Cisco UCS Mini 向け Cisco UCS Manager GUI ユーザ ガイド、リリース 3.0

初版：2014 年 07 月 14 日

最終更新：2014 年 07 月 23 日

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

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）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。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号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、ネットワーク トポロジ図、およびその他の図は、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および電話番号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。

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)

© 2014 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xxxi

対象読者 xxxi

表記法 xxxi

Cisco UCS の関連ドキュメント xxxiii

マニュアルに関するフィードバック xxxiii

Cisco Unified Computing System の概要 1

Cisco Unified Computing System について 1

ユニファイド ファブリック 3

Fibre Channel over Ethernet 3

リンクレベル フロー制御 4

プライオリティ フロー制御 4

IPv6 への準拠 4

サーバのアーキテクチャおよび接続性 6

サービス プロファイルの概要 6

サービス プロファイルによるネットワーク接続 7

サービス プロファイルによる設定 7

サーバ ID を上書きするサービス プロファイル 9

サーバ ID を継承するサービス プロファイル 9

サービス プロファイル テンプレート 10

ポリシー 11

Pools 11

CIMC インバンド管理 12

インバンド管理サポート 13

トラフィック管理 13

オーバーサブスクリプション 13

オーバーサブスクリプションにおける検討事項 14

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 14
ピン接続 15
サーバ トラフィックのサーバ ポートへのピン接続 15
ピン接続に関するガイドライン 15
Quality of Service 15
システム クラス 16
Quality of Service ポリシー 17
フロー制御ポリシー 18
オプトイン機能 18
ステートレス コンピューティング 18
マルチテナント機能 20
Cisco UCS でのバーチャライゼーション 21
バーチャライゼーションの概要 21
Cisco Virtual Machine ファブリック エクステンダの概要 21
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バーチャライゼーション 22
仮想インターフェイス カード アダプタでのバーチャライゼーション 22
Cisco UCS Manager の概要 23
Cisco UCS Manager の概要 23
Cisco UCS Manager で実行可能なタスク 25
Cisco UCS Manager で実行できないタスク 26
ハイ アベイラビリティ環境の Cisco UCS Manager 27
Cisco UCS Manager GUI の概要 29
Cisco UCS Manager GUI の概要 29
[Fault Summary] 領域 30
[Navigation] ペイン 31
ツールバー 34
[Work] ペイン 34
ステータスバー 34
テーブルのカスタマイズ 35
LAN アップリンク マネージャ 36
Internal Fabric Manager 36
ハイブリッド表示 37

HTTPS を使用した Cisco UCS Manager GUI へのログイン 37
HTTP を使用した Cisco UCS Manager GUI へのログイン 38
Cisco UCS Manager GUI からのログアウト 39
Web セッション制限 39
Cisco UCS Manager の Web セッション制限の設定 40
ログイン前バナー 40
ログイン前バナーの作成 40
ログイン前バナーの変更 41
ログイン前バナーの削除 42
Cisco UCS Manager GUI のプロパティ 42
Cisco UCS Manager GUI のセッションおよびログのプロパティの設定 42
確認メッセージのプロパティの設定 42
外部アプリケーションのプロパティの設定 43
Cisco UCS Manager GUI の表示のカスタマイズ 43
フィールド値の許容範囲の決定 44
ポリシーの使用場所の決定 44
プールの使用場所の決定 44
プール、ポリシー、その他のオブジェクトの削除 45
XML のコピー 45
ファブリック インターコネクトの設定 47
Initial System Setup 47
セットアップ モード 48
システム設定タイプ 48
管理ポートの IP アドレス 49
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 49
クラスタ設定の初期システム セットアップ 52
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 52
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 55
ファブリック インターコネクトへのアウトオブバンド IPv4 アドレスの追加 56
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 57
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 58

ポートおよびポート チャネルの設定 59
Cisco UCS 6324 ファブリック インターコネクト のユニファイド ポート 60
ポート モード 60
ポート タイプ 60
Cisco UCS Mini スケーラビリティ ポート 61
スケーラビリティ ポートの設定 61
ユニファイド ポートの設定に関するガイドライン 62
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 ポートに関する注意およびガイドライン 62
ポート モードの変更のデータ トラフィックへの影響 63
6324 ファブリック インターコネクトのポート モードの設定 64
サーバ ポート 65
サーバ ポートの設定 65
アップリンク イーサネット ポート 65
アップリンク イーサネット ポートの設定 65
アップリンク イーサネット ポートのプロパティの変更 66
ファブリック インターコネクトのポートの再設定 67
ファブリック インターコネクトのポートのイネーブル化またはディセーブル化 67
ファブリック インターコネクトのポート設定解除 68
アプライアンス ポート 68
アプライアンス ポートの設定 69
アプライアンス ポートのプロパティの変更 70
FCoE およびファイバ チャネル ストレージ ポート 71
FCoE ストレージ ポートの設定 71
アップリンク ファイバ チャネル ポートの復元 71
FCoE アップリンク ポート 72
FCoE アップリンク ポートの設定 73
ユニファイド アップリンク ポート 73
ユニファイド アップリンク ポートの設定 74
ユニファイド アップリンク ポートの設定解除 74
アップリンク イーサネット ポート チャネル 75
アップリンク イーサネット ポート チャネルの作成 76

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 76
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 77
アップリンク イーサネット ポート チャネルのポートの追加および削除 77
アップリンク イーサネット ポート チャネルの削除 78
アプライアンス ポート チャネル 78
アプライアンス ポート チャネルの作成 78
アプライアンス ポート チャネルのイネーブル化 79
アプライアンス ポート チャネルのディセーブル化 79
アプライアンス ポート チャネルのポートの追加および削除 80
アプライアンス ポート チャネルの削除 80
ファイバ チャネル ポート チャネル 80
ファイバ チャネル ポート チャネルの作成 81
ファイバ チャネル ポート チャネルのイネーブル化 81
ファイバ チャネル ポート チャネルのディセーブル化 82
ファイバ チャネル ポート チャネルのポートの追加および削除 82
ファイバ チャネル ポート チャネルのプロパティの変更 83
ファイバ チャネル ポート チャネルの削除 84
FCoE ポート チャネル 84
FCoE ポート チャネルの作成 84
FCoE ポート チャネルの削除 85
ユニファイド アップリンク ポート チャネル 85
アダプタ ポート チャネル 86
アダプタ ポート チャネルの表示 86
Internal Fabric Manager を使用したサーバ ポートの設定 86
Internal Fabric Manager 86
Internal Fabric Manager の起動 87
Internal Fabric Manager を使用したサーバ ポートの設定 87
Internal Fabric Manager を使用したサーバ ポートの設定解除 87
Internal Fabric Manager を使用したサーバ ポートのイネーブル化 88
Internal Fabric Manager を使用したサーバ ポートのディセーブル化 88
ライセンスの管理 89
ライセンス 89

ファブリック インターコネクトのホスト ID の入手方法 90
ライセンスの取得 90
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 91
リモート ロケーションからファブリック インターコネクトへのライセンスのダウンロード 92
ライセンスのインストール 93
ファブリック インターコネクトにインストールされているライセンスの表示 94
ポートまたは機能に使用できる猶予期間の決定 95
ライセンスの失効日の決定 95
ライセンスのアンインストール 95
コミュニケーション サービスの設定 97
Communication Services 97
CIM-XML の設定 99
HTTP の設定 100
HTTPS の設定 100
証明書、キー リング、トラスト ポイント 100
キー リングの作成 101
キー リングの証明書要求の作成 102
トラスト ポイントの作成 104
キー リングへの証明書のインポート 105
HTTPS の設定 106
キーリングの削除 107
トラスト ポイントの削除 108
SNMP の設定 108
SNMP に関する情報 108
SNMP 機能の概要 108
SNMP 通知 109
SNMP セキュリティ レベルおよび権限 109
SNMP セキュリティ モデルとレベルのサポートされている組み合わせ 110
SNMPv3 セキュリティ機能 111
SNMP サポート： Cisco UCS 111

SNMP のイネーブル化および SNMP プロパティの設定 112
SNMP トラップの作成 113
SNMP トラップの削除 115
SNMPv3 ユーザの作成 115
SNMPv3 ユーザの削除 116
Telnet のイネーブル化 117
CIMC Web サービスのイネーブル化 117
通信サービスのディセーブル化 117
「Configuring Authentication」 119
認証サービス 119
リモート認証プロバイダーに関するガイドラインおよび推奨事項 120
リモート認証プロバイダーにおけるユーザ属性 120
二要素認証 122
LDAP グループ ルール 124
ネストされた LDAP グループ 124
LDAP プロバイダーの設定 124
LDAP プロバイダーのプロパティの設定 124
LDAP プロバイダーの作成 125
LDAP プロバイダーの LDAP グループ ルールの変更 126
LDAP プロバイダーの削除 128
LDAP グループ マッピング 128
LDAP グループ マップの作成 129
LDAP グループ マップの削除 130
RADIUS プロバイダーの設定 130
RADIUS プロバイダーのプロパティの設定 130
RADIUS プロバイダーの作成 130
RADIUS プロバイダーの削除 132
TACACS+ プロバイダーの設定 132
TACACS+ プロバイダーのプロパティの設定 132
TACACS+ プロバイダーの作成 132
TACACS+ プロバイダーの削除 134
マルチ認証システムの設定 134

マルチ認証システム 134

プロバイダー グループ 134

LDAP プロバイダー グループの作成 134

LDAP プロバイダー グループの削除 135

RADIUS プロバイダー グループの作成 136

RADIUS プロバイダー グループの削除 136

TACACS+ プロバイダー グループの作成 137

TACACS+ プロバイダー グループの削除 137

認証ドメイン 138

認証ドメインの作成 138

プライマリ認証サービスの選択 141

コンソール認証サービスの選択 141

デフォルト認証サービスの選択 142

リモート ユーザのロール ポリシー 144

リモート ユーザのロール ポリシーの設定 145

組織の設定 147

マルチテナント環境の組織 147

マルチテナント環境における階層的な名前解決 148

ルート組織下の組織の作成 150

サブ組織下の組織の作成 150

組織の削除 151

ロールベース アクセス コントロールの設定 153

ロールベース アクセス コントロール 153

Cisco UCS のユーザ アカウント 154

Cisco UCS ユーザ名に関するガイドライン 155

予約語：ローカル認証されたユーザ アカウント 155

Cisco UCS パスワードに関するガイドライン 156

ユーザ アカウントの Web セッション制限 157

ユーザ ロール 157

デフォルト ユーザ ロール 158

予約語：ユーザ ロール 159

権限 159

ユーザ ロケール 162
ユーザ ロールの設定 163
ユーザ ロールの作成 163
ユーザ ロールへの権限の追加 164
ユーザ ロールからの権限の削除 164
ユーザ ロールの削除 164
ロケールの設定 165
ロケールの作成 165
ロケールへの組織の割り当て 166
ロケールからの組織の削除 166
ロケールの削除 167
ローカル認証されたユーザ アカウントの設定 167
ユーザ アカウントの作成 167
ローカル認証されたユーザへのパスワード強度チェックのイネーブル化 170
Cisco UCS Manager GUIユーザの Web セッション制限の設定 171
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 172
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 172
ユーザ アカウントの有効化 173
ユーザ アカウントの無効化 173
ローカル認証されたユーザのパスワード履歴のクリア 174
ローカルに認証されたユーザ アカウントの削除 174
ローカル認証されたユーザのパスワード プロファイル 175
変更間隔のパスワード変更の最大数の設定 176
パスワードの変更禁止間隔の設定 177
パスワード履歴カウントの設定 177
ユーザ セッションのモニタリング 178
DNS サーバの設定 181
Cisco UCS の DNS サーバ 181
DNS サーバの追加 182
DNS サーバの削除 182
システム関連ポリシーの設定 183
ラック サーバ ディスカバリ ポリシーの設定 183

ラック サーバ ディスカバリ ポリシー 183
ラック サーバ ディスカバリ ポリシーの設定 184
MAC アドレス テーブルのエージング タイムの設定 184
MAC アドレス テーブルのエージング タイム 184
MAC アドレス テーブルのエージング タイムの設定 185
仮想インターフェイスの管理 187
仮想インターフェイス 187
仮想インターフェイスの予約管理とエラー処理 188
Cisco UCS Central への Cisco UCS ドメインの登録 189
Cisco UCS ドメインの登録 189
Cisco UCS Manager と Cisco UCS Central 間のポリシー解決 190
Cisco UCS Central への Cisco UCS ドメインの登録 191
Cisco UCS Manager GUI を使用した Cisco UCS Manager と Cisco UCS Central 間のポリシー解決の変更 192
Cisco UCS Central からの Cisco UCS ドメインの登録解除 193
LAN アップリンク マネージャの使用 195
LAN アップリンク マネージャ 195
LAN アップリンク マネージャの起動 196
LAN アップリンク マネージャでのポートの設定 196
サーバ ポートの設定 197
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 197
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 197
アップリンク イーサネット ポートの設定 197
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 197
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 198
アップリンク イーサネット ポート チャネルの設定 199
LAN アップリンク マネージャでのポート チャネルの作成 199
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 199
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 200
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 200

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 201
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 201
LAN ピン グループの設定 201
LAN アップリンク マネージャでのピン グループの作成 201
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 202
ネームド VLAN の設定 203
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 203
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 203
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 204
VLAN の設定 207
ネームド VLAN 207
VLAN ポートの制限 208
ネームド VLAN の設定 210
ネームド VLAN の作成 210
ネームド VLANの削除 211
VLAN ポート数の表示 212
VLAN グループ 213
VLAN グループの作成 213
VLAN グループのメンバーの編集 214
VLAN グループに対する組織のアクセス権限の変更 214
VLAN グループの削除 215
VLAN 権限 215
VLAN 権限のイネーブル化 216
VLAN 権限のディセーブル化 216
VLAN 権限の追加または変更 217
LAN ピン グループの設定 219
LAN ピン グループ 219
LAN ピン グループの作成 220
LAN ピン グループの削除 221
MAC プールの設定 223
MAC プール 223
MAC プールの作成 224

MAC プールの削除 225
Quality of Service の設定 227
Quality of Service 227
システム クラスの設定 228
システム クラス 228
QoS システム クラスの設定 229
QoS システム クラスのイネーブル化 229
QoS システム クラスのディセーブル化 230
Quality of Service ポリシーの設定 230
Quality of Service ポリシー 230
QoS ポリシーの作成 231
QoS ポリシーの削除 231
フロー制御ポリシーの設定 232
フロー制御ポリシー 232
フロー制御ポリシーの作成 232
フロー制御ポリシーの削除 233
ネットワーク関連ポリシーの設定 235
vNIC テンプレートの設定 235
vNIC テンプレート 235
vNIC テンプレートの作成 236
vNIC テンプレートへの vNIC のバインディング 240
vNIC テンプレートからの vNIC のバインド解除 241
vNIC テンプレートの削除 241
イーサネット アダプタ ポリシーの設定 241
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 241
イーサネット アダプタ ポリシーの作成 243
Linux オペレーティング システムで MRQS 用の eNIC サポートをイネーブル化するためのイーサネット アダプタ ポリシーの設定 247
イーサネット アダプタ ポリシーの削除 248
デフォルトの vNIC 動作ポリシーの設定 248
デフォルトの vNIC 動作ポリシー 248
デフォルトの vNIC 動作ポリシーの設定 249

LAN 接続ポリシーの設定 249
LAN および SAN 接続ポリシー 249
LAN および SAN の接続ポリシーに必要な権限 250
サービス プロファイルと接続ポリシー間の相互作用 250
LAN 接続ポリシーの作成 251
LAN 接続ポリシー用の vNIC の作成 254
LAN 接続ポリシーからの vNIC の削除 254
LAN 接続ポリシー用の iSCSI vNIC の作成 255
LAN 接続ポリシーからの iSCSI vNIC の削除 256
LAN 接続ポリシーの削除 257
ネットワーク制御ポリシーの設定 257
ネットワーク制御ポリシー 257
ネットワーク制御ポリシーの作成 258
ネットワーク制御ポリシーの削除 259
マルチキャスト ポリシーの設定 259
マルチキャスト ポリシー 259
マルチキャスト ポリシーの作成 260
マルチキャスト ポリシーの変更 260
マルチキャスト ポリシーの削除 261
LACP ポリシーの設定 261
LACP ポリシー 261
LACP ポリシーの作成 262
LACP ポリシーの変更 262
UDLD リンク ポリシーの設定 263
UDLD の概要 263
UDLD 設定時の注意事項 265
リンク プロファイルの作成 265
UDLD リンク ポリシーの作成 266
UDLD システム設定の変更 266
リンク プロファイルのポート チャネル イーサネット インターフェイスへの割り当て 267

リンク プロファイルのアップリンク イーサネット インターフェイスへの割り当て 267
リンク プロファイルのポート チャネル FCoE インターフェイスへの割り当て 268
リンク プロファイルのアップリンク FCoE インターフェイスへの割り当て 268
VMQ 接続ポリシーの設定 268
VMQ 接続ポリシー 268
VMQ 接続ポリシーの作成 269
vNIC への仮想化プリファレンスの割り当て 270
アップストリーム分離レイヤ 2 ネットワークの設定 271
アップストリーム分離レイヤ 2 ネットワーク 271
アップストリーム分離 L2 ネットワークの設定に関するガイドライン 272
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考慮事項 274
アップストリーム分離 L2 ネットワークに関する Cisco UCS の設定 276
アップストリーム分離 L2 ネットワークに VLAN を作成 277
VLAN へのポートおよびポート チャネルの割り当て 278
VLAN からのポートおよびポート チャネルの削除 279
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 280
ネームド VSAN の設定 283
ネームド VSAN 283
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 284
VSAN に関するガイドラインおよび推奨事項 284
ネームド VSAN の作成 286
ストレージ VSAN の作成 286
VSAN の削除 287
ストレージ VSAN の FCoE VLAN の VLAN ID の変更 288
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 289
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 289
SAN ピン グループの設定 291
SAN ピン グループ 291
SAN ピン グループの作成 292
SAN ピン グループの削除 292
WWN プールの設定 293

WWN プール 293
WWNN プールの設定 294
WWNN プールの作成 294
WWNN プールへの WWN ブロックの追加 296
WWNN プールからの WWN ブロックの削除 297
WWNN プールへの WWNN イニシエータの追加 297
WWNN プールからの WWNN イニシエータの削除 298
WWNN プールの削除 299
WWPN プールの設定 299
WWPN プールの作成 299
WWPN プールへの WWN ブロックの追加 301
WWPN プールからの WWN ブロックの削除 302
WWPN プールへの WWPN イニシエータの追加 302
WWPN プールからの WWPN イニシエータの削除 304
WWPN プールの削除 304
WWxN プールの設定 305
WWxN プールの作成 305
WWxN プールへの WWN ブロックの追加 306
WWxN プールからの WWN ブロックの削除 307
WWxN プールの削除 308
ストレージ関連ポリシーの設定 309
vHBA テンプレートの設定 309
vHBA テンプレート 309
vHBA テンプレートの作成 309
vHBA テンプレートへの vHBA のバインディング 311
vHBA テンプレートからの vHBA のバインド解除 312
vHBA テンプレートの削除 313
ファイバ チャネル アダプタ ポリシーの設定 313
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 313
ファイバ チャネル アダプタ ポリシーの作成 315
ファイバ チャネル アダプタ ポリシーの削除 321
デフォルトの vHBA 動作ポリシーの設定 321

デフォルトの vHBA 動作ポリシー 321
デフォルトの vHBA 動作ポリシーの設定 322
SAN 接続ポリシーの設定 322
LAN および SAN 接続ポリシー 322
LAN および SAN の接続ポリシーに必要な権限 323
サービス プロファイルと接続ポリシー間の相互作用 323
SAN 接続ポリシーの作成 324
SAN 接続ポリシー用の vHBA の作成 325
SAN 接続ポリシーからの vHBA の削除 326
SAN 接続ポリシー用のイニシエータ グループの作成 326
SAN 接続ポリシーからのイニシエータ グループの削除 328
SAN 接続ポリシーの削除 328
ファイバ チャネル ゾーン分割の設定 329
ファイバ チャネル ゾーン分割に関する情報 329
ゾーンに関する情報 329
ゾーン セットに関する情報 330
Cisco UCS Manager でのファイバ チャネル ゾーン分割のサポート 330
Cisco UCS Manager ベースのファイバ チャネル ゾーン分割 331
vHBA イニシエータ グループ 331
ファイバ チャネル ストレージ接続ポリシー 332
ファイバ チャネル アクティブ ゾーン セット設定 332
スイッチベースのファイバ チャネル ゾーン分割 332
Cisco UCS Manager ベースのファイバ チャネル ゾーン分割に関するガイドラインおよび推奨事項 333
Cisco UCS でのファイバ チャネルのゾーン分割の設定 333
ファイバ チャネル ゾーン分割用の VSAN の作成 335
ファイバ チャネル ストレージ接続ポリシーの設定 338
ファイバ チャネル ストレージ接続ポリシーの作成 338
ファイバ チャネル ストレージ接続ポリシーの削除 340
サーバ関連プールの設定 341
サーバ プールの設定 341
サーバ プール 341

サーバ プールの作成 342
サーバ プールの削除 343
サーバ プールへのサーバの追加 343
サーバ プールからのサーバの削除 344
UUID 接尾辞プールの設定 344
UUID 接尾辞プール 344
UUID 接尾辞プールの作成 344
UUID 接尾辞プールの削除 346
IP プールの設定 346
IP プール 346
IP プールの作成 347
IP プールへのブロックの追加 349
IP プールからのブロックの削除 351
IP プールの削除 351
管理 IP アドレスの設定 353
管理 IP アドレス 353
ブレード サーバの管理 IP アドレスの設定 354
ブレード サーバでスタティック IP アドレスを使用するための設定 354
ブレード サーバで管理 IP プールを使用する設定 356
ブレード サーバからのインバンド設定の削除 358
ラック サーバの管理 IP アドレスの設定 359
ラック サーバでスタティック IP アドレスを使用するための設定 359
ラック サーバで管理 IP プールを使用する設定 361
ラック サーバからのインバンド設定の削除 363
サービス プロファイルの管理 IP アドレスの設定 364
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 368
管理 IP プールの設定 369
管理 IP プール 369
管理 IP プールでの IPv4 アドレス ブロックの作成 369
管理 IP プールでの IPv6 アドレス ブロックの作成 370
管理 IP プールからの IP アドレス ブロックの削除 371
サーバ関連ポリシーの設定 373

BIOS の設定 373
サーバ BIOS 設定 373
メイン BIOS 設定 374
プロセッサの BIOS 設定 376
Intel Directed I/O の BIOS 設定 383
RAS メモリの BIOS 設定 385
シリアル ポートの BIOS 設定 388
USB の BIOS 設定 388
PCI 設定の BIOS 設定 390
ブート オプションの BIOS 設定 391
サーバ管理 BIOS 設定 392
BIOS ポリシー 398
デフォルトの BIOS 設定 398
BIOS ポリシーの作成 399
BIOS のデフォルトの修正 400
サーバの実際の BIOS 設定の表示 401
CIMC セキュリティ ポリシー 402
IPMI アクセス プロファイル 402
IPMI アクセス プロファイルの作成 402
IPMI アクセス プロファイルの削除 404
KVM 管理ポリシー 404
KVM 管理ポリシーの作成 404
ローカル ディスク設定ポリシーの設定 405
ローカル ディスク設定ポリシー 405
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 406
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 406
ローカル ディスク設定ポリシーの作成 408
ローカル ディスク設定ポリシーの変更 412
ローカル ディスク設定ポリシーの削除 413
FlexFlash のサポート 414
FlexFlash SD カードのサポートのイネーブル化 415

スクラブ ポリシーの設定 416
スクラブ ポリシー 416
スクラブ ポリシーの作成 417
スクラブ ポリシーの削除 418
DIMM エラー管理の設定 418
DIMM の修正可能なエラー処理 418
メモリ エラーのリセット 419
DIMM のブラックリスト化 419
DIMM のブラックリストのイネーブル化 419
Serial over LAN ポリシーの設定 421
Serial over LAN ポリシー 421
Creating a Serial over LAN Policy 421
Serial over LAN ポリシーの削除 421
サーバ自動構成ポリシーの設定 422
サーバ自動構成ポリシー 422
自動構成ポリシーの作成 422
自動構成ポリシーの削除 424
サーバ ディスカバリ ポリシーの設定 424
サーバ ディスカバリ ポリシー 424
サーバ ディスカバリ ポリシーの作成 425
サーバ ディスカバリ ポリシーの削除 426
サーバ継承ポリシーの設定 426
サーバ継承ポリシー 426
サーバ継承ポリシーの作成 426
サーバ継承ポリシーの削除 428
サーバ プール ポリシーの設定 428
サーバ プール ポリシー 428
サーバ プール ポリシーの作成 428
サーバ プール ポリシーの削除 430
サーバ プール ポリシーの資格情報の設定 430
サーバ プール ポリシー資格情報 430
サーバ プール ポリシーの資格情報の作成 431

サーバ プール ポリシーの資格情報の削除 436
サーバ プール ポリシーの資格情報からの資格の削除 436
vNIC/vHBA 配置ポリシーの設定 437
vNIC/vHBA 配置ポリシー 437
vCon のアダプタへの配置 438
N20-B6620-2 および N20-B6625-2 ブレード サーバでの vCon のアダプタへの配置 439
vCon のアダプタへの配置（他のすべてのサポート対象サーバの場合） 439
vCon への vNIC/vHBA の割り当て 440
vNIC/vHBA 配置ポリシーの作成 442
vNIC/vHBA 配置ポリシーの削除 446
vCon への vNIC の明示的割り当て 447
vCon への vHBA の明示的割り当て 448
ダイナミック vNIC の前にスタティック vNIC を配置 450
CIMC マウント vMedia 452
vMedia ポリシーの作成 453
サービス プロファイルへの vMedia ポリシーの追加 455
CIMC vMedia ポリシーの表示 458
サーバ ブートの設定 459
ブート ポリシー 459
UEFI ブート モード 460
UEFI セキュア ブート 461
ブート ポリシーの作成 461
SAN ブート 463
ブート ポリシー用 SAN ブート ポリシー設定 463
iSCSI ブート 464
iSCSI ブート プロセス 464
iSCSI ブートのガイドラインと前提条件 465
イニシエータ IQN の設定 466
Windows での MPIO のイネーブル化 467
iSCSI ブートの設定 468
iSCSI アダプタ ポリシーの作成 469

iSCSI アダプタ ポリシーの削除 471

iSCSI 認証プロファイルの作成 471

iSCSI 認証プロファイルの削除 472

iSCSI イニシエータ IP プールの作成 473

iSCSI ブート ポリシーの作成 474

サービス プロファイル用 iSCSI vNIC の作成 475

サービス プロファイルからの iSCSI vNIC の削除 477

サービス プロファイル レベルでのイニシエータ IQN の設定 477

サービス プロファイル レベルでのイニシエータ IQN の変更 478

iSCSI ブート パラメータの設定 478

iSCSI ブート パラメータの変更 483

IQN プール 487

IQN プールの作成 487

IQN プールへのブロックの追加 489

IQN プールからのブロックの削除 490

IQN プールの削除 490

LAN ブート 491

ブート ポリシー用 LAN ブート ポリシー設定 491

ローカル デバイス ブート 492

ブート ポリシー用ローカル ディスク ブート ポリシー設定 493

ブート ポリシー用仮想メディア ブート ポリシー設定 494

vMedia ブート ポリシーの作成 495

vMedia サービス プロファイルへのブート ポリシーの追加 497

ブート ポリシーの削除 499

サービス プロファイル更新の遅延展開 501

サービス プロファイルの遅延展開 501

遅延展開スケジュール 502

メンテナンス ポリシー 502

保留アクティビティ 503

遅延展開に関するガイドラインおよび制限事項 504

スケジュールの設定 505

スケジュールの作成 505

スケジュールのワンタイム オカレンスの作成 511
スケジュールの繰り返しオカレンスの作成 514
スケジュールからのワンタイム オカレンスの削除 517
スケジュールからの繰り返しオカレンスの削除 517
スケジュールの削除 518
メンテナンス ポリシーの設定 518
メンテナンス ポリシーの作成 518
メンテナンス ポリシーの削除 520
保留アクティビティの管理 521
保留アクティビティの表示 521
ユーザの確認応答待ちサービス プロファイル変更の展開 521
ユーザの確認応答待ちのすべてのサービス プロファイル変更の展開 522
スケジュールされたサービス プロファイル変更の即時展開 522
スケジュールされたすべてのサービス プロファイル変更の即時展開 523
サービス プロファイルの設定 525
サーバ ID を上書きするサービス プロファイル 525
サーバ ID を継承するサービス プロファイル 526
サービス プロファイル テンプレート 527
サービス プロファイルに関するガイドラインおよび推奨事項 527
サービス プロファイルの作成 528
[Expert] ウィザードを使用したサービス プロファイルの作成 528
サーバ ID を継承するサービス プロファイルの作成 529
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 530
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 531
サービス プロファイル テンプレートの使用 532
サービス プロファイル テンプレートの作成 532
サービス プロファイル テンプレートから 1 つ以上のサービス プロファイルの作成 533
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 534
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 534
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 535
サービス プロファイルの管理 536

サービス プロファイルのクローン化 536
サービス プロファイルとサーバまたはサーバ プールの関連付け 536
サービス プロファイルとサーバまたはサーバ プールの関連付け解除 537
サービス プロファイルからのインバンド設定の削除 538
サービス プロファイルの名前の変更 538
サービス プロファイルの UUID の変更 539
サービス プロファイルのブート順序の変更 540
サービス プロファイル用の vNIC の作成 543
サービス プロファイルからの vNIC の削除 543
サービス プロファイル用の vHBA の作成 544
vHBA に対する WWPN の変更 544
vHBA の永続的なバインディングのクリア 545
サービス プロファイルからの vHBA の削除 545
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 545
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 548
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 549
サービス プロファイルの削除 549
サービス プロファイル テンプレートの管理 549
サービス プロファイル テンプレートとサーバ プールの関連付け 549
サーバ プールからのサービス プロファイル テンプレートの関連付け解除 550
サービス プロファイル テンプレートの UUID の変更 551
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 551
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 552
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 553
サービス プロファイル テンプレートからのインバンド設定の削除 554
Cisco UCS での電源管理 555
Cisco UCS での電源管理 555

ラック サーバの電源管理 555
電源管理の注意事項 556
電源ポリシーの設定 556
電源ポリシー 556
電源ポリシーの設定 556
グローバル電力割り当てポリシーの設定 557
グローバル電力割り当てポリシー 557
グローバル電力割り当てポリシーの設定 557
グローバル電力プロファイリング ポリシーの設定 558
グローバル電力プロファイリング ポリシーの設定 558
グローバル電力プロファイル ポリシーの設定 559
ポリシー方式のシャーシ グループの電力制限の設定 559
ポリシー方式のシャーシ グループの電力制限 559
電源グループの設定 560
電源グループ 560
電源グループの作成 561
電源グループへのシャーシの追加 562
電源グループからのシャーシの削除 563
電源グループの削除 563
電源制御ポリシーの設定 563
電源制御ポリシー 563
電力制御ポリシーの作成 564
電力制御ポリシーの削除 565
手動ブレード レベル電力制限の設定 566
手動によるブレード レベルの電力制限 566
サーバのブレード レベル電力制限の設定 566
ブレード レベル電力制限の表示 567
タイム ゾーンの管理 569
タイム ゾーン 569
時間帯の設定 569
NTP サーバの追加 570
NTP サーバの削除 570

シャーシの管理 571
Cisco UCS Manager GUI のシャーシ管理 571
シャーシの削除および解放に関するガイドライン 571
シャーシの確認 572
シャーシの稼働中止 573
シャーシの削除 573
単一シャーシの再稼動 573
複数のシャーシの再稼動 574
シャーシの番号付け直し 575
ロケータ LED の切り替え 576
シャーシのロケータ LED の電源投入 576
シャーシのロケータ LED の電源切断 576
ヘルス LED アラーム 576
ヘルス LED アラームの表示 577
ヘルス LED ステータスの表示 578
シャーシの POST 結果の表示 578
ブレード サーバの管理 581
ブレード サーバ管理 582
Cisco UCS B460 M4 ブレード サーバの管理 582
Cisco UCS B460 M4 ブレード サーバへのアップグレード 583
ブレード サーバの削除および解放に関するガイドライン 583
予期しないサーバ電力変更を回避するための推奨事項 584
ブレード サーバのブート 585
ブレード サーバのブート 585
サービス プロファイルからのサーバのブート 586
ブレード サーバのブート順序の決定 586
ブレード サーバのシャット ダウン 587
ブレード サーバのシャットダウン 587
サービス プロファイルからのサーバのシャットダウン 588
ブレード サーバのリセット 588
ブレード サーバの再確認 589
シャーシからのサーバの削除 590

ブレード サーバからのインバンド設定の削除 590
ブレード サーバの解放 591
ブレード サーバの再稼動 592
シャーシ内のサーバ スロットの再確認 592
存在しないブレード サーバの設定データベースからの削除 593
ブレード サーバのロケータ LED の切り替え 593
ブレード サーバの CMOS のリセット 594
ブレード サーバの CIMC のリセット 594
ブレード サーバの破損した BIOS の復旧 595
ブレード サーバの POST 結果の表示 596
ブレード サーバからの NMI の発行 596
ヘルス LED アラーム 597
ヘルス LED アラームの表示 597
ラックマウント サーバの管理 599
ラックマウント サーバ管理 600
ラックマウント サーバの削除および解放に関するガイドラインと推奨事項 600
予期しないサーバ電力変更を回避するための推奨事項 601
ラックマウント サーバのブート 602
ラックマウント サーバのブート 602
サービス プロファイルからのサーバのブート 602
ラックマウント サーバのブート順序の決定 603
ラックマウント サーバのシャット ダウン 604
ラックマウント サーバのシャットダウン 604
サービス プロファイルからのサーバのシャットダウン 604
ラックマウント サーバのリセット 605
ラックマウント サーバの再確認 606
ラック サーバからのインバンド設定の削除 606
ラックマウント サーバの解放 607
ラックマウント サーバの再稼動 607
ラックマウント サーバの番号付け直し 608
存在しないラックマウント サーバの設定データベースからの削除 608
ラックマウント サーバのロケータ LED の切り替え 609

ラックマウント サーバの CMOS のリセット 609
ラックマウント サーバの CIMC のリセット 610
ラックマウント サーバの破損した BIOS の復旧 610
ラックマウント サーバの POST 結果の表示 611
ラックマウント サーバからの NMI の発行 612
KVM コンソールの起動 613
KVM コンソール 613
仮想 KVM コンソール 614
KVM ダイレクト アクセス 619
サーバからの [KVM Console]KVM コンソールの起動 619
サービス プロファイルからの KVM コンソールの起動 620
KVM Launch Manager からの KVM コンソールの起動 621
[Cisco UCS KVM Direct] Web ページからの KVM コンソールの起動 622
CIMC セッション管理 625
CIMC セッション管理 625
すべての CIMC セッションの表示 626
サーバの CIMC セッションの表示 626
サービス プロファイルの CIMC セッションの表示 627
ローカル ユーザによって開かれた CIMC セッションの表示 627
リモート ユーザによって開かれた CIMC セッションの表示 627
開いているすべての CIMC セッションのクリア 628
サーバの CIMC セッションのクリア 628
サービス プロファイルの CIMC セッションのクリア 629
ローカル ユーザの CIMC セッションのクリア 629
リモート ユーザの CIMC セッションのクリア 629
設定のバックアップと復元 631
バックアップおよびエクスポートの設定 631
バックアップ タイプ 632
バックアップ操作の考慮事項と推奨事項 632
スケジュール バックアップ 633
Full State バックアップ ポリシー 633
All Configuration エクスポート ポリシー 634

Import Configuration 634
インポート方法 634
システムの復元 635
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 635
バックアップ操作の設定 636
バックアップ操作の作成 636
バックアップ操作の実行 640
バックアップ操作の変更 640
1 つまたは複数のバックアップ操作の削除 641
スケジュール バックアップの設定 642
Full State バックアップ ポリシーの設定 642
All Configuration エクスポート ポリシーの設定 644
インポート操作の設定 646
インポート操作の作成 646
インポート操作の実行 649
インポート操作の変更 650
1 つまたは複数のインポート操作の削除 651
ファブリック インターコネクトの設定の復元 651
失われたパスワードの復旧 655
失われたパスワードの復旧 655
amin アカウントのパスワードの復旧 655
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 656
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 656
スタンドアロン設定の admin アカウント パスワードの復旧 656
クラスタ設定の admin アカウント パスワードの復旧 658

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，xxxi ページ
- 表記法，xxxi ページ
- Cisco UCS の関連ドキュメント，xxxiii ページ
- マニュアルに関するフィードバック，xxxiii ページ

対象読者

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

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

表記法

テキストのタイプ	用途
GUI 要素	タブの見出し、領域名、フィールドのラベルのようなGUI要素は、[GUI要素] のように示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメイン タイトルは、[メイン タイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*italic*）で示しています。

テキストのタイプ	用途
TUI 要素	テキストベースのユーザ インターフェイスでは、システムによって表示されるテキストは、courier フォントで示しています。
システム出力	システムが表示するターミナル セッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体（**bold**）で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）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　時間を節約する方法です。 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

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

すべての B シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手できる『*Cisco UCS B-Series Servers Documentation Roadmap*』を参照してください。

すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

その他のマニュアル リソース

B シリーズと C シリーズのすべてのドキュメントが格納された ISO ファイルは、次の URL から入手できます。http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821 このページで、[Unified Computing System (UCS) Documentation Roadmap Bundle] をクリックします。

ISO ファイルは、ドキュメントのメジャー リリースの後に更新されます。

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

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTMLmailto:ucs-docfeedback@cisco.com 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 1 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，1 ページ
- ユニファイド ファブリック，3 ページ
- IPv6 への準拠，4 ページ
- サーバのアーキテクチャおよび接続性，6 ページ
- CIMC インバンド管理，12 ページ
- トラフィック管理，13 ページ
- オプトイン機能，18 ページ
- Cisco UCS でのバーチャライゼーション，21 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。

Cisco UCS Manager 3.0 は FI を UCS シャーシに統合し、小規模な導入環境向けの統合ソリューションを提供する 6324 ファブリック インターコネクトをサポートします。 Cisco UCS Mini はシステム管理を効率化し、小規模導入のコストを節約します。

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 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 の簡素化されたアーキテクチャは、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 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。

High Availability（高可用性）

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。

柔軟性

Cisco UCS ドメインは、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、ローカル エリア ネットワーク（LAN）、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、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 バーチャライゼーションに向けた最適化

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 バーチャライゼーション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、単一のデータセンター イーサネット（DCE）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。

