Cisco UCS Manager GUI コンフィギュレーション ガイド リリース 2.1

初版：2012 年 11 月 16 日

最終更新：2012 年 11 月 20 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/

Text Part Number: OL-28301-02-J

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。 マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。 説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2012 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xxxv

対象読者 xxxv

表記法 xxxv

Cisco UCS の関連資料 xxxvii

マニュアルに関するフィードバック xxxvii

概要 1

新機能および変更された機能に関する情報 3

このリリースの新規情報および変更情報 3

Cisco Unified Computing System の概要 11

Cisco Unified Computing System について 11

ユニファイド ファブリック 13

Fibre Channel over Ethernet 13

リンク レベル フロー制御 14

プライオリティ フロー制御 14

サーバのアーキテクチャおよび接続性 14

サービス プロファイルの概要 14

サービス プロファイルによるネットワーク接続 15

サービス プロファイルによる設定 15

サーバ ID を上書きするサービス プロファイル 16

サーバ ID を継承するサービス プロファイル 17

サービス プロファイル テンプレート 18

ポリシー 18

プール 19

トラフィック管理 19

オーバーサブスクリプション 19

オーバーサブスクリプションにおける検討事項 20

オーバーサブスクリプションの概算に関するガイドライン 21
ピン接続 22
サーバ トラフィックのサーバ ポートへのピン接続 22
ピン接続に関するガイドライン 24
Quality of Service 24
システム クラス 24
Quality Of Service ポリシー 25
フロー制御ポリシー 26
オプトイン機能 26
ステートレス コンピューティング 26
マルチテナント機能 28
Cisco UCS の仮想化 29
仮想化の概要 29
Cisco Virtual Machine Fabric Extender の概要 29
ネットワーク インターフェイス カードと統合ネットワーク アダプタを使用した仮想化 30
仮想インターフェイス カード アダプタでの仮想化 30
Cisco UCS Manager の概要 31
Cisco UCS Manager について 31
Cisco UCS Manager で実行できるタスク 33
Cisco UCS Manager で実行できないタスク 34
ハイ アベイラビリティ環境での Cisco UCS Manager 35
Cisco UCS Manager GUI の概要 37
Cisco UCS Manager GUI の概要 37
[Fault Summary] 領域 38
[Navigation] ペイン 39
ツールバー 42
[Work] ペイン 42
ステータスバー 42
テーブルのカスタマイズ 43
LAN アップリンク マネージャ 44
Internal Fabric Manager 45
ハイブリッド表示 45

HTTPS による Cisco UCS Manager GUI へのログイン 45
HTTP による Cisco UCS Manager GUI へのログイン 46
Cisco UCS Manager GUI からのログアウト 47
Web セッション制限 47
Cisco UCS Manager の Web セッション制限の設定 48
プリログイン バナー 48
プリログイン バナーの作成 48
プリログイン バナーの変更 49
プリログイン バナーの削除 50
Cisco UCS Manager GUI のプロパティ 50
Cisco UCS Manager GUI のセッションおよびログのプロパティの設定 50
確認メッセージのプロパティの設定 51
外部アプリケーションのプロパティの設定 52
Cisco UCS Manager GUI の表示のカスタマイズ 53
フィールドの値の許容範囲の確認 53
ポリシーの使用場所の確認 54
プールの使用場所の確認 54
XML のコピー 55
システム設定 57
ファブリック インターコネクトの設定 59
初期システム セットアップ 59
セットアップ モード 60
システム設定タイプ 60
管理ポートの IP アドレス 61
スタンドアロン設定用の初期システム セットアップの実行 61
クラスタ設定の初期システム セットアップ 63
第 1 ファブリック インターコネクトでの初期システム セットアップの実行 63
第 2 ファブリック インターコネクトでの初期システム セットアップの実行 66
スタンドアロン ファブリック インターコネクトに対するクラスタ設定のイネーブル化 67
イーサネット スイッチング モード 68
イーサネット スイッチング モードの設定 69

ファイバ チャネル スイッチング モード 69
ファイバ チャネル スイッチング モードの設定 70
ファブリック インターコネクトのプロパティの変更 71
ファブリック インターコネクトのリーダーシップ ロールの決定 72
ポートおよびポート チャネルの設定 73
6100 シリーズ ファブリック インターコネクト上のサーバ ポートおよびアップリンク ポート 74
6200 シリーズ ファブリック インターコネクト上のユニファイド ポート 75
ポート モード 75
ポート タイプ 75
ユニファイド ポートのビーコン LED 76
ユニファイド ポートの設定の注意事項 77
ユニファイド アップリンク ポートとユニファイド ストレージ ポート設定時の注意事項および注意 78
ポート モード変更によるデータ トラフィックへの影響 79
6248 ファブリック インターコネクトのポート モードの設定 80
6296 ファブリック インターコネクトのポート モードの設定 81
ユニファイド ポートのビーコン LED の設定 83
サーバ ポート 84
サーバ ポートの設定 84
アップリンク イーサネット ポート 84
アップリンク イーサネット ポートの設定 84
アップリンク イーサネット ポートのプロパティの変更 85
ファブリック インターコネクトのポートの再設定 86
ファブリック インターコネクト上のポートのイネーブル化 86
ファブリック インターコネクト上のポートのディセーブル化 87
ファブリック インターコネクトのポート設定解除 88
アプライアンス ポート 89
アプライアンス ポートの設定 89
アプライアンス ポートのプロパティの変更 92
FCoE ストレージ ポートおよびファイバ チャネル ストレージ ポート 94
FCoE ストレージ ポートの設定 94

ファイバ チャネル ストレージ ポートの設定 95
アップリンク ファイバ チャネル ポートの復元 96
FCoE アップリンク ポート 96
FCoE アップリンク ポートの設定 97
ユニファイド ストレージ ポート 97
ユニファイド ストレージ ポートとしてアプライアンス ポートを設定 98
ユニファイド ストレージ ポートの設定解除 99
ユニファイド アップリンク ポート 100
ユニファイド アップリンク ポートの設定 100
ユニファイド アップリンク ポートの設定解除 101
アップリンク イーサネット ポート チャネル 102
アップリンク イーサネット ポート チャネルの作成 102
アップリンク イーサネット ポート チャネルのイネーブル化 103
アップリンク イーサネット ポート チャネルのディセーブル化 104
アップリンク イーサネット ポート チャネルへのポートの追加および削除 104
アップリンク イーサネット ポート チャネルの削除 105
アプライアンス ポート チャネル 105
アプライアンス ポート チャネルの作成 105
アプライアンス ポート チャネルのイネーブル化 108
アプライアンス ポート チャネルのディセーブル化 109
アプライアンス ポート チャネルへのポートの追加および削除 109
アプライアンス ポート チャネルの削除 110
ファイバ チャネル ポート チャネル 110
ファイバ チャネル ポート チャネルの作成 110
ファイバ チャネル ポート チャネルのイネーブル化 112
ファイバ チャネル ポート チャネルのディセーブル化 112
ファイバ チャネル ポート チャネルへのポートの追加および削除 112
ファイバ チャネル ポート チャネルのプロパティの変更 113
ファイバ チャネル ポート チャネルの削除 114
FCoE ポート チャネル 114
FCoE ポート チャネルの作成 114
FCoE ポート チャネルの削除 115

ユニファイド アップリンク ポート チャネル 115
アダプタ ポート チャネル 116
アダプタ ポート チャネルの表示 116
ファブリック ポート チャネル 117
ファブリック ポート チャネルのケーブル接続の問題 117
ファブリック ポート チャネルの設定 118
ファブリック ポート チャネルの表示 119
ファブリック ポート チャネル メンバ ポートのイネーブル化またはディセーブル化 119
Internal Fabric Manager を使用したサーバ ポートの設定 120
Internal Fabric Manager 120
Internal Fabric Manager の起動 120
Internal Fabric Manager を使用したサーバ ポートの設定 120
Internal Fabric Manager を使用したサーバ ポートの設定解除 121
Internal Fabric Manager を使用したサーバ ポートのイネーブル化 121
Internal Fabric Manager を使用したサーバ ポートのディセーブル化 121
通信サービスの設定 123
通信サービス 123
CIM-XML の設定 125
HTTP の設定 125
HTTPS の設定 126
証明書、キー リング、トラスト ポイント 126
キー リングの作成 127
キー リングの証明書要求の作成 128
トラスト ポイントの作成 129
キー リングへの証明書のインポート 130
HTTPS の設定 131
キーリングの削除 132
トラスト ポイントの削除 133
SNMP の設定 133
SNMP に関する情報 133
SNMP 機能の概要 133

SNMP 通知 134
SNMP セキュリティ レベルおよび権限 134
SNMP セキュリティ モデルおよびセキュリティ レベルのサポートされる組み合わせ 135
SNMPv3 セキュリティの機能 136
Cisco UCS での SNMP サポート Cisco UCS 136
SNMP のイネーブル化および SNMP プロパティの設定 137
SNMP トラップの作成 138
SNMP トラップの削除 140
SNMPv3 ユーザの作成 140
SNMPv3 ユーザの削除 141
Telnet のイネーブル化 142
通信サービスのディセーブル化 142
認証の設定 143
認証サービス 143
リモート認証プロバイダーに関する注意事項および推奨事項 144
リモート認証プロバイダーのユーザ属性 144
LDAP グループ ルール 146
LDAP プロバイダーの設定 147
LDAP プロバイダーのプロパティの設定 147
LDAP プロバイダーの作成 148
LDAP プロバイダーの LDAP グループ ルールの変更 153
LDAP プロバイダーの削除 154
LDAP グループ マッピング 155
LDAP グループ マップの作成 155
LDAP グループ マップの削除 156
RADIUS プロバイダーの設定 156
RADIUS プロバイダーのプロパティの設定 156
RADIUS プロバイダーの作成 157
RADIUS プロバイダーの削除 159
TACACS+ プロバイダーの設定 160
TACACS+ プロバイダーのプロパティの設定 160

TACACS+ プロバイダーの作成 160
TACACS+ プロバイダーの削除 162
マルチ認証システムの設定 162
マルチ認証システム 162
プロバイダー グループ 163
LDAP プロバイダー グループの作成 163
LDAP プロバイダー グループの削除 164
RADIUS プロバイダー グループの作成 164
RADIUS プロバイダー グループの削除 165
TACACS+ プロバイダー グループの作成 165
TACACS+ プロバイダー グループの削除 166
認証ドメイン 166
認証ドメインの作成 167
プライマリ認証サービスの選択 168
コンソール認証サービスの選択 168
デフォルトの認証サービスの選択 169
リモート ユーザのロール ポリシー 171
リモート ユーザのロール ポリシーの設定 171
組織の設定 173
マルチテナント環境の組織 173
マルチテナント環境における階層的な名前解決 174
ルート組織下の組織の作成 176
サブ組織下の組織の作成 176
組織の削除 177
ロールベース アクセス コントロールの設定 179
ロールベース アクセス コントロール 179
Cisco UCS のユーザ アカウント 180
Cisco UCS ユーザ名に関する注意事項 181
予約語：ローカル認証されたユーザのアカウント 181
Cisco UCS パスワードの注意事項 182
ユーザ アカウントの Web セッション制限 183
ユーザ ロール 183

デフォルトのユーザ ロール 184

予約語：ユーザ ロール 185

権限 185

ユーザ ロケール 188

ユーザ ロールの設定 189

ユーザ ロールの作成 189

ユーザ ロールへの権限の追加 190

ユーザ ロールからの権限の削除 190

ユーザ ロールの削除 190

ロケールの設定 191

ロケールの作成 191

ロケールへの組織の割り当て 192

ロケールからの組織の削除 192

ロケールの削除 193

ローカル認証されたユーザ アカウントの設定 193

ユーザ アカウントの作成 193

ローカル認証されたユーザのパスワード強度チェックのイネーブル化 196

Cisco UCS Manager GUI ユーザの Web セッション制限の設定 197

ローカル認証されたユーザ アカウントに割り当てられたロケールの変更 197

ローカル認証されたユーザ アカウントに割り当てられたロールの変更 198

ユーザ アカウントの有効化 199

ユーザ アカウントの無効化 199

ローカル認証されたユーザのパスワード履歴のクリア 200

ローカルに認証されたユーザ アカウントの削除 200

ローカル認証されたユーザのパスワード プロファイル 200

変更間隔のパスワード変更の最大回数の設定 202

パスワードの変更なし間隔の設定 202

パスワード履歴カウントの設定 203

ユーザ セッションのモニタリング 203

DNS サーバの設定 205

Cisco UCS の DNS サーバ 205

DNS サーバの追加 205

DNS サーバの削除 206
システム関連ポリシーの設定 207
シャーシ ディスカバリ ポリシーの設定 207
シャーシ ディスカバリ ポリシー 207
シャーシ ディスカバリ ポリシーの設定 210
シャーシ接続ポリシーの設定 211
シャーシ接続ポリシー 211
シャーシ接続ポリシーの設定 212
ラック サーバ ディスカバリ ポリシーの設定 212
ラック サーバ ディスカバリ ポリシー 212
ラック サーバ ディスカバリ ポリシーの設定 213
MAC アドレス テーブルのエージング タイムの設定 214
MAC アドレス テーブルのエージング タイム 214
MAC アドレス テーブルのエージング タイムの設定 214
ライセンスの管理 217
ライセンス 217
ファブリック インターコネクトのホスト ID の入手方法 219
ライセンスの取得 219
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 220
離れた場所からのファブリック インターコネクトへのライセンスのダウンロード 221
ライセンスのインストール 223
ファブリック インターコネクトにインストールされたライセンスの表示 224
ポートまたは機能に使用できる猶予期間の決定 226
ライセンスの有効期限の決定 228
ライセンスのアンインストール 228
仮想インターフェイスの管理 231
仮想インターフェイス 231
仮想インターフェイスの加入者管理とエラー処理 232
Cisco UCS Central への Cisco UCS ドメインの登録 233
Cisco UCS ドメインの登録 233

Cisco UCS Manager と Cisco UCS Central 間のポリシー解決 234
Cisco UCS ドメインの Cisco UCS Central への登録 235
Cisco UCS Manager と Cisco UCS Central 間のポリシー解決の変更 236
Cisco UCS ドメインの Cisco UCS Central からの登録解除 237
ネットワーク設定 239
LAN アップリンク マネージャの使用 241
LAN アップリンク マネージャ 241
LAN アップリンク マネージャの起動 242
LAN アップリンク マネージャでのイーサネット スイッチング モードの変更 242
LAN アップリンク マネージャでのポートの設定 243
サーバ ポートの設定 243
LAN アップリンク マネージャを使用したサーバ ポートのイネーブル化 243
LAN アップリンク マネージャを使用したサーバ ポートのディセーブル化 244
LAN アップリンク マネージャを使用したサーバ ポートの設定解除 244
アップリンク イーサネット ポートの設定 245
LANアップリンク マネージャを使用したアップリンク イーサネット ポートのイネーブル化 245
LAN アップリンク マネージャを使用したアップリンク イーサネット ポートのディセーブル化 245
LANアップリンク マネージャを使用したアップリンク イーサネット ポートの設定解除 246
アップリンク イーサネット ポート チャネルの設定 246
LAN アップリンク マネージャでのポート チャネルの作成 246
LAN アップリンク マネージャを使用したポート チャネルのイネーブル化 247
LAN アップリンク マネージャを使用したポート チャネルのディセーブル化 248
LAN アップリンク マネージャを使用したポート チャネルへのポートの追加 248
LAN アップリンク マネージャを使用したポート チャネルからのポートの削除 249
LAN アップリンク マネージャを使用したポート チャネルの削除 249
LAN ピン グループの設定 249
LAN アップリンク マネージャでのピン グループの作成 249
LAN アップリンク マネージャを使用したピン グループの削除 250

ネームド VLAN の設定 250
LAN アップリンク マネージャを使用したネームド VLAN の作成 250
LAN アップリンク マネージャを使用したネームド VLAN の削除 253
LAN アップリンク マネージャでの QoS システム クラスの設定 254
VLAN の設定 257
ネームド VLAN 257
プライベート VLAN 258
VLAN ポートの制限事項 260
ネームド VLAN の設定 261
ネームド VLAN の作成 261
ネームド VLAN の削除 265
プライベート VLAN の設定 266
プライベート VLAN 用のプライマリ VLAN の作成 266
プライベート VLAN 用のセカンダリ VLAN の作成 271
VLAN ポート数の表示 275
VLAN のポート数の最適化 275
ポート VLAN 数の最適化のイネーブル化 276
ポート VLAN 数の最適化のディセーブル化 276
VLAN の最適化設定の表示 277
VLAN グループ 278
VLAN グループの作成 278
VLAN グループのメンバの編集 279
VLAN グループの組織アクセス権限の変更 280
VLAN グループの削除 281
VLAN の権限 281
VLAN の権限のイネーブル化 282
VLAN の権限のディセーブル化 282
VLAN の権限の追加または変更 282
LAN ピン グループの設定 285
LAN ピン グループ 285
LAN ピン グループの作成 286
LAN ピン グループの削除 287

MAC プールの設定 289

MAC プール 289

MAC プールの作成 290

MAC プールの削除 291

Quality of Service の設定 293

Quality of Service 293

システム クラスの設定 293

システム クラス 293

QoS システム クラスの設定 294

QoS システム クラスのイネーブル化 296

QoS システム クラスのディセーブル化 297

Quality of Service ポリシーの設定 297

Quality Of Service ポリシー 297

QoS ポリシーの作成 298

QoS ポリシーの削除 300

フロー制御ポリシーの設定 301

フロー制御ポリシー 301

フロー制御ポリシーの作成 301

フロー制御ポリシーの削除 303

ネットワーク関連ポリシーの設定 305

vNIC テンプレートの設定 305

vNIC テンプレート 305

vNIC テンプレートの作成 306

vNIC テンプレートへの vNIC のバインディング 310

vNIC テンプレートからの vNIC のバインド解除 311

vNIC テンプレートの削除 312

イーサネット アダプタ ポリシーの設定 312

イーサネットおよびファイバ チャネル アダプタ ポリシー 312

イーサネット アダプタ ポリシーの作成 314

Linux オペレーティング システム上の MRQS に対する eNIC サポートをイネーブルにするためのイーサネット アダプタ ポリシーの設定 317

イーサネット アダプタ ポリシーの削除 318

デフォルトの vNIC の動作のポリシーの設定 318
デフォルトの vNIC および vHBA の動作ポリシー 318
デフォルトの vNIC の動作ポリシーの設定 319
LAN 接続ポリシーの設定 320
LAN および SAN の接続ポリシー 320
LAN および SAN 接続ポリシーに必要な権限 320
サービス プロファイルと接続ポリシー間の相互作用 321
LAN 接続ポリシーの作成 321
LAN 接続ポリシーの vNIC の作成 328
LAN 接続ポリシーからの vNIC の削除 332
LAN 接続ポリシーの iSCSI vNIC の作成 333
LAN 接続ポリシーからの iSCSI vNIC の削除 334
LAN 接続ポリシーの削除 335
ネットワーク制御ポリシーの設定 335
ネットワーク制御ポリシー 335
ネットワーク制御ポリシーの作成 336
ネットワーク制御ポリシーの削除 339
マルチキャスト ポリシーの設定 339
マルチキャスト ポリシー 339
マルチキャスト ポリシーの作成 340
マルチキャスト ポリシーの変更 341
マルチキャスト ポリシーの削除 343
アップストリーム分離レイヤ 2 ネットワークの設定 345
アップストリーム分離レイヤ 2 ネットワーク 345
アップストリーム分離 L2 ネットワークの設定に関する注意事項 346
アップストリーム分離 L2 ネットワークのピン接続に関する注意事項 348
アップストリーム分離 L2 ネットワークの Cisco UCS の設定 349
アップストリーム分離 L2 ネットワークに対する VLAN の作成 351
VLAN へのポートおよびポート チャネルの割り当て 353
VLAN からのポートおよびポート チャネルの削除 355
VLAN に割り当てられたポートおよびポート チャネルの表示 356
ストレージ設定 357

ネームド VSAN の設定 359

ネームド VSAN 359

ネームド VSAN のファイバ チャネル アップリンク トランキング 360

VSAN に関する注意事項および推奨事項 360

ネームド VSAN の作成 362

ストレージ VSAN の作成 365

VSAN の削除 368

ストレージ VSAN 用の FCoE VLAN の VLAN ID の変更 368

ファイバ チャネル アップリンク トランキングのイネーブル化 369

ファイバ チャネル アップリンク トランキングのディセーブル化 370

SAN ピン グループの設定 371

SAN ピン グループ 371

SAN ピン グループの作成 372

SAN ピン グループの削除 372

WWN プールの設定 373

WWN プール 373

WWNN プールの設定 374

WWNN プールの作成 374

WWNN プールへの WWN ブロックの追加 376

WWNN プールからの WWN ブロックの削除 376

WWNN プールへの WWNN イニシエータの追加 377

WWNN プールからの WWNN イニシエータの削除 378

WWNN プールの削除 378

WWPN プールの設定 379

WWPN プールの作成 379

WWPN プールへの WWN ブロックの追加 381

WWPN プールからの WWN ブロックの削除 381

WWPN プールへの WWPN イニシエータの追加 382

WWPN プールからの WWPN イニシエータの削除 383

WWPN プールの削除 384

WWxN プールの設定 384

WWxN プールの作成 384

WWxN プールへの WWN ブロックの追加 386
WWxN プールからの WWN ブロックの削除 387
WWxN プールの削除 387
ストレージ関連ポリシーの設定 389
vHBA テンプレートの設定 389
vHBA テンプレート 389
vHBA テンプレートの作成 389
vHBA テンプレートへの vHBA のバインディング 391
vHBA テンプレートからの vHBA のバインド解除 392
vHBA テンプレートの削除 393
ファイバ チャネル アダプタ ポリシーの設定 393
イーサネットおよびファイバ チャネル アダプタ ポリシー 393
ファイバ チャネル アダプタ ポリシーの作成 395
ファイバ チャネル アダプタ ポリシーの削除 400
デフォルトの vHBA 動作ポリシーの設定 401
デフォルトの vNIC および vHBA の動作ポリシー 401
デフォルトの vHBA 動作ポリシーの設定 402
SAN 接続ポリシーの設定 402
LAN および SAN の接続ポリシー 402
LAN および SAN 接続ポリシーに必要な権限 403
サービス プロファイルと接続ポリシー間の相互作用 403
SAN 接続ポリシーの作成 404
SAN 接続ポリシーの vHBA の作成 408
SAN 接続ポリシーからの vHBA の削除 411
SAN 接続ポリシーのイニシエータ グループの作成 412
SAN 接続ポリシーからのイニシエータ グループの削除 413
SAN 接続ポリシーの削除 414
ファイバ チャネル ゾーン分割の設定 415
ファイバ チャネル ゾーン分割に関する情報 415
ゾーンに関する情報 415
ゾーン セットに関する情報 416
Cisco UCS Manager でのファイバ チャネル ゾーン分割のサポート 416

Cisco UCS Manager ベースのファイバ チャネル ゾーン分割 417
vHBA イニシエータ グループ 417
ファイバ チャネル ストレージ接続ポリシー 418
ファイバ チャネルのアクティブ ゾーン セットの設定 418
スイッチベースのファイバ チャネル ゾーン分割 418
Cisco UCS Manager ベースのファイバ チャネル ゾーン分割に関する注意事項および推奨事項 419
Cisco UCS でのファイバ チャネル ゾーン分割の設定 419
ファイバ チャネル ゾーン分割のための VSAN の作成 421
ファイバ チャネル ストレージ接続ポリシーの設定 424
ファイバ チャネル ストレージ接続ポリシーの作成 424
ファイバ チャネル ストレージ接続ポリシーの削除 426
サーバの設定 427
サーバ関連プールの設定 429
サーバ プールの設定 429
サーバ プール 429
サーバ プールの作成 430
サーバ プールの削除 431
サーバ プールへのサーバの追加 431
サーバ プールからのサーバの削除 432
UUID 接尾辞プールの設定 432
UUID 接尾辞プール 432
UUID 接尾辞プールの作成 432
UUID 接尾辞プールの削除 434
IP プールの設定 434
IP プール 434
IP プールの作成 435
IP プールへのブロックの追加 437
IP プールからのブロックの削除 438
IP プールの削除 438
管理 IP アドレスの設定 439
管理 IP アドレス 439

ブレード サーバの管理 IP アドレスの設定 440
スタティック IP アドレスを使用するブレード サーバの設定 440
管理 IP プールを使用するブレード サーバの設定 441
ラック サーバの管理 IP アドレスの設定 441
スタティック IP アドレスを使用するラック サーバの設定 441
管理 IP プールを使用するラック サーバの設定 442
サービス プロファイルの管理 IP アドレスの設定 442
サービス プロファイル テンプレートの管理 IP アドレスの設定 444
管理 IP プールの設定 444
管理 IP プール 444
管理 IP プールでの IP アドレス ブロックの作成 445
管理 IP プールからの IP アドレス ブロックの削除 446
サーバ関連ポリシーの設定 447
BIOS の設定 447
サーバ BIOS 設定 447
主要な BIOS 設定 448
プロセッサの BIOS 設定 450
Intel Directed I/O BIOS 設定 455
RAS メモリ BIOS 設定 457
シリアル ポートの BIOS 設定 460
USB の BIOS 設定 460
PCI 設定 BIOS 設定 462
ブート オプションの BIOS 設定 462
サーバ管理 BIOS 設定 464
BIOS ポリシー 469
デフォルトの BIOS 設定 469
BIOS ポリシーの作成 470
BIOS のデフォルトの修正 471
サーバの実際の BIOS 設定の表示 472
IPMI アクセス プロファイルの設定 473
IPMI アクセス プロファイル 473
IPMI アクセス プロファイルの作成 473

IPMI アクセス プロファイルの削除 474
ローカル ディスク設定ポリシーの設定 475
ローカル ディスク設定ポリシー 475
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 476
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 477
ローカル ディスク設定ポリシーの作成 479
ローカル ディスク設定ポリシーの変更 483
ローカル ディスク設定ポリシーの削除 484
スクラブ ポリシーの設定 484
スクラブ ポリシー 484
スクラブ ポリシーの作成 485
スクラブ ポリシーの削除 486
Serial over LAN ポリシーの設定 486
Serial over LAN ポリシー 486
Serial over LAN ポリシーの作成 486
Serial over LAN ポリシーの削除 488
サーバ自動構成ポリシーの設定 488
サーバ自動構成ポリシー 488
自動構成ポリシーの作成 488
自動構成ポリシーの削除 490
サーバ ディスカバリ ポリシーの設定 490
サーバ ディスカバリ ポリシー 490
サーバ ディスカバリ ポリシーの作成 491
サーバ ディスカバリ ポリシーの削除 492
サーバ継承ポリシーの設定 492
サーバ継承ポリシー 492
サーバ継承ポリシーの作成 492
サーバ継承ポリシーの削除 494
サーバ プール ポリシーの設定 494
サーバ プール ポリシー 494
サーバ プール ポリシーの作成 494

サーバ プール ポリシーの削除 495
サーバ プール ポリシーの資格情報の設定 496
サーバ プール ポリシー資格情報 496
サーバ プール ポリシーの資格情報の作成 497
サーバ プール ポリシーの資格情報の削除 502
サーバ プール ポリシーの資格情報からの資格の削除 502
vNIC/vHBA 配置ポリシーの設定 502
vNIC/vHBA 配置ポリシー 502
vCon からアダプタへの配置 503
N20-B6620-2 および N20-B6625-2 ブレード サーバの vCon からアダプタへの配置 504
その他すべてのサポートされているサーバの vCon からアダプタへの配置 504
vNIC/vHBA から vCon への割り当て 505
vNIC/vHBA 配置ポリシーの作成 508
vNIC/vHBA 配置ポリシーの削除 511
vCon への vNIC の明示的な割り当て 512
vCon への vHBA の明示的な割り当て 513
ダイナミック vNIC を配置する前のスタティック vNIC の配置 515
サーバのブート設定 517
ブート ポリシー 517
ブート ポリシーの作成 518
SAN ブート 519
ブート ポリシーに対する SAN ブートの設定 520
iSCSI ブート 522
iSCSI ブート プロセス 523
iSCSI ブートのガイドラインと前提条件 523
Windows での MPIO のイネーブル化 525
iSCSI のブート設定 526
iSCSI アダプタ ポリシーの作成 527
iSCSI アダプタ ポリシーの削除 529
認証プロファイルの作成 529

認証プロファイルの削除 531
iSCSI イニシエータの IP プールの作成 531
iSCSI ブート ポリシーの作成 532
サービス プロファイルに対する iSCSI vNIC の作成 533
サービス プロファイルからの iSCSI vNIC の削除 535
iSCSI ブート パラメータの設定 535
iSCSI ブート パラメータの変更 540
IQN プール 544
IQN プールの作成 544
IQN プールへのブロックの追加 546
IQN プールからのブロックの削除 547
IQN プールの削除 547
LAN ブート 548
ブート ポリシーに対する LAN ブートの設定 548
ローカル ディスク ブート 549
ブート ポリシーに対するローカル ディスク ブートの設定 549
仮想メディア ブート 550
ブート ポリシーに対する仮想メディア ブートの設定 550
ブート ポリシーの削除 552
サービス プロファイルの更新の展開の延期 553
サービス プロファイルの延期展開 553
延期展開スケジュール 554
メンテナンス ポリシー 554
保留中のアクティビティ 555
延期展開の注意事項および制限事項 555
スケジュールの設定 556
スケジュールの作成 556
スケジュールに対する 1 回のオカレンスの作成 562
スケジュールに対する繰り返すオカレンスの作成 565
スケジュールからの 1 回のオカレンスの削除 568
スケジュールからの繰り返すオカレンスの削除 568
スケジュールの削除 569

メンテナンス ポリシーの設定 569
メンテナンス ポリシーの作成 569
メンテナンス ポリシーの削除 571
保留中のアクティビティの管理 572
保留中のアクティビティの表示 572
ユーザによる確認を待機しているサービス プロファイル変更の展開 572
ユーザによる確認を待機しているすべてのサービス プロファイル変更の展開 573
予定されたサービス プロファイルの変更を即座に展開する 573
予定されたすべてのサービス プロファイルの変更を即座に展開する 574
サービス プロファイルの設定 575
サーバ ID を上書きするサービス プロファイル 575
サーバ ID を継承するサービス プロファイル 576
サービス プロファイル テンプレート 577
サービス プロファイルの注意事項および推奨事項 577
サービス プロファイルの作成 578
[Expert] ウィザードを使用したサービス プロファイルの作成 578
ページ 1：サービス プロファイルの識別 578
ページ 2：ネットワーキング オプションの設定 580
ページ 3：ストレージ オプションの設定 588
ページ 4: ファイバ チャネルの [Zoning] オプションの設定 595
ページ 5：vNIC/vHBA 配置の設定 597
ページ 6：サーバのブート順序の設定 602
ページ 7：メンテナンス ポリシーの追加 607
ページ 8：サーバの割り当ての指定 609
ページ 9：動作ポリシーの追加 611
サーバ ID を継承するサービス プロファイルの作成 614
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 618
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 619
サービス プロファイル テンプレートの操作 620
サービス プロファイル テンプレートの作成 620

ページ 1：サービス プロファイル テンプレートの識別 621
ページ 2：ネットワーキング オプションの指定 622
ページ 3: ストレージ オプションの指定 630
ページ 4: ファイバ チャネルの [Zoning] オプションの設定 637
ページ 5：vNIC/vHBA 配置の設定 639
ページ 6：サーバのブート順序の設定 644
ページ 7：メンテナンス ポリシーの追加 649
ページ 8：サーバの割り当てオプションの指定 651
ページ 9：動作ポリシーの追加 652
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 プロファイルを作成する 655
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 656
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 656
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 657
サービス プロファイルの管理 658
サービス プロファイルのクローン化 658
サーバまたはサーバ プールとのサービス プロファイルの関連付け 659
サーバまたはサーバ プールとのサービス プロファイルの関連付けの解除 660
サービス プロファイルの名前変更 661
サービス プロファイルでの UUID の変更 662
サービス プロファイルでのブート順序の変更 663
サービス プロファイル用の vNIC の作成 666
サービス プロファイルからの vNIC の削除 670
サービス プロファイル用の vHBA の作成 670
vHBA に対する WWPN の変更 674
vHBA の永続的なバインディングのクリア 676
サービス プロファイルからの vHBA の削除 676
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 676
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 679

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 679
サービス プロファイルの削除 680
サービス プロファイル テンプレートの管理 680
サーバ プールとサービス プロファイル テンプレートの関連付け 680
サーバ プールとサービス プロファイル テンプレートの関連付けの解除 681
サービス プロファイル テンプレートでの UUID の変更 681
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 682
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 683
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 684
Cisco UCS での電源の管理 687
Cisco UCS での電源管理 687
ラック サーバの電源管理 687
電源管理の注意事項 688
電源ポリシーの設定 688
電源ポリシー 688
電源ポリシーの設定 688
グローバル キャップ ポリシーの設定 689
グローバル キャップ ポリシー 689
グローバル キャップ ポリシーの設定 689
ポリシー方式のシャーシ グループの電力制限の設定 690
ポリシー方式のシャーシ グループの電力制限 690
電力グループの設定 690
電力グループ 690
電力グループの作成 691
電力グループへのシャーシの追加 693
電力グループからのシャーシの取り外し 693
電力グループの削除 694
電力制御ポリシーの設定 694

電力制御ポリシー 694
電力制御ポリシーの作成 695
電力制御ポリシーの削除 696
手動ブレード レベルの電力制限の設定 696
手動ブレード レベルの電力制限 696
サーバのブレード レベルの電力制限の設定 697
ブレード レベルの電力制限の表示 698
システム管理 699
タイム ゾーンの管理 701
タイム ゾーン 701
タイム ゾーンの設定 701
NTP サーバの追加 702
NTP サーバの削除 702
シャーシの管理 703
Cisco UCS Manager GUI でのシャーシ管理 703
シャーシの削除および稼働中止に関する注意事項 703
シャーシの確認 704
シャーシの稼働中止 705
シャーシの削除 705
単一シャーシの再稼働 705
複数のシャーシの再稼働 706
シャーシ番号の付け替え 707
ロケータ LED の切り替え 708
シャーシのロケータ LED の電源投入 708
シャーシのロケータ LED の電源切断 708
シャーシの POST 結果の表示 708
ブレード サーバの管理 711
ブレード サーバ管理 712
ブレード サーバの削除および稼働中止に関する注意事項 712
予期しないサーバの電源変更を回避するための推奨事項 713
ブレード サーバのブート 714
ブレード サーバのブート 714

サービス プロファイルからのサーバのブート 714
ブレード サーバのブート順序の決定 715
ブレード サーバのシャットダウン 715
ブレード サーバのシャットダウン 715
サービス プロファイルからのサーバのシャットダウン 716
ブレード サーバのリセット 717
ブレード サーバの再確認 717
シャーシからのサーバの削除 718
ブレード サーバの稼働中止 719
ブレード サーバの再稼働 719
シャーシ内のサーバ スロットの再確認 720
設定データベースからの存在しないブレード サーバの削除 720
ブレード サーバのロケータ LED のオンとオフを切り替える 721
ブレード サーバの CMOS のリセット 721
ブレード サーバの CIMC のリセット 722
ブレード サーバの破損した BIOS のリカバリ 723
ブレード サーバの POST 結果の表示 724
ブレード サーバからの NMI の発行 724
ラックマウント サーバの管理 725
ラックマウント サーバ管理 726
ラックマウント サーバの削除および稼働中止に関する注意事項 726
予期しないサーバの電源変更を回避するための推奨事項 727
ラックマウント サーバのブート 728
ラックマウント サーバのブート 728
サービス プロファイルからのサーバのブート 728
ラックマウント サーバのブート順序の決定 729
ラックマウント サーバのシャットダウン 730
ラックマウント サーバのシャットダウン 730
サービス プロファイルからのサーバのシャットダウン 730
ラックマウント サーバのリセット 731
ラックマウント サーバの再確認 732
ラックマウント サーバの稼働中止 732

ラックマウント サーバの再稼働 733
ラックマウント サーバ番号の付け替え 733
設定データベースからの存在しないラックマウント サーバの削除 734
ラックマウント サーバのロケータ LED のオンとオフを切り替える 735
ラックマウント サーバの CMOS のリセット 735
ラックマウント サーバの CIMC のリセット 735
ラックマウント サーバの破損した BIOS のリカバリ 736
ラックマウント サーバの POST 結果の表示 737
ラックマウント サーバからの NMI の発行 737
KVM コンソールの起動 739
KVM コンソール 739
仮想 KVM コンソール 740
サーバからの KVM コンソールの起動 744
サービス プロファイルからの KVM コンソールの起動 744
KVM Launch Manager からの KVM コンソールの起動 745
I/O モジュールの管理 747
Cisco UCS Manager GUI での I/O モジュール管理 747
I/O モジュールのリセット 747
I/O モジュールの POST 結果の表示 748
設定のバックアップと復元 749
バックアップおよびエクスポートの設定 749
バックアップ タイプ 750
バックアップ操作の考慮事項と推奨事項 750
スケジューリング バックアップ 751
完全な状態のバックアップ ポリシー 752
すべてのコンフィギュレーションのエクスポート ポリシー 752
コンフィギュレーションのインポート 752
インポート方法 752
システムの復元 753
バックアップ操作とインポート操作に必要なユーザ ロール 753
バックアップ操作の設定 753
バックアップ操作の作成 753

バックアップ操作の実行 758

バックアップ操作の変更 758

1 つまたは複数のバックアップ操作の削除 759

スケジュール バックアップの設定 760

完全な状態のバックアップ ポリシーの設定 760

すべてのコンフィギュレーションのエクスポート ポリシーの設定 762

インポート操作の設定 763

インポート操作の作成 763

インポート操作の実行 766

インポート操作の変更 767

1 つまたは複数のインポート操作の削除 768

ファブリック インターコネクトの設定の復元 769

失われたパスワードの復旧 771

失われたパスワードの復旧 771

admin アカウントのパスワードの復旧 771

ファブリック インターコネクトのリーダーシップ ロールの決定 772

ファブリック インターコネクトのファームウェア バージョンの確認 772

スタンドアロン設定の admin アカウント パスワードの復旧 772

クラスタ設定の admin アカウント パスワードの復旧 774

システム モニタリング 777

トラフィックのモニタリング 779

トラフィック モニタリング 779

トラフィック モニタリングに関する注意事項および推奨事項 780

イーサネット トラフィックのモニタリング セッションの作成 781

ファイバ チャネル トラフィック モニタリング セッションの作成 783

モニタリング セッションへのトラフィック送信元の追加 784

トラフィックのモニタリング セッションのアクティブ化 785

トラフィック モニタリング セッションの削除 785

ハードウェアのモニタリング 787

ファブリック インターコネクトのモニタリング 787

シャーシのモニタリング 788

ブレード サーバのモニタリング 790

ラックマウント サーバのモニタリング 793
I/O モジュールのモニタリング 796
管理インターフェイスのモニタリング 796
管理インターフェイスのモニタリング ポリシー 796
管理インターフェイスのモニタリング ポリシーの設定 797
サーバ ディスク ドライブ モニタリング 799
ディスク ドライブ モニタリングのサポート 800
ディスク ドライブ モニタリングの前提条件 800
を使用したディスク ドライブのステータスの確認 801
監視対象ディスク ドライブのステータスの解釈 802
統計関連ポリシーの設定 805
統計情報収集ポリシーの設定 805
統計情報収集ポリシー 805
統計情報収集ポリシーの変更 806
統計情報しきい値ポリシーの設定 808
統計情報しきい値ポリシー 808
サーバおよびサーバ コンポーネントのしきい値ポリシーの作成 808
既存サーバおよびサーバ コンポーネントしきい値ポリシーへのしきい値クラスの追加 810
サーバおよびサーバ コンポーネントのしきい値ポリシーの削除 812
アップリンク イーサネット ポートしきい値ポリシーへのしきい値クラスの追加 812
イーサネット サービス ポート、シャーシ、およびファブリック インターコネクトのしきい値ポリシーへのしきい値クラスの追加 814
ファイバ チャネル ポートしきい値ポリシーへのしきい値クラスの追加 815
Call Home の設定 817
Call Home 817
Call Home の考慮事項とガイドライン 819
Cisco UCS 障害と Call Home の重大度 820
Cisco Smart Call Home 821
Call Home の設定 822
Call Home のディセーブル化 826
Call Home のイネーブル化 826

システム インベントリ メッセージの設定 827
システム インベントリ メッセージの設定 827
システム インベントリ メッセージの送信 828
Call Home プロファイルの設定 828
Call Home プロファイル 828
Call Home アラート グループ 829
Call Home プロファイルの作成 830
Call Home プロファイルの削除 833
Call Home ポリシーの設定 833
Call Home ポリシー 833
Call Home ポリシーの設定 833
Call Home ポリシーのディセーブル化 834
Call Home ポリシーのイネーブル化 835
Call Home ポリシーの削除 835
例：Smart Call Home の Call Home の設定 835
Smart Call Home の設定 835
デフォルトの Cisco TAC-1 プロファイルの設定 838
Smart Call Home に対するシステム インベントリ メッセージの設定 838
Smart Call Home の登録 839
システム イベント ログの管理 841
システム イベント ログ 841
各サーバのシステム イベント ログの表示 842
シャーシ内のサーバのシステム イベント ログの表示 842
SEL ポリシーの設定 843
サーバのシステム イベント ログの管理 845
システム イベント ログの 1 つ以上のエントリのコピー 845
システム イベント ログの印刷 845
システム イベント ログのリフレッシュ 846
システム イベント ログの手動バックアップ 846
システム イベント ログの手動クリア 847
障害、イベント、およびログの設定 849
障害収集ポリシーの設定 849

障害収集ポリシー 849
障害収集ポリシーの設定 850
エラーの抑制の設定 852
エラーの抑制 852
抑制されたエラーの表示 853
シャーシのエラー抑制の設定 854
シャーシのエラー抑制タスクの設定 854
シャーシのエラー抑制タスクの削除 855
シャーシのエラー抑制タスクの表示 856
I/O モジュールのエラーの抑制の設定 856
IOM のエラー抑制タスクの設定 856
IOM のエラー抑制タスクの削除 857
IOM のエラー抑制タスクの表示 858
FEX のエラー抑制の設定 858
FEX のエラー抑制タスクの設定 858
FEX のエラー抑制タスクの表示 860
FEX のエラー抑制タスクの削除 860
サーバのエラー抑制の設定 861
ブレード サーバのエラー抑制タスクの設定 861
ラック サーバのエラー抑制タスクの設定 862
ブレード サーバのエラー抑制タスクの削除 863
ラック サーバのエラー抑制タスクの削除 863
ブレード サーバのエラー抑制タスクの表示 864
ラック サーバのエラー抑制タスクの表示 864
サービス プロファイルのエラー抑制の設定 865
サービス プロファイルのエラー抑制タスクの設定 865
サービス プロファイルのエラー抑制タスクの削除 866
サービス プロファイルのエラー抑制タスクの表示 867
組織のエラー抑制の設定 867
組織のエラー抑制タスクの設定 867
組織のエラー抑制タスクの削除 868
組織のエラー抑制タスクの表示 869

Core File Exporter の設定 869
Core File Exporter 869
Core File Exporter の設定 869
Core File Exporter のディセーブル化 871
syslog の設定 871

はじめに

この前書きは、次の項で構成されています。

- 対象読者，xxxv ページ
- 表記法，xxxv ページ
- Cisco UCS の関連資料，xxxvii ページ
- マニュアルに関するフィードバック，xxxvii ページ

対象読者

このガイドは、次の 1 つ以上に責任と専門知識を持つ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

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。

表記法	用途
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、イタリック体フォントで示しています。
courier フォント	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。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	必ずいずれか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。

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。

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。

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。 機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。 警告の各国語版については、各警告文の末尾に提示されている番号をもとに、この機器に付属している各国語で記述された安全上の警告を参照してください。

これらの注意事項を保存しておいてください。

Cisco UCS の関連資料

ドキュメント ロードマップ

B シリーズのすべてのマニュアルの完全なリストについては、次の URL で入手できる『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。 http://www.cisco.com/go/unifiedcomputing/b-series-doc

すべての C シリーズのマニュアルの完全なリストについては、次の URL にある『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。http://www.cisco.com/go/unifiedcomputing/c-series-doc

他のマニュアル リソース

B シリーズと C シリーズのすべてのマニュアルが含まれる ISO ファイルは、次の URL で入手できます。http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821 このページから、[Unified Computing System (UCS) Documentation Roadmap Bundle] をクリックします。

ISO ファイルは主要な各マニュアルのリリース後に更新されます。

マニュアルの更新通知を受信するには、Cisco UCS Docs on Twitter をフォローしてください。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバックフォームよりご連絡ください。 ご協力をよろしくお願いいたします。

第 I 部

概要

- 新機能および変更された機能に関する情報，3 ページ
- Cisco Unified Computing System の概要，11 ページ
- Cisco UCS Manager の概要，31 ページ
- Cisco UCS Manager GUI の概要，37 ページ

第 1 章

新機能および変更された機能に関する情報

この章の内容は、次のとおりです。

- このリリースの新規情報および変更情報，3 ページ

このリリースの新規情報および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。 この表は、コンフィギュレーション ガイドに加えられたすべての変更、またはこのリリースの新機能をすべて網羅したリストを示すものではありません。 このリリースで新しくサポートされるハードウェアについては、『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。 http://www.cisco.com/go/unifiedcomputing/b-series-docを参照してください。

表 *1*：*Cisco UCS Release 2.1(1)* の新機能および動作の変更

機能	説明	ドキュメント名
Cisco UCS Central	複数の Cisco UCS Manager セッションを介してデータセンター全体のグローバル ビューを示します。 Cisco UCS Central を使用して個々のデータセンターまたは複数のデータセンターの Cisco UCS 動作を管理できます。 Cisco UCS Central は、ファームウェア管理、カタログ管理、設定のバックアップおよび復元の操作、モニタリング ログ、コア ファイルおよび障害のために登録済み Cisco UCS ドメインの動作管理を容易にします。	この機能は、Cisco UCS Central のコンフィギュレーション ガイドおよびそのほかの資料に記載されています。 Cisco UCS Centralのマニュアルは、次の URL で入手できます。http://www.cisco.com/en/US/products/ps12502/products_installation_and_configuration_guides_list.html

機能	説明	ドキュメント名
シングル ワイヤ管理による Cisco UCS C シリーズ サーバの統合	ネットワーク コントローラのサイドバンド インターフェイス（NC-SI）を使用してシングルワイヤ管理モードで Cisco UCS C シリーズ ラック サーバを統合できます。 デュアルワイヤ管理による統合も、このリリースで使用できます。	この機能は、『*Cisco UCS C-Series Server Integration with Cisco UCS Manager 2.1*』に記載されています。 C シリーズの統合ガイドは、http://www.cisco.com/en/US/partner/products/ps11736/products_installation_and_configuration_guides_list.html にあります。
デフォルトの vNIC および vHBA の動作ポリシー	vNIC および vHBA がサービス プロファイルに対してどのように作成されるかを指定できます。 vNIC および vHBA を手動で作成するように選択することも、Cisco UCS Manager でそれらを自動的に作成することもできます。	デフォルトの vNIC 動作ポリシー：ネットワーク関連ポリシーの設定, （305 ページ） デフォルト vHBA 動作ポリシー：ストレージ関連ポリシーの設定, （389 ページ）
エラーの抑制	定期メンテナンス時間中に SNMP トラップと Call Home 通知を抑制できます。 エラーの抑制タスクを作成することで、一時的なエラーの発生時やクリア時に通知が送信されることを防ぐことができます。	エラーの抑制, （852 ページ）
FCoE アップリンク ポート	イーサネット トラフィックやファイバ チャネル トラフィックを伝送する FCoE アップリンク ポートとしてイーサネット ポートを設定できます。	FCoE アップリンク ポート, （96 ページ）
FCoE ポート チャネル	1 つの論理的な FCoE チャネル リンクを作成して耐障害性と高速接続を実現するために、複数の物理 FCoE ポートをグループ化できます。	FCoE ポート チャネル, （114 ページ）

機能	説明	ドキュメント名
ファイバ チャネル ゾーン分割	ファイバチャネルファブリックを1つ以上のゾーンに分割できます。各ゾーンは、VSAN で相互に通信できるファイバ チャネル イニシエータおよびファイバ チャネル ターゲットのセットを定義します。また、ゾーン分割により、ホストとストレージ デバイスまたはユーザ グループ間のアクセス コントロールの設定も可能になります。	ファイバチャネルゾーン分割の設定，（415 ページ）
ファームウェアの自動インストール	インフラストラクチャ ファームウェア アップグレードとサーバ ファームウェア アップグレードの2段階で、1つのパッケージに含まれるファームウェア バージョンにCisco UCS ドメインをアップグレードできます。	この機能は、次のコンフィギュレーション ガイドに記載されています。 • 『*Cisco UCS B-Series Firmware GUI Configuration Guide*』 • 『*Cisco UCS B-Series Firmware CLI Configuration Guide*』 ファームウェアのコンフィギュレーション ガイドは、http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html にあります。

機能	説明	ドキュメント名
ファームウェアのクロスバージョン サポート	Cisco UCS ドメインのインフラストラクチャ ファームウェアを Cisco UCS Release 2.1 にアップグレードし、サーバファームウェアを Cisco UCS Release 2.0 のまま残して、サーバ リブートによる中断を避けることができます。	この機能は、次のコンフィギュレーション ガイドに記載されています。 • 『*Cisco UCS B-Series Firmware GUI Configuration Guide*』 • 『*Cisco UCS B-Series Firmware CLI Configuration Guide*』 ファームウェアのコンフィギュレーション ガイドは、http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html にあります。
サービス プロファイル設定の LAN および SAN 接続ポリシー	ネットワーク上の LAN または SAN とサーバ間のネットワーク通信リソースと接続を制御する接続ポリシーを設定できます。 これらのポリシーでは、サービス プロファイルとサービス プロファイル テンプレートを作成するための適切な権限を従業員に許可しながらも、LAN および SAN 接続の作成をネットワーク管理者およびストレージ管理者に制限することができます。	LAN 接続ポリシー：ネットワーク関連ポリシーの設定, （305 ページ） SAN 接続ポリシー：ストレージ関連ポリシーの設定, （389 ページ）
マルチキャスト ポリシー	VLAN 上のいずれのホストが特定のマルチキャスト送信に含まれるかを動的に決定するように、インターネット グループ管理プロトコル（IGMP）スヌーピングおよび IGMP クエリアを設定できます。	マルチキャスト ポリシー, （339 ページ）

機能	説明	ドキュメント名
権限マニュアル	個別の参考文献にCisco UCSのユーザ権限に関する詳細情報を記載してあります。	この機能は「*Privileges in Cisco UCS*」に記載されており、次のURLからアクセスできます。http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html に記載されています。
スケジュール バックアップ	完全な状態のバックアップおよびすべての設定エクスポートをスケジュールできます。	スケジューリング バックアップ，（751 ページ）
サービス プロファイルの名前変更	既存のサービス プロファイルの名前を変更できます。	サービス プロファイルの設定，（575 ページ）
フラッシュ I/O デバイスのディスカバリのサポート	サポートされているCisco UCSサーバにPCIeベースのフラッシュ ストレージ デバイスのディスカバリおよびインベントリが含まれます。	
Linux での Multiple Receive Queue Support（MRQS）のサポート	Red Hat Enterprise Linux バージョン 6.x および SUSE Linux Enterprise Server バージョン 11.x に Multiple Receive Queue Support（MRQS）機能の eNIC サポートが含まれます。	Linux オペレーティング システム上の MRQS に対する eNIC サポートをイネーブルにするためのイーサネット アダプタ ポリシーの設定，（317 ページ）
Finite State Machine（FSM）プロセスのトラブルシューティング機能の拡張	予想される FSM の段階移行と現在および以前の段階履歴など FSM について表示される情報を拡張します。	
ユニファイド アップリンク ポート	同一物理ポートでイーサネット ポートおよび FCoE ポートを設定できます。	ユニファイドアップリンク ポート，（100 ページ）
ユニファイド アップリンク ポート チャネル	1 つの論理的なユニファイド アップリンク ポート チャネル リンクを作成して耐障害性と高速接続を実現するために、同じ ID でイーサネット ポート チャネルおよび FCoE ポート チャネルを設定できます。	ユニファイドアップリンク ポート チャネル，（115 ページ）

機能	説明	ドキュメント名
ユニファイド ストレージ ポート	イーサネット ストレージインターフェイスおよび FCoE ストレージインターフェイスと同じ物理ポートを設定できます。	ユニファイド ストレージ ポート, （97 ページ）
vCon の割り当てと配布	Cisco UCS で vCon に vNIC および vHBA を暗黙的に割り当てる際に使用されるアルゴリズムを変更し、vNIC/vHBA 配置ポリシーによって vCon に vNIC または vHBA を明示的に割り当てられるようにします。	サーバ関連ポリシーの設定, （447 ページ）
VLAN のポート数の最適化	複数の VLAN の状態を単一の内部状態にマッピングし、ポートVLAN数に基づいて VLAN を論理的にグループ化します。 このグループ化ではポート VLAN 数が増加し、VLAN状態が圧縮され、ファブリックインターコネクトのCPU負荷が軽減されます。	VLANのポート数の最適化, （275 ページ）
VLAN グループ	特定のネットワークに属するVLANまたは機能によってイーサネットポートの VLAN をグループ化します。	VLAN グループ, （278 ページ）
VLAN の権限	指定された組織に基づいて VLAN へのアクセスを制限し、サービスプロファイルのvNICに割り当てることができる VLAN のセットを制限します。	VLAN の権限, （281 ページ）

機能	説明	ドキュメント名
Hyper-V SRIOV の VM-FEX 統合	Hyper-V 向けの Cisco Virtual Machine Fabric Extender（VM-FEX）は Cisco UCS Manager および VMware vCenter 間の管理統合とネットワーク通信を提供します。	この機能は、次のコンフィギュレーションガイドに記載されています。 • 『*Cisco UCS Manager VM-FEX for Hyper-V GUI Configuration Guide*』 • 『*Cisco UCS Manager VM-FEX for Hyper-V CLI Configuration Guide*』 VM-FEX のコンフィギュレーションガイドは、http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html にあります。
KVM（Red Hat Linux）SRIOV の VM-FEX 統合	Cisco UCS ドメイン内の Linux ベースのハイパーバイザ KVM 上で実行されている仮想マシンに外部スイッチングを提供する KVM 向けの Cisco Virtual Machine Fabric Extender（VM-FEX）の機能に対する拡張と重要な改善が含まれます。	この機能は、次のコンフィギュレーションガイドに記載されています。 • 『*Cisco UCS Manager VM-FEX for KVM GUI Configuration Guide*』 • 『*Cisco UCS Manager VM-FEX for KVM CLI Configuration Guide*』 VM-FEX のコンフィギュレーションガイドは、http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html にあります。

第 2 章

Cisco Unified Computing System の概要

この章の内容は、次のとおりです。

- Cisco Unified Computing System について，11 ページ
- ユニファイド ファブリック，13 ページ
- サーバのアーキテクチャおよび接続性，14 ページ
- トラフィック管理，19 ページ
- オプトイン機能，26 ページ
- Cisco UCS の仮想化，29 ページ

Cisco Unified Computing System について

Cisco Unified Computing System（Cisco UCS）は、アクセス レイヤ ネットワーキングとサーバを融合します。 この高性能次世代サーバ システムは、作業負荷に対する敏捷性およびスケーラビリティの高いデータセンターを実現します。

ハードウェア コンポーネントおよびソフトウェア コンポーネントは、1 つの統合ネットワーク アダプタ上に複数のタイプのデータセンター トラフィックを通過させる、シスコのユニファイド ファブリックをサポートします。

アーキテクチャの単純化

Cisco UCS のアーキテクチャを単純化することにより、必要なデバイスの数を削減し、スイッチング リソースを中央に集中させることができます。 シャーシ内部でのスイッチングを止めると、ネットワーク アクセス レイヤのフラグメンテーションが大きく減少します。

Cisco UCS は、ラック、またはラックのグループでシスコのユニファイド ファブリックを実装し、10 ギガビット シスコ データセンター イーサネット リンクおよび Fibre Channel over Ethernet（FCoE）リンク経由でイーサネットおよびファイバ チャネル プロトコルをサポートします。

この徹底的な単純化により、スイッチ、ケーブル、アダプタ、および管理ポイントの最高 3 分の 2 が削減されます。 Cisco UCS ドメイン内のデバイスはすべて、1 つの管理ドメインの下にとどまり、冗長コンポーネントの使用中、ハイ アベイラビリティを保ちます。

ハイ アベイラビリティ

Cisco UCS の管理およびデータ プレーンはハイ アベイラビリティおよび冗長アクセス レイヤ ファブリック インターコネクトのために設計されています。 さらに、Cisco UCS は、データ レプリケーションやアプリケーションレベルのクラスタ処理テクノロジーなど、データセンターに対する既存のハイ アベイラビリティおよびディザスタ リカバリ ソリューションをサポートします。

拡張性

単一の Cisco UCS ドメインは複数のシャーシおよびそのサーバをサポートします。これらはすべて 1 つの Cisco UCS Manager を通じて管理されます。 スケーラビリティの詳細については、シスコの担当者にお問い合わせください。

柔軟性

Cisco UCS ドメインでは、データセンターのコンピューティング リソースを、急速に変化するビジネス要件にすばやく合せることができます。 この柔軟性を組み込むかどうかは、ステートレス コンピューティング機能の完全な実装が選択されているかどうかによって決定されます。

必要に応じて、サーバやその他のシステム リソースのプールを適用し、作業負荷の変動への対応、新しいアプリケーションのサポート、既存のソフトウェアおよびビジネス サービスの拡張、スケジュール済みのダウンタイムおよび予定されていないダウンタイムの両方への適応を行うことができます。 サーバの ID は、最小のダウンタイムで、追加のネットワーク設定を行わずにサーバからサーバへ移動できるモバイル サービス プロファイルに抽象化することができます。

このレベルの柔軟性により、サーバの ID を変更したり、サーバ、Local Area Network（LAN; ローカル エリア ネットワーク）、または Storage Area Network（SAN）を再設定したりせずに、すばやく、簡単にサーバの容量を拡張することができます。 メンテナンス ウィンドウでは、次の操作をすばやく行うことができます。

- 予測していなかった作業負荷要求に対応し、リソースとトラフィックのバランスを取り戻すために新しいサーバを導入します。
- あるサーバでデータベース管理システムなどのアプリケーションをシャットダウンし、I/O 容量とメモリ リソースを拡張した別のサーバでこれを再度起動します。

サーバ仮想化に向けた最適化

Cisco UCS は VM-FEX テクノロジーを実装するために最適化されています。 このテクノロジーは、より優れたポリシーベースの設定とセキュリティ、会社の運用モデルとの適合、VMware の VMotion への順応など、サーバ仮想化に対してより優れたサポートを実現します。

ユニファイド ファブリック

ユニファイド ファブリックを使用すると、単一の Data Center Ethernet（DCE; データセンター イーサネット）ネットワーク上で複数の種類のデータセンター トラフィックを行き来させることができます。 さまざまな一連のホスト バス アダプタ（HBA）およびネットワーク インターフェイス カード（NIC）をサーバに搭載させる代わりに、ユニファイド ファブリックは統合された単一のネットワーク アダプタを使用します。 このタイプのアダプタは、LAN および SAN のトラフィックを同一のケーブルで運ぶことができます。

Cisco UCS は、Fibre Channel over Ethernet（FCoE）を使用して、ファブリック インターコネクトとサーバ間をつなぐ同一の物理イーサネット接続でファイバ チャネルおよびイーサネットのトラフィックを運びます。 この接続はサーバ上の統合されたネットワーク アダプタで終端し、ユニファイド ファブリックはファブリック インターコネクトのアップリンク ポートで終端します。 コア ネットワークでは、LAN および SAN のトラフィックは分かれたままです。 Cisco UCS では、データセンター全体でユニファイド ファブリックを実装する必要はありません。

統合されたネットワーク アダプタは、オペレーティング システムに対してイーサネット インターフェイスおよびファイバ チャネル インターフェイスを提示します。 サーバ側では、標準のファイバ チャネル HBA を確認しているため、オペレーティング システムは FCoE のカプセル化を認識していません。

ファブリック インターコネクトでは、サーバ側イーサネット ポートでイーサネットおよびファイバ チャネルのトラフィックを受信します。 （フレームを区別する Ethertype を使用する）ファブリック インターコネクトは、2 つのトラフィックの種類に分かれます。 イーサネット フレームおよびファイバ チャネル フレームは、それぞれのアップリンク インターフェイスにスイッチされます。

Fibre Channel over Ethernet

Cisco UCS は、Fibre Channel over Ethernet（FCoE）標準プロトコルを使用して、ファイバ チャネルを提供します。 上部のファイバ チャネル レイヤは同じであるため、ファイバ チャネル動作モデルが維持されます。 FCoE ネットワーク管理と設定は、ネイティブのファイバ チャネル ネットワークと同様です。

FCoE は、物理イーサネット リンク上のファイバ チャネル トラフィックをカプセル化します。 FCoE は専用のイーサタイプ 0x8906 を使用して、イーサネット上でカプセル化されるため、FCoE トラフィックと標準イーサネット トラフィックは同じリンク上で処理できます。 FCoE は ANSI T11 標準委員会によって標準化されています。

ファイバ チャネル トラフィックには、ロスレス トランスポート層が必要です。 ネイティブ ファイバ チャネルが使用するバッファ間クレジット システムの代わりに、FCoE はイーサネット リンクを使用して、ロスレス サービスを実装します。

ファブリック インターコネクト上のイーサネット リンクは、2 つのメカニズムを使用して、FCoE トラフィックのロスレス トランスポートを保証します。

- リンク レベル フロー制御
- プライオリティ フロー制御

リンクレベル フロー制御

IEEE 802.3x リンクレベル フロー制御では、輻輳の発生している受信側からエンドポイントに対して、少しの間、データの送信を一時停止するように信号を送ることができます。 このリンクレベル フロー制御では、リンク上のすべてのトラフィックが一時停止します。

送受信方向は個別に設定できます。 デフォルトでは、リンクレベル フロー制御は両方向でディセーブルです。

各イーサネットインターフェイスで、ファブリックインターコネクトは、プライオリティフロー制御、またはリンクレベル フロー制御のいずれかをイネーブルにできます。両方をイネーブルにはできません。

プライオリティ フロー制御

プライオリティフロー制御（PFC）機能は、イーサネットリンク上の特定のトラフィック クラスにポーズ機能を適用します。 たとえば、PFC は FCoE トラフィックにロスレス サービスを、標準イーサネット トラフィックにベストエフォート サービスを提供します。 PFC は、（IEEE 802.1p トラフィック クラスを使用して）特定のイーサネット トラフィック クラスに、さまざまなレベルのサービスを提供することができます。

PFC は、IEEE 802.1p の CoS 値に基づき、ポーズを適用するかどうかを判断します。 ファブリック インターコネクトは、PFC をイネーブルにするときに、特定の CoS 値を持つパケットにポーズ機能を適用するように、接続されたアダプタを設定します。

デフォルトでは、ファブリック インターコネクトは、PFC 機能をイネーブルにするかどうかのネゴシエーションを行います。 ネゴシエーションに成功すると、PFC がイネーブルにされますが、リンクレベル フロー制御は（設定値に関係なく）ディセーブルのままです。 PFC ネゴシエーションに失敗した場合は、PFC をインターフェイスで強制的にイネーブルにするか、IEEE 802.x リンクレベル フロー制御をイネーブルにできます。

サーバのアーキテクチャおよび接続性

サービス プロファイルの概要

サービス プロファイルは、Cisco UCS の中心概念です。 各サービス プロファイルにより具体的な目的のサービスが提供されるため、関連付けられたサーバ ハードウェアでホスティングされるアプリケーションをサポートするために必要な設定が確実にハードウェアに設定されます。

サービスプロファイルには、サーバハードウェア、インターフェイス、ファブリック接続、およびサーバとネットワークの ID に関する設定情報が保持されます。 この情報は、Cisco UCS Manager を使って管理できる形式で保存されています。 すべてのサービスプロファイルは一元的に管理され、ファブリック インターコネクト上のデータベースに格納されます。

各サーバは、サービス プロファイルと関連付けられる必要があります。

重要 各サーバは、いつの時点においても 1 つのサービス プロファイルだけに関連付けることができます。 同様に、各サービス プロファイルは一度に 1 つのサーバだけに関連付けることができます。

サービスプロファイルをサーバと関連付けると、サーバではオペレーティングシステムとアプリケーションをインストールする準備が整います。サーバの設定はサービス プロファイルで確認することができます。サービスプロファイルとのアソシエーションを形成しているサーバで不具合が発生しても、サービス プロファイルが自動的に別のサーバにフェールオーバーすることはありません。

サーバからサービス プロファイルの関連付けが解除されると、サーバの ID および接続の情報は工場出荷時のデフォルトにリセットされます。

サービス プロファイルによるネットワーク接続

各サービス プロファイルは、このサーバについて、Cisco UCS インフラストラクチャを経由して外部ネットワークに接続する LAN および SAN ネットワーク接続を指定します。 Cisco UCS サーバおよびその他のコンポーネントについて、ネットワーク接続を手動で設定する必要はありません。 すべてのネットワーク設定は、サービス プロファイルを通じて行われます。

サービス プロファイルをサーバに関連付けると、サービス プロファイルの情報を使用して Cisco UCS 内部ファブリックが設定されます。 このプロファイルが以前に別のサーバと関連付けられていた場合、ネットワーク インフラストラクチャが再構成され、新しいサーバに対して同じネットワーク接続がサポートされます。

サービス プロファイルによる設定

サービスプロファイルはリソースプールとポリシーを利用して、サーバと接続設定を操作できます。

サービス プロファイルで設定されたハードウェア コンポーネント

サービス プロファイルがサーバに関連付けられているときには、プロファイルのデータに応じて次のコンポーネントが設定されます。

- BIOS および CIMC を含むサーバ
- アダプタ
- ファブリック インターコネクト

これらのコンポーネントを直接設定する必要はありません。

サービス プロファイルによるサーバ ID 管理

製造元がサーバ ハードウェアに記録したネットワーク ID およびデバイス ID を使用できます。あるいは、関連付けられたサービス プロファイルで指定した ID を直接または MAC、WWN、UUID などの ID プール経由で使用できます。

次の例は、サービス プロファイルに含めることができる設定情報の方法を示しています。

- プロファイル名と説明
- 一意のサーバ ID（UUID）
- MAC アドレスなどの LAN 接続属性
- WWN などの SAN 接続属性

サービス プロファイルで設定した操作面

次のように、サービス プロファイルで設定できるサーバ操作機能があります。

- ファームウェア パッケージとバージョン
- オペレーティング システム ブート順序と設定
- IPMI と KVM アクセス

サービス プロファイルによる vNIC 設定

vNIC は物理ネットワーク アダプタで設定される仮想化されたネットワーク インターフェイスであり、サーバのオペレーティング システムに物理 NIC として表示されます。 システムのアダプタの種類によって、作成できる vNIC の数は異なります。 たとえば、統合ネットワーク アダプタには NIC が 2 つあります。つまり、アダプタごとに最大 2 つの vNIC を作成できます。

vNIC はイーサネット上で通信し、LAN トラフィックを処理します。 少なくとも、各 vNIC には名前、ファブリック接続、ネットワーク接続を設定する必要があります。

サービス プロファイルによる vHBA 設定

vHBA とは、物理ネットワーク アダプタ上に設定される仮想化されたホスト バス アダプタのことで、サーバのオペレーティング システムには物理 HBA に見えます。 システムのアダプタの種類に応じて作成できる vHBA の数が決まります。 たとえば、統合ネットワーク アダプタには HBA が 2 つあります。つまり、アダプタごとに最大 2 つの vHBA を作成できます。 他方、ネットワーク インターフェイス カードには HBA がありません。これは、アダプタで vHBA を作成できないことを意味します。

vHBA は FCoE 上で通信し、SAN トラフィックを処理します。 少なくとも、各 vHBA には名前とファブリック接続を設定する必要があります。

サーバ 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。 このプロファイルを使用すると、関連付けの時点でサーバにある ID の値を上書きし、Cisco UCS Manager のリソース プールとポリシー設定を使用して管理タスクの一部を自動化できます。

このサービス プロファイルとサーバの関連付けを解除して、このプロファイルを別のサーバ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 プール ポリシーを通じて行うこともできます。 新しいサーバのハードウェアが持つ UUID や MAC

アドレスなどの工場出荷時の設定は、サービス プロファイルの設定で上書きされます。 その結果、サーバでの変更はネットワークには透過的に行われます。 新しいサーバ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、サーバプールの資格ポリシー、または個々のハードウェア設定を必要とする別のポリシーが含まれている場合、プロファイルは、Cisco UCS ドメインで、任意のタイプのサーバを使用できます。

これらのサービス プロファイルは、ラックマウント サーバまたはブレード サーバと関連付けることができます。 サービス プロファイルを移行する機能は、サービス プロファイルの移行の制限を選択するかどうかにより異なります。

（注） 移行を制限しない場合は、既存のサービス プロファイルを移行する前に、Cisco UCS Manager による新規サーバに対する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 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、サーバのデフォルト値を使用して、ラックマウント型サーバの管理を模倣します。 このプロファイルは特定のサーバに結び付けられており、別のサーバへの移動または移行はできません。

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
- サーバの UUID

重要 このプロファイルをサーバに関連付ける前に、製造元でサーバ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 テンプレート

サービス プロファイル テンプレートにより、同一の基本パラメータ（vNIC および vHBA の数など）や、同じプールから取得された ID 情報が含まれる複数のサービス プロファイルを迅速に作成できます。

ヒント 既存のサービス プロファイルに類似した値が含まれるサービス プロファイルが 1 つだけ必要な場合は、Cisco UCS Manager GUI でサービス プロファイルのクローニングが可能です。

たとえば、サーバをホストデータベース ソフトウェアに設定するために同様の値が含まれた複数のサービスプロファイルが必要な場合は、手作業でも既存のサービスプロファイルからでもサービス プロファイル テンプレートを作成できます。 次に、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。 しかし、プロファイルの作成後は、テンプレートへの接続が失われます。 このテンプレートから作成された 1 つ以上のプロファイルを変更する必要がある場合は、これらのプロファイルを個別に変更する必要があります。

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 プロファイルでは、テンプレートのすべてのプロパティが継承され、テンプレートへのつながりが保持されます。 テンプレートの何らかの変更があると、テンプレートから作成されたサービス プロファイルは自動的にアップデートされます。

ポリシー

ポリシーは、ある特定の状況で、Cisco UCS コンポーネントがどのように動作するかを決定します。 大半のポリシーで複数のインスタンスを作成することができます。 たとえば、サーバに応じて、PXE ブート、SAN ブート、ローカルストレージからのブートを使い分けられるように、異なるブート ポリシーが必要になる場合があります。

ポリシーにより、システム内で機能を区別することができます。 対象事象のエキスパートは、その対象事象を専門としない他者により作成されたサービス プロファイルで使用されるポリシーを定義できます。 たとえば、LAN アドミニストレータは、そのシステムのアダプタ ポリシー、お

よびQuality Of Serviceポリシーを作成できます。 次に、LAN管理に関する対象事項の専門知識が限られているか、あるいはまったく欠けている他者により作成されたサービス プロファイルで、これらのポリシーを使用できます。

Cisco UCS Managerでは、下記の2つのタイプのポリシーを作成して使用できます。

- サーバおよびその他のコンポーネントを設定する設定ポリシー
- 特定の管理、モニタリング、およびアクセス コントロール機能を制御する操作ポリシー

プール

プールは、システムで使用できるIDのコレクション、物理リソース、または論理リソースです。 すべてのプールは、サービスプロファイルの柔軟性を高め、ユーザがシステムリソースを中央で集中管理できるようにします。

プールを使用して、未設定のサーバや、使用可能なサーバID情報の範囲を、データセンターにとって意味のあるグループに分割することができます。 たとえば、類似する特性を持つ未設定のサーバのプールを作成して、このプールをサービス プロファイルにインクルードした場合、ポリシーを使用して、このサービス プロファイルと使用可能な未設定のサーバとのアソシエーションを形成することができます。

MACアドレスなどのID情報をプールした場合、特定のアプリケーションをホストするサーバに範囲をあらかじめ割り当てることができます。 たとえば、すべてのデータベースサーバを、同じ範囲のMACアドレス、UUID、およびWWN内に設定できます。

Domain Pools

[Domain Pools] はCisco UCSドメインにローカルに定義され、そのCisco UCSドメインでのみ使用できます。

Global Pools

[Global Pools] はCisco UCS Centralに定義され、Cisco UCSドメイン間で共有できます。 Cisco UCSドメインがCisco UCS Centralに登録されている場合、[Global Pools] をCisco UCS Managerに割り当てることができます。

トラフィック管理

オーバーサブスクリプション

オーバーサブスクリプションは、同じファブリックインターコネクトポートに複数のネットワークデバイスが接続されているときに発生します。 ポートが短時間でも最高速度で実行されることはほとんどないため、これにより、ファブリックインターコネクトの使用が最適化されます。 その結果、オーバーサブスクリプションが正しく設定されていれば、使用されていない帯域幅を活用できるようになります。 しかし、オーバーサブスクリプションの設定に間違いがあると、帯域

幅のコンテンションが起こり、オーバーサブスクライブ ポートを使用しているすべてのサービスで Quality Of Service が低下します。

たとえば、4 つのサーバが 1 つのアップリンク ポートを共有していて、これらのサーバがすべて、このアップリンク ポートで使用できる帯域幅よりも大きい累積率でデータを送信しようとした場合に、オーバーサブスクリプションが発生します。

オーバーサブスクリプションにおける検討事項

Cisco UCS ドメインでのオーバーサブスクリプションの設定に影響を与える可能性のある要因は次のとおりです。

アップリンク ポートに対するサーバに面したポートの比率

この比率はパフォーマンスに影響を与えるため、システム内のサーバに面したポートの数と、アップリンク ポートの数を知っている必要があります。たとえば、使用しているシステムに、サーバと通信できるポートが 20 個あるときに、ネットワークと通信できるポートが 2 つだけの場合、このアップリンク ポートはオーバーサブスクライブされます。この状況では、サーバにより作成されるトラフィックの量もパフォーマンスに影響を与えます。

ファブリック インターコネクトからネットワークへのアップリンク ポートの数

Cisco UCS ファブリック インターコネクトと LAN の上位層の間にさらにアップリンク ポートを追加して、帯域幅を増やすことができます。 Cisco UCS では、すべてのサーバと NIC が確実に LAN にアクセスできるようにするために、ファブリック インターコネクト 1 つにつき、少なくとも 1 つのアップリンク ポートが必要です。 LAN アップリンクの数は、すべての Cisco UCS サーバで使用される帯域幅の合計により決定されます。

6100 シリーズ ファブリック インターコネクトでは、ファイバ チャネル アップリンク ポートは拡張スロットのみで使用できます。使用可能なファイバチャネルアップリンクの数を増やすには、拡張スロットを追加する必要があります。 イーサネット アップリンク ポートは、固定スロットと拡張スロットに存在できます。

Cisco UCS Manager バージョン 2.0 以降を実行する 6200 シリーズ ファブリック インターコネクトでは、イーサネット アップリンク ポートとファイバ チャネル アップリンク ポートの両方を、ベース モジュールに加え、拡張ジュール上にも設定できます。

たとえば、2 つの Cisco UCS 5100 シリーズ シャーシに、ハーフ幅の Cisco UCS B200-M1 サーバが最大限に入っている場合、サーバの数は 16 台です。 ファブリック インターコネクト 1 つあたり LAN アップリンクが 1 つのクラスタ設定では、これら 16 台のサーバは 20GbE の LAN 帯域幅を共有します。より大きい容量が必要である場合、ファブリックインターコネクトからさらにアップリンクを追加する必要があります。 クラスタ設定では、アップリンクを対称設定にすることを推奨します。この例で、ファブリック インターコネクト 1 つにつき使用されるアップリンクの数が 4 つである場合、16 台のサーバが 80GB の帯域幅を共有することになるため、各サーバの容量は約 5GB になります。 Cisco UCS ファブリック インターコネクトで複数のアップリンクが使用されている場合、この容量を最大限有効活用するために、ネットワーク設計チームはポート チャネルの使用を検討する必要があります。

I/O モジュールからファブリック インターコネクトへのアップリンク ポートの数

使用するアップリンク ポートの数とケーブルの本数を増やすことにより、I/O モジュールとファブリックインターコネクトの間の帯域幅を増やすことができます。 Cisco UCS では、I/O モジュールと Cisco UCS 6100 シリーズ ファブリック インターコネクトを接続するために、ケーブルを 1 本、2 本、または 4 本使用できます。 2208 I/O モジュールと 6248 ファブリック インターコネクトを接続する場合、最大 8 本のケーブルを使用できます。 ケーブルの本数により、アクティブ アップリンク ポートの数、およびオーバーサブスクリプションの比率が決定されます。

サーバからファブリック インターコネクトへのアクティブ リンクの数

各サーバで使用可能なオーバーサブスクライブされていない帯域幅の量は、使用する I/O モジュール数と、それらの I/O モジュールをファブリック インターコネクトに接続するために使用するケーブル数によって異なります。 別の I/O モジュールを設置すると、サーバに追加の帯域幅と冗長性が提供されます。 設計のこのレベルの柔軟性により、80 Gbps（それぞれ 4 つのリンクを持つ 2 つの I/O モジュール）から 10 Gbps（1 つのリンクを持つ 1 つの I/O）までの任意の帯域幅をシャーシに提供できます。

シャーシに 80 Gbps を提供する場合、Cisco UCS ドメインの各ハーフ幅サーバが、オーバーサブスクライブされていない設定で最大 10 Gbps に達し、2:1 オーバーサブスクリプションで最大 20 Gbps 使用できます。

オーバーサブスクリプションの概算に関するガイドライン

ファブリックインターコネクトポートに対する最適なオーバーサブスクリプション率を概算する場合は、次のガイドラインを考慮してください。

コスト/パフォーマンス スライダ

コストとパフォーマンスの優先順位付けは、データセンターによってそれぞれ異なり、オーバーサブスクリプションの設定に直接影響します。 オーバーサブスクリプションにおけるハードウェアの使用方法を計画する場合は、このスライダでデータセンターが位置する場所を知る必要があります。 たとえば、データセンターでコストよりもパフォーマンスを重視する場合は、オーバーサブスクリプションを最小限に抑えることができます。 しかし、ほとんどのデータセンターでは、コストは大きい影響を与える要因であるため、オーバーサブスクリプションは慎重に計画する必要があります。

Bandwidth Usage

各サーバで実際に使用されると予想される帯域幅の概算値は、ファブリック インターコネクトポートへの各サーバの割り当て、およびその結果からポートのオーバーサブスクリプション率を決定するときに重要です。 オーバーサブスクリプションでは、サーバにより消費されるトラフィックの平均値（単位は GB）、設定された帯域幅に対する使用された帯域幅の比率、および帯域幅の使用が上昇する時間を考慮する必要があります。

Network Type

ネットワークタイプは、アップリンク ポート上のトラフィックだけに関係します。これは、Cisco UCS 以外のところには、FCoE が存在しないからです。 その他のデータセンター ネットワーク

は、LAN と SAN トラフィックを区別するだけです。 したがって、ファブリック インターコネクト ポートのオーバーサブスクリプションの概算を行う場合、ネットワーク タイプを考慮する必要はありません。

ピン接続

Cisco UCS でのピン接続は、アップリンク ポートだけに関係します。 イーサネット トラフィック、または FCoE トラフィックをあるサーバから、特定のアップリンク イーサネット ポート、またはアップリンク FC ポートにピン接続することができます。

物理サーバと仮想サーバの両方の NIC および HBA をアップリンク ポートにピン接続する場合、ファブリック インターコネクトからユニファイド ファブリックを制御できるようにします。 この制御により、アップリンク ポートの帯域幅の利用がさらに最適化されます。

Cisco UCS は、ピン グループを使用して、どの NIC、vNIC、HBA、vHBA をアップリンク ポートにピン接続するかを管理します。 サーバにピン接続を設定するには、ピン グループを直接的に割り当てるか、ピン グループを vNIC ポリシーに入れてから、サーバに割り当てられたサービス プロファイルにその vNIC ポリシーを追加します。 サーバ上の vNIC または vHBA からのトラフィックはすべて、I/O モジュールを通って、同じアップリンク ポートに進みます。

サーバ トラフィックのサーバ ポートへのピン接続

サーバ トラフィックはすべて、I/O モジュールを経由して、ファブリック インターコネクトのサーバ ポートへ進みます。 このトラフィックがどのようにピン接続されるかは、シャーシに設定されるリンクの数によって決まります。

ピン接続により、どのサーバ トラフィックが、ファブリック インターコネクトのどのサーバ ポートに進むかが決まります。 このピン接続は固定されています。 変更できません。 したがって、シャーシに対する帯域幅の適切な割り当てを決定する場合、サーバの位置を考慮する必要があります。

（注） サーバをスロットに割り当てる前に、ポートからリンクへの割り当てを見直す必要があります。 ケーブルで接続するポートは I/O モジュールのポート 1 およびポート 2 である必要はありません。 ファブリック インターコネクトと I/O モジュールの間のリンク数を変更した場合、トラフィックを再ルーティングするには、シャーシを再認識する必要があります。

ポート番号はすべて、この I/O モジュールのファブリック インターコネクト側ポートを参照します。

1 つの I/O モジュールを持つシャーシ（ファブリック ポート チャネルの場合は設定されません）

（注） サーバのアダプタがアダプタのポート チャネルをサポートし、それらのチャネルに応じて設定されている場合、次の表に示すように、ポートチャネルは同じリンクにピン接続されます。シャーシの I/O モジュールがファブック ポート チャネルをサポートし、それらのチャネルに応じて設定されている場合、サーバ スロットは個々のリンクでなくファブリック ポート チャネルにピン接続されます。

シャーシのリンク	リンク 1/ファブリック ポート チャネル	リンク 2	リンク 3	リンク 4	リンク 5	リンク 6	リンク 7	リンク 8
1 リンク	すべてのサーバスロット	なし	なし	なし	なし	なし	なし	なし
2 リンク	サーバスロット 1、3、5、および 7	サーバスロット 2、4、6、および 8	なし	なし	なし	なし	なし	なし
4 リンク	サーバスロット 1 および 5	サーバスロット 2 および 6	サーバスロット 3 および 7	サーバスロット 4 および 8	なし	なし	なし	なし
8 リンク	サーバスロット 1	サーバスロット 2	サーバスロット 3	サーバスロット 4	サーバスロット 5	サーバスロット 6	サーバスロット 7	サーバスロット 8
ファブリック ポート チャネル	すべてのサーバスロット	N/A	N/A	N/A	N/A	N/A	N/A	N/A

I/O モジュールを 2 つ持つシャーシ

シャーシに I/O モジュールが 2 つある場合、片方の I/O モジュールからのトラフィックは、ファブリック インターコネクトの 1 つに進み、もう 1 つの I/O モジュールからのトラフィックは、2 つめのファブリック インターコネクトに進みます。 1 つのファブリック インターコネクトに 2 つの I/O モジュールを接続できません。

vNIC で設定されたファブリック インターコネクト	サーバ トラフィック パス
A	サーバ トラフィックはファブリック インターコネクト A に向かいます。 A に不具合が生じた場合、サーバ トラフィックは B にフェールオーバーしません。
B	すべてのサーバ トラフィックはファブリック インターコネクト B に向かいます。 B に不具合が生じた場合、サーバ トラフィックは A にフェールオーバーしません。
A-B	すべてのサーバ トラフィックはファブリック インターコネクト A に向かいます。 A に不具合が生じた場合、サーバ トラフィックは B にフェールオーバーします。
B-A	すべてのサーバ トラフィックはファブリック インターコネクト B に向かいます。 B に不具合が生じた場合、サーバ トラフィックは A にフェールオーバーします。

ピン接続に関するガイドライン

ピング ループおよびアップリンク ポートに対するピン接続における最適な設定を判断する場合、サーバについて予想される帯域幅使用状況を考慮します。 システムに含まれるサーバの一部が大量の帯域幅を使用することがわかっている場合は、必ず、これらのサーバを別のアップリンク ポートにピン接続してください。

Quality of Service

Cisco UCS は、Quality Of Service を実装するために、次の方法を提供しています。

- システム全体にわたって、特定のタイプのトラフィックに対するグローバル設定を指定するためのシステム クラス
- 個々の vNIC にシステム クラスを割り当てる QoS ポリシー
- アップリンク イーサネット ポートによるポーズ フレームの扱い方法を決定するフロー制御ポリシー

システム クラス

Cisco UCS では、Cisco UCS ドメイン内のすべてのトラフィックを処理するために、Data Center Ethernet（DCE）が使用されます。 イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が 8 つの仮想レーンに分割されています。 内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。 それ以外の 6 つの仮想レーンの Quality of Service を設定

できます。 Cisco UCS ドメイン全体にわたり、これら 6 つの仮想レーンで DCE 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

各システムクラスでは、特定のトラフィックタイプのために、帯域幅の特定セグメントが予約されています。 これにより、オーバーサブスクライブされたシステムでも、ある程度のトラフィック管理ができるようになります。 たとえば、ファイバ チャネル プライオリティ システム クラスを設定して、FCoE トラフィックに割り当てられる DCE 帯域幅の割合を決定することができます。

次の表は、設定可能なシステム クラスをまとめたものです。

表 *2*：システム クラス

システム クラス	説明
Platinum Gold Silver Bronze	サービス プロファイルの QoS ポリシーにインクルードできる設定可能なシステム クラスのセット。 各システム クラスはトラフィック レーンを 1 つ管理します。 これらのシステムクラスのプロパティはすべて、カスタム設定やポリシーを割り当てるために使用できます。
Best Effort	ベーシック イーサネット トラフィックのために予約されたレーンに対する Quality Of Service を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。 たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップ ポリシーがあります。 このシステム クラスをディセーブルにはできません。
ファイバ チャネル	Fibre Channel over Ethernet トラフィックのために予約されたレーンに対する Quality Of Service を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。 たとえば、このクラスには、データ パケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。 このシステム クラスをディセーブルにはできません。

Quality Of Service ポリシー

Quality Of Service（QoS）ポリシーは、vNIC または vHBA に向けた発信トラフィックにシステム クラスを割り当てます。 このシステム クラスにより、このトラフィックに対する Quality Of Service が決定されます。 一部のアダプタでは、発信トラフィックでバーストやレートなど追加の制御を指定することもできます。

vNIC ポリシー、または vHBA ポリシーに QoS ポリシーをインクルードし、その後、このポリシーをサービス プロファイルにインクルードして、vNIC または vHBA を設定する必要があります。

フロー制御ポリシー

フロー制御ポリシーは、ポートの受信バッファがいっぱいになったときに、Cisco UCS ドメインのアップリンク イーサネット ポートが IEEE 802.3x ポーズ フレームを送信および受信するかどうかを決定します。 これらのポーズフレームは、バッファがクリアされるまでの数ミリ秒間、送信側ポートからのデータの送信を停止するように要求します。

LAN ポートとアップリンク イーサネット ポートの間でフロー制御が行われるようにするには、両方のポートで、対応する受信および送信フロー制御パラメータをイネーブルにする必要があります。 Cisco UCS では、これらのパラメータはフロー制御ポリシーによって設定されます。

送信機能をイネーブルにした場合、受信パケット レートが高くなりすぎたときに、アップリンク イーサネット ポートはネットワーク ポートにポーズ要求を送信します。 ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。 受信機能をイネーブルにした場合、アップリンク イーサネット ポートは、ネットワーク ポートからのポーズ要求すべてに従います。 ネットワーク ポートがポーズ要求をキャンセルするまで、すべてのトラフィックはこのアップリンク ポートで停止します。

ポートにフロー制御ポリシーを割り当てているため、このポリシーを変更すると同時に、ポーズ フレームやいっぱいになっている受信バッファに対するポートの反応も変わります。

オプトイン機能

各 Cisco UCS ドメインには、すべての機能に対して許可されます。 システムの設定方法に応じて、既存の環境への統合を簡単にするために、一部の機能をオプトインするか、これらをオプトアウトするかを決定することができます。 プロセスの変化が起こった場合、システム設定を変更して、オプトイン機能の 1 つまたは両方を加えることができます。

オプトイン機能は次のとおりです。

- サーバ、アダプタなどの各コンポーネントがステートレスであるプールおよびポリシーを持つモバイル サービス プロファイルを利用するステートレス コンピューティング
- 組織およびロールベースのアクセス コントロールを使用して、システムを複数の小さな論理セグメントに分割するマルチテナント機能

ステートレス コンピューティング

ステートレス コンピューティングにより、サービスプロファイルを使用して、あるサーバの固有情報を同じ Cisco UCS ドメイン内の別のサーバに適用できます。 サーバの固有情報には、サーバを認識し、Cisco UCS ドメイン内で一意にするための要素が含まれます。 これらの要素のいずれかを変更すると、サーバはブート ステータスのアクセス、使用、実現ができなくなります。

サーバの固有情報を構成する要素は次のとおりです。

- ファームウェア バージョン
- UUID（サーバの識別に使用される）

- MAC アドレス（LAN 接続に使用される）
- ワールド ワイド名（SAN 接続に使用される）
- ブート設定

ステートレス コンピューティングは、高度に柔軟なサーバを使ったダイナミックなサーバ環境を作成します。 Cisco UCS ドメインの各物理サーバは、それにサービス プロファイルを関連付けるまで匿名のままで、サーバの ID はサービス プロファイルに設定されます。 このサーバでのビジネス サービスが必要なくなったら、このサーバをシャットダウンし、サービスプロファイルのアソシエーションを解除してから、同じ物理サーバについて異なる ID を作成するために別のサービス プロファイルとのアソシエーションを形成します。 この「新しい」サーバは、別のビジネス サービスをホストできます。

ステートレス状態の柔軟性をフルに活用するためには、サーバのオプション ローカルディスクはスワップ用スペースまたは一時スペースだけに使用し、オペレーティング システムやアプリケーション データの保存には使用しないでください。

Cisco UCS ドメインのすべての物理サーバに対して、ステートレス コンピューティングを完全に実装するように選択することも、ステートレス サーバを使用しないことを選択することもできます。また、これら 2 種類を混在させることも可能です。

ステーレス コンピューティングをオプトインする場合

Cisco UCS ドメイン内の各物理サーバは、サービス プロファイルによって定義されます。 どのようなサーバでも、あるアプリケーションのセットをホストするために使用しているときに、データセンターの必要に応じて、別のアプリケーションやビジネス サービスのセットに割り当てなおすことができます。

Cisco UCS ドメインで定義されているポリシーやリソースのプールをポイントするサービス プロファイルを作成します。 サーバ プール、World Wide Name（WWN; ワールド ワイド名）プール、および MAC プールにより、未割り当てのリソースはすべて、必要に応じて使用できることが保証されます。 たとえば、物理サーバに障害が発生した場合、別のサーバにすぐにサービス プロファイルを割り当てることができます。 サービス プロファイルは、WWN や MAC アドレスを含め、オリジナルのサーバと同じ ID を新しいサーバに与えるため、データセンター インフラストラクチャの残りの部分では、この新しいサーバとオリジナルのサーバは同じものと認識されます。 LAN や SAN で設定を変更する必要はありません。

ステートレス コンピューティングからオプトアウトする場合

Cisco UCS ドメイン内の各サーバは、従来のラックマウント型サーバとして扱われます。

ハードウェアに書き込まれた ID 情報を継承するサービス プロファイルを作成し、これらのプロファイルを使用して、サーバに対する LAN または SAN 接続を設定します。 ただし、サーバ ハードウェアに障害が発生した場合、新しいサーバにサービス プロファイルを割り当てることはできません。

マルチテナント機能

マルチテナント機能を使用すると、Cisco UCS ドメインの大規模な物理インフラストラクチャを、組織と呼ばれる論理エンティティに分割することができます。 その結果、各組織に専用の物理インフラストラクチャを設けなくても各組織を論理的に分離できます。

マルチテナント環境では、関連する組織を通じて、各テナントに一意のリソースを割り当てられます。 これらのリソースには、各種のポリシー、プール、および Quality of Service 定義などがあります。 また、すべてのユーザがすべての組織にアクセスできるようにする必要がない場合は、ロケールを実装して、組織ごとにユーザ権限やロールを割り当てたり、制限したりすることもできます。

マルチテナント環境をセットアップする場合、すべての組織は階層的になります。 最上位の組織は常にルートです。 ルートに作成したポリシーおよびプールはシステム全体にわたるもので、このシステムに含まれるすべての組織で使用できます。 しかし、他の組織で作成されたポリシーやプールが使用できるのは、同じ階層でそれより上にある組織だけです。 たとえば、あるシステムに Finance と HR という組織があり、これらは同じ階層に存在しないとします。この場合、Finance は HR 組織にあるポリシーは一切使用できず、また、HR は Finance 組織にあるポリシーには一切アクセスできません。 しかし、Finance と HR は両方とも、ルート組織にあるポリシーやプールを使用できます。

マルチテナント環境に組織を作成する場合、各組織、または同じ階層のサブ組織に次のうち 1 つ以上をセットアップすることもできます。

- リソース プール
- ポリシー
- サービス プロファイル
- サービス プロファイル テンプレート

マルチテナント機能をオプトインする場合

各 Cisco UCS ドメインは複数の異なる組織に分割されます。 マルチテナント機能の実装で作成される組織のタイプは、企業のビジネスニーズによって異なります。 たとえば、次の単位を表す組織があげられます。

- マーケティング、財務、エンジニアリング、人事など、企業内のエンタープライズ グループまたは部門
- サービス プロバイダーに対するさまざまなカスタマー、またはネーム サービス ドメイン

管理が認可されている組織だけにユーザがアクセスできるように、ロケールを作成することができます。

マルチテナント機能からオプトアウトする場合

Cisco UCS ドメインは、ルート組織にすべてのデータが入った単一の論理エンティティのままです。 すべてのポリシーおよびリソース プールは Cisco UCS ドメイン内の任意のサーバに割り当てることができます。

Cisco UCS の仮想化

仮想化の概要

仮想化により、分離して実行する同じ物理マシン上で隣り合わせの複数の仮想マシン（VM）を作成することができます。

各仮想マシンは、仮想ハードウェア（メモリ、CPU、NIC）の独自のセットを持ち、その上でオペレーティング システムと十分に設定されたアプリケーションがロードされます。 オペレーティング システムは、実際の物理ハードウェア コンポーネントに関係なく、一貫性があり正常なハードウェア一式を認識します。

仮想マシンでは、物理サーバ間でのプロビジョニングおよび移動を迅速に行うために、ハードウェアとソフトウェアの両方が単一のファイルにカプセル化されます。 仮想マシンは 1 つの物理サーバから別のサーバへ数秒で移動することができ、メンテナンスのためのダウンタイムを必要とせず、途切れることのない作業負荷を集約します。

仮想ハードウェアは、多数のサーバ（それぞれのサーバは独立した仮想マシン内で実行する）を単一の物理サーバ上で実行できるようにします。 仮想化の利点は、コンピューティング リソースをより適切に使用でき、サーバ密度を高め、サーバの移行をスムーズに行えることです。

Cisco Virtual Machine Fabric Extender の概要

仮想サーバの実装は、1 つの物理サーバのゲストとして実行される 1 つまたは複数の VM で構成されます。 ゲスト VM は、ハイパーバイザまたは仮想コンピュータ マネージャ（VMM）と呼ばれるソフトウェア レイヤによってホストおよび管理されます。 通常、ハイパーバイザは各 VM への仮想ネットワーク インターフェイスを示し、VM から他のローカル VM、または別のインターフェイスを介した外部ネットワークへのトラフィックのレイヤ 2 スイッチングを実行します。

Cisco Virtual Interface Card（VIC）アダプタと連動して、Cisco Virtual Machine Fabric Extender（VM-FEX）はファブリック インターコネクトの外部ハードウェアベース スイッチング用のハイパーバイザによって VM トラフィックのソフトウェアベースのスイッチングをバイパスします。 この方法は、サーバの CPU 負荷を軽減し、高速スイッチングを行い、ローカルおよびリモートのトラフィックに豊富なネットワーク管理機能セットを適用します。

VM-FEX は、各 VM インターフェイスに仮想 Peripheral Component Interconnect Express（PCIe）デバイスとスイッチ上の仮想ポートを提供することで、IEEE 802.1Qbh ポート エクステンダ アーキテクチャを VM に拡張します。 このソリューションにより、VM インターフェイスで正確なレート制限を行い、Quality of Service（QoS）が確保されます。

ネットワーク インターフェイス カードと統合ネットワーク アダプタを使用した仮想化

ネットワーク インターフェイス カード（NIC）と統合ネットワーク アダプタによって、標準的な VMware のサーバにインストールされた ESX との統合による仮想環境と、VC から実行されるすべての仮想マシンの管理がサポートされます。

仮想マシンのポータビリティ

サービス プロファイルを実装すると、1 つのサーバから別のサーバに、サーバの識別情報を簡単に移動できるようになります。 新規サーバをイメージ化すると、ESX はそのサーバを元のサーバのように扱います。

同一サーバ上の仮想マシン間の通信

これらのアダプタは、同一サーバ上の仮想マシン間における標準の通信手段を実装します。 ESX ホストが複数の仮想マシンを含む場合、すべての通信はサーバ上の仮想スイッチを通過させる必要があります。

システムでネイティブな VMware ドライバを使用する場合、仮想スイッチはネットワーク管理者のドメインには参加せず、どのネットワーク ポリシーの制約も受けません。 結果として、たとえば、ネットワークの QoS ポリシーは、仮想スイッチを通って VM1 から VM2 に流れるどのデータパケットにも適用されません。

Nexus 1000 などの別の仮想スイッチがシステムに含まれている場合、その仮想スイッチは、ネットワーク管理者がそのスイッチ上で設定したネットワーク ポリシーに従います。

仮想インターフェイス カード アダプタでの仮想化

Cisco VIC アダプタ（Cisco UCS M81KR 仮想インターフェイス カードなど）は、単一 OS の導入と VM ベースの導入の両方に対応するように設計された統合型ネットワーク アダプタ（CNA）です。 VIC アダプタは静的または動的な仮想化インターフェイスをサポートし、最大 128 個の仮想ネットワーク インターフェイス カード（vNIC）を含みます。

VIC アダプタは、VM-FEX をサポートし、仮想マシン インターフェイスを対象に送受信されるトラフィックのハードウェア ベース スイッチングを提供します。

第 3 章

Cisco UCS Manager の概要

この章の内容は、次のとおりです。

- Cisco UCS Manager について，31 ページ
- Cisco UCS Manager で実行できるタスク，33 ページ
- Cisco UCS Manager で実行できないタスク，34 ページ
- ハイ アベイラビリティ環境での Cisco UCS Manager，35 ページ

Cisco UCS Manager について

Cisco UCS Manager は UCS Manager のすべてのコンポーネントに対する管理システムです。 Cisco UCS Manager はファブリック インターコネクト内で動作します。 この管理サービスで使用できるインターフェイスのいずれかを使用して、ファブリック インターコネクトに接続されたシャーシすべてのネットワークおよびサーバ リソースにアクセスしたり、これらを設定、管理、およびモニタしたりすることができます。

複数の管理インターフェイス

Cisco UCS Manager には Cisco UCS ドメインを管理するために使用できる次のインターフェイスが含まれます。

- Cisco UCS Manager GUI
- Cisco UCS Manager CLI
- XML API
- KVM
- IPMI

ほとんどすべてのタスクは、これらのインターフェイスのいずれでも実行できます。また、あるインターフェイスで実行されたタスクの結果は、他のタスクにも自動的に表示されます。

ただし、次の操作はできません。

- Cisco UCS Manager GUI を使用して Cisco UCS Manager CLI を呼び出す。
- Cisco UCS Manager GUI の Cisco UCS Manager CLI によって呼び出されたコマンドの結果を表示する。
- Cisco UCS Manager GUI から CLI の出力を生成する。

集中管理

Cisco UCS Manager Manager は、複数の管理ポイントを使用するのではなく、リソースおよびデバイスの管理を一元化します。 この集中型管理には、Cisco UCS ドメインでの次のデバイスの管理が含まれます。

- ファブリック インターコネクト。
- 仮想サーバ用ソフトウェア スイッチ。
- シャーシおよびサーバにおける電源および環境管理。
- サーバ ネットワーク インターフェイス（イーサネット NIC および統合ネットワーク アダプタ）の設定とファームウェア更新。
- サーバに対するファームウェアおよび BIOS 設定。

仮想サーバおよび物理サーバのサポート

Cisco UCS Manager は、サーバの ID、I/O 設定、MAC アドレスおよび World Wide 名、ファームウェアのバージョン、ネットワークプロファイルなどのサーバ状態情報をサービスプロファイルに要約します。 サービス プロファイルをシステム内のサーバ リソースに適用して、VIC アダプタの提供する仮想デバイスに接続されている物理サーバ、仮想サーバ、および仮想マシンに同様の柔軟性とサポートを提供することができます。

ロール ベース管理とマルチテナント機能のサポート

Cisco UCS Manager では、柔軟に定義されたロールがサポートされるため、データセンターは、ディスクリートサーバ、ストレージ、およびネットワークを管理する際に同じベストプラクティスを使用して、Cisco UCS ドメインを操作することができます。 データセンターでのユーザの責任を反映した権限を持つユーザ ロールを作成することができます。 たとえば、次のロールを作成できます。

- サーバ関連の設定を制御するサーバ アドミニストレータ ロール。
- SAN に関連するタスクを制御するストレージ アドミニストレータ ロール。
- LAN に関連するタスクを制御するネットワーク アドミニストレータ ロール

Cisco UCS はマルチテナント機能に対応し、API を使用するシステム管理ソフトウェアが Cisco UCS リソースへの制御されたアクセスを行うようにするプリミティブを公開します。 マルチテナント環境では、Cisco UCS Manager により、ユーザの範囲を特定の組織に制限できるユーザ ロールのロケールを作成することができます。

Cisco UCS Manager で実行できるタスク

Cisco UCS Manager を使用して Cisco UCS ドメイン内のすべての物理デバイスおよび仮想デバイスに管理タスクを実行できます。

Cisco UCS ハードウェア管理

次に示す Cisco UCS ドメイン内のすべてのハードウェアの管理に Cisco UCS Manager を使用できます。

- シャーシ
- サーバ
- ファブリック インターコネクト
- ファン
- ポート
- インターフェイス カード
- I/O モジュール

Cisco UCS リソース管理

次に示す Cisco UCS ドメイン内のすべてのリソースの作成および管理に Cisco UCS Manager を使用できます。

- サーバ
- WWN アドレス
- MAC アドレス
- UUID
- 帯域幅

サーバ管理

サーバ管理者は、次に示す Cisco UCS ドメイン内のサーバ管理タスクの実行に Cisco UCS Manager を使用できます。

- サーバ プール、および資格ポリシーなどこれらのプールに関係するポリシーの作成
- ディスカバリ ポリシー、スクラブ ポリシー、IPMI ポリシーなど、サーバで使用されるポリシーの作成
- サービス プロファイル、および必要な場合に、サービス プロファイル テンプレートの作成
- サーバへのサービス プロファイルの適用
- 障害、アラーム、および機器のステータスのモニタ

ネットワーク管理

ネットワーク管理者は、次に示す Cisco UCS ドメインの LAN 設定を作成するために必要なタスクの実行に Cisco UCS Manager を使用できます。

- アップリンク ポート、ポート チャネル、および LAN PIN グループの設定
- VLAN の作成
- Quality Of Service クラスおよび定義の設定
- MAC アドレス プール、イーサネット アダプタ プロファイルなど、ネットワーク設定に関連したプールおよびポリシーの作成

ストレージ管理

ストレージ管理者は、次に示す Cisco UCS ドメインの SAN 設定を作成するために必要なタスクの実行に Cisco UCS Manager を使用できます。

- ポート、ポート チャネル、および SAN PIN グループの設定
- VSAN の作成
- Quality Of Service クラスおよび定義の設定
- WWN アドレス プール、ファイバ チャネル アダプタ プロファイルなど、ネットワーク設定に関連したプールおよびポリシーの作成

Cisco UCS Manager で実行できないタスク

Cisco UCS Manager を使用して、Cisco UCS ドメイン内のデバイス管理に特に関連していないシステム管理タスクを実行することはできません。

システムを超えた管理はできない

Cisco UCS Manager がある Cisco UCS ドメイン外にあるシステムやデバイスの管理には Cisco UCS Manager を使用できません。 たとえば、Cisco UCS 以外の x86 システム、SPARC システム、PowerPC システムなどの異機種環境は管理できません。

オペレーティング システムやアプリケーションのプロビジョニングや管理はできない

Cisco UCS Manager はサーバのプロビジョニングを行うため、サーバのオペレーティング システムの下に存在します。 したがって、サーバでオペレーティング システムやアプリケーションのプロビジョニングや管理を行うためにこれを使用することはできません。 たとえば、次の操作を実行することはできません。

- Windows や Linux などの OS の展開
- OS やアプリケーションなどのソフトウェアに対するパッチの展開

- アンチウイルス ソフトウェア、モニタリング エージェント、バックアップ クライアントなどのベース ソフトウェア コンポーネントのインストール
- データベース、アプリケーション サーバ ソフトウェア、Web サーバなどのソフトウェア アプリケーションのインストール
- Oracle データベースの再起動、プリンタ キューの再起動、Cisco UCS 以外のユーザ アカウントの処理などのオペレータ処理の実行
- SAN や NAS ストレージ上の外部ストレージの設定または管理

ハイ アベイラビリティ環境での Cisco UCS Manager

2 つのファブリック インターコネクトを持つハイ アベイラビリティ環境では、各ファブリック インターコネクトで、別々の Cisco UCS Manager インスタンスを実行できます。 プライマリ ファブリック インターコネクトの Cisco UCS Manager はプライマリ管理インスタンスとして動作し、もう 1 つのファブリック インターコネクトの Cisco UCS Manager は従属管理インスタンスとなります。

Cisco UCS Manager の 2 つのインスタンスは、これらのファブリック インターコネクト上の L1 および L2 イーサネット ポートの間にあるプライベート ネットワーク上で通信します。 設定およびステータスに関する情報は、このプライベート ネットワーク経由でやりとりされ、すべての管理情報が確実に複製されます。 この継続的な通信により、プライマリ ファブリック インターコネクトに不具合が起きた場合でも、Cisco UCS に対する管理情報がそのまま持続されることが保証されます。 さらに、プライマリ Cisco UCS Manager 上で実行される「浮動」管理 IP アドレスにより、フェールオーバーが発生したときに、従属ファブリック インターコネクトへのスムーズな移行が確実に行われるようになります。

第 4 章

Cisco UCS Manager GUI の概要

この章の内容は、次のとおりです。

- Cisco UCS Manager GUI の概要，37 ページ
- HTTPS による Cisco UCS Manager GUI へのログイン，45 ページ
- HTTP による Cisco UCS Manager GUI へのログイン，46 ページ
- Cisco UCS Manager GUI からのログアウト，47 ページ
- Web セッション制限，47 ページ
- プリログイン バナー，48 ページ
- Cisco UCS Manager GUI のプロパティ，50 ページ
- フィールドの値の許容範囲の確認，53 ページ
- ポリシーの使用場所の確認，54 ページ
- プールの使用場所の確認，54 ページ
- XML のコピー，55 ページ

Cisco UCS Manager GUI の概要

Cisco UCS Manager GUI は Cisco UCS Manager の GUI インターフェイスを提供する Java アプリケーションです。『Cisco UCS ソフトウェア リリース ノート』の「システム要件」の項に記載されている要件を満たす任意のコンピュータから Cisco UCS Manager GUI を開始し、アクセスできます。

ユーザが Cisco UCS Manager GUI を起動するたびに、Cisco UCS Manager は Java Web Start テクノロジーを使用してコンピュータの現在のアプリケーションバージョンをキャッシュします。その結果、ログインするたびにアプリケーションをダウンロードする必要がなくなります。アプリケーションのダウンロードが必要なのは、Cisco UCS Manager ソフトウェアがシステムでアップデートされた後で、コンピュータから初めてログインする場合だけです。

ヒント　タイトル バーには、接続先の Cisco UCS ドメインの名前が表示されます。

[Fault Summary] 領域

[Fault Summary] 領域は、Cisco UCS Manager GUI の左上に表示されます。 この領域には、Cisco UCS ドメインで発生したすべての障害の要約が表示されます。

それぞれの種類の障害は異なるアイコンで表されます。 各アイコンの下にある数字は、システムで発生したその種類の障害の数を示しています。 アイコンをクリックすると、Cisco UCS Manager GUI によって [Work] 領域の [Faults] タブが開かれ、その種類のすべての障害の詳細が表示されます。

次の表に、[Fault Summary] 領域の各アイコンが表す障害の種類について説明します。

障害の種類	説明
緊急アラーム	1 つ以上のコンポーネントに緊急の問題が存在します。 これらの問題を調査し、すぐに修正する必要があります。
メジャー アラーム	1 つ以上のコンポーネントに重大な問題が存在します。 これらの問題を調査し、すぐに修正する必要があります。
マイナー アラーム	システムのパフォーマンスに悪影響を及ぼす可能性のある問題が 1 つ以上のコンポーネントに存在します。 これらの問題を調査し、重大な問題や緊急の問題に発展する前にできるだけ早く修正する必要があります。
警告アラーム	問題が解消されなければシステムのパフォーマンスに悪影響を及ぼす可能性のある潜在的な問題が 1 つ以上のコンポーネントに存在します。 これらの問題を調査し、問題が悪化する前にできるだけ早く修正する必要があります。
[Suppression Status] フィールド	コンポーネントのエラーの抑制状態タスク。 [Actions] 領域で [Suppression Task Properties] をクリックすると、すべてのエラー抑制タスクが表示されます。 （注）　このフィールドは、コンポーネントでエラーの抑制がサポートされている場合にのみ表示されます。

ヒント　特定のオブジェクトの障害だけを確認する場合は、そのオブジェクトに移動して、そのオブジェクトの [Faults] タブを確認します。

[Navigation] ペイン

[Navigation] ペインは、Cisco UCS Manager GUI の左側の [Fault Summary] 領域の下に表示されます。 このペインでは、Cisco UCS ドメインでのすべての機器とその他のコンポーネントへの集中化ナビゲーションが提供されています。 [Navigation] ペインでコンポーネントを選択すると、そのオブジェクトが [Work] 領域に表示されます。

[Navigation] ペインには 5 つのタブが存在します。 各タブの構成要素は次のとおりです。

- ナビゲーション ツリーをフィルタ処理し、すべてのノードまたは 1 つのノードだけを表示するために使用できる [Filter] コンボ ボックス。
- 該当するタブのすべてのコンポーネントにアクセスするために使用できる展開可能なナビゲーション ツリー。 ノードまたはフォルダにサブコンポーネントがあることを示すフォルダの隣のアイコン。

[Equipment] タブ

このタブには、Cisco UCS ドメイン ドメインの機器の基本的なインベントリが含まれます。 システム管理者またはサーバ管理者は、このタブを使用してシャーシ、ファブリック インターコネクト、サーバ、および他のハードウェアにアクセスしてこれらを管理できます。 デバイス名の周りに表示された赤色、オレンジ色、または黄色の長方形は、デバイスで障害が発生したことを示します。

このタブの主要なノードは次のとおりです。

- [Equipment]：アクティブおよび解放されたハードウェア、ファームウェア管理、機器関連ポリシー、電源グループ、および集約された障害のリストを含む、Cisco UCS ドメイン全体の概要。
- [Chassis]：Cisco UCS ドメイン内の各シャーシのファン、I/O モジュール、電源装置（PSU）、および Cisco UCS B シリーズ ブレード サーバ。
- [Rack-Mounts]：Cisco UCS ドメインと統合されている FEXes および Cisco UCS C シリーズ ラックマウント サーバ。
- [Fabric Interconnects]：Cisco UCS ドメインのファブリック インターコネクトに関連付けられた固定および拡張モジュール、ファン、および PSU。

[Servers] タブ

このタブには、サービス プロファイル、ポリシー、プールなどのサーバ関連のコンポーネントが含まれます。 通常、サーバ管理者はこのタブでコンポーネントにアクセスし、コンポーネントを管理します。

このタブの [Servers] ノード以下の主要なノードは次のとおりです。

- [Servers]：定義された組織とサービス プロファイルの間のサービス プロファイルおよびの関係。

- [Service Profiles]：組織によって分割された、システムに定義されているサービス プロファイル。
- [Service Profile Templates]：組織によって分割された、システムに定義されているサービス プロファイル テンプレート。
- [Policies]：アダプタ、BIOS、ファームウェア、IPMI アクセス、ローカル ディスク設定、保守、電源、ディスク スクラブ、Serial over LAN、サーバ プール、iSCSI 認証、vNIC/vHBA 配置、および障害しきい値に関するサーバ関連ポリシー。
- [Pools]：サーバ プールおよび UUID 接尾辞プール。
- [Schedules]：メンテナンスおよびエラーの抑制スケジュール。

[LAN] タブ

このタブには、LAN ピン グループ、Quality of Service クラス、VLAN、ポリシー、プール、内部ドメインなどの、LAN 設定に関連するコンポーネントが含まれます。 通常、ネットワーク管理者はこのタブでコンポーネントにアクセスし、コンポーネントを管理します。

このタブの [LAN] ノード以下の主要なノードは次のとおりです。

- [LAN Cloud]：Quality of Service の設定、ポート チャネル、ピン グループ、VLAN、VLAN の最適化セット、しきい値ポリシー。
- [Appliances]：インターフェイス、ポート チャネル、および VLAN。
- [Internal LAN]：内部ファブリックに関連付けられたポートおよびしきい値ポリシー。
- [Policies]：フロー制御、アダプタ、vNIC、vNIC テンプレート、QoS、および障害しきい値を制御するポリシー。
- [Pools]：システムで定義されている IP プールおよび MAC プール。
- [Traffic Monitoring Sessions]：システムで定義されているポート トラフィック モニタリング セッション。

[SAN] タブ

このタブには、ピン グループ、VSAN、ポリシー、プールなどの SAN に関連するコンポーネントが含まれます。 通常、ストレージ管理者はこのタブでコンポーネントにアクセスし、コンポーネントを管理します。

このタブの主要なノードは次のとおりです。

- [SAN]：SAN のアップリンク、ファイバ チャネル アドレス割り当て、SAN 関連プールおよび VSAN。
- [SAN Cloud]：SAN アップリンク、ファイバ チャネル アドレス割り当て、SAN 関連プール、および VSAN。
- [Storage Cloud]：ストレージ ポートおよび VSAN。

- [Policies]：ファイバ チャネル アダプタ ポリシー、デフォルト vHBA の動作、SAN 接続ポリシー、ストレージ接続ポリシー、vHBA テンプレート、および障害しきい値。
- [Pools]：システムに定義されている iSCSI Qualified Name（IQN）プールおよび World Wide Name プール。
- [Traffic Monitoring Sessions]：システムで定義されているポート トラフィック モニタリング セッション。

[VM] タブ

このタブには、VIC アダプタがあるサーバに対して VM-FEX を設定するのに必要なコンポーネントが含まれます。たとえば、このタブのコンポーネントを使用して Cisco UCS Manager と VMware vCenter 間の接続を設定したり、分散仮想スイッチとポート プロファイルを設定したり、Cisco UCS ドメインのサーバにホストされた仮想マシンを表示したりできます。

このタブの主要なノードは次のとおりです。

- [All]：ポート プロファイル、仮想マシンで、仮想スイッチ、証明書、ライフサイクル ポリシー、VM 関連イベント、および FSM タスク。
- [Clusters]：関連付けられている仮想マシンおよびポート プロファイルを含むクラスタ。
- [Port Profiles]：VMWare ポート プロファイル。
- [VMware]：フォルダ、データセンター、仮想マシン、および仮想スイッチを含む vCenter。

[Admin] タブ

このタブには、ユーザ マネージャや通信サービスなどのシステム全体の設定と障害やイベントなどのトラブルシューティング コンポーネントが含まれます。通常、システム管理者はこのタブでコンポーネントにアクセスし、コンポーネントを管理します。

このタブの主要なノードは次のとおりです。

- [All]：管理インターフェイス、バックアップおよびインポート設定、テクニカル サポート ファイル作成、完全な状態のバックアップ ポリシー、およびすべての設定エクスポート ポリシー。
- [Faults, Events and Audit Log]：システム全体の障害、イベント、監査ログ、syslog エントリ、コア ファイル、テクニカル サポート ファイル、およびグローバル障害ポリシー。
- [User Management]：認証方式、リモート アクセス方式、ローカル ユーザ、ロケール、およびユーザ ロール。
- [Key Management]：SSH キーおよびトラスト ポイント設定。
- [Communication Management]：SSH、Telnet、HTTP、HTTPS、および SNMP の通信サービス設定、Web セッション制限、Call Home 設定、DNS 管理、管理インターフェイス、および Cisco UCS Central 設定。
- [Stats Management]：システムによって障害が発行される条件を制御するしきい値統計設定。

- [Time Zone Management]：タイム ゾーンの同期を確立するための NTP サーバ設定。
- [Capability Catalog]：機能カタログ。つまり、調整可能なパラメータ、文字列、およびルールのセット。
- [Management Extension]：以前はサポートされていなかったサーバと他のハードウェアに対するサポートを Cisco UCS Manager に追加できる管理拡張。
- [License Management]：このシステムにインストールされている機能およびポート ライセンス。

ツールバー

ツールバーは、[Work] ペインの上の Cisco UCS Manager GUI の右側に表示されます。 ツールバーのメニュー ボタンを使用して、次のような一般的な処理を実行できます。

- [Work] ペインで以前表示した項目間を移動する
- Cisco UCS ドメインの要素を作成する
- Cisco UCS Manager GUI のオプションを設定する
- Cisco UCS Manager GUI のオンライン ヘルプにアクセスする

[Work] ペイン

[Work] ペインは、Cisco UCS Manager GUI の右側に表示されます。 このペインには、[Navigation] ペインで選択したコンポーネントに関する詳細が表示されます。

[Work] ペインは、次の要素で構成されます。

- [Navigation] ペインのタブのメイン ノードから選択したエレメントまでのパスが表示されるナビゲーション バー。 このパスの任意のコンポーネントをクリックして、[Work] ペインにこのコンポーネントを表示できます。
- [Navigation] ペインで選択したコンポーネントに関連する情報を示すタブが表示されるコンテンツ領域。 コンテンツ領域に表示されるタブは、選択したコンポーネントによって異なります。 これらのタブを使用して、コンポーネントに関する情報の表示、コンポーネントの作成、コンポーネントのプロパティの変更、および選択したオブジェクトの確認を実行できます。

ステータスバー

ステータスバーは、Cisco UCS Manager GUI の下に沿って表示されます。 ステータスバーは、アプリケーションの状態に関する情報を提供します。

ステータスバーの左側には、Cisco UCS Manager GUI の現在のセッションに関する次の情報が表示されます。

- ログインに使用したプロトコルを示すロック アイコン。アイコンがロックされている場合、HTTPS を使用して接続しました。アイコンのロックが解除されている場合、HTTP を使用して接続しました。
- ログインに使用したユーザ名。
- ログインしたサーバの IP アドレス。

ステータスバーの右側には、システムの時刻が表示されます。

テーブルのカスタマイズ

Cisco UCS Manager GUI では、各タブのテーブルをカスタマイズできます。 表示するコンテンツのタイプを変更し、コンテンツのフィルタリングを実行できます。

[Table Customization] メニュー ボタン

各テーブルの右上にあるこのメニュー ボタンでは、テーブルのビューを制御し、カスタマイズできます。 このボタンのドロップダウン メニューには、次のオプションが含まれます。

メニュー項目	説明
カラム名	メニューには、テーブルの各カラムのエントリが含まれます。 カラム名をクリックしてカラムを表示したり、非表示にしたりします。
Horizontal Scroll	選択されている場合、水平スクロール バーがテーブルに追加されます。 選択されていない場合、いずれかのカラムの幅を拡大したときに右側のすべてのカラムの幅が縮小され、スクロールしません。
Pack All Columns	すべてのカラムをデフォルトの幅に変更します。
Pack Selected Column	選択されたカラムだけをデフォルトの幅に変更します。

テーブル コンテンツのフィルタリング

各テーブルの上にある [Filter] ボタンでは、[Filter] ダイアログボックスで設定した基準に従ってテーブルのコンテンツをフィルタリングできます。 このダイアログボックスには、次のフィルタリング オプションが含まれています。

名前	説明
[Disable] オプション	このカラムの内容に対してフィルタリング基準を使用しません。これがデフォルト設定です。
[Equal] オプション	指定した値と厳密に一致するカラム内容だけを表示します。

名前	説明
[Not Equal] オプション	指定した値と一致しないカラム内容だけを表示します。
[Wildcard] オプション	入力する基準に、次のワイルドカードのいずれかを含められます。 • _（アンダースコア）または?（疑問符）：1つの文字と置き換わります。 • %（パーセント記号）または *（アスタリスク）：任意の連続した文字と置き換わります。
[Less Than] オプション	指定した値より小さいカラム内容だけを表示します。
[Less Than Or Equal] オプション	指定した値以下のカラム内容だけを表示します。
[Greater Than] オプション	指定した値より大きいカラム内容だけを表示します。
[Greater Than Or Equal] オプション	指定した値以上のカラム内容だけを表示します。

LAN アップリンク マネージャ

LAN アップリンク マネージャは、Cisco UCS と LAN 間の接続を設定できる単一インターフェイスを提供します。LANアップリンク マネージャを使用して次のものを作成および設定できます。

- イーサネット スイッチング モード
- アップリンク イーサネット ポート
- ポート チャネル
- LAN ピン グループ
- ネームド VLAN
- サーバ ポート
- QoS システム クラス

LAN アップリンク マネージャで行うことができる設定の一部は、[Equipment] タブまたは [LAN] タブなどの他のタブのノードでも行うことができます。

Internal Fabric Manager

Internal Fabric Manager は、Cisco UCS ドメインのファブリック インターコネクトに対してサーバ ポートを設定できる単一インターフェイスを提供します。 Internal Fabric Manager には、そのファブリック インターコネクトの [General] タブからアクセスできます。

Internal Fabric Manager で行うことができる設定の一部は、[Equipment] タブ、[LAN] タブ、または LAN アップリンク マネージャのノードでも行うことができます。

ハイブリッド表示

Cisco UCS ドメイン内のシャーシごとに、シャーシとファブリック インターコネクト間の物理コンポーネントおよび接続の両方を含むハイブリッド表示が Cisco UCS Manager GUI により提供されます。

このタブには、選択されたシャーシとファブリック インターコネクト間の接続に関する詳細情報が表示されます。 タブには次のものを示すアイコンがあります。

- システムの各ファブリック インターコネクト。
- 選択されたコンポーネントの I/O モジュール（IOM）。これは、接続パスを見やすくするために独立したユニットとして表示されます。
- サーバと PSU を示す選択されたシャーシ。

アイコン間の線は次のものの接続関係を表します。

- 各サーバ上の DCE インターフェイスと IOM 上の関連付けられたサーバ ポート。 これらの接続はシスコによって作成され、変更することはできません。
- IOM 上のサーバ ポートとファブリック インターコネクト上の関連付けられたポート。 必要に応じてこれらの接続は変更できます。

アイコンと線の上にマウスを移動すると、各コンポーネントや接続に関するヒントが表示されます。いずれかのコンポーネントをダブルクリックすると、そのコンポーネントのプロパティが表示されます。

コンポーネントまたはそのサブコンポーネントに関連付けられた障害が存在する場合、Cisco UCS Manager GUI は適切なコンポーネントの上部に障害のアイコンを表示します。 複数の障害メッセージが存在する場合、Cisco UCS Manager GUI はシステムの最も重大な障害メッセージに関連付けられたアイコンを表示します。

HTTPS による Cisco UCS Manager GUI へのログイン

Cisco UCS Manager GUI のデフォルトの HTTPS Web リンクは、*UCSManager_IP* が Cisco UCS Manager に割り当てられた IP アドレスを示す、`https://UCSManager_IP` です。 この IP アドレスは、次のいずれかです。

- クラスタ設定：*UCSManager_IP* は、Cisco UCS Manager に割り当てられている仮想またはクラスタ IP アドレスを表します。 ファブリック インターコネクト上の管理ポートに割り当てられた IP アドレスを使用しないでください。
- スタンドアロン設定：*UCSManager_IP* はファブリック インターコネクトの管理ポートの IP アドレスを表します。

手順

ステップ 1 Web ブラウザで、Cisco UCS Manager GUI Web リンクを入力するか、ブラウザでブックマークを選択します。

ステップ 2 [Security Alert] ダイアログボックスが表示された場合は、[Yes] をクリックしてセキュリティ証明書を受け入れ、続行します。

ステップ 3 Cisco UCS Manager の起動ページで、[Launch UCS Manager] をクリックします。
ログインに使用する Web ブラウザによって、.JNLP ファイルのダウンロードまたは保存を求められる場合があります。

ステップ 4 Cisco UCS Manager にログイン前のバナーが表示された場合は、メッセージを確認し、[OK] をクリックしてダイアログボックスを閉じます。

ステップ 5 [Security] ダイアログボックスが表示された場合、次の手順を実行します。

a) （任意） チェックボックスをオンにして、シスコからのすべてのコンテンツを受け入れます。
b) [Yes] をクリックして証明書を受け入れ、続行します。

ステップ 6 [Login] ダイアログボックスで、次の手順を実行します。

a) ユーザ名とパスワードを入力します。
b) Cisco UCS 実装に複数のドメインが含まれている場合は、[Domain] ドロップダウン リストから適切なドメインを選択します。
c) [Login] をクリックします。

HTTP による Cisco UCS Manager GUI へのログイン

Cisco UCS Manager GUI のデフォルトの HTTP Web リンクは、*UCSManager_IP* が Cisco UCS Manager に割り当てられた IP アドレスを示す、`http://UCSManager_IP` です。 この IP アドレスは、次のいずれかです。

- クラスタ設定：*UCSManager_IP* は、Cisco UCS Manager に割り当てられている仮想またはクラスタ IP アドレスを表します。 ファブリック インターコネクト上の管理ポートに割り当てられた IP アドレスを使用しないでください。
- スタンドアロン設定：*UCSManager_IP* はファブリック インターコネクトの管理ポートの IP アドレスを表します。

手順

ステップ 1 Web ブラウザで、Cisco UCS Manager GUI Web リンクを入力するか、ブラウザでブックマークを選択します。

ステップ 2 Cisco UCS Manager にログイン前のバナーが表示された場合は、メッセージを確認し、[OK] をクリックしてダイアログボックスを閉じます。

ステップ 3 Cisco UCS Manager の起動ページで、[Launch UCS Manager] をクリックします。
ログインに使用する Web ブラウザによって、.JNLP ファイルのダウンロードまたは保存を求められる場合があります。

ステップ 4 [Login] ダイアログボックスで、次の手順を実行します。

a) ユーザ名とパスワードを入力します。

b) Cisco UCS 実装に複数のドメインが含まれている場合は、[Domain] ドロップダウン リストから適切なドメインを選択します。

c) [Login] をクリックします。

Cisco UCS Manager GUI からのログアウト

手順

ステップ 1 Cisco UCS Manager GUI で、右上の [Exit] をクリックします。
使用できないことを示すために Cisco UCS Manager GUI が画面上で不鮮明になり、[Exit] ダイアログボックスが表示されます。

ステップ 2 ドロップダウン リストから、次のいずれかを選択します。

- ログアウトして Cisco UCS Manager GUI をシャットダウンするには、[Exit] を選択します。
- Cisco UCS Manager GUI からログアウトし、別のユーザがログインする場合は、[Log Off] を選択します。

ステップ 3 [OK] をクリックします。

Web セッション制限

Web セッション制限が、常時システムへのアクセスを許可される Web セッション（GUI および XML の両方）の数を制限するために Cisco UCS Manager によって使用されます。

デフォルトでは、Cisco UCS Manager により許可される同時 Web セッションの数は最大値の 256 に設定されます。

Cisco UCS Manager の Web セッション制限の設定

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

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

ステップ 4 [Web Session Limits] 領域で、次のフィールドに値を入力します。

名前	説明
[Maximum Sessions Per User] フィールド	各ユーザに許可されている HTTP および HTTPS の同時セッションの最大数。 1 ～ 256 の整数を入力します。
[Maximum Sessions] フィールド	システム内のすべてのユーザに許可されている HTTP および HTTPS の同時セッションの最大数。 1 ～ 256 の整数を入力します。

ステップ 5 [Save Changes] をクリックします。

プリログイン バナー

Pre-Login バナーを使用すると、ユーザが Cisco UCS Manager GUI にログインするときに、Cisco UCS Manager は [Create Pre-Login Banner] ダイアログボックスにバナー テキストを表示し、ユーザがそのダイアログボックスを却下するまで待機してから、ユーザ名およびパスワードを求めるプロンプトを表示します。 ユーザが Cisco UCS Manager CLI にログインすると、Cisco UCS Manager はダイアログボックスにバナー テキストを表示し、ユーザがそのダイアログボックスを却下するまで待機してから、パスワードを求めるプロンプトを出します。 次に、ユーザに表示する著作権ブロックの上に、バナー テキストを繰り返し表示します。

プリログイン バナーの作成

[Pre-Login Banner] が [Banners] タブに表示されない場合、ユーザがログインしたときに、Cisco UCS Manager にプリログイン バナーは表示されません。 [Pre-Login Banner] 領域が表示された場合、別

のプリログイン バナーは作成できません。 既存のバナーを削除または変更することのみできます。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] を展開します。

ステップ 3 [User Services] ノードをクリックします。

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

ステップ 5 [Actions] 領域の [Create Pre-Login Banner] をクリックします。

ステップ 6 [Create Pre-Login Banner] ダイアログボックスで、テキスト フィールドをクリックし、ユーザが Cisco UCS Manager にログインするときに表示するメッセージを入力します。
このフィールドには、標準 ASCII 文字を入力できます。

ステップ 7 [OK] をクリックします。

プリログイン バナーの変更

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] を展開します。

ステップ 3 [User Services] ノードをクリックします。

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

ステップ 5 [Pre-Login Banner] 領域のテキスト フィールドをクリックして、テキストに必要な変更を加えます。
このフィールドには、標準 ASCII 文字を入力できます。

ステップ 6 [Save Changes] をクリックします。

プリログイン バナーの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] を展開します。

ステップ 3 [User Services] ノードをクリックします。

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

ステップ 5 [Actions] 領域の [Delete] をクリックします。

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

Cisco UCS Manager GUI のプロパティ

Cisco UCS Manager GUI のセッションおよびログのプロパティの設定

これらのプロパティは、Cisco UCS Manager GUI がセッションの中断または非アクティブにどのように応答するかを決定し、Cisco UCS Manager GUI Java メッセージ ロギングを設定します。

手順

ステップ 1 ツールバーで [Option] をクリックして、[Properties] ダイアログボックスを開きます。

ステップ 2 右側のペインで、[Session] をクリックします。

ステップ 3 [Session] ページで、次に示す 1 つまたは複数のフィールドをアップデートします。

名前	説明
[Automatically Reconnect] チェックボックス	このチェックボックスをオンにすると、GUI とファブリック インターコネクトの間の通信が中断されたときに、システムによって再接続が試行されます。
[GUI Inactivity Time Out] ドロップダウン リスト	非アクティブのセッションを終了させる前にシステムが待機する分数。 非アクティブの状態がどれくらい長く続いても、セッションがタイムアウトしないことを指定するには、[NEVER] を選択します。

名前	説明
[Log Level] ドロップダウン リスト	ユーザのローカル マシンで Cisco UCS Manager GUI に対して行われる Java メッセージ ロギングの量。 次のいずれかになります。 • [All]：GUI に関連するすべての Java 情報がログに記録されます。 最大 10 個のログ ファイルがあり、それぞれのサイズは最大 10 MB です。 最後のファイルがいっぱいになると、Cisco UCS Manager は最も古いログ ファイルを削除して、新しいログ ファイルを開始します。 • [Off]：Cisco UCS Manager は、GUI の Java ログ ファイルを作成しません。 （注） ログ ファイルの場所は、ユーザのローカル マシンの Java ランタイム設定によって決定されます。 詳細については、使用している Java バージョンのマニュアルを参照してください。
[Max Log Size] ドロップダウン リスト	Cisco UCS Manager によっていずれかのログに割り当てられ、この Cisco UCS ドメイン用に保存される最大サイズ（メガバイト単位）。
[Reconnection Interval] フィールド	[Automatically Reconnect] チェックボックスをオンにした場合、このフィールドは、再接続を試行する前にシステムが待機する秒数です。

