdn0 になりますが、同じ vNIC でも [CDN Name] が指定されていない場合は [Oper CDN Name] は vnic0 になります。

ステップ 9 **[Save Changes]**をクリックします。

CIMC セキュリティ ポリシー

Cisco UCS Manager セキュリティを強化するために次のポリシーを提供しています。

- KVM 管理ポリシー
- IPMI アクセス プロファイル

IPMI アクセス プロファイル

このポリシーでは、IP アドレスを使用して、IPMI コマンドを直接サーバーに送信できるかどうかを決定することができます。たとえば、CIMCからセンサーデータを取得するためのコマンドを送信することができます。このポリシーは、サーバーでローカルに認証可能なユーザー名とパスワードを含む IPMI アクセス、およびこのアクセスが読み取り専用か、読み取りと書き込みであるかを定義します。

また、IPMI アクセス プロファイルの IPMI over LAN を無効または有効にして、リモート接続を制限することもできます。IPMI over LAN は、関連付けされていないすべてのサーバー、および IPMI アクセス ポリシーがないすべてのサーバーでデフォルトで無効になっています。IPMI アクセス ポリシーを作成すると、デフォルトで、IPMI over LAN が「有効」に設定されます。この値を「無効」に変更しない場合は、関連するすべてのサーバーで IPMI over LAN が有効になります。

このポリシーはサービス プロファイルに組み込む必要があります。また、このサービス プロファイルを有効にするには、サーバーに関連付ける必要があります。

IPMI アクセス プロファイルの作成

Before you begin

IPMI プロファイルは、次のリソースの 1 つ以上がシステムにすでに存在していることを前提にしています。

- 適切な権限があり、サーバのオペレーティング システムによる認証が可能なユーザ名
- このユーザ名のパスワード
- ユーザ名と関連付けられている権限

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]** > **[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 [IPMI Access Profiles] を右クリックし、[Create IPMI Access Profile] を選択します。

ステップ 5 [Create IPMI Access Profile] ダイアログボックスで次の手順を実行します。

a) プロファイルの一意の名前および説明を入力します。

b) [IPMI Over LAN] フィールドで、リモート接続を許可するか、禁止するかを選択します。

c) [OK] をクリックします。

ステップ 6 ナビゲータの [IPMI Users] 領域で、[+] をクリックします。

ステップ 7 [Create IPMI User] ダイアログボックスで、次の手順を実行します。

a) 次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	この IPMI またはRedfish プロファイルに関連付けたユーザ名。 1 ～ 16 文字の英数字を入力します。「@」（アット マーク）、「_」（アンダースコア）、「-」（ハイフン）も使用できます。プロファイルの保存後は、この名前を変更できません。

名前	説明
[Password] フィールド	このユーザ名に関連付けられるパスワード。 1 ～ 20 文字の標準 ASCII 文字を入力します（ただし、「=」（等号）、「$」（ドル記号）、「|」（縦棒）は除く）。
[パスワードの確認（Confirm Password）] フィールド	確認のためのパスワードの再入力。
[Role] フィールド	ユーザ ロール。次のいずれかになります。 • **[Admin]** • **[Read Only]**
[Description] フィールド	IPMI または Redfish ユーザのユーザ定義の説明。

b) [OK] をクリックします。

ステップ 8 別のユーザを追加するには、ステップ 6 および 7 を繰り返します。

ステップ 9 [OK] をクリックして、[Work] ペインの IPMI プロファイルに戻ります。

What to do next

IPMI プロファイルをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

IPMI アクセス プロファイルの削除

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（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [IPMI Profiles] ノードを展開します。

ステップ 4 削除する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 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。

KVM 管理ポリシー

KVM 管理ポリシーを使用して、KVM 経由でサーバーにアクセスするときに仮想メディア（vMedia）暗号化を有効にするかどうかを指定できます。

このポリシーはサービス プロファイルに組み込む必要があります。また、このサービス プロファイルを有効にするには、サーバーに関連付ける必要があります。

（注） KVM仮想メディア（vMedia）セッションがマッピングされた後、KVM管理ポリシーを変更すると、仮想メディア（vMedia）セッションは失われます。KVM 仮想メディア（vMedia）セッションを再度マッピングする必要があります。

Cisco UCS Manager リリース 4.0 (4) 以前では、ポート 2068 が唯一の KVM ポートでした。リリース 4.0(4) から、KVM ポートとして 1024 ~ 49151 のポート番号を設定できます。ポート 2068 は引き続きデフォルトの KVM ポート番号です。

KVM 管理ポリシーの作成

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 [KVM Management Policies] を右クリックし、[Create KVM Management Policy] を選択します。

ステップ 5 [Create KVM Management Policy] ダイアログ ボックスで次の手順を実行します。

a) ポリシーの一意の名前と説明を入力します。

b) [vMedia Encryption] フィールドで、vMedia 暗号化をイネーブルにするかどうかを選択します。

（注） UCS Manager 4.2 以降、vMedia 暗号化はセキュリティ目的で常に有効になっています。ユーザーが変更することはできません。

c) **[KVM ポート (KVM Port)]** フィールドで、KVM の場合は 1024 ~ 49151 の範囲のポート番号を入力します。

デフォルトの KVM ポート番号は 2068 です。

d) [OK] をクリックします。

（注） KVM 仮想メディア（vMedia）セッションがマッピングされた後、KVM 管理ポリシーを変更すると、仮想メディア（vMedia）セッションは失われます。KVM 仮想メディア（vMedia）セッションを再度マッピングする必要があります。

グラフィックス カード ポリシー

Cisco UCS Manager リリース 3.1(3) ではグラフィックス カードのサポートが拡張され、グラフィックス カード モードを変更する機能が追加されました。グラフィックス カード ポリシーを使用してグラフィックス カード モードを設定できます。グラフィックス カード モードを次に示します。

- コンピューティング
- Graphics
- Any Configuration

グラフィックス カード ポリシーの作成

（注） Cisco UCS Manager は、GPU の設定変更を、グラフィックス カード ポリシーを介して Processor Node Utility Operating System（PNuOS）にプッシュします。これらの変更は、サーバがリブートされるまで有効になりません。

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]** > **[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 [Graphics Card Policies] を右クリックして、[Create Graphics Card Policy] を選択します。

ステップ 5 [Create Graphics Card Policy] ダイアログボックスの [Main] ページで、次の操作を実行します。

a) ポリシーの一意の名前を入力します。

b) （任意） ポリシーの説明を入力します。

c) [Graphics Card Mode] フィールドで、次のいずれかを選択します。

- **コンピューティング**
- **Graphics**
- **Any Configuration**

d) [OK] をクリックします。

ローカル ディスク ポリシー

ローカル ディスク設定ポリシー

このポリシーは、ローカル ドライブのオンボードRAIDコントローラを通じて、サーバー上にインストールされているオプションの SAS ローカル ドライブを設定します。このポリシーでは、ローカル ディスク設定ポリシーをインクルードしているサービス プロファイルに関連付けられたすべてのサーバに対してローカル ディスク モードを設定できます。

ローカル ディスク モードには次のものがあります。

- [No Local Storage]：ディスクレス サーバーまたは 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ーに関連付けることができません。
- [RAID 0 Striped]：データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- **RAID 1 Mirrored**：データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合に完全なデータ冗長性を提供します。最大アレイ サイズは、2つのドライブの小さい方の空き容量に等しくなります。
- [Any Configuration]：変更なしのローカル ディスク設定を転送するサーバー設定で使用します。
- [No RAID]：RAID を削除し、ディスク MBR およびペイロードを変更しない状態のままにするサーバー設定で使用します。

  [No RAID] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバーに適用した場合、システムによってディスクの内容が削除されません。そのため、[No RAID] モードの適用後にサーバーでの違いがわからないことがあります。よって、ポリシーの RAID 設定と、サーバーの **[Inventory]** > **[Storage]** タブに表示される実際のディスク設定とが一致しない場合があります。

  以前のすべての RAID 設定情報をディスクから削除させるには、**No RAID** コンフィギュレーション モードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。
- **RAID 5 Striped Parity**：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 6 Striped Dual 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、2つのパリティディスクを使用して、最大2つの物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。

- **[RAID 10 Mirrored and Striped]**：RAID 10 はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。
- **[RAID 50 Striped Parity and Striped]**：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。
- **[RAID 60 Striped Dual Parity and Striped]** ：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。

このポリシーはサービス プロファイルに組み込む必要があります。また。このポリシーを有効にするには、サーバーに関連付ける必要があります。

Note 組み込みオンボード RAID コントローラを搭載した Cisco UCS Manager と統合された Cisco UCS C シリーズ サーバーの場合、ローカル ディスク モードは常に [Any Configuration] でなければならず、RAID はコントローラ上で直接設定する必要があります。

すべてのローカル ディスク設定ポリシーに関するガイドライン

ローカル ディスク設定ポリシーを作成する前に、次のガイドラインを考慮してください。

HDD と SSD を混合しない

1 台のサーバーや RAID 設定に、HDD と SSD を使用しないでください。

RAID 用に設定されているローカル ディスク設定ポリシーに関するガイドライン

MegaRAID ストレージ コントローラを搭載したサーバー用のローカル ディスク設定ポリシーに RAID 設定を設定する

ブレード サーバーまたは統合されたラックマウント サーバーに MegaRAID コントローラが搭載されている場合、そのサーバーのサービス プロファイルに含まれるローカル ディスク設定ポリシーでドライブの RAID 設定を設定する必要があります。これを実行するには、そのサーバーに定義されている RAID モードのいずれかを使用して、サービス プロファイルのローカル ディスク設定ポリシーを設定するか、**[Any Configuration]** モードと LSI ユーティリティ ツール セットを使用して、RAID ボリュームを作成します。

OS をインストールする前に RAID LUN を設定していないと、インストール時にディスク検出エラーが発生し、「No Device Found」といったエラー メッセージが表示される可能性があります。

サーバー プロファイルで [Any Configuration] モードが指定されている場合、RAID 1 クラスタ移行後にサーバーが起動しない

RAID 1 クラスタの移行後、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。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 **RAID 1** ではなく **[Any Configuration]** モードが設定されていると、RAID LUN は、関連付け中およびその後も「非アクティブ」状態のままになります。その結果、サーバーは起動できなくなります。

この問題を回避するには、サーバーに関連付けるサービスプロファイルに、移行前の元のサービス プロファイルとまったく同じローカル ディスク設定ポリシーが含まれるようにし、**[Any Configuration]** モードは含まれないようにします。

MegaRAID ストレージ コントローラを搭載したサーバー上で JBOD モードを使用しない

MegaRAID ストレージ コントローラが搭載されたブレード サーバーまたは統合ラックマウント サーバー上で JBOD モードまたは JBOD 操作を設定または使用しないでください。JBOD モードと操作は、このサーバーで完全に機能するよう設計されていません。

統合されたラックマウント サーバー内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

Cisco UCS Manager とともに登録されており、サーバー上に存在するハード ドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。

統合されたラックマウント サーバー内のローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。Cisco UCS Manager との統合では、ローカル ハード ドライブが単一のラックマウント サーバー内の複数の RAID コントローラに接続することはサポートされていません。そのため、Cisco UCS Manager と統合されるラックマウント サーバーを発注する際は、単一の RAID コントローラ構成を要求することを推奨します。

また、サードパーティ製ツールを使用して、ラックマウント サーバー上に複数の RAID LUN を作成しないでください。Cisco UCS Manager は、そのような設定をサポートしていません。

ブレード サーバー内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

ブレード サーバーは、サーバー内に存在するドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。ローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。

また、サードパーティ製ツールを使用して、ブレード サーバー上に複数の RAID LUN を作成しないでください。Cisco UCS Manager は、そのような設定をサポートしていません。

一部のサーバーの特定の RAID 設定オプションでは、ライセンスが必要

一部のCisco UCSサーバーには、特定の RAID 設定オプションの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 プロファイルとサーバーを関連付けると、Cisco UCS Manager によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。問題がある場合は、サービスプロファイルを関連付ける際に、Cisco UCS Manager に設定エラーが表示されます。

特定のCisco UCS サーバーの RAID ライセンス情報については、そのサーバーの『*Hardware Installation Guide*』を参照してください。

ローカル ディスク設定ポリシーの作成

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]** > **[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] を右クリックし、[Create Local Disk Configuration Policy] を選択します。

ステップ 5 [Create Local Disk 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	説明
[名前（Name）] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[説明（Description）] フィールド	ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

名前	説明
[Mode] ドロップダウン リスト	次のローカル ディスク ポリシー モードのいずれかを選択できます。 • **No Local Storage** • [RAID 0 Striped] • **RAID 1 Mirrored** • **[Any Configuration]** • **[No RAID]** [No RAID] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバーに適用した場合、システムによってディスクの内容が削除されません。そのため、[No RAID] モードの適用後にサーバーでの違いがわからないことがあります。よって、ポリシーの RAID 設定と、サーバーの **[Inventory]** > **[Storage]** タブに表示される実際のディスク設定とが一致しない場合があります。 以前のすべての RAID 設定情報をディスクから削除させるには、**No RAID** コンフィギュレーション モードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。 • **RAID 5 Striped Parity** • [RAID 6 Striped Dual Parity] • **[RAID 10 Mirrored and Striped]** • [RAID 50 Striped Parity and Striped] • [RAID 60 Striped Dual Parity and Striped] **Note** 一部のCisco UCSサーバーには、特定の RAID 設定オプションの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 プロファイルとサーバーを関連付けると、Cisco UCS Manager によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。問題がある場合は、サービス プロファイルを関連付ける際に、Cisco UCS Manager に設定エラーが表示されます。 特定のCisco UCS サーバーの RAID ライセンス情報については、そのサーバーの『*Hardware Installation Guide*』を参照してください。