IPv6 への準拠

Cisco UCS Manager は、IPv6 アドレッシングをサポートします。 このことは、次の理由により重要です。

- IPv4 アドレスは、IPv6 アドレスよりアドレス空間が小さい。
- 一意の IPv4 アドレスの数は有限であり、インターネットのアドレス資源管理団体が使用するアドレス指定方式が使用可能なアドレスの減少に拍車をかけている。
- IPv6 アドレスには大きなアドレス空間があり、使用可能な IPv6 アドレスのプールは、IPv4 アドレスのプールよりもはるかに多い。
- 顧客によっては、購入するすべてのネットワーキング ソフトウェアが IPv6 規格に準拠していることが求められる。

IPv4 アドレッシングをサポートしている Cisco UCS Manager の機能はすべて、IPv6 もサポートします。

（注） グローバル ユニキャスト IPv6 パブリック アドレスのみがサポートされます。

IPv6 アドレスは、管理インターフェイス、Cisco Cisco UCS Manager GUI、KVM コンソール、および SSH over SoL へのインバンド アクセスの設定に使用できます。

（注） IPv6 アドレスは、CIMC へのアウトオブバンド アクセスではサポートされません。

サポートされるサービス

IPv6 アドレスをサポートするサービスは次のとおりです。

- HTTP と HTTPS
- SSH
- Telnet
- CIM XML
- SNMP
- フラッシュ ポリシー サーバ

クライアントのサポート

IPv6 アドレスをサポートする外部クライアントは次のとおりです。

- NTP
- DNS
- DHCP
- LDAP
- RADIUS
- TACACS+
- SSH
- Syslog
- vCenter
- Call Home
- NFS

ファブリック インターコネクト

ファブリック インターコネクトの初期設定は、管理 IP アドレス、デフォルト ゲートウェイ、および DNS サーバに対する IPv6 アドレスの使用をサポートしています。
クラスタ セットアップでは、ファブリック A が IPv6 アドレスを使用して設定され、クラスタ設定が有効になっている場合に、続いてファブリック B が設定されると、セットアップ プロセスはファブリック A からアドレスタイプを取得し、IPv6 アドレスを使用するようユーザに促します。
初期セットアップの完了後、アウトオブバンド（OOB）アクセス用に、両方のファブリック インターコネクトに IPv4 アドレスを設定する必要があります。

Cisco UCS Manager およびファブリック インターコネクトは、IPv4 と IPv6 の両方のアドレスで OOB アクセス アドレスをサポートします。

IPv6 アドレッシングをサポートする設定

IIPv6 アドレスを使用して、キー リング証明書の要求、SNMP トラップ、管理 IP プールとアドレス ブロック、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、VLAN グループ、バックアップと復元操作、コア ファイルエクスポータ、Cisco UCS Manager Syslog、NTP サーバ、管理インターフェイス モニタリング ポリシーの ARP ターゲット、システムイベント ログ（SEL）管理、ライセンス管理、ファームウェアのダウンロード、Call Home、および vCenter を設定できます。

LDAP、RADIUS および TACACS+ 認証サービス プロバイダーの設定はすべて、IPv6 アドレッシングをサポートします。

サーバ

Cisco UCS ブレード サーバおよびラック サーバは、スタティック IPv6 アドレスを使用するように設定できます。 サーバ Cisco Integrated Management Controller（CIMC）へのインバンド アクセスは、IPv6 アドレスを使用して行うことができます。 管理トラフィックがより広い帯域幅のアップリンク ポート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流れるため、インバンド アクセスの方が高速です。

（注） Cisco UCS M3 サーバのみが IPv6 アドレスをサポートします。 Cisco UCS M1 および M2 サーバでは IPv6 アドレッシングはサポートされません。

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 の中心コンセプトです。 各サービス プロファイルには特定の目的があります。つまり、関連するサーバ ハードウェアでホスト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を、そのサーバ ハードウェアに確実に設定することです。

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 1 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に関連付けると、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 プロファイルに関連付けられたサーバで不具合が発生した場合でも、サービス プロファイルが別のサーバに自動的にフェールオーバーすることはありません。

サービス プロファイルとの関連付けが解除されると、サーバの ID および接続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、サーバに対して、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、そのサービス プロファイルの情報を使用して Cisco UCS の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します。

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、アソシエーション時にサーバに設定された ID 値を上書きし、Cisco UCS Manager で設定されたリソース プールとポリシーを使用して一部の管理タスクを自動化できます。

このサービス プロファイルは、あるサーバとの関連付けを解除して、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。 UUID や MAC アドレスなど、新しいサーバの工場出荷時の設定は、サービスプロファイルでの設定で上書きされます。その結果、サーバ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、サーバプール資格情報ポリシー、または特定のハードウェア設定が必要な別のポリシーが含まれていない場合は、そのサービスプロファイルを Cisco UCS ドメインのどのタイプのサーバにも使用できます。

これらのサービス プロファイルは、ラックマウント サーバまたはブレード サーバのどちらかに関連付けることができます。 サービス プロファイルの移行の可否は、サービス プロファイルの移行制限を選択するかどうかによって決まります。

（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。 これは特定のサーバに関連付けられているため、別のサーバへの移動や移行はできません。

このサービス プロファイルを使用するために、プールや設定ポリシーを作成する必要はありません。

このサービス プロファイルは、アソシエーション時に存在する次のような ID 情報および設定情報を継承し、適用します。

- 2 つの NIC の MAC アドレス
- 統合ネットワーク アダプタまたは仮想インターフェイス カードについては、2 つの HBA の WWN アドレス
- BIOS バージョン
- サーバの 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 テンプレートを使用して、vNIC や vHBA の個数などの同じ基本パラメータ、および同じプールから取得された ID 情報を使ってすばやく複数のサービス プロファイルを作成できます。

ヒント 既存のサービス プロファイルに類似した値を持つ 1 つのサービス プロファイルだけが必要な場合は、Cisco UCS Manager GUI でサービス プロファイルを複製できます。

たとえば、データベース ソフトウェアをホストするサーバの設定に、類似した値を持つ数個のサービス プロファイルが必要である場合、手動、または既存のサービス プロファイルから、サービス プロファイル テンプレートを作成できます。 その後、このテンプレートを使用して、サービス プロファイルを作成します。

Cisco UCS は、次のタイプのサービス プロファイル テンプレートをサポートしています。

初期テンプレート

初期テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承します。 初期のサービス プロファイル テンプレートから作成されたサービス プロファイルはテンプレートにバインドされます。 ただし、初期のテンプレートに対して行われた変更は、バインドされたサービス プロファイルに自動的に伝播されません。 バインドされたサービス プロファイルに変更を伝播したい場合は、そのサービス プロファイルをアンバインドしてから、再び初期テンプレートにバインドします。

アップデート テンプレート

アップデート テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承し、そのテンプレートへの接続をそのまま保持します。 アップデート テンプレートを変更すると、このテンプレートから作成されたサービス プロファイルが自動的にアップデートされます。

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。 対象に関する専門家は、その対象に関する専門知識を持た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。 その後、これらのポリシーは、LAN 管理に関する専門的な知識を持たない、または知識が限定されている他者によって作成されたサービス プロファイルで使用できます。

Cisco UCS Manager では、次の 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

Pools

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、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、特性が似ている未設定のサーバのプールを作成し、そのプールをサービス プロファイルに含めると、ポリシーを使用して、サービス プロファイルと使用可能な未設定のサーバを関連付けることができます。

MAC アドレスなどの ID 情報をプールすると、特定のアプリケーションをホストするサーバに事前に範囲を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 サーバに同じ範囲の MAC アドレス、UUID、WWN を設定できます。

Domain Pools

[Domain Pools] は、Cisco UCS ドメインで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 で定義され、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は、Cisco UCS Manager で [Global Pools] を割り当てることができます。

CIMC インバンド管理

マルチテナント、パブリックまたはプライベート サービス プロバイダー クラウド展開においてプロバイダー トラフィックからテナント トラフィックを分割したいという要望に応える形で、Cisco Integrated Management Controller（CIMC）へのインバンド管理アクセスの提供が推し進められました。アウトオブバンド（OOB）管理トラフィックは、ファブリック インターコネクト内外を移動し、管理ポート経由で管理プレーンを通過します。 これにより、ボトルネックを引き起し、管理ポートで CPU の帯域幅に影響を及ぼす可能性があります。

インバンド管理によって、CIMC トラフィックはデータ トラフィックと同じパスを使用してアップリンク ポート経由でファブリック インターコネクトに入退出することができます。 アップリンク ポートに使用可能な高帯域幅は、インバンドアクセスが管理トラフィックを大幅に加速し、トラフィック ボトルネックと CPU 負荷のリスクを軽減することを意味します。 アウトオブバンド（OOB）およびインバンド アドレス プールの両方を、Cisco UCS Manager の管理アクセス用に設定できます。 アウトオブバンド アクセスは IPv4 アドレスのみをサポートしています。 インバンド アクセスは、IPv4 および IPv6 アドレス両方をサポートし、シングルまたはデュアル スタック管理が可能です。

Cisco UCS Manager ブレードおよびラック サーバで設定できる 2 つの OOB 管理インターフェイス アドレスは以下になります。

- グローバル ext-mgmt プール経由で物理サーバに割り当てられた OOB IPv4 アドレス
- 物理サーバに関連付けられたサービス プロファイルから取得した OOB IPv4 アドレス

さらに、最大 4 つのインバンド管理インターフェイス アドレスを設定できます。

- 物理サーバに割り当てられたインバンド IPv4 アドレス
- 物理サーバに関連付けられたサービス プロファイルから取得したインバンド IPv4 アドレス
- 物理サーバに割り当てられたインバンド IPv6 アドレス
- 物理サーバに関連付けられたサービス プロファイルから取得したインバンド IPv6 アドレス

各サーバの複数のインバンド管理 IP アドレスは追加の CIMC セッションをサポートします。 OOB アドレスとインバンド アドレスの両方を設定すると、ユーザがサーバ、SSH to SoL、サービス プロファイル、KVM Launch Manager、または Cisco UCS Manager GUI web URL から KVM を開始するときに、[KVM Console] ダイアログボックスにあるこれらのアドレスのリストから選択することができます。

CIMC インバンド アクセスは次のサービスをサポートします。

- KVM コンソール
- SoL 用の CIMC への SSH
- ISO 準拠の vMedia、仮想 CD/DVD、リムーバブル ディスク、およびフロッピー

（注） Cisco UCS M3および M4 サーバだけが、インバンド CIMC アクセスをサポートします。 Cisco UCS M1 および M2 サーバ用のインバンド CIMC アクセスはサポートされません。

IPv4 または IPv6 アドレスのインバンド IP プールを設定し、それらを使用してサーバにアドレスを割り当てることができます。 インバンド VLAN グループを設定し、サービス プロファイルを使用してサーバに割り当てることができます。

サービス プロファイルおよびサービス プロファイル テンプレートでインバンド ネットワーク（VLAN）を選択するためには、インバンド VLAN グループでインバンド プロファイルを設定する必要があります。

インバンドプロファイルでネットワークおよびIPプール名を設定して、インバンドCIMCアドレスを Cisco UCS M3 サーバに割り当てることができます。

インバンド管理サポート

Cisco UCS Manager では、以下の外部サービスに対してインバンド管理アクセスがサポートされます。

- KVM
- ISO 準拠の vMedia、仮想 CD/DVD、リムーバブル ディスク、およびフロッピー
- SSH to SoL

IPv4 または IPv6 アドレスのインバンド IP プールを設定し、それらを使用してサーバにアドレスを割り当てることができます。 インバンド VLAN グループを設定し、サービス プロファイルを使用してサーバ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

以下の要因は、Cisco UCS ドメインでのオーバーサブスクリプションの設定方法に影響を与える可能性があります。

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 インターコネクトごとに少なくとも 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。

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。

ネットワーク タイプ

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にのみ関係します。これは、Cisco UCS の外部には 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、直接ピン グループを割り当てるか、ピン グループを vNIC ポリシーに含めてから、サーバに割り当てられているサービス 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、 FI-IO モジュールを経由して同じアップリンク ポートに流れます。

サーバ トラフィックのサーバ ポートへのピン接続

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。

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。

- 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システム全体にわたって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

Cisco UCS Mini での Quality of Service に関するガイドラインおよび制限事項

- Cisco UCS Mini では、すべてのシステム クラスで共有バッファが使用されます。
- Bronze クラスは SPAN とバッファを共有します。 SPAN または Bronze クラスを使用することを推奨します。
- マルチキャスト最適化はサポートされません。
- あるクラスの QoS パラメータを変更すると、すべてのクラスのトラフィックが中断されます。
- イーサネット トラフィックと FC または FCoE トラフィックが混在している場合は、帯域が均等に配分されません。
- 同じクラスからの複数のトラフィック ストリームが均等に分配されないことがあります。
- FC または FCoE のパフォーマンス問題を回避するために、すべての破棄なしポリシーに同じ CoS 値を使用してください。
- Platinum クラスと Gold クラスのみが破棄なしポリシーをサポートしています。

システム クラス

Cisco UCS は、DCE（Data Center Ethernet）を使用して、Cisco UCS ドメイン内のすべてのトラフィックを処理します。 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（QoS）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 クラスは特定のタイプのトラフィック用に帯域幅の特定のセグメントを予約します。これにより、過度に使用されるシステムでも、ある程度のトラフィック管理が提供されます。 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 *1*：システム クラス

システム クラス	説明
プラチナ ゴールド シルバー ブロンズ	サービスプロファイルの QoS ポリシーに含めることが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。 Cisco UCS Mini の場合、パケットの破棄は Platinum クラスと Gold クラスでのみ無効にできます。 1 つの Platinum クラスと 1 つの Gold クラスのみを no-drop クラスとして同時に設定できます。
ベスト エフォート	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 QoS 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 クラスは無効にできません。
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 クラスは無効にできません。 （注） FCoE トラフィックには、他のタイプのトラフィックで使用できない、予約された QoS システム クラスがあります。 他のタイプのトラフィックに FCoE で使用される CoS 値がある場合、その値は 0 にリマークされます。

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有効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り設定されます。

送信機能を有効にした場合、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。受信機能を有効にした場合、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 ドメインは、すべての機能を使用する許可を得ています。 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。

- ステートレス コンピューティング。この機能で利用されるモバイル サービス プロファイルには、各コンポーネント（サーバ、アダプタなど）がステートレスであるプールとポリシーが含まれています。
- 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、サーバを識別し Cisco UCS ドメイン内で一意のもの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 ドメイン内の物理サーバはすべて、サービス プロファイルとの関連付けが形成されるまで匿名のままです。その後、サービス プロファイルでこのサーバの ID が設定されます。 このサーバでビジネス サービスが不要になった場合は、サーバをシャットダウンし、サービスプロファイルの関連付けを解除してから、別のサービスプロファイルを関連付け、同じ物理サーバ用に別の ID を作成します。 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実装することもできますし、ステートレス サーバを使用しないことをもできます。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 プロファイルで定義されます。 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指し示すサービス プロファイルを作成します。 サーバ プール、WWN 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、物理サーバで不具合が発生した場合は、ただちにサービス プロファイルを別のサーバに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 アドレスなど、オリジナルのサーバと同じ ID を新しいサーバに与えるので、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、それらを使用してサーバの LAN または SAN 接続を設定します。 ただし、サーバ ハードウェアに不具合が発生した場合は、サービス プロファイルを新しいサーバに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 ドメインの大きな物理的インフラストラクチャを組織と呼ばれる論理的な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、すべてのユーザにすべての組織へのアクセス権を付与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と、すべての組織が階層的になります。 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対して、次のうちの 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選択する場合

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を選択しない場合

Cisco UCS ドメインは、ルート組織にすべてのデータが入った 1 つ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、この Cisco UCS ドメイン内のどのサーバにでも割り当てることができます。

Cisco UCS でのバーチャライゼーション

バーチャライゼーションの概要

仮想化により、独立して実行する複数の仮想マシン（VM）を同一の物理マシン上に隣接させて作成できます。

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、プロビジョニングと物理サーバ間での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。 バーチャライゼーションの利点は、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 ファブリック エクステンダの概要

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マシン 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され管理されます。 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 へのトラフィックのレイヤ 2 スイッチング、または外部ネットワークに対する別のインターフェイス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）アダプタと連携して、Cisco 仮想マシン ファブリック エクステンダ（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。 この方法により、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 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することができます。

VM-FEX は IEEE 802.1Qbh ポート エクステンダ アーキテクチャを VM に拡張するために、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します。このソリューションにより、VMインターフェイス上で、正確なレート制限と QoS（Quality of Service）保証が可能になります。

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バーチャライゼーション

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 アダプタでのバーチャライゼーション

Cisco VIC アダプタは、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、最大 128 の仮想ネットワーク インターフェイス カード（vNIC）を含む、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 インターフェイスとの間の、トラフィックのハードウェアベースのスイッチング機能を提供します。

第 2 章

Cisco UCS Manager の概要

この章の内容は、次のとおりです。

- Cisco UCS Manager の概要，23 ページ
- Cisco UCS Manager で実行可能なタスク，25 ページ
- Cisco UCS Manager で実行できないタスク，26 ページ
- ハイ アベイラビリティ環境の Cisco UCS Manager，27 ページ

Cisco UCS Manager の概要

Cisco UCS Manager は Cisco UCS ドメイン内のすべてのコンポーネントの管理システムです。Cisco UCS Manager は、ファブリック インターコネクト内で実行します。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 は Cisco UCS ドメインを管理するためにユーザが使用できる次のインターフェイスを含みます。

- 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 を介して実行されたコマンドの結果を参照する。
- Cisco UCS Manager GUI から CLI 出力を生成する。

集中管理

Cisco UCS 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。 この集中管理には、Cisco UCS ドメイン内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 インターフェイスの設定とファームウェアの更新（イーサネット NIC および統合型ネットワーク アダプタ）。
- 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、 FI-IO の設定、MAC アドレスおよびワールド ワイド名、ファームウェアのリビジョン、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管理と同じベスト 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。

- サーバ関連設定を制御できるサーバ アドミニストレータ ロール
- Storage Area Network（SAN）に関連するタスクを制御できるストレージ アドミニストレータ ロール
- ローカル エリア ネットワーク（LAN）に関連するタスクを制御できるネットワーク アドミニストレータ ロール

Cisco UCS はマルチテナント対応で、システムの管理ソフトウェアが API を使用して Cisco UCS リソースへ制御されたアクセスを行える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 で実行可能なタスク

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

Cisco UCS ハードウェア管理

Cisco UCS Manager を使用して、以下のような Cisco UCS ドメイン内のすべてのハードウェアを管理できます。

- シャーシ
- サーバ
- ファブリック インターコネクト
- Fans
- ポート
- インターフェイス カード

Cisco UCS リソース管理

Cisco UCS Manager を使用して、以下のような Cisco UCS ドメイン内のすべてのリソースを作成および管理できます。

- 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 Cisco UCS Manager を使用して、以下のような Cisco UCS ドメイン内のサーバ管理タスクを実行できます。

- 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、および必要に応じてサービス 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 Cisco UCS Manager を使用して、以下のような Cisco UCS ドメインの LAN 設定を作成するのに必要なタスクを実行できます。

- 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 Cisco UCS Manager を使用して、以下のような Cisco UCS ドメインの SAN 設定を作成するのに必要なタスクを実行できます。

- 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 ドメイン内のデバイス マネジメントに特に関連していないシステム管理タスクを実行するために、Cisco UCS Manager を使用できません。

システムを超えた管理はできない

Cisco UCS Manager がある Cisco UCS ドメインの外部にあるシステムやデバイスを管理するために 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、または Cisco UCS 以外のユーザ アカウントの処理を含む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、それぞれのファブリック インターコネクトで、別々の Cisco UCS Manager インスタンスを実行することができます。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 3 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，29 ページ
- HTTPS を使用した Cisco UCS Manager GUI へのログイン，37 ページ
- HTTP を使用した Cisco UCS Manager GUI へのログイン，38 ページ
- Cisco UCS Manager GUI からのログアウト，39 ページ
- Web セッション制限，39 ページ
- ログイン前バナー，40 ページ
- Cisco UCS Manager GUI のプロパティ，42 ページ
- フィールド値の許容範囲の決定，44 ページ
- ポリシーの使用場所の決定，44 ページ
- プールの使用場所の決定，44 ページ
- プール、ポリシー、その他のオブジェクトの削除，45 ページ
- XML のコピー，45 ページ

Cisco UCS Manager GUI の概要

Cisco UCS Manager GUI は、Cisco UCS Manager との 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 Manager GUI は、『Cisco UCS Software Release Notes（Cisco UCS ソフトウェア リリース ノート）』の「System Requirements（システム要件）」の項に記載されている要件を満たすコンピュータから起動してアクセスすることができます。

Cisco UCS Manager GUI が起動されるたびに、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、システムで Cisco UCS Manager ソフトウェアをアップデートした後に、コンピュータから初めてログインするときだけです。

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] 領域に [Faults] タブが開かれ、その種類の全障害について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	解消しないと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。
[抑制ステータス] フィールド	コンポーネント上のフォールト抑制タスクの状態。 [アクション] 領域の [抑制タスクのプロパティ] をクリックすると、すべてのフォールト抑制タスクが表示されます。 （注）　このフィールドは、コンポーネントがフォールト抑制をサポートし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、[Fault Summary] 領域の下に表示されます。このペインには、Cisco UCS ドメイン内のすべての機器とその他のコンポーネントに対する操作が集約されています。 [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 ドメイン内の機器の基本的なコンポーネントが含まれています。 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]：アクティブで動作していないハードウェア、ファームウェア管理、機器関連ポリシー、電源グループ、障害の集約リストを含む、Cisco UCS ドメイン全体の概要。
- [Chassis]：Cisco UCS ドメインの各シャーシのファン、 FI-IO モジュール、電源ユニット（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た Cisco UCS C シリーズ ラック 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モジュール、。

[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。

- [Server]：サービス プロファイルおよび定義された組織とサービス プロファイル間のリレーションシップ。
- [Service Profiles]：組織別に分割された、システムで定義されているサービス プロファイル。

- [Service Profile Templates]：組織別に分割された、システムで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 スクラビング、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]：メンテナンスとエラー抑制のスケジュール。

[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 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、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 プールと MAC プール。
- [Traffic Monitoring Sessions]：システムで定義されたポート トラフィック モニタリング セッション。

[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 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。
- [Policie]：ファイバ チャネル アダプタ ポリシー、デフォルトの vHBA 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]：システムで定義された iSCSI 修飾名（IQN）プールと WWN プール。

[VM] タブ

このタブには、VIC アダプタを備えたサーバに VM-FEX を設定するために必要なコンポーネントが含まれています。 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、分散仮想スイッチやポート プロファイルを設定したり、Cisco UCS ドメイン内のサーバにホストされている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、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、FSM タスク。
- [Clusters]：関連付けられている仮想マシンとポート プロファイルを含む、クラスタ。
- [Fabric Network Sets]：ファブリック ネットワークの定義
- [Port Profiles]：ポート プロファイル
- [VM Networks]：仮想ネットワーク
- [Mcrosoft]：Microsoft ネットワーク コンポーネント
- [VMware]：フォルダ、データセンター、仮想マシン、仮想スイッチなどを含む 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の設定、テクニカル サポート ファイルの作成、Full State バックアップ ポリシー、および All Configuration エクスポート ポリシー。
- [Faults]、[Events]、[Audit Log]：システム全体のエラー、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、およびグローバルな障害ポリシー。
- [User Management]：認証方式、リモートアクセス方法、ローカル ユーザ、ロケール、およびユーザ ロール。
- [Key Management]：SSH キーとトラストポイントの設定。
- [Communication Management]：SSH、Telnet、HTTP、HTTPS、SNMP、web session limits、Call Home の設定、DNS 管理、 管理インターフェイスのための通信サービスの設定、および Cisco UCS Central の構成。
- [Stats Management]：システムによって障害が発行されるタイミングを制御する統計情報のしきい値設定。
- [Time Zone Management]：タイムゾーンの同期を確立する NTP サーバの設定。
- [Capability Catalog]：調整可能なパラメータ、文字列、およびルールのセットである機能カタログ。

- [Management Extension]：管理の拡張。Cisco UCS Manager でサポートされていなかったサーバおよび他のハードウェアに対するサポートを追加できます。
- [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のライセンス。

ツールバー

ツールバーは、Cisco UCS Manager GUI の右側、[Work] ペインの上に表示されます。 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 ドメインのエレメントを作成する
- 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。
[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。

名前	説明
[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のインターフェイスを備えています。 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。

- アップリンクのイーサネット 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サーバ ポートを設定できる単一のインターフェイスを備えています。 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 Manager GUI では、Cisco UCS ドメインのシャーシごとに、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と接続の両方がハイブリッド表示されます。

このタブには、選択されたシャーシまたはラック サーバとファブリック 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。

- システム内の各 FI-IO モジュール。
- サーバと PSU を示すために選択されたシャーシ、または選択されたラック サーバ。

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 FI-IO モジュール上の関連サーバ 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。
- FI-IO モジュール上のサーバ 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 を使用した 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、`http://UCSManager_IPv4` または `http://UCSManager_IPv6` です。この *UCSManager_IPv4* と *UCSManager_IPv6* はそれぞれ、Cisco UCS Manager に割り当てられた IPv4 アドレスおよび IPv6 アドレスを表しています。 この IP アドレスは、次のいずれかです。

- クラスタ設定：*UCSManager_IPv4* または *UCSManager_IPv6* はそれぞれ、Cisco UCS Manager に割り当てられた仮想またはクラスタの IPv4 アドレスと IPv6 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_IPv4* または *UCSManager_IPv6* はそれぞれ、ファブリック インターコネクトの管理ポートの IPv4 アドレスと IPv6 アドレスを表します

（注） 一部のブラウザは、IPv6 アドレスを使用した HTTPS アクセスをサポートしていません。

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 を使用した 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、`http://UCSManager_IPv4` または `http://UCSManager_IPv6` です。この *UCSManager_IPv4* と *UCSManager_IPv6* はそれぞれ、Cisco UCS Manager に割り当てられた IPv4 アドレスおよび IPv6 アドレスを表しています。 この IP アドレスは、次のいずれかです。

- クラスタ設定：*UCSManager_IPv4* または *UCSManager_IPv6* はそれぞれ、Cisco UCS Managerに割り当てられた仮想またはクラスタのIPv4アドレスとIPv6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_IPv4* または *UCSManager_IPv6* はそれぞれ、ファブリック インターコネクトの管理ポートの IPv4 アドレスと IPv6 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 セッション制限は、ある時点における、システムにアクセス可能な Web セッション（GUI と 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 が許可する同時 Web セッション数は、最大値の 256 に設定されています。

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、必須フィールドに入力します。
ステップ 5 [Save Changes] をクリックします。

ログイン前バナー

ログイン前バナーを使用すると、ユーザが Cisco UCS Manager GUI にログインする場合、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、ユーザがダイアログボックスを閉じてからユーザ名とパスワードの入力を求めます。 ユーザが Cisco UCS Manager CLI にログインする場合、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、ユーザがダイアログボックスを閉じてからユーザ名とパスワードの入力を求めます。 その後は、ユーザに表示するコピーライト ブロックの上にバナーテキストを繰り返します。

ログイン前バナーの作成

[Banners] タブに [Pre-Login Banner] 領域が表示されない場合、Cisco UCS Manager はユーザがログインするときにログイン前バナーを表示しません。 [Pre-Login Banner] 領域が表示される場合は、2 つ目のログイン前バナーを作成することはできません。 既存のバナーの削除または変更だけができます。

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 [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] ペインの [Banners] タブをクリックします。

ステップ 5 [Actions] 領域で、 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て、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、標準の ASCII 文字を入力できます。

ステップ 7 [OK] をクリックします。

ログイン前バナーの変更

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] ペインの [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 フィールド内をクリックして、テキストに必要な変更を加えます。
このフィールドには、標準の 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。

ログイン前バナーの削除

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] ペインの [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、セッションの中断または非アクティブの状態に Cisco UCS Manager GUI が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] タブで、必要に応じてフィールドを更新します。
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、設定変更およびその他の操作の後に Cisco UCS Manager GUI が確認メッセージを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] タブで、必要に応じてフィールドを更新します。
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 は、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] タブで、[SSH] および [SSH Parameters] フィールドに値を指定します。
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] タブで、必要に応じてフィールドを更新します。
ステップ 4 [OK] をクリックします。

フィールド値の許容範囲の決定

あるプロパティには、入力できる値の範囲があります。 この手順によって、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対して許容範囲を決定することができます。 テーブルまたはツリーにリストされているプロパティの値の範囲の決定には、この手順を使用できません。

手順

ステップ 1 範囲を確認するフィールドにカーソルを置いて、フィールドにフォーカスを与えます。

ステップ 2 Alt+Shift+R を押します。
Cisco UCS Manager GUI が値の許容範囲を数秒間表示します。 範囲の表示は、画面上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決定

この手順を実行すれば、選択したポリシーに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 テンプレートを決定することができます。

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 が、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 [Service Profiles/Templates] ダイアログボックスに表示します。

プールの使用場所の決定

この手順を実行すれば、選択したプールに関連付けられサービス プロファイルとサービス プロファイル テンプレートを決定できます。

手順

ステップ 1 [Navigation] ペインで、使用状況を参照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] 領域で、[Show Pool Usage] をクリックします。
Cisco UCS Manager GUI が、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 [Service Profiles/Templates] ダイアログボックスに表示します。

プール、ポリシー、その他のオブジェクトの削除

プール、ポリシー、またはVLANなどの他のオブジェクトを削除するために使用する方法は、すべてのオブジェクトで同じです。

（注） オブジェクトを削除する前に、それらがシステム内の他のオブジェクトによって使用または参照されていないことを確認してください。たとえば、ネットワーク ポリシーを削除する前に、サービス プロファイルがそのポリシーを参照していないことを確認します。

手順

ステップ 1 [Navigation] ペインで、オブジェクトを表示するポッドを展開します。

ステップ 2 [Work] ペインで、適切なタブをクリックし、オブジェクトが置かれている場所に移動します。
たとえば、VLAN を削除する場合は、[VLANs] タブをクリックします。

ステップ 3 削除するオブジェクトを選択し、[Delete] をクリックします。

ステップ 4 [Delete] をクリックします。

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 4 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。

- Initial System Setup，47 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，49 ページ
- クラスタ設定の初期システム セットアップ，52 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，57 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，58 ページ

Initial System Setup

Cisco UCS ドメイン内のファブリック インターコネクトに初めてアクセスしたときは、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を設定する必要があります。

- 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 IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
- デフォルトのゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- DNS サーバの IPv4 または IPv6 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

Cisco UCS ドメインは、スタンドアロン構成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設定することもできますし、クラスタ構成でファブリック インターコネクトの冗長ペアを使用するように設定することもできます。

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、クラスタ構成では、冗長仮想インターフェイス（VIF）接続のフェールオーバー リカバリ時間が大幅に向上します。 アダプタに、あるファブリックインターコネクトへのアクティブな VIF 接続と別の（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 接続が存在する場合、アクティブなVIFの学習済みMACアドレスは複製されますが、第2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。 アクティブな VIF に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、それを Gratuitous ARP メッセージを介してネットワークにブロードキャストして、切り替え時間を短縮します。

（注） クラスタ構成では、管理プレーンに対してのみ冗長性が提供されます。データの冗長性はユーザの設定に依存するので、データの冗長性をサポートするにはサードパーティ製のツールが必要なこともあります。

クラスタ構成を使用するには、L1（L1 から L1）と L2（L2 から L2）のハイ アベイラビリティ ポート間で、イーサネット ケーブルを使用して 2 つのファブリック インターコネクトを直接接続し、その間に他のファブリック インターコネクトが含まれないようにする必要があります。 また、パッチパネルを介してファブリックインターコネクトを直接接続すると、それらは互いの状態を継続的にモニタして、一方で故障が発生した場合に即座にそれを検知できるようになります。

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。 クラスタ構成用に設定した 1 番目のファブリック インターコネクトをイネーブルにする必要があります。 2 番目のファブリック インターコネクトを設定すると、そのファブリック インターコネクトはクラスタ内のピア ファブリック インターコネクトとして 1 番目のファブリック インターコネクトを検出します。

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て IPv4 アドレス、ゲートウェイ、サブネット マスクを 1 つだけ、または IPv6 アドレス、ゲートウェイ、ネットワーク プレフィックスを 1 つだけ指定する必要があります。 管理ポートの IP アドレスに対して IPv4 または IPv6 アドレスのいずれかを設定できます。

クラスタ構成では、同一のサブネットに以下の 3 つの IPv4 アドレスを指定するか、プレフィックスが同じ 3 つの IPv6 アドレスを指定する必要があります。

- 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

（注） クラスタ構成では、両方のファブリック インターコネクトの管理ポートに同じアドレス タイプ（IPv4 または IPv6）を設定する必要があります。 最初の FI に IPv4 アドレスを設定し、2 番目の FI に IPv6 アドレスを設定すると、その構成は機能しません。

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 IPv4 およびサブネット マスク、または IPv6 アドレスとプレフィックス。
- デフォルト ゲートウェイ IPv4 アドレスまたは IPv6 アドレス。
- DNS サーバの IPv4 または IPv6 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 IPv4 アドレスまたは IPv6 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 IPv4 サブネットマスクまたは IPv6 プレフィックス
- 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 IPv4 アドレスまたは IPv6 アドレス

（注） Cisco UCS Manager は、IPv6 DHCP サーバまたは IPv6 ルータ アドバタイズメントからの自動設定をサポートしません。

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 インターコネクトの管理ポートのスタティック IPv4 または IPv6 アドレス。
[Mgmt IP Netmask] フィールドまたは [Mgmt IP Prefix] フィールド	ファブリック インターコネクトの管理ポートの IPv4 サブネット マスクまたは IPv6 プレフィクス。 （注） [Mgmt IP Address] フィールドに入力されたアドレス タイプに基づく、[Mgmt IP Netmask] または [Mgmt IP Prefix] 用のシステム プロンプト。
[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 IPv4 または IPv6 アドレス。 （注） [Mgmt IP Address] フィールドに入力されたアドレス タイプに基づく、[Default Gateway] 用のシステム プロンプト。
[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 IPv4 または IPv6 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。

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 つのスタティック IPv4 または IPv6 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 つのスタティック IPv4 アドレスのサブネット マスク、または 3 つのスタティック IPv6 アドレスのネットワーク プレフィックス。
- デフォルト ゲートウェイ IPv4 アドレスまたは IPv6 アドレス。

- DNS サーバの IPv4 または IPv6 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 IPv4 アドレスまたは IPv6 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 IPv4 サブネットマスクまたは IPv6 プレフィックス
- 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 IPv4 アドレスまたは IPv6 アドレス

（注） クラスタ設定では、設定時に両方のファブリックインターコネクトに同じ管理インターフェイスのアドレス タイプを割り当てる必要があります。

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 IPv4 アドレスまたは IPv6 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。

フィールド	説明
[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 インターコネクトの管理ポートのスタティック IPv4 または IPv6 アドレス。
[Mgmt IP Netmask] フィールドまたは [Mgmt IP Prefix] フィールド	ファブリック インターコネクトの管理ポートの IPv4 サブネット マスクまたは IPv6 プレフィクス。 （注） [Mgmt IP Address] フィールドに入力されたアドレス タイプに基づく、[Mgmt IP Netmask] または [Mgmt IP Prefix] 用のシステム プロンプト。
[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 IPv4 または IPv6 アドレス。 （注） [Mgmt IP Address] フィールドに入力されたアドレス タイプに基づく、[Default Gateway] 用のシステム プロンプト。
[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 IPv4 または IPv6 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 IPv4 アドレスまたは IPv6 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 IPv4 サブネットマスクまたは IPv6 プレフィックス
- 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 IPv4 アドレスまたは IPv6 アドレス

（注） クラスタ設定では、設定時に両方のファブリック インターコネクトに同じ管理インターフェイスのアドレス タイプを割り当てる必要があります。

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。
[Manager Initial Setup] 領域が表示されます。

ステップ 10 [Manager Initial Setup] 領域で表示されるフィールドは、第 1 ファブリック インターコネクトを IPv4 または IPv6 のどちらの管理アドレスで設定したかによって異なります。次のように、設定に適したフィールドに入力します。

フィールド	説明
[Peer FI is IPv4 Cluster enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv4 Address] フィールド	ローカル ファブリック インターコネクトの Mgmt0 インターフェイスの IPv4 アドレスを入力します。
[Peer FI is IPv6 Cluster Enabled. Please Provide Local Fabric Interconnect Mgmt0 IPv6 Address] フィールド	ローカル ファブリック インターコネクトの Mgmt0 インターフェイスの IPv6 アドレスを入力します。

ステップ 11 [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。

ファブリックインターコネクトへのアウトオブバンドIPv4アドレスの追加

すべてのファブリック インターコネクトでは、OOB IPv4 アドレス、ネットワーク マスク、およびゲートウェイが必要です。この手順では、スタティック IPv6 アドレスで設定されたファブリック インターコネクトに OOB IPv4 アドレスを設定する方法について説明します。

はじめる前に

ファブリックインターコネクトに割り当てるアウトオブバンド（OOB）IPv4アドレスを収集します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope fabric interconnect a**	ファブリック A のファブリック コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A/fabric-interconnect # **set out-of-band ip** *ip-addr* **netmask** *ip-addr***gw** *ip-addr*	OOB IPv4 アドレス、ネットワーク マスク、およびゲートウェイ アドレスを設定します。 システムは変更がコミットされると、コンソール セッションの変更が切断される可能性を警告します。
ステップ 3	UCS-A/fabric-interconnect # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次に、ファブリック インターコネクト A の OOB IPv4 アドレスを設定する例を示します。

```
UCS-A# scope fabric-interconnect a
UCS-A /fabric-interconnect # set out-of-band ip 10.105.214.107 netmask 255.255.255.0 gw
10.105.214.1
Warning: When committed, this change may disconnect the current CLI session
UCS-A /fabric-interconnect* # commit-buffer
```

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、2 番目のファブリック インターコネクトを追加できます。 これを行うには、クラスタの仮想 IP または IPv6 アドレスを使用して設定することでスタンドアロン 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し、その後、クラスタに 2 番目のファブリック 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*|*virtual-ip6-addr*}	指定の IPv4 または IPv6 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。 確認のために **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た IP アドレスではなく、クラスタ設定用の仮想 IPv4 または IPv6 アドレスである必要があります。