ステップ 4 [OK] をクリックします。

確認メッセージのプロパティの設定

これらのプロパティは、Cisco UCS Manager GUI が設定変更およびそのほかの操作後に確認メッセージ表示するかどうかを決定します。

手順

ステップ 1 ツールバーで [Option] をクリックして、[Properties] ダイアログボックスを開きます。

ステップ 2 右側のペインで、[Confirmation Messages] をクリックします。

ステップ 3 [Confirmation Messages] ページで、次のフィールドに値を入力します。

名前	説明
[Confirm Deletion] チェックボックス	このチェックボックスをオンにすると、すべての削除操作に対して Cisco UCS Manager GUI から確認が要求されます。
[Confirm Discard Changes] チェックボックス	このチェックボックスをオンにすると、システムで変更が破棄される前に、Cisco UCS Manager GUI から確認が要求されます。
[Confirm Modification/Creation] チェックボックス	このチェックボックスをオンにすると、システムでオブジェクトを修正または作成する前に、Cisco UCS Manager GUI から確認が要求されます。
[Confirm Successful Operations] チェックボックス	このチェックボックスをオンにすると、操作が正常に完了したときに、Cisco UCS Manager GUI から確認が表示されます。

ステップ 4 [OK] をクリックします。

外部アプリケーションのプロパティの設定

Cisco UCS Manager GUI これらのプロパティを SSH などの外部アプリケーションとの接続に使用します。

手順

ステップ 1 ツールバーで [Option] をクリックして、[Properties] ダイアログボックスを開きます。

ステップ 2 右側のペインで、[External Applications] をクリックします。

ステップ 3 [External Applications] ページで、次のフィールドに値を入力します。

名前	説明
[SSH] フィールド	SSH 処理に使用するアプリケーション。
[SSH Parameters] フィールド	すべての SSH コマンドに含めるパラメータ。

ステップ 4 [OK] をクリックします。

Cisco UCS Manager GUI の表示のカスタマイズ

これらのプロパティでは、Cisco UCS Manager GUI の一部の表示プロパティをカスタマイズできます。

手順

ステップ 1 ツールバーで [Option] をクリックして、[Properties] ダイアログボックスを開きます。

ステップ 2 右側のペインで、[Visual Enhancements] をクリックします。

ステップ 3 [Visual Enhancements] ページで、次に示す 1 つまたは複数のフィールドをアップデートします。

名前	説明
[Automatically Pack Table Columns] チェックボックス	このチェックボックスをオンにすると、Cisco UCS Manager GUI は、すべてのテーブルカラムのサイズをその内容に基づいて自動的に変更します。
[Max History Size] フィールド	[Forward] および [Back] ツールバー ボタンの対象となるタブがメモリに保存される数。
[Right Aligned Labels] チェックボックス	このチェックボックスをオンにすると、すべてのラベルが互いに対して右揃えになります。 オンにしなければ、すべてのラベルが左揃えになります。
[Show Image while Dragging] チェックボックス	このチェックボックスをオンにすると、オブジェクトをある場所から別の場所にドラッグするとき、そのオブジェクトを新しい場所にドロップするまでの間、そのオブジェクトを透明にしたものが GUI に表示されます。
[Wizard Transition Effects] チェックボックス	このチェックボックスをオンにすると、ウィザード内で新しいページに移動するときに、元のページからフェードアウトし、新しいページにフェードインします。 オンにしなければ、ページは視覚効果なしで変化します。

ステップ 4 [OK] をクリックします。

フィールドの値の許容範囲の確認

一部のプロパティは入力できる値の範囲に制限があります。 ダイアログボックス、ウィンドウ、またはタブのフィールドにその許容範囲を確認するには、この手順を使用できます。 テーブルま

たはツリーにリストされているプロパティに値の範囲を確認するには、この手順を使用できません。

手順

ステップ 1 フィールドにフォーカスを与えるために、範囲を確認するフィールドにカーソルを置きます。

ステップ 2 Alt+Shift+R を押します。
Cisco UCS Manager GUI に値の許容範囲が数秒間表示されます。 範囲は画面内の任意の場所をクリックすると消えます。

ポリシーの使用場所の確認

選択したポリシーに関連付けられているサービス プロファイルとサービス プロファイル テンプレートを確認するには、この手順を使用できます。

手順

ステップ 1 [Navigation] ペインで、使用状況を表示するポリシーをクリックします。

ステップ 2 [Work] ペインで、[General] タブをクリックします。

ステップ 3 [Actions] 領域の [Show Policy Usage] をクリックします。
Cisco UCS Manager GUI は、関連付けられたサービス プロファイルとサービス プロファイル テンプレートを示す [Service Profiles/Templates] ダイアログボックスを表示します。

プールの使用場所の確認

選択したプールに関連付けられている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を確認するには、この手順を使用できます。

手順

ステップ 1 [Navigation] ペインで、使用状況を表示するプールをクリックします。

ステップ 2 [Work] ペインで、[General] タブをクリックします。

ステップ 3 [Actions] 領域の [Show Pool Usage] をクリックします。
Cisco UCS Manager GUI は、関連付けられたサービス プロファイルとサービス プロファイル テンプレートを示す [Service Profiles/Templates] ダイアログボックスを表示します。

XML のコピー

Cisco UCS 向けの XML API を使用したスクリプトの開発やアプリケーションの作成を支援するために、Cisco UCS Manager GUI には Cisco UCS Manager でオブジェクトを作成するために使用された XML をコピーするオプションが含まれます。 このオプションは、[Navigation] ペインのほとんどのオブジェクト ノード（[Port Profiles] ノードまたは特定の サービス プロファイル のノードなど）の右クリック メニューで利用できます。

手順

ステップ 1 [Navigation] ペインで、XML をコピーするオブジェクトに移動します。

ステップ 2 このオブジェクトを右クリックして、[Copy XML] を選択します。

ステップ 3 XML を XML エディタ、Notepad、または他のアプリケーションに貼り付けます。

第 II 部

システム設定

- ファブリック インターコネクトの設定，59 ページ
- ポートおよびポート チャネルの設定，73 ページ
- 通信サービスの設定，123 ページ
- 認証の設定，143 ページ
- 組織の設定，173 ページ
- ロールベース アクセス コントロールの設定，179 ページ
- DNS サーバの設定，205 ページ
- システム関連ポリシーの設定，207 ページ
- ライセンスの管理，217 ページ
- 仮想インターフェイスの管理，231 ページ
- Cisco UCS Central への Cisco UCS ドメインの登録，233 ページ

第 5 章

ファブリック インターコネクトの設定

この章の内容は、次のとおりです。

- 初期システム セットアップ，59 ページ
- スタンドアロン設定用の初期システム セットアップの実行，61 ページ
- クラスタ設定の初期システム セットアップ，63 ページ
- スタンドアロン ファブリック インターコネクトに対するクラスタ設定のイネーブル化，67 ページ
- イーサネット スイッチング モード，68 ページ
- イーサネット スイッチング モードの設定，69 ページ
- ファイバ チャネル スイッチング モード，69 ページ
- ファイバ チャネル スイッチング モードの設定，70 ページ
- ファブリック インターコネクトのプロパティの変更，71 ページ
- ファブリック インターコネクトのリーダーシップ ロールの決定，72 ページ

初期システム セットアップ

Cisco UCS ドメイン内のファブリック インターコネクトへの初回アクセス時には、セットアップ ウィザードでシステム設定に必要な次の情報の入力を求められます。

- インストール方法（GUI または CLI）
- セットアップ モード（フル システム バックアップからの復元または初期セットアップ）
- システム設定タイプ（スタンドアロンまたはクラスタ設定）
- システム名
- admin パスワード

- 管理ポートの IP アドレスおよびサブネット マスク
- デフォルト ゲートウェイの IP アドレス
- DNS サーバの IP アドレス
- デフォルトのドメイン名

セットアップ モード

システム設定を既存のバックアップ ファイルから復元するか、セットアップ ウィザードを実行してシステムを手動でセットアップするか、選択できます。 システムを復元する場合は、バックアップ ファイルが、管理ネットワークから到達可能な場所に存在する必要があります。

システム設定タイプ

スタンドアロン設定で単一のファブリック インターコネクトを使用するように、またはクラスタ設定でファブリック インターコネクトの冗長ペアを使用するように、Cisco UCS ドメインを設定できます。

クラスタ設定では、ハイ アベイラビリティが提供されます。 一方のファブリック インターコネクトが使用不可能になっても、もう一方が代わりを務めます。 クラスタ設定をサポートするには、管理ポート（Mgmt0）接続が 1 つだけあれば十分です。しかし、リンク レベルの冗長性を実現するには、両方の Mgmt0 ポートを接続する必要があります。

さらに、クラスタ設定では、冗長仮想インターフェイス（VIF）接続のフェールオーバー リカバリ時間が大きく向上します。 アダプタに、1 つのファブリック インターコネクトへのアクティブ VIF 接続および第 2 のファブリック インターコネクトへのスタンバイ VIF 接続がある場合、アクティブ VIF 上で学習した MAC アドレスがレプリケートされますが、2 つめのファブリック インターコネクトにはインストールされません。 アクティブ VIF で障害が発生した場合、第 2 のファブリック インターコネクトは複製された MAC アドレスをインストールし、それらを Gratuitous ARP メッセージを介してネットワークへブロードキャストして、切り替え時間を短縮します。

（注） クラスタ設定では、管理プレーンの冗長性だけを提供します。 データの冗長性はユーザ設定に依存するものであり、データの冗長性をサポートするサードパーティ製のツールが必要になる可能性があります。

クラスタ設定を使用するには、2 つのファブリック インターコネクトが、イーサネット ケーブルを使用して、L1（L1 から L1）および L2（L2 から L2）ハイ アベイラビリティ ポート間で他のファブリックインターコネクトを挟まずにじかに相互接続される必要があります。 これにより、2 つのファブリック インターコネクトは、互いのステータスを継続的にモニタし、一方で故障が発生しても素早く検知できます。

クラスタ設定内の両方のファブリックインターコネクトに対して初期セットアッププロセスを実行する必要があります。 先に設定されるファブリックインターコネクトは、クラスタ設定用にイネーブルにされる必要があります。 その後、2 つめのファブリック インターコネクトが設定され

ると、クラスタ内のピア ファブリック インターコネクトとして最初のファブリック インターコネクトを検出します。

詳細については、『*Cisco UCS 6100 Series Fabric Interconnect Hardware Installation Guide*』を参照してください。

管理ポートの IP アドレス

スタンドアロン設定では、ファブリック インターコネクトの単一の管理ポートに対し、IP アドレスとサブネット マスクをそれぞれ 1 つだけ指定します。

クラスタ設定では、同じサブネット内で次の 3 つの IP アドレスを指定します。

- ファブリック インターコネクト A の管理ポートの IP アドレス
- ファブリック インターコネクト B の管理ポートの IP アドレス
- クラスタの IP アドレス

スタンドアロン設定用の初期システム セットアップの実行

はじめる前に

1. ファブリック インターコネクトにおける次の物理接続を確認します。
   - コンソール ポートがコンピュータ端末またはコンソール サーバに物理的に接続されている。
   - 管理イーサネット ポート（mgmt0）が外部のハブ、スイッチ、またはルータに接続されている。

   詳細については、お使いのファブリック インターコネクトに関する『*Cisco UCS Hardware Installation Guide*』を参照してください。
2. コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。
   - 9600 ボー
   - 8 データ ビット
   - パリティなし
   - 1 ストップ ビット
3. 初期設定で入力する必要がある次の情報を収集します。
   - システム名。
   - admin アカウントのパスワード。 Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。 このパスワードは空にできません。

- 管理ポートの IP アドレスおよびサブネット マスク。
- デフォルト ゲートウェイの IP アドレス。
- DNS サーバの IP アドレス（任意）。
- システムのドメイン名（任意）。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリックインターコネクトが起動すると、電源投入時セルフテストメッセージが表示されます。

ステップ 3 インストール方式プロンプトに gui と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

- ファブリック インターコネクトの管理ポートの IP アドレス
- ファブリック インターコネクトの管理ポートのサブネット マスク
- ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IP アドレス

ステップ 5 プロンプトから、サポートされる Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。

ステップ 6 Cisco UCS Manager GUI 起動ページで [Express Setup] を選択します。

ステップ 7 [Express Setup] ページで [Initial Setup] を選択し、[Submit] をクリックします。

ステップ 8 [Cluster and Fabric Setup] 領域で、[Standalone Mode] オプションを選択します。

ステップ 9 [System Setup] 領域で、次のフィールドに値を入力します。

フィールド	説明
[System Name] フィールド	Cisco UCS ドメインに割り当てられている名前。 スタンドアロン設定では、システム名に「-A」が追加されます。 クラスタ設定では、ファブリック A に割り当てられたファブリック インターコネクトに「-A」が、ファブリック B に割り当てられたファブリック インターコネクトに「-B」が追加されます。
[Admin Password] フィールド	ファブリック インターコネクト上の Admin アカウントに使用されるパスワード。 Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。 このパスワードは空にできません。

フィールド	説明
[Confirm Admin Password] フィールド	ファブリック インターコネクト上の Admin アカウントに使用されるパスワード。
[Mgmt IP Address] フィールド	ファブリック インターコネクト上の管理ポートの固定 IP アドレス。
[Mgmt IP Netmask] フィールド	ファブリック インターコネクト上の管理ポートのサブネット マスク。
[Default Gateway] フィールド	ファブリック インターコネクト上の管理ポートに割り当てられるデフォルト ゲートウェイの IP アドレス。
[DNS Server IP] フィールド	ファブリック インターコネクトに割り当てられる DNS サーバの IP アドレス。
[Domain Name] フィールド	ファブリック インターコネクトが存在するドメインの名前。

ステップ 10 [Submit] をクリックします。
セットアップ操作の結果がページに表示されます。

クラスタ設定の初期システム セットアップ

第 1 ファブリック インターコネクトでの初期システム セットアップの実行

はじめる前に

1. ファブリック インターコネクトにおける次の物理接続を確認します。
   - 第 1 のファブリック インターコネクトのコンソール ポートが、コンピュータ端末またはコンソール サーバに物理的に接続されている。
   - 管理イーサネット ポート（mgmt0）が外部のハブ、スイッチ、またはルータに接続されている。
   - 両方のファブリック インターコネクトの L1 ポートが互いに直接接続されている。
   - 両方のファブリック インターコネクトの L2 ポートが互いに直接接続されている。

詳細については、お使いのファブリック インターコネクトに関する『*Cisco UCS Hardware Installation Guide*』を参照してください。

2 コンソール ポートに接続しているコンピュータ端末（またはコンソール サーバ）でコンソール ポート パラメータが次のとおりであることを確認します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

3 初期設定で入力する必要がある次の情報を収集します。

- システム名。
- admin アカウントのパスワード。 Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。 このパスワードは空にできません。
- 3 つの固定 IP アドレス：両方のファブリック インターコネクトの管理ポートに 2 つ（各ファブリック インターコネクトに 1 つずつ）、および Cisco UCS Manager によって使用されるクラスタ IP アドレスに 1 つ。
- 3 つの固定 IP アドレスのサブネット マスク。
- デフォルト ゲートウェイの IP アドレス。
- DNS サーバの IP アドレス（任意）。
- システムのドメイン名（任意）。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリックインターコネクトが起動すると、電源投入時セルフテストメッセージが表示されます。

ステップ 3 インストール方式プロンプトに gui と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

- ファブリック インターコネクトの管理ポートの IP アドレス
- ファブリック インターコネクトの管理ポートのサブネット マスク
- ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IP アドレス

ステップ 5 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。

ステップ 6 Cisco UCS Manager GUI 起動ページで [Express Setup] を選択します。

ステップ 7 [Express Setup] ページで [Initial Setup] を選択し、[Submit] をクリックします。

ステップ 8 [Cluster and Fabric Setup] 領域で次の手順を実行します。

a) [Enable Clustering] オプションをクリックします。

b) [Fabric Setup] オプションに対して Fabric A を選択します。

c) [Cluster IP Address] フィールドに、Cisco UCS Manager が使用する IP アドレスを入力します。

ステップ 9 [System Setup] 領域で、次のフィールドに値を入力します。

フィールド	説明
[System Name] フィールド	Cisco UCS ドメインに割り当てられている名前。 スタンドアロン設定では、システム名に「-A」が追加されます。 クラスタ設定では、ファブリック A に割り当てられたファブリック インターコネクトに「-A」が、ファブリック B に割り当てられたファブリック インターコネクトに「-B」が追加されます。
[Admin Password] フィールド	ファブリック インターコネクト上の Admin アカウントに使用されるパスワード。 Cisco UCS Manager のパスワードのガイドラインに適合する強力なパスワードを選択します。 このパスワードは空にできません。
[Confirm Admin Password] フィールド	ファブリック インターコネクト上の Admin アカウントに使用されるパスワード。
[Mgmt IP Address] フィールド	ファブリック インターコネクト上の管理ポートの固定 IP アドレス。
[Mgmt IP Netmask] フィールド	ファブリック インターコネクト上の管理ポートのサブネット マスク。
[Default Gateway] フィールド	ファブリック インターコネクト上の管理ポートに割り当てられるデフォルト ゲートウェイの IP アドレス。
[DNS Server IP] フィールド	ファブリック インターコネクトに割り当てられる DNS サーバの IP アドレス。
[Domain Name] フィールド	ファブリック インターコネクトが存在するドメインの名前。

ステップ 10 [Submit] をクリックします。
セットアップ操作の結果がページに表示されます。

第 2 ファブリック インターコネクトでの初期システム セットアップの実行

はじめる前に

次の項目を確認しておく必要があります。

- 第 2 のファブリック インターコネクトのコンソール ポートが、コンピュータ端末またはコンソール サーバに物理的に接続されている。
- 設定した第 1 ファブリック インターコネクトでの admin アカウントのパスワードを知っている。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトの電源を入れます。
ファブリックインターコネクトが起動すると、電源投入時セルフテストメッセージが表示されます。

ステップ 3 インストール方式プロンプトに gui と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合は、次の情報を入力するよう求められます。

- ファブリック インターコネクトの管理ポートの IP アドレス
- ファブリック インターコネクトの管理ポートのサブネット マスク
- ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IP アドレス

ステップ 5 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。

ステップ 6 Cisco UCS Manager GUI 起動ページで [Express Setup] を選択します。

ステップ 7 [Express Setup] ページで [Initial Setup] を選択し、[Submit] をクリックします。
ファブリック インターコネクトは、第 1 ファブリック インターコネクトの設定情報を検出します。

ステップ 8 [Cluster and Fabric Setup] 領域で次の手順を実行します。

a) [Enable Clustering] オプションを選択します。

b) [Fabric Setup] オプションに対して Fabric B が選択されていることを確認します。

ステップ 9 [System Setup] 領域の [Admin Password of Master] フィールドに、Admin アカウントのパスワードを入力します。

ステップ 10 [Submit] をクリックします。
セットアップ操作の結果がページに表示されます。

スタンドアロン ファブリック インターコネクトに対するクラスタ設定のイネーブル化

1 つのスタンドアロン ファブリック インターコネクトを使用する既存の Cisco UCS ドメインに、別のファブリック インターコネクトを追加できます。 これには、クラスタの仮想 IP アドレスを使用して、クラスタ操作用にスタンドアロンファブリックインターコネクトをイネーブルにし、次にクラスタに第 2 のファブリック インターコネクトを追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **connect local-mgmt**	ローカル管理モードを開始します。
ステップ 2	UCS-A(local-mgmt) # **enable cluster** *virtual-ip-addr*	指定の IP アドレスを持つスタンドアロン ファブリック インターコネクトでクラスタ動作をイネーブルにします。このコマンドを入力すると、クラスタ動作をイネーブルにすることを確認するプロンプトが表示されます。 確認するには、**yes** と入力します。 IP アドレスは、クラスタに追加するファブリック インターコネクトに割り当てられている IP アドレスではなく、クラスタ設定用の仮想 IP アドレスである必要があります。