名前	説明
[Protect Configuration]チェックボックス	オンにすると、サーバーは、サービス プロファイルとの関連付けが解除されても、ローカル ディスク設定ポリシー内の設定を保持します。 **Caution** サーバー内の 1 つ以上のディスクに障害が発生すると、[Protect Configuration] は機能しなくなります。 このプロパティは、デフォルトでオンになっています。 サービス プロファイルがサーバから関連付けを解除され、新しいサービス プロファイルが関連付けられると、新しいサービス プロファイルの [設定の保護（Protect Configuration）] プロパティの設定が優先され、前のサービス プロファイルの設定が上書きされます。 このオプションが有効になっていると、サーバーが稼働停止して再稼働された後でもディスク上のデータは保護されます。したがって、サーバーとサービス プロファイルの再関連付けは失敗します。 **Note** このオプションが有効の状態でサーバーとサービス プロファイルの関連付けを解除した後、そのサーバー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、サーバー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。
[FlexFlash State]オプション ボタン	SD カードの FlexFlash コントローラを有効化または無効化にするには、該当するボタンをクリックしてください。 **Note** このパラメータは、SD カード モジュールのあるサーバーのみ該当します。
[FlexFlash RAID Reporting State] ラジオ ボタン	RAID レポートを有効化または無効化にするには、該当するボタンをクリックしてください。RAID レポートを有効にすると、RAID ステータスがモニターリングされ、障害が有効化されます。 **Note** 1 枚の SD カードのみが装着されている場合は、RAID レポートが有効な場合でも、RAID ステータスは「Disabled」と表示され、RAID の状態は「NA」と表示されます。

名前	説明
[FlexFlash Removable State] ラジオ ボタン	FlexFlash SD カードの [removable] 状態を選択するには、適切なボタンをクリックします。 • **[Yes]**: このオプションを使用して [removable] として、SD カードを定義します。 • **[No]**: このオプションを使用して [fixed] または [non-removable] として、SD カードを定義します。 • **[No Change]**: 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。

ステップ 6 **[OK]** をクリックします。

ローカル ディスク設定ポリシーの変更

この手順は、関連付けられた サービス プロファイル からローカル ディスク設定ポリシーを変更するものです。[Servers] の [Policies] ノードからローカル ディスク設定ポリシーを変更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、[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 変更するローカル ディスク設定ポリシーを持つサービス プロファイルを含む組織を展開します。

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 変更するローカル ディスク設定ポリシーを含む サービス プロファイル をクリックします。

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

ステップ 6 [Actions] 領域で、[Change Local Disk Configuration Policy] をクリックします。

ステップ 7 [Change Local Disk Configuration Policy] ダイアログボックスで、[Select the Local Disk Configuration Policy] ドロップダウン リストから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
Use a Disk Policy	このオプションのリストから既存のローカル ディスク設定ポリシーを選択します。Cisco UCS Manager はこのポリシーをサービス プロファイルに割り当てます。

オプション	説明
Create a Local Disk Policy	選択された サービス プロファイル だけがアクセスできるローカル ディスク設定ポリシーを作成できます。
No Disk Policy	デフォルトのローカル ディスク ポリシーを選択します。 （注） UCS サーバが Cisco UCS Manager に接続している場合、[No Disk Policy] を選択すると RAID が消去され、接続されているサーバでデフォルトの RAID 設定がサポートされていない場合は個々の RAID 0 ディスクで置き換えられます。

ステップ 8 [OK] をクリックします。

ステップ 9 （任意） [Local Disk Configuration Policy] 領域を展開し、変更が行われたことを確認します。

ローカル ディスク設定ポリシーの削除

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（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [Local Disk Config 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。

FlexFlash のサポート

概要

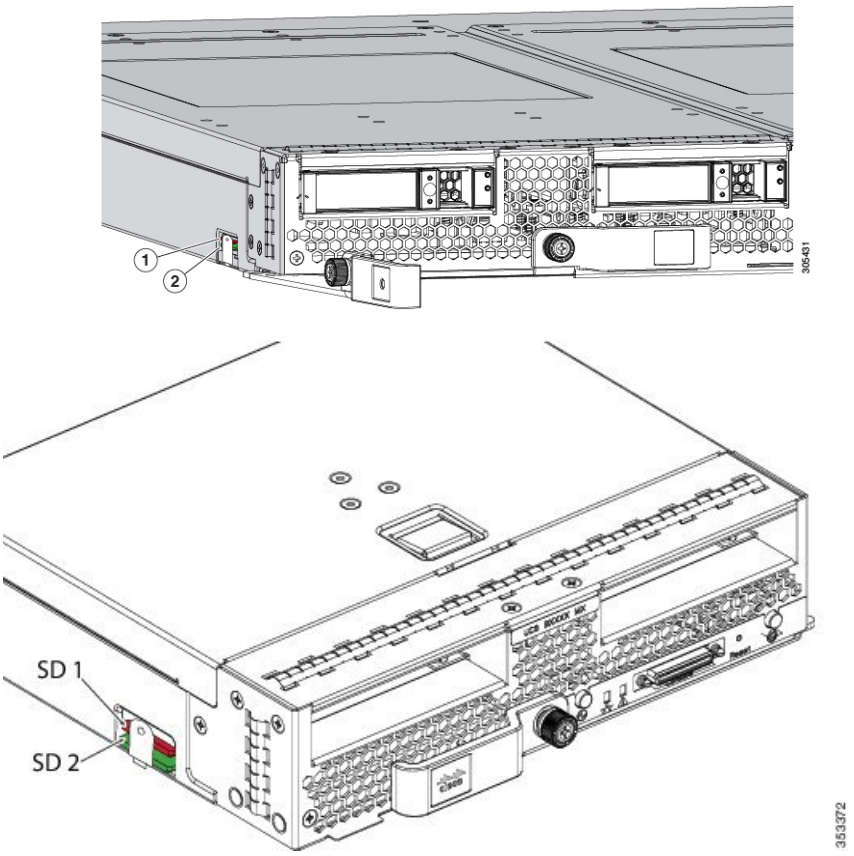
Cisco UCS B シリーズ サーバー、C シリーズ M4 以降のサーバー、S シリーズ M4 サーバーは、内部セキュア デジタル（SD）メモリ カードをサポートしています。SD カードは、Cisco Flexible Flash ストレージ コントローラ（SD カード用スロットが 2 つある PCI ベースのコントローラ）によってホストされます。カードには、HV と呼ばれる単一のパーティションが含まれます。FlexFlash が有効な場合、Cisco UCS Manager では、BIOS とホスト ホスト オペレーティング システムのどちらに対しても、HV パーティションを USB ド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

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

（注） サーバー内で異なる容量のカードを混在させないでください。

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

図 *1: 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 （377 ページ）を参照してください。
- サーバからサービス プロファイルの関連付けを解除します。デフォルトのスクラブ ポリシーを変更後サーバを認識し、サーバ プロファイルをサーバに再度関連付けます。

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

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

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

FlexFlash ファームウェア管理

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

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

- Cisco Flexible Flash ストレージ コントローラは 16 GB、32 GB および 64 GB の SD カードのみをサポートしています。

（注） 64 GB SD カードは M4 および M5 ブレード サーバでのみサポートされます。

- 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が、データを喪失する可能性があります。

- 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 UCS B200 M4 と M5 ブレード サーバー
- Cisco UCS C220 M4 と M5 ラック サーバー
- Cisco UCS C240 M4、 および M5 ラック サーバー
- 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、一対の 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 カードを使用したブレード サーバの起動

16 GB 以上の FlexFlash カードを使用してブレード サーバーを起動するには、次の手順を使用します。この手順では、ブレードサーバー、ソフトウェア、および関連付けられたインフラストラクチャを設定する方法を知っていることと、機能していることを確認することが必要です。この Cisco UCS Manager の制御手順は、任意のバージョンのファームウェアを実行しているすべてのブレードサーバに適用されます。この手順はラック サーバーには適用されません。作業環境で FlexFlash カードを有効にする前に、次の手順に従います。

注意 FlexFlash をすでに使用している状態で次の手順を使用すると、カードからすべてのデータが失われます。

（注） この手順では、FlexFlash カードの使用方法や、FlexFlash システムのその他の機能は扱っていません。

手順

ステップ 1 **[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 2 [Work] ペインで、[FlexFlash Controller] ウィンドウ内の FlexFlash カードの詳細情報を確認します。

ステップ 3 **[サーバ] > [サービスプロファイル]**を展開します。

ステップ 4 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 5 サービス プロファイルを含む組織のノードを展開し、[Storage] をクリックします。

ステップ 6 [Work] ペインで、[Actions] 領域の [Change Local Disk Configuration Policy] をクリックし、[Create Local Disk Configuration Policy] リンクを展開します。ローカル ディスク設定ポリシーの作成（367 ページ）の手順に従ってローカル ディスクの設定ポリシーを作成します。

FlexFlash ポリシー名には、空白や特殊文字を使用することはできません。

ステップ 7 [Change Disk Local Configuration Policy] を展開し、作成したポリシーを選択し、[OK] をクリックします。

ステップ 8 **[サーバ]** > **[ポリシー]**を展開します。

ステップ 9 スクラブ ポリシーの作成 （381 ページ）の手順に従って *Scrub-FF-name* などの名前でポリシーを作成し、[OK] をクリックします。

スクラブ ポリシー名には、空白や特殊文字を使用することはできません。

ステップ 10 ドロップダウン ボックスから作成したポリシーを選択します。

ステップ 11 **[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 12 [Work] ペインで、[General] タブをクリックし、[Actions] 領域から [Server Maintenance] を選択します。

ステップ 13 [Maintenance Server] ダイアログボックスで [Re-acknowledge] オプション ボタンをクリックし、[OK] をクリックします。

ステップ 14 [Action] 領域の [Server Maintenance] をクリックし、[Re-acknowledge] オプション ボタンをもう一度クリックします。

ステップ 15 [Inventory] タブで [Storage] サブタブを選択します。
[Work] 領域の [FlexFlash Controller] ウィンドウで、有効な FlexFlash カードの詳細情報を確認できます。

ステップ 16 KVM Manager を起動してオペレーティング システムにログオンします。デバイスとドライブ フォルダのハイパーバイザ パーティションの詳細を確認します。カード サイズによって、HV パーティションには 32GB、64GB、または 128 GB のいずれかの詳細情報が表示されます。
FlexFlash カードは同期され、使用可能になりました。

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 RAID Reporting 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 8 [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ーをクリックします。

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。

永続メモリ モジュール

Cisco UCS Manager Release 4.0 (4) では、第二世代インテル® Xeon® Scalable プロセッサに基づく UCS M5 サーバ上の Intel® Optane™ データ センター永続メモリ モジュールのサポートが導入されています。Cisco UCS Manager リリース 4.2 以降では、第二世代インテル® Xeon® Scalable プロセッサに基づく UCS M6 サーバーでの Intel® Optane™ データ センター永続メモリ モジュールのサポートも導入されています. 永続メモリ モジュールは、第二世代インテル® Xeon® Scalable プロセッサでのみ使用できます。

永続メモリ モジュールは、メモリの低遅延とストレージの永続化を実現する不揮発性メモリ モジュールです。永続メモリ モジュールに保存されているデータは、他のストレージ デバイスに比べてすぐにアクセスでき、電源サイクルで保持されます。

永続メモリ モジュールの設定の詳細については、『*Cisco UCS: Intel® Optane™ Data Center* 永続メモリモジュールの設定と管理』を参照してください。

スクラブ ポリシー

スクラブ ポリシーの設定

このポリシーは、ディスカバリ プロセス中にサーバーのローカル データおよび BIOS 設定に何が起こるか、サーバーがいつ再認識されるか、またはサーバーとサービス プロファイルの関連付けがいつ解除されるかを決定します。

Note ローカル ディスク スクラブ ポリシーは、 Cisco UCS Manager によって管理されるハード ドライブにのみ適用され、USB ドライブなど他のデバイスには適用されません。

スクラブ ポリシーの設定によっては、そのようなときに次の処理が行われます。

ディスク スクラブ

ローカル ドライブのデータに対しては、アソシエーションが解除されるときに、次のいずれかが発生します。

- 有効にすると、マスター ブート レコードまたはブート セクターからデータの最初の 200 MB が削除されます。そのため、すでにインストールされている OS がある場合、その OS

からシステムが起動するのを防ぐことができます。ドライブ上のデータの安全な削除については、『UCS Secure Data Deletion For Commission Regulation (EU) 2019 /424 Users Guide』を参照してください。

Note ディスク スクラブ ポリシーは、200 MBを超えるユーザ データを削除することを目的としていませんが、Cisco UCS Manager はデータ損失に対する保証はできません。

- 無効 (デフォルト) になっている場合は、ローカル ドライブ上のすべてのデータが保持されます（ローカル ストレージ設定を含む）。

サービス プロファイルに関連付けられているサーバーの場合、サービス プロファイルに使用されているスクラブ ポリシーに基づいて、割り当て解除時にディスク スクラブが行われます。関連付けられていないサーバーの場合、デフォルトのスクラブ ポリシーに基づいて、サーバー ディスカバリ プロセス時にディスク スクラブが行われます。

スクラブ ポリシーは、すべての B シリーズ プラットフォーム、および次に示す一部の C シリーズ プラットフォームでサポートされます。

- Cisco UCS C220 M4 サーバ
- Cisco UCS C240 M4 サーバ
- Cisco UCS C460 M4 ストレージ 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 C220 M6サーバ
- Cisco UCS C240 M6サーバ
- Cisco UCS C225 M6サーバ
- Cisco UCS C245 M6サーバ
- Cisco UCS C480 M5 ML サーバー
- Cisco UCS C3260 M4 ストレージ サーバ: 同じドライブを使用して作成されたブート ドライブと VD のみをスクラブできます。
- Cisco UCS S3260 M5 ストレージ サーバ: 同じドライブを使用して作成されたブート ドライブと VD のみをスクラブできます。

Note 次の場合、LUN の削除に関連する変更を確認するために、サーバを再認識させる必要があります。

- Cisco UCS C3260 M4 または Cisco UCS S3260 M5 ストレージ サーバ を使用して設定された SAS コントローラの下に LUN があるブート ドライブをスクラブしています。
- Cisco ブート最適化 M.2 RAID コントローラで LUN をスクラブしています。