	コマンドまたはアクション	目的

次に、仮想 IPv4 アドレス 192.168.1.101 を使用して、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. Also, any GUI or KVM sessions may be terminated. Are you sure you want
 to continue? (yes/no): yes
UCS-A(local-mgmt)#
```

次に、仮想 IPv6 アドレス 192.168.1.101 を使用して、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 ipv6 2001::109
This command will enable IPv6 cluster mode on this setup. You cannot change it
back to stand-alone. Also, any GUI or KVM sessions may be terminated. 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。

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 5 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。

- Cisco UCS 6324 ファブリック インターコネクト のユニファイド ポート，60 ページ
- サーバ ポート，65 ページ
- アップリンク イーサネット ポート，65 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，67 ページ
- ファブリック インターコネクトのポートのイネーブル化またはディセーブル化，67 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，68 ページ
- アプライアンス ポート，68 ページ
- FCoE およびファイバ チャネル ストレージ ポート，71 ページ
- FCoE アップリンク ポート，72 ページ
- ユニファイド アップリンク ポート，73 ページ
- アップリンク イーサネット ポート チャネル，75 ページ
- アプライアンス ポート チャネル，78 ページ
- ファイバ チャネル ポート チャネル，80 ページ
- FCoE ポート チャネル，84 ページ
- ユニファイド アップリンク ポート チャネル，85 ページ
- アダプタ ポート チャネル，86 ページ
- Internal Fabric Manager を使用したサーバ ポートの設定，86 ページ

Cisco UCS 6324 ファブリック インターコネクトのユニファイド ポート

ユニファイド ポートは Cisco UCS 6324 ファブリック インターコネクト 上のポートであり、イーサネットまたはファイバ チャネル トラフィックを伝送するように設定できます。 これらのポートは予約されていません。 設定するまで、Cisco UCS ドメインではそれらのポートを使用できません。

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

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

ポート モード

ポートモードは、ファブリックインターコネクト上の統合ポートが、イーサネットまたはファイバ チャネル トラフィックを転送するかどうかを決定します。 ポート モードは、ファブリック インターコネクトによって自動的に検出されません。これは Cisco UCS Manager で設定されます。

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

ポート タイプ

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

イーサネット ポート モードに変更された統合ポートは、デフォルトでアップリンク イーサネット ポート タイプに設定されます。 ファイバ チャネル ポート モードに変更された統合ポートは、ファイバ チャネル アップリンク ポート タイプに設定されます。 ファイバ チャネル ポートの設定を解除することはできません。

ポート タイプ変更時のリブートは不要です。

ポート モードがイーサネットに設定されたときには、次のポート タイプを設定できます。

- サーバ ポート
- イーサネット アップリンク ポート
- イーサネット ポート チャネル メンバ
- FCoE ポート

- アプライアンス ポート
- アプライアンス ポート チャネル メンバ
- SPAN 宛先ポート
- SPAN 送信元ポート

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

ポート モードがファイバ チャネルに設定されたときには、次のポート タイプを設定できます。

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

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

Cisco UCS Mini スケーラビリティ ポート

Cisco UCS 6324 ファブリック インターコネクト には 4 つのユニファイド ポートに加えて、1 つのスケーラビリティ ポートがあります。 スケーラビリティ ポートは 40GB QSFP+ ブレークアウト ポートで、適切な配線を使って 4 つの 1 G または 10G SFP+ ポートをサポートできます。 スケーラビリティ ポートは、サポート対象の Cisco UCS ラック サーバ、アプライアンス ポート、または FCoE ポート用のライセンス サーバ ポートとして使用できます。

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

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

スケーラビリティ ポートの設定

サポートされている任意のタイプのポートまたはスケーラビリティ ポートのポート メンバーを設定するには、[Ethernet Ports] モードを展開し、それから、[Scalability Port 5] 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、[Fabric Interconnects] > [*Fabric_Interconnect_Name*] > [Fixed Module] > [Ethernet Ports] > [Scalability Port 5] を展開します。

ステップ 3 [Scalability Port 5] ノード下のポートをクリックします。

ステップ 4 必要に応じて、ポートを設定します。

ユニファイド ポートの設定に関するガイドライン

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

ポート モードの設定

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

- イーサネット ポートがブロックにグループ化されていること。
- ファイバ チャネル ポートがブロックにグループ化されていること。
- イーサネット ポートとファイバ チャネル ポートの交替は、サポートされない。

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に関する注意およびガイドライン

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

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

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

- FCoE およびユニファイド アップリンク ポートでデフォルトでないネイティブ VLAN を設定する必要があります。 この VLAN は、トラフィックには使用されません。 Cisco UCS Manager はこの目的のために、既存の fcoe-storage-native-vlan を再利用します。 この fcoe-storage-native-vlan は、FCoE およびユニファイド アップリンクでネイティブ VLAN として使用されます。
- ユニファイド アップリンク ポートでは、イーサネット アップリンク ポートにデフォルトでない VLAN を設定しないと、fcoe-storage-native-vlan がユニファイド アップリンク ポートのネイティブ VLAN として割り当てられます。 イーサネット ポートにネイティブ VLAN として指定されているデフォルトでないネイティブ VLAN がある場合、ユニファイド アップリンク ポートのネイティブ VLAN としてこれが割り当てられます。
- イーサネット ポート チャネル下でメンバ ポートを作成または削除すると、Cisco UCS Manager は FCoE ポート チャネル下で自動的にメンバ ポートを作成または削除します。 FCoE ポート チャネルでメンバ ポートを作成または削除する場合も同じことが起こります。
- サーバ ポート、イーサネット アップリンク、FCoE アップリンクまたは FCoE ストレージなどのスタンドアロン ポートとしてイーサネット ポートを設定し、それをイーサネットまたは FCOE ポート チャネルのメンバ ポートにすると、Cisco UCS Manager は自動的にこのポートをイーサネットと FCoE ポート チャネル両方のメンバにします。
- サーバアップリンク、イーサネットアップリンク、FCoEアップリンクまたはFCoEストレージのメンバからメンバ ポートのメンバーシップを削除すると、Cisco UCS Manager はイーサネット ポート チャネルと FCoE ポート チャネルから対応するメンバ ポートを削除し、新しいスタンドアロン ポートを作成します。
- ユニファイドアップリンク ポートとユニファイド ストレージ ポートの場合、2 つのインターフェイスを作成するときは、1 つだけライセンスがチェックされます。 どちらかのインターフェイスが有効な限り、ライセンスはチェックされたままになります。 両方のインターフェイスがユニファイド アップリンク ポートまたはユニファイド ストレージ ポートでディセーブルの場合にのみライセンスが解放されます。

ポート モードの変更のデータ トラフィックへの影響

ポート モードの変更は、Cisco UCS ドメインのデータ トラフィックへの割り込みを引き起こす場合があります。 割り込みの長さや影響を受けるトラフィックは、Cisco UCS ドメインの設定およびポート モード変更を行ったモジュールに依存します。

ポート モード変更のクラスタ設定の固定モジュールへの影響

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

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

ポート モード変更のスタンドアロン設定の固定モジュールへの影響

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

6324 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 のポート モードを変更すると、データ トラフィックが中断されることがあります。これは、固定モジュールを変更するとファブリック インターコネクトのリブートが必要となり、。

Cisco UCS ドメインに、ハイ アベイラビリティ用に設定されたクラスタ構成が存在し、フェールオーバー用に設定されたサービス プロファイルを持つサーバが存在する場合、固定モジュールのポートモードを変更しても、トラフィックは他のファブリック インターコネクトにフェールオーバーし、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]：ポート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 Port] ダイアログ ボックスで、マウスを使用して、モジュールに必要なポート モードの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 他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 5 と 6 を繰り返します。

ステップ 8 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。
ファブリック インターコネクトがリブートします。 そのファブリック インターコネクトを経由するすべてのデータ トラフィックが中断されます。 ハイ アベイラビリティが提供され、フェールオーバー用に設定された vNIC があるサーバが含まれるクラスタ構成では、トラフィックは他のファブリック インターコネクトにフェールオーバーし、中断は発生しません。

次の作業

ポートのポートタイプを設定します。スライダの上に表示されるモジュールの任意のポートで右クリックして、そのポートに使用可能なポート タイプを設定できます。

サーバ ポート

サーバ ポートの設定

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

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] > [Ethernet Ports] を展開します。

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

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

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

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

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

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。 右クリック メニューからもアップリンク イーサネット 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 設定するポートのノードを展開します。

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

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

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

ステップ 7 ドロップダウン リストから [Configure as Uplink Port] を選択します。

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 設定するポートのノードを展開します。

ステップ 4 [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] 領域で、[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、ポートを識別するためのラベルを入力します。

b) [Flow Control Policy] ドロップダウン リストからフロー制御ポリシーを選択し、受信バッファがいっぱいになった場合にポートが IEEE 802.3x ポーズ フレームを送受信する方法を決定します。

c) [Admin Speed] フィールドで、次のオプション ボタンの 1 つをクリックします。

- 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ノードを展開します。

ステップ 4 再設定するポートを 1 つ以上クリックします。

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

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

ステップ 7 ドロップダウン リストからポートの再設定方法を選択します。

例：アップリンク イーサネット ポートをサーバ ポートとして再設定する

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

ファブリックインターコネクトのポートのイネーブル化またはディセーブル化

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

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

手順

ステップ 1 [Navigation] ペインの [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 イネーブルまたはディセーブルにするポートのノードを展開します。
ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
ステップ 5 [Work] ペインの [General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Enable Port] または [Disable Port] をクリックします。
ステップ 7 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。

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ノードを展開します。
ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
ステップ 5 [Work] ペインで、[General] タブをクリックします。
ステップ 6 [Actions] 領域で、[Unconfigure] をクリックします。
ステップ 7 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。

アプライアンス ポート

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

（注） 新しいアプライアンス VLAN を作成すると、IEEE VLAN ID は LAN クラウドに追加されません。 したがって、新しい VLAN に設定されたアプライアンスのポートは、ピン接続障害が原因でデフォルトでダウンしたままになります。 これらのアプライアンスのポートを起動するには、同じ IEEE VLAN ID を使用して LAN クラウドで VLAN を設定する必要があります。

アプライアンス ポートの設定

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

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 設定するポートのノードを展開します。

ステップ 4 [Ethernet Ports] ノードで、ポートを選択します。
サーバ ポート、アップリンク イーサネット ポート、または FCoE ストレージ ポートを再設定する場合は、適切なノードを展開します。

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

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

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

ステップ 8 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 [Configure as Appliance Port] ダイアログ ボックスで、必須フィールドに入力します。

ステップ 10 [VLANs] 領域で、次の手順を実行します。

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

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

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

（注） アプリケーション ポートでアップリンク ポートをトラバースする必要がある場合、LAN クラウドでこのポートによって使用される各 VLAN も定義する必要があります。 たとえば、ストレージが他のサーバでも使用される場合や、プライマリ ファブリック インターコネクトのストレージ コントローラに障害が発生したときにトラフィックがセカンダリ ファブリック インターコネクトに確実にフェールオーバーされるようにする必要がある場合は、トラフィックでアップリンク ポートをトラバースする必要があります。

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

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

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

ステップ 12 [OK] をクリックします。

アプライアンス ポートのプロパティの変更

手順

ステップ 1 [Navigation] ペインの [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 ポートのノードを展開します。

ステップ 4 [Ethernet Ports] を展開します。

ステップ 5 プロパティを変更するアプライアンス ポートをクリックします。

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

ステップ 7 [Actions] 領域で、[Show Interface] をクリックします。
すべてのフィールドを表示するには、[Properties] ダイアログ ボックスのスクロール バーの展開または使用が必要になる場合があります。

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

ステップ 9 [OK] をクリックします。

FCoE およびファイバ チャネル ストレージ ポート

FCoE ストレージ ポートの設定

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

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

はじめる前に

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

手順

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

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

ステップ 6 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。

アップリンク ファイバ チャネル ポートの復元

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

手順

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

ステップ 5 選択した 1 つ以上のポートを右クリックし、[Configure as Uplink Port] を選択します。

ステップ 6 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。

FCoE アップリンク ポート

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

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

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

次のいずれかと同じイーサネット ポートを設定できます。

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

FCoE アップリンク ポートの設定

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

手順

ステップ 1 [Navigation] ペインの [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 設定するポートのノードを展開します。

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

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

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

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

ステップ 8 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 が成功のメッセージを表示します。
[Properties] 領域で、[Role] が [FCoE Uplink] に変わります。

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

ユニファイド アップリンク ポート

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

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

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

ユニファイド アップリンク ポートの設定

次のいずれかから、ユニファイド アップリンク ポートを設定できます。

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

この手順では、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。

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 設定するポートのノードを展開します。

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

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

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

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

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

ステップ 9 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 が成功のメッセージを表示します。
[Properties] 領域で、[Role] が [Unified Uplink] に変わります。

ステップ 11 （任意）[Properties] 領域で、[VSAN] フィールドに [VSAN] 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解除して削除できます。 または、FCoE ポート設定またはイーサネット ポート設定のいずれか一方を設定解除し、もう一方をポートに保持することができます。

手順

ステップ 1 [Navigation] ペインの [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ノードを展開します。

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

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

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

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

ステップ 7 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 に成功メッセージが表示されます。 選択した設定解除オプションに基づいて、[Properties] 領域の [Role] が変更されます。

ステップ 9 [Save Changes] をクリックします。

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 チャネルを使用すると、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して（リンク集約）、1 つの論理イーサネット リンクを作成し、耐障害性と高速接続を実現できます。 Cisco UCS Manager で、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 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 チャネルの全ポートを個別のポートとして扱い、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 [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。

ステップ 6 [Add Ports] パネルで、追加するポートを指定します。

（注） Cisco UCS Manager では、サーバ ポートとして設定済みのポートを選択した場合、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] 領域で、[Add Ports] をクリックします。

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

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

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

アプライアンス ポート チャネルの作成

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] パネルで、必須フィールドにポート チャネルのアイデンティティ、およびその他のプロパティを指定します。
このパネルから LAN ピン グループ、ネットワーク制御ポリシーとフロー制御ポリシーを作成できます。
ステップ 6 [VLANs] 領域で、VLAN の [Port Mode] およびその他の情報を指定します。
このパネルから VLAN を作成できます。

ステップ 7 （任意） エンドポイントを追加する場合は、[Ethernet Target Endpoint] チェックボックスをオンにして名前と MAC アドレスを指定します。

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] パネルで、追加するポートを指定します。

（注） Cisco UCS Manager 入力した設定によりサービス プロファイルまたはポート設定で問題が発生する場合は、警告が表示されます。 これらの問題が発生する可能性があってもポート 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] 領域で、[Add Ports] をクリックします。

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

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

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、[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。

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 チャネルを使用すると、複数の物理ファイバ チャネル ポートをグループ化して（リンク集約）、1 つの論理ファイバ チャネル リンクを作成し、耐障害性と高速接続性

を実現できます。 Cisco UCS Manager で、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 2 つのファイバ チャネル ポート チャネルを作成できます。 各ファイバ チャネル ポート チャネルには、最大 4 つのアップリンク ファイバ チャネル ポートを含めることができます。

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 [Set Port Channel Name] パネルで、ID と名前を指定し、[Next] をクリックします。
ステップ 6 [Add Ports] パネルで、ポート チャネルの管理速度を指定し、ポート チャネルにポートを追加します。
ステップ 7 [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] 領域で、[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] 領域で、[Add Ports] をクリックします。

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

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

ステップ 7 [OK] をクリックします。

ファイバ チャネル ポート チャネルのプロパティの変更

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

手順

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

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

ステップ 6 [Save Changes] をクリックします。

ファイバ チャネル ポート チャネルの削除

手順

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

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

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] パネルで、ID と名前を指定し、[Next] をクリックします。
ステップ 6 [Create FCoE Port Channel] ウィザードの [Add Ports] パネルで、追加するポートを指定します。
ステップ 7 [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] タブの [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。

ユニファイド アップリンク ポート チャネル

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

次のルールは、ユニファイド アップリンク ポート チャネルのメンバ 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 チャネルと FCoE ポート チャネルは、同じメンバ ポートの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 ポートが追加されます。
- 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ー ポートを削除します。

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

アダプタ ポート チャネル

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

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

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] の順に展開します。

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] 列のリンクをクリックします。

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サーバ ポートを設定できる単一のインターフェイスを備えています。 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 6 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，89 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，90 ページ
- ライセンスの取得，90 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，91 ページ
- リモート ロケーションからファブリック インターコネクトへのライセンスのダウンロード，92 ページ
- ライセンスのインストール，93 ページ
- ファブリック インターコネクトにインストールされているライセンスの表示，94 ページ
- ポートまたは機能に使用できる猶予期間の決定，95 ページ
- ライセンスの失効日の決定，95 ページ
- ライセンスのアンインストール，95 ページ

ライセンス

各 Cisco UCS 6324 ファブリック インターコネクトにはポート ライセンスが付属します。このライセンスは工場でインストールされ、ハードウェアと共に出荷されます。 このライセンスは 4 つの 10G ユニファイド ポートに対応し、サポートされているあらゆる用途に使用できます。 スケーラビリティ ポート ライセンスは猶予期間付きで工場インストールされ、アプライアンス ポートまたは FCoE ポートとして Cisco UCS ラック サーバで使用できます。

猶予期間

ライセンスがインストールされていないポートを使用しようとすると、Cisco UCS は 120 日間の猶予期間を開始します。 猶予期間は、最初にライセンスなしでポートを使用した時点から測定さ

れ、有効なライセンスファイルがインストールされると一時停止されます。猶予期間中に使用された時間数はシステムに保存されます。

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

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

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数のライセンスされたポートを用意することを推奨します。 均衡が保たれていない状態でフェールオーバーが発生すると、Cisco UCS は欠けているライセンスを有効化して、フェールオーバー ノードで使用される各ポートに対して猶予期間を開始します。

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] 領域の [Serial Number (SN)] フィールドにホスト ID が表示されます。

次の作業

シスコから必要なライセンスを入手します。

ライセンスの取得

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

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 インターコネクトの権利証明書またはその他の購入証明書

手順

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

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

ステップ 3 ファブリック インターコネクトの Web サイト URL にアクセスし、シリアル番号と PAK を入力します。
シスコからライセンス ファイルが電子メールで送信されます。 ライセンス ファイルは、要求されたファブリック インターコネクトでの使用だけを許可するようにデジタル署名されています。Cisco UCS Manager がライセンス ファイルにアクセスすると、要求された機能も有効になります。

次の作業

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

はじめる前に

シスコから必要なライセンスを入手します。

手順

ステップ 1 [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 ファイルが配置されているフォルダへの正確なパスがわからない場合は、[Browse] をクリックしてファイルに移動します。

ステップ 8 [OK] をクリックします。
Cisco UCS Manager GUI によってファブリック インターコネクトへのライセンスのダウンロードが開始されます。

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

（注） Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、[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 必要なライセンスがすべてファブリック インターコネクトにダウンロードされるまで、このタスクを繰り返します。

次の作業

すべてのダウンロード タスクが完了した後、ライセンスをインストールします。

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

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

はじめる前に

シスコから必要なライセンスを入手します。

手順

ステップ 1 [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 プロトコルを指定し、必要な情報を入力します。

（注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で 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 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

ステップ 8 [OK] をクリックします。
Cisco UCS Manager GUI によってファブリック インターコネクトへのライセンスのダウンロードが開始されます。

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

（注） Cisco UCS Manager によって、ブートフラッシュの領域が不足していることが報告された場合は、[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 必要なライセンスがすべてファブリック インターコネクトにダウンロードされるまで、このタスクを繰り返します。

次の作業

すべてのダウンロード タスクが完了した後、ライセンスをインストールします。

ライセンスのインストール

はじめる前に

シスコから必要なライセンスを入手します。

手順

ステップ 1 [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、未ライセンスのポートまたは機能がアクティブ化されます。

ファブリックインターコネクトにインストールされているライセンスの表示

手順

ステップ 1 [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ているすべてのライセンスの詳細を表示します。

ステップ 4 表内のライセンスをクリックし、[Contents] タブにライセンスの詳細を表示します。
ファイル内の個々のライセンスの詳細を表示するには、ライセンス ファイルを展開する必要があります。

ポートまたは機能に使用できる猶予期間の決定

手順

ステップ 1 [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 動作状態、適用された猶予期間など機能の詳細を表示するには、テーブル中でその機能をクリックします。

ライセンスの失効日の決定

手順

ステップ 1 [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て、ライセンスの詳細を下の [Contents] タブに表示します。

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

ステップ 6 [Expiry] 列でライセンスの失効日を参照します。

ライセンスのアンインストール

（注） 使用中の永続ライセンスはアンインストールできません。 未使用の永久ライセンスだけをアンインストールできます。 使用中の永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 の設定をバックアップします。

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はライセンスを非アクティブ化し、ライセンスのリストからそのライセンスを削除し、ファブリックインターコネクトからライセンスを削除します。ポートは、ライセンスなしモードに移行します。クラスタ構成の場合は、他のファブリックインターコネクトからもライセンスをアンインストールする必要があります。

第 7 章

コミュニケーション サービスの設定

この章の内容は、次のとおりです。

- Communication Services，97 ページ
- CIM-XML の設定，99 ページ
- HTTP の設定，100 ページ
- HTTPS の設定，100 ページ
- SNMP の設定，108 ページ
- Telnet のイネーブル化，117 ページ
- CIMC Web サービスのイネーブル化，117 ページ
- 通信サービスのディセーブル化，117 ページ

Communication Services

以下に定義する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。

Cisco UCS Manager 次のサービスに対する IPv4 および IPv6 アドレス アクセスの両方をサポートします。

- CIM XML
- HTTP
- HTTPS
- SNMP
- SSH
- Telnet

Cisco UCS Manager Web ブラウザから [Cisco UCS KVM Direct] 起動ページへのアウトオブバンド IPv4アドレスアクセスをサポートします。このアクセスを提供するには、次のサービスをイネーブルにする必要があります。

- CIMC Web サービス

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。
CIMC Web サービス	このサービスは、デフォルトでディセーブルになります。 このサービスをイネーブルにすると、ユーザは直接サーバに割り当てられるか、またはサービス プロファイルを介しサーバに関連付けられたアウトオブバンドの管理IPアドレスの1つを使用して直接サーバCIMCにアクセスできます。 （注） CIMC Web サービスは全体的にイネーブルまたはディセーブルにすることのみが可能です。 個別の CIMC IP アドレスに対し KVM ダイレクト アクセスを設定できません。
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 経由の通信の試行をすべて同等の HTTPS 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、これはデフォルトでは発生しません。 HTTP 経由の通信の試行を同等の HTTPS にリダイレクトする場合、[Redirect HTTP to HTTPS] を Cisco UCS Manager で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 を使用すると、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。 セキュリティ上の目的から、HTTPS だけを使用するようにし、HTTP 通信は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。

通信サービス	説明
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になり、**show** コマンドなど、プロトコルの一部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] 領域が展開して、デフォルトの [Port] 番号 5988 を表示します。 このポート番号は変更できません。

ステップ 5 [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 ログインの HTTPS ログインへのリダイレクションをイネーブルにするには、HTTPS も設定して有効にする必要があります。いったんイネーブルにすると、HTTPS をディセーブルにするまでは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、Cisco UCS Manager GUI へのアクセスに HTTP は使用できません。 リダイレクションは、HTTP をディセーブルにして、自動的に HTTPS にリダイレクトします。

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、公開キー インフラストラクチャ（PKI）のコンポーネント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たり、証明書が期限切れになったりした場合は、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（ルート認証局（CA）、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 エンコード X.509（CER）フォーマット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 キー リングを含め、最大 8 個のキー 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	ネットワークに割り当てられたドメイン名（すべてのホストに共通）。
[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。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。

名前	説明
[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。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[Country] フィールド	会社所在国の国コード。 2 文字のアルファベットを入力します。
[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。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[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。任意の文字、数字、スペース、および次の特殊文字を使用できます：,（カンマ）、.（ピリオド）、@（アットマーク）、^（キャラット）、(（開き括弧）、)（閉じ括弧）、-（ダッシュ）、_（アンダースコア）、+（プラス記号）、:（コロン）、/（スラッシュ）。
[Email] フィールド	要求に関連付けられている電子メール 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。

ステップ 7 IP アドレスを割り当てるには、[IPv4] または [IPv6] のタブをクリックします。この選択は、Cisco UCS Manager をセットアップするときのファブリック インターコネクトの設定に応じて行います。

- [IPv4] タブをクリックし、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 ドメインの IPv4 アドレス。
[FI-A IP] フィールド	ファブリック インターコネクト A の IPv4 アドレス。
[FI-B IP] フィールド	ファブリック インターコネクト B の IPv4 アドレス。

- [IPv6] タブをクリックし、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 ドメインの IPv6 アドレス。
[FI-A IP] フィールド	ファブリック インターコネクト A の IPv6 アドレス。
[FI-B IP] フィールド	ファブリック インターコネクト B の IPv6 アドレス。

ステップ 8 [OK] をクリックします。

ステップ 9 [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 10 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[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 エンコード X.509（CER）フォーマット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、この証明書を付与したトラスト アンカーのトラスト 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 エンコード X.509（CER）フォーマット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 で使用するポートとキー リングの変更を含め、HTTPS の設定を完了した後、トランザクションを保存またはコミットするとすぐに、現在のすべての HTTP および HTTPS セッションは警告なく閉じられます。

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 [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
[管理状態] フィールド	次のいずれかになります。 • [有効化] • [無効化] [管理状態] が有効の場合は、Cisco UCS Manager GUI に、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	Cisco UCS Manager がシステム レベルの HTTPS 通信を行うために必要なポート。 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	Cisco UCS ドメインで使用される暗号スイート セキュリティのレベル。 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の文字列を指定できます。
[Cipher Suite] フィールド	[Cipher Suite Mode] フィールドで [Custom] を選択した場合は、このフィールドでユーザ定義の暗号スイート仕様の文字列を指定します。 暗号スイート仕様の文字列は最大256文字まで使用できますが、OpenSSL暗号スイート仕様に準拠する必要があります。 次を除き、スペースや特殊文字は使用できません。！（感嘆符）、+（プラス記号）、-（ハイフン）、および：（コロン）。 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、Cisco UCS Managerがデフォルトとして使用する中強度仕様の文字列は次のようになります： ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL

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てください。

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] > [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 では、ネットワーク内のデバイスのモニタリングと管理に使用する標準フレームワークと共通言語が提供されます。

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：管理対象デバイスである Cisco UCS 内のソフトウェア コンポーネント。Cisco UCS のデータを保守し、必要に応じてそのデータを SNMP に報告します。 Cisco UCS には、エージェントと一連の MIB が含まれています。 SNMP エージェントを有効にして、マネージャとエージェント間のリレーションシップを作成するには、Cisco UCS Manager で SNMP を有効にして設定します。
- 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 リリース 1.4(1)以降では、以前よりも多くの MIB をサポートしています。

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 は次のよう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 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受信時に確認応答を送信せず、Cisco UCS Manager はトラップが受信されたかどうかを確認できないため、トラップの信頼性はインフォームよりも低くなります。 インフォーム要求を受信する SNMP マネージャは、SNMP 応答プロトコル データ ユニット（PDU）でメッセージの受信を確認します。 Cisco UCS Manager が PDU を受信しない場合、インフォーム要求を再送できます。

SNMP セキュリティ レベルおよび権限

SNMPv1、SNMPv2c、および SNMPv3 はそれぞれ別のセキュリティ モデルを表します。 セキュリティ モデルは選択されたセキュリティ レベルと組み合わされ、SNMP メッセージの処理中に適用されるセキュリティ メカニズムを決定します。

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の表示に必要な権限を決定します。 権限レベルは、開示されないようメッセージを保護する必要があるか、またはメッセージを認証する必要があるかどうかを決定します。 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、次の権限の 1 つ以上をサポートします。

- noAuthNoPriv：認証なし、暗号化なし
- authNoPriv：認証あり、暗号化なし

- authPriv：認証あり、暗号化あり

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 モデルとレベルのサポートされている組み合わせ

次の表に、セキュリティ モデルとレベルの組み合わせの意味を示します。

表 *2*： *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	ユーザ名	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）メッセージダイジェスト 5（MD5）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 アルゴリズムまたは 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、および暗号ブロック連鎖（CBC）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：不正なユーザ、エンティティ、プロセスに対して情報を利用不可にしたり開示しないようにします。

SNMP サポート： Cisco UCS

Cisco UCS は、SNMP に対して以下のサポートを備えています。

MIB のサポート

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 およびその入手先については、B シリーズ サーバは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html を、C シリーズは http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html を参照してください。

SNMPv3 ユーザの認証プロトコル

Cisco UCS は、SNMPv3 ユーザ用に次の認証プロトコルをサポートしています。

- 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 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 つとして高度暗号化規格（AES）を使用し、コメント要求（RFC）3826 に準拠しています。

プライバシー パスワード（priv オプション）では、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 の設定を有効にして、SNMPv3 ユーザ用のプライバシー パスワードを含めると、Cisco UCS Manager はそのプライバシー パスワードを使用して 128 ビット AES キーを生成します。 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、次のフィールドに入力します。

名前	説明
[管理状態] フィールド	次のいずれかになります。 • [有効化] • [無効化] 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。 [管理状態] が有効の場合は、Cisco UCS Manager GUI に、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）または空欄スペース は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 の実装を担当するシステムの連絡先。 電子メール アドレス、名前、電話番号など、255 文字まで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）が実行するホストの場所。 最大 510 文字の英数字を入力します。

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。 SNMP ホストに IPv4 または IPv6 アドレスを使用できます。

名前	説明
[Community/Username] フィールド	Cisco UCS Manager がトラップを SNMP ホストに送信するときに含める SNMP v1/v2c 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たコミュニティまたはユーザ名と同じである必要があります。 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）または空欄スペース は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 バージョンおよびモデル。 次のいずれかになります。 • V1 • V2c • V3
[Type] フィールド	バージョンとして [V2c] または [V3] を選択した場合に、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	バージョンとして [V3] を選択した場合に、トラップに関連付ける権限。 次のいずれかになります。 • [Auth]：認証あり、暗号化なし • [Noauth]：認証なし、暗号化なし • [Priv]：認証あり、暗号化あり

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。 32 文字までの文字または数字を入力します。 名前は文字で始まる必要があり、_（アンダースコア）、.（ピリオド）、@（アット マーク）、-（ハイフン）も指定できます。 （注） ローカル側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

名前	説明
[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。
[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。

CIMC Web サービスのイネーブル化

CIMC Web サービスはデフォルトでイネーブルとなっています。ディセーブルにしている場合は、次の手順を行ってサービスをイネーブルにします。

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] > [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 [CIMC Web Service] 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

「Configuring Authentication」

この章の内容は、次のとおりです。

- 認証サービス，119 ページ
- リモート認証プロバイダーに関するガイドラインおよび推奨事項，120 ページ
- リモート認証プロバイダーにおけるユーザ属性，120 ページ
- 二要素認証，122 ページ
- LDAP グループ ルール，124 ページ
- ネストされた LDAP グループ，124 ページ
- LDAP プロバイダーの設定，124 ページ
- RADIUS プロバイダーの設定，130 ページ
- TACACS+ プロバイダーの設定，132 ページ
- マルチ認証システムの設定，134 ページ
- プライマリ認証サービスの選択，141 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 アカウントによって
- 次のいずれかのプロトコルによりリモートで
  - LDAP
  - RADIUS
  - TACACS+

リモート認証プロバイダーに関するガイドラインおよび推奨事項

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 にローカルに設定したり、リモート認証サーバに設定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ことがあり、その場合は読み取り専用権限だけが付与されます。

リモート認証プロバイダーにおけるユーザ属性

RADIUS および TACACS+ 構成では、ユーザが Cisco UCS Manager へのログインに使用する各リモート認証プロバイダーに Cisco UCS 用のユーザ属性を設定する必要があります。 このユーザ属性には、各ユーザに割り当てられたロールとロケールが含まれています。

（注） この手順は、LDAP グループ マッピングを使用してロールとロケールを割り当てる LDAP 設定では必要ありません。

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に問い合わせます。
2. ユーザを検証します。
3. ユーザが有効である場合は、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。

次の表は、Cisco UCS がサポートしているリモート認証プロバイダーのユーザ属性要件を比較して示しています。

表 *3*：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	スキーマの拡張	属性 ID 要件
LDAP	グループ マッピング使用時は不要 グループ マッピング不使用時は任意	オプション 次のいずれかを選択して実行できます。 • 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する。 • 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する。	シスコの LDAP の実装では、Unicode タイプの属性が必要です。 CiscoAVPair 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 サンプルの OID が次のセクションに示されています。
RADIUS	任意	オプション 次のいずれかを選択して実行できます。 • RADIUS スキーマを拡張せず、要件を満たす既存の未使用属性を使用する。 • 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する。	シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。 次の構文例は、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方法を示しています。`shell:roles="admin,aaa"` `shell:locales="L1,abc"`。 複数の値を区切るには、区切り文字としてカンマ「,」を使用します。

認証プロバイダー	カスタム属性	スキーマの拡張	属性 ID 要件
TACACS+	必須	必須です。 スキーマを拡張し、cisco-av-pair という名前のカスタム属性を作成する必要があります。	cisco-av-pair 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。 次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ 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"`。 cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。 複数の値を区切るには、区切り文字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

カスタム CiscoAVPair 属性のサンプル OID は、次のとおりです。