次に、仮想 IP アドレス 192.168.1.101 のスタンドアロン ファブリック インターコネクトのクラスタ動作をイネーブルにする例を示します。

```
UCS-A# connect local-mgmt
UCS-A(local-mgmt)# enable cluster 192.168.1.101
This command will enable cluster mode on this setup. You cannot change it
back to stand-alone. Are you sure you want to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

次の作業

クラスタに第 2 のファブリック インターコネクトを追加します。

イーサネット スイッチング モード

イーサネットスイッチングモードにより、サーバとネットワークの間のスイッチング装置としてファブリックインターコネクトがどのように動作するかが決定されます。 ファブリックインターコネクトは、次のイーサネット スイッチング モードのいずれかで動作します。

エンドホスト モード

エンドホスト モードでは、ファブリック インターコネクトはネットワークへのエンド ホストとして、vNIC を介して接続されているすべてのサーバ（ホスト）の代表として動作するようになります。 これは、vNIC をアップリンク ポートにピン接続することにより実現されます（動的なピン接続または固定のピン接続のいずれか）。これにより、ネットワークに対して冗長性が提供され、これらのアップリンク ポートはファブリックの残りの部分に対してサーバ ポートとなります。 エンドホスト モードの場合、ファブリック インターコネクトでスパニングツリー プロトコル（STP）は実行されません。ループは、アップリンク ポートがトラフィックを相互に転送するのを拒否すること、および同時に複数のアップリンク ポート上に存在する出力サーバ トラフィックを拒否することにより回避されます。 エンドホスト モードは、デフォルトのイーサネット スイッチング モードであり、次のいずれかがアップストリームで使用される場合に使用する必要があります。

- L2 集約用のレイヤ 2 スイッチング
- Virtual Switching System（VSS）集約レイヤ

（注） エンドホスト モードがイネーブルになっている場合、vNIC がアップリンク ポートに固定ピン接続されていて、このアップリンク ポートがダウンすると、システムはその vNIC をピン接続し直すことはできず、その vNIC はダウンしたままになります。

スイッチ モード

スイッチ モードは従来のイーサネット スイッチング モードです。 ループを回避するためにファブリック インターコネクトで STP が実行され、ブロードキャスト パケットとマルチキャスト パケットは従来の方法で処理されます。 スイッチ モードは、デフォルトのイーサネット スイッチングモードではありません。ファブリックインターコネクトをルータに直接接続する場合、または次のいずれかがアップストリームで使用される場合に限り使用する必要があります。

- レイヤ 3 集約
- ボックス内の VLAN

（注） どちらのイーサネット スイッチング モードの場合でも、サーバ アレイ内のすべてのサーバ間ユニキャスト トラフィックは、ファブリック インターコネクトを介してだけ送信され、アップリンク ポートを介して送信されることはありません。vNIC がアップリンク ポートに固定ピン接続されていたとしても同様です。 サーバ間のマルチキャスト トラフィックとブロードキャスト トラフィックは、同じ VLAN 内のすべてのアップリンク ポートを介して送信されます。

イーサネット スイッチング モードの設定

重要 イーサネット スイッチング モードを変更すると、Cisco UCS Manager により自動的にログアウトとファブリック インターコネクトの再起動が実行されます。 クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネクトが順番に再起動されます。 2 つめのファブリック インターコネクトがイーサネット スイッチング モードに変更され、システムが使用できるようになるまでには数分間かかります。 設定が保持されます。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] 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 [General] タブの [Actions] 領域で、次のリンクのいずれかをクリックします。

- Set Ethernet Switching Mode
- Set Ethernet End-Host Mode

現在のモードのリンクはグレー表示されます。

ステップ 5 ダイアログボックスで、[Yes] をクリックします。
Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager GUI との接続を解除します。

ファイバ チャネル スイッチング モード

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

エンドホスト モード

エンドホスト モードでは、ファブリック インターコネクトは接続されているファイバ チャネル ネットワークへのエンドホストとして、vHBA を介して接続されているすべてのサーバ（ホスト）の代表として動作するようになります。 これは、vHBA をファイバ チャネル アップリンク ポートにピン接続すること（動的なピン接続または固定のピン接続のいずれか）により実現されます。これにより、これらのファイバ チャネル アップリンク ポートはファブリックの残りの部分に対してサーバ ポート（N ポート）となります。 エンドホスト モードでは、ファブリック インターコネクトは、互いにトラフィックを受信しないようにアップリンク ポートの拒否によってループを回避します。

エンドホスト モードは、NPV モードと同義語です。 これがデフォルトのファイバ チャネル スイッチング モードです。

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

スイッチ モード

スイッチ モードは従来のファイバ チャネル スイッチング モードです。 スイッチ モードでは、ファブリック インターコネクトがストレージ デバイスに直接接続できます。 ファイバ チャネル スイッチ モードをイネーブルにすると、POD モデルにおいて、SAN が存在しない（たとえば、単一の Cisco UCS システムがストレージに直接接続されている）場合、または SAN が存在する（アップストリーム MDS に対して）場合に役立ちます。

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

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

ファイバ チャネル スイッチング モードの設定

重要 ファイバ チャネル スイッチング モードを変更すると、Cisco UCS Manager により自動的にログアウトとファブリック インターコネクトの再起動が実行されます。 クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネクトが順番に再起動されます。 2 つめのファブリック インターコネクトがファイバ チャネル スイッチング モードに変更され、システムが使用できるようになるまでには数分間かかります。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] 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 [General] タブの [Actions] 領域で、次のリンクのいずれかをクリックします。

- Set Fibre Channel Switching Mode
- Set Fibre Channel End-Host Mode

現在のモードのリンクはグレー表示されます。

ステップ 5 ダイアログボックスで、[Yes] をクリックします。
Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager GUI との接続を解除します。

ファブリック インターコネクトのプロパティの変更

（注） Cisco UCS ドメインのサブネットを変更するには、すべてのサブネット、Cisco UCS Manager へのアクセスに使用される仮想 IP アドレス、およびすべてのファブリック インターコネクトの IP アドレスを同時に変更する必要があります。

手順

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

ステップ 2 [Admin] タブで [ALL] をクリックします。

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 [Actions] 領域で [Management Interfaces] をクリックして、[Management Interfaces] ダイアログボックスを開きます。

ステップ 5 Cisco UCS Manager にアクセスするために使用する仮想 IP アドレスだけを変更するには、[Virtual IP] 領域の[IP Address] フィールドに目的の IP アドレスを入力します。

ステップ 6 Cisco UCS ドメインに割り当てられた名前だけを変更するには、[Virtual IP] 領域の[Name] フィールドに必要な名前を入力します。

ステップ 7 ファブリック インターコネクトに割り当てられたサブネット、IP アドレス、およびデフォルトゲートウェイを変更するには、次のフィールドをアップデートします。

a) [Virtual IP] 領域で、[IP Address] フィールドの、Cisco UCS Manager にアクセスするために使用する IP アドレスを変更します。

b) 各ファブリック インターコネクトの [Fabric Interconnect] 領域で、次のフィールドをアップデートします。

名前	説明
[IP Address] フィールド	ファブリック インターコネクトと通信するときに使用する IP アドレス。
[Subnet Mask] フィールド	関連付けられたサブネット マスク。
[Default Gateway] フィールド	関連付けられたゲートウェイ。

ステップ 8 [OK] をクリックします。

ステップ 9 Cisco UCS Manager GUI からログアウトし、再びログインして変更を確認します。

ファブリック インターコネクトのリーダーシップ ロールの決定

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

ステップ 3 ロールを識別するファブリック インターコネクトをクリックします。

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

ステップ 5 [General] タブで、[High Availability Details] バーの下矢印をクリックしてこの領域を展開します。

ステップ 6 [Leadership] フィールドを表示して、このファブリック インターコネクトがプライマリ ファブリック インターコネクトか、従属ファブリック インターコネクトかを決定します。

第 6 章

ポートおよびポート チャネルの設定

この章の内容は、次のとおりです。

- 6100 シリーズ ファブリック インターコネクト上のサーバ ポートおよびアップリンク ポート，74 ページ
- 6200 シリーズ ファブリック インターコネクト上のユニファイド ポート，75 ページ
- サーバ ポート，84 ページ
- アップリンク イーサネット ポート，84 ページ
- ファブリック インターコネクトのポートの再設定，86 ページ
- ファブリック インターコネクト上のポートのイネーブル化，86 ページ
- ファブリック インターコネクト上のポートのディセーブル化，87 ページ
- ファブリック インターコネクトのポート設定解除，88 ページ
- アプライアンス ポート，89 ページ
- FCoE ストレージ ポートおよびファイバ チャネル ストレージ ポート，94 ページ
- FCoE アップリンク ポート，96 ページ
- ユニファイド ストレージ ポート，97 ページ
- ユニファイド アップリンク ポート，100 ページ
- アップリンク イーサネット ポート チャネル，102 ページ
- アプライアンス ポート チャネル，105 ページ
- ファイバ チャネル ポート チャネル，110 ページ
- FCoE ポート チャネル，114 ページ
- ユニファイド アップリンク ポート チャネル，115 ページ
- アダプタ ポート チャネル，116 ページ
- ファブリック ポート チャネル，117 ページ

• Internal Fabric Manager を使用したサーバ ポートの設定，120 ページ

6100 シリーズ ファブリック インターコネクト上のサーバ ポートおよびアップリンク ポート

各 6100 シリーズ ファブリック インターコネクトには、サーバ ポートまたはアップリンク イーサネット ポートとして設定できるポートの集合が固定ポート モジュール内に存在します。 これらのポートは予約されていません。 設定しなければ、Cisco UCS ドメインで使用できません。 拡張モジュールを追加して、ファブリック インターコネクト上のアップリンク ポートの数を増やしたり、ファブリック インターコネクトにアップリンク ファイバ チャネル ポートを追加したりできます。

LAN ピン グループと SAN ピン グループを作成して、サーバからのトラフィックをアップリンク ポートにピン接続する必要があります。

（注） 6100 シリーズ ファブリック インターコネクト上のポートは統合されません。 ユニファイド ポートの詳細については、「6200 シリーズ ファブリック インターコネクト上のユニファイド ポート」を参照してください。

各ファブリック インターコネクトには次のポート タイプを含むことができます。

サーバ ポート

サーバ ポートは、ファブリック インターコネクトとサーバ上のアダプタ カードとの間のデータ トラフィックを処理します。

設定できるのは固定ポート モジュールのサーバ ポートだけです。 展開モジュールにはサーバ ポートは含まれません。

アップリンク イーサネット ポート

アップリンク イーサネット ポートは、ファブリック インターコネクトと次のレイヤのネットワークとの間のイーサネット トラフィックを処理します。 すべてのネットワーク行きのイーサネット トラフィックは、これらのポートのいずれかにピン接続されます。

デフォルトでは、イーサネット ポートは未設定です。 ただし、次のように動作するように設定できます。

- アップリンク
- FCoE
- アプライアンス

固定モジュールまたは展開モジュールのアップリンク イーサネット ポートを設定できます。

アップリンク ファイバ チャネル ポート

アップリンク ファイバ チャネル ポートは、ファブリック インターコネクトと Storage Area Network の次のレイヤとの間の FCoE トラフィックを処理します。 すべてのネットワーク行きの FCoE トラフィックは、これらのポートのいずれかにピン接続されます。

デフォルトでは、ファイバ チャネル ポートはアップリンクです。 ただし、ファイバ チャネル ストレージ ポートとして動作するよう設定できます。 これは、Cisco UCS で直接接続ストレージ（DAS）デバイスへの接続が必要な場合に役立ちます。

設定できるのは展開モジュールのアップリンク ファイバ チャネル ポートだけです。 固定モジュールには、アップリンク ファイバ チャネル ポートは含まれません。

6200 シリーズ ファブリック インターコネクト上のユニファイド ポート

ユニファイド ポートとは、6200 シリーズのファブリック インターコネクト上のポートで、イーサネットまたはファイバチャネルのいずれかのトラフィックを送信するように設定できます。 これらのポートは予約されていません。 設定しなければ、Cisco UCS ドメインで使用できません。

設定可能なビーコン LED は、選択されたポート モードにいずれのユニファイド ポートが設定されているかを示します。

ポート モード

ポート モードは、イーサネット トラフィックまたはファイバ チャネル トラフィックのいずれを伝送するようにファブリックインターコネクトのユニファイドポートが設定されているかを決定します。 ポートモードは、ファブリックインターコネクトによって自動的には検出されません。 これは Cisco UCS Manager で設定します。

ポート モードを変更すると、既存のポート設定は削除され、新しい論理ポートで置き換えられる結果になります。 VLAN および VSAN など、そのポート設定と関連付けられたすべてのオブジェクトが削除されます。 ポート モードをユニファイド ポート用に変更することができる回数に制限はありません。

ポート タイプ

ポートタイプでは、ユニファイドポート接続で伝送されるトラフィックのタイプを定義します。

リストされている全ポート タイプは、固定および拡張モジュール両方で設定可能です。サーバポートを含みますが、これは 6100 シリーズ ファブリック インターコネクトの拡張モジュールでは設定できませんが、6200 シリーズ ファブリック インターコネクトの拡張モジュールで設定可能です。

デフォルトでは、イーサネット ポート モードに変更されるユニファイド ポートはアップリンク イーサネット ポート タイプに設定されます。 ファイバ チャネル ポート モードに変更されるユニ

ファイド ポートはファイバ チャネル アップリンク ポート タイプに設定されます。 ファイバ チャネル ポートは未設定にできません。

ポート タイプを変更しても、リブートは不要です。

ポート モードがイーサネットに設定されている場合、次のポート タイプを設定できます。

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

（注） SPAN 送信元ポートには、ポート タイプの 1 つを設定し、SPAN 送信元としてポートを設定します。

ポート モードがファイバ チャネルに設定されている場合、次のタイプを設定することができます。

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

（注） SPAN 送信元ポートには、ポート タイプの 1 つを設定し、SPAN 送信元としてポートを設定します。

ユニファイド ポートのビーコン LED

6200 シリーズ ファブリック インターコネクトの各ポートに対応するビーコン LED があります。ビーコン LED のプロパティが設定されている場合、ビーコン LED は、どのポートが指定のポート モードに設定されているかを点灯で示します。

ビーコン LED のプロパティは、いずれのポートが 1 つのポート モード（イーサネットまたはファイバ チャネル）にグループ化されているかを示すように設定できます。デフォルトでは、ビーコン LED のプロパティは Off に設定されます。

（注） 拡張モジュールのユニファイド ポートの場合、ビーコン LED のプロパティは、拡張モジュールのリブート時にデフォルト値 Off にリセットされることがあります。

ユニファイド ポートの設定の注意事項

ユニファイド ポートを設定する場合、次の注意事項および制約事項を考慮してください。

ハードウェアおよびソフトウェアの要件

ユニファイド ポートは Cisco UCS Manager バージョン 2.0 では 6200 シリーズ ファブリック インターコネクトでサポートされます。

ユニファイド ポートは 6100 シリーズ ファブリック インターコネクトでは、Cisco UCS Manager バージョン 2.0 を実行していてもサポートされません。

ポート モードの配置

Cisco UCS Manager GUI インターフェイスはスライダを使用して固定または拡張モジュールのユニファイド ポートのポート モードを設定するので、ポート モードをユニファイド ポートにどのように割り当てることができるかを制限する次の制限が自動的に適用されます。 Cisco UCS Manager CLI インターフェイスを使用する場合は、これらの制約事項はトランザクションをシステム設定にコミットする場合に適用されます。 ポート モードの設定が次の制限事項に違反する場合、Cisco UCS Manager CLI にエラーが表示されます。

- イーサネット ポートはブロックにグループ化する必要があります。 モジュール（固定または拡張）ごとに、イーサネット ポート ブロックは最初のポートから開始し、偶数番号ポートで終了する必要があります。
- ファイバ チャネル ポートはブロックにグループ化する必要があります。 モジュール（固定または拡張）ごとに、ファイバ チャネル ポート ブロック内の最初のポートは最後のイーサネット ポートの後に続き、モジュールにポートの残りを含めるように拡張する必要があります。 ファイバ チャネル ポートだけを含む設定では、ファイバ チャネル ブロックは、固定または拡張モジュールの最初のポートから開始する必要があります。
- イーサネット ポートおよびファイバ チャネル ポートを交互にすることは単一モジュールではサポートされていません。

有効な設定の例：イーサネット ポート モードに設定された固定モジュールでユニファイド ポート 1 ～ 16 およびファイバ チャネル ポート モードでポート 17 ～ 32 を含む場合があります。 拡張モジュールではポート 1 ～ 4 をイーサネット ポート モードで設定してから、ポート 5 ～ 16 をファイバ チャネル モードで設定できます。 このポート配列では個々の各モジュールの規定に適合し

ているため、イーサネットおよびファイバ チャネル ポート タイプを交互にすることに関する規則には違反しません。

無効な設定の例：ポート 16 から始まるファイバ チャネル ポートのブロックを含む場合があります。 ポートの各ブロックは奇数ポートから開始する必要があるため、ポート 17 でブロックを開始する必要があります。

（注） 各ファブリック インターコネクト上で設定できるアップリンク イーサネット ポートおよびアップリンク イーサネット ポート チャネル メンバの総数は 31 に制限されます。 この制限は、拡張モジュールで設定されたアップリンク イーサネット ポートおよびアップリンク イーサネット ポート チャネル メンバを含みます。

ユニファイド アップリンク ポートとユニファイド ストレージ ポート設定時の注意事項および注意

次に示すのは、ユニファイド アップリンク ポートおよびユニファイド ストレージ ポートを使用中に従うべき注意と注意事項です。

- ユニファイドアップリンク ポートでは、SPAN 送信元として一方のコンポーネントをイネーブルにすると、他方のコンポーネントは自動的に、SPAN 送信元になります。

  （注） イーサネット アップリンク ポートで SPAN 送信元を作成または削除すると、Cisco UCS Manager は FCoE アップリンク ポートに SPAN 送信元を自動的に作成またはそれを削除します。 FCoE アップリンク ポートに SPAN 送信元を作成すると同様のことが起きます。

- FCoE アップリンク ポートおよびユニファイドアップリンク ポートにはデフォルト以外のネイティブ VLAN を設定する必要があります。 この VLAN は、いずれのトラフィックにも使用されません。 Cisco UCS Manager は既存の fcoe ストレージ ネイティブ VLAN をこの目的に再利用します。 この FCoE ストレージ ネイティブ VLAN は FCoE およびユニファイドアップリンクのネイティブ VLAN として使用されます。
- ユニファイド アップリンク ポートでは、イーサネット アップリンク ポートにデフォルト以外の VLAN を指定しないと、FCoE ストレージ ネイティブ VLAN はユニファイド アップリンク ポートのネイティブ VLAN として割り当てられます。 イーサネット ポートに、ネイティブ VLAN としてデフォルト以外のネイティブ VLAN が指定されていると、これはユニファイド アップリンク ポートには、ネイティブ VLAN として割り当てられます。
- イーサネット ポート チャネル下にメンバ ポートを作成または削除すると、Cisco UCS Manager は FCoE ポート チャネル下で自動的にメンバ ポートを作成または削除します。 FCoE ポート チャネルにメンバ ポートを作成または削除すると同様のことが起きます。
- サーバ ポート、イーサネット アップリンク、FCoE アップリンクまたは FCoE ストレージなどのスタンドアロン ポートとしてイーサネット ポートを設定し、それをイーサネットまた

はFCOポート チャネルのメンバ ポートにすると、Cisco UCS Managerは、このポートをイーサネットおよびFCoEの両方のポート チャネルのメンバに自動的にします。

- サーバアップリンク、イーサネットアップリンク、FCoEアップリンクまたはFCoEストレージのメンバであることからメンバ ポートのメンバーシップを削除すると、Cisco UCS Managerはイーサネット ポート チャネルおよびFCoEポート チャネルから対応するメンバ ポートを削除し新しいスタンドアロン ポートを作成します。
- リリース2.1から以前のリリースのいずれかにCisco UCS Managerをダウングレードする場合、ダウングレードが完了するとすべてのユニファイド アップリンク ポートおよびポート チャネルはイーサネット ポートおよびイーサネット ポート チャネルに変換されます。 同様に、すべてのユニファイド ストレージ ポートがアプライアンス ポートに変換されます。
- ユニファイド アップリンク ポートおよびユニファイド ストレージ ポートの場合は、2つのインターフェイスを作成すると、一度だけライセンスがチェックアウトされます。 いずれかのインターフェイスが有効な間、ライセンスはチェックアウトされたままです。 ライセンスは、ユニファイド アップリンク ポートまたはユニファイド ストレージ ポートの両方のインターフェイスがディセーブルの場合にのみ解放されます。
- Cisco UCS 6100シリーズ ファブリック インターコネクト スイッチは、同じダウンストリーム NPVスイッチに面する1VFまたは1VF POしかサポートできません。

ポート モード変更によるデータ トラフィックへの影響

ポート モードの変更によって、Cisco UCS ドメインのデータ トラフィックへの割り込みが起きる可能性があります。 割り込みの長さと影響を受けるトラフィックは、Cisco UCS ドメインの設定とポート モード変更を行ったモジュールに依存します。

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

ポート モード変更による拡張モジュールへの影響

ポートモード変更を拡張モジュールで行った後で、モジュールがリブートします。 拡張モジュールのポートを通過するすべてのトラフィックは、約1分間モジュールのリブート中に中断されます。

ポート モード影響によるクラスタ設定の固定モジュールへの変更

クラスタ設定には2つのファブリック インターコネクトがあります。 固定モジュールにポート変更を行ったら、ファブリック インターコネクトがリブートします。 データ トラフィックへの影響は、一方が故障したときに他方のファブリック インターコネクトにフェールオーバーするようにサーバ vNICを設定したかどうかに左右されます。

一方のファブリックインターコネクトの拡張モジュールのポートモードを変更し、それがリブートするまで待ってから第2のファブリック インターコネクトのポート モードの変更を行うと、次のようになります。

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

ただし、両方のファブリック インターコネクトの固定モジュールのポート モードを同時に変更すると、ファブリック インターコネクトを通るすべてのデータ トラフィックは、約 8 分間ファブリック インターコネクトがリブートする間、中断されます。

ポート モード影響によるスタンドアロン設定の固定モジュールへの変更

スタンドアロン設定のファブリック インターコネクトは 1 つだけです。 固定モジュールにポート変更を行ったら、ファブリック インターコネクトがリブートします。 ファブリック インターコネクトを通過するすべてのデータ トラフィックは、約 8 分間ファブリック インターコネクトがリブートする間、中断されます。

6248 ファブリック インターコネクトのポート モードの設定

注意 いずれかのモジュールでポート モードを変更すると、データ トラフィックで中断が生じる可能性があります。これは、固定モジュールに変更を行うと、ファブリック インターコネクトのリブートが必要になり、拡張モジュールに変更を行うと、そのモジュールのリブートが必要になるからです。

Cisco UCS ドメインに、ハイアベイラビリティ用にセットアップされたクラスタ設定と、フェールオーバー用に設定されているサービス プロファイルを持つサーバがある場合、トラフィックは他のファブリック インターコネクトにフェールオーバーし、固定モジュールでポート モードが変更されても、データ トラフィックは中断されません。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] 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 [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

ステップ 5 確認メッセージを確認し、次のいずれかをクリックします。

- [Yes]：ポート モードの設定を続行します。
- [No]： モードを設定せずに終了し、適切なメンテナンス ウィンドウを待ちます。

ステップ 6 ポート モードを設定するモジュールを選択するには、次のいずれかのボタンをクリックします。

- Configure Fixed Module
- Configure Expansion Module

ステップ 7 マウスを使用して、モジュールに必要なポート モード設定が表示されるまでバーに沿ってスライダをドラッグします。
以前に設定されたポートのポート モードを変更すると、ポートは未設定の状態に戻ります。

ステップ 8 他方のモジュールのポート モードを設定する必要がある場合は、ステップ 6 および 7 を繰り返します。

ステップ 9 ポート モードの設定を保存するには、[Finish] をクリックします。
ポート モードを設定したモジュールによっては、Cisco UCS ドメインのデータ トラフィックは次のように中断されます。

- 固定モジュール：ファブリック インターコネクトがリブートします。 そのファブリック インターコネクトを通過するすべてのデータ トラフィックが中断されます。 ハイ アベイラビリティを提供し、フェールオーバー用に設定された vNIC を持つサーバを含むクラスタ設定では、トラフィックは他のファブリック インターコネクトにフェールオーバーし、中断は発生しません。

  固定モジュールがリブートするまで、約 8 分かかります。

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

  拡張モジュールがリブートするまで、約 1 分かかります。

次の作業

ポートのポートタイプを設定します。 スライダの上のモジュール表示で任意のポートを右クリックし、そのポートを使用可能なポート タイプに設定できます。

6296 ファブリック インターコネクトのポート モードの設定

注意 いずれかのモジュールでポート モードを変更すると、データ トラフィックで中断が生じる可能性があります。これは、固定モジュールに変更を行うと、ファブリック インターコネクトのリブートが必要になり、拡張モジュールに変更を行うと、そのモジュールのリブートが必要になるからです。

Cisco UCS ドメインに、ハイアベイラビリティ用にセットアップされたクラスタ設定と、フェールオーバー用に設定されているサービス プロファイルを持つサーバがある場合、トラフィックは他のファブリック インターコネクトにフェールオーバーし、固定モジュールでポート モードが変更されても、データ トラフィックは中断されません。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] 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 [General] タブの [Actions] 領域で、[Configure Unified Ports] をクリックします。

ステップ 5 確認メッセージを確認し、次のいずれかをクリックします。

- [Yes]：[Configure Unified Ports] ウィザードが開いてポート モードの設定を続行します。
- [No]： モードを設定せずに終了し、適切なメンテナンス ウィンドウを待ちます。

ステップ 6 [Configure Fixed Module Ports] ページで、次の手順を実行します。

a) マウスを使用して、固定モジュールに必要なポート モード設定が表示されるまでバーに沿ってスライダをドラッグします。

b) ポートにポート タイプを設定する場合は、スライダの上のモジュール表示で任意のポートを右クリックし、そのポートを使用可能なポート タイプに設定できます。

c) 次のいずれかを実行します。

- [Next] をクリックして拡張モジュール 1 のポートのポート モードを設定します。
- 拡張モジュールのポートのポート モードを設定しない場合は、ステップ 9 に進みます。

以前に設定されたポートのポート モードを変更すると、ポートは未設定の状態に戻ります。

ステップ 7 [Configure Expansion Module 1 Ports] ページで、次の手順を実行します。

a) マウスを使用して、拡張モジュールに必要なポート モード設定が表示されるまでバーに沿ってスライダをドラッグします。

b) ポートにポート タイプを設定する場合は、スライダの上のモジュール表示で任意のポートを右クリックし、そのポートを使用可能なポート タイプに設定できます。

c) 次のいずれかを実行します。

- [Next] をクリックして拡張モジュール 2 のポートのポート モードを設定します。
- 残りの拡張モジュールのポートのポート モードを設定しない場合は、ステップ 9 に進みます。

以前に設定されたポートのポート モードを変更すると、ポートは未設定の状態に戻ります。

ステップ 8 拡張モジュール 3 のポート モードを設定する必要がある場合は、ステップ 7 を繰り返します。

ステップ 9 ポート モードの設定を保存するには、[Finish] をクリックします。
ポート モードを設定したモジュールによっては、Cisco UCS ドメインのデータ トラフィックは次のように中断されます。

- 固定モジュール：ファブリック インターコネクトがリブートします。 そのファブリック インターコネクトを通過するすべてのデータ トラフィックが中断されます。 ハイ アベイラビリティを提供し、フェールオーバー用に設定された vNIC を持つサーバを含むクラスタ設定では、トラフィックは他のファブリック インターコネクトにフェールオーバーし、中断は発生しません。

  固定モジュールがリブートするまで、約 8 分かかります。

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

  拡張モジュールがリブートするまで、約 1 分かかります。

ユニファイド ポートのビーコン LED の設定

ビーコン LED を設定する各モジュールに対して次のタスクを実行します。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 ビーコン LED を設定するユニファイド ポートの場所に応じて、次のいずれかをクリックします。

- Fixed Module
- Expansion Module

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

ステップ 5 [Properties] 領域で、[Beacon LED] 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。

- [Off]：すべての物理 LED がオフになります。
- [Eth]：すべてのイーサネット ポートの横にある物理 LED がオンになります。
- [Fc]：すべてのファイバ チャネル ポートの横にある物理 LED がオンになります。

ステップ 6 [Save Changes] をクリックします。

サーバ ポート

サーバ ポートの設定

設定できるのは固定ポートモジュールのサーバポートだけです。 展開モジュールにはサーバポートは含まれません。

このタスクでは、ポートの設定方法を 1 つだけ説明します。 ポートは、右クリック メニューでポートの [General] タブから設定したり、LAN アップリンク マネージャで設定したりすることもできます。

手順

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

ステップ 2 [Equipment] タブで、[Fabric Interconnects] > [*Fabric_Interconnect_Name*] > [Fixed Module] > [Unconfigured Ports] を展開します。

ステップ 3 [Unconfigured Ports] ノードの下の 1 つ以上のポートをクリックします。

ステップ 4 選択したポートをドラッグし、[Server Ports] ノードにドロップします。
ポートはサーバポートとして設定され、未設定のポートのリストから削除され、[Server Ports] ノードに追加されます。

アップリンク イーサネット ポート

アップリンク イーサネット ポートの設定

固定モジュールまたは展開モジュールのアップリンク イーサネット ポートを設定できます。

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

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module

- Expansion Module

ステップ 4 [Unconfigured Ethernet Ports] ノードの下で 1 つ以上のポートをクリックします。
サーバ ポート、アプライアンス ポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。

ステップ 5 選択したポートをドラッグし、[Uplink Ethernet Ports] ノードにドロップします。
ポートはアップリンク イーサネット ポートとして設定され、未設定のポートのリストから削除され、[Uplink Ethernet Ports] ノードに追加されます。

次の作業

必要に応じて、アップリンク イーサネット ポートのデフォルト フロー制御ポリシーおよび管理速度のプロパティを変更します。

アップリンク イーサネット ポートのプロパティの変更

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Uplink Ethernet Ports] ノードで、変更するアップリンク イーサネット ポートをクリックします。

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

ステップ 6 [Actions] 領域の [Show Interface] をクリックします。

ステップ 7 [Properties] 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。

a) （任意） [User Label] フィールドに、ポートを識別するラベルを入力します。

b) [Flow Control Policy] ドロップダウン リストから、受信バッファがいっぱいになったときに、ポートがどのように IEEE 802.3x ポーズ フレームを送受信するか決定するためのフロー制御ポリシーを選択します。

c) [Admin Speed] 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。

- 1Gbps
- 10 Gbps

ステップ 8 [OK] をクリックします。

ファブリック インターコネクトのポートの再設定

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 再設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 再設定するポートを 1 つ以上クリックします。

ステップ 5 選択したポートをドラッグし、該当するノードにドロップします。
ポートは適切なポート タイプとして再設定され、元のノードから削除され、新しいノードに追加されます。

例：アップリンク イーサネット ポートをサーバ ポートとして再設定する

1. [Uplink Ethernet Ports] ノードを展開し、再設定するノードを選択します。
2. ポートをドラッグし、[Server Ports] ノードにドロップします。

ファブリック インターコネクト上のポートのイネーブル化

ファブリック インターコネクトでポートをイネーブルまたはディセーブルにした後、シャーシを再認識するまで少なくとも 1 分間待ちます。 シャーシの再認識の完了が早すぎると、シャーシからのサーバ トラフィックのピニングが、イネーブルまたはディセーブルにしたポートへの変更で更新されない場合があります。

設定されている場合だけ、ポートをイネーブルまたはディセーブルにできます。 ポートが未設定の場合は、enable disable オプションは非アクティブです。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 イネーブルにするポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

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

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

ステップ 6 [Actions] 領域の [Enable Port] をクリックします。

ステップ 7 Cisco UCS Manager GUI から質問が表示されます。 [OK] をクリックします。

ステップ 8 Cisco UCS Manager GUI から確認メッセージが表示されます。

ファブリック インターコネクト上のポートのディセーブル化

ファブリック インターコネクトでポートをイネーブルまたはディセーブルにした後、シャーシを再認識するまで少なくとも 1 分間待ちます。 シャーシの再認識の完了が早すぎると、シャーシからのサーバ トラフィックのピニングが、イネーブルまたはディセーブルにしたポートへの変更で更新されない場合があります。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 イネーブルにするポートの場所に応じて、次のいずれかを展開します。

- Fixed Module

- Expansion Module

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

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

ステップ 6 [Actions] 領域の [Disable Port] をクリックします。

ステップ 7 Cisco UCS Manager GUI から質問が表示されます。 [OK] をクリックします。

ステップ 8 Cisco UCS Manager GUI から確認メッセージが表示されます。

ファブリック インターコネクトのポート設定解除

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定を解除するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 設定を解除するポートのタイプに応じて、次のいずれかを展開します。

- Appliance Ports
- FCoE Storage Ports
- Server Ports
- Storage FC Ports
- Uplink Ethernet Ports
- Uplink FC Ports

ステップ 5 設定解除するポートを 1 つ以上クリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 6 選択したポートを右クリックし、[Unconfigure] ノードを選択します。
ポートは設定が解除されて元のノードから削除され、[Unconfigured Ports] ノードに追加されます。

アプライアンス ポート

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

アプライアンス ポートの設定

固定モジュールまたは展開モジュールにアプライアンス ポートを設定できます。

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

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Unconfigured Ethernet Ports] ノードの下で 1 つ以上のポートをクリックします。
サーバ ポート、アップリンク イーサネット ポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。

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

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

ステップ 7 [Configure as Appliance Port] 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
[Priority] ドロップダウン リスト	このインターフェイスに関連付けられるサーバ設定の品質。 次のいずれかになります。 • [Fc]：このプライオリティは vHBA トラフィックのみに使用します。 • [Platinum]：このプライオリティは vNIC トラフィックのみに使用します。 • [Gold]：このプライオリティは vNIC トラフィックのみに使用します。 • [Silver]：このプライオリティは vNIC トラフィックのみに使用します。 • [Bronze]：このプライオリティは vNIC トラフィックのみに使用します。 • [Best Effort]：このプライオリティを使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。
[Pin Group] ドロップダウン リスト	指定したファブリックおよびポート、またはファブリックおよびポート チャネルへのアプライアンス ピン ターゲットとして使用する LAN ピン グループ。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Network Control Policy] ドロップダウン リスト	このポートと関連付けられるネットワーク制御ポリシー。
[Create Network Control Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。
[Flow Control Policy] ドロップダウン リスト	このポートと関連付けられるフロー制御ポリシー。
[Create Flow Control Policy] リンク	フロー制御ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Admin Speed] フィールド	ポートがリンクされている宛先に一致する必要があるポートのデータ転送速度。 次のいずれかになります。 • 1 Gbps • 10 Gbps • 20 Gbps • 40 Gbps （注） admin の速度は特定のポートについてのみ変更できます。また、すべての速度をすべてのシステムで使用できるわけではありません。 詳細については、ファブリック インターコネクトの『*Hardware Installation Guide*』を参照してください。

ステップ 8 [VLANs] 領域で、次の手順を実行します。

a) [Port Mode] フィールドで、ポート チャネルに使用するモードを選択するために、次のいずれかのオプション ボタンをクリックします。

- [Trunk]：使用する VLAN を選択できる [VLAN] テーブルが Cisco UCS Manager GUI によって表示されます。
- [Access]：[Select VLAN] ドロップダウン リストが Cisco UCS Manager GUI によって表示され、このポート チャネルに関連付ける VLAN を選択できます。

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

b) [Trunk] オプション ボタンをクリックした場合、[VLANs] テーブルの次のフィールドに入力します。

名前	説明
[Select] カラム	使用する VLAN ごとに、このカラムのチェックボックスをオンにします。
[Name] カラム	VLAN の名前。
[Native VLAN] カラム	VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。

c) [access] オプション ボタンをクリックした場合、[Select VLAN] ドロップダウン リストから VLAN を選択します。

ステップ 9 （任意） エンド ポイントを追加するには、[Ethernet Target Endpoint] チェックボックスをオンにして次のフィールドに値を入力します。

名前	説明
[Name] フィールド	エンド ポイントの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[MAC Address] フィールド	エンドポイントの MAC アドレス。

ステップ 10 [OK] をクリックします。
ポートはアプライアンス ポートとして設定され、未設定のポートのリストから削除され、[Appliance Ports] ノードに追加されます。

アプライアンス ポートのプロパティの変更

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 変更するアプライアンス ポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Appliance Ports] を展開します。

ステップ 5 プロパティを変更するアプライアンス ポートをクリックします。

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

ステップ 7 [Actions] 領域の [Show Interface] をクリックします。
[Properties] ダイアログボックスでスクロール バーを使用するか展開して、すべてのフィールドを表示する必要があります。

ステップ 8 [Properties] ダイアログボックスで、次の 1 つ以上のフィールドの値を変更します。

名前	説明
[User Label] フィールド	内部トラッキングまたはカスタマイズした識別に使用できるユーザ定義名。 32 文字まで入力します。`（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）を除く文字やスペースを使用できます。
[Admin Speed] フィールド	ポートがリンクされている宛先に一致する必要があるポートのデータ転送速度。 次のいずれかになります。 • 1 Gbps • 10 Gbps • 20 Gbps • 40 Gbps （注） admin の速度は特定のポートについてのみ変更できます。また、すべての速度をすべてのシステムで使用できるわけではありません。詳細については、ファブリック インターコネクトの『*Hardware Installation Guide*』を参照してください。
[Priority] ドロップダウン リスト	このインターフェイスに関連付けられるサーバ設定の品質。 次のいずれかになります。 • [Fc]：このプライオリティは vHBA トラフィックのみに使用します。 • [Platinum]：このプライオリティは vNIC トラフィックのみに使用します。 • [Gold]：このプライオリティは vNIC トラフィックのみに使用します。 • [Silver]：このプライオリティは vNIC トラフィックのみに使用します。 • [Bronze]：このプライオリティは vNIC トラフィックのみに使用します。 • [Best Effort]：このプライオリティを使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。

名前	説明
[Pin Group] ドロップダウン リスト	指定したファブリックおよびポート、またはファブリックおよびポートチャネルへのアプライアンスピンターゲットとして使用する LAN ピン グループ。
[Network Control Policy] ドロップダウン リスト	このポートと関連付けられるネットワーク制御ポリシー。
[MAC Address] フィールド	エンドポイントの MAC アドレス。 このフィールドが表示されない場合、ポートに設定されたイーサネットターゲットエンドポイントがありません。 エンドポイントを追加するには、[Actions] 領域で[Add Target Ethernet Endpoint] をクリックします。
[Port Mode] フィールド	この領域に表示されるフィールドは、[Port Mode] フィールドの設定によって異なります。 次を選択できます。 • [Trunk]：使用する VLAN を選択できる [VLAN] テーブルが Cisco UCS Manager GUI によって表示されます。 • [Access]：[Select VLAN] ドロップダウン リストが Cisco UCS Manager GUI によって表示され、このポート チャネルに関連付ける VLAN を選択できます。

ステップ 9 [OK] をクリックします。

FCoE ストレージ ポートおよびファイバ チャネル ストレージ ポート

FCoE ストレージ ポートの設定

固定モジュールまたは展開モジュールに FCoE ストレージ ポートを設定できます。

このタスクでは、FCoE ストレージ ポートの設定方法を 1 つだけ説明します。 ポートの [General] タブからも FCoE ストレージ ポートを設定できます。

はじめる前に

これらのポートを有効にするには、ファイバ チャネル スイッチング モードを [Switching] に設定する必要があります。 ストレージ ポートはエンドホスト モードでは動作できません。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Unconfigured Ethernet Ports] ノードの下で 1 つ以上のポートをクリックします。
アップリンク イーサネット ポート、サーバ ポート、またはアプライアンス ポートを再設定する場合は、適切なノードを展開します。

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

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

ステップ 7 [OK] をクリックします。
ポートはFCoEストレージポートとして設定され、未設定のポートのリストから削除され、[FCoE Storage Ports] ノードに追加されます。

ファイバ チャネル ストレージ ポートの設定

このタスクでは、FC ストレージ ポートの設定方法を 1 つだけ説明します。 ポートの [General] タブからも FC ストレージ ポートを設定できます。

はじめる前に

これらのポートを有効にするには、ファイバ チャネル スイッチング モードを [Switching] に設定する必要があります。 ストレージ ポートはエンドホスト モードでは動作できません。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [Expansion Module] ノードを展開します。

ステップ 4 [Uplink FC Ports] ノードの下で 1 つ以上のポートをクリックします。

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

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

ステップ 7 [OK] をクリックします。

ポートはFCストレージポートとして設定され、アップリンクFCポートのリストから削除され、[FC Storage Ports] ノードに追加されます。

アップリンク ファイバ チャネル ポートの復元

このタスクでは、アップリンクFCポートとして機能するFCストレージポートの復元方法を1つだけ説明します。 ポートの [General] タブから FC ストレージ ポートを再設定することもできます。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [Expansion Module] ノードを展開します。

ステップ 4 [Storage FC Ports] ノードの下で 1 つ以上のポートをクリックします。

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

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

ステップ 7 [OK] をクリックします。
ポートはアップリンクFCポートとして設定され、FCストレージポートのリストから削除され、[Uplink FC Ports] ノードに追加されます。

FCoE アップリンク ポート

FCoE アップリンク ポートは FCoE トラフィックの伝送に使用される、ファブリック インターコネクトとアップストリームイーサネットスイッチ間の物理イーサネットインターフェイスです。このサポートを使用すると同じ物理イーサネット ポートで、イーサネット トラフィックおよびファイバ チャネル トラフィックの両方を伝送できます。

FCoE アップリンク ポートはファイバ チャネル トラフィックに FCoE プロトコルを使用してアップストリーム イーサネット スイッチに接続されます。 これは、同じ物理イーサネット リンクでファイバ チャネルとイーサネットの両方のトラフィックが流れることを可能にします。

（注） FCoE アップリンクおよびユニファイド アップリンクは、ディストリビューション レイヤ スイッチまでユニファイドファブリックを拡張してFCoEマルチホップ機能をイネーブルにします。

次のいずれかと同じイーサネット ポートを設定できます。

- **FCoE アップリンク ポート**：ファイバ チャネル トラフィック専用の FCoE アップリンク ポートとして。
- **アップリンク ポート**：イーサネット トラフィック専用のイーサネット ポートとして。
- **ユニファイドアップリンク ポート**：イーサネットおよびファイバチャネル両方のトラフィックを伝送するユニファイド アップリンク ポートとして。

FCoE アップリンク ポートの設定

固定モジュールまたは拡張モジュールの FCoE アップリンク ポートを設定できます。 このタスクでは、FCoE アップリンク ポートの設定方法を 1 つだけ説明します。 FCoE アップリンク ポートは、右クリックメニューから設定したり、ポートの [General] タブから設定したりすることもできます。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Ethernet Ports] ノードの下で、いずれかの [Unconfigured] ポートを選択します。

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

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

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

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

ステップ 9 Cisco UCS Manager GUI から成功メッセージが表示されます。 [Properties] 領域で、[Role] が [Fcoe Uplink] に変更されます。

ステップ 10 （任意）[Properties] 領域で、[VSAN] フィールドを指定します。

ユニファイド ストレージ ポート

ユニファイド ストレージでは、イーサネット ストレージ インターフェイスおよび FCoE ストレージ インターフェイスと同じ物理ポートを設定しています。 固定モジュールまたは拡張モジュールでユニファイド ストレージ ポートとして任意のアプライアンス ポートまたは FCoE ストレージ

ポートを設定できます。ユニファイドストレージポートを設定するには、ファブリックインターコネクトがファイバ チャネル スイッチング モードである必要があります。

ユニファイド ストレージ ポートでは、個々の FCoE ストレージ インターフェイスまたはアプライアンス インターフェイスをイネーブル/ディセーブルにすることができます。

- ユニファイド ストレージ ポートでは、アプライアンス ポートにデフォルト以外の VLAN を指定しないと、fcoe ストレージ ネイティブ VLAN はユニファイド ストレージ ポートのネイティブ VLAN として割り当てられます。 アプライアンス ポートに、ネイティブ VLAN としてデフォルト以外のネイティブ VLAN が指定されていると、これはユニファイド ストレージ ポートには、ネイティブ VLAN として割り当てられます。
- アプライアンスインターフェイスをイネーブルまたはディセーブルにすると、対応する物理ポートがイネーブルまたはディセーブルになります。 したがって、ユニファイド ストレージのアプライアンス インターフェイスをディセーブルにすると、FCoE ストレージがイネーブルになっていても、物理ポートに対してダウン状態になります。
- FCoE ストレージ インターフェイスをイネーブルまたはディセーブルにすると、対応する VFC がイネーブルまたはディセーブルになります。 したがって、FCoE ストレージのインターフェイスがユニファイド ストレージ ポートでディセーブルの場合、アプライアンス インターフェイスは正常に機能し続けます。

ユニファイド ストレージ ポートとしてアプライアンス ポートを設定

アプライアンス ポートまたは FCoE ストレージ ポートからユニファイド ストレージ ポートを設定できます。 未設定ポートからユニファイド ストレージ ポートを設定することもできます。 未設定ポートから始める場合、ポートへアプライアンスまたは FCoE ストレージの設定を割り当ててから、ユニファイドストレージポートとしてイネーブルにするために別の設定を追加します。

重要 FI が FC スイッチング モードであることを確認してください。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Ethernet Ports] ノードの下で、アプライアンス ポートとしてすでに設定されているいずれかのポートを選択します。
[Work] ペインの [General] タブの下で、[Properties] 領域の [Role] に [Nas Storage] と表示されます。

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

ステップ 6 ドロップダウンのオプションから、[Configure as FCoE Storage Port] を選択します。

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

ステップ 8 Cisco UCS Manager GUI から成功メッセージが表示されます。 [Properties] 領域で、[Role] が [Unified Storage] に変更されます。

ユニファイド ストレージ ポートの設定解除

ユニファイド接続ポートから両方の設定を設定解除および削除できます。 あるいはFCoEストレージ ポート設定またはアプライアンス ストレージ ポート設定のいずれか一方を設定解除して、他方をポートに保持できます。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定を解除するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Ethernet Ports] ノードの下で、設定解除するポートを選択します。

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

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

- Unconfigure FCoE Storage Port
- Unconfigure Appliance Port
- Unconfigure both

ステップ 7 設定解除オプションの 1 つを選択します。

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

ステップ 9 Cisco UCS Manager GUI から成功メッセージが表示されます。 [Properties] 領域で、[Role] が設定解除の選択に基づいて変更されます。

ユニファイド アップリンク ポート

同じ物理イーサネット ポートにイーサネット アップリンクおよび FCoE アップリンクを設定すると、それはユニファイドアップリンク ポートと呼ばれます。 個別に FCoE インターフェイスまたはイーサネット インターフェイスを独立してイネーブルまたはディセーブルにできます。

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

イーサネットアップリンクをディセーブルにすると、ユニファイドアップリンクの基礎となる物理ポートがディセーブルになります。 したがって、FCoE アップリンクがイネーブルになっていても、FCoE アップリンクもダウン状態になります。 ただし、FCoE アップリンクをディセーブルにすると、VFC だけがダウンします。 イーサネットアップリンクがイネーブルの場合、それは引き続きユニファイド アップリンク ポートで正しく機能することができます。

ユニファイド アップリンク ポートの設定

次のいずれかからユニファイド アップリンク ポートを設定できます。

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

このプロセスでは、既存の FCoE アップリンク ポートからユニファイドアップリンク ポートを設定する 1 つの方法について説明します。 固定モジュールまたは拡張モジュールのユニファイド アップリンク ポートを設定できます。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

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

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

ステップ 6 [Properties] 領域で、[Role] に [Fcoe Uplink] と表示されていることを確認します。

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

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

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

ステップ 10 Cisco UCS Manager GUI から成功メッセージが表示されます。 [Properties] 領域で、[Role] が [Unified Uplink] に変更されます。

ステップ 11 （任意）[Properties] 領域で、[VSAN] フィールドを指定します。

ユニファイド アップリンク ポートの設定解除

ユニファイドアップリンク ポートから両方の設定を設定解除および削除できます。 あるいはFCoEポート設定またはイーサネット ポート設定のいずれか一方を設定解除して、他方をポートに保持できます。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定を解除するポートの場所に応じて、次のいずれかを展開します。

- Fixed Module
- Expansion Module

ステップ 4 [Ethernet Ports] ノードの下で、設定解除するポートを選択します。

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

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

- Unconfigure FCoE Uplink Port
- Unconfigure Uplink Port
- Unconfigure both

ステップ 7 設定解除オプションの 1 つを選択します。

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

ステップ 9 Cisco UCS Manager GUI から成功メッセージが表示されます。 [Properties] 領域で、[Role] が設定解除の選択に基づいて変更されます。

ステップ 10 [Save Changes] をクリックします。

アップリンク イーサネット ポート チャネル

アップリンク イーサネット ポート チャネルでは、1 つの論理イーサネット リンクを作成して耐障害性と高速接続を提供するために、複数の物理アップリンク イーサネット ポートをグループ化（リンク集約）することができます。 Cisco UCS Manager において、先にポート チャネルを作成してから、そのポート チャネルにアップリンク イーサネット ポートを追加します。 1 つのポート チャネルには、最大で 8 個のアップリンク イーサネット ポートを追加できます。

（注） Cisco UCS Cisco UCS では、ポート集約プロトコル（PAgP）ではなく、Link Aggregation Control Protocol（LACP）を使用して、アップリンク イーサネット ポートがポート チャネルにグループ化されます。 アップストリーム スイッチのポートが LACP に設定されていない場合、ファブリック インターコネクトは、アップリンク イーサネット ポート チャネルのすべてのポートを個々のポートとして処理し、したがってパケットを転送します。

アップリンク イーサネット ポート チャネルの作成

手順

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

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

ステップ 3 ポート チャネルを追加するファブリック インターコネクトのノードを展開します。

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

ステップ 5 [Create Port Channel] ウィザードの [Set Port Channel Name] 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
[ID] フィールド	ポート チャネルの ID。 1 ～ 256 の整数を入力します。 ポート チャネルが保存された後、この ID を変更することはできません。

名前	説明
[Name] フィールド	ポート チャネルのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 6 [Create Port Channel] ウィザードの [Add Ports] ページで、次の手順を実行します。

a) [Ports] テーブルで、ポート チャネルに含める 1 つ以上のポートを選択します。

b) [>>] ボタンをクリックして、[Ports in the port channel] テーブルにポートを追加します。
ポート チャネルからポートを削除するには、[<<] ボタンを使用できます。

（注） Cisco UCS Manager サーバ ポートとして設定済みのポートを選択した場合、Cisco UCS Manager で警告が表示されます。 ダイアログボックスの [Yes] をクリックして、このポートをアップリンク イーサネット ポートとして再設定し、ポート チャネルに含めることができます。

ステップ 7 [Finish] をクリックします。

アップリンク イーサネット ポート チャネルのイネーブル化

手順

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

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

ステップ 3 イネーブルにするポートチャネルが含まれるファブリックインターコネクトのノードを展開します。

ステップ 4 [Port Channels] ノードを展開します。

ステップ 5 イネーブルにするポート チャネルを右クリックし、[Enable Port Channel] を選択します。

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

アップリンク イーサネット ポート チャネルのディセーブル化

手順

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

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

ステップ 3 ディセーブルにするポートチャネルが含まれるファブリックインターコネクトのノードを展開します。

ステップ 4 [Port Channels] ノードを展開します。

ステップ 5 ディセーブルにするポート チャネルを右クリックし、[Enable Port Channel] を選択します。

アップリンク イーサネット ポート チャネルへのポートの追加および削除

手順

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

ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] > [*Fabric*] > [Port Channels] を展開します。

ステップ 3 ポートを追加または削除するポート チャネルをクリックします。

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

ステップ 5 [Actions] 領域の [Add Ports] をクリックします。

ステップ 6 [Add Ports] ダイアログボックスで、次のいずれかの手順を実行します。

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

ステップ 7 [OK] をクリックします。

アップリンク イーサネット ポート チャネルの削除

手順

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

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

ステップ 3 ポート チャネルを削除するファブリック インターコネクトのノードを展開します。

ステップ 4 [Port Channels] ノードをクリックします。

ステップ 5 [Port Channels] ノードの [General] タブで、削除するポート チャネルを選択します。

ステップ 6 ポート チャネルを右クリックし、[Delete] を選択します。

アプライアンス ポート チャネル

アプライアンス ポート チャネルでは、1 つの論理イーサネット ストレージ リンクを作成して耐障害性と高速接続を提供するために、複数の物理アプライアンス ポートをグループ化することができます。 Cisco UCS Manager において、先にポート チャネルを作成してから、そのポート チャネルにアプライアンス ポートを追加します。 1 つのポート チャネルには、最大で 8 個のアプライアンス ポートを追加できます。

アプライアンス ポート チャネルの作成

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Appliances] を展開します。

ステップ 3 ポート チャネルを追加するファブリック インターコネクトのノードを展開します。

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

ステップ 5 [Create Port Channel] ウィザードの [Set Port Channel Name] ページで、次のフィールドに値を入力して、ポート チャネルの ID とその他のプロパティを指定します。

名前	説明
[ID] フィールド	ポート チャネルの固有識別情報。 1 ～ 256 の整数を入力します。 ポート チャネルが保存された後、この ID を変更することはできません。

名前	説明
[Name] フィールド	ポート チャネルのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Priority] ドロップダウン リスト	このインターフェイスに関連付けられるサーバ設定の品質。 次のいずれかになります。 • [Fc]：このプライオリティは vHBA トラフィックのみに使用します。 • [Platinum]：このプライオリティは vNIC トラフィックのみに使用します。 • [Gold]：このプライオリティは vNIC トラフィックのみに使用します。 • [Silver]：このプライオリティは vNIC トラフィックのみに使用します。 • [Bronze]：このプライオリティは vNIC トラフィックのみに使用します。 • [Best Effort]：このプライオリティを使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。
[Protocol] フィールド	ポート チャネルのプロトコル。 次のいずれかになります。 • Static • Lacp
[Pin Group] ドロップダウン	このポート チャネルと関連付けられる LAN ピン グループ。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Network Control Policy] ドロップダウン リスト	このポート チャネルと関連付けられるネットワーク制御ポリシー。
[Create Network Control Policy] リンク	すべてのポート チャネルに使用可能なグローバル ネットワーク制御ポリシーを作成するには、このリンクをクリックします。

名前	説明
[Flow Control Policy] ドロップダウン リスト	このポート チャネルと関連付けられるフロー制御ポリシー。
[Create Flow Control Policy] リンク	すべてのポートチャネルに使用可能なグローバルフロー制御ポリシーを作成するには、このリンクをクリックします。

ステップ 6 [VLANs] 領域で、次の手順を実行します。

a) [Port Mode] フィールドで、ポート チャネルに使用するモードを選択するために、次のいずれかのオプション ボタンをクリックします。

- [Trunk]：使用する VLAN を選択できる [VLAN] テーブルが Cisco UCS Manager GUI によって表示されます。
- [Access]：[Select VLAN] ドロップダウン リストが Cisco UCS Manager GUI によって表示され、このポート チャネルに関連付ける VLAN を選択できます。

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

b) [Trunk] オプション ボタンをクリックした場合、[VLANs] テーブルの次のフィールドに入力します。

名前	説明
[Select] カラム	使用する VLAN ごとに、このカラムのチェックボックスをオンにします。
[Name] カラム	VLAN の名前。
[Native VLAN] カラム	VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。

c) [access] オプション ボタンをクリックした場合、[Select VLAN] ドロップダウン リストから VLAN を選択します。

ステップ 7 （任意） エンド ポイントを追加するには、[Ethernet Target Endpoint] チェックボックスをオンにして次のフィールドに値を入力します。

名前	説明
[Name] フィールド	エンド ポイントの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[MAC Address] フィールド	エンドポイントの MAC アドレス。

ステップ 8 [Next] をクリックします。

ステップ 9 [Create Port Channel] ウィザードの [Add Ports] ページで、次の手順を実行します。

a) [Ports] テーブルで、ポート チャネルに含める 1 つ以上のポートを選択します。

b) [>>] ボタンをクリックして、[Ports in the port channel] テーブルにポートを追加します。
ポート チャネルからポートを削除するには、[<<] ボタンを使用できます。

（注） Cisco UCS Manager Cisco UCS Manager で、設定によってサービス プロファイルまたはポート設定に問題が起きる可能性がある場合に警告が表示されます。 これらの潜在的な問題にかかわらずポート チャネルを作成する場合は、ダイアログボックスで [Yes] をクリックできます。

ステップ 10 [Finish] をクリックします。

アプライアンス ポート チャネルのイネーブル化

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Appliances] を展開します。

ステップ 3 イネーブルにするポートチャネルが含まれるファブリックインターコネクトのノードを展開します。

ステップ 4 [Port Channels] ノードを展開します。

ステップ 5 イネーブルにするポート チャネルを右クリックし、[Enable Port Channel] を選択します。

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

アプライアンス ポート チャネルのディセーブル化

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Appliances] を展開します。

ステップ 3 ディセーブルにするポートチャネルが含まれるファブリックインターコネクトのノードを展開します。

ステップ 4 [Port Channels] ノードを展開します。

ステップ 5 ディセーブルにするポート チャネルを右クリックし、[Disable Port Channel] を選択します。

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

アプライアンス ポート チャネルへのポートの追加および削除

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Appliances] > [*Fabric*] > [Port Channels] を展開します。

ステップ 3 ポートを追加または削除するポート チャネルをクリックします。

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

ステップ 5 [Actions] 領域の [Add Ports] をクリックします。

ステップ 6 [Add Ports] ダイアログボックスで、次のいずれかの手順を実行します。

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

ステップ 7 [OK] をクリックします。

アプライアンス ポート チャネルの削除

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Appliances] を展開します。

ステップ 3 イネーブルにするポートチャネルが含まれるファブリックインターコネクトのノードを展開します。

ステップ 4 [Port Channels] ノードを展開します。

ステップ 5 イネーブルにするポート チャネルを右クリックし、[Disable Port Channel] を選択します。

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

ファイバ チャネル ポート チャネル

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

各 Cisco UCS ドメインに最大 4 個のファイバ チャネル ポート チャネルを作成できます。 各ファイバ チャネル ポート チャネルには最大 16 のアップリンク ファイバ チャネル ポートを含めることができます。

ファイバ チャネル ポート チャネルの作成

手順

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

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

ステップ 3 ポート チャネルを作成するファブリックのノードを展開します。

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

ステップ 5 [Create Port Channel] ウィザードの [Set Port Channel Name] 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
[ID] フィールド	ポート チャネルの ID。 1 ～ 256 の整数を入力します。 ポート チャネルが保存された後、この ID を変更することはできません。
[Name] フィールド	ポート チャネルのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 6 [Create Port Channel] ウィザードの [Add Ports] ページで、次の手順を実行します。

a) [Port Channel Admin Speed] ドロップダウン リストで、ポート チャネルのトラフィックに次のいずれかのデータ転送速度を選択します。

- 1 Gbps
- 2 Gbps
- 4 Gbps
- 8 Gbps
- [Auto]：データ転送速度がCisco UCS判断されます。

b) [Ports] テーブルで、ポート チャネルに含める 1 つ以上のポートを選択します。

c) [>>] ボタンをクリックして、[Ports in the port channel] テーブルにポートを追加します。
ポート チャネルからポートを削除するには、[<<] ボタンを使用できます。

ステップ 7 [Finish] をクリックします。

ファイバ チャネル ポート チャネルのイネーブル化

手順

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

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

ステップ 3 イネーブルにするポート チャネルをクリックします。

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

ステップ 5 [Actions] 領域の [Enable Port Channel] をクリックします。

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

ファイバ チャネル ポート チャネルのディセーブル化

手順

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

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

ステップ 3 ディセーブルにするポート チャネルをクリックします。

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

ステップ 5 [Actions] 領域の [Disable Port Channel] をクリックします。

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

ファイバ チャネル ポート チャネルへのポートの追加および削除

手順

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

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

ステップ 3 ポートを追加または削除するポート チャネルをクリックします。

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

ステップ 5 [Actions] 領域の [Add Ports] をクリックします。

ステップ 6 [Add Ports] ダイアログボックスで、次のいずれかの手順を実行します。

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

ステップ 7 [OK] をクリックします。

ファイバ チャネル ポート チャネルのプロパティの変更

（注） 2 つのファイバ チャネル ポート チャネルを接続する場合、リンクが機能するためには両方のポート チャネルの管理速度が一致する必要があります。 1 つまたは両方のファイバ チャネル ポート チャネルの管理速度が自動に設定されている場合、Cisco UCS は管理速度を自動的に調整します。

手順

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

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

ステップ 3 変更するポート チャネルをクリックします。

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

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

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

ステップ 6 [Save Changes] をクリックします。

ファイバ チャネル ポート チャネルの削除

手順

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

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

ステップ 3 削除するポート チャネルを右クリックし、[Delete] を選択します。

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

FCoE ポート チャネル

FCoE ポート チャネルでは、1 個の FCoE 論理ポート チャネルを作成するために複数の物理 FCoE ポートをグループ化することができます。 物理レベルでは、FCoE ポート チャネルはイーサネット ポート チャネルで FCoE トラフィックを伝送します。 したがって、一連のメンバで構成される FCoE ポート チャネルは基本的には同じメンバを持つイーサネット ポート チャネルです。 このイーサネット ポート チャネルは、FCoE トラフィックの物理的な伝送に使用されます。

各 FCoE ポート チャネルについては、Cisco UCS Manager が VFC を内部的に作成し、イーサネット ポート チャネルにバインドします。 ホストから受信した FCoE トラフィックは、FCoE トラフィックが FC アップリンクで送信されるのと同じ方法により VFC で送信されます。

FCoE ポート チャネルの作成

手順

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

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

ステップ 3 ポート チャネルを作成するファブリックのノードを展開します。

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

ステップ 5 [Create FCoE Port Channel] ウィザードの [Set Port Channel Name] 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
[ID] フィールド	ポート チャネルの ID。 1 ～ 256 の整数を入力します。 ポート チャネルが保存された後、この ID を変更することはできません。
[Name] フィールド	ポート チャネルのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 6 [Create FCoE Port Channel] ウィザードの [Add Ports] ページで、次の手順を実行します。

a) [Ports] テーブルで、ポート チャネルに含める 1 つ以上のポートを選択します。

b) [>>] ボタンをクリックして、[Ports in the port channel] テーブルにポートを追加します。
ポート チャネルからポートを削除するには、[<<] ボタンを使用できます。

ステップ 7 [Finish] をクリックします。

FCoE ポート チャネルの削除

手順

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

ステップ 2 [SAN] タブで、[SAN] [SAN Cloud] [*Fabric*] [FCoE Port Channels] を展開します。

ステップ 3 削除するポート チャネルを右クリックし、[Delete] を選択します。

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

ユニファイド アップリンク ポート チャネル

同じ ID でイーサネット ポート チャネルおよび FCoE ポート チャネルを作成すると、それはユニファイド ポート チャネルと呼ばれます。 ユニファイド ポート チャネルが作成されると、物理イーサネット ポート チャネルおよび VFC が、指定されたメンバでファブリック インターコネクトに作成されます。 物理イーサネット ポート チャネルはイーサネット トラフィックと FCoE ト

ラフィックの両方を伝送するのに使用されます。 VFC はイーサネット ポート チャネルに FCoE トラフィックをバインドします。

次の規則はユニファイド アップリンク ポート チャネルのメンバ ポート セットに適用されます。

- ユニファイド ポート チャネルとして設定されている、同じ ID のイーサネット ポート チャネルおよび FCoE ポート チャネルは、同じメンバ ポート セットを持つ必要があります。
- イーサネット ポート チャネルにメンバ ポート チャネルを追加すると、Cisco UCS Manager は FCoE ポート チャネルにも同じポート チャネルを追加します。 同様に、FCoE ポート チャネルにメンバを追加すると、イーサネット ポート チャネルにそのメンバ ポートを追加します。
- ポート チャネルの 1 つからメンバ ポートを削除すると、Cisco UCS Manager は他のポート チャネルから自動的にそのメンバ ポートを削除します。

イーサネット アップリンク ポート チャネルをディセーブルにすると、ユニファイド アップリンク ポート チャネルの基礎となる物理ポート チャネルがディセーブルになります。 したがって、FCoE アップリンクがイネーブルになっていても、FCoE アップリンク ポート チャネルもダウン状態になります。 ただし、FCoE アップリンク ポート チャネルをディセーブルにすると、VFC だけがダウンします。 イーサネット アップリンク ポート チャネルがイネーブルの場合、それは引き続きユニファイド アップリンク ポート チャネルで正しく機能することができます。

アダプタ ポート チャネル

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

アダプタ ポート チャネルは Cisco UCS Manager が正しいハードウェアの存在を検出すると内部的に作成され管理されます。 アダプタ ポート チャネルは手動で設定できません。 アダプタ ポート チャネルは、Cisco UCS Manager GUI または Cisco UCS Manager CLI を使用して、表示できます

アダプタ ポート チャネルの表示

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > *[Chassis_Number]* > [Servers] > *[Server_Number]* > [Interface Cards] を展開します。

ステップ 3 アダプタ ポート チャネルを表示するアダプタをクリックします。

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

ステップ 5 アダプタ ポート チャネルの詳細を表示するには、[Port Channel] カラムのリンクをクリックします。

ファブリック ポート チャネル

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

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

- シャーシのディスカバリ中に、シャーシディスカバリ ポリシーに設定されている設定に従って。
- シャーシのディスカバリ後に、特定のシャーシのシャーシ接続ポリシーで設定されている設定に従って。

各IOMに、ファブリック ポート チャネルが1つあります。 ファブリック インターコネクトにIOMを接続する各アップリンクは個々のリンクとして設定するか、ポートチャネルに含めることができますが、アップリンクは複数のファブリックポートチャネルに属することができません。たとえば、2つのIOMを持つシャーシが検出されたときに、ファブリック ポートチャネルを作成するようにシャーシ ディスカバリ ポリシーが設定されている場合、Cisco UCS Managerは2つの別個のファブリックポートチャネルを作成します。一方はIOM-1を接続するアップリンク用で、もう一方はIOM-2を接続するアップリンク用です。 その他のシャーシがこれらのファブリック ポート チャネルに加入することはできません。 同様に、IOM-1のファブリック ポート チャネルに属するアップリンクはIOM-2のファブリック ポート チャネルに加入できません。

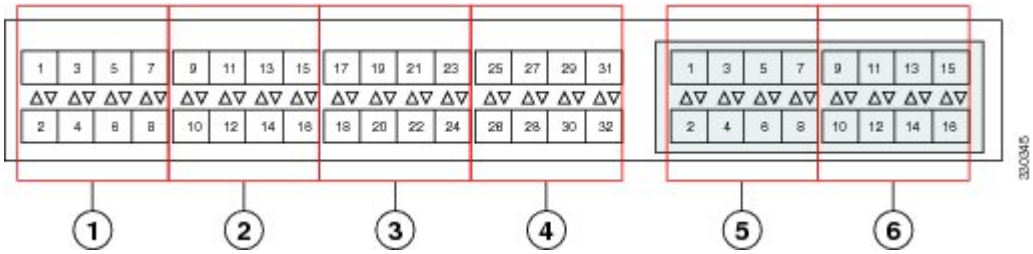
ファブリック ポート チャネルのケーブル接続の問題

Cisco UCS 2200シリーズIOMとCisco UCS 6200シリーズ ファブリック インターコネクト間のリンクをポートチャネルモードで設定した場合、アダプタの使用可能なVIF名前空間はIOMのアップリンクがファブリック インターコネクト ポートに接続されている場所によって異なります。

6248ファブリック インターコネクト内には、連続する8個のポートが6セットあり、それぞれのポートセットは単一チップで管理されます。 IOMからのアップリンクがすべて単一チップで管理されるポートセットに接続されるようにアップリンクが接続されているときに、Cisco UCS Managerはシャーシ内のブレードに導入されたサービス プロファイルで使用されるVIFの数を最大化しま

す。 IOM からのアップリンク接続が個別のチップで管理される複数のポートに分散している場合、VIF の数は少なくなります。

図 *1*：ファブリック ポート チャネルのポート グループ



注意 ファブリック ポート チャネルからリンクを削除または追加すると、中断して、VIF 名前空間の使用可能な量に影響を及ぼすことがあります。

ハイ アベイラビリティ クラスタ モードのアプリケーションの場合、対称のケーブル接続設定を強く推奨します。 ケーブル接続が非対称の場合、使用可能な VIF の最大数は 2 つのケーブル接続設定のうち少ない方になります。

Cisco UCS 環境の VIF の最大数の詳細については、ハードウェアおよびソフトウェア設定の設定制限に関するマニュアルを参照してください。

ファブリック ポート チャネルの設定

手順

ステップ 1 シャーシディスカバリの実行中に、IOMからファブリックインターコネクトへのすべてのリンクをファブリック ポート チャネルに含めるには、シャーシ ディスカバリ ポリシーのリンク グループ化プリファレンスをポート チャネルに設定します。
シャーシ ディスカバリ ポリシーの設定, （210 ページ）

ステップ 2 シャーシ ディスカバリの実行中に、個々のシャーシからのリンクをファブリック ポート チャネルに含めるには、シャーシ接続ポリシーのリンク グループ化プリファレンスをポートチャネルに設定します。
シャーシ接続ポリシーの設定, （212 ページ）

ステップ 3 シャーシ検出後、追加のファブリック ポートチャネル メンバ ポートをイネーブルまたはディセーブルにします。
ファブリック ポート チャネル メンバ ポートのイネーブル化またはディセーブル化, （119 ページ）

次の作業

シャーシ ディスカバリ ポリシーまたはシャーシ接続ポリシーに変更を加えた後でファブリック ポート チャネルからシャーシのリンクを削除または追加するには、シャーシを再認識します。シャーシの再認識は、ファブリック ポート チャネルからシャーシのメンバ ポートをイネーブルまたはディセーブルにする場合には必要はありません

ファブリック ポート チャネルの表示

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [IO Modules] を展開します。

ステップ 3 ファブリック ポート チャネルを表示する IOM をクリックします。

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

ステップ 5 ファブリック ポート チャネルの詳細を表示するには、[Port Channel] カラムのリンクをクリックします。

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

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Internal LAN] > [*Fabric*] > [Port Channels] を展開します。

ステップ 3 メンバ ポートをイネーブルまたはディセーブルにするポート チャネルを展開します。

ステップ 4 メンバポートをイネーブルまたはディセーブルにするイーサネットインターフェイスをクリックします。

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

ステップ 6 [Actions] 領域で、次のいずれかをクリックします。

- Enable Interface
- Disable Interface

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

Internal Fabric Manager を使用したサーバ ポートの設定

Internal Fabric Manager

Internal Fabric Manager は、Cisco UCS ドメインのファブリック インターコネクトに対してサーバ ポートを設定できる単一インターフェイスを提供します。 Internal Fabric Manager には、そのファブリック インターコネクトの [General] タブからアクセスできます。

Internal Fabric Manager で行うことができる設定の一部は、[Equipment] タブ、[LAN] タブ、または LAN アップリンク マネージャのノードでも行うことができます。

Internal Fabric Manager の起動

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [Fixed Module] をクリックします。

ステップ 4 [Work] ペインで、[Actions] 領域の [Internal Fabric Manager] をクリックします。
別のウィンドウで Internal Fabric Manager が開きます。

Internal Fabric Manager を使用したサーバ ポートの設定

手順

ステップ 1 Internal Fabric Manager で、下矢印をクリックして [Unconfigured Ports] 領域を展開します。

ステップ 2 設定するポートを右クリックし、[Configure as Server Port] を選択します。

ステップ 3 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 4 Internal Fabric Manager で、すべてのタスクが完了したら、[OK] をクリックします。

Internal Fabric Manager を使用したサーバ ポートの設定解除

手順

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバ ポートをクリックします。

ステップ 2 [Unconfigure Port] をクリックします。

ステップ 3 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 4 Internal Fabric Manager で、すべてのタスクが完了したら、[OK] をクリックします。

Internal Fabric Manager を使用したサーバ ポートのイネーブル化

手順

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバ ポートをクリックします。

ステップ 2 [Enable Port] をクリックします。

ステップ 3 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 4 Internal Fabric Manager で、すべてのタスクが完了したら、[OK] をクリックします。

Internal Fabric Manager を使用したサーバ ポートのディセーブル化

手順

ステップ 1 [Internal Fabric Manager] で、[Server Ports] テーブルのサーバ ポートをクリックします。

ステップ 2 [Disable Port] をクリックします。

ステップ 3 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 4 Internal Fabric Manager で、すべてのタスクが完了したら、[OK] をクリックします。

第 7 章

通信サービスの設定

この章の内容は、次のとおりです。

- 通信サービス，123 ページ
- CIM-XML の設定，125 ページ
- HTTP の設定，125 ページ
- HTTPS の設定，126 ページ
- SNMP の設定，133 ページ
- Telnet のイネーブル化，142 ページ
- 通信サービスのディセーブル化，142 ページ

通信サービス

次の通信サービスを使用してサードパーティ アプリケーションを Cisco UCS に接続できます。

通信サービス	説明
CIM XML	このサービスはデフォルトでディセーブルになり、読み取り専用モードでだけ利用できます。 デフォルトのポートは 5988 です。 この共通の情報モデルは、Distributed Management Task Force によって定義された標準の 1 つです。

通信サービス	説明
HTTP	このサービスは、デフォルトでポート 80 でイネーブルになります。 Cisco UCS Manager GUI を実行するには HTTP または HTTPS のいずれかをイネーブルにする必要があります。 HTTP を選択した場合、すべてのデータはクリア テキスト モードで交換されます。 セキュリティ上の理由により、HTTPS をイネーブルにし、HTTP をディセーブルにすることを推奨します。 デフォルトでは、Cisco UCS は HTTP 経由で通信するすべての試みを HTTPS 同等物にリダイレクトします。 この動作を変更しないことを推奨します。 （注） Cisco UCS バージョン 1.4(1) にアップグレードする場合は、これはデフォルトで行われません。 HTTP 経由で通信するすべての試みを HTTPS 同等物にリダイレクトする場合は、Cisco UCS Manager で [Redirect HTTP to HTTPS] をイネーブルにする必要があります。
HTTPS	このサービスは、デフォルトでポート 443 でイネーブルになります。 HTTPS では、すべてのデータはセキュアなサーバを介して暗号化モードで交換されます。 セキュリティ上の理由により、HTTPS のみを使用し、HTTP 通信をディセーブルにするかリダイレクトすることを推奨します。
SMASH CLP	このサービスは読み取り専用アクセスに対してイネーブルとなり、**show** コマンドなどの制限されたプロトコルのサブセットをサポートします。これをディセーブルにすることはできません。 このシェル サービスは、Distributed Management Task Force によって定義された標準の 1 つです。
SNMP	このサービスは、デフォルトでディセーブルになります。 イネーブルの場合、デフォルトのポートは 161 です。 コミュニティと少なくとも 1 つの SNMP トラップを設定する必要があります。 システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。
SSH	このサービスは、ポート 22 でイネーブルになります。 これはディセーブルにできず、デフォルトのポートを変更することもできません。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。
Telnet	このサービスは、デフォルトでディセーブルになります。 このサービスは Cisco UCS Manager CLI へのアクセスを提供します。

CIM-XML の設定

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [CIM-XML] 領域で、[enabled] オプション ボタンをクリックします。
[CIM-XML] 領域が展開され、利用可能な設定オプションが表示されます。

ステップ 5 （任意） [Port] フィールドで、Cisco UCS Manager GUI が CIM-XML に使用するデフォルトのポートを変更します。
デフォルトのポートは 5988 です。

ステップ 6 [Save Changes] をクリックします。

HTTP の設定

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブをクリックします。

ステップ 4 [HTTP] 領域で、[enabled] オプション ボタンをクリックします。
[HTTP] 領域が展開され、利用可能な設定オプションが表示されます。

ステップ 5 （任意） [Port] フィールドで、Cisco UCS Manager GUI が HTTP に使用するデフォルトのポートを変更します。
デフォルトのポートは 80 です。

ステップ 6 （任意） [Redirect HTTP to HTTPS] フィールドで、[enabled] オプション ボタンをクリックします。
HTTP ログインを HTTPS ログインにリダイレクションできるように HTTPS を設定してイネーブルにする必要もあります。 イネーブルにすると、HTTPS をディセーブルにするまでリダイレクションをディセーブルにできません。

（注） HTTP を HTTPS にリダイレクトする場合は、HTTP を使用して Cisco UCS Manager GUI にアクセスできません。 リダイレクションは HTTPS に自動的にリダイレクトするため、HTTP をディセーブルにします。

ステップ 7 [Save Changes] をクリックします。

HTTPS の設定

証明書、キー リング、トラスト ポイント

HTTPS は、Public Key Infrastructure（PKI）を使用してクライアントのブラウザと Cisco UCS Manager などの 2 つのデバイス間でセキュアな通信を確立します。

暗号キーとキー リング

各 PKI デバイスは、内部キー リングに非対称の Rivest-Shamir-Adleman（RSA）暗号キーのペア（1 つはプライベート、もう 1 つはパブリック）を保持します。 いずれかのキーで暗号化されたメッセージは、もう一方のキーで復号化できます。 暗号化されたメッセージを送信する場合、送信者は受信者の公開キーで暗号化し、受信者は独自の秘密キーを使用してメッセージを復号化します。 送信者は、独自の秘密キーで既知のメッセージを暗号化（「署名」とも呼ばれます）して公開キーの所有者を証明することもできます。 受信者が該当する公開キーを使用してメッセージを正常に復号化できる場合は、送信者が対応する秘密キーを所有していることが証明されます。 暗号キーの長さはさまざまであり、通常の長さは 512 ビット ～ 2048 ビットです。 一般的に、短いキーよりも長いキーの方がセキュアになります。 Cisco UCS Manager では、最初に 1024 ビットのキー ペアを含むデフォルトのキー リングが提供されます。そして、追加のキー リングを作成できます。

クラスタ名が変更されるか、証明書が期限切れになった場合は、デフォルトのキー リング証明書を手動で再生成する必要があります。

この操作は UCS Manager CLI のみで使用できます。

証明書

セキュアな通信を準備するには、まず2つのデバイスがそれぞれのデジタル証明書を交換します。 証明書は、デバイスの ID に関する署名済み情報とともにデバイスの公開キーを含むファイルです。 暗号化された通信をサポートするために、デバイスは独自のキーペアと独自の自己署名証明書を生成できます。 リモートユーザが自己署名証明書を提示するデバイスに接続する場合、ユーザはデバイスの ID を簡単に検証することができず、ユーザのブラウザは最初に認証に関する警告を表示します。 デフォルトでは、Cisco UCS Manager にはデフォルトのキー リングからの公開キーを含む組み込みの自己署名証明書が含まれます。

トラスト ポイント

Cisco UCS Manager に強力な認証を提供するために、デバイスの ID を証明する信頼できるソース（つまり、トラスト ポイント）からサードパーティ証明書を取得し、インストールできます。 サードパーティ証明書は、発行元トラスト ポイント（ルート Certificate Authority [CA; 認証局]、中間 CA、またはルート CA につながるトラスト チェーンの一部となるトラスト アンカーのいずれか）によって署名されます。 新しい証明書を取得するには、Cisco UCS Manager で証明書要求を生成し、トラスト ポイントに要求を送信する必要があります。

重要 証明書は Base64 で符号化された X.509（CER）形式である必要があります。

キー リングの作成

Cisco UCS Manager はデフォルトのキー リングを含む、最大 8 つのキー リングをサポートします。

手順

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

ステップ 2 [Admin] タブで、[All] > [Key Management] を展開します。

ステップ 3 [Key Management] を右クリックし、[Create Key Ring] を選択します。

ステップ 4 [Create Key Ring] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドで、キー リングの一意の名前を入力します。

b) [Modulus] フィールドで、次のいずれかのオプション ボタンを選択し、SSL キー長をビット単位で指定します。

- Mod512
- Mod1024
- Mod1536
- Mod2048
- Mod2560
- Mod3072
- Mod3584
- Mod4096

c) [OK] をクリックします。

次の作業

このキー リングの証明書要求を作成します。

キー リングの証明書要求の作成

手順

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

ステップ 2 [Admin] タブで、[All] > [Key Management] を展開します。

ステップ 3 証明書要求を作成するキー リングをクリックします。

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

ステップ 5 [General] タブで [Create Certificate Request] をクリックします。

ステップ 6 [Create Certificate Request] 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
[DNS] フィールド	要求に関連付けられたドメイン ネーム サーバ（DNS）アドレス。
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。 最大 64 文字まで入力できます。 文字、数字、またはスペースのほかに、,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(左括弧）、)（右括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）などの特殊文字を使用できます。
[State] フィールド	証明書を要求している会社の本社が存在する州または行政区分。 最大 64 文字まで入力できます。 文字、数字、またはスペースのほかに、,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(左括弧）、)（右括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）などの特殊文字を使用できます。
[Country] フィールド	会社が存在している国に対応する国コード。 2 文字の英文字を入力します。
[Organization Name] フィールド	証明書を要求している組織。 最大 64 文字まで入力できます。 文字、数字、またはスペースのほかに、,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(左括弧）、)（右括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）などの特殊文字を使用できます。

名前	説明
[Organization Unit Name] フィールド	組織ユニット 最大 64 文字まで入力できます。 文字、数字、またはスペースのほかに、,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(左括弧）、)（右括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）などの特殊文字を使用できます。
[Email] フィールド	要求に関連付けられた電子メールアドレス。
[Password] フィールド	この要求に対するオプションのパスワード。
[Confirm Password] フィールド	パスワードを指定した場合は、確認のためにそのパスワードを再入力します。
[Subject] フィールド	ファブリック インターコネクトの完全修飾ドメイン名。
[IP Address] フィールド	ファブリック インターコネクトの IP アドレス。

ステップ 7 [OK] をクリックします。

ステップ 8 [Request] フィールドから証明書要求のテキストをコピーし、ファイルに保存します。

ステップ 9 証明書要求を含むファイルをトラスト アンカーまたは認証局に送信します。

次の作業

トラストポイントを作成し、トラストアンカーから受け取ったトラストの証明書の証明書チェーンを設定します。

トラスト ポイントの作成

手順

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

ステップ 2 [Admin] タブで、[All] > [Key Management] を展開します。

ステップ 3 [Key Management] を右クリックし、[Create Trusted Point] を選択します。

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

名前	説明
[Name] フィールド	トラスト ポイントの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Certificate Chain] フィールド	このトラスト ポイントの証明書情報。 **重要** 証明書は Base64 で符号化された X.509（CER）形式である必要があります。

ステップ 5 [OK] をクリックします。

次の作業

トラスト アンカーまたは認証局から証明書を受信したら、キー リングにインポートします。

キー リングへの証明書のインポート

手順

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

ステップ 2 [Admin] タブで、[All] > [Key Management] を展開します。

ステップ 3 証明書のインポート先となるキー リングをクリックします。

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

ステップ 5 [Certificate] 領域で、次のフィールドに値を入力します。

a) [Trusted Point] ドロップダウン リストから、この証明書を与えたトラスト アンカーの信頼できるポイントを選択します。

b) [Certificate] フィールドに、トラスト アンカーまたは認証局から受け取った証明書のテキストを貼り付けます。

重要 証明書は Base64 で符号化された X.509（CER）形式である必要があります。

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

ステップ 6 [Save Changes] をクリックします。

次の作業

キー リングを使用して HTTPS サービスを設定します。

HTTPS の設定

注意 HTTPS によって使用されるポートとキー リングの変更をなど、HTTPS 設定がすべて完了すると、トランザクションを保存するかコミットするとすぐに、現在のすべての HTTP と HTTPS セッションは警告を出さずに終了します。

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [HTTPS] 領域で、[enabled] オプション ボタンをクリックします。
[HTTPS] 領域が展開され、利用可能な設定オプションが表示されます。

ステップ 5 次のフィールドに入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • Enabled • Disabled [Admin State] がイネーブルの場合、Cisco UCS Manager GUI にはこのセクションの残りのフィールドが表示されます。
[Port] フィールド	HTTPS 接続に使用するポート。 1 ～ 65535 の整数を指定します。 このサービスは、デフォルトでポート 443 でイネーブルになります。
[Operational Port] フィールド	システム レベルの HTTPS 通信には、ポート Cisco UCS Manager が必要です。 このポートは変更できません。
[Key Ring] ドロップダウン リスト	HTTPS 接続のキー リング。

名前	説明
[Cipher Suite Mode] フィールド	UCSCisco UCS ドメインで使用される暗号スイートのセキュリティ レベル。 次のいずれかになります。 • High Strength • Medium Strength • Low Strength • [Custom]：ユーザ定義の暗号スイート仕様ストリングを指定できます。
[Cipher Suite] フィールド	[Cipher Suite Mode] フィールドで [Custom] を選択する場合、このフィールドにユーザ定義の暗号スイート仕様を指定します。 暗号スイートの仕様文字列には最大 256 文字まで含めることができます。また、OpenSSL の暗号スイートの仕様に準拠する必要があります。！（感嘆符）、+（プラス記号）、-（ハイフン）、および（コロン）を除き、スペースや特殊文字は使用できません。 詳細については、http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite を参照してください。 たとえば、Medium Strength 仕様ストリング Cisco UCS Manager はデフォルトとして ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL を使用します

ステップ 6 [Save Changes] をクリックします。

キーリングの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [Key Management] を展開します。

ステップ 3 削除するキー リングを右クリックし、[Delete] を選択します。

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

トラスト ポイントの削除

はじめる前に

トラスト ポイントがキー リングによって使用されていないことを確認します。

手順

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

ステップ 2 [Admin] タブで、[All] > [Key Management] を展開します。

ステップ 3 削除するトラスト ポイントを右クリックし、[Delete] を選択します。

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

ステップ 5 [OK] をクリックします。

SNMP の設定

SNMP に関する情報

簡易ネットワーク管理プロトコル（SNMP）は、SNMP マネージャとエージェントの間の通信のメッセージ フォーマットを提供するアプリケーション層プロトコルです。 SNMP は、ネットワーク内のデバイスのモニタリングおよび管理に使用する標準フレームワークと共通言語を提供します。

SNMP 機能の概要

SNMP フレームワークは 3 つの部分で構成されます。

- SNMP マネージャ：SNMP を使用してネットワーク デバイスのアクティビティを制御し、モニタリングするシステム。
- SNMP エージェント：Cisco UCS のデータを保守し、必要に応じてデータを SNMP マネージャに報告する、Cisco UCS 内のソフトウェア コンポーネント、つまり管理対象デバイス。 Cisco UCS Cisco UCS はエージェントおよび MIB の収集を含みます。 SNMP エージェントをイネーブルにし、マネージャおよびエージェント間の関係を作成するには、Cisco UCS Manager で SNMP をイネーブルにして設定します。
- 管理情報ベース（MIB）：SNMP エージェント上の管理対象オブジェクトのコレクション。 Cisco UCS Cisco UCS リリース 1.4(1) 以降は以前のリリースに比べ多数の MIB をサポートします。

Cisco UCS Cisco UCS は SNMPv1、SNMPv2c、および SNMPv3 をサポートします。 SNMPv1 と SNMPv2c は、ともにコミュニティベース形式のセキュリティを使用します。 SNMP は、次に定義されています。

- RFC 3410（http://tools.ietf.org/html/rfc3410）
- RFC 3411（http://tools.ietf.org/html/rfc3411）
- RFC 3412（http://tools.ietf.org/html/rfc3412）
- RFC 3413（http://tools.ietf.org/html/rfc3413）
- RFC 3414（http://tools.ietf.org/html/rfc3414）
- RFC 3415（http://tools.ietf.org/html/rfc3415）
- RFC 3416（http://tools.ietf.org/html/rfc3416）
- RFC 3417（http://tools.ietf.org/html/rfc3417）
- RFC 3418（http://tools.ietf.org/html/rfc3418）
- RFC 3584（http://tools.ietf.org/html/rfc3584）

SNMP 通知

SNMP の重要な機能の 1 つは、SNMP エージェントから通知を生成できることです。 これらの通知では、要求を SNMP マネージャから送信する必要はありません。 通知は、不正なユーザ認証、再起動、接続の切断、隣接ルータとの接続の切断、その他の重要なイベントを表示します。

Cisco UCS Manager Cisco UCS Manager は、トラップまたはインフォームとして SNMP 通知を生成します。 SNMP マネージャはトラップを受信したときに確認応答をまったく送信しないため、トラップはインフォームより信頼性が低くなり、また、Cisco UCS Manager はトラップが受信されたかどうかを判断できません。 インフォーム要求を受信する SNMP マネージャは、SNMP 応答 Protocol Data Unit（PDU; プロトコル データ ユニット）でメッセージの受信を確認します。 PDU を受信しない場合、Cisco UCS Manager はインフォーム要求を再び送信できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 は、それぞれ異なるセキュリティ モデルを表します。 セキュリティ モデルと選択したセキュリティ レベルの組み合わせにより、SNMP メッセージの処理中に適用されるセキュリティ メカニズムが決まります。

セキュリティ レベルは、SNMP トラップに関連付けられているメッセージを表示するために必要な権限を決めます。 特権レベルは、メッセージが開示から保護する必要があるか、または認証が必要であるかを決定します。 サポートされるセキュリティ レベルは、実装されているセキュリティ モデルによって異なります。 SNMP セキュリティ レベルは次の特権の 1 つ以上をサポートします。

- noAuthNoPriv：非認証、非暗号化
- authNoPriv：認証、非暗号化

- authPriv：認証、暗号化

SNMPv3 では、セキュリティ モデルとセキュリティ レベルの両方が提供されています。 セキュリティ モデルは、ユーザおよびユーザが属するロールを設定する認証方式です。 セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。 セキュリティ モデルとセキュリティ レベルの組み合わせにより、SNMP パケット処理中に採用されるセキュリティ メカニズムが決まります。

SNMP セキュリティ モデルおよびセキュリティ レベルのサポートされる組み合わせ

次の表に、セキュリティ モデルとセキュリティ レベルの組み合わせの意味を示します。

表 *3*： *SNMP* セキュリティ モデルおよびセキュリティ レベル

モデル	レベル	認証	暗号化	結果
v1	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v2c	noAuthNoPriv	コミュニティ ストリング	No	コミュニティ ストリングの照合を使用して認証します。
v3	noAuthNoPriv	Username	No	ユーザ名の照合を使用して認証します。
v3	authNoPriv	HMAC-MD5 または HMAC-SHA	No	Hash-Based Message Authentication Code（HMAC）Message Digest 5（MD5; メッセージ ダイジェスト 5）アルゴリズムまたは HMAC Secure Hash Algorithm（SHA）アルゴリズムに基づいて認証します。

モデル	レベル	認証	暗号化	結果
v3	authPriv	HMAC-MD5 または HMAC-SHA	DES	HMAC-MD5 または HMAC-SHA アルゴリズムに基づいて認証します。データ暗号規格（DES）の 56 ビット暗号化、および Cipher Block Chaining（CBC; 暗号ブロック連鎖）DES（DES-56）標準に基づいた認証を提供します。

SNMPv3 セキュリティの機能

SNMPv3 は、ネットワーク経由のフレームの認証と暗号化を組み合わせることによって、デバイスへのセキュア アクセスを実現します。 SNMPv3 は、設定済みユーザによる管理動作のみを許可し、SNMP メッセージを暗号化します。 SNMPv3 ユーザベース セキュリティ モデル（USM）は SNMP メッセージレベル セキュリティを参照し、次のサービスを提供します。

- メッセージの完全性：メッセージが不正な方法で変更または破壊されていないことを保証します。また、データ シーケンスが、通常発生するものよりも高い頻度で変更されていないことを保証します。
- メッセージ発信元の認証：受信データを発信したユーザのアイデンティティが確認されたことを保証します。
- メッセージの機密性および暗号化：不正ユーザ、エンティティ、またはプロセスに情報が使用不可で開示されないことを保証します。

Cisco UCS での SNMP サポート Cisco UCS

Cisco UCS Cisco UCS には、SNMP に次のサポートが提供されます。

MIB のサポート

Cisco UCS Cisco UCS は、MIB への読み取り専用アクセスをサポートします。

Cisco UCS で使用可能な特定の MIB およびそれらをどこで取得できるかについては、『MIB Quick Reference for Cisco UCS』を参照してください。

SNMPv3 ユーザの認証プロトコル

Cisco UCS Cisco UCS は、SNMPv3 ユーザに次の認証プロトコルをサポートします。

- HMAC-MD5-96（MD5）
- HMAC-SHA-96（SHA）

SNMPv3 ユーザの AES プライバシー プロトコル

Cisco UCS Cisco UCS は、SNMPv3 メッセージ暗号化用のプライバシー プロトコルの 1 つとして Advanced Encryption Standard（AES）を使用し、RFC 3826 に準拠しています。

プライバシー パスワードつまり priv オプションで、SNMP セキュリティ暗号化方式として、DES または 128 ビット AES を選択できます。 AES-128 の設定を有効にし、SNMPv3 ユーザのプライバシー パスワードを指定すると、Cisco UCS Manager は 128 ビット AES キーを生成するためにプライバシー パスワードを使用します。 AES のプライバシー パスワードは最小で 8 文字です。 パスフレーズをクリア テキストで指定する場合、最大 64 文字を指定できます。

SNMP のイネーブル化および SNMP プロパティの設定

Cisco UCS ドメインからの SNMP メッセージには、システム名ではなくファブリック インターコネクト名が表示されます。

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [SNMP] 領域で、次のフィールドに値を入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • Enabled • Disabled システムに SNMP サーバとの統合が含まれる場合にだけこのサービスをイネーブルにします。 [Admin State] がイネーブルの場合、Cisco UCS Manager GUI にはこのセクションの残りのフィールドが表示されます。
[Port] フィールド	Cisco UCS Manager が SNMP ホストと通信するポート。 デフォルト ポートは変更できません。

名前	説明
[Community/Username] フィールド	Cisco UCS Manager が SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名。 1～32 文字の英数字文字列を入力します。@（アットマーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空のスペースを使用しないでください。 デフォルトは public です。
[System Contact] フィールド	SNMP 実装のシステム連絡先担当者。 電子メール アドレスまたは名前と電話番号など、最大 255 文字の文字列を入力します。
[System Location] フィールド	SNMPエージェント（サーバ）が実行されているホストの場所。 最大 510 文字の英数字文字列を入力します。

ステップ 5 [Save Changes] をクリックします。

次の作業

SNMP トラップおよびユーザを作成します。

SNMP トラップの作成

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [SNMP Traps] 領域で、[+] をクリックします。

ステップ 5 [Create SNMP Trap] 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
[IP Address] フィールド	Cisco UCS Manager がトラップを送信する必要のある SNMP ホストの IP アドレス。

名前	説明
[Community/Username] フィールド	Cisco UCS Manager が SNMP ホストにトラップを送信するときに含まれる SNMP v1 または v2c のコミュニティ名、または SNMP v3 ユーザ名。 これは SNMP サービスに設定されているコミュニティまたはユーザ名と同じであってはなりません。 1 ～ 32 文字の英数字文字列を入力します。@（アットマーク）、\（バックスラッシュ）、"（二重引用符）、?（疑問符）または空のスペースを使用しないでください。
[Port] フィールド	Cisco UCS Manager がトラップの SNMP ホストと通信するポート。 1 ～ 65535 の整数を入力します。 デフォルト ポートは 162 です。
[Version] フィールド	トラップに使用される SNMP バージョンとモデル。 次のいずれかになります。 • V1 • V2c • V3
[Type] フィールド	バージョンに [V2c] または [V3] を選択した場合の、送信するトラップのタイプ。 次のいずれかになります。 • Traps • Informs
[v3 Privilege] フィールド	バージョンに [V3] を選択する場合の、トラップに関連付けられる特権。 次のいずれかになります。 • [Auth]：認証されますが暗号化されません • [Noauth]：認証されないか、暗号化されません • [Priv]：認証および暗号化を行います

ステップ 6 [OK] をクリックします。

ステップ 7 [Save Changes] をクリックします。

SNMP トラップの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [SNMP Traps] 領域で、削除するユーザに対応するテーブルの行をクリックします。

ステップ 5 テーブルの右側の [Delete] アイコンをクリックします。

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

ステップ 7 [Save Changes] をクリックします。

SNMPv3 ユーザの作成

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [SNMP Users] 領域で、[+] をクリックします。

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

名前	説明
[Name] フィールド	SNMP ユーザに割り当てられるユーザ名。 最大 32 文字の文字または番号を入力します。 名前は文字で始まっている必要があり、_（アンダースコア）、.（ピリオド）、□（アットマーク）、および -（ハイフン）も使用できます。 （注） ローカルで認証されたユーザ名と同一の SNMP ユーザ名を作成することはできません。
[Auth Type] フィールド	許可タイプ。 次のいずれかになります。 • MD5 • SHA
[Use AES-128] チェックボックス	オンにすると、このユーザに AES-128 暗号化が使用されます。

名前	説明
[Password] フィールド	このユーザのパスワード。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Privacy Password] フィールド	このユーザのプライバシー パスワード。
[Confirm Privacy Password] フィールド	確認のためのプライバシー パスワードの再入力。

ステップ 6 [OK] をクリックします。

ステップ 7 [Save Changes] をクリックします。

SNMPv3 ユーザの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブを選択します。

ステップ 4 [SNMP Users] 領域で、削除するユーザに対応するテーブルの行をクリックします。

ステップ 5 テーブルの右側の [Delete] アイコンをクリックします。

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

ステップ 7 [Save Changes] をクリックします。

Telnet のイネーブル化

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブをクリックします。

ステップ 4 [Telnet] 領域で、[enabled] オプション ボタンをクリックします。

ステップ 5 [Save Changes] をクリックします。

通信サービスのディセーブル化

（注） 他のネットワーク アプリケーションとのインターフェイスに必要ない通信サービスは、すべてディセーブルにすることを推奨します。

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブで、ディセーブルにする各サービスの [disable] オプション ボタンをクリックします。

ステップ 4 [Save Changes] をクリックします。

第 8 章

認証の設定

この章の内容は、次のとおりです。

- 認証サービス，143 ページ
- リモート認証プロバイダーに関する注意事項および推奨事項，144 ページ
- リモート認証プロバイダーのユーザ属性，144 ページ
- LDAP グループ ルール，146 ページ
- LDAP プロバイダーの設定，147 ページ
- RADIUS プロバイダーの設定，156 ページ
- TACACS+ プロバイダーの設定，160 ページ
- マルチ認証システムの設定，162 ページ
- プライマリ認証サービスの選択，168 ページ

認証サービス

Cisco UCS では、ユーザ ログインを認証するために、2 種類の方法がサポートされています。

- Cisco UCS Manager にローカルなユーザ アカウントによる
- 次のいずれかのプロトコルによるリモート
  - LDAP
  - RADIUS
  - TACACS+

リモート認証プロバイダーに関する注意事項および推奨事項

システムを、サポートされているリモート認証サービスのいずれかに設定する場合は、そのサービス用のプロバイダーを作成して、Cisco UCS Managerがそのサービスと通信できるようにする必要があります。 また、ユーザ許可に影響する次のガイドラインに留意する必要があります。

リモート認証サービスのユーザ アカウント

ユーザ アカウントは、Cisco UCS Manager にローカルに、またはリモート認証サーバに存在することができます。

リモート認証サービスを介してログインしているユーザの一時的なセッションは、Cisco UCS Manager GUI または Cisco UCS Manager CLI で表示できます。

リモート認証サービスのユーザ ロール

リモート認証サーバでユーザ アカウントを作成する場合は、ユーザが Cisco UCS Manager で作業するために必要なロールをそれらのアカウントに含めること、およびそれらのロールの名前をCisco UCS Managerで使用される名前と一致させることが必要です。 ロール ポリシーによっては、ユーザがログインできない可能性があります。または、読み取り専用の権限だけが許可されます。

リモート認証プロバイダーのユーザ属性

RADIUS および TACACS+ 設定の場合は、ユーザが Cisco UCS Manager にログインする各リモート認証プロバイダーの Cisco UCS にユーザ属性を設定する必要があります。 このユーザ属性は、各ユーザに割り当てられたロールとロケールを保持します。

（注） このステップは、ロールとロケールを割り当てるために LDAP グループ マッピングを使用する LDAP 設定には必要ありません。

ユーザがログインすると、Cisco UCS Manager は以下を実行します。

1. リモート認証サービスを照会します。
2. ユーザを検証します。
3. ユーザが検証されると、そのユーザに割り当てられているロールとロケールをチェックします。

次の表に、Cisco UCS によってサポートされるリモート認証プロバイダーのユーザ属性要件の比較を示します。

表 *4*：リモート認証プロバイダー別のユーザ属性の比較

認証プロバイダー	カスタム属性	スキーマ拡張	属性 ID の要件
LDAP	グループ マッピングを使用する場合は不要 グループ マッピングを使用しない場合はオプション	オプション 次のいずれかを実行するように選択できます。 • LDAP スキーマを拡張せず、要件を満たす既存の未使用の属性を設定します。 • LDAP スキーマを拡張して、CiscoAVPair などの一意の名前でカスタム属性を作成します。	シスコの LDAP 実装では Unicode タイプの属性が必要です。 CiscoAVPair のカスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します。 サンプル OID は、次の項で説明します。
RADIUS	オプション	オプション 次のいずれかを実行するように選択できます。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用の属性を使用します。 • RADIUS スキーマを拡張して、cisco-avpair などの一意の名前でカスタム属性を作成します。	Cisco RADIUS 実装のベンダー ID は 009 で、属性のベンダー ID は 001 です。 次の構文は、cisco-avpair 属性を作成する場合に、複数のユーザロールとロケールを指定する例を示しています： `shell:roles="admin,aaa"` `shell:locales="L1,abc"`。 複数の値を区切るには、デリミタとしてカンマ（,）を使用します。

認証プロバイダー	カスタム属性	スキーマ拡張	属性 ID の要件
TACACS+	Required	必須です。 スキーマを拡張して、cisco-av-pair という名前でカスタム属性を作成する必要があります。	cisco-av-pair の名前は、TACACS+ プロバイダーに属性 ID を指定する文字列です。 次の構文は、cisco-av-pair 属性を作成する場合に、複数のユーザ ロールとロケールを指定する方法を示しています： `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。 アスタリスク（*）を cisco-av-pair 属性構文内で使用することで、オプションとしてロケールにフラグを立て、同じ認証プロファイルを使用する他のシスコデバイスに対する認証が失敗しないようにします。 複数の値を区切るには、デリミタとしてスペースを使用します。

LDAP ユーザ属性のサンプル OID

次に示すのは、カスタム CiscoAVPair 属性のサンプル OID です。

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

LDAP グループ ルール

LDAP グループ ルールは、ユーザ ロールとロケールをリモート ユーザに割り当てるときに Cisco UCS が LDAP グループを使用するかどうかを決定するために使用します。

LDAP プロバイダーの設定

LDAP プロバイダーのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されているこのタイプのすべてのプロバイダー接続のデフォルト設定になります。 個々のプロバイダーにこれらのプロパティのいずれかの設定が含まれている場合、Cisco UCS はその設定を使用し、デフォルト設定を無視します。

はじめる前に

LDAP サーバとして Active Directory を使用する場合、Cisco UCS にバインドする Active Directory サーバでユーザアカウントを作成します。 このアカウントには、期限切れにならないパスワードを設定する必要があります。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] を展開します。

ステップ 3 [Properties] 領域の次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力します。 デフォルト値は 30 秒です。 このプロパティは必須です。
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。 このプロパティは、常に、名前と値のペアで指定されます。 システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP スキーマを拡張しない場合、既存の、使用されていない LDAP 属性を Cisco UCS ロールとロケールで設定できます。 あるいは、CiscoAVPair という名前の属性を、属性 ID 1.3.6.1.4.1.9.287247.1 を使用してリモート認証サービスに作成できます。

名前	説明
[Base DN] フィールド	リモート ユーザがログインし、システムがユーザ名に基づいてユーザの DN を取得しようとするときに、サーバが検索を開始する必要のある LDAP 階層内の特定の識別名。 サポートされるストリングの最大長は 127 文字です。 このプロパティは必須です。 このタブで Base DN を指定しない場合、この UCS ドメインに定義されている LDAP プロバイダーごとに、[General]Cisco UCS ドメインタブに任意の値を指定する必要があります。
[Filter] フィールド	LDAP 検索は、定義したフィルタと一致するユーザ名に制限されます。 このプロパティは必須です。 このタブでフィルタを指定しない場合、この UCS ドメインに定義されている LDAP プロバイダーごとに、[General]Cisco UCS ドメインタブに任意のフィルタを指定する必要があります。

ステップ 4 [Save Changes] をクリックします。

次の作業

LDAP プロバイダーを作成します。

LDAP プロバイダーの作成

Cisco UCS Manager は最大 16 の LDAP プロバイダーをサポートします。

はじめる前に

LDAP サーバとして Active Directory を使用する場合、Cisco UCS にバインドする Active Directory サーバでユーザアカウントを作成します。 このアカウントには、期限切れにならないパスワードを設定する必要があります。

- LDAP サーバで、次のいずれかの設定を行います。
  - LDAP グループを設定します。 LDAP グループにはユーザ ロールとロケール情報が含まれます。
  - Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性を使用してユーザを設定します。 この属性の LDAP スキーマを拡張するかどうかを選択できます。 スキーマを拡張しない場合は、既存の LDAP 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。 スキーマを拡張する場合は、CiscoAVPair 属性など、カスタム属性を作成します。

シスコの LDAP 実装では Unicode タイプの属性が必要です。

CiscoAVPair のカスタム属性を作成する場合は、属性 ID として 1.3.6.1.4.1.9.287247.1 を使用します。

◦ クラスタ設定では、両方のファブリック インターコネクトに対する管理ポート IP アドレスを追加します。 この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモート ユーザは引き続きログインできることが保証されます。 ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

- セキュアな通信を使用する場合は、Cisco UCS Manager で LDAP サーバのルート認証局（CA）証明書を含むトラスト ポイントを作成します。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] 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 [Actions] エリアで、[Create LDAP Provider] をクリックします。

ステップ 5 ウィザードの [Create LDAP Provider] ページで、次を実行します。

a) 使用する LDAP サービスに関する情報を使用して、次のフィールドに値を入力します。

名前	説明
[Hostname] フィールド	LDAP プロバイダーのホスト名または IP アドレス。 SSL がイネーブルの場合、このフィールドは、LDAP データベースのセキュリティ証明書内の Common Name（CN; 通常名）と正確に一致している必要があります。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。

名前	説明
[Order] フィールド	Cisco UCS でこのプロバイダーをユーザの認証に使用する順序。 1 から 16 までの整数を入力するか、この Cisco UCS ドメインに定義されている他のプロバイダーに基づいて、次に使用できる順番を Cisco UCS で割り当てる場合は、使用可能な最も低い値または 0（ゼロ）を入力します。
[Bind DN] フィールド	ベース DN の下にあるすべてのオブジェクトに対する読み取りおよび検索の権限を持つ LDAP データベース アカウントの識別名（DN）。 サポートされるストリングの最大長は 127 ASCII 文字です。
[Base DN] フィールド	リモートユーザがログインし、システムがユーザ名に基づいてユーザの DN を取得しようとするときに、サーバが検索を開始する必要のある LDAP 階層内の特定の識別名。 サポートされるストリングの最大長は 127 文字です。 デフォルトのベース DN が LDAP の [General] タブで設定されていない場合、この値は必要です。
[Port] フィールド	Cisco UCS が LDAP データベースと通信するためのポート。 標準ポート番号は 389 です。
[Enable SSL] チェックボックス	このチェックボックスをオンにすると、LDAP データベースとの通信に暗号化が必要になります。 このチェックボックスをオフにすると、認証情報はクリア テキストで送信されます。 LDAP では STARTTLS が使用されます。 これにより、ポート 389 を使用した暗号化通信を行えます。
[Filter] フィールド	LDAP 検索は、定義したフィルタと一致するユーザ名に制限されます。 デフォルトのフィルタが LDAP の [General] タブで設定されていない場合、この値は必要です。

名前	説明
[Attribute] フィールド	ユーザ ロールとロケールの値を保管する LDAP 属性。 このプロパティは、常に、名前と値のペアで指定されます。 システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP スキーマを拡張しない場合、既存の、使用されていない LDAP 属性を Cisco UCS ロールとロケールで設定できます。 あるいは、CiscoAVPair という名前の属性を、属性 ID 1.3.6.1.4.1.9.287247.1 を使用してリモート認証サービスに作成できます。 デフォルトの属性が LDAP の [General] タブで設定されていない場合、この値は必要です。
[Password] フィールド	[Bind DN] フィールドで指定した LDAP データベース アカウントのパスワード。 スペース、§（セクション記号）、?（疑問符）、または =（等号）を除くすべての標準 ASCII 文字を入力できます。
[Confirm Password] フィールド	確認のための LDAP データベース パスワードの再入力。
[Timeout] フィールド	LDAP データベースへの問い合わせがタイム アウトするまでの秒数。 LDAP の [General] タブでグローバル タイムアウト値を使用するには、1 ～ 60 秒の整数か、0（ゼロ）を入力します。 デフォルトは 30 秒です。

b) [Next] をクリックします。

ステップ 6 ウィザードの [LDAP Group Rule] ページで、次を実行します。

a) 次のフィールドに入力します。

名前	説明
[Group Authorization] フィールド	ユーザ ロールとロケールを認証して、それらをリモートユーザに割り当てるときに、Cisco UCS が LDAP グループも検索するかどうか。 次のいずれかになります。 • [Disable]：Cisco UCSCisco UCSは LDAP グループにアクセスしません。 • [Enable]：Cisco UCS はこの Cisco UCS ドメイン内にマッピングされたすべての LDAP グループを検索します。 リモート ユーザが検出されると、Cisco UCS は関連付けられた LDAP グループ マップの LDAP グループに定義されたユーザ ロールとロケールを割り当てます。 （注） ロールとロケールの割り当ては累積されます。 ユーザが複数のグループに含まれているか、LDAP 属性に指定されているロールまたはロケールを持っている場合、Cisco UCS はそのユーザに、それらのグループまたは属性のいずれかにマップされているすべてのロールおよびロケールを割り当てます。
[Group Recursion] フィールド	Cisco UCS がマップされたグループとそれらの親グループの両方を検索するかどうか。 次のいずれかになります。 • [Non Recursive]：Cisco UCS は、この Cisco UCS ドメインにマップされたグループのみを検索します。 ユーザが含まれているグループのいずれも明示的にユーザ認可プロパティを設定していない場合、Cisco UCS はデフォルト設定を使用します。 • [Recursive]：Cisco UCS はマップされている各グループとそのすべての親グループに対して、ユーザの許可プロパティを検索します。 これらのプロパティは累積的であるため、各グループに対して、Cisco UCS は明示的な許可プロパティ設定を使用して検索し、それらの設定を現在のユーザに適用します。 それ以外の場合は、デフォルト設定を使用します。
[Target Attribute] フィールド	Cisco UCS で LDAP データベース内のグループ メンバーシップを決定する際に使用される属性。 サポートされる文字列長は 63 文字です。 デフォルトの設定は memberOf です。

b) [Finish] をクリックします。

次の作業

1 つの LDAP データベースを含む実装では、認証サービスとして [LDAP] を選択します。

複数の LDAP データベースを含む実装では LDAP プロバイダーのグループを設定します。

LDAP プロバイダーの LDAP グループ ルールの変更

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] を展開します。

ステップ 3 [LDAP Providers] を展開し、グループ ルールを変更する LDAP プロバイダーを選択します。

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

ステップ 5 [LDAP Group Rules] 領域で、次のフィールドに値を入力します。

名前	説明
[Group Authorization] フィールド	ユーザ ロールとロケールを認証して、それらをリモートユーザに割り当てるときに、Cisco UCS が LDAP グループも検索するかどうか。 次のいずれかになります。 • [Disable]：Cisco UCSCisco UCSは LDAP グループにアクセスしません。 • [Enable]：Cisco UCS はこの Cisco UCS ドメイン内にマッピングされたすべての LDAP グループを検索します。 リモート ユーザが検出されると、Cisco UCS は関連付けられた LDAP グループ マップの LDAP グループに定義されたユーザ ロールとロケールを割り当てます。 （注） ロールとロケールの割り当ては累積されます。 ユーザが複数のグループに含まれているか、LDAP 属性に指定されているロールまたはロケールを持っている場合、Cisco UCS はそのユーザに、それらのグループまたは属性のいずれかにマップされているすべてのロールおよびロケールを割り当てます。

名前	説明
[Group Recursion] フィールド	Cisco UCS がマップされたグループとそれらの親グループの両方を検索するかどうか。 次のいずれかになります。 • [Non Recursive]：Cisco UCS は、この Cisco UCS ドメインにマップされたグループのみを検索します。 ユーザが含まれているグループのいずれも明示的にユーザ認可プロパティを設定していない場合、Cisco UCS はデフォルト設定を使用します。 • [Recursive]：Cisco UCS はマップされている各グループとそのすべての親グループに対して、ユーザの許可プロパティを検索します。 これらのプロパティは累積的であるため、各グループに対して、Cisco UCS は明示的な許可プロパティ設定を使用して検索し、それらの設定を現在のユーザに適用します。 それ以外の場合は、デフォルト設定を使用します。
[Target Attribute] フィールド	Cisco UCS で LDAP データベース内のグループ メンバーシップを決定する際に使用される属性。 サポートされる文字列長は 63 文字です。 デフォルトの設定は memberOf です。

ステップ 6 [Save Changes] をクリックします。

LDAP プロバイダーの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] を展開します。

ステップ 3 [LDAP Providers] を展開します。

ステップ 4 削除する LDAP プロバイダーを右クリックし、[Delete] を選択します。

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

LDAP グループ マッピング

すでに LDAP グループを使用して LDAP データベースへのアクセスを制限している組織では、ログイン時に LDAP ユーザにロールまたはロケールを割り当てるために UCSM がグループ メンバーシップ情報を使用できます。 このため、Cisco UCS Manager が導入されるときに LDAP ユーザ オブジェクトにロールまたはロケール情報を定義する必要はありません。

ユーザが Cisco UCS Manager にログインすると、ユーザのロールおよびロケールに関する情報が LDAP グループ マップから取り出されます。 ロールとロケールの条件がポリシー情報と一致する場合、アクセスが許可されます。

ロールとロケールの定義は UCSCisco UCS Manager でローカルに設定され、LDAP ディレクトリに対する変更に基づいて自動的に更新されることはありません。 LDAP ディレクトリの LDAP グループを削除するか、ファイルの名前を変更する場合、その変更で Cisco UCS Manager を更新することが重要です。

LDAP グループ マップはロールとロケールの次の組み合わせを含むように設定できます。

- ロールのみ
- ロケールのみ
- ロールとロケール両方

たとえば、特定の場所でサーバ管理者グループを表す LDAP グループを考慮します。 LDAP グループ マップは server-profile および server-equipment などのユーザ ロールを含むように設定されている場合があります。 特定の場所でサーバ管理者へのアクセスを制限するには、ロケールを特定のサイト名に設定できます。

（注） Cisco UCS Manager には、多くのアウトオブザボックスのユーザ ロールが含まれていますが、ロケールはまったく含まれません。 ロケールへ LDAP プロバイダー グループをマッピングするには、カスタム ロケールを作成する必要があります。

LDAP グループ マップの作成

はじめる前に

- LDAP サーバで LDAP グループを作成します。
- LDAP サーバで LDAP グループの識別名を設定します。
- Cisco UCS Manager でロケールを作成します（任意）。
- Cisco UCS Manager でカスタム ロールを作成します（任意）。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] を展開します。

ステップ 3 [LDAP Group Maps] を右クリックし、[Create LDAP Group Map] を選択します。

ステップ 4 [Create LDAP Group Map] ダイアログボックスで、次を実行します。

a) [LDAP Group DN][LDAP Group DN] フィールドフィールドに、LDAP データベースのグループの識別名を入力します。

重要 この名前は、LDAP データベース名と正確に一致する必要があります。

b) [Roles] テーブルで、グループ マップに含まれているユーザに割り当てるすべてのロールのチェックボックスをオンにします。

c) [Locales] テーブルで、グループ マップに含まれているユーザに割り当てるすべてのロケールのチェックボックスをオンにします。

d) [OK] をクリックします。

次の作業

LDAP グループ ルールを設定します。

LDAP グループ マップの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] を展開します。

ステップ 3 [LDAP Group Maps] を展開します。

ステップ 4 削除する LDAP グループ マップを右クリックし、[Delete] を選択します。

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

RADIUS プロバイダーの設定

RADIUS プロバイダーのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されているこのタイプのすべてのプロバイダー接続のデフォルト設定になります。 個々のプロバイダーにこれらのプロパティのい

ずれかの設定が含まれている場合、Cisco UCS はその設定を使用し、デフォルト設定を無視します。

手順

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

ステップ 2 [Admin] タブで、[User Management] > [RADIUS] を展開します。

ステップ 3 [Properties] 領域の次のフィールドに値を入力します。

名前	説明
[Timeout] フィールド	RADIUS データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、または 0（ゼロ）を入力して RADIUS の [General] タブで指定されたグローバル タイムアウト値を使用します。 デフォルトは 5 秒です。
[Retries] フィールド	要求が失敗したと見なされるまでの接続の再試行の回数。

ステップ 4 [Save Changes] をクリックします。

次の作業

RADIUS プロバイダーを作成します。

RADIUS プロバイダーの作成

Cisco UCS Manager は最大 16 の RADIUS プロバイダーをサポートします。

はじめる前に

RADIUS サーバで、次の設定を行います。

- Cisco UCS Manager のユーザ ロールとロケール情報を保持する属性を使用してユーザを設定します。 この属性の RADIUS スキーマを拡張するかどうかを選択できます。 スキーマを拡張しない場合は、既存の RADIUS 属性を使用して Cisco UCS ユーザ ロールとロケールを保持します。 スキーマを拡張する場合は、cisco-avpair 属性などのカスタム属性を作成します。

  Cisco RADIUS 実装のベンダー ID は 009 で、属性のベンダー ID は 001 です。

  次の構文は、cisco-avpair 属性を作成する場合に、複数のユーザ ロールとロケールを指定する例を示しています：`shell:roles="admin,aaa" shell:locales="L1,abc"`。 複数の値を区切るには、デリミタとしてカンマ（,）を使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポート IP アドレスを追加します。 この設定では、1 つめのファブリック インターコネクトで障害が発生し、シ

ステムが2つめのファブリックインターコネクトにフェールオーバーしても、リモートユーザは引き続きログインできることが保証されます。 ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [RADIUS] を展開します。

ステップ 3 [Create RADIUS Provider] ダイアログボックスで、次の手順を実行します。

a) 使用する RADIUS サービスに関する情報を使用して、次のフィールドに値を入力します。

名前	説明
[Hostname] フィールド	RADIUS プロバイダーが存在する場所のホスト名または IP アドレス。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Order] フィールド	Cisco UCS でこのプロバイダーをユーザの認証に使用する順序。 1 から 16 までの整数を入力するか、この Cisco UCS ドメインに定義されている他のプロバイダーに基づいて、次に使用できる順番を Cisco UCS で割り当てる場合は、使用可能な最も低い値または 0（ゼロ）を入力します。
[Key] フィールド	データベースの Secure Socket Layer（SSL; セキュア ソケットレイヤ）暗号キー。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[Authorization Port] フィールド	Cisco UCS が RADIUS データベースと通信するために使用するポート。

名前	説明
[Timeout] フィールド	RADIUS データベースへの問い合わせがタイム アウトするまでの秒数。 1 ～ 60 秒の整数を入力するか、または 0（ゼロ）を入力して RADIUS の [General] タブで指定されたグローバルタイムアウト値を使用します。 デフォルトは 5 秒です。
[Retries] フィールド	要求が失敗したと見なされるまでの接続の再試行の回数。 必要に応じて、0 ～ 5 の整数を入力します。 値を指定しない場合、Cisco UCS は、RADIUS の [General] タブで指定された値を使用します。

b) [OK] をクリックします。

ステップ 4 [Save Changes] をクリックします。

次の作業

1 つの RADIUS データベースを含む実装では、プライマリ認証サービスとして [RADIUS] を選択します。

複数の RADIUS データベースを含む実装では RADIUS プロバイダーのグループを設定します。

RADIUS プロバイダーの削除

手順

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

ステップ 2 [Admin] タブで、[User Management] > [RADIUS] を展開します。

ステップ 3 削除する RADIUS プロバイダーを右クリックし、[Delete] を選択します。

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

TACACS+ プロバイダーの設定

TACACS+ プロバイダーのプロパティの設定

このタスクで設定するプロパティは、Cisco UCS Manager で定義されているこのタイプのすべてのプロバイダー接続のデフォルト設定になります。 個々のプロバイダーにこれらのプロパティのいずれかの設定が含まれている場合、Cisco UCS はその設定を使用し、デフォルト設定を無視します。

手順

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

ステップ 2 [Admin] タブで、[User Management] > [TACACS+] を展開します。

ステップ 3 [Properties] 領域で、 [Timeout] フィールドに値を入力します。
タイムアウトになるまで TACACS+ データベースとの接続が試みられる秒数。

1 ～ 60 秒の整数を入力するか、または 0（ゼロ）を入力して TACACS+ の [General] タブで指定したグローバル タイムアウト値を使用します。 デフォルトは 5 秒です。

ステップ 4 [Save Changes] をクリックします。

次の作業

TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの作成

Cisco UCS Manager は最大 16 の TACACS+ プロバイダーをサポートします。

はじめる前に

TACACS+ サーバで、次の設定を行います。

- cisco-av-pair 属性を作成します。 既存の TACACS+ 属性は使用できません。

  cisco-av-pair の名前は、TACACS+ プロバイダーに属性 ID を指定する文字列です。

  次の構文は、cisco-av-pair 属性を作成する場合に、複数のユーザ ロールとロケールを指定する方法を示しています：`cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`。アスタリスク（*）を cisco-av-pair 属性構文内で使用することで、オプションとしてロケールにフラグを立て、同じ認証プロファイルを使用する他のシスコ デバイスに対する認証が失敗しないようにします。 複数の値を区切るには、デリミタとしてスペースを使用します。

- クラスタ設定では、両方のファブリック インターコネクトに対する管理ポート IP アドレスを追加します。 この設定では、1 つめのファブリック インターコネクトで障害が発生し、システムが 2 つめのファブリック インターコネクトにフェールオーバーしても、リモート ユー

ザは引き続きログインできることが保証されます。 ログイン要求はすべて、これらの IP アドレスから送信されます。Cisco UCS Manager によって使用されている仮想 IP アドレスではありません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [TACACS+] を展開します。

ステップ 3 [General] タブの [Actions] 領域で、[Create TACACS+ Provider] をクリックします。

ステップ 4 [Create TACACS+ Provider] ダイアログボックスで、次の手順を実行します。

a) 使用する TACACS+ サービスに関する情報を使用して、フィールドに値を入力します。

名前	説明
[Hostname] フィールド	LDAP プロバイダーが存在する場所のホスト名または IP アドレス。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Order] フィールド	Cisco UCS でこのプロバイダーをユーザの認証に使用する順序。 1 から 16 までの整数を入力するか、この Cisco UCS ドメインに定義されている他のプロバイダーに基づいて、次に使用できる順番を Cisco UCS で割り当てる場合は、使用可能な最も低い値または 0（ゼロ）を入力します。
[Key] フィールド	データベースの Secure Socket Layer（SSL; セキュア ソケット レイヤ）暗号キー。
[Confirm Key] フィールド	確認のための SSL 暗号キーの再入力。
[Port] フィールド	Cisco UCS が TACACS+ データベースと通信するために使用するポート。 1 ～ 65535 の整数を入力します。 デフォルト ポートは 49 です。

名前	説明
[Timeout] フィールド	タイムアウトになるまで TACACS+ データベースとの接続が試みられる秒数。 1 ～ 60 秒の整数を入力するか、または 0（ゼロ）を入力して TACACS+ の [General] タブで指定したグローバル タイムアウト値を使用します。 デフォルトは 5 秒です。

b) [OK] をクリックします。

ステップ 5 [Save Changes] をクリックします。

次の作業

1 つの TACACS+ データベースを含む実装では、プライマリ認証サービスとして [TACACS+] を選択します。

複数の TACACS+ データベースを含む実装では TACACS+ プロバイダーのグループを設定します。

TACACS+ プロバイダーの削除

手順

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

ステップ 2 [Admin] タブで、[User Management] > [TACACS+] を展開します。

ステップ 3 削除する TACACS+ プロバイダーを右クリックし、[Delete] を選択します。

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

マルチ認証システムの設定

マルチ認証システム

次の機能を設定して、複数の認証システムを使用するように Cisco UCS を設定できます。

- プロバイダー グループ
- 認証ドメイン

プロバイダー グループ

プロバイダー グループは、認証プロセス中に Cisco UCS が使用する一連のプロバイダーです。Cisco UCS Manager Cisco UCS Manager では、グループごとに最大 8 プロバイダーが許可されるプロバイダー グループを最大 16 作成できます。

認証中、プロバイダー グループ内のすべてのプロバイダーは順番に試行されます。 設定されたサーバがすべて使用できないか、到達不能の場合、Cisco UCS Manager はローカル ユーザ名とパスワードを使用してローカル認証方式に自動的にフォールバックします。

LDAP プロバイダー グループの作成

LDAP プロバイダーのグループを作成すると、複数の LDAP データベースを使用して認証を行うことができます。

（注） 単一の LDAP データベースでの認証では、LDAP プロバイダーのグループを設定する必要はありません。

はじめる前に

1 つ以上の LDAP プロバイダーを作成します。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] を展開します。

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

ステップ 4 [Create LDAP Provider Group] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、グループの一意の名前を入力します。
この名前には、1 から 127 個の文字を使用できます。

b) [LDAP Providers] テーブルで、グループに含める一つ以上のプロバイダーを選択します。

c) [>>] ボタンをクリックして、[Included Providers] テーブルにプロバイダーを追加します。
グループからプロバイダーを削除するには、[<<] ボタンを使用できます。

d) 必要なすべてのプロバイダーをプロバイダー グループへ追加した後で、[OK] をクリックします。

次の作業

認証ドメインを設定するか、デフォルトの認証サービスを選択します。

LDAP プロバイダー グループの削除

はじめる前に

認証設定からプロバイダー グループを削除します。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [LDAP] を展開します。

ステップ 3 [LDAP Provider Groups] を展開します。

ステップ 4 削除する LDAP プロバイダー グループを右クリックし、[Delete] を選択します。

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

RADIUS プロバイダー グループの作成

RADIUS プロバイダーのグループを作成すると、複数の RADIUS データベースを使用して認証を行うことができます。

（注） 単一の RADIUS データベースでの認証では、RADIUS プロバイダーのグループを設定する必要はありません。

はじめる前に

1 つ以上の RADIUS プロバイダーを作成します。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [RADIUS] を展開します。

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

ステップ 4 [Create RADIUS Provider Group] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、グループの一意の名前を入力します。
この名前には、1 ～ 127 文字の ASCII 文字を使用できます。

b) [RADIUS Providers] テーブルで、グループに含める一つ以上のプロバイダーを選択します。

c) [>>] ボタンをクリックして、[Included Providers] テーブルにプロバイダーを追加します。
グループからプロバイダーを削除するには、[<<] ボタンを使用できます。

d) 必要なすべてのプロバイダーをプロバイダー グループへ追加した後で、[OK] をクリックします。

次の作業

認証ドメインを設定するか、デフォルトの認証サービスを選択します。

RADIUS プロバイダー グループの削除

認証設定によって使用されているプロバイダーのグループは削除できません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [RADIUS] を展開します。

ステップ 3 [RADIUS Provider Groups] を展開します。

ステップ 4 削除する RADIUS プロバイダー グループを右クリックし、[Delete] を選択します。

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

TACACS+ プロバイダー グループの作成

TACACS+ プロバイダーのグループを作成すると、複数の TACACS+ データベースを使用して認証を行うことができます。

（注） 単一の TACACS+ データベースでの認証では、TACACS+ プロバイダーのグループを設定する必要はありません。

はじめる前に

1 つ以上の TACACS+ プロバイダーを作成します。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [TACACS+] を展開します。

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

ステップ 4 [Create TACACS+ Provider Group] ダイアログボックスで、次を実行します。

a) [Name] フィールドに、グループの一意の名前を入力します。

この名前には、1 ～ 127 文字の ASCII 文字を使用できます。

b) [TACACS+ Providers] テーブルで、グループに含める一つ以上のプロバイダーを選択します。

c) [>>] ボタンをクリックして、[Included Providers] テーブルにプロバイダーを追加します。
グループからプロバイダーを削除するには、[<<] ボタンを使用できます。

d) 必要なすべてのプロバイダーをプロバイダー グループへ追加した後で、[OK] をクリックします。

TACACS+ プロバイダー グループの削除

認証設定によって使用されているプロバイダーのグループは削除できません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [TACACS+] を展開します。

ステップ 3 [TACACS+ Provider Groups] を展開します。

ステップ 4 削除する TACACS+ プロバイダー グループを右クリックし、[Delete] を選択します。

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

認証ドメイン

認証ドメインは、マルチ認証システムを活用するために Cisco UCS Manager によって使用されます。 各認証ドメインは、ログイン時に指定および設定されます。 認証ドメインが指定されない場合、デフォルトの認証サービス設定が使用されます。

最大 8 個の認証ドメインを作成できます。 各認証ドメインは、Cisco UCS Manager のプロバイダー グループとレルムに関連付けられます。 プロバイダー グループが指定されていない場合、レルム内のすべてのサーバが使用されます。

認証ドメインの作成

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [Authentication] を展開します。

ステップ 3 [Authentication Domains] を右クリックし、[Create a Domain] を選択します。

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

名前	説明
[Name] フィールド	ドメインの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。 （注） 優先する認証プロトコルとして RADIUS を使用するシステムの場合、認証ドメイン名はローカルに作成されたユーザ名に最大 32 文字のユーザ名および番号の一部と見なされます。 Cisco UCS はフォーマット用に 5 文字を挿入するため、ドメイン名とユーザ名を組み合わせた総数が 27 文字を超えると認証が失敗します。
[Web Session Refresh Period] フィールド	Web クライアントが Cisco UCS Manager に接続する場合、クライアントはリフレッシュ要求を Cisco UCS Manager に送信して Web セッションをアクティブに保つ必要があります。 このオプションによって、このドメイン内のユーザに対するリフレッシュ要求の間に許容される最大時間が指定されます。 この時間制限を超えると、Cisco UCS Manager は Web セッションが非アクティブであると見なしますが、セッションは終了されません。 60 ～ 172800 の整数を指定します。 デフォルトは 600 秒です。
[Web Session Timeout] フィールド	Cisco UCS Manager が、Web セッションが終了したと見なす前提となる最終リフレッシュ要求後の最大経過時間。 この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了します。 60 ～ 172800 の整数を指定します。 デフォルトは 7200 秒です。

名前	説明
[Realm] フィールド	このドメインのユーザに適用される認証プロトコル。 次のいずれかになります。 • [Local]：ユーザ アカウントはこの Cisco UCS ドメインでローカルで定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザは、この Cisco UCS ドメインに定義された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザは、この Cisco UCS ドメインに指定された LDAP サーバで定義する必要があります。
[Provider Group] ドロップダウンリスト	[Realm] が [Local] 以外に設定されている場合、このフィールドを使用して、関連するプロバイダーグループ（ある場合）を選択できます。

ステップ 5 [OK] をクリックします。

プライマリ認証サービスの選択

コンソール認証サービスの選択

はじめる前に

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダーを作成します。 システムが Cisco UCS を介してローカル認証のみを使用する場合は、最初にプロバイダーを作成する必要はありません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [Authentication] を展開します。

ステップ 3 [Native Authentication] をクリックします。

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

ステップ 5 [Console Authentication] タブ領域で、次のフィールドに値を入力します。

名前	説明
[Realm] フィールド	コンソールにログインするユーザが認証される方法。 次のいずれかになります。 • [Local]：ユーザ アカウントはこの Cisco UCS ドメインでローカルで定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザは、この Cisco UCS ドメインに定義された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザは、この Cisco UCS ドメインに指定された LDAP サーバで定義する必要があります。 • [None]：ユーザ アカウントがこの Cisco UCS ドメインに対してローカルである場合、ユーザがコンソールにログインするときにパスワードは必要ありません。
[Provider Group] ドロップダウン リスト	コンソールにログインするユーザの認証に使用するプロバイダーのグループ。

ステップ 6 [Save Changes] をクリックします。

デフォルトの認証サービスの選択

はじめる前に

システムでリモート認証サービスが使用されている場合は、その認証サービスに対するプロバイダーを作成します。 システムが Cisco UCS を介してローカル認証のみを使用する場合は、最初にプロバイダーを作成する必要はありません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [Authentication] を展開します。

ステップ 3 [Native Authentication] をクリックします。

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

ステップ 5 [Default Authentication] タブ領域で、次のフィールドに値を入力します。

名前	説明
[Realm] ドロップダウン リスト	リモート ログイン中にユーザが認証されるデフォルトの方法。 次のいずれかになります。 • [Local]：ユーザ アカウントはこの Cisco UCS ドメインでローカルで定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザは、この Cisco UCS ドメインに定義された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザは、この Cisco UCS ドメインに指定された LDAP サーバで定義する必要があります。 • [None]：ユーザ アカウントがこの Cisco UCS ドメインインスタンスに対してローカルである場合、ユーザがリモートでログインするときにパスワードは必要ありません。
[Provider Group] ドロップダウン リスト	リモートログイン中にユーザを認証するために使用するデフォルトプロバイダーのグループ。

ステップ 6 [Save Changes] をクリックします。

リモート ユーザのロール ポリシー

デフォルトでは、Cisco UCS Manager でユーザ ロールが設定されていない場合、読み取り専用アクセスが LDAP、RADIUS、または TACACS プロトコルを使用してリモート サーバから Cisco UCS Manager にログインしているすべてのユーザに許可されます。 セキュリティ上の理由から、Cisco UCS Manager で確立されたユーザ ロールに一致しているユーザへアクセスを制限するのが望ましい場合があります。

リモート ユーザのロール ポリシーは次の方法で設定可能です。

assign-default-role

ユーザ ロールに基づいて Cisco UCS Manager へのユーザ アクセスを制限しません。 Cisco UCS Manager でその他のユーザ ロールが定義されていない場合、すべてのユーザに読み取り専用アクセスが許可されます。

これはデフォルトの動作です。

no-login

ユーザ ロールに基づいて Cisco UCS Manager へのユーザ アクセスを制限します。 ユーザ ロールがリモート認証システムに割り当てられていない場合、アクセスは拒否されます。

リモート ユーザのロール ポリシーの設定

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [Authentication] を展開します。

ステップ 3 [Native Authentication] をクリックします。

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

ステップ 5 [Role Policy for Remote Users] フィールドでは、ユーザがログインしようとして、リモート認証プロバイダーでユーザ ロールに認証情報が提供されていないときに何が発生するかを決定するには次のいずれかのオプション ボタンをクリックします。

- [No Login]：ユーザ名とパスワードが正しくても、ユーザはシステムにログインできません。
- [Assign Default Role]：ユーザは、読み取り専用ユーザ ロールでログインできます。

ステップ 6 [Save Changes] をクリックします。

第 9 章

組織の設定

この章の内容は、次のとおりです。

- マルチテナント環境の組織，173 ページ
- マルチテナント環境における階層的な名前解決，174 ページ
- ルート組織下の組織の作成，176 ページ
- サブ組織下の組織の作成，176 ページ
- 組織の削除，177 ページ

マルチテナント環境の組織

マルチテナント機能を使用すると、Cisco UCS ドメインの大規模な物理インフラストラクチャを、組織と呼ばれる論理エンティティに分割することができます。 その結果、各組織に専用の物理インフラストラクチャを設けなくても各組織を論理的に分離できます。

マルチテナント環境では、関連する組織を通じて、各テナントに一意のリソースを割り当てられます。 これらのリソースには、各種のポリシー、プール、および Quality of Service 定義などがあります。 また、すべてのユーザがすべての組織にアクセスできるようにする必要がない場合は、ロケールを実装して、組織ごとにユーザ権限やロールを割り当てたり、制限したりすることもできます。

マルチテナント環境をセットアップする場合、すべての組織は階層的になります。 最上位の組織は常にルートです。 ルートに作成したポリシーおよびプールはシステム全体にわたるもので、このシステムに含まれるすべての組織で使用できます。 しかし、他の組織で作成されたポリシーやプールが使用できるのは、同じ階層でそれより上にある組織だけです。 たとえば、あるシステムに Finance と HR という組織があり、これらは同じ階層に存在しないとします。 この場合、Finance は HR 組織にあるポリシーは一切使用できず、また、HR は Finance 組織にあるポリシーには一切アクセスできません。 しかし、Finance と HR は両方とも、ルート組織にあるポリシーやプールを使用できます。

マルチテナント環境に組織を作成する場合、各組織、または同じ階層のサブ組織に次のうち 1 つ以上をセットアップすることもできます。

- リソース プール
- ポリシー
- サービス プロファイル
- サービス プロファイル テンプレート

ルート組織は、常にトップ レベルの組織です。

マルチテナント環境における階層的な名前解決

マルチテナント環境では、Cisco UCS は組織の階層を使用して、ポリシーおよびリソース プールの名前を解決します。 Cisco UCS Manager がプールに割り当てられているポリシーまたはリソースの詳細を検索すると、次のことが起こります。

1. Cisco UCS Manager Cisco UCS Manager が、サービス プロファイルまたはポリシーに割り当てられた組織内で指定した名前のポリシーまたはプールの有無を調べます。
2. ポリシーが検出されるか、使用可能なリソースがプール内に存在する場合、Cisco UCS Manager はこのポリシーまたはリソースを使用します。 ローカル レベルで使用可能なリソースがプールに存在しない場合、Cisco UCS Manager は階層内で上位の親組織に移動し、同じ名前のプールを検索します。 Cisco UCS Manager Cisco UCS Manager は、検索がルート組織に到達するまでこの手順を繰り返します。
3. 検索がルート組織まで到達し、使用可能なリソースまたはポリシーが検出されない場合、Cisco UCS Manager はローカル組織に戻り、デフォルト プール内でデフォルト ポリシーまたは使用可能なリソースの検出を開始します。
4. 適用可能なデフォルト ポリシーまたは使用可能なリソースがデフォルト プール内で検出されると、Cisco UCS Manager はこのポリシーまたはリソースを使用します。 プール内に使用可能なリソースが存在しない場合、Cisco UCS Manager は階層内で上位の親組織に移動し、デフォルト プールを検索します。 Cisco UCS Manager Cisco UCS Manager は、検索がルート組織に到達するまでこの手順を繰り返します。
5. Cisco UCS Manager は適用可能なポリシーまたは使用可能なリソースを階層内で検出できない場合、割り当てエラーを返します。

例：単一階層でのサーバ プール名の解決

この例では、すべての組織がルート組織下の同一レベルにあります。 たとえば、サービスプロバイダーは、各顧客に対して個別の組織を作成します。 この構成では、組織は、自身の組織およびルート組織に割り当てられたポリシーおよびリソースだけにアクセスできます。

この例では、XYZcustomer 組織のサービス プロファイルは、XYZcustomer サーバ プールのサーバを使用するように設定されています。 リソース プールおよびポリシーがサービス プロファイルに割り当てられると、次のことが発生します。

1. Cisco UCS Manager Cisco UCS Manager が、XYZcustomer サーバ プール内で使用可能なサーバの有無を調べます。

2. XYZcustomer サーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 プール内に使用可能なサーバが存在しない場合、Cisco UCS Manager はルート組織で同じ名前のサーバ プールの有無を調べます。
3. ルート組織に XYZcustomer サーバ プールが含まれており、このプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 プール内に使用可能なサーバが存在しない場合、Cisco UCS Manager は XYZcustomer 組織に戻り、デフォルトのサーバ プールを調べます。
4. XYZcustomer 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager はルート組織内でデフォルトのサーバ プールを調べます。
5. ルート組織内のデフォルトのサーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は割り当てエラーを返します。

例：多階層でのサーバ プール名の解決

この例では、各組織に少なくとも 1 つのサブ組織が含まれています。 たとえば、企業は、企業内の各主要部門に対しておよびこれらの部門のサブ部門に対して組織を作成できます。 この構成では、各組織が、自身のローカル ポリシーとリソース プール、および親階層内のリソース プールにアクセスできます。

この例では、Finance 組織に 2 つのサブ組織（AccountsPayable および AccountsReceivable）が含まれています。 AccountsPayable（AP）組織のサービス プロファイルは、AP サーバ プールのサーバを使用するように設定されています。 リソース プールおよびポリシーがサービス プロファイルに割り当てられると、次のことが発生します。

1. Cisco UCS Manager Cisco UCS Manager が、サービス プロファイルに定義されている AP サーバ プール内で使用可能なサーバの有無を調べます。
2. AP サーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、Finance 組織で同じ名前のプールの有無を調べます。
3. Finance 組織に同じ名前のプールが含まれており、このプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、ルート組織で同じ名前のプールの有無を調べます。
4. ルート組織に同じ名前のプールが含まれており、このプールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は AccountsPayable 組織に戻り、デフォルトのサーバ プールを調べます。

5. AccountsPayable 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、Finance 組織のデフォルトのサーバ プールを調べます。
6. Finance 組織内のデフォルト プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は 1 階層上位に移動し、ルート組織のデフォルトのサーバ プールを調べます。
7. ルート組織内のデフォルトのサーバ プールに使用可能なサーバが存在する場合、Cisco UCS Manager はこのサーバとサービス プロファイルを関連付け、検索を終了します。 デフォルト プールに使用可能なサーバが存在しない場合、Cisco UCS Manager は割り当てエラーを返します。

ルート組織下の組織の作成

手順

ステップ 1 ツールバーで、[New] > [Create Organization] を選択します。

ステップ 2 [Create Organization] ダイアログボックスの [Name] フィールドに、組織の一意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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

ステップ 3 [Description] フィールドに、組織の説明を入力します。

ステップ 4 [OK] をクリックします。

サブ組織下の組織の作成

手順

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

ステップ 2 [Servers] タブで、[Service Profiles] > [root] を展開します。
[Policies] ノードまたは [Pools] ノードの下の [Sub-Organizations] ノードにもアクセスできます。

ステップ 3 [Sub-Organizations] ノードを展開し、次のいずれかの手順を実行します。

- ルート直下に組織を作成するには、[Sub-Organizations] を右クリックし、[Create Organization] を選択します。

- より低いレベルのサブ組織の下に組織を作成するには、階層内のサブ組織ノードを展開してから、新しい組織を作成するサブ組織を右クリックし、[Create Organization] を選択します。

ステップ 4 [Create Organization] ダイアログボックスの [Name] フィールドに、組織の一意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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

ステップ 5 [Description] フィールドに、組織の説明を入力します。

ステップ 6 [OK] をクリックします。

組織の削除

手順

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

ステップ 2 削除する組織に移動します。

ステップ 3 組織を右クリックし、[Delete] を選択します。

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

第 10 章

ロールベース アクセス コントロールの設定

この章の内容は、次のとおりです。

- ロールベース アクセス コントロール，179 ページ
- Cisco UCS のユーザ アカウント，180 ページ
- ユーザ ロール，183 ページ
- ユーザ ロケール，188 ページ
- ユーザ ロールの設定，189 ページ
- ロケールの設定，191 ページ
- ローカル認証されたユーザ アカウントの設定，193 ページ
- ローカル認証されたユーザのパスワード プロファイル，200 ページ
- ユーザ セッションのモニタリング，203 ページ

ロールベース アクセス コントロール

ロールベース アクセス コントロール（RBAC）は、ユーザのロールとロケールに基づいてユーザのシステムアクセスを制限または許可する方法です。 ロールによってシステム内でのユーザの権限が定義され、ロケールによってユーザがアクセス可能な組織（ドメイン）が定義されます。 権限がユーザに直接割り当てられることはないため、個々のユーザ権限の管理では、適切なロールとロケールを割り当てることが主な作業になります。

必要なシステム リソースへの書き込みアクセス権限がユーザに与えられるのは、割り当てられたロールによりアクセス権限が与えられ、割り当てられたロケールによりアクセスが許可されている場合に限ります。 たとえば、エンジニアリング組織内のサーバ管理者ロールを持つユーザは、エンジニアリング組織内のサーバ設定を更新できますが、そのユーザに割り当てられたロケールに財務組織が含まれていなければ、財務組織内のサーバ設定を更新できません。

Cisco UCS のユーザ アカウント

ユーザ アカウントは、システムにアクセスするために使用されます。 最大で 48 のユーザ アカウントを各 Cisco UCS Manager ドメインで設定できます。 各ユーザ アカウントには、一意のユーザ名とパスワードが必要です。

ユーザ アカウントは、SSH 公開キーを付けて設定できます。 公開キーは、OpenSSH と SECSH のいずれかの形式で設定できます。

Admin アカウント

各 Cisco UCS ドメインに admin アカウントがあります。 管理者アカウントはデフォルト ユーザ アカウントで、変更も削除もできません。 このアカウントは、システム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられています。 admin アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

admin アカウントは常にアクティブで、有効期限がありません。 admin アカウントを非アクティブに設定することはできません。

ローカル認証されたユーザのアカウント

ローカル認証されたユーザのアカウントは、ファブリック インターコネクトによって直接認証され、admin または aaa 権限を持つ人なら誰でもイネーブルまたはディセーブルにすることができます。 ローカル ユーザ アカウントがディセーブルになっている場合、ユーザはログインできません。 ディセーブルにされたローカル ユーザ アカウントの設定の詳細はデータベースによって削除されません。 ディセーブルにされたローカル ユーザ アカウントを再度イネーブルにすると、そのアカウントはユーザ名とパスワードを含む既存の設定で再びアクティブになります。

リモート認証されたユーザのアカウント

リモート認証されたユーザのアカウントは、LDAP、RADIUS、または TACACS+ で認証されたユーザ アカウントです。

ユーザが、ローカルユーザアカウントとリモートユーザのアカウントを同時に保持すると、ローカル ユーザ アカウントに定義されているロールがリモート ユーザ アカウントに保持されているロールを上書きします。

ユーザ アカウントの有効期限

ユーザアカウントは、事前に定義した時間に有効期限が切れるように設定できます。 有効期限の時間になると、ユーザ アカウントはディセーブルになります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

（注） 有効期限の日付をユーザ アカウントに設定した後で、期限切れにならないようにそのアカウントを再設定することはできません。 ただし、使用可能な最新の有効期限日でそのアカウントを設定することはできます。

Cisco UCS ユーザ名に関する注意事項

ユーザ名は Cisco UCS Manager に対するログイン ID としても使用されます。 Cisco UCS のユーザ アカウントにログイン ID を割り当てるときは、次の注意事項および制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）
- ログイン ID は Cisco UCS Manager 内で固有でなければなりません。
- ログイン ID は英字で開始する必要があります。 アンダースコアなどの特殊文字または数字で開始することはできません。
- ログイン ID では、大文字と小文字が区別されます。
- すべて数字のログイン ID を作成することはできません。
- ユーザ アカウントを作成した後は、ログイン ID を変更できません ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

予約語：ローカル認証されたユーザのアカウント

次の語はローカル ユーザ アカウントを Cisco UCS で作成する場合に使用することはできません。

- root
- bin
- daemon
- adm
- lp
- sync
- shutdown

- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

Cisco UCS パスワードの注意事項

ローカル認証されたユーザの各アカウントにパスワードが必要です。 admin または aaa 権限を持つユーザは、ユーザ パスワードのパスワード強度チェックを実行するように、Cisco UCS Manager を設定できます。 パスワード強度チェックをイネーブルにすると、各ユーザには強力なパスワードが必要です。

シスコでは、各ユーザが強力なパスワードを持つことを推奨します。 ローカル認証されたユーザにパスワード強度チェックをイネーブルにした場合、Cisco UCS Manager は、次の要件を満たさないすべてのパスワードを拒否します。

- 8 ～ 80 文字で構成する必要がある。
- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字

- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントには、空白を含めない。

ユーザ アカウントの Web セッション制限

Web セッション制限が、特定のユーザ アカウントが常時アクセスを許可される Web セッション（GUI および XML の両方）の数を制限するために Cisco UCS Manager によって使用されます。

デフォルトでは、Cisco UCS Manager により許可される同時 Web セッションの数は 32 に設定されます。ただし、この値はシステムの最大値 256 まで設定可能です。

ユーザ ロール

ユーザ ロールは、ユーザに許可された操作を定義する 1 つ以上の権限を含みます。 1 つ以上のロールを各ユーザに割り当てることができます。 複数のロールを持つユーザは、すべての割り当てロールを組み合わせた権限を持ちます。 たとえば、Role1 にストレージ関連の権限があり、Role2 にサーバ関連の権限がある場合、Role1 と Role2 を持つユーザはストレージ関連およびサーバ関連の両方の権限を持ちます。

Cisco UCS ドメインにはデフォルト ユーザ ロールを含めて最大 48 のユーザ ロールを含めることができます。 最初の 48 より後で設定されたユーザ ロールはすべて受け入れられますが、エラーが生成されて非アクティブになります。

すべてのロールには、Cisco UCS ドメイン内のすべての設定に対する読み取りアクセス権限が含まれています。 読み取り専用ロールを持つユーザは、システム状態を変更できません。

ロールは、作成、変更（新しい権限の追加や既存の権限の削除）、および削除できます。 ロールを変更すると、そのロールを持つすべてのユーザに新しい権限が適用されます。 権限の割り当ては、デフォルトロールに定義されている権限に限定されません。 つまり、カスタムの権限の組み合わせを使用して、独自のロールを作成できます。 たとえば、デフォルトのサーバアドミニストレータ ロールとストレージ アドミニストレータ ロールの持つ権限の組み合わせは異なっていますが、両方のロールの権限を組み合わせた新しい 1 つのサーバおよびストレージ アドミニストレータ ロールを作成できます。

ロールがユーザへの割り当て後に削除されると、それらのユーザ アカウントからも削除されます。

AAA サーバ（RADIUS または TACACS+）上のユーザ プロファイルは、そのユーザに与える権限に対応したロールを追加するように変更する必要があります。 属性はロール情報を保存するために使用されます。 AAA サーバでは、要求とともにこの属性が返され、それを解析してロールが得られます。 LDAP サーバでは、ユーザ プロファイル属性内のロールが返されます。

（注） ローカルユーザアカウントおよびリモートユーザアカウントが同じユーザ名である場合は、リモートユーザに割り当てられたすべてのロールはローカルユーザに割り当てられているロールによって上書きされます。

デフォルトのユーザ ロール

システムには、次のデフォルトのユーザ ロールが用意されています。

AAA アドミニストレータ

ユーザ、ロール、およびAAA設定に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

アドミニストレータ

システム全体に対する完全な読み取りと書き込みのアクセス権。 デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

ファシリティ マネージャ

power-mgmt 権限による電源管理操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

ネットワーク管理者

ファブリック インターコネクト インフラストラクチャとネットワーク セキュリティ操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

オペレーション

システムのログ（syslog サーバを含む）と障害に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

Read-Only

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

サーバ計算

サービス プロファイルのほとんどの側面に対する読み取りと書き込みのアクセス権。 ただし、ユーザは vNIC または vHBA の作成、変更、削除ができません。

サーバ機器アドミニストレータ

物理サーバ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

サーバ プロファイル アドミニストレータ

論理サーバ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

サーバ セキュリティ アドミニストレータ

サーバ セキュリティ関連の操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

ストレージ アドミニストレータ

ストレージ操作に対する読み取りと書き込みのアクセス権。 システムの残りの部分に対する読み取りアクセス権。

予約語：ユーザ ロール

次の語はカスタム ロールを Cisco UCS で作成するときに使用することはできません。

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

権限

ユーザ ロールを割り当てられたユーザは、権限により、特定のシステム リソースへアクセスしたり、特定のタスクを実行したりできるようになります。 次の表に、各権限と、その権限がデフォルトで与えられるユーザ ロールのリストを示します。

ヒント これらの権限とそれによってユーザが実行できるタスクに関する詳細情報は、「*Privileges in Cisco UCS*」に記載されており、次の URL からアクセスできます。http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html

表 *5*：ユーザの権限

特権	説明	デフォルトのロール割り当て
aaa	システム セキュリティおよび AAA	AAA アドミニストレータ
admin	システム管理	アドミニストレータ

特権	説明	デフォルトのロール割り当て
ext-lan-config	外部 LAN 設定	ネットワーク管理者
ext-lan-policy	外部 LAN ポリシー	ネットワーク管理者
ext-lan-qos	外部 LAN QoS	ネットワーク管理者
ext-lan-security	外部 LAN セキュリティ	ネットワーク管理者
ext-san-config	外部 SAN 設定	ストレージアドミニストレータ
ext-san-policy	外部 SAN ポリシー	ストレージアドミニストレータ
ext-san-qos	外部 SAN QoS	ストレージアドミニストレータ
ext-san-security	外部 SAN セキュリティ	ストレージアドミニストレータ
fault	アラームおよびアラーム ポリシー	オペレーション
operations	ログおよび Smart Call Home	オペレーション
org-management	組織管理	オペレーション
pod-config	ポッド設定	ネットワーク管理者
pod-policy	ポッド ポリシー	ネットワーク管理者
pod-qos	ポッド QoS	ネットワーク管理者
pod-security	ポッド セキュリティ	ネットワーク管理者
power-mgmt	電源管理操作に対する読み取りと書き込みのアクセス権	ファシリティ マネージャ
read-only	読み取り専用アクセス権 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。	Read-Only
server-equipment	サーバ ハードウェア管理	サーバ機器アドミニストレータ
server-maintenance	サーバ メンテナンス	サーバ機器アドミニストレータ

特権	説明	デフォルトのロール割り当て
server-policy	サーバ ポリシー	サーバ機器アドミニストレータ
server-security	サーバ セキュリティ	サーバセキュリティアドミニストレータ
service-profile-compute	サービス プロファイル計算	サーバ計算アドミニストレータ
service-profile-config	サービス プロファイル設定	サーバプロファイルアドミニストレータ
service-profile-config-policy	サービスプロファイル設定ポリシー	サーバプロファイルアドミニストレータ
service-profile-ext-access	サービス プロファイル エンドポイント アクセス	サーバプロファイルアドミニストレータ
service-profile-network	サービス プロファイル ネットワーク	ネットワーク管理者
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	ネットワーク管理者
service-profile-qos	サービス プロファイル QoS	ネットワーク管理者
service-profile-qos-policy	サービス プロファイル QoS ポリシー	ネットワーク管理者
service-profile-security	サービス プロファイル セキュリティ	サーバセキュリティアドミニストレータ
service-profile-security-policy	サービス プロファイル セキュリティ ポリシー	サーバセキュリティアドミニストレータ
service-profile-server	サービス プロファイル サーバ管理	サーバプロファイルアドミニストレータ
service-profile-server-oper	サービス プロファイル コンシューマ	サーバプロファイルアドミニストレータ
service-profile-server-policy	サービス プロファイル プールポリシー	サーバセキュリティアドミニストレータ
service-profile-storage	サービスプロファイルストレージ	ストレージアドミニストレータ

特権	説明	デフォルトのロール割り当て
service-profile-storage-policy	サービスプロファイルストレージ ポリシー	ストレージアドミニストレータ

ユーザ ロケール

ユーザには、ロケールを 1 つ以上割り当てることができます。 各ロケールには、ユーザからのアクセスを許可する 1 つ以上の組織（ドメイン）を定義します。アクセスは、このロケールで指定された組織の範囲内に制限されます。 このルールの 1 つの例外として、組織が指定されていないロケールがあります。この場合、すべての組織内のシステム リソースに対して無制限のアクセスが可能になります。

Cisco UCS ドメインには最大 48 のユーザ ロケールを含めることができます。 最初の 48 より後で設定されたユーザ ロケールはすべて受け入れられますが、エラーが生成されて非アクティブになります。

admin または aaa 権限を持つユーザは、組織を他のユーザのロケールに割り当てることができます。 組織の割り当ては、それを行うユーザのロケール内の組織だけに制限されます。 たとえば、ロケールにエンジニアリング組織しか含まれていない場合、そのロケールを割り当てられたユーザは、他のユーザにエンジニアリング組織のみを割り当てることできます。

（注） 次の権限を 1 つ以上持つユーザにロケールを割り当てることはできません。

- aaa
- admin
- fault
- operations

組織は階層的に管理できます。 トップ レベルの組織に割り当てられたユーザは、自動的にその下にあるすべての組織にアクセスできます。 たとえば、エンジニアリング組織が、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織で構成されているとします。 ソフトウェア エンジニアリング組織のみを含むロケールでは、その組織内のシステム リソースにしかアクセスできません。一方、エンジニアリング組織が含まれるロケールでは、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織の両方のリソースにアクセスできます。

ユーザ ロールの設定

ユーザ ロールの作成

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [User Services] を右クリックし、[Create Role] を選択します。
[Roles] を右クリックしてそのオプションにアクセスすることもできます。

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

名前	説明
[Name] フィールド	このユーザ ロールのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Privileges] リスト ボックス	システムに定義されている権限のリスト。 その権限の説明を表示するには、権限をクリックします。チェックボックスをオンにすると、選択したユーザにその権限が割り当てられます。
[Help] セクション	
[Description] フィールド	[Privileges] リスト ボックス内で最後にクリックした権限の説明。

ステップ 5 [OK] をクリックします。

ユーザ ロールへの権限の追加

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Roles] ノードを展開します。

ステップ 4 権限を追加するロールを選択します。

ステップ 5 [General] タブで、ロールに追加する権限に対応する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。

ユーザ ロールからの権限の削除

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Roles] ノードを展開します。

ステップ 4 権限を削除するロールを選択します。

ステップ 5 [General] タブで、ロールから削除する権限に対応するボックスをオフにします。

ステップ 6 [Save Changes] をクリックします。

ユーザ ロールの削除

あるユーザ ロールを削除すると、Cisco UCS Manager により、そのロールは割り当て先のすべてのユーザ アカウントから削除されます。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Roles] ノードを展開します。

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

ステップ 5 [Delete] ダイアログボックスで、[Yes] をクリックします。

ロケールの設定

ロケールの作成

はじめる前に

ロケールを作成するには、1 つ以上の組織が存在する必要があります。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locales] を右クリックし、[Create a Locale] を選択します。

ステップ 4 [Create Locale] ページで、次の手順を実行します。

a) [Name] フィールドに、ロケールの一意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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 5 [Assign Organizations] ダイアログボックスで、次の手順を実行します。

a) Cisco UCS ドメイン内の組織を表示するには、[Organizations] 領域を展開します。

b) [root] ノードを展開して、サブ組織を表示します。

c) ロケールを割り当てる組織をクリックします。

d) [Organizations] 領域の組織を右側のペインの設計領域にドラッグ アンド ドロップします。

e) すべての適切な組織をロケールに割り当てるまで、ステップ b および c を繰り返します。

ステップ 6 [Finish] をクリックします。

次の作業

ロケールを 1 つまたは複数のユーザ アカウントに追加します。 詳細については、ローカル認証されたユーザ アカウントに割り当てられたロケールの変更, （197 ページ）を参照してください。

ロケールへの組織の割り当て

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locales] ノードを展開し、組織を追加するロケールをクリックします。

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

ステップ 5 [Organizations] 領域のテーブル アイコン バーで [+] をクリックします。

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

a) Cisco UCS ドメイン内の組織を表示するには、[Organizations] 領域を展開します。

b) [root] ノードを展開して、サブ組織を表示します。

c) ロケールを割り当てる組織をクリックします。

d) [Organizations] 領域の組織を右側のペインの設計領域にドラッグ アンド ドロップします。

e) すべての適切な組織をロケールに割り当てるまで、ステップ b および c を繰り返します。

ステップ 7 [OK] をクリックします。

ロケールからの組織の削除

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locales] ノードを展開し、組織を削除するロケールをクリックします。

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

ステップ 5 [Organizations] 領域で、ロケールから削除する組織を右クリックし、[Delete] を選択します。

ステップ 6 [Save Changes] をクリックします。

ロケールの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locales] ノードを展開します。

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

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

ローカル認証されたユーザ アカウントの設定

ユーザ アカウントの作成

少なくとも、次のユーザを作成することを推奨します。

- サーバ アドミニストレータ アカウント
- ネットワーク アドミニストレータ アカウント
- ストレージ アドミニストレータ

はじめる前に

システムに次のいずれかがある場合は、該当するタスクを実行します。

- リモート認証サービス：ユーザがリモート認証サーバに存在すること、および適切なロールと権限を持っていることを確認します。
- 組織のマルチテナント機能：1 つ以上のロケールを作成します。 ロケールが 1 つもない場合、すべてのユーザはルートに作成され、すべての組織のロールと権限が割り当てられます。
- SSH 認証。SSH キーを取得します。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [User Services] を右クリックし、[Create User] を選択して [User Properties] ダイアログボックスを開きます。

[Locally Authenticated Users] を右クリックしてそのオプションにアクセスすることもできます。

ステップ 4 ユーザに関して要求される情報を使用して、次のフィールドに値を入力します。

名前	説明
[Login ID] フィールド	このアカウントにログインするときに使用されるアカウント名。このアカウントは固有であるとともに、Cisco UCS Manager ユーザアカウントに関する次のガイドラインと制約事項を満たしている必要があります。 • ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。 ◦ 任意の英字 ◦ 任意の数字 ◦ _（アンダースコア） ◦ -（ダッシュ） ◦ .（ドット） • ログイン ID は Cisco UCS Manager 内で固有でなければなりません。 • ログイン ID は英字で開始する必要があります。 アンダースコアなどの特殊文字または数字で開始することはできません。 • ログイン ID では、大文字と小文字が区別されます。 • すべて数字のログイン ID を作成することはできません。 • ユーザ アカウントを作成した後は、ログイン ID を変更できません ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。 ユーザを保存した後は、ログイン ID を変更できません。 ユーザアカウントを削除し、新しいユーザアカウントを作成する必要があります。
[First Name] フィールド	ユーザの名。 このフィールドには、32 文字までの値を入力できます。
[Last Name] フィールド	ユーザの姓。 このフィールドには、32 文字までの値を入力できます。
[Email] フィールド	ユーザの電子メール アドレス。
[Phone] フィールド	ユーザの電話番号。

名前	説明
[Password] フィールド	このアカウントに関連付けられているパスワード。 パスワード強度のチェックをイネーブルにすると、ユーザパスワードを強くする必要があり、次の要件を満たしていないパスワードは Cisco UCS Manager によってすべて拒否されます。 • 8 ～ 80 文字で構成する必要がある。 • 次の少なくとも 3 種類を含む。 ◦ 小文字 ◦ 大文字 ◦ 数字 ◦ 特殊文字 • aaabbb など連続して 3 回を超えて繰り返す文字を含まない。 • ユーザ名と同一、またはユーザ名を逆にしたものではない。 • パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。 • 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。 • ローカルユーザアカウントおよびadminアカウントには、空白を含めない。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[Account Status] フィールド	ステータスが [Active] に設定されている場合、ユーザはこのログイン ID とパスワードを使用して Cisco UCS Manager にログインできます。
[Account Expires] チェックボックス	オンにすると、[Expiration Date] フィールドに指定された日を経過した後、このアカウントは期限切れになり、使用できなくなります。 （注） 有効期限の日付をユーザアカウントに設定した後で、期限切れにならないようにそのアカウントを再設定することはできません。 ただし、使用可能な最新の有効期限日でそのアカウントを設定することはできます。

名前	説明
[Expiration Date] フィールド	アカウントの期限が切れる日付。 日付の形式は yyyy-mm-dd です。 このフィールドの終端にある下矢印をクリックするとカレンダーが表示されるので、それを使用して期限日を選択できます。 （注） [Account Expires] チェックボックスをオンにすると、Cisco UCS Manager GUI にこのフィールドが表示されます。

ステップ 5 [Roles] 領域で 1 つ以上のボックスをオンにして、ユーザ アカウントにロールと権限を割り当てます。

（注） admin または aaa ロールを持つユーザにロケールを割り当てないでください。

ステップ 6 （任意） システムに組織が含まれる場合、[Locales] 領域の 1 つ以上のチェックボックスをオンにして、適切なロケールをユーザに割り当てます。

ステップ 7 [SSH] 領域で、次のフィールドに値を入力します。

a) [Type] フィールドで、次をクリックします。

- [Password Required]：ユーザはログインするときにパスワードを入力する必要があります。
- [Key]：このユーザがログインするときに、Secure Shell（SSH; セキュア シェル） 暗号化が使用されます。

b) [Key] を選択する場合、[SSH data] フィールドに SSH キーを入力します。

ステップ 8 [OK] をクリックします。

ローカル認証されたユーザのパスワード強度チェックのイネーブル化

パスワード強度のチェックを有効にするには、admin または aaa 権限を持つユーザである必要があります。 パスワード強度のチェックをイネーブルにすると、Cisco UCS Manager によって、ユーザは強力なパスワードのガイドラインを満たしていないパスワードを選択できなくなります。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Work] ペインで、[Properties] 領域の[Password Strength Check] チェックボックスをオンにします。

ステップ 5 [Save Changes] をクリックします。

Cisco UCS Manager GUI ユーザの Web セッション制限の設定

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Communication Services] を展開します。

ステップ 3 [Communication Services] タブをクリックします。

ステップ 4 [Web Session Limits] 領域で、次のフィールドに値を入力します。

名前	説明
[Maximum Sessions Per User] フィールド	各ユーザに許可されている HTTP および HTTPS の同時セッションの最大数。 1 ～ 256 の整数を入力します。
[Maximum Sessions] フィールド	システム内のすべてのユーザに許可されている HTTP および HTTPS の同時セッションの最大数。 1 ～ 256 の整数を入力します。

ステップ 5 [Save Changes] をクリックします。

ローカル認証されたユーザ アカウントに割り当てられたロケールの変更

（注） admin または aaa ロールを持つユーザにロケールを割り当てないでください。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] > [Locally Authenticated Users] を展開します。

ステップ 3 修正するユーザ アカウントをクリックします。

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

ステップ 5 [Locales] 領域で、次の手順を実行します。

- ユーザアカウントに新しいロケールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザアカウントからロケールを削除するには、適切なチェックボックスをオフにします。

ステップ 6 [Save Changes] をクリックします。

ローカル認証されたユーザ アカウントに割り当てられたロールの変更

ユーザロールと権限の変更は、ユーザが次にログインするまで有効になりません。新しいロールをユーザアカウントに追加するか、既存のロールをユーザアカウントから削除するときにユーザがログインしていると、前のロールと権限を使用してアクティブなセッションが続行されます。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] > [Locally Authenticated Users] を展開します。

ステップ 3 修正するユーザ アカウントをクリックします。

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

ステップ 5 [Roles] 領域で、次の手順を実行します。

- ユーザアカウントに新しいロールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザ アカウントからロールを削除するには、適切なチェックボックスをオフにします。

ステップ 6 [Save Changes] をクリックします。

ユーザ アカウントの有効化

ローカル ユーザ アカウントを有効または無効にするには、admin または aaa 権限を持つユーザである必要があります。

はじめる前に

ローカル ユーザ アカウントを作成します。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] > [Locally Authenticated Users] を展開します。

ステップ 3 有効にするユーザをクリックします。

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

ステップ 5 [Account Status] フィールドで、[active] オプション ボタンをクリックします。

ステップ 6 [Save Changes] をクリックします。

ユーザ アカウントの無効化

ローカル ユーザ アカウントを有効または無効にするには、admin または aaa 権限を持つユーザである必要があります。

（注） ディセーブルにされているアカウントのパスワードを Cisco UCS Manager GUI によって変更すると、ユーザはアカウントをイネーブルにしてアクティブにした後でこの変更されたパスワードを使用できません。 ユーザはアカウントがイネーブルにされアクティブになった後で、必要なパスワードをもう一度入力する必要があります。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] > [Locally Authenticated Users] を展開します。

ステップ 3 無効にするユーザをクリックします。

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

ステップ 5 [Account Status] フィールドで、[inactive] オプション ボタンをクリックします。
admin ユーザ アカウントは常にアクティブに設定されます。 これは変更できません。

ステップ 6 [Save Changes] をクリックします。

ローカル認証されたユーザのパスワード履歴のクリア

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] > [Locally Authenticated Users] を展開します。

ステップ 3 パスワード履歴をクリアするユーザをクリックします。

ステップ 4 [Actions] 領域で、[Clear Password History] をクリックします。

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

ローカルに認証されたユーザ アカウントの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locally Authenticated Users] ノードを展開します。

ステップ 4 削除するユーザ アカウントを右クリックし、[Delete] を選択します。

ステップ 5 [Delete] ダイアログボックスで、[Yes] をクリックします。

ローカル認証されたユーザのパスワード プロファイル

パスワード プロファイルには、Cisco UCS Manager のすべてのローカル認証されたユーザのパスワード履歴およびパスワード変更間隔のプロパティが含まれます。 それぞれのローカル認証されたユーザに異なるパスワード プロファイルを指定することはできません。

（注） パスワード プロファイル プロパティを変更するには、admin または AAA 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは admin または AAA 権限を持つユーザには適用されません。

パスワード履歴カウント

パスワード履歴カウントにより、ローカル認証されたユーザが同じパスワードを何度も再利用することを防止できます。 このプロパティが設定されている場合、Cisco UCS Manager は、ローカル認証されたユーザが以前に使用したパスワードを最大15パスワードまで保存します。 パスワードは、履歴カウントしきい値に達した場合に最も古いパスワードだけが再使用できるように、最新パスワードから最初に新しい順に保存されます。

ユーザは、パスワード履歴に設定されている数のパスワードを作成して使用しなければ、パスワードを再利用できるようになりません。 たとえば、パスワード履歴カウントを 8 に設定した場合、ローカル認証されたユーザは、9 番めのパスワードが期限切れになってからでなければ、最初のパスワードを再利用できません。

デフォルトでは、パスワード履歴は 0 に設定されます。 この値は、履歴カウントをディセーブルにし、ユーザがいつでも前のパスワードを使用できるようになります。

必要に応じて、ローカル認証されたユーザに対してパスワード履歴カウントをクリアし、以前のパスワードの再利用をイネーブルにできます。

パスワード変更間隔

パスワード変更間隔を使用すると、ローカル認証されたユーザが一定の時間内に行うことができるパスワード変更の回数を制限できます。 次の表に、パスワード変更間隔の 2 つの設定オプションについての説明を示します。

間隔の設定	説明	例
許可するパスワード変更なし	このオプションは、ローカル認証されたユーザのパスワードが、パスワード変更後の指定時間内に変更されることを許可しません。 変更なし間隔に指定できる時間の範囲は、1 ～ 745 時間です。 デフォルトでは、変更なし間隔は 24 時間です。	たとえば、ローカル認証されたユーザが自分のパスワードを変更してから 48 時間以内に、パスワードが変更されないようにするには、次のように設定します。 • 間隔中の変更をディセーブル • 変更なし間隔を 48
変更間隔内でパスワード変更を許可	このオプションはローカル認証されたユーザのパスワードを定義済み間隔内に変更できる最大回数を指定します。 変更間隔は 1 ～ 745 時間の範囲で、パスワード変更の最大回数は 0 ～ 10 の範囲で指定できます。 デフォルトでは、ローカル認証されたユーザは、48 時間間隔内で最大 2 回のパスワード変更を許可されます。	たとえば、ローカル認証されたユーザが自分のパスワードを変更してから 24 時間以内に、最大 1 回の変更を許可するには、次のように設定します。 • 間隔中の変更をイネーブル • 変更カウントを 1 • 変更間隔を 24

変更間隔のパスワード変更の最大回数の設定

パスワード プロファイル プロパティを変更するには、admin または AAA 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは admin または AAA 権限を持つユーザには適用されません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Password Profile] 領域で、次の手順を実行します。

a) [Change During Interval] フィールドで、[Enable]をクリックします。

b) [Change Count] フィールドで、間隔の変更中に、ローカルで認証されたユーザが自分のパスワードを変更できる最大回数を入力します。
この値は 0 ～ 10 の間で、自由に設定できます。

c) [Change Interval] フィールドで、[Change Count] フィールドに指定されているパスワードの変更回数が適用される最大時間数を入力します。
この値は 1 ～ 745 時間の間で、自由に設定できます。

たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカルで認証されたユーザは48時間以内に2回しかパスワードの変更を行えません。

ステップ 5 [Save Changes] をクリックします。

パスワードの変更なし間隔の設定

パスワード プロファイル プロパティを変更するには、admin または AAA 権限を持っている必要があります。 パスワード履歴を除き、これらのプロパティは admin または AAA 権限を持つユーザには適用されません。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Password Profile] 領域で、次の手順を実行します。

a) [Change During Interval] フィールドで、[Disable] をクリックします。

b) [No Change Interval] フィールドで、新しく作成されたパスワードを変更するまでに、ローカルで許可されたユーザが待機する必要のある最小時間数を入力します。

この値は 1 ～ 745 時間の間で、自由に設定できます。

この間隔は、[Change During Interval] プロパティが [Disable] に設定されていない場合は無視されます。

ステップ 5 [Save Changes] をクリックします。

パスワード履歴カウントの設定

パスワード プロファイル プロパティを変更するには、admin または AAA 権限を持っている必要があります。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] > [User Services] を展開します。

ステップ 3 [Locally Authenticated Users] ノードをクリックします。

ステップ 4 [Password Profile] 領域で、[History Count] フィールドに、ローカル認証されたユーザが以前に使用したパスワードを再使用できるようになる前に作成する必要がある一意のパスワードの数を入力します。
この値は 0 ～ 15 の間で、自由に設定できます。

デフォルトで、[History Count] フィールドは 0 に設定されます。これによって履歴数がディセーブルになり、ユーザは以前に使用したパスワードをいつでも使用できるようになります。

ステップ 5 [Save Changes] をクリックします。

ユーザ セッションのモニタリング

CLI または GUI のいずれでログインしているかに関係なく、ローカル認証されたユーザとリモート認証されたユーザの両方について、Cisco UCS Manager セッションをモニタできます。

手順

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

ステップ 2 [Admin] タブで、[All] > [User Management] を展開します。

ステップ 3 [User Services] ノードをクリックします。

ステップ 4 [Work] ペインで [Sessions] タブをクリックします。
このタブには、ユーザ セッションに関する次の詳細情報が表示されます。

名前	説明
[Name] カラム	セッションの名前。
[User] カラム	セッションに参加しているユーザ名。
[Fabric ID] カラム	このセッションのためにユーザがログインしているファブリック インターコネクト。
[Login Time] カラム	セッションが開始された日時。
[Refresh Period] カラム	Web クライアントが Cisco UCS Manager に接続する場合、クライアントはリフレッシュ要求を Cisco UCS Manager に送信して Web セッションをアクティブに保つ必要があります。 このオプションによって、このドメイン内のユーザに対するリフレッシュ要求の間に許容される最大時間が指定されます。 この時間制限を超えると、Cisco UCS Manager は Web セッションが非アクティブであると見なしますが、セッションは終了されません。
[Session Timeout] カラム	Cisco UCS Manager が、Web セッションが終了したと見なす前提となる最終リフレッシュ要求後の最大経過時間。 この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了します。
[Terminal Type] カラム	ユーザがログインするときに使用する端末の種類。
[Host] カラム	ユーザのログイン元である IP アドレス。
[Current Session] カラム	このカラムに [Y] が表示された場合、関連付けられているユーザ セッションは現在アクティブです。

第 11 章

DNS サーバの設定

この章の内容は、次のとおりです。

- Cisco UCS の DNS サーバ，205 ページ
- DNS サーバの追加，205 ページ
- DNS サーバの削除，206 ページ

Cisco UCS の DNS サーバ

システムがホスト名の名前解決を必要とする場合は、使用する外部 DNS サーバを各 Cisco UCS ドメインに指定する必要があります。 たとえば、DNS サーバを設定していないと、ファブリックインターコネクトに関する設定を行うときに、www.cisco.com などの名前を使用できません。 サーバの IP アドレスを使用しなければならなくなります。

DNS サーバの追加

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Services] を展開します。

ステップ 3 [DNS Management] をクリックします。

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

ステップ 5 [DNS Server] 領域で、[+] をクリックします。

ステップ 6 [Specify DNS Server] ダイアログボックスで、ドメイン ネーム システム（DNS）サーバの IP アドレスを入力します。

ステップ 7 [OK] をクリックします。

DNS サーバの削除

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Services] を展開します。

ステップ 3 [DNS Management] をクリックします。

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

ステップ 5 [DNS Server] 領域で、削除する DNS サーバを右クリックし、[Delete] を選択します。

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

ステップ 7 [Save Changes] をクリックします。

第 12 章

システム関連ポリシーの設定

この章の内容は、次のとおりです。

- シャーシ ディスカバリ ポリシーの設定，207 ページ
- シャーシ接続ポリシーの設定，211 ページ
- ラック サーバ ディスカバリ ポリシーの設定，212 ページ
- MAC アドレス テーブルのエージング タイムの設定，214 ページ

シャーシ ディスカバリ ポリシーの設定

シャーシ ディスカバリ ポリシー

シャーシディスカバリ ポリシーでは、新しいシャーシを追加した際のシステムによる対応方法が規定されます。 Cisco UCS Manager は、シャーシ ディスカバリ ポリシー内の設定を使用して、シャーシとファブリック インターコネクトの間のリンク数の最小しきい値と、IOM からファブリック ポート チャネルのファブリック インターコネクトへのリンクをグループ化するかどうかを決定します。

シャーシ リンク

リンク数 1、2、4、および 8 のリンクで配線されたシャーシの Cisco UCS ドメインがある場合は、Cisco UCS Manager が、すべてのシャーシを検出できるように、ドメインの最小リンク数にシャーシ ディスカバリ ポリシーを設定することを推奨します。

ヒント　リンク数が異なる IOM が混在する Cisco UCS 実装については、プラットフォーム最大値を使用することを推奨します。 プラットフォーム最大値を使用すると、Cisco UCS Manager は、使用可能な IOM アップリンクの最大数を使用することが保証されます。

初回の検出後、設定よりも配線されるリンク数が多いシャーシを再認識させると、すべての使用可能なリンクをシャーシが使用するように Cisco UCS Manager によって設定されます。

Cisco UCS Manager は、シャーシ ディスカバリ ポリシーで設定されたリンク数よりも、配線されるリンク数が少ないシャーシを検出できません。 たとえば、シャーシ ディスカバリ ポリシーがリンク数 4 で設定されている場合、Cisco UCS Manager は配線されるリンク数が 1 または 2 のシャーシを検出できません。 シャーシを再認識させても、この問題は解決されません。

次の表は、複数のシャーシで構成された Cisco UCS ドメインにおけるシャーシ ディスカバリ ポリシーの動作の概要を示しています。

表 *6*：シャーシ ディスカバリ ポリシーとシャーシのリンク

シャーシで配線されるリンク数	シャーシ ディスカバリ ポリシーのリンク数が 1	シャーシ ディスカバリ ポリシーのリンク数が 2	シャーシ ディスカバリ ポリシーのリンク数が 4	シャーシ ディスカバリ ポリシーのリンク数が 8	プラットフォーム最大値ディスカバリ ポリシー
IOM とファブリック インターコネクト間で 1 つのリンクが存在	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 1 で配線されるシャーシとして追加されます。	シャーシは Cisco UCS Manager で検出できず、Cisco UCS ドメインに追加されません。	シャーシは Cisco UCS Manager で検出できず、Cisco UCS ドメインに追加されません。	シャーシは Cisco UCS Manager で検出できず、Cisco UCS ドメインに追加されません。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 1 で配線されるシャーシとして追加されます。
IOM とファブリック インターコネクト間で 2 つのリンクが存在	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 1 で配線されるシャーシとして追加されます。 初回の検出の後にシャーシを再認識させると、Cisco UCS Manager で再認識され、追加のリンクが使用されます。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 2 で配線されるシャーシとして追加されます。	シャーシは Cisco UCS Manager で検出できず、Cisco UCS ドメインに追加されません。	シャーシは Cisco UCS Manager で検出できず、Cisco UCS ドメインに追加されません。	シャーシは Cisco UCS Manager で検出できず、Cisco UCS ドメインに追加されません。

シャーシで配線されるリンク数	シャーシディスカバリポリシーのリンク数が 1	シャーシディスカバリポリシーのリンク数が 2	シャーシディスカバリポリシーのリンク数が 4	シャーシ ディスカバリ ポリシーのリンク数が 8	プラットフォーム最大値ディスカバリ ポリシー
IOM とファブリック インターコネクト間で 4 つのリンクが存在	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 1 で配線されるシャーシとして追加されます。 初回の検出の後にシャーシを再認識させると、Cisco UCS Manager で再認識され、追加のリンクが使用されます。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 2 で配線されるシャーシとして追加されます。 初回の検出の後にシャーシを再認識させると、Cisco UCS Manager で再認識され、追加のリンクが使用されます。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 4 で配線されるシャーシとして追加されます。	シャーシは Cisco UCS Manager で検出できず、Cisco UCS ドメインに追加されません。	IOM のリンク数が 4 の場合、シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 4 で配線されるシャーシとして追加されます。 IOM のリンク数が 8 の場合、シャーシは Cisco UCS Manager で完全には検出されません。
IOM とファブリック インターコネクト間で 8 つのリンクが存在	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 1 で配線されるシャーシとして追加されます。 初回の検出の後にシャーシを再認識させると、Cisco UCS Manager で再認識され、追加のリンクが使用されます。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 2 で配線されるシャーシとして追加されます。 初回の検出の後にシャーシを再認識させると、Cisco UCS Manager で再認識され、追加のリンクが使用されます。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 4 で配線されるシャーシとして追加されます。 初回の検出の後にシャーシを再認識させると、Cisco UCS Manager で再認識され、追加のリンクが使用されます。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 8 で配線されるシャーシとして追加されます。	シャーシは Cisco UCS Manager で検出され、Cisco UCS ドメインにリンク数 8 で配線されるシャーシとして追加されます。

リンクのグループ化

ファブリック ポートチャネルをサポートするハードウェア構成については、IOMからファブリック インターコネクトへのすべてのリンクをシャーシ ディスカバリの実行中にファブリック ポートチャネルにグループ化するかどうかは、リンクのグループ化によって決まります。 リンクのグループ化の設定が port channel に設定されている場合、IOM からファブリック インターコネクトへのすべてのリンクはファブリック ポートのチャネルにグループ化されます。 グループなしに設定すると、IOM からファブリック インターコネクトへのリンクはファブリック ポート チャネルにグループ化されません。

ファブリック ポート チャネルが作成されると、リンク グループの設定を変更してシャーシを再認識させ、ポート チャネルからシャーシをイネーブルまたはディセーブルにすることによって、リンクを追加または削除できます。

（注） リンク グループのプリファレンスは、IOM または FEX とファブリック インターコネクトの間のリンクの両方の側がファブリック ポート チャネルをサポートする場合にのみ影響を及ぼします。 リンクの一方の側がファブリック ポート チャネルをサポートしていない場合、このプリファレンスは無視され、リンクはポート チャネルにグループ化されません。

シャーシ ディスカバリ ポリシーの設定

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 [Chassis Discovery Policy] 領域で、次のフィールドに値を入力します。

名前	説明
[Action] フィールド	シャーシとファブリック インターコネクトの間のリンクの最小しきい値を指定します。 次のいずれかになります。 • 1-link • 2-link • 4-link • 8-link • プラットフォームの最大値

名前	説明
[Link Grouping Preference] フィールド	IOM からファブリック インターコネクトへのリンクがポートチャネルにグループ化されるかどうかを指定します。 次のいずれかになります。 • [None]：ポート チャネルにリンクはグループ化されません。 • [Port Channel]：IOM からファブリック インターコネクトへのすべてのリンクがポートチャネルにグループ化されます。 （注） リンク グループのプリファレンスは、IOM または FEX とファブリック インターコネクトの間のリンクの両方の側がファブリック ポート チャネルをサポートする場合にのみ影響を及ぼします。 リンクの一方の側がファブリック ポート チャネルをサポートしていない場合、このプリファレンスは無視され、リンクはポート チャネルにグループ化されません。

ステップ 6 [Save Changes] をクリックします。

次の作業

特定のシャーシのファブリック ポートのチャネル接続をカスタマイズするには、シャーシの接続ポリシーを設定します。

シャーシ接続ポリシーの設定

シャーシ接続ポリシー

シャーシ接続ポリシーは、シャーシの検出後に特定のシャーシをファブリック ポートチャネルに含めるかどうかを決定します。 このポリシーは、グローバル シャーシ ディスカバリ ポリシーで指定されたものと異なるように 1 つ以上のシャーシを設定するユーザに役立ちます。 シャーシ接続ポリシーは、ファブリック インターコネクトごとに異なる接続モードにも対応し、シャーシ接続に関して提供される制御レベルをそれ以上に拡張できます。

デフォルトでは、シャーシ接続ポリシーは、global に設定されます。 これは、シャーシが新たに検出されたときに、接続制御がシャーシディスカバリ ポリシーで設定されている設定値を使用して設定されることを意味します。 シャーシが検出されると、シャーシ接続ポリシーは、接続制御が none または port channel のいずれに設定されるかを制御します。

（注） シャーシ接続ポリシーは、ハードウェア構成がファブリック ポート チャネルをサポートする場合にだけ Cisco UCS Manager によって作成されます。 現時点では、6200 シリーズ ファブリック インターコネクトおよび 2200 シリーズ IOM のみがこの機能をサポートしています。 他のすべてのハードウェアの組み合わせでは、Cisco UCS Manager はシャーシ接続ポリシーを作成しません。

シャーシ接続ポリシーの設定

シャーシの接続モードを変更すると、VIF のネーム スペースが減少する可能性があります。

注意 シャーシに対する接続モードを変更すると、シャーシの再認識が行われます。 その期間は、トラフィックが中断されることがあります。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 IOM とファブリック インターコネクト間の接続を設定するシャーシをクリックします。

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

ステップ 5 シャーシの各 IOM について、[Admin State] フィールドでシャーシとファブリック接続用の次のいずれかの値を選択します。

- [None]：ポート チャネルにリンクはグループ化されません。
- [Port Channel]：IOM からファブリック インターコネクトへのすべてのリンクがポート チャネルにグループ化されます。
- [Global]：シャーシ ディスカバリ ポリシーからシャーシはこの設定を継承します。 768 ビットは、デフォルト値です。

ステップ 6 [Save Changes] をクリックします。

ラック サーバ ディスカバリ ポリシーの設定

ラック サーバ ディスカバリ ポリシー

ラック サーバ ディスカバリ ポリシーでは、新しいラックマウント サーバを追加した際のシステムによる対応方法が規定されます。 Cisco UCS Manager Cisco UCS Manager は、ラック サーバ ディ

スカバリ ポリシーの設定を使用して、ハードディスクのすべてのデータがスクラビングされるかどうか、およびサーバ ディスカバリをただちに実行するのか明示的なユーザの確認を待機する必要があるのかを決定します。

Cisco UCS Manager Cisco UCS Manager は、ファブリック インターコネクトに正しくケーブル接続されず、接続されていないラックマウント サーバを検出できません。 サポートされている Cisco UCS ラックマウント サーバを Cisco UCS Manager に統合する方法については、そのサーバのハードウェア インストレーション ガイドを参照してください。

ラック サーバ ディスカバリ ポリシーの設定

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 [Rack Server Discovery Policy] 領域で、次のフィールドに値を入力します。

名前	説明
[Action] フィールド	新しいラック サーバを追加すると、Cisco UCS Manager がどのように反応するか。 次のいずれかになります。 • [Immediate]：Cisco UCS Manager は新しいサーバを自動的に検出しようとします • [User Acknowledged]：Cisco UCS Manager はユーザが新しいサーバの検索を指示するまで待機します
[Scrub Policy] ドロップダウン リスト	新しく検出されたサーバが、選択したサーバ プール ポリシー資格内の基準と一致する場合に、そのサーバ上で実行するスクラブ ポリシー。

ステップ 6 [Save Changes] をクリックします。

MAC アドレス テーブルのエージング タイムの設定

MAC アドレス テーブルのエージング タイム

ポート間でパケットを効率的に切り替えるために、ファブリック インターコネクトは MAC アドレス テーブルを保持しています。 ファブリック インターコネクトは、受信したパケットの MAC ソース アドレスと、パケットが読み取られた関連ポートを使用して、MAC アドレス テーブルを動的に構築します。 ファブリック インターコネクトは、設定可能なエージング タイマーで定義されたエージング メカニズムを使用して、エントリが MAC アドレス テーブル内にとどまる期間を判断します。 アドレスの非アクティブ状態が所定の秒数続くと、そのアドレスは MAC アドレス テーブルから削除されます。

MAC アドレス エントリ（MAC アドレスとその関連ポート）が MAC アドレス テーブルにとどまる時間（エージ）はユーザが設定できます。

MAC アドレス テーブルのエージング タイムの設定

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 [MAC Address Table Aging] 領域で、次のフィールドに値を入力します。

名前	説明
[Aging Time] フィールド	使用されていない MAC アドレスが、Cisco UCS によって削除されるまで、MAC アドレス テーブル内に留まる時間の長さ。 次のいずれかになります。 • [Never]：MAC アドレスは、使用されていない時間がどの程度長くなっても、テーブルから削除されません。 • [Mode-Default]：システムのデフォルト値が使用されます。 ファブリック インターコネクトがエンドホスト モードに設定されている場合、デフォルトは 14,500 秒です。 スイッチング モードに設定されている場合、デフォルトは 300 秒です。 • [other]：Cisco UCS Manager GUI に、カスタム値を入力できる [dd:hh:mm:ss] フィールドが表示されます。

名前	説明
[dd:hh:mm:ss] フィールド	MAC アドレスが Cisco UCS によって MAC アドレス テーブルから削除されるまでに、その MAC アドレスが使用されない状態である必要のある時間の長さ。 このフィールドは、エージング タイムに [other] を選択した場合にだけ表示されます。 時間を days:hours:minutes:seconds の形式で入力します。

ステップ 6 [Save Changes] をクリックします。

第 13 章

ライセンスの管理

この章の内容は、次のとおりです。

- ライセンス，217 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，219 ページ
- ライセンスの取得，219 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，220 ページ
- 離れた場所からのファブリック インターコネクトへのライセンスのダウンロード，221 ページ
- ライセンスのインストール，223 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たライセンスの表示，224 ページ
- ポートまたは機能に使用できる猶予期間の決定，226 ページ
- ライセンスの有効期限の決定，228 ページ
- ライセンスのアンインストール，228 ページ

ライセンス

各 Cisco UCS ファブリック インターコネクトには、工場でインストールされ、ハードウェアとともに出荷される複数のポートライセンスが付属しています。 完全にライセンスされたファブリックインターコネクト、または部分的にライセンスされたファブリックインターコネクトを購入できます。 納品後に追加のライセンスを購入することもできます。

各ファブリック インターコネクトは、少なくとも次にカウントされたライセンスがプリインストールされた状態で出荷されます。

- Cisco UCS 6120XP ファブリック インターコネクト：Cisco UCS Manager でイネーブルにされる最初の 8 個のイーサネット ポート用および拡張モジュール上のすべてのファイバ チャネル ポート用のプリインストール ライセンス
- Cisco UCS 6140XP ファブリック インターコネクト：Cisco UCS Manager でイネーブルにされる最初の 16 個のイーサネット ポート用および拡張モジュール上のすべてのファイバ チャネル ポート用のプリインストール ライセンス
- Cisco UCS 6248 ファブリック インターコネクト：Cisco UCS Manager でイネーブルにされる最初の 12 個のユニファイド ポート用のプリインストール ライセンス 拡張モジュールには、拡張モジュールまたはベース モジュールで使用できる 8 個のライセンスが付属しています。
- Cisco UCS 6296 ファブリック インターコネクト：Cisco UCS Manager でイネーブルにされる最初の 18 個のユニファイド ポート用のプリインストール ライセンス 拡張モジュールには、拡張モジュールまたはベース モジュールで使用できる 8 個のライセンスが付属しています。

（注） 6200 シリーズ ファブリック インターコネクト拡張モジュールに付属する 8 個のデフォルトのライセンスは、ベース モジュールでポートをイネーブルにするために使用できますが、削除された場合は拡張モジュールに移動します。 拡張モジュールを取り外すと、ベース モジュールによって使用されているデフォルトの拡張モジュール ライセンスがベース モジュールのポートから削除されます。これにより、ライセンスされてないポートになります。

ポート ライセンスは、物理ポートにバインドされません。 ライセンスされているポートをディセーブルにすると、そのライセンスは次回イネーブルにされたポートで使用するために保持されます。 追加の固定ポートを使用する場合は、それらのポート用のライセンスを購入し、インストールする必要があります。

重要 ライセンスは、製品の世代間では移行できません。 6100 シリーズ ファブリック インターコネクト用に購入したライセンスを使用して 6200 シリーズ ファブリック インターコネクトをイネーブルにすること、またその逆を行うことはできません。

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、ライセンスなしでポートを最初に使用したときから測定され、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。 猶予期間で使用された期間は、システムによって保持されます。

（注） 各物理ポートには、独自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、ライセンスは残りの猶予期間が最も短いポートに移動されます。

High Availability 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じ数のポートがライセンスされていることを推奨します。 対称性が維持されていない場合にフェールオーバーが発生すると、Cisco UCS は欠落しているライセンスをイネーブルにし、フェールオーバー ノードで使用される各ポートの猶予期間を開始します。

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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] 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] ペインの [General] タブをクリックします。

ステップ 5 [Properties] 領域では、ホスト ID は [Serial Number (SN)] フィールドに表示されます。

次の作業

シスコから必要なライセンスを取得します。

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。

はじめる前に

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、Product Authorization Key（PAK; 製品認証キー）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、要求された機能もイネーブルになります。

次の作業

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 セットアップでは、一致する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。

はじめる前に

シスコから必要なライセンスを取得します。

手順

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

ステップ 2 [Admin] タブで、[All] > [License Management] 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。

ライセンス ファイルがあ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、[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、[Equipment] タブのファブリック インターコネクトにナビゲートし、[General] タブの [Local Storage Information] 領域を展開します。

ステップ 10 必要なすべてのライセンスがファブリック 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。

次の作業

すべてのダウンロード タスクを完了した後に、ライセンスをインストールします。

離れた場所からの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 セットアップでは、一致する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。

はじめる前に

シスコから必要なライセンスを取得します。

手順

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

ステップ 2 [Admin] タブで、[All] > [License Management] 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 次のフィールドに入力します。

名前	説明
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。 次のいずれかになります。 • FTP • TFTP • SCP • SFTP
[Server] フィールド	ファイルが存在するリモート サーバの IP アドレスまたはホスト名。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Filename] フィールド	ダウンロードするライセンス ファイルの名前。
[Path] フィールド	必要に応じて、リモート サーバ上のライセンス ファイルの絶対パスを指定します。 SCP を使用する場合、絶対パスは常に必要です。 他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロード フォルダにあれば、リモート パスを指定する必要はありません。 ファイル サーバの設定方法の詳細については、システム管理者に問い合わせてください。

名前	説明
[User] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。

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、[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、[Equipment] タブのファブリック インターコネクトにナビゲートし、[General] タブの [Local Storage Information] 領域を展開します。

ステップ 10 必要なすべてのライセンスがファブリック 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。

次の作業

すべてのダウンロード タスクを完了した後に、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

はじめる前に

シスコから必要なライセンスを取得します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[All] > [License Management] 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。
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、ライセンスされていない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たライセンスの表示

手順

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

ステップ 2 [Admin] タブで、[All] > [License Management] 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たすべてのライセンスに関して次の詳細を表示します。

名前	説明
[License File ID] カラム	ライセンスの一意の識別子。
[Operational State] カラム	ライセンスの動作状態。
[Operational State Description] カラム	動作状態に関する詳細。
[Scope] カラム	このライセンスがインストールされているファブリック。
[Version] カラム	ライセンスのバージョン。

名前	説明
[Administrative State] カラム	ライセンスの管理状態。 次のいずれかになります。 • [Delete Failed]：Cisco UCS はライセンスを削除できませんでした。 削除に失敗したのが最初の場合は、削除要求を再送信します。 再度失敗した場合は、Cisco TAC に連絡してください。 • [Delete Pending]：ユーザは Cisco UCS がこのファブリック インターコネクトからライセンス ファイルを削除することを要求しました。 • [Deleted]：Cisco UCS はライセンス ファイルの削除を完了しましたが、データベースからはまだ除去されていません。 • [Deleting]：Cisco UCS は、現在ライセンスを削除しています。 • [Install Failed]：Cisco UCS はライセンスをインストールできませんでした。 インストールに失敗したのが最初の場合は、ライセンスを再インストールします。 再度失敗した場合は、Cisco TAC に連絡してください。 • [Install Pending]：ライセンスはダウンロードされましたが、まだインストールされていません。 • [Installed]：ライセンス ファイルはファブリック インターコネクトにインストールされています。 • [Installing]：Cisco UCS は、現在ライセンスをインストールしています。 • [Stale]：ライセンス ファイルは古いファブリック インターコネクトに適用され、現在のファブリック インターコネクトでは使用できません。 ライセンス ファイルを削除する必要があります。また、必要に応じて現在のライセンスに置き換える必要があります。 • [Unknown]：状態を判別できません。 • [Validated]：Cisco UCS は、これが有効な Cisco ライセンス ファイルであることを検証しました。

ステップ 4 テーブル内のライセンスをクリックし、[Contents] タブに、そのライセンスの次の詳細を表示します。
ファイルの個別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る場合があります。

名前	説明
[Name] カラム	特定のコンポーネントとそのサブコンポーネントを表示できるナビゲーションツリー。コンポーネントを右クリックすると、そのコンポーネントに使用できる処理を表示できます。
[Total Qty] カラム	ライセンス パッケージ ファイルで使用可能なライセンスの総数。
[Type] カラム	ライセンス タイプ。
[Expiry] カラム	ライセンスが期限切れになる日付。
[Quantity] カラム	ライセンスパッケージファイルの指定されたタイプのライセンスの数量。
[PAK] カラム	このライセンスに関連付けられた製品認証キー（PAK）（利用できる場合）。
[Signature] カラム	指定されたタイプのライセンスに関連付けられた署名キー。
[Vendor] カラム	ライセンス パッケージ ファイルを発行した会社。
[Version] カラム	ライセンス パッケージ ファイルのバージョン。

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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [License Management] 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 テーブル内の機能をクリックし、[General] タブに、その機能に関する次の詳細（使用されている猶予期間を含む）を表示します。

名前	説明
[Name] フィールド	ライセンスを適用する機能の名前。
[Scope] フィールド	ライセンスに関連付けられたファブリック。

名前	説明
[Absolute Quantity] フィールド	使用可能なライセンスの総数。 この値は、デフォルトのライセンス数と、購入ライセンス数の合計です。
[Used Quantity] フィールド	システムによって現在使用されているライセンスの数。 この値が使用可能なライセンスの総数を超えると、関連する猶予時間が経過した後、一部のポートが機能を停止します。
[Default Quantity] フィールド	この Cisco UCS ドメインに提供されているライセンスのデフォルト数。
[Operational State] フィールド	ライセンスの動作状態。
[Grace Period Used] フィールド	このライセンスが使用した猶予期間の日数。 猶予期間が終了すると、新しいライセンスが購入されるまで、Cisco UCS はアラート メッセージを送信します。
[Peer License Count Comparison] フィールド	このファブリック インターコネクトと比較した場合の、ピア ファブリック インターコネクトにあるライセンス数。 次のいずれかになります。 • [exceeds]：ピア ファブリック インターコネクトには、このファブリック インターコネクトより多くのライセンスがインストールされています。 • [lacks]：ピア ファブリック インターコネクトには、このファブリック インターコネクトより少ないライセンスがインストールされています。 • [matching]：両方のファブリック インターコネクトに、同じ数のライセンスがインストールされています。

ライセンスの有効期限の決定

手順

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

ステップ 2 [Admin] タブで、[All] > [License Management] 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、下の[Contents] タブにそのライセンスの詳細を表示します。

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のすべてのライセンスを表示します。

ステップ 6 [Expiry] カラムで、ライセンスの有効期限を表示します。

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。 使用中の永続ライセンスを削除しようとすると、Cisco UCS Manager はその要求を拒否し、エラー メッセージを表示します。

はじめる前に

- Cisco UCS Manager 設定をバック アップします。
- アンインストールするライセンスに関連付けられた機能またはポートをディセーブルにします。

手順

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

ステップ 2 [Admin] タブで、[All] > [License Management] 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

Cisco UCS Manager はライセンスを無効にし、ライセンスのリストからライセンスを削除して、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。 クラスタ セットアップでは、他のファブリック インターコネクトからライセンスをアンインストールする必要があります。

第 14 章

仮想インターフェイスの管理

この章の内容は、次のとおりです。

- 仮想インターフェイス，231 ページ
- 仮想インターフェイスの加入者管理とエラー処理，232 ページ

仮想インターフェイス

ブレード サーバ環境では、サービス プロファイル向けに設定可能な vNIC および vHBA の数は、アダプタの機能とアダプタで利用できる仮想インターフェイス（VIF）名前空間の容量によって決定されます。 Cisco UCS では、VIF の名前空間部分は VIF というチャンクで割り当てられます。ハードウェアに応じて、VIF の最大数は、定義済みのポート単位で割り当てられます。
VIF の最大数は、ハードウェア機能とポート接続によって異なります。 設定された各 vNIC または vHBA には、1 つまたは 2 つの VIF が割り当てられます。 スタンドアロン vNIC および vHBA は 1 つの VIF を使用し、フェールオーバー vNIC および vHBA は 2 つ使用します。

次の変数は、ブレードサーバに使用可能な VIF の数、およびサービス プロファイルに対して設定可能な vNIC と vHBA の数に影響を与えます。

- ファブリック インターコネクトでサポートされている VIF の最大数
- ファブリック インターコネクトをケーブル接続する方法
- ファブリック インターコネクトと IOM がファブリック ポート チャネル モードで設定されている場合

ハードウェア設定によってサポートされている VIF の最大数の詳細については、ソフトウェア リリースの『*Cisco UCS 6100 and 6200 Series Configuration Limits for Cisco UCS Manager*』を参照してください。

仮想インターフェイスの加入者管理とエラー処理

ポートチャネルでグループ化されたファブリックインターコネクトでは、ファブリックインターコネクトを I/O モジュールに接続する方法を変更すると、ブレード サーバに使用可能な VIF の数が大幅に変化する可能性があります。 これらの変更効果の追跡を支援するため、Cisco UCS Manager は次のメトリックを維持しています。

- ハードウェアによってサポートされる VIF の最大数
- 接続タイプ

ブレードに使用可能な VIF の数を減らすような方法で設定を変更すると、UCS Manager は警告を表示し、操作を続行するかどうかを尋ねます。 これには、接続の追加または移動によって VIF の数が減らされる回数を含む、いくつかのシナリオが含まれています。

第 15 章

Cisco UCS Central への Cisco UCS ドメインの登録

この章の内容は、次のとおりです。

- Cisco UCS ドメインの登録，233 ページ
- Cisco UCS Manager と Cisco UCS Central 間のポリシー解決，234 ページ
- Cisco UCS ドメインの Cisco UCS Central への登録，235 ページ
- Cisco UCS Manager と Cisco UCS Central 間のポリシー解決の変更，236 ページ
- Cisco UCS ドメインの Cisco UCS Central からの登録解除，237 ページ

Cisco UCS ドメインの登録

Cisco UCS Central により、データセンターで一部またはすべての Cisco UCS ドメイン を管理できます。

Cisco UCS Central によって Cisco UCS ドメイン を管理する場合は、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、どのポリシーのタイプ、およびバックアップとファームフェアなどのその他の設定が Cisco UCS Central または Cisco UCS Manager によって管理されるかを選択する必要があります。 登録されたすべての Cisco UCS ドメイン で同じタイプのポリシーおよび設定を Cisco UCS Central によって管理するか、または登録された各 Cisco UCS ドメイン に異なる設定を選択できます。

Cisco UCS ドメイン を Cisco UCS Central に登録する前に、次の作業を実行します。

- NTP サーバと正しいタイム ゾーンを、Cisco UCS Manager と Cisco UCS Central の両方に設定して、それらが同期されるようにします。 Cisco UCS ドメイン と Cisco UCS Centralの日時が同期していない場合、登録が失敗する可能性があります。
- 次のホスト名または IP アドレスを取得します： Cisco UCS Central
- Cisco UCS Central を展開した際に設定した共有秘密を取得します

（注） Cisco UCS Central に登録されているドメイン内の Cisco UCS Manager によって使用されている IP アドレスを変更またはスワップすることはできません。 その IP アドレスを変更またはスワップする必要がある場合は、最初にCisco UCS Central からのドメインを登録解除する必要があります。 IPアドレスを変更またはスワップした後、Cisco UCS ドメインを再登録できます。

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 では、特定のポリシーおよび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 に登録したすべての Cisco UCS ドメイン で同じである必要はありません。

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。

次のテーブルには、Cisco UCS Manager または Cisco UCS Central のいずれかで管理するように選択できるポリシーおよび設定のリストを示します。

名前	説明
[Infrastructure & Catalog Firmware]	機能カタログおよびインフラストラクチャ ファームウェア ポリシーがローカルで定義されるか、または Cisco UCS Central から取得されるかどうかを決定します。
[Time Zone Management]	タイム ゾーンおよび NTP サーバの設定がローカルで定義されるか、または Cisco UCS Central から取得されるかどうかを決定します。
[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リング ポリシー設定が、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。
[Global Fault Policy]	グローバル障害ポリシーが、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。
[User Management]	認証とネイティブ 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 ロールが、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。
[DNS Management]	DNS サーバが、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。

名前	説明
[Backup & Export Policies]	完全な状態のバックアップ ポリシーおよびすべてのコンフィギュレーションのエクスポート 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。
[Monitoring]	Call Home、Syslog、および TFTP Core Exporter 設定がローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[SEL Policy]	SEL 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。
[Power Allocation Policy]	グローバルな電力割り当て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。
[Power Policy]	電源ポリシーが、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。

Cisco UCS ドメインの Cisco UCS Central への登録

（注） Cisco UCS Central に登録されているドメイン内の Cisco UCS Manager によって使用されている IP アドレスを変更またはスワップすることはできません。 その IP アドレスを変更またはスワップする必要がある場合は、最初にCisco UCS Central からのドメインを登録解除する必要があります。 IPアドレスを変更またはスワップした後、Cisco UCS ドメインを再登録できます。

はじめる前に

NTP サーバと正しいタイム ゾーンを、Cisco UCS Manager と Cisco UCS Central の両方に設定して、それらが同期されるようにします。 Cisco UCS ドメイン と Cisco UCS Centralの日時が同期していない場合、登録が失敗する可能性があります。

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] 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 [Work] ペインの [UCS Central] タブをクリックします。

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 が展開される仮想マシンのホスト名または IP アドレス。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Shared Secret] フィールド	Cisco UCS Central が配置された後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 Manager と Cisco UCS Central 間のポリシー解決の変更

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] 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 [Work] ペインの [UCS Central] タブをクリックします。

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 ドメインの Cisco UCS Central からの登録解除

Cisco UCS ドメインをCisco UCS Centralから登録解除すると、Cisco UCS Managerはグローバル ポリシーへの更新を受け取らなくなります。

手順

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

ステップ 2 [Admin] タブで、[All] > [Communication Management] 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 [Work] ペインの [UCS Central] タブをクリックします。

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 7 [OK] をクリックします。

第 III 部

ネットワーク設定

- LAN アップリンク マネージャの使用，241 ページ
- VLAN の設定，257 ページ
- LAN ピン グループの設定，285 ページ
- MAC プールの設定，289 ページ
- Quality of Service の設定，293 ページ
- ネットワーク関連ポリシーの設定，305 ページ
- アップストリーム分離レイヤ 2 ネットワークの設定，345 ページ

第 16 章

LAN アップリンク マネージャの使用

この章の内容は、次のとおりです。

- LAN アップリンク マネージャ，241 ページ
- LAN アップリンク マネージャの起動，242 ページ
- LAN アップリンク マネージャでのイーサネット スイッチング モードの変更，242 ページ
- LAN アップリンク マネージャでのポートの設定，243 ページ
- サーバ ポートの設定，243 ページ
- アップリンク イーサネット ポートの設定，245 ページ
- アップリンク イーサネット ポート チャネルの設定，246 ページ
- LAN ピン グループの設定，249 ページ
- ネームド VLAN の設定，250 ページ
- LAN アップリンク マネージャでの QoS システム クラスの設定，254 ページ

LAN アップリンク マネージャ

LAN アップリンク マネージャは、Cisco UCS と LAN 間の接続を設定できる単一インターフェイスを提供します。LAN アップリンク マネージャを使用して次のものを作成および設定できます。

- イーサネット スイッチング モード
- アップリンク イーサネット ポート
- ポート チャネル
- LAN ピン グループ
- ネームド VLAN
- サーバ ポート

- QoS システム クラス

LAN アップリンク マネージャで行うことができる設定の一部は、[Equipment] タブまたは [LAN] タブなどの他のタブのノードでも行うことができます。

LAN アップリンク マネージャの起動

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

LAN アップリンク マネージャでのイーサネット スイッチング モードの変更

重要 イーサネット スイッチング モードを変更すると、Cisco UCS Manager により自動的にログアウトとファブリック インターコネクトの再起動が実行されます。 クラスタ設定では、Cisco UCS Manager により両方のファブリック インターコネクトが順番に再起動されます。 2 つめのファブリック インターコネクトがイーサネット スイッチング モードに変更され、システムが使用できるようになるまでには数分間かかります。 設定が保持されます。

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Uplink Mode] 領域で、次のいずれかのボタンをクリックします。

- Set Ethernet Switching Mode
- Set Ethernet End-Host Mode

現在のスイッチング モードのボタンはグレー表示されています。

ステップ 3 ダイアログボックスで、[Yes] をクリックします。
Cisco UCS Manager はファブリック インターコネクトを再起動し、ユーザをログアウトし、Cisco UCS Manager GUI との接続を解除します。

LAN アップリンク マネージャでのポートの設定

設定できるのは固定ポート モジュールのサーバ ポートだけです。 展開モジュールにはサーバ ポートは含まれません。

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Ports] 領域で、下矢印をクリックして [Unconfigured Ports] セクションを展開します。

ステップ 3 [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 4 次のいずれかを展開します。

- [Fixed Module]：固定モジュールのポートをサーバ ポートまたはアップリンク イーサネット ポートとして設定します。
- [Expansion Module *Number*]：拡張モジュールのポートをアップリンク イーサネット ポートとしてイネーブルにします。 拡張モジュールのポートはサーバ ポートとして設定できません。

展開したノード以下にポートがリストされていない場合は、そのモジュールのすべてのポートがすでに設定されています。

ステップ 5 設定するポートを右クリックし、次のいずれかを選択します。

- Configure as Server Port
- Configure as Uplink Port

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

サーバ ポートの設定

LAN アップリンク マネージャを使用したサーバ ポートのイネーブル化

この手順は、ポートがサーバ ポートとして設定されているものの、ディセーブルになっていることを前提としています。

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Ports] 領域で、下矢印をクリックして [Server Ports] セクションを展開します。

ステップ 3 [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 4 イネーブルにするポートを右クリックし、[Enable] を選択します。

LAN アップリンク マネージャを使用したサーバ ポートのディセーブル化

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Ports] 領域で、下矢印をクリックして [Server Ports] セクションを展開します。

ステップ 3 [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 4 ディセーブルにするポートを右クリックし、[Disable] を選択します。

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

LAN アップリンク マネージャを使用したサーバ ポートの設定解除

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Ports] 領域で、下矢印をクリックして [Server Ports] セクションを展開します。

ステップ 3 [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 4 設定を解除するポートを右クリックし、[Unconfigure] を選択します。

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

アップリンク イーサネット ポートの設定

LANアップリンクマネージャを使用したアップリンクイーサネットポートのイネーブル化

この手順は、ポートがアップリンクイーサネットポートとして設定されているものの、ディセーブルになっていることを前提としています。

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Interfaces] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 イネーブルにするポートを右クリックし、[Enable Interface] を選択します。

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

LAN アップリンク マネージャを使用したアップリンク イーサネット ポートのディセーブル化

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Interfaces] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 ディセーブルにするポートを右クリックし、[Disable Interfaces] を選択します。
複数のアップリンクイーサネットポートをディセーブルにする場合は、複数のポートを選択できます。

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

ディセーブルにされたポートは、イネーブルのインターフェイスのリストから削除され、[Unconfigured Ports] リストに戻されます。

LAN アップリンク マネージャを使用したアップリンク イーサネット ポートの設定解除

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Interfaces] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 設定を解除するポートをクリックします。
複数のアップリンク イーサネット ポートの設定を解除する場合は、複数のポートを選択できます。

ステップ 4 [Disable Interface] をクリックします。

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

ディセーブルにされたポートは、イネーブルのインターフェイスのリストから削除され、[Unconfigured Ports] リストに戻されます。

アップリンク イーサネット ポート チャネルの設定

LAN アップリンク マネージャでのポート チャネルの作成

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Create Port Channel] をクリックします。

ステップ 3 ポップアップ メニューから、ポート チャネルを作成する次のいずれかのファブリック インターコネクトを選択します。

- Fabric Interconnect A
- Fabric Interconnect B

ステップ 4 [Create Port Channel] ウィザードの [Set Port Channel Name] 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
[ID] フィールド	ポート チャネルの ID。 1 ～ 256 の整数を入力します。 ポート チャネルが保存された後、この ID を変更することはできません。
[Name] フィールド	ポート チャネルのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 5 [Create Port Channel] ウィザードの [Add Ports] ページで、次の手順を実行します。

a) [Ports] テーブルで、ポート チャネルに含める 1 つ以上のポートを選択します。

b) [>>] ボタンをクリックして、[Ports in the port channel] テーブルにポートを追加します。
ポート チャネルからポートを削除するには、[<<] ボタンを使用できます。

（注） Cisco UCS Manager サーバ ポートとして設定済みのポートを選択した場合、Cisco UCS Manager で警告が表示されます。 ダイアログボックスの [Yes] をクリックして、このポートをアップリンク イーサネット ポートとして再設定し、ポート チャネルに含めることができます。

ステップ 6 [Finish] をクリックします。

LAN アップリンク マネージャを使用したポート チャネルのイネーブル化

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 イネーブルにするポート チャネルを右クリックし、[Enable Port Channel] を選択します。

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

LAN アップリンク マネージャを使用したポート チャネルのディセーブル化

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 ディセーブルにするポート チャネルを右クリックし、[Disable Port Channel] を選択します。

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

LAN アップリンク マネージャを使用したポート チャネルへのポートの追加

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 ポートを追加するポート チャネルを右クリックして、[Add Ports] を選択します。

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

a) [Ports] テーブルで、ポート チャネルに含める 1 つ以上のポートを選択します。

b) [>>] ボタンをクリックして、[Ports in the port channel] テーブルにポートを追加します。
ポート チャネルからポートを削除するには、[<<] ボタンを使用できます。

（注） Cisco UCS Manager サーバ ポートとして設定済みのポートを選択した場合、Cisco UCS Manager で警告が表示されます。 ダイアログボックスの [Yes] をクリックして、このポートをアップリンク イーサネット ポートとして再設定し、ポートチャネルに含めることができます。

ステップ 5 [OK] をクリックします。

LAN アップリンク マネージャを使用したポート チャネルからのポートの削除

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 ポートを削除するポート チャネルを展開します。

ステップ 4 ポート チャネルから削除するポートを右クリックし、[Delete] を選択します。

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

LAN アップリンク マネージャを使用したポート チャネルの削除

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Port Channels] > [Fabric Interconnects] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 削除するポート チャネルを右クリックし、[Delete] を選択します。

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

LAN ピン グループの設定

LAN アップリンク マネージャでのピン グループの作成

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

はじめる前に

ピン グループの設定に使用するポートおよびポート チャネルを設定します。 使用できるのは、LAN ピン グループでアップリンク ポートとして設定されているポートおよびポート チャネルだけです。

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Port Channels and Uplinks] 領域で、[Create Pin Group] をクリックします。

ステップ 3 [Create LAN Pin Group] ダイアログボックスで、ピン グループの一意の名前と説明を入力します。

ステップ 4 ファブリック インターコネクト A のトラフィックをピン接続するには、[Targets] 領域で次の手順を実行します。

a) [Fabric Interconnect A] チェックボックスをオンにします。

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

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

a) [Fabric Interconnect B] チェックボックスをオンにします。

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

ステップ 6 [OK] をクリックします。

次の作業

ピン グループは、vNIC テンプレートにインクルードします。

LAN アップリンク マネージャを使用したピン グループの削除

手順

ステップ 1 [LAN Uplinks Manager] で [LAN Uplinks] タブをクリックします。

ステップ 2 [Pin Groups] 領域で、削除するピン グループを右クリックし、[Delete] を選択します。

ステップ 3 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ネームド VLAN の設定

LAN アップリンク マネージャを使用したネームド VLAN の作成

2 つのスイッチを持つ Cisco UCS ドメインでは、両方のスイッチまたは 1 つのスイッチだけにアクセスできるネームド VLAN を作成できます。

重要 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。

LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

手順

ステップ 1 [LAN Uplinks Manager] で [VLANs] タブをクリックします。

ステップ 2 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 3 [Create VLANs] 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
[VLAN Name/Prefix] フィールド	単一の VLAN の場合、VLAN 名を指定します。 VLAN の範囲の場合、各 VLAN 名に使用される接頭辞を指定します。 VLAN 名の大文字と小文字は区別されます。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Multicast Policy] ドロップダウン リスト	この VLAN に関連付けられたマルチキャスト ポリシー。 ポリシーを選択しなかった場合、Cisco UCS Manager はデフォルトのマルチキャスト ポリシーの設定を使用します。
[Create Multicast Policy] リンク	すべての VLAN に使用可能な新しいマルチキャスト ポリシーを作成するには、このリンクをクリックします。

名前	説明
設定オプション	次のいずれかを選択できます。 • [Common/Global]：指定した VLAN は両方のファブリックに適用され、どちらのファブリックでも同じ設定パラメータが使用されます。 • [Fabric A]：指定した VLAN は、ファブリック A だけに適用されます。 • [Fabric B]：指定した VLAN は、ファブリック B だけに適用されます。 • [Both Fabrics Configured Differently]：指定した VLAN は、両方のファブリックに適用されますが、ファブリックごとに異なる VLAN ID を指定できます。 アップストリーム disjoint L2 ネットワークの場合、[Common/Global] を選択して、両方のファブリックに適用する VLAN を作成することをお勧めします。
[VLAN IDs] フィールド	1 つの VLAN を作成するには、単一の数値 ID を入力します。複数の VLAN を作成するには、個々の ID や ID の範囲をカンマで区切って入力します。 VLAN ID には次の値を入力できます。 • 1 ～ 3967 の範囲 • 4048 ～ 4093 の範囲 • システム上ですでに定義されている他の VLAN ID と重複する値 たとえば、ID が 4、22、40、41、42、および 43 の 6 つの VLAN を作成するには、4, 22, 40-43 を入力します。 **重要** 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。 LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

名前	説明
[Sharing Type] フィールド	この VLAN がプライベート VLAN またはセカンダリ VLAN に再分割されるかどうか。 次のいずれかになります。 • [None]：この VLAN には、セカンダリ VLAN またはプライベート VLAN がありません。 • [Primary]：[Secondary VLANs] 領域に示すように、この VLAN には 1 つ以上のセカンダリ VLAN が存在できます。 • [Isolated]：これはプライベート VLAN です。 プライマリ VLAN とこれが関連付けられた VLAN は、[Primary VLAN] ドロップダウン リストに表示されます。
[Primary VLAN] ドロップダウン リスト	[Sharing Type] フィールドが [Isolated] に設定されている場合、これはこのプライベート VLAN に関連付けられたプライマリ VLAN です。
VLAN の許容組織	VLAN に表示されるリストから組織を選択します。 この VLAN は、ここで選択する組織で使用できます。
[Check Overlap] ボタン	このボタンをクリックして、VLAN ID がシステム上の他の ID と重複していないかどうか確認します。

ステップ 4 [OK] をクリックします。
Cisco UCS Manager によって次の [VSANs] ノードの 1 つに VSAN が追加されます。

- 両方のファブリック インターコネクトにアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのファブリック インターコネクトだけにアクセス可能な VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

LAN アップリンク マネージャを使用したネームド VLAN の削除

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

手順

ステップ 1 [LAN Uplinks Manager] で [VLANs] タブをクリックします。

ステップ 2 削除する VLAN のタイプに応じて、次のいずれかのサブタブをクリックします。

サブタブ	説明
All	Cisco UCS ドメインのすべての VLAN を表示します。
Dual Mode	両方のファブリック インターコネクトにアクセス可能な VLAN を表示します。
Fabric A	ファブリック インターコネクト A にのみアクセス可能な VLAN を表示します。
Fabric B	ファブリック インターコネクト B にのみアクセス可能な VLAN を表示します。

ステップ 3 テーブルで、削除する VLAN をクリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 4 強調表示された 1 つまたは複数の VLAN を右クリックし、[Delete] を選択します。

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

LAN アップリンク マネージャでの QoS システム クラスの設定

サーバ内のアダプタのタイプによっては、サポートされる MTU の最大値が制限される場合があります。 たとえば、ネットワーク MTU が最大値を超えた場合、次のアダプタでパケットがドロップする可能性があります。

- Cisco UCS M71KR CNA アダプタ：サポートされる MTU の最大値は 9216 です。
- Cisco UCS 82598KR-CI アダプタ：サポートされる MTU の最大値は 14000 です。

手順

ステップ 1 LAN アップリンク マネージャで、[QoS] タブをクリックします。

ステップ 2 システムのトラフィック管理ニーズを満たすために設定するシステム クラスの次のプロパティを更新します。

（注） 一部のプロパティはすべてのシステム クラスに対して設定できない場合があります。

名前	説明
[Enabled] チェックボックス	このチェックボックスをオンにすると、対応する QoS クラスがファブリック インターコネクト上で設定され、QoS ポリシーに割り当て可能になります。 このチェックボックスをオフにすると、このクラスはファブリック インターコネクト上で設定されず、このクラスに関連付けられた QoS ポリシーはデフォルトの [Best Effort] になるか、（システム クラスが 0 の Cos で設定されている場合は）Cos 0 システム クラスになります。 （注） このフィールドは、[Best Effort] と [Fibre Channel] の場合は常にオンです。
[Cos] フィールド	サービス クラス。 0 ～ 6 の整数を入力できます。0 は最低プライオリティを表し、6 は最高プライオリティを表します。 QoS ポリシーが削除されるか、割り当てられたシステム クラスがディセーブルになったときに、システム クラスをトラフィックのデフォルト システム クラスにする必要がある場合を除き、この値を 0 に設定することは推奨しません。 （注） このフィールドは、内部トラフィックの場合は 7 に、[Best Effort] の場合は [any] に設定されます。 これらの値は両方とも予約されており、他のプライオリティに割り当てることはできません。
[Packet Drop] チェックボックス	このチェックボックスをオンにすると、このクラスに対してパケットの破棄が許可されます。 このチェックボックスをオフにすると、送信時にパケットを破棄できません。 このフィールドは、[Fibre Channel] クラスの場合は常にオフであり（破棄パケットは決して許可されない）、[Best Effort] の場合は常にオンです（破棄パケットは常に許可される）。
[Weight] ドロップダウン リスト	次のいずれかになります。 • 1 ～ 10 の整数。 整数を入力すると、[Weight (%)] フィールドの説明に従って、このプライオリティ レベルに割り当てられるネットワーク帯域幅の割合が Cisco UCS によって決定されます。 • best-effort. • none.

名前	説明
[Weight (%)] フィールド	チャネルに割り当てられる帯域幅を決定するために、Cisco UCS によって次の作業が実行されます。 **1** すべてのチャネルの重みを加算します。 **2** チャネルの重みをすべての重みの和で割って、割合を求めます。 **3** その割合の帯域幅をチャネルに割り当てます。
[MTU] ドロップダウン リスト	チャネルの最大伝送単位。 次のいずれかになります。 • 1500 ～ 9216 の整数。 この値は最大パケット サイズに対応します。 • [fc]：事前に定義されている 2240 のパケット サイズ。 • [normal]：事前に定義されている 1500 のパケット サイズ。 （注） このフィールドは、[Fibre Channel] の場合は常に [fc] に設定されます。
[Multicast Optimized] チェックボックス	このチェックボックスをオンにすると、パケットを複数の宛先に同時に送信するように、クラスが最適化されます。 （注） このオプションは、[Fibre Channel] には適用されません。

ステップ 3 次のいずれかを実行します。

- [OK] をクリックして変更を保存し、LAN アップリンク マネージャを終了します。
- [Apply] をクリックし、LAN アップリンク マネージャを終了せずに変更を保存します。

第 17 章

VLAN の設定

この章の内容は、次のとおりです。

- ネームド VLAN，257 ページ
- プライベート VLAN，258 ページ
- VLAN ポートの制限事項，260 ページ
- ネームド VLAN の設定，261 ページ
- プライベート VLAN の設定，266 ページ
- VLAN ポート数の表示，275 ページ
- VLAN のポート数の最適化，275 ページ
- VLAN グループ，278 ページ
- VLAN の権限，281 ページ

ネームド VLAN

ネームド VLAN は、所定の外部 LAN への接続を作成します。 VLAN は、ブロードキャスト トラフィックを含む、その外部 LAN へのトラフィックを切り離します。

VLAN ID に割り当てる名前によって抽象化層が追加されることで、ネームド VLAN を使用するサービス プロファイルに関連付けされたすべてのサーバを一括してアップデートできるようになります。 外部 LAN との通信を維持するために、サーバを個別に再設定する必要はありません。

同じ VLAN ID を使用して、複数のネームド VLAN を作成できます。 たとえば、HR および Finance のビジネス サービスをホストするサーバが同一の外部 LAN にアクセスする必要がある場合、同じ VLAN ID を使用して HR と Finance という名前の VLAN を作成できます。 その後でネットワークが再設定され、Finance が別の LAN に割り当てられた場合、変更する必要があるのは Finance のネームド VLAN の VLAN ID だけです。

クラスタ設定では、ネームド VLAN が 1 つのファブリック インターコネクトだけにアクセスできるようにすることも、両方のファブリック インターコネクトにアクセスできるように設定することも可能です。

VLAN ID に関するガイドライン

重要 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。

LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

VLAN 4048 はユーザによる設定が可能です。 ただし、Cisco UCS Manager は次のデフォルト値に VLAN 4048 を使用します。 VLAN に 4048 を割り当てる場合は、これらの値を再設定する必要があります。

- Cisco UCS のリリース 2.0 にアップグレードした後：FCoE ストレージ ポートのネイティブ VLAN では、デフォルトで VLAN 4048 が使用されます。 アップグレード前にデフォルトの FCoE VSAN が VLAN 1 を使用するように設定されていた場合、使用または予約されていない VLAN ID にそれを変更する必要があります。 たとえば、VLAN ID が使用中でない場合、デフォルトを 4049 に変更することを検討してください。
- Cisco UCS のリリース 2.0 を新規インストールした後：デフォルトの VSAN の FCoE VLAN では、デフォルトで VLAN 4048 が使用されます。 FCoE ストレージ ポートのネイティブ VLAN は VLAN 4049 を使用します。

VLAN 名の大文字と小文字は区別されます。

プライベート VLAN

プライベート VLAN（PVLAN）は、VLAN のイーサネット ブロードキャスト ドメインをサブドメインに分割し、一部のポートを分離できるようにします。 PVLAN の各サブドメインには、プライマリ VLAN と 1 つ以上のセカンダリ VLAN が含まれています。 PVLAN のすべてのセカンダリ VLAN は、同じプライマリ VLAN を共有する必要があります。 セカンダリ VLAN ID は、各サブドメインの区別に使用されます。

独立 VLAN

Cisco UCS ドメインのすべてのセカンダリ VLAN は、独立 VLAN である必要があります。 Cisco UCS は、コミュニティ VLAN をサポートしていません。

独立 VLAN のポート

独立 VLAN の通信が使用できるのは、プライマリ VLAN の関連ポートだけです。 これらのポートは独立ポートであり、Cisco UCS Manager では設定できません。 プライマリ VLAN に複数のセカンダリ VLAN が含まれている場合、それらの独立 VLAN は互いに直接通信できません。

独立セカンダリ VLAN に属するホスト ポート。 このポートは、同じプライベート VLAN ドメイン内の他のポートから完全に隔離されています。 PVLAN は、無差別ポートからのトラフィックを除き、独立ポート宛のトラフィックをすべてブロックします。 独立ポートから受信されたトラフィックは、無差別ポートにだけ転送されます。 指定した独立 VLAN には、複数の独立ポートを含めることができます。 各ポートは、独立 VLAN にある他のすべてのポートから、完全に隔離されています。

アップリンク ポートに関するガイドライン

PVLAN を作成する場合は、次のガイドラインに注意してください。

- アップリンク イーサネット ポート チャネルを無差別モードにすることはできません。
- 各プライマリ VLAN には、独立 VLAN が 1 つだけ存在できます。
- VNTAG アダプタの VIF には、独立 VLAN が 1 つだけ存在できます。

VLAN ID に関するガイドライン

重要 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。

LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

VLAN 4048 はユーザによる設定が可能です。 ただし、Cisco UCS Manager は次のデフォルト値に VLAN 4048 を使用します。 VLAN に 4048 を割り当てる場合は、これらの値を再設定する必要があります。

- Cisco UCS のリリース 2.0 にアップグレードした後：FCoE ストレージ ポートのネイティブ VLAN では、デフォルトで VLAN 4048 が使用されます。 アップグレード前にデフォルトの FCoE VSAN が VLAN 1 を使用するように設定されていた場合、使用または予約されていない VLAN ID にそれを変更する必要があります。 たとえば、VLAN ID が使用中でない場合、デフォルトを 4049 に変更することを検討してください。
- Cisco UCS のリリース 2.0 を新規インストールした後：デフォルトの VSAN の FCoE VLAN では、デフォルトで VLAN 4048 が使用されます。 FCoE ストレージ ポートのネイティブ VLAN は VLAN 4049 を使用します。

VLAN 名の大文字と小文字は区別されます。

VLAN ポートの制限事項

Cisco UCS Manager は、ファブリック インターコネクトの境界ドメインおよびサーバ ドメイン下で設定可能な VLAN ポート インスタンスの数を 6000 に制限しています。

VLAN のポート数に含まれるポートのタイプ

次のポートのタイプが VLAN ポートの計算でカウントされます。

- 境界アップリンク イーサネット ポート
- 境界アップリンク イーサネット チャネル メンバ ポート
- SAN クラウド内の FCoE ポート
- NAS クラウド内のイーサネット ポート
- サービス プロファイルを通して作成されたスタティックおよびダイナミック vNIC
- ハイパーバイザ ドメイン内のハイパーバイザにあるポート プロファイルの一部として作成された VM vNIC

これらのポートに設定されている VLAN の数に基づいて、Cisco UCS Manager は VLAN ポート インスタンスの累積数を追跡し、検証中に VLAN のポート制限を強制的に適用します。 Cisco UCS Manager は、制御トラフィック用に事前定義された VLAN ポート リソースをいくつか予約しています。 これらには、HIF ポートおよび NIF ポート下で設定された管理 VLAN が含まれます。

VLAN のポート制限の実施

Cisco UCS Manager は、次の操作中に VLAN ポートの可用性を検証します。

- 境界ポートおよび境界ポート チャネルの設定および設定解除
- クラウドからの VLAN の追加または削除
- SAN ポートまたは NAS ポートの設定または設定解除
- 設定の変更を含むサービス プロファイルの関連付けまたは関連付け解除
- vNIC または vHBA 下での VLAN の設定または設定解除
- ESX ハイパーバイザから、VMWare vNIC からの作成通知または削除通知の受信時

（注） これは、Cisco UCS Manager の制御対象外です

- ファブリック インターコネクトのリブート
- Cisco UCS Manager のアップグレードまたはダウングレード

Cisco UCS Manager は、サービス プロファイルの操作に対して VLAN のポート制限を強制的に適用します。 Cisco UCS Manager が VLAN のポート制限を超過したことを検出した場合、展開中にサービス プロファイル設定が失敗します。

境界ドメイン内で VLAN のポート数を超えても、それほど中断が発生しません。 境界ドメインで VLAN ポート数が超過した場合、Cisco UCS Manager は割り当てステータスを Exceeded に変更します。 ステータスを Available に戻すには、次のいずれかのアクションを実行する必要があります。

- 1 つ以上の境界ポートの設定を解除します
- LAN クラウドから VLAN を削除します
- 1 つ以上の vNIC または vHBA の設定を解除します

ネームド VLAN の設定

ネームド VLAN の作成

ハイ アベイラビリティ用に設定された Cisco UCS ドメインでは、両方のファブリック インターコネクトまたは 1 つのファブリック インターコネクトだけにアクセスできるネームド VLAN を作成できます。

重要 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。

LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create VLANs] 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
[VLAN Name/Prefix] フィールド	単一の VLAN の場合、VLAN 名を指定します。 VLAN の範囲の場合、各 VLAN 名に使用される接頭辞を指定します。 VLAN 名の大文字と小文字は区別されます。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Multicast Policy] ドロップダウン リスト	この VLAN に関連付けられたマルチキャスト ポリシー。 ポリシーを選択しなかった場合、Cisco UCS Manager はデフォルトのマルチキャスト ポリシーの設定を使用します。
[Create Multicast Policy] リンク	すべての VLAN に使用可能な新しいマルチキャスト ポリシーを作成するには、このリンクをクリックします。
設定オプション	次のいずれかを選択できます。 • [Common/Global]：指定した VLAN は両方のファブリックに適用され、どちらのファブリックでも同じ設定パラメータが使用されます。 • [Fabric A]：指定した VLAN は、ファブリック A だけに適用されます。 • [Fabric B]：指定した VLAN は、ファブリック B だけに適用されます。 • [Both Fabrics Configured Differently]：指定した VLAN は、両方のファブリックに適用されますが、ファブリックごとに異なる VLAN ID を指定できます。 アップストリーム disjoint L2 ネットワークの場合、[Common/Global] を選択して、両方のファブリックに適用する VLAN を作成することをお勧めします。

名前	説明
[VLAN IDs] フィールド	1 つの VLAN を作成するには、単一の数値 ID を入力します。複数の VLAN を作成するには、個々の ID や ID の範囲をカンマで区切って入力します。 VLAN ID には次の値を入力できます。 • 1 ～ 3967 の範囲 • 4048 ～ 4093 の範囲 • システム上ですでに定義されている他の VLAN ID と重複する値 たとえば、ID が 4、22、40、41、42、および 43 の 6 つの VLAN を作成するには、4, 22, 40-43 を入力します。 **重要** 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。 LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます
[Sharing Type] フィールド	この VLAN がプライベート VLAN またはセカンダリ VLAN に再分割されるかどうか。 次のいずれかになります。 • [None]：この VLAN には、セカンダリ VLAN またはプライベート VLAN がありません。 • [Primary]：[Secondary VLANs] 領域に示すように、この VLAN には 1 つ以上のセカンダリ VLAN が存在できます。 • [Isolated]：これはプライベート VLAN です。 プライマリ VLAN とこれが関連付けられた VLAN は、[Primary VLAN] ドロップダウン リストに表示されます。
[Primary VLAN] ドロップダウン リスト	[Sharing Type] フィールドが [Isolated] に設定されている場合、これはこのプライベート VLAN に関連付けられたプライマリ VLAN です。
VLAN の許容組織	VLAN に表示されるリストから組織を選択します。 この VLAN は、ここで選択する組織で使用できます。

名前	説明
[Check Overlap] ボタン	このボタンをクリックして、VLAN ID がシステム上の他の ID と重複していないかどうか確認します。

ステップ 6 [Check Overlap] ボタンをクリックした場合は、次の作業を実行します。

a) [Overlapping VLANs] タブをクリックし、次の各フィールドを確認して VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリックインターコネクトでもアクセスできます。 この設定は、ファブリックインターコネクトレベルとは対照的に、システムレベルで作成された仮想 LAN および SAN ネットワークに適用されます。
[Name] カラム	VLAN の名前。
[VLAN] カラム	VLAN の数値 ID。
[DN] カラム	VLAN へのフルパス。 VALN のプロパティを表示するには、このカラムのリンクをクリックします。

b) [Overlapping VSANs] タブをクリックし、次の各フィールドを確認して VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリックインターコネクトでもアクセスできます。 この設定は、ファブリックインターコネクトレベルとは対照的に、システムレベルで作成された仮想 LAN および SAN ネットワークに適用されます。

名前	説明
[Name] カラム	VSAN の名前。
[ID] カラム	VSAN の数値 ID。
[FCoE VLAN ID] カラム	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。
[DN] カラム	VSAN へのフルパス。 VSAN のプロパティを表示するには、このカラムのリンクをクリックします。

c) [OK] をクリックします。

d) Cisco UCS Manager によって VLAN ID または FCoE VLAN ID の重複が識別された場合には、既存の VLAN と重複しない VLAN ID に変更します。

ステップ 7 [OK] をクリックします。

Cisco UCS Manager によって次の [VSANs] ノードの 1 つに VSAN が追加されます。

- 両方のファブリック インターコネクトにアクセス可能な VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのファブリック インターコネクトだけにアクセス可能な VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

ネームド VLAN の削除

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

プライベート プライマリ VLAN を削除する場合は、機能している別のプライマリ VLAN にセカンダリ VLAN を再割り当てします。

はじめる前に

ファブリック インターコネクトから VLAN を削除する前に、VLAN がすべての vNIC および vNIC テンプレートから削除されたことを確認します。

（注） vNIC または vNIC テンプレートに割り当てられた VLAN を削除する場合、vNIC によってその VLAN をフラップさせることができます。

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

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

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

サブタブ	説明
All	Cisco UCS ドメインのすべての VLAN を表示します。
Dual Mode	両方のファブリック インターコネクトにアクセス可能な VLAN を表示します。
Fabric A	ファブリック インターコネクト A にのみアクセス可能な VLAN を表示します。
Fabric B	ファブリック インターコネクト B にのみアクセス可能な VLAN を表示します。

ステップ 5 テーブルで、削除する VLAN をクリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 6 強調表示された 1 つまたは複数の VLAN を右クリックし、[Delete] を選択します。

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

プライベート VLAN の設定

プライベート VLAN 用のプライマリ VLAN の作成

ハイ アベイラビリティ用に設定された Cisco UCS ドメインでは、両方のファブリック インターコネクトまたは 1 つのファブリック インターコネクトだけにアクセスできるプライマリ VLAN を作成できます。

重要 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。

LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create VLANs] 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
[VLAN Name/Prefix] フィールド	単一の VLAN の場合、VLAN 名を指定します。 VLAN の範囲の場合、各 VLAN 名に使用される接頭辞を指定します。 VLAN 名の大文字と小文字は区別されます。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Multicast Policy] ドロップダウン リスト	この VLAN に関連付けられたマルチキャスト ポリシー。 ポリシーを選択しなかった場合、Cisco UCS Manager はデフォルトのマルチキャスト ポリシーの設定を使用します。
[Create Multicast Policy] リンク	すべての VLAN に使用可能な新しいマルチキャスト ポリシーを作成するには、このリンクをクリックします。

名前	説明
設定オプション	次のいずれかを選択できます。 • [Common/Global]：指定した VLAN は両方のファブリックに適用され、どちらのファブリックでも同じ設定パラメータが使用されます。 • [Fabric A]：指定した VLAN は、ファブリック A だけに適用されます。 • [Fabric B]：指定した VLAN は、ファブリック B だけに適用されます。 • [Both Fabrics Configured Differently]：指定した VLAN は、両方のファブリックに適用されますが、ファブリックごとに異なる VLAN ID を指定できます。 アップストリーム disjoint L2 ネットワークの場合、[Common/Global] を選択して、両方のファブリックに適用する VLAN を作成することをお勧めします。
[VLAN IDs] フィールド	1 つの VLAN を作成するには、単一の数値 ID を入力します。複数の VLAN を作成するには、個々の ID や ID の範囲をカンマで区切って入力します。 VLAN ID には次の値を入力できます。 • 1 ～ 3967 の範囲 • 4048 ～ 4093 の範囲 • システム上ですでに定義されている他の VLAN ID と重複する値 たとえば、ID が 4、22、40、41、42、および 43 の 6 つの VLAN を作成するには、4, 22, 40-43 を入力します。 **重要** 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。 LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

名前	説明
[Sharing Type] フィールド	この VLAN がプライベート VLAN またはセカンダリ VLAN に再分割されるかどうか。 次のいずれかになります。 • [None]：この VLAN には、セカンダリ VLAN またはプライベート VLAN がありません。 • [Primary]：[Secondary VLANs] 領域に示すように、この VLAN には 1 つ以上のセカンダリ VLAN が存在できます。 • [Isolated]：これはプライベート VLAN です。 プライマリ VLAN とこれが関連付けられた VLAN は、[Primary VLAN] ドロップダウン リストに表示されます。
[Primary VLAN] ドロップダウン リスト	[Sharing Type] フィールドが [Isolated] に設定されている場合、これはこのプライベート VLAN に関連付けられたプライマリ VLAN です。
VLAN の許容組織	VLAN に表示されるリストから組織を選択します。 この VLAN は、ここで選択する組織で使用できます。
[Check Overlap] ボタン	このボタンをクリックして、VLAN ID がシステム上の他の ID と重複していないかどうか確認します。

ステップ 6 [Check Overlap] ボタンをクリックした場合は、次の作業を実行します。

a) [Overlapping VLANs] タブをクリックし、次の各フィールドを確認して VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリック インターコネクトでもアクセスできます。 この設定は、ファブリック インターコネクトレベルとは対照的に、システム レベルで作成された仮想 LAN および SAN ネットワークに適用されます。
[Name] カラム	VLAN の名前。
[VLAN] カラム	VLAN の数値 ID。

名前	説明
[DN] カラム	VLAN へのフル パス。 VALN のプロパティを表示するには、このカラムのリンクをクリックします。

b) [Overlapping VSANs] タブをクリックし、次の各フィールドを確認して VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリック インターコネクトでもアクセスできます。 この設定は、ファブリック インターコネクトレベルとは対照的に、システムレベルで作成された仮想 LAN および SAN ネットワークに適用されます。
[Name] カラム	VSAN の名前。
[ID] カラム	VSAN の数値 ID。
[FCoE VLAN ID] カラム	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。
[DN] カラム	VSAN へのフル パス。 VSAN のプロパティを表示するには、このカラムのリンクをクリックします。

c) [OK] をクリックします。

d) Cisco UCS Manager によって VLAN ID または FCoE VLAN ID の重複が識別された場合には、既存の VLAN と重複しない VLAN ID に変更します。

ステップ 7 [OK] をクリックします。

Cisco UCS Manager は、次のいずれかの [VLANs] ノードにプライマリ VLAN を追加します。

- 両方のファブリック インターコネクトにアクセス可能なプライマリ VLAN の場合は、[LAN Cloud] > [VLANs] ノード。
- 1 つのファブリック インターコネクトだけにアクセス可能なプライマリ VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

プライベート VLAN 用のセカンダリ VLAN の作成

ハイ アベイラビリティ用に設定された Cisco UCS ドメインでは、両方のファブリック インターコネクトまたは 1 つのファブリック インターコネクトだけにアクセスできるセカンダリ VLAN を作成できます。

重要 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。

LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

はじめる前に

プライマリ VLAN を作成します。

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create VLANs] 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
[VLAN Name/Prefix] フィールド	単一の VLAN の場合、VLAN 名を指定します。 VLAN の範囲の場合、各 VLAN 名に使用される接頭辞を指定します。 VLAN 名の大文字と小文字は区別されます。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Multicast Policy] ドロップダウン リスト	この VLAN に関連付けられたマルチキャスト ポリシー。 ポリシーを選択しなかった場合、Cisco UCS Manager はデフォルトのマルチキャスト ポリシーの設定を使用します。

名前	説明
[Create Multicast Policy] リンク	すべての VLAN に使用可能な新しいマルチキャスト ポリシーを作成するには、このリンクをクリックします。
設定オプション	次のいずれかを選択できます。 • [Common/Global]：指定した VLAN は両方のファブリックに適用され、どちらのファブリックでも同じ設定パラメータが使用されます。 • [Fabric A]：指定した VLAN は、ファブリック A だけに適用されます。 • [Fabric B]：指定した VLAN は、ファブリック B だけに適用されます。 • [Both Fabrics Configured Differently]：指定した VLAN は、両方のファブリックに適用されますが、ファブリックごとに異なる VLAN ID を指定できます。 アップストリーム disjoint L2 ネットワークの場合、[Common/Global] を選択して、両方のファブリックに適用する VLAN を作成することをお勧めします。
[VLAN IDs] フィールド	1 つの VLAN を作成するには、単一の数値 ID を入力します。複数の VLAN を作成するには、個々の ID や ID の範囲をカンマで区切って入力します。 VLAN ID には次の値を入力できます。 • 1 ～ 3967 の範囲 • 4048 ～ 4093 の範囲 • システム上ですでに定義されている他の VLAN ID と重複する値 たとえば、ID が 4、22、40、41、42、および 43 の 6 つの VLAN を作成するには、4, 22, 40-43 を入力します。 **重要** 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。 LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

名前	説明
[Sharing Type] フィールド	この VLAN がプライベート VLAN またはセカンダリ VLAN に再分割されるかどうか。 次のいずれかになります。 • [None]：この VLAN には、セカンダリ VLAN またはプライベート VLAN がありません。 • [Primary]：[Secondary VLANs] 領域に示すように、この VLAN には 1 つ以上のセカンダリ VLAN が存在できます。 • [Isolated]：これはプライベート VLAN です。 プライマリ VLAN とこれが関連付けられた VLAN は、[Primary VLAN] ドロップダウン リストに表示されます。
[Primary VLAN] ドロップダウン リスト	[Sharing Type] フィールドが [Isolated] に設定されている場合、これはこのプライベート VLAN に関連付けられたプライマリ VLAN です。
VLAN の許容組織	VLAN に表示されるリストから組織を選択します。 この VLAN は、ここで選択する組織で使用できます。
[Check Overlap] ボタン	このボタンをクリックして、VLAN ID がシステム上の他の ID と重複していないかどうか確認します。

（注） マルチキャスト ポリシーは、セカンダリ VLAN ではなく、プライマリ VLAN に関連付けられます。

ステップ 6 [Check Overlap] ボタンをクリックした場合は、次の作業を実行します。

a) [Overlapping VLANs] タブをクリックし、次の各フィールドを確認して VLAN ID が既存の VLAN に割り当てられた ID と重複していないことを確認します。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリック インターコネクトでもアクセスできます。 この設定は、ファブリック インターコネクトレベルとは対照的に、システム レベルで作成された仮想 LAN および SAN ネットワークに適用されます。
[Name] カラム	VLAN の名前。

名前	説明
[VLAN] カラム	VLAN の数値 ID。
[DN] カラム	VLAN へのフル パス。 VALN のプロパティを表示するには、このカラムのリンクをクリックします。

b) [Overlapping VSANs] タブをクリックし、次の各フィールドを確認して VLAN ID が既存の VSAN に割り当てられた FCoE VLAN ID と重複していないことを確認します。

名前	説明
[Fabric ID] カラム	次のいずれかになります。 • A • B • [Dual]：コンポーネントはどちらのファブリック インターコネクトでもアクセスできます。 この設定は、ファブリック インターコネクトレベルとは対照的に、システムレベルで作成された仮想 LAN および SAN ネットワークに適用されます。
[Name] カラム	VSAN の名前。
[ID] カラム	VSAN の数値 ID。
[FCoE VLAN ID] カラム	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。
[DN] カラム	VSAN へのフル パス。 VSAN のプロパティを表示するには、このカラムのリンクをクリックします。

c) [OK] をクリックします。

d) Cisco UCS Manager によって VLAN ID または FCoE VLAN ID の重複が識別された場合には、既存の VLAN と重複しない VLAN ID に変更します。

ステップ 7 [OK] をクリックします。

Cisco UCS Manager は、次のいずれかの [VLANs] ノードにプライマリ VLAN を追加します。

- 両方のファブリック インターコネクトにアクセス可能なプライマリ VLAN の場合は、[LAN Cloud] > [VLANs] ノード。

- 1 つのファブリック インターコネクトだけにアクセス可能なプライマリ VLAN の場合は、[*Fabric_Interconnect_Name*] > [VLANs] ノード。

VLAN ポート数の表示

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

ステップ 3 VLAN ポート数を表示するファブリック インターコネクトをクリックします。

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

ステップ 5 [General] タブで、[VLAN Port Count] バーの下矢印をクリックしてその領域を展開します。
Cisco UCS Manager GUI に、次の詳細が表示されます。

名前	説明
[VLAN Port Limit] フィールド	このファブリック インターコネクトで許可される VLAN ポートの最大数。
[Access VLAN Port Count] フィールド	使用可能な VLAN アクセス ポートの数。
[Border VLAN Port Count] フィールド	使用可能な VLAN ボーダー ポートの数。
[Allocation Status] フィールド	VLAN ポート割り当てのステータス。

VLAN のポート数の最適化

VLAN のポート数の最適化により、複数の VLAN の状態を単一の内部状態にマップできます。 VLAN のポート数の最適化をイネーブルにすると、Cisco UCS Manager は、ポート VLAN メンバーシップに基づいて VLAN を論理的にグループ化します。 このグループ化により、ポート VLAN 数の制限が増加します。 また、VLAN のポート数の最適化により、VLAN ステートが圧縮され、ファブリック インターコネクトの CPU の負荷が軽減されます。 この CPU の負荷の軽減により、より多くの VLAN をより多くの vNIC に展開できます。 VLAN のポート数を最適化しても、vNIC 上の既存の VLAN 設定は変更されません。

デフォルトでは、VLAN ポート数の最適化はディセーブルです。 要件に基づいて、オプションをイネーブルまたはディセーブルにできます。

重要

- VLAN ポート数の最適化をイネーブルにすると、使用可能な VLAN ポート数が増加します。 ポート VLAN 数が非最適化された状態の VLAN の最大数を超えると、VLAN ポート数の最適化をディセーブルにできません。
- VLAN ポート数の最適化は、Cisco UCS 6100 シリーズ ファブリック インターコネクトではサポートされていません。

ポート VLAN 数の最適化のイネーブル化

デフォルトでは、ポート VLAN 数の最適化はディセーブルです。 この機能をイネーブルにすると、CPU の使用率を最適化し、ポート VLAN 数を増加できます。

手順

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

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

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

ステップ 4 [Port, VLAN Count Optimization] セクションで、[Enabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Port, VLAN Count Optimization] オプションが正常にイネーブルになると、確認メッセージが表示されます。 [OK] をクリックして、ダイアログボックスを閉じます。

ポート VLAN 数の最適化のディセーブル化

デフォルトでは、ポート VLAN 数の最適化はディセーブルです。 この機能をイネーブルにしてポート VLAN 数が増加した場合で、CPU の使用率を最適化する場合は、この機能をディセーブルにできます。

手順

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

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

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

ステップ 4 [Port, VLAN Count Optimization] セクションで、[Disabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Port, VLAN Count Optimization] オプションが正常にディセーブルになると、確認メッセージが表示されます。 [OK] をクリックして、ダイアログボックスを閉じます。

VLAN の最適化設定の表示

システム内の VLAN ID に基づいて VLAN のポート数の最適化グループが自動的に作成されます。グループ内のすべての VLAN によって、同じ IGMP ポリシーが共有されます。 次の VLAN は VLAN ポート数の最適化グループに含められません。

- FCoE VLAN
- プライマリ PVLAN とセカンダリ PVLAN
- SPAN 送信元として指定された VLAN
- インターフェイス上で、単一の許可された VLAN として設定された VLAN、および単一の VLAN のあるポート プロファイル

Cisco UCS Manager GUI は、最適化された VLAN を自動的にグループ化します。

手順

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

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

ステップ 3 [Navigation] ペインで [Fabric A] または [Fabric B] をクリックし、リストを展開します。

ステップ 4 [VLAN Optimization Sets] をクリックします。
[Work] ペインに、VLAN の最適化グループのリストが [Name] および [Size] とともに表示されます。

VLAN グループ

VLAN グループでは、機能または特定のネットワークに属する VLAN により、イーサネット アップリンク ポート上の VLAN をグループ化できます。 VLAN メンバーシップを定義し、そのメンバーシップをファブリック インターコネクト上の複数のイーサネット アップリンク ポートに適用できます。

VLAN を VLAN グループに割り当てた後、VLAN グループへの変更が、VLAN グループで設定されているすべてのイーサネット アップリンク ポートに適用されます。 また、VLAN グループにより、分離された VLAN 間の VLAN の重複も識別できます。

VLAN グループ下で、アップリンク ポートを設定できます。 VLAN グループのアップリンク ポートを設定すると、そのアップリンク ポートは、そのグループ内のすべての VLAN だけをサポートします。

VLAN グループは、LAN クラウドまたは LAN アップリンク マネージャから作成できます。