BIOS 設定スクラブ

BIOS 設定に対しては、スクラブ ポリシーを含むサービス プロファイルがサーバからアソシエーション解除されるときに、次のいずれかが発生します。

- 有効になっている場合は、サーバーのすべての BIOS 設定が消去され、サーバー タイプとベンダーに応じた BIOS のデフォルトにリセットされます。
- 無効 (デフォルト) になっている場合は、サーバの既存の BIOS 設定が保持されます。

FlexFlash スクラブ

FlexFlash スクラブにより、新規またはデグレードした SD カードの組み合わせ、FlexFlash メタデータの設定エラーの解決、4 パーティションの旧式 SD カードから単一パーティション SD カードへの移行を実行することができます。スクラブ ポリシーを含むサービス プロファイルとサーバとの関連付けが解除されるとき、またはサーバが再認識されるときに、SD カードに対して次のいずれかが発生します。

- 有効になっている場合は、PNUOS フォーマット ユーティリティにより SD カードの HV パーティションがフォーマットされます。SD カードが 2 枚ある場合、それらカードは RAID-1 ペアになっており、両方のカードの HV パーティションが有効と見なされます。スロット 1 のカードはプライマリ、スロット 2 のカードはセカンダリと見なされます。
- 無効 (デフォルト) の場合、既存の SD カード設定が保持されます。

Note

- サービス プロファイルに関連付けられているサーバーの場合、サービス プロファイルに使用されているスクラブ ポリシーに基づいて、割り当て解除時に FlexFlash スクラブが行われます。関連付けられていないサーバーの場合、デフォルトのスクラブ ポリシーに基づいて、サーバー ディスカバリ プロセス時に FlexFlash スクラブが行われます。
- FlexFlash スクラブによって SD カードの HV パーティションが消去されるため、FlexFlash スクラブを実行する前に、使用しているホスト オペレーティング システムのユーティリティを使用して SD カードを完全にバックアップすることをお勧めします。
- サービス プロファイルのメタデータ設定の不具合を解決するには、FlexFlash スクラブを実行する前にローカル ディスク設定ポリシーの FlexFlash を無効にして、サーバーが再認識された後に FlexFlash を有効にする必要があります。
- ペアリングが完了したら、またはメタデータの不具合が解決したら、ただちにスクラブ ポリシーを無効にしてください。
- Cisco UCS S3260 ストレージ サーバ では FlexFlash スクラブはサポートされません。

永続メモリ スクラブ

永続メモリ スクラブを使用すると、サーバ上の永続メモリの設定とデータを保存または削除することができます。

- 有効な場合:
  - すべての永続メモリ データを消去します。
  - 工場出荷時のデフォルト設定にリセットします
  - DIMM セキュリティを無効にします
- 無効(デフォルト)の場合、サーバ上の既存の永続メモリ設定とデータを保持します。DIMM ロック状態は変更されません。

スクラブ ポリシーの作成

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]** > **[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 [Scrub Policies] を右クリックし、[Create Scrub Policy] を選択します。

Note Cisco UCS Manager は、NVME ローカル ディスク スクラブをサポートしていません。

ステップ 5 [Create Scrub Policy] ウィザードで、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[説明（Description）] フィールド	ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[ディスク スクラブ（Disk Scrub）] フィールド	このフィールドが**[はい (Yes)]**に設定されている場合、このスクラブ ポリシーを含むサービス プロファイルがサーバとの関連付けを解除されると、最初の 200MB のデータがマスター ブート レコードまたはブート セクターから削除されます。そのため、すでにインストールされている OS がある場合、その OS からシステムが起動するのを防ぐことができます。ドライブ上のデータの安全な削除については、『UCS Secure Data Deletion For Commission Regulation (EU) 2019 /424 Users Guide』を参照してください。このフィールドを [No] に設定すると、すべてのローカル ストレージ設定を含むローカル ドライブ上のデータは保存されます。 **Note** ディスク スクラブ ポリシーは、200MB を超えるユーザ データを削除することを意図したものではありませんが、 Cisco UCS Manager はデータ損失に対して保証することはできません。
[BIOS 設定スクラブ（BIOS Settings Scrub）] フィールド	このフィールドを [はい（Yes）] に設定すると、このスクラブ ポリシーを含むサービス プロファイルがサーバーとの関連付けを解除されたときに、そのサーバーの BIOS 設定が消去され、そのサーバー タイプとベンダーのデフォルトにリセットされます。このフィールドを [No] に設定すると、BIOS 設定は保存されます。

名前	説明
[FlexFlash スクラブ（FlexFlash Scrub）] フィールド	フィールドを [はい（Yes）] に設定すると、サーバーが再認識されたときに、SD カードの HV パーティションは PNUOS フォーマット ユーティリティを使用してフォーマットされます。このフィールドを [No] に設定すると、SD カードは保存されます。
[Persistent Memory Scrub (永続メモリ スクラブ)] フィールド	このフィールドを [Yes] に設定すると、このスクラブ ポリシーを含むサービス プロファイルがサーバとの関連付けを解除されたときに、そのサーバのすべての永続メモリ モジュールが消去され、そのサーバ タイプとベンダーのデフォルトにリセットされます。このフィールドが **[No (いいえ)]** に設定されている場合、永続メモリ モジュールは保持されます。

ステップ 6 [OK] をクリックします。

Note Disk Scrub オプションは、Cisco UCS S3260 ストレージ サーバ の boot-lun/boot-disk のみをスクラブし、data-lun/data-disk はスクラブしません。Cisco UCS S3260 ストレージ サーバ では FlexFlash スクラブはサポートされません。

スクラブ ポリシーの削除

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（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [Scrub 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。

DIMM エラー管理

DIMM の修正可能なエラー処理

Cisco UCS Manager では、DIMM が事前定義されたウィンドウにおいて修正可能な重大エラーに遭遇した場合、ステータスが Degraded と表され、機能しないデバイスと見なされます。

DIMM の修正可能なエラー処理機能により、サーバー内のすべての DIMM に関する修正可能および修正不可能なメモリ エラーをすべてリセットできます。エラー設定をリセットすると、当該 DIMM のエラー数はクリアされ、ステータスは操作可能に変わり、DIMM のセンサー状態がリセットされます。

メモリ エラーのリセット

Cisco UCS Manager とベースボード管理コントローラ（BMC）で発生したすべての修正可能および修正不可能なメモリ エラーをリセットするには、この手順を使用します。

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）]** > **[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 エラー設定をリセットするサーバを右クリックし、[Reset All Memory Errors] を選択します。また、[Actions] 領域から [Reset All Memory Errors] を選択することもできます。

ステップ 4 UCS Manager Cisco UCS Manager GUI に確認のダイアログボックスが表示された場合は、**[Yes]** をクリックします。

DIMM のブラックリスト化

Cisco UCS Manager で、デュアル インライン メモリ モジュール（DIMM）の状態は、SEL イベント レコードに基づいています。メモリ テストの実行中に BIOS で修正不可能なメモリ エラーに遭遇した場合、DIMM は不良としてマークされます。不良な DIMM は機能しないデバイスと見なされます。

DIMM のブラックリスト化を有効にすると、Cisco UCS Manager はメモリ テスト実行メッセージをモニターし、DIMM SPD データ内でメモリ エラーに遭遇した DIMM をブラックリストに載せます。これにより、ホストは修正不可能な ECC エラーに遭遇した DIMM をマップから外すことができます。

DIMM のブラックリストのイネーブル化

メモリ ポリシーは、Cisco UCS ドメイン の既存のサーバー、およびメモリ ポリシーを設定した後で追加されたサーバーに適用できるグローバル ポリシーです。

（注）
- この機能は、Cisco UCS Bシリーズ ブレード サーバーおよび UCS C シリーズ ラック サーバーの両方でサポートされています。
- このグローバル ポリシーをサービス プロファイルに追加することはできません。

始める前に

- Cisco B シリーズ ブレード サーバーの場合、サーバー ファームウェアはリリース 2.2(1) 以降のリリースである必要があります。
- シスコ C シリーズ および S シリーズ ラック サーバの場合、サーバ ファームウェアはリリース 2.2(3) である必要があります。
- 次の権限のいずれかでログインする必要があります。
  - 管理者
  - サーバー ポリシー
  - サーバー プロファイルのサーバー ポリシー

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 ブラックリストをイネーブルに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 [Memory Policy] を展開して [default] を選択します。

ステップ 5 [Blacklisting] 領域で、[Enabled] オプション ボタンをクリックします。

DIMM のブラックリストは、ドメイン レベル ポリシーでイネーブルにされ、これらの変更は、その特定のドメイン内のすべてのサーバに適用されます。

（注） サーバの Cisco IMC が DIMM のブラックリストをサポートしない場合、情報レベルのエラーが生成されます。

Serial over LAN ポリシー設定

Serial over LAN ポリシーの概要

このポリシーは、このポリシーを使用するサービス プロファイルと関連付けられているすべてのサーバーに対する Serial over LAN 接続の設定を行います。デフォルトでは、Serial over LAN 接続はディセーブルにされています。

Serial over LAN ポリシーを実装する場合、IPMI プロファイルを作成することも推奨します。

このポリシーはサービス プロファイルに組み込む必要があります。また、このサービス プロファイルを有効にするには、サーバーに関連付ける必要があります。

Serial over LAN 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 [Serial over LAN Policies] を右クリックし、[Create Serial over LAN Policy] を選択します。

ステップ 5 [Create Serial over LAN Policy] ウィザードで、次のフィールドに値を入力します。

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

名前	説明
[Speed] ドロップダウン リスト	次のいずれかになります。 • **[9600]** • **[19200]** • **[38400]** • **[57600]** • **115200**

ステップ 6 [OK] をクリックします。

Serial over LAN 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、[サーバ]をクリックします。
ステップ 2 **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
ステップ 3 [Serial over LAN 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。

サーバ自動構成ポリシー

サーバー自動構成ポリシーの概要

Cisco UCS Manager では、このポリシーを使用して、新しいサーバーの設定方法を決定します。サーバー自動構成ポリシーを作成すると、新しいサーバーの起動時に次の処理が行われます。

1. サーバーに対してサーバー自動構成ポリシーの資格認定が実行されます。
2. 必要な資格を満たしている場合、サーバーは、サーバー自動構成ポリシーで設定されたサービス プロファイル テンプレートから作成されたサービス プロファイルと関連付けられます。そのサービスプロファイルの名前は、Cisco UCS Manager によって付与されるサーバーの名前に基づきます。
3. サービスプロファイルは、サーバー自動構成ポリシーで設定された組織に割り当てられます。

自動構成ポリシーの作成

始める前に

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

- サーバ プール ポリシー資格情報
- サービス プロファイル テンプレート
- 組織(システムによりマルチテナンシーが実装されている場合)

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]** ノードをクリックします。

ステップ 3 [Work] ペインの [Policies] タブをクリックします。

ステップ 4 [Autoconfig Policies] サブタブをクリックします。

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 Autoconfiguration Policy] ダイアログボックスで、次のフィールドに値を入力します。

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

名前	説明
[認定（Qualification）] ドロップダウン リスト	この自動設定ポリシーに関連付けられているサーバプール ポリシー資格情報。 サーバプール ポリシー資格情報で指定された基準に合致する新しいサーバが検出されると、Cisco UCS は、[サービス プロファイルのテンプレート名（Service Profile Template Name）] ドロップダウン リスト で選択されたサービス プロファイル テンプレートに基づいて、自動的にサービス プロファイルを作成し、それをサーバに関連付けます。
[組織（Org）] ドロップダウン リスト	この自動構成ポリシーに関連付けられた組織。 Cisco UCS が自動的にサービス プロファイルを作成してサーバに関連付ける場合、サービス プロファイルはこのフィールドで選択された組織に配置されます。
[サービスプロファイルのテンプレート名（Service Profile Template Name）] ドロップダウン リスト	このポリシーに関連付けられたサービスプロファイルテンプレート。

ステップ 7 [OK] をクリックします。

自動構成ポリシーの削除

手順

ステップ 1 [ナビゲーション]ペインで、[機器]をクリックします。
ステップ 2 **[機器]** ノードをクリックします。
ステップ 3 [Work] ペインの [Policies] タブをクリックします。
ステップ 4 [Autoconfig Policies] サブタブをクリックします。
ステップ 5 削除する自動構成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。

サーバ ディスカバリ ポリシー設定

サーバー ディスカバリ ポリシーの概要

サーバー ディスカバリ ポリシーにより、新しい UCS ブレード サーバーや UCS Mini を追加したときの UCS Manager の対応方法を定義します。サーバー ディスカバリ ポリシーを作成する場合、サーバーがシャーシに追加されたときに、システムにより詳細なディスカバリを行うのか、または、ユーザーがまず新しいサーバーを確認する必要があるのかどうかを制御できます。デフォルトでは、システムにより完全なディスカバリが実行されます。

サーバー ディスカバリ ポリシーを作成した場合は、新しいサーバーを起動すると次の処理が行われます。

1. サーバー ディスカバリ ポリシー資格情報はサーバーに対して実行されます。
2. サーバーが必要な資格を満たしている場合、Cisco UCS Manager はサーバーに次の処理を適用します。
   - この処理に関して選択されたオプションに応じて、UCS Manager が新しいサーバーをただちに検出するか、または新しいサーバーに対するユーザーの確認応答を待機する
   - サーバーにスクラブ ポリシーを適用する

ハードウェアの挿入、削除、または交換によって自動的に詳細なディスカバリがトリガーされると、以下が実行されます。

1. サーバーが「保留アクティビティ」リストに移動されます。
2. サーバーで重大なハードウェア不一致エラーが発生し、ハードウェアの不一致が UCSM により検出されたことが示されます。
3. 詳細なディスカバリをトリガーするには、サーバーを明示的に認識する必要があります。