```
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
```

二要素認証

Cisco UCS Manager は、ユーザ名とパスワードの組み合わせによるユーザ ログイン操作をサポートしています。 覚えやすいパスワードを設定するユーザもいますが、そのようなパスワードはマルウェア、スパイウェア、コンピュータ ウイルスに対して脆弱な恐れがあります。 保護されてい

ないネットワークからシステムにリモート アクセスするユーザや安全ではないサービスを使用しているユーザは、パスワードがスヌーピング ソフトウェアによって侵害されている可能性があります。 フィッシング攻撃は、ユーザをだましてパスワードを暴露させるウイルス攻撃です。

ユーザ認証を強化する 1 つの方法は、ユーザ名とパスワードに加えて第 2 の要素を要求することです。 二要素認証では、3 つの認証要素のうち 2 つが必要になります。 二要素認証では、ユーザが知っているものの組み合わせ（パスワードまたは PIN と、証明書やトークンなどユーザが所有しているもの）が使用されます。 二要素認証はリモート ユーザに対してのみサポートされており、IPMI はサポートされません。

Cisco UCS Manager では、認証アプリケーションを使用して二要素認証を提供しています。このアプリケーションはトークン サーバを保持して、ログインプロセス中にユーザ用のワンタイム トークンを生成します。 パスワードは AAA サーバに保存されるため、ログイン時、ユーザはユーザ名を入力してから、パスワード フィールドにトークンとパスワードの組み合わせを入力する必要があります。ベンダー固有の属性を取得するために、リクエストがトークン サーバに送信されます。 Cisco UCS Manager は、トークン サーバがリクエストを AAA サーバに転送できるように、トークン サーバを AAA サーバと統合することを要求します。 パスワードとトークンは、AAA サーバによって同時に検証されます。ユーザは、AAA サーバで設定されているのと同じ順序で、トークンとパスワードを入力する必要があります。

この機能は、RADIUS または TACACS+ プロバイダー グループを指定認証ドメインに関連付け、それらのドメインで二要素認証を有効にすることによってサポートされます。

（注） 二要素認証は、認証レルムが LDAP、local、または none に設定されている場合はサポートされません。

Web セッションの更新および Web セッションのタイムアウト期限

Web セッションのタイムアウト期限は、アクティビティに関係なく、セッションの最長継続時間を制御します。 二要素認証を設定すると、Web セッションのタイムアウト期限もより大きいデフォルト値に設定されます。 Web セッションの更新期間が過ぎると、Cisco UCS Manager GUI クライアントはプロンプトを自動的に生成し、新しいトークンとパスワードの組み合わせを入力するようユーザに求めます。

Web セッションの更新期間は、ユーザの Web セッションの有効期間を制御します。 二要素認証が設定されている場合、ユーザは、Web セッションの更新期間が切れるたびに、トークンとパスワードの組み合わせを入力してログインする必要があります。セッションタイムアウトが頻発して、ユーザに何度もトークンとパスワードの作り直しと再入力を要求することがないように、Web セッションの更新間隔は、二要素認証が有効化されると、より大きい初期デフォルト値に設定されます。 これにより、リモート ユーザは長時間アクティブ セッションを維持することができます。 無活動により Web セッションの更新が期限切れになった場合、ユーザは新しいトークンを生成して再度ログインするよう要求されます。

LDAP グループ ルール

LDAP グループ ルールは、リモート ユーザにユーザ ロールとロケールを割り当てるときに、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されます。

ネストされた LDAP グループ

Cisco UCS Manager のリリース 2.1(2) 以降では、LDAP グループ マップで定義された他のグループ内にネストされた LDAP グループを検索できます。 この新しい機能を使用すると、Cisco UCS Manager のグループ マップでサブグループを常に作成する必要がなくなります。

（注） ネストされた LDAP の検索サポートは Microsoft Active Directory サーバに対してのみサポートされます。 サポート対象のバージョンは Microsoft Windows 2003 SP3、Microsoft Windows 2008 R2、および Microsoft Windows 2012 です。

LDAP ネスティング機能を使用して、LDAP グループを他のグループおよびネスト グループのメンバとして追加し、メンバ アカウントを統合してトラフィックの重複を減らすことができます。

デフォルトでは、ユーザ権限は他のグループ内の LDAP グループをネストするときに継承されます。 たとえば、Group_2 のメンバとして Group_1 を作成すると、Group_1 のユーザは Group_2 のメンバと同じ権限が与えられます。その結果、Group_1 のメンバであるユーザを検索するときは、Group_1 と Group_2 を別々に検索するのではなく LDAP グループ マップの Group_2 を選択するだけで済みます。

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 で定義された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です。 個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

はじめる前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドする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 [Properties] 領域で、すべてのフィールドに入力します。

（注） ユーザ ログインは LDAP ユーザの userdn が 255 文字を超えると失敗します。

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 では、最大 16 の LDAP プロバイダーがサポートされます。

はじめる前に

Active Directory を LDAP サーバとして使用している場合は、Active Directory サーバで Cisco UCS にバインドする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します。

- 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、ユーザのロールとロケール情報が含まれています。
  - 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ユーザに対して設定します。 この属性について 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 属性などのカスタム属性を作成します。

    シスコの LDAP の実装では、Unicode タイプの属性が必要です。

    CiscoAVPair 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の IPv4 または IPv6 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 により使用されている仮想 IPv4 または IPv6 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、LDAP サーバのルート認証局（CA）の証明書が格納されたトラスト ポイントを Cisco UCS Manager で作成します。

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、すべてのフィールドに適切な LDAP サービス情報を入力します。

（注） IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

ステップ 6 ウィザードの [LDAP Group Rule] ページで、すべてのフィールドに適切な LDAP グループ ルール情報を入力します。

（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属している場合や LDAP 属性で指定されたロールまたはロケールを持っている場合、Cisco UCS は、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とロケールをそのユーザに割り当てます。

次の作業

単一の LDAP データベースが関係する実装の場合は、認証サービスとして LDAP を選択します。

複数の LDAP データベースが関係する実装の場合は、LDAP プロバイダー 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	Cisco UCS が、ユーザ ロールとロケールを認証してリモート ユーザに割り当てるときに、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 UCS 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、関連する LDAP グループ マップでその LDAP グループに対して定義されているユーザ 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属している場合や LDAP 属性で指定されたロールまたはロケールを持っている場合、Cisco UCS は、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とロケールをそのユーザに割り当てます。
[Group Recursion] フィールド	Cisco UCS が、マッピング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 ドメインでマッピングされたグループだけを検索します。 ユーザが属するいずれのグループでもユーザの認証プロパティが明示的に設定されていない場合、Cisco UCS はデフォルトの設定を使用します。 • [Recursive]：Cisco UCS は、マップされた各グループおよびそのすべての親グループでユーザの認証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、Cisco UCS は、明示的な認証プロパティ設定を備えたグループを検出すると、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、デフォルト設定が使用されます。
[Target Attribute] フィールド	Cisco UCS が LDAP データベース内のグループ メンバーシップを判別するために使用する属性。 サポートされるストリングの長さは 63 文字です。 デフォルトの文字列は「memberOf」です。

名前	説明
[Use Primary Group] フィールド	メンバーシップの確認のための LDAP グループ マップとしてプライマリ グループを設定できるかどうかを判断するために、Cisco UCS で使用される属性。 このオプションを使用すると、Cisco UCS Manager はユーザのプライマリグループ メンバーシップをダウンロードして検証できます。

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

LDAP データベースへのアクセスを制限するためにすでに LDAP グループを使用している組織では、UCSM でグループ メンバーシップ情報を使用して、ログイン時に LDAP ユーザにロールやロケールを割り当てることができます。 これにより、Cisco UCS Manager を導入するときに、LDAP ユーザ オブジェクトでロールやロケール情報を定義する必要がなくなります。

ユーザが Cisco UCS Manager にログインすると、ユーザのロールと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基準がポリシー情報と一致する場合は、アクセスが許可されます。

ロールとロケールの定義は Cisco 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 ディレクトリ内の LDAP グループの削除や名前変更を行う場合は、変更に合わせて Cisco UCS Manager も更新する必要があります。

LDAP グループ マップは、次のロールとロケールのいずれか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
- ロールとロケールの両方

たとえば、特定の場所のサーバ管理者グループを表す LDAP グループがあるとします。 LDAP グループ マップは、server-profile や server-equipment などのユーザ ロールを含むように設定されることもあります。 特定の場所のサーバ管理者へのアクセスを制限するために、ロケールに特定のサイト名を設定することができます。

（注） Cisco UCS Manager にはすぐに使用できる多数のユーザ ロールが含まれていますが、ロケールは含まれていません。 LDAP プロバイダー グループをロケールに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、必要に応じてすべての LDAP グループ マップ情報を指定します。

重要 [LDAP Group DN][LDAP Group DN] フィールドフィールドで指定する名前は、LDAP データベース内の名前と正確に一致させる必要があります。

（注） [LDAP Group DN] フィールドに特殊文字を使用する場合は、特殊文字の前にエスケープ文字 \（シングル バックスラッシュ）を付ける必要があります。

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 で定義された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です。 個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

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、[User Management] > [RADIUS] を展開します。
ステップ 3 [Properties] 領域で、すべてのフィールドに入力します。
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 では、最大 16 の RADIUS プロバイダーがサポートされます。

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ユーザに対して設定します。 この属性について 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。

  シスコによる RADIUS の実装のベンダー ID は 009 であり、属性のベンダー ID は 001 です。

  次の構文例は、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方法を示しています。`shell:roles="admin,aaa" shell:locales="L1,abc"`。 複数の値を区切るには、区切り文字としてカンマ「,」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の IPv4 または IPv6 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 により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、該当するすべての RADIUS サービス情報を指定します。

（注） IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているように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

単一の RADIUS データベースが関係する実装の場合は、RADIUS をプライマリ認証サービスとして選択します。

複数の RADIUS データベースが関係する実装の場合は、RADIUS プロバイダー 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 で定義された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です。 個々のプロバイダーにこれらのうちいずれかのプロパティの設定が含まれている場合、Cisco UCS でその設定が使用され、デフォルト設定は無視されます。

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、[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。
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 では、最大 16 の TACACS+ プロバイダーがサポートされます。

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 名は、TACACS+ プロバイダーの属性 ID を提供する文字列です。

次の構文例は、cisco-av-pair 属性を作成するときに複数のユーザ 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"`。cisco-av-pair 属性構文でアスタリスク（*）を使用すると、ロケールがオプションとして指定され、同じ認可プロファイルを使用する他のシスコデバイスで認証の失敗を防ぐことができます。 複数の値を区切るには、区切り文字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の IPv4 または IPv6 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 により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) 必要に応じてすべてのフィールドに TACACS+ サービス情報を入力します。

（注） IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

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

単一の TACACS+ データベースが関係する実装の場合は、TACACS+ をプライマリ認証サービスとして選択します。

複数の TACACS+ データベースが関係する実装の場合は、TACACS+ プロバイダー 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

次の機能を実装して、Cisco UCS が複数の認証システムを使用するように設定することができます。

- 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 によって使用されるプロバイダーのセットです。 Cisco UCS Manager では、最大 16 のプロバイダー グループを作成でき、グループごとに最大 8 つのプロバイダーを含めることが可能です。

認証中は、プロバイダー グループ内のすべてのプロバイダーが順番に試行されます。設定されているどのサーバも使用できない場合、またはどのサーバにも到達できない場合、Cisco UCS Manager は、ローカル ユーザ名とパスワードを使用して自動的にローカル認証方式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 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できます。

（注） 単一の LDAP データベースを使用した認証では、LDAP プロバイダー 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。

（注） IPv4 または IPv6 のアドレスの代わりにホスト名を使用する場合、DNS サーバにはホスト名が必ず設定されているようにする必要があります。

ステップ 4 [Create LDAP Provider Group] ダイアログボックスで、適切なすべての LDAP プロバイダー グループ情報を指定します。

次の作業

認証ドメインを設定するか、デフォルト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 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できます。

（注） 単一の RADIUS データベースを使用した認証では、RADIUS プロバイダー 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 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 1 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。
[<<] ボタン を使用して、グループからプロバイダーを排除できます。

d) （任意）プロバイダーが認証のためにアクセスされる順序を変更するには、[Included Providers] リストの [Move Up] または [Move Down] の矢印を使用します。

e) 必要なすべてのプロバイダーをプロバイダー グループに追加した後、[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

認証設定で使用されているプロバイダー 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 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できます。

（注） 単一の TACACS+ データベースを使用した認証では、TACACS+ プロバイダー 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、必要に応じてすべての TACACS+ プロバイダーのグループ情報を指定します。

TACACS+ プロバイダー グループの削除

認証設定で使用されているプロバイダー 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、複数の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、ログイン中に指定および設定されます。 認証ドメインを指定しないと、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 内のプロバイダー グループと領域に関連付けられています。 プロバイダー グループが指定されていない場合は、領域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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。 （注） リモート認証プロトコルを使用するシステムの場合、認証ドメイン名はユーザ名の一部と見なされ、ローカルに作成されたユーザ名に対して 32 文字の制限が適用されます。 Cisco UCS ではフォーマットに 5 文字が挿入されるため、ドメイン名とユーザ名の合計が 27 文字を超えると、認証に失敗します。
[Web Session Refresh Period (sec)] フィールド	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、Cisco UCS Manager に更新要求を送信する必要があります。 このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションの終了は行いません。 60 ～ 172800 の整数を指定します。 デフォルトは 600 秒です。 （注） [Web Session Refresh Period] に設定する秒数は、[Web Session Timeout] に設定する秒数未満である必要があります。 [Web Session Refresh Period] に [Web Session Timeout] と同じ値を設定しないでください。
[Web Session Timeout (sec)] フィールド	最後の更新要求から Cisco UCS Manager が Web セッションが終了したと見なすまでの最大経過時間。 この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。 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に定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに対して指定された 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 ドメインに対して指定された 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 ドメインに対して指定された 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	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 グループ。 （注） [Provider Group] ドロップダウン リストは、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。
[Two Factor Authentication] チェックボックス	[Two Factor Authentication] は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。 このチェックボックスを選択すると、Cisco UCS Manager と KVM launch manager は、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするように求めます。 [Web Session Refresh Period] の期限が切れた場合、ユーザはセッションを続行するために新しいトークンを作成し、そのトークンとパスワードを入力する必要があります。

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。 Cisco UCS を通じた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] 領域で、次のフィールドに入力します。

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に定義する必要があります。 • [Radius]：ユーザは、この Cisco UCS ドメインに対して指定された 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 ドメインに対して指定された 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 ドメインに対して指定された 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は、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。

名前	説明
[Provider Group] ドロップダウン リスト	ユーザがコンソールにログインするときに認証に使用するプロバイダー グループ。 （注） [Provider Group] ドロップダウン リストは、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。
[Two Factor Authentication] チェックボックス	二要素認証は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。 このチェックボックスをオンにすると、コンソールは、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするように求めます。

ステップ 6 [Save Changes] をクリックします。

デフォルト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。 Cisco UCS を通じた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] 領域で、次のフィールドに入力します。

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に定義する必要があります。 • [Radius]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された RADIUS サーバで定義する必要があります。 • [Tacacs]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された TACACS+ サーバで定義する必要があります。 • [Ldap]：ユーザ アカウントは、この Cisco UCS ドメインに対して指定された 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は、ユーザがリモート 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 グループ。 （注） [Provider Group] ドロップダウンは、ユーザを認証する方法として [Ldap]、[Radius]、または [Tacacs] を選択した場合に表示されます。
[Web Session Refresh Period (sec)] フィールド	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、Cisco UCS Manager に更新要求を送信する必要があります。 このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションの終了は行いません。 60 ～ 172800 の整数を指定します。 デフォルトは 600 秒です。

名前	説明
[Web Session Timeout (sec)] フィールド	最後の更新要求から Cisco UCS Manager が Web セッションが終了したと見なすまでの最大経過時間。この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。 60 ～ 172800 の整数を指定します。デフォルトは 7200 秒です。
[Two Factor Authentication] チェックボックス	[Two Factor Authentication] は、[Realm] が [Radius] または [Tacacs] に設定されている場合にのみ使用できます。このチェックボックスを選択すると、Cisco UCS Manager と KVM launch manager は、アカウントが RADIUS または TACACS サーバによって認証されるユーザにトークンとパスワードを入力してログインするように求めます。[Web Session Refresh Period] の期限が切れた場合、ユーザはセッションを続行するために新しいトークンを作成し、そのトークンとパスワードを入力する必要があります。 （注） 二要素認証をイネーブルにして設定を保存した後、デフォルトの [Web Session Refresh Period (sec)] フィールドは 7200、デフォルトの [Web Session Timeout (sec)] フィールドは 8000 に変わります。

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は、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読み取り専用アクセス権が付与されます。セキュリティ上の理由から、Cisco UCS Manager で確立されたユーザ ロールに一致するユーザだけにアクセスを限定するのが望ましい場合もあります。

リモート ユーザのロール ポリシーは、次の方法で設定できます。

assign-default-role

Cisco UCS Manager へのユーザ アクセスをユーザ ロールに基づいて制限しません。その他のユーザ ロールが Cisco UCS Manager で定義されていない限り、すべてのユーザに読み取り専用アクセス権が付与されます。

これはデフォルトの動作です。

no-login

Cisco UCS Manager へのユーザ アクセスをユーザ ロールに基づいて制限します。 リモート認証システムにユーザ ロールが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、ユーザがログインを試行した際に、リモート認証プロバイダーが認証情報を伴うユーザ ロールを提供しない場合にどのように処理するかを決定するために、次のオプション ボタンのいずれかをクリックします。

- [No Login]：ユーザ名とパスワードが正しい場合でも、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，147 ページ
- マルチテナント環境における階層的な名前解決，148 ページ
- ルート組織下の組織の作成，150 ページ
- サブ組織下の組織の作成，150 ページ
- 組織の削除，151 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 ドメインの大きな物理的インフラストラクチャを組織と呼ばれる論理的な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、すべてのユーザにすべての組織へのアクセス権を付与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と、すべての組織が階層的になります。 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対して、次のうちの 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 は、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際に、以下の操作を実行します。

1. Cisco UCS Manager は、サービス プロファイルまたはポリシーに割り当てられている組織内で、指定された名前のポリシーとプールの有無をチェックします。
2. ポリシーを検出したか、使用可能なリソースがプール内にある場合、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内に存在しない場合、Cisco UCS Manager は上位階層の親組織に移動し、同じ名前のプールを検索します。 Cisco UCS Manager は、ルートの組織に到達するまでこの手順を繰り返します。
3. ルート組織まで検索し、使用可能なリソースまたはポリシーを検出できない場合、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. デフォルト プール内で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を検出した場合、Cisco UCS Manager はこのポリシーまたはリソースを使用します。 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 は上位階層の親組織に移動し、デフォルト プールを検索します。 Cisco UCS Manager は、ルートの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 プールとポリシーがサービス プロファイルに割り当てられると、以下の動作が発生します。

1. Cisco UCS Manager は、XYZcustomer サーバ プール内で使用可能なサーバをチェックします。
2. 使用可能なサーバが XYZcustomer サーバ プールに存在する場合、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をチェックします。
3. ルート組織に XYZcustomer サーバ プールが含まれており、そ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 サーバ プールを調べます。
5. ルート組織内のデフォルト 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 プールとポリシーがサービス プロファイルに割り当てられると、以下の動作が発生します。

1. Cisco UCS Manager は、サービス プロファイルに定義されている AP サーバ プールで使用可能なサーバをチェックします。
2. 使用可能なサーバが AP サーバ プールに存在する場合、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 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 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

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，153 ページ
- Cisco UCS のユーザ アカウント，154 ページ
- ユーザ ロール，157 ページ
- ユーザ ロケール，162 ページ
- ユーザ ロールの設定，163 ページ
- ロケールの設定，165 ページ
- ローカル認証されたユーザ アカウントの設定，167 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，175 ページ
- ユーザ セッションのモニタリング，178 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。 各 Cisco UCS Managerで、最大 48 のローカル ユーザ アカウントを設定できます。 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。

管理者アカウント

各 Cisco UCS ドメインには管理者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 アカウントであり、変更や削除はできません。 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。

管理者アカウントは常にアクティブで、有効期限がありません。 管理者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 アカウント

ローカル認証されたユーザアカウントは、ファブリック インターコネクトのを介して直接認証され、admin または aaa 権限の所有者によって有効または無効にできます。 ローカル ユーザ アカウントが無効になっている場合、ユーザはログインできません。 無効化されたローカル ユーザ アカウントの設定の詳細は、データベースから削除されません。 無効化されたローカル ユーザ アカウントを再び有効にすると、そのアカウントは、ユーザ名とパスワードを含め、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 アカウント

リモート認証されたユーザ アカウントとは、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 アカウントを同時に保持している場合は、ローカル ユーザ アカウントで定義されたロールによってリモート ユーザ アカウントのロールが上書きされます。

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。 有効期限に達すると、ユーザ アカウントは無効になります。

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） ユーザ アカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。 ただし、アカウントの有効期限を使用可能な最も遅い日付に設定することは可能です。

Cisco UCS ユーザ名に関するガイドライン

ユーザ名は、Cisco UCS Manager のログイン 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 を割り当てる際は、次のガイドラインおよび制約事項を考慮してください。

- 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 内で一意である必要があります。
- ログイン ID は、英文字から始まる必要があります。 アンダースコアなどの特殊文字や数字から始め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。
- すべてが数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、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 アカウント

次の語は Cisco UCS でローカル ユーザ アカウントを作成するときに使用できません。

- root
- bin
- daemon
- adm
- lp
- sync
- シャットダウン
- halt
- news
- uucp
- operator
- games

- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

Cisco UCS パスワードに関するガイドライン

ローカル認証されるユーザ アカウントのそれぞれにパスワードが必要です。 admin または aaa の権限を持つユーザは、Cisco UCS Manager を設定して、ユーザ パスワードの強度確認を実行できます。 パスワードの強度確認が有効になっている場合は、各ユーザが強力なパスワードを使用する必要があります。

各ユーザが強力なパスワードを設定することを推奨します。 ローカル認証ユーザに対するパスワードの強度確認を有効にすると、Cisco UCS Manager は、次の要件を満たさないパスワードを拒否します。

- 8 ～ 80 文字を含む。
- 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 アカウントのパスワードは空白にしない。

ユーザ アカウントの Web セッション制限

Web セッション制限は、ある時点おいて、特定のユーザ アカウントがアクセス可能な Web セッションの数（GUI と XML の両方）を制限するために、Cisco UCS Manager によって使用されます。

各 Cisco UCS Manager ドメインは、ユーザごとに最大 32 の同時 Web セッションをサポートし、合計 256 のユーザ セッションをサポートします。 デフォルトでは、Cisco UCS Manager が許可する同時 Web セッションはユーザ 1 人あたり 32 に設定されます。ただし、この値はシステム上限である 256 まで設定できます。

ユーザ ロール

ユーザ ロールには、ユーザに許可する操作を定義する 1 つ以上の権限が含まれています。 各ユーザに 1 つ以上のロールを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、割り当てられたすべての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含まれ、Role2 にサーバ関連の権限が含まれている場合、Role1 と Role2 の両方を持つユーザは、ストレージ関連の権限とサーバ関連の権限を持つことになります。

Cisco UCS ドメインには、デフォルトのユーザ 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 のユーザ ロール以降に設定されたユーザ ロールは受け入れられますが、エラーが発生し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、システムのステータスを変更できません。

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 ロールの権限は異なっていますが、両方のロールの権限を組み合わせて、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 アカウントとリモート ユーザ アカウントが同じユーザ名の場合、リモート ユーザに割り当てられているすべてのロールは、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 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。

管理者

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アクセス。 システムの残りの部分に対する読み取りアクセス権。

Network Administrator

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。

動作

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。

Server Compute

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 や vHBA を作成、変更、削除できません。

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

次の単語は、Cisco UCS でカスタム ロールを作成するときに使用できません。

- ネットワーク管理者
- ネットワーク オペレータ
- VDC 管理者
- VDC オペレータ
- 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 これらの権限および権限によってユーザが実行可能なタスクの詳細情報は、http://preview.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html で入手可能な『*Privileges in Cisco UCS*』にあります。

表 *4*：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

特権	説明	デフォルトのロール割り当て
admin	システム管理	管理者
ext-lan-config	外部 LAN 設定	Network Administrator
ext-lan-policy	外部 LAN ポリシー	Network Administrator
ext-lan-qos	外部 LAN QoS	Network Administrator
ext-lan-security	外部 LAN セキュリティ	Network Administrator
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
障害	アラームおよびアラーム ポリシー	動作
operations	ログおよび Smart Call Home	動作
org-management	組織管理	動作
pod-config	ポッド設定	Network Administrator
pod-policy	ポッド ポリシー	Network Administrator
pod-qos	ポッド QoS	Network Administrator
pod-security	ポッド セキュリティ	Network Administrator
power-mgmt	電源管理操作に対する読み取りおよび書き込みアクセス権	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

特権	説明	デフォルトのロール割り当て
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
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 プロファイルの計算	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	Network Administrator
service-profile-network-policy	サービス プロファイル ネットワーク ポリシー	Network Administrator
service-profile-qos	サービス プロファイル QoS	Network Administrator
service-profile-qos-policy	サービス プロファイル QoS ポリシー	Network Administrator
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

特権	説明	デフォルトのロール割り当て
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
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 のユーザ ローケル以降に設定されたユーザ ロケールは受け入れられますが、エラーが発生して非アクティブになります。

admin または aaa の権限を持つユーザは、他のユーザのロケールに組織を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） 次の権限の 1 つ以上を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
- 障害
- 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。
また、[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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[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、こ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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
b) [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) [Organizations] 領域を展開して、Cisco UCS ドメイン内の組織を表示します。
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, （172 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) [Organizations] 領域を展開して、Cisco UCS ドメイン内の組織を表示します。

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

（注） ユーザ アカウントの作成後、Cisco UCS Manager GUI からユーザ アカウントのフィールドのいずれかを変更する場合は、パスワードをもう一度入力する必要があります。

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] の右クリックでもそのオプションにアクセスできます。

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。このアカウントは一意のものであるとともに、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 内で一意である必要があります。 • ログイン ID は、英文字から始まる必要があります。 アンダースコアなどの特殊文字や数字から始め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。 • すべてが数字のログイン ID は作成できません。 • ユーザ アカウントの作成後は、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。

名前	説明
[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。
[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。 パスワード強度チェックを有効にした場合は、ユーザ パスワードを強固なものにする必要があります。Cisco UCS Manager は次の要件を満たしていないパスワードを拒否します。 • 8 ～ 80 文字を含む。 • 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 アカウントのパスワードは空白にしない。
[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。

名前	説明
[Account Expires] チェックボックス	オンにすると、このアカウントは [Expiration Date] フィールドで指定した日付に期限切れになり、それ以降は使用できなくなります。 （注） ユーザ アカウントに有効期限を設定した後、「有効期限なし」に再設定することはできません。ただし、アカウントの有効期限を使用可能な最も遅い日付に設定することは可能です。
[Expiration Date] フィールド	アカウントが期限切れになる日付。 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、SSH 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へのパスワード強度チェックのイネーブル化

パスワードの強度の確認を有効にするには、ユーザが admin または aaa 権限を持っている必要があります。 パスワードの強度の確認が有効になっている場合、Cisco UCS Manager では、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 [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] タブの [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、次回ユーザがログインするまで有効になりません。 ユーザ アカウントへの新しいロールの割り当てや既存のロールの削除を行うときにユーザがログインしている場合、アクティブなセッションは以前のロールや権限を引き続き使用します。

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] タブの [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、ユーザが admin または aaa 権限を持っている必要があります。

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、ユーザが admin または aaa 権限を持っている必要があります。

（注） Cisco UCS Manager GUI を介して無効化されたアカウントのパスワードを変更した場合、アカウントを有効化してアクティブ化した後、ユーザはこの変更されたパスワードを使用できません。 アカウントを有効化してアクティブ化した後に、必要なパスワードを再び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。 変更はできません。
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 のローカル認証されたユーザ全員のパスワード履歴とパスワード変更間隔のプロパティが含まれています。 ローカル認証されたユーザそれぞれ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適用されません。

Password History Count

パスワード履歴カウントによって、ローカル認証されたユーザが何度も同じパスワードを再利用しないようにすることができます。 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これまでに使用した最大 15 個のパスワードを保存します。 パスワードは最近のものから時系列に逆順で格納され、履歴カウントがしきい値に達すると、最も古いパスワードだけが再利用可能になります。

あるパスワードが再利用可能になるまでに、ユーザはパスワード履歴カウントで設定された数だけパスワードを作成して使用する必要があります。 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 番目のパスワードが期限切れになるまで、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。 この値によって履歴カウントが無効化されるため、ユーザはいつでも以前のパスワードを使用できます。

必要に応じて、ローカル認証されたユーザの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有効にできます。

パスワード変更間隔

パスワード変更間隔によって、ローカル認証されたユーザが特定の時間内に実施できるパスワード変更の回数を制限することができます。 次の表は、パスワード変更間隔の 2 つの設定オプションを示しています。

間隔の設定	説明	例
No password change allowed	このオプションを設定すると、ローカル認証されたユーザは、パスワードを変更してから特定の時間内はパスワードを変更できなくなります。 1 ～ 745 時間の変更禁止間隔を指定できます。 デフォルトでは、変更禁止間隔は 24 時間です。	たとえば、ローカル認証されたユーザが 48 時間以内にパスワードを変更できないようにするには、次のように設定します。 • [Change During Interval] を無効に設定 • [No Change Interval] を 48 に設定
Password changes allowed within change interval	このオプションでは、事前に定義した時間内にローカル認証ユーザがパスワードを変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間、パスワード変更の最大回数を 0 ～ 10 に指定できます。 デフォルトでは、ローカル認証されたユーザは、48 時間以内に最大 2 回パスワードを変更できます。	たとえば、ローカル認証されたユーザがパスワードを変更した後 24 時間以内に最大 1 回それを変更できるようにするには、次のように設定します。 • [Change During Interval] を有効に設定 • [Change Count] を 1 に設定 • [Change Interval] を 24 に設定

変更間隔のパスワード変更の最大数の設定

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、 をクリックします。

b) [Change Count] フィールド で、[Change Interval] の間に、ローカル認証されたユーザが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 から自由に設定できます。

c) [Change Interval] フィールドで、[Change Count] フィールドで指定したパスワード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 時間から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、ローカル認証されたユーザは 48 時間以内に 2 回以上パスワードを変更できません。

ステップ 5 [Save Changes] をクリックします。

パスワードの変更禁止間隔の設定

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、 をクリックします。

b) [No Change Interval] フィールドで、新たに作成したパスワードが変更可能になるまでに、ローカル認証されたユーザが待つ必要がある最小時間数。 を入力します。
この値は、1 ～ 745 時間から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、ローカル認証されたユーザが、以前 [History Count] フィールド で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 から自由に設定できます。

デフォルトでは、[History Count] フィールドは 0 に設定されます。この値によって履歴カウントが無効化されるため、ユーザはいつでも以前のパスワードを使用できます。

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、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。

名前	説明
[Refresh Period] カラム	Cisco UCS Manager に接続している場合、Web クライアントは、Web セッションをアクティブに保つために、Cisco UCS Manager に更新要求を送信する必要があります。 このオプションを使用して、このドメインのユーザに許可する更新要求間隔の最大時間数を指定します。 この時間制限を超えると、Cisco UCS Manager は Web セッションを非アクティブであると見なしますが、セッションの終了は行いません。
[Session Timeout] カラム	最後の更新要求から Cisco UCS Manager が Web セッションが終了したと見なすまでの最大経過時間。 この時間制限を超えると、Cisco UCS Manager は自動的に Web セッションを終了させます。
[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] が表示された場合は、関連するユーザ セッションが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，181 ページ
- DNS サーバの追加，182 ページ
- DNS サーバの削除，182 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、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 アドレスを使用する必要があり、IPv4 または IPv6 アドレスのいずれかを使用できます。各Cisco UCS ドメインに対し最大 4 台の DNS サーバを設定できます。

（注） 複数の DNS サーバを設定する場合、システムによるサーバの検索順はランダムになります。ローカル管理コマンドが DNS サーバの検索を必要とする場合、3 台の DNS サーバのみをランダムに検索します。

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、DNS サーバの IPv4 または IPv6 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。

- ラック サーバ ディスカバリ ポリシーの設定，183 ページ
- MAC アドレス テーブルのエージング タイムの設定，184 ページ

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 ポリシーは、新しいラックマウント サーバを追加したときのシステムの対処方法を決定します。 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 ディスク上のデータをスクラビングするかどうか、サーバ検出をただちに開始するかユーザの明示的な確認応答を待つ必要があるかを決定します。

Cisco UCS Manager では、正しく配線されておらず、ファブリック インターコネクトに接続されていないラックマウント サーバは検出できません。 サポート対象の 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、適切な『rack-mount server integration guide（ラックマウント サーバのインストール 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、新しいラック サーバが追加されたときに実行させるアクションとスクラブ ポリシーを指定します。

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、エージング タイムと期間を指定します。

ステップ 6 [Save Changes] をクリックします。

第 13 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，187 ページ
- 仮想インターフェイスの予約管理とエラー処理，188 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 プロファイルに対して設定可能な vNIC と 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）のネームスペースの量で決まります。 Cisco UCS では、VIF ネームスペースの各部分は VIF という固まりで割り当てられます。 ハードウェアによっては、VIF の最大数が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 つを使用します。

次の変数はブレード サーバで利用可能な VIF の数に影響するため、サービス プロファイルに設定可能な vNIC と vHBA の数にも影響します。

- ファブリック インターコネクトでサポートされる VIF の最大数
- ファブリック インターコネクトがどのように接続されているか
- 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かどうか

ご使用のハードウェア設定でサポートされる VIF の最大数について詳しくは、該当するソフトウェア リリースの『*Cisco UCS 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予約管理とエラー処理

ポートチャネルでグループ化されたファブリック インターコネクトの場合、I/O モジュールへのファブリック インターコネクトの接続方法を変更すると、ブレードサーバで使用可能な VIF の数が大幅に変化します。 変更の影響を追跡できるように、Cisco UCS Manager には次のメトリックが保持されます。

- ハードウェアがサポートする VIF の最大数
- 接続タイプ

ブレードで使用可能な VIF の数を削減するように設定を変更すると、UCS Manager は警告を表示し、続行するかどうか確認を求めます。 これには、接続の追加または変更によって VIF の数を削減する場合など、いくつかの状況があります。

第 14 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，189 ページ
- Cisco UCS Manager と Cisco UCS Central 間のポリシー解決，190 ページ
- Cisco UCS Central への Cisco UCS ドメインの登録，191 ページ
- Cisco UCS Manager GUI を使用した Cisco UCS Manager と Cisco UCS Central 間のポリシー解決の変更，192 ページ
- Cisco UCS Central からの Cisco UCS ドメインの登録解除，193 ページ

Cisco UCS ドメインの登録

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

Cisco UCS Centralに Cisco UCS ドメイン を管理させる場合、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、Cisco UCS Centralと Cisco UCS Manager でそれぞれ管理するポリシー タイプやその他の設定（バックアップやファームウェアなど）を選択する必要があります。 Cisco UCS Centralによって、登録されたすべての Cisco UCS ドメイン で同じポリシー タイプおよび設定を管理するか、または登録された各 Cisco UCS ドメイン に異なる設定を行うこともできます。

Cisco UCS Centralに Cisco UCS ドメインを登録する前に、以下を実行します。

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

（注） Cisco UCS Central に登録されているドメインでは、Cisco UCS Manager で使用される IP アドレスの変更や交換はできません。 その IP アドレスを変更または交換する必要がある場合は、まず Cisco UCS Central から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交換した後で、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 に対して、特定のポリシーや設定を管理するアプリケーションを選択できます。 このポリシー解決は、同じ Cisco UCS Central に登録するすべての Cisco UCS ドメイン で同じである必要はありません。

これらのポリシーおよび設定を解決するには、次のオプションを使用します。

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

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

名前	説明
[Infrastructure & Catalog Firmware]	機能カタログとインフラストラクチャ ファームウェア ポリシーが、ローカルで定義されるかまたは Cisco UCS Central から取得されるかを決定します。
[Time Zone Management]	日付と時刻がローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[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 ポリシー設定を、ローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[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]	認証およびネイティブ ドメイン、LDAP、RADIUS、TACACS+、トラストポイント、ロケールおよびユーザ ロールをローカルまたは Cisco UCS Central のどちらで定義するかを決定します。
[DNS 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。

Cisco UCS Central への Cisco UCS ドメインの登録

名前	説明
[Backup & Export Policies]	Full State バックアップ ポリシーおよび All Configuration エクスポート ポリシーが、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、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]	管理対象エンドポイントがローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[Power Management]	電源管理がローカルまたは Cisco UCS Central のどちらで定義されるかを決定します。
[Power Supply Unit]	電源モジュ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。

Cisco UCS Central への Cisco UCS ドメインの登録

（注） Cisco UCS Central に登録されているドメインでは、Cisco UCS Manager で使用される IP アドレスの変更や交換はできません。 その IP アドレスを変更または交換する必要がある場合は、まず Cisco UCS Central から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交換した後で、Cisco UCS ドメイン を再登録できます。

はじめる前に

Cisco UCS Manager と Cisco UCS Central の両方において NTP サーバと正しいタイム ゾーンを設定し、それらが同期していることを確認します。 Cisco UCS ドメインと Cisco UCS Central の日時が同期していないと、登録に失敗する可能性があります。

手順

ステップ 1 [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 [Actions] 領域の、[UCS Central] をクリックします。