VLAN グループの作成

[LAN Cloud] または [LAN Uplinks Manager] から、[VLAN Group] を作成できます。 この手順では、[LAN Cloud] から VLAN グループを作成する方法について説明します。

手順

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

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

ステップ 3 [LAN Cloud] を右クリックして、ドロップダウン オプションから [Create VLAN Group] を選択します。
[Create VLAN Group] ウィザードが起動します。

ステップ 4 [Select VLANs] ペインで、次の操作を実行して [Next] をクリックします。

名前	説明
Name	VLAN グループの名前を入力します。 VLAN グループ名では、大文字と小文字が区別されます。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

名前	説明
VLANs	表示されたリストから、グループに追加する VLAN を選択します。 選択したいずれかの VLAN を [Native VLAN] として選択できます。
Create VLAN	このグループに新しいVLANを追加するには、[Create VLAN] をクリックします。

ステップ 5 （任意）[Add Uplink Ports] ペインで、表示されたリストから [Uplink Ports] を選択して [Selected Uplink Ports] に追加します。

ステップ 6 （任意）[Add Port Channels] ペインで、[Port Channels] を選択して [Selected Port Channels] に追加します。

ステップ 7 （任意）[Org Permissions] ペインで、表示されたリストから適切なグループを選択します。
ここで作成するグループに属する VLAN は、ここで選択したグループだけにアクセスできます。

ステップ 8 [Finish] をクリックします。
この VLAN グループは、[LAN] > [LAN Cloud] > [VLAN Groups] の下にある [VLAN Groups] のリストに追加されます。

VLAN グループのメンバの編集

手順

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

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

ステップ 3 [Navigation] ペインで、[VLAN Groups] をクリックして VLAN グループのリストを展開します。

ステップ 4 表示された VLAN グループのリストから、グループ メンバの VLAN を編集する VLAN グループ名を選択します。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 5 強調表示された 1 つまたは複数の VLAN グループを右クリックし、[Edit VLAN Group Members] を選択します。
[Modify VLAN Group *VLAN Group Name*] ダイアログボックスが開きます。

ステップ 6 [Modify VLAN Group *VLAN Group Name*] ダイアログボックスで、表示されたリストから追加または削除する VLAN を選択し、[Next] をクリックします。

ステップ 7 （任意）[Add Port Channels] ペインで、[Port Channels] を選択して [Selected Port Channels] に追加します。

ステップ 8 （任意）[Org Permissions] ペインで、表示されたリストから適切なグループを選択します。
ここで作成するグループに属する VLAN は、ここで選択したグループだけにアクセスできます。

ステップ 9 [Finish] をクリックします。

ステップ 10 この VLAN グループは、選択に基づいて変更されます。

VLAN グループの組織アクセス権限の変更

VLAN グループの組織アクセス権限を変更すると、権限の変更はその VLAN グループのすべての VLAN に適用されます。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] > [VLAN Group] を展開し、[VLAN group name] を選択します。

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 [Actions] で、[Modify VLAN Groups Org Permissions] をクリックします。
[Modify VLAN Groups Org Permissions] ダイアログボックスが開きます。

ステップ 5 [Org Permissions] で、次の作業を実行します。

- 組織を追加する場合は、組織を選択します。
- 組織からアクセス権限を削除する場合は、クリックして選択を削除します。

ステップ 6 [OK] をクリックします。

VLAN グループの削除

手順

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

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

ステップ 3 [Navigation] ペインで、[VLAN Groups] をクリックして VLAN グループのリストを展開します。

ステップ 4 表示された VLAN グループのリストから、削除する VLAN グループの名前を選択します。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 5 強調表示された 1 つまたは複数の VLAN グループを右クリックし、[Delete] を選択します。

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

VLAN の権限

VLAN の権限は、指定された組織に基づいて VLAN へのアクセスを制限します。 また、VLAN が属するサービス プロファイルの組織に基づいて、サービス プロファイル vNIC に割り当てることができる VLAN のセットも制限します。 VLAN の権限はオプションの機能であり、デフォルトではディセーブルです。 要件に基づいて、機能をイネーブルまたはディセーブルにできます。 機能をディセーブルにすると、すべての VLAN は、すべての組織に対してグローバルにアクセスできます。

（注） [LAN] > [LAN Cloud] > [Global Policies] > [Org Permissions] で組織の権限をイネーブルにした場合、VLAN を作成すると、[Create VLANs] ダイアログボックスに [Permitted Orgs for VLAN(s)] オプションが表示されます。 [Org Permissions] をイネーブルにしない場合は、[Permitted Orgs for VLAN(s)] オプションが表示されません。

組織の権限をイネーブルにした場合は、VLAN の作成時に VLAN に組織を指定します。 組織を指定すると、その VLAN は、その特定組織および構造下にあるすべてのサブ組織で使用可能になります。 他の組織のユーザは、この VLAN にアクセスできません。 また、VLAN のアクセス要件の変更に基づいて、VLAN の権限を任意の時点で変更することもできます。

注意 ルート レベルで組織に VLAN 組織の権限を割り当てると、すべてのサブ組織が VLAN にアクセスできます。 ルート レベルで組織の権限を割り当てた後、サブ組織に属する VLAN の権限を変更した場合は、その VLAN がルート レベルの組織で使用できなくなります。

VLAN の権限のイネーブル化

デフォルトでは、VLAN の権限はディセーブルになっています。 異なる組織の権限を作成して VLAN アクセスを制限する場合は、組織の権限オプションをイネーブルにする必要があります。

手順

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

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

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

ステップ 4 [Org Permissions] セクションで、[Enabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Org Permissions] オプションが正常にイネーブルになると、確認メッセージが表示されます。 [OK] をクリックして、ダイアログボックスを閉じます。

VLAN の権限のディセーブル化

デフォルトでは、VLAN の権限はディセーブルになっています。 このオプションをイネーブルにした後、VLAN の権限を別のネットワーク グループに割り当てたため、このオプションを使用しなくなった場合は、オプションをグローバルにディセーブルにできます。 VLAN の組織の権限機能をディセーブルにした場合、VLAN に割り当てた権限は引き続きシステム内に存在しますが、施行されません。 組織の権限を後で使用する場合は、この機能をイネーブルにして割り当てられた権限を使用できます。

手順

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

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

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

ステップ 4 [Org Permissions] セクションで、[Disabled] を選択します。

ステップ 5 [Save Changes] をクリックします。

ステップ 6 [Org Permissions] オプションが正常にディセーブルになると、確認メッセージが表示されます。 [OK] をクリックして、ダイアログボックスを閉じます。

VLAN の権限の追加または変更

VLAN の許可された組織を追加または削除できます。

（注） VLAN の許可された組織として組織を追加すると、すべての下位組織が VLAN にアクセスできます。 このため、組織から VLAN へのアクセス権限を削除すると、すべての下位組織が VLAN にアクセスできなくなります。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] > [VLANs] を展開し、*[VLAN name]* を選択します。

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 [Actions] で、[Modify VLAN Org Permissions] をクリックします。
[Modify VLAN Org Permissions] ダイアログボックスが開きます。

ステップ 5 [Permitted Orgs for VLAN(s)] で、

- 組織を追加する場合は、組織を選択します。
- 組織からアクセス権限を削除する場合は、クリックして選択を削除します。

ステップ 6 [OK] をクリックします。

第 18 章

LAN ピン グループの設定

この章の内容は、次のとおりです。

- LAN ピン グループ，285 ページ
- LAN ピン グループの作成，286 ページ
- LAN ピン グループの削除，287 ページ

LAN ピン グループ

Cisco UCS は LAN ピン グループを使用して、サーバ上の vNIC から、ファブリック インターコネクトのアップリンク イーサネット ポートまたはポート チャネルに、イーサネット トラフィックをピン接続します。 このピン接続を使用して、サーバからのトラフィックの分散を管理できます。

サーバにピン接続を設定するには、LAN ピン グループを vNIC ポリシーにインクルードする必要があります。 次に、vNIC ポリシーは、そのサーバに割り当てられたサービス プロファイル内に取り込まれます。 vNIC からのすべてのトラフィックは、I/O モジュールを経由して所定のアップリンク イーサネット ポートに進みます。

（注） ピン グループが vNIC ポリシーを使用してサーバ インターフェイスに割り当てられていない場合、Cisco UCS Manager は、そのサーバ インターフェイスからのトラフィックに対するアップリンク イーサネット ポートまたはポート チャネルを動的に選択します。 この選択は永続的ではありません。 インターフェイス フラップまたはサーバのリブートの後は、そのサーバ インターフェイスからのトラフィックに対して別のアップリンク イーサネット ポートまたはポート チャネルが使用される可能性があります。

LAN ピン グループの作成

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

はじめる前に

ピン グループの設定に使用するポートおよびポート チャネルを設定します。 使用できるのは、LAN ピン グループでアップリンク ポートとして設定されているポートおよびポート チャネルだけです。

手順

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

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

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

ステップ 4 [Create LAN Pin Group] ダイアログボックスで、ピン グループの一意の名前と説明を入力します。

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

a) [Fabric Interconnect A] チェックボックスをオンにします。

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

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

a) [Fabric Interconnect B] チェックボックスをオンにします。

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

ステップ 7 [OK] をクリックします。

次の作業

ピン グループは、vNIC テンプレートにインクルードします。

LAN ピン グループの削除

手順

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

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

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

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

第 19 章

MAC プールの設定

この章の内容は、次のとおりです。

- MAC プール，289 ページ
- MAC プールの作成，290 ページ
- MAC プールの削除，291 ページ

MAC プール

MAC プールは、ネットワーク ID（MAC アドレス）の集まりです。MAC アドレスはレイヤ 2 環境では一意で、サーバの vNIC に割り当てることができます。サービス プロファイルで MAC プールを使用する場合、サービス プロファイルに関連付けられたサーバで使用できるように MAC アドレスを手動で設定する必要はありません。

マルチテナント機能を実装しているシステムでは、組織階層を使用して、この MAC プールが特定のアプリケーションまたはビジネス サービスでのみ使用できるようにすることができます。Cisco UCS Manager は名前解決ポリシーを使用してプールから MAC アドレスを割り当てます。

サーバに MAC アドレスを割り当てるには、vNIC ポリシーに MAC プールをインクルードする必要があります。 次に、vNIC ポリシーは、そのサーバに割り当てられたサービス プロファイル内に取り込まれます。

独自の MAC アドレスを指定することもできますし、シスコにより提供された MAC アドレスのグループを使用することもできます。

MAC プールの作成

手順

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

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

名前	説明
[Name] フィールド	MAC 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	MAC プールの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Assignment Order] フィールド	次のいずれかになります。 • [Default]：Cisco UCS Manager はプールからランダム ID を選択します。 • [Sequential]：Cisco UCS Manager はプールから最も小さい使用可能 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 MAC Pool] ウィザードの [Add MAC Addresses] ページで、[Add] をクリックします。

ステップ 8 [Create a Block of MAC Addresses] ページで、次のフィールドに値を入力します。

名前	説明
[First MAC Address] フィールド	ブロック内の最初の MAC アドレス。

名前	説明
[Size] フィールド	ブロック内の MAC アドレスの数。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックします。

次の作業

MAC プールは、vNIC テンプレートにインクルードします。

MAC プールの削除

プールを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられたアドレスをプールから再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたプールからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

ステップ 3 [MAC Pools] ノードを展開します。

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

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

第 20 章

Quality of Service の設定

この章の内容は、次のとおりです。

- Quality of Service，293 ページ
- システム クラスの設定，293 ページ
- Quality of Service ポリシーの設定，297 ページ
- フロー制御ポリシーの設定，301 ページ

Quality of Service

Cisco UCS は、Quality Of Service を実装するために、次の方法を提供しています。

- システム全体にわたって、特定のタイプのトラフィックに対するグローバル設定を指定するためのシステム クラス
- 個々の vNIC にシステム クラスを割り当てる QoS ポリシー
- アップリンク イーサネット ポートによるポーズ フレームの扱い方法を決定するフロー制御ポリシー

システム クラスの設定

システム クラス

Cisco UCS では、Cisco UCS ドメイン内のすべてのトラフィックを処理するために、Data Center Ethernet（DCE）が使用されます。 イーサネットに対するこの業界標準の機能拡張では、イーサネットの帯域幅が 8 つの仮想レーンに分割されています。 内部システムと管理トラフィック用に 2 つの仮想レーンが予約されています。 それ以外の 6 つの仮想レーンの Quality of Service を設定できます。 Cisco UCS ドメイン全体にわたり、これら 6 つの仮想レーンで DCE 帯域幅がどのように割り当てられるかは、システム クラスによって決定されます。

各システムクラスでは、特定のトラフィックタイプのために、帯域幅の特定セグメントが予約されています。 これにより、オーバーサブスクライブされたシステムでも、ある程度のトラフィック管理ができるようになります。 たとえば、ファイバ チャネル プライオリティ システム クラスを設定して、FCoE トラフィックに割り当てられる DCE 帯域幅の割合を決定することができます。

次の表は、設定可能なシステム クラスをまとめたものです。

表 7: システム クラス

システム クラス	説明
Platinum Gold Silver Bronze	サービス プロファイルの QoS ポリシーにインクルードできる設定可能なシステム クラスのセット。 各システム クラスはトラフィック レーンを 1 つ管理します。 これらのシステムクラスのプロパティはすべて、カスタム設定やポリシーを割り当てるために使用できます。
Best Effort	ベーシック イーサネット トラフィックのために予約されたレーンに対する Quality Of Service を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。 たとえば、このクラスには、必要に応じて、データ パケットのドロップを許可するドロップ ポリシーがあります。 このシステム クラスをディセーブルにはできません。
ファイバ チャネル	Fibre Channel over Ethernet トラフィックのために予約されたレーンに対する Quality Of Service を設定するシステム クラス。 このシステム クラスのプロパティの中にはあらかじめ設定されていて、変更できないものもあります。 たとえば、このクラスには、データ パケットが絶対にドロップされないことを保証するドロップなしポリシーがあります。 このシステム クラスをディセーブルにはできません。

QoS システム クラスの設定

サーバ内のアダプタのタイプによっては、サポートされる MTU の最大値が制限される場合があります。 たとえば、ネットワーク MTU が最大値を超えた場合、次のアダプタでパケットがドロップする可能性があります。

- Cisco UCS M71KR CNA アダプタ：サポートされる MTU の最大値は 9216 です。
- Cisco UCS 82598KR-CI アダプタ：サポートされる MTU の最大値は 14000 です。

手順

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

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

ステップ 3 [QoS System Class] ノードを選択します。

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

ステップ 5 システムのトラフィック管理ニーズを満たすために設定するシステム クラスの次のプロパティを更新します。

（注） 一部のプロパティはすべてのシステム クラスに対して設定できない場合があります。

名前	説明
[Enabled] チェックボックス	このチェックボックスをオンにすると、対応する QoS クラスがファブリック インターコネクト上で設定され、QoS ポリシーに割り当て可能になります。 このチェックボックスをオフにすると、このクラスはファブリック インターコネクト上で設定されず、このクラスに関連付けられた QoS ポリシーはデフォルトの [Best Effort] になるか、（システム クラスが 0 の Cos で設定されている場合は）Cos 0 システム クラスになります。 （注） このフィールドは、[Best Effort] と [Fibre Channel] の場合は常にオンです。
[Cos] フィールド	サービス クラス。 0 ～ 6 の整数を入力できます。0 は最低プライオリティを表し、6 は最高プライオリティを表します。 QoS ポリシーが削除されるか、割り当てられたシステム クラスがディセーブルになったときに、システム クラスをトラフィックのデフォルト システム クラスにする必要がある場合を除き、この値を 0 に設定することは推奨しません。 （注） このフィールドは、内部トラフィックの場合は 7 に、[Best Effort] の場合は [any] に設定されます。 これらの値は両方とも予約されており、他のプライオリティに割り当てることはできません。
[Packet Drop] チェックボックス	このチェックボックスをオンにすると、このクラスに対してパケットの破棄が許可されます。 このチェックボックスをオフにすると、送信時にパケットを破棄できません。 このフィールドは、[Fibre Channel] クラスの場合は常にオフであり（破棄パケットは決して許可されない）、[Best Effort] の場合は常にオンです（破棄パケットは常に許可される）。

名前	説明
[Weight] ドロップダウン リスト	次のいずれかになります。 • 1 ～ 10 の整数。 整数を入力すると、[Weight (%)] フィールドの説明に従って、このプライオリティ レベルに割り当てられるネットワーク帯域幅の割合が Cisco UCS によって決定されます。 • best-effort. • none.
[Weight (%)] フィールド	チャネルに割り当てられる帯域幅を決定するために、Cisco UCS によって次の作業が実行されます。 **1** すべてのチャネルの重みを加算します。 **2** チャネルの重みをすべての重みの和で割って、割合を求めます。 **3** その割合の帯域幅をチャネルに割り当てます。
[MTU] ドロップダウン リスト	チャネルの最大伝送単位。 次のいずれかになります。 • 1500 ～ 9216 の整数。 この値は最大パケット サイズに対応します。 • [fc]：事前に定義されている 2240 のパケット サイズ。 • [normal]：事前に定義されている 1500 のパケット サイズ。 （注） このフィールドは、[Fibre Channel] の場合は常に [fc] に設定されます。
[Multicast Optimized] チェックボックス	このチェックボックスをオンにすると、パケットを複数の宛先に同時に送信するように、クラスが最適化されます。 （注） このオプションは、[Fibre Channel] には適用されません。

ステップ 6 [Save Changes] をクリックします。

QoS システム クラスのイネーブル化

デフォルトでは、Best Effort システム クラスまたは Fibre Channel システム クラスはイネーブルになっています。

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。
ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] を展開します。
ステップ 3 [QoS System Class] ノードを選択します。
ステップ 4 [Work] ペインの [General] タブをクリックします。
ステップ 5 イネーブルにする QoS システム クラスの [Enabled] 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。

QoS システム クラスのディセーブル化

ベスト エフォート システム クラスやファイバ チャネル システム クラスはディセーブルにできません。

ディセーブルにされたシステム クラスに関連付けられているすべての QoS ポリシーのデフォルトは、Best Effort です。ディセーブルにされたシステムの Class of Service（CoS; クラス オブ サービス）が 0 に設定されている場合のデフォルトは、Cos 0 システム クラスになります。

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。
ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] を展開します。
ステップ 3 [QoS System Class] ノードを選択します。
ステップ 4 [Work] ペインの [General] タブをクリックします。
ステップ 5 ディセーブルにする QoS システムの [Enabled] チェックボックスをオフにします。
ステップ 6 [Save Changes] をクリックします。

Quality of Service ポリシーの設定

Quality Of Service ポリシー

Quality Of Service（QoS）ポリシーは、vNIC または vHBA に向けた発信トラフィックにシステム クラスを割り当てます。 このシステム クラスにより、このトラフィックに対する Quality Of Service が決定されます。 一部のアダプタでは、発信トラフィックでバーストやレートなど追加の制御を指定することもできます。

vNICポリシー、またはvHBAポリシーにQoSポリシーをインクルードし、その後、このポリシーをサービス プロファイルにインクルードして、vNIC または vHBA を設定する必要があります。

QoS ポリシーの作成

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] 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 [QoS Policy] を右クリックし、[Create QoS Policy] を選択します。

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

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

名前	説明
[Priority] ドロップダウン リスト	この QoS 定義に割り当てられたプライオリティ。 次のいずれかになります。 • [Fc]：vHBA トラフィックだけを制御する QoS ポリシーにこのプライオリティを使用します。 • [Platinum]：vNIC トラフィックだけを制御する QoS ポリシーにこのプライオリティを使用します。 • [Gold]：vNIC トラフィックだけを制御する QoS ポリシーにこのプライオリティを使用します。 • [Silver]：vNIC トラフィックだけを制御する QoS ポリシーにこのプライオリティを使用します。 • [Bronze]：vNIC トラフィックだけを制御する QoS ポリシーにこのプライオリティを使用します。 • [Best Effort]：このプライオリティを使用しないでください。 ベーシック イーサネット トラフィック レーンのために予約されています。 このプライオリティを QoS ポリシーに割り当て、別のシステム クラスを CoS 0 に設定する場合、Cisco UCS Manager はこのシステム クラスのデフォルトには戻りません。 そのトラフィックの CoS 0 でプライオリティがデフォルトに戻ります。
[Burst] フィールド	このポリシーを使用するサーバの通常バースト サイズ。 このフィールドにより、トラフィックがレート制限を超えていると見なされずに到達できるトラフィック バーストの最大サイズが決定されます。 デフォルトは 10240 です。 最小値は 0 で、最大値は 65535 です。 この設定は、一部のアダプタには適用されません。

名前	説明
[Rate] フィールド	想定されるトラフィックの平均レート。 このレートを下回るトラフィックは、常に準拠です。 デフォルトは回線速度です。 これは、値が 0 の場合と等しく、レート制限が指定されません。 最小値は 8 で、最大値は 40,000,000 です。 Cisco UCS M81KR 仮想インターフェイス カードアダプタのレート制限の粒度は、1Mbps です。 これらのアダプタでは、要求したレートが「超えてはならない」レートとして扱われます。 したがって、4.5Mbps の値は 4Mbps と解釈されます。 0 より大きくて 1Mbps より小さい要求レートは、1Mbps と解釈されます。 これは、サポートされる最低のハードウェア レート制限です。 レート制限は、一部のアダプタには適用されません。 たとえば、この設定は Cisco UCS M82-8P 仮想インターフェイス カードでサポートされていません。
[Host Control] フィールド	Cisco UCS がサービス クラス（CoS）を制御するかどうか。 次のいずれかになります。 • [None]：ホストによって割り当てられた CoS 値に関係なく、[Priority] ドロップダウン リストで選択されたプライオリティに関連付けられている CoS 値が Cisco UCS で使用されます。 • [Full]：ホストによって割り当てられた有効な CoS 値がパケットにある場合、その値が Cisco UCS で使用されます。 そうでなければ、[Priority] ドロップダウン リストで選択されたプライオリティと関連付けられている CoS 値が Cisco UCS で使用されます。 この設定は、一部のアダプタには適用されません。

ステップ 6 [OK] をクリックします。

次の作業

QoS ポリシーは、vNIC または vHBA テンプレートにインクルードします。

QoS ポリシーの削除

使用中の QoS ポリシーを削除した場合、または QoS ポリシーで使用されているシステム クラスをディセーブルにした場合、この QoS ポリシーを使用している vNIC と vHBA はすべて、ベストエフォート システム クラスまたは CoS が 0 のシステム クラスに割り当てられます。 マルチテナ

ント機能を実装しているシステムでは、Cisco UCS Manager はまず、組織階層から一致する QoS ポリシーを見つけようとします。

手順

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

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

ステップ 3 [QoS Policies] ノードを展開します。

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

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

フロー制御ポリシーの設定

フロー制御ポリシー

フロー制御ポリシーは、ポートの受信バッファがいっぱいになったときに、Cisco UCS ドメインのアップリンク イーサネット ポートが IEEE 802.3x ポーズ フレームを送信および受信するかどうかを決定します。 これらのポーズフレームは、バッファがクリアされるまでの数ミリ秒間、送信側ポートからのデータの送信を停止するように要求します。

LAN ポートとアップリンク イーサネット ポートの間でフロー制御が行われるようにするには、両方のポートで、対応する受信および送信フロー制御パラメータをイネーブルにする必要があります。 Cisco UCS では、これらのパラメータはフロー制御ポリシーによって設定されます。

送信機能をイネーブルにした場合、受信パケット レートが高くなりすぎたときに、アップリンク イーサネット ポートはネットワーク ポートにポーズ要求を送信します。 ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。 受信機能をイネーブルにした場合、アップリンク イーサネット ポートは、ネットワーク ポートからのポーズ要求すべてに従います。 ネットワーク ポートがポーズ要求をキャンセルするまで、すべてのトラフィックはこのアップリンク ポートで停止します。

ポートにフロー制御ポリシーを割り当てているため、このポリシーを変更すると同時に、ポーズ フレームやいっぱいになっている受信バッファに対するポートの反応も変わります。

フロー制御ポリシーの作成

はじめる前に

必要なフロー制御に対応する設定を使用して、ネットワーク ポートを設定します。 たとえば、ポリシーのフロー制御ポーズ フレームに対する送信設定をイネーブルにした場合は、必ず、ネットワーク ポートの受信パラメータを on または desired に設定します。 Cisco UCS ポートでフロー制御フレームを受信する場合は、ネットワーク ポートの送信パラメータが on または desired に設定

されていることを確認します。フロー制御を使用する必要がない場合は、ネットワーク ポートの受信パラメータと送信パラメータを off に設定できます。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。
ルート組織内のフロー制御ポリシーだけを作成できます。 サブ組織内のフロー制御ポリシーは、作成できません。

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

ステップ 5 [Create Flow Control 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Priority] フィールド	次のいずれかになります。 • [Auto]：このファブリック インターコネクト上で PPP を使用するかどうかを決めるために、Cisco UCS とネットワークがネゴシエーションします。 • [On]：このファブリック インターコネクト上で PPP をイネーブルにします。
[Receive] フィールド	次のいずれかになります。 • [Off]：ネットワークからのポーズ要求は無視され、トラフィック フローは通常どおり継続します。 • [On]：ポーズ要求に従い、そのアップリンク ポート上のすべてのトラフィックは、ネットワークでポーズ要求が取り消されるまで停止されます。

名前	説明
[Send] フィールド	次のいずれかになります。 • [Off]：パケット負荷に関係なくポート上のトラフィックが通常どおり流れます。 • [On]：着信パケット レートが高くなり過ぎると、Cisco UCS からポーズ要求がネットワークに送信されます。 ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。

ステップ 6 [OK] をクリックします。

次の作業

フロー制御ポリシーと、アップリンク イーサネット ポート、またはポート チャネルを関連付けます。

フロー制御ポリシーの削除

手順

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

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

ステップ 3 [Flow 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

第 21 章

ネットワーク関連ポリシーの設定

この章の内容は、次のとおりです。

- vNIC テンプレートの設定，305 ページ
- イーサネット アダプタ ポリシーの設定，312 ページ
- デフォルトの vNIC の動作のポリシーの設定，318 ページ
- LAN 接続ポリシーの設定，320 ページ
- ネットワーク制御ポリシーの設定，335 ページ
- マルチキャスト ポリシーの設定，339 ページ

vNIC テンプレートの設定

vNIC テンプレート

このポリシーは、サーバ上の vNIC が LAN に接続する方法を定義します。 このポリシーは、vNIC LAN 接続ポリシーとも呼ばれます。

Cisco UCS Manager は、vNIC テンプレートを作成する場合に、適切な設定で VM-FEX ポート プロファイルを自動的に作成しません。 VM-FEX ポート プロファイルを作成する場合は、vNIC テンプレートのターゲットを VM として設定する必要があります。

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

（注） サーバに 2 つの Emulex または QLogic NIC（Cisco UCS CNA M71KR-E または Cisco UCS CNA M71KR-Q）がある場合は、サービス プロファイル内で両方のアダプタの vNIC ポリシーを設定し、両方の NIC のユーザ定義の MAC アドレスを取得する必要があります。 両方の NIC のポリシーを設定しない場合、Windows は、引き続き両方の NIC を PCI バスで検出します。 次に、2 番目のイーサネットがサービス プロファイルの一部ではないため、Windows がハードウェアの MAC アドレスを割り当てます。 次に、サービス プロファイルを別のサーバに移動した場合は、1 つの NIC にユーザ定義の MAC アドレスがないため、Windows は追加の NIC を表示します。

vNIC テンプレートの作成

はじめる前に

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

- ネームド VLAN
- MAC プール
- QoS ポリシー
- LAN ピン グループ
- 統計情報しきい値ポリシー

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] 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 Templates] ノードを右クリックし、[Create vNIC Template] を選択します。

ステップ 5 [Create vNIC Template] ダイアログボックスで、次の手順を実行します。

a) [General] 領域で、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	virtual Network Interface Card（vNIC; 仮想ネットワーク インターフェイス カード）テンプレートの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	テンプレートのユーザ定義による説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。 デフォルトのファブリック インターコネクトが使用できない場合に、このテンプレートから作成された vNIC から第 2 のファブリック インターコネクトにアクセスできるようにするには、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックのフェールオーバーをイネーブルにしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のものにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバを、このテンプレートから作成された 1 つ以上の vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のものにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバをこの vNIC 設定に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。

名前	説明
[Target] リスト ボックス	このテンプレートから作成された vNIC に可能なターゲットのリスト。 選択したターゲットにより、Cisco UCS Manager が、vNIC テンプレートの適切な設定によって自動的に VM-FEX ポート プロファイルを作成するかどうかを決定します。 次のいずれかになります。 • [Adapter]：vNIC はすべてのアダプタに適用されます。 このオプションを選択すると、VM-FEX ポート プロファイルは作成されません。 • [VM]：vNIC はすべての仮想マシンに適用されます。 このオプションを選択すると、VM-FEX ポート プロファイルが作成されます。
[Template Type] フィールド	次のいずれかになります。 • [Initial Template]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされません。 • [Undating Template]：テンプレートが変更された場合、このテンプレートから作成された vNIC はアップデートされます。

b) [VLANs] 領域で、このテンプレートから作成された vNIC に割り当てる VLAN をテーブルを使用して選択します。 テーブルには、次のカラムがあります。

名前	説明
[Select] カラム	使用する VLAN ごとに、このカラムのチェックボックスをオンにします。
[Name] カラム	VLAN の名前。
[Native VLAN] カラム	VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

c) [Policies] 領域で、次のフィールドに値を入力します。

名前	説明
[MTU] フィールド	この vNIC テンプレートから作成された vNIC によって使用される最大伝送単位、つまりパケット サイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC テンプレートにある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[MAC Pool] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される MAC アドレス プール。
[QoS Policy] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用されるサービス ポリシーの品質。
[Network Control Policy] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用されるネットワーク制御ポリシー。
[Pin Group] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される LAN ピン グループ。
[Stats Threshold Policy] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用される統計情報収集ポリシー。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC テンプレートから作成された vNIC によって使用されるダイナミック vNIC 接続ポリシー。

ステップ 6 [OK] をクリックします。

次の作業

vNIC テンプレートはサービス プロファイルにインクルードします。

vNIC テンプレートへの vNIC のバインディング

サービス プロファイルと関連付けられた vNIC を vNIC テンプレートにバインドすることができます。 vNIC を vNIC テンプレートにバインドした場合、Cisco UCS Manager は vNIC テンプレートで定義された値を使って vNIC を設定します。 既存の vNIC 設定が vNIC テンプレートと一致しない場合、Cisco UCS Manager によって vNIC が再設定されます。 バインドされた vNIC の設定は、関連付けられた vNIC テンプレートを使用してのみ変更できます。 vNIC をインクルードしている

サービスプロファイルがすでにサービスプロファイルテンプレートにバインドされている場合、vNIC を vNIC テンプレートにバインドできません。

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

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

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

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

ステップ 5 テンプレートにバインドする vNIC をクリックします。

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

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

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

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

b) [OK] をクリックします。

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

vNIC テンプレートからの vNIC のバインド解除

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

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

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

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

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

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

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

vNIC テンプレートの削除

手順

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

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

ステップ 3 [vNIC Templates] 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

イーサネット アダプタ ポリシーの設定

イーサネットおよびファイバ チャネル アダプタ ポリシー

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

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

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

- ターゲットごとの最大 LUN：SANsurfer の最大 LUN は 256 であり、この数値を超える値は表示されません。 Cisco UCS Manager でサポートされている最大 LUN 数はこれよりも大きくなっています。
- リンク ダウン タイムアウト：SANsurfer では、リンク ダウンのタイムアウトしきい値を秒単位で設定します。 Cisco UCS Manager では、この値をミリ秒で設定します。 したがって、Cisco UCS Manager で 5500 ミリ秒と設定された値は、SANsurfer では 5 秒として表示されます。
- 最大データ フィールド サイズ：SANsurfer で許可される値は 512、1024、および 2048 です。 Cisco UCS Manager では、任意のサイズの値を設定できます。 したがって、Cisco UCS Manager で 900 と設定された値は、SANsurfer では 512 として表示されます。

オペレーティング システム固有のアダプタ ポリシー

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

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

ただし、（デフォルトの Windows のアダプタ ポリシーを使用する代わりに）Windows OS のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算します。

完了キュー = 送信キュー + 受信キュー
割り込み回数 = (完了キュー + 2) 以上である 2 のべき乗の最小値

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9
割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

イーサネット アダプタ ポリシーの作成

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

手順

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

ステップ 2　[Servers] タブで、[Servers] > [Policies] 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 Ethernet Adapter Policy] を選択します。

ステップ 5　次のフィールドに、ポリシーの名前および説明を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

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

名前	説明
[Transmit Queues] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Ring Size] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

名前	説明
[Receive Queues] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。
[Ring Size] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[Completion Queues] フィールド	割り当てる完了キューリソースの数。 通常、割り当てなければならない完了キューリソースの数は、送信キューリソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
[Interrupts] フィールド	割り当てる割り込みリソースの数。 通常、この値は、完了キューリソースの数と同じにします。 1 ～ 514 の整数を入力します。

ステップ 7 （任意） [Options] 領域で、次の値を調整します。

名前	説明
[Transmit Checksum Offload] フィールド	次のいずれかになります。 • [Disabled]：CPU ですべてのパケット チェックサムが計算されます。 • [Enabled]：チェックサムを計算できるように、CPU からすべてのパケットがハードウェアに送信されます。 このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 **（注）** このオプションは、インターフェイスから送信されたパケットにのみ影響します。
[Receive Checksum Offload] フィールド	次のいずれかになります。 • [Disabled]：CPU ですべてのパケット チェックサムが検証されます。 • [Enabled]：CPU からすべてのパケット チェックサムが検証のためにハードウェアへ送信されます。 このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 **（注）** このオプションは、インターフェイスによって受信されたパケットにのみ影響します。

名前	説明
[TCP Segmentation Offload] フィールド	次のいずれかになります。 • [Sisabled]：大きい TCP パケットが CPU で分割されます。 • [Enabled]：大きい TCP パケットが、CPU からハードウェアに送信されて分割されます。 このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれ、インターフェイスから送信されるパケットのみに影響を及ぼします。
[TCP Large Receive Offload] フィールド	次のいずれかになります。 • [Disabled]：CPU ですべての大きいパケットが処理されます。 • [Enabled]：すべての分割パケットが、CPU に送信される前にハードウェアによって再構築されます。 このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 （注） このオプションは、インターフェイスによって受信されたパケットにのみ影響します。
[Receive Side Scaling] フィールド	RSS により、マルチプロセッサ システムにおいてネットワークの受信処理が複数の CPU に分散されます。 次のいずれかになります。 • [Disabled]：ネットワーク受信処理は、追加のプロセッサが使用可能であっても、常に 1 つのプロセッサで処理されます。 • [Enabled]：ネットワーク受信処理は、可能な場合は常にプロセッサ間で分担されます。
[Failback Timeout] フィールド	セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 0 ～ 600 の範囲の秒数を入力します。

名前	説明
[Interrupt Mode] フィールド	優先ドライバ割り込みモード。 次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。 これは推奨オプションです。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。
[Interrupt Coalescing Type] フィールド	次のいずれかになります。 • [Min]：別の割り込みイベントを送信する前に、[Interrupt Timer] フィールドに指定された時間だけシステムは待機します。 • [Idle]：アクティビティなしの期間が少なくとも [Interrupt Timer] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[Interrupt Timer] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の値を入力します。 割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。

ステップ 8 [OK] をクリックします。

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

Linux オペレーティング システム上の MRQS に対する eNIC サポートをイネーブルにするためのイーサネット アダプタ ポリシーの設定

Cisco UCS Manager には、Red Hat Enterprise Linux バージョン 6.x および SUSE Linux Enterprise Server バージョン 11.x 上の Multiple Receive Queue Support（MRQS）機能に対する eNIC サポートが含まれています。

手順

ステップ 1 イーサネット アダプタ ポリシーを作成します。
イーサネット アダプタ ポリシーを作成する場合は、次のパラメータを使用します。

- 送信キュー = 1

- 受信キュー = n（最大 8）
- 完了キュー = 送信キューの数 + 受信キューの数
- 割り込み = 完了キューの数 + 2
- Receive Side Scaling（RSS）= イネーブル化
- 割り込みモード = Msi-X

イーサネット アダプタ ポリシーの作成, （314 ページ）を参照してください。

ステップ 2 eNIC ドライバ バージョン 2.1.1.35 以降をインストールします。
『Cisco UCS Virtual Interface Card Drivers for Linux Installation Guide』を参照してください。

ステップ 3 サーバをリブートします

イーサネット アダプタ ポリシーの削除

手順

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

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

ステップ 3 [Adapter Policies] ノードを展開します。

ステップ 4 削除するイーサネット 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 5 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

デフォルトの vNIC の動作のポリシーの設定

デフォルトの vNIC および vHBA の動作ポリシー

デフォルトの vNIC および vHBA の動作ポリシーでは、サービス プロファイル用に vNIC および vHBA を作成する方法を設定できます。 vNICS および vHBA を選択して手動で作成するか、または自動的に作成することができます。

デフォルトの vNIC の動作ポリシー

デフォルトの vNIC の動作ポリシーを設定し、vNIC の作成方法を定義できます。 次のいずれかになります。

- [None]：Cisco UCS Manager はサービス プロファイルのデフォルト vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。

- [HW Inherit]：サービス プロファイルに vNIC が必要であるときに、いずれも明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて、必要な vNIC を作成します。

（注） vNIC のデフォルトの動作ポリシーを指定しない場合は、デフォルトで [HW Inherit] が使用されます。

デフォルトの vHBA の動作ポリシー

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

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

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

デフォルトの vNIC の動作ポリシーの設定

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。
ルート組織内のデフォルトの vNIC の動作ポリシーのみを設定できます。 サブ組織内のデフォルトの vNIC の動作ポリシーは設定できません。

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

ステップ 5 [General] タブの [Properties] 領域で、[Action] フィールドにある次のいずれかのオプション ボタンをクリックします。

- [None]：Cisco UCS Manager はサービス プロファイルのデフォルト vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。
- [HW Inherit]：サービス プロファイルに vNIC が必要であるときに、いずれも明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて、必要な vNIC を作成します。

ステップ 6 [Save Changes] をクリックします。

LAN 接続ポリシーの設定

LAN および SAN の接続ポリシー

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

（注） これらのポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートにインクルードされ、複数のサーバの設定に使用できるため、接続ポリシーでスタティック ID を使用することは推奨されません。

LAN および SAN 接続ポリシーに必要な権限

接続ポリシーにより、ネットワーク権限またはストレージ権限のないユーザが、ネットワーク接続およびストレージ接続によってサービス プロファイルとサービス プロファイル テンプレートを作成および変更できるようになります。 ただし、接続ポリシーを作成するためには、ユーザは適切なネットワーク権限およびストレージ権限を持つ必要があります。

接続ポリシーの作成に必要な権限

接続ポリシーには、他のネットワーク設定およびストレージ設定と同じ権限が必要です。 たとえば、接続ポリシーを作成するには、少なくとも次のいずれかの権限が必要です。

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

接続ポリシーをサービス プロファイルに追加するのに必要な権限

接続ポリシーを作成した後、ls-compute 権限を持つユーザは、それら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 権限のみを持つユーザは、接続ポリシーを作成できません。

サービス プロファイルと接続ポリシー間の相互作用

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

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

Cisco UCS は、サービス プロファイル内で、接続ポリシーとローカル vNIC および vHBA 設定間の相互排他を維持します。 接続ポリシーとローカルに作成された vNIC または vHBA を組み合わせることはできません。 サービス プロファイルに LAN 接続ポリシーを含めると、すべての既存の vNIC 設定が消去され、SAN 接続ポリシーを含めると、そのサービス プロファイル内のすべての既存の vHBA 設定が消去されます。

LAN 接続ポリシーの作成

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] 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 [LAN Connectivity Policies] を右クリックし、[Create LAN Connectivity Policy] を選択します。

ステップ 5 [Create LAN Connectivity Policy] ダイアログボックスで、次のフィールドにポリシーの名前および説明を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

ステップ 6 次のいずれかを実行します。

- vNIC を LAN 接続ポリシーに追加するには、ステップ 7 に進みます。
- iSCSI vNIC を LAN 接続ポリシーに追加して、サーバで iSCSI ブートを使用するには、ステップ 8 に進みます。

ステップ 7 vNIC を追加するには、[vNIC Table] 領域でテーブル アイコン バーの [+] をクリックし、[Create vNIC] ダイアログボックスの次のフィールドに値を入力します。

a) 次のフィールドに値を入力して、vNIC の ID 情報を指定します。

名前	説明
[Name] フィールド	この vNIC のユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vNIC Template] チェックボックス	テンプレートを使用して vNIC を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vNIC Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vNIC テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vNIC Template] リンク	vNIC テンプレートを作成する場合は、このリンクをクリックします。

名前	説明
[MAC Address Assignment] ドロップダウン リスト	項目 • デフォルトの MAC アドレス プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた MAC アドレスを使用する場合は、[Hardware Default] を選択します。 • 特定の MAC アドレスを使用する場合は、[02:25: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。

b) ファブリック接続情報を指定するには、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC から第 2 のファブリック インターコネクトにアクセスできるようにする場合は、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックのフェールオーバーをイネーブルにしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のものにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバをこの vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。
[VLANs] テーブル	次の表には、この vNIC に関連付けることができる VLAN がリストされています。 各カラムの説明は次のとおりです。 • [Select]：使用する VLAN ごとに、このカラムのチェックボックスをオンにします。 • [Name]：VLAN の名前。 • [Native VLAN]：VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

名前	説明
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC にある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[Pin Group] ドロップダウン リスト	この vNIC と関連付ける LAN ピン グループを選択します。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト	この vNIC と関連付ける統計情報収集ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト	この vNIC と関連付けるイーサネット アダプタ ポリシー。
[Create Ethernet Adapter Policy] リンク	イーサネット アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC が関連付けられているダイナミック vNIC 接続ポリシー。
[Create Dynamic vNIC Connection Policy] リンク	ダイナミック vNIC 接続ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト	この vNIC と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	Quality Of Service ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Network Control Policy] ドロップダウン リスト	この vNIC と関連付けるネットワーク制御ポリシー。
[Create Network Control Policy Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。

d) [OK] をクリックします。

ステップ 8 サーバで iSCSI ブートを使用する場合は、下矢印をクリックして [Add iSCSI vNICs] バーを展開し、次の手順を実行します。

a) テーブル アイコン バーで、[+] をクリックします。

b) [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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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（ある場合）。
[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（ある場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC に使用可能な新しい iSCSI アダプタ ポリシーを作成するには、このリンクをクリックします。
[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（ある場合）。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 M82-8P 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 上のネイティブ 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、指定する VLAN はオーバーレイ vNIC に割り当てられたどの VLAN にすることもできます。

c) [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 アドレスは割り当てないまま、[Select (None used by default)] を選択してください。このサービス プロファイルに関連付けられるサーバに 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 M82-8P 仮想インターフェイス カード が含まれている場合、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るサーバに Cisco UCS NIC M51KR-B アダプタが含まれている場合、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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。

d) （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] ウィザードのフィールドに値を入力します。
詳細については、MAC プールの作成, （290 ページ）を参照してください。

e) [OK] をクリックします。

ステップ 9 ポリシーに必要なすべての vNIC または iSCSI vNIC を作成したら、[OK] をクリックします。

次の作業

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

LAN 接続ポリシーの vNIC の作成

手順

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

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

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

ステップ 4 vNIC を追加するポリシーを選択します。

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

ステップ 6 [vNICs] テーブルのアイコン バーで、[Add] をクリックします。

ステップ 7 [Create 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。

a) 次のフィールドに値を入力して、vNIC の ID 情報を指定します。

名前	説明
[Name] フィールド	この vNIC のユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vNIC Template] チェックボックス	テンプレートを使用して vNIC を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vNIC Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vNIC テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vNIC Template] リンク	vNIC テンプレートを作成する場合は、このリンクをクリックします。

名前	説明
[MAC Address Assignment] ドロップダウン リスト	項目 • デフォルトの MAC アドレス プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた MAC アドレスを使用する場合は、[Hardware Default] を選択します。 • 特定の MAC アドレスを使用する場合は、[02:25: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。

b) ファブリック接続情報を指定するには、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC から第 2 のファブリック インターコネクトにアクセスできるようにする場合は、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックのフェールオーバーをイネーブルにしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のものにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバをこの vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。
[VLANs] テーブル	次の表には、この vNIC に関連付けることができる VLAN がリストされています。 各カラムの説明は次のとおりです。 • [Select]：使用する VLAN ごとに、このカラムのチェックボックスをオンにします。 • [Name]：VLAN の名前。 • [Native VLAN]：VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

名前	説明
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC にある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[Pin Group] ドロップダウン リスト	この vNIC と関連付ける LAN ピン グループを選択します。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト	この vNIC と関連付ける統計情報収集ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト	この vNIC と関連付けるイーサネット アダプタ ポリシー。
[Create Ethernet Adapter Policy] リンク	イーサネット アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC が関連付けられているダイナミック vNIC 接続ポリシー。
[Create Dynamic vNIC Connection Policy] リンク	ダイナミック vNIC 接続ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト	この vNIC と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	Quality Of Service ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Network Control Policy] ドロップダウン リスト	この vNIC と関連付けるネットワーク制御ポリシー。
[Create Network Control Policy Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。

d) [OK] をクリックします。

ステップ 8 [OK] をクリックします。

ステップ 9 [Save Changes] をクリックします。

LAN 接続ポリシーからの vNIC の削除

手順

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

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

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

ステップ 4 vNIC を削除するポリシーを選択します。

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

ステップ 6 [vNIC] テーブルで、次の手順を実行します。

a) 削除する vNIC をクリックします。

b) アイコン バーで、[Delete] をクリックします。

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

ステップ 8 [Save Changes] をクリックします。

LAN 接続ポリシーの iSCSI vNIC の作成

手順

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

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

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

ステップ 4 iSCSI vNIC を追加するポリシーを選択します。

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

ステップ 6 [Add iSCSI vNICs] テーブルのアイコン バーで、[Add] をクリックします。

ステップ 7 [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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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（ある場合）。
[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（ある場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC に使用可能な新しい iSCSI アダプタ ポリシーを作成するには、このリンクをクリックします。
[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（ある場合）。 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 M82-8P 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 上のネイティブ 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、指定する VLAN はオーバーレイ vNIC に割り当てられたどの VLAN にすることもできます。

ステップ 8 [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 アドレスは割り当てないまま、[Select (None used by default)] を選択してください。 このサービス プロファイルに関連付けられるサーバに 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 M82-8P 仮想インターフェイス カード が含まれている場合、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るサーバに Cisco UCS NIC M51KR-B アダプタが含まれている場合、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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。

ステップ 9 （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] ウィザードのフィールドに値を入力します。
詳細については、MAC プールの作成, （290 ページ）を参照してください。

ステップ 10 [OK] をクリックします。

ステップ 11 [Save Changes] をクリックします。

LAN 接続ポリシーからの iSCSI vNIC の削除

手順

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

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

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

ステップ 4 iSCSI vNIC を削除するポリシーを選択します。

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

ステップ 6 [Add iSCSI vNICs] テーブルで、次の手順を実行します。

a) 削除する iSCSI vNIC をクリックします。

b) アイコン バーで、[Delete] をクリックします。

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

ステップ 8 [Save Changes] をクリックします。

LAN 接続ポリシーの削除

サービス プロファイルに含まれている LAN 接続ポリシーを削除すると、そのサービス プロファイルからすべての vNIC と iSCSI vNIC が削除され、サービス プロファイルに関連付けられたサーバに対する LAN データ トラフィックが中断されます。

手順

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

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

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

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

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

ネットワーク制御ポリシーの設定

ネットワーク制御ポリシー

このポリシーは、次を含めて Cisco UCS ドメインのネットワーク制御設定を行います。

- Cisco Discovery Protocol（CDP）がイネーブルか、ディセーブルか
- エンドホストモードで、使用できるアップリンク ポートが存在しない場合、VIF はどのように動作するか
- 関連付けられている境界ポートの障害時に、Cisco UCS Manager がリモート イーサネット インターフェイス、vEthernet インターフェイス、または vFibreChannel インターフェイスで実行するアクション
- ファブリック インターコネクトへのパケット送信時に複数の異なる MAC アドレスをサーバが使用できるかどうか
- MAC 登録が各 VNIC 単位またはすべての VLAN で発生するかどうか。

アップリンク障害時のアクション

デフォルトでは、ネットワーク制御ポリシーの [Action on Uplink Fail] プロパティは、リンクダウンの値で設定されます。 Cisco UCS M81KR 仮想インターフェイス カードなどのアダプタでは、関連する境界ポートが失敗した場合、このデフォルトの動作は、vEthernet または vFibreChannel インターフェイスをダウンするよう Cisco UCS Manager に指示します。 Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E など、イーサネットと FCoE トラフィックの両方をサポートする非 VM FEX 対応統合型ネットワーク アダプタを使用する Cisco UCS システムでは、関連する境界ポートが失敗した場合、このデフォルトの動作は、リモートイーサネットインターフェイスをダウンするよう Cisco UCS Manager に指示します。 このシナリオでは、リモート イーサネット インターフェイスにバインドされた vFibreChannel インターフェイスもダウンします。

（注） リリース 1.4(2) 以前の Cisco UCS Manager では、上記の非 VM FEX 対応統合型ネットワーク アダプタのタイプには [Action on Uplink Fail] プロパティが強制されませんでした。 [Action on Uplink Fail] プロパティがリンクダウンに設定された場合、Cisco UCS Manager はこの設定を無視し、代わりに警告を発行します。 現在のバージョンの Cisco UCS Manager では、この設定が強制的に適用されます。 したがって、いずれかの統合型ネットワーク アダプタが実装に含まれている場合で、アダプタでイーサネットと FCoE トラフィックの両方を処理することを想定している場合は、警告の値で [Action on Uplink Fail] プロパティを設定することを推奨します。

この設定では、境界ポートがダウンした場合に、イーサネット チーミング ドライバがリンク障害を検出できなくなる可能性があることに注意してください。

MAC 登録モード

リリース 1.4 以前の Cisco UCS Manager では、インターフェイスに属するすべての VLAN に MAC アドレスがインストールされていました。 リリース 2.0 以降では、MAC アドレスは、デフォルトでネイティブ VLAN にのみインストールされています。 ほとんどの実装では、これによって VLAN のポート数が最大化されます。

（注） トランキング ドライバがホストで実行され、インターフェイスが無差別モードの場合は、MAC 登録モードを [All VLANs] に設定することを推奨します。

ネットワーク制御ポリシーの作成

Emulex 統合型ネットワーク アダプタ（N20-AE0102）の MAC アドレス ベースのポート セキュリティはサポートされていません。 MAC アドレス ベースのポート セキュリティがイネーブルの場合、ファブリック インターコネクトは、最初に取得した MAC アドレスを含むパケットにトラフィックを制限します。 これは、FCoE 初期化プロトコル パケットで使用されているソース MAC アドレス、またはイーサネット パケットで使用されている MAC アドレスのうち、アダプタによって最初に送信されたほうになります。 この設定により、FCoE またはイーサネット パケットのいずれかがドロップされる可能性があります。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] 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 [Network Control Policies] ノードを右クリックし、[Create Network 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[CDP] フィールド	このオプションにより、このポリシーが含まれているサービスプロファイルと関連付けられたサーバ上で Cisco Discovery Protocol（CDP）をイネーブルにするかどうかが決定されます。次のいずれかになります。 • Disabled • Enabled
[MAC Register Mode] フィールド	アダプタ登録された MAC アドレスがインターフェイスに関連付けられたネイティブの VLAN にのみ追加されるか、インターフェイスに関連付けられたすべての VLAN に追加されるか。 次のいずれかになります。 • [Only Native Vlan]：MAC アドレスはネイティブの VLAN にのみ追加されます。 このオプションがデフォルトです。最大値はポート数と VLAN の数の合計です。 • [All Host Vlans]：MAC アドレスは関連付けられるすべての VLAN に追加されます。 VLAN がトランキングは使用するが、無差別モードで実行するようには設定されていない場合、このオプションを選択します。

名前	説明
[Action on Uplink Fail] フィールド	このオプションにより、ファブリック インターコネクトがエンドホスト モードのときに、使用可能なアップリンク ポートがないと、VIF がどのように動作するか決定されます。 次のいずれかになります。 • [Link Down]：ファブリック インターコネクト上でアップリンク接続が失われたときに vNIC の動作状態をダウンに変更します。vNIC のファブリック フェールオーバーはイネーブルになります。 • [Warning]：使用可能なアップリンク ポートがない場合であっても、サーバ間の接続を維持します。ファブリック インターコネクト上でアップリンク接続が失われた場合、ファブリック フェールオーバーはディセーブルになります。 デフォルトは [Link Down] です。 （注） リリース 1.4(2) 以前の Cisco UCS Manager では、上記の非 VM FEX 対応統合型ネットワーク アダプタのタイプには [Action on Uplink Fail] プロパティが強制されませんでした。 [Action on Uplink Fail] プロパティがリンクダウンに設定された場合、Cisco UCS Manager はこの設定を無視し、代わりに警告を発行します。 現在のバージョンの Cisco UCS Manager では、この設定が強制的に適用されます。 したがって、いずれかの統合型ネットワーク アダプタが実装に含まれている場合で、アダプタでイーサネットと FCoE トラフィックの両方を処理することを想定している場合は、警告の値で [Action on Uplink Fail] プロパティを設定することを推奨します。 この設定では、境界ポートがダウンした場合に、イーサネット チーミング ドライバがリンク障害を検出できなくなる可能性があることに注意してください。

ステップ 6 [MAC Security] 領域で次の手順を実行して、ファブリック インターコネクトへのパケット送信時に、サーバが異なる MAC アドレスを使用できるかどうかを決定します。

a) [Expand] アイコンをクリックして領域を展開し、オプション ボタンを表示します。

b) 次のオプション ボタンのいずれかをクリックして、サーバからファブリック インターコネクトへのパケット送信時に偽の MAC アドレスが使用できるか、拒否されるかを決定します。

- [Allow]：すべてのサーバ パケットは、そのパケットと関連付けられている MAC アドレスとは無関係に、ファブリック インターコネクトで受け入れられます。

- [Deny]：最初のパケットがファブリック インターコネクトに送信された後、それ以降のすべてのパケットでそれと同じMACアドレスを使用する必要があります。そうでないパケットは、ファブリック インターコネクトからメッセージなしで拒否されます。 実質的に、このオプションによって、関連するvNICのポートセキュリティがイネーブルになります。

関連付けられたサーバに VMware ESX をインストールする予定の場合は、デフォルトの vNIC に適用されるネットワーク制御ポリシーの [MAC Security] を [allow] に設定する必要があります。 [MAC Security] を [allow] に設定しない場合、ESX のインストールは失敗します。インストール プロセスでは複数の MAC アドレスが必要ですが、MAC セキュリティでは 1 つの MAC アドレスだけが許可されるためです。

ステップ 7 [OK] をクリックします。

ネットワーク制御ポリシーの削除

手順

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

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

ステップ 3 [Network 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

マルチキャスト ポリシーの設定

マルチキャスト ポリシー

このポリシーは、インターネット グループ管理プロトコル（IGMP）スヌーピングおよび IGMP クエリアを設定するために使用されます。 IGMP スヌーピングは、特定のマルチキャスト送信に含まれる必要がある VLAN のホストを動的に決定します。 1 つ以上の VLAN に関連付けることができるマルチキャストポリシーを作成、変更、および削除できます。 マルチキャストのポリシーが変更されると、そのマルチキャスト ポリシーに関連付けられたすべての VLAN が再処理されて、変更が適用されます。 デフォルトでは、IGMP スヌーピングがイネーブルになり、IGMP クエリアがディセーブルになります。 プライベート VLAN の場合、プライマリ VLAN に複数のポリシーを設定できますが、Cisco NX-OS の転送実装により、プライマリ VLAN に関連付けられている独立 VLAN には設定できません。

次の制限事項は、Cisco UCS 6100 シリーズ ファブリック インターコネクトおよび 6200 シリーズ ファブリック インターコネクトのマルチキャスト ポリシーに適用されます。

- Cisco UCS ドメインに 6100 シリーズ ファブリック インターコネクトだけが含まれている場合：
  - デフォルトのマルチキャスト ポリシーだけが、ローカル VLAN またはグローバル VLAN で許可されます。
- Cisco UCS ドメインに 1 つの 6100 シリーズ ファブリック インターコネクトと 1 つの 6200 シリーズ ファブリック インターコネクトが含まれている場合:
  - デフォルトのマルチキャスト ポリシーだけが、6100 シリーズ ファブリック インターコネクトのローカル VLAN で許可されます。
  - 6200 シリーズ ファブリック インターコネクトでは、ユーザ定義のマルチキャスト ポリシーをデフォルトのマルチキャスト ポリシーとともに割り当てることもできます。
  - デフォルトのマルチキャスト ポリシーだけがグローバル VLAN で許可されます（クラスタ内の 1 つの 6100 シリーズ ファブリック インターコネクトによって制限されているため）。
- Cisco UCS ドメインに 6200 シリーズ ファブリック インターコネクトだけが含まれている場合:
  - どのマルチキャスト ポリシーでも割り当てることができます。

マルチキャスト ポリシーの作成

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。

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

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

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

名前	説明
[IGMP Snooping State] フィールド	IGMP スヌーピングが、VLAN 内の IGMP プロトコル メッセージを調べて、マルチキャスト トラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているインターフェイスを検出するかどうか。 次のいずれかになります。 • [Enabled]：このポリシーに関連付けられた VLAN に IGMP スヌーピングが使用されます。 • [Disabled]：関連付けられた VLAN に IGMP スヌーピングは使用されません。
[IGMP Snooping Querier State] フィールド	IGMP スヌーピング クエリアが定期的に IGMP クエリーを送信し、IP マルチキャスト トラフィックを受信するホストから IGMP レポート メッセージを発信するかどうか。 次のいずれかになります。 • [Enabled]：定期的な IGMP クエリーが送信されます。 • [Disabled]：IGMP クエリーは送信されません。
[IGMP Snooping Querier IPv4 Address] フィールド	IGMP スヌーピング クエリアのインターフェイスの IPv4 アドレス。

ステップ 6 [OK] をクリックします。

マルチキャスト ポリシーの変更

この手順では、既存のマルチキャスト ポリシーの IGMP スヌーピング状態および IGMP スヌーピング クエリア状態を変更する方法について説明します。

（注） 作成されたマルチキャスト ポリシーの名前は変更できません。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。

ステップ 4 変更するポリシーをクリックします。

ステップ 5 [Work] ペインで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[IGMP Snooping State] フィールド	IGMP スヌーピングが、VLAN 内の IGMP プロトコル メッセージを調べて、マルチキャスト トラフィックの受信に関連のあるホストまたはその他のデバイスに接続されているインターフェイスを検出するかどうか。 次のいずれかになります。 • [Enabled]：このポリシーに関連付けられた VLAN に IGMP スヌーピングが使用されます。 • [Disabled]：関連付けられた VLAN に IGMP スヌーピングは使用されません。
[IGMP Snooping Querier State] フィールド	IGMP スヌーピング クエリアが定期的に IGMP クエリーを送信し、IP マルチキャスト トラフィックを受信するホストから IGMP レポート メッセージを発信するかどうか。 次のいずれかになります。 • [Enabled]：定期的な IGMP クエリーが送信されます。 • [Disabled]：IGMP クエリーは送信されません。
[IGMP Snooping Querier IPv4 Address] フィールド	IGMP スヌーピング クエリアのインターフェイスの IPv4 アドレス。

ステップ 6 [Save Changes] をクリックします。

マルチキャスト ポリシーの削除

（注） VLAN にデフォルト以外（ユーザ定義）のマルチキャスト ポリシーを割り当てた場合で、そのマルチキャスト ポリシーを削除する場合、関連付けられた VLAN は、削除されたポリシーが再作成されるまで、デフォルトのマルチキャスト ポリシーからのマルチキャスト ポリシーの設定を継承します。

手順

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

ステップ 2 [LAN] タブで、[LAN] > [Policies] を展開します。

ステップ 3 [root] ノードを展開します。

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

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

第 22 章

アップストリーム分離レイヤ 2 ネットワークの設定

この章の内容は、次のとおりです。

- アップストリーム分離レイヤ 2 ネットワーク，345 ページ
- アップストリーム分離 L2 ネットワークの設定に関する注意事項，346 ページ
- アップストリーム分離 L2 ネットワークのピン接続に関する注意事項，348 ページ
- アップストリーム分離 L2 ネットワークの Cisco UCS の設定，349 ページ
- アップストリーム分離 L2 ネットワークに対する VLAN の作成，351 ページ
- VLAN へのポートおよびポート チャネルの割り当て，353 ページ
- VLAN からのポートおよびポート チャネルの削除，355 ページ
- VLAN に割り当てられたポートおよびポート チャネルの表示，356 ページ

アップストリーム分離レイヤ 2 ネットワーク

互いに接続されることはないものの、同じ Cisco UCS ドメイン内のサーバまたは仮想マシンからアクセスする必要があるイーサネット「クラウド」が 2 つ以上存在する場合は、アップストリーム分離レイヤ 2 ネットワーク（分離 L2 ネットワーク）が必要です。 たとえば、次のいずれかを必要とする場合は、分離 L2 ネットワークを設定します。

- パブリック ネットワークおよびバックアップ ネットワークにアクセスするサーバまたは仮想マシン
- マルチテナント システムでは、複数の顧客のサーバまたは仮想マシンが同じCisco UCS ドメイン内にあり、両方の顧客の L2 ネットワークにアクセスする必要があります。

（注） デフォルトでは、Cisco UCS のデータ トラフィックは、相互包含の原則で機能します。 すべての VLAN およびアップストリーム ネットワークのすべてのトラフィックは、すべてのアップリンク ポートおよびポート チャネルに沿って移動します。 アップストリーム分離レイヤ 2 ネットワークをサポートしていないリリースからアップグレードした場合は、適切なアップリンク インターフェイスを VLAN に割り当てる必要があります。割り当てない場合は、これらの VLAN のトラフィックが引き続きすべてのアップリンク ポートおよびポート チャネルに沿って流れます。

分離 L2 ネットワークの設定は、選択的排他の原則で機能します。 分離ネットワークの一部として指定された VLAN のトラフィックは、その VLAN に特別に割り当てられたアップリンク イーサネット ポートまたはポート チャネルに沿ってのみ移動でき、その他すべてのアップリンク ポートおよびポート チャネルから選択的に排除されます。 ただし、アップリンク イーサネット ポートまたはポート チャネルに特別に割り当てられていない VLAN のトラフィックは、分離 L2 ネットワークのトラフィックを伝送するアップリンク ポートまたはポート チャネルを含めて、すべてのアップリンク ポートまたはポート チャネルで引き続き移動できます。

Cisco UCS では、VLAN は、アップストリーム分離 L2 ネットワークを表します。 分離 L2 ネットワークのネットワーク トポロジを設計する場合は、VLAN をアップリンク インターフェイスに割り当てるのではなく、アップリンク インターフェイスを VLAN に割り当てる必要があります。

サポートされているアップストリーム分離 L2 ネットワークの最大数については、『Cisco UCS 6100 and 6200 Series Configuration Limits for Cisco UCS Manager, Release 2.0』を参照してください。

アップストリーム分離 L2 ネットワークの設定に関する注意事項

アップストリーム分離 L2 ネットワークの設定を計画する場合は、次のことを考慮してください。

イーサネット スイッチング モードは、エンドホスト モードである必要があります

エンドホスト モードに対してファブリック インターコネクトのイーサネット スイッチング モードが設定されている場合、Cisco UCS は分離 L2 ネットワークだけをサポートします。 ファブリック インターコネクトのイーサネット スイッチング モードがスイッチ モードの場合は、分離 L2 ネットワークに接続できません。

ハイ アベイラビリティのために、対称的な設定が推奨されます

Cisco UCS ドメインが 2 つのファブリック インターコネクトでハイ アベイラビリティ用に設定されている場合は、両方のファブリック インターコネクトを同じ VLAN のセットで設定することを推奨します。

VLAN 検証基準は、アップリンク イーサネット ポートとポート チャネルで同一です

アップリンク イーサネット ポートまたはアップリンク イーサネット ポート チャネルには、分離 L2 ネットワークで使用される VLAN を設定および割り当てる必要があります。 ポートまたはポート チャネルに VLAN が含まれていない場合は、Cisco UCS Manager は VLAN を無効と見なして次の処理を行います。

- サーバの [Status Details] 領域に、設定の警告が表示されます。
- ポートまたはポート チャネルの設定を無視し、その VLAN のすべてのトラフィックをドロップします。

（注） 検証基準は、アップリンク イーサネット ポートとアップリンク イーサネット ポート チャネルで同一です。 Cisco UCS Manager は、この 2 つの違いを区別しません。

重複する VLAN はサポートされません

Cisco UCS は、分離 L2 ネットワークで重複する VLAN をサポートしません。 各 VLAN が 1 つのアップストリーム分離 L2 ドメインだけに接続するようにする必要があります。

各 vNIC が通信できるのは 1 つの分離 L2 ネットワークだけです

vNIC は、1 つの分離 L2 ネットワークとのみ通信できます。 サーバが複数の分離 L2 ネットワークと通信する必要がある場合は、それらの各ネットワークで vNIC を設定する必要があります。

3 つ以上の分離 L2 ネットワークと通信するには、3 つ以上の vNIC をサポートする Cisco VIC アダプタが必要です。

アプライアンス ポートは、アップリンク イーサネット ポートまたはポート チャネルと同一の VLAN で設定する必要があります

分離 L2 ネットワークと通信するアプライアンス ポートでは、少なくとも 1 つのアップリンク イーサネット ポートまたはポート チャネルが同じネットワーク内にあり、アプライアンス ポートによって使用される VLAN と同じ VLAN に割り当てられていることを確認する必要があります。 Cisco UCS Manager がアプライアンス ポートのトラフィックを伝送するすべての VLAN を含むアップリンク イーサネット ポートまたはポート チャネルを識別できない場合は、アプライアンス ポートでピン接続障害が発生してダウンします。

たとえば、Cisco UCS ドメインには、ID が 500 で vlan500 という名前のグローバル VLAN が含まれています。 vlan500 は、アップリンク イーサネット ポート上でグローバル VLAN として作成されます。 ただし、Cisco UCS Manager は、この VLAN をアプライアンス ポートに伝播しません。 vlan500 でアプライアンス ポートを設定するには、そのアプライアンス ポートに対して ID が 500 で vlan500 という名前の別の VLAN を作成する必要があります。 この重複 VLAN は、Cisco UCS Manager GUI の [LAN] タブの [Appliances] ノード、または Cisco UCS Manager CLI の **eth-storage** スコープで作成できます。 VLAN の重複を確認するプロンプトが表示された場合は、重複を受け入れ、Cisco UCS Manager によってアプライアンス ポートに対して重複 VLAN を作成します。

デフォルトの VLAN 1 は、アップリンク イーサネット ポートまたはポート チャネルで明示的に設定できません

Cisco UCS Manager は、デフォルトの VLAN 1 をすべてのアップリンク ポートとポート チャネルに暗黙的に割り当てます。 他の VLAN を設定しない場合でも、Cisco UCS は、デフォルトの VLAN 1 を使用してすべてのアップリンク ポートおよびポート チャネルのデータ トラフィックを処理します。

（注） UCSCisco UCS ドメインで VLAN を設定した後、デフォルトの VLAN 1 は、すべてのアップリンク ポートとポート チャネルで暗黙的に維持されます。 デフォルトの VLAN 1 を明示的にアップリンク ポートまたはポート チャネルに割り当てることも、またアップリンク ポートまたはポート チャネルから削除することもできません。

デフォルトの VLAN 1 を特定のポートまたはポート チャネルに割り当てようとすると、Cisco UCS Manager で更新失敗エラーが発生します。

したがって、分離 L2 ネットワークに対して Cisco UCS ドメインを設定する場合は、そのサーバのすべてのデータ トラフィックがすべてのアップリンク イーサネット ポートおよびポート チャネルで伝送され、すべてのアップストリーム ネットワークに送信されるようにする場合を除いて、デフォルトの VLAN 1 で vNIC を設定しないでください。

アップストリーム分離 L2 ネットワークのピン接続に関する注意事項

アップストリーム分離 L2 ネットワークとの通信を行うには、ピン接続が適切に設定されていることを確認する必要があります。 ソフト ピン接続またはハード ピン接続ソフトを実装するかどうかに関係なく、VLAN メンバーシップの不一致は、1 つ以上の VLAN のトラフィックがドロップされる原因となります。

ソフト ピン接続

ソフト ピン接続は、Cisco UCS のデフォルトの動作です。 ソフト ピン接続を実装する場合は、LAN ピン グループを作成して vNIC のピン ターゲットを指定する必要はありません。 代わりに、Cisco UCS Manager は、VLAN メンバーシップ基準に従って、vNIC をアップリンク イーサネット ポートまたはポート チャネルにピン接続します。

ソフト ピン接続を使用すると、Cisco UCS Manager は、すべてのアップリンク イーサネット ポートおよびポート チャネルの VLAN メンバーシップに対して vNIC からのデータ トラフィックを検証します。 分離 L2 ネットワークを設定した場合は、vNIC 上のすべての VLAN に割り当てられるアップリンク イーサネット ポートまたはポート チャネルを Cisco UCS Manager によって検出できる必要があります。 アップリンク イーサネット ポートまたはポート チャネルが vNIC 上のすべての VLAN で設定されていない場合、Cisco UCS Manager によって次の処理が行われます。

- リンクをダウンします。
- vNIC 上のすべての VLAN のトラフィックをドロップします。
- 次の障害を発行します。
  - Link Down
  - VIF Down

Cisco UCS Manager は、VLAN 設定に関する障害または警告を発行しません。

たとえば、サーバ上の vNIC は、VLAN 101、102、および 103 で設定されます。 インターフェイス 1/3 は、VLAN 102 だけに割り当てられます。 インターフェイス 1/1 および 1/2 は、VLAN に明

示的には割り当てられていません。これにより、VLAN 101 および 103 のトラフィックで利用可能になります。この設定の結果、Cisco UCS ドメインには、vNIC が設定される 3 つすべての VLAN のトラフィックを伝送できる境界ポートインターフェイスが含まれません。その結果、Cisco UCS Manager は、vNIC をダウンさせて vNIC 上の 3 つすべての VLAN のトラフィックをドロップし、Link Down および VIF Down 障害を発行します。

ハード ピン接続

ハード ピン接続は、LAN ピン グループを使用して、分離 L2 ネットワークに向けられたトラフィックのピン接続ターゲットを指定する場合に発生します。次に、ピン接続ターゲットであるアップリンク イーサネット ポートまたはポート チャネルを、適切な分離 L2 ネットワークと通信するように設定する必要があります。

ハード ピン接続により、Cisco UCS Manager は、すべてのアップリンク イーサネット ポートおよびポート チャネルに対して vNIC からのデータ トラフィックを検証し、LAN ピン グループ設定を検証して VLAN およびアップリンク イーサネット ポートまたはポート チャネルが含まれていることを確認します。いずれかの時点で検証に失敗した場合、Cisco UCS Manager は次の処理を行います。

- 警告の重大度によってピン接続 VLAN ミスマッチ障害を発行します。
- VLAN のトラフィックをドロップします。
- 他の VLAN のトラフィックがフローを継続できるように、リンクをダウンしません。

たとえば、VLAN 177 を使用するアップストリーム分離 L2 ネットワークのハード ピン接続を設定する場合は、次の作業を実行します。

- 分離 L2 ネットワークのトラフィックを伝送するアップリンク イーサネット ポートまたはポート チャネルで LAN ピン グループを作成します。
- VLAN 177 および LAN ピン グループで、サービス プロファイルに少なくとも 1 つの vNIC を設定します。
- VLAN 177 を LAN ピン グループに含まれているアップリンク イーサネット ポートまたはポート チャネルに割り当てます。

これら 3 つのいずれかの時点で設定が失敗した場合、Cisco UCS Manager は、VLAN 177 の VLAN ミスマッチに対して警告を生成し、その VLAN だけのトラフィックをドロップします。

アップストリーム分離 L2 ネットワークの Cisco UCS の設定

アップストリーム分離 L2 ネットワークに接続するように Cisco UCS ドメインを設定した場合は、次のすべての手順を完了する必要があります。

はじめる前に

この設定を開始する前に、ファブリック インターコネクトのポートが適切にケーブル接続され、分離 L2 ネットワーク設定をサポートしていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	両方のファブリック インターコネクトのイーサネット スイッチング モードをイーサネット エンドホスト モードに設定します。	Cisco UCS がアップストリーム分離 L2 ネットワークと通信できるようにするためには、イーサネット スイッチング モードをエンドホスト モードにする必要があります。 「イーサネット スイッチング モードの設定」を参照してください。
ステップ 2	分離 L2 ネットワークのトラフィックの伝送に必要なポートおよびポート チャネルを設定します。	ポートおよびポート チャネルの設定, （73 ページ）を参照してください。
ステップ 3	適切なアップリンク イーサネット ポートまたはポート チャネルのトラフィックをピン接続するために必要な LAN ピン グループを設定します。	（任意） LAN ピン グループの設定, （285 ページ）を参照してください。
ステップ 4	1 つ以上の VLAN を作成します。	これらは、ネームド VLAN またはプライベート VLAN です。 クラスタ設定について、VLAN Manager で Common/Global 設定を使用して VLAN を作成し、両方のファブリック インターコネクトにアクセス可能であることを確認するよう推奨します。 アップストリーム分離 L2 ネットワークに対する VLAN の作成, （351 ページ）を参照してください。
ステップ 5	目的のポートまたはポート チャネルを分離 L2 ネットワークの VLAN に割り当てます。	この手順が完了すると、これらの VLAN のトラフィックは、割り当てられたポートおよびポート チャネルまたはそのいずれかのトランクを介してのみ送信できます。 VLAN へのポートおよびポート チャネルの割り当て, （353 ページ）
ステップ 6	分離 L2 ネットワークと通信する必要があるすべてのサーバのサービス プロファイルに、vNIC が適切な VLAN にトラフィックを送信するための正しい LAN 接続設定が含まれていることを確認します。	この設定は、1 つ以上の vNIC テンプレートを介して、またはサービス プロファイルのネットワーク オプションを設定すると完了できます。 サービス プロファイルの設定, （575 ページ）を参照してください。

アップストリーム分離 L2 ネットワークに対する VLAN の作成

アップストリーム分離 L2 ネットワークに対して、VLAN Manager で VLAN を作成することを推奨します。

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 [LAN Uplinks Manager] で [VLANs] > [VLAN Manager] をクリックします。
任意のサブタブで VLAN を作成できます。 ただし、[All] サブタブを使用すると、設定済みのすべての VLAN がテーブルに表示されます。

ステップ 5 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[VLAN Name/Prefix] フィールド	単一の VLAN の場合、VLAN 名を指定します。 VLAN の範囲の場合、各 VLAN 名に使用される接頭辞を指定します。 VLAN 名の大文字と小文字は区別されます。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Multicast Policy] ドロップダウン リスト	この VLAN に関連付けられたマルチキャスト ポリシー。 ポリシーを選択しなかった場合、Cisco UCS Manager はデフォルトのマルチキャスト ポリシーの設定を使用します。
[Create Multicast Policy] リンク	すべての VLAN に使用可能な新しいマルチキャスト ポリシーを作成するには、このリンクをクリックします。

名前	説明
設定オプション	次のいずれかを選択できます。 • [Common/Global]：指定した VLAN は両方のファブリックに適用され、どちらのファブリックでも同じ設定パラメータが使用されます。 • [Fabric A]：指定した VLAN は、ファブリック A だけに適用されます。 • [Fabric B]：指定した VLAN は、ファブリック B だけに適用されます。 • [Both Fabrics Configured Differently]：指定した VLAN は、両方のファブリックに適用されますが、ファブリックごとに異なる VLAN ID を指定できます。 アップストリーム disjoint L2 ネットワークの場合、[Common/Global] を選択して、両方のファブリックに適用する VLAN を作成することをお勧めします。
[VLAN IDs] フィールド	1 つの VLAN を作成するには、単一の数値 ID を入力します。複数の VLAN を作成するには、個々の ID や ID の範囲をカンマで区切って入力します。 VLAN ID には次の値を入力できます。 • 1 ～ 3967 の範囲 • 4048 ～ 4093 の範囲 • システム上ですでに定義されている他の VLAN ID と重複する値 たとえば、ID が 4、22、40、41、42、および 43 の 6 つの VLAN を作成するには、4, 22, 40-43 を入力します。 **重要** 3968 から 4047 の ID を使用して VLAN を作成することはできません。 この範囲の VLAN ID は予約されています。 LAN クラウドの VLAN および SAN クラウドの FCoE VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

名前	説明
[Sharing Type] フィールド	この VLAN がプライベート VLAN またはセカンダリ VLAN に再分割されるかどうか。 次のいずれかになります。 • [None]：この VLAN には、セカンダリ VLAN またはプライベート VLAN がありません。 • [Primary]：[Secondary VLANs] 領域に示すように、この VLAN には 1 つ以上のセカンダリ VLAN が存在できます。 • [Isolated]：これはプライベート VLAN です。 プライマリ VLAN とこれが関連付けられた VLAN は、[Primary VLAN] ドロップダウン リストに表示されます。
[Primary VLAN] ドロップダウン リスト	[Sharing Type] フィールドが [Isolated] に設定されている場合、これはこのプライベート VLAN に関連付けられたプライマリ VLAN です。
VLAN の許容組織	VLAN に表示されるリストから組織を選択します。 この VLAN は、ここで選択する組織で使用できます。
[Check Overlap] ボタン	このボタンをクリックして、VLAN ID がシステム上の他の ID と重複していないかどうか確認します。

ステップ 7 さらに VLAN を作成するには、ステップ 6 および 7 を繰り返します。

次の作業

VLAN にポートおよびポート チャネルを割り当てます。

VLAN へのポートおよびポート チャネルの割り当て

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 [LAN Uplinks Manager] で [VLANs] > [VLAN Manager] をクリックします。

任意のサブタブで VLAN を作成できます。 ただし、[All] サブタブを使用すると、設定済みのすべての VLAN がテーブルに表示されます。

ステップ 5 次のいずれかのサブタブをクリックして、ファブリック インターコネクトのポートおよびポート チャネルを設定します。

サブタブ	説明
Fabric A	ファブリック インターコネクト A にアクセス可能なポート、ポート チャネル、および VLAN を表示します。
Fabric B	ファブリック インターコネクト B にアクセス可能なポート、ポート チャネル、および VLAN を表示します。

ステップ 6 [Ports and Port Channels] テーブルで、次の作業を実行します。

- アップリンク イーサネット ポート チャネルを VLAN に割り当てるには、[Port Channels] ノードを展開し、VLAN に割り当てるポート チャネルをクリックします。
- アップリンク イーサネット ポートを VLAN に割り当てるには、[Uplink Interfaces] ノードを展開し、VLAN に割り当てるポートをクリックします。

Ctrl キーを押しながら複数のポートまたはポート チャネルをクリックすることにより、それらを同じ VLAN または VLAN のセットに割り当てることができます。

ステップ 7 [VLAN] テーブルで、必要に応じて適切なノードを展開し、ポートまたはポート チャネルを割り当てる VLAN をクリックします。
複数の VLAN をポートまたはポート チャネルのセットに割り当てる場合は、Ctrl キーを押しながら複数の VLAN をクリックします。

ステップ 8 [Add to VLAN] ボタンをクリックします。

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

ステップ 10 追加のポートまたはポート チャネルを同じファブリックの VLAN に割り当てるには、ステップ 6、7 および 8 を繰り返します。

ステップ 11 追加のポートまたはポート チャネルを別のファブリックの VLAN に割り当てるには、ステップ 5 ～ 8 を繰り返します。
Cisco UCS ドメインがハイ アベイラビリティ用に 2 つのファブリック インターコネクトで設定されている場合は、両方のファブリック インターコネクトで同じ VLAN のセットを作成することを推奨します。

ステップ 12 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 13 VLAN Manager で作業を続行する場合は、[Apply] をクリックします。ウィンドウを閉じる場合は、[OK] をクリックします。
ポートまたはポート チャネルが 1 つ以上の VLAN に割り当てられると、他のすべての VLAN から削除されます。

VLAN からのポートおよびポート チャネルの削除

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 [LAN Uplinks Manager] で [VLANs] > [VLAN Manager] をクリックします。
任意のサブタブで VLAN を作成できます。 ただし、[All] サブタブを使用すると、設定済みのすべての VLAN がテーブルに表示されます。

ステップ 5 次のいずれかのサブタブをクリックして、ファブリック インターコネクトのポートおよびポート チャネルを設定します。

サブタブ	説明
Fabric A	ファブリック インターコネクト A にアクセス可能なポート、ポート チャネル、および VLAN を表示します。
Fabric B	ファブリック インターコネクト B にアクセス可能なポート、ポート チャネル、および VLAN を表示します。

ステップ 6 [VLAN] テーブルで、該当するノードを展開し、ポートまたはポート チャネルを削除する VLAN を展開します。

ステップ 7 VLAN から削除するポートまたはポート チャネルをクリックします。
Ctrl キーを押しながら複数のポートまたはポート チャネルをクリックします。

ステップ 8 [Remove from VLAN] ボタンをクリックします。

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

ステップ 10 VLAN Manager で作業を続行する場合は、[Apply] をクリックします。ウィンドウを閉じる場合は、[OK] をクリックします。

重要 すべてのポートまたはポートチャネルインターフェイスをVLANから削除すると、VLANはデフォルトの動作に戻り、その VLAN 上のデータ トラフィックはすべてのアップリンク ポートとポート チャネルにフローします。 Cisco UCS ドメインでの設定によって、このデフォルトの動作により、Cisco UCS Manager はその VLAN のトラフィックをドロップする場合があります。 これを回避するために、少なくとも 1 つのインターフェイスを VLAN に割り当てるか、VLAN を削除することをお勧めします。

VLAN に割り当てられたポートおよびポート チャネルの表示

手順

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

ステップ 2 [LAN] タブで、[LAN] ノードを展開します。

ステップ 3 [Work] ペインの [LAN Uplinks] タブで、[LAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [LAN Uplinks Manager] が開きます。

ステップ 4 [LAN Uplinks Manager] で [VLANs] > [VLAN Manager] をクリックします。
任意のサブタブで VLAN を作成できます。 ただし、[All] サブタブを使用すると、設定済みのすべての VLAN がテーブルに表示されます。

ステップ 5 次のいずれかのサブタブをクリックして、ファブリック インターコネクトのポートおよびポート チャネルを設定します。

サブタブ	説明
Fabric A	ファブリック インターコネクト A にアクセス可能なポート、ポート チャネル、および VLAN を表示します。
Fabric B	ファブリック インターコネクト B にアクセス可能なポート、ポート チャネル、および VLAN を表示します。

ステップ 6 [VLAN] テーブルで、該当するノードを展開し、割り当てられたポートまたはポート チャネルを表示する VLAN を展開します。

第 IV 部

ストレージ設定

- ネームド VSAN の設定，359 ページ
- SAN ピン グループの設定，371 ページ
- WWN プールの設定，373 ページ
- ストレージ関連ポリシーの設定，389 ページ
- ファイバ チャネル ゾーン分割の設定，415 ページ

第 23 章

ネームド VSAN の設定

この章の内容は、次のとおりです。

- ネームド VSAN，359 ページ
- ネームド VSAN のファイバ チャネル アップリンク トランキング，360 ページ
- VSAN に関する注意事項および推奨事項，360 ページ
- ネームド VSAN の作成，362 ページ
- ストレージ VSAN の作成，365 ページ
- VSAN の削除，368 ページ
- ストレージ VSAN 用の FCoE VLAN の VLAN ID の変更，368 ページ
- ファイバ チャネル アップリンク トランキングのイネーブル化，369 ページ
- ファイバ チャネル アップリンク トランキングのディセーブル化，370 ページ

ネームド VSAN

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

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

クラスタ設定のネームド VSAN

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

ネームド VSAN と FCoE VLAN ID

各ネームド VSAN を FCoE VLAN ID で設定する必要があります。 このプロパティは、VSAN およびそのファイバ チャネル パケットを転送するために使用される VLAN を決定します。

FIPS 対応の場合、Cisco UCS CNA M72KR-Q および Cisco UCS CNA M72KR-E などの統合型ネットワーク アダプタであるネームド VSAN は、FCoE VLAN ID のネイティブ VLAN ではないネームド VLAN で設定する必要があります。 この設定により、FCoE トラフィックがこれらのアダプタをパススルーできるようにします。

次の設定例では、ファブリック A にマップされる vNIC および vHBA を持つサービス プロファイルは、FIP 対応統合型ネットワーク アダプタを持つサーバに関連付けられます。

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

ネームド VSAN のファイバ チャネル アップリンク トランキング

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

VSAN に関する注意事項および推奨事項

次の注意事項と推奨事項が、ストレージ VSAN を含むすべてのネームド VSAN に適用されます。

VSAN 4079 は予約済み VSAN ID です。

VSAN を 4079 として設定しないでください。 この VSAN は予約済みであり、FC スイッチ モードまたは FC エンドホスト モードでは使用できません。

ID 4079 でネームド VSAN を作成すると、Cisco UCS Manager は、その VSAN をエラーとしてマークして障害を発行します。

FC スイッチ モードでのネームド VSAN の予約済み VSAN の範囲

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

ファブリック インターコネクトが FC スイッチ モードで動作するように設定されている場合、その範囲の VSAN は動作しません。 Cisco UCS Manager は、その VSAN をエラーとしてマークして障害を発行します。

FC エンドホスト モードでのネームド VSAN の予約済み VSAN の範囲

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

次の条件が Cisco UCS ドメインに存在する場合、その範囲の VSAN は動作しません。

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

これらの設定が存在する場合は、Cisco UCS Manager によって次の処理が行われます。

1. 3840 ～ 4079 の範囲の ID を持つすべての VSAN が動作不能になります。
2. 動作不能の VSAN に対してエラーを発行します。
3. すべての動作不能の VSAN をデフォルトの VSAN に転送します。
4. 動作不能の VSAN に関連付けられているすべての vHBA を、デフォルトの VSAN に転送します。

ファイバ チャネル トランキングをディセーブルにして既存の SAN ポート チャネルを削除すると、Cisco UCS Manager によって 3840 ～ 4078 の範囲のすべての VSAN が動作状態に戻され、関連付けられている vHBA がそれらの VSAN に復元されます。

FC スイッチ モードでのネームド VSAN ID の範囲の制限

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

FC スイッチ モードで動作するファブリック インターコネクトがアップストリーム スイッチとして MDS に接続されると、3040 ～ 4078 の範囲の Cisco UCS Manager で設定され、ポート VSAN として割り当てられた VSAN を MDS で作成できません。 この設定により、ポート VSAN の不一致が発生する場合があります。

FCoE VLAN ID に関する注意事項

（注） SAN クラウドの FCoE VLAN、および LAN クラウドの VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、FCoE VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

VLAN 4048 はユーザによる設定が可能です。 ただし、Cisco UCS Manager は次のデフォルト値に VLAN 4048 を使用します。 VLAN に 4048 を割り当てる場合は、これらの値を再設定する必要があります。

- Cisco UCS のリリース 2.0 にアップグレードした後：FCoE ストレージ ポートのネイティブ VLAN では、デフォルトで VLAN 4048 が使用されます。 アップグレード前にデフォルトの FCoE VSAN が VLAN 1 を使用するように設定されていた場合、使用または予約されていない VLAN ID にそれを変更する必要があります。 たとえば、VLAN ID が使用中でない場合、デフォルトを 4049 に変更することを検討してください。
- Cisco UCS のリリース 2.0 を新規インストールした後：デフォルトの VSAN の FCoE VLAN では、デフォルトで VLAN 4048 が使用されます。 FCoE ストレージ ポートのネイティブ VLAN は VLAN 4049 を使用します。

ネームド VSAN の作成

（注） SAN クラウドの FCoE VLAN、および LAN クラウドの VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、FCoE VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

手順

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

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

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+]アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[Name] フィールド	ネットワークに割り当てられている名前。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[FC Zoning] フィールド	Cisco UCS Manager が Cisco UCS ドメインのファイバ チャネル ゾーン分割を設定するかどうかを判断するには、オプション ボタンをクリックします。 次のいずれかになります。 • [Disabled]：アップストリーム スイッチによってファイバ チャネル ゾーン分割を処理するか、またはファイバ チャネル ゾーン分割は Cisco UCS ドメインに実装されません。Cisco UCS Manager は、ファイバ チャネル ゾーン分割を設定しません。 • [Enabled]：Cisco UCS ドメインのファイバ チャネル ゾーン分割は、Cisco UCS Manager によって設定および制御されます。 （注） Cisco UCS Manager を介してファイバ チャネル ゾーン分割をイネーブルにした場合は、ファイバ チャネル ゾーン分割に使用している VSAN でアップストリーム スイッチを設定しないでください。
[Type] オプション ボタン	オプション ボタンをクリックして、VSAN の設定方法を決定します。 次のいずれかになります。 • [Common/Global]：VSAN は、すべての使用可能なファブリック内で同じ VSAN ID にマッピングされます。 • [Fabric A]：VSAN は、ファブリック A にのみ存在する VSAN ID にマッピングされます。 • [Fabric B]：VSAN は、ファブリック B にのみ存在する VSAN ID にマッピングされます。 • [Both Fabrics Configured Differently]：VSAN は、使用可能なファブリックごとに異なる VSAN ID にマッピングされます。 このオプションを選択すると、Cisco UCS Manager GUI に、各ファブリックの [VSAN ID] フィールドと [FCoE VLAN] フィールドが表示されます。

名前	説明
[VSAN ID] フィールド	ネットワークに割り当てられている固有識別情報。 ID は、1 ～ 4078 または 4080 ～ 4093 の間に存在する可能性があります。 4079 は予約済みの VSAN ID です。 また、FC エンドホスト モードを使用する場合は、3840 ～ 4079 の範囲も VSAN ID の範囲として予約されています。
[FCoE VLAN] フィールド	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。 VLAN 4048 はユーザによる設定が可能です。 ただし、Cisco UCS Manager は次のデフォルト値に VLAN 4048 を使用します。 VLAN に 4048 を割り当てる場合は、これらの値を再設定する必要があります。 • Cisco UCS のリリース 2.0 にアップグレードした後：FCoE ストレージ ポートのネイティブ VLAN では、デフォルトで VLAN 4048 が使用されます。 アップグレード前にデフォルトの FCoE VSAN が VLAN 1 を使用するように設定されていた場合、使用または予約されていない VLAN ID にそれを変更する必要があります。 たとえば、VLAN ID が使用中でない場合、デフォルトを 4049 に変更することを検討してください。 • Cisco UCS のリリース 2.0 を新規インストールした後：デフォルトの VSAN の FCoE VLAN では、デフォルトで VLAN 4048 が使用されます。 FCoE ストレージポートのネイティブ VLAN は VLAN 4049 を使用します。 FIPS 対応の場合、Cisco UCS CNA M72KR-Q および Cisco UCS CNA M72KR-E などの統合型ネットワーク アダプタであるネームド VSAN は、FCoE VLAN ID のネイティブ VLAN ではないネームド VLAN で設定する必要があります。 この設定により、FCoE トラフィックがこれらのアダプタをパススルーできるようにします。

ステップ 6 [OK] をクリックします。

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

- 両方のファブリック インターコネクトにアクセス可能なストレージ VSAN の場合は、[SAN Cloud] > [VLANs] ノード。

- 1 つのファブリック インターコネクトだけにアクセス可能な VSAN の場合は、[SAN Cloud] > [*Fabric_Name*] > [VSANs] ノード。

ストレージ VSAN の作成

（注） SAN クラウドの FCoE VLAN、および LAN クラウドの VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、FCoE VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

手順

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

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

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

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[Name] フィールド	ネットワークに割り当てられている名前。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

名前	説明
[FC Zoning] フィールド	Cisco UCS Manager が Cisco UCS ドメインのファイバ チャネル ゾーン分割を設定するかどうかを判断するには、オプション ボタンをクリックします。 次のいずれかになります。 • [Disabled]：アップストリーム スイッチによってファイバ チャネル ゾーン分割を処理するか、またはファイバ チャネル ゾーン分割は Cisco UCS ドメインに実装されません。Cisco UCS Manager は、ファイバ チャネル ゾーン分割を設定しません。 • [Enabled]：Cisco UCS ドメインのファイバ チャネル ゾーン分割は、Cisco UCS Manager によって設定および制御されます。 （注） Cisco UCS Manager を介してファイバ チャネル ゾーン分割をイネーブルにした場合は、ファイバ チャネル ゾーン分割に使用している VSAN でアップストリーム スイッチを設定しないでください。
[Type] オプション ボタン	オプション ボタンをクリックして、VSAN の設定方法を決定します。 次のいずれかになります。 • [Common/Global]：VSAN は、すべての使用可能なファブリック内で同じ VSAN ID にマッピングされます。 • [Fabric A]：VSAN は、ファブリック A にのみ存在する VSAN ID にマッピングされます。 • [Fabric B]：VSAN は、ファブリック B にのみ存在する VSAN ID にマッピングされます。 • [Both Fabrics Configured Differently]：VSAN は、使用可能なファブリックごとに異なる VSAN ID にマッピングされます。 このオプションを選択すると、Cisco UCS Manager GUI に、各ファブリックの [VSAN ID] フィールドと [FCoE VLAN] フィールドが表示されます。
[VSAN ID] フィールド	ネットワークに割り当てられている固有識別情報。 ID は、1 ～ 4078 または 4080 ～ 4093 の間に存在する可能性があります。 4079 は予約済みの VSAN ID です。 また、FC エンドホスト モードを使用する場合は、3840 ～ 4079 の範囲も VSAN ID の範囲として予約されています。

名前	説明
[FCoE VLAN] フィールド	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。 VLAN 4048 はユーザによる設定が可能です。 ただし、Cisco UCS Manager は次のデフォルト値に VLAN 4048 を使用します。 VLAN に 4048 を割り当てる場合は、これらの値を再設定する必要があります。 • Cisco UCS のリリース 2.0 にアップグレードした後：FCoE ストレージ ポートのネイティブ VLAN では、デフォルトで VLAN 4048 が使用されます。 アップグレード前にデフォルトの FCoE VSAN が VLAN 1 を使用するように設定されていた場合、使用または予約されていない VLAN ID にそれを変更する必要があります。 たとえば、VLAN ID が使用中でない場合、デフォルトを 4049 に変更することを検討してください。 • Cisco UCS のリリース 2.0 を新規インストールした後：デフォルトの VSAN の FCoE VLAN では、デフォルトで VLAN 4048 が使用されます。 FCoE ストレージポートのネイティブ VLAN は VLAN 4049 を使用します。 FIPS 対応の場合、Cisco UCS CNA M72KR-Q および Cisco UCS CNA M72KR-E などの統合型ネットワーク アダプタであるネームド VSAN は、FCoE VLAN ID のネイティブ VLAN ではないネームド VLAN で設定する必要があります。 この設定により、FCoE トラフィックがこれらのアダプタをパススルーできるようにします。

ステップ 6 [OK] をクリックします。

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

- 両方のファブリック インターコネクトにアクセス可能なストレージ VSAN の場合は、[Storage Cloud] > [VSANs] ノード。
- 1 つのファブリック インターコネクトだけにアクセス可能な VSAN の場合は、[Storage Cloud] > [*Fabric_Name*] > [VSANs] ノード。

VSAN の削除

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

手順

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

ステップ 2 [SAN] タブで、[SAN] ノードをクリックします。

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

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

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

ステップ 5 テーブルで、削除する VSAN をクリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

ステップ 6 強調表示された 1 つまたは複数の VSAN を右クリックし、[Delete] を選択します。

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

ストレージ VSAN 用の FCoE VLAN の VLAN ID の変更

（注） SAN クラウドの FCoE VLAN、および LAN クラウドの VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、FCoE VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

手順

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

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

ステップ 3 FCoE VLAN ID を変更する VSAN を選択します。

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

ステップ 5 [FCoE VLAN] フィールドで、目的の VLAN ID を入力します。

ステップ 6 [Save Changes] をクリックします。

ファイバ チャネル アップリンク トランキングのイネーブル化

（注） ファブリック インターコネクトがファイバ チャネル エンドホスト モードに設定されている場合、ファイバ チャネル アップリンクのトランキングをイネーブルにすると、3840 から 4079 の ID を持つすべての VSAN が使用不能になります。

手順

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

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

ステップ 3 FC アップリンク トランキングをイネーブルにするファブリックのノードをクリックします。

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

ステップ 5 [Actions] 領域で、[Enable FC Uplink Trunking] をクリックします。

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

ファイバ チャネル アップリンク トランキングのディセーブル化

手順

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

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

ステップ 3 ファイバ チャネル アップリンク トランキングをディセーブルにするファブリックのノードをクリックします。

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

ステップ 5 [Actions] 領域で、[Disable FC Uplink Trunking] をクリックします。

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

第 24 章

SAN ピン グループの設定

この章の内容は、次のとおりです。

- SAN ピン グループ，371 ページ
- SAN ピン グループの作成，372 ページ
- SAN ピン グループの削除，372 ページ

SAN ピン グループ

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

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

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

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

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

SAN ピン グループの作成

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

手順

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

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

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

ステップ 4 ピン グループの一意の名前および説明を入力します。

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

a) [Fabric A] チェックボックスをオンにします。

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

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

a) [Fabric B] チェックボックスをオンにします。

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

ステップ 7 [OK] をクリックします。

次の作業

ピン グループは、vHBA テンプレートにインクルードします。

SAN ピン グループの削除

手順

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

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

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

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

第 25 章

WWN プールの設定

この章の内容は、次のとおりです。

- WWN プール，373 ページ
- WWNN プールの設定，374 ページ
- WWPN プールの設定，379 ページ
- WWxN プールの設定，384 ページ

WWN プール

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

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

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

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

WWN をブロック単位でプールに割り当てます。

WWNN プール

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

WWPN プール

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

WWxN プール

WWxN プールは、WW ノード名および WW ポート名の両方を含む WWN プールです。 ノードごとに WWxN プールで作成されるポート数を指定できます。 プール サイズは、ノードごとのポートに 1 を加えた数の倍数である必要があります。 たとえば、ノードごとに 7 個のポートを指定した場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 個のポートを指定した場合、プール サイズは、64 の倍数である必要があります。

WWNN プールの設定

WWNN プールの作成

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

名前	説明
[Name] フィールド	World Wide Node Name 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	プールの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Assignment Order] フィールド	次のいずれかになります。 • [Default]：Cisco UCS Manager はプールからランダム ID を選択します。 • [Sequential]：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。

ステップ 6 [Next] をクリックします。

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

ステップ 8 [Create WWN Block] ページで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 である必要があります。 たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 個のポートがある場合、プール サイズは 64 の倍数である必要があります。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックします。

次の作業

WWNN プールはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

WWNN プールへの WWN ブロックの追加

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 [WWNN Pools] ノードを展開します。

ステップ 4 World Wide Name（WWN; ワールド ワイド名）ブロックを追加する World Wide Node Name（WWNN; ワールド ワイド ノード名）プールを右クリックして、[Create WWN Block] を選択します。

ステップ 5 [Create WWN Block] ページで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 である必要があります。 たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 個のポートがある場合、プール サイズは 64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWNN プールからの WWN ブロックの削除

プールからアドレス ブロックを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられているブロック内のどのアドレスも再割り当てしません。 次のいずれかの条件が満たされる

まで、削除されたブロックからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

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

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

WWNN プールへの WWNN イニシエータの追加

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 [WWNN Pools] ノードを展開します。

ステップ 4 World Wide Node Name（WWNN; ワールド ワイド ノード名）イニシエータを追加する WWNN プールを右クリックして、[Create WWNN Initiator] を選択します。

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

名前	説明
[World Wide Name] フィールド	WWN。

名前	説明
[Name] フィールド	WWNN イニシエータの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	WWNN イニシエータのユーザ定義による説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

ステップ 6 [OK] をクリックします。

WWNN プールからの WWNN イニシエータの削除

手順

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

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

ステップ 3 [WWPN Pools] ノードを展開します。

ステップ 4 WWNN イニシエータを削除する WWNN プールを選択します。

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

ステップ 6 削除するイニシエータを右クリックし、[Delete] を選択します。

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

WWNN プールの削除

プールを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられたアドレスをプールから再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたプールからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

ステップ 3 [WWNN Pools] ノードを展開します。

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

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

WWPN プールの設定

WWPN プールの作成

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

名前	説明
[Name] フィールド	World Wide Port Name 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	プールの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Assignment Order] フィールド	次のいずれかになります。 • [Default]：Cisco UCS Manager はプールからランダム ID を選択します。 • [Sequential]：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。

ステップ 6 [Next] をクリックします。

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

ステップ 8 [Create WWN Block] ページで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 である必要があります。 たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 個のポートがある場合、プール サイズは 64 の倍数である必要があります。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックします。

次の作業

WWPN プールは、vHBA テンプレートにインクルードします。

WWPN プールへの WWN ブロックの追加

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 [WWPN Pools] ノードを展開します。

ステップ 4 World Wide Name（WWN; ワールド ワイド名）ブロックを追加する World Wide Port Name（WWPN; ワールド ワイド ポート名）プールを右クリックして、[Create WWN Block] を選択します。

ステップ 5 [Create WWN Block] ページで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 である必要があります。 たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 個のポートがある場合、プール サイズは 64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWPN プールからの WWN ブロックの削除

プールからアドレス ブロックを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられているブロック内のどのアドレスも再割り当てしません。 次のいずれかの条件が満たされる

まで、削除されたブロックからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

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

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

WWPN プールへの WWPN イニシエータの追加

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 [WWPN Pools] ノードを展開します。

ステップ 4 World Wide Port Name（WWPN; ワールド ワイド ポート名）イニシエータを追加する WWPN プールを右クリックして、[Create WWPN Initiator] を選択します。

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

名前	説明
[World Wide Name] フィールド	WWN。

名前	説明
[Name] フィールド	WWPN イニシエータの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	WWPN イニシエータのユーザ定義による説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

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

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

ステップ 7 [OK] をクリックします。

WWPN プールからの WWPN イニシエータの削除

手順

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

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

ステップ 3 [WWPN Pools] ノードを展開します。

ステップ 4 WWPN イニシエータを削除する WWPN プールを選択します。

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

ステップ 6 削除するイニシエータを右クリックし、[Delete] を選択します。

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

WWPN プールの削除

プールを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられたアドレスをプールから再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたプールからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

ステップ 3 [WWPN Pools] ノードを展開します。

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

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

WWxN プールの設定

WWxN プールの作成

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

名前	説明
[Name] フィールド	World Wide Port Name 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	プールの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Max Ports per Node] フィールド	このプールの各ノード名に割り当てることができるポートの最大数。 オブジェクトを保存した後にこの値を変更することはできません。
[Assignment Order] フィールド	次のいずれかになります。 • [Default]：Cisco UCS Manager はプールからランダム ID を選択します。 • [Sequential]：Cisco UCS Manager はプールから最も小さい使用可能 ID を選択します。

ステップ 6 [Next] をクリックします。

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

ステップ 8 [Create WWN Block] ページで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。

名前	説明
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 である必要があります。 たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 個のポートがある場合、プール サイズは 64 の倍数である必要があります。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックします。

次の作業

WWxN プールはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

WWxN プールへの WWN ブロックの追加

重要 WWN プールは、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF、または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内の WWNN または WWPN だけをインクルードできます。 その他の WWN 範囲はすべて予約されています。 SAN ファブリックで Cisco UCS WWNN と WWPN を確実に一意にするには、プールのすべてのブロックに 20:00:00:25:B5:XX:XX:XX の WWN プレフィックスを使用することをお勧めします。

手順

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

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

ステップ 3 [WWxN Pools] ノードを展開します。

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

ステップ 5 [Create WWN Block] ページで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。

名前	説明
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 である必要があります。 たとえば、ノードごとに 7 個のポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 個のポートがある場合、プール サイズは 64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWxN プールからの WWN ブロックの削除

プールからアドレス ブロックを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられているブロック内のどのアドレスも再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたブロックからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

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

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

WWxN プールの削除

プールを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられたアドレスをプールから再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたプールからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

ステップ 3 [WWxN Pools] ノードを展開します。

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

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

第 26 章

ストレージ関連ポリシーの設定

この章の内容は、次のとおりです。

- vHBA テンプレートの設定，389 ページ
- ファイバ チャネル アダプタ ポリシーの設定，393 ページ
- デフォルトの vHBA 動作ポリシーの設定，401 ページ
- SAN 接続ポリシーの設定，402 ページ

vHBA テンプレートの設定

vHBA テンプレート

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

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

vHBA テンプレートの作成

はじめる前に

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

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

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

名前	説明
[Name] フィールド	virtual Host Bus Adapter（vHBA; 仮想ホスト バス アダプタ）テンプレートの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	テンプレートのユーザ定義による説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Fabric ID] フィールド	このテンプレートで作成された vHBA が関連付けられているファブリック インターコネクトの名前。
[Select VSAN] ドロップダウンリスト	このテンプレートから作成された vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Template Type] フィールド	次のいずれかになります。 • [Initial Template]：テンプレートが変更されても、このテンプレートから作成された vHBA はアップデートされません。 • [Updating Template]：テンプレートが変更されると、このテンプレートから作成された vHBA がアップデートされます。

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

ステップ 6 [OK] をクリックします。

次の作業

vHBA テンプレートはサービス プロファイルにインクルードします。

vHBA テンプレートへの vHBA のバインディング

サービス プロファイルと関連付けられた vHBA を vHBA テンプレートにバインドすることができます。 vHBA を vHBA テンプレートにバインドした場合、Cisco UCS Manager は vHBA テンプレートで定義された値を使って vHBA を設定します。 既存の vHBA 設定が vHBA テンプレートと一致しない場合、Cisco UCS Manager によって vHBA が再設定されます。 バインドされた vHBA の設定は、関連付けられた vHBA テンプレートを使用してのみ変更できます。 vHBA をインクルードしているサービス プロファイルがすでにサービス プロファイル テンプレートにバインドされている場合、vHBA を vHBA テンプレートにバインドできません。

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

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

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

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

ステップ 5 テンプレートにバインドする vHBA をクリックします。

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

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

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

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

b) [OK] をクリックします。

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

vHBA テンプレートからの vHBA のバインド解除

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

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

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

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

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

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

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

vHBA テンプレートの削除

手順

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

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

ステップ 3 [vHBA Templates] ノードを展開します。

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

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

ファイバ チャネル アダプタ ポリシーの設定

イーサネットおよびファイバ チャネル アダプタ ポリシー

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

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

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

- ターゲットごとの最大 LUN：SANsurfer の最大 LUN は 256 であり、この数値を超える値は表示されません。 Cisco UCS Manager でサポートされている最大 LUN 数はこれよりも大きくなっています。
- リンク ダウン タイムアウト：SANsurfer では、リンク ダウンのタイムアウトしきい値を秒単位で設定します。 Cisco UCS Manager では、この値をミリ秒で設定します。 したがって、Cisco UCS Manager で 5500 ミリ秒と設定された値は、SANsurfer では 5 秒として表示されます。
- 最大データ フィールド サイズ：SANsurfer で許可される値は 512、1024、および 2048 です。 Cisco UCS Manager では、任意のサイズの値を設定できます。 したがって、Cisco UCS Manager で 900 と設定された値は、SANsurfer では 512 として表示されます。

オペレーティング システム固有のアダプタ ポリシー

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

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

ただし、（デフォルトの Windows のアダプタ ポリシーを使用する代わりに）Windows OS のイーサネット アダプタ ポリシーを作成する場合は、次の式を使用して Windows で動作する値を計算します。

完了キュー = 送信キュー + 受信キュー
割り込み回数 = (完了キュー + 2) 以上である 2 のべき乗の最小値

たとえば、送信キューが 1 で受信キューが 8 の場合、

完了キュー = 1 + 8 = 9
割り込み回数 = (9 + 2) 以上の 2 のべき乗の最小値 = 16

ファイバ チャネル アダプタ ポリシーの作成

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

手順

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

ステップ 2　[Servers] タブで、[Servers] > [Policies] 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　[Fibre Channel Policies] を右クリックし、[Create Fibre Channel Adapter Policy] を選択します。

ステップ 5　次のフィールドに、ポリシーの名前および説明を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

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

名前	説明
[Transmit Queues] フィールド	割り当てる送信キュー リソースの数。 この値は変更できません。

名前	説明
[Ring Size] フィールド	各送信キュー内の記述子の数。 このパラメータは、一般的なサービスの Extended Link Services（ELS）および Common Transport（CT）ファイバ チャネル フレームに適用されます。これは、アダプタのパフォーマンスには影響を及ぼしません。 64 ～ 128 の整数を入力します。 デフォルトは 64 です。
[Receive Queues] フィールド	割り当てる受信キュー リソースの数。 この値は変更できません。
[Ring Size] フィールド	各受信キュー内の記述子の数。 このパラメータは、一般的なサービスの Extended Link Services（ELS）および Common Transport（CT）ファイバ チャネル フレームに適用されます。これは、アダプタのパフォーマンスには影響を及ぼしません。 64 ～ 128 の整数を入力します。 デフォルトは 64 です。
[SCSI I/O Queues] フィールド	システムで割り当てる SCSI IO キュー リソースの数。 1 ～ 8 の整数を入力します。 デフォルトは 1 です。 （注） 現時点では、Cisco UCS M81KR 仮想インターフェイス カードのアダプタは、SCSI I/O キューを 1 つのみサポートします。
[Ring Size] フィールド	各 SCSI I/O キュー内の記述子の数。 64 ～ 512 の整数を入力します。 デフォルトは 512 です。 （注） 記述子数は、アダプタのパフォーマンスに影響を与えることがあるため、デフォルト値を変更しないことを推奨します。

ステップ 7 （任意） [Options] 領域で、次の値を調整します。

名前	説明
[FCP Error Recovery] フィールド	テープ デバイスを使用するシーケンス レベルのエラー検出に FCP Sequence Level Error Recovery（FC-TAPE）プロトコルを使用するかどうか。 これにより、VIC ファームウェアで Read Exchange Concise（REC）および Sequence Retransmission Request（SRR）機能が有効または無効になります。 次のいずれかになります。 • [Disabled]：これがデフォルトです。 • [Enabled]：システムが 1 つ以上のテープ ドライブ ライブラリに接続されている場合は、このオプションを選択する必要があります。 （注） このパラメータは、Cisco UCS M81KR 仮想インターフェイス カードなど、仮想インターフェイス カード（VIC）アダプタを持つサーバに対してのみ適用されます。
[Flogi Retries] フィールド	システムがファブリックへのログインを最初に失敗してから再試行する回数。 任意の整数を入力します。 システムが無限に試行し続けるように指定するには、infinite をこのフィールドに入力します。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは VIC アダプタ、または Cisco UCS M71KR-E Emulex 統合型ネットワーク アダプタなどの統合型ネットワーク アダプタを持つサーバに対してのみ適用されます。
[Flogi Timeout] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1000 ～ 255000 の整数を入力します。 デフォルトは 4,000 です。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは、VIC アダプタまたは統合ネットワーク アダプタを持つサーバにのみ適用されます。
[Plogi Retries] フィールド	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。 デフォルトは 8 です。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは、VIC アダプタを持つサーバにのみ適用されます。

名前	説明
[Plogi Timeout] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1000 ～ 255000 の整数を入力します。 デフォルトは 20,000 です。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは、VIC アダプタを持つサーバにのみ適用されます。
[Error Detect Timeout] フィールド	エラーが発生したと見なす前にシステムが待機するミリ秒数。 この値は変更できません。
[Port Down Timeout] フィールド	リモート ファイバ チャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。 このパラメータは、ホスト上のマルチパス ドライバにとって重要であり、エラー処理に使用される主要なインジケータの 1 つです。 0 ～ 240000 の整数を入力します。 デフォルトは 30,000 です。 ESX が稼働している VIC アダプタがあるサーバの推奨値は 10,000 です。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは、VIC アダプタを持つサーバにのみ適用されます。
[Port Down IO Retry] フィールド	ポートが使用不可能であるとシステムが判断する前に、そのポートへの IO 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。 デフォルトは 8 です。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは、Windows 上で稼働している VIC アダプタを持つサーバにのみ適用されます。
[Link Down Timeout] フィールド	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0 ～ 240000 の整数を入力します。 デフォルトは 30,000 です。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは、Windows 上で稼働している VIC アダプタを持つサーバにのみ適用されます。

名前	説明
[Resource Allocation Timeout] フィールド	リソースを適切に割り当てることができないと見なす前にシステムが待機するミリ秒数。 この値は変更できません。
[IO Throttle Count] フィールド	vHBA 内に同時に保留可能なデータまたは制御 I/O 操作の最大数。 この値を超えると、追加 I/O 操作は、保留中の I/O 操作数が減少し、追加操作を処理できるようになるまで、キューで待機します。 （注） このパラメータは、サーバにインストールされているオペレーティング システムに基づいて Cisco UCS Manager Manager によって制御される LUN のキュー項目数とは異なります。 1 ～ 1024 の整数を入力します。 デフォルトは 16 です。 このパラメータの最適値を得るために、ストレージアレイのマニュアルを参照することをお勧めします。 （注） このパラメータは、Cisco UCS M71KR-E Emulex 統合型ネットワーク アダプタまたは Cisco UCS M71KR-Q QLogic 統合型ネットワーク アダプタなどのネットワーク アダプタを持つサーバに対してのみ適用されます。VIC アダプタがあるサーバはこのパラメータを無視します。
[Max LUNs Per Target] フィールド	ファイバ チャネル ドライバがエクスポートまたは表示する LUN の最大数。 通常、LUN の最大数はサーバで実行されているオペレーティング システムによって制御されます。 1 ～ 1024 の整数を入力します。 デフォルト値は、256 です。 ESX または Linux を実行しているサーバについては、推奨値は 1024 です。 このパラメータの最適値を得るために、オペレーティング システムのマニュアルを参照することをお勧めします。 （注） このパラメータは、VIC アダプタまたはネットワーク アダプタを持つサーバにのみ適用されます。

名前	説明
[Interrupt Mode] フィールド	ドライバからオペレーティング システムへの割り込みを送信するために使用される方式です。 次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。サーバのオペレーティング システムがこのオプションをサポートする場合は、それを選択することを推奨します。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。 （注） このパラメータは、Windows 以外のオペレーティング システムを実行している VIC アダプタまたはネットワーク アダプタを持つサーバにのみ適用されます。Windows オペレーティング システムはこのパラメータを無視します。

ステップ 8 [OK] をクリックします。

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

ファイバ チャネル アダプタ ポリシーの削除

手順

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

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

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

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

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

デフォルトの vHBA 動作ポリシーの設定

デフォルトの vNIC および vHBA の動作ポリシー

デフォルトの vNIC および vHBA の動作ポリシーでは、サービス プロファイル用に vNIC および vHBA を作成する方法を設定できます。 vNICS および vHBA を選択して手動で作成するか、または自動的に作成することができます。

デフォルトの vNIC の動作ポリシー

デフォルトの vNIC の動作ポリシーを設定し、vNIC の作成方法を定義できます。 次のいずれかになります。

- [None]：Cisco UCS Manager はサービス プロファイルのデフォルト vNIC を作成しません。すべての vNIC を明示的に作成する必要があります。
- [HW Inherit]：サービス プロファイルに vNIC が必要であるときに、いずれも明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられたサーバにインストールされたアダプタに基づいて、必要な vNIC を作成します。

（注） vNIC のデフォルトの動作ポリシーを指定しない場合は、デフォルトで [HW Inherit] が使用されます。

デフォルトの vHBA の動作ポリシー

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

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

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

デフォルトの vHBA 動作ポリシーの設定

手順

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

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

ステップ 3 [root] ノードを展開します。
ルート組織内のデフォルトの vHBA の動作ポリシーのみを設定できます。 サブ組織内のデフォルトの vHBA の動作ポリシーは設定できません。

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

ステップ 5 [General] タブの [Properties] 領域で、[Action] フィールドにある次のいずれかのオプション ボタンをクリックします。

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

ステップ 6 [Save Changes] をクリックします。

SAN 接続ポリシーの設定

LAN および SAN の接続ポリシー

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

（注） これらのポリシーは、サービス プロファイルおよびサービス プロファイル テンプレートにインクルードされ、複数のサーバの設定に使用できるため、接続ポリシーでスタティック ID を使用することは推奨されません。

LAN および SAN 接続ポリシーに必要な権限

接続ポリシーにより、ネットワーク権限またはストレージ権限のないユーザが、ネットワーク接続およびストレージ接続によってサービス プロファイルとサービス プロファイル テンプレートを作成および変更できるようになります。 ただし、接続ポリシーを作成するためには、ユーザは適切なネットワーク権限およびストレージ権限を持つ必要があります。

接続ポリシーの作成に必要な権限

接続ポリシーには、他のネットワーク設定およびストレージ設定と同じ権限が必要です。 たとえば、接続ポリシーを作成するには、少なくとも次のいずれかの権限が必要です。

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

接続ポリシーをサービス プロファイルに追加するのに必要な権限

接続ポリシーを作成した後、ls-compute 権限を持つユーザは、それら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 権限のみを持つユーザは、接続ポリシーを作成できません。

サービス プロファイルと接続ポリシー間の相互作用

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

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

Cisco UCS は、サービス プロファイル内で、接続ポリシーとローカル vNIC および vHBA 設定間の相互排他を維持します。 接続ポリシーとローカルに作成された vNIC または vHBA を組み合わせることはできません。 サービス プロファイルに LAN 接続ポリシーを含めると、すべての既存の vNIC 設定が消去され、SAN 接続ポリシーを含めると、そのサービス プロファイル内のすべての既存の vHBA 設定が消去されます。

SAN 接続ポリシーの作成

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

ステップ 5 [Create SAN Connectivity Policy] ダイアログボックスで、次のフィールドにポリシーの名前および説明を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。 `（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）を除く文字やスペースを使用できます。

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

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

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

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

ステップ 7 [vHBAs] テーブルで、テーブル アイコン バーの [+] をクリックし、[Create vHBA] ダイアログボックスの次のフィールドに値を入力します。

a) 次のフィールドに値を入力して、vHBA の ID 情報を指定します。

名前	説明
[Name] フィールド	この vHBA 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vHBA Template] チェックボックス	テンプレートを使用して vHBA を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vHBA Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vHBA テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vHBA Template] リンク	vHBA テンプレートを作成する場合は、このリンクをクリックします。

名前	説明
[WWPN Assignment] ドロップダウン リスト	Cisco UCS が World Wide Port Node を vHBA に割り当てる方法。 Cisco UCS について、次のように設定します。 • デフォルトの WWPN プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた WWPN を使用する場合は、[Derived] を選択します。 • 特定の WWPN を使用する場合は、[20:00:00:25:B5:00:00:00]、[20:XX:XX:XX:XX:XX:XX:XX]、または [5X:XX:XX:XX:XX:XX:XX:XX] を選択し、使用する WWPN を [WWPN] フィールドに入力します。 WWPN が Cisco MDS ファイバ チャネル スイッチと互換性を持つようにするには、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • プール内の WWPN 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アドレスの数であり、2 番めの数字はそのプール内の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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[Create WWPN Pool] リンク	Cisco UCS ドメイン内のすべてのオブジェクトで使用可能な新しい WWPN プールを作成する場合は、このリンクをクリックします。
[WWPN] フィールド	[WWPN Assignment] ドロップダウン リストが手動テンプレートのいずれかに設定されている場合、手動で割り当てた WWPN。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN 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。

b) [VSAN] 領域で、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。
[Select VSAN] ドロップダウン リスト ボックス	この vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Pin Group] ドロップダウン リスト ボックス	この vHBA が関連付けられる SAN ピン グループ。
[Create SAN Pin Group] リンク	ピン グループを作成する場合は、このリンクをクリックします。
[Persistent Binding] フィールド	次のいずれかになります。 • Disabled • Enabled
[Max Data Field Size] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の範囲の整数を入力します。 デフォルトは 2048 です。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト ボックス	この vHBA と関連付ける統計しきい値ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト ボックス	この vHBA と関連付けるファイバ チャネル アダプタ ポリシー。
[Create Fibre Channel Adapter Policy] リンク	ファイバ チャネル アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト ボックス	この vHBA と関連付ける Quality Of Service ポリシー。

名前	説明
[Create QoS Policy] リンク	QoS ポリシーを作成する場合は、このリンクをクリックします。

d) [OK] をクリックします。

ステップ 8 ポリシーに必要なすべての vHBA を作成したら、[OK] をクリックします。

次の作業

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

SAN 接続ポリシーの vHBA の作成

手順

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

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

ステップ 3 vHBA を作成するポリシーを選択します。

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

ステップ 5 テーブル アイコン バーで、[+] ボタンをクリックします。

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

a) 次のフィールドに値を入力して、vHBA の ID 情報を指定します。

名前	説明
[Name] フィールド	この vHBA 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vHBA Template] チェックボックス	テンプレートを使用して vHBA を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vHBA Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vHBA テンプレートがシステムに存在する場合のみ、このオプションを選択できます。

名前	説明
[Create vHBA Template] リンク	vHBA テンプレートを作成する場合は、このリンクをクリックします。
[WWPN Assignment] ドロップダウン リスト	Cisco UCS が World Wide Port Node を vHBA に割り当てる方法。 Cisco UCS について、次のように設定します。 • デフォルトの WWPN プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた WWPN を使用する場合は、[Derived] を選択します。 • 特定の WWPN を使用する場合は、[20:00:00:25:B5:00:00:00]、[20:XX:XX:XX:XX:XX:XX:XX]、または [5X:XX:XX:XX:XX:XX:XX:XX] を選択し、使用する WWPN を [WWPN] フィールドに入力します。 WWPN が Cisco MDS ファイバ チャネル スイッチと互換性を持つようにするには、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • プール内の WWPN 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アドレスの数であり、2 番めの数字はそのプール内の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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[Create WWPN Pool] リンク	Cisco UCS ドメイン内のすべてのオブジェクトで使用可能な新しいWWPNプールを作成する場合は、このリンクをクリックします。

名前	説明
[WWPN] フィールド	[WWPN Assignment] ドロップダウン リストが手動テンプレートのいずれかに設定されている場合、手動で割り当てた WWPN。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN 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。

b) [VSAN] 領域で、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。
[Select VSAN] ドロップダウン リスト ボックス	この vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Pin Group] ドロップダウン リスト ボックス	この vHBA が関連付けられる SAN ピン グループ。
[Create SAN Pin Group] リンク	ピン グループを作成する場合は、このリンクをクリックします。
[Persistent Binding] フィールド	次のいずれかになります。 • Disabled • Enabled
[Max Data Field Size] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の範囲の整数を入力します。 デフォルトは 2048 です。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト ボックス	この vHBA と関連付ける統計しきい値ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト ボックス	この vHBA と関連付けるファイバ チャネル アダプタ ポリシー。
[Create Fibre Channel Adapter Policy] リンク	ファイバ チャネル アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト ボックス	この vHBA と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	QoS ポリシーを作成する場合は、このリンクをクリックします。

d) [OK] をクリックします。

ステップ 7 [Save Changes] をクリックします。

SAN 接続ポリシーからの vHBA の削除

手順

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

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

ステップ 3 vHBA を削除するポリシーを選択します。

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

ステップ 5 [vHBAs] テーブルで、次の手順を実行します。

a) 削除する vHBA をクリックします。

b) アイコン バーで、[Delete] をクリックします。

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

SAN 接続ポリシーのイニシエータ グループの作成

手順

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

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

ステップ 3 イニシエータ グループを作成するポリシーを選択します。

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

ステップ 5 テーブル アイコン バーで、[+] ボタンをクリックします。

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

名前	説明
[Name] フィールド	vHBA イニシエータ グループの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	グループの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Select vHBA Initiators] テーブル	使用する vHBA ごとに、[Select] カラムのチェックボックスをオンにします。

名前	説明
[Storage Connection Policy] ドロップダウン リスト	この vHBA イニシエータ グループに関連付けられたストレージ接続ポリシー。 • 既存のストレージ接続ポリシーを使用して、ドロップダウン リストからそのポリシーを選択します。 Cisco UCS Manager GUI には、[Global Storage Connection Policy] 領域のポリシーとその FC ターゲット エンドポイントの情報が表示されます。 グローバルに使用可能な新しいストレージ接続ポリシーを作成し、[Create Storage Connection Policy] リンクをクリックします。 • この vHBA 発信者グループにのみ使用できるローカル ストレージ接続ポリシーを作成し、[Specific Storage Connection Policy] オプションを選択します。 Cisco UCS Manager GUI には、ローカル ストレージ接続ポリシーを設定できる [Specific Storage Connection Policy] 領域が表示されます。
[Create Storage Connection Policy] リンク	すべてのサービス プロファイルとサービス プロファイル テンプレートに使用可能な新しいストレージ接続ポリシーを作成するには、このリンクをクリックします。

ステップ 7 [OK] をクリックします。

SAN 接続ポリシーからのイニシエータ グループの削除

手順

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

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

ステップ 3 イニシエータ グループから削除するポリシーを選択します。

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

ステップ 5 テーブルで、次の手順を実行します。

a) 削除するイニシエータ グループをクリックします。

b) アイコン バーで、[Delete] をクリックします。

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

SAN 接続ポリシーの削除

サービス プロファイルに含まれている SAN 接続ポリシーを削除すると、そのサービス プロファイルからすべての vHBA が削除され、サービス プロファイルに関連付けられたサーバに対する SAN データ トラフィックが中断されます。

手順

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

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

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

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

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

第 27 章

ファイバ チャネル ゾーン分割の設定

この章の内容は、次のとおりです。

- ファイバ チャネル ゾーン分割に関する情報，415 ページ
- Cisco UCS Manager でのファイバ チャネル ゾーン分割のサポート，416 ページ
- Cisco UCS Manager ベースのファイバ チャネル ゾーン分割に関する注意事項および推奨事項，419 ページ
- Cisco UCS でのファイバ チャネル ゾーン分割の設定，419 ページ
- ファイバ チャネル ゾーン分割のための VSAN の作成，421 ページ
- ファイバ チャネル ストレージ接続ポリシーの設定，424 ページ

ファイバ チャネル ゾーン分割に関する情報

ファイバ チャネル ゾーン分割では、ファイバ チャネル ファブリックを 1 つ以上のゾーンにパーティショニングできます。 各ゾーンは、VSAN で相互に通信できるファイバ チャネル イニシエータおよびファイバ チャネル ターゲットのセットを定義します。 また、ゾーン分割により、ホストとストレージ デバイスまたはユーザ グループ間のアクセス コントロールの設定も可能になります。

ゾーン分割によって提供されるアクセスとデータ トラフィック制御では、次の処理が行われます。

- SAN ネットワーク セキュリティを強化します
- データの損失や破損の防止に役立ちます
- パフォーマンスの問題を軽減します

ゾーンに関する情報

ゾーンは複数のゾーン メンバで構成されており、次の特性があります。

- ゾーンのメンバ同士はアクセスできますが、異なるゾーンのメンバ同士はアクセスできません。
- ゾーン分割がアクティブでない場合、すべてのデバイスがデフォルトゾーンのメンバとなります。
- ゾーン分割がアクティブの場合、アクティブ ゾーン（アクティブ ゾーン セットに含まれるゾーン）にないデバイスがデフォルト ゾーンのメンバとなります。
- ゾーンのサイズを変更できます。
- デバイスは複数のゾーンに所属できます。
- 物理ファブリックでは、最大 8,000 ゾーンを収容できます。

ゾーン セットに関する情報

各ゾーン セットは、1 つ以上のゾーンで構成されます。 ゾーンセットを使用して、ファイバチャネル ファブリック内でアクセス コントロールを強制的に適用できます。 また、ゾーン セットは次の利点を提供します。

- 常にアクティブにできるのは、1 つのゾーン セットだけです。
- ゾーンセットのすべてのゾーンは、ファブリックのすべてのスイッチで、単一エンティティとしてアクティブ化または非アクティブ化できます。
- 1 つのゾーンを複数のゾーン セットのメンバにできます。
- ゾーンのスイッチは、最大 500 ゾーン セットを持つことができます。

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

Cisco UCS Manager は、スイッチベースのファイバ チャネル ゾーン分割および Cisco UCS Manager ベースのファイバ チャネル ゾーン分割をサポートしています。 同じ Cisco UCS ドメイン でゾーン分割タイプの組み合わせを設定できません。 次のいずれかのタイプのゾーン分割で Cisco UCS ドメイン を設定できます。

- ゾーン分割なし
- Cisco UCS Manager ベースのファイバ チャネル ゾーン分割
- スイッチベースのファイバ チャネル ゾーン分割

（注） ゾーン分割は、VSAN 単位で設定されます。 ファブリック レベルでゾーン分割をイネーブルにすることはできません。

Cisco UCS Manager ベースのファイバ チャネル ゾーン分割

Cisco UCS Manager ベースのゾーン分割により、Cisco UCS Manager は、このタイプのゾーン分割で設定するすべての VSAN のゾーンの作成およびアクティブ化を含めて、Cisco UCS ドメインのファイバ チャネル ゾーン分割設定を制御します。

（注） VSAN が、アップストリーム スイッチ上で VSAN と通信するように設定されている場合は、Cisco UCS Manager ベースのゾーン分割を実装できません。

サポートされているファイバ チャネル ゾーン分割モード

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

- 単一のイニシエータと単一のターゲット：Cisco UCS Manager は、各 vHBA とストレージ ポートのペアに対して 1 つのゾーンを自動的に作成します。 各ゾーンには、2 つのメンバがあります。 ゾーン数がサポートされている最大数を超えると予想される場合を除いて、このようなタイプのゾーン分割を設定することを推奨します。
- 単一のイニシエータと複数のターゲット：Cisco UCS Manager は、各 vHBA に対して 1 つのゾーンを自動的に作成します。 ゾーン数がサポートされている最大数を超えると予想される場合は、このようなタイプのゾーン分割を設定することを推奨します。

サポートされるトポロジ

Cisco UCS Manager ベースのゾーン分割は、次のトポロジをサポートしています。

- Cisco UCS Manager ベースのゾーン分割との直接接続で、アップストリーム ファイバ チャネル スイッチなし。
- 直接接続ストレージに使用される VSAN がファイバ チャネル アップリンク ポートで設定されていない場合に限り、Cisco UCS Manager ベースのゾーン分割との直接接続、およびアップストリーム ファイバ チャネル スイッチへの接続。

vHBA イニシエータ グループ

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

vHBA イニシエータ グループ内の設定により、次の項目が決定されます。

- 通常 vHBA イニシエータと呼ばれ、イニシエータ グループに含まれる vHBA。
- 関連付けられた VSAN およびストレージ アレイ上のファイバ チャネル ターゲット ポートを含めて、ファイバ チャネル ストレージ接続ポリシー。

- グループに含まれる vHBA 用に設定される、ファイバ チャネル ゾーン分割のタイプ。

ファイバ チャネル ストレージ接続ポリシー

ファイバ チャネル ストレージ接続ポリシーには、Cisco UCS Manager ベースのファイバ チャネル ゾーン分割の設定に使用する、ストレージアレイ上のターゲットのストレージポートの集合が含まれます。 組織またはイニシエータ グループ下でこのポリシーを作成できます。

これらのゾーン内のストレージアレイは、ファブリック インターコネクトに直接接続する必要があります。 ファイバ チャネル ストレージ接続ポリシーに含めるこれらのアレイ上のターゲット ストレージ ポートは、ファイバ チャネル ストレージ ポートまたは FCoE のストレージ ポートにすることができます。 ポートの WWN を使用してそれをポリシーに追加し、ファイバ チャネル ゾーンのポートを識別します。

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

ファイバ チャネルのアクティブ ゾーン セットの設定

ファイバ チャネル ゾーン分割が有効になっている各 VSAN では、Cisco UCS Manager は、自動的に 1 つのゾーン セットと複数のゾーンを設定します。 ゾーン メンバーシップは、相互に通信可能なイニシエータおよびターゲットのセットを指定します。 Cisco UCS Manager は、ゾーン セットを自動的にアクティブにします。

Cisco UCS Manager は、ユーザ設定の vHBA イニシエータ グループおよびそれに関連付けられたファイバ チャネル ストレージ接続ポリシーを処理して、ファイバ チャネル イニシエータとターゲット間で必要な接続を判別します。 Cisco UCS Manager は、次の情報を使用してイニシエータとターゲット間のペアでのゾーン メンバーシップを構築します。

- vHBA イニシエータ グループから取得した vHBA イニシエータの WWN。
- ストレージ接続ポリシーから取得したストレージ アレイのポート WWN。

スイッチベースのファイバ チャネル ゾーン分割

スイッチベースのゾーン分割では、Cisco UCS ドメイン は、アップストリーム スイッチからゾーン分割設定を継承します。 Cisco UCS Manager で、ゾーン分割設定に関する情報を設定または表示することはできません。 その VSAN にスイッチベースのゾーン分割を使用するには、Cisco UCS Manager で VSAN のゾーン分割をディセーブルにする必要があります。

Cisco UCS Manager ベースのファイバ チャネル ゾーン分割に関する注意事項および推奨事項

ファイバチャネルゾーン分割の設定を計画するときは、次の注意事項と推奨事項を考慮してください。

ファイバ チャネル スイッチング モードは、Cisco UCS Manager 設定のスイッチ モードである必要があります

Cisco UCS Manager でファイバ チャネル ゾーン分割を処理する場合、ファブリック インターコネクトはファイバ チャネル スイッチ モードにする必要があります。 エンドホスト モードではファイバ チャネル ゾーン分割を設定できません。

ハイ アベイラビリティのために、対称的な設定が推奨されます

Cisco UCS ドメインが 2 つのファブリック インターコネクトでハイ アベイラビリティ用に設定されている場合は、両方のファブリック インターコネクトを同じ VSAN のセットで設定することを推奨します。

Cisco UCS でのファイバ チャネル ゾーン分割の設定

（注） この手順は、Cisco UCS Manager で制御されるファイバ チャネル ゾーン分割のために、Cisco UCS ドメインを設定するのに必要な手順の概要を示します。 次のすべてのステップを完了したことを確認する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	まだ実行していない場合は、MDS などの外部のファイバ チャネル スイッチから UCSCisco UCS ドメイン内のファブリック インターコネクトを接続解除します。	
ステップ 2	Cisco UCS ドメインが引き続き外部ファイバチャネルスイッチで管理されるゾーンを含む場合、各影響を受けるすべての VSAN に対して **clear-unmanaged-fc-zone-all** コマンドを実行して、それらのゾーンを削除します。	この機能は、現在、Cisco UCS Manager GUI では使用できません。 この手順は、Cisco UCS Manager CLI で実行する必要があります。
ステップ 3	ファイバ チャネル スイッチ モードの両方のファブリック インターコネクトに対	エンドホスト モードではファイバ チャネル ゾーン分割を設定できません。

	コマンドまたはアクション	目的
	して、ファイバ チャネル スイッチング モードを設定します。	ファイバ チャネル スイッチング モードの設定，（70 ページ）を参照してください。
ステップ 4	ファイバチャネルゾーンにトラフィックを伝送する必要があるファイバ チャネルおよび FCoE ストレージ ポートを設定します。	ポートおよびポート チャネルの設定，（73 ページ）を参照してください。
ステップ 5	1 つ以上の VSAN を作成し、ファイバ チャネル ゾーンにトラフィックを伝送する必要があるすべての VSAN に対して、ファイバチャネルゾーン分割をイネーブルにします。	クラスタ設定について、SAN Uplinks Manager で共通/グローバル設定を使用してファイバ チャネル ゾーンに含める VLAN を作成し、両方のファブリック インターコネクトにアクセス可能であることを確認するよう推奨します。 ファイバ チャネル ゾーン分割のための VSAN の作成，（421 ページ）を参照してください。
ステップ 6	1 つまたは複数のファイバ チャネル ストレージ接続ポリシーを作成します。	この手順は、サービス プロファイル内のファイバ チャネル ゾーン分割を設定する場合に適宜実行できます。 ファイバチャネルストレージ接続ポリシーの作成，（424 ページ）を参照してください。
ステップ 7	ファイバチャネルゾーンを介して通信する必要のあるサーバに関して、サービス プロファイルまたはサービス プロファイル テンプレートでゾーン分割を設定します。	この設定を完了するには、次の手順を実行します。 • VHBA に割り当てられた 1 つまたは複数の VSAN 上でゾーン分割をイネーブルにします。 • 1 つ以上の vHBA イニシエータのグループを設定します。 サービス プロファイルの設定，（575 ページ）を参照してください。

ファイバ チャネル ゾーン分割のための VSAN の作成

（注） SAN クラウドの FCoE VLAN、および LAN クラウドの VLAN には、異なる ID を割り当てる必要があります。 VLAN と VSAN の FCoE VLAN に同じ ID を使用すると、重大な障害が発生し、FCoE VLAN を使用するすべての vNIC とアップリンク ポートでトラフィックの中断が発生します。 イーサネット トラフィックは、FCoE VLAN ID と重複する ID を持つ VLAN でドロップされます

手順

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

ステップ 2 [SAN] タブで [SAN] ノードをクリックします。

ステップ 3 [Work] ペインで、[SAN Uplinks] タブの [SAN Uplinks Manager] リンクをクリックします。
別のウィンドウで [SAN Uplinks Manager] が開きます。

ステップ 4 [SAN Uplinks Manager] で [VSAN] タブをクリックします。
VSAN は、任意のサブタブ上に作成できます。 ただし、[All] サブタブを使用すると、設定されたすべての VSAN がテーブルに表示されます。

ステップ 5 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[Name] フィールド	ネットワークに割り当てられている名前。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

名前	説明
[FC Zoning] フィールド	Cisco UCS Manager が Cisco UCS ドメインのファイバ チャネル ゾーン分割を設定するかどうかを判断するには、オプション ボタンをクリックします。 次のいずれかになります。 • [Disabled]：アップストリーム スイッチによってファイバ チャネル ゾーン分割を処理するか、またはファイバ チャネル ゾーン分割は Cisco UCS ドメインに実装されません。 Cisco UCS Manager は、ファイバ チャネル ゾーン分割を設定しません。 • [Enabled]：Cisco UCS ドメインのファイバ チャネル ゾーン分割は、Cisco UCS Manager によって設定および制御されます。 （注） Cisco UCS Manager を介してファイバ チャネル ゾーン分割をイネーブルにした場合は、ファイバ チャネル ゾーン分割に使用している VSAN でアップストリーム スイッチを設定しないでください。
[Type] オプション ボタン	オプション ボタンをクリックして、VSAN の設定方法を決定します。 次のいずれかになります。 • [Common/Global]：VSAN は、すべての使用可能なファブリック内で同じ VSAN ID にマッピングされます。 • [Fabric A]：VSAN は、ファブリック A にのみ存在する VSAN ID にマッピングされます。 • [Fabric B]：VSAN は、ファブリック B にのみ存在する VSAN ID にマッピングされます。 • [Both Fabrics Configured Differently]：VSAN は、使用可能なファブリックごとに異なる VSAN ID にマッピングされます。 このオプションを選択すると、Cisco UCS Manager GUI に、各ファブリックの [VSAN ID] フィールドと [FCoE VLAN] フィールドが表示されます。
[VSAN ID] フィールド	ネットワークに割り当てられている固有識別情報。 ID は、1 ～ 4078 または 4080 ～ 4093 の間に存在する可能性があります。 4079 は予約済みの VSAN ID です。 また、FC エンドホスト モードを使用する場合は、3840 ～ 4079 の範囲も VSAN ID の範囲として予約されています。

名前	説明
[FCoE VLAN] フィールド	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。 VLAN 4048 はユーザによる設定が可能です。 ただし、Cisco UCS Manager は次のデフォルト値に VLAN 4048 を使用します。 VLAN に 4048 を割り当てる場合は、これらの値を再設定する必要があります。 • Cisco UCS のリリース 2.0 にアップグレードした後：FCoE ストレージ ポートのネイティブ VLAN では、デフォルトで VLAN 4048 が使用されます。 アップグレード前にデフォルトの FCoE VSAN が VLAN 1 を使用するように設定されていた場合、使用または予約されていない VLAN ID にそれを変更する必要があります。 たとえば、VLAN ID が使用中でない場合、デフォルトを 4049 に変更することを検討してください。 • Cisco UCS のリリース 2.0 を新規インストールした後：デフォルトの VSAN の FCoE VLAN では、デフォルトで VLAN 4048 が使用されます。 FCoE ストレージポートのネイティブ VLAN は VLAN 4049 を使用します。 FIPS 対応の場合、Cisco UCS CNA M72KR-Q および Cisco UCS CNA M72KR-E などの統合型ネットワーク アダプタであるネームド VSAN は、FCoE VLAN ID のネイティブ VLAN ではないネームド VLAN で設定する必要があります。 この設定により、FCoE トラフィックがこれらのアダプタをパススルーできるようにします。

ステップ 7 [OK] をクリックします。

ファイバ チャネル ストレージ接続ポリシーの設定

ファイバ チャネル ストレージ接続ポリシーの作成

手順

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

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

ステップ 3 ポリシーを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

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

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1～16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

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

- [None]：Cisco UCS Manager は、ファイバ チャネル ゾーン分割を設定しません。
- [Single Initiator Single Target]：Cisco UCS Manager は、各 vHBA とストレージ ポートのペアに対して 1 つのゾーンを自動的に作成します。 各ゾーンには、2 つのメンバがあります。 ゾーン数がサポートされている最大数を超えると予想される場合を除いて、このような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、各 vHBA に対して 1 つのゾーンを自動的に作成します。ゾーン数がサポートされている最大数を超えると予想される場合は、このようなタイプのゾーン分割を設定することを推奨します。

ステップ 7 [FC Target Endpoints] テーブルで、テーブルの右側にあるアイコン バーで [+] をクリックします。[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[WWPN] フィールド	ストレージ アレイに設定されている LUN にアクセスするためにサーバが使用するファイバ チャネルまたは FCoE ストレージ アレイ上の物理ターゲット ポートに割り当てられた WWPN（WWN）。
[Description] フィールド	ターゲット エンドポイントの説明。 ターゲット エンドポイントが接続するポート、LUN、またはストレージアレイに関する情報を入れることをお勧めします。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Path] フィールド	ターゲットエンドポイントとの通信に使用するファブリック インターコネクト。
[Select VSAN] ドロップダウン リスト	ターゲット エンドポイントとの通信に使用する VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。

ポリシーに関して、目的のすべてのターゲット エンドポイントを作成するまでこの手順を繰り返します。

ステップ 9 ポリシーに関する目的のすべてのターゲットエンドポイントを作成した後、[OK] をクリックします。

ファイバ チャネル ストレージ接続ポリシーの削除

手順

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

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

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

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

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

第 V 部

サーバの設定

- サーバ関連プールの設定，429 ページ
- 管理 IP アドレスの設定，439 ページ
- サーバ関連ポリシーの設定，447 ページ
- サーバのブート設定，517 ページ
- サービス プロファイルの更新の展開の延期，553 ページ
- サービス プロファイルの設定，575 ページ
- Cisco UCS での電源の管理，687 ページ

第 28 章

サーバ関連プールの設定

この章の内容は、次のとおりです。

- サーバ プールの設定，429 ページ
- UUID 接尾辞プールの設定，432 ページ
- IP プールの設定，434 ページ

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、同じ特性を持っています。 これらの特性は、シャーシ内の位置であったり、サーバ タイプ、メモリ容量、ローカル ストレージ、CPU のタイプ、ローカル ドライブ設定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

手順

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

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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。`（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）を除く文字やスペースを使用できます。

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

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバ プールへのサーバの追加

手順

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

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

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 キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

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 [Navigation] ペインの [Servers] タブをクリックします。

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

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 キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

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、競合を避けるため、その特定のプールを使用するサービス プロファイルに関連付けられたサーバごとに、これらの変数値が固有であることを保証します。

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、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 [Navigation] ペインの [Servers] タブをクリックします。

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [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 [Create UUID Suffix Pool] ウィザードの [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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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。`（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）を除く文字やスペースを使用できます。
[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 Cisco UCS Manager GUI にテキスト フィールドが表示され、そこに任意の接尾辞を *XXXXXXXX-XXXX-XXXX* の形式で入力できます。
[Assignment Order] フィールド	次のいずれかになります。 • [Default]：Cisco UCS Manager はプールからランダム ID を選択します。 • [Sequential]：Cisco UCS Manager はプールから最も小さい使用可能 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 UUID Suffix Pool] ウィザードの [Add UUID Blocks] ページで、[Add] をクリックします。

ステップ 8 [Create a Block of UUID Suffixes] ページで、次のフィールドに入力します。

名前	説明
[From] 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。

次の作業

UUID接尾辞プールはサービスプロファイルとテンプレートのうち一方、または両方にインクルードします。

UUID 接尾辞プールの削除

プールを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられたアドレスをプールから再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたプールからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

IP プールの設定

IP プール

IP プールは、デフォルトの目的がない IP アドレスの集合です。 Cisco UCS Manager で IP プールを作成して、次の作業を実行できます。

- デフォルトの iSCSI Boot IP プール [iscsi-initiator-pool] を置換します。 Cisco UCS Manager は、指定した IP プールに IP アドレスの各ブロックを予約しています。

- 関連付けられたサービス プロファイルがあるサーバのデフォルトの管理 IP プール [ext-mgmt] を交換します。 Cisco UCS Manager は、サーバ上の 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。 関連付けられたサービス プロファイルが存在しない場合、CIMC が IP アドレスを取得できるように [ext-mgmt] IP プールを使用する必要があります。
- 管理 IP アドレスと iSCSI ブート IP アドレスの両方を置換します。

（注） IP プールには、サーバまたはサービス プロファイルの静的 IP アドレスとして割り当てられているどの IP アドレスも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 [Navigation] ペインの [LAN] タブをクリックします。

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、次のフィールドを入力します。

名前	説明
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	IP アドレス 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。`（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）を除く文字やスペースを使用できます。

名前	説明
[Assignment Order] フィールド	次のいずれかになります。 • [Default]：Cisco UCS Manager はプールからランダム ID を選択します。 • [Sequential]：Cisco UCS Manager はプールから最も小さい使用可能 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 IP Blocks] ページで、[Add] をクリックします。

ステップ 7 [Create a Block of IP 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
[From] フィールド	ブロック内の最初の IP アドレス。
[Size] フィールド	プール内の IP アドレスの数。
[Subnet Mask] フィールド	ブロック内の IP 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 IP アドレスと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	このブロックの IP アドレスがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] フィールド	このブロックの IP アドレスがアクセスする必要のあるセカンダリ DNS サーバ。

ステップ 8 [OK] をクリックします。

ステップ 9 [Finish] をクリックして、ウィザードを終了します。

次の作業

IP プールはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

IP プールへのブロックの追加

手順

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

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] 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、[Create Block of IP Addresses] を選択します。

ステップ 5 [Create a Block of IP 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
[From] フィールド	ブロック内の最初の IP アドレス。
[Size] フィールド	プール内の IP アドレスの数。
[Subnet Mask] フィールド	ブロック内の IP 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 IP アドレスと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	このブロックの IP アドレスがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] フィールド	このブロックの IP アドレスがアクセスする必要のあるセカンダリ 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 [Navigation] ペインの [LAN] タブをクリックします。

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、[Delete] を選択します。

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

IP プールの削除

プールを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられたアドレスをプールから再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたプールからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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] 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。

（注） デフォルトのプール [ext-mgmt] と [iscsi-initiator-pool] は削除できません。

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

第 29 章

管理 IP アドレスの設定

この章の内容は、次のとおりです。

- 管理 IP アドレス，439 ページ
- ブレード サーバの管理 IP アドレスの設定，440 ページ
- ラック サーバの管理 IP アドレスの設定，441 ページ
- サービス プロファイルの管理 IP アドレスの設定，442 ページ
- サービス プロファイル テンプレートの管理 IP アドレスの設定，444 ページ
- 管理 IP プールの設定，444 ページ

管理 IP アドレス

Cisco UCS ドメイン内の各サーバには、Cisco Integrated Management Controller（CIMC）に割り当てられる管理IPアドレス、またはサーバに関連付けられたサービスプロファイルに割り当てられる管理 IP アドレスが必要です。 Cisco UCS Manager は、CIMC で終端する外部アクセス用にこの IP アドレスを使用します。 この外部アクセスは、次のいずれかが可能です。

- KVM コンソール
- Serial over LAN
- IPMI ツール

サーバ上の CIMC へのアクセスには、次のいずれかの管理 IP アドレスを使用できます。

- サーバに直接割り当てられたスタティック IPv4 アドレス。
- サービス プロファイルに割り当てられたスタティック IPv4 アドレス。 スタティック IP アドレスでは、サービス プロファイル テンプレートを設定できません。
- 管理 IP アドレスのプールから取り込まれ、サービス プロファイルまたはサービス プロファイル テンプレートに割り当てられた IP アドレス。

サーバ上の CIMC とサーバに関連付けられたサービス プロファイルに、管理 IP アドレスを割り当てることができます。 実行する場合、それぞれに異なる IP アドレスを使用する必要があります。

（注） スタティック IP アドレスが Cisco UCS ドメイン内のサーバまたはサービス プロファイルにすでに割り当てられている場合、サーバまたはサービス プロファイルにその IP アドレスを割り当てることはできません。 割り当てを試みると、Cisco UCS Manager は、その IP アドレスがすでに使用中であることを警告し、設定を拒否します。

サービス プロファイルに割り当てられた管理 IP アドレスは、サービス プロファイルとともに移動します。 別のサーバにサービス プロファイルを移行するときに KVM または SoL セッションがアクティブな場合、Cisco UCS Manager は、そのセッションを終了し、移行の完了後に再開しません。 サービス プロファイルを作成または変更するときに、この IP アドレスを設定します。

ブレード サーバの管理 IP アドレスの設定

スタティック IP アドレスを使用するブレード サーバの設定

このアクションがグレー表示されている場合、サーバにすでにスタティック IP アドレスが割り当てられています。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 IP アドレスを設定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 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Modify Static Management IP] をクリックします。

ステップ 7 [Modify Static Management IP] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
IP Address	サーバに割り当てられるスタティック IPv4 アドレス。
Subnet Mask	IP アドレスのサブネット マスク。
Default Gateway	IP アドレスで使用する必要のあるデフォルト ゲートウェイ。

ステップ 8 [OK] をクリックします。

管理 IP プールを使用するブレード サーバの設定

このアクションがグレー表示されている場合、サーバは、すでに管理 IP プールを使用するように設定されています。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 管理 IP プールを使用するように設定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 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Use Pooled Management IP] をクリックします。

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

ステップ 8 [OK] をクリックします。

ラック サーバの管理 IP アドレスの設定

スタティック IP アドレスを使用するラック サーバの設定

このアクションがグレー表示されている場合、サーバにすでにスタティック IP アドレスが割り当てられています。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 IP アドレスを設定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 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Modify Static Management IP] をクリックします。

ステップ 7 [Modify Static Management IP] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
IP Address	サーバに割り当てられるスタティック IPv4 アドレス。
Subnet Mask	IP アドレスのサブネット マスク。
Default Gateway	IP アドレスで使用する必要のあるデフォルト ゲートウェイ。

ステップ 8 [OK] をクリックします。

管理 IP プールを使用するラック サーバの設定

このアクションがグレー表示されている場合、サーバは、すでに管理 IP プールを使用するように設定されています。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 管理 IP プールを使用するように設定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 [CIMC] サブタブをクリックします。

ステップ 6 [Actions] 領域で、[Use Pooled Management IP] をクリックします。

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

ステップ 8 [OK] をクリックします。

サービス プロファイルの管理 IP アドレスの設定

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 管理 IP アドレスを設定するサービス 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 管理 IP アドレスを設定するサービス プロファイルをクリックします。

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

ステップ 6 [Actions] 領域で、[Change Management IP Address] をクリックします。

ステップ 7 [IChange Management IP Address] ダイアログボックスで、次のいずれかを選択します。

- [None]：管理 IP アドレスがサービス プロファイルを介してサーバに割り当てられていません。 管理 IP アドレスは、サーバ上で定義される CIMC 管理 IP アドレスに基づいています。
- [Static]：サービス プロファイルによって、スタティック管理 IP アドレスが関連付けられたサーバに割り当てられます。 サービスプロファイルを新しいサーバに移行すると、管理 IPv4 アドレスもサービス プロファイルとともに移動します。

  Cisco UCS Manager GUI には、スタティック IP アドレスを定義できる [Static IP Address] 領域が表示されます。
- *[IP-pool-name]*：サービス プロファイルは、選択した IP プールから関連付けられたサーバに管理 IP アドレスを割り当てます。

  [Create IP Pool] をクリックして、すべてのサービス プロファイルとサービス プロファイル テンプレートが使用できる IP アドレスのグローバル プールを作成します。

ステップ 8 [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
[IP Address] フィールド	サービスプロファイルを通してサーバに割り当てられた管理 IP アドレス。
[Subnet Mask] フィールド	管理 IP アドレスのサブネット マスク。
[Default Gateway] フィールド	管理 IP アドレスのデフォルト ゲートウェイ。

ステップ 9 [Save Changes] をクリックします。

サービス プロファイル テンプレートの管理 IP アドレスの設定

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profile Templates] を展開します。

ステップ 3 管理 IP アドレスを設定するサービス プロファイル テンプレート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 管理 IP アドレスを設定するサービス プロファイル テンプレートをクリックします。

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

ステップ 6 [Management IP Address] 領域を展開します。

ステップ 7 [Management IP Address Policy] 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。

- [None]：管理 IP アドレスがサービス プロファイルを介してサーバに割り当てられていません。 管理 IP アドレスは、サーバ上で定義される CIMC 管理 IP アドレスに基づいています。
- [Pooled]：サービス プロファイルによって、 [Pool Name] に示すプールからの管理 IP アドレスが関連付けられたサーバに割り当てられます。 サービス プロファイルを新しいサーバに移行すると、管理 IP アドレスもサービス プロファイルとともに移動します。

ステップ 8 [Save Changes] をクリックします。

管理 IP プールの設定

管理 IP プール

デフォルトの管理 IP プール [ext-mgmt] は、外部 IP アドレスの集合です。 Cisco UCS Manager サーバの CIMC で終端する外部アクセスのために、管理 IP プールに IP アドレスの各ブロックを予約しています。

管理 IP プールからの IP アドレスを使用するように、サービス プロファイルとサービス プロファイル テンプレートを設定できます。 管理 IP プールを使用するようにサーバを設定できません。

管理 IP プールのすべての IP アドレスが、ファブリック インターコネクトの IP アドレスと同じサブネット上にある必要があります。

（注） 管理 IP プールには、サーバまたはサービス プロファイルの静的 IP アドレスとして割り当てられているどの IP アドレスも含まれていてはなりません。

管理 IP プールでの IP アドレス ブロックの作成

管理 IP プールには、サーバまたはサービス プロファイルの静的 IP アドレスとして割り当てられているどの IP アドレスも含まれていてはなりません。

手順

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

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] ノードを展開します。

ステップ 4 [IP Pool ext-mgmt] を右クリックし、[Create Block of IP Addresses] を選択します。

ステップ 5 [Create a Block of IP 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
[From] フィールド	ブロック内の最初の IP アドレス。
[Size] フィールド	プール内の IP アドレスの数。
[Subnet Mask] フィールド	ブロック内の IP 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 IP アドレスと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	このブロックの IP アドレスがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] フィールド	このブロックの IP アドレスがアクセスする必要のあるセカンダリ DNS サーバ。

ステップ 6 [OK] をクリックします。

次の作業

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て、管理 IP プールから CIMC IP アドレスを取得します。

管理 IP プールからの IP アドレス ブロックの削除

手順

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

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] ノードを展開します。

ステップ 4 [IP Pool ext-mgmt] を選択します。

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、[Delete] を選択します。

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

第 30 章

サーバ関連ポリシーの設定

この章の内容は、次のとおりです。

- BIOS の設定，447 ページ
- IPMI アクセス プロファイルの設定，473 ページ
- ローカル ディスク設定ポリシーの設定，475 ページ
- スクラブ ポリシーの設定，484 ページ
- Serial over LAN ポリシーの設定，486 ページ
- サーバ自動構成ポリシーの設定，488 ページ
- サーバ ディスカバリ ポリシーの設定，490 ページ
- サーバ継承ポリシーの設定，492 ページ
- サーバ プール ポリシーの設定，494 ページ
- サーバ プール ポリシーの資格情報の設定，496 ページ
- vNIC/vHBA 配置ポリシーの設定，502 ページ

BIOS の設定

サーバ BIOS 設定

Cisco UCS には、Cisco UCS ドメイン内のサーバ上の BIOS 設定をグローバルに変更する 2 種類の方法が用意されています。 サーバまたはサーバ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 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 ポリシーとサーバ 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 によって管理されているサーバの BIOS 設定を微調整できます。

データセンターの要件によっては、一部のサービス プロファイルの 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 プロファイルで BIOS デフォルトを使用するか、それらのいずれかを使用することができます。 また、Cisco UCS Manager を使用して、サーバの実際の 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 設定の変更内容を BIOS ポリシーまたはデフォルト BIOS 設定を使用して Cisco Integrated Management Controller（CIMC）のバッファにプッシュします。 これらの変更は、サーバがリブートされるまでバッファに残り、有効になりません。

設定するサーバの 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 モードおよび予備モードなどの一部の設定は、すべての Cisco UCS Server ではサポートされているわけではありません。

主要な BIOS 設定

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できる主要なサーバ BIOS 設定を示します。

名前	説明
[Reboot on BIOS Settings Change]	1 つ以上の BIOS 設定を変更した後に、サーバがリブートされます。 この設定を有効にした場合、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がリブートされます。 たとえば、メンテナンス ポリシーで確認が必要な場合、サーバはリブートされず、ユーザ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。 この設定をイネーブルにしない限り、別のサーバ設定変更または手動リブートの結果としてサーバが次に再起動されるまで、BIOS の変更は適用されません。
[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]：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]：BIOS は、ロゴ画面を表示しますが、ブート中にメッセージまたはオプション ROM 情報を表示しません。 • [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
[Post Error Pause]	POST 中にサーバ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]：BIOS はサーバのブートを続行します。 • [enabled]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブートを一時停止し、Error Manager を開きます。 • [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。
[Resume Ac On 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がどのように動作するか。 次のいずれかになります。 • [stay-off]：手動で電源をオンにするまでサーバの電源がオフになります。 • [last-state]：サーバ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]：サーバの電源がオンになり、自動的にリセットされます。 • [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]：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、サーバに影響を与えるために使用できます。 • [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 からだけです。 • [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

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できるプロセッサ BIOS 設定を示します。

名前	説明
[Turbo Boost]	プロセッサで Intel Turbo Boost Technology 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]：プロセッサの周波数を自動的には上げません。 • [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]：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。
[Enhanced Intel Speedstep]	システムがプロセッサ電圧とコア周波数を調整できる Enhanced Intel SpeedStep Technology をプロセッサで使用するかどうか。 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]：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]：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]：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
[Hyper Threading]	プロセッサで Intel Hyper-Threading Technology 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]：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]：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]：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。
[Core Multi Processing]	パッケージ内の論理的なプロセッサ コアの状態を設定します。 この設定をディセーブルにした場合、Hyper Threading もディセーブルになります。 次のいずれかになります。 • [all]：すべての論理プロセッサ コアの多重処理をイネーブルにします。 • [1]~[10]：サーバで実行できる論理プロセッサ コアの数を指定します。 多重処理をディセーブルにして、サーバで実行される論理プロセッサ コアを 1 個のみにするには、[1] を選択します。 • [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
[Execute Disabled Bit]	サーバ上のメモリ領域を分類して、アプリケーションコードを実行できる場所を指定します。 この分類の結果、悪意のあるワームによってバッファへのコード挿入が試行された場合に、プロセッサはコードの実行をディセーブルにします。 この設定を使用すると、損傷、ワームの伝播、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できます。 次のいずれかになります。 • [disabled]：プロセッサはメモリ領域を分類しません。 • [enabled]：プロセッサはメモリ領域を分類します。 • [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。
[Virtualization Technology (VT)]	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]：プロセッサでの仮想化を禁止します。 • [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]：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） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。

名前	説明
[Direct Cache Access]	データを I/O デバイスからプロセッサ キャッシュに直接配置することによって、プロセッサで I/O パフォーマンスを向上させることができます。 この設定により、キャッシュ ミスが少なくなります。 次のいずれかになります。 • [disabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されません。 • [enabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されます。 • [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。
[Processor C State]	アイドル期間にシステムを省電力モードにすることができるかどうか。 次のいずれかになります。 • [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]：システムは、DIMM や CPU などのシステム コンポーネントに対する電力を削減できます。 • [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 状態に入ると、プロセッサは最小周波数に移行できます。 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]：CPU は C1 状態でも最大周波数で動作し続けます。 • [enabled]：CPU は最小周波数に移行します。 このオプションを使用すると、C1 状態で電力が最大限に節約されます。 • [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
[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。 • [disabled]：プロセッサから C3 レポートを送信しません。 • [acpi-c2]：ACPI C2 フォーマットを使用してプロセッサから C3 レポートを送信します。 • [acpi-c3]：ACPI C3 フォーマットを使用してプロセッサから C3 レポートを送信します。 • [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。 B440 サーバの場合、[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]：プロセッサから C6 レポートを送信しません。 • [enabled]：プロセッサから C6 レポートを送信します。 • [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。
[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。 • [disabled]：プロセッサから C7 レポートを送信しません。 • [enabled]：プロセッサから C7 レポートを送信します。 • [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
[CPU Performance]	サーバの 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。 • [enterprise]：すべてのプリフェッチャおよびデータ再利用はディセーブルです。 • [high-throughput]：すべてのプリフェッチャがイネーブルになり、データ再利用はディセーブルです。 • [hpc]：すべてのプリフェッチャおよびデータ再利用はイネーブルです。 この設定は、高パフォーマンス コンピューティングとも呼ばれます。 • [Platform Default]：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。
[Max Variable MTRR Setting]	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]：BIOS はプロセッサのデフォルト値を使用します。 • [8]：BIOS は MTRR 変数で指定した数を使用します。 • [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 Directed I/O BIOS 設定

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できる Intel Directed I/O BIOS 設定を示します。

名前	説明
[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]：プロセッサで仮想化テクノロジーを使用しません。 • [enabled]：プロセッサで仮想化テクノロジーを使用します。 • [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） このオプションは、他の Intel Directed I/O BIOS 設定を変更する場合は、イネーブルにする必要があります。
[Interrupt Remap]	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]：プロセッサでリマッピングをサポートしません。 • [enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。 • [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。
[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]：プロセッサでコヒーレンシをサポートしません。 • [enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。 • [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
[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]：プロセッサで ATS をサポートしません。 • [enabled]：プロセッサで VT-d ATS を必要に応じて使用します。 • [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。
[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]：プロセッサでパススルー DMA をサポートしません。 • [enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。 • [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。

RAS メモリ BIOS 設定

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できる RAS メモリ BIOS 設定を示します。

名前	説明
[Memory RAS Config]	サーバのメモリの信頼性、可用性、サービス性（RAS）を設定するかどうか。 次のいずれかになります。 • [maximum performance]：システムのパフォーマンスが最適化されます。 • [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。 • [lockstep]：サーバ内の 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イネーブルにして、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 サーバでは lockstep がデフォルトでイネーブルになっています。 • [sparing]：ある程度のメモリ冗長性によりシステムの信頼性が向上し、オペレーティングシステムで利用できるメモリがミラーリングよりも多くなります。 • [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。
[NUMA]	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]：BIOS で NUMA をサポートしません。 • [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]：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
[Mirroring Mode]	メモリのミラーリングでは、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、システムの信頼性が向上します。 このオプションは、[Memory RAS Config] で [mirroring] オプションを選択した場合のみ使用できます。 次のいずれかを指定できます。 • [inter-socket]：異なる CPU ソケットに含まれる 2 つの統合メモリ コントローラ（IMC）間でメモリがミラーリングされます。 • [intra-socket]：1 つの IMC が同じソケット内の別の IMC とミラーリングされます。 • [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。
[Sparing Mode]	スペアリングでは、他の DIMM で障害が発生した場合に使用できるように予約メモリに維持することにより、信頼性が最適化されます。 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のモードは、現在のメモリ配備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場合にのみ使用できます。 次のいずれかを指定できます。 • [dimm-sparing]：1 つの DIMM が予約で保持されます。 DIMM が失敗すると、失敗した DIMM の内容がスペア DIMM に転送されます。 • [rank-sparing]：DIMM の予備のランクが予約で保持されます。 DIMM のランクが失敗すると、失敗したランクの内容がスペア ランクに転送されます。 • [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 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。 • [power-saving-mode]：低電圧のメモリ動作が高周波数の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]：高周波数の動作が低電圧の動作よりも優先されます。 • [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。

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の BIOS 設定を介して実行できるシリアル ポート BIOS 設定を示します。

名前	説明
[Serial Port A]	シリアル ポート A をイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [disabled]：シリアル ポートはディセーブルになります。 • [enabled]：シリアル ポートはイネーブルになります。 • [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 の BIOS 設定

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できる USB の BIOS 設定を示します。

名前	説明
[Make Device Non Bootable]	サーバを 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]：サーバを USB デバイスからブートできます。 • [enabled]：サーバを USB デバイスからブートできません。 • [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 System Idle Power Optimizing Setting]	USB EHCI アイドル電力消費を減らすために [USB System Idle Power Optimizing Setting] を使用するかどうか。 この設定では、選択した値によって、パフォーマンスが影響を受ける場合があります。 次のいずれかになります。 • [high-performance]：最適なパフォーマンスが省電力より優先されるため、[USB System Idle Power Optimizing Setting] 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。 サイトにサーバ電源の制限がない場合は、このオプションを選択するよう推奨します。 • [lower-idle-power]：省電力が最適なパフォーマンスより優先するため、[USB System Idle Power Optimizing Setting] がイネーブルにされます。 • [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 Lock Access]	USB の前面パネルのロックが、USB ポートに前面パネルからアクセス可能または不可能に設定されます。 次のいずれかになります。 • disabled • enabled • [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 BIOS 設定

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できる PCI 設定 BIOS 設定を示します。

名前	説明
[Max Memory Below 4G]	システム設定に依存して、BIOS が PAE をサポートなしでオペレーティング システムの 4GB 未満のメモリ使用率を最大にするかどうか。 次のいずれかになります。 • [disabled]：メモリ使用率を最大にしません。 PAE サポートのあるすべてのオペレーティング システムでは、このオプションを選択します。 • [enabled]：PAE サポートのないオペレーティング システムで 4GB 未満のメモリ使用率を最大にします。 • [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。
[Memory Mapped IO Above 4Gb Config]	4 GB 以上のアドレス空間に対する 64 ビット PCI デバイスのメモリ マップ I/O をイネーブルにするか、ディセーブルにするか。 レガシー オプション ROM では、4 GB を超えるアドレスにアクセスできません。 64 ビットに対応し、レガシー オプション ROM を使用する PCI デバイスは、この設定がイネーブルの場合に正しく動作しないことがあります。 次のいずれかになります。 • [disabled]：64 ビット PCI デバイスの I/O を 4GB 以上のアドレス空間にマッピングしません。 • [enabled]：64 ビット PCI デバイスの I/O を 4GB 以上のアドレス空間にマッピングします。 • [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

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できるブート オプションの BIOS 設定を示します。

名前	説明
[Boot Option Retry]	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。 次のいずれかになります。 • [disabled]：NON-EFI ベースのブート オプションを再試行する前にユーザ入力を待機します。 • [enabled]：ユーザ入力を待機しないで NON-EFI ベースのブート オプションを持続的に試行します。 • [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 Entry SAS RAID]	Intel SA 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。 • [disabled]：Intel SAS Entry RAID モジュールはディセーブルです。 • [enabled]：Intel SA Entry RAID モジュールはイネーブルです。 • [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 Entry SAS RAID Module]	Intel SA 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]：RAID モジュールを Intel IT/IR RAID を使用するように設定します。 • [intel-esrtii]：RAID モジュールを Intel Embedded Server RAID Technology II を使用するように設定します。 • [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 SCU Storage Support]	オンボード ソフトウェア RAID コントローラがサーバで使用できるかどうか。 次のいずれかになります。 • [disabled]：ソフトウェア RAID コントローラは使用できません。 • [enabled]：ソフトウェア RAID コントローラを使用できます。 • [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。

サーバ管理 BIOS 設定

次の表に、BIOS ポリシーまたはデフォルトの BIOS 設定を介して実行できるサーバ管理 BIOS 設定を示します。

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 でマスク不能割り込み（NMI）を生成して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]：BIOS は SERR の発生時に NMI を生成せず、エラーを記録しません。 • [enabled]：BIOS は SERR の発生時に NMI を生成し、エラーをログに記録します。 [Assert NMI on PERR] をイネーブルにする場合は、この設定をイネーブルにする必要があります。 • [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 でマスク不能割り込み（NMI）を生成して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]：BIOS は PERR の発生時に NMI を生成せず、エラーを記録しません。 • [enabled]：BIOS は PERR の発生時に 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]：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]	BIOS で事前定義されたタイムアウト値を使用してウォッチドッグ タイマーをプログラミングするかどうか。 タイマーの期限が切れるまでにオペレーティング システムのブートが完了しない場合は、CIMC によってシステムがリセットされ、エラーがログに記録されます。 次のいずれかになります。 • [disabled]：サーバでブートにかかる時間を追跡するためにウォッチドッグ タイマーを使用しません。 • [enabled]：サーバでブートにかかる時間を追跡するためにウォッチドッグタイマーを使用します。 サーバが事前に定義した時間内にブートしない場合、CIMC はシステムをリセットし、エラーのログを記録します。 • [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。 この機能には、オペレーティング システムのサポートまたは Intel の管理ソフトウェアが必要です。

名前	説明
[OS Boot Watchdog Timer Timeout Policy]	ウォッチドッグタイマーの期限が切れた場合に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、サーバの電源がオフになります。 • [reset]：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、サーバはリセットされます。 • [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のみ使用できます。
[OS Boot Watchdog Timer Timeout]	BIOS でウォッチドッグ タイマーの設定に使用するタイムアウト値。 次のいずれかになります。 • [5-minutess]：ウォッチドッグ タイマーは、OS のブートが開始されてから 5 分後に期限が切れます。 • [10-minutes]：ウォッチドッグ タイマーは、OS のブートが開始されてから 10 分後に期限が切れます。 • [15-minutes]：ウォッチドッグ タイマーは、OS のブートが開始されてから 15 分後に期限が切れます。 • [20-minutes]：ウォッチドッグ タイマーは、OS のブートが開始されてから 20 分後に期限が切れます。 • [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のみ使用できます。

コンソール リダイレクションの設定

名前	説明
[Console Redirection]	POST 中および BIOS ブート中にコンソール リダイレクションでシリアル ポートを使用できます。 BIOS のブートが終了し、オペレーティング システムがサーバの役割を果たすと、コンソール リダイレクションは無関係になり、効果がなくなります。 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実行されません。 • [serial-port-a]：POST 中にシリアル ポート A をコンソール リダイレクション用にイネーブルにします。このオプションは、ブレードサーバとラックマウント サーバに対して有効です。 • [serial-port-b]：シリアル ポート B をコンソール リダイレクション用にイネーブルにし、サーバ管理タスクを実行可能にします。 このオプションは、ラックマウント サーバでのみ有効です。 • [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） このオプションをイネーブルにすると、POST 中に Quiet Boot ロゴ画面の表示がディセーブルになります。
[Flow Control]	ハンドシェイク プロトコルをフロー制御に使用するかどうか。 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]：フロー制御に RTS/CTS が使用されます。 • [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 アプリケーションの設定と一致している必要があります。

名前	説明
[Baud Rate]	シリアル ポートの送信速度に使用するボー レート。[Console Redirection] をディセーブルにした場合、このオプションは使用できません。 次のいずれかになります。 • [9600]：9600 ボー レートが使用されます。 • [19200]：19200 ボー レートが使用されます。 • [38400]：38400 ボー レートが使用されます。 • [57600]：57600 ボー レートが使用されます。 • [115200]：115200 ボー レートが使用されます。 • [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 アプリケーションの設定と一致している必要があります。
[Terminal Type]	コンソール リダイレクションに使用する文字形式のタイプ。 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-plus 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]：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 アプリケーションの設定と一致している必要があります。

名前	説明
[Legacy OS Redirect]	DOS などのレガシー オペレーティング システムからのリダイレクションをシリアルポートでイネーブルにするかどうか。 次のいずれかになります。 • [disabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されません。 • [enabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されます。 • [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 ポリシー

BIOS ポリシーは、サーバまたはサーバ 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だけ使用可能な 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 によってサーバ上の BIOS 設定が BIOS ポリシー内の設定と一致するように変更されます。 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、サーバの BIOS 設定にそのサーバ 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 によってサポートされている各タイプのサーバに対するデフォルトの BIOS 設定のセットが含まれています。 デフォルトの BIOS 設定は、ルート組織だけで使用可能であり、グローバルです。 Cisco UCS でサポートされている各サーバ プラットフォームには、一組の BIOS 設定だけを適用できます。 デフォルトの BIOS 設定を変更できますが、追加のデフォルトの BIOS 設定のセットは作成できません。

デフォルトの BIOS 設定の各セットは、サポートされている特定タイプのサーバ用に設計されており、BIOS ポリシーがサービス プロファイルに含まれていない、その特定のタイプのすべてのサーバに適用されます。

Cisco UCS の実装にサーバ固有の設定によって満たされない特定の要求がない場合、Cisco UCS ドメインの各タイプのサーバ用に設計されたデフォルトの BIOS 設定を使用することを推奨します。

Cisco UCS Manager により、これらのサーバ 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 ポリシーでは、特定の設定に対して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の 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に適用されます。 特定のサーバの BIOS 設定だけを変更する場合は、BIOS ポリシーを使用することを推奨します。

BIOS ポリシーの作成

（注） Cisco UCS Manager は、BIOS 設定の変更内容を BIOS ポリシーまたはデフォルト BIOS 設定を使用して Cisco Integrated Management Controller（CIMC）のバッファにプッシュします。 これらの変更は、サーバがリブートされるまでバッファに残り、有効になりません。

設定するサーバの 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 モードおよび予備モードなどの一部の設定は、すべての Cisco UCS Server では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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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、[Name] フィールド の 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

ステップ 6 [Create BIOS Policy] ウィザードで、次の手順を実行して BIOS 設定を行います。

a) BIOS 設定を変更する場合は、目的のオプション ボタンをクリックするか、ドロップダウン リストから適切な選択肢を選択します。
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： 主要な BIOS 設定, （448 ページ）
- [Processor] ページ： プロセッサの BIOS 設定, （450 ページ）
- [Intel Directed IO] ページ： Intel Directed I/O BIOS 設定, （455 ページ）
- [RAS Memory] ページ： RAS メモリ BIOS 設定, （457 ページ）
- [Serial Port] ページ: シリアル ポートの BIOS 設定, （460 ページ）
- [USB] ページ: USB の BIOS 設定, （460 ページ）
- [PCI Configuration] ページ: PCI 設定 BIOS 設定, （462 ページ）
- [Boot Options] ページ: ブート オプションの BIOS 設定, （462 ページ）
- [Server Management] ページ サーバ管理 BIOS 設定, （464 ページ）

b) 各ページの後で [Next] をクリックして移動します。

ステップ 7 ポリシーのすべての BIOS 設定が完了したら、[Finish] をクリックします。

BIOS のデフォルトの修正

設定するサーバの 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 モードおよび予備モードなどの一部の設定は、すべての Cisco UCS Server ではサポートされているわけではありません。

Cisco UCS の実装にサーバ固有の設定によって満たされない特定の要求がない場合、Cisco UCS ドメインの各タイプのサーバ用に設計されたデフォルトの BIOS 設定を使用することを推奨します。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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、デフォルトの BIOS 設定を変更するサーバ モデル番号を選択します。

ステップ 5 [Work] ペインで適切なタブをクリックし、目的のオプション 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。 サーバのタイプによっては、BIOS 設定が利用できない場合があります。

- [Main] タブ： 主要な BIOS 設定, （448 ページ）
- [Advanced] タブ：
  - [Processor] サブタブ: プロセッサの BIOS 設定, （450 ページ）
  - [Intel Directed IO] サブタブ： Intel Directed I/O BIOS 設定, （455 ページ）
  - [RAS Memory] サブタブ: RAS メモリ BIOS 設定, （457 ページ）
  - [Serial Port] サブタブ: シリアル ポートの BIOS 設定, （460 ページ）
  - [USB] サブタブ: USB の BIOS 設定, （460 ページ）
  - [PCI Configuration] サブタブ: PCI 設定 BIOS 設定, （462 ページ）
- [Boot Options] タブ: ブート オプションの BIOS 設定, （462 ページ）
- [Server Management] タブ： サーバ管理 BIOS 設定, （464 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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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、見出しの右側の [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含まれています。

IPMI アクセス プロファイルの設定

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、サーバでローカルに認証可能なユーザ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。

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

はじめる前に

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

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 Profiles] を右クリックし、[Create IPMI Profiles] を選択します。

ステップ 5 [Create IPMI 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) [OK] をクリックします。

ステップ 6 ナビゲータの [IPMI Profile Users] 領域で、[+] をクリックします。

ステップ 7 [User Properties] 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
[Name] フィールド	この IPMI プロファイルと関連付けるユーザ名。 1 ～ 16 の英数字を入力できます。@（アットマーク）、_（アンダースコア）、および -（ハイフン）も使用できます。 プロファイルを保存した後にこの名前を変更することはできません。
[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。 =（等号）、$（ドル記号）、および|（垂直バー）以外の 1 ～ 20 文字の標準 ASCII 文字を入力します。
[Confirm Password] フィールド	確認のためのパスワードの再入力。
[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

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。

次の作業

IPMI プロファイルはサービスプロファイルとテンプレートのうち一方、または両方にインクルードします。

IPMI アクセス プロファイルの削除

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ローカル ディスク設定ポリシーの設定

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 サーバまたは SAN 専用の設定で使用します。 このオプションを選択する場合、このポリシーを使用する任意のサービスプロファイルを、ローカルディスクを持つサーバに関連付けることができません。
- [RAID 0 Striped]：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] モードの適用後に違いがわからないことがあります。 これにより、ポリシー内の RAID 設定と、サーバの[Inventory] > [Storage] タブに表示される実際のディスク設定の間に不一致が生じる場合があります。

  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。
- [RAID10 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。

このポリシーはサービス プロファイルにインクルードする必要があります。また。このポリシーを有効にするには、サーバに関連付ける必要があります。

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

単一サーバまたは RAID 設定に HDD と SSD を含めないでください。

B200 M1 または M2 からのデフォルトのローカル ディスク設定ポリシーがあるサービス プロファイルを B200 M3 に割り当てないでください。

B200 M1 および M2 サーバのストレージ コントローラによって提供される RAID/JBOD サポートと、B200 M3 サーバのストレージ コントローラによって提供される RAID/JBOD サポートは異なるため、B200M1 または M2 サーバからのデフォルトの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 B200 M3 サーバに割り当てる、または再割り当てすることはできません。デフォルトのローカル ディスク設定ポリシーには、Any Configuration または JBOD 設定が含まれます。

リリース 1.3（1i）より前のリリースからのアップグレードによる影響

古い Cisco UCS ファームウェア リリースをリリース 1.3（1i）以降にアップグレードすると、アップグレード後にサーバが初めてサーバプロファイルに関連付けられるときに、ローカルディスク設定ポリシーの Protect Configuration プロパティに次の影響が生じます。

関連付けられていないサーバ

Cisco UCS ドメインをアップグレードすると、ローカルディスク設定ポリシーがサーバハードウェアと一致するかどうかに関係なく、初期サーバ アソシエーションは設定エラーを生じずに処理が進められます。 Protect Configuration プロパティをイネーブルにしていても、前のサービス プロファイルと新しいサービス プロファイルの間でローカル ディスク設定ポリシーの設定に不一致がある場合、Cisco UCS はサーバ上のユーザ データを保護しません。

（注） Protect Configuration プロパティをイネーブルにした場合、前のサービス プロファイルと新しいサービス プロファイルの間でローカル ディスク設定ポリシーに不一致があると、サーバに対する後続のサービス プロファイル アソシエーションはすべてブロックされます。

関連付けられたサーバ

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は、アップグレード後にリブートしません。 Cisco UCS Manager はローカル ディスクの設定ポリシーとサーバ ハードウェアが一致しない場合、設定エラーを報告しません。

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 Protect Configuration プロパティが優先され、前のサービス プロファイルの設定は上書きされます。

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

HDD と SSD を混合しない

単一の RAID 設定に HDD と SSD を含めないでください。

MegaRAID ストレージ コントローラを搭載したサーバ上で Any Configuration モードを使用しない

Cisco UCS ドメイン内のブレード サーバまたはラックマウント サーバに MegaRAID ストレージ コントローラが搭載されている場合は、そのサーバ用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 Any Configuration モードを設定しないでください。 MegaRAID ストレージ コントローラを搭載したサーバにこのモードを使用すると、オペレーティング システムのインストーラは、サーバ上のローカル ストレージを検出できなくなります。

MegaRAID ストレージ コントローラを搭載したサーバ上のローカル ストレージにオペレーティング システムをインストールする場合は、サーバ上で RAID LUN（RAID ボリューム）を作成するモードでローカル ディスク設定ポリシーを設定する必要があります。

サーバ プロファイルで Any Configuration モードが指定されている場合、RAID1 クラスタ移行後にサーバが起動しない

RAID1 クラスタの移行後、サービス プロファイルをサーバ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 RAID1 ではなく Any Configuration モードが設定されている場合は、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 サーバまたは統合されたラックマウント サーバに MegaRAID コントローラが搭載されている場合、そのサーバ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。

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。

MegaRAID ストレージ コントローラを搭載したサーバ上で 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 サーバまたは統合ラックマウント サーバ上で 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、これらのサーバで十分に機能することを意図していません。

統合されたラックマウント サーバ内の 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 と統合されているラックマウント サーバは、サーバ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 つしか設定できません。

統合されたラックマウント サーバ内のローカル 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、サードパーティ製のツールを使用して、ラックマウント サーバ上に複数の RAID LUN を作成しないでください。 Cisco UCS Manager は、その設定をサポートしていません。

ブレード サーバ内の 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 サーバは、サーバ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。 たとえば、B200 M3 に LSI コントローラと Intel Patsburg コントローラが搭載されていても、LSI コントローラだけが RAID コントローラして使用できます。

また、サードパーティ製のツールを使用して、ブレード サーバ上に複数の RAID LUN を作成しないでください。 Cisco UCS Manager は、その設定をサポートしていません。

ミラー RAID で選択されるディスクの数は 2 つまでにする

ミラー RAID で選択されたディスクの数が 2 つを超えると、RAID 1 は RAID 10 LUN として作成されます。 この問題は、Cisco UCS B440 M1 サーバと B440 M2 サーバで発生する可能性があります。

一部のサーバの特定の RAID 設定オプションに必要なライセンス

一部の Cisco UCS サーバでは、特定の RAID 設定オプションにライセンスが必要です。 Cisco UCS Manager がこのローカル ディスク ポリシーを含むサービス プロファイルをサーバに関連付けると、Cisco UCS Manager は、選択した RAID オプションに適切なライセンスが付与されていることを確認します。 問題がある場合は、サービス プロファイルの関連付け中に Cisco UCS Manager によって設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。

B420 M3 サーバはすべての設定モードをサポートしない

B420 M3 サーバは、ローカル ディスク設定ポリシーで次の設定モードをサポートしていません。

- No RAID

- RAID 6 Striped Dual Parity

また、B420 M3 は、JBOD モードまたは JBOD 操作をサポートしていません。

ローカル ディスク設定ポリシーの作成

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

名前	説明
[Mode] ドロップダウン リスト	

名前	説明
	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]：ディスクレス サーバまたは SAN 専用の設定で使用します。 このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカルディスクを持つサーバに関連付けることができません。 • [RAID 0 Striped]：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] モードの適用後に違いがわからないことがあります。 これにより、ポリシー内の RAID 設定と、サーバの[Inventory] > [Storage] タブに表示される実際のディスク設定の間に不一致が生じる場合があります。 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

名前	説明
	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。 • [RAID10 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。 （注） 一部の Cisco UCS サーバでは、特定の RAID 設定オプションにライセンスが必要です。 Cisco UCS Manager がこのローカル ディスク ポリシーを含むサービス プロファイルをサーバに関連付けると、Cisco UCS Manager は、選択した RAID オプションに適切なライセンスが付与されていることを確認します。 問題がある場合は、サービスプロファイルの関連付け中にCisco UCS Manager によって設定エラーが表示されます。 特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。
[Protect Configuration] チェックボックス	オンにすると、サーバは、サービスプロファイルとの関連付けが解除されても、ローカルディスク設定ポリシー内の設定を保持します。 **注意** サーバ内の 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 Protect Configuration プロパティが優先され、前のサービス プロファイルの設定は上書きされます。 （注） このオプションがイネーブルの状態でサーバとサービス プロファイルの関連付けを解除した後、そのサーバに新しいサービス プロファイルを関連付け、そのサービス プロファイル内のローカル ディスク設定ポリシーに前とは異なるプロパティが含まれていると、サーバから設定不一致のエラーが返され、関連付けは失敗します。

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方法について説明します。 [Servers] タブの [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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [Policies] 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 このポリシーを サービス プロファイル に割り当てます。
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	選択された 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使用しません。

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

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

スクラブ ポリシーの設定

スクラブ ポリシー

このポリシーは、ディスカバリ プロセス中にサーバのローカル データおよび BIOS 設定に何が起こるか、およびサーバとサービスプロファイルの関連付けはいつ解除されるかを決定します。 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。

- イネーブルの場合、ローカル ドライブ上のすべてのデータが破棄されます。
- ディセーブルの場合、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）。

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。

- イネーブルの場合、サーバのすべての BIOS 設定が消去され、そのサーバ タイプとベンダーに合わせた BIOS のデフォルトにリセットされます。
- ディセーブルの場合、サーバの既存の BIOS 設定が保持されます。

スクラブ ポリシーの作成

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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。

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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Disk Scrub] 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、サーバのローカル ドライブにあるすべてのデータが完全に消去されます。 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が維持されます。
[BIOS Settings Scrub] 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 BIOS 設定が消去され、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。 このフィールドを [No] に設定すると、BIOS 設定が維持されます。

ステップ 6 [OK] をクリックします。

スクラブ ポリシーの削除

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

Serial over LAN ポリシーの設定

Serial over LAN ポリシー

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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Serial over LAN State] フィールド	次のいずれかになります。 • [Disable]：Serial over LAN アクセスがブロックされます。 • [Enable]：Serial over LAN アクセスが許可されます。
[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 [Navigation] ペインの [Servers] タブをクリックします。

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバ自動構成ポリシーの設定

サーバ自動構成ポリシー

Cisco UCS Manager このポリシーを使用して、新しいサーバの設定方法を決定します。 サーバ自動構成ポリシーを作成すると、新しいサーバの起動時に次の処理が行われます。

1. サーバに対してサーバ自動構成ポリシーの資格認定が実行されます。
2. サーバが必要な資格を満たす場合、サーバは、サーバ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 プロファイルに関連付けられます。 そのサービス プロファイルの名前は、Cisco UCS Manager によってサーバに指定された名前に基づきます。
3. サービス プロファイルは、サーバ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

はじめる前に

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ト機能が実装されている場合）

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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

ステップ 6 [Create 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Qualification] 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サーバプール ポリシー資格。 サーバプール ポリシー資格に指定されている条件と一致する新しいサーバが検出されると、Cisco UCS は自動的に、[Service Profile Template Name] ドロップダウン リストで選択されているサービス プロファイル テンプレートに基づいてサービス プロファイルを作成し、新しく作成されたサービス プロファイルをサーバに関連付けます。
[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と、このフィールドで選択された組織の下にそのサービス プロファイルが置かれます。
[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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバ ディスカバリ ポリシーの設定

サーバ ディスカバリ ポリシー

このディスカバリ ポリシーは、新しいサーバが追加されたときのシステムの反応を決定します。サーバディスカバリ ポリシーを作成する場合、サーバ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、ユーザがまず新しいサーバ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。

サーバディスカバリ ポリシーを作成した場合は、新しいサーバを起動すると次の処理が行われます。

1. サーバに対してサーバ ディスカバリ ポリシーの資格認定が行われます。
2. サーバが必要な資格情報と一致する場合、Cisco UCS Manager はサーバ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、新しいサーバをただちに検出するか、またはユーザが新しいサーバを確認するまで待機する
   - サーバにスクラブ ポリシーを適用する

サーバ ディスカバリ ポリシーの作成

はじめる前に

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。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 [Server Discovery Policies] サブタブをクリックします。

ステップ 5 テーブル アイコン バーの [+] 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 6 [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 7 [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 は新しいサーバを自動的に検出しようとします
- [User Acknowledged]：Cisco UCS Manager はユーザが新しいサーバの検索を指示するまで待機します

ステップ 8 （任意） このポリシーをサーバ プールに関連付けるには、[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 9 （任意） 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 10 [OK] をクリックします。

次の作業

サーバ ディスカバリ ポリシーはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

サーバ ディスカバリ ポリシーの削除

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 [Server Discovery Policies] サブタブをクリックします。

ステップ 5 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 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバ継承ポリシーの設定

サーバ継承ポリシー

このポリシーは、サーバのサービス プロファイルを作成するためのサーバ 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すべてのサービスプロファイルは、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。

- サーバのインベントリの分析
- 選択された組織へのサーバの割り当て（設定されている場合）
- 製造元でサーバに設定された ID を持つサーバのサービス プロファイルの作成

このポリシーによって作成されたサービス プロファイルを別のサーバに移行できません。

サーバ継承ポリシーの作成

VIC アダプタを持つブレード 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）には、工場でサーバハードウェアに刻印されたサーバID値はありません。このため、アダプタ ID 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、サーバに割り当てられるものへの十分なエントリが含まれていない場合、サービス プロファイルのアソシエーションは設定エラーで失敗します。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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

ステップ 6 [Create 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[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 プールの資格ポリシーをドロップダウン リストから選択します。
[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、または現在のアソシエーションを変更する場合は、該当する組織をドロップダウン リストから選択します。

ステップ 7 [OK] をクリックします。

サーバ継承ポリシーの削除

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 [Server Inheritance Policies] サブタブをクリックします。

ステップ 5 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 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバ プール ポリシーの設定

サーバ プール ポリシー

このポリシーはサーバ 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 プール ポリシー資格情報により、サーバと、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 プール ポリシーがあった場合、このサーバ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

はじめる前に

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。

- 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）

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[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。
[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の資格ポリシーをドロップダウン リストから選択します。

ステップ 6 [OK] をクリックします。

サーバ プール ポリシーの削除

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバ プール ポリシーの資格情報の設定

サーバ プール ポリシー資格情報

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のインベントリに基づいて、サーバを資格認定します。 資格情報は、サーバ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
- 電源のグループ
- CPU のコア数、タイプ、および設定
- ストレージの設定と容量
- サーバのモデル

実装によっては、サーバ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できます。

- 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 ディスカバリ ポリシー
- サーバ継承ポリシー
- サーバ 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

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 （任意） 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、目的の最大容量を入力します。 1 ～ 65535 の任意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 （任意） 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 [Chassis Qualifications] 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）。

例：
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。

ヒント 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 （任意） 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 [Chassis Qualifications] 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) [Server Qualifications] 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 （任意） 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）。

名前	説明
[Min Cap] フィールド	最小限必要なメモリ容量（メガバイト単位）。
[Max Cap] フィールド	メモリの許容最大容量（メガバイト単位）。
[Width] フィールド	データ バスの最小幅。
[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 （任意） 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、関連付けられたテキスト 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、関連付けられたテキスト 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、関連付けられたテキスト 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、関連付けられたテキスト 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。

名前	説明
[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 （任意） 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がディスクレスである必要があるかどうか。 次のいずれかになります。 • [Unspecified]：いずれのストレージ タイプも使用できます。 • [Yes]：ストレージはディスクレスである必要があります。 • [No]：ストレージをディスクレスにすることはできません。
[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] を選択してブロック数を入力します。
[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] を選択してブロック 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にわたる最小ストレージ容量（メガバイト単位）。 容量を指定するには、[select] を選択して最小ストレージ容量を入力します。
[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] を選択して最大ストレージ容量を入力します。

名前	説明
[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] を選択して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] を選択して目的のユニットを入力します。

c) [OK] をクリックします。

ステップ 12 （任意） 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 （任意） このポリシーを使用して、電源の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 Power Group Qualifications] をクリックします。
b) [Create Power Group Qualifications] ダイアログボックスで、[Power Group] ドロップダウン リストから電源の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 （任意） 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 Rack 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から取得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

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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。

手順

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

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

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 配置ポリシーの設定

vNIC/vHBA 配置ポリシー

vNIC/vHBA 配置ポリシーは、次を判別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）がサーバ上の物理アダプタにどのようにマッピングされるか。
- どのタイプの vNIC または vHBA が各 vCon に割り当て可能か。

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に関連付けられると、vNIC/vHBA 配置ポリシーの vCons が物理アダプタに割り当てられ、vNIC および 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またはラック サーバでは、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2、vCon3 を Adapter3、vCon4 を Adapter4 に割り当てます。

2 つまたは 3 つのアダプタを備えたブレードまたはラック サーバについて、Cisco UCS UCS は、サーバのタイプ、および [Round Robin] または [Linear Ordered] である選択した仮想スロット マッピング スキームに基づいて vCon を割り当てます。 使用可能なマッピング スキームに関する詳細については、vCon からアダプタへの配置, （503 ページ）を参照してください。

Cisco UCS によって vCon が割り当てられた後、各 vCon の [Selection Preference] に基づいて vNIC と vHBA が割り当てられます。これは次のいずれかになります。

- [All]：明示的に割り当てられているか、未割り当てであるか、または動的に割り当てられているかどうかに関係なく、すべての設定済みの vNIC と vHBA を vCon に割り当てることができます。 これはデフォルトです。
- [Assigned Only]：vNIC と vHBA を vCon に明示的に割り当てる必要があります。 サービス プロファイルまたは vNIC または vHBA のプロパティを介して、vNIC および vHBA を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 と vHBA を vCon に割り当てることはできません。 vCon は、未割り当てか、または明示的に割り当てられているかに関係なく、すべてのスタティック vNIC と vHBA に対して使用できます。
- [Exclude Unassigned]：未割り当ての vNIC と vHBA 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ダイナミック vNIC と vHBA、およびスタティック vNIC と vHBA に対して使用できます。

サービス プロファイルに vNIC/vHBA 配置ポリシーを含めない場合、Cisco UCS Manager は、[Round Robin] の vCon マッピング スキームおよび [All] の vNIC/vHBA 選択プリファレンスにデフォルトで設定され、各アダプタの機能および相対容量に基づいてアダプタ間に vNIC および vHBA を配布します。

vCon からアダプタへの配置

Cisco UCS Manager は、サービス プロファイルのすべての vCon をサーバ上の物理アダプタにマッピングします。 マッピングがどのように発生し、vCon がサーバの特定のアダプタにどのように割り当てられるかは、次の条件によって異なります。

- サーバのタイプ。 2 枚のアダプタ カード付きの N20-B6620-2 および N20-B6625-2 ブレード サーバは、他のサポートされているラックまたはブレード サーバとは異なるマッピング スキームを使用します。
- サーバ内のアダプタ数。
- vNIC/vHBA 配置ポリシーの仮想スロット マッピング スキームの設定（該当する場合）。

vNIC/vHBA の選択プリファレンスを設定して vNIC および vHBA を vCon に割り当てる場合は、この配置を考慮する必要があります。

（注） vCon からアダプタへの配置は、アダプタの PCIE スロット番号には依存しません。 vCon 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 ディスカバリ中に割り当てられた ID です。

N20-B6620-2 および N20-B6625-2 ブレード サーバの vCon からアダプタへの配置

N20-B6620-2 および N20-B6625-2 ブレード サーバでは、2 つのアダプタには左から右に番号が付けられ、vCon には右から左に番号が付けられます。 いずれかのブレード サーバに単一のアダプタがある場合、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 サーバに 2 つのアダプタがある場合、vCons の割り当ては、仮想スロット マッピング スキームによって異なります。

- [Round Robin]：Cisco UCS は、vCon2 と vCon4 を Adapter1 に割り当て、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 Adapter1 に割り当て、vCon1 と vCon2 を Adapter2 に割り当てます。

その他すべてのサポートされているサーバの vCon からアダプタへの配置

N20-B6620-2 および N20-B6625-2 ブレード サーバ以外の Cisco UCS でサポートされているその他すべてのサーバについて、vCon の割り当ては、サーバのアダプタ数および仮想スロット マッピング スキームによって異なります。

1 つのアダプタを持つブレードまたはラック サーバでは、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2、vCon3 を Adapter3、vCon4 を Adapter4 に割り当てます。

2 つまたは 3 つのアダプタを備えたブレードまたはラック サーバについて、Cisco UCS は、選択した仮想スロット マッピング スキームに基づいて vCon を割り当てます。 この仮想スロット マッピング スキームは、[Round Robin] または [Linear Ordered] です。

表 *8*：ラウンド ロビン マッピング スキームを使用した *vCon* からアダプタへの配置

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	Adapter1	Adapter1	Adapter1	Adapter1
2	Adapter1	Adapter2	Adapter1	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter2
4	Adapter1	Adapter2	Adapter3	Adapter4

[Round Robin] は、デフォルトのマッピング スキームです。

表 *9*：リニア順のマッピング スキームを使用した *vCon* からアダプタへの配置

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	Adapter1	Adapter1	Adapter1	Adapter1
2	Adapter1	Adapter1	Adapter2	Adapter2
3	Adapter1	Adapter2	Adapter3	Adapter3
4	Adapter1	Adapter2	Adapter3	Adapter4

vNIC/vHBA から vCon への割り当て

Cisco UCS Manager vNIC/vHBA 配置ポリシーを通して vCon に vNIC および vHBA を割り当てるための 2 つのオプション（明示的な割り当ておよび暗黙的な割り当て）を提供します。

vNIC および vHBA の明示的な割り当て

明示的な割り当てでは、vCon、および vNIC または vHBA が割り当てられるアダプタを指定します。 サーバのアダプタ間で vNIC および vHBA が配布される方法を決定する必要がある場合は、この割り当てオプションを使用します。

vCon、および関連付けられた vNIC および vHBA を明示的な割り当てに設定するには、次の手順を実行します。

- vCon 設定を、いずれかの使用可能なオプションに設定します。 vNIC/vHBA 配置ポリシー、またはサーバに関連付けられたサービス プロファイルで vCon を設定できます。 vCon が [All] に設定されている場合も、その vCon に vNIC または vHBA を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、またはサーバに関連付けられたサービス プロファイルで実行できます。

vNIC または vHBA をそれらのタイプ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が発生したことを示すメッセージが表示されます。

サービス プロファイルの関連付け中に、Cisco UCS Manager は、ポリシーの設定に応じて vNIC および vHBA を割り当てる前に、サーバ上の物理アダプタの数および機能に対して vNIC および vHBA の設定された配置を検証します。 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います。

アダプタが 1 つ以上の vNIC または vHBA の割り当てをサポートしていない場合は、Cisco UCS Manager によってサービス プロファイルに対するエラーが生成されます。

vNIC および vHBA の暗黙的な割り当て

暗黙的な割り当てでは、Cisco UCS Manager は、vCon、およびアダプタの機能とそれらの相対容量に応じて vNIC または vHBA が割り当てられるアダプタを判断します。 vNIC または vHBA が割り当てられるアダプタがシステム設定にとって重要でない場合は、この割り当てオプションを使用します。

vCon を暗黙的な割り当てに設定するには、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。 vNIC/vHBA 配置ポリシー、またはサーバに関連付けられたサービス プロファイルで vCon を設定できます。
- vCon 設定を [Assigned Only] に設定しないでください。 暗黙的な割り当てをこの設定で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に、Cisco UCS Manager は、サーバ上の物理アダプタの数および機能を確認し、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おり、vNIC および vHBA の配置は、システムによって決定される実際の順番に従って実行されます。 たとえば、あるアダプタが別のアダプタよりも多くの vNIC に対応できる場合、そのアダプタにはより多くの vNIC が割り当てられます。

アダプタがそのサーバに対して設定された vNIC および vHBA の数をサポートしていない場合は、Cisco UCS Manager によってサービス プロファイルに対するエラーが生成されます。

デュアル アダプタ環境における vNIC の暗黙的な割り当て

各スロットでアダプタ カード付きのデュアル スロット サーバに暗黙的な vNIC の割り当てを使用すると、Cisco UCS Manager は、通常、次のように vNIC と vHBA を割り当てます。

- サーバの両方のスロットに同じアダプタがある場合、Cisco UCS Manager は、vNIC の半分および vHBA の半分を各アダプタに割り当てます。

- サーバに 1 つの非 VIC アダプタおよび 1 つの VIC アダプタがある場合、Cisco UCS Manager は、2 つの vNIC および 2 つの vHBA を非 VIC アダプタに割り当て、残りの vNIC および vHBA を VIC アダプタに割り当てます。
- サーバに 2 つの異なる VIC アダプタがある場合、Cisco UCS Manager は、2 つのアダプタの能力比に基づいて、vNIC および vHBA を比例的に割り当てます。

次に、Cisco UCS Manager がサポートされているアダプタ カードの異なる組み合わせで vNIC および vHBA を割り当てる一般的な方法の例を示します。

- 4 つの vNIC を設定する場合で、サーバに 2 つの Cisco UCS M51KR-B Broadcom BCM57711アダプタ（それぞれに 2 つの vNIC）が含まれている場合、Cisco UCS Manager は 2 つの vNIC を各アダプタに割り当てます。
- 50 個の vNIC を設定する場合にサーバに Cisco UCS CNA M72KR-Eアダプタ（2 つの vNIC）と Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 個の vNIC）が含まれている場合、Cisco UCS Manager は 2 つの vNIC を Cisco UCS CNA M72KR-Eアダプタに割り当て、48 個の 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 個の vNIC を設定する場合で、サーバに Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 個の vNIC）と Cisco UCS M82-8P 仮想インターフェイス カードアダプタ（256 個の vNIC）が含まれている場合、Cisco UCS Manager は 50 個の 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、100 個の vNIC を Cisco UCS M82-8P 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 をサーバ用に設定した場合は、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ていない vNIC ファブリック フェールオーバーを含む設定の場合、Cisco UCS Manager は、イネーブルにされたファブリック フェールオーバーがあるすべての 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 だけが含まれている設定の場合、vNIC をサポートしていないアダプタに暗黙的に割り当てられる vNIC はありません。 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。

ダイナミック vNIC が含まれている設定では、同じ暗黙的な割り当てが発生します。 Cisco UCS Manager は、すべてのダイナミック 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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 は、仮想ネットワーク インターフェイス（vCon）接続をサーバの PCIe アダプタ カードに割り当てます。 各 vCon は、vNIC および vHBA を割り当てることができる物理アダプタの仮想表現です。 1 つのアダプタを持つブレードまたはラック サーバでは、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2、vCon3 を Adapter3、vCon4 を Adapter4 に割り当てます。 2 つまたは 3 つのアダプタを備えたブレードまたはラック サーバについて、Cisco UCS は、選択した仮想スロット 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 カード付きのサーバでは、Cisco UCS は、vCon1 と vCon3 を Adapter1 に割り当て、次に vCon2 と vCon4 を Adapter2 に割り当てます。 3 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 と vCon4 を Adapter2、vCon3 を Adapter3 に割り当てます。 これはデフォルトのスキームです。 • [Linear Ordered]：2 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 と vCon2 を Adapter1 に割り当て、次に vCon3 と vCon4 を Adapter2 に割り当てます。 3 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2 に割り当て、次に vCon3 と vCon4 を Adapter3 に割り当てます。 （注） N20-B6620-2 および N20-B6625-2 ブレード サーバでは、2 つのアダプタには左から右に番号が付けられ、vCon には右から左に番号が付けられます。 いずれかのブレード サーバに単一のアダプタがある場合、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 サーバに 2 つのアダプタがある場合、vCons の割り当ては、仮想スロット マッピング スキームによって異なります。 • [Round Robin]：Cisco UCS は、vCon2 と vCon4 を Adapter1 に割り当て、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 Adapter1 に割り当て、vCon1 と vCon2 を Adapter2 に割り当てます。 Cisco UCS によって vCon が割り当てられた後、各 vCon の [Selection Preference] に基づいて vNIC と vHBA が割り当てられます。

b) 各 [Virtual Slot] の [Selection Preference] カラムで、ドロップダウン リストから次のいずれかを選択します。

- [All]：明示的に割り当てられているか、未割り当てであるか、または動的に割り当てられているかどうかに関係なく、すべての設定済みの vNIC と vHBA を vCon に割り当てることができます。 これはデフォルトです。
- [Assigned Only]：vNIC と vHBA を vCon に明示的に割り当てる必要があります。 サービス プロファイルまたは vNIC または vHBA のプロパティを介して、vNIC および vHBA を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 と vHBA を vCon に割り当てることはできません。 vCon は、未割り当てか、または明示的に割り当てられているかに関係なく、すべてのスタティック vNIC と vHBA に対して使用できます。
- [Exclude Unassigned]：未割り当ての vNIC と vHBA 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ダイナミック vNIC と vHBA、およびスタティック vNIC と vHBA に対して使用できます。

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 [Navigation] ペインの [Servers] タブをクリックします。

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

vCon への vNIC の明示的な割り当て

はじめる前に

次のいずれかの値を使用して、vNIC/vHBA配置ポリシーを介して、あるいはサービスプロファイルで、vCons を設定します。

- Assigned Only
- Exclude Dynamic
- Exclude Unassigned

vCon が [All] に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。 ただし、この設定では制御性が低くなります。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 明示的に vCon に割り当てる vNIC のサービスプロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Service_Profile_Name] > [vNICs] の順に展開します。

ステップ 5 vCon に明示的に割り当てる vNIC をクリックします。

ステップ 6 [Work] ペインの [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、次のフィールドに値を入力します。

名前	説明
[Desired Placement] ドロップダウン リスト	vNIC に対するユーザ指定の仮想ネットワーク インターフェイス接続（vCon）の配置。 次のいずれかになります。 • [Any]：Cisco UCS Manager は、vNIC が割り当てられる vCon を決定できます。 • [1]：vNIC を明示的に vCon1 に割り当てます。 • [2]：vNIC を明示的に vCon2 に割り当てます。 • [3]：vNIC を明示的に vCon3 に割り当てます。 • [4]：vNIC を明示的に vCon4 に割り当てます。
[Actual Assignment] フィールド	サーバ上の vNIC の実際の vCon の割り当て。

vNIC をそのタイプの vNIC 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が発生したことを示すメッセージが表示されます。 vNIC を別の vCon に割り当てるか、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、次のフィールドに値を入力します。

名前	説明
[Desired Order] フィールド	vNIC に対するユーザ指定の PCI の順序。 0 ～ 128 の整数を入力します。 サーバに対して 128 個を超える vNIC は作成できません。
[Actual Order] フィールド	サーバ上の vNIC の実際の PCI の順序。

ステップ 9 [Save Changes] をクリックします。

vCon への vHBA の明示的な割り当て

はじめる前に

次のいずれかの値を使用して、vNIC/vHBA 配置ポリシーを介して、あるいはサービスプロファイルで、vCons を設定します。

- Assigned Only
- Exclude Dynamic
- Exclude Unassigned

vCon が [All] に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。 ただし、この設定では制御性が低くなります。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 明示的に vCon に割り当てる vHBA のサービス プロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

ステップ 5 vCon に明示的に割り当てる vHBA をクリックします。

ステップ 6 [Work] ペインの [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、次のフィールドに値を入力します。

名前	説明
[Desired Placement] フィールド	vHBA 用のユーザ指定の仮想ネットワークインターフェイス接続（vCon）の配置。 次のいずれかになります。 • [Any]：Cisco UCS Manager は、vHBA に割り当てられる vCon を決定できます。 • [1]：vHBA を明示的に vCon1 に割り当てます。 • [2]：vHBA を明示的に vCon2 に割り当てます。 • [3]：vHBA を明示的に vCon3 に割り当てます。 • [4]：vHBA を明示的に vCon4 に割り当てます。
[Actual Assignment] フィールド	サーバ上の vHBA の実際の vCon の割り当て。

vHBA をそのタイプの vHBA 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が発生したことを示すメッセージが表示されます。 vHBA を別の vCon に割り当てるか、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、次のフィールドに値を入力します。

名前	説明
[Desired Order] フィールド	vHBA に対するユーザ指定の PCI の順序。 0 ～ 128 の整数を入力します。 サーバに対して 128 個を超える vHBA は作成できません。
[Actual Order] フィールド	サーバ上の vHBA の実際の PCI の順序。

ステップ 9 [Save Changes] をクリックします。

ダイナミック vNIC を配置する前のスタティック vNIC の配置

最適なパフォーマンスを得るには、PCIe バスでダイナミック vNIC を配置する前に、スタティック vNIC およびスタティック vHBA を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 およびスタティック vHBA の両方を指します。 Cisco UCS Manager リリース 2.1 は、スタティック vNIC とダイナミック vNIC の順序に関して次の機能を提供します。

- 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 より前のリリースで定義されたプロファイル）に対する変更がない場合は、vNIC の順序は変更されません。
- Cisco UCS Manager リリース 2.1 にアップグレードした後、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。 その結果、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 の前の順序で配置されます。
- 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シーケンスとは無関係です。
- SRIOV 対応サービス プロファイルでは、UCSM は、対応する仮想関数（VF）の前に vNIC 物理関数（PF）を挿入します。 このスキームにより、VF が PCIe バスの親 PF vNIC の近くに配置され、BDFs が VF の連続した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 の最初のデバイスの順序。