Important 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 サーバーではサポートされませんが、ラックマウント サーバーではサポートされます。ブロック サイズが 4 K のドライブがブレード サーバーに挿入された場合、検出は失敗し、次のエラー メッセージが表示されます。

`Unable to get Scsi Device Information from the system`（システムからSCSIデバイス情報を取得できません）

このエラーが発生した場合は、次の手順を実行します。

1. 4 K のドライブを取り外します。
2. サーバーを再認識します。

サーバーを再認識するとサーバーがリブートし、その結果、サービスが失われます。

サーバ ディスカバリ ポリシーの作成

Before you begin

このポリシーとサーバ プールを関連付ける予定がある場合は、サーバ プール ポリシー資格情報を作成します。

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 [Work] ペインの [Policies] タブをクリックします。

ステップ 3 [Server Discovery Policies] サブタブをクリックします。

ステップ 4 テーブル アイコン バーの [+] アイコンをクリックして、[Create Server Discovery Policy] ダイアログボックスを開きます。

ステップ 5 **[説明（Description）]** フィールドに、ディカバリ ポリシーの説明を入力します。

ステップ 6 [Action] フィールドで、次のオプションのいずれかを選択します。

- **[immediate]**：Cisco UCS Manager によって新しいサーバの自動検出が試みられます。
- **[User Acknowledged]**— ユーザーが新しいサーバの検索を指示するまで Cisco UCS Manager は待機します。

ステップ 7 (Optional) このポリシーをサーバ プールに関連付けるには、[認定（Qualification）] ドロップダウン リストでサーバ プール ポリシーの資格情報を選択します。

ステップ 8 (Optional) スクラブ ポリシーを含めるには、[Scrub Policy] ドロップダウン リストでポリシーを選択します。

ステップ 9 **[OK]** をクリックします。

What to do next

サーバ ディスカバリ ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

サーバー ディスカバリ ポリシーの削除

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 [Work] ペインの [Policies] タブをクリックします。
ステップ 3 [Server Discovery Policies] サブタブをクリックします。
ステップ 4 削除するサーバ ディスカバリ 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。

ハードウェア変更検出ポリシー

ハードウェア変更検出は、ハードウェア コンポーネントの変更が生じた場合の Cisco UCS Managerの動作を設定するためのグローバル ポリシーです。ポリシーには次の 2 つの値があります。

- [User Acknowledged]：ハードウェア インベントリ不一致エラーをすべてクリアするには、サーバーを確認する必要があります。
- [Auto Acknowledged]：ハードウェア コンポーネントの変更が検出されると、自動の詳細なディスカバリがトリガーされます。

UCSM がサーバー ハードウェア コンポーネントの変更を検出すると、クリティカル ハードウェア インベントリ不一致エラーがサーバーで発生します。エラーをクリアしてハードウェア インベントリを完了するには、手動でサーバーを確認する必要があります。サーバーを確認すると、詳細なディスカバリと詳細な関連付けがトリガーされます。

ラック サーバーの場合、エラーをクリアしてハードウェア インベントリを完了するには、サーバーを解放してから、再稼働する必要があります。

ハードウェア インベントリ不一致エラーがある場合には、ポリシーを変更できません。

ハードウェア変更検出ポリシーの設定

手順

ステップ 1 **[Equipment]** > **[Policies]** > **[Global Policies]** を選択します。

ステップ 2 [Hardware Change Discovery Policy] ポリシーで次のいずれかを選択します。

- [User Acknowledged]：ハードウェア インベントリ不一致エラーをすべてクリアするには、サーバを確認する必要があります。
- [Auto Acknowledged]：ハードウェア コンポーネントの変更が検出されると、自動の詳細なディスカバリがトリガーされます。

ステップ 3 [Save Changes] をクリックします。

サーバ継承ポリシー設定

サーバー継承ポリシーの概要

このポリシーは、サーバー用のサービス プロファイルを作成するために、サーバー ディスカバリ プロセス中に呼び出されます。このポリシーから作成されたサービス プロファイルはすべて、製造元でブレードに設定された値を使用します。このポリシーは次の機能を実行します。

- サーバーのインベントリの分析
- 選択された組織へのサーバーの割り当て（設定されている場合）
- 製造元でサーバーに設定された ID を使って、このサーバーのサービス プロファイルを作成

このポリシーを使って作成したサービス プロファイルは他のサーバーに移行できません。

サーバ継承ポリシーの作成

VIC アダプタが搭載されたブレード サーバまたはラックマウント サーバ（Cisco UCS M81KR 仮想インターフェイス カードなど）の場合、サーバのアイデンティティ値は製造時にサーバ ハードウェアに書き込まれません。その結果、アダプタのアイデンティティは、デフォルト プールから取得する必要があります。デフォルト プールに、サーバに割り当てるのに十分なエントリが格納されていない場合、サービス プロファイルの関連付けが設定エラーにより失敗します。

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 [Work] ペインの [Policies] タブをクリックします。

ステップ 3 [Server Inheritance Policies] サブタブをクリックします。

ステップ 4 テーブルの下部にあるアイコン バーで、[+ Add] をクリックします。

[+ Add] が無効になっている場合は、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 Server Inheritance Policy] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[説明（Description）] フィールド	ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[認定（Qualification）] ドロップダウン リスト	このポリシーを 1 つ以上の特定のサーバプールに関連付ける場合は、これらのプールを識別するサーバ プール資格ポリシーを選択します。
[組織（Org）] ドロップダウン リスト	このポリシーに組織を関連付ける場合、または現在の関連付けを変更する場合は、ドロップダウン リストから組織を選択します。

ステップ 6 [OK] をクリックします。

サーバー継承ポリシーの削除

手順

ステップ 1 [ナビゲーション]ペインで、[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 [Server Inheritance Policies] サブタブをクリックします。
ステップ 4 削除するサーバ継承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。

サーバ プール ポリシー設定

サーバー プール ポリシーの概要

このポリシーはサーバー ディスカバリ プロセス中に呼び出されます。これは、サーバー プール ポリシー資格情報により、サーバーと、ポリシーで指定されたターゲット プールが一致した場合にどのような処理が行われるかを定義します。

サーバーが複数のプールに適合したときに、これらのプールにサーバー プール ポリシーがあった場合、このサーバーはこれらすべてのプールに追加されます。

サーバ プール ポリシーの作成

Before you begin

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

- 少なくとも 1 つのサーバ プール
- サーバ プール ポリシー資格情報（サーバをプールに自動的に追加する場合）

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]** > **[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 [Server Pool Policies] を右クリックし、[Create Server Pool Policy] を選択します。
ステップ 5 [Create Server Pool Policy] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
[説明（Description）] フィールド	ポリシーの説明。ポリシーを使用すべき場所や条件についての情報を含めることをお勧めします。 256 文字以下で入力します。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Target Pool] ドロップダウン リスト	このポリシーをサーバ プールに関連付ける場合は、ドロップダウン リストから該当のプールを選択します。
[認定（Qualification）] ドロップダウン リスト	このポリシーを 1 つ以上の特定のサーバプールに関連付ける場合は、これらのプールを識別するサーバ プール資格ポリシーを選択します。

ステップ 6 **[OK]** をクリックします。

サーバー プール ポリシーの削除

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（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
ステップ 3 [Server Pool 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。

サーバ プール ポリシー資格情報設定

サーバー プール ポリシー資格情報の概要

このポリシーは、ディスカバリ プロセス中に実行されたサーバーのインベントリに基づいて、サーバーを資格認定します。資格情報は、サーバーが選択基準を満たすかどうかを判断するために、ポリシーで設定されたルールです。たとえば、データセンタープールのサーバーの最小メモリ容量を指定するルールを作成できます。

資格情報は、サーバ プール ポリシーだけではなく、その他のポリシーでも、サーバを配置するために使用されます。たとえば、サーバがある資格ポリシーの基準を満たしている場合、このサーバを 1 つ以上のサーバ プールに追加したり、自動的にサービス プロファイルと関連付けたりできます。

サーバプールポリシー資格情報を使用すると、次の基準に従ってサーバを資格認定できます。

- アダプタのタイプ
- シャーシの場所
- メモリのタイプと設定
- 電源グループ
- CPU のコア数、タイプ、および設定
- ストレージの設定と容量
- サーバーのモデル

実装によっては、サーバー プール ポリシー資格情報を使用して、次を含む複数のポリシーを設定する必要があります。

- 自動構成ポリシー
- シャーシ ディスカバリ ポリシー
- サーバー ディスカバリ ポリシー
- サーバー継承ポリシー
- サーバー プール ポリシー

サーバ プール ポリシーの資格情報の作成

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]** > **[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 [Server Pool Policy Qualifications] ノードを右クリックし、[Create Server Pool Policy Qualification] を選択します。

ステップ 5 [Create Server Pool Policy Qualification] ダイアログボックスに、ポリシーの一意の名前および説明を入力します。

ステップ 6 (Optional) このポリシーを使用して、アダプタ構成に基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Adapter Qualifications] をクリックします。

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

名前	説明
[Type] ドロップダウン リスト	アダプタ タイプ アダプタの資格を保存すると、このタイプは変更できなくなります。
[PID] フィールド	アダプタ PID が一致する必要のある正規表現。
[Maximum Capacity] フィールド	選択されたタイプの最大容量 容量を指定するには、[Select] を選択し、必要な最大容量を入力します。1 ～ 65535 の整数を入力できます。

c) [OK] をクリックします。

ステップ 7 (Optional) このポリシーを使用して、サーバが物理的に存在するシャーシに基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Chassis/Server Qualifications] をクリックします。

b) [Create Chassis and Server Qualifications] ダイアログボックスの 領域で次のフィールドに値を入力して、使用するシャーシの範囲を指定します。

- **[First Chassis ID]** フィールド—このポリシーに関連付けられたサーバ プールが使用できる最初のシャーシ ID。
- **[Number of Chassis]** フィールド—プールに含めるシャーシの合計数（**[First Chassis ID]** フィールドで指定されたシャーシから始まります）。

Example:

たとえば、シャーシ 5、6、7、および 8 を使用する場合、**[First Chassis ID]** フィールドに **5** を入力し、**[Number of Chassis]** フィールドに **4** を入力します。シャーシ 3 だけを使用する場合、**[First Chassis ID]** フィールドに **3** を入力し、**[Number of Chassis]** フィールドに **1** を入力します。

Tip シャーシ5、6、および9を使用する場合、5 ～ 6の範囲のシャーシ/サーバ資格を作成し、シャーシ9には別の資格を作成します。必要に応じた数のシャーシ/サーバ資格を作成できます。

c) [Finish] をクリックします。

ステップ 8 (Optional) このポリシーを使用して、サーバが物理的に存在するシャーシとスロットの両方に基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Chassis/Server Qualifications] をクリックします。

b) [Create Chassis and Server Qualifications] ダイアログボックスの 領域で次のフィールドに値を入力して、使用するシャーシの範囲を指定します。

- **[First Chassis ID]** フィールド—このポリシーに関連付けられたサーバ プールが使用できる最初のシャーシ ID。
- **[Number of Chassis]** フィールド—プールに含めるシャーシの合計数（**[First Chassis ID]** フィールドで指定されたシャーシから始まります）。

c) テーブルで、[Add] をクリックします。

d) [Create Server Qualifications] ダイアログボックスで次のフィールドに値を入力して、使用する範囲のサーバの範囲を指定します。

- **[First Slot ID]** フィールド—このポリシーに関連付けられているサーバ プールから取得できる最初のスロット ID。
- **[Number of Slots]** フィールド—このポリシーに関連付けられているサーバ プールから取得できるスロットの合計数。

e) [Finish Stage] をクリックします。

f) 別のスロットの範囲を追加するには、[Add] をクリックし、ステップ d および e を繰り返します。

g) スロット範囲の指定を終了したら、[Finish] をクリックします。

ステップ 9 (Optional) このポリシーを使用して、メモリ構成に基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Memory Qualifications] をクリックします。

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

名前	説明
[Clock] フィールド	必要な最小クロック速度（MHz）。
[Latency] フィールド	許容される最大遅延（ナノ秒）。
[Min Cap] フィールド	最小限必要なメモリ容量（MB 単位）。
[Max Cap] フィールド	メモリの許容最大容量（MB 単位）。
[Width] フィールド	データ バスの最小幅。

名前	説明
[Units] フィールド	[Width] フィールドの値と関連付けられる測定単位。

c) [OK] をクリックします。

ステップ 10 (Optional) このポリシーを使用して、CPU/コア構成に基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create CPU/Cores Qualifications] をクリックします。

b) [Create CPU/Cores Qualifications] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Processor Architecture] ドロップダウン リスト	このポリシーが適用される CPU アーキテクチャ。
[PID] フィールド	プロセッサ PID が一致する必要のある正規表現。
[Min Number of Cores] フィールド	最小限必要な CPU コアの数。 容量を指定するには、[select] を選択し、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。
[Max Number of Cores] フィールド	CPU コアの許容最大数。 容量を指定するには、[select] を選択し、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。
[Min Number of Threads] フィールド	最小限必要な CPU スレッドの数。 容量を指定するには、[select] を選択し、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。
[Max Number of Threads] フィールド	CPU スレッドの許容最大数。 容量を指定するには、[select] を選択し、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。
[CPU Speed] フィールド	最小限必要な CPU 速度。 容量を指定するには、[select] を選択し、CPU の最小速度を入力します。
[CPU Stepping] フィールド	最小限必要な CPU バージョン。 容量を指定するには、[select] を選択し、CPU の最大速度を入力します。

c) [OK] をクリックします。

ステップ 11 (Optional) このポリシーを使用して、ストレージ構成および容量に基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Storage Qualifications] をクリックします。