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

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

a) 次のフィールドに入力します。

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

b) [Policy Resolution Control] 領域の各フィールドで、次のいずれかのオプション ボタンをクリックします。
   - [Local]：ポリシーまたは設定は、Cisco UCS Manager によって決定および管理されます。
   - [Global]：ポリシーまたは設定は、Cisco UCS Central によって決定および管理されます。

c) [OK] をクリックします。

Cisco UCS Manager GUI を使用した 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 [Actions] 領域の、[UCS Central] をクリックします。

ステップ 5 [Policy Resolution Control] 領域の各フィールドで、次のいずれかのオプション ボタンをクリックします。
   - [Local]：ポリシーまたは設定は、Cisco UCS Manager によって決定および管理されます。

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

ステップ 6 [Save Changes] をクリックします。

Cisco UCS Central からの Cisco UCS ドメインの登録解除

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

手順

ステップ 1 [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 [Actions] 領域の、[UCS Central] をクリックします。
ステップ 5 [Actions] 領域で、[Unregister From UCS Central] をクリックします。
ステップ 6 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 15 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，195 ページ
- LAN アップリンク マネージャの起動，196 ページ
- LAN アップリンク マネージャでのポートの設定，196 ページ
- サーバ ポートの設定，197 ページ
- アップリンク イーサネット ポートの設定，197 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，199 ページ
- LAN ピン グループの設定，201 ページ
- ネームド VLAN の設定，203 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，204 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のインターフェイスを備えています。 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。

- アップリンクのイーサネット 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 マネージャでのポートの設定

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 ポートを設定するノードを展開します。
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。

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。

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

ステップ 5 [Add Ports] パネルで、追加するポートを指定します。

（注） Cisco UCS Manager では、サーバ ポートとして設定済みのポートを選択した場合、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、追加するポートを指定します。

（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、 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 グループを vNIC テンプレートに含めます。

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

ID が 3968 ～ 4047 の VLAN は作成できません。 この範囲の VLAN ID は予約されています。

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

手順

ステップ 1 [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、必須フィールドを指定し、[OK] をクリックします。
プライベート VLAN は Cisco UCS Mini ではサポートされません。

ステップ 4 [OK] をクリックします。
Cisco UCS Manager は、VLAN を次の [VLAN] ノードのいずれかに追加します。

- 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 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）。 Cisco UCS Mini の場合、パケットの破棄は Platinum クラスと Gold クラスでのみオフにできます。
[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。 Cisco UCS Mini の場合、このオプションはすべてのクラスで無効になります。

ステップ 3 次のどちらかを実行します。

- [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 16 章

VLAN の設定

この章の内容は、次のとおりです。

- ネームド VLAN，207 ページ
- VLAN ポートの制限，208 ページ
- ネームド VLAN の設定，210 ページ
- VLAN ポート数の表示，212 ページ
- VLAN グループ，213 ページ
- VLAN 権限，215 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 VLAN 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 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

ID が 3968 ～ 4047 の VLAN は作成できません。 この範囲の VLAN ID は予約されています。

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

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

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

VLAN 名の大文字と小文字は区別されます。

VLAN ポートの制限

Cisco UCS Manager では、1 つのファブリック インターコネクト上の境界ドメインとサーバ ドメインで設定可能な VLAN ポート インスタンスの数は 6000 に制限されます。

VLAN ポート数に含まれるポートのタイプ

次のタイプのポートが VLAN ポートの計算でカウントされます。

- ボーダー アップリンク イーサネット ポート
- ボーダー アップリンク イーサチャネル メンバ ポート
- SAN クラウドの FCoE ポート
- NAS クラウドのイーサネット ポート
- サービス プロファイルによっ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のポート 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 ポート制限を実行します。 Cisco UCS Manager は、制御トラフィック用に事前定義されたいくつかの VLAN ポート リソースを予約します。 これには、HIF および NIF ポートに設定された管理 VLAN が含まれます。

VLAN ポートの制限の実行

Cisco UCS Manager は、次の操作中に VLAN ポートのアベイラビリティを検証します。

- 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
- クラウドへの VLAN の追加またはクラウドからの VLAN の削除
- SAN 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 での VLAN の設定または設定解除
- VMWare vNIC から、ESX ハイパーバイザから作成通知または削除通知を受け取ったとき

（注） これは、Cisco UCS Manager の制御外です

- 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 プロファイルの動作に対して厳密な VLAN ポート制限を適用します。 VLAN ポート制限を超過したことを Cisco UCS Manager が検出した場合、サービス プロファイル設定は展開時に失敗します。

境界ドメインでの VLAN ポート数の超過は、それほど混乱をもたらしません。 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を設定解除する
- LAN クラウドから VLAN を削除する
- 1 つ以上の vNIC または vHBA を設定解除する

ネームド VLAN の設定

ネームド VLAN の作成

ハイ アベイラビリティが設定されている Cisco UCS ドメインでは、ネームド VLAN を作成して、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、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可能です。

重要 ID が 3968 ～ 4047 の VLAN は作成できません。 この範囲の VLAN ID は予約されています。

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

手順

ステップ 1 [Navigation] ペインの [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、必須フィールドに値を入力します。
プライベート VLAN は Cisco UCS Mini ではサポートされません。

ステップ 6 [Check Overlap] ボタンをクリックした場合は、以下を行ってください。

a) [Overlapping VLANs] タブをクリックしてフィールドを確認し、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。

b) [Overlapping VSANs] タブをクリックしてフィールドを確認し、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。

c) [OK] をクリックします。

d) Cisco UCS Manager が重複している VLAN ID または FCoE VLAN ID を確認した場合は、VLAN ID を既存の VLAN と重複しないものに変更してください。

ステップ 7 [OK] をクリックします。
Cisco UCS Manager は、VLAN を次の [VLAN] ノードのいずれかに追加します。

- 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 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、セカンダリ VLAN を動作している別のプライマリ VLAN に必ず再割り当てします。

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、その VLAN がすべての vNIC と vNIC テンプレートから削除されていることを確認します。

（注） vNIC または vNIC テンプレートに割り当てられている VLAN を削除すると、vNIC によって VLAN がフラップす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] 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。

サブタブ	説明
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。

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
[Port VLAN Limit] フィールド	このファブリック インターコネクトの最大許容 VLAN ポート数。
[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 ポートの割り当て状態。

VLAN グループ

VLAN グループでは、イーサネット アップリンク ポートの VLAN を機能別または特定のネットワークに属する VLAN 別に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 ポートに適用することができます。

インバンドおよびアウトオブバンド（OOB）VLAN グループを設定し、それを使用してブレードおよびラック サーバの Cisco Integrated Management Interface（CIMC）にアクセスすることができます。 Cisco UCS Manager は、アップリンク インターフェイスまたはアップリンク ポート チャネルでの OOB IPv4 およびインバンド IPv4/IPv6 VLAN グループの使用をサポートします。

VLAN を VLAN グループに割り当てた後、VLAN グループに対する変更は VLAN グループで設定された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 グループによって、分離 VLAN 間での VLAN の重複を識別することができます。

VLAN グループ下にアップリンク ポートを設定できます。 VLAN グループ用のアップリンク 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 VLAN のみをサポートします。

[LAN Cloud] または [LAN Uplinks Manager] から VLAN グループを作成できます。

VLAN グループの作成

[VLAN 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。 サービス プロファイルを使用したインバンドおよびアウトオブバンドアクセスに使用する別の VLAN グループを作成できます。

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 [LAN Cloud] を右クリックし、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] ダイアログボックスで、名前および VLAN を指定し、[Next] をクリックします。

ステップ 5 （任意）[Add Uplink Ports] ダイアログボックスで、表示されたリストから [Uplink Ports] を選択して [Selected Uplink Ports] に追加し、[Next] をクリックします。

ステップ 6 （任意）[Add Port Channels] ダイアログボックスで、[Port Channels] を選択して [Selected Port Channels] に追加し、[Next] をクリックします。

ステップ 7 （任意）[Org Permissions] ダイアログボックスで、表示されたリストから適切なグループを選択し、[Next] をクリックします。

ここで作成しているグループに属する VLAN は、ここで選択するグループにだけアクセスできます。

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] の下の [VLAN Groups] のリストに追加されます。

VLAN グループのメンバーの編集

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 メンバーである VLAN を編集する 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 VLAN グループを右クリックして、[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、表示されたリストの追加または除外する VLAN を選択して [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] を選択してそれらを [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。
ここで作成しているグループに属する VLAN は、ここで選択するグループにだけアクセスできます。

ステップ 9 [Finish] をクリックします。

ステップ 10 この VLAN グループがユーザの選択にしたがって変更されます。

VLAN グループに対する組織のアクセス権限の変更

VLAN グループに対する組織のアクセス権限を変更すると、権限の変更がその VLAN グループ内のすべての 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] を展開して、[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] の [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、次の手順を実行します。

- 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 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 権限

VLAN 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 権限は、VLAN が属してい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の 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 権限はオプションの機能であり、デフォルトでは無効になっています。 この機能は、要件に応じて有効または無効にできま

す。 この機能を無効にすると、すべての VLAN にすべての組織からグローバルでアクセスできるようになります。

（注） [LAN] > [LAN Cloud] > [Global Policies] > [Org Permissions] の順で組織権限を有効にすると、VLAN の作成時に、[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] を有効にしないと、[Permitted Orgs for VLAN(s)] オプションは表示されません。

組織権限を有効にした場合は、VLAN の作成時に VLAN に対して組織を指定します。 組織を指定すると、その VLAN は特定の組織とその下にあるすべてのサブ組織で利用可能になります。 他の組織のユーザはこの VLAN にアクセスすることはできません。 また、VLAN 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できます。

注意 VLAN の組織権限をルート レベルで組織に割り当てると、すべてのサブ組織が VLAN にアクセスできるようになります。 ルート レベルで組織権限を割り当てた後で、サブ組織に属する VLAN の権限を変更すると、その VLAN はルート レベルの組織で使用できなくなります。

VLAN 権限のイネーブル化

VLAN 権限は、デフォルトで無効になっています。 異なる組織ごとに権限を作成して VLAN アクセスを制限する場合は、組織の権限オプションを有効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 権限のディセーブル化

VLAN 権限は、デフォルトで無効になっています。 このオプションを有効にして VLAN 権限を異なるネットワーク グループに割り当て、その後はこのオプションを使用しない場合は、このオプションをグローバルに無効できます。 VLAN の組織の権限機能が無効になっている場合は、VLAN に割り当てた権限はシステムにまだ存在しますが、有効ではありません。 組織の権限を後で使用

する必要が生じた場合は、この機能を有効にして、割り当てられている権限を使用することができます。

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] > [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] セクションの [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無効にされた場合、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 権限の追加または変更

VLAN を許可された組織を追加または削除できます。

（注） 組織を、VLAN を許可された組織として追加する場合、すべての子組織が VLAN にアクセスできます。 組織から VLAN へのアクセス権を削除すると、すべての子組織は 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] を展開して、[VLAN name] を選択をします。

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 17 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，219 ページ
- LAN ピン グループの作成，220 ページ
- LAN ピン グループの削除，221 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。 その後、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）

vNIC ポリシーを使用してピン グループがサーバ 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用としてアップリンク 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。

アップリンクが LAN ピン グループに属している場合、そのアップリンクは所属グループ専用に予約されているわけではありません。 LAN ピン グループを指定していない他の vNIC ポリシーは、動的なアップリンクとしてそのアップリンクを使用できます。

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 グループを vNIC テンプレートに含めます。

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 18 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，223 ページ
- MAC プールの作成，224 ページ
- MAC プールの削除，225 ページ

MAC プール

MAC プールは、ネットワーク ID（MAC アドレス）の集合です。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 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。 その後、vNIC ポリシーは、そのサーバに割り当てられたサービス プロファイルに取り込まれます。

独自の MAC アドレスを指定することも、シスコから提供された 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 [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	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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	MAC プールの説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[割り当て順序] フィールド	次のいずれかになります。 • [デフォルト]：Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル]：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] 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 MAC Address] フィールド	ブロック内の最初の MAC アドレス。
[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 プールを vNIC テンプレートに含めます。

MAC プールの削除

プールを削除した場合、Cisco UCS Manager は、 でそのプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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 19 章

Quality of Service の設定

この章の内容は、次のとおりです。

- Quality of Service，227 ページ
- システム クラスの設定，228 ページ
- Quality of Service ポリシーの設定，230 ページ
- フロー制御ポリシーの設定，232 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。

- 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システム全体にわたって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

Cisco UCS Mini での Quality of Service に関するガイドラインおよび制限事項

- Cisco UCS Mini では、すべてのシステム クラスで共有バッファが使用されます。
- Bronze クラスは SPAN とバッファを共有します。 SPAN または Bronze クラスを使用することを推奨します。
- マルチキャスト最適化はサポートされません。
- あるクラスの QoS パラメータを変更すると、すべてのクラスのトラフィックが中断されます。
- イーサネット トラフィックと FC または FCoE トラフィックが混在している場合は、帯域が均等に配分されません。

- 同じクラスからの複数のトラフィック ストリームが均等に分配されないことがあります。
- FC または FCoE のパフォーマンス問題を回避するために、すべての破棄なしポリシーに同じ CoS 値を使用してください。
- Platinum クラスと Gold クラスのみが破棄なしポリシーをサポートしています。

システム クラスの設定

システム クラス

Cisco UCS は、DCE（Data Center Ethernet）を使用して、Cisco UCS ドメイン内のすべてのトラフィックを処理します。 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（QoS）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 クラスは特定のタイプのトラフィック用に帯域幅の特定のセグメントを予約します。これにより、過度に使用されるシステムでも、ある程度のトラフィック管理が提供されます。 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 *5*：システム クラス

システム クラス	説明
プラチナ ゴールド シルバー ブロンズ	サービスプロファイルの QoS ポリシーに含めることが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。 Cisco UCS Mini の場合、パケットの破棄は Platinum クラスと Gold クラスでのみ無効にできます。 1 つの Platinum クラスと 1 つの Gold クラスのみを no-drop クラスとして同時に設定できます。
ベスト エフォート	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 QoS 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 クラスは無効にできません。

システム クラス	説明
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 クラスは無効にできません。 （注） FCoE トラフィックには、他のタイプのトラフィックで使用できない、予約された QoS システム クラスがあります。 他のタイプのトラフィックに FCoE で使用される CoS 値がある場合、その値は 0 にリマークされます。

QoS システム クラスの設定

重要 すべての破棄なしポリシーで UCS および N5K に同じ CoS（サービス クラス）値を使用します。 エンドツーエンド PFC が正常に動作することを保証するには、すべての中間スイッチで同じ QoS ポリシーを設定します。

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 [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。 MTU の最大値は 9216 です。

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クラス オブ サービス（CoS）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、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

次の作業

QoS ポリシーを vNIC または vHBA テンプレートに含めます。

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 クラスを無効にした場合、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有効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り設定されます。

送信機能を有効にした場合、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。受信機能を有効にした場合、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有効にした場合は、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、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

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 20 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，235 ページ
- イーサネット アダプタ ポリシーの設定，241 ページ
- デフォルトの vNIC 動作ポリシーの設定，248 ページ
- LAN 接続ポリシーの設定，249 ページ
- ネットワーク制御ポリシーの設定，257 ページ
- マルチキャスト ポリシーの設定，259 ページ
- LACP ポリシーの設定，261 ページ
- UDLD リンク ポリシーの設定，263 ページ
- VMQ 接続ポリシーの設定，268 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。

vNIC テンプレートを作成する際に、Cisco UCS Manager では正しい設定で VM-FEX ポート プロファイルが自動作成されません。 VM-FEX ポート プロファイルを作成するには、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。

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

（注） サーバに 2 つの Emulex NIC または QLogic NIC（Cisco UCS CNA M71KR-E または Cisco UCS CNA M71KR-Q）がある場合は、両方の NIC にユーザ定義の MAC アドレスが取得されるように、サービス プロファイルで両方のアダプタの vNIC ポリシーを設定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でも、Windows は PCI バス上で両方の NIC を検出します。 2 番目のイーサネットがサービス プロファイルに含まれていないため、Windows はそれにハードウェア MAC アドレスを割り当てます。 その後でサービス プロファイルを異なるサーバに移動すると、Windows によって追加の NIC が検出されますが、これは 1 つの NIC でユーザ定義の MAC アドレスが取得されなかったためです。

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
[名前] フィールド	仮想ネットワーク インターフェイス カード（vNIC）テンプレートの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[ファブリック 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。 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、[フェールオーバーの有効化] チェックボックスをオンにします。 （注） 次の状況下では、vNIC ファブリック フェールオーバーを有効化しないでください。 • Cisco UCS ドメインイーサネット スイッチ モードで動作している場合。 vNIC ファブリック フェールオーバーは、そのモードではサポートされません。 1 つのファブリック インターコネクト上のすべてのイーサネット アップリンクが障害になった場合、vNIC は他のイーサネット アップリンク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）があるサーバに、このテンプレートから作成された 1 つ以上の vNIC を関連付ける予定がある場合。 これを行った場合、Cisco UCS Manager により、サービス プロファイルとサーバを関連付けたときに設定エラーが生成されます。

名前	説明
[ターゲット] 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って、Cisco UCS Manager が、vNIC テンプレートの適切な設定を使用して、自動的に VM-FEX ポート プロファイルを作成するかどうかが決まります。 次のいずれかになります。 • [アダプタ] : 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した場合、VM-FEX ポート プロファイルが作成されません。 • [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した場合、VM-FEX ポート プロファイルが作成されます。
[テンプレートのタイプ] フィールド	次のいずれかになります。 • [初期テンプレート] : 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。 • [テンプレートの更新] : 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。 （注） VLAN と PVLAN を同じ vNIC に割り当てることはできません。
[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） vNIC テンプレートに QoS ポリシーが関連付けられている場合、ここで指定された MTU は、関連付けられている QoS システム クラスで指定された MTU 以下であることが必要です。 この MTU 値が QoS システム クラスの MTU 値を超えている場合、データ転送中にパケットがドロップされる可能性があります。
[MACプール] 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ポリシー] 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。
[ネットワーク制御ポリシー] 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。
[ピングループ] 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。
[統計しきい値ポリシー] 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。
接続ポリシー	ダイナミック vNIC、usNIC、または VMQ など、3 種類のオプション ボタンから 1 つを選択します。 ここでの選択に基づいて、ドロップダウン リストから適切な接続ポリシーを選択します。

ステップ 6 [OK] をクリックします。

次の作業

vNIC テンプレートをサービス プロファイルに含めます。

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 により、vNIC テンプレートで定義された値を使って vNIC が設定されます。 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 により 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 を含むサービス プロファイルがすでにサービス プロファイル テンプレートにバインドされている場合、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 vNIC とバインドする サービス プロファイル が含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [*Service_Profile_Name*] > [vNICs] の順に展開します。

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] の順に展開します。

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

名前	説明
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Owner] フィールド	次のいずれかになります。 • [Local]：このポリシーは、Cisco UCS ドメイン内のサービス プロファイルとサービス プロファイル テンプレートでのみ使用できます。 • [Pending Global]：このポリシーの制御は Cisco UCS Central に移行中です。 移行が完了すると、このポリシーは Cisco UCS Central に登録されているすべての Cisco UCS ドメインで使用可能になります。 • [Global]：このポリシーは Cisco UCS Central によって管理されます。 このポリシーを変更する場合は、必ず Cisco UCS Central を使用して変更してください。

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。
[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。

名前	説明
[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る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、インターフェイスが受信するパケットにのみ影響します。
[TCP Segmentation Offload] フィールド	次のいずれかになります。 • [Disabled]：大きい TCP パケットは CPU で分割されます。 • [Enabled]：大きい TCP パケットは、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にのみ影響します。

名前	説明
[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は、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、インターフェイスが受信する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、別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。
[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。

名前	説明
[Interrupt Coalescing Type] フィールド	次のいずれかになります。 • [Min]：システムは、別の割り込みイベントを送信する前に、[Interrupt Timer] フィールドで指定された時間だけ待機します。 • [Idle]：少なくとも [Interrupt Timer] フィールドで指定された時間の長さだけアクティビティがない状態が続くまで、システムは割り込みを送信しません。
[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 システムで MRQS 用の eNIC サポートをイネーブル化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 での Multiple Receive Queue Support（MRQS）機能向けの eNIC サポートが含まれます。

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）= Enabled
- 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, （243 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（Linux 用 Cisco UCS 仮想インターフェイス カード ドライバ インストレーション ガイド）』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 動作ポリシーの設定

デフォルトの vNIC 動作ポリシー

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

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

- [None]：Cisco UCS Manager は、サービス プロファイルにデフォルトの 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 プロファイルが vNIC を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられている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、[HW Inherit] がデフォルトで使用されます。

デフォルトの vNIC 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 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 動作の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オプション ボタンの内の 1 つをクリックします。

- [None]：Cisco UCS Manager は、サービス プロファイルにデフォルトの 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 プロファイルが vNIC を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられている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 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 と vHBA を識別します。

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

LAN および SAN の接続ポリシーに必要な権限

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

接続ポリシーの作成に必要な権限

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

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

接続ポリシーをサービス プロファイルに追加するために必要な権限

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

サービス プロファイルと接続ポリシー間の相互作用

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

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

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

の vNIC 設定がすべて消去されます。SAN 接続ポリシーを含めた場合は、そのサービス プロファイル内の既存の vHBA 設定がすべて消去されます。

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と説明を入力します。

名前	説明
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 6 次のどちらかを実行します。

- LAN 接続ポリシーに vNIC を追加するには、ステップ 7 に進みます。

- LAN 接続ポリシーに iSCSI vNIC を追加し、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 ボックスで、次のフィールドに値を入力します。

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] バーを展開し以下を行います。

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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC に関連付けられた LAN vNIC（存在する場合）。
[iSCSI Adapter Policy] ドロップダウン リスト	この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー（存在する場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI アダプタを作成するには、このリンクをクリックします。
[VLAN] ドロップダウン リスト	この iSCSI vNIC に関連付けられた仮想 LAN。 デフォルトの VLAN は [default] です。 （注） Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合は、オーバレイ vNIC のネイティブ VLAN と同じ VLAN を指定する必要があります。 Cisco UCS M51KR-B Broadcom BCM57711の場合は、オーバーレイ vNIC に割り当てられているどの VLAN でも指定できます。

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 アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。 このサービス プロファイルに関連付けるサーバに Cisco UCS M81KR 仮想インター

フェイス カードまたは Cisco UCS VIC-1240 仮想インターフェイス カードがある場合は、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るサーバに Cisco UCS NIC M51KR-Bがある場合は、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、[MAC Address] フィールドにアドレスを入力します。 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、プール カテゴリが 2 つ存在することがあります。 ドメイン プールは Cisco UCS ドメインでローカルに定義され、グローバル プールは、Cisco UCS Central で定義されます。

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] ウィザードで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, （224 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

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

LAN 接続ポリシー用の 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 [vNIC] 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。
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 [vNICs] 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 接続ポリシー用の 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 バーの、[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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC に関連付けられた LAN vNIC（存在する場合）。
[iSCSI Adapter Policy] ドロップダウン リスト	この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー（存在する場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI アダプタを作成するには、このリンクをクリックします。
[VLAN] ドロップダウン リスト	この iSCSI vNIC に関連付けられた仮想 LAN。 デフォルトの VLAN は [default] です。 （注） Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合は、オーバレイ vNIC のネイティブ VLAN と同じ VLAN を指定する必要があります。 Cisco UCS M51KR-B Broadcom BCM57711の場合は、オーバーレイ vNIC に割り当てられているどの VLAN でも指定できます。

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 アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。 このサービス プロファイルに関連付けるサーバに Cisco UCS M81KR 仮想インターフェイス カード または Cisco UCS VIC-1240 仮想インターフェイス カードがある場合は、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るサーバに Cisco UCS NIC M51KR-Bがある場合は、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、[MAC Address] フィールドにアドレスを入力します。 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、プール カテゴリが 2 つ存在することがあります。 ドメイン プールは Cisco UCS ドメインでローカルに定義され、グローバル プールは、Cisco UCS Central で定義されます。

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] ウィザードで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, （224 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る LAN 接続ポリシーを削除する場合、すべての vNIC と iSCSI vNIC をそのサービス プロファイルから削除し、そのサービス プロファイルに関連付けられているサーバの LAN データ トラフィックを中断します。

手順

ステップ 1 [Navigation] ペインの [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 Cisco UCS ドメインのネットワーク制御を設定するもので、次の設定も含まれます。

- Cisco Discovery Protocol（CDP）の有効化/無効化
- 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の、仮想インターフェイス（VIF）の動作方法
- 関連付けられているボーダー ポートの障害時に、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 vFibre チャネル インターフェイスで Cisco UCS Manager が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、異なる MAC アドレスをサーバが使用できるかどうか
- MAC 登録を VNIC ごとに実行するか、またはすべての VLAN に対して実行するか

[アップリンクのアクションに失敗しました] プロパティ

デフォルトでは、ネットワーク制御ポリシー内の [アップリンクのアクションに失敗しました] プロパティは、リンクダウンの値を使用して設定されます。 Cisco UCS M81KR 仮想インターフェイス カードなどのアダプタの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Manager に対して vEthernet または vFibre チャネル インターフェイスをダウンさせるように指示します。 Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの、イーサネットと FCoE トラフィックの両方をサポートする VM-FEX 非対応の統合型ネットワーク アダプタを使用する Cisco UCS システムの場合、このデフォルトの動作では、関連付けられたボーダ ポートに障害が発生した場合に、Cisco UCS Manager に対してリモート イーサネット インターフェイスをダウンさせるように指示します。 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ている vFibre チャネル インターフェイスもダウンします。

（注） このセクションに記載されている VM-FEX 非対応の統合型ネットワーク アダプタのタイプが実装に含まれ、そのアダプタがイーサネットと FCoE の両方のトラフィックを処理することが予想される場合は、警告の値を使用して [アップリンクのアクションに失敗しました] プロパティを設定することをお勧めします。 ただし、この設定にすると、ボーダ ポートがダウンした場合に、イーサネット チーミング ドライバでリンク障害を検出できなくなる場合があります。

MAC 登録モード

MAC アドレスは、ネイティブ VLAN でのみデフォルトでインストールされます。これにより、ほとんどの実装で VLAN ポート数が最大になります。

（注） トランキング ドライバがホスト上で実行され、インターフェイスがプロミスキャス モードになっている場合、Mac 登録モードをすべての VLAN に設定することをお勧めします。

ネットワーク制御ポリシーの作成

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 [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、必須フィールドに値を入力します。
ステップ 6 [OK] をクリックします。

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）のスヌーピングおよびIGMP クエリアの設定に使用されます。 IGMP スヌーピングは、特定のマルチキャスト伝送に含まれるべき 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、削除できます。 マルチキャスト 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が再処理され変更が適用されます。デフォルトでは、IGMP スヌーピングが有効になり、IGMP クエリアが無効になります。

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、名前と IGMP スヌーピング情報を指定します。
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） 作成後にマルチキャスト ポリシーの名前を変更することはできません。

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、必要に応じてフィールドを編集します。
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 にデフォルト以外の（ユーザ定義）マルチキャスト ポリシーを割り当て、そのマルチキャスト ポリシーを削除すると、関連付けられた VLAN は削除済み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 ポリシーからマルチキャスト ポリシー設定を継承します。

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。

LACP ポリシーの設定

LACP ポリシー

リンク集約は、複数のネットワーク接続を並列に組み合わせて、スループットを向上させ、冗長性を実現します。 Link Aggregation Control Protocol（LACP）は、それらのリンク集約グループにさらに利点をもたらします。 Cisco UCS Manager では、LACP ポリシーを使用して LACP のプロパティを設定することができます。

LACP ポリシーには以下を設定できます。

- **個別一時停止**：LACP でアップストリーム スイッチのポートを設定しない場合、ファブリック インターコネクトは、すべてのポートをアップリンク イーサネット ポートとして扱い、パケットを転送します。 ループを回避するために、LACP ポートを一時停止状態にすることができます。 LACP を使用してポートチャネルに個別一時停止を設定すると、そのポートチャネルの一部であるポートがピア ポートから PDU を受信しない場合、そのポートは一時停止状態になります。
- **タイマー値**：rate-fast または rate-normal を設定できます。 rate-fast 設定では、ポートはピア ポートから 1 秒ごとに 1 PDU を受信します。 このタイムアウトは 3 秒です。 rate-normal 設定では、ポートは 30 秒ごとに 1 PDU を受信します。 このタイムアウトは 90 秒です。

システムの起動時に、デフォルトの LACP ポリシーが作成されます。 このポリシーを変更したり、新規のポリシーを作成できます。 また、複数のポートチャネルに 1 つの LACP ポリシーを適用することもできます。

LACP 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 [Work] ペインで、[LACP Policies] タブをクリックし、[+] 記号をクリックします。
ステップ 5 [Create LACP Policy] ダイアログ ボックスで、必須フィールドに入力します。
ステップ 6 [OK] をクリックします。

LACP ポリシーの変更

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 [Work] ペインの [LACP Policies] タブで、編集するポリシーをクリックします。
ステップ 5 右側の [Properties] アイコンをクリックします。
ステップ 6 [Properties] ダイアログ ボックスで、必要な変更を行って [Apply] をクリックします。
ステップ 7 [OK] をクリックします。

UDLD リンク ポリシーの設定

UDLD の概要

UniDirectional Link Detection（UDLD）は、光ファイバまたはツイストペア イーサネット ケーブルを通して接続されたデバイスからケーブルの物理設定をモニタリングしたり、単一方向リンクの存在を検出できるようにするためのレイヤ 2 プロトコルです。 このプロトコルが単一方向リンクを正常に識別してディセーブルにするには、接続されたすべてのデバイスで UDLD プロトコルがサポートされている必要があります。 UDLD は、単一方向リンクを検出するとそのリンクを単方向としてマークします。 単一方向リンクは、スパニングツリー トポロジ ループをはじめ、さまざまな問題を引き起こす可能性があります。

UDLD は、レイヤ 1 メカニズムと連動してリンクの物理ステータスを判断します。 レイヤ 1 では、物理的シグナリングおよび障害検出は、自動ネゴシエーションによって処理されます。UDLD は、ネイバーの ID の検知、誤って接続されたインターフェイスのシャットダウンなど、自動ネゴシエーションでは実行不可能な処理を実行します。 自動ネゴシエーションと UDLD の両方をイネーブルにすると、レイヤ 1 と 2 の検出機能が連動し、物理的および論理的な単一方向接続、および他のプロトコルの誤動作を防止します。

ローカル デバイスが送信したトラフィックをネイバーが受信するにもかかわらず、ネイバーから送信されたトラフィックをローカル デバイスが受信しない場合に、単一方向リンクが発生します。

動作モード

UDLD は、ノーマル（デフォルト）とアグレッシブの 2 つの動作モードをサポートしています。通常モードの UDLD は、光ファイバ接続におけるインターフェイスの誤接続に起因する単一方向リンクを検出します。 アグレッシブ モードの UDLD は、光ファイバ リンクやツイストペア リンク上の片方向トラフィックに起因する単一方向リンク、および光ファイバ リンク上のインターフェイスの誤接続に起因する単一方向リンクも検出できます。

通常モードの UDLD は、光ファイバ インターフェイスの光ファイバが誤接続されている場合に単一方向リンクを検出しますが、レイヤ 1 メカニズムは、この誤接続を検出しません。 インターフェイスが正しく接続されていてもトラフィックが片方向である場合は、単一方向リンクを検出するはずのレイヤ 1 メカニズムがこの状況を検出できないため、UDLD は単一方向リンクを検出できません。 その場合、論理リンクは不明となり、UDLD はインターフェイスをディセーブルにしません。 UDLD が通常モードのときに、ペアの一方の光ファイバが切断されており、自動ネゴシエーションがアクティブであると、レイヤ 1 メカニズムはリンクの物理的な問題を検出しないため、リンクは稼働状態でなくなります。 この場合は、UDLD は何のアクションも行わず、論理リンクは不確定と見なされます。

デフォルトでは、UDLD アグレッシブ モードはディセーブルになっています。 UDLD アグレッシブ モードは、そのモードをサポートするネットワーク デバイス間のポイントツーポイントのリンク上に限って設定してください。 UDLD アグレッシブ モードが有効になっている場合、UDLD ネイバー関係が確立されている双方向リンク上のポートが UDLD パケットを受信しなくなると、UDLD はネイバーとの接続の再確立を試み、影響を受けたポートを管理シャットダウンします。

アグレッシブ モードの UDLD は、2 つのデバイス間の障害発生が許されないポイントツーポイントリンクの単一方向リンクも検出できます。また、次のいずれかの問題が発生している場合に、単一方向リンクも検出できます。

- 光ファイバまたはツイストペア リンクのインターフェイスの片方で、トラフィックの送受信ができない場合。
- 光ファイバまたはツイストペア リンクのインターフェイスの片方がダウン状態で、もう片方がアップ状態の場合。
- ケーブルのうち 1 本の光ファイバが切断されている。

単一方向の検出方法

UDLD は 2 つのメカニズムを使用して動作します。

- ネイバー データベース メンテナンス

  UDLD は、すべてのアクティブ インターフェイスで Hello パケット（別名アドバタイズメントまたはプローブ）を定期的に送信して、他の UDLD 対応ネイバーについて学習し、各デバイスがネイバーに関しての最新情報を維持できるようにします。 スイッチが hello メッセージを受信すると、エージング タイム（ホールド タイムまたは存続可能時間）が経過するまで、情報をキャッシュします。 古いキャッシュ エントリの期限が切れる前に、スイッチが新しい hello メッセージを受信すると、古いエントリが新しいエントリで置き換えられます。

  インターフェイスがディセーブルになり UDLD が実行中の場合、インターフェイスで UDLD がディセーブルになった場合、またはスイッチがリセットされた場合、UDLD は、設定変更によって影響を受けるインターフェイスの既存のキャッシュ エントリをすべてクリアします。UDLD は、ステータス変更の影響を受けるキャッシュの一部をフラッシュするようにネイバーに通知するメッセージを 1 つまたは複数送信します。 このメッセージは、キャッシュを継続的に同期するためのものです。

- イベントドリブン検出およびエコー

  UDLD は検出メカニズムとしてエコーを利用します。 UDLD デバイスが新しいネイバーを学習するか、または同期していないネイバーから再同期要求を受信すると、接続の UDLD デバイス側の検出ウィンドウを再起動して、エコー メッセージを返送します。 この動作はすべての UDLD ネイバーに対して同様に行われるため、エコー送信側では返信エコーを受信するように待機します。

  検出ウィンドウが終了し、有効な応答メッセージが受信されなかった場合、リンクは、UDLD モードに応じてシャットダウンされることがあります。UDLD が通常モードにある場合、リンクは不確定と見なされ、シャットダウンされない場合があります。UDLD がアグレッシブ モードのときは、リンクは単一方向であると見なされ、インターフェイスはシャットダウンされます。

通常モードにある UDLD が、アドバタイズまたは検出段階にあり、すべてのネイバーのキャッシュ エントリが期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。

アグレッシブ モードをイネーブルにしていて、ポートのすべてのネイバーがアドバタイズまたは検出段階で期限切れになると、UDLD はリンク起動シーケンスを再起動し、未同期の可能性のあるネイバーとの再同期を行います。高速な一連のメッセージの送受信後に、リンク ステートが不確定のままの場合、UDLD はポートをシャットダウンします。

UDLD 設定時の注意事項

次のガイドラインと推奨事項は、UDLD を設定する場合に該当します。

- UDLD対応インターフェイスを別のスイッチのUDLD非対応ポートに接続すると、そのUDLD対応インターフェイスも単方向リンクを検出できなくなります。
- モード（通常またはアグレッシブ）を設定する場合、リンクの両側に同じモードを設定します。
- UDLD は、UDLD 対応デバイスに接続されているインターフェイスでのみ有効にする必要があります。 次のインターフェイス タイプがサポートされます。
  - イーサネット アップリンク
  - FCoE アップリンク
  - イーサネット アップリンク ポート チャネル メンバ
  - FCoE アップリンク ポート チャネル メンバ

リンク プロファイルの作成

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] > [Policies] > [LAN Cloud] を展開します。

ステップ 3 [Link Profile] ノードを右クリックし、[Create Link Profile] を選択します。

ステップ 4 [Create Link Profile] ダイアログ ボックスで、名前と UDLD リンク ポリシーを指定します。

ステップ 5 [OK] をクリックします。

UDLD リンク 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] > [LAN Cloud] を展開します。
ステップ 3 [UDLD Link Policies] ノードを右クリックし、[Create UDLD Link Policy] を選択します。
ステップ 4 [Create UDLD Link Policy] ダイアログボックスで、名前、管理ステータスおよびモードを指定します。
ステップ 5 [OK] をクリックします。

UDLD システム設定の変更

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] > [LAN Cloud] を展開します。
ステップ 3 [LAN] タブで、[LAN] > [Policies] > [root] を展開します。
ステップ 4 [Link Protocol Policy] ノードを展開し、[UDLD System Settings] 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 [Properties] 領域で、必要に応じてフィールドを変更します。
ステップ 7 [Save Changes] をクリックします。

リンク プロファイルのポート チャネル イーサネット インターフェイスへの割り当て

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] > [LAN Cloud] > [*Fabric*] > [Port Channels] を展開します。
ステップ 3 ポート チャネルのノードを展開し、リンク プロファイルを割り当てる [Eth Interface] 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、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

リンク プロファイルのアップリンク イーサネット インターフェイスへの割り当て

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] > [LAN Cloud] > *[Fabric]* > [Uplink Eth Interface] を展開します。
ステップ 3 リンク プロファイルを割り当てる [Eth Interface] 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、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

リンク プロファイルのポート チャネル FCoE インターフェイスへの割り当て

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] タブの [SAN] > [SAN Cloud] > *[Fabric]* > [FC Port Channels] を展開します。
ステップ 3 FCoE ポート チャネルのノードを展開し、リンク プロファイルを割り当てる FCoE インターフェイスをクリックします。
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、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