```
dyn-vNIC-1 1
dyn-vNIC-2 2
```

Cisco UCS Manager リリース 2.0 の新しいデバイスの順序（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 にアップグレードした後（サービス プロファイルに対する vNIC 関連の変更前）。

```
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 の新しいデバイスの順序（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（各スタティック vNIC 用の新しい 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、最後のスタティック vNIC/vHBA の配置後に新しいバス スロットから配置されます。

（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ます。

表 *10*：バージョンの互換性

Cisco UCS Manager		
バージョン 1.4 **スキーム：ZeroFunction**	**バージョン 2.0** **スキーム：ZeroFunction/MultiFunction**	**バージョン 2.1** **スキーム：ZeroFunction/MultiFunction/StaticZero**
すべてのスタティック vNIC およびダイナミック vNIC は、バス [0-57]、機能 [0] にあります。 < ZeroFunction モード >	静的 vNIC およびダイナミック vNIC は、バス [0-57]、機能 [0-7] にあります。 バス 0、機能 0 バス 0、機能 7 バス 1、機能 0 < MultiFunction モード >	スタティック vNIC または PF は、バス [0-57]、機能 [0] にあります。 SRIOV：対応する VF は同一バスおよび機能 [1-255] にあります。No-SRIOV：ダイナミック vNIC はバス [0-57]、機能 [0-7] にあります。 < StaticZero モード >
	Balboa からのアップグレードは、バス <= 57 まで BDF（ZeroFunction モードのまま）の番号を付け直すことはしません。 デバイスが 58 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は、バス <= 57 まで BDF（ZeroFunction モードのまま）の番号を付け直すことはしません。 デバイスが 58 またはプラットフォーム固有の最大 PCIe バス番号を超えるか、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は、BDF（ZeroFunction / MultiFunction モードのまま）の番号を付け直すことはしません。 デバイスが 58 またはプラットフォーム固有の最大 PCIe バス番号を超えるか、SRIOV 設定に変更されると、StaticZero モードに切り替わります。

第 31 章

サーバのブート設定

この章の内容は、次のとおりです。

- ブート ポリシー，517 ページ
- ブート ポリシーの作成，518 ページ
- SAN ブート，519 ページ
- iSCSI ブート，522 ページ
- LAN ブート，548 ページ
- ローカル ディスク ブート，549 ページ
- 仮想メディア ブート，550 ページ
- ブート ポリシーの削除，552 ページ

ブート ポリシー

ブート ポリシーにより決定されることは次のとおりです。

- ブート デバイスの設定
- サーバのブート元である場所
- ブート デバイスの起動順序

たとえば、ローカル ディスクや CD-ROM（VMedia）などのローカル デバイスから関連するサーバを選択するか、または SAN ブートもしくは LAN（PXE）ブートを選択することができます。

このポリシーはサービス プロファイルにインクルードする必要があります。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 ポリシーをインクルードしなかった場合、サーバは BIOS のデフォルト設定を使用して、ブート順序を決定します。

重要 ブートポリシーに対する変更は、そのブートポリシーをインクルードしている、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との再アソシエーションは自動的にトリガーされます。

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。 ただし、iSCSI ブートを除き、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めることができるグローバルなブートポリシーを作成することをお勧めします。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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、[Reboot on boot Order Change] チェックボックスがブート ポリシーに対して選択されており、CD-ROM またはフロッピーがブート順で最後のデバイスの場合に、デバイスを取り外すか、装着しても、ブート順に直接影響は及ぼされず、サーバはリブートされません。

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 を確認します。

- これをオンにすると、Cisco UCS Manager は設定エラーを表示し、[Boot Order] テーブルにリストされている vNIC、vHBA、または iSCSI の vNIC の 1 つ以上がサービス プロファイルのサーバ設定と一致するかどうかをレポートします。
- オフになっている場合、（ブート オプションに適するように）Cisco UCS Manager はサービス プロファイルのサーバ設定から vNIC、vHBA、または iSCSI vNIC を使用します。 ブート

ポリシーで指定された vNIC、vHBA、または iSCSI の vNIC がサービス プロファイルのサーバ設定と一致するかどうかはレポートしません。

ステップ 8 ブート ポリシーに 1 つ以上の次のブート オプションを設定し、ブート順序を設定します。

- SAN ブート：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 ポリシーに対する SAN ブートの設定, （520 ページ）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、サーバはセカンダリからのブートを試行します。

- iSCSI ブート：iSCSI LUN から起動するには、iSCSI ブート ポリシーの作成, （532 ページ）に進みます。

- LAN ブート：中央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 ポリシーに対する LAN ブートの設定, （548 ページ）に進みます。

- ローカル ディスク ブート：サーバのローカル ディスクから起動するには、ブート ポリシーに対するローカル ディスク ブートの設定, （549 ページ）に進みます。

- 仮想メディアのブート：サーバに物理 CD またはフロッピー ドライブの挿入を模倣する仮想メディアから起動するには、ブート ポリシーに対する仮想メディア ブートの設定, （550 ページ）に進みます。

次の作業

ブートポリシーはサービスプロファイルとテンプレートのうち一方、または両方にインクルードします。

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。

SAN ブート

SAN のオペレーティング システム イメージから 1 つ以上のサーバを起動するようにブート ポリシーを設定できます。 ブート ポリシーはプライマリ SAN ブートとセカンダリ 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、サーバはセカンダリからのブートを試行します。

システムに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ます。SANからブートした場合、あるサーバから別のサーバにサービスプロファイルを移動すると、移動後のサーバは、まったく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、この新しいサーバはまったく同じサーバと認識されます。

SAN ブートを使用するには、以下が設定されている必要があります。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストする SAN ストレージ デバイスと通信する必要があります。

- オペレーティング システムのイメージのあるデバイスのブート ターゲット LUN。

ブート ポリシーに対する SAN 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。 ただし、iSCSI ブートを除き、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めることができるグローバルなブート ポリシーを作成することをお勧めします。

ヒント　ブート ポリシーのブート順序には、ローカル ディスクと SAN LUN の両方ではなく一方のみをインクルードし、サーバが誤ったストレージ タイプからブートしないようにすることを推奨します。 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, （518 ページ）から直接続行されます。

はじめる前に

（注）　SAN LUN からサーバをブートするブート ポリシーを作成し、安定した SAN ブート操作が必要な場合は、ブート ポリシーを含むサービス プロファイルに関連付けられたサーバからすべてのローカル ディスクを最初に削除することを推奨します。

手順

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 で次のフィールドに値を入力し、[OK] をクリックします。

名前	説明
[vHBA] フィールド	SAN ブートに使用する vHBA の名前を入力します。

名前	説明
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブート デバイス クラスに定義されている最初のアドレス。 ブート ポリシーには、1つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブート デバイス クラスに定義されている 2 番目のアドレス。 各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブート デバイス」や「セカンダリ ブート デバイス」はブート順序を表す用語ではありません。 同じデバイス クラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

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 で次のフィールドに値を入力して、[OK] をクリックします。

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

名前	説明
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブート デバイス クラスに定義されている最初のアドレス。ブート ポリシーには、1 つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブート デバイス クラスに定義されている 2 番目のアドレス。各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブート デバイス」や「セカンダリ ブート デバイス」はブート順序を表す用語ではありません。 同じデバイス クラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

ステップ 5 次のいずれかを実行します。

- [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。

次の作業

ブート ポリシーはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

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 ブートは、サーバがそのオペレーティング システムを、リモートにある iSCSI ターゲット マシンからネットワーク経由でブートできるようにします。

iSCSI ブートは次の Cisco UCS ハードウェアでサポートされます。

- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタがあり、Broadcom から提供されるデフォルトの MAC アドレスを使用する Cisco UCS サーバ ブレード。

- Cisco UCS M81KR 仮想インターフェイス カード
- Cisco UCS M82-8P 仮想インターフェイス カード

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, （523 ページ）を参照してください。

iSCSI ブートを実装するためのハイレベルな手順については、iSCSI のブート設定, （526 ページ）を参照してください。

iSCSI ブート プロセス

サービス プロファイル用に作成された Cisco UCS Manager iSCSI vNIC と iSCSI ブート情報は、ブレード サーバにあるメザニン アダプタをプログラムするためにアソシエーション プロセスで使用されます。 アダプタのプログラミング後に、ブレード サーバは最新のサービス プロファイル値を使用してリブートします。 電源投入時セルフテスト（POST）のあと、アダプタは、これらのサービスプロファイル値を使用して初期化しようとします。 アダプタがこれらの値を使用し、指定されたターゲットにログインできる場合は、アダプタは初期化され、iSCSI ブートのファームウェアのテーブル（iBFT）がホスト メモリに、有効でブート可能な LUN がシステム BIOS に公開されます。 ホスト メモリに公開される 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ます。

（注） iBFT は、イニシエータからターゲットへの初期化に対して最初の iSCSI vNIC とターゲット 1 のみ使用します。 このシナリオは、第 2 ターゲット（ターゲット 2）が最初の iSCSI vNIC 用に存在している場合にも適用されます。

オペレーティング システム（OS）のインストールを行う次の手順には、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 の情報を使用してブート デバイスを検出し、ターゲット LUN に iSCSI パスを作成します。 一部の OS では、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に、OS のインストーラは、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 インストール済み環境のソフトウェア レベルで動作し、HBA モード（別名 TCP オフロード）では動作しない可能性があります。 iBFT が HBA モードで動作するかどうかは、インストール時の OS の対応状況によって異なります。 また、Cisco UCS M51KR-B Broadcom BCM57711 アダプタが含まれるサーバの場合、iBFT はジャンボ設定に関係なく、1500 の最大伝送単位（MTU）サイズで正常に動作します。 OS が HBA モードをサポートする場合は、iSCSI のインストール プロセスの後で 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、次のガイドラインおよび前提条件を満たしている必要があります。

- 2 番目の vNIC（フェールオーバー vNIC）を iSCSI LUN から起動する必要がある Windows 2008 サーバから iSCSI ブートを設定するには、Microsoft 社のサポート技術情報の記事 976042 を参照してください。 Microsoft には、ネットワーク ハードウェアが変更された場合に、Windows が iSCSI ドライブから起動できなくなるか、bugcheck エラーが発生する可能性がある既知の問題があります。 この問題を回避するには、Microsoft の推奨する解決方法に従ってください。
- ストレージ アレイには iSCSI ブートのライセンスが付与され、アレイ側の LUN のマスキングが正しく設定されている必要があります。
- 2 つの IP アドレスは、iSCSI イニシエータごとに決定する必要があります。 可能であれば、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。 IP アドレスが Dynamic Host Configuration Protocol（DHCP）を使用してスタティックまたはダイナミックに割り当てられます。
- グローバル ブート ポリシーにはブート パラメータを設定できません。 代わりに、ブート パラメータを設定した後、適切なサービス プロファイルにブート ポリシーを含める必要があります。
- オペレーティング システム（OS）は iSCSI ブート ファームウェア テーブル（iBFT）互換である必要があります。
- Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタの場合：
  - iSCSI ブートを使用するブレードには、Cisco UCS M51KR-B Broadcom BCM57711 ネットワーク アダプタが装着されている必要があります。 アダプタ カードを取り付けまたは交換する方法については、*Cisco UCS B250* 拡張メモリ ブレード サーバの取り付けおよびサービス ノートを参照してください。 このサービス ノートは、『*Cisco UCS B-Series Servers Documentation Roadmap*』（http://www.cisco.com/go/unifiedcomputing/b-series-doc）で参照できます。
  - iSCSI デバイスに MAC アドレスを設定します。
  - DHCP のベンダー ID（オプション 43）を使用している場合、iSCSI デバイスの MAC アドレスが /etc/dhcpd.conf に設定されている必要があります。
  - 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、インストール時の HBA モードをサポートするのは Windows OS だけです。
  - 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 設定をディセーブルにして、OS をインストールした後で、Boot to Target 設定を再びイネーブルにします。

    （注） アダプタ ポリシーの設定を変更するたびにアダプタがリブートして、新しい設定が適用されます。

  - OS を iSCSI ターゲットにインストールする場合、iSCSI ターゲットの順序は OS イメージが存在するデバイスの前でなければなりません。 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 iSCSI ターゲット、CD となります。

- サーバが iSCSI ブートされたあとは、Broadcom ツールを使用してイニシエータ名、ターゲット名、LUN、iSCSI デバイス IP、またはネットマスク/ゲートウェイを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 アダプタの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 と Cisco UCS M82-8P 仮想インターフェイス カード の場合：
  - iSCSI デバイスに 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ません。
  - OS を iSCSI ターゲットにインストールする場合、iSCSI ターゲットの順序は OS イメージが存在するデバイスの後でなければなりません。 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 CD、iSCSI ターゲットとなります。
  - DHCP のベンダー 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 アドレスが /etc/dhcpd.conf に設定されている必要があります。
  - サーバが iSCSI ブートされたあとは、オーバーレイ vNIC の IP の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 ディスクに書き込まれる必要があります。

Windows での MPIO のイネーブル化

（注） ネットワーク ハードウェアを変更した場合、Windows は iSCSI ドライブからのブートに失敗する可能性があります。 詳細については、 Microsoft 社のサポート技術情報 ID：976042 を参照してください。

はじめる前に

MPIO をイネーブルにするサーバには、VIC ドライバが必要です。

手順

ステップ 1 サーバに関連付けられたサービス プロファイルでは、プライマリおよびセカンダリの iSCSI vNIC を設定します。
詳細については、サービス プロファイルに対する iSCSI vNIC の作成, （533 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、Microsoft ソフトウェアの iSCSI Initiator を使用して、セカンダリ iSCSI vNIC に接続します。

ステップ 4 ホストでの MPIO のイネーブル化

ステップ 5 サーバ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, （532 ページ）を参照してください。

iSCSI のブート設定

LUN ターゲットから iSCSI のブートを行うため、Cisco UCS にアダプタまたはブレードを設定した場合、次のすべての手順を完了する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	iSCSI ブートのアダプタ ポリシーを設定します。	（任意） 詳細については、iSCSI アダプタ ポリシーの作成, （527 ページ）を参照してください。
ステップ 2	イニシエータおよびターゲットで使用される認証プロファイルを設定します。	（任意） 詳細については、認証プロファイルの作成, （529 ページ）を参照してください。
ステップ 3	IP アドレス プールからの IP アドレスを使用するように iSCSI イニシエータを設定する場合は、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。	（任意） 詳細については、iSCSI イニシエータの IP プールの作成, （531 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、特定のサービス ポリシーに対してだけローカル ブート ポリシーを作成できます。 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。	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, （532 ページ）を参照してください。
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 ポリシーを作成する場合	ステップ 7 で、サービス プロファイルに iSCSI ブートおよび vNIC パラメータを設

	コマンドまたはアクション	目的
	は、サービス プロファイルにブート ポリシーを割り当てる必要があります。それ以外の場合は、次のステップに進みます。	定する際に、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 プロファイルに iSCSI vNIC を作成します。	詳細については、サービス プロファイルに対する iSCSI vNIC の作成, （533 ページ）を参照してください。
ステップ 7	イニシエータおよびターゲットインターフェイスを含む iSCSI ブート パラメータ、およびエキスパートモードでのサービス 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 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, （578 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, （620 ページ）をそれぞれ参照してください。
ステップ 8	iSCSI ブート動作を確認します。	詳細については、iSCSI ブートの確認を参照してください。
ステップ 9	サーバに OS をインストールします。	詳細については、次のいずれかのガイドを参照してください。 • *Cisco UCS B シリーズ ブレード サーバ 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 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 Windows インストレーション ガイド*
ステップ 10	サーバをブートします。	

iSCSI アダプタ ポリシーの作成

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Connection Timeout] フィールド	最初のログインが失敗し、iSCSIアダプタを使用できないとCisco UCS が判断するまでの待機時間（秒）。 0 ～ 255 の整数を入力します。 0 を入力すると、Cisco UCS はアダプタのファームウェアの値セットを使用します（デフォルトは 15 秒）。
[LUN Busy Retry Count] フィールド	iSCSI LUN 検出中に障害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 はアダプタのファームウェアの値セットを使用します（デフォルトは 15 秒）。
[DHCP Timeout] フィールド	DHCP サーバを使用できないとイニシエータが判断するまでの待機秒数。 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。 この設定を使用すると、必要に応じてパケットの往復時間を計算できるように、送信されたパケットにはパケットの送信時にタイムスタンプが指定されます。 **（注）** このオプションは、Cisco UCS NIC M51KR-B アダプタを持つサーバに対してのみ適用されます。
[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。 **重要** 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を持つサーバに対してのみイネーブルにする必要があります。

名前	説明
[Boot to Target] チェックボックス	iSCSI ターゲットから起動するには、このボックスをオンにします。 （注） このオプションは、Cisco UCS NIC M51KR-B アダプタを持つサーバに対してのみ適用されます。これは、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ディセーブルにする必要があります。

ステップ 6 [OK] をクリックします。

次の作業

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のうち一方、または両方に組み込みます。

iSCSI アダプタ ポリシーの削除

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 [Authentication Profiles] を右クリックし、[Create 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[User Id] フィールド	このサービス プロファイルに関連付けられているユーザ ID。 1 ～ 128 文字の文字、スペース、または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ているパスワード。 特殊文字を含む 12 ～ 16 文字を入力します。
[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。

次の作業

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のうち一方、または両方に組み込みます。

認証プロファイルの削除

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 [Authentication Profiles] ノードを展開します。

ステップ 5 削除する IP プロバイダーを右クリックし、[Delete] を選択します。

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

iSCSI イニシエータの 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 指定した IP アドレスのブロックを予約します。

IP プールには、サーバまたはサービス プロファイルの静的 IP アドレスとして割り当てられているどの IP アドレスも含まれていてはなりません。

手順

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

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [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 IP Addresses] を選択します。

ステップ 6 [Create a Block of IP 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
[From] フィールド	ブロック内の最初の IP アドレス。
[Size] フィールド	プール内の IP アドレスの数。
[Subnet Mask] フィールド	ブロック内の IP アドレスと関連付けられたサブネットマスク。

名前	説明
[Default Gateway] フィールド	ブロック内の IP アドレスと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	このブロックの IP アドレスがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] フィールド	このブロックの IP アドレスがアクセスする必要のあるセカンダリ DNS サーバ。

ステップ 7 [OK] をクリックします。

次の作業

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て、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 ポリシーごとに最大 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 ソースとして機能し、もう一方がセカンダリ iSCSI ブート ソースとして機能します。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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、[Reboot on boot Order Change] チェックボックスがブート ポリシーに対して選択されており、CD-ROM またはフロッピーがブート順で最後のデバイスの場合に、デバ

イスを取り外すか、装着しても、ブート順に直接影響は及ぼされず、サーバはリブートされません。

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 を確認します。

- これをオンにすると、Cisco UCS Manager は設定エラーを表示し、[Boot Order] テーブルにリストされている vNIC、vHBA、または iSCSI の vNIC の 1 つ以上がサービス プロファイルのサーバ設定と一致するかどうかをレポートします。
- オフになっている場合、（ブート オプションに適するように）Cisco UCS Manager はサービス プロファイルのサーバ設定から vNIC、vHBA、または iSCSI vNIC を使用します。 ブート ポリシーで指定された vNIC、vHBA、または iSCSI の vNIC がサービス プロファイルのサーバ設定と一致するかどうかはレポートしません。

ステップ 8 ブート ポリシーに iSCSI ブートを追加するには、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に iSCSI vNIC の名前を入力し、[OK] をクリックします。
d) ステップ b と c を繰り返して別の iSCSI vNIC を作成します。

次の作業

ブートポリシーはサービスプロファイルとテンプレートのうち一方、または両方にインクルードします。

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。

サービス プロファイルに対する iSCSI vNIC の作成

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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る組織に対応するノードを展開します。

ステップ 4 iSCSI の 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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（ある場合）。
[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（ある場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC に使用可能な新しい iSCSI アダプタ ポリシーを作成するには、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（ある場合）。MAC アドレスが設定されていない場合、Cisco UCS Manager GUI には [Derived] が表示されます。
[MAC Pool] フィールド	この iSCSI vNIC に関連付けられた MAC プール（ある場合）。
[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（ある場合）。 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 M82-8P 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 上のネイティブ 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、指定する VLAN はオーバーレイ vNIC に割り当てられたどの VLAN にすることもできます。

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 アドレスは割り当てないまま、[Select (None used by default)] を選択してください。 このサービス プロファイルに関連付けられるサーバに 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 M82-8P 仮想インターフェイス カード が含まれている場合、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るサーバに Cisco UCS NIC M51KR-B アダプタが含まれている場合、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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。

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] ウィザードのフィールドに値を入力します。
詳細については、MAC プールの作成, （290 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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

iSCSI ブート パラメータの設定

iSCSI の vNIC のブート順、ブート ポリシー、認証プロファイル、送信側インターフェイスとターゲット インターフェイスなどの iSCSI ブート パラメータを設定できます。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 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、[Boot Order] テーブルに追加するサーバを起動する iSCSI vNIC をダブルクリックします。

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 個の iSCSI vNIC がある場合は、ブート パラメータを設定する iSCSI vNIC 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、次のフィールドに値を入力します。

名前	説明
[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。
[Authentication Profile] ドロップダウン リスト	関連付けられている認証プロファイルの名前。
[Create iSCSI Authentication Profile] リンク	すべての iSCSI vNIC に使用可能な新しい認証プロファイル ポリシーを作成するには、このリンクをクリックします。

ステップ 10 [Initiator Name] 領域で、次のフィールドに値を入力します。

名前	説明
[Initiator Name Assignment] ドロップダウン リスト	Cisco UCS が iSCSI ブート イニシエータの名前をどのように割り当てるか。 Cisco UCS で、次のように実行します。 • 特定のイニシエータの名前を使用する場合は、[Manual] を選択します。 Cisco UCS Manager GUI は、イニシエータの名前を指定できる [Initiator Name] フィールドを表示します。 • プールから IQN 接尾辞を選択する場合は、リストから IQN 接尾辞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。 最初の数字はプール内で使用可能な IQN 接尾辞の数であり、2 番目の数字はプール内の接尾辞の合計数です。 この Cisco UCS ドメインが Cisco UCS Central に登録されている場合、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[Create IQN Suffix Pool] リンク	Cisco UCS ドメイン内のすべてのオブジェクト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 イニシエータの名前を定義する正規表現。 次の特殊文字を含め、最大 223 文字の英数字を指定できます。 • .（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]（デフォルトで使用される DHCP）	システムは、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 アドレスは、この領域に入力された情報に基づいて iSCSI ブートの vNIC に割り当てられます。 ステップ 12 に進みます。

オプション	説明
Pool	IPv4 アドレスは管理 IP アドレスのプールから iSCSI ブートの 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] を選択している場合は、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には、[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。
[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。
[Primary DNS] フィールド	プライマリ DNS サーバ アドレス。
[Secondary DNS] フィールド	セカンダリ DNS サーバ 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	システムは、設定する必要があるスタティック ターゲット インターフェイスを作成します。 ステップ 14 に進みます。
iSCSI Auto Target Interface	システムは自動ターゲット インターフェイスを作成します。 自動ターゲットがイニシエータまたは DHCP ベンダー ID を使用するかを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 [Static Target Interface] テーブルで [iSCSI Static Target Interface] を選択している場合は [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、次のフィールドに値を入力します。

名前	説明
[iSCSI Target Name] フィールド	iSCSI ターゲットの iSCSI Qualified Name（IQN）または Extended Unique Identifier（EUI）の名前を定義する正規表現。 英数字のほかに、次の特殊文字も使用できます。 • .（ピリオド） • :（コロン） • -（ダッシュ） **重要** この名前は、標準 IQN または EUI のガイドラインを使用して、適切にフォーマットされている必要があります。 次の例は、適切にフォーマット設定された iSCSI ターゲット名を示しています。 • 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	iSCSI ターゲット用にシステムによって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。
[Authentication Profile] ドロップダウン リスト	関連付けられている認証プロファイルの名前。
[Create iSCSI Authentication Profile] リンク	すべての iSCSI vNIC に使用可能な新しい認証プロファイル ポリシーを作成するには、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 ID。

ステップ 16 [iSCSI Auto Target Interface] を選択している場合は、[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されている必要があります。 ベンダー ID には、最大 32 文字の英数字を使用できます。

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 の vNIC のブート順、ブート ポリシー、認証プロファイル、イニシエータ インターフェイスとターゲット インターフェイスなどの iSCSI ブート パラメータを変更できます。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 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 iSCSI vNIC を追加する、またはブート順序から削除するか、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、[iSCSI vNICs] 領域に追加するには、iSCSI vNIC をダブルクリックし、[Boot Order] テーブルに追加します。
- [Boot Order] テーブルで iSCSI vNIC をブート順序から削除するには、[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、[Boot Order] テーブルで変更するには、iSCSI vNIC を選択して [Move Up] か [Move Down] をクリックします。

ステップ 8 ブート パラメータを、[iSCSI vNICs] 領域で変更するには、[Set Boot Parameters] のリンクをクリックします。
2 個の iSCSI vNIC がある場合は、ブート パラメータを変更する iSCSI vNIC 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、次のフィールドの値を変更します。

名前	説明
[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。
[Authentication Profile] ドロップダウン リスト	関連付けられている認証プロファイルの名前。

名前	説明
[Create iSCSI Authentication Profile] リンク	すべての iSCSI vNIC に使用可能な新しい認証プロファイル ポリシーを作成するには、このリンクをクリックします。

ステップ 10 [Initiator Name] 領域で、次のフィールドに値を入力します。

名前	説明
[Initiator Name Assignment] ドロップダウン リスト	Cisco UCS が iSCSI ブート イニシエータの名前をどのように割り当てるか。 Cisco UCS で、次のように実行します。 • 特定のイニシエータの名前を使用する場合は、[Manual] を選択します。 Cisco UCS Manager GUI は、イニシエータの名前を指定できる [Initiator Name] フィールドを表示します。 • プールから IQN 接尾辞を選択する場合は、リストから IQN 接尾辞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。 最初の数字はプール内で使用可能な IQN 接尾辞の数であり、2 番目の数字はプール内の接尾辞の合計数です。 この Cisco UCS ドメインが Cisco UCS Central に登録されている場合、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[Create IQN Suffix Pool] リンク	Cisco UCS ドメイン内のすべてのオブジェクト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 イニシエータの名前を定義する正規表現。 次の特殊文字を含め、最大 223 文字の英数字を指定できます。 • .（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、次のいずれかの選択を変更します。

オプション	説明
[Select]（デフォルトで使用される DHCP）	システムは、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 アドレスは、この領域に入力された情報に基づいて iSCSI ブートの vNIC に割り当てられます。 ステップ 12 に進みます。
Pool	IPv4 アドレスは管理 IP アドレスのプールから iSCSI ブートの 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] を選択している場合は、次のフィールドを入力または変更します。

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には、[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。
[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。
[Primary DNS] フィールド	プライマリ DNS サーバ アドレス。
[Secondary DNS] フィールド	セカンダリ DNS サーバ 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	システムは、設定する必要があるスタティック ターゲット インターフェイスを作成します。 ステップ 14 に進みます。

オプション	説明
iSCSI Auto Target Interface	システムは自動ターゲット インターフェイスを作成します。 自動ターゲットがイニシエータまたはDHCP ベンダー ID を使用するかを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] を選択している場合は、[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、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 ターゲットを選択して、[Modify] をクリックします。 続いて [Create iSCSI Static Target] ダイアログボックスで、次のフィールドに値を入力または変更する場合、次の手順を実行します。

名前	説明
[iSCSI Target Name] フィールド	iSCSI ターゲットの iSCSI Qualified Name（IQN）または Extended Unique Identifier（EUI）の名前を定義する正規表現。 英数字のほかに、次の特殊文字も使用できます。 • .（ピリオド） • :（コロン） • -（ダッシュ） **重要** この名前は、標準IQN またはEUI のガイドラインを使用して、適切にフォーマットされている必要があります。 次の例は、適切にフォーマット設定された iSCSI ターゲット名を示しています。 • 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	iSCSI ターゲット用にシステムによって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。

名前	説明
[Authentication Profile] ドロップダウン リスト	関連付けられている認証プロファイルの名前。
[Create iSCSI Authentication Profile] リンク	すべての iSCSI vNIC に使用可能な新しい認証プロファイル ポリシーを作成するには、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 ID。

- 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 個の iSCSI スタティック ターゲットがあり、最優先ターゲットを削除すると、2 番目の優先目標は、Cisco UCS Managerは引き続き第 2 優先目標を示していますが、最初のプライオリティのターゲットになります。

ステップ 15 [iSCSI Auto Target Interface] を選択している場合は、[DHCP Vendor Id] フィールドのイニシエータ名または DHCP ベンダー ID にエントリを変更します。 イニシエータがすでに設定されている必要があります。 ベンダー ID には、最大 32 文字の英数字を使用できます。

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 ドメインの iSCSI vNIC によってイニシエータ ID として使用する iSCSI Qualified Name（IQN）の集合です。

IQN プール メンバの形式は、*prefix*:*suffix*:*number* で、それぞれプレフィックス、サフィックス、数値のブロック（範囲）を指定できます。

IQN プールには、数の範囲とサフィックスが異なり、同じプレフィックスを共有する複数の IQN ブロックを含めることができます。

IQN プールの作成

（注） 大部分の場合、IQN の最大サイズ（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 のサイズを 128 文字に制限する必要があります。

手順

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

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

ステップ 3 プールを作成する組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [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、次のフィールドに入力します。

名前	説明
[Name] フィールド	iSCSI Qualified Name（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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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。`（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）を除く文字やスペースを使用できます。
[Prefix] フィールド	このプール用に作成された IQN ブロックのプレフィックス。 1～150 文字まで入力できます。 文字または数字のほかに、.（ピリオド）、:（コロン）、および -（ハイフン）などの特殊文字も使用できます。 たとえば、iqn1.alpha.com を使用できます。
[Assignment Order] フィールド	次のいずれかになります。 • [Default]：Cisco UCS Manager はプールからランダム ID を選択します。 • [Sequential]：Cisco UCS Manager はプールから最も小さい使用可能 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	このブロックの iSCSI Qualified Names（IQN）の接尾辞。 1～64 文字まで入力できます。 文字または数字のほかに、.（ピリオド）、:（コロン）、および -（ハイフン）などの特殊文字も使用できます。 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の数。
[Size] フィールド	ブロック内の接頭辞の数。

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。

次の作業

IQN 接尾辞プールをサービス プロファイルまたはテンプレートのいずれか一方、または両方に含めます。

IQN プールへのブロックの追加

手順

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

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

ステップ 3 プールが格納さ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 [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	このブロックの iSCSI Qualified Names（IQN）の接尾辞。 1～64 文字まで入力できます。 文字または数字のほかに、.（ピリオド）、:（コロン）、および -（ハイフン）などの特殊文字も使用できます。 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の数。

名前	説明
[Size] フィールド	ブロック内の接頭辞の数。

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 vNIC または vHBA に割り当てられているブロック内のどのアドレスも再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたブロックからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

ステップ 3 プールが格納さ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 [IQN Pools] ノードを展開します。

ステップ 5 IQN サフィックス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] ペインの [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て [Delete] を選択します。

ステップ 8 削除を確定するには、[はい（Yes）] をクリックします。

ステップ 9 [Save Changes] をクリックします。

IQN プールの削除

プールを削除すると、Cisco UCS Manager は vNIC または vHBA に割り当てられたアドレスをプールから再割り当てしません。 次のいずれかの条件が満たされるまで、削除されたプールからのすべての割り当て済みアドレスは、それらが割り当てられた 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 vHBA または vNIC が削除される。
- vNIC または vHBA が別のプールに割り当てられる。

手順

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

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

ステップ 3 プールが格納さ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 [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、[Delete] を選択します。

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

LAN ブート

LAN の集中型プロビジョニング サーバから 1 つ以上のサーバを起動するようにブート ポリシーを設定できます。 その LAN サーバから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ため、LAN（または PXE）ブートが頻繁に使用されます。

複数のタイプのブート デバイスを LAN ブート ポリシーに追加できます。 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 ブートまたは仮想メディア ブートを追加できます。

ブート ポリシーに対する LAN 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。 ただし、iSCSI ブートを除き、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めることができるグローバルなブート ポリシーを作成することをお勧めします。

複数のタイプのブート デバイスをブート ポリシーに追加できます。 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 ブートまたは仮想メディア 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, （518 ページ）から直接続行されます。

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 次のいずれかを実行します。

- [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。

次の作業

ブート ポリシーはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

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 ディスク ブート

サーバにローカル ドライブがある場合は、そのドライブからサーバを起動するようにブート ポリシーを設定できます。

（注） Cisco UCS Manager では、ローカル ドライブのタイプを区別しません。 オペレーティング システムが複数のローカル ドライブにインストールされている場合や内蔵USB ドライブ（eUSB）にインストールされている場合、サーバがブート ドライブとしてどのローカル ドライブを使用するのか指定できません。

ブート ポリシーに対するローカル 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。 ただし、iSCSI ブートを除き、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めることができるグローバルなブート ポリシーを作成することをお勧めします。

複数のタイプのブート デバイスをブート ポリシーに追加できます。 たとえば、セカンダリ ブート デバイスとして、仮想メディア 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, （518 ページ）から直接続行されます。

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 [Boot Order] テーブルにデバイスを追加するには、[Add Local Disk] をクリックします。

ステップ 3 次のいずれかを実行します。

- [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。

次の作業

ブートポリシーはサービスプロファイルとテンプレートのうち一方、または両方にインクルードします。

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。

仮想メディア ブート

サーバからアクセスできる仮想メディア デバイスから 1 つ以上のサーバを起動するようにブート ポリシーを設定できます。 仮想メディア デバイスは、サーバへの物理 CD-ROM 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）の挿入を模倣します。 このタイプのサーバのブートは、通常、オペレーティング システムをサーバに手動でインストールするために使用されます。

ブート ポリシーに対する仮想メディア 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。 ただし、iSCSI ブートを除き、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めることができるグローバルなブート ポリシーを作成することをお勧めします。

複数のタイプのブート デバイスをブート ポリシーに追加できます。 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 ブートを追加できます。

（注） 仮想メディアでは、USB をイネーブルにする必要があります。 USB 機能に影響を及ぼす BIOS 設定を変更すると、仮想メディアにも影響を及ぼします。 このため、最良のパフォーマンスを得るために、次の USB BIOS デフォルトは変更しないことを推奨します。

- [Make Device Non Bootable]：[disabled] に設定
- [USB Idle Power Optimizing Setting]：[high-performance] に設定

この手順は、ブート ポリシーの作成, （518 ページ）から直接続行されます。

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-ROM
- Add Floppy

ステップ 3 次のいずれかを実行します。

- [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。

次の作業

ブート ポリシーはサービス プロファイルとテンプレートのうち一方、または両方にインクルードします。

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 ポリシーの削除

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

第 32 章

サービス プロファイルの更新の展開の延期

この章の内容は、次のとおりです。

- サービス プロファイルの延期展開，553 ページ
- スケジュールの設定，556 ページ
- メンテナンス ポリシーの設定，569 ページ
- 保留中のアクティビティの管理，572 ページ

サービス プロファイルの延期展開

一部のサービス プロファイルまたは更新中のサービス プロファイル テンプレートへの変更が中断し、サーバのリブートが必要になることがあります。 ただし、これらの中断を伴う設定変更が行われたときに、延期展開を制御するように設定することができます。 たとえば、サービスプロファイルの変更をすぐに展開するか、または指定されたメンテナンス時間帯に展開させるかを選択することができます。 サービスプロファイルの延期展開に明示的なユーザの受信が必要かどうかも選択できます。

延期展開は、サーバとサービス プロファイルのアソシエーションによって発生するすべての設定変更に使用できます。 これらの設定変更は、サービス プロファイル、サービス プロファイルに含まれているポリシー、または更新中のサービスプロファイルテンプレートへの変更によって発生する可能性があります。 たとえば、サーバ BIOS、RAID コントローラ、ホスト HBA、ネットワーク アダプタなどのホスト ファームウェア パッケージおよび管理ファームウェア パッケージによって、ファームウェアのアップグレードとアクティベーションを延期できます。 ただし、Cisco UCS Manager、ファブリック インターコネクト、I/O モジュールなどの、ファームウェア パッケージのいずれも使用していないコンポーネントのファームウェア イメージの直接展開を延期することはできません。

延期展開は、サーバのリブートが必要な次の操作では使用できません。

- サーバとサービス プロファイルとの最初のアソシエーション
- サービス プロファイルと別のサーバとのアソシエーションを伴わない、現在のサーバとサービス プロファイルとの最終的なアソシエーションの解除

- サーバの稼働停止
- サーバの再確認
- サーバのリセット

サービス プロファイルの変更の展開を延期する場合は、1 つまたは複数のメンテナンス ポリシーを設定し、1 つのメンテナンス ポリシーを使用して各サービス プロファイルを設定する必要があります。 展開が発生する必要がある期間を定義する場合は、1 回以上繰り返すオカレンス、または 1 回のオカレンスのあるスケジュールを少なくとも 1 つ作成し、そのスケジュールをメンテナンス ポリシーに含める必要もあります。

延期展開スケジュール

1 つのスケジュールには、一連のオカレンスが含まれます。 これらのオカレンスは 1 回だけであるか、毎週指定の日時に繰り返されます。 オカレンスの時間や実行するタスクの最大数など、オカレンスに定義済みのオプションで、サービス プロファイルの変更を展開するかが決まります。 たとえば、時間またはタスクが最大数に達したため、特定のメンテナンス時間帯に変更を展開できない場合、その展開は次のメンテナンス時間帯に継承されます。

各スケジュールでは、Cisco UCS ドメインが 1 つまたは複数のメンテナンス時間帯を入力したかどうかを定期的に確認します。 入力されている場合は、スケジュールはメンテナンスポリシーで指定された制約に従って適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間帯を決定する 1 つ以上のオカレンスが含まれています。 オカレンスは次のいずれかになります。

1 回のオカレンス

1 回のオカレンスは、単一のメンテナンス時間帯を定義します。 この時間帯は、時間帯の最大時間または時間帯で実行できるタスクの最大数に達するまで続行されます。

繰り返すオカレンス

繰り返すオカレンスは、一連のメンテナンス時間帯を定義します。 この時間帯は、タスクの最大数またはオカレンスで指定された日の終わりに達するまで続行されます。

メンテナンス ポリシー

サーバに関連付けられているサービス プロファイル、または 1 つ以上のサービス プロファイルにバインドされる更新中のサービス プロファイルに対して、サーバのリブートが必要な変更が行われた場合、Cisco UCS Manager がどのように応答するかについて、メンテナンス ポリシーで指定されます。

メンテナンス ポリシーは、Cisco UCS Manager がサービス プロファイルの変更を展開する方法を指定します。 展開は、次のいずれかの方法で発生します。

- 即時
- admin 権限を持つユーザによって検証された場合

- スケジュールで指定された時刻に自動で

スケジュールされたメンテナンス時間中に変更を展開するために保守ポリシーが設定されている場合は、有効なポリシースケジュールを含める必要があります。 スケジュールは、使用可能な最初のメンテナンス時間帯で変更を展開します。

保留中のアクティビティ

Cisco UCS ドメインに延期展開を設定する場合、Cisco UCS Manager によって、保留中のすべてのアクティビティを表示することができます。 ユーザの確認応答を待つアクティビティと予定されたアクティビティが表示されます。

Cisco UCS ドメインに保留中のアクティビティがある場合、Cisco UCS Manager GUI はログイン時に admin 権限を使用してユーザに通知します。

Cisco UCS Manager は、保留中のすべてのアクティビティについて次のような情報を表示します。

- 展開されサーバと関連付けられたサービス プロファイルの名前
- 展開の影響を受けるサーバ
- 展開による中断
- 展開によって実行される変更

（注） 保留中の特定のアクティビティがサーバに適用されるメンテナンス時間帯は指定できません。 メンテナンス時間帯は、保留中のアクティビティの数と、サービス プロファイルに割り当てられているメンテナンス ポリシーによって異なります。 ただし、admin 権限を持つすべてのユーザは、保留中のアクティビティがユーザによる確認またはメンテナンス時間帯を待機するかどうかにかかわらず、保留中のアクティビティを手動で開始してすぐにサーバをリブートすることができます。

延期展開の注意事項および制限事項

サービス プロファイルまたはサービス プロファイル テンプレートに対する変更はすべて取り消しできません

保留中の変更をキャンセルする場合、Cisco UCS Manager は、サーバを再起動しなくても、変更をロールバックしようとします。 ただし、複雑な変更を行った場合、変更をロールバックするため、Cisco UCS Manager でサーバのリブートがもう一度必要な場合があります。 たとえば、vNIC を削除すると、Cisco UCS Manager は、サービス プロファイルに含まれているメンテナンス ポリシーに従ってサーバをリブートします。 サービス プロファイルの元の vNIC を復元してもこのリブートと変更は取り消せません。 代わりに、Cisco UCS Manager はサーバの 2 度目の展開とリブートをスケジュールします。

サービス プロファイルのアソシエーションが、メンテナンス時間帯の境界を超えてもかまいません

Cisco UCS Manager がサービス プロファイルのアソシエーションを開始すると、スケジューラとメンテナンス ポリシーには手順へのコントロールがなくなります。 サービス プロファイルのアソシエーションが割り当てられたメンテナンス時間帯で完了しない場合、プロセスが完了するまで続行されます。 たとえば、再試行されるステージやそのほかの問題が原因で、アソシエーションが時間内に完了しない場合にこの状況が発生することがあります。

保留中のアクティビティの実行順序を指定できません

予定されている展開は同時かつ別個に実行されます。 展開が実行される順序は指定できません。あるサービスプロファイルの展開を、別のサービスプロファイルの完了に応じて行うことはできません。

保留中のアクティビティの部分的な展開を実行することはできません

Cisco UCS Manager は予定されているメンテナンス時間帯に、サービス プロファイルへのすべての変更を適用します。 サービスプロファイルに対して同時に複数の変更を行うことはできないため、この変更は複数のメンテナンス時間帯に分けて行われます。 Cisco UCS Manager がサービス プロファイルの変更を展開すると、データベースの最新の設定に合わせてサービス プロファイルを更新します。

スケジュールの設定

スケジュールの作成

手順

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

ステップ 2 [Servers] タブで [Schedules] を右クリックし、[Create Schedule] を選択します。

ステップ 3 [Create Schedule] ウィザードの [Identify Schedule] ページで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	スケジュールの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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	スケジュールの説明。 スケジュール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。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Owner] フィールド	スケジュールのオーナー。 次のいずれかになります。 • [Local]：このCisco UCS ドメインで設定されたスケジュールを Cisco UCS Manager が所有しています。 • [Pending Global]：Cisco UCS Manager がこのスケジュールを Cisco UCS Central に転送中です。 • [Global]：リモート サーバ上で設定されたスケジュールを Cisco UCS Central が所有しています。

ステップ 4 [Next] をクリックします。

ステップ 5 [One Time Occurrences] ページで次のいずれかをクリックします。

オプション	説明
Next	次のページに移動します。 このスケジュールに対して1回のオカレンスを作成しない場合はこのオプションを選択します。 このオプションを選択した場合は、ステップ 8 に進みます。
Add	[Create a One Time Occurrence] ダイアログボックスで、このスケジュールを実行する 1 回の時間を指定します。 このオプションを選択した場合は、ステップ 6 に進みます。

ステップ 6 （任意） [Create a One Time Occurrence] 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
[Name] フィールド	このスケジュールの 1 回のオカレンスの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

名前	説明
[Start Time] フィールド	オカレンスが実行される日時。 フィールドの終端にある下矢印をクリックして、カレンダーから開始日を選択します。

b) 下矢印をクリックして [Options] 領域を展開します。

c) [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	スケジュールされたオカレンスを実行できる最大時間長。 次のいずれかになります。 • [None]：オカレンスは、すべてのタスクが完了するまで実行されます。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、オカレンスを実行できる最大時間長を指定できます。 Cisco UCS は、指定された時間内にできるだけ多くのスケジュールされたタスクを完了します。 デフォルトでは、最大期間は [none] に設定されています。 この設定を変更せず、タスクの最大数を設定しない場合は、保留中のすべてのアクティビティが完了するまでメンテナンスウィンドウが続行されます。
[Max Number of Tasks] フィールド	このオカレンス中に実行可能なスケジュールされたタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、スケジュールされたタスクが [Max Duration] フィールドで指定された最大時間を超えない限り、すべてのスケジュールされたタスクを実行します。 [Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンスウィンドウが続行されます。 • [other]：Cisco UCS Manager GUI によってテキストフィールドが表示され、このオカレンス中に実行できるタスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。

名前	説明
[Max Number of Concurrent Tasks] フィールド	このオカレンス中に同時に実行可能なタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、システムが処理できる、できるだけ多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI によってテキスト フィールドが表示され、このオカレンス中に実行できる同時タスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。
[Minimum Interval Between Tasks] フィールド	新しいタスクを開始するまでシステムが待機する最小時間長。この設定は、同時タスクの最大数が None 以外の値に設定されている場合にだけ有効です。 次のいずれかになります。 • [None]：Cisco UCS は、次のタスクをできるだけ早く実行します。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、タスク間で Cisco UCS が待機する最小時間長を指定できます。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。

d) [OK] をクリックします。

ステップ 7 別の 1 回のオカレンスを追加するには、[Add] をクリックしてステップ 6 を繰り返します。 それ以外の場合は、[Next] をクリックします。

ステップ 8 （任意） [Recurring Occurrences] ページで、このスケジュールに対して繰り返すオカレンスを定義する場合は、[Add] をクリックします。

a) [Create a Recurring Occurrence] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	このスケジュールの繰り返すオカレンスの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Day] フィールド	Cisco UCS がこのスケジュールのオカレンスを実行する曜日。次のいずれかになります。 • every day • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday • odd days • even days
[Hour] フィールド	スケジュールのこのオカレンスが開始される指定した曜日の時刻。 0 ～ 24 の整数を入力します。0 と 24 は両方とも深夜を意味しています。 （注） Cisco UCS は、最大期間に到達していない場合でも、その日に開始されたすべての繰り返すオカレンスをその日に終了します。 たとえば、開始時刻を 11 p.m に指定して最大期間を 3 時間に設定すると、Cisco UCS は 11 p.m にオカレンスを開始しますが、59 分後の 11:59 p.m に それを終了します。 繰り返すオカレンスが 11:59 p.m よりも前に完了するように、早めに開始時刻を指定してください。
[Minute] フィールド	スケジュール オカレンスを開始する時間（分単位）。 0 ～ 60 の整数を入力できます。

b) 下矢印をクリックして [Options] 領域を展開します。
c) [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	このスケジュールの各オカレンスを実行できる最大時間長。次のいずれかになります。 • [None]：オカレンスは、すべてのタスクが完了するまで実行されます。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、オカレンスを実行できる最大時間長を指定できます。 Cisco UCS は、指定された時間内にできるだけ多くのスケジュールされたタスクを完了します。
[Max Number of Tasks] フィールド	各オカレンス中に実行可能なスケジュールされたタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、スケジュールされたタスクが [Max Duration] フィールドで指定された最大時間を超えない限り、すべてのスケジュールされたタスクを実行します。 [Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続行されます。 • [other]：Cisco UCS Manager GUI によってテキスト フィールドが表示され、このオカレンス中に実行できるタスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。
[Max Number of Concurrent Tasks] フィールド	各オカレンス中に同時に実行可能なタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、システムが処理できる、できるだけ多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI によってテキスト フィールドが表示され、このオカレンス中に実行できる同時タスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。

名前	説明
[Minimum Interval Between Tasks] フィールド	新しいタスクを開始するまでシステムが待機する最小時間長。この設定は、同時タスクの最大数が None 以外の値に設定されている場合にだけ有効です。 次のいずれかになります。 • [None]：Cisco UCS は、次のタスクをできるだけ早く実行します。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、タスク間で Cisco UCS が待機する最小時間長を指定できます。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。

d) [OK] をクリックします。
e) 別の繰り返すオカレンスを追加するには、[Add] をクリックしてこのステップを繰り返します。

ステップ 9 [Finish] をクリックします。

スケジュールに対する 1 回のオカレンスの作成

（注） デフォルトでは、タスクの最大時間と最大数は none に設定されています。 これらのデフォルトをいずれも変更しない場合、Cisco UCS Manager はメンテナンス期間が継続する時間の長さに制限を課しません。 保留中のすべてのアクティビティは、スケジュール設定されたメンテナンス期間が始まるとすぐに適用され、Cisco UCS Manager はこれらのすべてのタスクが完了するまで、保留中のアクティビティによって影響を受けるサーバをリブートし続けます。

手順

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

ステップ 2 [Servers] タブで、[Schedules] を展開します。

ステップ 3 オカレンスの追加先であるスケジュールを右クリックして [Create a One Time Occurrence] を選択します。

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

名前	説明
[Name] フィールド	このスケジュールの 1 回のオカレンスの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Start Time] フィールド	オカレンスが実行される日時。 フィールドの終端にある下矢印をクリックして、カレンダーから開始日を選択します。

ステップ 5 下矢印をクリックして [Options] 領域を展開します。

ステップ 6 [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	スケジュールされたオカレンスを実行できる最大時間長。 次のいずれかになります。 • [None]：オカレンスは、すべてのタスクが完了するまで実行されます。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、オカレンスを実行できる最大時間長を指定できます。 Cisco UCS は、指定された時間内にできるだけ多くのスケジュールされたタスクを完了します。 デフォルトでは、最大期間は [none] に設定されています。 この設定を変更せず、タスクの最大数を設定しない場合は、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続行されます。

名前	説明
[Max Number of Tasks] フィールド	このオカレンス中に実行可能なスケジュールされたタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、スケジュールされたタスクが [Max Duration] フィールドで指定された最大時間を超えない限り、すべてのスケジュールされたタスクを実行します。 [Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続行されます。 • [other]：Cisco UCS Manager GUI によってテキスト フィールドが表示され、このオカレンス中に実行できるタスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。
[Max Number of Concurrent Tasks] フィールド	このオカレンス中に同時に実行可能なタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、システムが処理できる、できるだけ多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI によってテキスト フィールドが表示され、このオカレンス中に実行できる同時タスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。
[Minimum Interval Between Tasks] フィールド	新しいタスクを開始するまでシステムが待機する最小時間長。 この設定は、同時タスクの最大数が None 以外の値に設定されている場合にだけ有効です。 次のいずれかになります。 • [None]：Cisco UCS は、次のタスクをできるだけ早く実行します。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、タスク間で Cisco UCS が待機する最小時間長を指定できます。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。

ステップ 7 [OK] をクリックします。

スケジュールに対する繰り返すオカレンスの作成

手順

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

ステップ 2 [Servers] タブで、[Schedules] を展開します。

ステップ 3 オカレンスの追加先であるスケジュールを右クリックして [Create a Recurring Occurrence] を選択します。

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

名前	説明
[Name] フィールド	このスケジュールの繰り返すオカレンスの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Day] フィールド	Cisco UCS がこのスケジュールのオカレンスを実行する曜日。次のいずれかになります。 • every day • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday • odd days • even days

名前	説明
[Hour] フィールド	スケジュールのこのオカレンスが開始される指定した曜日の時刻。 0 ～ 24 の整数を入力します。0 と 24 は両方とも深夜を意味しています。 （注） Cisco UCS は、最大期間に到達していない場合でも、その日に開始されたすべての繰り返すオカレンスをその日に終了します。 たとえば、開始時刻を 11 p.m に指定して 最大期間を 3 時間に設定すると、Cisco UCS は 11 p.m にオカレンスを開始しますが、 59 分後の 11:59 p.m に それを終了します。 繰り返すオカレンスが 11:59 p.m よりも前に完了するように、早めに開始時刻を指定してください。
[Minute] フィールド	スケジュール オカレンスを開始する時間（分単位）。 0 ～ 60 の整数を入力できます。

ステップ 5 下矢印をクリックして [Options] 領域を展開します。

ステップ 6 [Options] 領域で、次のフィールドに値を入力します。

名前	説明
[Max Duration] フィールド	このスケジュールの各オカレンスを実行できる最大時間長。 次のいずれかになります。 • [None]：オカレンスは、すべてのタスクが完了するまで実行されます。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、オカレンスを実行できる最大時間長を指定できます。 Cisco UCS は、指定された時間内にできるだけ多くのスケジュールされたタスクを完了します。

名前	説明
[Max Number of Tasks] フィールド	各オカレンス中に実行可能なスケジュールされたタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、スケジュールされたタスクが [Max Duration] フィールドで指定された最大時間を超えない限り、すべてのスケジュールされたタスクを実行します。 [Max Duration] が [none] に設定されている場合にこのオプションを選択すると、保留中のすべてのアクティビティが完了するまでメンテナンス ウィンドウが続行されます。 • [other]：Cisco UCS Manager GUI によってテキスト フィールドが表示され、このオカレンス中に実行できるタスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。
[Max Number of Concurrent Tasks] フィールド	各オカレンス中に同時に実行可能なタスクの最大数。 次のいずれかになります。 • [Unlimited]：Cisco UCS は、システムが処理できる、できるだけ多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI によってテキスト フィールドが表示され、このオカレンス中に実行できる同時タスクの最大数を指定できます。 1 ～ 65535 の整数を入力します。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。
[Minimum Interval Between Tasks] フィールド	新しいタスクを開始するまでシステムが待機する最小時間長。この設定は、同時タスクの最大数が None 以外の値に設定されている場合にだけ有効です。 次のいずれかになります。 • [None]：Cisco UCS は、次のタスクをできるだけ早く実行します。 • [other]：Cisco UCS Manager GUI によって [dd:hh:mm:ss] フィールドが表示され、タスク間で Cisco UCS が待機する最小時間長を指定できます。 （注） このオプションは、このスケジュールがエラー抑制タスクと関連付けられている場合は適用されません。

ステップ 7 [OK] をクリックします。

スケジュールからの 1 回のオカレンスの削除

これがスケジュール内の唯一のオカレンスである場合は、オカレンスなしでスケジュールが再設定されます。 スケジュールがメンテナンスポリシーに含まれ、そのポリシーがサービスプロファイルに割り当てられている場合、サービスプロファイルに関連付けられたサーバに関連するすべての保留中のアクティビティは展開できません。 保留中のアクティビティを展開するには、1 回のオカレンスまたは繰り返すオカレンスをスケジュールに追加する必要があります。

手順

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

ステップ 2 [Servers] タブで、[Schedules] > [*Schedule_Name*] を展開します。

ステップ 3 [One Time Occurrences] を展開します。

ステップ 4 削除するオカレンスを右クリックし、[Delete] を選択します。

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

スケジュールからの繰り返すオカレンスの削除

これがスケジュール内の唯一のオカレンスである場合は、オカレンスなしでスケジュールが再設定されます。 スケジュールがメンテナンスポリシーに含まれ、そのポリシーがサービスプロファイルに割り当てられている場合、サービスプロファイルに関連付けられたサーバに関連するすべての保留中のアクティビティは展開できません。 保留中のアクティビティを展開するには、1 回のオカレンスまたは繰り返すオカレンスをスケジュールに追加する必要があります。

手順

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

ステップ 2 [Servers] タブで、[Schedules] > [*Schedule_Name*] を展開します。

ステップ 3 [Recurring Occurrences] を展開します。

ステップ 4 削除するオカレンスを右クリックし、[Delete] を選択します。

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

スケジュールの削除

このスケジュールがメンテナンス ポリシーに含まれている場合、ポリシーはスケジュールなしで再構成されます。 そのポリシーがサービス プロファイルに割り当てられている場合、サービス プロファイルに関連付けられたサーバに関連するすべての保留アクティビティは展開できません。保留中のアクティビティを展開するには、メンテナンス ポリシーにスケジュールを追加する必要があります。

手順

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

ステップ 2 [Servers] タブで、[Schedules] を展開します。

ステップ 3 削除するスケジュールを右クリックし、[Delete] を選択します。

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

メンテナンス ポリシーの設定

メンテナンス ポリシーの作成

はじめる前に

自動延期展開にこのメンテナンス ポリシーを設定する場合は、スケジュールを作成します。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 [Maintenance Policies] を右クリックし、[Create Maintenance Policy] を選択します。

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

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Reboot Policy] フィールド	サービスプロファイルがサーバに関連付けられているか、サーバにすでに関連付けられているサービスプロファイルに変更を加えた場合、プロセスを完了するには、サーバをリブートする必要があります。[Reboot Policy] フィールドは、このメンテナンス ポリシーを含むサービス プロファイルに関連付けられたサーバについて、リブートがいつ行われるかを決定します。次のいずれかになります。 • [Immediate]：サービス プロファイルのアソシエーションが完了するか、サービス プロファイルの変更がユーザによって保存されるとすぐに、サーバが自動的にリブートされます。 • [User Ack]：ユーザがサービス プロファイルのアソシエーションが完了するか、または変更を行うと、サーバを手動で再起動する必要があります。 • [Timer Automatic]：Cisco UCS はすべてのサービス プロファイルのアソシエーションと変更を、[Schedule] フィールドに示されているスケジュールによって定義されたメンテナンス期間延長します。

名前	説明
[Schedule] ドロップダウン リスト	[Reboot Policy] が [Timer Automatic] に設定されている場合、スケジュールによってメンテナンス操作をサーバに適用できる時期が指定されます。 Cisco UCS はサーバをリブートし、スケジュール設定された時間にサービス プロファイルの変更を完了します。
[Create Schedule] リンク	このリンクをクリックすると、この Cisco UCS ドメイン内のすべてオブジェクトに使用できる新しいスケジュールが作成されます。

ステップ 6 [OK] をクリックします。

次の作業

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

メンテナンス ポリシーの削除

手順

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

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

ステップ 3 [Maintenance Policies] を展開します。

ステップ 4 削除するメンテナンス ポリシーを右クリックし、[Delete] を選択します。

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

保留中のアクティビティの管理

保留中のアクティビティの表示

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 次のいずれかのタブをクリックします。

- [User Acknowledged Activities]：完了する前にユーザの確認を必要とするタスクを表示する [Service Profiles] タブおよび [Fabric Interconnects] タブが含まれています。
- [Scheduled Activities]：関連付けられているメンテナンス スケジュールに基づいて実行されるタスクを表示します。

ステップ 3 保留中のアクティビティの詳細を表示するには、テーブルの行をクリックします。
[Server] カラムのリンクをクリックすると、Cisco UCS Manager にそのサーバのプロパティが表示されます。

ユーザによる確認を待機しているサービス プロファイル変更の展開

重要 保留中のアクティビティを確認した後で、影響を受けるサーバの Cisco UCS Manager によるリブートを停止することはできません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスで、[User Acknowledged Activities] タブをクリックします。

ステップ 3 テーブルの [Reboot Now] カラムで、すぐに展開する保留中のアクティビティの [Acknowledge All] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。
Cisco UCS Manager は、保留中のアクティビティの影響を受けるサーバをすぐにリブートします。

ユーザによる確認を待機しているすべてのサービス プロファイル変更の展開

重要 保留中のアクティビティを確認した後で、影響を受けるサーバの Cisco UCS Manager によるリブートを停止することはできません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスで、[User Acknowledged Activities] タブをクリックします。

ステップ 3 ツールバーの [Acknowledge All] チェックボックスをオンにします。
Cisco UCS Manager GUI は、テーブルに記載されている保留中のアクティビティについて [Reboot Now] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。
Cisco UCS Manager は、テーブルにリストされている保留中のアクティビティの影響を受けるすべてのサーバをすぐにリブートします。

予定されたサービス プロファイルの変更を即座に展開する

重要 保留中のアクティビティを確認した後で、影響を受けるサーバの Cisco UCS Manager によるリブートを停止することはできません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスで、[Scheduled Activities] タブをクリックします。

ステップ 3 テーブルの [Reboot Now] カラムで、すぐに展開する保留中のアクティビティの [Acknowledge All] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。
Cisco UCS Manager は、保留中のアクティビティの影響を受けるサーバをすぐにリブートします。

予定されたすべてのサービス プロファイルの変更を即座に展開する

重要 保留中のアクティビティを確認した後で、影響を受けるサーバの Cisco UCS Manager によるリブートを停止することはできません。

手順

ステップ 1 ツールバーの [Pending Activities] をクリックします。

ステップ 2 [Pending Activities] ダイアログボックスで、[Scheduled Activities] タブをクリックします。

ステップ 3 ツールバーの [Acknowledge All] チェックボックスをオンにします。
Cisco UCS Manager GUI は、テーブルに記載されている保留中のアクティビティについて [Reboot Now] チェックボックスをオンにします。

ステップ 4 [OK] をクリックします。
Cisco UCS Manager は、テーブルにリストされている保留中のアクティビティの影響を受けるすべてのサーバをすぐにリブートします。

第 33 章

サービス プロファイルの設定

この章の内容は、次のとおりです.