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

名前	説明
[Diskless] フィールド	使用可能なストレージをディスクレスにする必要があるかどうか。次のいずれかになります。 • [Unspecified]：どのストレージ タイプも受け入れ可能です。 • [Yes]：ストレージをディスクレスにする必要があります。 • [No]：ストレージをディスクレスにできません。
[Number of Blocks] フィールド	最小限必要なブロック数。 容量を指定するには、[select] を選択し、ブロックの数を入力します。
[Block Size] フィールド	最小限必要なブロック サイズ（バイト単位）。 容量を指定するには、[select] を選択し、ブロックのサイズを入力します。
[Min Cap] フィールド	サーバ内のすべてのディスクの最小ストレージ容量（MB 単位）。 容量を指定するには、[select] を選択し、ストレージの最小容量を入力します。
[Max Cap] フィールド	ストレージの許容最大容量（メガバイト単位）。 容量を指定するには、[select] を選択し、ストレージの最大容量を入力します。
[Per Disk Cap] フィールド	最小限必要なディスクあたりのストレージ容量（ギガバイト単位）。 容量を指定するには、[select] を選択し、各ディスクの最小容量を入力します。
[Units] フィールド	ユニット数。 容量を指定するには、[select] を選択し、必要なユニットを入力します。

名前	説明
[Number of Flex Flash Cards] フィールド	FlexFlash カードの数。 容量を指定するには、[select] を選択し、必要なユニットを入力します。
[Disk Type] フィールド	ディスク タイプ。次のいずれかになります。 • [Unspecified]：どのディスク タイプも受け入れ可能です。 • [HDD]：ディスクは HDD にする必要があります。 • [SSD]：ディスクは SSD （SATA または SAS）にする必要があります。

c) [OK] をクリックします。

ステップ 12 (Optional) このポリシーを使用して、サーバのモデルに基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Server Model Qualifications] をクリックします。
b) [Create Server Model Qualifications] ダイアログボックスに、[Model] フィールドと一致する正規表現を入力します。
c) [OK] をクリックします。

ステップ 13 (Optional) このポリシーを使用して、電源グループに基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Group Power Qualifications] をクリックします。
b) [Create Group Power Qualifications] ダイアログボックスで、[Power Group] ドロップダウンリストから電源グループを選択します。
c) [OK] をクリックします。

ステップ 14 (Optional) このポリシーを使用して、関連付けられたサーバ プールに追加できるラックマウント サーバの資格認定を実行するには、次の手順を実行します。

a) [Create Rack Qualifications] をクリックします。
b) [Create Storage Qualifications] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[First Slot ID] フィールド	このポリシーに関連付けられているサーバ プールが取得に使用できる最初のラックマウント サーバ スロット ID。
[Number of Slots] フィールド	このポリシーに関連付けられているサーバ プールが取得に使用できるラックマウント サーバ スロットの合計数。

ステップ 15 テーブル内の資格を確認し、必要に応じて修正します。

ステップ 16 **[OK]** をクリックします。

サーバ プール ポリシーの資格情報の削除

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（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
ステップ 3 [Server Pool Policy Qualifications] ノードを展開します。
ステップ 4 削除するポリシー資格情報を右クリックし、[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。

サーバ プール ポリシーの資格情報からの資格の削除

1 つまたは複数の資格のセットを削除してサーバプールポリシーの資格情報を変更するには、この手順を使用します。

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（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。
ステップ 3 [Server Pool Policy Qualifications] ノードを展開します。
ステップ 4 変更するポリシーを選択します。
ステップ 5 [Work] ペインで、[Qualifications] タブを選択します。
ステップ 6 資格のセットを削除するには、次の手順を実行します。
a) テーブルで、資格のセットを示す行を選択します。
b) この行を右クリックし、[Delete] を選択します。
ステップ 7 **[Save Changes]**をクリックします。

vNIC/vHBA 配置ポリシー設定

vNIC/vHBA 配置ポリシー

vNIC/vHBA 配置ポリシーは、次のことを決定するために使用されます。

- 仮想ネットワーク インターフェイス接続（vCon）をサーバー上の物理アダプタにマッピングする方法。
- 各 vCon に割り当てることのできる vNIC または vHBA のタイプ。

各 vNIC/vHBA 配置ポリシーには、物理アダプタの仮想表現である 4 つの vCon が含まれています。vNIC/vHBA 配置ポリシーがサービス プロファイルに割り当てられ、サービス プロファイルがサーバーに関連付けられると、vNIC/vHBA 配置ポリシーの vCon が物理アダプタに割り当てられ、vNIC と vHBA がそれらの vCon に割り当てられます。

1 つのアダプタを持つブレード サーバーやラック サーバーの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを含むサーバーでは、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバーまたはラック サーバーの場合、Cisco UCS は、サーバーのタイプと選択された仮想スロット マッピング スキーム（**ラウンド ロビン**または**線形順序**）に基づいて vCon を割り当てます。使用可能なマッピング スキームの詳細については、vCon のアダプタへの配置 （405 ページ）を参照してください。

Cisco UCS は、vCon の割り当て後、vNIC と vHBA を各 vCon の **[Selection Preference]**に基づいて割り当てます。 次のいずれかになります。

（注） vHBA の PCI 順序を指定できますが、任意の順序は、vNIC または vHBA など、相互間ではなく、デバイスのクラス内で機能します。アダプタ内で、vNIC は vHBA よりも常に前に配置されます。

- **[All]**：設定されている vNIC および vHBA すべてを vCon に割り当て可能です。明示的に割り当てられているか、割り当て解除されているか、ダイナミック割り当てかは問いません。これはデフォルトです。
- **[Assigned Only]**：vNIC および vHBA は vCon に明示的に割り当てる必要があります。サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。
- **[Exclude Dynamic]**：ダイナミック vNIC および vHBA を vCon に割り当てることはできません。vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- **[Exclude Unassigned]**：設定解除されている vNIC および vHBA を vCon に割り当てることはできません。vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。
- **[Exclude usNIC]**：Cisco usNIC を vCon に割り当てることはできません。vCon は、明示的に割り当てられている、割り当てられていない、または動的であっても、その他すべての設定された vNIC と vHBA に使用できます。

（注） **exclude-usnic** に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

vNIC/vHBA 配置ポリシーをサービス プロファイルに含めない場合、Cisco UCS Manager はデフォルトで、vCon マッピング スキームを [ラウンド ロビン（Round Robin）]、vNIC/vHBA 選択プリファレンスを [すべて（All）] に設定し、各アダプタの機能と相対的な処理能力に基づいて vNIC と vHBA をアダプタ間に配分します。

vCon のアダプタへの配置

Cisco UCS は、サービス プロファイルの各 vCon をサーバー上の物理アダプタにマッピングします。マッピングの実行方法、およびサーバー内の特定のアダプタへの vCon の割り当て方法は、次の条件によって決まります。

- サーバーのタイプ。2 つのアダプタ カードを搭載した N20-B6620-2 および N20-B6625-2 ブレード サーバーは、他のサポートされるラック サーバーまたはブレード サーバーとは異なるマッピング スキームを使用します。
- サーバー内のアダプタの数。
- vNIC/vHBA 配置ポリシー内の仮想スロット マッピング スキームの設定（該当する場合）。

vNIC および vHBA を vCon に割り当てるための vNIC/vHBA 選択環境設定を設定するときは、この配置を検討する必要があります。

（注） vCon のアダプタへの配置は、アダプタの PCIE スロット番号とは関係ありません。vCon の配置のために使用されるアダプタ番号は、アダプタの PCIE スロット番号ではなく、サーバー検出中にそれらに割り当てられる ID です。

N20-B6620-2 および N20-B6625-2 ブレード サーバーでの vCon のアダプタへの配置

N20-B6620-2 および N20-B6625-2 ブレード サーバーの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。これらのブレード サーバーのうちの 1 台に単一のアダプタが備えられている場合、Cisco UCS は、そのアダプタにすべての vCon を割り当てます。サーバーに 2 個のアダプタがある場合、vCons 割り当ては仮想スロットのマッピング方式によって異なります。

- **[Round Robin]**：Cisco UCS は vCon4 を Adapter1 に、vCon1 と vCon3 を Adapter2 に割り当てます。これはデフォルトです。
- **[Linear Ordered]**—Cisco UCS は vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。

vCon のアダプタへの配置（他のすべてのサポート対象サーバーの場合）

N20-B6620-2 および N20-B6625-2 ブレード サーバーに加え、Cisco UCS によりサポートされるその他すべてのサーバーでは、vCon の割り当ては、サーバーに搭載されるアダプタ数と仮想スロット マッピング スキームに応じて異なります。

1 つのアダプタを持つブレード サーバーやラック サーバーの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを含むサーバーでは、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバーまたはラック サーバーの場合、Cisco UCS は、選択した仮想スロット マッピング スキーム（ラウンド ロビンまたは線形順序）に基づいて vCons を割り当てます。

表 *8:* ラウンドロビン マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1
2	アダプタ1	アダプタ2	アダプタ1	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ2
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

ラウンドロビンはデフォルトのマッピング スキームです。

表 *9:* 線形順序マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1
2	アダプタ1	アダプタ1	アダプタ2	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ3
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

vCon への vNIC/vHBA の割り当て

Cisco UCS Manager には、vNIC/vHBA 配置ポリシーによって vCon に vNIC および vHBA を割り当てる 2 種類のオプション（明示的割り当てと暗黙的割り当て）があります。

vNIC および vHBA の明示的割り当て

明示的割り当てでは、vCon を指定してから、vNIC または vHBA を割り当てるアダプタを指定します。この割り当てオプションは、サーバー上のアダプタに vNIC および vHBA を配布する方法を決める必要がある場合に使用します。

明示的割り当ての場合、vCon および関連付ける vNIC と vHBA を設定するには、次の手順を実行します。

- vCon 設定を任意の使用可能なオプションに設定します。vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバーに関連付けられているサービス プロファイルで設定できます。vCon で [All] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。
- vNIC および vHBA を vCon に割り当てます。この割り当ては、vNIC または vHBA の仮想ホスト インターフェイス配置プロパティを使用して行うか、サーバーに関連付けられているサービス プロファイルで設定できます。

vNIC や vHBA をそれらのタイプ用に設定されていない vCon に割り当てようとすると、Cisco UCS Manager によって、設定エラーを示すメッセージ表示されます。

サービス プロファイルの関連付け中、Cisco UCS Manager は、ポリシーの設定に従って vNIC および vHBA を割り当てる前に、設定された vNIC および vHBA の配置をサーバー内の物理アダプタの数および機能と比較して検証します。負荷分散は、このポリシーで設定された vCon およびアダプタへの明示的な割り当てに基づいて実行されます。

1 つ以上の vNIC または vHBA の割り当てがアダプタでサポートされない場合、Cisco UCS Manager はサービス プロファイルに対してエラーを発生させます。

（注） vHBA の PCI 順序を指定できますが、任意の順序は、vNIC または vHBA など、相互間ではなく、デバイスのクラス内で機能します。アダプタ内で、vNIC は vHBA よりも常に前に配置されます。

vNIC および vHBA の暗黙的割り当て

暗黙的割り当てでは、Cisco UCS Manager は vCon を決定した後で、アダプタの機能とそれらの相対的な処理能力に基づいて vNIC または vHBA を割り当てるアダプタを決定します。この割り当てオプションは、vNIC または vHBA を割り当てるアダプタがシステム設定において重要ではない場合に使用します。

暗黙的割り当ての場合に vCon を設定するには、次の手順を実行します。

- vCon 設定を [All]、[Exclude Dynamic]、または [Exclude Unassigned] に設定します。vCon は、vNIC/vHBA配置ポリシーを使用して設定するか、サーバーに関連付けられているサービス プロファイルで設定できます。
- vCon 設定を [Assigned Only] にしないでください。この設定を使用して暗黙的割り当てを実行することはできません。

- vNIC または vHBA を vCon に割り当てないでください。

サービス プロファイルの関連付け中、Cisco UCS Manager は、サーバー内の物理アダプタの数および機能を検証し、それに従って vNIC および vHBA を割り当てます。負荷分散はアダプタの機能に基づいて実行され、vNIC および vHBA の配置は、システムで決定された実際の順序に従って実行されます。たとえば、あるアダプタが他のアダプタよりも多くの vNIC を処理できる場合、そのアダプタにはより多くの vNIC が割り当てられます。

サーバーに設定されている数の vNIC および vHBA をアダプタでサポートできない場合、Cisco UCS Manager は、サービス プロファイルに対する障害を生成します。

デュアル アダプタ環境での vNIC の暗黙的割り当て

各スロットにアダプタ カードを搭載したデュアル スロット サーバーで暗黙的な vNIC 割り当てを使用する場合、Cisco UCS Manager は通常、次のように vNIC/vHBA を割り当てます。

- サーバーの両方のスロットに同じアダプタがある場合、Cisco UCS Manager は、各アダプタに vNIC と vHBA を半分ずつ割り当てます。
- サーバーに 1 つの非 VIC アダプタと 1 つの VIC アダプタがある場合、Cisco UCS Manager は、2 つの vNIC と 2 つの vHBA を非 VIC アダプタに割り当て、残りの vNIC と vHBA を VIC アダプタに割り当てます。
- サーバーに 2 つの異なる VIC アダプタがある場合、Cisco UCS Manager は、2 つのアダプタの相対的な処理能力に基づいて、vNIC と vHBA を比例的に割り当てます。

次の例は、サポートされるアダプタ カードのさまざまな組み合わせに対して、Cisco UCS Manager が vNIC と vHBA を割り当てる一般的な方法を示しています。

- 4 つの vNIC を設定するときに、サーバーに 2 つの Cisco UCS M51KR-B Broadcom BCM57711 アダプタ（それぞれ 2 つの vNIC）が搭載されている場合、Cisco UCS Manager は 2 つの vNIC を各アダプタに割り当てます。
- 50 の vNIC を設定するときに、サーバーに 1 つの Cisco UCS CNA M72KR-E アダプタ（2 つの vNIC）および 1 つの Cisco UCS M81KR 仮想インターフェイス カード アダプタ（128 の vNIC）が搭載されている場合、Cisco UCS Manager は 2 つの vNIC を Cisco UCS CNA M72KR-E アダプタに割り当て、48 の vNIC を Cisco UCS M81KR 仮想インターフェイス カード アダプタに割り当てます。
- 150 の vNIC を設定するときに、サーバーに 1 つの Cisco UCS M81KR 仮想インターフェイス カード アダプタ（128 の vNIC）および 1 つの Cisco UCS VIC-1240 仮想インターフェイス カード アダプタ（256 の vNIC）が搭載されている場合、Cisco UCS Manager は 50 の vNIC を Cisco UCS M81KR 仮想インターフェイス カード アダプタに割り当てて、100 の vNIC を Cisco UCS VIC-1240 仮想インターフェイス カード アダプタに割り当てます。