リンク プロファイルのアップリンク FCoE インターフェイスへの割り当て

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]* > [Uplink FC Interfaces] を展開します。
ステップ 3 リンク プロファイルを割り当てる FC0E インターフェイスをクリックします。
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、割り当てるリンク プロファイルを選択します。
ステップ 6 [Save Changes] をクリックします。

VMQ 接続ポリシーの設定

VMQ 接続ポリシー

Cisco UCS Manager Manager では、vNIC に対し VMQ 接続ポリシーを設定することができます。VMQにより、管理オペレーティング システム全体のネットワーク パフォーマンスが向上します。VMQ vNIC 接続ポリシーを設定するには、次の作業を実行します。

- VMQ 接続ポリシーの作成
- サービス プロファイルでのスタティック vNIC の作成
- vNIC への VMQ 接続ポリシーの適用

サーバのサービス プロファイルで VMQ vNIC を設定する場合は、サーバ内の少なくとも 1 つのアダプタが VMQ をサポートしている必要があります。以下のアダプタのうち少なくとも 1 つがサーバにインストールされていることを確認してください。

- UCS-VIC-M82-8P
- UCSB-MLOM-40G-01
- UCSC-PCIE-CSC-02

以下は VMQ でサポートされるオペレーティング システムです。

- Windows 2012
- Windows 2012 R2

サービス プロファイルで 1 度に適用できる vNIC 接続ポリシーは 1 つだけです。 vNIC に対して 3 つのオプション（ダイナミック、usNIC、VMQ 接続ポリシー）のいずれか 1 つを選択してください。 サービス プロファイルで VMQ vNIC が設定されている場合は、次のように設定されていることを確認してください。

- BIOS ポリシーで [SRIOV] を選択する。
- アダプタ ポリシーで [Windows] を選択する。

VMQ 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 [VMQ Connection Policies] ノードを右クリックし、[Create VMQ Connection Policy] を選択します。

ステップ 5 [Create VMQ Connection Policy] ダイアログボックスに必要な情報を指定します。
割り込み回数は、少なくともサーバの論理プロセッサ数（32, 64 など）以上である必要があります。

ステップ 6 [OK] をクリックします。

vNIC への仮想化プリファレンスの割り当て

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] > [target service profile] > [root] > [vNICs] を展開します。

ステップ 3 vNIC 名をクリックして [Work] ペインにプロパティを表示します。

ステップ 4 [Connection Policies] セクションで、[VMQ] のオプション ボタンを選択し、ドロップ ダウンから [VMQ Connection Policy] を選択します。
[Properties] 領域で、この vNIC の [Vitalization Preference] が [VMQ] に変わります。

第 21 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，271 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ガイドライン，272 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考慮事項，274 ページ
- アップストリーム分離 L2 ネットワークに関する Cisco UCS の設定，276 ページ
- アップストリーム分離 L2 ネットワークに VLAN を作成，277 ページ
- VLAN へのポートおよびポート チャネルの割り当て，278 ページ
- VLAN からのポートおよびポート チャネルの削除，279 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，280 ページ

アップストリーム分離レイヤ 2 ネットワーク

接続していない 2 つ以上のイーサネット「クラウド」があり、それらに同一の Cisco UCS ドメイン内に存在するサーバや仮想マシンがアクセスする必要がある場合は、レイヤ 2 ネットワークのアップストリーム分離（分離 L2 ネットワーク）が必要です。 たとえば、次のいずれかが必要な場合、分離 L2 ネットワークを設定できます。

- 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、複数のカスタマー用のサーバまたは仮想マシンが同一の Cisco UCS ドメイン内に存在しており、それらは両方のカスタマーのために 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 内のデータ トラフィックは相互包含の原則で動作します。 VLAN およびアップストリーム ネットワークへのトラフィックはすべて、すべてのアップリンク ポートとポート チャネルで伝送されます。 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する場合は、VLAN に適切なアップリンク インターフェイスを割り当てる必要があります。これを行わないと、VLAN へのトラフィックがすべてのアップリンク ポートとポート チャネルに流れ続けます。

分離 L2 ネットワークのコンフィギュレーションは、選択的排除の原則で動作します。 分離ネットワークの一部として指定された VLAN へのトラフィックは、その VLAN に特別に割り当てられたポート チャネルまたはアップリンク イーサネット ポートだけを移動でき、他の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除外されます。 ただし、アップリンク イーサネット ポートまたはポート チャネルが特別に割り当てられていない VLAN へのトラフィックは、分離 L2 ネットワークへのトラフィックを伝送するものを含め、すべてのアップリンク ポートまたはポート チャネルを移動できます。

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 ネットワーク向けのネットワーク トポロジを設計する際は、アップリンク インターフェイスを VLAN に割り当て、逆にならないようにする必要があります。

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 Configuration Limits for Cisco UCS Manager Guide*（*Cisco UCS Manager* 向け *Cisco UCS* 設定制限ガイド）』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ガイドライン

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際は、次の事項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 モードでなければならない

Cisco UCS は、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 モードがエンドホスト モードに設定されている場合にのみ、分離 L2 ネットワークをサポートします。 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、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構成を推奨

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

VLAN の有効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

分離 L2 ネットワークで使用する VLAN は、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 チャネル向けに設定して、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、Cisco UCS Manager は VLAN を無効と見なし、次の操作を実行します。

- サーバの [Status Details] 領域に設定に関する警告を表示します。
- 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） 有効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 2 つを区別しません。

重複 VLAN はサポート対象外

Cisco UCS は、分離 L2 ネットワーク内の重複 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 は 1 つの分離 L2 ネットワークとのみ通信できる

1 つの 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、それらのネットワークにそれぞれ vNIC を設定する必要があります。

複数の分離 L2 ネットワークと通信するには、2 つ以上の vNIC をサポートする Cisco VIC アダプタをサーバに搭載する必要があります。

アプライアンス ポートにはアップリンク イーサネット ポートまたはポート チャネルと同じ VLAN を設定する必要がある

分離 L2 ネットワークと通信するアプライアンス ポートの場合は、最低 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、それがアプライアンス ポートで使用される 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。 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 を含んでいるアップリンク イーサネット ポートやポート チャネルを Cisco UCS Manager が識別できないと、ピン接続障害が発生し、アプライアンス ポートはダウン状態になります。

たとえば、Cisco UCS ドメインには、ID が 500、名前が vlan500 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 ポートのグローバル VLAN として作成されます。 ただし、Cisco UCS Manager はアプライアンス ポートにこの VLAN を伝播しません。 vlan500 をアプライアンス ポートに設定するには、ID が 500 で vlan500 という名前を持つ別の VLAN をアプライアンス ポートに作成する必要があります。 この複製 VLAN は、Cisco UCS Manager CLI の [LAN] タブの [Appliances] ノード、または Cisco UCS Manager GUI 内の **eth-storage** スコープで作成できます。 VLAN の重複チェックを求めるプロンプトが表示されたときに重複を受け入れると、Cisco UCS Manager によってアプライアンス ポートの複製 VLAN が作成されます。

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ない

Cisco UCS Manager は、すべてのアップリンク ポートとポート チャネルにデフォルトの VLAN 1 を暗黙的に割り当てます。 他の VLAN が設定されていない場合でも、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 ポートとポート チャネルへのデータ トラフィックを扱います。

（注） Cisco UCS ドメインに VLAN が設定された後も、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 チャネルに暗黙的に残ります。 デフォルトの VLAN 1 は、アップリンク ポートやポート チャネルに明示的に割り当てることができず、それらから削除することもできません。

特定のポートまたはポート チャネルにデフォルトの VLAN 1 を割り当てようとすると、Cisco UCS Manager は Update Failed 障害を生成します。

したがって、Cisco UCS ドメインに分離 L2 ネットワークを設定する場合は、そのサーバへのすべてのデータ トラフィックをすべてのアップリンク イーサネット ポートとポートチャネルで伝送し、すべてのアップストリーム ネットワークに送信するのでない限り、どの vNIC にもデフォルト VLAN 1 を設定しないでください。

両方の FI の VLAN を同時に割り当てる必要がある

グローバル VLAN にポートを割り当てると、両方のファブリック インターコネクトの VLAN に明示的に割り当てられていないすべてのポートから VLAN が削除されます。 両方の FI のポートを同時に設定する必要があります。 1 番目の FI にのみポートを設定すると、2 番目の FI のトラフィックが中断されます。

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考慮事項

アップストリーム分離L2ネットワークと通信するには、ピン接続を適切に設定する必要があります。 ソフトピン接続とハードピン接続のどちらを実装しているかにかかわらず、VLANメンバーシップの不一致によって、1 つ以上の VLAN のトラフィックがドロップされることになります。

ソフト ピン接続

ソフト ピン接続は Cisco UCS でのデフォルト動作です。 ソフト ピン接続の実装を計画する場合は、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 が VLAN メンバーシップの条件に基づいて、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 ピン接続の場合、Cisco UCS Manager は、すべてのアップリンク イーサネット ポートとポート チャネルの VLAN メンバーシップに対して、vNIC のデータ トラフィックを検証します。 分離 L2 ネットワークが設定されている場合は、vNIC 上のすべての VLAN に割り当てられている

アップリンク イーサネット ポートやポート チャネルを Cisco UCS Manager が検出できる必要があります。 アップリンク イーサネット ポートやポート チャネルが vNIC のすべての VLAN に設定されていない場合、Cisco UCS Manager は次の動作を実行します。

- リンクをダウンさせます。
- vNIC のすべての VLAN のトラフィックをドロップします。
- 次のエラーを発生させます。
  - Link Down
  - VIF Down

Cisco UCS Manager は、VLAN 設定に関するエラーや警告を発生させません。

たとえば、サーバ上の vNIC に VLAN 101、102、103 が設定されているとします。 インターフェイス 1/3 が VLAN 102 にだけ割り当てられています。 インターフェイス 1/1 および 1/2 は VLAN に明示的に割り当てられていないため、VLAN 101 と 103 のトラフィックで利用できます。 この設定の結果として、Cisco UCS ドメインには、vNIC が設定された 3 つの VLAN すべてへのトラフィックを伝送可能な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、vNIC の 3 つの VLAN すべてのトラフィックをドロップし、Link Down および VIF Down エラーを発生させます。

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 ネットワーク用のトラフィックにピン接続ターゲットを指定すると発生します。 また、ピン接続ターゲットであるアップリンク イーサネット ポートやポート チャネルが、適切な分離 L2 ネットワークと通信できるように設定されている必要があります。

ハード ピン接続の場合、Cisco UCS Manager は、すべてのアップリンク イーサネット ポートとポート チャネルの VLAN メンバーシップに対して、vNIC のデータ トラフィックを検証します。 また、LAN ピン グループの設定を検証して、VLAN とアップリンク イーサネット ポートまたはポート チャネルが含まれていることを確認します。 いずれかの点で検証に失敗した場合、Cisco UCS Manager は次の動作を実行します。

- 重大度が「警告」の Pinning VLAN Mismatch エラーを発生させます。
- VLAN へのトラフィックをドロップします。
- 他の VLAN へのトラフィックが継続して流れるようにするため、リンクはダウンさせません。

たとえば、VLAN 177 を使用するアップストリーム分離 L2 ネットワークにハード ピン接続を設定する場合は、次の手順を実行します。

- 分離 L2 ネットワークへ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 チャネルを持つ LAN ピン グループを作成します。
- サービス プロファイルで、VLAN 177 と LAN ピン グループを持つ少なくとも 1 つの vNIC を設定します。

- LAN ピン グループに含まれるアップリンク イーサネット ポートまたはポート チャネルに VLAN 177 を割り当てます

この設定が前述の 3 つのポイントのいずれかで失敗した場合、Cisco UCS Manager は VLAN 177 への VLAN ミスマッチについて警告し、その VLAN へのトラフィックだけをドロップします。

アップストリーム分離L2ネットワークに関するCiscoUCSの設定

アップストリーム分離 L2 ネットワークと接続する Cisco UCS ドメインを設定する場合、次のすべてのステップ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、分離 L2 ネットワーク設定をサポートするために、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	イーサネット エンドホスト モードの両方のファブリック インターコネクトに対しイーサネット スイッチング モードを設定します。	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、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。
ステップ 2	分離 L2 ネットワークのトラフィックを伝送するため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, （59 ページ）を参照してください。
ステップ 3	該当するアップリンク 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, （219 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。	クラスタ設定では、VLAN マネージャで VLAN を作成することを推奨します。また、それらの VLAN がアップリンク イーサネット モードで両方のファブリック インターコネクトにアクセスできるようにするために、共通/グローバル コンフィギュレーションを使用することを推奨します。 アップストリーム分離 L2 ネットワークに VLAN を作成, （277 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 5	分離 L2 ネットワークの VLAN に目的のポートまたはポート チャネルを割り当てます。	このステップが完了した場合、それらの VLAN のトラフィックは、割り当てられたポート、ポート チャネル、またはその両方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, （278 ページ）
ステップ 6	vNIC が適切な VLAN にトラフィックを送信できるようにするために、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、正しい LAN 接続設定を含める必要があります。	1 つ以上の vNIC テンプレートを使用して、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きに、この設定を完了できます。 サービス プロファイルの設定, （525 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 VLAN を作成

アップストリーム分離 L2 ネットワークの場合、VLAN マネージャで 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、必須フィールドを指定し、[OK] をクリックします。
ID が 3968 ～ 4047 の VLAN は作成できません。 この範囲の VLAN ID は予約されています。 プライベート VLAN は Cisco UCS Mini ではサポートされません。

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、次の手順を実行します。

- 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 キーを押したまま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で、それらを同じ VLAN または VLAN セットに割り当てることができます。

ステップ 7 [VLANs] テーブルで、必要に応じて該当するノードを展開し、ポートまたはポート チャネルを割り当てる VLAN をクリックします。
同じポート セット、ポート チャネル、またはその両方を複数の VLAN に割り当てる場合、Ctrl キーを押したまま複数の VLAN をクリックできます。

ステップ 8 [Add to VLAN/VLAN Group] 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 同じファブリックの VLAN に追加のポートまたはポート チャネルを割り当てるには、ステップ 6、7、および 8 を繰り返します。

ステップ 11 別のファブリックの VLAN に追加のポートまたはポート チャネルを割り当てるには、ステップ 5 ～ 8 を繰り返します。
ハイ アベイラビリティのために Cisco UCS ドメインに 2 つのファブリック インターコネクトが設定されている場合、両方のファブリック インターコネクトで同じ VLAN 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 マネージャでの作業を継続する場合は、[Apply] をクリックします。ウィンドウを閉じるには、[OK] をクリックします。
ポートまたはポート チャネルを 1 つ以上の VLAN に割り当てると、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。

サブタブ	説明
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 [VLANs] 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/VLAN Group] 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 マネージャでの作業を継続する場合は、[Apply] をクリックします。ウィンドウを閉じるには、[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 チャネル上で伝送されます。 このデフォルトの動作により、Cisco UCS ドメインでの設定に応じて、Cisco UCS Manager でその VLAN のトラフィックがドロップされることがあります。 これを避けるには、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 [VLANs] テーブルで、該当するノードを展開し、割り当て済みの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 22 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，283 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，284 ページ
- VSAN に関するガイドラインおよび推奨事項，284 ページ
- ネームド VSAN の作成，286 ページ
- ストレージ VSAN の作成，286 ページ
- VSAN の削除，287 ページ
- ストレージ VSAN の FCoE VLAN の VLAN ID の変更，288 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，289 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，289 ページ

ネームド VSAN

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

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

クラスタ構成内のネームド VSAN

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

ネームド VSAN と FCoE VLAN ID

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

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

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

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

ネームド VSAN のファイバ チャネル アップリンク トランキング

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

VSAN に関するガイドラインおよび推奨事項

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

VSAN 4079 は予約済み VSAN ID です。

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

ID 4079 でネームド VSAN を作成すると、Cisco UCS Manager はその VSAN をエラーと見なし、障害を生成します。

FC スイッチ モードのネームド VSAN 用に予約された VSAN 範囲

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

ファブリック インターコネクトが FC スイッチ モードで動作するように設定されている場合、その範囲内の VSAN は動作しません。 Cisco UCS Manager はその VSAN をエラーと見なし、障害を生成します。

FC スイッチ モードのネームド VSAN ID の範囲に関する制約事項

Cisco UCS ドメインで FC スイッチ モードの使用を計画している場合は、3040 ～ 4078 の範囲に VSAN を設定しないでください。

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

FCoE VLAN ID に関するガイドライン

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

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

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

ネームド VSAN の作成

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

手順

ステップ 1 [Navigation] ペインの [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、必須情報を入力します。

ステップ 6 [OK] をクリックします。
Cisco UCS Manager GUI で、次の [VSANs] ノードの 1 つに VSAN が追加されます。

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

ストレージ VSAN の作成

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

手順

ステップ 1 [Navigation] ペインの [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、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。
Cisco UCS Manager GUI で、次の [VSANs] ノードの 1 つに VSAN が追加されます。

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

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。

サブタブ	説明
Switch B	ファブリック インターコネクト B だけにアクセスできる VSAN を表示します。

ステップ 5 テーブルで、削除する VSAN をクリックします。
Shift キーまたは Ctrl キーを使用して、複数のエントリを選択できます。

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

ステップ 7 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 の FCoE VLAN の VLAN ID の変更

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

手順

ステップ 1 [Navigation] ペインの [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 トランキングを有効にすると、ID が 3840 ～ 4079 の範囲にあるすべての VSAN が動作不能になります。

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] 領域の [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 23 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，291 ページ
- SAN ピン グループの作成，292 ページ
- SAN ピン グループの削除，292 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 グループは不適切です。 既存の SAN ピン グループはすべて無視されます。

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

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

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 グループを vHBA テンプレートに含めます。

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 24 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，293 ページ
- WWNN プールの設定，294 ページ
- WWPN プールの設定，299 ページ
- WWxN プールの設定，305 ページ

WWN プール

ワールド ワイド名（WWN）のプールは、Cisco UCS ドメイン内のファイバ 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 だけを含めることができます。 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 プールを含めると、関連付けられているサーバにそのプールから WWNN が割り当てられます。

WWPN プール

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

WWxN プール

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

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

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

WWNN プールの設定

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 だけを含めることができます。 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] ダイアログボックスで、次のフィールドに値を入力します:

名前	説明
[Name] フィールド	ワールド ワイド ノード名プールの名前。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	プールの説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[割り当て順序] フィールド	次のいずれかになります。 • [デフォルト]：Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル]：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] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 の倍数である必要があります。 たとえば、ノードごとに 7 つのポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 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 プールをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

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 だけを含めることができます。 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 WWN ブロックを追加する WWNN プールを右クリックして、[Create WWN Block] を選択します。

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

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 の倍数である必要があります。 たとえば、ノードごとに 7 つのポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWNN プールからの WWN ブロックの削除

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

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

手順

ステップ 1 [Navigation] ペインの [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 だけを含めることができます。 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 WWNN イニシエータを追加する WWNN プールを右クリックして、[Create WWNN Initiator] を選択します。

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

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

ステップ 6 [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

プールを削除した場合、Cisco UCS Manager は、 でそのプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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 だけを含めることができます。 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	ワールド ワイド ポート名（WWPN）プールの名前。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	プールの説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[割り当て順序] フィールド	次のいずれかになります。 • [デフォルト]：Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル]：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] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 の倍数である必要があります。 たとえば、ノードごとに 7 つのポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 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 プールを vHBA テンプレートに含めます。

WWPN プールへの WWN ブロックの追加

重要 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 だけを含めることができます。 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 WWN ブロックを追加する WWPN プールを右クリックして、[Create WWN Block] を選択します。

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

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 の倍数である必要があります。 たとえば、ノードごとに 7 つのポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 のポートがある場合、プール サイズは、64 の倍数である必要があります。

ステップ 6 [OK] をクリックします。

WWPN プールからの WWN ブロックの削除

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

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

手順

ステップ 1 [Navigation] ペインの [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 だけを含めることができます。 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 WWPN イニシエータを追加する WWPN プールを右クリックして、[Create WWPN Initiator] を選択します。

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

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

ステップ 6 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
[ブートターゲットWWPN] フィールド	ブート イメージの場所に対応する WWPN。
[ブートターゲットLUN] 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

プールを削除した場合、Cisco UCS Manager は、 でそのプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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 だけを含めることができます。 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	ワールド ワイド ポート名（WWPN）プールの名前。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	プールの説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Max Ports per Node] フィールド	このプール内の各ノード名に割り当てることができるポートの最大数。 オブジェクトの保存後は、この値を変更できません。

名前	説明
[割り当て順序] フィールド	次のいずれかになります。 • [デフォルト]：Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル]：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] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 の倍数である必要があります。 たとえば、ノードごとに 7 つのポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 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 プールをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

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 だけを含めることができます。 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] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[From] フィールド	ブロック内の最初の WWN。
[Size] フィールド	ブロック内の WWN の数。 WWxN プールの場合、プール サイズは *ports-per-node* + 1 の倍数である必要があります。 たとえば、ノードごとに 7 つのポートがある場合、プール サイズは 8 の倍数である必要があります。 ノードごとに 63 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 はそのブロックの中の vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたブロックのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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

プールを削除した場合、Cisco UCS Manager は、 でそのプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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 25 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，309 ページ
- ファイバ チャネル アダプタ ポリシーの設定，313 ページ
- デフォルトの vHBA 動作ポリシーの設定，321 ページ
- SAN 接続ポリシーの設定，322 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 と SAN の接続方法を定義するポリシーです。 これは、vHBA SAN 接続テンプレートとも呼ばれます。

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

vHBA テンプレートの作成

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	仮想ホスト バス アダプタ（vHBA）テンプレートの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[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 テンプレートをサービス プロファイルに含めます。

vHBA テンプレートへの vHBA のバインディング

サービス プロファイルと関連付けられた vHBA を vHBA テンプレートにバインドすることができます。 vHBA を vHBA テンプレートにバインドした場合、Cisco UCS Manager によって、vHBA テンプレートで定義された値を使って vHBA が設定されます。 既存の vHBA 設定が vHBA テンプレートと一致しない場合、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 を含むサービス プロファイルがすでにサービス プロファイル テンプレートにバインドされている場合、vHBA を vHBA テンプレートにバインドできません。

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

手順

ステップ 1 [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 とバインドする サービス プロファイル が含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

ステップ 5 テンプレートにバインドする vHBA をクリックします。

ステップ 6 [Work] ペインの [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の [Yes] をクリックすることにより、バインディングによって vHBA の再設定が生じた場合に Cisco UCS Manager でサーバのリブートが必要になる場合があることを確認します。

vHBA テンプレートからの vHBA のバインド解除

手順

ステップ 1 [Navigation] ペインの [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、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ことがあります。 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、あらゆる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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

名前	説明
[Owner] フィールド	次のいずれかになります。 • [Local]：このポリシーは、Cisco UCS ドメイン内のサービス プロファイルとサービス プロファイル テンプレートでのみ使用できます。 • [Pending Global]：このポリシーの制御は Cisco UCS Central に移行中です。 移行が完了すると、このポリシーは Cisco UCS Central に登録されているすべての Cisco UCS ドメインで使用可能になります。 • [Global]：このポリシーは Cisco UCS Central によって管理されます。 このポリシーを変更する場合は、必ず Cisco UCS Central を使用して変更してください。

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

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

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

ステップ 7 （任意） [Options] 領域で、次の値を調整します。

名前	説明
[FCP Error Recovery] フィールド	テープ デバイスによるシーケンス レベル エラーの修復に FCP Sequence Level Error Recovery（FC-TAPE）プロトコルを使用するかどうかを選択します。 これにより、VIC ファームウェアの Read Exchange Concise（REC）および Sequence Retransmission Request（SRR）機能を有効または無効にできます。 次のいずれかになります。 • [Disabled]：デフォルトです。 • [Enabled]：システムが 1 つ以上のテープ ドライブ ライブラリに接続している場合は、このオプションを選択します。 （注） このパラメータは、Cisco UCS M81KR 仮想インターフェイス カードなどの VIC アダプタを搭載したサーバにのみ適用されます。
[Flogi Retries] フィールド	システムがファブリックへのログインを最初に失敗してから再試行する回数。 任意の整数を入力します。 システムが無限に試行し続けるように指定するには、このフィールドに「infinite」と入力します。 ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタを搭載したサーバや、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 アダプタを搭載したサーバにのみ適用されます。

名前	説明
[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。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタまたは統合型ネットワーク アダプタを搭載したサーバにのみ適用されます。
[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。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。
[Plogi Timeout] 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。ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。
[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 マルチパス ドライバにとって重要であり、エラー処理に使用される主要指標の 1 つとなります。 0 ～ 240000 の整数を入力します。デフォルトは 30,000 です。ESX を実行している VIC アダプタ搭載のサーバの場合、推奨値は 10,000 です。 ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタを搭載したサーバにのみ適用されます。

名前	説明
[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。 ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、Windows を実行している VIC アダプタ搭載のサーバにのみ適用されます。
[Link Down Timeout] 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。 ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、Windows を実行している VIC アダプタ搭載のサーバにのみ適用されます。
[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 内で同時に保留可能なデータまたは制御 I/O 操作の最大数。 この値を超えると、保留中の I/O 操作の数が減り、追加の操作が処理できるようになるまで、キューで I/O 操作が待機します。 （注） このパラメータは、LUN キューの長さと同じではありません。LUN キューの長さは、サーバにインストールされている OS に基づいて、Cisco UCS Manager により管理されます。 1 ～ 1024 の整数を入力します。 デフォルトは 16 です。 ストレージアレイのドキュメントでこのパラメータの最適な値を確認することをお勧めします。

名前	説明
[Max LUNs Per Target] フィールド	ファイバチャネル ドライバがエクスポートまたは表示する LUN の最大数。 LUN の最大数は、通常、サーバで実行されている OS により管理されます。 1 ～ 1024 の整数を入力します。 デフォルト値は 256 です。 ESX または Linux を実行しているサーバの場合、推奨値は 1024 です。 オペレーティングシステムのドキュメントでこのパラメータの最適な値を確認することをお勧めします。 （注） このパラメータは、VIC アダプタまたはネットワーク アダプタを搭載したサーバにのみ適用されます。
[Interrupt Mode] フィールド	ドライバからオペレーティング システムに割り込みを送信する方法。 次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。 サーバのオペレーティングシステムがこれに対応している場合には、このオプションを選択することをお勧めします。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。 （注） このパラメータは、VIC アダプタを搭載しているサーバや、Window 以外の OS を実行しているネットワーク アダプタ搭載のサーバにのみ適用されます。 Windows OS では、このパラメータは無視されます。

ステップ 8 [OK] をクリックします。

ステップ 9 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 vHBA 動作ポリシー

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

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

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

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

デフォルトの vHBA 動作ポリシーの設定

手順

ステップ 1 [Navigation] ペインの [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 動作ポリシーのみを設定できます。 サブ組織内のデフォルトの vHBA 動作ポリシーは設定できません。

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

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

- [None]：Cisco UCS Manager は、サービス プロファイルにデフォルトの vHBA を作成しません。 すべての vHBA を明示的に作成する必要があります。
- [HW Inherit]：サービス プロファイルが vHBA を必要とし、何も明示的に定義されていない場合、Cisco UCS Manager はサービス プロファイルに関連付けられている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 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 と vHBA を識別します。

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

LAN および SAN の接続ポリシーに必要な権限

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

接続ポリシーの作成に必要な権限

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

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

接続ポリシーをサービス プロファイルに追加するために必要な権限

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

サービス プロファイルと接続ポリシー間の相互作用

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

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

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

SAN 接続ポリシーの作成

手順

ステップ 1 [Navigation] ペインの [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、ポリシーの名前と説明を次のフィールドに入力します。

名前	説明
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Owner] フィールド	次のいずれかになります。 • [Local]：このポリシーは、Cisco UCS ドメイン内のサービス プロファイルとサービス プロファイル テンプレートでのみ使用できます。 • [Pending Global]：このポリシーの制御は Cisco UCS Central に移行中です。 移行が完了すると、このポリシーは Cisco UCS Central に登録されているすべての Cisco UCS ドメインで使用可能になります。 • [Global]：このポリシーは Cisco UCS Central によって管理されます。 このポリシーを変更する場合は、必ず Cisco UCS Central を使用して変更してください。

ステップ 6 [World Wide Node Name] 領域の [WWNN Assignment][WWNN Assignment] ドロップダウン リスト 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 が使用可能か確認できます。
- 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で、次のフィールドを入力します。

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

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

SAN 接続ポリシー用の vHBA の作成

手順

ステップ 1 [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 バーの [+] 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。

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 接続ポリシー用のイニシエータ グループの作成

手順

ステップ 1 [Navigation] ペインの [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 バーの [+] ボタンをクリックします。

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

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

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

ステップ 7 [OK] をクリックします。

SAN 接続ポリシーからのイニシエータ グループの削除

手順

ステップ 1 [Navigation] ペインの [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る SAN 接続ポリシーを削除する場合、すべての vHBA をそのサービス プロファイルから削除し、そのサービス プロファイルに関連付けられているサーバの SAN データ トラフィックを中断します。

手順

ステップ 1 [Navigation] ペインの [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 26 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，329 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，330 ページ
- Cisco UCS Manager ベースのファイバ チャネル ゾーン分割に関するガイドラインおよび推奨事項，333 ページ
- Cisco UCS でのファイバ チャネルのゾーン分割の設定，333 ページ
- ファイバ チャネル ゾーン分割用の VSAN の作成，335 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，338 ページ

ファイバ チャネル ゾーン分割に関する情報

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

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

- SAN ネットワーク セキュリティの強化
- データの損失や破損の防止
- パフォーマンス問題の軽減

ゾーンに関する情報

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

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

ゾーン セットに関する情報

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

- アクティブにできるのは、常に 1 つのゾーン セットだけです。
- ゾーン セット内のすべてのゾーンは、ファブリック内のスイッチ全体で単一のエンティティとしてアクティブまたは非アクティブにできます。
- 1 つのゾーンを 複数のゾーン セットのメンバにできます。
- ゾーン内の各スイッチは最大 500 のゾーン セットを持つことができます。

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

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

- 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：この設定は、直接接続ストレージとローカル ゾーン分割の組み合わせです。 ファイバ チャネルまたは FCoE のストレージはファブリック インターコネクトに直接接続され、ゾーン分割は、Cisco UCS ローカル ゾーン分割を使用して Cisco UCS Manager で実行されます。既存のファイバチャネルまたはFCoEのアップリンク接続を無効にする必要があります。現時点では、 Cisco UCS は、UCS ローカル ゾーン分割機能の利用において、アクティブなファイバチャネル/FCoEアップリンク接続をサポートしていません。
- スイッチベースのファイバ チャネル ゾーン分割：この設定は、直接接続ストレージとアップリンク ゾーン分割の組み合わせです。 ファイバチャネルまたはFCoEのストレージはファブリック インターコネクトに直接接続され、ゾーン分割は、MDS または Nexus 5000 スイッチを介して Cisco UCS ドメイン の外部から実行されます。 この設定では、Cisco UCS ドメインでのローカル ゾーン分割はサポートされません。

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

Cisco UCS Manager ベースのファイバ チャネル ゾーン分割

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

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

サポートされているファイバ チャネル ゾーン分割モード

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

- 単一のイニシエータと単一のターゲット：Cisco UCS Manager は、vHBA とストレージ ポートの組み合わせごとに 1 つのゾーンを自動作成します。 各ゾーンには 2 つのメンバが含まれます。 ゾーンの数がサポートされる最大数を超える見込みがない場合は、このタイプのゾーン分割を設定することをお勧めします。
- 単一のイニシエータと複数のターゲット：Cisco UCS Manager は、vHBA ごとに 1 つゾーンを自動作成します。 ゾーンの数がサポートされている最大値に到達またはそれを超えると予想される場合は、このタイプのゾーン分割を設定することを推奨します。

vHBA イニシエータ グループ

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

vHBA イニシエータ グループでの設定により、以下が決定されます。

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

ファイバ チャネル ストレージ接続ポリシー

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

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

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

ファイバ チャネル アクティブ ゾーン セット設定

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

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

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

スイッチベースのファイバ チャネル ゾーン分割

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

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

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

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

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

ハイ アベイラビリティのために対称構成を推奨

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

Cisco UCS でのファイバ チャネルのゾーン分割の設定

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

手順

	コマンドまたはアクション	目的
ステップ 1	まだ完了してない場合は、Cisco UCS ドメイン内のファブリック インターコネクトの接続を、外付けファイバ チャネル スイッチ（MDS など）から切り離してください。	
ステップ 2	Cisco UCS ドメインにまだ外部ファイバ チャネル スイッチによって管理されたゾーンが含まれる場合は、これらのゾーンを削除するために、影響を受けたすべての VSAN で **clear-unmanaged-fc-zone-all** コマンドを実行します。	この機能は現在、Cisco UCS Manager GUI では使用できません。 このステップは、Cisco UCS Manager CLI で実行する必要があります。

	コマンドまたはアクション	目的
ステップ 3	ファイバ チャネル スイッチ モードの両方のファブリック インターコネクトでファイバ チャネル スイッチング モードを設定します。	エンドホスト モードではファイバチャネル ゾーン分割を設定できません。 ファイバ チャネル スイッチング モードの設定を参照してください。
ステップ 4	ファイバ チャネル ゾーンのトラフィック転送に必要なファイバチャネルとFCoE ストレージ ポートを設定します。	ポートおよびポート チャネルの設定, （59 ページ）を参照してください。
ステップ 5	1 つ以上の VSAN を作成し、ファイバ チャネル ゾーンのトラフィック転送に必要なすべての VSAN で、ファイバ チャネルのゾーン分割を有効にします。	クラスタ設定では、SAN アップリンク マネージャのファイバチャネル ゾーンに含める予定の VSAN を作成し、共通/グローバル コンフィギュレーションを使用して、両方のファブリック インターコネクトにアクセスできるようにすることを推奨します。 ファイバ チャネル ゾーン分割用の VSAN の作成, （335 ページ）を参照してください。
ステップ 6	1 つ以上のファイバ チャネル ストレージ接続ポリシーを作成します。	必要に応じて、この手順を実行してサービス プロファイルにファイバ チャネル ゾーン分割を設定することができます。 ファイバ チャネル ストレージ接続ポリシーの作成, （338 ページ）を参照してください。
ステップ 7	ファイバ チャネル ゾーン経由で通信する必要があるサーバに対してサービス プロファイルまたはサービス プロファイル テンプレートにゾーン分割を設定します。	この設定を完了するには、次の手順を完了します。 • VHBA に割り当てられた VSAN（複数の場合あり）のゾーン分割を有効にします。 • 1 つ以上の vHBA イニシエータ グループを設定します。 サービス プロファイルの設定, （525 ページ）を参照してください。

ファイバ チャネル ゾーン分割用の VSAN の作成

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

手順

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

ステップ 2 [SAN] タブの [SAN] ノードをクリックします。

ステップ 3 [Work] ペインの [SAN Uplinks] タブの [SAN Uplinks Manager] リンクをクリックします。
別のウィンドウに [SAN Uplinks Manager] が開きます。

ステップ 4 [SAN Uplinks Manager] で [VSAN] タブをクリックします。
VSAN は、どのサブタブでも作成できます。 ただし、[All] サブタブを使用した場合は、設定されたすべての VSAN が表に表示されます。

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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

名前	説明
[FC Zoning] フィールド	Cisco UCS Manager が Cisco UCS ドメインに対してファイバ チャネル ゾーン分割を設定するかどうかを決定するためのオプション ボタンをクリックします。 次のいずれかになります。 • [Disabled]：アップストリーム スイッチがファイバ チャネル ゾーン分割を処理します。またはファイバチャネルゾーン分割は、Cisco UCS ドメインに対して実行されません。Cisco UCS Manager はファイバ チャネル ゾーン分割を設定しません。 • [Enabled]：Cisco UCS Manager は Cisco UCS ドメインに対してファイバチャネルゾーン分割を設定し、制御します。 （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する場合は、ファイバ チャネル ゾーン分割に使用されている VSAN でアップストリーム スイッチを設定しないでください。
[Type] オプション ボタン	オプション ボタンをクリックして、VSAN の設定方法を決定します。 次のいずれかになります。 • [Common/Global]：VSAN は、すべての使用可能なファブリック内で同じ VSAN ID にマッピングされます。 • [Fabric A]：VSAN は、ファブリック A にだけ存在する VSAN ID にマッピングされます。 • [Fabric B]：VSAN は、ファブリック B にだけ存在する VSAN ID にマッピングされます。 • [Both Fabrics Configured Differently]：VSAN は、使用可能なファブリックごとに異なる VSAN ID にマッピングされます。 このオプションを選択すると、Cisco UCS Manager GUI に、各ファブリックの [VSAN ID] フィールドと [FCoE VLAN] フィールドが表示されます。