- サーバ ID を上書きするサービス プロファイル，575 ページ
- サーバ ID を継承するサービス プロファイル，576 ページ
- サービス プロファイル テンプレート，577 ページ
- サービス プロファイルの注意事項および推奨事項，577 ページ
- サービス プロファイルの作成，578 ページ
- サービス プロファイル テンプレートの操作，620 ページ
- サービス プロファイルの管理，658 ページ
- サービス プロファイル テンプレートの管理，680 ページ

サーバ 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。 このプロファイルを使用すると、関連付けの時点でサーバにある ID の値を上書きし、Cisco UCS Manager のリソース プールとポリシー設定を使用して管理タスクの一部を自動化できます。

このサービス プロファイルとサーバの関連付けを解除して、このプロファイルを別のサーバ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 プール ポリシーを通じて行うこともできます。 新しいサーバのハードウェアが持つ UUID や MAC アドレスなどの工場出荷時の設定は、サービス プロファイルの設定で上書きされます。 その結果、サーバでの変更はネットワークには透過的に行われます。 新しいサーバ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、サーバプールの資格ポリシー、または個々のハードウェア設定を必要とする別のポリシーが含まれている場合、プロファイルは、Cisco UCS ドメインで、任意のタイプのサーバを使用できます。

これらのサービス プロファイルは、ラックマウント サーバまたはブレード サーバと関連付けることができます。 サービス プロファイルを移行する機能は、サービス プロファイルの移行の制限を選択するかどうかにより異なります。

（注） 移行を制限しない場合は、既存のサービス プロファイルを移行する前に、Cisco UCS Manager による新規サーバに対する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 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、サーバのデフォルト値を使用して、ラックマウント型サーバの管理を模倣します。 このプロファイルは特定のサーバに結び付けられており、別のサーバへの移動または移行はできません。

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
- サーバの UUID

重要 このプロファイルをサーバに関連付ける前に、製造元でサーバ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 テンプレート

サービス プロファイル テンプレートにより、同一の基本パラメータ（vNIC および vHBA の数など）や、同じプールから取得された ID 情報が含まれる複数のサービス プロファイルを迅速に作成できます。

ヒント　既存のサービス プロファイルに類似した値が含まれるサービス プロファイルが 1 つだけ必要な場合は、Cisco UCS Manager GUI でサービス プロファイルのクローニングが可能です。

たとえば、サーバをホストデータベース ソフトウェアに設定するために同様の値が含まれた複数のサービスプロファイルが必要な場合は、手作業でも既存のサービスプロファイルからでもサービス プロファイル テンプレートを作成できます。 次に、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。 しかし、プロファイルの作成後は、テンプレートへの接続が失われます。 このテンプレートから作成された 1 つ以上のプロファイルを変更する必要がある場合は、これらのプロファイルを個別に変更する必要があります。

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 プロファイルでは、テンプレートのすべてのプロパティが継承され、テンプレートへのつながりが保持されます。 テンプレートの何らかの変更があると、テンプレートから作成されたサービス プロファイルは自動的にアップデートされます。

サービス プロファイルの注意事項および推奨事項

ローカル ディスク設定ポリシーなどの、サービス プロファイルとサービス プロファイル テンプレートに含まれるポリシーとプールに固有な注意事項や推奨事項に加えて、サービス プロファイルとサーバを関連付ける機能に影響する次の注意事項と推奨事項に留意する必要があります。

ラックマウント サーバで設定できる vNIC 数の制限

Cisco UCS Manager と統合されるすべてのラックマウント サーバに、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アダプタについて、それぞれ最大 56 個の vNIC を設定できます。

ラックマウント サーバの電力制限のサポートなし

電力制限はラック サーバではサポートされません。ラックマウント サーバに関連付けられたサービス プロファイルに電力制御ポリシーを含めると、そのポリシーは設定されません。

サービス プロファイルの作成

[Expert] ウィザードを使用したサービス プロファイルの作成

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 [Create Service Profile (expert)] ウィザードで、次の手順を実行します。

- ページ 1：サービス プロファイルの識別 ，（578 ページ）
- ページ 2：ネットワーキング オプションの設定，（580 ページ）
- ページ 3：ストレージ オプションの設定，（588 ページ）
- ページ 4: ファイバ チャネルの [Zoning] オプションの設定，（595 ページ）
- ページ 5：vNIC/vHBA 配置の設定，（597 ページ）
- ページ 6：サーバのブート順序の設定，（602 ページ）
- ページ 7：メンテナンス ポリシーの追加，（607 ページ）
- ページ 8：サーバの割り当ての指定，（609 ページ）
- ページ 9：動作ポリシーの追加，（611 ページ）

ページ 1：サービス プロファイルの識別

この手順は、[Expert] ウィザードを使用したサービス プロファイルの作成，（578 ページ）に記載されているステップから直接続くものです。 [Create Service Profile (expert)] ウィザードの [Identify Service Profile] ページで、サービス プロファイルの ID を設定する方法について説明します。

手順

ステップ 1 [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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

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 2 [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 5 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 5 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 3 に進みます。

オプション	説明
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5に進みます。

ステップ 3 （任意） XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX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 4 （任意） このサービス プロファイルで使用するために新しい UUID サフィックス プールを作成する場合は、[Create UUID Suffix Pool] をクリックして [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, （432 ページ）を参照してください。

ステップ 5 （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。`（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）を除く文字やスペースを使用できます。

ステップ 6 [Next] をクリックします。

次の作業

ページ 2：ネットワーキング オプションの設定, （580 ページ）の手順を完了します。

ページ 2：ネットワーキング オプションの設定

この手順は、ページ 1：サービス プロファイルの識別 , （578 ページ）から直接続くものです。
[Create Service Profile (expert)] ウィザードの [Networking] ページで、LAN 接続を含むネットワーキング 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 （任意） ダイナミック vNIC をサポートするアダプタを備えたサーバにこのサービス プロファイルを割り当てる予定の場合、[Dynamic vNIC Connection] 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
[Select a Policy to use]	ダイナミック vNIC をサポートしないアダプタを備えるサーバには、ダイナミック vNIC 接続ポリシーなしでサービス プロファイルを作成できます。 このオプションでは、サービスプロファイルにダイナミック vNIC 接続ポリシーは含まれません。 iSCSI ブート用にこのサービス プロファイルまたはテンプレートを設定する場合は、このオプションを選択します。 ステップ 4 に進みます。
[Create a Specific Dynamic vNIC Connection Policy]	このサービス プロファイルだけがアクセスできるダイナミック vNIC 接続ポリシーを作成できます。 ステップ 2 に進みます。
[Dynamic vNIC Connection Policies] *Policy_Name*	ドロップダウン リストの最下部にあるリストから既存のダイナミック vNIC 接続ポリシーを選択します。 Cisco UCS Manager で、サービス プロファイルにこのポリシーが割り当てられます。 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、ステップ 3 に進みます。 それ以外の場合は、ステップ 4 に進みます。

ステップ 2 （任意） [Create a Specific Dynamic vNIC Connection Policy] をクリックした場合、このサービス プロファイルだけが使用できる新しいダイナミック vNIC 接続ポリシーを作成するには、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
[Number of Dynamic vNICs] フィールド	このポリシーの影響を受けるダイナミック vNIC の数。
[Adapter Policy] ドロップダウン リスト	このポリシーと関連付けられるアダプタ プロファイル。 すでに存在しているプロファイルだけが、このドロップダウン リストに表示されます。

名前	説明
[Protection] フィールド	ダイナミック vNIC は Cisco UCS で常に保護されますが、優先するファブリックがある場合はこのフィールドを使用してそれを選択することができます。 次のいずれかを選択できます。 • [Protected Pref A]：Cisco UCS はファブリック A を使用しようとしますが、必要に応じてファブリック B にフェールオーバーします。 • [Protected Pref B]：Cisco UCS はファブリック B を使用しようとしますが、必要に応じてファブリック A にフェールオーバーします。 • [Protected]：Cisco UCS は、使用可能であればどのファブリックでも使用します。

b) ステップ 4 に進みます。

ステップ 3 （任意） すべてのサービス プロファイルが使用できるダイナミック vNIC 接続ポリシーを作成するには、次の手順を実行します。

a) [Create Dynamic vNIC Connection Policy] をクリックします。

b) [Create Dynamic vNIC Connect Policy] ダイアログボックスで、フィールドに値を入力します。詳細については、『*Cisco UCS Manager VM-FEX for VMware GUI Configuration Guide*』を参照してください。

c) [OK] をクリックします。

d) [Dynamic vNIC Connection] ドロップダウン リストで、作成したポリシーを選択します。

e) ステップ 4 に進みます。

ステップ 4 [How would you like to configure LAN connectivity?] フィールドで、次のオプションのいずれかをクリックします。

オプション	説明
[Simple]	このサービス プロファイルに、デュアル ファブリック モードで最大 2 つの vNIC を作成できます。 ステップ 5 に進みます。
[Expert]	このサービス プロファイルに、vNIC を無制限に作成できます。 iSCSI ブート用にこのサービス プロファイルまたはテンプレートを設定する場合は、このオプションを選択します。 iSCSI ブート用にこのサービス プロファイルを設定する場合は、ステップ 7 に進みます。 そのほかすべての設定については、ステップ 6 に進みます。

オプション	説明
[No vNICs]	サービス プロファイルには、LAN 接続用の vNIC は含まれません。 このサービス プロファイルに関連付けられているサーバは、サービス プロファイルを変更して vNIC を追加する場合を除き、LAN と通信できません。 ステップ 9 に進みます。
[Hardware Inherited]	サーバに関連付けられたイーサネット アダプタ プロファイルに割り当てられた vNIC を使用します。 ステップ 9 に進みます。
[Use Connectivity Policy]	このサービスプロファイルに対して LAN 接続ポリシーを使用できるようにします。 ステップ 8 に進みます。 （注） 同じサービス プロファイルに、LAN 接続ポリシーと、ローカルで作成された vNIC を設定することはできません。 サービス プロファイルに LAN 接続ポリシーを追加すると、既存の vNIC 設定はすべて消去されます。

ステップ 5 （任意） シンプル LAN 接続オプションを選択した場合、次の手順を実行します。

a) [vNIC 0 (Fabric A)] 領域で、次のフィールドに値を入力します。

- [Name] フィールドに、vNIC の一意の名前を入力します。
- [Select Native VLAN] ドロップダウン リストで、この vNIC が通信する VLAN の名前を選択します。

必要な VLAN がドロップダウン リストに表示されない場合は、[Create VLAN] リンクをクリックします。 詳細については、ネームド VLAN の作成, （261 ページ）を参照してください。

b) この vNIC に VLAN を作成するには、[vNIC 1 (Fabric B)] 領域でステップ 2a を繰り返します。

c) ステップ 9 に進みます。

ステップ 6 エキスパート LAN 接続オプションを選択し、iSCSI ブート用にこのサービス プロファイルを設定していない場合、次の手順を実行します。

a) テーブルのアイコン バーで [Add] をクリックし、[Create vNICs] ダイアログボックスを開きます。

b) 次のフィールドに値を入力して、vNIC の ID 情報を指定します。

名前	説明
[Name] フィールド	この vNIC のユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vNIC Template] チェックボックス	テンプレートを使用して vNIC を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vNIC Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vNIC テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vNIC Template] リンク	vNIC テンプレートを作成する場合は、このリンクをクリックします。
[MAC Address Assignment] ドロップダウン リスト	項目 • デフォルトの MAC アドレス プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた MAC アドレスを使用する場合は、[Hardware Default] を選択します。 • 特定の MAC アドレスを使用する場合は、[02:25: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。

c) [Fabric Interconnect] 領域で、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC から第 2 のファブリック インターコネクトにアクセスできるようにする場合は、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックのフェールオーバーをイネーブルにしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のものにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバをこの vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。
[VLANs] テーブル	次の表には、この vNIC に関連付けることができる VLAN がリストされています。 各カラムの説明は次のとおりです。 • [Select]：使用する VLAN ごとに、このカラムのチェックボックスをオンにします。 • [Name]：VLAN の名前。 • [Native VLAN]：VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

名前	説明
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC にある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[Pin Group] ドロップダウン リスト	この vNIC と関連付ける LAN ピン グループを選択します。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト	この vNIC と関連付ける統計情報収集ポリシー。

d) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト	この vNIC と関連付けるイーサネット アダプタ ポリシー。
[Create Ethernet Adapter Policy] リンク	イーサネット アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC が関連付けられているダイナミック vNIC 接続ポリシー。
[Create Dynamic vNIC Connection Policy] リンク	ダイナミック vNIC 接続ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト	この vNIC と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	Quality Of Service ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Network Control Policy] ドロップダウン リスト	この vNIC と関連付けるネットワーク制御ポリシー。
[Create Network Control Policy Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。

e) [OK] をクリックします。
f) ステップ 9 に進みます。

ステップ 7 エキスパート LAN 接続オプションを選択し、iSCSI ブート用にこのサービス プロファイルを設定している場合、次の手順を実行します。

a) 下矢印をクリックして [iSCSI vNICs] バーを展開します。
b) テーブルのアイコン バーで [Add] をクリックし、[Create iSCSI vNIC] ダイアログボックスを開きます。
c) 次のフィールドに値を入力して、iSCSI vNIC の ID 情報を指定します。

名前	説明
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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（ある場合）。
[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（ある場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC に使用可能な新しい iSCSI アダプタ ポリシーを作成するには、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（ある場合）。 MAC アドレスが設定されていない場合、Cisco UCS Manager GUI には [Derived] が表示されます。
[MAC Pool] フィールド	この iSCSI vNIC に関連付けられた MAC プール（ある場合）。

名前	説明
[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（ある場合）。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 M82-8P 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 上のネイティブ 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、指定する VLAN はオーバーレイ vNIC に割り当てられたどの VLAN にすることもできます。

d) [OK] をクリックします。
e) 追加の iSCSI vNIC を設定するために、ステップ b から d を繰り返します。
f) ステップ 9 に進みます。

ステップ 8 [Use Connectivity Policy]を選択した場合、次の手順を実行します。

- 既存の LAN 接続ポリシーを使用するには、[LAN Connectivity Policy] ドロップダウン リストでそのポリシーを選択します。
- 既存の LAN 接続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 LAN Connectivity Policy] リンクをクリックし、フィールドに値を入力します。

LAN 接続のポリシーの詳細については、LAN 接続ポリシーの作成, （321 ページ）を参照してください。

ステップ 9 [Next] をクリックします。

次の作業

ページ 3：ストレージ オプションの設定, （588 ページ）を実行します。

ページ 3：ストレージ オプションの設定

この手順は、ページ 2：ネットワーキング オプションの設定, （580 ページ）から直接続くものです。 [Create Service Profile (expert)] ウィザードの [Storage] ページでサービス プロファイルのストレージ 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 [Local Storage] 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 Local Storage Policy to use]	このサービス プロファイルにデフォルトのローカル ディスク ストレージ ポリシーを割り当てます。 ステップ 4 に進みます。
[Create a Specific Storage 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 ディスク ポリシーを作成できます。 ステップ 2 に進みます。
[Storage Policies *Policy_Name]*	ドロップダウン リストの最下部にあるリストから既存のローカル ディスク 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。 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、ステップ 3 に進みます。 それ以外の場合は、ステップ 4 に進みます。

ステップ 2 （任意） [Create a Specific Storage Policy] を選択し、このサービス プロファイルだけが使用できる新しいポリシーを作成する場合は、次の手順を実行します。:

a) [Mode] ドロップダウン リストで、次のいずれかを選択します。

- [No Local Storage]：ディスクレス サーバまたは SAN 専用の設定で使用します。 このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0 Striped]：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] モードの適用後に違いがわからないことがあります。 これにより、ポリシー内の RAID 設定と、サーバの[Inventory] > [Storage] タブに表示される実際のディスク設定の間に不一致が生じる場合があります。

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。
- [RAID10 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。

（注） 一部の Cisco UCS サーバでは、特定の RAID 設定オプションにライセンスが必要です。 Cisco UCS Manager がこのローカル ディスク ポリシーを含むサービス プロファイルをサーバに関連付けると、Cisco UCS Manager は、選択した RAID オプションに適切なライセンスが付与されていることを確認します。 問題がある場合は、サービス プロファイルの関連付け中に Cisco UCS Manager によって設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。

b) サーバと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たい場合、[Protect Configuration] チェックボックス をオンにします。
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 Protect Configuration プロパティが優先され、前のサービス プロファイルの設定は上書きされます。

（注） このオプションがイネーブルの状態でサーバとサービス プロファイルの関連付けを解除した後、そのサーバに新しいサービス プロファイルを関連付け、そのサービス プロファイル内のローカル ディスク設定ポリシーに前とは異なるプロパティが含まれていると、サーバから設定不一致のエラーが返され、関連付けは失敗します。

c) ステップ 4 に進みます。

ステップ 3 （任意） すべてのサービス プロファイルが使用できるローカル ディスク設定ポリシーを作成するには、次の手順を実行します。

a) [Create Local Disk Configuration Policy] リンク をクリックします。
b) [Create Local Disk Configuration] 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。
詳細については、ローカルディスク設定ポリシーの作成, （479ページ）を参照してください。
c) [OK] をクリックします。
d) [Local Storage] ドロップダウン リストで、作成したポリシーを選択します。

ステップ 4 [How would you like to configure SAN storage?] フィールドで、次のオプションのいずれかをクリックします。

オプション	説明
[Simple]	このサービス プロファイルに、最大 2 つの vHBA を作成できます。 ステップ 5 に進みます。
[Expert]	このサービス プロファイルに、vHBA を無制限に作成できます。 ステップ 6 に進みます。
[No vHBAs]	サービス プロファイルには、ファイバ チャネル SAN 接続用の vHBA は含まれません。 iSCSI ブート用にこのサービス プロファイルまたはテンプレートを設定する場合は、このオプションを選択します。 ステップ 8 に進みます。
[Hardware Inherited]	サーバに関連付けられたファイバチャネルアダプタプロファイルに割り当てられた vHBA を使用します。 ステップ 8 に進みます。
[Use Connectivity Policy]	このサービスプロファイルに対して SAN 接続ポリシーを使用できるようにします。 ステップ 7 に進みます。 （注） 同じサービス プロファイルに、SAN 接続ポリシーと、ローカルで作成された vHBA を設定することはできません。 サービス プロファイルに SAN 接続ポリシーを追加すると、既存の vHBA 設定はすべて消去されます。

ステップ 5 （任意） シンプル SAN ストレージ オプションを選択した場合、次の手順を実行します。

a) [WWNN Assignment] ドロップダウン リストで、次のいずれかを選択します。

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

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

b) [vHBA 0 (Fabric A)] 領域で、次のフィールドに値を入力します。

- [Name] フィールドに、vHBA の一意の名前を入力します。
- [Select VSAN] ドロップダウン リストで、この vHBA を関連付ける VSAN の名前を選択します。

必要な VSAN がドロップダウン リストに表示されない場合は、[Create VSAN] リンクをクリックします。 詳細については、ネームド VSAN の作成, （362 ページ）を参照してください。

c) この vHBA に VSAN を作成するには、[vHBA 1 (Fabric B)] 領域でステップ 5b を繰り返します。

d) ステップ 8 に進みます。

ステップ 6 （任意） エキスパート SAN ストレージ オプションを選択した場合、次の手順を実行します。

a) [WWNN Assignment] ドロップダウン リストで、次のいずれかを選択します。

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

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

b) テーブルのアイコン バーで [Add] をクリックし、[Create vHBA] ダイアログボックスを開きます。

c) 次のフィールドに値を入力して、vHBA の ID 情報を指定します。

名前	説明
[Name] フィールド	この vHBA 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vHBA Template] チェックボックス	テンプレートを使用して vHBA を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vHBA Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vHBA テンプレートがシステムに存在する場合のみ、このオプションを選択できます。

名前	説明
[Create vHBA Template] リンク	vHBA テンプレートを作成する場合は、このリンクをクリックします。
[WWPN Assignment] ドロップダウン リスト	Cisco UCS が World Wide Port Node を vHBA に割り当てる方法。 Cisco UCS について、次のように設定します。 • デフォルトの WWPN プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた WWPN を使用する場合は、[Derived] を選択します。 • 特定の WWPN を使用する場合は、[20:00:00:25:B5:00:00:00]、[20:XX:XX:XX:XX:XX:XX:XX]、または [5X:XX:XX:XX:XX:XX:XX:XX] を選択し、使用する WWPN を [WWPN] フィールドに入力します。 WWPN が Cisco MDS ファイバ チャネル スイッチと互換性を持つようにするには、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • プール内の WWPN 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アドレスの数であり、2 番めの数字はそのプール内の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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[Create WWPN Pool] リンク	Cisco UCS ドメイン内のすべてのオブジェクトで使用可能な新しいWWPNプールを作成する場合は、このリンクをクリックします。

名前	説明
[WWPN] フィールド	[WWPN Assignment] ドロップダウン リストが手動テンプレートのいずれかに設定されている場合、手動で割り当てた WWPN。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN 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。

d) [VSAN] 領域で、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。
[Select VSAN] ドロップダウン リスト ボックス	この vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Pin Group] ドロップダウン リスト ボックス	この vHBA が関連付けられる SAN ピン グループ。
[Create SAN Pin Group] リンク	ピン グループを作成する場合は、このリンクをクリックします。
[Persistent Binding] フィールド	次のいずれかになります。 • Disabled • Enabled
[Max Data Field Size] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の範囲の整数を入力します。 デフォルトは 2048 です。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト ボックス	この vHBA と関連付ける統計しきい値ポリシー。

e) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト ボックス	この vHBA と関連付けるファイバ チャネル アダプタ ポリシー。
[Create Fibre Channel Adapter Policy] リンク	ファイバ チャネル アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト ボックス	この vHBA と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	QoS ポリシーを作成する場合は、このリンクをクリックします。

f) [OK] をクリックします。

g) ステップ 8 に進みます。

ステップ 7 [Use Connectivity Policy]を選択した場合、次の手順を実行します。

- 既存の SAN 接続ポリシーを使用するには、[SAN Connectivity Policy] ドロップダウン リストでそのポリシーを選択します。
- 既存の SAN 接続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 SAN Connectivity Policy] リンクをクリックし、フィールドに値を入力します。

SAN 接続のポリシーの詳細については、SAN 接続ポリシーの作成, （404 ページ）を参照してください。

ステップ 8 [Next] をクリックします。

次の作業

ページ 4: ファイバ チャネルの [Zoning] オプションの設定, （595 ページ）を実行します。

ページ 4: ファイバ チャネルの [Zoning] オプションの設定

この手順は、ページ 3：ストレージ オプションの設定, （588 ページ）から直接続くものです。[Create Service Profile (expert)] ウィザードの [Zoning] ページで、サービス プロファイルに対するファイバチャネルのゾーン分割に必要な vHBA イニシエータ グループを設定する方法について説明します。

手順

ステップ 1 まだ実行していない場合は、次の手順に従い、1 つ以上の vHBA イニシエータ グループを作成します。

a) [Select vHBA Initiator Groups] テーブルの最下部のアイコン バーの [+] をクリックします。

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

名前	説明
[Name] フィールド	vHBA イニシエータ グループの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	グループの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Storage Connection Policy] ドロップダウン リスト	この vHBA イニシエータ グループに関連付けられたストレージ接続ポリシー。 次のいずれかになります。 • 既存のストレージ接続ポリシーを使用して、ドロップダウン リストからそのポリシーを選択します。 Cisco UCS Manager GUI には、[Global Storage Connection Policy] 領域のポリシーとその FC ターゲット エンドポイントの情報が表示されます。 グローバルに使用可能な新しいストレージ接続ポリシーを作成し、[Create Storage Connection Policy] リンクをクリックします。 • この vHBA 発信者グループにのみ使用できるローカル ストレージ接続ポリシーを作成し、[Specific Storage Connection Policy] オプションを選択します。 Cisco UCS Manager GUI には、ローカル ストレージ接続ポリシーを設定できる [Specific Storage Connection Policy] 領域が表示されます。
[Create Storage Connection Policy] リンク	すべてのサービス プロファイルとサービス プロファイル テンプレートに使用可能な新しいストレージ接続ポリシーを作成するには、このリンクをクリックします。

ストレージ接続ポリシーの作成方法の詳細については、ファイバ チャネル ストレージ接続ポリシーの作成, （424 ページ）を参照してください。

c) [OK] をクリックします。

ステップ 2 [Select vHBA Initiators] テーブルで、vHBA イニシエータ グループに追加する 1 つ以上の vHBA イニシエータをクリックします。

ステップ 3 [Select vHBA Initiator Groups] テーブルで、選択した vHBA イニシエータの追加先である vHBA イニシエータ グループをクリックします。

ステップ 4 [>> Add To >>] ボタンをクリックして、選択した vHBA イニシエータ グループに選択した vHBA イニシエータを追加します。

ステップ 5 vHBA イニシエータを、関連付けられているサーバとの通信先となるゾーンに必要なすべての vHBA イニシエータ グループに追加して [Next] をクリックします。

次の作業

ページ 5：vNIC/vHBA 配置の設定, （597 ページ）を実行します。

ページ 5：vNIC/vHBA 配置の設定

この手順は、ページ 4: ファイバ チャネルの [Zoning] オプションの設定, （595 ページ）から直接続くものです。 [Create Service Profile (expert)] ウィザードの [vNIC/vHBA Placement] ページで、vNIC および vHBA の配置を設定する方法について説明します。

手順

ステップ 1 [Select Placement] 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
[Let System Perform Placement]	Cisco UCS Manager によってサービス プロファイルに関連付けられたサーバの vNIC/vHBA 配置が決定されることを指定します。 配置は、[PCI Order] テーブルの順序セットによって決定されます。 iSCSI ブート用にこのサービス プロファイルまたはテンプレートを設定する場合は、このオプションを選択します。 iSCSI ブート用にこのサービス プロファイルを設定する場合は、ステップ 5 に進みます。 すべての設定については、ステップ 2 に進みます。

オプション	説明
[Specify Manually]	次の機能が利用できるようになります。 • このサービス プロファイルに関連付けられた vNIC と vHBA を仮想ネットワーク インターフェイス（vCON）に明示的に割り当てます。 • vCON に割り当てられるタイプの vNIC と vHBA を、手動または vNIC/vHBA 配置ポリシーで設定します。 ステップ 3 に進みます。
[vNIC/vHBA Placement Profiles *Placement Profile Name]*	サービス プロファイルに既存の vNIC/vHBA 配置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 Placement Policy] をクリックし、ステップ 4 に進みます。 それ以外の場合は、ステップ 5 に進みます。

ステップ 2 （任意） [Let System Perform Placement] を選択した場合、次の手順を実行します。

a) 次のボタンの 1 つ以上を使用して、vNIC および vHBA の順序を調整します。

名前	説明
[Move Up] ボタン	リスト内で、選択した vNIC または VHBA をより高いプライオリティに移動します。
[Move Down] ボタン	リスト内で、選択した vNIC または VHBA をより低いプライオリティに移動します。
[Delete] ボタン	選択した vNIC または vHBA を削除します。
[Reorder] ボタン	すての vNIC および vHBA を元の順番に戻します。
[Modify] ボタン	現在選択されている vNIC または vHBA を変更できます。 （注） その vNIC または vHBA に対して名前以外のすべてのオプションを変更できます。

b) ステップ 5 に進みます。

ステップ 3 （任意） [Specify Manually]を選択した場合、次の手順を実行します。

a) [vNIC/vHBA] テーブルの適切なタブで、vNIC または vHBA をクリックします。
b) 必要に応じて、[Virtual Host Interface] テーブルで vCON 行をクリックし、[Selection Preference] カラムで次のいずれかの値を選択します。

- [All]：明示的に割り当てられているか、未割り当てであるか、または動的に割り当てられているかどうかに関係なく、すべての設定済みの vNIC と vHBA を vCon に割り当てることができます。 これはデフォルトです。
- [Assigned Only]：vNIC と vHBA を vCon に明示的に割り当てる必要があります。 サービス プロファイルまたは vNIC または vHBA のプロパティを介して、vNIC および vHBA を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 と vHBA を vCon に割り当てることはできません。 vCon は、未割り当てか、または明示的に割り当てられているかに関係なく、すべてのスタティック vNIC と vHBA に対して使用できます。
- [Exclude Unassigned]：未割り当ての vNIC と vHBA 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ダイナミック vNIC と vHBA、およびスタティック vNIC と vHBA に対して使用できます。

c) [Assign] をクリックします。
割り当てを取り消す場合は、[Remove] をクリックします。
d) すべての vNIC および vHBA を割り当てるまで、ステップ a ～ c を繰り返します。
e) すべての vNIC および vHBA の配置を指定したら、ステップ 5 に進みます。

ステップ 4 [Create Placement Policy] をクリックした場合、[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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 は、仮想ネットワーク インターフェイス（vCon）接続をサーバの PCIe アダプタ カードに割り当てます。 各 vCon は、vNIC および vHBA を割り当てることができる物理アダプタの仮想表現です。 1 つのアダプタを持つブレードまたはラック サーバでは、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2、vCon3 を Adapter3、vCon4 を Adapter4 に割り当てます。 2 つまたは 3 つのアダプタを備えたブレードまたはラック サーバについて、Cisco UCS は、選択した仮想スロット 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 カード付きのサーバでは、Cisco UCS は、vCon1 と vCon3 を Adapter1 に割り当て、次に vCon2 と vCon4 を Adapter2 に割り当てます。 3 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 と vCon4 を Adapter2、vCon3 を Adapter3 に割り当てます。 これはデフォルトのスキームです。 • [Linear Ordered]：2 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 と vCon2 を Adapter1 に割り当て、次に vCon3 と vCon4 を Adapter2 に割り当てます。 3 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2 に割り当て、次に vCon3 と vCon4 を Adapter3 に割り当てます。 （注） N20-B6620-2 および N20-B6625-2 ブレード サーバでは、2 つのアダプタには左から右に番号が付けられ、vCon には右から左に番号が付けられます。 いずれかのブレード サーバに単一のアダプタがある場合、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 サーバに 2 つのアダプタがある場合、vCons の割り当ては、仮想スロット マッピング スキームによって異なります。 • [Round Robin]：Cisco UCS は、vCon2 と vCon4 を Adapter1 に割り当て、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 Adapter1 に割り当て、vCon1 と vCon2 を Adapter2 に割り当てます。 Cisco UCS によって vCon が割り当てられた後、各 vCon の [Selection Preference] に基づいて vNIC と vHBA が割り当てられます。

b) 各 [Virtual Slot] の [Selection Preference] カラムで、ドロップダウン リストから次のいずれかを選択します。

- [All]：明示的に割り当てられているか、未割り当てであるか、または動的に割り当てられているかどうかに関係なく、すべての設定済みの vNIC と vHBA を vCon に割り当てることができます。 これはデフォルトです。
- [Assigned Only]：vNIC と vHBA を vCon に明示的に割り当てる必要があります。 サービス プロファイルまたは vNIC または vHBA のプロパティを介して、vNIC および vHBA を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 と vHBA を vCon に割り当てることはできません。 vCon は、未割り当てか、または明示的に割り当てられているかに関係なく、すべてのスタティック vNIC と vHBA に対して使用できます。
- [Exclude Unassigned]：未割り当ての vNIC と vHBA 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ダイナミック vNIC と vHBA、およびスタティック vNIC と vHBA に対して使用できます。

c) [OK] をクリックします。

d) ダイアログボックスを閉じたら、作成したポリシーを[Select Placement] ドロップダウン リストで選択します。

ステップ 5 [Next] をクリックします。

次の作業

ページ 6：サーバのブート順序の設定, （602 ページ）を実行します。

ページ 6：サーバのブート順序の設定

この手順は、ページ 5：vNIC/vHBA 配置の設定, （597 ページ）から直接続くものです。 [Create Service Profile (expert)] ウィザードの [Server Boot Order] ページで、サーバのブート順序オプションを設定する方法について説明します。

ヒント　ブート ポリシーのブート順序には、ローカル ディスクと SAN LUN の両方ではなく一方のみをインクルードし、サーバが誤ったストレージ タイプからブートしないようにすることを推奨します。 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。

手順

ステップ 1　[Boot 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 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 9 に進みます。
[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 3 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、リストでポリシーを選択し、ステップ 9 に進みます。

ステップ 2　[Create Boot Policy] をクリックして、すべてのサービス プロファイルおよびテンプレートが使用できるブート ポリシーを作成する場合、次の手順を実行します。

a) [Create Boot Policy] 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。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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

b) ステップ 3 に進みます。

ステップ 3 （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、[Reboot on boot Order Change] チェックボックスがブート ポリシーに対して選択されており、CD-ROM またはフロッピーがブート順で最後のデバイスの場合に、デバイスを取り外すか、装着しても、ブート順に直接影響は及ぼされず、サーバはリブートされません。

ステップ 4 （任意） 必要に応じて、[Enforce vNIC/vHBA/iSCSI Name] チェックボックス を確認します。

- これをオンにすると、Cisco UCS Manager は設定エラーを表示し、[Boot Order] テーブルにリストされている vNIC、vHBA、または iSCSI の vNIC の 1 つ以上がサービス プロファイルのサーバ設定と一致するかどうかをレポートします。
- オフになっている場合、（ブート オプションに適するように）Cisco UCS Manager はサービス プロファイルのサーバ設定から vNIC、vHBA、または iSCSI vNIC を使用します。 ブート ポリシーで指定された vNIC、vHBA、または iSCSI の vNIC がサービス プロファイルのサーバ設定と一致するかどうかはレポートしません。

ステップ 5 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。
   - Add Local Disk
   - Add CD-ROM
   - Add Floppy
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 6 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 7 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 で次のフィールドに値を入力し、[OK] をクリックします。

名前	説明
[vHBA] フィールド	SAN ブートに使用する vHBA の名前を入力します。

名前	説明
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブート デバイス クラスに定義されている最初のアドレス。 ブート ポリシーには、1 つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブート デバイス クラスに定義されている 2 番目のアドレス。 各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブート デバイス」や「セカンダリ ブート デバイス」はブート順序を表す用語ではありません。 同じデバイス クラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

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 で次のフィールドに値を入力して、[OK] をクリックします。

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

名前	説明
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブートデバイスクラスに定義されている最初のアドレス。ブート ポリシーには、1 つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブートデバイスクラスに定義されている 2 番目のアドレス。 各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブートデバイス」や「セカンダリ ブートデバイス」はブート順序を表す用語ではありません。 同じデバイスクラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

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 8 iSCSI 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) [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。

b) [iSCSI vNICs] 領域で、[Boot Order] テーブルに追加するサーバを起動する iSCSI vNIC をダブルクリックします。

c) [iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。
2 個の iSCSI vNIC がある場合は、ブート パラメータを設定する iSCSI vNIC を選択します。

d) **[Set iSCSI Boot Parameters]** ダイアログボックスのフィールドに値を入力して [OK] をクリックします。
フィールドの詳細については、iSCSI ブート パラメータの設定, （535 ページ）を参照してください。

e) （任意） ステップ c および d を繰り返し、追加の iSCSI vNIC に対してブート パラメータを設定します。

ステップ 9 すべてのサービスプロファイルおよびテンプレートが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 リストでこのポリシーを選択します。

ステップ 10 [Next] をクリックします。

次の作業

ページ 7：メンテナンス ポリシーの追加, （607 ページ）を実行します。

ページ 7：メンテナンス ポリシーの追加

この手順は、ページ6：サーバのブート順序の設定, （602ページ）から直接続くものです。 [Create Service Profile (expert)] ウィザードの [Maintenance Policy] ページでサービス プロファイルにメンテナンス ポリシーを追加する方法について説明します。

手順

ステップ 1 [Maintenance 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 a Maintenance Policy to Use]（デフォルトのポリシーが表示されます）	このサービスプロファイルにデフォルトのメンテナンスポリシーを割り当てます。 ステップ 4 に進みます。
[Maintenance Policies] [*Policy_Name*]	サービス プロファイルに既存のメンテナンス ポリシーを割り当てます。 このオプションを選択すると、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 Maintenance 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、リストでポリシーを選択し、ステップ 4 に進みます。

ステップ 2 [Create Maintenance Policy] をクリックして、すべてのサービス プロファイルおよびテンプレートが使用できるメンテナンス ポリシーを作成する場合、次の手順を実行します。

a) [Create Maintenance Policy] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Reboot Policy] フィールド	サービス プロファイルがサーバに関連付けられているか、サーバにすでに関連付けられているサービス プロファイルに変更を加えた場合、プロセスを完了するには、サーバをリブートする必要があります。 [Reboot Policy] フィールドは、このメンテナンス ポリシーを含むサービス プロファイルに関連付けられたサーバについて、リブートがいつ行われるかを決定します。 次のいずれかになります。 • [Immediate]：サービス プロファイルのアソシエーションが完了するか、サービス プロファイルの変更がユーザによって保存されるとすぐに、サーバが自動的にリブートされます。 • [User Ack]：ユーザがサービス プロファイルのアソシエーションが完了するか、または変更を行うと、サーバを手動で再起動する必要があります。 • [Timer Automatic]：Cisco UCS はすべてのサービス プロファイルのアソシエーションと変更を、[Schedule] フィールドに示されているスケジュールによって定義されたメンテナンス期間延長します。
[Schedule] ドロップダウン リスト	[Reboot Policy] が [Timer Automatic] に設定されている場合、スケジュールによってメンテナンス操作をサーバに適用できる時期が指定されます。 Cisco UCS はサーバをリブートし、スケジュール設定された時間にサービス プロファイルの変更を完了します。

名前	説明
[Create Schedule] リンク	このリンクをクリックすると、このCisco UCSドメイン内のすべてオブジェクトに使用できる新しいスケジュールが作成されます。

b) [OK] をクリックし、ステップ 3 に進みます。

ステップ 3 すべてのサービスプロファイルおよびテンプレートがアクセスできる新しいブートポリシーを作成したら、[Maintenance Policy] ドロップダウン リストでこのポリシーを選択します。

ステップ 4 [Next] をクリックします。

次の作業

ページ 8：サーバの割り当ての指定, （609 ページ）を実行します。

ページ 8：サーバの割り当ての指定

この手順は、ページ 7：メンテナンス ポリシーの追加, （607 ページ）から直接続くものです。[Create Service Profile (expert)] ウィザードの [Server Assignment] ページで、サーバの割り当て方法を指定する方法およびサービスプロファイルに関連付けられるファームウェアパッケージについて説明します。

手順

ステップ 1 [Server Assignment] 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
[Assign Later]	サービス プロファイルを作成して設定したら、サーバを割り当てることができます。 ステップ 6 に進みます。
[Pre-provision a slot]	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 2 に進みます。
[Select existing Server]	サービス プロファイルに割り当てられるサーバを選択するのに使用できる、関連付けられていないサーバのテーブルを表示します。 ステップ 3 に進みます。

オプション	説明
Select from a Pool *Pool_Name*	ドロップダウン リストの最下部の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が割り当てられます。 ステップ 4 に進みます。

ステップ 2 [Pre-provision a slot]を選択した場合、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) [Slot Id] フィールドに、選択したサーバが配置されるスロットの番号を入力します。

c) ステップ 4 に進みます。

ステップ 3 [Select existing Server]を選択した場合、次の手順を実行します。

a) 使用可能なサーバのテーブルの [Select] カラムで、このサービス プロファイルのニーズを満たすサーバのオプション ボタンをクリックします。

b) ステップ 4 に進みます。

ステップ 4 [Power State] 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て、このサービス プロファイルに関連付けられた場合、サーバに適用される電源の状態を設定します。

- [Down]：プロファイルがサーバに関連付けられる前はサーバの電源を切断しておく場合
- [Up]：プロファイルがサーバに関連付けられる前にサーバの電源を投入しておく場合

デフォルトでは、サーバの電源は投入されています。

ステップ 5 サービスプロファイルがサーバに関連付けられた後にそのサービスプロファイルの移行を制限する場合は、[Restrict Migration] チェックボックスをオンにします。
移行を制限しない場合は、既存のサービス プロファイルを移行する前に、Cisco UCS Manager による新規サーバに対する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 6 （任意） [Firmware Management] 領域で次の手順を実行して、サービス プロファイルに関連付けられているサーバで、ポリシーを使用してファームウェアをアップデートします。

a) [Firmware Management] バーの下矢印をクリックして、領域を展開します。

b) 次のフィールドに入力します。

名前	説明
[Host Firmware] ドロップダウン リスト	ホスト ファームウェア パッケージをこのサービス プロファイルと関連付けるには、その名前をドロップダウン リストから選択します。
[Create Host Firmware Package] リンク	ホスト ファームウェア パッケージを作成する場合は、このリンクをクリックします。

ステップ 7 [Next] をクリックします。

次の作業

ページ 9：動作ポリシーの追加，（611 ページ）を実行します。

ページ 9：動作ポリシーの追加

この手順は、ページ 8：サーバの割り当ての指定，（609 ページ）から直接続くものです。 [Create Service Profile (expert)] ウィザードの [Operational Policies] ページでサービス プロファイルに動作ポリシーを追加する方法について説明します。 これらのポリシーは、任意です。

手順

ステップ 1 デフォルトの BIOS 設定を上書きし、サービスプロファイル全体で設定するには、下矢印をクリックして [BIOS Configuration] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[BIOS Policy] ドロップダウン リスト で適切な BIOS ポリシーを選択します。
- すべてのサービス プロファイル テンプレートで使用できる BIOS ポリシーを作成するには、[create bios policy][Create BIOS Policy]をクリックし、ダイアログボックスのフィールドに値を入力してから、[BIOS Policy] ドロップダウン リスト でこのポリシーを選択します。

BIOS ポリシーの作成方法の詳細については、BIOS ポリシーの作成，（470 ページ）を参照してください。

ステップ 2 サーバの Cisco Integrated Management Controller（CIMC）への外部アクセスを提供するには、下矢印をクリックして [External IPMI Management Configuration] バーを展開し、IPMI プロファイルおよび Serial over LAN ポリシーを追加します。
外部アクセスを提供しない場合は、ステップ 4 に進みます。

ステップ 3 サービスプロファイルに IPMI プロファイルを追加するには、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[IPMI Access Profile] ドロップダウン リストで適切な IPMI プロファイルを選択します。
- [IPMI Access Profile] ドロップダウン リスト適切なユーザ アクセスが設定されている IPMI プロファイルが含まれていない場合、[Create Access IPMI Profile] リンクをクリックし、すべてのサービス プロファイルで使用できる IPMI プロファイルを作成して、そのプロファイルを [IPMI Access Profile] ドロップダウン リストから選択します。

IPMI プロファイルの作成方法の詳細については、IPMI アクセス プロファイルの作成，（473 ページ）を参照してください。

ステップ 4 サービス プロファイルに Serial over LAN ポリシーを追加するには、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[SoL Configuration Profile] ドロップダウン リストで適切な Serial over LAN ポリシーを選択します。
- このテンプレートから作成されたサービス プロファイルだけが使用できる Serial over LAN ポリシーを作成するには、[Create a Specific SoL Policy][Create a Specific SoL Policy]を[SoL Configuration Profile] ドロップダウン リストから選択して[Admin State] フィールドと[Speed] ドロップダウン リストに値を入力します。
- すべてのサービス プロファイル テンプレートが使用できる Serial over LAN ポリシーを作成するには、[Create Serial over LAN Policy] リンクをクリックし、ダイアログボックスのフィールドに値を入力してから、[SoL Configuration Profile] ドロップダウン リストでそのポリシーを選択します。

Serial over LAN ポリシーの作成方法の詳細については、Serial over LAN ポリシーの作成, （486 ページ）を参照してください。

ステップ 5 サーバの CIMC への外部アクセスに必要な管理 IP を設定するには、下矢印をクリックして [Management IP Address] バーを展開し、次の手順を実行します。

a) [Management IP Address 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。

- [None]：管理 IP アドレスがサービス プロファイルを介してサーバに割り当てられていません。 管理 IP アドレスは、サーバ上で定義される CIMC 管理 IP アドレスに基づいています。
- [Static]：サービス プロファイルによって、スタティック管理 IP アドレスが関連付けられたサーバに割り当てられます。 サービス プロファイルを新しいサーバに移行すると、管理 IPv4 アドレスもサービス プロファイルとともに移動します。

  Cisco UCS Manager GUI には、スタティック IP アドレスを定義できる [Static IP Address] 領域が表示されます。
- *[IP-pool-name]*：サービス プロファイルは、選択した IP プールから関連付けられたサーバに管理 IP アドレスを割り当てます。

  [Create IP Pool] をクリックして、すべてのサービス プロファイルとサービス プロファイル テンプレートが使用できる IP アドレスのグローバル プールを作成します。

b) [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
[IP Address] フィールド	サービス プロファイルを通してサーバに割り当てられた管理 IP アドレス。
[Subnet Mask] フィールド	管理 IP アドレスのサブネット マスク。
[Default Gateway] フィールド	管理 IP アドレスのデフォルト ゲートウェイ。

ステップ 6 しきい値をモニタし、関連付けられているサーバの統計情報を収集するには、下矢印をクリックして [Monitoring Configuration(Thresholds)] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[Threshold Policy] ドロップダウン リストで適切なしきい値ポリシーを選択します。
- すべてのサービス プロファイルで使用できるしきい値ポリシーを作成するには、[Create Threshold Policy] リンクをクリックし、ダイアログボックスのフィールドに値を入力してから、[Threshold Policy] ドロップダウン リストでこのポリシーを選択します。

しきい値ポリシーの作成方法の詳細については、サーバおよびサーバ コンポーネントのしきい値ポリシーの作成，（808 ページ）を参照してください。

ステップ 7 電力制御ポリシーとサービスプロファイルを関連付けるには、下矢印をクリックして [Power Control Policy Configuration] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[Power Control Policy] ドロップダウン リストで適切な電力制御ポリシーを選択します。
- すべてのサービスプロファイルで使用できる電力制御ポリシーを作成するには、[Create Power Control Policy] リンク をクリックし、ダイアログボックスのフィールドに値を入力してから、[Power Control Policy] ドロップダウン リストでこのポリシーを選択します。

電源モジュールの制御ポリシーの作成方法の詳細については、電力制御ポリシーの作成，（695 ページ）を参照してください。

ステップ 8 スクラブ ポリシーとサービスプロファイルを関連付けるには、下矢印をクリックして [Scrub Policy] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[Scrub Policy] ドロップダウン リスト で適切なスクラブ ポリシーを選択します。
- すべてのサービスプロファイルで使用できるスクラブ ポリシーを作成するには、[Create Scrub Policy] リンク をクリックし、ダイアログボックスのフィールドに値を入力してから、[Scrub Policy] ドロップダウン リスト でこのポリシーを選択します。

スクラブ ポリシーの作成方法の詳細については、スクラブ ポリシーの作成，（485 ページ）を参照してください。

ステップ 9 [Finish] をクリックします。

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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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) [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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

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、次のフィールドに値を入力します。

名前	説明
[Primary vNIC] セクション	
[Primary vNIC] チェックボックス	このサービス プロファイル用に vNIC を作成する場合は、このチェックボックスをオンにします。 このチェックボックスをオンにすると、Cisco UCS Manager GUI に、このセクション内の残りのフィールドが表示されます。
[Name] フィールド	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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Fabric] フィールド	この vNIC が関連付けられるファブリック インターコネクト。
[Network] ドロップダウン リスト	この vNIC が関連付けられる LAN。
[Secondary vNIC] セクション	

名前	説明
[Secondary vNIC] チェックボックス	このサービス プロファイル用に別の vNIC を作成する場合は、このチェックボックスをオンにします。 このチェックボックスをオンにすると、Cisco UCS Manager GUI に、このセクション内の残りのフィールドが表示されます。
[Name] フィールド	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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Fabric] フィールド	この vNIC が関連付けられるファブリック インターコネクト。
[Network] ドロップダウン リスト	この vNIC が関連付けられる LAN。

ステップ 7 [Create Service Profile] ダイアログボックスの [vHBAs] 領域で、次のフィールドに値を入力します。

名前	説明
[Primary vHBA] セクション	
[Primary vHBA] チェックボックス	このサービスプロファイル用に vHBA を作成する場合は、このチェックボックスをオンにします。 このチェックボックスをオンにすると、Cisco UCS Manager GUI に、このセクション内の残りのフィールドが表示されます。
[Name] フィールド	vHBA 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Fabric] フィールド	この vHBA が関連付けられるファブリック インターコネクト。プライマリ vHBA をセカンダリ vHBA と同じファブリックに関連付けてはいけません。
[Secondary vHBA] セクション	

名前	説明
[Secondary vHBA] チェックボックス	このサービスプロファイル用に別の vHBA を作成する場合は、このチェックボックスをオンにします。 このチェックボックスをオンにすると、Cisco UCS Manager GUI に、このセクション内の残りのフィールドが表示されます。
[Name] フィールド	vHBA 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Fabric] フィールド	この vHBA が関連付けられるファブリックインターコネクト。セカンダリ vHBA をプライマリ vHBA と同じファブリックに関連付けてはいけません。

ステップ 8 [Create Service Profile] ダイアログボックスの [Boot Order] 領域で、次のフィールドに値を入力します。

名前	説明
[Primary Boot Device] セクション	
[Primary Boot Device] チェックボックス	このサービスプロファイル用にブートデバイスを設定する場合は、このチェックボックスをオンにします。 このチェックボックスをオンにすると、Cisco UCS Manager GUI に、このセクション内の残りのフィールドが表示されます。

名前	説明
[Type] フィールド	次のいずれかになります。 • [local-disk]：サーバは、ローカル ディスクからブートします。 （注） このオプションを選択すると、セカンダリ ブート タイプに [local-disk] と [san] を選択できなくなります。 • [san]：サーバは、SAN に保存されたイメージからブートします。 このオプションを選択すると、Cisco UCS Manager GUI に [SAN] 領域が表示されます。 • [Lan]：サーバは LAN からブートされます。 このオプションを選択すると、Cisco UCS Manager GUI に [Network] 領域が表示され、サーバの PXE ブートに使用する vNIC を指定できるようになります。 • [CD-ROM]：サーバは仮想 CD-ROM からブートします。 • [Floppy]：サーバは仮想フロッピーからブートします。
[SAN] 領域	[Type] が [san] に設定されている場合、この領域には次のフィールドが表示されます。 • [vHBA]：SAN ブート イメージにアクセスするために使用される vHBA • [LUN]：ブート イメージの場所に対応する LUN • [WWN]：ブート イメージの場所に対応する WWN
[Network (PXE)] 領域	[Type] に [lan] を設定した場合、この領域に [vNIC] ドロップダウン リストが表示され、サーバのブートに使用する vNIC を選択できます。
[Secondary Boot Device] セクション	
[Secondary Boot Device] チェックボックス	このサービスプロファイル用に別のブートデバイスを設定する場合は、このチェックボックスをオンにします。 このチェックボックスをオンにすると、Cisco UCS Manager GUI に、このセクション内の残りのフィールドが表示されます。

名前	説明
[Type] フィールド	次のいずれかになります。 • [local-disk]：サーバは、ローカル ディスクからブートします。 • [san]：サーバは、SANに保存されたイメージからブートします。 このオプションを選択すると、Cisco UCS Manager GUI に [SAN] 領域が表示されます。 • [Lan]：サーバは LAN からブートされます。 このオプションを選択すると、Cisco UCS Manager GUI に [Network] 領域が表示され、サーバの PXE ブートに使用する vNIC を指定できるようになります。 • [CD-ROM]：サーバは仮想 CD-ROM からブートします。 • [Floppy]：サーバは仮想フロッピーからブートします。
[SAN] 領域	[Type] に [san] を設定した場合、この領域に次のフィールドが表示されます。 • [vHBA]：SAN ブート イメージにアクセスするために使用される vHBA • [LUN]：ブート イメージの場所に対応する LUN • [WWN]：ブート イメージの場所に対応する WWN
[Network (PXE)] 領域	[Type] に [lan] を設定した場合、この領域に [vNIC] ドロップダウン リストが表示され、サーバのブートに使用する vNIC を選択できます。

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。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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 リストで、サービス プロファイルを作成する組織を選択します。

b) [Hardware Based Service Profile] オプション 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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

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適用し、サービス プロファイルを作成してから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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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 リストで、サービス プロファイルを作成する組織を選択します。
b) [Hardware Based Service Profile]オプション 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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。
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適用し、サービス プロファイルを作成してからサーバに関連付けます。

サービス プロファイル テンプレートの操作

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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profile Templates] 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 [Create Service Profile Template] ウィザードで、次の手順を実行します。

- ページ 1：サービス プロファイル テンプレートの識別, （621 ページ）
- ページ 2：ネットワーキング オプションの指定, （622 ページ）
- ページ 3: ストレージ オプションの指定, （630 ページ）
- ページ 4: ファイバ チャネルの [Zoning] オプションの設定, （637 ページ）
- ページ 5：vNIC/vHBA 配置の設定, （639 ページ）
- ページ 6：サーバのブート順序の設定, （644 ページ）

- ページ 7：メンテナンス ポリシーの追加, （649 ページ）
- ページ 8：サーバの割り当てオプションの指定, （651 ページ）
- ページ 9：動作ポリシーの追加, （652 ページ）

ページ 1：サービス プロファイル テンプレートの識別

この手順は、サービス プロファイル テンプレートの作成, （620 ページ）に記載されているステップから直接続くものです。 [Create Service Profile Template] ウィザードの [Identify Service Profile] ページで、サービス プロファイル テンプレートの ID を設定する方法について説明します。

手順

ステップ 1 [Name] フィールドに、このサービス プロファイル テンプレート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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

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

- [Initial Template]：テンプレートが変更されても、このテンプレートから作成されたサービス プロファイルはアップデートされません。
- [Updating Template]：テンプレートが変更されると、このテンプレートから作成されたサービス プロファイルがアップデートされます。

ステップ 3 [UUID Assignment] 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 (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。
[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。

オプション	説明
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 4 （任意） テキスト ボックスに、このサービス プロファイル テンプレートの説明を入力します。サービス プロファイル テンプレートのユーザ定義の説明。

256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

ステップ 5 [Next] をクリックします。

次の作業

ページ 2：ネットワーキング オプションの指定, （622 ページ）の手順を完了します。

ページ 2：ネットワーキング オプションの指定

この手順は、ページ 1：サービス プロファイル テンプレートの識別, （621 ページ）から直接続くものです。 [Create Service Profile Template] ウィザードの [Networking] ページで、LAN 接続を含むネットワーキング 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 （任意） ダイナミック vNIC をサポートするアダプタを備えるサーバにこのテンプレートから作成されたサービス プロファイルを割り当てる予定の場合、[Dynamic vNIC Connection] ドロップダウン リストで次のオプションのいずれかを選択します。

オプション	説明
[Select a Policy to use]	ダイナミック vNIC をサポートしないアダプタを備えるサーバには、ダイナミック vNIC 接続ポリシーなしでサービス プロファイル テンプレートを作成できます。 このオプションでは、テンプレートにダイナミック vNIC 接続ポリシーは含まれません。 iSCSI ブート用にこのサービス プロファイルまたはテンプレートを設定する場合は、このオプションを選択します。 ステップ 4 に進みます。

オプション	説明
[Create a Specific Dynamic vNIC Connection 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ダイナミック vNIC 接続ポリシーを作成できます。 ステップ 2 に進みます。
[Dynamic vNIC Connection Policies] *Policy_Name*	ドロップダウンリストの最下部にあるリストから既存のダイナミック vNIC 接続ポリシーを選択します。 Cisco UCS Manager で、サービス プロファイル テンプレートにこのポリシーが割り当てられます。 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およびテンプレートがアクセスできるポリシーを作成する場合は、ステップ 3 に進みます。 それ以外の場合は、ステップ 4 に進みます。

ステップ 2 （任意） [Create a Specific Dynamic vNIC Connection Policy]をクリックした場合、このサービス プロファイルだけが使用できる新しいダイナミック vNIC 接続ポリシーを作成するには、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
[Number of Dynamic vNICs] フィールド	このポリシーの影響を受けるダイナミック vNIC の数。
[Adapter Policy] ドロップダウン リスト	このポリシーと関連付けられるアダプタ プロファイル。 すでに存在しているプロファイルだけが、このドロップダウンリストに表示されます。
[Protection] フィールド	ダイナミック vNIC は Cisco UCS で常に保護されますが、優先するファブリックがある場合はこのフィールドを使用してそれを選択することができます。 次のいずれかを選択できます。 • [Protected Pref A]：Cisco UCS はファブリック A を使用しようとしますが、必要に応じてファブリック B にフェールオーバーします。 • [Protected Pref B]：Cisco UCS はファブリック B を使用しようとしますが、必要に応じてファブリック A にフェールオーバーします。 • [Protected]：Cisco UCS は、使用可能であればどのファブリックでも使用します。

b) ステップ 4 に進みます。

ステップ 3 （任意） すべてのサービス プロファイルおよびテンプレートが使用できるダイナミック vNIC 接続ポリシーを作成するには、次の手順を実行します。

a) [Create Dynamic vNIC Connection Policy]をクリックします。

b) [Create Dynamic vNIC Connect Policy] ダイアログボックスで、フィールドに値を入力します。詳細については、『Cisco UCS Manager VM-FEX Configuration Guide』を参照してください。

c) [OK] をクリックします。

d) [Dynamic vNIC Connection] ドロップダウン リストで、作成したポリシーを選択します。

e) ステップ 4 に進みます。

ステップ 4 [How would you like to configure LAN connectivity?] フィールドで、次のオプションのいずれかをクリックします。

オプション	説明
[Simple]	このテンプレートから作成された各サービス プロファイルに、デュアル ファブリック モードで最大 2 つの vNIC を作成できます。 ステップ 5 に進みます。
[Expert]	このテンプレートから作成された各サービス プロファイルに、vNIC を無制限に作成できます。 iSCSI ブート用にこのサービス プロファイルを設定する場合は、ステップ 7 に進みます。 そのほかすべての設定については、ステップ 6 に進みます。
[No vNICs]	このテンプレートから作成されたサービス プロファイルには、LAN 接続用の vNIC は含まれません。 これらのサービス プロファイルに関係付けられているサーバは、後で個別のサービス プロファイルを変更する場合を除き、LAN と通信できません。 ステップ 9 に進みます。
[Use Connectivity Policy]	このサービス プロファイルに対して LAN 接続ポリシーを使用できるようにします。 ステップ 8 に進みます。 （注） 同じサービス プロファイルに、LAN 接続ポリシーと、ローカルで作成された vNIC を設定することはできません。 サービス プロファイルに LAN 接続ポリシーを追加すると、既存の vNIC 設定はすべて消去されます。

ステップ 5 （任意） シンプル LAN 接続オプションを選択し、iSCSI ブート用にこのサービス プロファイルを設定していない場合、次の手順を実行します。

a) [vNIC 0 (Fabric A)] 領域で、次の手順を実行します。

- [Name] フィールドに、vNIC の一意の名前を入力します。

- [Select Native VLAN] ドロップダウン リストで、この vNIC が通信する VLAN の名前を選択します。

必要な VLAN がドロップダウン リストに表示されない場合は、[Create VLAN] リンクをクリックします。 詳細については、ネームド VLAN の作成, （261 ページ）を参照してください。

b) この vNIC に VLAN を作成するには、[vNIC 1 (Fabric B)] 領域でステップ 2a を繰り返します。
c) ステップ 9 に進みます。

ステップ 6 エキスパート LAN 接続オプションを選択した場合、次の手順を実行します。

a) テーブルのアイコン バーで [Add] をクリックし、[Create vNICs] ダイアログボックスを開きます。
b) 次のフィールドに値を入力して、vNIC の ID 情報を指定します。

名前	説明
[Name] フィールド	この vNIC のユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vNIC Template] チェックボックス	テンプレートを使用して vNIC を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vNIC Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vNIC テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vNIC Template] リンク	vNIC テンプレートを作成する場合は、このリンクをクリックします。

名前	説明
[MAC Address Assignment] ドロップダウン リスト	項目 • デフォルトの MAC アドレス プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた MAC アドレスを使用する場合は、[Hardware Default] を選択します。 • 特定の MAC アドレスを使用する場合は、[02:25: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。

c) [Fabric Interconnect] 領域で、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC から第 2 のファブリック インターコネクトにアクセスできるようにする場合は、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックのフェールオーバーをイネーブルにしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のものにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバをこの vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。
[VLANs] テーブル	次の表には、この vNIC に関連付けることができる VLAN がリストされています。 各カラムの説明は次のとおりです。 • [Select]：使用する VLAN ごとに、このカラムのチェックボックスをオンにします。 • [Name]：VLAN の名前。 • [Native VLAN]：VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

名前	説明
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC にある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[Pin Group] ドロップダウン リスト	この vNIC と関連付ける LAN ピン グループを選択します。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト	この vNIC と関連付ける統計情報収集ポリシー。

d) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト	この vNIC と関連付けるイーサネット アダプタ ポリシー。
[Create Ethernet Adapter Policy] リンク	イーサネット アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC が関連付けられているダイナミック vNIC 接続ポリシー。
[Create Dynamic vNIC Connection Policy] リンク	ダイナミック vNIC 接続ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト	この vNIC と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	Quality Of Service ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Network Control Policy] ドロップダウン リスト	この vNIC と関連付けるネットワーク制御ポリシー。
[Create Network Control Policy Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。

e) [OK] をクリックします。

ステップ 7 エキスパート LAN 接続オプションを選択し、iSCSI ブート用にこのサービス プロファイルを設定している場合、次の手順を実行します。

a) 下矢印をクリックして [iSCSI vNICs] バーを展開します。

b) テーブルのアイコン バーで [Add] をクリックし、[Create iSCSI vNIC] ダイアログボックスを開きます。

c) 次のフィールドに値を入力して、iSCSI vNIC の ID 情報を指定します。

名前	説明
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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（ある場合）。
[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（ある場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC に使用可能な新しい iSCSI アダプタ ポリシーを作成するには、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（ある場合）。 MAC アドレスが設定されていない場合、Cisco UCS Manager GUI には [Derived] が表示されます。
[MAC Pool] フィールド	この iSCSI vNIC に関連付けられた MAC プール（ある場合）。

名前	説明
[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（ある場合）。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 M82-8P 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 上のネイティブ 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、指定する VLAN はオーバーレイ vNIC に割り当てられたどの VLAN にすることもできます。

d) [OK] をクリックします。
e) 追加の iSCSI vNIC を作成するために、ステップ b から d を繰り返します。

ステップ 8 [Use Connectivity Policy]を選択した場合、次の手順を実行します。

- 既存の LAN 接続ポリシーを使用するには、[LAN Connectivity Policy] ドロップダウン リストでそのポリシーを選択します。
- 既存の LAN 接続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 LAN Connectivity Policy] リンクをクリックし、フィールドに値を入力します。

LAN 接続のポリシーの詳細については、LAN 接続ポリシーの作成, （321 ページ）を参照してください。

ステップ 9 [Next] をクリックします。

次の作業

ページ 3: ストレージ オプションの指定, （630 ページ）を実行します。

ページ 3: ストレージ オプションの指定

この手順は、ページ 2：ネットワーキング オプションの指定, （622 ページ）から直接続くものです。 [Create Service Profile Template] ウィザードの [Storage] ページでサービス プロファイル テンプレートのストレージ 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 [Local Storage] 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 Local Storage Policy to use]	このテンプレートから作成された各サービスプロファイルにデフォルトのローカル ディスク ストレージ ポリシーを割り当てます。 ステップ 4 に進みます。
[Create a Specific Storage Policy]	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だけがアクセスできるローカル ディスク ポリシーを作成できます。 ステップ 2 に進みます。
Storage Policies *Policy_Name*	ドロップダウン リストの最下部にあるリストから既存のローカルディスク ポリシーを選択できるようになります。 Cisco UCS Manager で、このテンプレートから作成された各サービスプロファイルにこのポリシーが割り当てられます。 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およびテンプレートがアクセスできる新しいポリシーを作成する場合は、ステップ 3 に進みます。 それ以外の場合は、ステップ 4 に進みます。

ステップ 2 （任意） [Create a Specific Storage Policy]を選択し、このサービス プロファイル テンプレートから作成されたサービス プロファイルだけが使用できる新しいポリシーを作成する場合は、次の手順を実行します。

a) [Mode] ドロップダウン リストで、次のいずれかを選択します。

- [No Local Storage]：ディスクレス サーバまたは SAN 専用の設定で使用します。 このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0 Striped]：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] モードの適用後に違いがわからないことがあ

ります。 これにより、ポリシー内の RAID 設定と、サーバの[Inventory] > [Storage] タブに表示される実際のディスク設定の間に不一致が生じる場合があります。

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。
- [RAID10 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。

（注） 一部の Cisco UCS サーバでは、特定の RAID 設定オプションにライセンスが必要です。 Cisco UCS Manager がこのローカル ディスク ポリシーを含むサービス プロファイルをサーバに関連付けると、Cisco UCS Manager は、選択した RAID オプションに適切なライセンスが付与されていることを確認します。 問題がある場合は、サービス プロファイルの関連付け中に Cisco UCS Manager によって設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。

b) サーバと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たい場合、[Protect Configuration] チェックボックスをオンにします。
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 Protect Configuration プロパティが優先され、前のサービス プロファイルの設定は上書きされます。

（注） このオプションがイネーブルの状態でサーバとサービス プロファイルの関連付けを解除した後、そのサーバに新しいサービス プロファイルを関連付け、そのサービス プロファイル内のローカル ディスク設定ポリシーに前とは異なるプロパティが含まれていると、サーバから設定不一致のエラーが返され、関連付けは失敗します。

c) ステップ 4 に進みます。

ステップ 3 （任意） すべてのサービス プロファイルおよびテンプレートが使用できるローカル ディスク設定ポリシーを作成するには、次の手順を実行します。

a) [Create Local Disk Configuration Policy] リンクをクリックします。

b) [Create Local Disk Configuration] 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。
詳細については、ローカルディスク設定ポリシーの作成, （479ページ）を参照してください。

c) [OK] をクリックします。

d) [Local Storage] ドロップダウン リストで、作成したポリシーを選択します。

ステップ 4 [How would you like to configure SAN storage?] フィールドで、次のオプションのいずれかをクリックします。

オプション	説明
[Simple]	このテンプレートから作成された各サービス プロファイルに、最大 2 つの vHBA を作成できます。 ステップ 5 に進みます。
[Expert]	このテンプレートから作成された各サービス プロファイルに、vHBA を無制限に作成できます。 ステップ 6 に進みます。
[No vHBAs]	このテンプレートから作成されたサービス プロファイルには、ファイバチャネル SAN 接続用の vHBA は含まれません。 iSCSI ブート用にこのサービス プロファイルまたはテンプレートを設定する場合は、このオプションを選択します。 ステップ 8 に進みます。
[Use Connectivity Policy]	このサービス プロファイルに対して SAN 接続ポリシーを使用できるようにします。 ステップ 7 に進みます。 （注） 同じサービス プロファイルに、SAN 接続ポリシーと、ローカルで作成された vHBA を設定することはできません。 サービス プロファイルに SAN 接続ポリシーを追加すると、既存の vHBA 設定はすべて消去されます。

ステップ 5 （任意） シンプル SAN ストレージ オプションを選択した場合、次の手順を実行します。

a) [WWNN Assignment] ドロップダウン リストで、次のいずれかを選択します。

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

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

b) [vHBA 0 (Fabric A)] 領域で、次のフィールドに値を入力します。

- [Name] フィールドに、vHBA の一意の名前を入力します。
- [Select VSAN] ドロップダウン リストで、この vHBA を関連付ける VSAN の名前を選択します。

必要な VSAN がドロップダウン リストに表示されない場合は、[Create VSAN] リンクをクリックします。 詳細については、ネームド VSAN の作成, （362 ページ）を参照してください。

c) この vHBA に VSAN を作成するには、[vHBA 1 (Fabric B)] 領域でステップ 5b を繰り返します。

d) ステップ 8 に進みます。

ステップ 6 （任意） エキスパート SAN ストレージ オプションを選択した場合、次の手順を実行します。

a) [WWNN Assignment] ドロップダウン リストで、次のいずれかを選択します。

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

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

b) テーブルのアイコン バーで [Add] をクリックし、[Create vHBA] ダイアログボックスを開きます。

c) 次のフィールドに値を入力して、vHBA の ID 情報を指定します。

名前	説明
[Name] フィールド	この vHBA 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

名前	説明
[Use vHBA Template] チェックボックス	テンプレートを使用してvHBAを作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vHBA Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vHBA テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vHBA Template] リンク	vHBA テンプレートを作成する場合は、このリンクをクリックします。
[WWPN Assignment] ドロップダウン リスト	Cisco UCS が World Wide Port Node を vHBA に割り当てる方法。 Cisco UCS について、次のように設定します。 • デフォルトの WWPN プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた WWPN を使用する場合は、[Derived] を選択します。 • 特定の WWPN を使用する場合は、[20:00:00:25:B5:00:00:00]、[20:XX:XX:XX:XX:XX:XX:XX]、または [5X:XX:XX:XX:XX:XX:XX:XX] を選択し、使用する WWPN を [WWPN] フィールドに入力します。 WWPN が Cisco MDS ファイバ チャネル スイッチと互換性を持つようにするには、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • プール内の WWPN 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アドレスの数であり、2 番めの数字はそのプール内の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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[Create WWPN Pool] リンク	Cisco UCS ドメイン内のすべてのオブジェクトで使用可能な新しいWWPNプールを作成する場合は、このリンクをクリックします。

名前	説明
[WWPN] フィールド	[WWPN Assignment] ドロップダウン リストが手動テンプレートのいずれかに設定されている場合、手動で割り当てた WWPN。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN 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。

d) [VSAN] 領域で、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。
[Select VSAN] ドロップダウン リスト ボックス	この vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Pin Group] ドロップダウン リスト ボックス	この vHBA が関連付けられる SAN ピン グループ。
[Create SAN Pin Group] リンク	ピン グループを作成する場合は、このリンクをクリックします。
[Persistent Binding] フィールド	次のいずれかになります。 • Disabled • Enabled
[Max Data Field Size] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の範囲の整数を入力します。 デフォルトは 2048 です。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト ボックス	この vHBA と関連付ける統計しきい値ポリシー。

e) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト ボックス	この vHBA と関連付けるファイバ チャネル アダプタ ポリシー。
[Create Fibre Channel Adapter Policy] リンク	ファイバ チャネル アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト ボックス	この vHBA と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	QoS ポリシーを作成する場合は、このリンクをクリックします。

f) [OK] をクリックします。

g) ステップ 8 に進みます。

ステップ 7 [Use Connectivity Policy]を選択した場合、次の手順を実行します。

- 既存の SAN 接続ポリシーを使用するには、[SAN Connectivity Policy] ドロップダウン リストでそのポリシーを選択します。
- 既存の SAN 接続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 SAN Connectivity Policy] リンクをクリックし、フィールドに値を入力します。

SAN 接続のポリシーの詳細については、SAN 接続ポリシーの作成, （404 ページ）を参照してください。

ステップ 8 [Next] をクリックします。

次の作業

ページ 4: ファイバ チャネルの [Zoning] オプションの設定, （637 ページ）を実行します。

ページ 4: ファイバ チャネルの [Zoning] オプションの設定

この手順は、ページ 3: ストレージ オプションの指定, （630 ページ）から直接続くものです。[Create Service Profile Template] ウィザードの [Zoning] ページで、サービス プロファイルに対するファイバチャネルのゾーン分割に必要な vHBA イニシエータ グループを設定する方法について説明します。

手順

ステップ 1 まだ実行していない場合は、次の手順に従い、1 つ以上の vHBA イニシエータ グループを作成します。

a) [Select vHBA Initiator Groups] テーブルの最下部のアイコン バーの [+] をクリックします。

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

名前	説明
[Name] フィールド	vHBA イニシエータ グループの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	グループの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Storage Connection Policy] ドロップダウン リスト	この vHBA イニシエータ グループに関連付けられたストレージ接続ポリシー。 次のいずれかになります。 • 既存のストレージ接続ポリシーを使用して、ドロップダウン リストからそのポリシーを選択します。 Cisco UCS Manager GUI には、[Global Storage Connection Policy] 領域のポリシーとその FC ターゲット エンドポイントの情報が表示されます。 グローバルに使用可能な新しいストレージ接続ポリシーを作成し、[Create Storage Connection Policy] リンクをクリックします。 • この vHBA 発信者グループにのみ使用できるローカル ストレージ接続ポリシーを作成し、[Specific Storage Connection Policy] オプションを選択します。 Cisco UCS Manager GUI には、ローカル ストレージ接続ポリシーを設定できる [Specific Storage Connection Policy] 領域が表示されます。
[Create Storage Connection Policy] リンク	すべてのサービス プロファイルとサービス プロファイル テンプレートに使用可能な新しいストレージ接続ポリシーを作成するには、このリンクをクリックします。

ストレージ接続ポリシーの作成方法の詳細については、ファイバ チャネル ストレージ接続ポリシーの作成, （424 ページ）を参照してください。

c) [OK] をクリックします。

ステップ 2 [Select vHBA Initiators] テーブルで、vHBA イニシエータ グループに追加する 1 つ以上の vHBA イニシエータをクリックします。

ステップ 3 [Select vHBA Initiator Groups] テーブルで、選択した vHBA イニシエータの追加先である vHBA イニシエータ グループをクリックします。

ステップ 4 [>> Add To >>] ボタンをクリックして、選択した vHBA イニシエータ グループに選択した vHBA イニシエータを追加します。

ステップ 5 vHBA イニシエータを、関連付けられているサーバとの通信先となるゾーンに必要なすべての vHBA イニシエータ グループに追加して [Next] をクリックします。

次の作業

ページ 5：vNIC/vHBA 配置の設定, （639 ページ）を実行します。

ページ 5：vNIC/vHBA 配置の設定

この手順は、ページ 4: ファイバ チャネルの [Zoning] オプションの設定, （637 ページ）から直接続くものです。 [Create Service Profile Template] ウィザードの [vNIC/vHBA Placement] ページで、vNIC および vHBA の配置を設定する方法について説明します。

手順

ステップ 1 [Select Placement] 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
[Let System Perform Placement]	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られるすべてのサーバの vNIC/vHBA 配置が Cisco UCS Manager で決定されるように指定します。 配置は、[PCI Order] テーブルの順序セットによって決定されます。 iSCSI ブート用にこのサービス プロファイルまたはテンプレートを設定する場合は、このオプションを選択します。 iSCSI ブート用にこのサービス プロファイルを設定する場合は、ステップ 5 に進みます。 すべての設定については、ステップ 2 に進みます。

オプション	説明
[Specify Manually]	次の機能が利用できるようになります。 • このサービス プロファイル テンプレートに関連付けられた vNIC と vHBA を仮想ネットワーク インターフェイス（vCON）に明示的に割り当てます。 • vCON に割り当てられるタイプの vNIC と vHBA を、手動または vNIC/vHBA 配置ポリシーで設定します。 ステップ 3 に進みます。
[vNIC/vHBA Placement Profiles *Placement Profile Name]*	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既存の vNIC/vHBA 配置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。 vNIC/vHBA 配置ポリシーが Cisco UCS Manager に設定されていない場合、このオプションはドロップダウン リストに表示されないことがあります。 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およびテンプレートがアクセスできるポリシーを作成する場合は、[Create Placement Policy] をクリックし、ステップ 4 に進みます。 それ以外の場合は、ステップ 5 に進みます。

ステップ 2 （任意） [Let System Perform Placement] を選択した場合、次の手順を実行します。

a) 次のボタンの 1 つ以上を使用して、vNIC および vHBA の順序を調整します。

名前	説明
[Move Up] ボタン	リスト内で、選択した vNIC または VHBA をより高いプライオリティに移動します。
[Move Down] ボタン	リスト内で、選択した vNIC または VHBA をより低いプライオリティに移動します。
[Delete] ボタン	選択した vNIC または vHBA を削除します。
[Reorder] ボタン	すての vNIC および vHBA を元の順番に戻します。
[Modify] ボタン	現在選択されている vNIC または vHBA を変更できます。 （注） その vNIC または vHBA に対して名前以外のすべてのオプションを変更できます。

b) ステップ 5 に進みます。

ステップ 3 （任意） [Specify Manually] を選択した場合、次の手順を実行します。

a) [vNIC/vHBA] テーブル の適切なタブで、vNIC または vHBA をクリックします。

b) 必要に応じて、[Virtual Host Interface] テーブル で vCoN 行をクリックし、[Selection Preference] カラム で次のいずれかの値を選択します。

- [All]：明示的に割り当てられているか、未割り当てであるか、または動的に割り当てられているかどうかに関係なく、すべての設定済みの vNIC と vHBA を vCon に割り当てることができます。 これはデフォルトです。
- [Assigned Only]：vNIC と vHBA を vCon に明示的に割り当てる必要があります。 サービス プロファイルまたは vNIC または vHBA のプロパティを介して、vNIC および vHBA を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 と vHBA を vCon に割り当てることはできません。 vCon は、未割り当てか、または明示的に割り当てられているかに関係なく、すべてのスタティック vNIC と vHBA に対して使用できます。
- [Exclude Unassigned]：未割り当ての vNIC と vHBA 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ダイナミック vNIC と vHBA、およびスタティック vNIC と vHBA に対して使用できます。

c) [Assign] をクリックします。
割り当てを取り消す場合は、[Remove] をクリックします。

d) すべての vNIC および vHBA を割り当てるまで、ステップ a ～ c を繰り返します。

e) すべての vNIC および vHBA の配置を指定したら、ステップ 5 に進みます。

ステップ 4 [Create Placement Policy] をクリックした場合、[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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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 は、仮想ネットワーク インターフェイス（vCon）接続をサーバの PCIe アダプタ カードに割り当てます。 各 vCon は、vNIC および vHBA を割り当てることができる物理アダプタの仮想表現です。 1 つのアダプタを持つブレードまたはラック サーバでは、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2、vCon3 を Adapter3、vCon4 を Adapter4 に割り当てます。 2 つまたは 3 つのアダプタを備えたブレードまたはラック サーバについて、Cisco UCS は、選択した仮想スロット 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 カード付きのサーバでは、Cisco UCS は、vCon1 と vCon3 を Adapter1 に割り当て、次に vCon2 と vCon4 を Adapter2 に割り当てます。 3 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 と vCon4 を Adapter2、vCon3 を Adapter3 に割り当てます。 これはデフォルトのスキームです。 • [Linear Ordered]：2 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 と vCon2 を Adapter1 に割り当て、次に vCon3 と vCon4 を Adapter2 に割り当てます。 3 つのアダプタ カード付きのサーバでは、Cisco UCS は、vCon1 を Adapter1、vCon2 を Adapter2 に割り当て、次に vCon3 と vCon4 を Adapter3 に割り当てます。 （注） N20-B6620-2 および N20-B6625-2 ブレード サーバでは、2 つのアダプタには左から右に番号が付けられ、vCon には右から左に番号が付けられます。 いずれかのブレード サーバに単一のアダプタがある場合、Cisco UCS は、すべての vCon をそのアダプタに割り当てます。 サーバに 2 つのアダプタがある場合、vCons の割り当ては、仮想スロット マッピング スキームによって異なります。 • [Round Robin]：Cisco UCS は、vCon2 と vCon4 を Adapter1 に割り当て、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 Adapter1 に割り当て、vCon1 と vCon2 を Adapter2 に割り当てます。 Cisco UCS によって vCon が割り当てられた後、各 vCon の [Selection Preference] に基づいて vNIC と vHBA が割り当てられます。

b) 各 [Virtual Slot] の [Selection Preference] カラムで、ドロップダウン リストから次のいずれかを選択します。

- [All]：明示的に割り当てられているか、未割り当てであるか、または動的に割り当てられているかどうかに関係なく、すべての設定済みの vNIC と vHBA を vCon に割り当てることができます。 これはデフォルトです。
- [Assigned Only]：vNIC と vHBA を vCon に明示的に割り当てる必要があります。 サービス プロファイルまたは vNIC または vHBA のプロパティを介して、vNIC および vHBA を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 と vHBA を vCon に割り当てることはできません。 vCon は、未割り当てか、または明示的に割り当てられているかに関係なく、すべてのスタティック vNIC と vHBA に対して使用できます。
- [Exclude Unassigned]：未割り当ての vNIC と vHBA 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ダイナミック vNIC と vHBA、およびスタティック vNIC と vHBA に対して使用できます。

c) [OK] をクリックします。

d) ダイアログボックスを閉じたら、作成したポリシーを [Select Placement] ドロップダウン リストで選択します。

ステップ 5 [Next] をクリックします。

次の作業

ページ 6：サーバのブート順序の設定, （644 ページ）を実行します。

ページ 6：サーバのブート順序の設定

この手順は、ページ 5：vNIC/vHBA 配置の設定, （639 ページ）から直接続くものです。 [Create Service Profile Template] ウィザードの [Server Boot Order] ページで、サーバのブート順序オプションを設定する方法について説明します。

ヒント　ブート ポリシーのブート順序には、ローカル ディスクと SAN LUN の両方ではなく一方のみをインクルードし、サーバが誤ったストレージ タイプからブートしないようにすることを推奨します。 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。

手順

ステップ 1　[Boot 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 Boot Policy to use]	このテンプレートから作成された各サービス 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 9 に進みます。
[Create a Specific Boot Policy]	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 3 に進みます。
[Boot Policies *Policy_Name]*	このテンプレートから作成された各サービス 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 プロファイルおよびテンプレートがアクセスできるポリシーを作成する場合は、ステップ 2 に進みます。 それ以外の場合は、リストでポリシーを選択し、ステップ 9 に進みます。

ステップ 2　[Create Boot Policy] をクリックして、すべてのサービス プロファイルおよびテンプレートが使用できるブート ポリシーを作成する場合、次の手順を実行します。

a) [Create Boot Policy] 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。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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

b) ステップ 3 に進みます。

ステップ 3 （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、[Reboot on boot Order Change] チェックボックスがブート ポリシーに対して選択されており、CD-ROM またはフロッピーがブート順で最後のデバイスの場合に、デバイスを取り外すか、装着しても、ブート順に直接影響は及ぼされず、サーバはリブートされません。

ステップ 4 （任意） 必要に応じて、[Enforce vNIC/vHBA/iSCSI Name] チェックボックス を確認します。

- これをオンにすると、Cisco UCS Manager は設定エラーを表示し、[Boot Order] テーブルにリストされている vNIC、vHBA、または iSCSI の vNIC の 1 つ以上がサービス プロファイルのサーバ設定と一致するかどうかをレポートします。
- オフになっている場合、（ブート オプションに適するように）Cisco UCS Manager はサービス プロファイルのサーバ設定から vNIC、vHBA、または iSCSI vNIC を使用します。 ブート ポリシーで指定された vNIC、vHBA、または iSCSI の vNIC がサービス プロファイルのサーバ設定と一致するかどうかはレポートしません。

ステップ 5 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。
   - Add Local Disk
   - Add CD-ROM
   - Add Floppy
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 6 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 7 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 で次のフィールドに値を入力し、[OK] をクリックします。

名前	説明
[vHBA] フィールド	SAN ブートに使用する vHBA の名前を入力します。

名前	説明
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブート デバイス クラスに定義されている最初のアドレス。 ブート ポリシーには、1 つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブート デバイス クラスに定義されている 2 番目のアドレス。 各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブート デバイス」や「セカンダリ ブート デバイス」はブート順序を表す用語ではありません。 同じデバイス クラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

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 で次のフィールドに値を入力して、[OK] をクリックします。

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

名前	説明
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブートデバイスクラスに定義されている最初のアドレス。ブート ポリシーには、1 つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブートデバイスクラスに定義されている 2 番目のアドレス。 各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブートデバイス」や「セカンダリ ブートデバイス」はブート順序を表す用語ではありません。 同じデバイスクラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

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 8 iSCSI 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) [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。

b) [iSCSI vNICs] 領域で、[Boot Order] テーブルに追加するサーバを起動する iSCSI vNIC をダブルクリックします。

c) [iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。
2 個の iSCSI vNIC がある場合は、ブート パラメータを設定する iSCSI vNIC を選択します。

d) **[Set iSCSI Boot Parameters]** ダイアログボックスのフィールドに値を入力して [OK] をクリックします。
フィールドの詳細については、iSCSI ブート パラメータの設定, （535 ページ）を参照してください。

e) ステップ c および d を繰り返し、追加の iSCSI vNIC に対してブート パラメータを設定します。

ステップ 9 すべてのサービスプロファイルおよびテンプレートが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 でこのポリシーを選択します。

ステップ 10 [Next] をクリックします。

次の作業

ページ 7：メンテナンス ポリシーの追加, （649 ページ）を実行します。

ページ 7：メンテナンス ポリシーの追加

この手順は、ページ6：サーバのブート順序の設定，（644ページ）から直接続くものです。[Create Service Profile (expert)] ウィザードの [Maintenance Policy] ページでサービス プロファイルにメンテナンス ポリシーを追加する方法について説明します。

手順

ステップ 1 [Maintenance 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 a Maintenance Policy to Use]（デフォルトのポリシーが表示されます）	このサービスプロファイルにデフォルトのメンテナンスポリシーを割り当てます。 ステップ 4 に進みます。
[Maintenance Policies] [*Policy_Name*]	サービス プロファイルに既存のメンテナンス ポリシーを割り当てます。 このオプションを選択すると、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 Maintenance 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、リストでポリシーを選択し、ステップ 4 に進みます。

ステップ 2 [Create Maintenance Policy] をクリックして、すべてのサービス プロファイルおよびテンプレートが使用できるメンテナンス ポリシーを作成する場合、次の手順を実行します。

a) [Create Maintenance Policy] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Reboot Policy] フィールド	サービス プロファイルがサーバに関連付けられているか、サーバにすでに関連付けられているサービス プロファイルに変更を加えた場合、プロセスを完了するには、サーバをリブートする必要があります。 [Reboot Policy] フィールドは、このメンテナンス ポリシーを含むサービス プロファイルに関連付けられたサーバについて、リブートがいつ行われるかを決定します。 次のいずれかになります。 • [Immediate]：サービス プロファイルのアソシエーションが完了するか、サービス プロファイルの変更がユーザによって保存されるとすぐに、サーバが自動的にリブートされます。 • [User Ack]：ユーザがサービス プロファイルのアソシエーションが完了するか、または変更を行うと、サーバを手動で再起動する必要があります。 • [Timer Automatic]：Cisco UCS はすべてのサービス プロファイルのアソシエーションと変更を、[Schedule] フィールドに示されているスケジュールによって定義されたメンテナンス期間延長します。
[Schedule] ドロップダウン リスト	[Reboot Policy] が [Timer Automatic] に設定されている場合、スケジュールによってメンテナンス操作をサーバに適用できる時期が指定されます。 Cisco UCS はサーバをリブートし、スケジュール設定された時間にサービス プロファイルの変更を完了します。

名前	説明
[Create Schedule] リンク	このリンクをクリックすると、このCisco UCSドメイン内のすべてオブジェクトに使用できる新しいスケジュールが作成されます。

b) [OK] をクリックし、ステップ 3 に進みます。

ステップ 3 すべてのサービスプロファイルおよびテンプレートがアクセスできる新しいブートポリシーを作成したら、[Maintenance Policy] ドロップダウン リストでこのポリシーを選択します。

ステップ 4 [Next] をクリックします。

次の作業

ページ 8：サーバの割り当てオプションの指定, （651 ページ）を実行します。

ページ 8：サーバの割り当てオプションの指定

この手順は、ページ 7：メンテナンス ポリシーの追加, （649 ページ）から直接続くものです。[Create Service Profile Template] ウィザードの [Server Assignment] ページで、このテンプレートから作成されたサービス プロファイルへのサーバの割り当て方法を指定する方法について説明します。

手順

ステップ 1 [Pool Assignment] 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
[Assign Later]	サービス プロファイル テンプレートを作成して設定したら、サーバを割り当てることができます。 ステップ 2 に進みます。
Select from a Pool *Pool_Name*	ドロップダウン リストの最下部のリストからサーバ プールを選択します。 Cisco UCS Manager で、このテンプレートから作成したサービス プロファイルにこのプールのサーバが割り当てられます。 ステップ 2 に進みます。

ステップ 2 [Power State] 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て、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られた場合にサーバに適用される電源の状態を設定します。

- [Down]：プロファイルがサーバに関連付けられる前はサーバの電源を切断しておく場合

- [Up]：プロファイルがサーバに関連付けられる前にサーバの電源を投入しておく場合

デフォルトでは、サーバの電源は投入されています。

ステップ 3 サービスプロファイルがサーバに関連付けられた後にそのサービスプロファイルの移行を制限する場合は、[Restrict Migration] チェックボックスをオンにします。
移行を制限しない場合は、既存のサービス プロファイルを移行する前に、Cisco UCS Manager による新規サーバに対する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 4 （任意） [Firmware Management] 領域で次の手順を実行し、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られているサーバで、ポリシーを使用してファームウェアをアップデートします。

a) [Firmware Management] バーの下矢印をクリックします。
b) 次のフィールドに入力します。

名前	説明
[Host Firmware] ドロップダウン リスト	ホスト ファームウェア パッケージをこのサービス プロファイルと関連付けるには、その名前をドロップダウン リストから選択します。
[Create Host Firmware Package] リンク	ホスト ファームウェア パッケージを作成する場合は、このリンクをクリックします。

ステップ 5 [Next] をクリックします。

次の作業

ページ 9：動作ポリシーの追加, （652 ページ）を実行します。

ページ 9：動作ポリシーの追加

この手順は、ページ 8：サーバの割り当てオプションの指定, （651 ページ）から直接続くものです。 [Create Service Profile Template] ウィザードの [Operational Policies] ページでサービス プロファイルテンプレートに動作ポリシーを追加する方法について説明します。 これらのポリシーは、任意です。

手順

ステップ 1 デフォルトの BIOS 設定を上書きし、サービスプロファイル全体で設定するには、下矢印をクリックして [BIOS Configuration] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[BIOS Policy] ドロップダウン リスト で適切な BIOS ポリシーを選択します。
- すべてのサービス プロファイルで使用できる BIOS ポリシーを作成するには、[Create BIOS Policy]をクリックし、ダイアログボックスのフィールドに値を入力してから、[BIOS Policy] ドロップダウン リスト で適切な BIOS ポリシーを選択します。

BIOS ポリシーの作成方法の詳細については、BIOS ポリシーの作成, （470 ページ）を参照してください。

ステップ 2 サーバの Cisco Integrated Management Controller（CIMC）への外部アクセスを提供するには、下矢印をクリックして [External IPMI Management Configuration] バーを展開し、IPMI プロファイルおよび Serial over LAN ポリシーを追加します。
外部アクセスを提供しない場合は、ステップ 4 に進みます。

ステップ 3 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 IPMI プロファイルを追加するには、次の手順のいずれかを実行します。

- 既存のポリシーを追加するには、[IPMI Access Profile] ドロップダウン リストで適切な IPMI プロファイルを選択します。
- 適切なユーザ アクセスが設定されている IPMI プロファイルが [IPMI Access Profile] ドロップダウン リストに含まれない場合、[Create Access IPMI Profile] リンクをクリックしてすべてのサービス プロファイル テンプレートで使用できる IPMI プロファイルを作成してから、[IPMI Access Profile] ドロップダウン リストでこのプロファイルを選択します。

IPMI プロファイルの作成方法の詳細については、IPMI アクセス プロファイルの作成, （473 ページ）を参照してください。

ステップ 4 このテンプレートから作成したサービス プロファイルに Serial over LAN ポリシーを追加するには、次の手順のいずれかを実行します。

- 既存のポリシーを追加するには、[SoL Configuration Profile] ドロップダウン リストで適切な Serial over LAN ポリシーを選択します。
- このテンプレートから作成されたサービス プロファイルだけが使用できる Serial over LAN ポリシーを作成するには、[Create a Specific SoL Policy]を[SoL Configuration Profile] ドロップダウン リストで選択し、[Admin State] フィールドおよび[Speed] ドロップダウン リストを入力します。
- すべてのサービス プロファイル テンプレートが使用できる Serial over LAN ポリシーを作成するには、[Create Serial over LAN Policy] リンクをクリックし、ダイアログボックスのフィールドに値を入力してから、[SoL Configuration Profile] ドロップダウン リストでこのポリシーを選択します。

Serial over LAN ポリシーの作成方法の詳細については、Serial over LAN ポリシーの作成, （486 ページ）を参照してください。

ステップ 5 サーバの CIMC への外部アクセスに必要な管理 IP を設定するには、下矢印をクリックして [Management IP Address] バーを展開し、次のオプション ボタンのいずれかをクリックします。

- [None]：管理 IP アドレスがサービス プロファイルを介してサーバに割り当てられていません。 管理 IP アドレスは、サーバ上で定義される CIMC 管理 IP アドレスに基づいています。
- [Pooled]：サービス プロファイルによって、 [Pool Name] に示すプールからの管理 IP アドレスが関連付けられたサーバに割り当てられます。 サービス プロファイルを新しいサーバに移行すると、管理 IP アドレスもサービス プロファイルとともに移動します。

ステップ 6 しきい値をモニタし、関連付けられているサーバの統計情報を収集するには、下矢印をクリックして [Monitoring Configuration] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[Threshold Policy] ドロップダウン リストで適切なしきい値ポリシーを選択します。
- すべてのサービス プロファイルで使用できるしきい値ポリシーを作成するには、[Create Threshold Policy] リンクをクリックし、ダイアログボックスのフィールドに値を入力してから、[Threshold Policy] ドロップダウン リストでこのポリシーを選択します。

しきい値ポリシーの作成方法の詳細については、サーバおよびサーバ コンポーネントのしきい値ポリシーの作成，（808 ページ）を参照してください。

ステップ 7 電力制御ポリシーとサービスプロファイルテンプレートを関連付けるには、下矢印をクリックして [Power Control Policy Configuration] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[Power Control Policy] ドロップダウン リストで適切な電力制御ポリシーを選択します。
- すべてのサービスプロファイルおよびテンプレートで使用できる電力制御ポリシーを作成するには、[Create Power Control Policy] リンク をクリックし、ダイアログボックスのフィールドに値を入力してから、[Power Control Policy] ドロップダウン リストでこのポリシーを選択します。

電源モジュールの制御ポリシーの作成方法の詳細については、電力制御ポリシーの作成,（695 ページ）を参照してください。

ステップ 8 スクラブ ポリシーとサービス プロファイル テンプレートを関連付けるには、下矢印をクリックして [Scrub Policy] バーを展開し、次のいずれかの手順を実行します。

- 既存のポリシーを追加するには、[Scrub Policy] ドロップダウン リスト で適切なスクラブ ポリシーを選択します。
- すべてのサービス プロファイルおよびテンプレートで使用できるスクラブ ポリシーを作成するには、[Create Scrub Policy] リンク をクリックし、ダイアログボックスのフィールドに値を入力してから、[Scrub Policy] ドロップダウン リスト でこのポリシーを選択します。

スクラブ ポリシーの作成方法の詳細については、スクラブ ポリシーの作成,（485 ページ）を参照してください。

ステップ 9 [Finish] 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 1 つ以上のサービス プロファイルを作成する

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profile Templates] を展開します。

ステップ 3 サービス プロファイルの基盤として使用するサービス プロファイル テンプレート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 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、次のフィールドに値を入力します。

名前	説明
[Naming Prefix] フィールド	テンプレート名に使用する接頭辞。 システムによってサービスプロファイルが作成されるとき、この接頭辞に一意の数値 ID が追加されます。 1 ～ 29 文字の英数字を入力します。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。 たとえば、MyProfile という接頭辞を指定した場合、2 つのプロファイルを要求すると、最初のサービスプロファイルの名前は MyProfile1 になり、2 つめの名前は MyProfile2 になります。 後日、さらに 3 つのプロファイルを同じ接頭辞で作成すると、それらの名前は MyProfile3、MyProfile4、および MyProfile5 になります。
[Number] フィールド	作成するサービス プロファイルの数。 1 ～ 255 の範囲内の数を入力してください。

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

はじめる前に

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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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) [Template Based Service Profile] オプション 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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

c) [Service Profile Template] 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。

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

はじめる前に

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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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) [Template Based Service Profile]オプション 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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

c) [Service Profile Template] 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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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、次のフィールドに値を入力します。

名前	説明
[Service Profile Template Name] フィールド	サービス プロファイル テンプレートの名前。 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）以外の特殊文字またはスペースは使用できません。また、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とサービスプロファイルテンプレートで一意である必要があります。
[Org] ドロップダウン リスト	このテンプレートを関連付ける組織を選択します。
[Type] フィールド	次のいずれかになります。 • [Initial Template]：テンプレートが変更されても、このテンプレートから作成されたサービス プロファイルはアップデートされません。 • [Updating Template]：テンプレートが変更されると、このテンプレートから作成されたサービスプロファイルがアップデートされます。

ステップ 6 [OK] をクリックします。

サービス プロファイルの管理

サービス プロファイルのクローン化

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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）以外の特殊文字またはスペースは使用できません。また、

この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

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。

サーバまたはサーバ プールとのサービス プロファイルの関連付け

作成時にサービスプロファイルとブレードサーバまたはサーバプールを関連付けなかった場合、またはサービス プロファイルを関連付けるブレード サーバまたはサーバ プールを変更する場合には、次の手順を実行します。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 新規のサーバやサーバプールと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、[Change Service Profile Association] 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
Server Pool	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が割り当てられます。 ステップ 7 に進みます。
Server	ナビゲーション ツリーで使用可能な目的のサーバに移動し、サービス プロファイルに割り当てられるサーバを選択します。 ステップ 7 に進みます。

オプション	説明
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 サービスプロファイルがサーバに関連付けられた後にそのサービスプロファイルの移行を制限する場合は、[Restrict Migration] チェックボックスをオンにします。
移行を制限しない場合は、既存のサービス プロファイルを移行する前に、Cisco UCS Manager による新規サーバに対する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。

サーバまたはサーバ プールとのサービス プロファイルの関連付けの解除

サービス プロファイルの関連付けを解除すると、Cisco UCS Manager はサーバのオペレーティング システムのシャットダウンを試みます。 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。

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 サーバや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て [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、サービス プロファイルの関連付けの解除を確定します。

ステップ 6 （任意） サーバのステータスおよび Finite State Machine（FSM; 有限状態マシン）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 プロファイルの名前変更

サービス プロファイルの名前を変更すると、次のことが発生します。

- サービス プロファイルの前の名前を参照するイベント ログと監査ログは、その名前で保持されます。
- 名前の変更操作をログに記録するための新しい監査レコードが作成されます。
- 前の名前で保持されていた、サービスプロファイルに対する障害のすべてのレコードは、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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 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] ペインの [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の[New Name] フィールド[New Name] 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）以外の特殊文字またはスペースは使用できません。また、この名前は同じ組織内のすべてのサービス プロファイルとサービス プロファイル テンプレートで一意である必要があります。

ステップ 8 [OK] をクリックします。

サービス プロファイルでの UUID の変更

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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を変更するために UUID を必要とするサービス プロファイルを選択します。

ステップ 5 [Work] ペインの [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。

オプション	説明
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） XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX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 プロファイルでのブート順序の変更

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 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 1 つを選択します。

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。

オプション	説明
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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、[Reboot on boot Order Change] チェックボックスがブート ポリシーに対して選択されており、CD-ROM またはフロッピーがブート順で最後のデバイスの場合に、デバイスを取り外すか、装着しても、ブート順に直接影響は及ぼされず、サーバはリブートされません。

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 を確認します。

- これをオンにすると、Cisco UCS Manager は設定エラーを表示し、[Boot Order] テーブルにリストされている vNIC、vHBA、または iSCSI の vNIC の 1 つ以上がサービス プロファイルのサーバ設定と一致するかどうかをレポートします。
- オフになっている場合、（ブート オプションに適するように）Cisco UCS Manager はサービス プロファイルのサーバ設定から vNIC、vHBA、または iSCSI vNIC を使用します。 ブート ポリシーで指定された vNIC、vHBA、または iSCSI の vNIC がサービス プロファイルのサーバ設定と一致するかどうかはレポートしません。

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。
   - Add Local Disk
   - Add CD-ROM

- Add Floppy

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 で次のフィールドに値を入力し、[OK] をクリックします。

名前	説明
[vHBA] フィールド	SAN ブートに使用する vHBA の名前を入力します。
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブート デバイス クラスに定義されている最初のアドレス。 ブート ポリシーには、1 つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブート デバイス クラスに定義されている 2 番目のアドレス。 各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブート デバイス」や「セカンダリ ブート デバイス」はブート順序を表す用語ではありません。 同じデバイス クラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

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 で次のフィールドに値を入力して、[OK] をクリックします。

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

名前	説明
[Type] フィールド	次のいずれかになります。 • [Primary]：関連するブートデバイスクラスに定義されている最初のアドレス。ブート ポリシーには、1 つのプライマリ LAN、SAN、または iSCSI ブート ロケーションのみを指定できます。 • [Secondary]：関連するブートデバイスクラスに定義されている 2 番目のアドレス。 各ブート ポリシーには、LAN または SAN のセカンダリ ブート ロケーションを 1 つだけ設定できます。 「プライマリ ブートデバイス」や「セカンダリ ブートデバイス」はブート順序を表す用語ではありません。 同じデバイスクラス内での実際のブート順序は、PCIe バス スキャン順序により決定されます。

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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 [Create vNIC] ダイアログボックスで、次の手順を実行します。

a) 次のフィールドに値を入力して、vNIC の ID 情報を指定します。

名前	説明
[Name] フィールド	この vNIC のユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vNIC Template] チェックボックス	テンプレートを使用して vNIC を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vNIC Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vNIC テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vNIC Template] リンク	vNIC テンプレートを作成する場合は、このリンクをクリックします。
[MAC Address Assignment] ドロップダウン リスト	項目 • デフォルトの MAC アドレス プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた MAC アドレスを使用する場合は、[Hardware Default] を選択します。 • 特定の MAC アドレスを使用する場合は、[02:25: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。

b) ファブリック接続情報を指定するには、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。 デフォルトのファブリック インターコネクトが使用できない場合に、この vNIC から第 2 のファブリック インターコネクトにアクセスできるようにする場合は、[Enable Failover] チェックボックスをオンにします。 （注） 次の状況では、vNIC のファブリックのフェールオーバーをイネーブルにしないでください。 • Cisco UCS ドメインがイーサネット スイッチ モードで実行している場合。 vNIC のファブリック フェールオーバーは、このモードではサポートされません。 1 つのファブリック インターコネクトですべてのイーサネット アップリンクが失敗すると、vNICs は別のものにフェールオーバーしません。 • ファブリック フェールオーバーをサポートしないアダプタ（Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter など）があるサーバをこの vNIC に関連付ける予定がある場合。 選択した場合、サービス プロファイルとサーバを関連付けたときに、Cisco UCS Manager によって設定エラーが生成されます。
[VLANs] テーブル	次の表には、この vNIC に関連付けることができる VLAN がリストされています。 各カラムの説明は次のとおりです。 • [Select]：使用する VLAN ごとに、このカラムのチェックボックスをオンにします。 • [Name]：VLAN の名前。 • [Native VLAN]：VLAN のいずれかをネイティブ VLAN として指定するには、このカラムのオプション ボタンをクリックします。
[Create VLAN] リンク	VLAN を作成する場合は、このリンクをクリックします。

名前	説明
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケットサイズ。 1500 ～ 9216 の範囲の整数を入力します。 （注） 関連付けられた QoS ポリシーが vNIC にある場合、ここで指定される MTU は、関連付けられた QoS システム クラスで指定された MTU 以下でなければなりません。 この MTU 値が QoS システム クラスの MTU 値を超えると、データ伝送中にパケットがドロップされる可能性があります。
[Pin Group] ドロップダウン リスト	この vNIC と関連付ける LAN ピン グループを選択します。
[Create LAN Pin Group] リンク	LAN ピン グループを作成する場合は、このリンクをクリックします。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト	この vNIC と関連付ける統計情報収集ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト	この vNIC と関連付けるイーサネット アダプタ ポリシー。
[Create Ethernet Adapter Policy] リンク	イーサネット アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[Dynamic vNIC Connection Policy] ドロップダウン リスト	この vNIC が関連付けられているダイナミック vNIC 接続ポリシー。
[Create Dynamic vNIC Connection Policy] リンク	ダイナミック vNIC 接続ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト	この vNIC と関連付ける Quality Of Service ポリシー。
[Create QoS Policy] リンク	Quality Of Service ポリシーを作成する場合は、このリンクをクリックします。

名前	説明
[Network Control Policy] ドロップダウン リスト	この vNIC と関連付けるネットワーク制御ポリシー。
[Create Network Control Policy Policy] リンク	ネットワーク制御ポリシーを作成する場合は、このリンクをクリックします。

d) [OK] をクリックします。

サービス プロファイルからの vNIC の削除

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サービス プロファイル用の vHBA の作成

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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、次の手順を実行します。

a) 次のフィールドに値を入力して、vHBA の ID 情報を指定します。

名前	説明
[Name] フィールド	この vHBA 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Use vHBA Template] チェックボックス	テンプレートを使用して vHBA を作成する場合は、このチェックボックスをオンにします。 Cisco UCS Manager GUI に [vHBA Template] ドロップダウン リストが表示され、それを使用して適切なテンプレートと [Adapter Performance Profile] 領域を選択し、そこからアダプタ プロファイルを選択できます。 （注） 1 つ以上の vHBA テンプレートがシステムに存在する場合のみ、このオプションを選択できます。
[Create vHBA Template] リンク	vHBA テンプレートを作成する場合は、このリンクをクリックします。

名前	説明
[WWPN Assignment] ドロップダウン リスト	Cisco UCS が World Wide Port Node を vHBA に割り当てる方法。 Cisco UCS について、次のように設定します。 • デフォルトの WWPN プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた WWPN を使用する場合は、[Derived] を選択します。 • 特定の WWPN を使用する場合は、[20:00:00:25:B5:00:00:00]、[20:XX:XX:XX:XX:XX:XX:XX]、または [5X:XX:XX:XX:XX:XX:XX:XX] を選択し、使用する WWPN を [WWPN] フィールドに入力します。 WWPN が Cisco MDS ファイバ チャネル スイッチと互換性を持つようにするには、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • プール内の WWPN 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アドレスの数であり、2 番めの数字はそのプール内の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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[Create WWPN Pool] リンク	Cisco UCS ドメイン内のすべてのオブジェクトで使用可能な新しい WWPN プールを作成する場合は、このリンクをクリックします。
[WWPN] フィールド	[WWPN Assignment] ドロップダウン リストが手動テンプレートのいずれかに設定されている場合、手動で割り当てた WWPN。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN 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。

b) [VSAN] 領域で、次のフィールドに値を入力します。

名前	説明
[Fabric ID] フィールド	コンポーネントに関連付けられたファブリック インターコネクトです。
[Select VSAN] ドロップダウン リスト ボックス	この vHBA と関連付ける VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。
[Pin Group] ドロップダウン リスト ボックス	この vHBA が関連付けられる SAN ピン グループ。
[Create SAN Pin Group] リンク	ピン グループを作成する場合は、このリンクをクリックします。
[Persistent Binding] フィールド	次のいずれかになります。 • Disabled • Enabled
[Max Data Field Size] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の範囲の整数を入力します。 デフォルトは 2048 です。
[Operational Parameters] セクション	
[Stats Threshold Policy] ドロップダウン リスト ボックス	この vHBA と関連付ける統計しきい値ポリシー。

c) [Adapter Performance Profile] 領域で、次のフィールドに値を入力します。

名前	説明
[Adapter Policy] ドロップダウン リスト ボックス	この vHBA と関連付けるファイバ チャネル アダプタ ポリシー。
[Create Fibre Channel Adapter Policy] リンク	ファイバ チャネル アダプタ ポリシーを作成する場合は、このリンクをクリックします。
[QoS] ドロップダウン リスト ボックス	この vHBA と関連付ける Quality Of Service ポリシー。

名前	説明
[Create QoS Policy] リンク	QoS ポリシーを作成する場合は、このリンクをクリックします。

d) [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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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、次のフィールドに値を入力します。

名前	説明
[WWPN Assignment] ドロップダウン リスト	Cisco UCS が World Wide Port Node を vHBA に割り当てる方法。Cisco UCS について、次のように設定します。 • デフォルトの WWPN プールを使用する場合は、このフィールドを [Select (pool default used by default)] のままにします。 • 製造元でサーバに割り当てられた WWPN を使用する場合は、[Derived] を選択します。 • 特定の WWPN を使用する場合は、[20:00:00:25:B5:00:00:00]、[20:XX:XX:XX:XX:XX:XX:XX]、または [5X:XX:XX:XX:XX:XX:XX:XX] を選択し、使用する WWPN を [WWPN] フィールドに入力します。 WWPN が Cisco MDS ファイバ チャネル スイッチと互換性を持つようにするには、WWPN テンプレート 20:00:00:25:B5:XX:XX:XX を使用します。 • プール内の WWPN 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アドレスの数であり、2 番めの数字はそのプール内の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、2 つのプール カテゴリがある可能性があります。 [Domain Pools] は Cisco UCS ドメインにローカルに定義され、[Global Pools] は Cisco UCS Central に定義されます。
[WWPN] フィールド	[WWPN Assignment] ドロップダウン リストが手動テンプレートのいずれかに設定されている場合、手動で割り当てた WWPN。 WWPN は、20:00:00:00:00:00:00:00 ～ 20:FF:FF:FF:FF:FF:FF:FF または 50:00:00:00:00:00:00:00 ～ 5F:FF:FF:FF:FF:FF:FF:FF の範囲内で指定できます。 WWPN 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。

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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サービス プロファイルからの vHBA の削除

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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 [Servers] タブで、[Servers] > [Service Profiles] 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 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] ペインの[Storage] > [vHBA Initiator Groups]をクリックします。

ステップ 5 [Select vHBA Initiator Groups] 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 6 [Create vHBA Initiator Group] ダイアログボックスに名前と説明を設定するため、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	vHBA イニシエータ グループの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	グループの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

ステップ 7 vHBA イニシエータ グループに含む各 vHBA について、[Select vHBA Initiators] テーブルで、[Select] カラム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、次のいずれかのオプションを選択します。

- [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[Create Storage Connection Policy] リンク内の他の vHBA イニシエータ グループから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、Cisco UCS ドメインをクリックします。 詳細については、ファイバ チャネル ストレージ接続ポリシーの作成, （424 ページ）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ら、ステップ 10 に進みます。
- この vHBA イニシエータ グループにだけ使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] 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 [Specific Storage Connection Policy] 領域で、この vHBA イニシエータ グループにだけ使用可能なストレージ接続ポリシーを作成するには、次のフィールドに値を入力します。

名前	説明
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Zoning Type] フィールド	次のいずれかになります。 • [None]：Cisco UCS Manager は、ファイバ チャネル ゾーン分割を設定しません。 • [Single Initiator Single Target]：Cisco UCS Manager は、各 vHBA とストレージ ポートのペアに対して 1 つのゾーンを自動的に作成します。 各ゾーンには、2 つのメンバがあります。 ゾーン数がサポートされている最大数を超えると予想される場合を除いて、このような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、各 vHBA に対して 1 つのゾーンを自動的に作成します。 ゾーン数がサポートされている最大数を超えると予想される場合は、このような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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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すると、Cisco UCS Manager によって、サービス プロファイル テンプレートで定義された値でサービス 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テンプレートと一致しない場合、Cisco UCS Manager によってサービス 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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サービス プロファイルの削除

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 5 [OK] をクリックします。

サービス プロファイル テンプレートの管理

サーバ プールとサービス プロファイル テンプレートの関連付け

作成時にサービス プロファイル テンプレートとサーバ プールを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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profile Templates] 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。

サーバ プールとサービス プロファイル テンプレートの関連付けの解除

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profile Templates] 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サービス プロファイル テンプレートでの UUID の変更

手順

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

ステップ 2 [Servers] タブで、[Servers] > [Service Profile Templates] 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 テンプレートが含まれている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 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] ペインの [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。
[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。
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 接尾辞プールを変更しても、そのテンプレートによって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 により変更されません。 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、これを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 がインクルードされている。
- 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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [OK] をクリックします。

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、そのテンプレートにより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 により変更されません。 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、これを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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 9 [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、そのテンプレートによって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 により変更されません。 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、これを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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 9 [OK] をクリックします。

第 34 章

Cisco UCS での電源の管理

この章の内容は、次のとおりです。

- Cisco UCS での電源管理，687 ページ
- ラック サーバの電源管理，687 ページ
- 電源管理の注意事項，688 ページ
- 電源ポリシーの設定，688 ページ
- グローバル キャップ ポリシーの設定，689 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，690 ページ
- 手動ブレード レベルの電力制限の設定，696 ページ

Cisco UCS での電源管理

次の機能のいずれかを設定することにより、Cisco UCS Manager から電源を管理できます。

- Cisco UCS ドメインのすべてのシャーシに対する電源の冗長性
- ポリシー方式のシャーシ レベルの電力制限
- 手動ブレード レベルの電力制限

ラック サーバの電源管理

電力制限はラック サーバではサポートされません。

電源管理の注意事項

CIMC がリセットされると、Cisco UCS の電力モニタリング機能は、CIMC をリブートするために短時間使用できなくなります。 通常、これには 20 秒しかかかりませんが、その時間内にピーク時の電力制限を超過する可能性があります。 非常に低い電力制限環境で、設定された電力制限を超過し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ずらすことを検討してください。

電源ポリシーの設定

電源ポリシー

電源ポリシーは、Cisco UCS ドメインでのすべてのシャーシの電源の冗長性を指定するグローバル ポリシーです。 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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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]：すべての取り付け済み電源装置がオンになり、負荷が均等に分散されます。小規模の構成（必要な電力が 2500 W 未満）に限り、1 つの電源装置でも電力を供給できます。
- [N+1]：非冗長性を満たす電源装置の合計数に、冗長性を与える追加の電源装置を 1 つ加えたものです。これらすべての電源装置がオンになり、シャーシの電力負荷が均等に分担されます。 電源装置がこれ以上取り付けられても、それらは Cisco UCS Manager によって「オフ」状態に設定されます。
- [Grid]：2 つの電源がオンになります。そうならない場合、シャーシに N+1 よりも高い冗長性が要求されます。 電源の 1 つに障害が発生しても（それにより、1 つまたは 2 つの電源装置への電力供給が失われる）、別の電力回路に接続されている残りの電源装置により、シャーシへの電力供給は継続されます。

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。

ステップ 6 [Save Changes] をクリックします。

グローバル キャップ ポリシーの設定

グローバル キャップ ポリシー

グローバルキャップポリシーは、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ブレード レベルの電力制限のどちらをシャーシ内のすべてのサーバに適用するかを指定するグローバルポリシーです。

デフォルトの電力制限方式（ポリシー方式のシャーシ グループの電力制限）を使用することを推奨します。

重要 手動ブレード レベルの電力制限の設定に加えた変更は、そのポリシー方式のシャーシ グループの電力制限に設定されたグループまたは設定オプションの損失につながります。

グローバル キャップ ポリシーの設定

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 Cap Policy] 領域で、Cisco UCS ドメインで使用される電源キャップの管理モードを決定するため、[Allocation Method] 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。

- [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 サーバごとに設定されます。 このオプションを選択すると、電源のグループを作成することはできません。
- [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ている電力制御ポリシーに沿ったシャーシ レベルで設定されます。 このオプションを選択すると、1 つ以上のシャーシを含む電力グループを Cisco UCS ドメインに作成することもできます。

デフォルトでは、電力割り当ては電力制御ポリシーに沿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。

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

ポリシー方式の電源シャーシ グループの電力制限がグローバル キャップ ポリシーで選択されていると、Cisco UCS は、電力障害による損失の危険性を回避してサーバのオーバーサブスクリプションを維持できます。 これは、2層プロセスによって実現されます。 シャーシ レベルで、Cisco UCS は電力グループのメンバ間で使用可能な電力量を分割します。 ブレード レベルで、シャーシへ割り当てられた電力量は、優先順位に基づいてブレード間で分割されます。

サービス プロファイルが関連付けまたは関連付け解除されるたびに、UCS Manager はシャーシ内の各ブレードサーバの電力の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 プロファイルから、優先順位の高いサービス プロファイルに電力を再配布します。

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、UCS 電力グループは 1 秒未満で電力を制限します。 シャーシの電力の配布が最適化されるまでの 20 秒間、ブレードをその制限に留めておく必要があります。 これは、一時的なスパイクの需要に反応することがないよう、意図的にゆっくりとしたタイムスケールで実行されます。

（注） システムには、スロットが空でも、各スロットでサーバを起動できるだけの十分な電力が用意されています。 この予約電力は多くの電力を必要とするサーバでは利用できません。 この電力制限に準拠しないブレードは、中断またはシャットダウンします。

電力グループの設定

電力グループ

電力グループは、同じ配電ユニット（PDU）からすべての電力を取る一連のシャーシです。 Cisco UCS Manager に、1 つ以上のシャーシを含む電力グループを作成し、次にその電力グループに対して、ピーク時の電力制限を AC ワットで設定することができます。

シャーシ レベルでの電力制限には次の仕様が必要です。

- IOM、CIMC、および BIOS のバージョン 1.4 以上
- 2 台の PSU

ピーク時の電力制限は、特定の電力グループ内のすべてのブレード サーバで使用可能な最大電力を表す固定値です。 ブレードを追加する、またはブレードを電力グループから削除する一方で、

手動でピーク時の電力値を変更しない場合は、電力グループは、その電力グループ内のすべてのブレードの基本的な電源投入時の要件に対応するために、ピーク時の電力制限を調整します。

シャーシごとに、最低 1556 AC ワットを設定する必要があります。 これによって、DC 電力が完全に装着されたシャーシへの電力供給に必要な電力の最小量である 1400 W に変換されます。

シャーシが電力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各サービスプロファイルも、その電力グループの一部になります。 同様に、シャーシに新しいブレードを追加すると、そのブレードは、本質的に、シャーシの電力グループの一部になります。

（注） 電力グループを作成することは、サーバ プールを作成することと同じではありません。 ただし、電力修飾子を作成し、これをサーバ プール ポリシーに追加することによって、同じ電力グループのメンバをサーバ プールに追加できます。

シャーシが取り外しまたは削除されると、そのシャーシは電力グループから削除されます。

次のテーブルには、電力使用量を割り当て、電力グループでの操作をする際に表示される可能性のあるエラー メッセージが記載されています。

エラー メッセージ	原因	推奨処置
`Insufficient budget for power group POWERGROUP_NAME`	電力制限をシャーシに割り当てる際に最低制限を満たしていない場合、このメッセージが表示されます。	AC での電力制限を 1556 ワット（DC の場合は 1400 ワット）より大きくします。
`Insufficient power available to discover server Chassis ID/BladeID`	新しいブレードを導入し、ブレードの検出に使用できるブートの電力が不十分な場合、このメッセージが表示されます。	次のいずれかの操作を実行して、電力使用量を再割り当てできます。 • 電力グループのシャーシまたはブレードを削除または稼働停止します。 • グループの電力使用量を上げます。 • グループのブレードに関連付けられている優先順位を下げます。

電力グループの作成

はじめる前に

グローバルな電力割り当てポリシーが[Global Policies] タブの [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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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

ステップ 6 [Create 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) 電力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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、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、電力グループに含める 1 つ以上のシャーシを選択します。

b) [>>] ボタンをクリックすると、電力グループに含まれるすべてのシャーシを表示する [Selected Chassis] テーブルに選択されたシャーシが追加されます。
[<<] ボタンで電力グループから 1 つ以上のシャーシを取り外すことができます。

c) [Next] をクリックします。

ステップ 8 [Create Power Group] ウィザードの [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
[Power Cap] フィールド	電源グループで使用可能な最大ピーク電力（W）。 0 ～ 10000000 の整数を入力します。
[Enable Dynamic Reallocation] フィールド	次のいずれかになります。 • [Chassis]：Cisco UCS で電力消費量をモニタし、電力を最大限に利用するために必要に応じてブレードの割り当てが変更されます。 • [None]：ブレードの割り当ては動的に調整されません。

b) [Finish] をクリックします。

電力グループへのシャーシの追加

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [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力グループを右クリックして、[Add Chassis Members] を選択します。

ステップ 5 [Add Chassis Members] ダイアログボックスで、次の手順を実行します。

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

b) [>>] ボタンをクリックすると、電力グループに含まれるすべてのシャーシを表示する [Selected Chassis] テーブルに選択されたシャーシが追加されます。
[<<] ボタンで電力グループから 1 つ以上のシャーシを取り外すことができます。

c) [OK] をクリックします。

電力グループからのシャーシの取り外し

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

ステップ 3 [Work] ペインの [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力グループを展開します。

ステップ 5 電力グループから取り外すシャーシを右クリックし、[Delete] を選択します。

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

電力グループの削除

手順

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

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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

ステップ 4 削除する電力グループを右クリックし、[Delete] を選択します。

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

電力制御ポリシーの設定

電力制御ポリシー

Cisco UCS は、ブレード タイプと設定とともに電力制御ポリシーでの優先度設定を使用して、シャーシ内の各ブレードに対する初期電力の割り当てを算出します。 通常の動作中に、シャーシ内のアクティブなブレードが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、優先順位の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、優先度の低い電力制御ポリシーの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 のスケールでランク付けされます。1 が最優先を示し、10 が最も低い優先順位を示します。 デフォルトの優先順位は 5 です。

ミッションクリティカル アプリケーションには非キャップと呼ばれる特殊な優先順位も使用できます。 非キャップに優先順位を設定すると、Cisco UCS では、その特定のブレード サーバから未使用の電力を利用することができなくなります。 サーバには、そのブレードが到達できる電力の最大量が割り当てられます。

（注） 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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 Power 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。 ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。
[Power Capping] フィールド	電源グループ内の電源に対する要求が電源を超える場合のサーバの処理。 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所要電力に関係なく、サーバはフル キャパシティで動作します。 • [cap]：サーバ グループ内の他のサーバに対するサーバの相対的なプライオリティに基づいて、最小限の電力容量がサーバに割り当てられます。 より多くの電力が使用可能になった場合、Cisco UCS は、電力を制限されていたサーバがそれまで以上の電力を使用することを許可します。 電源グループに供給される総電力量が低下した場合には、割り当てられる電力が低下します。 [cap] を選択すると、[Priority] フィールドが Cisco UCS Manager GUI によって表示されます。