（注） vNIC をファブリック フェールオーバー用に設定し、ダイナミック vNIC をサーバー用に設定した場合に、この暗黙的な割り当てに対する例外が発生します。

1 つのアダプタが vNIC フェールオーバーをサポートしない環境で vNIC ファブリック フェールオーバーを含む設定を行った場合、Cisco UCS Manager は、ファブリック フェールオーバーが有効になっているすべての vNIC を、それらをサポートしているアダプタに暗黙的に割り当てます。ファブリック フェールオーバー用に設定された vNIC のみが設定に含まれている場合、それらをサポートしてないアダプタには vNIC が暗黙的に割り当てられません。一部の vNIC がファブリック フェールオーバー用に設定され、一部の vNIC がそうでない場合、Cisco UCS Manager は、上記の比率に従って、すべてのフェールオーバー vNIC をそれらをサポートしているアダプタに割り当て、少なくとも 1 つの非フェールオーバー vNIC をそれらをサポートしていないアダプタに割り当てます。

動的 vNIC が含まれる設定の場合、同じ暗黙的割り当てが実行されます。Cisco UCS Manager は、すべての動的 vNIC を、それらをサポートするアダプタに割り当てます。ただし、ダイナミック vNIC とスタティック vNIC の組み合わせでは、少なくとも 1 つのスタティック vNIC がダイナミック vNIC をサポートしていないアダプタに割り当てられます。

vNIC/vHBA 配置ポリシーの作成

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 [vNIC/vHBA Placement Policies] を右クリックし、[Create Placement Policy] を選択します。

ステップ 5 [Create Placement Policy] ダイアログボックスで、次の手順を実行します。

a) 次のフィールドに入力します。

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

名前	説明
[Virtual Slot Mapping Scheme] フィールド	

名前	説明
	Cisco UCS サーバーの PCIe アダプタ カードに、仮想ネットワーク インターフェイス接続（vCon）を割り当てます。各 vCon は、vNICs や vHBA に割り当て可能な物理アダプタとして仮想表示されます。 1 つのアダプタを持つブレード サーバーやラック サーバーの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを含むサーバーでは、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。 2 つまたは 3 つのアダプタを持つブレード サーバーやラック サーバーの場合は、Cisco UCS は選択された仮想スロット マッピング スキームに基づいて、vCon を割り当てます。次のいずれかになります。 • [Round Robin]：2 つのアダプタ カードを持つサーバーの場合、Cisco UCS は vCon1 と vCon3 をアダプタ 1 に、vCon2 と vCon4 をアダプタ 2 に割り当てます。 サーバーに 3 つのアダプタ カードがある場合、Cisco UCS は vCon1 をアダプタ 1 に、vCon2 と vCon4 をアダプタ 2 に、vCon3 をアダプタ 3 に割り当てます。 これがデフォルトのスキームです。 • [Linear Ordered]：2 つのアダプタ カードを持つサーバーの場合、Cisco UCS は vCon1 と vCon2 をアダプタ 1 に、vCon3 と vCon4 をアダプタ 2 に割り当てます。 サーバーに 3 つのアダプタ カードがある場合、Cisco UCS は vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 と vCon4 をアダプタ 3 に割り当てます。 （注） N20-B6620-2 および N20-B6625-2 ブレード サーバーの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。これらのブレード サーバーのうちの 1 台に単一のアダプタが備えられている場合、Cisco UCS は、そのアダプタにすべての vCon を割り当てます。サーバーに 2 個のアダプタがある場合、vCons 割り当ては仮想スロットのマッピング方式によって異なります。 • **[Round Robin]**：Cisco UCS は vCon4 を Adapter1 に、vCon1 と vCon3 を Adapter2 に割り当てます。これはデフォルトです。

名前	説明
	• **[Linear Ordered]**—Cisco UCS は vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。 Cisco UCS は、vCon の割り当て後、vNIC と vHBA を各 vCon の **[Selection Preference]**に基づいて割り当てます。

b) 各 **[Virtual Slot]** の **[Selection Preference]** カラム のドロップダウン リストで、次のいずれかを選択します。

- **[All]**：設定されている vNIC および vHBA すべてを vCon に割り当て可能です。明示的に割り当てられているか、割り当て解除されているか、ダイナミック割り当てかは問いません。これはデフォルトです。
- **[Assigned Only]**：vNIC および vHBA は vCon に明示的に割り当てる必要があります。サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。
- **[Exclude Dynamic]**：ダイナミック vNIC および vHBA を vCon に割り当てることはできません。vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- **[Exclude Unassigned]**：設定解除されている vNIC および vHBA を vCon に割り当てることはできません。vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。
- **[Exclude usNIC]**：Cisco usNIC を vCon に割り当てることはできません。vCon は、明示的に割り当てられている、割り当てられていない、または動的であっても、その他すべての設定された vNIC と vHBA に使用できます。

  （注） **exclude-usnic** に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

c) [OK] をクリックします。

vNIC/vHBA 配置ポリシーの削除

手順

ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[サーバ（Servers）]** > **[ポリシー（Policies）]** > ***[Organization_Name]*** の順に展開します。

ステップ 3 [NIC/vHBA Placement 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。

vCon への vNIC の明示的割り当て

始める前に

次のいずれかの値と共に、vNIC/vHBA 配置ポリシーまたはサービス プロファイルを介して vCon を設定します。

- **[割り当てのみ（Assigned Only）]**
- **[ダイナミックを除外（Exclude Dynamic）]**
- **[割り当て解除を除外（Exclude Unassigned）]**

vCon で **[すべて（All）]** が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。しかし、この設定では制御が限定されます。

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 vNIC を、明示的に vCon に割り当てるサービス プロファイ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 **[Service_Profile_Name]** > **[vNICs]** の順に展開します。

ステップ 5 明示的に vCon に割り当てる vNIC 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 [Virtual Host Interface Placement] セクションで、次のフィールドに入力します。

名前	説明
[Desired Placement] ドロップダウン リスト	vNIC 用のユーザー指定仮想ネットワーク インターフェイス（vCon）配置。次のいずれかになります。 • **[Any]**：Cisco UCS Managerが vNIC の割り当てられる vCon を決定できます。 • [1]：vNIC を vCon1 に明示的に割り当てます。 • [2]：vNIC を vCon2 に明示的に割り当てます。 • [3]：vNIC を vCon3 に明示的に割り当てます。 • [4]：vNIC を vCon4 に明示的に割り当てます。
[Actual Assignment] フィールド	サーバーの vNIC の実際の vCon 割り当て。

vNIC をその vNIC タイプ用に設定されていない vCon に割り当てようとすると、Cisco UCS Manager は設定エラーを知らせるメッセージ ボックスを表示します。別の vCon に vNIC を割り当てるか、サービス プロファイルの vCon 設定を変更する必要があります。

ステップ 8 [Order] セクションで、次のフィールドに入力します。

名前	説明
[Desired Order] フィールド	vNIC のユーザー指定の PCI 順序。 0 ～ 128 の整数を入力します。サーバーには 128 を超える vNIC を作成できません。
[Actual Order] フィールド	サーバーの vNIC の実際の PCI 順序。

ステップ 9 **[Save Changes]**をクリックします。

vCon への vHBA の明示的割り当て

始める前に

次のいずれかの値と共に、vNIC/vHBA 配置ポリシーまたはサービス プロファイルを介して vCon を設定します。

- **[割り当てのみ（Assigned Only）]**
- **[ダイナミックを除外（Exclude Dynamic）]**
- **[割り当て解除を除外（Exclude Unassigned）]**

vCon で **[すべて（All）]** が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。しかし、この設定では制御が限定されます。

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 を明示的に vCon に割り当てるサービス プロファイ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 [Service_Profile_Name] > **[vHBAs]**を展開します。

ステップ 5 明示的に vCon に割り当てる 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 [Virtual Host Interface Placement] セクションで、次のフィールドに入力します。

名前	説明
[Desired Placement] フィールド	vHBA 用のユーザ指定仮想ネットワーク インターフェイス（vCon）配置。次のいずれかになります。 • [Any]：Cisco UCS Manager が、vHBA を割り当てる vCon を決定できるようにします。 • [1]：vHBA を vCon1 に明示的に割り当てます。 • [2]：vHBA を vCon2 に明示的に割り当てます。 • [3]：vHBA を vCon3 に明示的に割り当てます。 • [4]：vHBA を vCon4 に明示的に割り当てます。
[Actual Assignment] フィールド	サーバの vHBA の実際の vCon 割り当て。

vHBA をその vHBA タイプ用に設定されていない vCon に割り当てようとすると、Cisco UCS Manager は設定エラーを知らせるメッセージ ボックスを表示します。別の vCon に vHBA を割り当てるか、サービス プロファイルの vCon 設定を変更する必要があります。

ステップ 8 [Order] セクションで、次のフィールドに入力します。

名前	説明
[Desired Order] フィールド	vHBA のユーザ指定の PCI 順序。 0 ～ 128 の整数を入力します。サーバには 128 を超える vHBA を作成できません。
[Actual Order] フィールド	サーバの vHBA の実際の PCI 順序。

ステップ 9 **[Save Changes]**をクリックします。

ダイナミック vNIC の前にスタティック vNIC を配置

最適なパフォーマンスを得るために、スタティック vNIC とスタティック vHBA は、PCIe バス上のダイナミック vNIC の前に配置する必要があります。スタティック vNIC は、スタティック vNIC および vHBA の両方を参照します。Cisco UCS Manager リリース 2.1 は、スタティックおよびダイナミック vNIC の順序に関する次の機能を備えています。

- Cisco UCS Manager リリース 2.1 にアップグレードした後、既存のサービス プロファイル（Cisco UCS Manager リリース 2.1 以前のリリースで定義されたプロファイル）に変更がない場合は、vNIC の順序は変更されません。
- Cisco UCS Manager リリース 2.1 へのアップグレード後、vNIC 関連の変更によって vNIC マップの順序が変更される場合があります。その場合、結果としてすべてのダイナミック vNIC がスタティック vNIC の後に配置されます。
- Cisco UCS Manager リリース 2.1 で新しく作成されたサービス プロファイルでは、スタティック vNIC が常にダイナミック vNIC の前に順序付けられます。
- 上記の動作は、スタティック vNIC またはダイナミック vNIC の作成または削除の順番に依存しません。
- SRIOV 対応のサービス プロファイルの場合は、UCSM によって対応する仮想関数（VF）の前に vNIC 物理関数（PF）が挿入されます。この方式では、VF が PCIe バスおよび BDF 上の親 PF vNIC の近くに配置され、VF の継続的な増分順序になることが保証されます。

例

Cisco UCS Manager リリース 2.0 での当初のデバイス順序

```
dyn-vNIC-1 1
dyn-vNIC-2 2
```

Cisco UCS Manager リリース 2.0 での新たなデバイス順序（2 つのスタティック vNIC を追加）

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

Cisco UCS Manager リリース 2.1 へのアップグレード後（vNIC 関連の変更がサービス プロファイルで行われる前）

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

Cisco UCS Manager リリース 2.1 での新たなデバイス順序（ポリシー数を 2 から 4 に変更することによって 2 つのダイナミック vNIC を追加）

```
dyn-vNIC-1 3
dyn-vNIC-2 4
eth-vNIC-1 1
eth-vNIC-2 2
dyn-vNIC-3 5
dyn-vNIC-4 6
```

多機能 PCIe デバイスとしてのダイナミック vNIC

Cisco UCS Manager バージョン 2.1 は、0 機能デバイス（すべてのスタティック vNIC に対応する新しい BUS）としてスタティック vNIC をプロビジョニングします。多機能ダイナミック vNIC は、新しいバス スロットから最後のスタティック vNIC/vHBA の後に配置されます。

（注） Cisco UCS Manager バージョン 2.1 は、新しい StaticZero モードをサポートしています。

表 *10* : バージョンの互換性

Cisco UCS Manager		
バージョン 1.4 **方式：ZeroFunction**	**バージョン 2.0** **方式：ZeroFunction/MultiFunction**	**バージョン 2.1** **方式：ZeroFunction/MultiFunction/StaticZero**
スタティックおよびダイナミック vNIC はすべて、バス [0-57]、関数 [0] 上にあります。 < ZeroFunction モード >	スタティック vNIC およびダイナミック vNIC は、バス [0-57]、関数 [0-7] 上にありますバス 0、関数 0 バス 0、関数 7 バス 1、関数 0 < MultiFunction モード >	スタティック vNIC または PF は、バス [0-57]、関数 [0] 上にあります。SRIOV：対応する VF が同一バスおよび関数 [1-255] 上にあります。 No-SRIOV：ダイナミック vNIC は、バス [0-57]、関数 [0-7] 上にあります。 < StaticZero モード>

Cisco UCS Manager		
バージョン 1.4 方式：ZeroFunction	バージョン 2.0 方式：ZeroFunction/MultiFunction	バージョン 2.1 方式：ZeroFunction/MultiFunction/StaticZero
	Balboa からのアップグレードでは、バスが <= 57 になるまで BDF の番号の付け直しは行われません（ZeroFunction モードのまま）。 デバイスが 58 台を超えると、MultiFunction モードに切り替わります。	Balboa からのアップグレードでは、バスが <= 57 になるまで BDF の番号の付け直しは行われません（ZeroFunction モードのまま）。デバイスが 58 台またはプラットフォーム固有の最大 PCIe バス数を超えるか、SRIOV 設定に変更されると、StaticZero モードに切り替わります。
		Cisco UCS Manager バージョン 2.0 からのアップグレードでは、BDF の番号の付け直しは行われません（ZeroFunction/MultiFunction モードのまま）。デバイスが 58 台またはプラットフォーム固有の最大 PCIe バス数を超えるか、SRIOV 設定に変更されると、StaticZero モードに切り替わります。

vNIC/vHBA のホスト ポートの配置

vNIC/vHBA を vCon に割り当てた後、それを特定のアダプタのホスト ポートのいずれかに配置できます。配置先のホスト ポートは明示的に指定するか、または Cisco UCS Manager により自動的にホスト ポートに vNICs/vHBA を割り当てることができます。