[VSAN ID] フィールド	ネットワークに割り当てられている固有識別情報。 ID は、1 ～ 4078 または 4080 ～ 4093 の間で設定できます。 4079 は予約済み VSAN ID です。 また、FC エンドホスト モードを使用する場合は、3840 ～ 4079 も予約済みの VSAN ID 範囲です。

名前	説明
[FCoE VLAN] フィールド	ファイバチャネル接続に使用される VLAN に割り当てられた固有識別情報。 VLAN 4048 はユーザが設定可能です。 ただし、Cisco UCS Manager では、VLAN 4048 が次のデフォルト値に使用されます。 4048 を VLAN に割り当てる場合は、これらの値を再設定する必要があります。 • Cisco UCS リリース 2.0 へのアップグレード後：FCoE ストレージポートのネイティブ VLAN は、デフォルトで VLAN 4048 を使用します。 デフォルト FCoE VSAN が、アップグレード前に VLAN 1 を使用するように設定されていた場合は、使用または予約されていない VLAN ID に変更する必要があります。 たとえば、デフォルトを 4049 に変更することを検討します（その VLAN ID が使用されていない場合）。 • Cisco UCS リリース 2.0 の新規インストール後：デフォルト VSAN 用の FCoE VLAN は、デフォルトで VLAN 4048 を使用します。 FCoE ストレージポート ネイティブ VLAN は VLAN 4049 を使用します。 Cisco UCS CNA M72KR-Q や Cisco UCS CNA M72KR-E などの FIP 対応統合型ネットワーク アダプタの場合は、FCoE VLAN ID のネイティブ VLAN ではないネームド VLAN を使ってネームド VSAN を設定する必要があります。 この設定により、FCoE トラフィックが確実にこれらのアダプタを通過できるようになります。

ステップ 7 [OK] をクリックします。

ファイバ チャネル ストレージ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、次のフィールドを入力します。

名前	説明
[名前] フィールド	ポリシーの名前。 この名前には、1～16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 6 [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、vHBA とストレージ ポートの組み合わせごとに 1 つのゾーンを自動作成します。 各ゾーンには 2 つのメンバが含まれます。 ゾー

ンの数がサポートされる最大数を超える見込みがない場合は、このタイプのゾーン分割を設定することをお勧めします。

- [Single Initiator Multiple Targets]：Cisco UCS Manager は、vHBA ごとに 1 つゾーンを自動作成します。ゾーンの数がサポートされている最大値に到達またはそれを超えると予想される場合は、このタイプのゾーン分割を設定することを推奨します。

ステップ 7 [FC Target Endpoints] テーブル で、テーブルの右側にあるアイコン バーで [+] をクリックします。[+] アイコンがディセーブルの場合、テーブルのエントリをクリックして、イネーブルにします。

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

名前	説明
[WWPN] フィールド	ファイバ チャネルまたは FCoE ストレージ アレイ上の物理ターゲット ポートに割り当てられた WWPN（WWN）です。サーバは、この WWPN（WWN）を使用して、ストレージ アレイに設定された LUN にアクセスします。
[説明] フィールド	ターゲット エンドポイントの説明。 ターゲット エンドポイントが接続するポート、LUN、またはストレージ アレイに関する情報を含めることを推奨します。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Path] フィールド	ターゲットエンドポイントとの通信に使用するファブリック インターコネクト。
[Select VSAN] ドロップダウン リスト	ターゲット エンドポイントとの通信に使用する VSAN。
[Create VSAN] リンク	VSAN を作成する場合は、このリンクをクリックします。

ポリシーの対象となるすべてのターゲット エンドポイントを作成するまでこの手順を繰り返し行います。

ステップ 9 ポリシーの対象となるすべてのターゲット エンドポイントを作成したら、[OK] をクリックします。

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 27 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，341 ページ
- UUID 接尾辞プールの設定，344 ページ
- IP プールの設定，346 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	サーバ プールのユーザ定義による説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 6 [Next] をクリックします。

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

a) [Available Servers] テーブルで、1 つ以上のサーバを選択します。

b) [>>] ボタンをクリックして、サーバ プールにサーバを追加します。

c) 適切なサーバをすべてプールに追加したら、[Finish] をクリックします。

サーバ プールの削除

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、特定のプールを使用するサービス プロファイルに関連づけられた各サーバについて、これらの変数が一意であることを保証して競合を回避します。

サービス プロファイルで UUID 接尾辞プールを使用する場合は、サービス プロファイルに関連付けられたサーバの UUID を手動で設定する必要はありません。

UUID 接尾辞プールの作成

手順

ステップ 1 [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、次のフィールドに値を入力します。

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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	プールのユーザ定義による説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Prefix] フィールド	次のいずれかになります。 • [Derived]：システムによって接尾辞が作成されます。 • [other]：任意の接尾辞を指定します。 このオプションを選択すると、任意の接尾辞を *XXXXXXXX-XXXX-XXXX* の形式で入力できるテキスト フィールドが Cisco UCS Manager GUI に表示されます。
[割り当て順序] フィールド	次のいずれかになります。 • [デフォルト]：Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル]：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] 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 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接尾辞プールをサービスプロファイルとテンプレートのうち一方、または両方に含めます。

UUID 接尾辞プールの削除

プールを削除した場合、Cisco UCS Manager は、 でそのプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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、用途が初期設定されていない IP アドレスの集合です。 Cisco UCS Manager で IPv4 または IPv6 アドレス プールを作成して以下を行うことができます。

-
- サービス プロファイルが関連付けられているサーバのデフォルトの管理 IP プール ext-mgmt の置き換え。 Cisco UCS Manager は、サーバ上の Cisco Integrated Management Controller（CIMC）で終端する外部アクセス用に、IP プールの各 IP アドレス ブロックを予約します。 サービス

プロファイルが関連付けられていない場合は、CIMC 用の ext-mgmt IP プールを使用して IP アドレスを取得する必要があります。

- CIMC 用の管理インバンドまたはアウトオブバンド IP アドレスの置き換え。

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

Cisco UCS Manager で IPv4 アドレス プールを作成して以下を行うことができます。

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

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

IP プールの作成

手順

ステップ 1 [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、次のフィールドに入力します。

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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

名前	説明
[Description] フィールド	ユーザ定義による IP アドレス プールの説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[割り当て順序] フィールド	次のいずれかになります。 • [デフォルト]：Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル]：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 IPv4 Blocks] ページで、[Add] をクリックします。

ステップ 7 [Create a Block of IPv4 Addresses] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[From] フィールド	ブロック内の最初の IPv4 アドレス。
[Size] フィールド	プール内の IP アドレスの数。
[Subnet Mask] フィールド	ブロック内の IPv4 アドレスと関連付けられたサブネット マスク。
[Default Gateway] フィールド	ブロック内の IPv4 アドレス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	IPv4 アドレスのこのブロック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	IPv4 アドレスのこのブロック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

ステップ 9 [Next] をクリックします。

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

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

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

ステップ 12 [OK] をクリックします。

ステップ 13 [Finish] をクリックして、ウィザードを終了します。

次の作業

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

IP プールへのブロックの追加

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

手順

ステップ 1 [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、次のうちの 1 つを選択します。

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

ステップ 5 適切なダイアログ ボックスのフィールドに入力します。

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

名前	説明
[名前] カラム	ブロックに割り当てられた IPv4 アドレスの範囲。
[From] カラム	ブロック内の最初の IPv4 アドレス。
[To] カラム	ブロック内の最後の IPv4 アドレス。
[Subnet] カラム	ブロック内の IPv4 アドレスと関連付けられたサブネット マスク。
[Default Gateway] カラム	ブロック内の IPv4 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] カラム	IPv4 アドレスのこのブロックがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] カラム	IPv4 アドレスのこのブロックがアクセスする必要のあるセカンダリ DNS サーバ。

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

名前	説明
[名前] カラム	ブロックに割り当てられている IPv6 アドレスの範囲。
[From] カラム	ブロック内の最初の IPv6 アドレス。
[To] カラム	ブロック内の最後の IPv6 アドレス。
[Prefix] カラム	ブロック内の IPv6 アドレスに関連付けられたネットワーク アドレス プレフィクス。
[Default Gateway] カラム	ブロック内の IPv6 アドレスに関連付けられたデフォルト ゲートウェイ。
[Primary DNS] カラム	この IPv6 アドレスのブロックがアクセスするプライマリ DNS サーバ。
[Secondary DNS] カラム	この IPv6 アドレスのブロックがアクセスするセカンダリ DNS サーバ。

ステップ 6 [OK] をクリックします。

IP プールからのブロックの削除

手順

ステップ 1 [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

プールを削除した場合、Cisco UCS Manager は、 でそのプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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 プールである [ext-mgmt] および [iscsi-initiator-pool] は削除できません。
ステップ 5 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 28 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，353 ページ
- ブレード サーバの管理 IP アドレスの設定，354 ページ
- ラック サーバの管理 IP アドレスの設定，359 ページ
- サービス プロファイルの管理 IP アドレスの設定，364 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，368 ページ
- 管理 IP プールの設定，369 ページ

管理 IP アドレス

Cisco UCS ドメイン ドメインの各サーバには 1 つ以上の管理 IP アドレスが必要です。これらの IP アドレスは、Cisco Integrated Management Controller（CIMC）に割り当てられたり、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ます。 Cisco UCS Manager は、CIMC で終端する外部アクセスに対してこれらの IP アドレスを使用します。 この外部アクセスは、次のいずれかのサービスを経由することが可能です。

- KVM コンソール
- Serial over LAN
- IPMI ツール

サーバの CIMC にアクセスするための管理 IP アドレスとして、アウトオブバンド（OOB）アドレス（このアドレスから管理ポート経由で、トラフィックがファブリック インターコネクトを通過）、またはインバンドアドレス（このアドレスからファブリック アップリンク ポート経由で、トラフィックがファブリック インターコネクトを通過）を使用できます。 サーバの CIMC にアクセスする最大 6 つの IP アドレスを設定できます（2 つはアウトオブバンド（OOB）アドレス、他の 4 つはインバンド アドレス）。

以下の管理 IP アドレスを設定できます。

- サーバに直接割り当てられるスタティック OOB IPv4 アドレス。
- グローバル ext-mgmt プールからサーバに割り当てられる OOB IPv4 アドレス
- サーバに関連付けられたサービス プロファイルから取得するインバンド IPv4 アドレス
- 管理 IP 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るインバンド IPv4 アドレス
- サーバに直接割り当てられるスタティック インバンド IPv6 アドレス
- サーバに関連付けられたサービス プロファイルから取得するインバンド IPv6 アドレス

サーバの各 CIMC およびサーバに関連付けられたサービス プロファイルに、複数の管理 IP アドレスを割り当てることができます。その場合は、それぞれ異なる IP アドレスを使用する必要があります。

サービス プロファイルに関連付けられた管理 IP アドレスはそのサービス 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 はセッションを終了させ、移行完了後もそのセッションを再開しません。管理 IP アドレスは、サービス プロファイルを作成または変更するときに設定します。

（注） 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スタティック IP アドレスが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スタティック IP アドレスを割り当てることはできません。そのような設定を試みると、Cisco UCS Manager は 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。

ブレード サーバの管理 IP アドレスの設定

ブレード サーバでスタティック IP アドレスを使用するための設定

このアクションがグレー表示されている場合、サーバには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。

サーバ 1 台あたり合計 3 つのスタティック管理アドレスを設定できます。

- アウトバンド IPv4
- インバンド IPv4
- インバンド IPv6

（注） 3 つをすべて設定する必要はありません。

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 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。
[Actions] 領域では、管理 IP アドレスに関して 2 つの選択肢があります。

- [Modify Outband Static Management IP]
- [Change Inband Management IP]

ステップ 6 アウトバンド スタティック管理 IP アドレスを変更するには、[Actions] 領域で [Modify Outband Static Management IP] をクリックします。

ステップ 7 [Modify Outband Static Management IP] ダイアログ ボックスで、次のフィールドに入力します。

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。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

ステップ 8 [OK] をクリックします。

ステップ 9 インバンド管理 IP アドレスを変更するには、[Change Inband Management IP] をクリックします。
[Change Management IP Address] ダイアログ ボックスには、2 つのタブがあります。

- [Inband IPv4]
- [Inband IPv6]

a) スタティック インバンド管理 IPv4 アドレスを変更するには、[In-Band IPv4] サブタブをクリックします。

b) [Change Management IP Address] ダイアログ ボックスで、次のフィールドに入力します。

フィールド	説明
[Management IP Address Policy] ドロップダウン	[Static] をクリックします。

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。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

c) [OK] をクリックします。
d) スタティック インバンド管理 IPv6 アドレスを変更するには、[In-Band IPv6] サブタブをクリックします。
e) [Change Management IP Address] ダイアログ ボックスで、次のフィールドに入力します。

フィールド	説明
[Management IP Address Policy] ドロップダウン	[Static] をクリックします。
IP Address	サーバに割り当てられるスタティック IPv6 アドレス。
Prefix	IP アドレスのネットワーク プレフィックス。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

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。

ブレード サーバで管理 IP プールを使用する設定

この手順のなかのどれかのアクションがグレー表示されている場合、設定がすでに完了していることを示します。

サーバ 1 台あたりに合計 3 つの管理 IP プールを設定できます。

- アウトバンド IPv4
- インバンド IPv4
- インバンド IPv6

（注） 3 つをすべて設定する必要はありません。

はじめる前に

サーバで管理 IP プールを使用するように設定する前に、管理 IP プールを設定します。

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 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。

- アウトバンド IP プール管理 IP アドレス ポリシーを設定するには、ステップ 6 に進みます。
- インバンド IPv4、IPv6 管理 IP アドレス ポリシーを設定するには、ステップ 8 に進みます。

ステップ 6 [Actions] 領域で、[Use Outband Pooled Management IP] をクリックします。

ステップ 7 [Use Outband Pooled Management IP] の確認ダイアログ ボックスで [Yes] をクリックし、[OK] をクリックします。
これで管理 IP アドレス ポリシーが、アウトバンド管理 IP プールの OOB IP アドレスを使用するように設定されます。

ステップ 8 [Actions] 領域で、[Change Inband Management IP] をクリックします。

ステップ 9 [Change Management IP] ダイアログ ボックスには、2 つのタブがあります。

- [Inband IPv4]
- [Inband IPv6]

a) インバンド IPv4 管理 IP プールを変更するには、[Inband IPv4] タブをクリックし、次のフィールドに入力します。

フィールド	説明
[Network] ドロップダウン リスト	関連付けられている VLAN グループから選択された VLAN。

フィールド	説明
[Management IP Address Policy] ドロップダウン リスト	サーバに割り当てる管理 IP プール。 使用可能なプールが 2 種類あります。 • Domain Pools • Global Pools [Domain Pools] のエントリ、または [Global Pools] のエントリから使用可能なプールを 1 つ選択します。

b) インバンド IPv6 管理 IP プールを変更するには、[Inband IPv6] タブをクリックし、次のフィールドに入力します。

フィールド	説明
[Network] ドロップダウン リスト	関連付けられている VLAN グループから選択された VLAN。
[Management IP Address Policy] ドロップダウン リスト	サーバに割り当てる管理 IP プール。 使用可能なプールが 2 種類あります。 • Domain Pools • Global Pools [Domain Pools] のエントリ、または [Global Pools] のエントリから使用可能なプールを 1 つ選択します。

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。

ブレード サーバからのインバンド設定の削除

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

手順

ステップ 1 [Navigation] ペインの [Servers] 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 Name]* を展開します。

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

ステップ 4 [CIMC] サブタブをクリックします。

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

ステップ 6 [Delete] の確認ダイアログボックスで [Yes] をクリックします。
サーバのインバンド設定が削除されます。

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

ラック サーバの管理 IP アドレスの設定

ラック サーバでスタティック IP アドレスを使用するための設定

このアクションがグレー表示されている場合、サーバには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。

サーバ 1 台あたり合計 3 つのスタティック管理アドレスを設定できます。

- アウトバンド IPv4
- インバンド IPv4
- インバンド IPv6

（注） 3 つをすべて設定する必要はありません。

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 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。
[Actions] 領域では、管理 IP アドレスに関して 2 つの選択肢があります。

- [Modify Outband Static Management IP]
- [Change Inband Management IP]

ステップ 6 アウトバンドのスタティック管理 IP アドレスを変更するには、[Actions] 領域で、[Modify Outband Static Management IP] をクリックします。

ステップ 7 [Modify Outband Static Management IP] ダイアログ ボックスで、次のフィールドに入力します。

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。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

ステップ 8 [OK] をクリックします。

ステップ 9 インバンド管理 IP アドレスを変更するには、[Change Inband Management IP] をクリックします。
[Change Management IP Address] ダイアログ ボックスには、2 つのタブがあります。

- [Inband IPv4]
- [Inband IPv6]

ステップ 10 スタティック インバンド IPv4 管理アドレスを変更するには、[Inband IPv4] タブをクリックします。

ステップ 11 [Change Management IP Address] ダイアログ ボックスで、次のフィールドに入力します。

フィールド	説明
[Management IP Address Policy] ドロップダウン	[Static] をクリックします。
IP Address	サーバに割り当てられるスタティック IPv4 アドレス。

フィールド	説明
Subnet Mask	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	IP アドレスで使用するデフォルト ゲートウェイ。

ステップ 12 [OK] をクリックします。

ステップ 13 スタティック インバンド IPv6 管理アドレスを変更するには、[Inband IPv6] タブをクリックします。

ステップ 14 [Change Management IP Address] ダイアログ ボックスで、次のフィールドに入力します。

フィールド	説明
[Management IP Address Policy] ドロップダウン	[Static] をクリックします。
IP Address	サーバに割り当てられるスタティック IPv6 アドレス。
Prefix	IP アドレスのプレフィックス。
デフォルト ゲートウェイ	IP アドレスで使用するデフォルト ゲートウェイ。

ステップ 15 [OK] をクリックします。

ステップ 16 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 サーバで管理 IP プールを使用する設定

この手順のなかのどれかのアクションがグレー表示されている場合、設定がすでに完了していることを示します。

サーバ 1 台あたりに合計 3 つの管理 IP プールを設定できます。

- アウトバンド IPv4
- インバンド IPv4
- インバンド IPv6

（注） 3 つをすべて設定する必要はありません。

はじめる前に

サーバで管理 IP プールを使用するように設定する前に、管理 IP プールを設定します。

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 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。

- アウトバンド IP プール管理 IP アドレス ポリシーを設定するには、ステップ 6 に進みます。
- インバンド IPv4、IPv6 管理 IP アドレス ポリシーを設定するには、ステップ 8 に進みます。

ステップ 6 [Actions] 領域で、[Use Outband Pooled Management IP] をクリックします。

ステップ 7 [Use Outband Pooled Management IP] の確認ダイアログ ボックスで [Yes] をクリックし、[OK] をクリックします。
これで管理 IP アドレス ポリシーが、アウトバンド管理 IP プールの OOB IP アドレスを使用するように設定されます。

ステップ 8 [Actions] 領域で、[Change Inband Management IP] をクリックします。

ステップ 9 [Change Management IP] ダイアログ ボックスには、2 つのタブがあります。

- [Inband IPv4]
- [Inband IPv6]

a) インバンド IPv4 管理 IP プールを変更するには、[Inband IPv4] タブをクリックし、次のフィールドに入力します。

フィールド	説明
[Network] ドロップダウン リスト	サーバに使用させるネットワーク（VLAN）。

フィールド	説明
[Management IP Address Policy] ドロップダウン リスト	サーバに割り当てる管理 IP プール。 使用可能なプールが 2 種類あります。 • Domain Pools • Global Pools [Domain Pools] のエントリ、または [Global Pools] のエントリから使用可能なプールを 1 つ選択します。

b) インバンド IPv6 管理 IP プールを変更するには、[Inband IPv6] タブをクリックし、次のフィールドに入力します。

フィールド	説明
[Network] ドロップダウン リスト	サーバに使用させるネットワーク（VLAN）。
[Management IP Address Policy] ドロップダウン リスト	サーバに割り当てる管理 IP プール。 使用可能なプールが 2 種類あります。 • Domain Pools • Global Pools [Domain Pools] のエントリ、または [Global Pools] のエントリから使用可能なプールを 1 つ選択します。

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。

ラック サーバからのインバンド設定の削除

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

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Rack-Mounts] > [Servers] > *[Server Name]* を展開します。

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

ステップ 4 [CIMC] サブタブをクリックします。

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

ステップ 6 [Delete] の確認ダイアログボックスで [Yes] をクリックします。
サーバのインバンド設定が削除されます。

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

サービス プロファイルの管理 IP アドレスの設定

サービス プロファイルで次の管理 IP アドレスを設定できます。

- アウトオブバンド（OOB）IPv4 アドレス
- インバンド IPv4 アドレス
- インバンド IPv6 アドレス

この手順では、サービス プロファイルの管理 IP アドレスを設定するプロセスを説明します。

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 管理 IP アドレスを設定するサービス プロファイルを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 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 アウトオブバンド IPv4 アドレスを変更するには、[Outband IPv4] タブをクリックして次のフィールドに入力します。

名前	説明
[Management IP Address Policy] ドロップダウン	このサービス プロファイルに関連付けられたサーバ用の OOB 管理 IPv4 アドレスの取得方法。 次のいずれかになります。 • [None]：サービス プロファイルによってサーバに割り当てられた管理 IP アドレスはありません。 管理 IP アドレスは、サーバで定義される CIMC 管理 IP アドレスに基づきます。 • [Static]：サービス プロファイルは、関連するサーバにスタティック管理 IP アドレスを割り当てます。 サービス プロファイルを新しいサーバに移行すると、この管理 IP アドレスも一緒に移動します。 • [Domain Pools]：サービス プロファイルは、プール リストから選択されたプールから IP 管理アドレスを関連するサーバに割り当てます。 サービス プロファイルを新しいサーバに移行すると、この管理 IP アドレスも一緒に移動します。
[IP Address] フィールド	サービス プロファイルを介してサーバに割り当てられた OOB 管理 IPv4 アドレス。 （注） IP アドレス フィールドは、[Management IP Address Policy] を [Static] に設定した場合、または、[Domain Pools] の IP アドレス プールのいずれかを [Management IP Address Policy] フィールドのドロップダウン リストから選択した場合にのみ表示されます。
[Subnet Mask] フィールド	OOB 管理 IPv4 アドレスのサブネット マスク。
[Default Gateway] フィールド	OOB 管理 IPv4 アドレスのデフォルトのゲートウェイ。

a) [Management IP Address Policy] ドロップダウン リストから [Static] を選択した場合は、次のフィールドに入力します。

名前	説明
[IP Address] フィールド	サービス プロファイルを介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のゲートウェイ。

ステップ 8 インバンド IPv4 アドレスを変更するには、[Inband] タブをクリックし、[Inband IPv4] サブタブをクリックして次のフィールドに入力します。

名前	説明
[Network] ドロップダウン	関連付けられている VLAN グループから選択された VLAN。
[Management IP Address Policy] ドロップダウン	このサービス プロファイルに関連付けられたサーバ用のインバンド管理 IPv4 アドレスの取得方法。 次のいずれかになります。 • [None]：サービス プロファイルによってサーバに割り当てられた管理 IP アドレスはありません。 管理 IP アドレスは、サーバで定義される CIMC 管理 IP アドレスに基づきます。 • [Static]：サービス プロファイルは、関連するサーバにスタティック管理 IP アドレスを割り当てます。 サービス プロファイルを新しいサーバに移行すると、この管理 IP アドレスも一緒に移動します。 • [Domain Pools]：サービス プロファイルは、プール リストから選択されたプールから IP 管理アドレスを関連するサーバに割り当てます。 サービス プロファイルを新しいサーバに移行すると、この管理 IP アドレスも一緒に移動します。
[IP Address] フィールド	サービス プロファイルを介してサーバに割り当てられたインバンド管理 IPv4 アドレス。 （注） IP アドレス フィールドは、[Management IP Address Policy] を [Static] に設定した場合、または、[Domain Pools] の IP アドレス プールのいずれかを [Management IP Address Policy] フィールドのドロップダウン リストから選択した場合にのみ表示されます。
[Subnet Mask] フィールド	インバンド管理 IPv4 アドレスのサブネット マスク。
[Default Gateway] フィールド	インバンド管理 IPv4 アドレスのデフォルトのゲートウェイ。

a) [Management IP Address Policy] ドロップダウン リストから [Static] を選択した場合は、次のフィールドに入力します。

名前	説明
[IP Address] フィールド	このサービス プロファイルに関連付けられたサーバのインバンド管理 IPv4 アドレス。
[Subnet Mask] フィールド	OOB 管理 IPv4 アドレスのサブネット マスク。

名前	説明
[Default Gateway] フィールド	OOB 管理 IPv4 アドレスのデフォルトのゲートウェイ。

ステップ 9 インバンド IPv6 アドレスを変更するには、[Inband] タブをクリックし、[Inband IPv6] サブタブをクリックして次のフィールドに入力します。

名前	説明
[Network] ドロップダウン	関連付けられている VLAN グループから選択された VLAN。
[Management IP Address Policy] ドロップダウン	このサービス プロファイルに関連付けられたサーバ用のインバンド管理 IPv6 アドレスの取得方法。 次のいずれかになります。 • [None]：サービス プロファイルによってサーバに割り当てられた管理 IP アドレスはありません。 管理 IP アドレスは、サーバで定義される CIMC 管理 IP アドレスに基づきます。 • [Static]：サービス プロファイルは、関連するサーバにスタティック管理 IP アドレスを割り当てます。 サービス プロファイルを新しいサーバに移行すると、この管理 IP アドレスも一緒に移動します。 • [Domain Pools]：サービス プロファイルは、プール リストから選択されたプールから IP 管理アドレスを関連するサーバに割り当てます。 サービス プロファイルを新しいサーバに移行すると、この管理 IP アドレスも一緒に移動します。
[IP Address] フィールド	サービス プロファイルを介してサーバに割り当てられたインバンド管理 IPv6 アドレス。 （注） IP アドレス フィールドは、[Management IP Address Policy] を [Static] に設定した場合、または、[Domain Pools] の IP アドレス プールのいずれかを [Management IP Address Policy] フィールドのドロップダウン リストから選択した場合にのみ表示されます。
[Prefix] フィールド	インバンド管理 IPv6 アドレスのプレフィックス。
[Default Gateway] フィールド	インバンド管理 IPv6 アドレスのデフォルト ゲートウェイ。

a) [Management IP Address Policy] ドロップダウン リストから [Static] を選択した場合は、次のフィールドに入力します。

名前	説明
[IP Address] フィールド	サービス プロファイルを介してサーバに割り当てられたインバンド管理 IPv6 アドレス。
[Prefix] フィールド	インバンド管理IPv6アドレスのプレフィックス。
[Default Gateway] フィールド	インバンド管理 IPv6 アドレスのデフォルト ゲートウェイ。

ステップ 10 [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 テンプレートを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。
ステップ 4 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 [Actions] 領域で、[Change Management IP Address] をクリックします。
ステップ 8 [Change Management IP Address] ダイアログボックスのフィールドに入力します。
ステップ 9 [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、外部の IPv4 および IPv6 アドレスの集合です。 Cisco UCS Manager は、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。

個別のアウトオブバンド IPv4 アドレス プール、およびインバンド IPv4 または IPv6 アドレス プールを設定できます。 IPv4 と IPv6 アドレス ブロックの両方を含むインバンド プールを設定できます。

ヒント　サーバ CIMC に IPv4 アドレスのみを含む IP プールをインバンド IPv6 ポリシーとして割り当てたり、IPv6 アドレスのみ含む IP プールをインバンド IPv4 ポリシーとして割り当てることを回避するために、それぞれが IPv4 または IPv6 アドレスのみを持つ個別のインバンド アドレス プールを設定することを推奨します。

管理 IP プールの 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サーバを設定することはできません。

管理 IP プール内のすべての IP アドレスは、同じ IPv4 サブネットに含まれるか、ファブリック インターコネクトの IPアドレスと同じ IPv6 ネットワーク プレフィックスが付けられている必要があります。

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

管理 IP プールでの IPv4 アドレス ブロックの作成

サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、管理 IP プールに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 IPv4 Addresses] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[名前] カラム	ブロックに割り当てられた IPv4 アドレスの範囲。
[From] カラム	ブロック内の最初の IPv4 アドレス。
[To] カラム	ブロック内の最後の IPv4 アドレス。
[Subnet] カラム	ブロック内の IPv4 アドレスと関連付けられたサブネット マスク。
[Default Gateway] カラム	ブロック内の IPv4 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] カラム	IPv4 アドレスのこのブロックがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] カラム	IPv4 アドレスのこのブロック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、管理 IP プールから CIMC IP アドレスを取得します。

管理 IP プールでの IPv6 アドレス ブロックの作成

サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、管理 IP プールに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 IPv6 Addresses] ダイアログボックスで、必要な情報を指定します。
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、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 29 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，373 ページ
- CIMC セキュリティ ポリシー，402 ページ
- ローカル ディスク設定ポリシーの設定，405 ページ
- スクラブ ポリシーの設定，416 ページ
- DIMM エラー管理の設定，418 ページ
- Serial over LAN ポリシーの設定，421 ページ
- サーバ自動構成ポリシーの設定，422 ページ
- サーバ ディスカバリ ポリシーの設定，424 ページ
- サーバ継承ポリシーの設定，426 ページ
- サーバ プール ポリシーの設定，428 ページ
- サーバ プール ポリシーの資格情報の設定，430 ページ
- vNIC/vHBA 配置ポリシーの設定，437 ページ
- CIMC マウント vMedia，452 ページ

BIOS の設定

サーバ BIOS 設定

Cisco UCSでは、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方法が 2 通り用意されています。 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 ポリシーおよびサーバ プラットフォームのデフォルトの BIOS 設定のいずれを使用しても、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。

データセンターのニーズに応じて、一部のサービス プロファイルについては BIOS ポリシーを設定し、同じ Cisco UCS ドメイン内の他のサービス プロファイルについては BIOS のデフォルトを使用したり、そのいずれかのみを使用したりできます。 また、Cisco UCS Manager を使用して、サーバの実際の BIOS 設定を表示し、それらが現在のニーズを満たしているかどうかを確認できます。

（注） Cisco UCS Manager は、BIOS ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。 これらの変更はバッファ内にとどまり、サーバがリブートされるまでは有効になりません。

設定するサーバで BIOS 設定のサポートを確認することをお勧めします。RAS メモリのミラーリング モードなど一部の設定は、すべての Cisco UCS サーバでサポートされているわけではありません。

メイン BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるメイン サーバの BIOS 設定を示しています。

名前	説明
[Reboot on BIOS Settings Change]	1 つ以上の BIOS 設定を変更した後にサーバをリブートするタイミング。 この設定を有効にした場合は、サーバのサービス プロファイルのメンテナンス ポリシーに従ってリブートされます。 たとえば、メンテナンス ポリシーでユーザの確認応答が必要な場合、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。 この設定を有効にしない場合は、別のサーバ設定の変更によるリブートであれ手動によるリブートであれ、次回サーバがリブートされるまで BIOS の変更は適用されません。

名前	説明
[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やオプション 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。
[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、電力が復帰したときにサーバが実行する動作を決定します。 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。

名前	説明
[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

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるプロセッサの BIOS 設定を示しています。

名前	説明
[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は自動的には上がりません。 • [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。

名前	説明
[Enhanced Intel Speedstep]	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。 このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。 次のいずれかになります。 • [disabled]：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。
[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。

名前	説明
[Core Multi Processing]	パッケージ内の論理プロセッサ コアの状態を設定します。 この設定をディセーブルにすると、ハイパー スレッディング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 コアでマルチ プロセッシングを有効にします。 • [1] ～ [10]：サーバで実行可能な論理プロセッサ コアの数を指定します。 マルチプロセッシングをディセーブルにし、サーバ上で動作する論理プロセッサ コアを 1 つだけにするには、[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。
[Execute Disabled Bit]	サーバのメモリ領域を分類し、アプリケーション コードを実行可能な場所を指定します。 この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行をディセーブルにします。 この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。 次のいずれかになります。 • [disabled]：プロセッサでメモリ領域を分類しません。 • [enabled]：プロセッサで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。

名前	説明
[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]：プロセッサでのバーチャライゼーションを禁止します。 • [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。
[Direct Cache Access]	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。 この設定はキャッシュミスを減らすのに役立ちます。 次のいずれかになります。 • [disabled]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [enabled]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。 • [platform-default]：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 C State]	アイドル期間中にシステムが省電力モードに入ることができるかどうか。 次のいずれかになります。 • [disabled]：システムはアイドル時でもハイ パフォーマンス状態のままになります。 • [enabled]：システムは DIMM や CPU などのシステム コンポーネントへの電力を低減できます。 • [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 ステートになったときに、プロセッサが最小周波数に移行できるようにします。 この設定は、サーバをリブートするまで有効になりません。 次のいずれかになります。 • [disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [enabled]：CPU は最小周波数に移行します。 このオプションでは C1 ステートで節約される電力量が最大になります。 • [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。

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] メニューでは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]：M3 サーバの場合、すべてのプリフェッチャとデータの再利用がイネーブルになります。 M1 および M2 サーバの場合は、データの再利用と DCU IP プリフェッチャはイネーブルになり、他のすべてのプリフェッチャはディセーブルになります。 • [high-throughput]：データの再利用と DCU IP プリフェッチャはイネーブルになり、他のすべてのプリフェッチャはディセーブルになります。 • [hpc]：プリフェッチャはすべてイネーブルになり、データの再利用はディセーブルになります。 この設定はハイ パフォーマンス コンピューティングとも呼ばれます。
[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 変数に対して指定された数を使用します。 • [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。

名前	説明
[Local X2 APIC]	APIC アーキテクチャのタイプを設定できます。 次のいずれかになります。 • [xapic]：標準の xAPIC アーキテクチャを使用します。 • [x2apic]：拡張 x2APIC アーキテクチャを使用してプロセッサの 32 ビット アドレス指定機能をサポートします。 • [auto]：検出された xAPIC アーキテクチャを自動的に使用します。 • [platform-default]：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 の BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる Intel Directed I/O の BIOS 設定を示しています。

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]：プロセッサでバーチャライゼーションテクノロジーを使用しません。 • [enabled]：プロセッサでバーチャライゼーション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） 他の Intel Directed I/O BIOS 設定を変更する場合は、このオプションを有効にする必要があります。

名前	説明
[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。
[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。

名前	説明
[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 メモリの BIOS 設定

次の表に、BIOS ポリシーまたはデフォルト BIOS 設定を介して実行できる RAS メモリの BIOS 設定の一覧を示します。

名前	説明
[Memory RAS Config]	サーバに対するメモリの Reliability, Availability, and Serviceability（RAS）の設定方法。 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。 • [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
[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。
[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ときのみ使用可能です。 次のいずれかを指定できます。 • [inter-socket]：メモリは、CPU ソケットをまたいで 2 台の Integrated Memory Controller（IMC）間でミラーリングされます。 • [intra-socket]：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。

名前	説明
[Sparing Mode]	スペアリングはメモリを予備に保持することで信頼性を最適化し、別のDIMMの障害発生時に使用できるようにします。このオプションは、メモリの冗長性を実現しますが、ミラーリングほどの冗長性は提供されません。使用可能なスペアリングのモードは、現在のメモリの数によって異なります。 このオプションは、[Memory RAS Config] で [sparing] オプションを選択したときのみ使用可能です。次のいずれかを指定できます。 • [dimm-sparing]：1 枚の DIMM が予備に保持されます。DIMM に障害が発生すると、その DIMM の内容はスペア DIMM に移されます。 • [rank-sparing]：DIMM のスペア ランクが予備に保持されます。DIMM のランクに障害が発生した場合、そのランクの内容がスペア ランクに移されます。 • [platform-default]：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。
[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。
[DRAM Refresh Rate]	このオプションは、内部メモリの更新頻度を制御します。

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 BIOS 設定を介して実行できるシリアル ポートの BIOS 設定の一覧を示します。

名前	説明
[Serial Port A]	シリアル ポート A がイネーブルかディセーブルか。 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 BIOS 設定を介して実行できる USB BIOS 設定の一覧を示します。

名前	説明
[Make Device Non Bootable]	サーバが USB デバイスからブートできるかどうか。 次のいずれかになります。 • [disabled]：サーバは USB デバイスからブートできます。 • [enabled]：サーバは 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。

名前	説明
[Legacy USB Support]	システムでレガシーUSBデバイスをサポートするかどうか。 次のいずれかになります。 • [disabled]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [enabled]：レガシーUSBのサポートは常に使用できます。 • [auto]：USB デバイスが接続されていない場合、レガシーUSBのサポートがディセーブルになります。 • [platform-default]：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 のアイドル時電力消費を減らすために USB システムにアイドル時電力最適化設定を使用するかどうか。 この設定で選択した値によって、パフォーマンスが影響を受けることがあります。 次のいずれかになります。 • [high-performance]：最適なパフォーマンスを電力節約より優先するため、USBシステムのアイドル時電力最適化設定はディセーブルにされます。 このオプションを選択すると、パフォーマンスが大幅に向上します。 サイトにサーバの電源制限がない場合はこのオプションを選択することを推奨します。 • [lower-idle-power]：電力節約を最適なパフォーマンスより優先するため、USBシステムのアイドル時電力最適化設定はイネーブルにされます。 • [platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[USB Front Panel Access Lock]	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 設定の BIOS 設定

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができる PCI 設定の BIOS 設定を示しています。

名前	説明
[Max Memory Below 4G]	システム設定に応じて、PAE 非対応のオペレーティング システムのメモリ使用量を BIOS で 4 GB 以下に最大化するかどうか。 次のいずれかになります。 • [disabled]：メモリ使用量を最大化しません。 PAE 対応のオペレーティング システムすべてに対してこのオプションを選択します。 • [enabled]：PAE 非対応のオペレーティング システムに対して、メモリ使用量を 4 GB 以下に最大化します。 • [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
[Memory Mapped IO Above 4Gb Config]	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O をイネーブルにするか、ディセーブルにするか。 レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。 PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。 次のいずれかになります。 • [disabled]：64 ビット PCI デバイスを 4 GB 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 デバイスを 4 GB 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

次の表は、BIOS ポリシーまたはデフォルトの BIOS 設定を介して行うことができるブート オプションの BIOS 設定を示しています。

名前	説明
[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]：ユーザ入力を待機してから非 EFI ベースのブート オプションを再試行します。 • [enabled]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。

名前	説明
[Intel Entry SAS RAID]	Intel SAS Entry RAID モジュールがイネーブルかどうか。次のいずれかになります。 • [disabled]：Intel SAS Entry RAID モジュールはディセーブルです。 • [enabled]：Intel SAS 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 SAS Entry RAID モジュールをどのように設定するか。 次のいずれかになります。 • [it-ir-raid]：Intel IT/IR RAID を使用するよう RAID モジュールを設定します。 • [intel-esrtii]：Intel Embedded Server RAID Technology II を使用するよう RAID モジュールを設定します。 • [platform-default]：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。
[Onboard SCU Storage Support]	オンボード ソフトウェア RAID コントローラを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 コントローラを使用できません。 • [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 BIOS 設定を介して実行できるサーバ管理 BIOS 設定の一覧を示します。

[General Settings]

名前	説明
[Assert Nmi on Serr]	システムエラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。 次のいずれかになります。 • [disabled]：SERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [enabled]：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 [Assert Nmi on Perr] を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。
[Assert Nmi on Perr]	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、エラーをログに記録するかどうか。 次のいずれかになります。 • [disabled]：PERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [enabled]：PERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 この設定を使用するには、[Assert Nmi on Serr] をイネーブルにする必要があります。 • [platform-default]：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
[OS Boot Watchdog Timer]	BIOSが、定義済みのタイムアウト値を持つウォッチドッグ タイマーをプログラムするかどうか。 タイマーが切れる前にオペレーティング システムのブートを完了しない場合、CIMC はシステムをリセットし、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]：サーバのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [enabled]：サーバのブートにかかる時間をウォッチドッグ タイマーでトラッキングします。 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 管理ソフトウェアが必要です。
[OS Boot Watchdog Timer Timeout Policy]	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。 次のいずれかになります。 • [power-off]：OSブート中にウォッチドッグ タイマーが期限切れになった場合、サーバは電源オフになります。 • [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だけ利用できます。

名前	説明
[OS Boot Watchdog Timer Timeout]	BIOS でウォッチドッグ タイマーの設定に使用されるタイムアウト値。 次のいずれかになります。 • [5-minutes]：ウォッチドッグ タイマーは OS ブート開始から 5 分後に期限切れになります。 • [10-minutes]：ウォッチドッグ タイマーは OS ブート開始から 10 分後に期限切れになります。 • [15-minutes]：ウォッチドッグ タイマーは OS ブート開始から 15 分後に期限切れになります。 • [20-minutes]：ウォッチドッグ タイマーは OS ブート開始から 20 分後に期限切れになります。 • [platform-default]：BIOS は、サーバ タイプとベンダーのBIOS デフォルト値に含まれるこの属性の値を使用します。 このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にだけ利用できます。

コンソール リダイレクション設定

名前	説明
[Console Redirection]	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。 次のいずれかになります。 • [disabled]：POST 中にコンソール リダイレクションは発生しません。 • [serial-port-a]：POST 中のコンソール リダイレクションのためシリアル ポート A をイネーブルにします。このオプションはブレードサーバおよびラックマウント サーバに対して有効です。 • [serial-port-b]：コンソール リダイレクションのためシリアル ポート B をイネーブルにし、サーバ管理タスク実行を許可します。 このオプションは、ラックマウント サーバでのみ有効です。 • [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場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。
[Flow Control]	フロー制御にハンドシェイク プロトコルを使用するかどうか。 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]：RTS/CTS がフロー制御に使用されます。 • [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 アプリケーション上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 ポートの伝送速度として使用されるボー レート。 [Console Redirection] をディセーブルにした場合は、このオプションを使用できません。 次のいずれかになります。 • [9600]：ボー レート 9600 が使用されます。 • [19200]：ボー レート 19200 が使用されます。 • [38400]：ボー レート 38400 が使用されます。 • [57600]：ボー レート 57600 が使用されます。 • [115200]：ボー レート 115200 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 アプリケーション上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される文字フォーマットのタイプ。 次のいずれかになります。 • [pc-ansi]：PC-ANSI 端末フォントが使用されます。 • [vt100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [vt100-plus]：サポートされている vt100-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 アプリケーション上の設定と一致している必要があります。