名前	説明
[Priority] フィールド	電源の制限が有効な場合の、電源グループ内におけるサーバのプライオリティ。 1 ～ 10 の整数を入力します。ここで、最も高いプライオリティは 1 です。

ステップ 6 [OK] をクリックします。

次の作業

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

電力制御ポリシーの削除

手順

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

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

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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

手動ブレード レベルの電力制限の設定

手動ブレード レベルの電力制限

手動ブレード レベルの電力制限がグローバル キャップ ポリシーに設定されていると、Cisco UCS ドメイン内の各ブレード サーバについて、電力制限を設けることができます。

次の設定オプションを使用できます。

Enabled

サーバ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 ～ 1100 W の任意の量を指定できます。

Disabled

サーバに対して電力使用量の制限を課しません。 サーバは、必要なだけ電力を使用できます。

サーバの電力使用量の瞬間的な上昇がそのサーバ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、Cisco UCS Manager によってサーバで使用可能な電力が削減されます。 この削減により、サーバの速度（CPU 速度など）が低下する可能性があります。

（注） 手動ブレード レベルの電力制限が、[Equipment] > [Policies] > [Global Policies] > [Global Power Allocation Policy] 使用して設定されている場合、電力制御ポリシーで設定された優先順位は、現在は無関係です。

サーバのブレード レベルの電力制限の設定

はじめる前に

グローバルな電力割り当てポリシーが[Global Policies] タブの [Manual Blade Level Cap] に設定されていることを確認します。

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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) 見出しの右側にある [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	このサーバで電力が制限されるかどうか。 次のいずれかになります。 • [Unbounded]：どのような状況でも、サーバで電力は制限されません。 • [Enabled]：Cisco UCS Manager GUI に [Watts] フィールドが表示されます。 （注） 電力制限は、要求を満たすのに十分な電力がシャーシにない場合にのみ実行されます。 十分な電力がある場合、サーバは必要なだけ電力を使用できます。
[Watts] フィールド	要求を満たすのに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。 0 ～ 10000000 の整数を入力します。

ステップ 6 [Save Changes] をクリックします。

ブレード レベルの電力制限の表示

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] 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。

第 VI 部

システム管理

- タイム ゾーンの管理，701 ページ
- シャーシの管理，703 ページ
- ブレード サーバの管理，711 ページ
- ラックマウント サーバの管理，725 ページ
- KVM コンソールの起動，739 ページ
- I/O モジュールの管理，747 ページ
- 設定のバックアップと復元，749 ページ
- 失われたパスワードの復旧，771 ページ

第 35 章

タイム ゾーンの管理

この章の内容は、次のとおりです。

- タイム ゾーン，701 ページ
- タイム ゾーンの設定，701 ページ
- NTP サーバの追加，702 ページ
- NTP サーバの削除，702 ページ

タイム ゾーン

Cisco UCS は、Cisco UCS Manager で正確な時間を表示するため、ドメイン固有のタイムゾーン設定および NTP サーバを必要とします。 これらの両方を Cisco UCS ドメインに設定しなければ、時間は正確に表示されません。

タイム ゾーンの設定

手順

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

ステップ 2 [Admin] タブで、[All] を展開します。

ステップ 3 [Time Zone Management] をクリックします。

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

ステップ 5 [Time Zone] ドロップダウン リストから、Cisco UCS ドメインに使用するタイム ゾーンを選択します。

ステップ 6 [Save Changes] をクリックします。

NTP サーバの追加

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] を展開します。

ステップ 3 [Time Zone Management] をクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [NTP Servers] 領域のテーブル アイコン バーにある [+] ボタンをクリックします。

ステップ 6 [Add NTP Server] ダイアログボックスで、次の手順を実行します。

a) [NTP Server] フィールドに、この Cisco UCS ドメインに使用する NTP サーバの IP アドレスまたはホスト名を入力します。

b) [OK] をクリックします。

NTP サーバの削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] を展開します。

ステップ 3 [Time Zone Management] をクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [NTP Servers] 領域で、削除するサーバを右クリックし、[Delete] を選択します。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 7 [Save Changes] をクリックします。

第 36 章

シャーシの管理

この章の内容は、次のとおりです。

- Cisco UCS Manager GUI でのシャーシ管理，703 ページ
- シャーシの削除および稼働中止に関する注意事項，703 ページ
- シャーシの確認，704 ページ
- シャーシの稼働中止，705 ページ
- シャーシの削除，705 ページ
- 単一シャーシの再稼働，705 ページ
- 複数のシャーシの再稼働，706 ページ
- シャーシ番号の付け替え，707 ページ
- ロケータ LED の切り替え，708 ページ
- シャーシの POST 結果の表示，708 ページ

Cisco UCS Manager GUI でのシャーシ管理

Cisco UCS Manager GUI を使用して Cisco UCS ドメインのすべてのシャーシを管理およびモニタできます。

シャーシの削除および稼働中止に関する注意事項

Cisco UCS Manager 使用してシャーシを削除する、または稼働を中止するかどうかを判断する際には、次の注意事項を考慮してください。

シャーシの稼働中止

シャーシが物理的に存在し、接続されているが、一時的に設定から削除したい場合、稼働中止が実行されます。 稼働を停止しているシャーシは最終的に再稼働することが予測されるため、シャーシの情報部分は将来の使用に備えて Cisco UCS Manager によって保持されます。

シャーシの削除

システムから物理的にシャーシを削除するときに実行されます。 シャーシの物理的な削除が完了すると、そのシャーシの設定は、Cisco UCS Manager で削除されます。

（注） シャーシが物理的に存在し、接続されている場合は、そのシャーシを Cisco UCS Manager から削除することはできません。

削除したシャーシを設定に戻す必要がある場合は、再接続してから再検出する必要があります。 再検出中に、Cisco UCS Manager はシャーシに対して、以前の ID と異なる場合がある新しい ID を割り当てます。

シャーシの確認

シャーシをファブリック インターコネクトに接続するリンクの数を増減させた場合は、次の手順を実行します。 シャーシを確認することにより、Cisco UCS Manager がリンク数の変化を認識していること、および使用可能なリンクすべてでトラフィックがフローしていることを確認できます。

ファブリック インターコネクトでポートをイネーブルまたはディセーブルにした後、シャーシを再認識するまで少なくとも 1 分間待ちます。 シャーシの再認識の完了が早すぎると、シャーシからのサーバ トラフィックのピニングが、イネーブルまたはディセーブルにしたポートへの変更で更新されない場合があります。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 確認するシャーシを選択します。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域の [Acknowledge Chassis] をクリックします。

ステップ 6 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[Yes] をクリックします。
Cisco UCS Manager によって、シャーシの接続が解除され、システム内にシャーシとファブリック インターコネクトとの接続が再確立されます。

シャーシの稼働中止

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 稼働を停止するシャーシを選択します。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Decommission Chassis] をクリックします。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。
稼働が停止するまでには、数分間かかります。 シャーシが構成から削除されたら、Cisco UCS Manager でシャーシが [Decommissioned] タブに追加されます。

シャーシの削除

はじめる前に

次の手順を実行する前に、シャーシを物理的に取り外します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 削除するシャーシを選択します。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で [Remove Chassis] をクリックします。

ステップ 6 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[Yes] をクリックします。
削除が完了するまでに数分かかる場合があります。

単一シャーシの再稼働

この手順により、シャーシがコンフィギュレーションに再度追加され、このシャーシにシャーシディスカバリポリシーが適用されます。 この手順を実行すると、シャーシおよびシャーシ内のすべてのサーバにアクセスできるようになります。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで [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 再稼働するシャーシの場合、次の手順を実行します。

a) シャーシを右クリックし、[Re-commission Chassis] を選択します。

b) [Re-commission Chassis] ダイアログボックスの [Chassis ID] フィールドで、シャーシに割り当てる ID を入力するか、矢印を使用して ID を選択します。

c) [OK] をクリックします。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。この手順が終 了するまでに数分かかる場合があります。 シャーシが再稼働すると、Cisco UCS Manager はシャーシ検出ポリシーを実行し、シャーシを [Navigation] ペインのリストに追加します。

複数のシャーシの再稼働

この手順により、シャーシがコンフィギュレーションに再度追加され、このシャーシにシャーシディスカバリ ポリシーが適用されます。 この手順を実行すると、シャーシおよびシャーシ内のすべてのサーバにアクセスできるようになります。

（注） 複数のシャーシを同時に再稼働する場合、シャーシに番号を付け直すことはできません。 Cisco UCS Manager は、シャーシに登録されていた同じ ID を割り当てます。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで [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 再稼働する各シャーシの行で、[Re-commission] 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。

ステップ 7 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

この手順が終 了するまでに数分かかる場合があります。 シャーシが再稼働すると、Cisco UCS Manager はシャーシ検出ポリシーを実行し、シャーシを [Navigation] ペインのリストに追加します。

シャーシ番号の付け替え

（注） Cisco UCS Manager を使用してブレードサーバに番号を付け直すことはできません。 ブレードサーバに割り当てられた ID は、シャーシの物理スロットによって決まります。 ブレードサーバに番号を付け直すには、シャーシの別のスロットにサーバを物理的に移動する必要があります。

はじめる前に

シャーシ間で ID を交換する場合は、最初にシャーシを解放し、リナンバリング手順を進める前にシャーシの稼働中止 FSM が完了するまで待つ必要があります。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 [Chassis] ノードに次が含まれていないことを確認してください。

- 番号を付け替えるシャーシ
- 使用したい番号が付いているシャーシ

これらのシャーシのいずれかが [Chassis] ノードにリストされている場合は、そのシャーシの稼働を中止します。 次の手順に進む前に、稼働中止 FSM が完了し、シャーシが [Chassis] 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 （数分かかる場合があります）。

ステップ 4 [Equipment] タブの [Chassis] ノードをクリックします。

ステップ 5 [Work] ペインで [Decommissioned] タブをクリックします。

ステップ 6 番号を付け替えるシャーシの場合、次の手順を実行します。

a) シャーシを右クリックし、[Re-commission Chassis] を選択します。

b) [Re-commission Chassis] ダイアログボックスの [Chassis ID] フィールドで、シャーシに割り当てる ID を入力するか、矢印を使用して ID を選択します。

c) [OK] をクリックします。

ステップ 7 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ロケータ LED の切り替え

シャーシのロケータ LED の電源投入

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 位置を特定する必要があるシャーシをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で [Turn on Locator LED] をクリックします。
ロケータ LED の電源がすでにオンになっている場合、この処理は実行できません。

シャーシの LED が点滅を開始します。

シャーシのロケータ LED の電源切断

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 ロケータ LED の電源をオフにするシャーシを選択します。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で [Turn off Locator LED] をクリックします。
ロケータ LED の電源がすでにオフになっている場合、この処理は実行できません。

シャーシの LED の点滅が停止します。

シャーシの POST 結果の表示

シャーシ内のすべてのサーバおよびアダプタに対する Power On Self-Test プロセスで収集されたすべてのエラーを表示できます。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 Power On Self-Test（POST）の結果を表示するシャーシを選択します。

ステップ 4 [Work] ペインの [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、シャーシ内の各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。

第 37 章

ブレード サーバの管理

この章の内容は、次のとおりです。

- ブレード サーバ管理，712 ページ
- ブレード サーバの削除および稼働中止に関する注意事項，712 ページ
- 予期しないサーバの電源変更を回避するための推奨事項，713 ページ
- ブレード サーバのブート，714 ページ
- ブレード サーバのシャットダウン，715 ページ
- ブレード サーバのリセット，717 ページ
- ブレード サーバの再確認，717 ページ
- シャーシからのサーバの削除，718 ページ
- ブレード サーバの稼働中止，719 ページ
- ブレード サーバの再稼働，719 ページ
- シャーシ内のサーバ スロットの再確認，720 ページ
- 設定データベースからの存在しないブレード サーバの削除，720 ページ
- ブレード サーバのロケータ LED のオンとオフを切り替える，721 ページ
- ブレード サーバの CMOS のリセット，721 ページ
- ブレード サーバの CIMC のリセット，722 ページ
- ブレード サーバの破損した BIOS のリカバリ，723 ページ
- ブレード サーバの POST 結果の表示，724 ページ
- ブレード サーバからの NMI の発行，724 ページ

ブレード サーバ管理

Cisco UCS Manager を使用して Cisco UCS ドメイン内のすべてのブレードを管理およびモニタすることができます。 電源状態の変更などの一部のブレードサーバの管理タスクは、サーバとサービス プロファイルから行うことができます。

残りの管理タスクは、サーバ上でだけ実行できます。

シャーシ内のブレードサーバ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 ミスマッチ エラーを解決し、そのスロット内のブレード サーバを Cisco UCS Manager で再検出するために、スロットを再認識することもできます。

ブレード サーバの削除および稼働中止に関する注意事項

Cisco UCS Manager を使用してブレード サーバを削除する、または稼働を中止するかどうかを判断する際には、次の注意事項を考慮してください。

ブレード サーバの稼働中止

ブレード サーバが物理的に存在し、接続されているが、一時的に設定から削除したい場合、稼働中止が実行されます。 稼働を停止しているブレードサーバは最終的に再稼働することが予測されるため、サーバの情報部分は将来の使用に備えて Cisco UCS Manager によって保持されます。

ブレード サーバの削除

削除は、ブレードサーバとシャーシとの接続を解除することにより、ブレードサーバをサーバから物理的に削除するときに実行されます。 ブレードサーバが物理的に存在し、シャーシに接続されている場合は、そのブレード サーバを Cisco UCS Manager から削除することはできません。 ブレード サーバの物理的な削除が完了すると、そのブレード サーバの設定は、Cisco UCS Manager で削除されます。

削除中に、ブレードサーバへのアクティブ リンクがディセーブルになり、データベースからすべてのエントリが削除され、検出時に割り当てられたサーバ プールからサーバが自動的に削除されます。

（注） 検出中にサーバ プールに自動的に追加されたサーバだけが自動的に削除されます。 サーバ プールに手動で追加したサーバは手動で削除する必要があります。

削除したブレード サーバを設定に戻す必要がある場合は、再接続してから再検出する必要があります。 サーバが Cisco UCS Manager に再導入された場合は新しいサーバと同様に処理され、詳細な検出プロセスの実行対象となります。 したがって、Cisco UCS Manager はサーバに対して、以前の ID と異なる場合がある新しい ID を割り当てることができます。

予期しないサーバの電源変更を回避するための推奨事項

サーバがサービス プロファイルに関連付けられていない場合、サーバの物理的な [Power] ボタンまたは [Reset] ボタンなど、サーバ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、次の方法を使用するだけでサーバの電源状態を変更することができます。

- Cisco UCS Manager GUI で、サーバ、または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、サーバに関連付けられているサービス プロファイルに対して **power up** コマンドまたは **power down** コマンドを使用します。

重要 関連付けられているサーバで、現在電源がオフになっているサーバには、次のオプションのいずれも使用しないでください。

- GUI での [Reset]
- CLI での **cycle cycle-immediate** または **reset hard-reset-immediate**
- サーバの [Power] ボタンまたは [Reset] ボタン

現在電源がオフになっているサーバに対して、リセットまたはサイクルを実施するか、サーババの物理的な [Power] ボタンを使用すると、サーバの実際の電源状態が、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。 サーバと Cisco UCS Manager 間の通信が中断した場合や、サービス プロファイルの設定が変更されると、Cisco UCS Manager に、必要とされる電源状態がサービス プロファイルからサーバに適用されることがあり、この結果予期しない電源変更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	現在のサーバの電源状態	通信の後にサーバ電力状態が中断する
Up	電源オフ	電源オン
Down	電源オン	電源オン （注） 実行中のサーバは、サービス プロファイルで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 サーバのブート

ブレード サーバのブート

[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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバがブートした後は、[General] タブの [Overall Status] フィールドに [OK] ステータスが表示されます。

サービス プロファイルからのサーバのブート

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [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　[Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2　[Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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 サーバのシャットダウン

ブレード 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 システムでサーバをシャットダウンする場合、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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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 システムでサーバをシャットダウンする場合、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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドにダウン ステータスまたは電源オフ状態が表示されます。

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。 Cisco UCS Manager に、サーバをリセットする前にすべての管理操作を完了させるオプションでは、これらの操作がサーバのリセット前に完了するかどうかは保証されていません。

（注） 電源オフの状態からサーバをブートする場合、[Reset] を使用しないでください。

このプロセスで起動を続行すると、サーバに求められる電源状態は実際の電源状態と同期しなくなり、後でサーバが予期せずシャット ダウンする可能性があります。 選択したサーバを電源オフの状態から安全にリブートするには、[Cancel] をクリックしてから、[Boot Server] アクションを選択します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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） Cisco UCS Manager に、このサーバで保留中のすべての管理操作を完了させる場合は、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 サーバの再確認

Cisco UCS Manager にサーバ、およびそのサーバのすべてのエンドポイントを再検出させる必要がある場合は、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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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 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の削除

はじめる前に

次の手順を実行する前に、サーバをシャーシから物理的に取り外します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [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。

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 ハードウェアを取り外します。
サーバ 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。

次の作業

ブレード サーバを物理的に取り付けなおす場合は、スロットを再確認して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

詳細については、シャーシ内のサーバ スロットの再確認, （720 ページ）を参照してください。

ブレード サーバの稼働中止

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [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。

次の作業

ブレード サーバを物理的に取り付けなおす場合は、スロットを再確認して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

詳細については、シャーシ内のサーバ スロットの再確認, （720 ページ）を参照してください。

ブレード サーバの再稼働

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブの [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 再稼働する各ブレード サーバの行で、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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 6 （任意） サーバの再稼働状況と、サーバの [FSM] タブの検出をモニタします。

次の作業

-

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サーバを解放した場合に、Cisco UCS Manager にサーバを再検出させ、再稼働させるには、次の手順を実行します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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 [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。

設定データベースからの存在しないブレード サーバの削除

最初にサーバを解放せずにサーバのハードウェアを物理的にサーバから取り外すには、次の手順を実行します。 サーバが物理的に存在する場合、この手順を実行することはできません。

サーバを物理的に削除する場合は、シャーシからのサーバの削除, （718 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [Remove] をクリックします。

b) [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 のオンとオフを切り替える

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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

ブレード サーバの CMOS のリセット

非常に珍しいケースですが、サーバのトラブルシューティング時に、CMOS のリセットが必要になることがあります。 この手順は、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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [Reset CMOS] をクリックします。

b) [OK] をクリックします。

ブレード サーバの CIMC のリセット

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMCのリセットが必要になることがあります。 この手順は、通常のサーバ メンテナンスには含まれません。 CIMC のリセット後、サーバは、そのサーバで実行されているバージョンのファームウェアを使ってブートされます。

CIMC がリセットされると、Cisco UCS の電力モニタリング機能は、CIMC をリブートするために短時間使用できなくなります。 通常、これには 20 秒しかかかりませんが、その時間内にピーク時の電力制限を超過する可能性があります。 非常に低い電力制限環境で、設定された電力制限を超過し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ずらすことを検討してください。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [Reset CIMC (Server Controller)] をクリックします。

b) [OK] をクリックします。

ブレード サーバの破損した BIOS のリカバリ

非常に珍しいケースですが、サーバの問題により、破損した BIOS の復旧が必要になることがあります。 この手順は、通常のサーバ メンテナンスには含まれません。 BIOS の復旧後、サーバは、そのサーバで実行されているバージョンのファームウェアを使ってブートされます。 BIOS が復旧を必要としていない場合、またはそのサーバではこのオプションが使用できない場合は、このオプション ボタンが淡色表示されることがあります。

はじめる前に

重要 サーバ上で破損している BIOS の復旧を試行する前に、そのサーバに接続またはマップされている USB ストレージをすべて取り外します。 外部 USB ドライブが vMedia からサーバに取り付けられた、またはマップされている場合、BIOS の回復に失敗します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 BIOS を回復させるサーバを選択します。

ステップ 4 [Work] ペインの [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、次の手順を実行します。

a) [Recover Corrupt BIOS] をクリックします。

（注） このオプションが特定のサーバに使用できない場合は、次の手順を実行して、サーバの BIOS を更新し、アクティブにします。

b) [OK] をクリックします。

ステップ 7 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [Recover Corrupt BIOS] 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
[Version To Be Activated] ドロップダウン リスト	アクティブ化するファームウェア バージョンをドロップダウン リストから選択します。

b) [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。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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。

ブレード サーバからの NMI の発行

システムが応答不能のままになり、Cisco UCS Manager に Non Maskable Interrupt（NMI）を BIOS に発行させるか、CIMC からオペレーティング システムに発行させる場合は、次の手順を実行します。サーバにインストールされているオペレーティング システムに応じて、このアクションによってコア 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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

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] ペインの [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 は BIOS またはオペレーティング システムに NMI を送信します。

第 38 章

ラックマウント サーバの管理

この章の内容は、次のとおりです。

- ラックマウント サーバ管理，726 ページ
- ラックマウント サーバの削除および稼働中止に関する注意事項，726 ページ
- 予期しないサーバの電源変更を回避するための推奨事項，727 ページ
- ラックマウント サーバのブート，728 ページ
- ラックマウント サーバのシャットダウン，730 ページ
- ラックマウント サーバのリセット，731 ページ
- ラックマウント サーバの再確認，732 ページ
- ラックマウント サーバの稼働中止，732 ページ
- ラックマウント サーバの再稼働，733 ページ
- ラックマウント サーバ番号の付け替え，733 ページ
- 設定データベースからの存在しないラックマウント サーバの削除，734 ページ
- ラックマウント サーバのロケータ LED のオンとオフを切り替える，735 ページ
- ラックマウント サーバの CMOS のリセット，735 ページ
- ラックマウント サーバの CIMC のリセット，735 ページ
- ラックマウント サーバの破損した BIOS のリカバリ，736 ページ
- ラックマウント サーバの POST 結果の表示，737 ページ
- ラックマウント サーバからの NMI の発行，737 ページ

ラックマウント サーバ管理

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 サーバを管理およびモニタすることができます。 すべての管理機能およびモニタリング機能は、電力制限を除くラックマウントサーバでサポートされます。 電源状態の変更などの一部のラックマウント サーバの管理タスクは、サーバとサービス 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、サーバ上でだけ実行できます。

Cisco UCS Manager は、検出した各ラックマウント サーバの情報、エラー、および障害を提供します。

ヒント　サポートされている Cisco UCS ラックマウント サーバを Cisco UCS Manager と統合する方法の詳細については、該当する Cisco UCS Manager リリースの Cisco UCS C シリーズ サーバ統合ガイドを参照してください。

ラックマウント サーバの削除および稼働中止に関する注意事項

Cisco UCS Manager を使用してラックマウント サーバを削除する、または稼働を中止するかどうかを判断する際には、次の注意事項を考慮してください。

ラックマウント サーバの稼働中止

ラックマウント サーバが物理的に存在し、接続されているが、一時的に設定から削除したい場合、稼働中止が実行されます。 稼働を停止しているラックマウントサーバは最終的に再稼働することが予測されるため、サーバの情報部分は将来の使用に備えて Cisco UCS Manager によって保持されます。

ラックマウント サーバの削除

削除は、ファブリック エクステンダとラックマウントサーバの接続を解除することで、システムからサーバを物理的に削除するときに実行されます。 ラックマウントサーバが物理的に存在し、ファブリック エクステンダに接続されている場合は、そのラックマウント サーバを Cisco UCS Manager から削除することはできません。 ラックマウント サーバの接続が解除されると、そのラックマウント サーバの設定は、Cisco UCS Manager で削除できます。

削除中に、管理インターフェイスの接続が解除され、データベースからすべてのエントリが削除され、検出時に割り当てられたサーバ プールからサーバが自動的に削除されます。

（注）　検出中にサーバ プールに自動的に追加されたサーバだけが自動的に削除されます。 サーバ プールに手動で追加したサーバ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 サーバを設定に戻す必要がある場合は、再接続してから再検出する必要があります。 サーバが Cisco UCS Manager に再導入された場合は新しいサーバと同様に処理され、

詳細な検出プロセスの実行対象となります。 したがって、Cisco UCS Manager はサーバに対して、以前の ID と異なる場合がある新しい ID を割り当てることができます。

予期しないサーバの電源変更を回避するための推奨事項

サーバがサービス プロファイルに関連付けられていない場合、サーバの物理的な [Power] ボタンまたは [Reset] ボタンなど、サーバ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、次の方法を使用するだけでサーバの電源状態を変更することができます。

- Cisco UCS Manager GUI で、サーバ、または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、サーバに関連付けられているサービス プロファイルに対して **power up** コマンドまたは **power down** コマンドを使用します。

重要 関連付けられているサーバで、現在電源がオフになっているサーバには、次のオプションのいずれも使用しないでください。

- GUI での [Reset]
- CLI での **cycle cycle-immediate** または **reset hard-reset-immediate**
- サーバの [Power] ボタンまたは [Reset] ボタン

現在電源がオフになっているサーバに対して、リセットまたはサイクルを実施するか、サーバの物理的な [Power] ボタンを使用すると、サーバの実際の電源状態が、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。 サーバと Cisco UCS Manager 間の通信が中断した場合や、サービス プロファイルの設定が変更されると、Cisco UCS Manager に、必要とされる電源状態がサービス プロファイルからサーバに適用されることがあり、この結果予期しない電源変更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	現在のサーバの電源状態	通信の後にサーバ電力状態が中断する
Up	電源オフ	電源オン

サービス プロファイルで必要とされる電源状態	現在のサーバの電源状態	通信の後にサーバ電力状態が中断する
Down	電源オン	電源オン （注） 実行中のサーバは、サービス プロファイルで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 サーバのブート

ラックマウント サーバのブート

[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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバがブートした後は、[General] タブの [Overall Status] フィールドに [OK] ステータスが表示されます。

サービス プロファイルからのサーバのブート

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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 サーバのシャットダウン

ラックマウント 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 システムでサーバをシャットダウンする場合、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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

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 システムでサーバをシャットダウンする場合、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 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] 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] ペインの [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバが正常にシャットダウンされると、[General] タブの [Overall Status] フィールドにダウン ステータスまたは電源オフ状態が表示されます。

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。 Cisco UCS Manager に、サーバをリセットする前にすべての管理操作を完了させるオプションでは、これらの操作がサーバのリセット前に完了するかどうかは保証されていません。

（注） 電源オフの状態からサーバをブートする場合、[Reset] を使用しないでください。

このプロセスで起動を続行すると、サーバに求められる電源状態は実際の電源状態と同期しなくなり、後でサーバが予期せずシャット ダウンする可能性があります。 選択したサーバを電源オフの状態から安全にリブートするには、[Cancel] をクリックしてから、[Boot Server] アクションを選択します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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） Cisco UCS Manager に、このサーバで保留中のすべての管理操作を完了させる場合は、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 サーバの再確認

Cisco UCS Manager にサーバ、およびそのサーバのすべてのエンドポイントを再検出させる必要がある場合は、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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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 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。

ラックマウント サーバの稼働中止

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [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。

ラックマウント サーバの再稼働

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブの [Rack-Mounts] 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 再稼働する各ラックマウント サーバの行で、次の手順を実行します。

a) [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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 6 （任意） サーバの再稼働状況と、サーバの [FSM] タブの検出をモニタします。

ラックマウント サーバ番号の付け替え

はじめる前に

サーバ間で ID を交換する場合は、最初にサーバを解放し、リナンバリング手順を進める前にサーバの稼働中止 FSM が完了するまで待つ必要があります。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 [Servers] ノードを展開し、次が含まれていないことを確認してください。

- 番号を付け替えるラックマウント サーバ
- 使用したい番号が付いているラックマウント サーバ

これらのサーバのいずれかが [Servers] ノードにリストされている場合は、そのサーバの稼働を中止します。 次の手順に進む前に、稼働中止 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 （数分かかる場合があります）。

ステップ 4 番号を付け替えるラックマウント サーバを選択します。

ステップ 5 [Equipment] タブの [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 番号を付け替える各ラックマウント サーバの行で、次の手順を実行します。

a) [ID] フィールドをダブルクリックして、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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 9 （任意） サーバの再稼働状況と、サーバの [FSM] タブの検出をモニタします。

設定データベースからの存在しないラックマウント サーバの削除

最初にサーバを解放せずにサーバのハードウェアを物理的にサーバから取り外すには、次の手順を実行します。 サーバが物理的に存在する場合、この手順を実行することはできません。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [Remove] をクリックします。

b) [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 のオンとオフを切り替える

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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 CMOS のリセット

非常に珍しいケースですが、サーバのトラブルシューティング時に、CMOS のリセットが必要になることがあります。 この手順は、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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [Reset CMOS] をクリックします。

b) [OK] をクリックします。

ラックマウント サーバの CIMC のリセット

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMC のリセットが必要になることがあります。 この手順は、

通常のサーバ メンテナンスには含まれません。 CIMC のリセット後、サーバは、そのサーバで実行されているバージョンのファームウェアを使ってブートされます。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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、次の手順を実行します。

a) [Reset CIMC (Server Controller)] をクリックします。

b) [OK] をクリックします。

ラックマウント サーバの破損した BIOS のリカバリ

非常に珍しいケースですが、サーバの問題により、破損した BIOS の復旧が必要になることがあります。 この手順は、通常のサーバ メンテナンスには含まれません。 BIOS の復旧後、サーバは、そのサーバで実行されているバージョンのファームウェアを使ってブートされます。 BIOS が復旧を必要としていない場合、またはそのサーバではこのオプションが使用できない場合は、このオプション ボタンが淡色表示されることがあります。

はじめる前に

重要 サーバ上で破損している BIOS の復旧を試行する前に、そのサーバに接続またはマップされている USB ストレージをすべて取り外します。 外部 USB ドライブが vMedia からサーバに取り付けられた、またはマップされている場合、BIOS の回復に失敗します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 BIOS を回復させるサーバを選択します。

ステップ 4 [Work] ペインの [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、次の手順を実行します。

a) [Recover Corrupt BIOS] をクリックします。

b) [OK] をクリックします。

ステップ 7 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [Recover Corrupt BIOS] 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
[Version To Be Activated] ドロップダウン リスト	アクティブ化するファームウェア バージョンをドロップダウン リストから選択します。

b) [OK] をクリックします。

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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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。

ラックマウント サーバからの NMI の発行

システムが応答不能のままになり、Cisco UCS Manager に Non Maskable Interrupt（NMI）を BIOS に発行させるか、CIMC からオペレーティング システムに発行させる場合は、次の手順を実行します。サーバにインストールされているオペレーティング システムに応じて、このアクションによってコア 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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

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] ペインの [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 は BIOS またはオペレーティング システムに NMI を送信します。

第 39 章

KVM コンソールの起動

この章の内容は、次のとおりです。

- KVM コンソール，739 ページ
- サーバからの KVM コンソールの起動，744 ページ
- サービス プロファイルからの KVM コンソールの起動，744 ページ
- KVM Launch Manager からの KVM コンソールの起動，745 ページ

KVM コンソール

KVM コンソールは、Cisco UCS Manager GUI または KVM の直接接続をエミュレートする KVM Launch Manager からアクセスできるインターフェイスです。 サーバに物理的に接続する必要がある KVM ドングルとは異なり、KVM コンソールを使用すると、ネットワーク上のリモート ロケーションからサーバに接続できます。

サーバへのアクセスに KVM コンソールを使用する場合は、サーバまたはサーバに関連付けられたサービス プロファイルが CIMC の IP アドレスで設定できるようにする必要があります。 KVM コンソールは、サーバまたはサービス プロファイルに割り当てられた CIMC IP アドレスを使用して、Cisco UCS ドメイン内の適切なサーバを識別し、このサーバに接続します。

CD、DVD、またはフロッピー ドライブを使用してサーバに直接接続する代わりに、KVM コンソールでは仮想メディアを使用します。仮想メディアは、仮想 CD、DVD、またはフロッピー ドライブにマップされた実際のディスク ドライブまたはディスク イメージ ファイルです。 次に示す任意の仮想ドライブをマップできます。

- お使いのコンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージ ファイル
- ネットワーク上の CD/DVD またはフロッピー ドライブ
- ネットワーク上のディスク イメージ ファイル

サーバ OS のインストールでの KVM コンソールの使用に関する推奨事項

仮想 CD/DVD またはフロッピー ドライブから OS をインストールするには、その仮想 CD/DVD またはフロッピー ドライブがサービス プロファイルで最初のブート デバイスとして設定されている必要があります。

KVM コンソールを使用した OS のインストールは、KVM ドングルを使用する場合よりも時間がかかることがあります。これは、ネットワークを介してインストール ファイルをサーバにダウンロードする必要があるためです。 ディスク ドライブまたはディスク イメージ ファイルをネットワーク共有から仮想ドライブにマップする場合は、インストールにさらに時間がかかることがあります。これは、インストール ファイルをネットワークから KVM コンソール（お使いのコンピュータ）にダウンロードした後、KVM コンソールからサーバにダウンロードする必要があるからです。 このインストール方式を使用する場合は、KVM コンソールを搭載したシステムのできる限り近くにインストール メディアを配置することを推奨します。

仮想 KVM コンソール

KVM コンソールは CIMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。 これにより、リモート ロケーションからのサーバへの接続とサーバの制御ができるようになり、この KVM セッション中にサーバがアクセスできる仮想ドライブに物理的な場所をマッピングできるようになります。

重要 KVM コンソールには Java Runtime Environment（JRE）バージョン 1.5.0 以降が必要です。

[KVM] タブ

このタブは、サーバへのコマンドラインアクセスを提供します。 このタブで使用できるメニューオプションは次のとおりです。

[Virtual Media] タブ

サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、KVM コンソールは仮想メディアを使用します。 これは、サーバ上の仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージ ファイルです。 [Client View] テーブルは、サーバが使用できるフロッピー イメージ、フロッピー ドライブ、CD/DVD ドライブおよび ISO イメージを表示します。

名前	説明
[Mapped] カラム	このカラムのチェックボックスをオンにすると、関連するディスク ドライブまたはイメージファイルにサーバからアクセスできます。 ドライブまたはイメージファイルからサーバを切断するには、このチェックボックスをクリアします。 各ドライブまたはイメージファイルは、ユーザのローカル コンピュータまたはネットワークに設定でき、それぞれが次の 3 つのカテゴリのうちのいずれかに分類されます。 • 仮想 CD/DVD • リムーバブル メディア • フロッピー：このカテゴリには、USB キーまたはフラッシュ ドライブがあります。 この3つのカテゴリのそれぞれに、1つのドライブまたはイメージの仮想メディアをイネーブルにできますが、同じカテゴリに複数のドライブまたはイメージを仮想化することはできません。
[Read Only] カラム	オンにすると、仮想メディア デバイスに書き込み機能があっても、サーバはそのメディアに書き込むことができなくなります。
[Drive] カラム	サーバによって使用されるデバイスへのパスを表示します。
[Exit] ボタン	[KVM] タブに戻ります。
[Create Image] ボタン	サーバにマップするローカルフォルダにナビゲートする [Open] ダイアログボックスが開きます。 システムがイメージを生成したら、デスクトップにIMGファイルを保存し、[Client View] テーブルに追加します。 マッピングプロセスを完了するには、[Mapped] カラムのチェックボックスをオンにします。
[Add Image] ボタン	サーバにアクセスする ISO または IMG ファイルに移動する [Open] ダイアログボックスが開きます。 ファイルを選択すると、システムはそのファイルを [Client View] テーブルに追加します。 マッピング プロセスを完了するには、[Mapped] カラムのチェックボックスをオンにします。
[Remove Image] ボタン	[Client View] テーブルから選択したイメージを削除します。

名前	説明
[Details] ボタン	[Details] 領域の表示を切り替えます。 この領域には、3 つのデバイス カテゴリ、このカテゴリのマッピング ステータス、読み取りおよび書き込み統計、デバイスがマッピングされている期間を示すテーブルが含まれます。
[USB Reset] ボタン	サーバに接続されているすべての USB デバイスをリセットします。 （注） このボタンを使用するには、[Details] 領域が表示されていなければなりません。

[File] メニュー

メニュー項目	説明
Capture to File	JPG イメージとして現在の画面を保存できる [Save] ダイアログ ボックスが開きます。 （注） このオプションは、[KVM] タブでのみ使用できます。
Exit	KVM コンソールを閉じます。

[KVM] タブの [View] メニュー

メニュー項目	説明
Refresh	サーバの現在のビデオ出力を使用してコンソール表示を更新します。
Full Screen	画面全体に表示されるように KVM コンソールを拡張します。
Windowed	サイズを変更できる [Windowed] モードに KVM コンソールを戻します。
Fit	コンソール ウィンドウのサイズを、サーバからのビデオ映像を表示するために必要な最小サイズに変更します。 このオプションは、コンソールが [Windowed] モードの場合にのみ使用できます。

[KVM] タブの [Macros] メニュー

リモート システムで実行するキーボード ショートカットを選択します。

[KVM] タブの [Tools] メニュー

メニュー項目	説明
Session Options	[Session Options] ダイアログボックスでは次のオプションを指定できます。 • コンソールが [Windowed] モードになっているときにすべてのキーストロークをターゲットシステムに渡すかどうかを指定します。 デフォルトは no です。 • シングル カーソル モードになっているときの終了キーを指定します。 デフォルトは F12 です。 • ターゲットシステムに使用するマウスのアクセラレーションを指定します。 デフォルトは [Windows] です。
Single Cursor	一部のリモートオペレーティングシステムで検出されたマウスの配置に関する問題を解決するシングルカーソル機能をオンにします。 この機能をオンにすると、マウスポインタがビューアウィンドウ内でトラップされます。 機能をオフにするには、[Session Options] ダイアログボックスで指定された終了キーを押します。
Stats	次の項目を表示する [Stas] ダイアログボックスが開きます。 • フレーム レート（フレーム数/秒で測定されます） • 帯域幅（KB 数/秒で測定されます） • 圧縮（使用される圧縮率で測定されます） • パケット レート（パケット数/秒で測定されます）
Session User List	アクティブ KVM セッションを持つすべてのユーザ ID を示す [Session User List] ダイアログボックスが開きます。

サーバからの KVM コンソールの起動

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 **KVM コンソール**からアクセスするサーバを選択します。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で [KVM Console] をクリックします。
KVM コンソールが別ウィンドウで開きます。

ヒント KVM セッションを開いたときにキーボードの Caps Lock キーがオンになっており、その後に続いて Caps Lock キーをオフにすると、**KVM コンソール**は Caps Lock キーがオンのときのように動作する場合があります。**KVM コンソール**とキーボードを同期させるには、**KVM コンソール**にフォーカスがない状態で Caps Lock キーを一度押し、次に**KVM コンソール**にフォーカスを置いて Caps Lock キーをもう一度押します。

サービス プロファイルからの KVM コンソールの起動

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 [KVM Console] を起動するサービス 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 関連付けられたサーバに KVM アクセスを必要とするサービス プロファイルを選択します。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Actions] 領域で [KVM Console] をクリックします。
別ウィンドウに KVM コンソールが表示されます。

ヒント KVM セッションを開いたときにキーボードの Caps Lock キーがオンになっており、その後に続いて Caps Lock キーをオフにすると、**KVM コンソール**は Caps Lock キーがオンのときのように動作する場合があります。**KVM コンソール**とキーボードを同期させるには、**KVM コンソール**にフォーカスがない状態で Caps Lock キーを一度押し、次に**KVM コンソール**にフォーカスを置いて Caps Lock キーをもう一度押します。

KVM Launch Manager からの KVM コンソールの起動

KVM Launch Manager では、Cisco UCS Manager にログインせずに KVM コンソールからサーバにアクセスできます。

はじめる前に

KVM Launch Manager からサーバの KVM コンソールにアクセスするには、次の情報が必要です。

- Cisco UCS のユーザ名およびパスワード。
- アクセスする KVM のサーバに関連付けられたサーバ プロファイル名。

手順

ステップ 1 Web ブラウザで、Cisco UCS Manager GUI の Web リンクを入力または選択します。

例：
デフォルトの Web リンクは `http://UCSManager_IP` または `https://UCSManager_IP` です。 スタンドアロン構成の場合、*UCSManager_IP*はファブリック インターコネクトの管理ポートの IP アドレスです。 クラスタ構成の場合、*UCSManager_IP* は Cisco UCS Manager に割り当てられている IP アドレスです。

ステップ 2 [Launch Page]Cisco UCS Manager の起動ページの [Launch KVM Manager] をクリックします。

ステップ 3 [Security Alert] ダイアログボックスが表示された場合は、[Yes] をクリックしてセキュリティ証明書を受け入れ、続行します。

ステップ 4 [UCS - KVM Launch Manager Login] ページで、次の手順を実行します。

a) Cisco UCS のユーザ名およびパスワードを入力します。
b) （任意） Cisco UCS 実装に複数のドメインが含まれている場合は、[Domain] ドロップダウンリストから適切なドメインを選択します。
c) [OK] をクリックします。

ステップ 5 KVM Launch Manager の [Service Profiles] テーブルで、次の手順を実行します。

a) サービス プロファイルと、KVM アクセスが必要な関連するサーバを含む行を探します。
b) そのサーバの [Launch KVM] 列の [Launch] をクリックします。
別ウィンドウに KVM コンソールが表示されます。

ヒント KVM セッションを開いたときにキーボードの Caps Lock キーがオンになっており、その後に続いて Caps Lock キーをオフにすると、**KVM コンソール**は Caps Lock キーがオンのときのように動作する場合があります。 **KVM コンソール** とキーボードを同期させるには、**KVM コンソール**にフォーカスがない状態で Caps Lock キーを一度押し、次に **KVM コンソール**にフォーカスを置いて Caps Lock キーをもう一度押します。

第 40 章

I/O モジュールの管理

この章の内容は、次のとおりです。

- Cisco UCS Manager GUI での I/O モジュール管理，747 ページ
- I/O モジュールのリセット，747 ページ
- I/O モジュールの POST 結果の表示，748 ページ

Cisco UCS Manager GUI での I/O モジュール管理

Cisco UCS Manager GUI を使用して Cisco UCS ドメイン 内のすべての I/O モジュールを管理およびモニタできます。

I/O モジュールのリセット

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [IO Modules] を展開します。

ステップ 3 リセットする I/O モジュールをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で [Reset IO Module] をクリックします。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

I/O モジュールの POST 結果の表示

I/O モジュールに対する 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 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [IO Modules] を展開します。

ステップ 3 POST の結果を表示する I/O モジュールを選択します。

ステップ 4 [Work] ペインの [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、I/O モジュールの POST の結果が一覧表示されます。

ステップ 6 [OK] をクリックして [POST Results] ダイアログボックスを閉じます。

第 41 章

設定のバックアップと復元

この章の内容は、次のとおりです。

- バックアップおよびエクスポートの設定，749 ページ
- バックアップ タイプ，750 ページ
- バックアップ操作の考慮事項と推奨事項，750 ページ
- スケジューリング バックアップ，751 ページ
- コンフィギュレーションのインポート，752 ページ
- インポート方法，752 ページ
- システムの復元，753 ページ
- バックアップ操作とインポート操作に必要なユーザ ロール，753 ページ
- バックアップ操作の設定，753 ページ
- スケジュール バックアップの設定，760 ページ
- インポート操作の設定，763 ページ
- ファブリック インターコネクトの設定の復元，769 ページ

バックアップおよびエクスポートの設定

Cisco UCS Manager からバックアップを実行する場合は、システム設定全体またはその一部のスナップショットを作成し、ファイルをネットワーク上の場所にエクスポートします。 Cisco UCS Manager を使用して、サーバにデータをバックアップすることはできません。

バックアップは、システムが起動されて動作している間に実行できます。 バックアップ操作では、管理プレーンからの情報だけが保存されます。 バックアップは、サーバまたはネットワークトラフィックには影響しません。

バックアップ タイプ

Cisco UCS から次のタイプのバックアップを 1 つ以上実行できます。

- [Full state]：システム全体のスナップショットが含まれるバイナリ ファイル。 このバックアップにより生成されたファイルを使用して、ディザスタ リカバリ時にシステムを復元できます。 このファイルにより、元のファブリック インターコネクト上で設定を復元または再構築できます。また、別のファブリック インターコネクト上で設定を再現することもできます。 このファイルは、インポートには使用できません。
- [All configuration]：すべてのシステム設定と論理設定が含まれる XML ファイル。 このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。 このファイルは、システムの復元には使用できません。 このファイルには、ローカル認証されたユーザのパスワードは含まれません。
- [System configuration]：ユーザ名、ロール、ロケールなどのすべてのシステム設定が含まれる XML ファイル。 このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。 このファイルは、システムの復元には使用できません。
- [Logical configuration]：サービス プロファイル、VLAN、VSAN、プール、ポリシーなどのすべての論理設定が含まれる XML ファイル。 このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。 このファイルは、システムの復元には使用できません。

バックアップ操作の考慮事項と推奨事項

バックアップ操作を作成する前に、次のことを考慮してください。

バックアップの場所

バックアップの場所とは、Cisco UCS Central でファイルをエクスポートするネットワーク上の宛先またはフォルダのことです。 バックアップ操作は、バックアップ ファイルを保存する場所ごとに 1 つしか保持できません。

バックアップ ファイルを上書きする可能性

ファイル名を変更しないでバックアップ操作を再実行すると、サーバ上にすでに存在するファイルが Cisco UCS Central によって上書きされます。 既存のバックアップ ファイルが上書きされるのを回避するには、バックアップ操作内のファイル名を変更するか、既存のファイルを別の場所にコピーします。

複数のバックアップのタイプ

同じ場所に対して複数種類のバックアップを実行し、エクスポートできます。 バックアップ操作を再実行する前に、バックアップ タイプを変更する必要があります。 バックアップ タイプの識別を容易にし、また既存のバックアップ ファイルが上書きされるのを回避するために、ファイル名を変更することを推奨します。

スケジューリング バックアップ

バックアップ操作を前もって作成し、そのバックアップの実行準備が整うまで管理状態をディセーブルのままにしておくことはできます。 Cisco UCS Central は、バックアップ操作の管理状態がイネーブルに設定されるまで、バックアップ操作を実行したり、コンフィギュレーション ファイルを保存したり、エクスポートしたりしません。

Cisco UCS Central を使用して、Cisco UCS Central 自身または Cisco UCS Manager のバックアップと復元ができます。 バックアップと復元のポリシーをスケジュールするか、バックアップ操作はただちに実行することができます。 スケジュールされるバックアップ操作と即時バックアップ操作には、次の 2 つのタイプがあります。

- Cisco UCS Central のバックアップおよび復元機能ポリシーのスケジュールされた操作と即時操作。
- Cisco UCS Central でポリシーが解決した場合の Cisco UCS Manager のバックアップおよび復元機能ポリシーのスケジュールされた操作と即時操作。

ポリシーには、スケジュールされた全コンフィギュレーションのバックアップ ポリシーと、スケジュールされた db バックアップ ポリシーという 2 種類のポリシーがあります。 これらのポリシーは、ローカルまたは Cisco UCS Central に定義できます

増分バックアップ

Cisco UCS の増分バックアップは実行できません。

完全な状態のバックアップの暗号化

完全な状態のバックアップでは、パスワードや他の機密情報がクリアテキストでエクスポートされないように暗号化されます。

スケジューリング バックアップ

次のタイプのバックアップをスケジュールするように、Cisco UCS にポリシーを設定することができます。

- 完全な状態
- すべてのコンフィギュレーション

他のタイプのバックアップはスケジュールできません。

完全な状態のバックアップ ポリシー

完全な状態のバックアップ ポリシーにより、システム全体のスナップショットの完全な状態の定期的なバックアップをスケジュールすることができます。 完全な状態のバックアップを日単位、週単位、または隔週単位で行うように設定するかどうか選択することもできます。

Cisco UCS は、リモート サーバ上のバックアップ ファイルの最大数を維持します。 この数を超えると、Cisco UCS では最も古いバックアップ ファイルが上書きされます。

すべてのコンフィギュレーションのエクスポート ポリシー

すべてのコンフィギュレーションのバックアップのポリシーにより、すべてのシステム設定および論理コンフィギュレーション設定の定期的なバックアップおよびエクスポートをスケジュールすることができます。 このバックアップには、ローカル認証されたユーザのパスワードは含まれません。 すべてのコンフィギュレーションのバックアップを日単位、週単位、または隔週単位で行うように設定するかどうか選択することもできます。

Cisco UCS は、リモート サーバ上のバックアップ ファイルの最大数を維持します。 この数を超えると、Cisco UCS では最も古いバックアップ ファイルが上書きされます。

コンフィギュレーションのインポート

Cisco UCS からエクスポートされたコンフィギュレーション ファイルをインポートできます。ファイルは、同じ Cisco UCS からエクスポートされる必要はありません。

インポート機能は、すべてのコンフィギュレーションファイル、システムコンフィギュレーション ファイル、および論理コンフィギュレーション ファイルで使用できます。 インポートは、システムがアップ状態で、稼働中に実行できます。 インポート操作によって情報が変更されるのは、管理プレーンだけです。 インポート操作によって行われる一部の変更（サーバに割り当てられた Virtual Network Interface Card（vNIC; 仮想ネットワーク インターフェイス カード）に対する変更など）により、サーバのリブートまたはトラフィックを中断する他の動作が行われることがあります。

インポート操作はスケジュールできません。 ただし、インポート操作を前もって作成し、そのインポートの実行準備が整うまで管理状態をディセーブルのままにしておくことはできます。Cisco UCS では、管理状態がイネーブルに設定されるまで、コンフィギュレーション ファイルでインポート操作が実行されません。

インポート操作は、コンフィギュレーション バックアップ ファイルを保存する場所ごとに 1 つしか保持できません。

インポート方法

次のいずれかの方法を使用して、Cisco UCS によるシステム設定のインポートおよびアップデートを実行できます。

- [Merge]：インポートされたコンフィギュレーション ファイルの情報は、既存の設定情報と比較されます。 矛盾が存在する場合、インポート操作によって、インポートされたコンフィギュレーション ファイルの情報で Cisco UCS ドメインの情報が上書きされます。
- [Replace]：現在の設定情報が、インポートされたコンフィギュレーション ファイルの情報で一度に 1 つのオブジェクトについて置き換えられます。

システムの復元

この復元機能は、ディザスタ リカバリに使用できます。

Cisco UCS からエクスポートされた任意の完全な状態のバックアップ ファイルからシステム設定を復元できます。 このファイルは、復元するシステム上の Cisco UCS からエクスポートされたものでなくてもかまいません。 別のシステムからエクスポートされたバックアップ ファイルを使用して復元する場合、ファブリック インターコネクト、サーバ、アダプタ、I/O モジュールまたは FEX の接続も含め、同一または同様のシステム設定およびハードウェアを使用することを強く推奨します。 ハードウェアまたはシステム設定、あるいはこの両方が一致していない場合、復元されたシステムが完全に機能しない可能性があります。 2 つのシステムで、I/O モジュールのリンクまたはサーバ間に不一致がある場合は、復元操作の後にシャーシまたはサーバ、あるいはこの両方を確認します。

この復元機能は、完全な状態のバックアップ ファイルにだけ使用できます。 完全な状態のバックアップ ファイルはインポートできません。 復元は、初期システム セットアップで実行します。

バックアップ操作とインポート操作に必要なユーザ ロール

バックアップ操作とインポート操作を作成し、実行するには、管理ロールを持つユーザ アカウントが必要です。

バックアップ操作の設定

バックアップ操作の作成

はじめる前に

バックアップ サーバの IP アドレスおよび認証クレデンシャルを取得します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域の [Backup] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスで、[Create Backup Operation] をクリックします。

ステップ 6 [Create Backup Operation] 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
[Admin State] フィールド	次のいずれかになります。 • [Enabled]：[OK] をクリックするとすぐに、Cisco UCS Manager によってバックアップ操作が実行されます。 • [Disabled]：[OK] をクリックしても、Cisco UCS Manager によってバックアップ操作は実行されません。 このオプションを選択すると、ダイアログボックスのすべてのフィールドが表示されたままになります。 ただし、[Backup Configuration] ダイアログボックスからバックアップを手動で実行する必要があります。

名前	説明
[Type] フィールド	バックアップ コンフィギュレーション ファイルに保存された情報。 次のいずれかになります。 • [Full state]：システム全体のスナップショットが含まれるバイナリ ファイル。 このバックアップにより生成されたファイルを使用して、ディザスタ リカバリ時にシステムを復元できます。 このファイルにより、元のファブリック インターコネクト上で設定を復元または再構築できます。 また、別のファブリック インターコネクト上で設定を再現することもできます。 このファイルは、インポートには使用できません。 • [All configuration]：すべてのシステム設定と論理設定が含まれる XML ファイル。 このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。 このファイルは、システムの復元には使用できません。 このファイルには、ローカル認証されたユーザのパスワードは含まれません。 • [System configuration]：ユーザ名、ロール、ロケールなどのすべてのシステム設定が含まれる XML ファイル。 このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。 このファイルは、システムの復元には使用できません。 • [Logical configuration]：サービス プロファイル、VLAN、VSAN、プール、ポリシーなどのすべての論理設定が含まれる XML ファイル。 このバックアップにより生成されたファイルを使用して、これらの設定を元のファブリック インターコネクトまたは別のファブリック インターコネクトにインポートできます。 このファイルは、システムの復元には使用できません。
[Preserve Identities] チェックボックス	このチェックボックスをオンにすると、バックアップ ファイルに、MAC アドレス、WWPN、WWNN、および UUID などのプールから派生したすべての ID が維持されます。

名前	説明
[Location of the Backup File] フィールド	バックアップファイルの保存場所。 次のいずれかになります。 • [Remote File System]：バックアップ XML ファイルはリモートサーバに保存されます。 Cisco UCS Manager GUI によって次に示すフィールドが表示され、リモートシステムのプロトコル、ホスト、ファイル名、ユーザ名、パスワードを指定できます。 • [Local File System]：バックアップ XML ファイルはローカルに保存されます。 Cisco UCS Manager GUI によって [Filename] フィールドが、関連付けられた [Browse] ボタンとともに表示され、バックアップファイルの名前と場所を指定できます。 （注） [OK] をクリックした後、場所は変更できません。
[Protocol] フィールド	リモートサーバとの通信時に使用するプロトコル。 次のいずれかになります。 • FTP • TFTP • SCP • SFTP
[Hostname] フィールド	バックアップファイルが格納されている場所のホスト名または IP アドレス。 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。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Remote File] フィールド	バックアップ コンフィギュレーション ファイルのフル パス。 このフィールドには、ファイル名とパスを含めることができます。 ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。

名前	説明
[User] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。 Cisco UCS Manager ではこのパスワードは保存されません。 そのため、バックアップ操作をすぐにイネーブルにして、実行する予定がない限り、このパスワードを入力する必要はありません。

ステップ 7 [OK] をクリックします。

ステップ 8 Cisco UCS Manager に確認ダイアログボックスが表示されたら、[OK] をクリックします。
[Admin State] フィールド をイネーブルに設定すると、Cisco UCS Manager によって、選択した設定タイプのスナップショットが取得され、ファイルがネットワークの場所にエクスポートされます。 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

ステップ 9 （任意） バックアップ操作の進行状況を表示するには、次の操作を実行します。

a) [Properties] 領域に操作が表示されない場合、[Backup Operations] テーブルの操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 10 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。
バックアップ操作は完了するまで実行し続けます。 進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

バックアップ操作の実行

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域の [Backup] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルで、実行するバックアップ操作をクリックします。
選択されたバックアップ操作の詳細が [Properties] 領域に表示されます。

ステップ 6 [Properties] 領域で、次のフィールドに値を入力します。

a) [Admin State] フィールドで、[Enabled] オプション ボタンをクリックします。

b) TFTP を除くすべてのプロトコルについて、ユーザ名に対応するパスワードを [Password] フィールドに入力します。

c) （任意） その他の使用可能なフィールドでコンテンツを変更します。

ステップ 7 [Apply] をクリックします。
Cisco UCS Manager は、選択された設定タイプのスナップショットを作成し、ファイルをネットワークの場所にエクスポートします。 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルに、バックアップ操作が表示されます。

ステップ 8 （任意） バックアップ操作の進捗状況を確認するには、[FSM Details] バーの下矢印をクリックします。
[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 9 [OK] をクリックし、[Backup Configuration] ダイアログボックスを閉じます。
バックアップ操作は完了するまで実行し続けます。 進捗を表示するには、[Backup Configuration] ダイアログボックスを再度開きます。

バックアップ操作の変更

バックアップ操作を修正して、別のバックアップ タイプのファイルをその場所に保存したり、前のバックアップ ファイルが上書きされないようにファイル名を変更したりすることができます。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域の [Backup] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Backup Operations] 領域で、変更するバックアップ操作をクリックします。
選択されたバックアップ操作の詳細が [Properties] 領域に表示されます。 バックアップ操作がディセーブル状態の場合、このフィールドはグレー表示されています。

ステップ 6 [Admin State] フィールドで、[enabled] オプション ボタンをクリックします。

ステップ 7 該当するフィールドを変更します。
バックアップ操作をただちに実行する場合を除き、パスワードを入力する必要はありません。

ステップ 8 （任意） バックアップ操作を今すぐに実行しない場合は、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。

ステップ 9 [OK] をクリックします。

1 つまたは複数のバックアップ操作の削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域の [Backup] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Backup Operations] テーブルで、削除するバックアップ操作をクリックします。

ヒント 操作の管理状態が [Enabled] に設定されている場合、テーブルでバックアップ操作をクリックすることはできません。

ステップ 6 [Backup Operations] テーブルのアイコン バーの [Delete] アイコンをクリックします。

ステップ 7 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [Backup Configuration] ダイアログボックスで、次のいずれかをクリックします。

オプション	説明
Apply	ダイアログボックスを閉じずに、選択したバックアップ操作を削除します。

オプション	説明
OK	選択したバックアップ操作を削除し、ダイアログボックスを閉じます。

スケジュール バックアップの設定

完全な状態のバックアップ ポリシーの設定

はじめる前に

バックアップ サーバの IP アドレスおよび認証クレデンシャルを取得します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインの [Backup and Export Policy] タブをクリックします。

ステップ 4 [Full State Backup Policy] で、次のフィールドに値を入力します。

名前	説明
[Hostname] フィールド	ポリシーバックアップ ファイルが格納されている場所のホスト名または IP アドレス。 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。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。

名前	説明
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。 次のいずれかになります。 • FTP • TFTP • SCP • SFTP
[User] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。
[Remote File] フィールド	ポリシー バックアップ ファイルへのフル パス。 このフィールドには、ファイル名とパスを含めることができます。 ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
[Admin State] フィールド	次のいずれかになります。 • [Enabled]：Cisco UCS Manager は [Schedule] フィールドに指定されているスケジュールを使用して、すべてのポリシー情報をバックアップします。 • [Disabled]：Cisco UCS Manager はポリシー情報をバックアップしません。
[Schedule] フィールド	Cisco UCS Manager がポリシー情報をバックアップする頻度。
[Max Cap] フィールド	Cisco UCS Manager が保持するバックアップ ファイルの最大数。 この値は変更できません。
[Description] フィールド	バックアップ ポリシーの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

ステップ 5 [Save Changes] をクリックします。

すべてのコンフィギュレーションのエクスポート ポリシーの設定

はじめる前に

バックアップ サーバの IP アドレスおよび認証クレデンシャルを取得します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

ステップ 3 [Work] ペインの [Backup and Export Policy] タブをクリックします。

ステップ 4 [All Configuration Export Policy] で、次のフィールドに値を入力します。

名前	説明
[Hostname] フィールド	設定ポリシーバックアップ ファイルが格納されている場所のホスト名または IP アドレス。 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。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Protocol] フィールド	リモート サーバとの通信時に使用するプロトコル。 次のいずれかになります。 • FTP • TFTP • SCP • SFTP
[User] フィールド	システムがリモート サーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。

名前	説明
[Password] フィールド	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。
[Remote File] フィールド	バックアップ コンフィギュレーション ファイルのフル パス。 このフィールドには、ファイル名とパスを含めることができます。 ファイル名を省略すると、バックアップ手順によって、ファイルに名前が割り当てられます。
[Admin State] フィールド	次のいずれかになります。 • [Enabled]：Cisco UCS Manager は [Schedule] フィールドに指定されているスケジュールを使用して、すべてのポリシー情報をバックアップします。 • [Disabled]：Cisco UCS Manager はポリシー情報をバックアップしません。
[Schedule] フィールド	Cisco UCS Manager がポリシー情報をバックアップする頻度。
[Max Cap] フィールド	Cisco UCS Manager が保持する設定バックアップ ファイルの最大数。 この値は変更できません。
[Description] フィールド	設定エクスポート ポリシーの説明。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

ステップ 5 [Save Changes] をクリックします。

インポート操作の設定

インポート操作の作成

Full State コンフィギュレーション ファイルはインポートできません。 次のコンフィギュレーション ファイルのいずれもインポートできます。

- すべてのコンフィギュレーション

- システム コンフィギュレーション
- 論理コンフィギュレーション

はじめる前に

コンフィギュレーション ファイルのインポートに必要な次の情報を収集します。

- バックアップ サーバの IP アドレスおよび認証クレデンシャル
- バックアップ ファイルの完全修飾名

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Import Configuration] ダイアログボックスで、[Create Import Operation] をクリックします。

ステップ 6 [Create Import Operation] 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
[Admin State] フィールド	次のいずれかになります。 • [Enabled]：[OK] をクリックするとすぐに、Cisco UCS Manager によってインポート操作が実行されます。 • [Disabled]：[OK] をクリックしても、Cisco UCS Manager によってインポート操作は実行されません。 このオプションを選択すると、ダイアログボックスのすべてのフィールドが表示されたままになります。 ただし、インポートは [Import Configuration] ダイアログボックスから手動で実行する必要があります。
[Action] フィールド	次のいずれかになります。 • [Merge]：設定情報が既存の情報とマージされます。 競合する場合、現在のシステム上の情報が、インポート設定ファイル内の情報に置き換えられます。 • [Replace]：インポート設定ファイル内の各オブジェクトが採用され、現在の設定内の対応するオブジェクトは上書きされます。

名前	説明
[Location of the Import File] フィールド	インポートするバックアップファイルが置かれている場所。 次のいずれかになります。 • [Remote File System]：バックアップ XML ファイルはリモートサーバに保存されます。 Cisco UCS Manager GUI によって次に示すフィールドが表示され、リモートシステムのプロトコル、ホスト、ファイル名、ユーザ名、パスワードを指定できます。 • [Local File System]：バックアップ XML ファイルはローカルに保存されます。 Cisco UCS Manager GUI によって [Filename] フィールドが、関連付けられた [Browse] ボタンとともに表示され、バックアップファイルの名前と場所を指定できます。
[Protocol] フィールド	リモートサーバとの通信時に使用するプロトコル。 次のいずれかになります。 • FTP • TFTP • SCP • SFTP
[Hostname] フィールド	設定ファイルのインポート元のホスト名または IP アドレス。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Remote File] フィールド	XML コンフィギュレーション ファイルの名前。
[User] フィールド	システムがリモートサーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。

名前	説明
[Password] フィールド	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。 Cisco UCS Manager ではこのパスワードは保存されません。 したがって、インポート操作をイネーブルにしてただちに実行する場合を除き、このパスワードを入力する必要はありません。

ステップ 7 [OK] をクリックします。

ステップ 8 確認ダイアログボックスで、[OK] をクリックします。
[Admin State] をイネーブルに設定した場合、Cisco UCS Manager は、ネットワークの場所から設定をインポートします。 選択した処理に応じて、ファイル内の情報が既存の設定と結合されるか、既存の設定と置き換えられます。 インポート操作は、[Import Configuration] ダイアログボックスの [Import Operations] テーブルに表示されます。

ステップ 9 （任意） インポート操作の進捗状況を表示するには、次の手順を実行します。

a) [Properties] 領域にインポート操作が自動的に表示されない場合は、[Import Operations] テーブルでインポート操作をクリックします。

b) [Properties] 領域で、[FSM Details] バーの下矢印をクリックします。

[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 10 [OK] をクリックして、[Import Configuration] ダイアログボックスを閉じます。
インポート操作は、終了するまで実行されます。 進捗状況を表示するには、[Import Configuration] を再度開きます。

インポート操作の実行

Full State コンフィギュレーション ファイルはインポートできません。 次のコンフィギュレーション ファイルのいずれもインポートできます。

- すべてのコンフィギュレーション
- システム コンフィギュレーション
- 論理コンフィギュレーション

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Import Configuration] ダイアログボックスの [Import Operations] テーブルで、実行する操作をクリックします。
選択されたインポート操作の詳細が [Properties] 領域に表示されます。

ステップ 6 [Properties] 領域で、次のフィールドに値を入力します。

a) [Admin State] フィールドで、[Enabled] オプション ボタンをクリックします。

b) TFTP を除くすべてのプロトコルについて、ユーザ名に対応するパスワードを [Password] フィールドに入力します。

c) （任意） その他の使用可能なフィールドでコンテンツを変更します。

ステップ 7 [Apply] をクリックします。
Cisco UCS Manager は、ネットワークの場所から設定ファイルをインポートします。 選択した処理に応じて、ファイル内の情報が既存の設定と結合されるか、既存の設定と置き換えられます。
インポート操作は、[Import Configuration] ダイアログボックスの [Import Operations] テーブルに表示されます。

ステップ 8 （任意） インポート操作の進捗状況を確認するには、[FSM Details] バーの下矢印をクリックします。
[FSM Details] 領域が展開され、操作のステータスが表示されます。

ステップ 9 [OK] をクリックして、[Import Configuration] ダイアログボックスを閉じます。
インポート操作は、終了するまで実行されます。 進捗状況を表示するには、[Import Configuration] を再度開きます。

インポート操作の変更

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Import Configuration] ダイアログボックスの [Import Operations] 領域で、変更するインポート操作をクリックします。

選択されたインポート操作の詳細が [Properties] 領域に表示されます。 インポート操作がディセーブル状態の場合、このフィールドはグレー表示されています。

ステップ 6 [Admin State] フィールドで、[enabled] オプション ボタンをクリックします。

ステップ 7 該当するフィールドを変更します。
インポート操作をただちに実行する場合を除き、パスワードを入力する必要はありません。

ステップ 8 （任意） インポート操作を今すぐに実行しない場合は、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。

ステップ 9 [OK] をクリックします。

1 つまたは複数のインポート操作の削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [All] ノードをクリックします。

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 [Actions] 領域で、[Import Configuration] をクリックします。

ステップ 5 [Backup Configuration] ダイアログボックスの [Import Operations] テーブルで、削除するインポート操作をクリックします。

ヒント 操作の管理状態が [Enabled] に設定されている場合、テーブルでインポート操作をクリックすることはできません。

ステップ 6 [Import Operations] テーブルのアイコン バーの [Delete] アイコンをクリックします。

ステップ 7 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ステップ 8 [Import Configuration] ダイアログボックスで、次のいずれかをクリックします。

オプション	説明
Apply	ダイアログボックスを閉じずに、選択したインポート操作を削除します。
OK	選択したインポート操作を削除し、ダイアログボックスを閉じます。

ファブリック インターコネクトの設定の復元

はじめる前に

システム コンフィギュレーションを復元するために必要な次の情報を収集します。

- ファブリック インターコネクト管理ポートの IP アドレスおよびサブネット マスク
- デフォルト ゲートウェイの IP アドレス
- バックアップ サーバの IP アドレスおよび認証クレデンシャル
- Full State バックアップ ファイルの完全修飾名

（注） システムを復元するには、Full State コンフィギュレーション ファイルへのアクセスが必要です。 その他のタイプのコンフィギュレーション ファイルやバックアップ ファイルでは、システムを復元できません。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 ファブリック インターコネクトがオフの場合はオンにします。
ファブリック インターコネクトがブートする際、Power On Self-Test のメッセージが表示されます。

ステップ 3 インストール方式プロンプトに gui と入力します。

ステップ 4 システムが DHCP サーバにアクセスできない場合、次の情報を入力するよう求められることがあります。

- ファブリック インターコネクトの管理ポートの IP アドレス
- ファブリック インターコネクトの管理ポートのサブネット マスク
- ファブリック インターコネクトに割り当てられたデフォルト ゲートウェイの IP アドレス

ステップ 5 プロンプトから、Web ブラウザに Web リンクをコピーし、Cisco UCS Manager GUI 起動ページに移動します。

ステップ 6 起動ページで [Express Setup] を選択します。

ステップ 7 [Express Setup] ページで [Restore From Backup] を選択し、[Submit] をクリックします。

ステップ 8 [Cisco UCS Manager Initial Setup] ページの [Protocol] 領域で、完全な状態のバックアップ ファイルをアップロードするために使用するプロトコルを選択します。

- SCP
- TFTP

- FTP
- SFTP

ステップ 9 [Server Information] 領域で、次のフィールドに値を入力します。

名前	説明
Server IP	完全な状態のバックアップ ファイルがあるコンピュータの IP アドレス。 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。
Backup File Path	フォルダ名やファイル名など、完全な状態のバックアップ ファイルがあるファイルのパス。
User ID	システムがリモート サーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。
Password	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。

ステップ 10 [Submit] をクリックします。
コンソールに戻ってシステム復元の進捗状況を確認できます。

ファブリック インターコネクトはバックアップ サーバにログインし、指定された完全な状態のバックアップ ファイルのコピーを取得し、システム設定を復元します。

クラスタ設定の場合、セカンダリ ファブリック インターコネクトを復元する必要はありません。セカンダリ ファブリック インターコネクトがリブートすると、Cisco UCS Manager はただちにその設定をプライマリ ファブリック インターコネクトと同期させます。

第 42 章

失われたパスワードの復旧

この章の内容は、次のとおりです。

- 失われたパスワードの復旧，771 ページ

失われたパスワードの復旧

admin アカウントのパスワードの復旧

admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。 アドミニストレータが admin アカウントのパスワードを失うと、重大なセキュリティ上の問題が発生する可能性があります。 その結果、admin アカウントのパスワードを復旧するために、Cisco UCS ドメインのすべてのファブリック インターコネクトの電源を再投入する必要が生じます。

admin アカウントのパスワードを復旧する場合、実際にはそのアカウントのパスワードを変更します。 admin アカウントに対応する元のパスワードを取得することはできません。

admin 以外のすべてのローカル アカウントのパスワードは、Cisco UCS Manager からリセットできます。 ただし、AAA または admin 権限を持つアカウントを使用して Cisco UCS Manager にログインする必要があります。

注意 この手順では、Cisco UCS ドメインのすべてのファブリック インターコネクトの電源を切断する必要があります。 したがって、Cisco UCS ドメイン内のすべてのデータ送信は、ファブリック インターコネクトが再起動されるまで停止します。

ファブリック インターコネクトのリーダーシップ ロールの決定

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

ステップ 3 ロールを識別するファブリック インターコネクトをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [General] タブで、[High Availability Details] バーの下矢印をクリックしてこの領域を展開します。

ステップ 6 [Leadership] フィールドを表示して、このファブリック インターコネクトがプライマリ ファブリック インターコネクトか、従属ファブリック インターコネクトかを決定します。

ファブリック インターコネクトのファームウェア バージョンの確認

次の手順を使用して、Cisco UCS ドメインのすべてのファブリック インターコネクトのファームウェア バージョンを確認できます。 ファブリック インターコネクトの [Installed Firmware] タブを使用すると、単一のファブリック インターコネクトのファームウェアを確認できます。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで [Equipment] ノードをクリックします。

ステップ 3 [Work] ペインの [Firmware Management] タブをクリックします。

ステップ 4 [Installed Firmware] タブで、次に示す各ファブリック インターコネクトのファームウェア バージョンが、アップデートしたファームウェアのバージョンと一致していることを確認します。

- カーネル バージョン
- システム バージョン

スタンドアロン設定の admin アカウント パスワードの復旧

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。 admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

はじめる前に

1. ファブリック インターコネクトのコンソール ポートを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次のファームウェアの実行中のバージョンを確認します。
   - ファブリック インターコネクトのファームウェア カーネル バージョン
   - ファームウェア システム バージョン

ヒント　この情報を検索するには、Cisco UCS ドメインで任意のユーザ アカウントを使用してログインします。

手順

ステップ 1　コンソール ポートに接続します。

ステップ 2　ファブリック インターコネクトの電源を次のように再投入します。

a) ファブリック インターコネクトの電源をオフにします。
b) ファブリック インターコネクトの電源をオンにします。

ステップ 3　コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- Ctrl+l
- Ctrl+Shift+r

`loader` プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 4　ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader >
boot /installables/switch/
kernel_firmware_version
```

例：

```
loader >
boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

ステップ 5　config ターミナル モードを入力します。

```
Fabric(boot)#
config terminal
```

ステップ 6　admin パスワードをリセットします。

```
Fabric(boot)(config)#
admin-password
```

password

大文字と数字がそれぞれ 1 つ以上含まれる強力なパスワードを選択します。 このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 7 config ターミナル モードを終了し、ブート プロンプトに戻ります。

ステップ 8 ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)#
load /installables/switch/
system_firmware_version
```

例：

```
Fabric(boot)#
load /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

ステップ 9 システム イメージがロードされたら、Cisco UCS Manager にログインします。

クラスタ設定の admin アカウント パスワードの復旧

この手順により、ファブリック インターコネクトで初期システム セットアップの実行時に admin アカウントに設定したパスワードを復旧できます。 admin アカウントは、システム アドミニストレータまたはスーパーユーザのアカウントです。

はじめる前に

1. ファブリック インターコネクトのコンソール ポートのいずれか 1 つを、コンピュータ ターミナルまたはコンソール サーバに物理的に接続します。
2. 次の情報を入手します。
   - ファブリック インターコネクトのファームウェア カーネル バージョン
   - ファームウェア システム バージョン
   - プライマリ リーダーシップ ロールを持つファブリック インターコネクトと、従属ファブリック インターコネクト

ヒント この情報を検索するには、Cisco UCS ドメインで任意のユーザ アカウントを使用してログインします。

手順

ステップ 1 コンソール ポートに接続します。

ステップ 2 従属ファブリック インターコネクトの場合は、次の手順を実行します。

a) ファブリック インターコネクトの電源をオフにします。

b) ファブリック インターコネクトの電源をオンにします。

c) コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- Ctrl+l
- Ctrl+Shift+r

`loader` プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 3 プライマリ ファブリック インターコネクトの電源を次のように再投入します。

a) ファブリック インターコネクトの電源をオフにします。

b) ファブリック インターコネクトの電源をオンにします。

ステップ 4 コンソールで次のいずれかのキーの組み合わせを押して、起動時に `loader` プロンプトを表示させます。

- Ctrl+l
- Ctrl+Shift+r

`loader` プロンプトを画面に表示するには、選択したキーの組み合わせを複数回押さなければならない場合があります。

ステップ 5 プライマリ ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader > boot /installables/switch/
kernel_firmware_version
```

例：

```
loader > boot /installables/switch/ucs-6100-k9-kickstart.4.1.3.N2.1.0.11.gbin
```

ステップ 6 config ターミナル モードを入力します。

```
Fabric(boot)# config terminal
```

ステップ 7 admin パスワードをリセットします。

```
Fabric(boot)(config)# admin-password password
```

大文字と数字がそれぞれ 1 つ以上含まれる強力なパスワードを選択します。 このパスワードは空にできません。

新しいパスワードはクリア テキスト モードで表示されます。

ステップ 8 config ターミナル モードを終了し、ブート プロンプトに戻ります。

ステップ 9 プライマリ ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```

例：

```
Fabric(boot)# load /installables/switch/ucs-6100-k9-system.4.1.3.N2.1.0.211.bin
```

ステップ 10 システム イメージがロードされたら、Cisco UCS Manager にログインします。

ステップ 11 従属ファブリック インターコネクトのコンソールで、次の手順を実行してシステムを起動します。

a) 従属ファブリック インターコネクトのカーネル ファームウェア バージョンをブートします。

```
loader > boot /installables/switch/
kernel_firmware_version
```

b) 従属ファブリック インターコネクトのシステム ファームウェア バージョンをブートします。