（注） Cisco UCS VIC 1340/1380 アダプタをサポートするサーバへの vNIC/vHBA ホスト ポート配置を実行できます。

Cisco UCS 1300 シリーズ アダプタには、2x8 PCIe 第 3 世代ホスト トポートがあります。各 PCIe ホストポートは、最大 64 Gbps の帯域幅に対応しています。

vNIC/vHBA のホスト ポート配置により、アダプタの vNIC/vHBA の順序が決まります。最初のホスト ポートに配置された vNIC/vHBA は最初に列挙され、2 番目のホスト ポートの vNIC/vHBA がそれに続きます。

（注） 最大 64 Gbps は理論上の最大値であり、実際のデータ転送は約 40 Gbps に制限されます。

同じ PCIe ホストポートを共有するすべての vNIC がこの帯域幅を共有します。PCIe ホストポートの帯域幅を最適に使用するには、2 つのホスト ポートに vNIC を分散する必要があります。

ホスト ポート配置の設定

Cisco UCS VIC 1340 および VIC 1380 アダプタをサポートするサーバへの vNIC のホスト ポート配置を実行できます。

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 ホスト ポートに配置する vNIC と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 4 ***[Service_Profile_Name]*** > **[vNICs]** の順に展開します。

ステップ 5 **[Network (ネットワーク)]** タブの **[vNICs]** サマリー テーブルで、設定する vNIC の **[管理ホスト ポート (Admin Host Port)]** の値をダブルクリックし、次のいずれかを選択します。

- **[Any]**：Cisco UCS Manager が、vNIC を割り当てるホスト ポートを決定できるようにします。
- [1]：ホスト ポート 1 に vNIC を明示的に割り当てます。
- [2]：ホスト ポート 2 に vNIC を明示的に割り当てます。

[Actual Host Port] には、ホスト ポートの vNIC の実際の割り当てが表示されます。この機能がサポートされていない場合は、[None] と表示されます。

ステップ 6 **[Save Changes]**をクリックします。

CIMC マウント vMedia

スクリプト可能な vMedia の使用

Cisco UCS Manager リモート UCS サーバーの vMedia デバイス ISO イメージをプロビジョニングできます。Scriptable vMedia を使用して、リモート サーバーに IMG または ISO イメージをマウントするようにプログラミングできます。CIMC マウント vMedia を使用すると、メディア接続を追加することなく、データセンター内の他のマウント メディア間で通信できるように

なります。Scriptable vMedia を使用すると、ブラウザを使用せずに仮想メディア デバイスを制御して、手動で各 UCS サーバーを個別にマッピングできます。

スクリプト可能 vMedia は、NFS、CIFS、HTTP、および HTTPS の共有など、複数の共有タイプをサポートします。**スクリプト可能な vMedia** は BIOS 設定によって有効になり、Web GUI および CLI インターフェイスを介して設定されます。

Cisco UCS Manager スクリプト可能な vMedia は次の機能をサポートしています。

- 特定の vMedia デバイスからのブート
- マウントされた共有からローカル ディスクへのファイルのコピー
- OS ドライバのインストールおよび更新

（注） Cisco UCS Manager スクリプト可能 vMedia のサポートは、CIMC マップド デバイスにのみ適用します。既存の KVM ベースの vMedia デバイスはサポートされません。

次の条件に合致する場合、vMedia のマウントは失敗します。

1. vMedia ポリシー内のリモート vMedia イメージ ファイル名が [Service-Profile-Name] に設定されている。
2. サービス プロファイルの名前が変更されている。

これは、サービス プロファイルの名前を変更しても、vMedia ポリシー内のリモート vMedia イメージ ファイル名は変更されないためです。イメージ ファイル名は引き続き、リモート デバイス上の古いイメージをポイントするため、検出できません。

vMedia ポリシーの作成

リモートの vMedia デバイスのマッピング情報を設定するために、vMedia ポリシーが使用されます。vMedia ポリシー内で 2 つの vMedia デバイスと、CD および HDD に対するマッピングが使用できます。同時に、1 つの ISO と 1 つの IMG を設定できます。ISO 構成は CD ドライブに、IMG 構成は HDD デバイスにマッピングします。

（注） デバイスをリモート フォルダにマッピングする場合、IMG を作成し、HDD デバイスとしてマッピングします。

始める前に

次にアクセスできることを確認します。

- リモート vMedia サーバー
- vMedia デバイス

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 [vMedia Policies] ポリシーを右クリックし、[Create vMedia Policy] を選択します。

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

名前	説明
名前（**Name**）	vMedia ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
説明	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推奨します。最大 115 文字。
マウント失敗時の再試行（**Retry on Mount Failure**）	マウント障害が発生した場合に vMedia のマウントを続行するかどうかを指定します。次のように指定します。 • ○ • **[いいえ（No）]** （注） デフォルト設定は、[Yes] です。[はい（Yes）] を選択すると、マウントに成功するか、このオプションが無効化されるまで、リモート サーバは vMedia マウント プロセスのマウントを試行し続けます。[No] を選択すると、警告メッセージが表示され、マウントが失敗した場合にはリトライが機能しないことが示されます。

ステップ 6 テーブルの右側のアイコン バーの [+] をクリックします。

ステップ 7 [Create vMedia Mount] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
名前（**Name**）	vMedia マウント ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後に、この名前を変更することはできません。
デバイス タイプ	マウントするリモート vMedia のタイプ。次のように指定します。 • [CDD]：スクリプト可能な vMedia CD。 • [HDD]：スクリプト可能な vMedia HDD。
[Protocol]	リモート サーバとの通信時に使用するプロトコル。次のオプション ボタンのいずれかをクリックして、マウントされたリモート サーバとの通信に使用するプロトコルを指定します。ここに表示される値は次のとおりです。 • [NFS]：Network Files System。 • [CIFS]：Common Internet File System。 • [HTTP]：Hypertext Transfer Protocol。 • [HTTPS]：Hypertext Transfer Protocol over Secure。

名前	説明
Authentication Protocol	リモート サーバと通信するためのプロトコルとして CIFS を使用する場合に、認証に使用するプロトコル。CIFS 以外のプロトコルを使用する場合、このフィールドは使用できません。認証プロトコルを指定するには、ドロップダウン リストから次のいずれかを選択します。 • **[default]**：NT LAN Manager のセキュリティ サポート プロバイダー（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • **[None]**：認証は使用されません。 • **[ntlm]**：NT LAN Manager（NTLM）セキュリティ プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [Ntlmi]：NTLMi セキュリティ プロトコル。このオプションは、CIFS Windows サーバで [デジタル署名（Digital Signing）] を有効にした場合にのみ使用します。 • [Ntlmssp]：NT LAN Manager Security Support Provider（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 • [Ntlmsspi]：NTLMSSPi プロトコル。このオプションは、CIFS Windows サーバで [デジタル署名（Digital Signing）] を有効にした場合にのみ使用します。 • [Ntlmv2]：NTLMv2 セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 • [Ntlmv2i]：NTLMv2i セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 （注） 認証プロトコル オプションは、プロトコルとして [CIFS] を選択した場合のみ使用可能です。他のすべてのプロトコルでは、[Authentication Protocol] フィールドは無効になります。

名前	説明
[Hostname/IPAddress]	バックアップファイルを格納する場所のIPアドレスまたはホスト名を入力します。これは、サーバ、ストレージアレイ、ローカルドライブ、またはファブリックインターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。 ホスト名を使用する場合、Cisco UCS Manager で DNS サーバを使用するように設定する必要があります。[Inband] ネットワークがそのサーバに設定されている場合、ホスト名（DNS）を使用できます。
[Image Name Variable]	イメージに使用される名前。ここに表示される値は次のとおりです。 • [None]：ファイル名を [Remote File] フィールドに入力する必要があります。 • [Service Profile Name]：ファイル名は自動的に、仮想メディア（vMedia）ポリシーが関連付けられているサービス プロファイルの名前になります。 （注） • [Service Profile Name] を [Image Name] 変数として選択した場合、[Remote File] フィールドは無効になります。 • [Service Profile Name] を [Image Name] 変数として選択した場合は、サービスプロファイルの名前を変更しないでください。サービスプロファイルの名前を変更すると、仮想メディア（vMedia）のマウントが失敗することがあります。
[Remote File]	ISO やその他のイメージ ファイルのフル パスを入力します。 （注） ファイルへのフル パスは、共有名に続き「/」で始まることを確認します。 このフィールドにはファイル名（ファイル拡張子付き）だけを含めることができます。
Remote Path	リモートサーバの共有の名前（たとえば「share」）を入力します。

名前	説明
Username	Cisco UCS Manager でのリモート サーバーへのログインに使用するユーザー名を入力します。 プロトコルが NFS の場合、このフィールドは適用されません。プロトコルが HTTP の場合、このフィールドの選択は任意です。
Password	ユーザ名に関連付けるパスワードを入力します。 プロトコルが NFS の場合、このフィールドは適用されません。プロトコルが HTTP の場合、このフィールドの選択は任意です。
イジェクト時の再マッピング	このチェックボックスをオンにすると、マウントされた vMedia がイジェクトされた後に再マッピングされます。
writable	このチェックボックスをオンにすると、vMedia マウントを書き込み可能として設定します。このチェックボックスをオフにすると、vMedia マウントは読み取り専用のままになります。 vMedia マウントは、デフォルトでは読み取り専用です。 次の両方の条件が満たされている場合にのみ、vMedia マウントを書き込み可能として設定できます。 • **デバイス タイプ**は **HDD** です • **プロトコル**は **NFS** または **CIFS** です

ステップ 8 [OK] をクリックします。
リモート サーバの詳細は、[Create vMedia Mount] ダイアログ ボックスの [vMedia Mounts] 領域に一覧表示されます。

次のタスク

vMedia ブート ポリシーを作成します。

サービス プロファイルへの vMedia ポリシーの追加

Scriptable vMedia を使用する前に、vMedia および Boot ポリシーをサービス プロファイルに追加する必要があります。vMedia ポリシーとブート ポリシーがサービス プロファイルに追加された後、そのサービス プロファイルを Cisco UCS サーバに関連付けることができます。次の手順に、vMedia ポリシーをサービス プロファイルに追加する方法を示します。

始める前に

サービス プロファイルに追加する vMedia ポリシーを設定します。

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]**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。
[Unified Computing System Manager] ペインが表示されます。

ステップ 5 [名前（Name）] フィールドに、サービス プロファイルの識別に使用できる一意の名前を入力します。

この名前には、2 ～ 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。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

この名前は、サービスプロファイルを作成する組織またはサブ組織内で一意である必要があります。

ステップ 6 **[UUID Assignment]** ドロップダウン リストで、次のいずれかの手順を実行します。

オプション	説明
Select (pool default used by default)	デフォルトの UUID 接尾辞プールから UUID を割り当てます。 ステップ 8 に進みます。
	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUID はサービス プロファイルがサーバと関連付けられるまで割り当てられません。この時点で、UUIDは製造元によってサーバに割り当てられた UUID 値に設定されます。サービス プロファイルを後で別のサーバに移動すると、UUIDは新しいサーバに一致するように変更されます。 ステップ 8 に進みます。
	手動で割り当てる UUID を使用します。 ステップ 7 に進みます。
Pools ***Pool_Name***	ドロップダウン リストの下部のリストから選択する UUID 接尾辞プールから UUID を割り当てます。

オプション	説明
	各プール名の後には、プール内で利用可能な UUID の数および UUID 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。 既存のプールを使用するのではなく、すべてのサービス プロファイルがアクセスできるプールを作成する場合は、ステップ 4 に進みます。それ以外の場合はステップ 8 に進みます。

ステップ 7 （任意） オプションを選択した場合は、次の手順を実行します。

a) [UUID] フィールドに、このサービス プロファイルを使用するサーバに割り当てる有効な UUID を入力します。

b) 選択した UUID が使用可能であることを確認するには、[here] リンクをクリックします。

ステップ 8 （任意） このサービス プロファイルで使用する新しい UUID 接尾辞プールを作成する場合は、[Create UUID Suffix Pool] をクリックし、[Create UUID Suffix Pool] ウィザードのフィールドに値を入力します。

ステップ 9 （任意） テキスト ボックスに、このサービス プロファイルの説明を入力します。

このサービス プロファイル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）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 10 [Next] をクリックします。

ステップ 11 [vMedia] ドロップダウン リストから、次のいずれかを選択します。

オプション	説明
[Select vMedia Policy to use]	このサービス プロファイルに vMedia ポリシーを割り当てられるようにします。 ステップ 12 に進みます。
[Create a Specific vMedia Policy]	このサービス プロファイル テンプレートだけがアクセスできるローカル vMedia ポリシーを作成できます。
vMedia Policies ***Policy_Name***	サービス プロファイルに既存の vMedia ポリシーを割り当てます。このオプションを選択した場合、Cisco UCS Manager でポリシーの詳細が表示されます。 既存のポリシーを使用するのではなく、すべてのサービス プロファイルがアクセスできるポリシーを作成する場合は、[Create vMedia Policy] をクリックします。それ以外の場合は、リストでポリシーを選択し、ステップ 13 に進みます。

ステップ 12 すべてのサービス プロファイルおよびテンプレートにアクセスできる新しい vMedia ポリシーを作成したら、[vMedia] ドロップダウン リストからそのポリシーを選択します。

ステップ 13 [Next] をクリックします。

CIMC vMedia ポリシーの表示

始める前に

vMedia ポリシーを設定しておきます。

手順

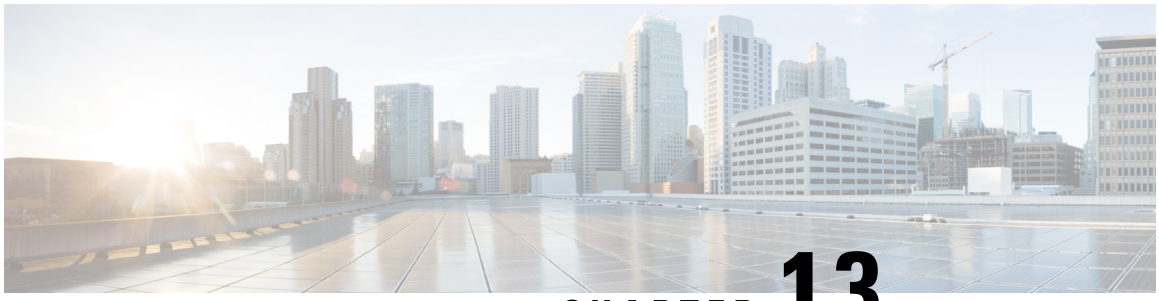
ステップ 1 [ナビゲーション]ペインで、[サーバ]をクリックします。

ステップ 2 **[Policies]** > **[vMedia Policies]** を展開します。

ステップ 3 [vMedia Policies] ノードを展開して、[vMedia Policies] のリストを表示します。

ステップ 4 vMedia ポリシーの名前をダブルクリックし、選択した [vMedia Mount] のプロパティを表示します。

[Properties] ページで、[vMedia Mounts] で使用されるプロパティを変更できます。



CHAPTER 13

ファームウェア アップグレード

- ファームウェア アップグレード （429 ページ）
- コンポーネントのファームウェア バージョンの確認, on page 429

ファームウェア アップグレード

Cisco UCS Manager リリース 4.1(1) 以降、Cisco は Cisco UCS Manager の各リリースと併せて、次の各プラットフォーム用のユニファイド Cisco UCS Manager ソフトウェアおよびファームウェア アップグレードをリリースしています。

- Cisco UCS 6400 シリーズ ファブリック インターコネクト Cisco UCS B シリーズ、C シリーズ、および S シリーズ サーバ
- Cisco UCS 6300 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、C シリーズ、および S シリーズ サーバー
- Cisco UCS 6200 シリーズ Fabric Interconnect と Cisco UCS B シリーズ、C シリーズ、および S シリーズ
- Cisco UCS B シリーズおよび C シリーズ サーバーとの Cisco UCS 6324 ファブリック インターコネクト（別名 UCS Mini）

サービスプロファイル内のパッケージである自動インストール機能により、ファームウェア自動同期サーバーポリシーを使用して、またはエンドポイントで直接、ファームウェアをアップグレードできます。ファームウェアのガイドラインとインストール方法の詳細については、『*Cisco UCS Firmware Management Guide*』を参照してください。

コンポーネントのファームウェア バージョンの確認

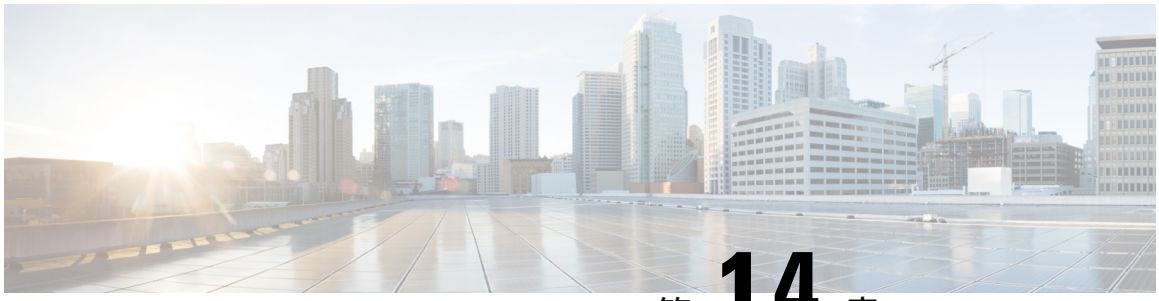
Procedure

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 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 3 [Installed Firmware] タブで、各コンポーネントに対して一覧表示されたファームウェア バージョンを確認します。

ファームウェアのガイドラインとインストール方法の詳細については、『*Cisco UCS Firmware Management Guide*』を参照してください。



第 14 章

診断の設定

- Cisco UCS Manager 診断の概要 （431 ページ）
- 診断ポリシーの作成 （432 ページ）
- ブレード サーバでの診断テスト （433 ページ）
- ラック サーバでの診断テスト （433 ページ）
- すべてのサーバでの診断テストの開始 （434 ページ）
- すべてのサーバでの診断テストの停止 （435 ページ）
- サーバ診断のステータス/結果の表示 （435 ページ）
- 診断のトラブルシューティング （437 ページ）

Cisco UCS Manager 診断の概要

Cisco UCS Manager 診断ツールでは、サーバーのハードウェア コンポーネントの状態を検証できます。診断ツールには各種テストが用意されており、サーバーのさまざまなハードウェア サブシステム（メモリやCPUなど）に対して、負荷を与えたりすることができます。ハードウェア コンポーネントを修復するか、交換した後のサーバーの状態の健全性チェックを実行するためのツールを使用できます。このツールは、実稼働環境に新しいサーバーを導入する前に、包括的なバーンイン テストを実行するときにも使用できます。

新しいシステムの場合、orgスコープでデフォルトの診断ポリシーが作成されます。このデフォルトのポリシーは default という名前であり、削除できません。ユーザーがこのポリシーを削除しようとするとエラー メッセージが表示されます。デフォルトの診断ポリシーは、すべてのサーバーで同じテスト セットを実行する際に推奨される方法です。デフォルト ポリシーを含むすべての診断ポリシーはカスタマイズ可能です。

デフォルト ポリシーには 1 つのメモリ テストだけが含まれています。メモリ テストのデフォルトのパラメータは変更できます。また、デフォルト診断ポリシー内のメモリ テストは削除できます。メモリ テストがない場合、診断ポリシーは実行されません。

診断ポリシーの作成

始める前に

このタスクを実行するには、admin 権限が必要です。

手順

ステップ 1 **[Servers]** > **[Policies]** > **[Diagnostics Policies]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 次のフィールドに入力します。

フィールド	説明
名前（Name）	診断ポリシーの名前。文字数制限は16文字です。
Description	診断ポリシーの説明。これは任意です。

ステップ 4 [Next] をクリックします。

ステップ 5 [Add] をクリックします。

ステップ 6 次のフィールドに入力します。

名前	説明
注文	テストの実行順序。
[CPU Filter]	CPU フィルタをすべての CPU または指定した CPU に設定します。
[Loop Count]	ループ カウントを指定された反復回数に設定します。値の範囲は 1 ～ -1000 です。
[Memory Chunk Size]	メモリ チャンクを 5mb-chunk または big-chunk に設定します。
Memory Size	メモリ サイズを特定の値に設定します。
Pattern	メモリ テストを butterfly、killer、prbs、prbs-addr、または prbs-killer に設定します。

ステップ 7 [**OK**] をクリックします。

ステップ 8 **[終了]** をクリックします。

ブレード サーバでの診断テスト

ブレード サーバでの診断テストの開始

始める前に

このタスクを実行するには、admin 権限が必要です。

手順

ステップ 1 **[Equipment]** > **[Chassis]** > **[Server]** を選択します。
ステップ 2 診断テストを開始するサーバを選択します。
ステップ 3 [Diagnostics] タブをクリックします。
ステップ 4 [Start] をクリックします。診断テストが開始されると、ボタンはグレー表示になります。

ブレード サーバでの診断テストの停止

手順

ステップ 1 **[Equipment]** > **[Chassis]** > **[Server]** を選択します。
ステップ 2 診断テストを停止するサーバを選択します。
ステップ 3 [Diagnostics] タブをクリックします。
ステップ 4 [Stop] をクリックします。診断テストが停止すると、ボタンはグレー表示になります。

ラック サーバでの診断テスト

ラック サーバでの診断テストの開始

診断テストは、 C220 M5、C240 M5、C220 M6、C240 M6、 および C480 M5/C480 M5 ML ラック サーバーで使用できます。

始める前に

このタスクを実行するには、admin 権限が必要です。

手順

ステップ 1 **[Equipment]** > **[Rack Mounts]** > **[Server]** に移動します。
ステップ 2 診断テストを開始するサーバを選択します。
ステップ 3 [Diagnostics] タブをクリックします。
ステップ 4 [Start] をクリックします。診断テストが開始されると、ボタンはグレー表示になります。

ラック サーバでの診断テストの停止

手順

ステップ 1 **[Equipment]** > **[Rack Mounts]** > **[Server]** に移動します。
ステップ 2 診断テストを停止するサーバを選択します。
ステップ 3 [Diagnostics] タブをクリックします。
ステップ 4 [Stop] をクリックします。診断テストが停止すると、ボタンはグレー表示になります。

すべてのサーバでの診断テストの開始

（注） すべてのサーバの診断テストを開始すると、個々のサーバがリブートされます。

始める前に

このタスクを実行するには、admin 権限が必要です。

手順

ステップ 1 **[Equipment]** > **[Diagnostics]** を選択します。
ステップ 2 [Start] をクリックします。診断テストが開始されると、リンクはグレー表示になります。
[Diagnostic Result] テーブルで、次の情報を確認できます。

フィールド	説明
名前（**Name**）	システム定義のサーバ名。

Chassis ID	シャーシの固有識別情報。この数字の識別情報は、システム内のこのシャーシの場所に基づいて割り当てられます。 （注） ラック サーバには適用されません。
PID	サーバ モデル PID。
[Overall Progress Percentage]	サーバでの診断テストの全体的な進捗割合の説明。
Operation Status	サーバの診断操作ステータスの説明。

（注） サーバが診断テストを実行できない場合は、サーバ リンクをクリックし、[Diagnostics] タブでエラーの説明を確認してください。また、[Faults] タブで生成されたエラーを確認することもできます。

すべてのサーバでの診断テストの停止

始める前に

このタスクを実行するには、admin 権限が必要です。

手順

ステップ 1 **[Equipment]** > **[Diagnostics]** を選択します。

ステップ 2 [Stop] をクリックします。診断テストが停止すると、リンクはグレー表示になります。

サーバ診断のステータス/結果の表示

始める前に

CLI から個々のサーバに対して診断テストを実行し、このページでステータスを確認できます。

手順

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

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

または、ラック サーバの場合は、[Equipment] > [Rack Mounts] > [Server] の順に展開します。

ステップ 3 診断ステータスを確認するサーバを選択し、[Diagnostics] タブをクリックします。

以下の情報を確認できます。

名前	説明
[Diagnostic Policies]	ユーザが診断ポリシーを選択して特定のサーバに適用できるようにします。
[Start]/[Stop]	ユーザが特定のサーバに対する診断テストを開始または停止できるようにします。
[Operation State]	サーバの診断操作ステータス。有効な値は [Idle]、[In-Progress]、[Completed]、[Failed]、[Cancelled] です。
[FSM Status Descr]	サーバの診断操作での現行タスクの簡単な説明。
[FSM Progress]	サーバで実行中の診断操作の全体的な進行状況。
[Test Overall Progress]	診断テストの全体的な進行状況。
[Error Description]	診断操作から返されるエラーの説明。

表 *11* : 診断結果

名前	説明
[ID]	テストに関連付けられている固有識別情報
[Test Type]	診断テストのタイプ。
[Status]	テスト実行のステータス。値は [Idle]、[In Progress]、[Completed]、[Failed] です。
Description	診断テスト実行の説明。テストが完了すると、結果の詳細な説明が表示されます。
結果	診断テストの結果。値は [Pass]、[Fail]、または [NA] です。
[Progress Percentage]	診断テストの進捗状況の割合。

診断のトラブルシューティング

問題	デバッグ手順
BIOSが不良DIMMを検出すると、そのDIMMは無効になり、診断操作では認識されません。	診断操作の結果の他に、メモリ関連のエラーを参照してください。

DIMMブラックリスト機能が有効であり、DIMMがブラックリストに追加されると、そのDIMMは診断操作では認識されません。	診断操作の結果の他に、メモリ関連のエラーを参照してください。

サーバーに不良DIMMがあり、これが原因でサーバーが起動できない場合、診断操作が正常に実行されない可能性があります。	該当なし

修正できないエラーが原因でサーバーリブートが行われる場合、診断操作が失敗する可能性があります。	該当なし

メモリ エラーが原因で診断操作が停止する場合、診断操作エラーが発生する可能性があります。	該当なし

	このエラーは外部イベントによってトリガーされます。診断操作をやり直します。

診断操作は、管理型エンドポイントのフェールオーバーやクリティカルなUCSMプロセスの再起動などの外部イベントにより中断することがあります。このような状況では、診断操作が取り消さ	

れ、メモリ テストが失敗としてマークされます。	
メモリ テストが失敗してエラーが発生します。修正できないエラーが検出されます。	[Chassis/Server/Faults] タブで、サーバー エラーを確認します。 [Chassis/Server/SEL Logs] タブで、SEL ログを調べて DIMM エラーを確認します。
メモリ テスト エラーをさらに分析する必要があります。	プライマリ FI の /workspace パーティションにある次のログ ファイル アーカイブで、診断操作のログを確認します : diagnostics/diag_log_<system-name>_<timestamp>_<chassis-id>_<blade-id>.tgz 前述のログ ファイル アーカイブ内で分析ファイル tmp/ServerDiags/MemoryPmem2.<id>/MemoryPmem2.analysis を参照します。 次のコマンドを使用して、分析ファイルで診断ログを見つけます。 # for file in `ls /workspace/diagnostics/*diag*`; do tar -tzvf $file | grep analysis && echo "IN " $file; done

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。