```
Fabric(boot)# load /installables/switch/
system_firmware_version
```

第 VII 部

システム モニタリング

- トラフィックのモニタリング，779 ページ
- ハードウェアのモニタリング，787 ページ
- 統計関連ポリシーの設定，805 ページ
- Call Home の設定，817 ページ
- システム イベント ログの管理，841 ページ
- 障害、イベント、およびログの設定，849 ページ

第 43 章

トラフィックのモニタリング

この章の内容は、次のとおりです。

- トラフィック モニタリング，779 ページ
- トラフィック モニタリングに関する注意事項および推奨事項，780 ページ
- イーサネット トラフィックのモニタリング セッションの作成，781 ページ
- ファイバ チャネル トラフィック モニタリング セッションの作成，783 ページ
- モニタリング セッションへのトラフィック送信元の追加，784 ページ
- トラフィックのモニタリング セッションのアクティブ化，785 ページ
- トラフィック モニタリング セッションの削除，785 ページ

トラフィック モニタリング

トラフィック モニタリングは、1 つ以上の送信元からトラフィックをコピーし、コピーしたトラフィックをネットワーク アナライザによる分析用の専用宛先ポートに送信します。この機能は、Switched Port Analyzer（SPAN）をしても認識されています。

セッションのタイプ

トラフィックモニタリングセッションを作成すると、トラフィックの受信に、イーサネットまたはファイバチャネル宛先ポートを選択できます。宛先ポートのタイプで、使用可能なトラフィックの送信元のタイプを判別するセッションのタイプが決まります。イーサネットトラフィックのモニタリングセッションの場合、宛先ポートは未設定の物理ポートである必要があります。ファイバ チャネル トラフィックのモニタリング セッションの場合、宛先ポートはファイバ チャネル アップリンク ポートである必要があります。

トラフィックの送信元

イーサネットトラフィックのモニタリングセッションは、次のトラフィックの送信元のいずれかをモニタできます。

- アップリンク イーサネット ポート
- イーサネット ポート チャネル
- VLAN
- サービス プロファイル vNIC
- サービス プロファイル vHBA
- FCoE ポート
- ポート チャネル
- サーバ ポート
- ユニファイド アップリンク ポート

ファイバ チャネル トラフィックのモニタリング セッションは、次のトラフィックの送信元のいずれかをモニタできます。

- アップリンク ファイバ チャネル ポート
- SAN ポート チャネル
- VSAN
- サービス プロファイル vHBA
- ファイバ チャネル ストレージ ポート

トラフィック モニタリングに関する注意事項および推奨事項

トラフィック モニタリングを設定するか、またはアクティブにする場合は、次の注意事項を考慮してください。

- 最大 16 個のトラフィックのモニタリング セッションを作成および保存できます。同時にアクティブにすることができるのは 2 つだけです。
- トラフィックのモニタリングセッションは、作成時には、デフォルトでディセーブルです。トラフィックのモニタを開始するには、セッションをアクティブにする必要があります。
- サーバからのトラフィックをモニタするには、サーバに対応するサービスプロファイルからすべての vNIC を追加します。
- ファイバ チャネル トラフィック アナライザまたはイーサネット トラフィック アナライザを使用して、ファイバチャネル トラフィックをモニタできます。 ファイバチャネル トラフィックが、イーサネット宛先ポートを備えたイーサネット トラフィックのモニタリング セッションを使用してモニタされると、宛先トラフィックは FCoE になります。
- トラフィック モニタリングの宛先は単一の物理ポートであるため、トラフィック モニタリング セッションは 1 つのファブリックだけをモニタできます。 ファブリック フェールオーバー間で連続する vNIC のトラフィックをモニタするには、2 つのセッション（ファブリック

ごとに 1 個）を作成し、2 つのアナライザを接続する必要があります。 両方のセッションのトラフィックの送信元として vNIC を追加します。

- すべてのトラフィックの送信元は宛先ポートと同じスイッチ内にある必要があります。
- 宛先ポートとして設定されたポートを送信元ポートとしても設定することはできません。
- ポート チャネルのメンバ ポートは、送信元として個別に設定することはできません。 ポート チャネルが送信元として設定されている場合、すべてのメンバ ポートが送信元ポートです。
- vHBA はイーサネットまたはファイバ チャネルのモニタリング セッションの送信元として設定できますが、両方に対して同時に送信元として使用できません。
- サーバ ポートは、非仮想化されたラック サーバ アダプタ側のポートである場合にのみ送信元にすることができます。
- Cisco UCS 6248 ファブリック インターコネクトのファイバ チャネル ポートは送信元ポートとして設定できません。
- 仮想マシンのポート プロファイルを変更した場合、関連付けられている vNIC で、送信元ポートとして使用されるポートはモニタから削除されますが、モニタリング セッションを再設定する必要があります。
- トラフィックのモニタリング セッションが、Cisco UCS Manager Release 2.0 以前のリリースで、ダイナミック vNIC に設定されていた場合、アップグレード後にトラフィックのモニタリング セッションを再設定する必要があります。

（注） トラフィック モニタリングは、システム リソースに著しい負荷をかける可能性があります。負荷を最小限にするには、不要なトラフィックの伝送ができるだけ少ない送信元を選択して、トラフィック モニタリングが不要な場合はディセーブルにします。

イーサネット トラフィックのモニタリング セッションの作成

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [*Fabric_Interconnect_Name*] を右クリックし、[Create Traffic Monitoring Session] を選択します。

ステップ 4 [Create Traffic Monitoring Session] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	トラフィック モニタリング セッションの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Admin State] フィールド	[Destination] フィールドで選択した物理ポートで、トラフィックがモニタされるかどうか。 次のいずれかになります。 • [Enabled]：一部の送信元コンポーネントがセッションに追加されると、Cisco UCS によってただちにポート アクティビティのモニタリングが開始されます。 • [Disabled]：ポート アクティビティは、Cisco UCS によってモニタされません。
[Destination] ドロップダウン リスト	ナビゲーション ツリーから通信トラフィックを監視する物理ポートを選択します。
[Admin Speed] フィールド	モニタされるポート チャネルのデータ転送速度。 使用可能なデータ レートは、Cisco UCS ドメインにインストールされているファブリック インターコネクトによって異なります。

ステップ 5 [OK] をクリックします。

次の作業

- トラフィックのモニタリング セッションにトラフィック ソースを追加します。
- トラフィックのモニタリング セッションをアクティブにします。

ファイバ チャネル トラフィック モニタリング セッションの作成

手順

ステップ 1 [Navigation] ペインの [SAN] タブをクリックします。

ステップ 2 [LAN] タブで、[SAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 [*Fabric_Interconnect_Name*] を右クリックし、[Create Traffic Monitoring Session] を選択します。

ステップ 4 [Create Traffic Monitoring Session] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	トラフィック モニタリング セッションの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Admin State] フィールド	[Destination] フィールドで選択した物理ポートで、トラフィックがモニタされるかどうか。 次のいずれかになります。 • [Enabled]：一部の送信元コンポーネントがセッションに追加されると、Cisco UCS によってただちにポート アクティビティのモニタリングが開始されます。 • [Disabled]：ポート アクティビティは、Cisco UCS によってモニタされません。
[Destination] ドロップダウン リスト	ナビゲーション ツリーから通信トラフィックを監視する物理ポートを選択します。
[Speed Admin] ドロップダウン リスト	モニタされるポート チャネルのデータ転送速度。 次のいずれかになります。 • 1 Gbps • 2 Gbps • 4 Gbps • 8 Gbps • [Auto]：データ転送速度がCisco UCS判断されます。

ステップ 5 [OK] をクリックします。

次の作業

- トラフィックのモニタリング セッションにトラフィック ソースを追加します。
- トラフィックのモニタリング セッションをアクティブにします。

モニタリング セッションへのトラフィック送信元の追加

トラフィックのモニタリング セッションがモニタする複数の送信元タイプから複数の送信元を選択できます。 利用可能な送信元は、Cisco UCS ドメインに設定されたコンポーネントによって異なります。

（注） この手順では、イーサネット トラフィックのモニタリング セッションに対して送信元を追加する方法について説明します。 ファイバ チャネルのモニタリング セッションに送信元を追加するには、ステップ 2 の [LAN] タブの代わりに [SAN] タブを選択します。

はじめる前に

トラフィックのモニタリング セッションを作成する必要があります。

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 *Fabric_Interconnect_Name* を展開して設定するモニタ セッションをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Sources] 領域で、追加するトラフィックの送信元のタイプのセクションを展開します。

ステップ 6 モニタリングに使用できるコンポーネントを表示するには、テーブルの右端にある[+] ボタンをクリックして [Create Monitoring Session Source] ダイアログボックスを開きます。

ステップ 7 送信元のコンポーネントを選択して [OK] をクリックします。
必要に応じて前述の 3 つのステップを繰り返し、複数の送信元のタイプから複数の送信元を追加します。

ステップ 8 [Save Changes] をクリックします。

次の作業

トラフィック モニタリング セッションをアクティブにします。 セッションがすでにアクティブ化されている場合、トラフィックは送信元の追加時にモニタリングの宛先に転送されます。

トラフィックのモニタリング セッションのアクティブ化

（注） この手順では、イーサネット トラフィックのモニタリング セッションをアクティブにする方法について説明します。 ファイバ チャネルのモニタリング セッションをアクティブにするには、ステップ 2 の [LAN] タブの代わりに [SAN] タブを選択します。

はじめる前に

トラフィックのモニタリング セッションを作成する必要があります。

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 *Fabric_Interconnect_Name* を展開してアクティブにするモニタ セッションをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Properties] 領域で、[Admin State] に対する [enabled] をクリックします。

ステップ 6 [Save Changes] をクリックします。

トラフィック モニタリングの送信元が設定されている場合、トラフィックはトラフィック モニタリングの宛先ポートにフローを開始します。

トラフィック モニタリング セッションの削除

（注） この手順では、イーサネット トラフィックのモニタリング セッションを削除する方法について説明します。 ファイバ チャネルのモニタリング セッションを削除するには、ステップ 2 の [LAN] タブの代わりに [SAN] タブを選択します。

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [Traffic Monitoring Sessions] > [*Fabric_Interconnect_Name*] を展開します。

ステップ 3 *Fabric_Interconnect_Name* を展開して削除するモニタ セッションをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Delete] アイコンをクリックします。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

第 44 章

ハードウェアのモニタリング

この章の内容は、次のとおりです。

- ファブリック インターコネクトのモニタリング，787 ページ
- シャーシのモニタリング，788 ページ
- ブレード サーバのモニタリング，790 ページ
- ラックマウント サーバのモニタリング，793 ページ
- I/O モジュールのモニタリング，796 ページ
- 管理インターフェイスのモニタリング，796 ページ
- サーバ ディスク ドライブ モニタリング，799 ページ

ファブリック インターコネクトのモニタリング

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Fabric Interconnects] を展開します。

ステップ 3 モニタするファブリック 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] ペインで次のタブのいずれかをクリックして、ファブリック インターコネクトのステータスを表示します。

オプション	説明
[General] タブ	障害の概要、ファブリック インターコネクト プロパティの概要、ファブリック インターコネクトとそのコンポーネントの物理表示など、ファブリック インターコネクトのステータスの概要が示されます。

オプション	説明
[Physical Ports] タブ	ファブリック インターコネクトのすべてのポートのステータスが表示されます。 このタブには次のサブタブが含まれます。 • [Uplink Ports] タブ • [Server Ports] タブ • [Fibre Channel Ports] タブ • [Unconfigured Ports] タブ
[Fans] タブ	ファブリックインターコネクトのすべてのファンモジュールのステータスが表示されます。
[PSUs] タブ	ファブリック インターコネクトのすべての電源モジュールのステータスが表示されます。
[Physical Display] タブ	ファブリック インターコネクトとすべてのポートおよびその他のコンポーネントがグラフィック表示されます。 コンポーネントに障害がある場合、そのコンポーネントの横に障害アイコンが表示されます。
[Faults] タブ	ファブリックインターコネクトで発生した障害の詳細が表示されます。
[Events] タブ	ファブリック インターコネクトで発生したイベントの詳細が表示されます。
[Statistics] タブ	ファブリック インターコネクトとそのコンポーネントに関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。

シャーシのモニタリング

ヒント シャーシ内の個々のコンポーネントをモニタするには、そのコンポーネントのノードを展開します。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 モニタするシャーシをクリックします。

ステップ 4 次のタブのいずれかをクリックして、シャーシのステータスを表示します。

オプション	説明
[General] タブ	障害の概要、シャーシプロパティの概要、シャーシとそのコンポーネントの物理表示など、シャーシのステータスの概要が示されます。
[Servers] タブ	シャーシ内の全サーバのステータスと選択されたプロパティが表示されます。
[Service Profiles] タブ	シャーシ内のサーバに関連付けられたサービスプロファイルのステータスを表示します。
[IO Modules] タブ	シャーシ内のすべての IO モジュールのステータスと選択されたプロパティが表示されます。
[Fans] タブ	シャーシ内のすべてのファン モジュールのステータスが表示されます。
PSUs	シャーシ内のすべての電源モジュールのステータスが表示されます。
[Hybrid Display] タブ	シャーシとファブリックインターコネクト間の接続に関する詳細情報が表示されます。 この表示には、次のコンポーネントを表すアイコンがあります。 • システムの各ファブリック インターコネクト。 • 選択されたコンポーネントの I/O モジュール（IOM）。これは、接続パスを見やすくするために独立したユニットとして表示されます。 • サーバと PSU を示す選択されたシャーシ。
[Slots] タブ	シャーシ内のすべてのスロットのステータスが表示されます。
[Installed Firmware] タブ	シャーシ内の IO モジュールおよびサーバの現在のファームウェア バージョンが表示されます。 このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。

オプション	説明
[SEL Logs] タブ	シャーシ内のサーバに対するシステム イベント ログが表示され、そのログにアクセスできます。
[Faults] タブ	シャーシで発生した障害の詳細が表示されます。
[Events] タブ	シャーシで発生したイベントの詳細が表示されます。
[FSM] タブ	シャーシに関連する FSM タスクの詳細およびステータスが表示されます。 この情報を使用して、これらのタスクにおけるエラーを診断できます。
[Statistics] タブ	シャーシとそのコンポーネントに関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Temperatures] タブ	シャーシのコンポーネントの温度に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Power] タブ	シャーシのコンポーネントの電力に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。

ブレード サーバのモニタリング

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 モニタするサーバをクリックします。

ステップ 4 [Work] ペインで次のタブのいずれかをクリックして、サーバのステータスを表示します。

オプション	説明
[General] タブ	障害の概要、サーバ プロパティの概要、サーバとそのコンポーネントの物理表示など、サーバのステータスの概要が示されます。

オプション	説明
[Inventory] タブ	サーバのコンポーネントのプロパティとステータスに関する詳細情報が次のサブタブに表示されます。 • [Motherboard]：マザーボードとサーバ BIOS 設定に関する情報。 このサブタブから、破損した BIOS ファームウェアを復旧させることもできます。 • [CIMC]：CIMC とそのファームウェアに関する情報。サーバの SEL にもアクセスできます。 また、スタティックまたはプーリング済み管理 IP アドレスを割り当て、このサブタブから CIMC ファームウェアを更新し、アクティブにすることもできます。 • [CPUs]：サーバの各 CPU に関する情報。 • [Memory]：サーバの各メモリ スロットと、スロットの DIMM に関する情報。 • [Adapters]：サーバに取り付けられた各アダプタに関する情報。 • [HBAs]：各 HBA のプロパティと、サーバに関連付けられたサービス プロファイルでの HBA の設定。 • [NICs]：各 NIC のプロパティと、サーバに関連付けられたサービス プロファイルでの NIC の設定。 各行を展開すると、関連する VIF および vNIC に関する情報を表示できます。 • [iSCSI vNICs]：各 iSCSI vNIC のプロパティと、サーバに関連付けられたサービス プロファイルでの vNIC の設定。 • [Storage]：ストレージ コントローラのプロパティ、サーバに関連付けられたサービス プロファイルでのローカル ディスク設定ポリシー、サーバの各ハード ディスクに関する情報。 **ヒント** ハード ディスク ドライブやソリッド ステート ドライブなどの SATA デバイスがサーバに 1 つ以上 搭載されている場合、Cisco UCS Manager GUI の [Vendor] フィールドにはその SATA デバイスのベンダー名が表示されます。 ただし、Cisco UCS Manager CLI では、[Vendor] フィールドに ATA が表示され、ベンダー名などのベンダー情報は [Vendor Description] フィールドに表示されます。 この 2 番目のフィールドは Cisco UCS Manager GUI にはありません。
[Virtual Machines] タブ	サーバでホストされている仮想マシンの詳細情報が表示されます。
[Installed Firmware] タブ	CIMC、アダプタ、その他のサーバ コンポーネントのファームウェア バージョンが表示されます。 このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。

オプション	説明
[SEL Logs] タブ	サーバのシステム イベント ログが表示されます。
[VIF Paths] タブ	サーバのアダプタの VIF パスを表示します。
[Faults] タブ	サーバで発生した障害の概要が表示されます。 障害をクリックすると、詳細情報が表示されます。
[Events] タブ	サーバで発生したイベントの概要が表示されます。 イベントをクリックすると、詳細情報が表示されます。
[FSM] タブ	タスクのステータスなど、サーバで実行されている現在の FSM タスクに関する詳細情報が表示されます。 この情報を使用して、これらのタスクにおけるエラーを診断できます。
[Statistics] タブ	サーバとそのコンポーネントに関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Temperatures] タブ	サーバのコンポーネントの温度に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Power] タブ	サーバのコンポーネントの電力に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。

ステップ 5 [Navigation] ペインで、[*Server_ID*] > [Adapters] > *[Adapter_ID]* を展開します。

ステップ 6 [Work] ペインで、次のアダプタのコンポーネントの 1 つ以上を右クリックしてナビゲータを開き、コンポーネントのステータスを表示します。

- アダプタ
- DCE インターフェイス
- HBA
- NIC

ヒント 子ノードを表示するには、テーブル内のノードを展開します。 たとえば、[NIC] ノードを展開すると、その NIC で作成された各 VIF を表示できます。

ラックマウント サーバのモニタリング

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 モニタするサーバをクリックします。

ステップ 4 [Work] ペインで次のタブのいずれかをクリックして、サーバのステータスを表示します。

オプション	説明
[General] タブ	障害の概要、サーバ プロパティの概要、サーバとそのコンポーネントの物理表示など、サーバのステータスの概要が示されます。

オプション	説明
[Inventory] タブ	サーバのコンポーネントのプロパティとステータスに関する詳細情報が次のサブタブに表示されます。 • [Motherboard]：マザーボードとサーバ BIOS 設定に関する情報。 このサブタブから、破損した BIOS ファームウェアを復旧させることもできます。 • [CIMC]：CIMC とそのファームウェアに関する情報。サーバの SEL にもアクセスできます。 また、スタティックまたはプーリング済み管理 IP アドレスを割り当て、このサブタブから CIMC ファームウェアを更新し、アクティブにすることもできます。 • [CPU]：サーバの各 CPU に関する情報。 • [Memory]：サーバの各メモリ スロットと、スロットの DIMM に関する情報。 • [Adapters]：サーバに取り付けられた各アダプタに関する情報。 • [HBAs]：各 HBA のプロパティと、サーバに関連付けられたサービス プロファイルでの HBA の設定。 • [NICs]：各 NIC のプロパティと、サーバに関連付けられたサービス プロファイルでの NIC の設定。 各行を展開すると、関連する VIF および vNIC に関する情報を表示できます。 • [iSCSI vNICs]：各 iSCSI vNIC のプロパティと、サーバに関連付けられたサービス プロファイルでの vNIC の設定。 • [Storage]：ストレージ コントローラのプロパティ、サーバに関連付けられたサービス プロファイルでのローカル ディスク設定ポリシー、サーバの各ハード ディスクに関する情報。 **ヒント** ハード ディスク ドライブやソリッド ステート ドライブなどの SATA デバイスがサーバに 1 つ以上 搭載されている場合、Cisco UCS Manager GUI の [Vendor] フィールドにはその SATA デバイスのベンダー名が表示されます。 ただし、Cisco UCS Manager CLI では、[Vendor] フィールドに ATA が表示され、ベンダー名などのベンダー情報は [Vendor Description] フィールドに表示されます。 この 2 番目のフィールドは Cisco UCS Manager GUI にはありません。
[Virtual Machines] タブ	サーバでホストされている仮想マシンの詳細情報が表示されます。
[Installed Firmware] タブ	CIMC、アダプタ、その他のサーバ コンポーネントのファームウェア バージョンが表示されます。 このタブを使用して、これらのコンポーネントのファームウェアをアップデートおよびアクティブ化することもできます。

オプション	説明
[SEL Logs] タブ	サーバのシステム イベント ログが表示されます。
[VIF Paths] タブ	サーバのアダプタの VIF パスを表示します。
[Faults] タブ	サーバで発生した障害の概要が表示されます。 障害をクリックすると、詳細情報が表示されます。
[Events] タブ	サーバで発生したイベントの概要が表示されます。 イベントをクリックすると、詳細情報が表示されます。
[FSM] タブ	タスクのステータスなど、サーバで実行されている現在の FSM タスクに関する詳細情報が表示されます。 この情報を使用して、これらのタスクにおけるエラーを診断できます。
[Statistics] タブ	サーバとそのコンポーネントに関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Temperatures] タブ	サーバのコンポーネントの温度に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。
[Power] タブ	サーバのコンポーネントの電力に関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。

ステップ 5 [Navigation] ペインで、[*Server_ID*] > [Adapters] > [*Adapter_ID*] と展開します。

ステップ 6 [Work] ペインで、次のアダプタのコンポーネントの 1 つ以上を右クリックしてナビゲータを開き、コンポーネントのステータスを表示します。

- アダプタ
- DCE インターフェイス
- HBA
- NIC

ヒント 子ノードを表示するには、テーブル内のノードを展開します。 たとえば、[NIC] ノードを展開すると、その NIC で作成された各 VIF を表示できます。

I/O モジュールのモニタリング

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [IO Modules] を展開します。

ステップ 3 モニタする I/O モジュールをクリックします。

ステップ 4 次のタブのいずれかをクリックして、I/O モジュールのステータスを表示します。

オプション	説明
[General] タブ	障害の概要、モジュール プロパティの概要、モジュールとそのコンポーネントの物理表示など、I/Oモジュールのステータスの概要が示されます。
[Fabric Ports] タブ	I/O モジュールのすべてのファブリック ポートのステータスおよび選択されたプロパティが表示されます。
[Backplane Ports] タブ	I/O モジュールのすべてのバックアップ ポートのステータスおよび選択されたプロパティが表示されます。
[Faults] タブ	I/O モジュールで発生した障害の詳細が表示されます。
[Events] タブ	I/O モジュールで発生したイベントの詳細が表示されます。
[FSM] タブ	I/O モジュールに関連する FSM タスクの詳細およびステータスが表示されます。 この情報を使用して、これらのタスクにおけるエラーを診断できます。
[Statistics] タブ	I/Oモジュールとそのコンポーネントに関する統計情報が表示されます。 これらの統計情報は図表形式で表示できます。

管理インターフェイスのモニタリング

管理インターフェイスのモニタリング ポリシー

このポリシーは、ファブリック インターコネクトの mgmt0 イーサネット インターフェイスの監視方法を定義します。 Cisco UCS が管理インターフェイスの障害を検出すると、障害レポートが生成されます。 障害レポート数が設定された回数に達した場合、システムは管理インターフェイ

スを使用できないと判断し、エラーを生成します。 デフォルトでは、管理インターフェイスのモニタリング ポリシーはディセーブルです。

影響を受ける管理インターフェイスが管理インスタンスであるファブリック インターコネクトに属する場合、Cisco UCS は従属ファブリック インターコネクトのステータスが稼働状態で、それに対して記録された現在の障害のレポートがないことを確認した後、エンドポイントの管理インスタンスを変更します。

影響を受けるファブリックインターコネクトが現在ハイアベイラビリティ設定のプライマリ内部である場合、管理プレーンのフェールオーバーがトリガーされます。データプレーンはこのフェールオーバーの影響を受けません。

管理インターフェイスのモニタリングに関連する次のプロパティを設定できます。

- 管理インターフェイスをモニタリングするために使用されるメカニズムのタイプ。
- 管理インターフェイスのステータスをモニタリングする間隔。
- システムが管理を行えないと判断し、障害メッセージを生成するまでに、モニタリングの試行に失敗する最大回数。

重要 ファブリック インターコネクトで管理インターフェイスに障害が発生した場合に次のいずれかが発生すると、管理インスタンスを変更できない可能性があります。

- 下位のファブリック インター コネクトを通るエンド ポイントへのパスが存在しない。
- 従属ファブリック インターコネクトの管理インターフェイスが失敗した。
- 従属ファブリック インターコネクトを通るエンドポイントへのパスが失敗した。

管理インターフェイスのモニタリング ポリシーの設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] を展開します。

ステップ 3 [Management Interfaces] をクリックします。

ステップ 4 [Work] ペインで、[Management Interfaces Monitoring Policy] タブをクリックします。

ステップ 5 次のフィールドに入力します。

名前	説明
[Admin Status] フィールド	管理インターフェイスに対して、モニタリング ポリシーをイネーブルまたはディセーブルにするかどうか。

名前	説明
[Poll Interval] フィールド	データ レコーディングの間に、Cisco UCS が待機する必要のある秒数。 90 ～ 300 の整数を入力します。
[Max Fail Report Count] フィールド	Cisco UCS が管理インターフェイスを使用できないと判断して、エラー メッセージを生成するまでに、モニタリングの試行が失敗する最大回数。 2 ～ 5 の整数を入力します。
[Monitoring Mechanism] フィールド	Cisco UCS で使用するモニタリングのタイプ。 次のいずれかになります。 • [Mii Status]：Cisco UCS は Media Independent Interface（MII）のアベイラビリティをモニタリングします。 このオプションを選択すると、Cisco UCS Manager GUI に [Media Independent Interface Monitoring] 領域が表示されます。 • [Ping Arp Targets]：Cisco UCS は Address Resolution Protocol（ARP）を使用して、指定されたターゲットを ping します。 このオプションを選択すると、Cisco UCS Manager GUI には [ARP Target Monitoring] 領域が表示されます。 • [Ping Gateway]：Cisco UCS は [Management Interfaces] タブでこの Cisco UCS ドメインに指定されたデフォルト ゲートウェイ アドレスを ping します。 このオプションを選択すると、Cisco UCS Manager GUI には [Gateway Ping Monitoring] 領域が表示されます。

ステップ 6 モニタリング メカニズムに [Mii Status] を選択する場合、[Media Independent Interface Monitoring] 領域 の次のフィールドに入力します。

名前	説明
[Retry Interval] フィールド	前の試行が失敗した場合に、MII から別の応答を要求するまで、Cisco UCS が待機する必要のある秒数。 3 ～ 10 の範囲の整数を入力します。
[Max Retry Count] フィールド	インターフェイスが使用不可であるとシステムが判断するまで、Cisco UCS が MII をポーリングする回数。 1 ～ 3 の整数を入力します。

ステップ 7 モニタリング メカニズムに [Ping Arp Targets] を選択する場合、[ARP Target Monitoring] 領域 の次のフィールドに入力します。

名前	説明
[Target IP 1] フィールド	Cisco UCS が ping する最初の IP アドレス。
[Target IP 2] フィールド	Cisco UCS が ping する 2 番目の IP アドレス。
[Target IP 3] フィールド	Cisco UCS が ping する 3 番目の IP アドレス。
[Number of ARP Requests] フィールド	Cisco UCS がターゲット IP アドレスに送信する ARP 要求数。 1 ～ 5 の整数を入力します。
[Max Deadline Timeout] フィールド	ARP ターゲットを使用できないとシステムが判断するまで、Cisco UCS が ARP ターゲットからの応答を待機する秒数。 5 ～ 15 の整数を入力します。

0.0.0.0 を入力して、ARP ターゲットを削除します。

ステップ 8 モニタリング メカニズムに [Ping Gateway] を選択する場合、[Gateway Ping Monitoring] 領域 の次のフィールドに入力します。

名前	説明
[Number of Ping Requests] フィールド	Cisco UCS がゲートウェイを ping する必要がある回数。 1 ～ 5 の整数を入力します。
[Max Deadline Timeout] フィールド	アドレスを使用できないと Cisco UCS が判断するまで、Cisco UCS がゲートウェイからの応答を待機する秒数。 5 ～ 15 の整数を入力します。

ステップ 9 [Save Changes] をクリックします。

サーバ ディスク ドライブ モニタリング

Cisco UCS のディスク ドライブ モニタリングにより、Cisco UCS ドメイン内のサポート対象ブレード サーバについて、ブレードに搭載されているディスク ドライブのステータスが Cisco UCS Manager に提供されます。ディスク ドライブ モニタリングは、LSI ファームウェアから Cisco UCS Manager への単方向の障害信号により、ステータス情報を提供します。

次のサーバ コンポーネントおよびファームウェア コンポーネントが、サーバ内のディスク ドライブ ステータスに関する情報の収集、送信、および集約を行います。

- 物理的なプレゼンス センサー：ディスク ドライブがサーバ ドライブ ベイに挿入されているかどうかを調べます。
- 物理的な障害センサー：ディスク ドライブの LSI ストレージ コントローラ ファームウェアからレポートされる操作可能性のステータスを調べます。
- IPMI ディスク ドライブの障害センサーおよびプレゼンス センサー：センサーの結果を Cisco UCS Manager に送信します。
- ディスク ドライブの障害 LED 制御および関連する IPMI センサー：ディスク ドライブの障害 LED の状態（オン/オフ）を制御し、それらの状態を Cisco UCS Manager に伝えます。

ディスク ドライブ モニタリングのサポート

ディスク ドライブ モニタリングは、一部のブレード サーバと特定の LSI ストレージ コントローラ ファームウェア レベルのみをサポートします。

サポートされている Cisco UCS サーバ

Cisco UCS Manager では、次のサーバのディスク ドライブをモニタできます。

- B-200 ブレード サーバ
- B-230 ブレード サーバ
- B-250 ブレード サーバ
- B-440 ブレード サーバ

Cisco UCS Manager は、他のブレード サーバまたはラックマウント サーバ内のディスク ドライブをモニタすることはできません。

ストレージ コントローラのファームウェア レベル

サポートされるサーバ上のストレージ コントローラには、LSI 1064E ファームウェアが組み込まれている必要があります。

Cisco UCS Manager は、異なるレベルのストレージ コントローラ ファームウェアが組み込まれたサーバ上のディスク ドライブをモニタすることはできません。

ディスク ドライブ モニタリングの前提条件

ディスク ドライブ モニタリングで有用なステータス情報を得るには、サーバとストレージ コントローラ ファームウェア バージョンがサポートされていることに加えて、次の前提条件が満たされていることを確認する必要があります。

- ドライブがサーバ ドライブ ベイに挿入されている必要があります。

- サーバの電源が投入されている。
- サーバが検出を完了している。
- BIOS POST の完了結果が正常である。

を使用したディスク ドライブのステータスの確認

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 アダプタのステータスを確認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 下矢印をクリックして [Disks] バーを展開し、各ディスク ドライブの [States] セクション内のフィールドを確認します。

名前	説明
[Operability] フィールド	ドライブの動作状態。 次のものがあります。 • [Operable]：ディスク ドライブは操作可能です。 • [Inoperable]：ディスク ドライブは操作不可能です。不良ブロックなどのハードウェアの問題が原因である可能性があります。 • [N/A]：ディスク ドライブの運用性を判断できません。 このことは、サーバまたはファームウェアでディスク ドライブ モニタリングがサポートされていないか、サーバの電源がオフになっていることによって発生する可能性があります。 （注） [Operability] フィールドには、ディスクが故障した RAID セットの一部である、BIOS POST（電源投入時自己診断テスト）が完了していない、などのいくつかの理由で、誤ったステータスが表示される場合があります。

名前	説明
[Presence] フィールド	ディスク ドライブのプレゼンス（サーバ ドライブ ベイ内で検出されるかどうかであり、動作状態は関係ない）。 次のものがあります。 • [Equipped]：サーバ ドライブ ベイ内でディスク ドライブを検出できます。 • [Missing]：サーバ ドライブ ベイ内でディスク ドライブを検出できません。

監視対象ディスク ドライブのステータスの解釈

Cisco UCS Manager では、モニタリング対象のディスク ドライブごとに次のプロパティが表示されます。

- [Operability]：ドライブの動作状態。
- [Presence]：ディスク ドライブのプレゼンス（サーバ ドライブ ベイ内で検出されるかどうかであり、動作状態は関係ない）。

監視対象のディスク ドライブのステータスを判断するには、両方のプロパティを確認する必要があります。 次の表に、これらのプロパティ値の一般的な解釈を示します。

[Operability] のステータス	**[Presence]** のステータス	解釈
Operable	Equipped	障害が発生していない状態。ディスク ドライブは、サーバ内に存在し、使用できます。
Inoperable	Equipped	障害が発生している状態。ディスク ドライブはサーバ内に存在していますが、次のいずれかが原因で操作可能性の問題が発生している可能性があります。 • 不良ブロックなどのハードウェアの問題が原因でディスク ドライブを使用できません。 • ストレージ コントローラへの IPMI リンクに問題が発生しています。

[Operability] のステータス	[Presence] のステータス	解釈
N/A	Missing	障害が発生している状態。サーバ ドライブ ベイにディスク ドライブが搭載されていません。
N/A	Equipped	障害が発生している状態。ディスク ドライブはサーバ内に存在していますが、次のいずれかが原因で操作可能性の問題が発生している可能性があります。 • サーバの電源がオフになっています。 • ストレージコントローラ ファームウェアは、バージョンが不適切なため、ディスク ドライブ モニタリングをサポートしていません。 • サーバでディスク ドライブ モニタリングがサポートされていません。

（注） [Operability] フィールドには、ディスクが故障した RAID セットの一部である、BIOS POST（電源投入時自己診断テスト）が完了していない、などのいくつかの理由で、誤ったステータスが表示される場合があります。

第 45 章

統計関連ポリシーの設定

この章の内容は、次のとおりです。

- 統計情報収集ポリシーの設定，805 ページ
- 統計情報しきい値ポリシーの設定，808 ページ

統計情報収集ポリシーの設定

統計情報収集ポリシー

統計情報収集ポリシーは、統計情報を収集する頻度（収集インターバル）、および統計情報を報告する頻度（報告インターバル）を定義します。 レポート インターバル中に複数の統計データポイントを収集できるように、レポート インターバルは収集インターバルよりも長くなります。これにより、最小値、最大値、平均値を計算して報告するために十分なデータが Cisco UCS Manager に提供されます。

NIC 統計情報の場合、Cisco UCS Manager は最後の統計情報収集以降の平均値、最小値、最大値の変化を表示します。 値が 0 の場合、最後の収集以降変化はありません。

統計情報は、Cisco UCS システムの次の 5 種類の機能エリアについて収集し、報告できます。

- アダプタ：アダプタ関連統計情報
- シャーシ：ブレード シャーシ関連統計情報
- ホスト：このポリシーは、将来サポートされる機能のためのプレースホルダです
- ポート：サーバ ポート、アップリンク イーサネット ポート、およびアップリンク ファイバ チャネル ポートを含むポートに関連した統計情報
- サーバ：サーバ関連統計情報

（注） Cisco UCS Manager には、5 つの機能エリアそれぞれについて、デフォルト統計情報収集ポリシーが 1 つずつあります。 追加で統計情報収集ポリシーを作成できません。また、既存のデフォルト ポリシーを削除できません。 デフォルト ポリシーを変更することだけが可能です。

統計情報収集ポリシーの変更

（注） Cisco UCS Manager には、5 つの機能エリアそれぞれについて、デフォルト統計情報収集ポリシーが 1 つずつあります。 追加で統計情報収集ポリシーを作成できません。また、既存のデフォルト ポリシーを削除できません。 デフォルト ポリシーを変更することだけが可能です。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Stats Management] > [Stats] を展開します。

ステップ 3 変更するポリシーを右クリックし、[Modify Collection Policy] を選択します。

ステップ 4 [Modify Collection Policy] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	収集ポリシーの名前。 この名前は、Cisco UCS によって割り当てられ、変更できません。
[Collection Interval] フィールド	データのレコーディングから次のレコーディングまでファブリック インターコネクトが待機する時間の長さ。 次のいずれかになります。 • 30 Seconds • 1 Minute • 2 Minutes • 5 Minutes

名前	説明
[Reporting Interval] フィールド	カウンタについて収集されたデータが Cisco UCS Manager に送信されるまでファブリック インターコネクトが待機する時間の長さ。 次のいずれかになります。 • 2 Minutes • 15 Minutes • 30 Minutes • 60 Minutes • 2 Hours • 4 Hours • 8 Hours この時間が経過すると、ファブリック インターコネクトによって、Cisco UCS Manager に最後に情報を送信してから収集されたすべてのデータがグループ化され、そのグループから次の 4 種類の情報が抽出されて Cisco UCS Manager に送信されます。 • 最後に収集された統計情報 • このグループの統計情報の平均値 • このグループ内の最大値 • このグループ内の最小値 たとえば、収集インターバルを 1 分に設定し、報告インターバルを 15 分に設定した場合、ファブリック インターコネクトによって 15 分の報告インターバルに 15 個のサンプルが収集されます。 Cisco UCS Manager に 15 個の統計情報が送信される代わりに、グループ全体の平均値、最小値、および最大値とともに最新のレコーディングのみが送信されます。
[States] セクション	
[Current Task] フィールド	このフィールドは、このコンポーネントの代わりに実行中のタスクを表示します。 詳細については、関連する [FSM] タブを参照してください。 （注） 現在のタスクが存在しない場合、このフィールドは表示されません。

ステップ 5 [OK] をクリックします。

統計情報しきい値ポリシーの設定

統計情報しきい値ポリシー

統計情報しきい値ポリシーは、システムの特定の側面についての統計情報をモニタし、しきい値を超えた場合にはイベントを生成します。最小値と最大値の両方のしきい値を設定できます。たとえば、CPU の温度が特定の値を超えた場合や、サーバを過度に使用していたり、サーバの使用に余裕がある場合には、アラームを発生するようにポリシーを設定できます。

これらのしきい値ポリシーが、CIMC などのエンドポイントに適用される、ハードウェアやデバイス レベルのしきい値を制御することはありません。 このしきい値は、製造時にハードウェアコンポーネントに焼き付けられます。

Cisco UCS を使用して、次のコンポーネントに対して統計情報のしきい値ポリシーを設定できます。

- サーバおよびサーバ コンポーネント
- アップリンク イーサネット ポート
- イーサネット サーバ ポート、シャーシ、およびファブリック インターコネクト
- ファイバ チャネル ポート

（注） イーサネット サーバ ポート、アップリンクのイーサネット ポート、またはアップリンクのファイバチャネルポートには、統計情報のしきい値ポリシーを作成したり、削除できません。既存のデフォルト ポリシーの設定だけを行うことができます。

サーバおよびサーバ コンポーネントのしきい値ポリシーの作成

ヒント この手順では、[Server] タブでサーバおよびサーバ コンポーネントのしきい値ポリシーを作成する方法について説明します。 これらのしきい値は、[LAN] タブ、[SAN] タブの [Policies] ノードの適切な組織内、および [Admin] タブの [Stats Management] ノードでも作成し、設定できます。

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] 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 [Threshold Policies] を右クリックし、[Create Threshold Policy] を選択します。

ステップ 5 [Create Threshold Policy] ウィザードの [Define Name and Description] 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
[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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Description] フィールド	ポリシーの説明。ポリシーが使用される場所と条件についての情報を含めることを推奨します。 256 文字以下で入力します。`（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）を除く文字やスペースを使用できます。

b) [Next] をクリックします。

ステップ 6 [Create Threshold Policy] ウィザードの [Threshold Classes] ページで、次の手順を実行します。

a) [Add] をクリックします。

b) [Choose Statistics Class] ダイアログ ボックスで、カスタムしきい値を設定する統計情報クラスを [Stat Class] ドロップダウン リストから選択します。

c) [Next] をクリックします。

ステップ 7 [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

d) [Alarm Triggers (Above Normal Value)] フィールド で、次のチェックボックスの 1 つ以上をオンにします。

- Critical
- Major
- Minor
- Warning
- Condition

- Info

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
f) [Alarm Triggers (Below Normal Value)] フィールド で、次のチェックボックスの 1 つ以上をオンにします。
   - Info
   - Condition
   - Warning
   - Minor
   - Major
   - Critical
g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。
   - クラスに別のしきい値のプロパティを定義するには、ステップ 7 を繰り返します。
   - クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

ステップ 8 [Create Threshold Policy] ウィザードの [Threshold Classes] ページで、次の手順を実行します。
- ポリシーの別のしきい値クラスを設定するには、ステップ 6 および 7 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

ステップ 9 [OK] をクリックします。

既存サーバおよびサーバコンポーネントしきい値ポリシーへのしきい値クラスの追加

ヒント この手順では、[Server] タブでサーバおよびサーバ コンポーネントのしきい値ポリシーにしきい値クラスを追加する方法を示します。 これらのしきい値は、[LAN] タブ、[SAN] タブの [Policies] ノードの適切な組織内、および [Admin] タブの [Stats Management] ノードでも作成し、設定できます。

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。

ステップ 3 [Threshold Policies] ノードを展開します。

ステップ 4 しきい値クラスを追加するポリシーを右クリックして、[Create Threshold Class] を選択します。

ステップ 5 [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。

b) [Next] をクリックします。

ステップ 6 [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- Critical
- Major
- Minor
- Warning
- Condition
- Info

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- Info
- Condition
- Warning
- Minor
- Major
- Critical

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

h) [Finish Stage] をクリックします。

i) 次のいずれかを実行します。

- クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
- クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

ステップ 7 [Create Threshold Class] ウィザードの[Choose Statistics Class] ページで、次の手順を実行します。

- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

ステップ 8 [OK] をクリックします。

サーバおよびサーバ コンポーネントのしきい値ポリシーの削除

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。

ステップ 3 [Threshold 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 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

アップリンク イーサネット ポートしきい値ポリシーへのしきい値クラスの追加

ヒント アップリンク イーサネット ポートしきい値ポリシーは作成できません。 デフォルト ポリシーを修正または削除するだけです。

手順

ステップ 1 [Navigation] ペインの [LAN] タブをクリックします。

ステップ 2 [LAN] タブで、[LAN] > [LAN Cloud] を展開します。

ステップ 3 [Threshold Policies] ノードを展開します。

ステップ 4 [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。

ステップ 5 [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。

b) [Next] をクリックします。

ステップ 6 [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- Critical
- Major
- Minor
- Warning
- Condition
- Info

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- Info
- Condition
- Warning
- Minor
- Major
- Critical

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

h) [Finish Stage] をクリックします。

i) 次のいずれかを実行します。

- クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
- クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

ステップ 7 [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。

- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

イーサネット サービス ポート、シャーシ、およびファブリック インターコネクトのしきい値ポリシーへのしきい値クラスの追加

ヒント　イーサネット サーバ ポート、シャーシ、およびファブリック インターコネクトのしきい値ポリシーは作成できません。 デフォルト ポリシーを修正または削除するだけです。

手順

ステップ 1　[Navigation] ペインの [LAN] タブをクリックします。

ステップ 2　[LAN] タブで、[LAN] > [Internal LAN] を展開します。

ステップ 3　[Threshold Policies] ノードを展開します。

ステップ 4　[Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。

ステップ 5　[Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。

b) [Next] をクリックします。

ステップ 6　[Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。
[Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。

c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。

d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- Critical
- Major
- Minor
- Warning
- Condition
- Info

e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。

f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。

- Info

- Condition
- Warning
- Minor
- Major
- Critical

g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。
   - クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
   - クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

ステップ 7 [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。

- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

ファイバ チャネル ポートしきい値ポリシーへのしきい値クラスの追加

ファイバ チャネル ポートしきい値ポリシーは作成できません。 デフォルト ポリシーを修正または削除するだけです。

手順

ステップ 1 [Navigation] ペインの [SAN] タブをクリックします。

ステップ 2 [SAN] タブで、[SAN] > [SAN Cloud] を展開します。

ステップ 3 [Threshold Policies] ノードを展開します。

ステップ 4 [Thr-policy-default] を右クリックして、[Create Threshold Class] を選択します。

ステップ 5 [Create Threshold Class] ウィザードの [Choose Statistics Class] ページで、次の手順を実行します。

a) [Stat Class] ドロップダウン リストから、カスタムしきい値を設定する統計情報クラスを選択します。
b) [Next] をクリックします。

ステップ 6 [Threshold Definitions] ページで、次の手順を実行します。

a) [Add] をクリックします。
   [Create Threshold Definition] ダイアログボックスが開きます。

b) [Property Type] フィールドから、クラスに定義するしきい値のプロパティを選択します。
c) [Normal Value] フィールドに、そのプロパティ タイプに対して必要な値を入力します。
d) [Alarm Triggers (Above Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - Critical
   - Major
   - Minor
   - Warning
   - Condition
   - Info
e) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
f) [Alarm Triggers (Below Normal Value)] フィールドで、次のチェックボックスの 1 つまたは複数をオンにします。
   - Info
   - Condition
   - Warning
   - Minor
   - Major
   - Critical
g) [Up] フィールドおよび [Down] フィールドに、アラームを発行する値の範囲を入力します。
h) [Finish Stage] をクリックします。
i) 次のいずれかを実行します。
   - クラスに別のしきい値プロパティを定義するには、ステップ 6 を繰り返します。
   - クラスに必要なすべてのプロパティを定義したら、[Finish Stage] をクリックします。

ステップ 7 [Create Threshold Policy] ウィザードの [Create Threshold Class] ページで、次のいずれかの手順を実行します。

- ポリシーに別のしきい値クラスを設定するには、ステップ 5 および 6 を繰り返します。
- ポリシーに必要なすべてのしきい値クラスを設定したら、[Finish] をクリックします。

第 46 章

Call Home の設定

この章の内容は、次のとおりです。

- Call Home，817 ページ
- Call Home の考慮事項とガイドライン，819 ページ
- Cisco UCS 障害と Call Home の重大度，820 ページ
- Cisco Smart Call Home，821 ページ
- Call Home の設定，822 ページ
- Call Home のディセーブル化，826 ページ
- Call Home のイネーブル化，826 ページ
- システム インベントリ メッセージの設定，827 ページ
- Call Home プロファイルの設定，828 ページ
- Call Home ポリシーの設定，833 ページ
- 例：Smart Call Home の Call Home の設定，835 ページ

Call Home

Call Home では、重要なシステム ポリシーに対して電子メールベースの通知が提供されます。 ポケットベル サービスや XML ベースの自動化された解析アプリケーションとの互換性のために、さまざまなメッセージ フォーマットが用意されています。 この機能を使用して、ネットワーク サポート エンジニアにポケットベルで連絡したり、ネットワーク オペレーション センターに電子メールを送信したりできます。また、Cisco Smart Call Home サービスを使用して TAC のケースを生成できます。

Call Home 機能では、診断情報および環境の障害とイベントに関する情報が含まれるアラート メッセージを配信できます。

Call Home 機能では、複数の受信者（Call Home 宛先プロファイルと呼びます）にアラートを配信できます。 各プロファイルには、設定可能なメッセージ フォーマットとコンテンツ カテゴリが含まれます。 Cisco TAC へアラートを送信するための宛先プロファイルが事前に定義されていますが、独自の宛先プロファイルを定義することもできます。

メッセージを送信するように Call Home を設定すると、Cisco UCS Manager は CLI の適切な **show** コマンドを実行し、そのコマンドの出力をメッセージに添付します。

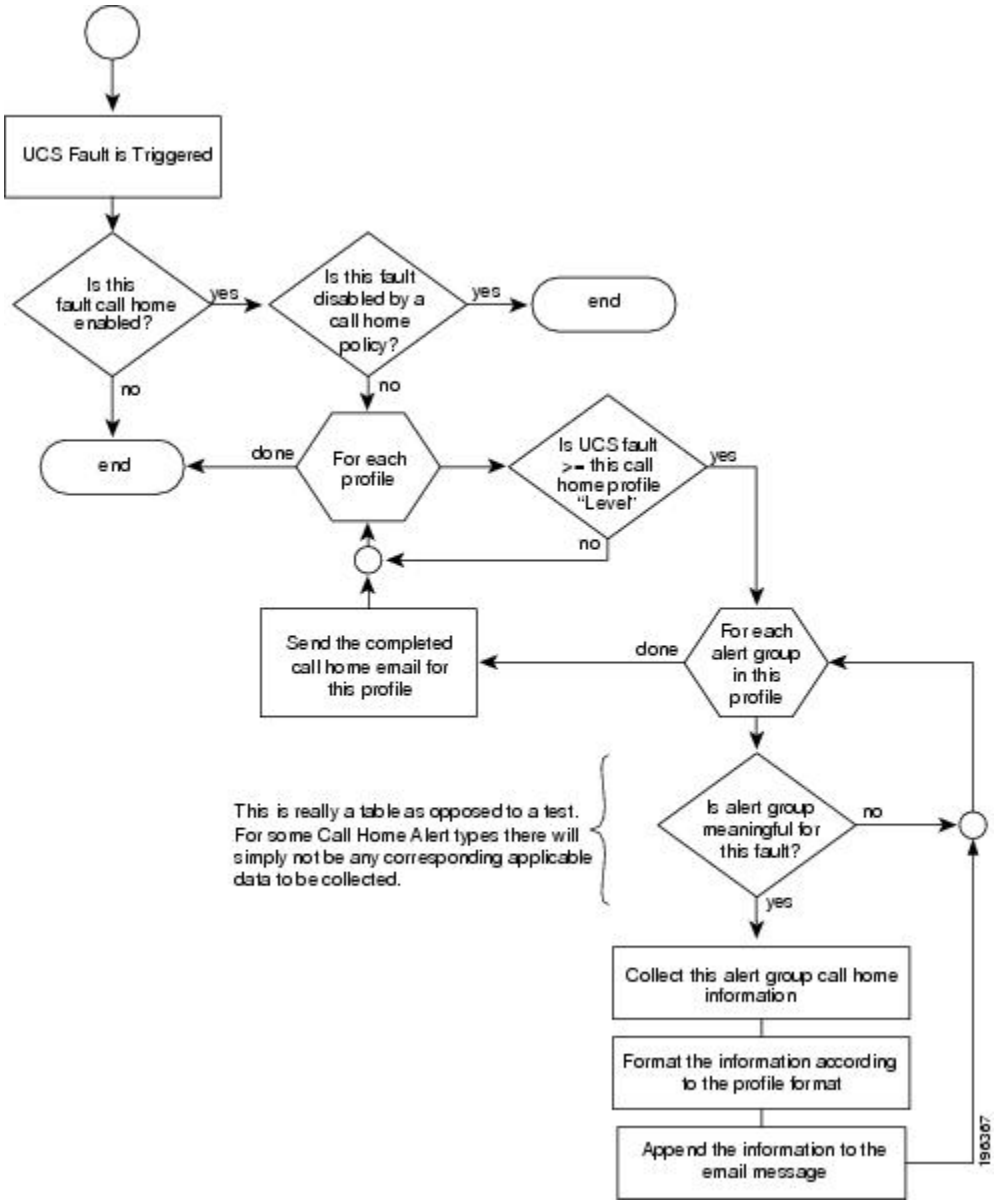
Cisco UCS では、Call Home メッセージが次のフォーマットで配信されます。

- 1 または 2 行で障害を説明する、ポケットベルや印刷レポートに適したショート テキスト フォーマット
- 詳細な情報を十分に書式が整えられたメッセージで提供する、ユーザが読むのに適したフル テキスト フォーマット
- Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML schema definition（XSD）を使用する、コンピュータで読み取り可能な XML フォーマット。 AML XSD は、Cisco.com Web サイトで公開されています。 XML フォーマットでは、シスコの Technical Assistance Center との通信が可能になります。

Call Home 電子メール アラートが送信される可能性のある障害についての情報は、『*Cisco UCS Faults and Error Messages Reference*』を参照してください。

次の図は、Call Home が設定されたシステムで Cisco UCS 障害が発生した後のイベントの流れを示しています。

図 *2* : 障害発生後のイベントの流れ



Call Home の考慮事項とガイドライン

Call Home の設定方法は、機能の使用目的によって異なります。 Call Home を設定する前に考慮すべき情報には次のものがあります。

宛先プロファイル

少なくとも 1 つの宛先プロファイルを設定する必要があります。 使用する 1 つまたは複数の宛先プロファイルは、受信エンティティがポケットベル、電子メール、または自動化されたサービス（Cisco Smart Call Home など）のいずれであるかによって異なります。

宛先プロファイルで電子メール メッセージ配信を使用する場合は、Call Home を設定するときに Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）サーバを指定する必要があります。

連絡先情報

受信者が Cisco UCS ドメインから受信したメッセージの発信元を判別できるように、連絡先の電子メール、電話番号、および所在地住所の情報を設定する必要があります。

Cisco Smart Call Home は、システム インベントリを送信して登録プロセスを開始した後に、この電子メール アドレスに登録の電子メールを送信します。

電子メール アドレスに #（ハッシュ）、スペース、または &（アンパサンド）などの特殊文字が含まれていると、電子メールサーバは電子メールメッセージをそのアドレスに配信できない場合があります。 シスコでは、RFC2821 および RFC-2822 に従い、7bit ASCII 文字のみを含む電子メール アドレスを使用することを推奨します。

電子メール サーバまたは HTTP サーバへの IP 接続

ファブリック インターコネクトに、電子メール サーバまたは宛先 HTTP サーバへの IP 接続を与える必要があります。 クラスタ設定の場合は、両方のファブリック インターコネクトに IP 接続を与える必要があります。 この接続により、現在のアクティブなファブリック インターコネクトで Call Home 電子メール メッセージを送信できることが保証されます。 これらの電子メール メッセージの発信元は、常にファブリック インターコネクトの IP アドレスになります。 クラスタ設定で Cisco UCS Manager によって割り当てられた仮想 IP アドレスが、電子メールの発信元になることはありません。

Smart Call Home

Cisco Smart Call Home を使用する場合は、次のことが必要です。

- 設定するデバイスが、有効なサービス契約でカバーされている必要があります。
- Cisco UCS 内で Smart Call Home 設定と関連付けられるカスタマー ID は、Smart Call Home が含まれるサポート契約と関連付けられている CCO（Cisco.com）アカウント名にする必要があります。

Cisco UCS 障害と Call Home の重大度

Call Home は複数の Cisco 製品ラインにまたがって存在するため、独自に標準化された重大度が開発されています。 次の表に、基礎をなす Cisco UCS の障害レベルと、Call Home 重大度のマッピングを示します。 Call Home のプロファイルにレベルを設定するときには、このマッピングを理解しておくことが必要です。

表 *11*：障害と *Call Home* の重大度のマッピング

Call Home の重大度	Cisco UCS 障害	Call Home での意味
(9) Catastrophic	N/A	ネットワーク全体に壊滅的な障害が発生しています。
(8) Disaster	N/A	ネットワークへの重大な影響。
(7) Fatal	N/A	システムを使用できません。
(6) Critical	Critical	クリティカルな状態、ただちに注意が必要。
(5) Major	Major	重大な状態。
(4) Minor	Minor	軽微な状態。
(3) Warning	Warning	警告状態です。
(2) Notification	Info	基本的な通知と情報メッセージ。 他と関係しない、重要性の低い障害。
(1) Normal	Clear	通常のイベント。通常の状態に戻ることを意味します。
(0) debug	N/A	デバッグ メッセージです。

Cisco Smart Call Home

Cisco Smart Call Home は、Cisco UCS の Call Home 機能を使用する Web アプリケーションです。Smart Call Home により、予防的な診断および重要なシステム イベントのリアルタイムの電子メール アラートが提供されます。それにより、ネットワークの可用性が高まり、運用効率が向上します。 Smart Call Home は、Cisco UCS の Cisco Unified Computing Support Service と Cisco Unified Computing Mission Critical Support Service によって提供されるセキュア接続のサービスです。

（注） Smart Call Home を使用するには、次のものが必要です。

- 対応する Cisco Unified Computing Support Service 契約または Cisco Unified Computing Mission Critical Support Service 契約と関連付けられた CCO ID
- 登録されるデバイス用の Cisco Unified Computing Support Service または Cisco Unified Computing Mission Critical Support Service

Smart Call Home 電子メール アラートを Smart Call Home System またはセキュアな Transport Gateway のいずれかに送信するように、Cisco UCS Manager を設定し、登録できます。 セキュアな Transport Gateway に送信された電子メール アラートは、HTTPS を使用して Smart Call Home System に転送されます。

（注） セキュリティ上の理由から、Transport Gateway オプションの使用を推奨します。 Transport Gateway は、シスコからダウンロードできます。

Smart Call Home を設定するには、次の手順を実行する必要があります。

- Smart Call Home 機能をイネーブルにします。
- 連絡先情報を設定します。
- 電子メール情報を設定します。
- SMTP サーバ情報を設定します。
- デフォルトの CiscoTAC-1 プロファイルを設定します。
- Smart Call Home インベントリ メッセージを送信して、登録プロセスを開始します。
- Cisco UCS ドメインの Call Home Customer ID として使用する予定の CCO ID に、その資格として登録の契約番号が追加されていることを確認します。 この ID は、CCO の Profile Manager の Additional Access の下にあるアカウント プロパティ内で更新できます。

Call Home の設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] 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 [Admin] 領域で次のフィールドに入力し、[Call Home] をイネーブルにします。

名前	説明
[State] フィールド	次のいずれかになります。 • [Off]：この Cisco UCS ドメインでは Call Home は使用されません。 • [On]：Cisco UCS では、システムで定義されている Call Home ポリシーおよびプロファイルに基づいて Call Home アラートが生成されます。 （注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。
[Switch Priority] ドロップダウンリスト	次のいずれかになります。 • Alerts • Critical • Debugging • Emergencies • Errors • Information • Notifications • Warnings
[Throttling] フィールド	同じイベントについて受信する重複メッセージの数を制限するかどうかを指定します。 次のいずれかになります。 • [On]：送信される重複メッセージの数が 2 時間以内に 30 件を超えると、そのアラート タイプに関するそれ以降のメッセージは破棄されます。 • [Off]：検出された数に関係なく、すべての重複メッセージが送信されます。

a) [State] フィールドで、[on] をクリックします。

（注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。

b) [Switch Priority] ドロップダウン リストから、次のいずれかのレベルを選択します。

- Alerts
- Critical

- Debugging
- Emergencies
- Errors
- Information
- Notifications
- Warnings

ファブリック インターコネクトの複数のペアがある大規模な Cisco UCS の展開の場合は、メッセージの受信者がメッセージの優先度を判断できるように、このフィールドを使用して特定の 1 つの Cisco UCS ドメインからのメッセージに重大度を割り当てることができます。 このフィールドは、小規模な Cisco UCS の展開（単一の Cisco UCS ドメインなど）には有用でないことがあります。

ステップ 5 [Contact Information] 領域で、次のフィールドに必要な連絡先情報を入力します。

名前	説明
[Contact] フィールド	主要 Call Home 連絡先。 255 文字以下の ASCII 文字で入力します。
[Phone] フィールド	主要連絡先の電話番号。 +（プラス記号）と国番号から始まる国際形式の番号を入力します。 ハイフンは使用できますが、カッコは使用できません。
[Email] フィールド	主要連絡先の電子メール アドレス。 Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。 （注） 電子メールアドレスに#（ハッシュ）、スペース、または&（アンパサンド）などの特殊文字が含まれていると、電子メール サーバは電子メール メッセージをそのアドレスに配信できない場合があります。 シスコでは、RFC2821 および RFC-2822 に従い、7bit ASCII 文字のみを含む電子メール アドレスを使用することを推奨します。
[Address] フィールド	主要連絡先の住所。 255 文字以下の ASCII 文字で入力します。

ステップ 6 [Ids] 領域で、Call Home が使用する ID 情報を次のフィールドに入力します。

ヒント Smart Call Home を設定しない場合は、この手順を省略できます。

名前	説明
[Customer Id] フィールド	ライセンス上のサポート契約の契約番号を含む Cisco Connection Online（CCO）ID。 510 文字以下の ASCII 文字で入力します。
[Contract Id] フィールド	お客様の Call Home 契約番号。 510 文字以下の ASCII 文字で入力します。
[Site Id] フィールド	お客様のサイトに固有の Call Home ID。 510 文字以下の ASCII 文字で入力します。

ステップ 7 [Email Addresses] 領域で、Call Home アラート メッセージの電子メール情報を次のフィールドに入力します。

名前	説明
[From] フィールド	システムによって送信される Call Home アラート メッセージの [From] フィールドに表示される電子メール アドレス。
[Reply To] フィールド	システムによって送信される Call Home アラート メッセージの [From] フィールドに表示される返信電子メール アドレス。

ステップ 8 [SMTP Server] 領域で、Call Home が電子メール メッセージを送信する SMTP サーバに関する情報を次のフィールドに入力します。

名前	説明
[Host] フィールド	Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）サーバの IP アドレスまたはホスト名。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Port] フィールド	SMTP サーバとの通信に使用されるポート番号。 1 ～ 65535 の整数を入力します。 デフォルトは 25 です。

ステップ 9 [Save Changes] をクリックします。

Call Home のディセーブル化

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] 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 [Admin] 領域の [State] フィールドで、[off] をクリックします。

（注） このフィールドが [off] に設定されている場合、Cisco UCS Manager ではこのタブの残りのフィールドが表示されません。

ステップ 5 [Save Changes] をクリックします。

Call Home のイネーブル化

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] 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 [Admin] 領域の [State] フィールドで、[on] をクリックします。

（注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。

ステップ 5 [Save Changes] をクリックします。

次の作業

Call Home が完全に設定されていることを確認します。

システム インベントリ メッセージの設定

システム インベントリ メッセージの設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

ステップ 3 [Work] ペインで [System Inventory] タブをクリックします。

ステップ 4 [Properties] 領域で、次のフィールドに値を入力します。

名前	説明
[Send Periodically] フィールド	このフィールドを [ON] に設定すると、Cisco UCS によってシステム インベントリが Call Home データベースに送信されます。この情報がいつ送信されるかは、この領域の他のフィールドによって決まります。
[Send Interval] フィールド	自動システム インベントリ データ収集の間隔（日数）。 1 ～ 30 の整数を入力します。
[Hour of Day to Send] フィールド	データを送信する時間（24 時間時計形式）。
[Minute of Hour] フィールド	データを送信する時間（分数）。
[Time Last Sent] フィールド	情報が最後に送信された日時。 （注） このフィールドは、最初のインベントリが送信された後に表示されます。
[Next Scheduled] フィールド	次のデータ収集の日時。 （注） このフィールドは、最初のインベントリが送信された後に表示されます。

ステップ 5 [Save Changes] をクリックします。

システム インベントリ メッセージの送信

スケジュール済みメッセージ以外のシステムインベントリ メッセージを手動で送信する必要がある場合は、この手順を使用します。

（注） システム インベントリ メッセージは、CiscoTAC-1 プロファイルで定義された受信者だけに送信されます。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

ステップ 3 [Work] ペインで [System Inventory] タブをクリックします。

ステップ 4 [Actions] 領域で [Send System Inventory Now] をクリックします。
Cisco UCS Manager は、ただちに Call Home に設定された受信者にシステム インベントリ メッセージを送信します。

Call Home プロファイルの設定

Call Home プロファイル

Call Home プロファイルは、指定した受信者にどのアラートが送信されるかを決定します。 任意の重大度のイベントおよび障害と、アラートのカテゴリを表す特定のアラート グループの電子メールアラートを送信するためのプロフィルを設定できます。 また、これらのプロファイルを使用して特定の受信者およびアラート グループのセットに対してアラートの形式を指定することもできます。

アラート グループと Call Home プロファイルを使用してアラートをフィルタリングし、特定のプロファイルがアラートの特定のカテゴリのみを受信するように設定できます。 たとえば、データセンターに、ファンおよび電源の問題を処理するハードウェアのチームがある場合があります。 このハードウェアのチームはサーバの POST 障害またはライセンスの問題を考慮しません。 ハードウェア チームが関連するアラートのみを受信するようにするには、ハードウェアのチーム用に Call Home プロファイルを作成し、「Environmental」アラート グループのみをオンにします。

デフォルトでは、Cisco TAC-1 プロファイルを設定する必要があります。 しかし、プロファイルを追加作成することにより、指定したレベルでイベントが発生したときに、指定された 1 つ以上のグループにアラート メールを送信し、それらのアラートに関する適切な量の情報を受信者に提供できます。

たとえば、高い重大度の障害に対して次の 2 つのプロファイルを設定できます。

- アラート グループにアラートを送信する短いテキスト形式のプロファイル。 このグループのメンバは、障害に関する 1 ～ 2 行の説明を受け取ります（この説明を使用して問題を追跡できます）。
- CiscoTAC アラート グループにアラートを送信する XML 形式のプロファイル。 このグループのメンバは、マシンが読み取り可能な形式で詳細なメッセージを受け取ります（Cisco Systems Technical Assistance Center 推奨）。

Call Home アラート グループ

アラート グループは、事前定義された Call Home アラートのサブセットです。 アラート グループ機能を使用すると、定義済みまたはカスタム Call Home プロファイルに送信する一連の Call Home アラートを選択できます。 Call Home アラートが宛先プロファイルにアソシエートされたいずれかのアラート グループに属する場合、およびアラートで、Call Home メッセージ重大度が宛先プロファイルに設定されているメッセージ重大度と同じか、それ以上である場合のみ、Cisco UCS は Call Home アラートを宛先プロファイルの電子メールの宛先に送信します。

Cisco UCS が生成する各アラートは、アラート グループによって表される何らかのカテゴリに適合します。 次の表には、これらのアラート グループが説明されています。

アラート グループ	説明
Cisco TAC	Smart Call Home 宛ての、他のアラート グループからのすべてのクリティカル アラート。
Diagnostic	サーバでの POST の完了など、診断によって生成されるイベント。
Environmental	電源、ファン、および温度アラームなどの環境検知要素に関連するイベント。
Inventory	ユニットがコールドブートされるか、現場交換可能ユニット（FRU）が挿入または除去されるときに必ず提供される在庫ステータスに関連するイベント。 このアラートは重要でないイベントであり、情報はステータスおよび使用権に使用されます。
License	イベントは、Cisco UCS ライセンスに関連します。
Life Cycle	イベントは、Cisco UCS ドメインの設定のライフサイクルに関連します。
Linecard	標準またはインテリジェント スイッチング モジュールに関連するイベント
Supervisor	スーパーバイザ モジュールに関連するイベント
Syslog port	syslog に関連するイベント。

アラート グループ	説明
System	Cisco UCS に必要なソフトウェア システムの障害によって生成されたイベント。
Test	テスト メッセージ。

Call Home プロファイルの作成

デフォルトでは、Cisco TAC-1 プロファイルを設定する必要があります。 しかし、プロファイルを追加作成することにより、指定したレベルでイベントが発生したときに、指定された 1 つ以上のグループにアラート メールを送信することもできます。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

ステップ 3 [Work] ペインで、[Profiles] タブをクリックします。

ステップ 4 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create Call Home Profile] ダイアログボックスで、次の情報フィールドに値を入力します。

名前	説明
[Name] フィールド	このプロファイルのユーザ定義名。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

名前	説明
[Level] フィールド	Cisco UCS の障害がこのレベル以上の場合は、プロファイルがトリガーされます。 次のいずれかになります。 • Critical • Debug • Disaster • Fatal • Major • Minor • Normal • Notification • Warning
[Alert Groups] フィールド	この Call Home プロファイルに基づいて警告されるグループ。これは次のいずれか、または複数の値になります。 • Cisco Tac • Diagnostic • Environmental • Inventory • License • Life Cycle • Linecard • Supervisor • Syslog Port • System • Test

ステップ 6 [Email Configuration] 領域で、次のフィールドに値を入力して電子メール アラートを設定します。

名前	説明
[Format] フィールド	次のいずれかになります。 • [Xml]：Extensible Markup Language（XML）と Adaptive Messaging Language（AML）XML Schema Definition（XSD）を使用するマシンが読み取り可能な形式。 この形式により、Cisco Systems Technical Assistance Center との通信が可能になります。 • [Full Txt]：人間が判読するのに適している完全にフォーマットされたメッセージ（詳細な情報付き）。 • [Short Txt]：ポケットベルまたは印刷されたレポートに適している 1 ～ 2 行の障害の説明。
[Max Message Size] フィールド	指定された Call Home 受信者に送信される最大メッセージ サイズ。 1 ～ 5000000 の整数を入力します。 デフォルトは 5000000 です。 フルテキスト メッセージおよび xml メッセージの推奨最大サイズは 5000000 です。 ショートテキスト メッセージの推奨最大サイズは 100000 です。 Cisco TAC アラート グループの場合、最大メッセージ サイズは 5000000 である必要があります。

ステップ 7 [Recipients] 領域で次の手順を実行して電子メール アラートの 1 つ以上の電子メール受信者を追加します。

a) テーブルの右側のアイコン バーの [+] をクリックします。

b) [Add Email Recipients] ダイアログボックスで、[Email] フィールドでの Call Home アラートの送信先となる電子メール アドレスを入力します。
保存した電子メール アドレスは削除できますが、変更はできません。

c) [OK] をクリックします。

ステップ 8 [OK] をクリックします。

Call Home プロファイルの削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

ステップ 3 [Work] ペインで、[Profiles] タブをクリックします。

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 [Save Changes] をクリックします。

Call Home ポリシーの設定

Call Home ポリシー

Call Home ポリシーは、特定の種類の障害またはシステム イベントに対して Call Home アラートを送信するかどうかを決定します。デフォルトでは、特定の種類の障害およびシステムイベントに対してアラートを送信するよう Call Home がイネーブルになります。 ただし、Cisco UCS が特定の種類を処理しないよう設定できます。

ある種類の障害またはイベントに対してアラートをディセーブルするには、その種類に対して Call Home ポリシーを作成する必要があります。まず最初にその種類に対してポリシーを作成し、次にポリシーをディセーブルにします。

Call Home ポリシーの設定

ヒント デフォルトでは、すべての Call Home ポリシーがイネーブルになっており、重要なシステム イベントすべてについてアラートが電子メールで送信されます。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

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 テーブルの右側のアイコン バーの [+] をクリックします。
[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

ステップ 5 [Create Call Home 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
[State] フィールド	このフィールドが [Enabled] の場合、関連付けられた原因と一致するエラーが発生した際にシステムはこのポリシーを使用します。それ以外の場合、一致するエラーが発生しても、システムはこのポリシーを無視します。デフォルトでは、すべてのポリシーがイネーブルになります。
[Cause] フィールド	このアラートをトリガーするイベント。各ポリシーは、アラートがいずれかのタイプのイベントに送信されるかどうかを定義します。

ステップ 6 [OK] をクリックします。

ステップ 7 異なる種類の障害またはイベントに Call Home ポリシーを設定する場合は、ステップ 6 および 7 を繰り返します。

Call Home ポリシーのディセーブル化

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

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 ディセーブルにするポリシーを右クリックし、[Show Navigator] を選択します。

ステップ 5 [State] フィールドで、[Disabled] をクリックします。

ステップ 6 [OK] をクリックします。

Call Home ポリシーのイネーブル化

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。
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 イネーブルにするポリシーを右クリックし、[Show Navigator] を選択します。
ステップ 5 [State] フィールドで、[Enabled] をクリックします。
ステップ 6 [OK] をクリックします。

Call Home ポリシーの削除

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。
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 ディセーブルに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 [Save Changes] をクリックします。

例：Smart Call Home の Call Home の設定

Smart Call Home の設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] 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 [Admin] 領域で次の作業を行い、Call Home をイネーブルにします。
a) [State] フィールドで、[on] をクリックします。

（注） Cisco UCS Manager GUI では、このフィールドを [On] に設定すると、このタブに残りのフィールドが表示されます。

b) [Switch Priority] ドロップダウン リストから、次の緊急度レベルのいずれかを選択します。

- Alerts
- Critical
- Debugging
- Emergencies
- Errors
- Information
- Notifications
- Warnings

ステップ 5 [Contact Information] 領域で、次のフィールドに必要な連絡先情報を入力します。

名前	説明
[Contact] フィールド	主要 Call Home 連絡先。 255 文字以下の ASCII 文字で入力します。
[Phone] フィールド	主要連絡先の電話番号。 +（プラス記号）と国番号から始まる国際形式の番号を入力します。 ハイフンは使用できますが、カッコは使用できません。
[Email] フィールド	主要連絡先の電子メール アドレス。 Cisco Smart Call Home によってこの電子メール アドレスに登録メールが送信されます。 （注） 電子メールアドレスに#（ハッシュ）、スペース、または&（アンパサンド）などの特殊文字が含まれていると、電子メール サーバは電子メール メッセージをそのアドレスに配信できない場合があります。 シスコでは、RFC2821 および RFC-2822 に従い、7bit ASCII 文字のみを含む電子メール アドレスを使用することを推奨します。
[Address] フィールド	主要連絡先の住所。 255 文字以下の ASCII 文字で入力します。

ステップ 6 [Ids] 領域で、次のフィールドに Smart Call Home ID 情報を入力します。

名前	説明
[Customer Id] フィールド	ライセンス上のサポート契約の契約番号を含む Cisco Connection Online（CCO）ID。 510 文字以下の ASCII 文字で入力します。
[Contract Id] フィールド	お客様の Call Home 契約番号。 510 文字以下の ASCII 文字で入力します。
[Site Id] フィールド	お客様のサイトに固有の Call Home ID。 510 文字以下の ASCII 文字で入力します。

ステップ 7 [Email Addresses] 領域で、次のフィールドに Smart Call Home アラート メッセージの電子メール情報を入力します。

名前	説明
[From] フィールド	システムによって送信される Call Home アラート メッセージの [From] フィールドに表示される電子メール アドレス。
[Reply To] フィールド	システムによって送信される Call Home アラート メッセージの [From] フィールドに表示される返信電子メール アドレス。

ステップ 8 [SMTP Server] 領域で、次のフィールドに Call Home が電子メール メッセージを送信するために使用する SMTP サーバに関する情報を入力します。

名前	説明
[Host] フィールド	Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）サーバの IP アドレスまたはホスト名。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Port] フィールド	SMTP サーバとの通信に使用されるポート番号。 1 ～ 65535 の整数を入力します。 デフォルトは 25 です。

ステップ 9 [Save Changes] をクリックします。

デフォルトの Cisco TAC-1 プロファイルの設定

CiscoTAC-1 プロファイルのデフォルト設定は次のとおりです。

- レベルは標準です
- CiscoTAC 警報グループだけが選択されています
- 形式は xml です
- 最大メッセージ サイズは 5000000 です

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

ステップ 3 [Work] ペインで、[Profiles] タブをクリックします。

ステップ 4 Cisco TAC-1 プロファイルを右クリックし、[Recipient] を選択します。

ステップ 5 [Add Email Recipients] ダイアログボックスで、次の手順を実行します。

a) [Email] フィールドで、Call Home アラートの送信先の電子メール アドレスを入力します。たとえば、「callhome@cisco.com」と入力します。

保存した電子メール アドレスは削除できますが、変更はできません。

b) [OK] をクリックします。

Smart Call Home に対するシステム インベントリ メッセージの設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

ステップ 3 [Work] ペインで [System Inventory] タブをクリックします。

ステップ 4 [Properties] 領域で、次のフィールドに値を入力して、システム インベントリ メッセージを Smart Call Home に送信する方法を指定します。

名前	説明
[Send Periodically] フィールド	このフィールドを [ON] に設定すると、Cisco UCS によってシステム インベントリが Call Home データベースに送信されます。この情報がいつ送信されるかは、この領域の他のフィールドによって決まります。
[Send Interval] フィールド	自動システム インベントリ データ収集の間隔（日数）。 1 ～ 30 の整数を入力します。
[Hour of Day to Send] フィールド	データを送信する時間（24 時間時計形式）。
[Minute of Hour] フィールド	データを送信する時間（分数）。
[Time Last Sent] フィールド	情報が最後に送信された日時。 （注） このフィールドは、最初のインベントリが送信された後に表示されます。
[Next Scheduled] フィールド	次のデータ収集の日時。 （注） このフィールドは、最初のインベントリが送信された後に表示されます。

ステップ 5 [Save Changes] をクリックします。

Smart Call Home の登録

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Communication Management] > [Call Home] を展開します。

ステップ 3 [Work] ペインで [System Inventory] タブをクリックします。

ステップ 4 [Actions] 領域で [Send System Inventory Now] をクリックし、登録プロセスを開始します。
シスコがシステム インベントリを受信すると、Smart Call Home 登録メールが [General] タブの [Contact Information] 領域に設定した電子メール アドレスに送信されます。

ステップ 5 シスコから登録メールを受信したら、次の作業を完了して Smart Call Home の登録を完了します。

a) 電子メールのリンクをクリックします。
このリンクによって、Cisco Smart Call Home ポータルが Web ブラウザで開きます。

b) Cisco Smart Call Home ポータルにログインします。
c) Cisco Smart Call Home によって示される手順に従います。
ご使用条件に同意すると、Cisco UCS ドメインの Cisco Smart Call Home 登録が完了します。

第 47 章

システム イベント ログの管理

この章の内容は、次のとおりです。

- システム イベント ログ，841 ページ
- 各サーバのシステム イベント ログの表示，842 ページ
- シャーシ内のサーバのシステム イベント ログの表示，842 ページ
- SEL ポリシーの設定，843 ページ
- サーバのシステム イベント ログの管理，845 ページ

システム イベント ログ

システム イベント ログ（SEL）は、NVRAM 内の CIMC に存在します。 過不足の電圧、温度イベント、ファン イベント、BIOS からのイベントなど、ほとんどのサーバ関連イベントが記録されます。 SEL は、主にトラブルシューティングのために使用します。

SEL ファイルのサイズは約 40KB で、ファイルがいっぱいになるとそれ以上イベントを記録できません。 新たなイベントを記録できるようにするには、ファイルの中身をクリアする必要があります。

SEL ポリシーを使用して、SEL をリモート サーバにバックアップできます。また、必要に応じて、バックアップ操作後に SEL をクリアすることもできます。 バックアップ操作は、特定のアクションに基づいて起動するか、定期的に実行できます。 SEL のバックアップやクリアは、手動で行うこともできます。

バックアップ ファイルは、自動的に生成されます。 このファイル名の形式は、sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp* です。たとえば、sel-UCS-A-ch01-serv01-QCI12522939-20091121160736 となります。

各サーバのシステム イベント ログの表示

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 システム イベント ログを表示するサーバをクリックします。

ステップ 4 [Work] ペインの [SEL Logs] タブをクリックします。
Cisco UCS Manager によってサーバのシステム イベント ログが取得され、イベントのリストが表示されます。

シャーシ内のサーバのシステム イベント ログの表示

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > *[Chassis_Name]* を展開します。

ステップ 3 [Work] ペインの [SEL Logs] タブをクリックします。
Cisco UCS Manager によってサーバのシステム イベント ログが取得され、イベントのリストが表示されます。

ステップ 4 [Server] テーブルで、システム イベント ログを表示するサーバを選択します。
Cisco UCS Manager によってサーバのシステム イベント ログが取得され、イベントのリストが表示されます。

SEL ポリシーの設定

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] ノードを展開します。

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 [SEL Policy] サブタブをクリックします。

ステップ 5 （任意） [General] 領域で、[Description] フィールドにポリシーの説明を入力します。
この領域の他のフィールドは読み取り専用です。

ステップ 6 [Backup Configuration] 領域で、次のフィールドに値を入力します。

名前	説明
[Protocol] フィールド	リモートサーバとの通信時に使用するプロトコル。 次のいずれかになります。 • FTP • TFTP • SCP • SFTP
[Hostname] フィールド	バックアップ設定が存在する場所のサーバのホスト名または IP アドレス。 IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。 （注） バックアップ ファイルの名前は Cisco UCS によって生成されます。 名前は次の形式になります。 `sel-system-name-chchassis-id-servblade-id-blade-serial-timestamp`

名前	説明
[Remote Path] フィールド	必要に応じて、リモートサーバ上のファイルの絶対パスを指定します。 SCP を使用する場合、絶対パスは常に必要です。 他のプロトコルを使用する場合は、ファイルがデフォルトのダウンロードフォルダにあれば、リモートパスを指定する必要はありません。 ファイルサーバの設定方法の詳細については、システム管理者に問い合わせてください。
[Backup Interval] ドロップダウン リスト	自動バックアップ間の待機時間。 次のいずれかになります。 • [Never]：自動 SEL データ バックアップを実行しません。 • 1 Hour • 2 Hours • 4 Hours • 8 Hours • 24 Hours （注） システムによって自動バックアップを作成する場合は、[Action] オプション ボックス内の [Timer] チェックボックスがオンになっていることを確認してください。
[Format] フィールド	バックアップ ファイルに使用する形式。 次のいずれかになります。 • Ascii • 2 進数
[Clear on Backup] チェックボックス	このチェックボックスをオンにすると、バックアップ後に、すべてのシステム イベント ログが Cisco UCS によってクリアされます。
[User] フィールド	システムがリモートサーバへのログインに使用する必要のあるユーザ名。 プロトコルが TFTP の場合、このフィールドは適用されません。
[Password] フィールド	リモート サーバのユーザ名のパスワード。 プロトコルが TFTP の場合、このフィールドは適用されません。

名前	説明
[Action] オプション ボックス	オンにした各チェックボックスのイベントが発生したとき、システムによって SEL バックアップが作成されます。 • [Log Full]：ログが許容される最大サイズに到達。 • [On Change of Association]：サーバとそのサービス プロファイルの間のアソシエーションが変化。 • [On Clear]：システム イベント ログがユーザによって手動でクリア。 • [Timer]：[Backup Interval] ドロップダウン リストで指定された時間間隔に到達。
[Reset Configuration] ボタン	このボタンをクリックすると、バックグラウンドの設定情報がリセットされます。

ステップ 7 [Save Changes] をクリックします。

サーバのシステム イベント ログの管理

システム イベント ログの 1 つ以上のエントリのコピー

このタスクでは、サーバまたはシャーシの [SEL Logs] タブからサーバのシステム イベント ログが表示されていることを前提にしています。

手順

ステップ 1 Cisco UCS Manager GUI によって [SEL Logs] タブにシステム イベント ログが表示されたら、マウスを使用してシステム イベント ログからコピーするエントリを強調表示します。

ステップ 2 [Copy] をクリックして、強調表示されたテキストをクリップボードにコピーします。

ステップ 3 強調表示されたテキストをテキスト エディタまたは他のドキュメントに貼り付けます。

システム イベント ログの印刷

このタスクでは、サーバまたはシャーシの [SEL Logs] タブからサーバのシステム イベント ログが表示されていることを前提にしています。

手順

ステップ 1 Cisco UCS Manager GUI の [SEL Logs] タブにシステム イベント ログが表示されたら、[Print] をクリックします。

ステップ 2 [Print] ダイアログボックスで、次の手順を実行します。

a) （任意） デフォルト プリンタ、あるいはその他の任意のフィールドまたはオプションを修正します。

b) [Print] をクリックします。

システム イベント ログのリフレッシュ

このタスクでは、サーバまたはシャーシの [SEL Logs] タブからサーバのシステム イベント ログが表示されていることを前提にしています。

手順

Cisco UCS Manager GUI の [SEL Logs] タブにシステム イベント ログが表示されたら、[Refresh] をクリックします。
Cisco UCS Manager はサーバのシステム イベント ログを取得し、アップデートされたイベント リストを表示します。

システム イベント ログの手動バックアップ

このタスクでは、サーバまたはシャーシの [SEL Logs] タブからサーバのシステム イベント ログが表示されていることを前提にしています。

はじめる前に

システム イベント ログ ポリシーを設定します。 手動によるバックアップ操作では、システム イベント ログ ポリシーで設定されたリモート宛先を使用します。

手順

Cisco UCS Manager GUI の [SEL Logs] タブにシステム イベント ログが表示されたら、[Backup] をクリックします。
Cisco UCS Manager は、SEL ポリシーで指定された場所にシステム イベント ログをバックアップします。

システム イベント ログの手動クリア

このタスクでは、サーバまたはシャーシの [SEL Logs] タブからサーバのシステム イベント ログが表示されていることを前提にしています。

手順

Cisco UCS Manager GUI の [SEL Logs] タブにシステム イベント ログが表示されたら、[Clear] をクリックします。

（注） SEL ポリシーの [Action] オプション ボックスで [Clear] がイネーブルになっていると、この処理によって自動バックアップが実行されます。

第 48 章

障害、イベント、およびログの設定

この章の内容は、次のとおりです。

- 障害収集ポリシーの設定，849 ページ
- エラーの抑制の設定，852 ページ
- Core File Exporter の設定，869 ページ
- syslog の設定，871 ページ

障害収集ポリシーの設定

障害収集ポリシー

障害収集ポリシーは、障害がクリアされた日時、フラッピング間隔（障害が発生した時点と状態がクリアされた時点の間の時間）、および保持間隔（システムで障害が発生していた時間）など、Cisco UCS ドメインの障害のライフサイクルを制御します。

Cisco UCS の障害には、次のライフサイクルがあります。

1. ある状況がシステムで発生し、Cisco UCS Manager で障害が発生します。 これはアクティブな状態です。
2. 障害が軽減されると、フラッピングまたはフラッピングを防ぐことを目的としたソーキング間隔になります。 障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 フラッピング間隔のうち、障害収集ポリシーに指定されている期間は、障害の重要度が保持されます。
3. フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。
4. クリアされた障害は保持期間になります。 この期間があるため、障害が発生した状態が改善され、さらに障害が早々に削除されていない場合でも管理者が障害に気付くことができます。 保持期間のうち、障害収集ポリシーに指定された期間はクリアされた障害が保持されます。

5 保持期間にその状態が再発すると、障害はアクティブな状態を返します。 この状況が再発生しない場合は、障害が削除されます。

障害収集ポリシーの設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Settings] をクリックします。

ステップ 4 [Work] ペインの [Global Fault Policy] タブをクリックします。

ステップ 5 [Global Fault Policy] タブで、次のフィールドに値を入力します。

名前	説明
[Flapping Interval] フィールド	障害が発生し、すぐに何度かクリアされると、フラッピングが発生します。 これを防止するため、Cisco UCS Manager では、最後に状態が変更されてからこの時間が経過するまで、障害が発生しても状態は変更されません。 フラッピング間隔中に同じ条件が再発生した場合は、障害がアクティブ状態に戻ります。 フラッピング間隔中に同じ条件が再発生しない場合は、障害がクリアされます。 その時点で何が発生するかは、[Clear Action] フィールドの設定によって異なります。 5 ～ 3,600 の範囲の整数を入力します。 デフォルトは 10 です。
[Initial Severity] フィールド	次のいずれかになります。 • Info • Condition • Warning
[Action on Acknowledgment] フィールド	確認された操作は、ログがクリアされると常に削除されます。 このオプションは変更できません。

名前	説明
[Clear Action] フィールド	障害がクリアされると Cisco UCS Manager が実行するアクション。 次のいずれかになります。 • [Retain]：Cisco UCS Manager GUI に [Length of time to retain cleared faults] セクションが表示されます。 • [Delete]：障害メッセージにクリアのマークが付いた時点で、Cisco UCS Manager はそれらのメッセージをすべて削除します。
[Clear Interval] フィールド	特定の時間が経過した後に、Cisco UCS Manager が自動的に障害をクリアするかどうか。 次のいずれかになります。 • [Never]：Cisco UCS Manager はどの障害も自動的にはクリアしません。 • [other]：Cisco UCS Manager GUI に [dd:hh:mm:ss] フィールドが表示されます。
[dd:hh:mm:ss] フィールド	Cisco UCS Manager が障害にクリアのマークを自動的に付けるまでの時間（日、時、分、および秒）。 何が発生するかは、[Clear Action] フィールドの設定によって異なります。
[Length of Time to Retain Cleared Faults] セクション	
[Retention Interval] フィールド	[Clear Action] フィールドが [Retain] に設定されている場合、これは障害にクリアのマークが付けられてから Cisco UCS Manager が障害を保持する時間です。 次のいずれかになります。 • [Forever]：Cisco UCS Manager では、システムに存在している期間に関係なく、ファブリックインターコネクト上でクリアされたすべての障害メッセージはそのまま残されます。 • [other]：Cisco UCS Manager GUI に [dd:hh:mm:ss] フィールドが表示されます。
[dd:hh:mm:ss] フィールド	Cisco UCS Manager が、クリアされた障害メッセージを削除するまでの時間（日、時、分、および秒）。

ステップ 6 [Save Changes] をクリックします。

エラーの抑制の設定

エラーの抑制

エラーの抑制により、定期メンテナンス時間中に SNMP トラップと Call Home 通知を抑制することができます。 エラーの抑制タスクを作成することで、一時的なエラーの発生時やクリア時に通知が送信されることを防ぐことができます。

指定した期限が切れるまで、またはユーザによってエラーの抑制タスクが手動で停止されるまで、エラーは抑制されます。 エラーの抑制が終了すると、Cisco UCS Manager はクリアされていない未処理の抑制されたエラーに関する通知を送信します。

エラーの抑制には次が使用されます。

固定時間間隔またはスケジュール

次を使用して、エラーを抑制するメンテナンス時間帯を指定できます。

- 固定時間間隔を使用して、エラーの抑制が有効になる開始時刻と実行期間を作成できます。固定時間間隔は再利用できません。
- スケジュールは、1 回のみのオカレンスまたは繰り返しの期間として使用されます。また、スケジュールは保存および再利用できます。

抑制ポリシー

これらのポリシーによって、抑制するエラーの原因とタイプが定義されます。 1 つのタスクに割り当てられるのは 1 つのポリシーのみです。 Cisco UCS Manager では、次のポリシーが定義されています。

- [default-chassis-all-maint]：すべてのブレードサーバ、電源、ファンモジュール、および IOM など、シャーシに取り付けられているすべてのコンポーネントとシャーシに関するエラーを抑制します。

  このポリシーはシャーシにのみ適用されます。

- [default-chassis-phys-maint]：シャーシに取り付けられているすべてのファン モジュールと電源、およびシャーシに関するエラーを抑制します。

  このポリシーはシャーシにのみ適用されます。

- [default-fex-all-maint]：FEX と、FEX 内のすべての電源、ファン モジュール、および IOM に関するエラーを抑制します。

  このポリシーは FEX にのみ適用されます。

- [default-fex-phys-maint]：FEX と、FEX 内のすべてのファン モジュールおよび電源に関するエラーを抑制します。

  このポリシーは FEX にのみ適用されます。

- [default-server-maint]：ブレード サーバおよび/またはラック サーバに関するエラーを抑制します。

  このポリシーは、シャーシ、組織、およびサービス プロファイルに適用されます。

  （注） シャーシに適用される場合、ブレード サーバのみが影響を受けます。

- [default-iom-maint]：シャーシまたは FEX 内の IOM に関するエラーを抑制します。

  このポリシーは、シャーシ、FEX、および IOM にのみ適用されます。

抑制タスク

これらのタスクを使用して、スケジュール設定または固定された時間間隔と抑制ポリシーをコンポーネントに関連付けることができます。

（注） 抑制タスクを作成したら、固定時間間隔、またはタスクのスケジュールを、Cisco UCS Manager GUI と Cisco UCS Manager CLI の両方で編集できるようになります。 ただし、変更できるのは固定時間間隔を使用するか、Cisco UCS Manager CLI でスケジュールを使用するかのいずれかです。

抑制されたエラーの表示

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Faults] をクリックします。

ステップ 4 [Work] ペインで、[Show:] フィールドの抑制アイコンを選択します。
抑制されたエラーのみを表示するには、[Show:] フィールドで他のアイコンを選択解除します。

シャーシのエラー抑制の設定

シャーシのエラー抑制タスクの設定

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 エラーの抑制タスクを作成するシャーシをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント 複数のシャーシに対してエラー抑制タスクを設定するには、Ctrl キーを使用して、[Navigation] ペインで複数のシャーシを選択します。 選択したシャーシのいずれかを右クリックし、[Start Fault Suppression] を選択します。

ステップ 6 [Start Fault Suppression] 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。

[Name] フィールド	障害抑制タスクの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Select Fixed Time Interval/Schedule] フィールド	障害抑制タスクを実行する場合。 次のいずれかになります。 • [Fixed Time Interval]：障害抑制タスクの開始時刻および期間を指定するには、このオプションを選択します。 [Start Time] フィールドで、障害抑制タスクを開始する日時を指定します。 このフィールドの終端にある下矢印をクリックして、ポップアップ カレンダーから開始時刻を選択します。 [Task Duration] フィールドで、このタスクを実行する時間の長さを指定します。 手動で停止するまでこのタスクが実行されるように指定するには、このフィールドに「00:00:00:00」と入力します。 • [Schedule]：事前定義されたスケジュールを使用して開始時刻と期間を設定するには、このオプションを選択します。 [Schedule] ドロップダウン リストからスケジュールを選択します。 新しいスケジュールを作成するには、[Create Schedule] をクリックします。

[Policy] ドロップダウン リスト	ドロップダウン リストから抑制ポリシーを選択します。 • [default-chassis-all-maint]：すべてのブレード サーバ、電源、ファン モジュール、および IOM など、シャーシに取り付けられているすべてのコンポーネントとシャーシに関するエラーを抑制します。 • [default-chassis-phys-maint]：シャーシに取り付けられているすべてのファン モジュールと電源、およびシャーシに関するエラーを抑制します。 • [default-server-maint]：ブレード サーバおよび/またはラック サーバに関するエラーを抑制します。 （注） シャーシに適用される場合、ブレード サーバのみが影響を受けます。 • [default-iom-maint]：シャーシまたは FEX 内の IOM に関するエラーを抑制します。

ステップ 7 [OK] をクリックします。

シャーシのエラー抑制タスクの削除

この手順では、シャーシのすべてのエラー抑制タスクが削除されます。 個々のタスクを削除するには、[Suppression Tasks] ダイアログボックスの [Delete] ボタンを使用します。 シャーシのエラー抑制タスクの表示, （856 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 すべてのエラーの抑制タスクを削除するシャーシをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Stop Suppression] をクリックします。

ヒント 複数のシャーシに対してエラー抑制タスクを削除するには、Ctrl キーを使用して、[Navigation] ペインで複数のシャーシを選択します。 選択したシャーシのいずれかを右クリックし、[Stop Fault Suppression] を選択します。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

シャーシのエラー抑制タスクの表示

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] を展開します。

ステップ 3 エラーの抑制タスクのプロパティを表示するシャーシをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Suppression Task Properties] をクリックします。
[Suppression Tasks] ダイアログボックスで、新しいエラー抑制タスクの追加、既存のエラー抑制タスクの削除、または既存のエラー抑制タスクの変更を行えます。

I/O モジュールのエラーの抑制の設定

IOM のエラー抑制タスクの設定

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 （任意） シャーシで IOM モジュールを選択するには、[Equipment] タブで、[Equipment] > [Chassis] > *[Chassis Number]* > [IO Modules] を展開します。

ステップ 3 （任意） FEX で IOM モジュールを選択するには、[Epment] タブで、[Equipment] > [FEX] > *[FEX Number]* > [IO Modules] を展開します。

ステップ 4 エラーの抑制タスクを作成する IOM をクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント 複数の IOM に対してエラー抑制タスクを設定するには、Ctrl キーを使用して、[Navigation] ペインで複数の IOM を選択します。 選択した IOM のいずれかを右クリックし、[Start Fault Suppression] を選択します。

シャーシまたは FEX のいずれか、あるいはそれらの両方で IOM を選択できます。

ステップ 7 **[Start Fault Suppression]** 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。

[Name] フィールド	障害抑制タスクの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

[Select Fixed Time Interval/Schedule] フィールド	障害抑制タスクを実行する場合。 次のいずれかになります。 • [Fixed Time Interval]：障害抑制タスクの開始時刻および期間を指定するには、このオプションを選択します。 [Start Time] フィールドで、障害抑制タスクを開始する日時を指定します。 このフィールドの終端にある下矢印をクリックして、ポップアップ カレンダーから開始時刻を選択します。 [Task Duration] フィールドで、このタスクを実行する時間の長さを指定します。 手動で停止するまでこのタスクが実行されるように指定するには、このフィールドに「00:00:00:00」と入力します。 • [Schedule]：事前定義されたスケジュールを使用して開始時刻と期間を設定するには、このオプションを選択します。 [Schedule] ドロップダウン リストからスケジュールを選択します。 新しいスケジュールを作成するには、[Create Schedule] をクリックします。
[Policy] ドロップダウン リスト	デフォルトで、次の抑制ポリシーが選択されます。 • [default-iom-maint]：シャーシまたは FEX 内の IOM に関するエラーを抑制します。

ステップ 8 [OK] をクリックします。

IOM のエラー抑制タスクの削除

この手順では、IOM のすべてのエラー抑制タスクが削除されます。 個々のタスクを削除するには、[Suppression Tasks] ダイアログボックスの [Delete] ボタンを使用します。 IOM のエラー抑制タスクの表示, （858 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 （任意） シャーシで IOM モジュールを選択するには、[Equipment] タブで、[Equipment] > [Chassis] > *[Chassis Number]* > [IO Modules] を展開します。

ステップ 3 （任意） FEX で IOM モジュールを選択するには、[Epment] タブで、[Equipment] > [FEX] > *[FEX Number]* > [IO Modules] を展開します。

ステップ 4 すべてのエラーの抑制タスクを削除する IOM をクリックします。

ステップ 5 [Work] ペインの [General] タブをクリックします。

ステップ 6 [Actions] 領域で、[Stop Suppression] をクリックします。

ヒント　複数のIOMに対してエラー抑制タスクを削除するには、Ctrlキーを使用して、[Navigation] ペインで複数の IOM を選択します。 選択した IOM のいずれかを右クリックし、[Stop Fault Suppression] を選択します。

シャーシまたは FEX のいずれか、あるいはそれらの両方で IOM を選択できます。

ステップ 7　Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

IOM のエラー抑制タスクの表示

手順

ステップ 1　[Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2　（任意） シャーシで IOM モジュールを選択するには、[Equipment] タブで、[Equipment] > [Chassis] > *[Chassis Number]* > [IO Modules] を展開します。

ステップ 3　（任意） FEX で IOM モジュールを選択するには、[Epment] タブで、[Equipment] > [FEX] > *[FEX Number]* > [IO Modules] を展開します。

ステップ 4　エラーの抑制タスクのプロパティを表示する IOM をクリックします。

ステップ 5　[Work] ペインの [General] タブをクリックします。

ステップ 6　[Actions] 領域で、[Suppression Task Properties] をクリックします。
[Suppression Tasks] ダイアログボックスで、新しいエラー抑制タスクの追加、既存のエラー抑制タスクの削除、または既存のエラー抑制タスクの変更を行えます。

FEX のエラー抑制の設定

FEX のエラー抑制タスクの設定

手順

ステップ 1　[Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2　[Equipment] タブで、[Equipment] > [Rack Mounts] > [FEX] を展開します。

ステップ 3　エラーの抑制タスクを作成する FEX をクリックします。

ステップ 4　[Work] ペインの [General] タブをクリックします。

ステップ 5　[Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント　複数のFEXに対してエラー抑制タスクを設定するには、Ctrlキーを使用して、[Navigation] ペインで複数の FEX を選択します。 選択した FEX のいずれかを右クリックし、[Start Fault Suppression] を選択します。

ステップ 6 **[Start Fault Suppression]** 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。

[Name] フィールド	障害抑制タスクの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Select Fixed Time Interval/Schedule] フィールド	障害抑制タスクを実行する場合。 次のいずれかになります。 • [Fixed Time Interval]：障害抑制タスクの開始時刻および期間を指定するには、このオプションを選択します。 [Start Time] フィールドで、障害抑制タスクを開始する日時を指定します。 このフィールドの終端にある下矢印をクリックして、ポップアップ カレンダーから開始時刻を選択します。 [Task Duration] フィールドで、このタスクを実行する時間の長さを指定します。 手動で停止するまでこのタスクが実行されるように指定するには、このフィールドに「00:00:00:00」と入力します。 • [Schedule]：事前定義されたスケジュールを使用して開始時刻と期間を設定するには、このオプションを選択します。 [Schedule] ドロップダウン リストからスケジュールを選択します。 新しいスケジュールを作成するには、[Create Schedule] をクリックします。
[Policy] ドロップダウン リスト	ドロップダウン リストから抑制ポリシーを選択します。 • [default-fex-all-maint]：FEX と、FEX 内のすべての電源、ファン モジュール、および IOM に関するエラーを抑制します。 • [default-fex-phys-maint]：FEX と、FEX 内のすべてのファン モジュールおよび電源に関するエラーを抑制します。 • [default-iom-maint]：シャーシまたは FEX 内の IOM に関するエラーを抑制します。

ステップ 7 [OK] をクリックします。

FEX のエラー抑制タスクの表示

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [FEX] を展開します。

ステップ 3 エラーの抑制タスクのプロパティを表示する FEX をクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Suppression Task Properties] をクリックします。
[Suppression Tasks] ダイアログボックスで、新しいエラー抑制タスクの追加、既存のエラー抑制タスクの削除、または既存のエラー抑制タスクの変更を行えます。

FEX のエラー抑制タスクの削除

この手順では、FEX のすべてのエラー抑制タスクが削除されます。 個々のタスクを削除するには、[Suppression Tasks] ダイアログボックスの [Delete] ボタンを使用します。 FEX のエラー抑制タスクの表示, （860 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [FEX] を展開します。

ステップ 3 すべてのエラーの抑制タスクを削除する FEX をクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Stop Suppression] をクリックします。

ヒント 複数の FEX に対してエラー抑制タスクを削除するには、Ctrl キーを使用して、[Navigation] ペインで複数の FEX を選択します。 選択した FEX のいずれかを右クリックし、[Stop Fault Suppression] を選択します。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サーバのエラー抑制の設定

ブレード サーバのエラー抑制タスクの設定

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 エラーの抑制タスクを作成するサーバをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント 複数のブレード サーバに対してエラー抑制タスクを設定するには、Ctrl キーを使用して、[Navigation] ペインで複数のブレード サーバを選択します。 選択したサーバのいずれかを右クリックし、[Start Fault Suppression] を選択します。

ステップ 6 [Start Fault Suppression] 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。

[Name] フィールド	障害抑制タスクの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Select Fixed Time Interval/Schedule] フィールド	障害抑制タスクを実行する場合。 次のいずれかになります。 • [Fixed Time Interval]：障害抑制タスクの開始時刻および期間を指定するには、このオプションを選択します。 [Start Time] フィールドで、障害抑制タスクを開始する日時を指定します。 このフィールドの終端にある下矢印をクリックして、ポップアップ カレンダーから開始時刻を選択します。 [Task Duration] フィールドで、このタスクを実行する時間の長さを指定します。 手動で停止するまでこのタスクが実行されるように指定するには、このフィールドに「00:00:00:00」と入力します。 • [Schedule]：事前定義されたスケジュールを使用して開始時刻と期間を設定するには、このオプションを選択します。 [Schedule] ドロップダウン リストからスケジュールを選択します。 新しいスケジュールを作成するには、[Create Schedule] をクリックします。
[Policy] ドロップダウン リスト	デフォルトで、次の抑制ポリシーが選択されます。 • [default-server-maint]：ブレード サーバおよび/またはラック サーバに関するエラーを抑制します。

ステップ 7 [OK] をクリックします。

ラック サーバのエラー抑制タスクの設定

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 エラーの抑制タスクを作成するサーバをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント 複数のラック サーバに対してエラー抑制タスクを設定するには、Ctrl キーを使用して、[Navigation] ペインで複数のラック サーバを選択します。 選択したサーバのいずれかを右クリックし、[Start Fault Suppression] を選択します。

ステップ 6 **[Start Fault Suppression]** 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。

[Name] フィールド	障害抑制タスクの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。
[Select Fixed Time Interval/Schedule] フィールド	障害抑制タスクを実行する場合。 次のいずれかになります。 • [Fixed Time Interval]：障害抑制タスクの開始時刻および期間を指定するには、このオプションを選択します。 [Start Time] フィールドで、障害抑制タスクを開始する日時を指定します。 このフィールドの終端にある下矢印をクリックして、ポップアップ カレンダーから開始時刻を選択します。 [Task Duration] フィールドで、このタスクを実行する時間の長さを指定します。 手動で停止するまでこのタスクが実行されるように指定するには、このフィールドに「00:00:00:00」と入力します。 • [Schedule]：事前定義されたスケジュールを使用して開始時刻と期間を設定するには、このオプションを選択します。 [Schedule] ドロップダウン リストからスケジュールを選択します。 新しいスケジュールを作成するには、[Create Schedule] をクリックします。

[Policy] ドロップダウン リスト	デフォルトで、次の抑制ポリシーが選択されます。 • [default-server-maint]：ブレード サーバおよび/またはラック サーバに関するエラーを抑制します。

ステップ 7 [OK] をクリックします。

ブレード サーバのエラー抑制タスクの削除

この手順では、ブレードサーバのすべてのエラー抑制タスクが削除されます。 個々のタスクを削除するには、[Suppression Tasks] ダイアログボックスの [Delete] ボタンを使用します。 ブレードサーバのエラー抑制タスクの表示, （864 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 すべてのエラーの抑制タスクを削除するサーバをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Stop Suppression] をクリックします。

ヒント 複数のブレード サーバに対してエラー抑制タスクを削除するには、Ctrl キーを使用して、[Navigation] ペインで複数のブレード サーバを選択します。 選択したサーバのいずれかを右クリックし、[Stop Fault Suppression] を選択します。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ラック サーバのエラー抑制タスクの削除

この手順では、ラック サーバのすべてのエラー抑制タスクが削除されます。 個々のタスクを削除するには、[Suppression Tasks] ダイアログボックスの [Delete] ボタンを使用します。 ラック サーバのエラー抑制タスクの表示, （864 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 すべてのエラーの抑制タスクを削除するサーバをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Stop Suppression] をクリックします。

ヒント 複数のラック サーバに対してエラー抑制タスクを削除するには、Ctrl キーを使用して、[Navigation] ペインで複数のラック サーバを選択します。 選択したサーバのいずれかを右クリックし、[Stop Fault Suppression] を選択します。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

ブレード サーバのエラー抑制タスクの表示

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Chassis] > [*Chassis Number*] > [Servers] を展開します。

ステップ 3 エラーの抑制タスクのプロパティを表示するサーバをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスで、新しいエラー抑制タスクの追加、既存のエラー抑制タスクの削除、または既存のエラー抑制タスクの変更を行えます。

ラック サーバのエラー抑制タスクの表示

手順

ステップ 1 [Navigation] ペインの [Equipment] タブをクリックします。

ステップ 2 [Equipment] タブで、[Equipment] > [Rack Mounts] > [Servers] を展開します。

ステップ 3 エラーの抑制タスクのプロパティを表示するサーバをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Suppression Task Properties] をクリックします。

[Suppression Tasks] ダイアログボックスで、新しいエラー抑制タスクの追加、既存のエラー抑制タスクの削除、または既存のエラー抑制タスクの変更を行えます。

サービス プロファイルのエラー抑制の設定

サービス プロファイルのエラー抑制タスクの設定

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 エラーの抑制タスク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 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Start Fault Suppression] をクリックします。

ヒント 複数のサービスプロファイルに対してエラー抑制タスクを設定するには、Ctrl キーを使用して、[Navigation] ペインで複数のサービス プロファイルを選択します。 選択したサービス プロファイルのいずれかを右クリックし、[Start Fault Suppression] を選択します。

ステップ 6 **[Start Fault Suppression]** 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。

[Name] フィールド	障害抑制タスクの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

[Select Fixed Time Interval/Schedule] フィールド	障害抑制タスクを実行する場合。 次のいずれかになります。 • [Fixed Time Interval]：障害抑制タスクの開始時刻および期間を指定するには、このオプションを選択します。 [Start Time] フィールドで、障害抑制タスクを開始する日時を指定します。 このフィールドの終端にある下矢印をクリックして、ポップアップ カレンダーから開始時刻を選択します。 [Task Duration] フィールドで、このタスクを実行する時間の長さを指定します。 手動で停止するまでこのタスクが実行されるように指定するには、このフィールドに「00:00:00:00」と入力します。 • [Schedule]：事前定義されたスケジュールを使用して開始時刻と期間を設定するには、このオプションを選択します。 [Schedule] ドロップダウン リストからスケジュールを選択します。 新しいスケジュールを作成するには、[Create Schedule] をクリックします。
[Policy] ドロップダウン リスト	デフォルトで、次の抑制ポリシーが選択されます。 • [default-server-maint]：ブレード サーバおよび/またはラック サーバに関するエラーを抑制します。

ステップ 7 [OK] をクリックします。

サービス プロファイルのエラー抑制タスクの削除

この手順では、サービスプロファイルのすべてのエラー抑制タスクが削除されます。 個々のタスクを削除するには、[Suppression Tasks] ダイアログボックスの [Delete] ボタンを使用します。 サービス プロファイルのエラー抑制タスクの表示, （867 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3 すべてのエラーの抑制タスクを削除するサービス プロファイルをクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Stop Suppression] をクリックします。

ヒント　複数のサービス プロファイルに対してエラー抑制タスクを削除するには、Ctrl キーを使用して、[Navigation] ペインで複数のサービス プロファイルを選択します。 選択したサービス プロファイルのいずれかを右クリックし、[Stop Fault Suppression] を選択します。

ステップ 6　Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

サービス プロファイルのエラー抑制タスクの表示

手順

ステップ 1　[Navigation] ペインの [Servers] タブをクリックします。

ステップ 2　[Servers] タブで、[Servers] > [Service Profiles] を展開します。

ステップ 3　エラーの抑制タスクのプロパティを表示するサービス プロファイルをクリックします。

ステップ 4　[Work] ペインの [General] タブをクリックします。

ステップ 5　[Actions] 領域で、[Suppression Task Properties] をクリックします。
[Suppression Tasks] ダイアログ ボックスで、新しいエラー抑制タスクの追加、既存のエラー抑制タスクの削除、または既存のエラー抑制タスクの変更を行えます。

組織のエラー抑制の設定

組織のエラー抑制タスクの設定

手順

ステップ 1　[Navigation] ペインの [Servers] タブをクリックします。

ステップ 2　[Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。

ステップ 3　エラーの抑制タスクを作成する組織をクリックします。

ステップ 4　[Work] ペインの [General] タブをクリックします。

ステップ 5　[Actions] 領域で、[Start Fault Suppression] をクリックします。

ステップ 6　**[Start Fault Suppression]** 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。

[Name] フィールド	障害抑制タスクの名前。 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）以外の特殊文字またはスペースは使用できません。また、オブジェクトを保存した後、この名前を変更することはできません。

[Select Fixed Time Interval/Schedule] フィールド	障害抑制タスクを実行する場合。 次のいずれかになります。 • [Fixed Time Interval]：障害抑制タスクの開始時刻および期間を指定するには、このオプションを選択します。 [Start Time] フィールドで、障害抑制タスクを開始する日時を指定します。 このフィールドの終端にある下矢印をクリックして、ポップアップ カレンダーから開始時刻を選択します。 [Task Duration] フィールドで、このタスクを実行する時間の長さを指定します。 手動で停止するまでこのタスクが実行されるように指定するには、このフィールドに「00:00:00:00」と入力します。 • [Schedule]：事前定義されたスケジュールを使用して開始時刻と期間を設定するには、このオプションを選択します。 [Schedule] ドロップダウン リストからスケジュールを選択します。 新しいスケジュールを作成するには、[Create Schedule] をクリックします。
[Policy] ドロップダウン リスト	デフォルトで、次の抑制ポリシーが選択されます。 • [default-server-maint]：ブレード サーバおよび/またはラック サーバに関するエラーを抑制します。

ステップ 7 [OK] をクリックします。

組織のエラー抑制タスクの削除

この手順では、組織のすべてのエラー抑制タスクが削除されます。 個々のタスクを削除するには、[Suppression Tasks] ダイアログボックスの [Delete] ボタンを使用します。 組織のエラー抑制タスクの表示, （869 ページ）を参照してください。

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。

ステップ 3 すべてのエラーの抑制タスクを削除する組織をクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Stop Suppression] をクリックします。

ステップ 6 Cisco UCS Manager GUI に確認ダイアログボックスが表示されたら、[Yes] をクリックします。

組織のエラー抑制タスクの表示

手順

ステップ 1 [Navigation] ペインの [Servers] タブをクリックします。

ステップ 2 [Servers] タブで、[Servers] > [Policies] > [*Organization_Name*] を展開します。

ステップ 3 エラーの抑制タスクのプロパティを表示する組織をクリックします。

ステップ 4 [Work] ペインの [General] タブをクリックします。

ステップ 5 [Actions] 領域で、[Suppression Task Properties] をクリックします。
[Suppression Tasks] ダイアログ ボックスで、新しいエラー抑制タスクの追加、既存のエラー抑制タスクの削除、または既存のエラー抑制タスクの変更を行えます。

Core File Exporter の設定

Core File Exporter

Cisco UCS は、コア ファイルが発生するとただちに Core File Exporter を使用して、TFTP を介してネットワーク上の指定の場所にエクスポートします。 この機能を使用することにより、tar ファイルをコア ファイルのコンテンツと一緒にエクスポートできます。

Core File Exporter の設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Settings] をクリックします。

ステップ 4 [Work] ペインの [TFTP Core Exporter] タブをクリックします。

ステップ 5 [TFTP Core Exporter] タブで、次のフィールドに入力します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • [Enabled]：エラーによってサーバでコア ダンプが実行されると、Cisco UCS によって FTP を介して指定された場所にコア ダンプ ファイルが送信されます。 このオプションを選択すると、Cisco UCS Manager GUI によってこの領域に他のフィールドが表示され、FTP エクスポート オプションを指定できます。 • [Disabled]：コア ダンプ ファイルは自動的にエクスポートされません。
[Description] フィールド	コア 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。`（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）を除く文字やスペースを使用できます。
[Port] フィールド	Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）を介してコア ダンプ ファイルをエクスポートするときに使用されるポート番号。
[Hostname] フィールド	TFTP を介して接続されるホスト名または IP アドレス。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。
[Path] フィールド	リモート システムにコア ダンプ ファイルを保存するときに使用するパス。

ステップ 6 [Save Changes] をクリックします。

Core File Exporter のディセーブル化

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Settings] をクリックします。

ステップ 4 [Work] ペインで [Settings] タブをクリックします。

ステップ 5 [TFTP Core Exporter] 領域で、[Admin State] フィールドの [disabled] オプション ボタンをクリックします。

ステップ 6 [Save Changes] をクリックします。

syslog の設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブで、[All] > [Faults]、[Events]、[Audit Log] を展開します。

ステップ 3 [Syslog] をクリックします。

ステップ 4 [Work] ペインで [Syslog] タブをクリックします。

ステップ 5 [Local Destinations] 領域で、次のフィールドに値を入力します。

名前	説明
[Console] セクション	
[Admin State] フィールド	Cisco UCS によって Syslog メッセージがコンソールに表示されるかどうか。 次のいずれかになります。 • [Enabled]：Syslog メッセージがコンソールに表示され、ログにも追加されます。 • [Disabled]：Syslog メッセージはログに追加されますが、コンソールには表示されません。

名前	説明
[Level] フィールド	このオプションを [Enabled] にした場合は、表示するメッセージの最も低いレベルを選択します。 そのレベル以上のメッセージが Cisco UCS によってコンソールに表示されます。 次のいずれかになります。 • Emergencies • Alerts • Critical
[Monitor] セクション	
[Admin State] フィールド	Cisco UCS によって Syslog メッセージがモニタに表示されるかどうか。 次のいずれかになります。 • [Enabled]：Syslog メッセージがモニタに表示され、ログにも追加されます。 • [Disabled]：Syslog メッセージはログに追加されますが、モニタには表示されません。 [Admin State] がイネーブルの場合、Cisco UCS Manager GUI にはこのセクションの残りのフィールドが表示されます。
[Level] ドロップダウン リスト	このオプションを [Enabled] にした場合は、表示するメッセージの最も低いレベルを選択します。 モニタにはそのレベル以上のメッセージが表示されます。 次のいずれかになります。 • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information • Debugging
[File] セクション	

名前	説明
[Admin State] フィールド	Cisco UCS によって、ファブリック インターコネクトのシステム ログ ファイルにメッセージが保存されるかどうか。 次のいずれかになります。 • [Enabled]：メッセージはログ ファイルに保存されます。 • [Disabled]：メッセージは保存されません。 [Admin State] がイネーブルの場合、Cisco UCS Manager GUI にはこのセクションの残りのフィールドが表示されます。
[Level] ドロップダウン リスト	システムに保存するメッセージの最も低いレベルを選択します。 Cisco UCS は、そのレベル以上のメッセージをファブリック インターコネクト上のファイルに保存します。 次のいずれかになります。 • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information • Debugging
[Name] フィールド	メッセージが記録されるファイルの名前。 名前には16文字以内の英数字を使用できます。 名前にはスペースを使用できず、また-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）以外の特殊文字は使用できません。 デフォルトは「messages」です。
[Size] フィールド	ファイルで可能な最大サイズ（バイト単位）。ファイルがこのサイズを超えると、Cisco UCS Manager によって最も古いメッセージから最新メッセージへの上書きが開始されます。 4096 ～ 4194304 の整数を入力します。

ステップ 6 [Remote Destinations] 領域で、次のフィールドに情報を入力し、Cisco UCS コンポーネントによって生成されたメッセージを保存できる最大 3 つの外部ログを設定します。

名前	説明
[Admin State] フィールド	次のいずれかになります。 • Enabled • Disabled [Admin State] がイネーブルの場合、Cisco UCS Manager GUI にはこのセクションの残りのフィールドが表示されます。
[Level] ドロップダウン リスト	システムに保存するメッセージの最も低いレベルを選択します。リモートファイルにそのレベル以上のメッセージが保存されます。 次のいずれかになります。 • Emergencies • Alerts • Critical • Errors • Warnings • Notifications • Information • Debugging
[Hostname] フィールド	リモートログファイルが存在するホスト名またはIPアドレス。 （注） IP 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、DNS Management が [local] に設定されている場合、DNS サーバを Cisco UCS Manager に設定します。 Cisco UCS ドメインが Cisco UCS Central に登録されており、DNS Management が [global] に設定されている場合、DNS サーバを Cisco UCS Central に設定します。

名前	説明
[Facility] ドロップダウン リスト	次のいずれかになります。 • Local0 • Local1 • Local2 • Local3 • Local4 • Local5 • Local6 • Local7

ステップ 7 [Save Changes] をクリックします。

索 引

記号

[Fault Summary] 領域 38
[Navigation] ペイン 39
[Work] ペイン 42

A

admin アカウント 180
admin パスワードの復旧 771, 772, 774
all configuration 750
API、XML のコピー 55
authNoPriv 134
authPriv 134

B

BIOS 447, 448, 450, 455, 457, 460, 462, 464, 469, 470, 471, 472
　実際の設定 472
　設定 447, 448, 450, 455, 457, 460, 462, 464
　　Intel Directed I/O 455
　　PCI 設定 462
　　RAS メモリ 457
　　USB 460
　　概要 447
　　サーバ管理 464
　　主要 448
　　シリアル ポート 460
　　ブート オプション 462
　　プロセッサ 450
　デフォルト設定 469
　デフォルトの修正 471
　ポリシー 469
　ポリシーの作成 470
BIOS、回復 723, 736
BIOS の回復 723, 736
　ブレード サーバ 723
　ラックマウント サーバ 736
Bronze システム クラス 25, 294

C

Call Home 817, 819, 820, 821, 822, 826, 827, 828, 829, 830, 833, 834, 835, 838, 839
　Cisco TAC-1 プロファイル 838
　Smart Call Home 821
　Smart Call Home の登録 839
　イネーブル化 826
　概要 817
　考慮事項 819
　システム インベントリ メッセージ 827, 828
　重大度 820
　設定 822
　ディセーブル化 826
　プロファイル 828, 829
　プロファイルの削除 833
　プロファイルの作成 830
　ポリシー 833
　ポリシーのイネーブル化 835
　ポリシーの削除 835
　ポリシーの設定 833
　ポリシーのディセーブル化 834
CDP 336
CIM-XML、設定 125
CIMC 439, 440, 441, 442, 444, 722, 735
　IP アドレス 439
　管理 IP 440, 441, 442, 444
　　サービス プロファイル 442
　　サービス プロファイル テンプレート 444
　　ブレード サーバ 440
　　ラック サーバ 441
　リセット 722, 735

Cisco VM-FEX 29
cisco-av-pair 144
CiscoAVPair 144
Cisco Discovery Protocol 335, 336
Cisco TAC-1 プロファイル、設定 838
Cisco UCS Central 234, 235, 236, 237
登録 235
登録解除 237
ポリシー解決 234, 236
Cisco UCS Manager 31, 37
GUI 37
概要 31
Cisco UCS Manager ベースのゾーン分割 417, 418, 424, 426
vHBA イニシエータ グループ 417
アクティブ ゾーン セットの設定 418
概要 417
ファイバ チャネル ストレージ接続 418, 424, 426
CMOS のリセット 721, 735
Core File Exporter 869, 871
概要 869
設定 869
ディセーブル化 871

D

DNS サーバ 205, 206
概要 205
削除 206
追加 205

F

FCoE 13, 114, 115
ポート チャネル 114, 115
削除 115
FCoE VLAN ID 368
変更 368
FCoE ストレージ ポート、設定 94
FC アップリンク 360, 369, 370
トランキング 360, 369, 370
イネーブル化 369
概要 360
ディセーブル化 370
FC エンドホスト モード 360
VSAN ID の制限 360
FC スイッチ モード 360
VSAN ID の制限 360
fex 858, 860
エラー抑制 858
エラー抑制タスクのプロパティ 860
full state 750

G

Gold システム クラス 25, 294
GUI 37, 38, 39, 42, 43, 45, 46, 47, 50, 55
[Fault Summary] 領域 38
[Navigation] ペイン 39
[Work] ペイン 42
XML のコピー 55
概要 37
ステータスバー 42
セッションのプロパティ 50
ツールバー 42
テーブルのカスタマイズ 43
ハイブリッド表示 45
ログアウト 47
ログイン、HTTP 46
ログイン、HTTPS 45
GUI 非アクティブ タイムアウト 50

H

HTTP 46, 47, 48, 125, 197
Web セッション制限 47, 48, 197
設定 125
ログイン 46
HTTPS 45, 47, 48, 127, 128, 129, 130, 131, 197
Web セッション制限 47, 48, 197
キー リングの作成 127
証明書のインポート 130
証明書要求 128
設定 131
トラスト ポイント 129
ログイン 45

I

I/O モジュール 747, 748, 796
POST の結果 748
管理 747
モニタリング 796
リセット 747

IEEE 802.1Qbh 29
IEEE 802.3x リンクレベル フロー制御 14
Intel Directed I/O、BIOS 設定 455
Internal Fabric Manager 45, 120, 121
　概要 45, 120
　起動 120
　ポートのイネーブル化 121
　ポートの設定 120
　ポートの設定解除 121
　ポートのディセーブル化 121
iom 856, 858
　エラー抑制 856
　エラー抑制タスクのプロパティ 858
IOM 748, 796
　POST の結果 748
　モニタリング 796
IP 438, 446
　プール 438, 446
IPMI アクセス プロファイル 473, 474
　概要 473
　削除 474
　作成 473
IP アドレス 61, 438, 439, 444
　CIMC 439
　管理 IP プール 444
　管理ポート 61
　プールの削除 438
IP プール 434, 435, 437, 438, 444, 445, 531
　IP アドレス ブロックの削除 438
　IP アドレス ブロックの作成 437, 445
　iSCSI イニシエータ アドレス ブロックの作成 531
　概要 434
　管理 444
　削除 438
　作成 435
IQN プール 544, 546, 547
　概要 544
　削除 547
　作成 544
　ブロックの削除 547
　ブロックの追加 546
iSCI vNIC 333, 334
　LAN 接続ポリシー 333, 334
iSCSI 531
　認証プロファイル 531
　　削除 531
iSCSI vNIC 533, 535
　サービス プロファイルからの削除 535
iSCSI vNIC *(続き)*
　サービス プロファイルに対する作成 533
iSCSI アダプタ ポリシー 527, 529
　削除 529
　作成 527
iSCSI イニシエータのインターフェイス 535, 540
　設定 535
　変更 540
iSCSI ターゲットのインターフェイス 535, 540
　設定 535
　変更 540
iSCSI ブート 522, 523, 526, 529
　概要 522
　設定 526
　　高レベルのタスク 526
　前提条件 523
　認証プロファイル 529
iSCSI ブート パラメータ 535, 540
　設定 535
　変更 540
iSCSI ブート プロセス 523
iSCSI ブート ポリシー 532
　作成 532

K

KVM Launch Manager 739, 745
KVM コンソール 439, 739, 744, 745
　IP アドレス 439
　Launch Manager 745
　概要 739
　サーバから起動 744
　サービス プロファイルからの起動 744

L

L2 ネットワーク、分離 345
LAN 44, 241, 249, 250, 253, 257, 258, 261, 265, 285, 286, 287, 290, 291, 305, 345, 438
　IP プール 438
　MAC プール 290, 291
　PVLAN 258
　VLAN 257
　vNIC ポリシー 305
　アップリンク マネージャ 44, 241

LAN *(続き)*
ネームド VLAN 250, 253, 261, 265
削除 253, 265
作成 250, 261
ピン グループ 249, 250, 285, 286, 287
削除 250, 287
作成 249, 286
分離 L2 ネットワーク 345
LAN アップリンク マネージャ 44, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 253, 254
uplinkEthernet ポートのディセーブル化 245
アップリンク イーサネット ポートのイネーブル化 245
アップリンク イーサネット ポートの設定解除 246
イーサネット スイッチング モードの変更 242
概要 44, 241
起動 242
サーバ ポートのイネーブル化 243
サーバ ポートの設定解除 244
サーバ ポートのディセーブル化 244
システム クラス、設定 254
ネームド VLAN 250, 253
削除 253
作成 250
ピン グループ 249, 250
削除 250
作成 249
ポート チャネル 246, 247, 248, 249
イネーブル化 247
削除 249
作成 246
ディセーブル化 248
ポートの削除 249
ポートの追加 248
ポートの設定 243
LAN 接続ポリシー 320, 321, 328, 332, 333, 334, 335, 402, 403
iSCSI vNIC の削除 334
iSCSI vNIC の作成 333
vNIC の削除 332
vNIC の作成 328
概要 320, 402
権限 320, 403
サービス プロファイル 321, 403
削除 335
作成 321
LAN ピン グループ 249, 250, 286, 287
削除 250, 287
作成 249, 286
LAN ブート 548
概要 548
Launch Manager、KVM 739, 745
LDAP 155, 156, 163, 164
グループ マップ 155, 156
削除 156
作成 155
プロバイダー グループ 163, 164
削除 164
作成 163
LDAP グループ マッピング 155
LDAP グループ ルール 146
LDAP プロバイダー 144, 147, 148, 154, 155, 156, 163, 164
概要 144
グループ 163, 164
削除 164
作成 163
グループ マップ 155, 156
削除 156
作成 155
削除 154
作成 148
プロパティの設定 147
ユーザ属性 144
LED、ビーコン 83
LED ロケータ 708, 721, 735
シャーシ 708
ブレード サーバ 721
ラックマウント サーバ 735
logical configuration 750

M

MAC アドレス 289, 290, 291
プール 289
プールの削除 291
プールの作成 290
MAC アドレス テーブル 214
エージング タイム、概要 214
エージング タイムの設定 214
MAC 同期 60
MAC プール 290, 291
削除 291
作成 290

N

NAS ポート、アプライアンス ポートを参照 92
NAS ポート、設定 95
NIC アダプタ 30
　仮想化 30
NMI 724, 737
　ブレード サーバ 724
　ラックマウント サーバ 737
NMI の発行 724, 737
　ブレード サーバ 724
　ラックマウント サーバ 737
noAuthNoPriv 134
NTP サーバ 701, 702
　概要 701
　削除 702
　追加 702

O

OS のインストール 739
　KVM コンソール 739

P

PCI 設定、BIOS 設定 462
PFC 14
PKI 126
POST 708, 724, 737, 748
　I/O モジュールの表示 748
　シャーシの表示 708
　ブレード サーバ 724
　ラックマウント サーバ 737
PSU ポリシー 688
PVLAN 258, 266, 271
　概要 258
　セカンダリの作成 271
　プライマリの作成 266

Q

Quality of Service（QoS）ポリシー 25, 297, 298, 300
　概要 25, 297
　削除 300
　作成 298
Quality of Service 24, 25, 26, 254, 293, 294, 296, 297, 298, 300, 301
　概要 24, 293
　システム クラス 24, 254, 293, 294, 296, 297
　　LAN アップリンク マネージャ 254
　　イネーブル化 296
　　設定 294
　　ディセーブル化 297
　フロー制御ポリシー 26, 301
　ポリシー 25, 297, 298, 300

R

RADIUS 164, 165
　プロバイダー グループ 164, 165
　　削除 165
　　作成 164
RADIUS プロバイダー 144, 156, 157, 159, 164, 165
　概要 144
　グループ 164, 165
　　削除 165
　　作成 164
　削除 159
　作成 157
　プロパティの設定 156
　ユーザ属性 144
RAID 設定、ローカル ディスク設定ポリシー 477
RAS メモリ、BIOS 設定 457
RSA 126

S

SAN 359, 362, 365, 368, 371, 372, 389
　vHBA ポリシー 389
　VSAN 359
　ストレージ VSAN 365
　　作成 365
　ネームド VSAN 362, 368
　　削除 368
　　作成 362
　ピン グループ 371, 372
SAN 接続ポリシー 320, 321, 402, 403, 404, 408, 411, 412, 413, 414
　vHBA の削除 411, 413
　vHBA の作成 408, 412
　概要 320, 402
　権限 320, 403
　サービス プロファイル 321, 403

SAN 接続ポリシー *(続き)*
削除 414
作成 404
SAN ピン グループ 372
削除 372
作成 372
SAN ブート 519, 520
概要 519
設定 520
SEL 841
概要 841
SEL ポリシー 843
設定 843
Serial over LAN ポリシー 486, 488
概要 486
削除 488
作成 486
Silver システム クラス 25, 294
Smart Call Home 819, 820, 821, 835, 838, 839
Cisco TAC-1 プロファイル 838
概要 821
考慮事項 819
システム インベントリ メッセージ 838
重大度 820
設定 835
登録 839
SNMP 133, 134, 136, 137, 138, 140, 141
SNMPv3 ユーザ 140, 141
イネーブル化 137
概要 133
権限 134
コミュニティ 137
サポート 133, 136
セキュリティ レベル 134
通知 134
トラップ 138, 140
削除 140
作成 138
バージョン 3 のセキュリティ機能 136
ユーザ 140, 141
削除 141
作成 140
SNMPv3 136
セキュリティ機能 136
SPAN。参照先： トラフィック モニタリング
SSH、プロパティ 52
syslog 871
システム設定 750

T

TACACS+ 165, 166
プロバイダー グループ 165, 166
削除 166
作成 165
TACACS+ プロバイダー 144, 160, 165, 166
概要 144
グループ 165, 166
削除 166
作成 165
作成 160
ユーザ属性 144
TACACS プロバイダー 160, 162
削除 162
プロパティの設定 160
Telnet、イネーブル化 142
TFTP Core Exporter 869, 871

U

UCS Manager 37
GUI 37
USB、BIOS 設定 460
UUID 662, 681, 682
サービス プロファイル テンプレートでの変更 681
変更 662
リセット 682
UUID 接尾辞プール 432, 434
概要 432
削除 434
作成 432

V

VALN 276, 281
権限 281
概要 281
ポート数の最適化 276
enable 276
VALN グループ 278
概要 278
vCon 502, 503, 504, 505, 512, 513
N20-B6620-2 および N20-B6625-2 ブレード サーバのアダプタ配置 504
vNIC/vHBA の割り当て 505, 512, 513
アダプタの配置 503

vCon *(続き)*
概要 502
その他すべてのサーバのアダプタの配置 504
vHBA 320, 321, 391, 392, 402, 403, 408, 411, 412, 413, 505, 513, 670, 674, 676, 684
SAN 接続ポリシー 320, 321, 402, 403, 408, 411, 412, 413
vCon への割り当て 505, 513
vHBA イニシエータ グループの追加 676
vHBA テンプレートからのバインド解除 392
vHBA テンプレートへのバインディング 391
WWPN の変更 674
WWPN のリセット 684
永続的なバインディングのクリア 676
サービス プロファイルからの削除 676
サービス プロファイル用の作成 670
vHBA SAN 接続ポリシー 389, 391, 392
vHBA のバインディング 391
vHBA のバインド解除 392
概要 389
作成 389
vHBA イニシエータ グループ 417
概要 417
vHBA テンプレート 389, 391, 392, 393
vHBA のバインディング 391
vHBA のバインド解除 392
概要 389
削除 393
作成 389
VIC アダプタ 30
仮想化 30
VIF のステータス 792, 795
VLAN 92, 250, 253, 257, 258, 261, 265, 266, 271, 275, 276, 277, 278, 279, 280, 281, 282, 345, 346, 348, 349, 351, 353, 355, 356
VLAN Group 278
作成 278
VLAN グループ 278, 279, 280, 281
概要 278
delete 281
組織の権限 280
変更 280
メンバの編集 279
VLAN の最適化設定 277
VLAN のポート数の最適化 275
概要 275
アプライアンス ポート 92
権限 282
変更 282
VLAN *(続き)*
組織の権限 282
ディセーブル化 282
ネームド 250, 253, 257, 261, 265
概要 257
削除 253, 265
作成 250, 261
プライベート 258, 266, 271
概要 258
セカンダリの作成 271
プライマリの作成 266
分離 L2 ネットワーク 345, 346, 348, 349
分離 L2 ネットワークに対する作成 351
ポート VLAN 数の最適化 276
ディセーブル化 276
ポートおよびポート チャネルの削除 355
ポートおよびポート チャネルの表示 356
ポートおよびポート チャネルの割り当て 353
ポート数 275
VLAN ポートの制限事項 260
VM-FEX 29
概要 29
vNIC 305, 310, 311, 320, 321, 328, 332, 402, 403, 505, 512, 533, 535, 666, 670, 683
iSCSI 533, 535
サービス プロファイルからの削除 535
サービス プロファイルに対する作成 533
LAN 接続ポリシー 320, 321, 328, 332, 402, 403
MAC アドレスのリセット 683
vCon への割り当て 505, 512
vNIC テンプレートからのバインド解除 311
vNIC テンプレートへのバインディング 310
サービス プロファイルからの削除 670
サービス プロファイル用の作成 666
ポリシー 305
vNIC LAN 接続ポリシー 305, 306, 310, 311, 312
vNIC のバインディング 310
vNIC のバインド解除 311
概要 305
削除 312
作成 306
vNIC/vHBA 配置ポリシー 502, 503, 504, 505, 508, 511
N20-B6620-2 および N20-B6625-2 ブレード サーバの vCon 504
vCon 502, 503
vNIC/vHBA の割り当て 505
概要 502
削除 511

vNIC/vHBA 配置ポリシー *(続き)*
作成 508
その他すべてのサーバの vCon 504
vNIC テンプレート 305, 306, 310, 311, 312
vNIC のバインディング 310
vNIC のバインド解除 311
概要 305
削除 312
作成 306
VSAN 359, 360, 362, 365, 368, 416, 417, 418, 419, 421, 424, 426
削除 368
作成 362, 365, 421
ネームド 362
ストレージ 365
ネームド 359, 360
ファイバ チャネル ゾーン分割 416, 417, 418, 419, 421, 424, 426

W

Web セッション制限 47, 48, 183, 197
WWN 374, 378, 379, 384, 387
削除 378, 384, 387
WWNN プール 378
WWPN プール 384
WWxN プール 387
作成 374, 379, 384
WWNN プール 374
WWPN プール 379
WWxN プール 384
WWNN イニシエータ 377, 378
WWNN プールへの追加 377
削除 378
WWNN プール 373, 374, 376, 377, 378
WWNN イニシエータの削除 378
WWNN イニシエータの追加 377
WWN ブロックの削除 376
WWN ブロックの追加 376
概要 373
削除 378
作成 374
WWN プール 373
概要 373
WWN ブロック 376, 381, 386, 387
WWNN プールからの削除 376
WWNN プールへの追加 376
WWPN プールからの削除 381
WWN ブロック *(続き)*
WWPN プールへの追加 381
WWxN プールからの削除 387
WWxN プールへの追加 386
WWPN イニシエータ 382, 383
WWPN プールへの追加 382
削除 383
WWPN プール 373, 379, 381, 382, 383, 384
WWN ブロックの削除 381
WWN ブロックの追加 381
WWPN イニシエータの削除 383
WWPN イニシエータの追加 382
概要 373
削除 384
作成 379
WWxN プール 373, 384, 386, 387
WWN ブロックの削除 387
WWN ブロックの追加 386
概要 373
削除 387
作成 384

X

XML、コピー 55
XML のコピー 55

あ

アーキテクチャの単純化 11
アカウント 180, 181, 182, 193, 199, 200, 202, 203
admin 180
イネーブル化 199
失効 180
ディセーブル化 199
ユーザ 180, 182
ユーザの作成 193
ユーザ名の注意事項 181
リモート認証された 180
ローカル認証された 180, 200, 202, 203
ローカルの削除 200
アクティビティ 555, 572, 573, 574
保留中 555, 572, 573, 574
値、範囲 53

アダプタ 30, 116, 503, 504
N20-B6620-2 および N20-B6625-2 ブレード サーバの vCon 配置 504
NIC 30
vCon の配置 503
VIC 30
仮想化 30
その他すべてのサーバの vCon の配置 504
ポート チャネル 116
アダプタ ポート チャネル 116
表示 116
アップストリーム分離L2ネットワーク。参照先：分離L2ネットワーク
アップリンク、LAN のマネージャ 44, 241
アップリンク イーサネット ポート 84, 85, 94, 95, 243, 245, 246
イネーブル化 245
設定 84, 94, 95, 243
[Equipment] タブ 84
FCoE ストレージ 94
LAN アップリンク マネージャ 243
NAS 95
設定解除 246
速度 85
ディセーブル化 245
フロー制御ポリシー 85
アップリンク トランキング 360, 369, 370
ファイバ チャネル 360, 369, 370
イネーブル化 369
概要 360
ディセーブル化 370
アップリンク ファイバ チャネル ポート 96
復元 96
アップリンク ポート 26, 74, 84, 102, 249, 250, 285, 286, 287, 301, 371, 372
イーサネット 84
概要 74
ピン グループ 249, 250, 285, 286, 287, 371, 372
削除 250, 287
作成 249, 286
フロー制御ポリシー 26, 301
ポート チャネル 102
アップリンク イーサネット 102
アップリンク ポート チャネル 102, 103, 104, 105, 246, 247, 248, 249
イーサネット 102, 103, 104, 105
イネーブル化 103
削除 105
作成 102
アップリンク ポート チャネル *(続き)*
イーサネット *(続き)*
ディセーブル化 104
イネーブル化 247
削除 249
作成 246
ディセーブル化 248
ポートの削除 249
ポートの追加 248
アプライアンス ポート 89, 92
設定 89
変更 92
アプライアンス ポート チャネル 105, 108, 109, 110
イネーブル化 108
削除 110
作成 105
ディセーブル化 109
ポートの削除 109
ポートの追加 109
アラート グループ 828, 829
プロファイル 828, 829
暗黙的な割り当て 505

い

イーサネット 13, 26, 69, 74, 80, 81, 83, 84, 85, 89, 92, 94, 102, 103, 104, 105, 108, 109, 110, 242, 246, 301
FCoE ストレージ ポート 94
Fibre Channel over 13
アップリンク ポート 74, 84
アップリンク ポート チャネル 102, 103, 104, 105, 246
削除 105
ディセーブル化 104
ポートの削除 104
ポートの追加 104
アップリンク ポートの変更 85
アプライアンス ポート 89, 92
アプライアンス ポート チャネル 105, 108, 109, 110
サーバ ポート 84
スイッチング モード 69, 242
ビーコン LED 83
フロー制御ポリシー 26, 301
ポート モード 80, 81
イーサネット アダプタ ポリシー 312, 314, 318, 393
概要 312, 393
削除 318
作成 314

イーサネット スイッチング モード 68
　概要 68
イーサネット ポート 86, 87
　イネーブル化 86
　ディセーブル化 87
位置特定 708
　シャーシ 708
1 回のオカレンス 554, 562, 568
　概要 554
　削除 568
　作成 562
イニシエータ 377, 378, 382, 383
　WWNN 377, 378
　WWPN 382, 383
イニシエータ グループ 417, 676
　概要 417
　追加 676
イネーブル化 86, 121, 137, 142, 243, 245, 247, 705, 706, 822, 826, 835, 869
　Call Home 822, 826
　Core File Exporter 869
　Smart Call Home 835
　SNMP 137
　Telnet 142
　uplinkEthernet ポート 245
　イーサネット ポート 86
　稼働を停止しているシャーシ 705, 706
　サーバ ポート 243
　ポート 121
　ポート チャネル 247
イベント 842, 843, 845, 846, 847
　SEL ポリシー 843
　システム イベント ログ 842, 845, 846, 847
　　印刷 845
　　クリア 847
　　コピー 845
　　バックアップ 846
　　表示 842
　　リフレッシュ 846
インフォーム 134
　概要 134
インポート 752, 753, 763, 767, 768
　概要 752
　操作の削除 768
　操作の作成 763
　操作の変更 767
　復元方法 752
　ユーザ ロール 753
インポート操作 763, 766, 767, 768
　削除 768
　作成 763
　実行 766
　変更 767

う

上書き 578
　サーバ ID 578

え

永続的なバインディング、クリア 676
エージング タイム 214
　MAC アドレス テーブル 214
エクスポート 749, 750, 753
　設定 749
　バックアップ 753
　バックアップ タイプ 750
　ユーザ ロール 753
エラーの抑制 852, 855, 857, 860, 863, 866, 868
　fex の停止 860
　iom の停止 857
　サーバの停止 863
　サービス プロファイルの停止 866
　シャーシの停止 855
　組織の停止 868
エラーの抑制タスク 853
　表示 853
エラーの抑制タスクの削除 855, 857, 860, 863, 866, 868
　fex 860
　iom 857
　サーバ 863
　サービス プロファイル 866
　シャーシ 855
　マニュアルの構成 868
エラーの抑制の停止 855, 857, 860, 863, 866, 868
　fex 860
　iom 857
　サーバ 863
　サービス プロファイル 866
　シャーシ 855
　マニュアルの構成 868
エラー抑制 854, 856, 858, 861, 862, 865, 867
　fex 858

エラー抑制 *(続き)*
iom 856
サーバ 861, 862
サービス プロファイル 865
シャーシ 854
マニュアルの構成 867
エラー抑制タスクのプロパティ 856, 858, 860, 864, 867, 869
fex 860
iom 858
サーバ 864
サービス プロファイル 867
シャーシ 856
マニュアルの構成 869
エンドホスト モード 69, 70, 242
イーサネット 69
ファイバ チャネル 70

お

オーバーサブスクリプション 19, 20, 21
概要 19
考慮事項 20
注意事項 21
オカレンス 554, 562, 565, 568
1 回 554, 562, 568
概要 554
削除 568
作成 562
繰り返す 554, 565, 568
概要 554
削除 568
作成 565
オプトアウト 26, 27, 29
ステートレス コンピューティング 27
マルチテナント 29
オプトイン 26, 27, 28
概要 26
ステートレス コンピューティング 27
マルチテナント 28
オペレーティング システムのインストール 739
KVM コンソール 739

か

解決、名前 205
外部アプリケーション 52
概要 11
確認 704, 717, 732
シャーシ 704
ブレード サーバ 717
ラックマウント サーバ 732
確認メッセージ 51
カスタム ロール 185
予約語 185
仮想 IP アドレス、変更 71
仮想 KVM コンソール 740
仮想化 29, 30
NIC アダプタ 30
VIC アダプタ 30
VM-FEX 29
概要 29
概要 29
統合型ネットワーク アダプタ 30
仮想マシン 29
仮想メディア ブート 550
概要 550
設定 550
仮想レーン 24, 293
稼働中止 705, 719, 732
シャーシ 705
ブレード サーバ 719
ラックマウント サーバ 732
下部 176
管理 31, 703, 712, 726, 747
I/O モジュール 747
シャーシ 703
ブレード サーバ 712
ラックマウント サーバ 726
管理 IP アドレス 439
管理 IP プール 441, 442, 444, 445, 446, 531
IP アドレス ブロックの削除 446
IP アドレス ブロックの作成 445
iSCSI イニシエータ 531
IP アドレス プール 531
iSCSI イニシエータの IP アドレス ブロックの作成 531
概要 444
ブレード サーバ 441
ラック サーバ 442
管理インターフェイスのモニタリング ポリシー 796, 797
概要 796
設定 797
管理ポートの IP アドレス 61

き

キー リング 126, 127, 128, 129, 130, 132
　概要 126
　削除 132
　作成 127
　証明書のインポート 130
　証明書要求 128
　トラスト ポイント 129
起動 45, 46, 120, 242, 744, 745
　GUI 45, 46
　GUI、HTTP 46
　GUI、HTTPS 45
　Internal Fabric Manager 120
　KVM Launch Manager 745
　KVM コンソールをサーバから 744
　LAN アップリンク マネージャ 242
　サービス プロファイルからの KVM コンソール 744
機能 26, 217
　オプトイン 26
　ステートレス コンピューティング 26
　ライセンス 217
許容範囲の確認 53
許容範囲の検索 53

く

クラスタ設定 63, 66
　従属ファブリック インターコネクト 66
　プライマリ ファブリック インター コネクト 63
繰り返すオカレンス 554, 565, 568
　概要 554
　削除 568
　作成 565
グループ マップ 155, 156
　LDAP 155, 156
　　削除 156
　　作成 155
グレースフル シャットダウン 717, 731
グローバル キャップ ポリシー 689
　設定 689
グローバル プール 19

け

継承、サーバ 492
継承された値 17, 576
権限 185, 190, 320, 403
　概要 185
　削除 190
　接続ポリシー 320, 403
　追加 190

こ

更新 553
　サービス プロファイル 553
考慮事項 750, 819
　Call Home 819
　バックアップ操作 750
コミュニティ、SNMP 137
コンソール、KVM 739, 744, 745
コンソール認証サービス 168

さ

サーバ 14, 15, 16, 22, 26, 28, 205, 206, 429, 430, 431, 432, 440, 441, 442, 447, 448, 450, 455, 457, 460, 462, 464, 469, 470, 471, 472, 473, 474, 475, 479, 483, 484, 490, 491, 492, 494, 495, 496, 497, 502, 517, 518, 527, 529, 532, 552, 553, 575, 578, 614, 618, 619, 620, 621, 655, 656, 657, 658, 659, 660, 661, 662, 680, 682, 697, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 724, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 744, 745, 790, 793, 799, 800, 801, 802, 808, 810, 812, 842, 843, 861, 862, 864
　BIOS ポリシー 469, 470
　BIOS 設定 447, 448, 450, 455, 457, 460, 462, 464
　BIOS の回復 736
　BIOS のデフォルト 469, 471
　DNS 205, 206
　IPMI アクセス 473, 474
　iSCSI アダプタ ポリシー 527, 529
　iSCSI ブート ポリシー 532
　KVM コンソール 744, 745
　NMI の発行 724, 737
　POST の結果 724, 737
　SEL ポリシー 843
　UUID の変更 662
　UUID のリセット 682
　エラー抑制 861, 862
　エラー抑制タスクのプロパティ 864
　稼働中止 719, 732
　継承ポリシー 492
　サービス プロファイル 14, 16, 553, 575, 680

サーバ *(続き)*
サービス プロファイルからのテンプレート 657
サービス プロファイル テンプレートの作成 620, 621
サービス プロファイルとの関連付け 659
サービス プロファイルとの関連付けの解除 660
サービス プロファイルのクローン化 658
サービス プロファイルの作成 578, 614
サービス プロファイルの名前変更 661
再確認 717, 732
再稼働 719, 733
削除 718, 720, 734
シャーシから 718
データベースから 720, 734
システム イベント ログ 842
実際の BIOS 設定 472
シャットダウン 715, 716, 730
ステートレス 26
スロットの再確認 720
設定 15
ディスカバリ ポリシー 490, 491, 492
ディスク ドライブ ステータス 801, 802
ディスク ドライブのサポート 800
ディスク ドライブ モニタリング 799, 800
テンプレートからのサービス プロファイル 655
テンプレート ベースのサービス プロファイル 656
電力ブレード レベルの電力制限の設定 697
統計情報しきい値ポリシー 808, 810, 812
ハードウェア ベースのサービス プロファイル 618, 619
ハード リセット 717, 731
番号の付け替え 733
ピン接続 22
ブート 714, 728
ブート順 715, 729
ブート ポリシー 517, 518, 552
プール 429, 430, 431
プールからの削除 432
プールの資格情報 496, 497, 502
プールへの追加 431
プール ポリシー 494, 495
ブレード 440, 441, 712, 714
管理 IP プール 441
スタティック管理 IP 440
ブート 714
マルチテナント 28
モニタリング 790, 793
予期しない電源変更 713, 727

サーバ *(続き)*
ラック 441, 442
管理 IP プール 442
スタティック管理 IP 441
ラックマウント 726, 728
ブート 728
リセット 721, 722, 735
CIMC 722, 735
CMOS 721, 735
ローカル ディスク設定 475, 479, 483, 484
ロケータ LED 721, 735
サーバ ID の上書き 16, 575, 578
サーバ管理 712, 726
サーバ管理、BIOS 設定 464
サーバ継承ポリシー 492, 494
概要 492
削除 494
作成 492
サーバ自動構成ポリシー 488, 490
概要 488
削除 490
作成 488
サーバ ディスカバリ ポリシー 490, 491, 492
概要 490
削除 492
作成 491
サーバ電力使用量の制限 697
サーバの仮想化 12
サーバの稼働中止 712
サーバの関連付け 659
サーバの関連付けの解除 660
サーバの起動 714, 728
サーバの削除 712
サーバのシャットダウン 716, 730
サーバの停止 715, 716, 730
サーバ プール 430, 431, 432, 659, 660, 680, 681
サーバの削除 432
サーバの追加 431
サービス プロファイル テンプレートの関連付け 680
サービス プロファイル テンプレートの関連付けの解除 681
サービス プロファイルの関連付け 659
サービス プロファイルの関連付けの解除 660
削除 431
作成 430
サーバ プール ポリシー 494, 495
概要 494

サーバ プール ポリシー *(続き)*
削除 495
作成 494
サーバ プール ポリシーの資格情報 496, 497, 502
概要 496
削除 502
作成 497
資格の削除 502
サーバ ポート 45, 74, 84, 120, 121, 243, 244
Internal Fabric Manager 45, 120
イネーブル化 121, 243
Internal Fabric Manager 121
概要 74
設定 84, 120, 243
[Equipment] タブ 84
Internal Fabric Manager 120
LAN アップリンク マネージャ 243
設定解除 121, 244
Internal Fabric Manager 121
ディセーブル化 121, 244
Internal Fabric Manager 121
サービス プロファイル 14, 15, 16, 17, 18, 54, 320, 321, 402, 403, 442, 533, 535, 553, 575, 576, 577, 578, 580, 588, 595, 597, 602, 607, 609, 611, 614, 618, 619, 655, 656, 657, 658, 659, 660, 661, 662, 663, 666, 670, 674, 676, 679, 682, 683, 684, 713, 714, 716, 727, 728, 730, 744, 865, 867
iSCSI vNIC 533, 535
作成 533
MAC アドレスのリセット 683
UUID の変更 662
UUID のリセット 682
vHBA 670, 674, 676
vHBA イニシエータ グループの追加 676
vNIC 666, 670
WWPN のリセット 684
ウィザードを使用した作成 578, 580, 588, 595, 597, 602, 607, 609, 611
vNIC/vHBA 配置 597
アイデンティティ 578
サーバのブート順 602
サーバの割り当て 609
ストレージ 588
ゾーン分割 595
ネットワーキング 580
ポリシー 611
メンテナンス ポリシー 607
エラー抑制 865
エラー抑制タスクのプロパティ 867
オーバーライド ID 16, 575
サービス プロファイル *(続き)*
概要 14
管理 IP の設定 442
関連付け 659
関連付けの解除 660
クローン化 658
継承された値 17, 576
継承された値を使用した作成 614
サーバ 714, 716, 728, 730, 744
KVM コンソール 744
シャットダウン 716, 730
ブート 714, 728
使用されるプール 54
使用されるポリシー 54
接続ポリシー 320, 321, 402, 403
設定 15
注意事項 577
展開の延期 553
テンプレート 18, 577
テンプレートからの作成 655
テンプレートからのバインド解除 679
テンプレートの作成 657
テンプレート ベースの作成 656
ブレード サーバ 656
ラックマウント サーバ 656
テンプレートへのバインディング 679
名前の変更 661
ネットワーク接続 15
ハードウェア ベースの作成 618, 619
ブレード サーバ 618
ラックマウント サーバ 619
ブート順序の変更 663
予期しない電源変更 713, 727
サービス プロファイル ウィザード 578, 580, 588, 595, 597, 602, 607, 609, 611
開く 578
ページ 1、ID 578
ページ 2、ネットワーキング 580
ページ 3、ストレージ 588
ページ 4、ゾーン分割 595
ページ 5、vNIC/vHBA 配置 597
ページ 6、サーバのブート順序 602
ページ 7、メンテナンス ポリシー 607
ページ 8、サーバの割り当て 609
ページ 9、ポリシー 611

サービス プロファイル テンプレート 54, 444, 620, 621, 622, 630, 637, 639, 644, 649, 651, 652, 679, 680, 681
UUID の変更 681
ウィザードを使用した作成 649
メンテナンス ポリシー 649
管理 IP の設定 444
サーバ プールとの関連付け 680
サーバ プールとの関連付けの解除 681
サービス プロファイルのバインディング 679
サービス プロファイルのバインド解除 679
作成 620, 621, 622, 630, 637, 639, 644, 651, 652
vNIC/vHBA 配置 639
アイデンティティ 621
サーバのブート順 644
サーバの割り当て 651
ゾーン分割 637
動作ポリシー 652
ネットワーキング 622
使用されるプール 54
使用されるポリシー 54
サービス プロファイル テンプレートのウィザード 620, 621, 622, 630, 637, 639, 644, 649, 651, 652
開く 620
ページ 1、ID 621
ページ 2、ネットワーキング 622
ページ 3、ストレージ 630
ページ 4、ゾーン分割 637
ページ 5、vNIC/vHBA 配置 639
ページ 6、サーバのブート順序 644
ページ 6、メンテナンス ポリシー 649
ページ 8、サーバの割り当て 651
ページ 9、動作ポリシー 652
サービス プロファイルのクローン化 658
サービス プロファイルの名前変更 661
再確認 717, 720, 732
サーバ スロット 720
ブレード サーバ 717
ラックマウント サーバ 732
再稼働 719, 733
ブレード サーバ 719
ラックマウント サーバ 733
再稼働、シャーシ 705, 706
再接続間隔 50
削除 249, 680, 705, 718, 720, 734
サービス プロファイル 680
シャーシ 705
シャーシからのサーバ 718
削除 *(続き)*
設定からのブレード サーバ 720
設定からのラックマウント サーバ 734
ポート チャネルからのポート 249
作成 655, 657
サービス プロファイル 655
サービス プロファイル テンプレート 657
サブネット、変更 71
サポートされていないタスク 34
サポートされるタスク 33

し

しきい値ポリシー 808, 810, 812, 814, 815
アップリンク イーサネット ポート 812
しきい値クラスの追加 812
イーサネット サーバ ポート 814
しきい値クラスの追加 814
概要 808
サーバおよびサーバ コンポーネント 808, 810, 812
削除 812
作成 808
しきい値クラスの追加 810
ファイバ チャネル ポート 815
しきい値クラスの追加 815
システム イベント ログ 841
概要 841
システム イベント ログの印刷 845
システム イベント ログのクリア 847
システム イベント ログのコピー 845
システム イベント ログのリフレッシュ 846
システム インベントリ メッセージ 827, 828, 838
設定 827
送信 828
システム管理 703, 712, 726, 747
I/O モジュール 747
シャーシ 703
ブレード サーバ 712
ラックマウント サーバ 726
システム クラス 24, 25, 293, 294, 296, 297
bronze 25, 294
Gold 25, 294
platinum 25, 294
silver 25, 294
イネーブル化 296
設定 294
ディセーブル化 297

システム クラス *(続き)*
Fibre Channel 25, 294
ベスト エフォート 25, 294
実行 758, 766
インポート操作 766
バックアップ操作 758
自動構成ポリシー 488, 490
概要 488
削除 490
作成 488
自動的に再接続 50
シャーシ 45, 207, 210, 691, 693, 694, 703, 704, 705, 706, 707, 708, 717, 718, 720, 724, 788, 854, 856
NMI の発行 724
POST の結果 708
エラー抑制 854
エラー抑制タスクのプロパティ 856
確認 704
稼働中止 705
稼働停止のイネーブル化 705, 706
管理 703
サーバの確認 717
サーバの削除 718
削除 705
スロットの再確認 720
ディスカバリ ポリシー 207, 210
電力グループ 691, 693, 694
削除 694
作成 691
シャーシの追加 693
シャーシの取り外し 693
ハイブリッド表示 45
番号の付け替え 707
モニタリング 788
ロケータ LED での消灯 708
ロケータ LED での点灯 708
シャーシ管理 703, 704, 705, 706, 708, 788
確認 704
稼働停止のイネーブル化 705, 706
削除 705
モニタリング 788
ロケータ LED での消灯 708
ロケータ LED での点灯 708
シャーシ接続ポリシー 212
システム関連ポリシー 212
シャーシ 212
シャーシ ディスカバリ ポリシー 207, 210
概要 207
設定 210
シャーシの稼働中止、注意事項 703
シャーシの削除、注意事項 703
シャットダウン 715, 730
ブレード サーバ 715
ラックマウント サーバ 730
シャットダウン、グレースフル 717, 731
従属ファブリック インターコネクト 66
初期設定 66
重大度、Call Home 820
柔軟性 12
終了 47
手動ブレード レベルの電力制限 696
主要、BIOS 設定 448
障害 820, 849, 850, 853, 854, 856, 858, 861, 862, 865, 867, 869, 871
Call Home の重大度 820
Core File Exporter 869, 871
収集ポリシー 849, 850
抑制 854, 856, 858, 861, 862, 865, 867
抑制された表示 853
ライフサイクル 849
障害収集ポリシー 849, 850
概要 849
設定 850
証明書 126, 128
HTTPS 128
概要 126
初期設定 59, 60, 61, 63, 66
概要 59
管理ポートの IP アドレス 61
クラスタ設定 63, 66
スタンドアロン設定 61
セットアップ モード 60
初期テンプレート 18, 577
シリアル番号、入手方法 219
シリアル ポート、BIOS 設定 460

す

推奨事項 750
バックアップ操作 750
スイッチベースのゾーン分割 418
概要 418
スイッチング モード 69, 70, 242
イーサネット 69

スイッチング モード *(続き)*
ファイバ チャネル 70
スクラブ ポリシー 484, 485, 486
概要 484
削除 486
作成 485
スケーラビリティ 12
スケジューリング 751, 752
すべてのコンフィギュレーションのエクスポート 752
データベースのバックアップ 752
バックアップ 751
スケジュール 554, 556, 562, 565, 568, 569
1 回のオカレンス 562, 568
削除 568
作成 562
概要 554
繰り返すオカレンス 565, 568
削除 568
作成 565
削除 569
作成 556
スタンドアロン設定 61
ステータスバー 42
ステートレス 26
ステートレス コンピューティング 26, 27
オプトアウト 27
オプトイン 27
概要 26
ストレージ VSAN 365, 368, 421
削除 368
作成 365
ファイバ チャネル ゾーン分割 421
ストレージ VSANS 368
FCoE VLAN ID 368
ストレージ接続ポリシー 418, 424, 426
概要 418
削除 426
作成 424

せ

セカンダリ VLAN 271
セッションのプロパティ 50
セッション、ユーザ 203
設定 50, 51, 52, 53, 69, 70, 84, 97, 98, 100, 120, 125, 127, 128, 129, 130, 131, 142, 242, 243, 752, 753, 758, 763, 769
CIM-XML 125
設定 *(続き)*
HTTP 125
HTTPS 127, 128, 129, 130, 131
インポート 752
インポート方法 752
外部アプリケーションのプロパティ 52
確認メッセージ 51
サーバ ポート 84
スイッチング モード 69, 70, 242
セッションのプロパティ 50
通信サービス 142
バックアップ 753, 758
表示機能拡張のプロパティ 53
復元 753, 763, 769
ポート 100, 120, 243
ユニファイド アップリンク ポート 100
ポートの設定 97
FCoE アップリンク ポート 97
ユニファイド接続ポート 98
設定解除 121
ポート 121
設定、クラスタ 63, 66
設定された値 17, 576
設定、スタンドアロン 61
設定の置き換え 752
設定のマージ 752
セットアップ 63, 66
従属ファブリック インターコネクト 66
プライマリ ファブリック インター コネクト 63
セットアップ モード 60
選択 168, 169
コンソール認証サービス 168
デフォルトの認証サービス 169
選択的排他 345

そ

相互包含 345
操作 753, 758, 759, 763, 768
インポート 763, 768
バックアップ 753, 758, 759
操作、確認 51
ゾーン分割 419, 421
VSAN 421
ファイバ チャネル 419
組織 28, 173, 174, 176, 177, 188, 191, 192, 193
概要 173

組織 (続き)
削除 177
作成 176
名前解決 174
マルチテナント 28
ロケール 188
ロケールからの削除 192
ロケールの削除 193
ロケールの作成 191
ロケールへの追加 192
マニュアルの構成 867, 869
エラー抑制 867
エラー抑制タスクのプロパティ 869

た

タイム ゾーン 701
概要 701
設定 701
ダウンロード 220, 221
ライセンス 220, 221
タスク 33, 34
サポート 33
サポートされていない 34

ち

注意事項 21, 24, 181, 182, 346, 360, 419, 476, 477, 555, 577, 780
延期展開 555
オーバーサブスクリプション 21
サービス プロファイル 577
トラフィック モニタリング 780
ネームド VSAN 360
パスワード 182
ピン接続 24
ファイバ チャネル ゾーン分割 419
分離 L2 ネットワーク 346
ユーザ名 181
ローカル ディスク設定ポリシー 476, 477

つ

追加 248, 702
NTP サーバ 702
ポート チャネルへのポート 248
通信サービス 47, 48, 123, 125, 127, 128, 129, 130, 131, 137, 138, 140, 141, 142, 197
CIM-XML 125
HTTP 125
HTTPS 127, 128, 129, 130, 131
SNMP 137, 138, 140, 141
Telnet 142
Web セッション制限 47, 48, 197
概要 123
設定 142
ツールバー 42

て

ディザスタ リカバリ 749, 753
ディスカバリ ポリシー 207, 210, 212, 213, 490, 491, 492
サーバ 490, 491, 492
シャーシ 207, 210
ラック サーバ 212, 213
ディスク ドライブ モニタリング 799, 800, 801, 802
概要 799
結果の解釈 801, 802
サポート 800
制限事項 800
前提条件 800
ディセーブル化 87, 104, 121, 142, 244, 245, 248, 826, 871
Call Home 826
Core File Exporter 871
uplinkEthernet ポート 245
アップリンク イーサネット ポート チャネル 104
イーサネット ポート 87
サーバ ポート 244
通信サービス 142
ポート 121
ポート チャネル 248
データベース 749, 753
バックアップ 749
復元 753
テーブル 43
カスタマイズ 43
テーブルのカスタマイズ 43
フィルタリング 43
フィルタリング テーブル 43
デフォルトの vhba の動作ポリシー 318, 401, 402
デフォルトの vnic の動作ポリシー 318, 319, 401
デフォルトのサービス プロファイル 17, 576, 618, 619
デフォルトの認証サービス 169

展開の延期 553, 554, 555, 556, 562, 565, 568, 569, 572, 573, 574
1 回のオカレンス 562, 568
繰り返すオカレンス 565, 568
サービス プロファイル 553
スケジュール 554, 556, 569
注意事項 555
保留中のアクティビティ 555, 572, 573, 574
展開 572, 573, 574
表示 572
メンテナンス ポリシー 554, 569
電源オフ 708
シャーシ ロケータ LED 708
電源オン 708
シャーシ ロケータ LED 708
電源管理 687, 690, 691, 693, 694, 695, 696
電力グループ 690, 691, 693, 694
削除 694
作成 691
シャーシの追加 693
シャーシの取り外し 693
電力制御ポリシー 695, 696
削除 696
作成 695
ポリシー 694
電力制御 694
ラック サーバ 687
電源状態、同期化 713, 727
電源投入時自己診断テスト 708, 724, 737, 748
I/O モジュールの表示 748
シャーシの表示 708
ブレード サーバ 724
ラックマウント サーバ 737
電源ポリシー 688
概要 688
設定 688
電源を再投入する 717, 731
ラックマウント サーバ 717, 731
テンプレート 18, 577, 655, 657
サービス プロファイル 18, 577
サービス プロファイルからの作成 657
サービス プロファイルの作成 655
テンプレートの更新 18, 577
テンプレート ベースのサービス プロファイル 656
電力グループ 690, 691, 693, 694
削除 694
作成 691
シャーシの追加 693
電力グループ *(続き)*
シャーシの取り外し 693
電力制御ポリシー 694, 695, 696
削除 696
作成 695
電力制限 690, 696, 698
手動ブレード レベル 696
表示 698
ポリシー方式のシャーシ グループ 690

と

統計情報 808, 810, 812, 814, 815
しきい値ポリシー 808, 810, 812, 814, 815
アップリンク イーサネット ポート 812
イーサネット サーバ ポート 814
サーバおよびサーバ コンポーネント 808, 810, 812
ファイバ チャネル ポート 815
統計情報収集ポリシー 805, 806
概要 805
変更 806
統合型ネットワーク アダプタ 30
仮想化 30
登録、Cisco UCS Central 234, 235, 236
登録、Smart Call Home 839
登録解除、Cisco UCS Central 237
独立 VLAN 271
ドメイン プール 19
ドメイン、分離 L2 345
トラスト ポイント 126, 129, 133
概要 126
削除 133
作成 129
トラップ 134, 138, 140
概要 134
削除 140
作成 138
トラフィック管理 19, 20, 21, 24, 293
Quality of Service 24, 293
オーバーサブスクリプション 19, 20, 21
仮想レーン 24, 293
システム クラス 24, 293
トラフィック モニタリング 779, 780, 781, 783, 784, 785
イーサネット セッション 781
概要 779
セッションのアクティブ化 785

トラフィック モニタリング *(続き)*
セッションの削除 **785**
送信元の追加 **784**
注意事項 **780**
ファイバ チャネル セッション **783**
トランキング **360, 369, 370**
ファイバ チャネル **360, 369, 370**
アップリンク **360, 369, 370**
トランキング、ネームド VSAN **360, 369, 370**

な

名前解決 **174, 205**

に

認証 **143, 144**
primary **143**
リモート **144**
認証サービス **143, 168, 169**
概要 **143**
コンソール **168**
デフォルト **169**
認証ドメイン **166, 167**
概要 **166**
作成 **167**
認証プロファイル **529, 531**
削除 **531**

ね

ネームド VLAN **250, 253, 257, 261, 265**
概要 **257**
削除 **253, 265**
作成 **250, 261**
ネームド VSAN **359, 360, 362, 368, 369, 370**
FCoE VLAN ID **368**
FC アップリンク トランキング **360, 369, 370**
ID の範囲の制限 **360**
概要 **359**
削除 **368**
作成 **362**
ネットワーク **15, 250, 253, 257, 258, 261, 265, 359, 362, 365, 368**
作成 **362, 365**
接続性 **15**
ネットワーク *(続き)*
ネームド VLAN **250, 253, 257, 261, 265**
削除 **253, 265**
作成 **250, 261**
ネームド VSAN **359, 362, 365, 368**
削除 **368**
プライベート VLAN **258**
ネットワーク制御ポリシー **335, 336, 339**
削除 **339**
作成 **336**
ネットワーク、分離 L2 **345**

は

ハードウェア、ステートレス **26**
ハードウェア ベースのサービス プロファイル **618, 619**
ハードウェアベースのサービス プロファイル **17, 576**
ハード リセット **717, 731**
ブレード サーバ **717**
ラックマウント サーバ **731**
ハイ アベイラビリティ **12, 35, 60, 63, 66**
概要 **35**
初期設定 **63, 66**
ファブリック インターコネクトのフェールオーバー **60**
ハイ アベイラビリティの設定 **35**
概要 **35**
ハイブリッド表示 **45**
バインディング **310, 391, 679**
vHBA **391**
vNIC **310**
サービス プロファイル **679**
バインド解除 **311, 392, 679**
vHBA **392**
vNIC **311**
サービス プロファイル **679**
パスワード **196, 201**
強度チェック **196**
変更間隔 **201**
履歴カウント **201**
パスワード、admin の復旧 **771, 772, 774**
パスワード強度の適用 **196**
パスワード、注意事項 **182**
パスワード プロファイル **200, 202, 203**
概要 **200**
パスワード履歴カウント **203**
パスワード履歴のクリア **200**
変更間隔 **202**

パスワード プロファイル *(続き)*
変更なし間隔 **202**
破損した BIOS **723, 736**
バックアップ **749, 750, 751, 752, 753, 758, 759, 843, 846**
概要 **749**
考慮事項 **750**
システム イベント ログ **843, 846**
手動 **846**
スケジュール済み **843**
スケジューリング **751**
すべてのコンフィギュレーションのエクスポート ポリシー **752**
操作の削除 **759**
操作の作成 **753**
操作の実行 **758**
操作の変更 **758**
タイプ **750**
データベース バックアップ ポリシー **752**
ユーザ ロール **753**
バックアップ操作 **753, 758, 759**
削除 **759**
作成 **753**
実行 **758**
変更 **758**
バナー **48, 49, 50**
プリログイン **48, 49, 50**
範囲、許容 **53**
範囲の制限、VSAN ID **360**
番号の付け替え **707, 733**
シャーシ **707**
ブレード サーバ **707**
ラックマウント サーバ **733**

ひ

ビーコン **708, 721, 735**
シャーシ **708**
ブレード サーバ **721**
ラックマウント サーバ **735**
ビーコン LED **76, 83**
表示 **698, 842, 856, 858, 860, 864, 867, 869**
fex のエラー抑制プロパティ **860**
iom のエラー抑制プロパティ **858**
サーバのエラー抑制プロパティ **864**
サービス プロファイルのエラー抑制プロパティ **867**
システム イベント ログ **842**
表示 *(続き)*
シャーシのエラー抑制プロパティ **856**
組織のエラー抑制プロパティ **869**
ブレード レベルの電力制限 **698**
表示機能拡張 **53**
ピン グループ **22, 249, 250, 285, 286, 287, 371, 372**
LAN **249, 250, 285, 286, 287**
SAN **371, 372**
概要 **22**
ピン接続 **22, 24, 348**
概要 **22**
サーバからサーバ ポートへ **22**
注意事項 **24**
分離 L2 ネットワーク **348**

ふ

ファームウェア **772**
ファブリック インターコネクト **772**
ファイバ チャネル **13, 14, 70, 74, 80, 81, 83, 95, 96, 110, 112, 113, 114**
over Ethernet **13**
アップリンク ポート **74**
スイッチング モード **70**
ストレージ ポート **95, 96**
ビーコン LED **83**
プライオリティ フロー制御 **14**
ポート チャネル **110, 112, 113, 114**
削除 **114**
ディセーブル化 **112**
変更 **113**
ポートの削除 **112**
ポートの追加 **112**
ポート モード **80, 81**
リンクレベル フロー制御 **14**
ファイバ チャネル アダプタ ポリシー **312, 393, 395, 400**
概要 **312, 393**
削除 **400**
作成 **395**
ファイバ チャネル システム クラス **25, 294**
ファイバ チャネル スイッチング モード **69**
概要 **69**
ファイバ チャネル ゾーン分割 **416, 417, 418, 419, 421, 424, 426**
Cisco UCS Manager ベース **417**
VSAN の作成 **421**
アクティブ ゾーン セットの設定 **418**
サポート **416**
スイッチベース **418**

ファイバ チャネル ゾーン分割 *(続き)*
ストレージ接続ポリシー 418, 424, 426
設定 419
注意事項 419
ファブリック 117
ポート チャネル 117
ファブリック インターコネクト 35, 59, 60, 61, 63, 66, 67, 68, 69, 70, 71, 72, 86, 87, 88, 217, 219, 223, 224, 226, 228, 360, 369, 370, 769, 771, 772, 774, 787
admin パスワードの復旧 771, 772, 774
FC アップリンク トランキング 360, 369, 370
イーサネット スイッチング モード 68
イーサネット ポートのイネーブル化 86
イーサネット ポートのディセーブル化 87
クラスタ用のスタンドアロンのイネーブル 67
システム設定タイプ 60
初期設定 59, 60, 61, 63, 66
概要 59
管理ポート 61
スタンドアロン 61
セットアップ モード 60
第 1 63
第 2 66
設定の復元 769
ハイ アベイラビリティ 35
ファームウェアの確認 772
ファイバ チャネル スイッチング モード 69
フェールオーバー 60
変更 71
Virtual IP Address（仮想 IP アドレス） 71
サブネット 71
ポート 226
猶予期間 226
ポートの設定解除 88
ポートの変更 86
ホスト ID 219
モード 69, 70
モニタリング 787
ライセンス 217, 223, 224, 226, 228
インストール 223
クリア 228
表示 224
有効期限 228
猶予期間 226
リーダーシップ ロールの決定 72, 772
ファブリック フェールオーバー 336
ファブリック ポート 119
ポート チャネル 119
メンバ ポート、削除 119
ファブリック ポート チャネル 119
表示 119
メンバ ポート 119
削除 119
フィールド、許容範囲 53
ブート 519, 520, 548, 549, 550, 714, 715, 728, 729
LAN 548
SAN 519, 520
仮想メディア 550
サービス プロファイルからのサーバ 714, 728
ブート順序の決定 715, 729
ブレード サーバ 714
ラックマウント サーバ 728
ローカル ディスク 549
ブート オプション、BIOS 設定 462
ブート順 535, 540, 715, 729
設定 535
ブレード サーバ 715
変更 540
ラックマウント サーバ 729
ブート順序、変更 663
ブート パラメータ 535, 540
iSCSI ブート 535, 540
設定 535
変更 540
ブート プロセス 523
iSCSI 523
ブート ポリシー 517, 518, 519, 520, 548, 549, 550, 552
LAN ブート 548
SAN ブート 519, 520
概要 517
仮想メディア ブート 550
削除 552
作成 518
ローカル ディスク ブート 549
プール 19, 54, 289, 290, 291, 373, 374, 379, 384, 429, 430, 431, 432, 434, 435, 438, 444, 445, 446, 531, 544, 547
IP 434, 435, 438
IQN 544, 547
iSCSI イニシエータの IP 531
MAC 289, 290, 291
UUID 接尾辞 432, 434
WWN 373
WWNN 374
WWPN 379

プール (続き)
WWxN 384
概要 19
管理 IP 444, 445, 446
グローバル 19
サーバ 429, 430, 431, 432
使用場所 54
ドメイン 19
プールの使用状況の確認 54
復元 753, 763, 769
インポート操作 763
概要 753
設定 769
ユーザ ロール 753
プライオリティ フロー制御 14
プライベート VLAN 258, 266, 271
概要 258
セカンダリの作成 271
プライマリの作成 266
プライマリ VLAN 266
プライマリ認証 144, 148, 154, 157, 159, 160, 162, 168, 169
LDAP プロバイダー 148, 154
RADIUS プロバイダー 157, 159
TACACS+ プロバイダー 160
TACACS プロバイダー 162
コンソールの選択 168
デフォルトの選択 169
リモート 144
プラチナ システム クラス 25, 294
プリログイン バナー 48, 49, 50
削除 50
作成 48
変更 49
ブレード 698
電力制限の表示 698
ブレード サーバ 618, 656, 712, 713, 714, 715, 717, 719, 720, 721, 722, 723, 724, 727, 790
BIOS の回復 723
NMI の発行 724
POST の結果 724
稼働中止 719
管理 712, 714
再確認 717
削除 720
データベースから 720
シャットダウン 715
電源の再投入 717
ブレード サーバ (続き)
テンプレート ベースのサービス プロファイル 656
ハードウェア ベースのサービス プロファイル 618
ブート順序の決定 715
モニタリング 790
予期しない電源変更 713, 727
リセット 721, 722
CIMC 722
CMOS 721
ロケータ LED 721
ブレード レベルの電力制限 697
サーバ用の設定 697
フロー制御 14
プライオリティ 14
リンク レベル 14
フロー制御ポリシー 26, 85, 301, 303
アップリンク イーサネット ポート 85
概要 26, 301
削除 303
作成 301
プロセッサ、BIOS 設定 450
プロバイダー 148, 154, 157, 159, 160, 162
LDAP 148, 154
作成 148
RADIUS 157, 159
TACACS 162
TACACS+ 160
プロバイダー グループ 163, 164, 165, 166, 167
LDAP 163, 164
削除 164
作成 163
RADIUS 164, 165
削除 165
作成 164
TACACS+ 165, 166
削除 166
作成 165
認証ドメイン 166, 167
プロパティ 50, 51, 52, 53, 71
外部アプリケーション 52
確認メッセージ 51
セッション 50
表示機能拡張 53
ファブリック インターコネクト 71
プロファイル 14, 200, 828, 829
Call Home アラート グループ 828, 829
パスワード 200

分離 L2 ネットワーク 345, 346, 348, 349, 353, 355, 356
VLAN 353, 355, 356
ポートおよびポート チャネルの削除 355
ポートおよびポート チャネルの割り当て 353
ポートおよびポートチャネルの割り当ての表示 356
概要 345
設定 349
注意事項 346
ピン接続に関する注意事項 348

へ

ペイン 39, 42
Work 42
ナビゲーション 39
ベスト エフォート システム クラス 25, 294
変更 50, 86
プロパティ 50
ポート 86

ほ

ポート 22, 61, 74, 75, 77, 80, 81, 83, 84, 85, 86, 88, 89, 92, 94, 95, 96, 101, 102, 110, 114, 115, 116, 117, 119, 120, 121, 217, 243, 244, 245, 246, 249, 250, 275, 285, 286, 287, 336, 351, 353, 355, 356, 371, 372, 812, 814, 815
FCoE アップリンク 96
概要 96
FCoE ストレージ ポート 94
MAC セキュリティ 336
VLAN、数 275
VLAN からの削除 355
VLAN への割り当て 351, 353
VLAN 割り当ての表示 356
アップリンク 74
アップリンク イーサネット 84, 243, 812
アップリンク イーサネットの変更 85
アプライアンス 89
アプライアンス、NAS 74
アプライアンス ポート 89, 92
イーサネット サーバ ポート 814
イネーブル化 243, 245
管理 61
サーバ 74, 84, 120, 121, 243
サーバ トラフィックのピン接続 22
設定解除 88, 244, 246
ポート *(続き)*
ディセーブル化 244, 245
ビーコン LED 83
ピン グループ 249, 250, 285, 286, 287, 371, 372
ファイバ チャネル ストレージ ポート 95, 96
ファイバ チャネル ポート 815
ファブリック インターコネクト 74
ファブリック ポート チャネル 119
メンバ ポート、削除 119
変更 86
ポート チャネル 102, 110, 114, 115, 116, 117
FCoE 114
ファイバ チャネル 110
ポートの設定解除 101
モード 80, 81
ユニファイド 75, 77
ライセンス 217
ポート{ユニファイド アップリンク ポート チャネル 115
ポート チャネル 102, 110, 114, 115, 116, 117
ポート タイプ 75
ポート チャネル 102, 103, 104, 105, 108, 109, 110, 112, 113, 114, 115, 116, 117, 119, 246, 247, 248, 249, 351, 353, 355, 356
FCoE 114, 115
削除 115
作成 114
VLAN からの削除 355
VLAN への割り当て 351, 353
VLAN 割り当ての表示 356
アダプタ 116
アップリンク イーサネット 102, 103
イネーブル化 103
作成 102
アプライアンス 105, 108, 109, 110
イネーブル化 108
削除 110
作成 105
ディセーブル化 109
ポートの削除 109
ポートの追加 109
イーサネット 104, 105
削除 105
ディセーブル化 104
ポートの削除 104
ポートの追加 104
イネーブル化 247
削除 249
作成 246

ポート チャネル *(続き)*
ディセーブル化 **248**
ファイバ チャネル **110, 112, 113, 114**
削除 **114**
作成 **110, 112**
ディセーブル化 **112**
変更 **113**
ポートの削除 **112**
ポートの追加 **112**
ファブリック **117, 119**
ポートの削除 **249**
ポートの追加 **248**
ユニファイド アップリンク ポート **115**
ポート チャネル モードのケーブル接続の問題 **117**
概要 **117**
ポートの設定 **78**
FCoE アップリンク ポート **78**
注意 **78**
ポートの設定解除 **88, 244, 246**
ポート モード **75, 79**
概要 **75**
データ トラフィックへの影響 **79**
ホスト ID、入手方法 **219**
ホスト ポート チャネル **116**
表示 **116**
ポリシー **18, 25, 26, 54, 171, 207, 210, 212, 213, 234, 235, 236, 237, 297, 298, 300, 301, 303, 305, 312, 320, 321, 328, 332, 333, 334, 335, 336, 339, 389, 393, 402, 403, 404, 408, 411, 412, 413, 414, 418, 424, 426, 469, 470, 473, 474, 475, 479, 483, 484, 485, 486, 488, 490, 491, 492, 494, 495, 496, 497, 502, 517, 518, 527, 529, 532, 552, 554, 569, 688, 689, 694, 695, 696, 751, 752, 796, 797, 805, 806, 808, 810, 812, 833, 834, 835, 843, 849, 850**
BIOS **469, 470**
Call Home **833, 834, 835**
Cisco UCS Central からの登録解除 **237**
Cisco UCS Central への登録 **235**
IPMI アクセス **473, 474**
iSCSI アダプタ **527, 529**
iSCSI ブート **532**
LAN 接続 **320, 321, 328, 332, 333, 334, 335, 402, 403**
PSU **688**
QoS **25, 297, 298, 300**
SAN 接続 **320, 321, 402, 403, 404, 408, 411, 412, 413, 414**
SEL **843**
Serial over LAN **486, 488**
概要 **486**
削除 **488**
作成 **486**
vHBA **389**
ポリシー *(続き)*
vHBA テンプレート **393**
vNIC **305**
vNIC/vHBA 配置 **502**
イーサネット **312, 393**
解決 **234, 236**
概要 **18**
管理インターフェイスのモニタリング **796, 797**
グローバル キャップ **689**
グローバル キャップ ポリシー **689**
サーバ継承 **492, 494**
概要 **492**
削除 **494**
作成 **492**
サーバ ディスカバリ **490, 491, 492**
サーバ プール **494, 495**
サーバ プールの資格情報 **496, 497, 502**
しきい値 **808, 810, 812**
自動設定 **488, 490**
シャーシ ディスカバリ **207, 210**
障害収集 **849, 850**
使用場所 **54**
スクラブ **484, 485, 486**
ストレージ接続 **418, 424, 426**
すべてのコンフィギュレーションのエクスポート **752**
データベースのバックアップ **751, 752**
電源 **688**
電力制御 **694, 695, 696**
統計情報収集 **805, 806**
ネットワーク制御 **335, 336, 339**
ファイバ チャネル アダプタ **312, 393**
ブート **517, 518, 552**
フロー制御 **26, 301, 303**
メンテナンス **554, 569**
ラック サーバ ディスカバリ **212, 213**
リモート ユーザのロール **171**
ローカル ディスク設定 **475, 479, 483, 484**
ポリシーの使用状況の確認 **54**
ポリシー方式のシャーシ グループの電力制限 **690**
保留中のアクティビティ **555, 572, 573, 574**
概要 **555**
展開 **572, 573, 574**
表示 **572**

ま

マルチテナント 28, 29, 173, 174, 176, 177
オプトアウト 29
オプトイン 28
概要 28
組織 173, 176, 177
削除 177
作成 176
名前解決 174
マルチ認証システム 162

め

明示的な割り当て 505, 512, 513
メッセージ、システム インベントリ 827, 828, 838
メンテナンス ポリシー 554, 556, 569, 571
概要 554
削除 571
作成 569
スケジュール 556, 569

も

モード 60, 68, 69, 70, 242
イーサネット スイッチング 68
end-host 68, 69, 70, 242
スイッチング 69, 70, 242
セットアップ 60
ファイバ チャネル スイッチング 69
モニタリング 203, 787, 788, 790, 793, 796, 799, 800, 801, 802
I/O モジュール 796
シャーシ 788
ディスク ドライブ 799, 800, 801, 802
ファブリック インターコネクト 787
ブレード サーバ 790
ユーザ セッション 203
ラックマウント サーバ 793
モビリティ 26

ゆ

有効期限、アカウント 180
ユーザ 47, 48, 140, 141, 143, 144, 171, 179, 180, 181, 182, 183, 184, 185, 188, 189, 190, 191, 192, 193, 196, 197, 198, 199, 200, 202, 203, 771, 772, 774
admin パスワードの復旧 771, 772, 774
SNMPv3 140, 141
Web セッション制限 47, 48, 183, 197
アカウント 180, 182
アカウントのイネーブル化 199
アカウントの作成 193
アカウントのディセーブル化 199
アクセス コントロール 179
権限 185
権限の削除 190
権限の追加 190
セッションのモニタリング 203
注意事項 181
デフォルト ロール 184
認証 143
パスワード強度チェック 196
リモート認証 144
リモート認証された 180
リモート、ロール ポリシー 171
ローカル アカウントの削除 200
ローカル認証された 180, 200, 202, 203
ロール 183, 198
変更 198
ロールの削除 190
ロールの作成 189
ロケール 188, 191, 192, 193, 197
概要 188
削除 193
作成 191
組織の削除 192
組織の追加 192
変更 197
ユーザ アカウント 180, 181, 182, 183, 193, 197, 199, 200, 202, 203
Web セッション制限 183
イネーブル化 199
概要 180, 182
削除 200
作成 193
ディセーブル化 199
パスワード プロファイル 200, 202, 203
ユーザ名の注意事項 181
ロケールの変更 197
ユーザ アカウントのアクティブ化 199
ユーザ アカウントの非アクティブ化 199

ユーザ属性 144
LDAP 144
RADIUS 144
TACACS+ 144
ユーザ名、注意事項 181
ユーザ ロール 183, 184, 185, 189, 190
概要 183
権限 185
権限の削除 190
権限の追加 190
削除 190
作成 189
デフォルト 184
ユニファイド アップリンク ポート 115
ポート チャネル 115
ユニファイド接続 97
概要 97
ユニファイド ファブリック 13
概要 13
ファイバ チャネル 13
ユニファイド ポート 75, 77, 79, 80, 81, 83
注意事項 77
ビーコン LED 83
ポート 77
ユニファイド 77
注意事項 77
ポート タイプ 75
ポート モード 75, 79
モードの設定 80, 81

よ

予期しない電源変更、回避 713, 727
抑制されたエラーの表示 853
予約語 181, 185
カスタム ロール 185
ローカル認証されたユーザのアカウント 181

ら

ライセンス 217, 219, 220, 221, 223, 224, 226, 228
アンインストール 228
インストール 223
概要 217
クリア 228
取得 219
ライセンス *(続き)*
ダウンロード 220, 221
表示 224
ホスト ID の入手方法 219
有効期限 228
猶予期間 226
ライセンスのクリア 228
ライフサイクル、障害 849
ラック サーバ ディスカバリ ポリシー 212, 213
概要 212
設定 213
ラック サーバの電源管理 687
ラックマウント サーバ 212, 213, 577, 619, 656, 726, 728, 729, 730, 731, 732, 734, 735, 736, 737, 793
BIOS の回復 736
NMI の発行 737
POST の結果 737
稼働中止 732
管理 726
サービス プロファイルに関する注意事項 577
再確認 732
削除 734
データベースから 734
シャットダウン 730
ディスカバリ ポリシー 212, 213
電源の再投入 731
テンプレート ベースのサービス プロファイル 656
ハードウェア ベースのサービス プロファイル 619
ブート 728
ブート順序の決定 729
モニタリング 793
リセット 735
CIMC 735
CMOS 735
ロケータ LED 735
ラックマウント サーバの稼働中止 726
ラックマウント サーバの削除 726

り

リセット 717, 721, 722, 731, 735, 747
CIMC 722, 735
ブレード サーバ 722
ラックマウント サーバ 735
CMOS 721, 735
IOM 747
ブレード サーバ 717

リセット *(続き)*
ラックマウント サーバ 731
リブート 717, 731
ブレード サーバ 717
ラックマウント サーバ 731
リモート認証 144
ユーザ アカウント 144
ユーザ ロール 144
リモート認証されたユーザ 180
アカウント 180
リモート ユーザのロール ポリシー 171
概要 171
設定 171
領域、Fault Summary 38
履歴、パスワード 201
リンク レベル フロー制御 14

る

ルート組織 176

れ

レーン、仮想 24, 293

ろ

ローカル ディスク設定ポリシー 475, 476, 477, 479, 483, 484
RAID 設定 477
概要 475
削除 484
作成 479
注意事項 476
変更 483
ローカル ディスク ブート 549
概要 549
設定 549
ローカル認証されたユーザ 180, 181, 193, 199, 200, 202, 203
アカウント 180
ローカル認証されたユーザ *(続き)*
アカウントの予約語 181
イネーブル化 199
削除 200
作成 193
ディセーブル化 199
パスワード プロファイル 200
パスワード履歴カウント 203
パスワード履歴のクリア 200
変更間隔 202
変更なし間隔 202
ロール 183, 184, 185, 189, 190, 198, 753
概要 183
権限 185
権限の削除 190
権限の追加 190
削除 190
作成 189
デフォルト 184
バックアップ 753
ユーザの変更 198
ロールベース アクセス コントロール 179
ログ 50, 843
Cisco UCS Manager GUI 50
システム イベント 843
ログアウト 47
ログイン 45, 46, 48, 49, 50
HTTP 46
HTTPS 45
バナー 48, 49, 50
ログ、システム 871
ログ、システム イベント 841
概要 841
ロケール 188, 191, 192, 193, 197
概要 188
削除 193
作成 191
組織の削除 192
組織の割り当て 192
ユーザの変更 197