名前	説明
[Legacy OS Redirect]	シリアル ポートでレガシーなオペレーティング システム（DOS など）からのリダイレクションを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 リダイレクションがイネーブルになっているシリアル ポートは、レガシーなオペレーティング システムから認識されません。 • [enabled]：コンソール リダイレクションがイネーブルになっているシリアル ポートは、レガシーなオペレーティング システムから認識できます。 • [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。

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 はサーバ上の BIOS 設定を BIOS ポリシー内の設定と一致するように変更します。 BIOS ポリシーを作成せず、BIOS ポリシーをサービス プロファイルに割り当てていない場合は、サーバの 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 がサポートするサーバの各タイプのための 1 セットのデフォルト BIOS 設定が含まれます。 デフォルト BIOS 設定は、ルート組織だけで使用でき、グローバルです。 Cisco UCS でサポートされている各サーバ プラットフォームには、1 セットの BIOS 設定だけを適用できます。 デフォルト BIOS 設定は変更できますが、デフォルト BIOS 設定の追加セットの作成はできません。

デフォルト BIOS 設定の各セットは、サポートされているサーバの特定のタイプに合わせて設計されており、サービス プロファイルに BIOS ポリシーが含まれていない、特定のタイプのすべてのサーバに適用されます。

Cisco UCS 実装にサーバ特定の設定によって満たされない特定の要件がない限り、Cisco UCS ドメインのサーバの各タイプ用に設計されたデフォルト BIOS 設定を使用するよう推奨します。

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 ポリシーはインクルードされません。
- 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 ポリシーまたはデフォルトの BIOS 設定による BIOS 設定の変更を Cisco Integrated Management Controller（CIMC）バッファにプッシュします。 これらの変更はバッファ内にとどまり、サーバがリブートされるまでは有効になりません。

設定するサーバで BIOS 設定のサポートを確認することをお勧めします。 RAS メモリのミラーリング モードなど一部の設定は、すべての Cisco UCS サーバでサポートされているわけではありません。

手順

ステップ 1 [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 [名前] 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

ステップ 6 [Create BIOS Policy] ウィザードで、次の手順を実行して BIOS 設定を実行します。

a) BIOS 設定を変更する場合は、該当するオプション ボタンをクリックするか、ドロップダウン リストから適切な項目を選択します。
各 BIOS 設定のオプションに関する説明および情報については、次のトピックを参照してください。

- [Main] ページ： メイン BIOS 設定, （374 ページ）
- [Processor] ページ： プロセッサの BIOS 設定, （376 ページ）
- [Intel Directed IO] ページ： Intel Directed I/O の BIOS 設定, （383 ページ）
- [RAS Memory] ページ： RAS メモリの BIOS 設定, （385 ページ）
- [Serial Port] ページ： シリアル ポートの BIOS 設定, （388 ページ）
- [USB] ページ： USB の BIOS 設定, （388 ページ）
- [PCI Configuration] ページ： PCI 設定の BIOS 設定, （390 ページ）
- [Boot Options] ページ： ブート オプションの BIOS 設定, （391 ページ）
- [Server Management] ページ： サーバ管理 BIOS 設定, （392 ページ）

b) 次のページに移動するには、[Next] をクリックします

ステップ 7 ポリシーの BIOS 設定すべてが完了したら、[Finish] をクリックします。

BIOS のデフォルトの修正

設定するサーバで BIOS 設定のサポートを確認することをお勧めします。 RAS メモリのミラーリング モードなど一部の設定は、すべてのCisco UCS サーバでサポートされているわけではありません。

Cisco UCS 実装にサーバ特定の設定によって満たされない特定の要件がない限り、Cisco UCS ドメインのサーバの各タイプ用に設計されたデフォルト BIOS 設定を使用するよう推奨します。

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] を展開して、デフォルトの BIOS 設定を変更するサーバのモデル番号を選択します。

ステップ 5 [Work] ペインで該当するタブをクリックしてから、必要なオプション ボタンをクリックするか、ドロップダウン リストから選択してデフォルトの BIOS 設定を変更します。
各 BIOS 設定のオプションに関する説明および情報については、次のトピックを参照してください。 すべての BIOS 設定がサーバの各タイプに使用できるわけではありません。

- [Main] タブ： メイン BIOS 設定, （374 ページ）
- [Advanced] タブ：
  - [Processor] サブタブ： プロセッサの BIOS 設定, （376 ページ）
  - [Intel Directed IO] サブタブ： Intel Directed I/O の BIOS 設定, （383 ページ）
  - [RAS Memory] サブタブ： RAS メモリの BIOS 設定, （385 ページ）
  - [Serial Port] サブタブ： シリアル ポートの BIOS 設定, （388 ページ）
  - [USB] サブタブ： USB の BIOS 設定, （388 ページ）
  - [PCI Configuration] サブタブ： PCI 設定の BIOS 設定, （390 ページ）
- [Boot Options] タブ： ブート オプションの BIOS 設定, （391 ページ）
- [Server Management] タブ： サーバ管理 BIOS 設定, （392 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、見出しの右側にある [Expand] アイコンをクリックして領域を開きます。
[BIOS Settings] 領域の各タブに、そのサーバ プラットフォームの設定が表示されます。 いくつかのタブには追加情報を含むサブタブがあります。

CIMC セキュリティ ポリシー

Cisco UCS Manager は、セキュリティを強化するために次のポリシーを提供しています。

- KVM 管理ポリシー
- IPMI アクセス プロファイル

IPMI アクセス プロファイル

このポリシーでは、IPアドレスを使用して、IPMIコマンドを直接サーバ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 Access Profiles] を右クリックし、[Create IPMI Access Profile] を選択します。

ステップ 5 [Create IPMI Access Profile] ダイアログボックスで次の手順を実行します。

a) プロファイルの一意の名前および説明を入力します。

b) [IPMI Over LAN] フィールドで、リモート接続を許可するか、禁止するかを選択します。

c) [OK] をクリックします。

ステップ 6 ナビゲータの [IPMI Users] 領域で、[+] をクリックします。

ステップ 7 [Create IPMI User] ダイアログボックスで、次の手順を実行します。

a) 次のフィールドに入力します。

名前	説明
[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 文字の英数字を入力します。「@」（アット マーク）、「_」（アンダースコア）、「-」（ハイフン）も使用できます。プロファイルの保存後は、この名前を変更できません。
[Password] フィールド	このユーザ名に関連付けられるパスワード。 1 ～ 20 文字の標準 ASCII 文字を入力します（ただし、「=」（等号）、「$」（ドル記号）、「|」（縦棒）は除く）。
[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 プロファイルをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

IPMI アクセス プロファイルの削除

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。

KVM 管理ポリシー

このポリシーを使用して、KVM 経由でサーバにアクセスするときに vMedia 暗号化を有効にするかどうかを指定できます。

このポリシーはサービスプロファイルに組み込む必要があります。また。このサービスプロファイルを有効にするには、サーバに関連付ける必要があります。

KVM 管理ポリシーの作成

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 [KVM Management Policies] を右クリックし、[Create KVM Management Policy] を選択します。
ステップ 5 [Create KVM Management Policy] ダイアログ ボックスで次の手順を実行します。
a) ポリシーの一意の名前と説明を入力します。
b) [vMedia Encryption] フィールドで、vMedia 暗号化をイネーブルにするかどうかを選択します。
c) [OK] 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含む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 モードを設定できるようにします。

ローカル ディスク モードには次のものがあります。

- [ローカルストレージなし] : 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がストライプ済み] : 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がミラー済み] : 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でも完全なデータ冗長性を提供します。 最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。
- [任意の設定] : 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。
- [RAIDなし] : 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。

  [RAIDなし] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。 そのため、[RAIDなし]モードの適用後にサーバでの違いがわからないことがあります。 よって、ポリシーの RAID 設定と、サーバの [インベントリ] > [ストレージ] タブに表示される実際のディスク設定とが一致しない場合があります。

  以前のすべての RAID 設定情報をディスクから削除するには、[RAIDなし] 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が部分的にストライプ済み] : 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が部分的にデュアルストライプ済み] : データはアレイのすべてのディスクにストライプ化され、2 つのパリティ ディスクを使用して、最大 2 つの物理ディスクの障害に対する保護を提供します。 データ ブロックの各行に、2 セットのパリティ データが格納されます。
- [RAID 10がミラーおよびストライプ済み] : RAID 10 はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。

- [RAID 50が部分的にストライプおよびストライプ済み] : データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。
- [RAID 60部分的にストライプおよびストライプ済み] : データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。

このポリシーはサービス プロファイルに組み込む必要があります。また。このポリシーを有効にするには、サーバ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

1 台のサーバや RAID 設定に、HDD と SSD を使用しないでください。

JBOD モードのサポート

B200 M3 サーバはローカル ディスクの JBOD モードをサポートします。

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

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。 これを実行するには、そのサーバに定義されている RAID モードのいずれかを使用して、サービス プロファイルのローカル ディスク設定ポリシーを設定するか、[任意の設定] モードと LSI ユーティリティ ツールセットを使用して、RAID ボリュームを作成します。

OS をインストールする前に RAID LUN を設定していないと、インストール時にディスク検出エラーが発生し、「No Device Found」といったエラー メッセージが表示される可能性があります。

サーバ プロファイルで [任意の設定] モードが指定されている場合、RAID 1 クラスタ移行後にサーバが起動しない

RAID 1 クラスタの移行後、サービス プロファイルをサーバに関連付ける必要があります。 サービス プロファイル内のローカル ディスク設定ポリシーに RAID 1 ではなく [任意の設定] モードが設定されていると、RAID LUN は、関連付け中およびその後も「非アクティブ」状態のままになります。 その結果、サーバ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、[任意の設定] 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、このサーバで完全に機能するよう設計されていません。

統合されたラックマウント サーバ内の 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、Cisco UCS Central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 つまでしか設定できません。

統合されたラックマウント サーバ内のローカル 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 では、そのような設定はサポートされていません。

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 では、そのような設定はサポートされていません。

一部のサーバの特定の RAID 設定オプションでは、ライセンスが必要

一部の Cisco UCS サーバには、特定の RAID 設定オプションのライセンスが必要です。 Cisco UCS Manager で、このローカル ディスク ポリシーを含むサービス プロファイルとサーバを関連付けると、Cisco UCS Manager によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。 問題がある場合は、サービス プロファイルを関連付ける際に、Cisco UCS Manager に設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『ハードウェア インストール ガイド』を参照してください。

ローカル ディスク設定ポリシーの作成

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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[所有者] フィールド	次のいずれかになります。 • [ローカル]：このポリシーは、Cisco UCS ドメイン内のサービス プロファイルとサービス プロファイル テンプレートでのみ使用できます。 • [Pending Global]：このポリシーの制御は Cisco UCS Central に移行中です。 移行が完了すると、このポリシーは Cisco UCS Centralに登録されているすべての Cisco UCS ドメインで使用可能になります。 • [Global]：このポリシーは Cisco UCS Centralによって管理されます。 このポリシーを変更する場合は、必ず Cisco UCS Centralを使用して変更してください。

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。 • [ローカルストレージなし] : 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がストライプ済み] : 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がミラー済み] : 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でも完全なデータ冗長性を提供します。 最大アレイ サイズは、2つのドライブの小さい方の空き容量に等しくなります。 • [任意の設定] : 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。 • [RAIDなし] : 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。 [RAIDなし] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。 そのため、[RAIDなし] モードの適用後にサーバでの違いがわからないことがあります。 よって、ポリシーの RAID 設定と、サーバの [インベントリ] > [ストレージ] タブに表示される実際のディスク設定とが一致しない場合があります。 以前のすべての RAID 設定情報をディスクから削除するには、[RAIDなし] 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が部分的にストライプ済み] : 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

名前	説明
	が部分的にデュアルストライプ済み]：データはアレイのすべてのディスクにストライプ化され、2つのパリティディスクを使用して、最大2つの物理ディスクの障害に対する保護を提供します。データブロックの各行に、2セットのパリティ データが格納されます。 • [RAID 10がミラーおよびストライプ済み]：RAID 10 はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。 • [RAID 50が部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティディスクセットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。 • [RAID 60部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。 （注） 一部の Cisco UCS サーバには、特定の RAID 設定オプションのライセンスが必要です。 Cisco UCS Manager で、このローカル ディスク ポリシーを含むサービス プロファイルとサーバを関連付けると、Cisco UCS Manager によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。 問題がある場合は、サービス プロファイルを関連付ける際に、Cisco UCS Manager に設定エラーが表示されます。 特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『ハードウェア インストール ガイド』を参照してください。

名前	説明
[設定の保護]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、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、[設定の保護] 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 プロパティの設定が優先され、前のサービス プロファイルの設定が上書きされます。 （注） このオプションが有効な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。
[FlexFlashステータス] オプション ボタン	SD カードの FlexFlash コントローラを有効化または無効化にするには、該当するボタンをクリックしてください。 （注） このパラメータは、SD カード モジュールのあるサーバのみ該当します。
[FlexFlash RAIDレポートステータス] オプション ボタン	RAID レポートを有効化または無効化にするには、該当するボタンをクリックしてください。RAID レポートを有効にすると、RAID ステータスがモニタリングされ、障害が有効化されます。 （注） 1 枚の SD カードのみが装着されている場合は、RAID レポートが有効な場合でも、RAID ステータスは「無効化」と表示され、RAID の状態は「NA」と表示されます。

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ものです。 [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] ペインで、[Storage] タブをクリックします。

ステップ 6 [Actions] 領域で、[Change Local Disk Configuration Policy] をクリックします。

ステップ 7 [Change Local Disk Configuration Policy] ダイアログボックスで、[Select the Local Disk Configuration Policy] ドロップダウン リストから次のいずれかのオプションを選択します。

オプション	説明
Use a Disk Policy	このオプションのリストから既存のローカルディスク設定ポリシーを選択します。 Cisco UCS Manager 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。

FlexFlash のサポート

概要

Cisco UCS B シリーズおよび C シリーズ M3 サーバは内部セキュア デジタル（SD）メモリ カードをサポートします。 SD カードは、Cisco Flexible Flash ストレージ コントローラ（SD カード用スロットが 2 つある PCI ベースのコントローラ）によってホストされます。 カードには、HV と呼ばれる単一のパーティションが含まれます。 FlexFlash がイネーブルの場合、Cisco UCS Manager には、BIOS とホスト オペレーティング システムの両方に対する USB ドライブとして HV パーティションが表示されます。

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

サポートされるサーバでFlexFlashをディセーブルにすると、ホストの再起動がトリガーされ、再起動の警告メッセージが表示されます。 FlexFlash コントローラは、関連サービス プロファイルの関連付け解除の一環としてもディセーブルになります。

FlexFlash コントローラはデュアル SD カード用の RAID-1 をサポートします。 FlexFlash スクラブ ポリシーを作成しサーバを再認識することで RAID ペアに新しい SD カードを設定できます。 FlexFlash スクラブ ポリシーは、両方のカードの HV パーティションを削除し、そのカードを正常な RAID 状態にすることができます。

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

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

FlexFlash ファームウェア管理

FlexFlash コントローラ ファームウェアは、CIMC イメージの一部としてバンドルされます。 CIMC をアップグレードする際に、最新のファームウェア バージョンが FlexFlash コントローラで使用可能な場合、コントローラは管理されなくなり、FlexFlash インベントリには、コントローラ ステータスが [Waiting For User Action]、コントローラ ヘルスが [Old Firmware Running] と表示されます。 FlexFlash コントローラのファームウェアをアップグレードするには、ボード コントローラの更新を行う必要があります。 詳細については、適切な『*Cisco UCS B-Series Firmware Management Guide*（*Cisco UCS B* シリーズのファームウェアの管理ガイド）』を参照してください。

制限事項：

- 16 GB の SD カードのみサポートされます。

- ラック サーバの SD カードをブレード サーバで使用したり、ブレード サーバの SD カードをラック サーバで使用することは推奨されません。 サーバ タイプ間での SD カードの交換は SD カードのデータ損失につながる可能性があります。
- 一部の Cisco UCS C シリーズ ラックマウント サーバには、4 つのパーティション（HV、HUU、SCU、ドライバ）を持つ SD カードが搭載されています。 Cisco UCS Manager では HV パーティションのみが表示されます。 FlexFlash スクラブ ポリシーを使用して、4 つのパーティションを持つ SD カードを単一 HV パーティション カードに移行できます。
- FlexFlash コントローラは RAID-1 同期（ミラー再構築）をサポートしません。 SD カードが RAID デグレード状態である場合、あるいはメタデータ エラーがコントローラによって報告された場合は、FlexFlash スクラブ ポリシーを実行して RAID のためのカードを組み合わせる必要があります。 FlexFlash スクラブ ポリシーの詳細については、スクラブ ポリシー，（416 ページ） を参照してください。 次の条件によって RAID デグレードやメタデータ エラーが引き起こされる可能性があります。
  - サーバの 1 つのスロットにすでに SD カードが装着されているときに、別のスロットに新しいまたは使用されていた SD カードを挿入する。
  - 異なるサーバの 2 つの SD カードを挿入する。
- サーバのファームウェア バージョンは、2.2(1a) 以上が必要です。

FlexFlash SD カードのサポートのイネーブル化

手順

ステップ 1 [Navigation] ペインの [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] を展開し、FlexFlash サポートをイネーブルにするローカル ディスク設定ポリシーを選択します。

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

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

ステップ 7 [FlexFlash RAID Reporting State] フィールドで、[Enable] オプション ボタンをクリックします。

ステップ 8 [Save Changes] をクリックします。

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、サーバがいつ再認識されるか、またはサーバとサービス プロファイルの関連付けがいつ解除されるかを決定します。

（注） ローカル ディスク スクラブ ポリシーは、Cisco UCS Manager によって管理されるハード ドライブにのみ適用され、USB ドライブなど他のデバイスには適用されません。

スクラブ ポリシーの設定によっては、そのようなときに次の処理が行われます。

ディスク スクラブ

ローカル ドライブのデータに対しては、アソシエーションが解除されるときに、次のいずれかが発生します。

- 有効になっている場合は、ローカル ドライブ上のすべてのデータが破棄されます。
- 無効になっている場合は、ローカル ドライブ上のすべてのデータが保持されます（ローカル ストレージ設定を含む）。

BIOS 設定スクラブ

BIOS 設定に対しては、スクラブ ポリシーを含むサービス プロファイルがサーバからアソシエーション解除されるときに、次のいずれかが発生します。

- 有効になっている場合は、サーバのすべての BIOS 設定が消去され、そのサーバ タイプとベンダーに応じた BIOS のデフォルトにリセットされます。
- 無効になっている場合は、サーバの既存の BIOS 設定が保持されます。

FlexFlash スクラブ

FlexFlash スクラブにより、新規またはデグレードしたSD カードの組み合わせ、FlexFlash メタデータの設定エラーの解決、4 パーティションの旧式 SD カードから単一パーティション SD カードへの移行を実行することができます。 スクラブ ポリシーを含むサービス プロファイルとサーバとの関連付けが解除されるとき、またはサーバが再認識されるときに、SD カードに対して次のいずれかが発生します。

- 有効になっている場合は、PNUOS フォーマット ユーティリティにより SD カードの HV パーティションがフォーマットされます。 SD カードが 2 枚ある場合、それらカードは RAID-1 ペアになっており、両方のカードの HV パーティションが有効と見なされます。 スロット 1 のカードはプライマリ、スロット 2 のカードはセカンダリと見なされます。

- 無効になっている場合は、既存の SD カード設定が保持されます。

（注）
- FlexFlash スクラブを行うと SD カードの HV パーティションが消去されるため、FlexFlash スクラブを実行する前に、ホスト オペレーティング システム用の適切なユーティリティを使用して SD カードの完全バックアップを行うことを推奨します。
- サービス プロファイルのメタデータ設定の不具合を解決するには、FlexFlash スクラブを実行する前に、ローカル ディスク設定ポリシーの FlexFlash を無効にして、サーバが再認識された後に FlexFlash を有効にする必要があります。
- ペアリングが完了したら、またはメタデータの不具合が解決したら、ただちにスクラブ ポリシーを無効にしてください。

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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

名前	説明
[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。

DIMM エラー管理の設定

DIMM の修正可能なエラー処理

Cisco UCS Manager では、DIMM が事前定義されたウィンドウにおいて修正可能な重大エラーに遭遇した場合、ステータスが Degraded と表され、機能しないデバイスと見なされます。

DIMM の修正可能なエラー処理機能により、サーバ内のすべての DIMM に関する修正可能および修正不可能なメモリ エラーをすべてリセットできます。エラー設定をリセットすると、当該DIMM

のエラー数はクリアされ、ステータスは操作可能に変わり、DIMM のセンサー状態がリセットされます。

メモリ エラーのリセット

Cisco UCS Manager とベースボード管理コントローラ（BMC）で発生したすべての修正可能および修正不可能なメモリ エラーをリセットするには、この手順を使用します。

手順

ステップ 1 [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 エラー設定をリセットするサーバをクリックします。
ステップ 4 [Work] ペインの [Inventory] タブをクリックします。
ステップ 5 [Memory] サブタブをクリックします。
ステップ 6 コンポーネントを右クリックし、[Reset Memory Errors] 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。

DIMM のブラックリスト化

Cisco UCS Manager で、デュアル インライン メモリ モジュール（DIMM）の状態は、SEL イベント レコードに基づいています。 BIOS が BIOS ポスト中のメモリ テスト実行時に修正不可能なメモリ エラーに遭遇した場合、DIMM は不良と判別されます。 不良と判別された DIMM は機能しないデバイスと見なされます。

DIMM のブラックリスト化を有効にすると、Cisco UCS Manager はメモリ テスト実行メッセージをモニタし、DIMM SPD データ内でメモリ エラーに遭遇した DIMM をブラックリストに載せます。 これにより、ホストは修正不可能な ECC エラーに遭遇した DIMM をマップから外すことができます。

DIMM のブラックリストのイネーブル化

メモリ ポリシーは、Cisco UCS ドメインの既存のサーバ、およびメモリ ポリシーを設定した後で追加されたサーバに適用できるグローバル ポリシーです。

（注）
- このグローバル ポリシーをサービス プロファイルに追加することはできません。
- Cisco UCS B シリーズ M1 ブレード サーバはこの機能をサポートしません。
- Cisco UCS C シリーズ ラック サーバへのサポートは今後のリリースで可能になる予定です。

はじめる前に

- サーバのファームウェアはリリース 2.2(1) 以降である必要があります。
- 次の権限のいずれかでログインする必要があります。
  - Admin
  - サーバ ポリシー
  - サーバ プロファイルのサーバ ポリシー

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 ブラックリストをイネーブルにする組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Memory Policy] を展開して [default] を選択します。

ステップ 5 [Blacklisting] 領域で、[enabled] オプション ボタンをクリックします。

DIMMのブラックリストは、ドメイン レベル ポリシーでイネーブルにされ、これらの変更は、その特定のドメイン内のすべてのサーバに適用されます。

（注） サーバの CIMC が DIMM のブラックリストをサポートしない場合、info レベルの障害が生成されます。

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。

Creating a Serial over LAN Policy

手順

ステップ 1 On the menu bar, click Servers.

ステップ 2 In the **Navigation** Pane, expand Servers > Policies > root.
If you want to create or access a policy in a sub-organization, expand Sub-Organizations > *Organization_Name*.

ステップ 3 Right-click Serial over LAN Policies and choose Create Serial over LAN Policy.

ステップ 4 In the Create Serial over LAN Policy dialog box, enter the Name and optional description, choose the Serial over LAN State, and choose a Speed from the drop-down list.

ステップ 5 Click OK.

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 では、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. 必要な資格を満たしている場合、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と関連付けられます。 そのサービス プロファイルの名前は、Cisco UCS Manager によって付与されるサーバの名前に基づきます。
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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[認定] ドロップダウン リスト	この自動設定ポリシーに関連付けられているサーバプールポリシー資格情報。 サーバプールポリシー資格情報で指定された基準に合致する新しいサーバが検出されると、Cisco UCS は、[policy template][サービスプロファイルのテンプレート名] ドロップダウン リスト フィールドで選択されたサービスプロファイルテンプレートに基づいて、自動的にサービス プロファイルを作成し、それをサーバに関連付けます。
[ORG] ドロップダウン リスト	この自動構成ポリシーに関連付けられた組織。 Cisco UCS が自動的にサービス プロファイルを作成してサーバに関連付ける場合、サービスプロファイルはこのフィールドで選択された組織に配置されます。
[サービスプロファイルのテンプレート名] 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を満たしている場合、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 [説明] 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、自動的に新しいサーバの検出を試みます。
- [User Acknowledged]：Cisco UCS Manager は、新しいサーバの検索が指示されるまで待機します。

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、[認定] 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 ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

サーバ 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、サーバ用のサービス プロファイルを作成するために、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サービスプロファイルはすべて、製造元でブレードに設定された値を使用します。 このポリシーは次の機能を実行します。

- サーバ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 を使って、このサーバのサービス プロファイルを作成

このポリシーを使って作成したサービス プロファイルは他のサーバに移行できません。

サーバ継承ポリシーの作成

VIC アダプタが搭載されたブレード サーバまたはラックマウント サーバ（Cisco UCS M81KR 仮想インターフェイスカードなど）、サーバのアイデンティティ値が製造時にサーバハードウェアに書き込まれていません。 その結果、アダプタのアイデンティティは、デフォルトプールから取得する必要があります。 デフォルトプールに、サーバに割り当てるのに十分なエントリが格納されていない場合、サービス プロファイルの関連付けが設定エラーで失敗します。

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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[認定] 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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Target Pool] ドロップダウン リスト	このポリシーをサーバプールに関連付ける場合は、ドロップダウン リストから該当のプールを選択します。
[認定] 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する必要があります。

- 自動構成ポリシー

- シャーシ ディスカバリ ポリシー
- サーバ 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 が一致する必要のある正規表現。
[Maximum Capacity] フィールド	選択されたタイプの最大容量 容量を指定するには、[Select] を選択し、必要な最大容量を入力します。 1 ～ 65535 の整数を入力できます。

c) [OK] をクリックします。

ステップ 7 （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 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 領域で次のフィールドに値を入力して、使用するシャーシの範囲を指定します。

- [First Chassis ID] フィールド—このポリシーに関連付けられたサーバ プールが使用できる最初のシャーシ ID。
- [Number of Chassis] フィールド—プールに含めるシャーシの合計数（[First Chassis ID] フィールドで指定されたシャーシから始まります）。

c) テーブルで、[Add] をクリックします。
d) [Create Server Qualifications] ダイアログボックスで次のフィールドに値を入力して、使用する範囲のサーバの範囲を指定します。

- [First Slot ID] フィールド—このポリシーに関連付けられているサーバ プールから取得できる最初のスロット ID。
- [Number of Slots] フィールド—このポリシーに関連付けられているサーバ プールから取得できるスロットの合計数。

e) [Finish Stage] をクリックします。
f) 別のスロットの範囲を追加するには、[Add] をクリックし、ステップ d および e を繰り返します。
g) スロット範囲の指定を終了したら、[Finish] をクリックします。

ステップ 9 （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）。
[Min Cap] フィールド	最小限必要なメモリ容量（MB 単位）。
[Max Cap] フィールド	メモリの許容最大容量（MB 単位）。
[Width] フィールド	データ バスの最小幅。
[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、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。
[Max Number of Cores] フィールド	CPU コアの許容最大数。 容量を指定するには、[select] を選択し、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。
[Min Number of Threads] フィールド	最小限必要な CPU スレッドの数。 容量を指定するには、[select] を選択し、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。

名前	説明
[Max Number of Threads] フィールド	CPU スレッドの許容最大数。 容量を指定するには、[select] を選択し、関連するテキスト フィールドに 1 ～ 65535 の整数を入力します。
[CPU Speed] フィールド	最小限必要な CPU 速度。 容量を指定するには、[select] を選択し、CPU の最小速度を入力します。
[CPU Stepping] フィールド	最小限必要な CPU バージョン。 容量を指定するには、[select] を選択し、CPU の最大速度を入力します。

c) [OK] をクリックします。

ステップ 11 （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をディスクレスにする必要があるかどうか。 次のいずれかになります。 • [Unspecified]：どのストレージ タイプも受け入れ可能です。 • [Yes]：ストレージをディスクレスにする必要があります。 • [No]：ストレージをディスクレスにできません。
[Number of Blocks] フィールド	最小限必要なブロック数。 容量を指定するには、[select] を選択し、ブロックの数を入力します。
[Block Size] フィールド	最小限必要なブロック サイズ（バイト単位）。 容量を指定するには、[select] を選択し、ブロックのサイズを入力します。

名前	説明
[Min Cap] フィールド	サーバ内のすべてのディスクの最小ストレージ容量（MB 単位）。 容量を指定するには、[select] を選択し、ストレージの最小容量を入力します。
[Max Cap] フィールド	ストレージの許容最大容量（メガバイト単位）。 容量を指定するには、[select] を選択し、ストレージの最大容量を入力します。
[Per Disk Cap] フィールド	最小限必要なディスクあたりのストレージ容量（ギガバイト単位）。 容量を指定するには、[select] を選択し、各ディスクの最小容量を入力します。
[Units] フィールド	ユニット数。 容量を指定するには、[select] を選択し、必要なユニットを入力します。
[Number of Flex Flash Cards] フィールド	FlexFlash カードの数。 容量を指定するには、[select] を選択し、必要なユニットを入力します。

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、電源グループに基づいたサーバの資格認定を実行するには、次の手順を実行します。

a) [Create Group Power Qualifications] をクリックします。
b) [Create Group Power Qualifications] ダイアログボックスで、[Power Group] ドロップダウン リストから電源グループを選択します。
c) [OK] をクリックします。

ステップ 14 （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 Storage Qualifications] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[First Slot ID] フィールド	このポリシーに関連付けられているサーバプールが取得に使用できる最初のラックマウント サーバ スロット ID。
[Number of Slots] フィールド	このポリシーに関連付けられているサーバプールが取得に使用できるラックマウント サーバ スロットの合計数。

ステップ 15 テーブル内の資格を確認し、必要に応じて修正します。

ステップ 16 [OK] をクリックします。

サーバ プール ポリシーの資格情報の削除

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、以下を決定するために使用されます。

- 仮想ネットワーク インターフェイス接続（vCon）をサーバ上の物理アダプタにマッピングする方法。
- 各 vCon に割り当てることができる vNIC または vHBA のタイプ。

各 vNIC/vHBA 配置ポリシーには、物理アダプタの仮想表現である 4 つの vCon が含まれています。 vNIC/vHBA 配置ポリシーがサービス プロファイルに割り当てられ、サービス プロファイルがサーバに関連付けられると、vNIC/vHBA配置ポリシーのvConが物理アダプタに割り当てられ、vNIC と vHBA がそれらの vCon に割り当てられます。

1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、サーバのタイプと選択された仮想スロット マッピング スキーム（[Round Robin] または [Linear Ordered]）に基づいて vCon を割り当てます。 使用可能なマッピング スキームの詳細については、vCon のアダプタへの配置, （438 ページ） を参照してください。

Cisco UCS は、vCon の割り当て後、vNIC と vHBA を各 vCon の選択プリファレンスに基づいて割り当てます。これは次のいずれかになります。

- [すべて]：設定されたすべての vNIC と vHBA が vCon に割り当てられます。明示的な割り当て、割り当て解除、動的のいずれかとなります。 これがデフォルトです。

- [割り当てのみ]：vNICs 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 プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。
- [動的を除く]：動的な vNIC や vHBA を vCon に割り当てることはできません。 vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- [割り当て解除を除く]：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。 vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。
- [Exclude usNIC]：Cisco usNICs を vCon に割り当てることができません。 vCon は他のすべての設定された vNIC と vHBA で使用できます。それらが明示的に vCon に割り当てられているか、未割り当てか、動的であるかについては問いません。

（注） [Exclude usNIC] に設定された vCon に明示的に割り当てられている SRIOV usNIC は割り当てられたままになります。

vNIC/vHBA 配置ポリシーをサービス プロファイルに含めない場合、Cisco UCS Manager はデフォルトで、vCon マッピング スキームを [Round Robi]、vNIC/vHBA 選択プリファレンスを [All] に設定し、各アダプタの機能と相対的な処理能力に基づいて vNIC と vHBA をアダプタに配分します。

vCon のアダプタへの配置

Cisco UCS は、サービス プロファイル内のすべての vCon をサーバ上の物理アダプタにマッピングします。 マッピングの実行方法、およびサーバ内の特定のアダプタへの vCon の割り当て方法は、次の条件によって決まります。

- サーバのタイプ。 2 つのアダプタ カードを搭載した N20-B6620-2 および N20-B6625-2 ブレード サーバは、他のサポートされるラック サーバまたはブレード 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の数。
- vNIC/vHBA 配置ポリシー内の仮想スロット マッピング スキームの設定（該当する場合）。

vNIC および vHBA を vCon に割り当てるための vNIC/vHBA 選択環境設定を設定するときは、この配置を検討する必要があります。

（注） vCon のアダプタへの配置は、アダプタの PCIE スロット番号とは関係ありません。 vCon の配置のために使用されるアダプタ番号は、アダプタの PCIE スロット番号ではなく、サーバ検出中にそれらに割り当てられる ID です。

N20-B6620-2 および N20-B6625-2 ブレード サーバでの vCon のアダプタへの配置

N20-B6620-2 および N20-B6625-2 ブレード サーバの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。 これらのブレード サーバの 1 台が 1 つのアダプタを持つ場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 サーバが 2 つのアダプタを持つ場合は、vCon の割り当ては仮想スロット マッピング スキームに基づいて行われます。

- ラウンド ロビン：Cisco UCS が vCon2 と vCon4 をアダプタ 1 に、vCon1 と vCon3 をアダプタ 2 に割り当てます。 これがデフォルトです。
- 線形順序：Cisco UCS が vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。

vCon のアダプタへの配置（他のすべてのサポート対象サーバの場合）

N20-B6620-2 と N20-B6625-2 ブレード サーバに加え、Cisco UCS でサポートされるその他すべてのサーバにおいて、vCon の割り当ては、サーバ内のアダプタの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 サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、選択された仮想スロット マッピング スキーム（「ラウンドロビン」または「線形順序」）に基づいて vCon を割り当てます。

表 *6*：ラウンドロビン マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ 1	アダプタ 1	アダプタ 1	アダプタ 1
2	アダプタ 1	アダプタ 2	アダプタ 1	アダプタ 2
3	アダプタ 1	アダプタ 2	アダプタ 3	アダプタ 2
4	アダプタ 1	アダプタ 2	アダプタ 3	アダプタ 4

ラウンドロビンはデフォルトのマッピング スキームです。

表 *7*：線形順序マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ 1	アダプタ 1	アダプタ 1	アダプタ 1

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
2	アダプタ1	アダプタ1	アダプタ2	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ3
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

（注） Cisco UCS B440 M2 ブレード サーバ内の 2 つのアダプタで vCon ポリシーを使用している場合は、次のマッピングに注意してください。

- 最初に vCon 2 からアダプタ 1 へのマッピング
- 2 番目に vCon 1 からアダプタ 2 へのマッピング

vCon への vNIC/vHBA の割り当て

Cisco UCS Manager には、vNIC/vHBA 配置ポリシーによって vCon に vNIC および vHBA を割り当てる 2 種類のオプション（明示的割り当てと暗黙的割り当て）があります。

vNIC および vHBA の明示的割り当て

明示的割り当てでは、vCon を指定してから、vNIC または vHBA を割り当てるアダプタを指定します。 この割り当てオプションは、サーバ上のアダプタに vNIC および vHBA を配布する方法を決める必要がある場合に使用します。

明示的割り当ての場合、vCon および関連付ける vNIC と vHBA を設定するには、次の手順を実行します。

- vCon 設定を任意の使用可能なオプションに設定します。 vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。 vCon で [All] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。
- vNIC および vHBA を vCon に割り当てます。 この割り当ては、vNIC または vHBA の仮想ホストインターフェイス配置プロパティを使用して行うか、サーバに関連付けられているサービス プロファイルで設定できます

vNIC や vHBA をそれらのタイプ用に設定されていない vCon に割り当てようとすると、Cisco UCS Manager によって、設定エラーを示すメッセージ表示されます。

サービス プロファイルの関連付け中、Cisco UCS Manager は、ポリシーの設定に従って vNIC および vHBA を割り当てる前に、設定された vNIC および vHBA の配置をサーバ内の物理アダプタの

数および機能と比較して検証します。 負荷分散は、このポリシーで設定された vCon およびアダプタへの明示的な割り当てに基づいて実行されます。

1 つ以上の vNIC または vHBA の割り当てがアダプタでサポートされない場合、Cisco UCS Manager はサービス プロファイルに対してエラーを発生させます。

vNIC および vHBA の暗黙的割り当て

暗黙的割り当てでは、Cisco UCS Manager は vCon を決定した後で、アダプタの機能とそれらの相対的な処理能力に基づいて vNIC または vHBA を割り当てるアダプタを決定します。 この割り当てオプションは、vNIC または vHBA を割り当てるアダプタがシステム設定において重要ではない場合に使用します。

暗黙的割り当ての場合に vCon を設定するには、次の手順を実行します。

- vCon 設定を [All]、[Exclude Dynamic]、または [Exclude Unassigned] に設定します。 vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。
- vCon 設定を [Assigned Only] にしないでください。 この設定を使用して暗黙的割り当てを実行することはできません。
- vNIC または vHBA を vCon に割り当てないでください。

サービス プロファイルの関連付け中、Cisco UCS Manager は、サーバ内の物理アダプタの数および機能を検証し、それに従って vNIC および vHBA を割り当てます。 負荷分散はアダプタの機能に基づいて実行され、vNIC および vHBA の配置は、システムで決定された実際の順序に従って実行されます。 たとえば、あるアダプタが他のアダプタよりも多くの vNIC を処理できる場合、そのアダプタにはより多くの vNIC が割り当てられます。

アダプタがそのサーバに対して設定された vNIC と 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 アダプタ環境での vNIC の暗黙的割り当て

各スロットにアダプタ カードを搭載したデュアル スロット サーバで暗黙的な vNIC 割り当てを使用する場合、Cisco UCS Manager は通常、次のように vNIC/vHBA を割り当てます。

- サーバの両方のスロットに同じアダプタがある場合、Cisco UCS Manager は、各アダプタに vNIC と vHBA を半分ずつ割り当てます。
- サーバに 1 つの非 VIC アダプタと 1 つの VIC アダプタがある場合、Cisco UCS Manager は、2 つの vNIC と 2 つの vHBA を非 VIC アダプタに割り当て、残りの vNIC と vHBA を VIC アダプタに割り当てます。
- サーバに 2 つの異なる VIC アダプタがある場合、Cisco UCS Manager は、2 つのアダプタの相対的な処理能力に基づいて、vNIC と vHBA を比例的に割り当てます。

次の例は、サポートされるアダプタ カードのさまざまな組み合わせに対して、Cisco UCS Manager が vNIC と vHBA を割り当てる一般的な方法を示しています。

- 4 つの vNIC と、2 つの Cisco UCS M51KR-B Broadcom BCM57711アダプタ（それぞれに 2 つの vNIC）を搭載したサーバを設定する場合、Cisco UCS Manager は 2 つの vNIC を各アダプタに割り当てます。
- 50 の vNIC と、Cisco UCS CNA M72KR-Eアダプタ（2 つの vNIC）および Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）を搭載したサーバを設定する場合、Cisco UCS Manager は、2 つの vNIC を Cisco UCS CNA M72KR-Eアダプタに割り当て、48 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当てます。
- 150 の vNIC と、Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）および Cisco UCS VIC-1240 仮想インターフェイス カードアダプタ（256 の vNIC）を搭載したサーバを設定する場合、Cisco UCS Manager は、50 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当て、100 の vNIC を Cisco UCS VIC-1240 仮想インターフェイス カードアダプタに割り当てます。

（注） vNIC をファブリック フェールオーバー用に設定し、ダイナミック vNIC をサーバ用に設定した場合に、この暗黙的な割り当てに対する例外が発生します。

1 つのアダプタが vNIC フェールオーバーをサポートしない環境で vNIC ファブリック フェールオーバーを含む設定を行った場合、Cisco UCS Manager は、ファブリック フェールオーバーが有効になっているすべての vNIC を、それらをサポートしているアダプタに暗黙的に割り当てます。ファブリック フェールオーバー用に設定された vNIC のみが設定に含まれている場合、それらをサポートしてないアダプタには vNIC が暗黙的に割り当てられません。 一部の vNIC がファブリック フェールオーバー用に設定され、一部の vNIC がそうでない場合、Cisco UCS Manager は、上記の比率に従って、すべてのフェールオーバー vNIC をそれらをサポートしているアダプタに割り当て、少なくとも 1 つの非フェールオーバー vNIC をそれらをサポートしていないアダプタに割り当てます。

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

名前	説明
[仮想スロットマッピングスキーム] フィールド	

名前	説明
	Cisco UCS は、サーバの PCIe アダプタ カードに、仮想ネットワーク インターフェイス接続（vCon）を割り当てます。 各 vCon は、vNICs や vHBA に割り当て可能な物理アダプタとして仮想表示されます。 1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。 2 つまたは 3 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS が選択された仮想スロット マッピング スキームに基づいて、vCon を割り当てます。 次のいずれかになります。 • ラウンドロビン：2 つのアダプタ カードを持つサーバの場合は、Cisco UCS が vCon1 と vCon3 をアダプタ 1 に、vCon2 と vCon4 をアダプタ 2 に割り当てます。 3 つのアダプタ カードを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 と vCon4 をアダプタ 2 に、vCon3 をアダプタ 3 に割り当てます。 これがデフォルトのスキームです。 • 線形順序：Cisco UCS が vCon1 と vCon2 をアダプタ 1 に、vCon3 と vCon4 をアダプタ 2 に割り当てます。 3 つのアダプタ カードを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に割り当て、 vCon3 と vCon4 をアダプタ 3 に割り当てます。 （注） N20-B6620-2 および N20-B6625-2 ブレード サーバの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。 これらのブレード サーバの 1 台が 1 つのアダプタを持つ場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。 サーバが 2 つのアダプタを持つ場合は、vCon の割り当ては仮想スロット マッピング スキームに基づいて行われます。 • ラウンドロビン：Cisco UCS が vCon2 と vCon4 をアダプタ 1 に、vCon1 と vCon3 をアダプタ 2 に割り当てます。 これがデフォルトです。 • 線形順序：Cisco UCS が vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り

名前	説明
	当てます。 Cisco UCS は、vCon の割り当て後、vNIC と vHBA を各 vCon の選択プリファレンスに基づいて割り当てます。

b) 各 [Virtual Slot] の [Selection Preference][選択プリファレンス] カラムカラムで、ドロップダウンリストから次のいずれかを選択します。

- [すべて]：設定されたすべての vNIC と vHBA が vCon に割り当てられます。明示的な割り当て、割り当て解除、動的のいずれかとなります。 これがデフォルトです。
- [割り当てのみ]：vNICs 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 プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。
- [動的を除く]：動的な vNIC や vHBA を vCon に割り当てることはできません。 vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- [割り当て解除を除く]：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。 vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。
- [Exclude usNIC]：Cisco usNICs を vCon に割り当てることができません。 vCon は他のすべての設定された vNIC と vHBA で使用できます。それらが明示的に vCon に割り当てられているか、未割り当てか、動的であるかについては問いません。

  （注） [Exclude usNIC] に設定された vCon に明示的に割り当てられている SRIOV usNIC は割り当てられたままになります。

c) [OK] をクリックします。

vNIC/vHBA 配置ポリシーの削除

手順

ステップ 1 [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 の明示的割り当て

はじめる前に

vNIC/vHBA 配置ポリシーまたはサービス プロファイルで次のいずれかの値を使用して、vCon を設定します。

- Assigned Only
- Exclude Dynamic
- Exclude Unassigned

vCon で [All] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。 しかし、この設定ではほとんど制御ができません。

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 vNIC を、明示的に vCon に割り当てるサービス プロファイルを含む組織のノードを展開します。システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 [Service_Profile_Name] > [vNICs] の順に展開します。

ステップ 5 明示的に vCon に割り当てる vNIC をクリックします。

ステップ 6 [Work] ペインの [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、次のフィールドに入力します。

名前	説明
[Desired Placement] ドロップダウン リスト	vNIC 用のユーザ指定仮想ネットワーク インターフェイス（vCon）配置。 次のいずれかになります。 • [Any]：Cisco UCS Manager が、vNIC を割り当てる vCon を決定できるようにします。 • [1]：vNIC を vCon1 に明示的に割り当てます。 • [2]：vNIC を vCon2 に明示的に割り当てます。 • [3]：vNIC を vCon3 に明示的に割り当てます。 • [4]：vNIC を vCon4 に明示的に割り当てます。
[Actual Assignment] フィールド	サーバの vNIC の実際の vCon 割り当て。

vNIC をその vNIC タイプ用に設定されていない vCon に割り当てようとすると、Cisco UCS Manager は設定エラーを知らせるメッセージボックスを表示します。 別の vCon に vNIC を割り当てるか、サービス プロファイルの vCon 設定を変更する必要があります。

ステップ 8 [Order] セクションで、次のフィールドに入力します。

名前	説明
[Desired Order] フィールド	vNIC のユーザ指定の PCI 順序。 0 ～ 128 の範囲の整数を入力します。 サーバには 128 を超える vNIC を作成できません。
[Actual Order] フィールド	サーバの vNIC の実際の PCI 順序。

ステップ 9 [Save Changes] をクリックします。

vCon への vHBA の明示的割り当て

はじめる前に

vNIC/vHBA 配置ポリシーまたはサービス プロファイルで次のいずれかの値を使用して、vCon を設定します。

- Assigned Only
- Exclude Dynamic
- Exclude Unassigned

vCon で [All] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。 しかし、この設定ではほとんど制御ができません。

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 vHBA を明示的に vCon に割り当てるサービス プロファイルを含む組織のノードを展開します。 システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

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

ステップ 5 明示的に vCon に割り当てる vHBA をクリックします。

ステップ 6 [Work] ペインの [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、次のフィールドに入力します。

名前	説明
[Desired Placement] フィールド	vHBA 用のユーザ指定仮想ネットワーク インターフェイス（vCon）配置。 次のいずれかになります。 • [Any]：Cisco UCS Manager が、vHBA を割り当てる vCon を決定できるようにします。 • [1]：vHBA を vCon1 に明示的に割り当てます。 • [2]：vHBA を vCon2 に明示的に割り当てます。 • [3]：vHBA を vCon3 に明示的に割り当てます。 • [4]：vHBA を vCon4 に明示的に割り当てます。
[Actual Assignment] フィールド	サーバの vHBA の実際の vCon 割り当て。

vHBA をその vHBA タイプ用に設定されていない vCon に割り当てようとすると、Cisco UCS Manager は設定エラーを知らせるメッセージ ボックスを表示します。 別の vCon に vHBA を割り当てるか、サービス プロファイルの vCon 設定を変更する必要があります。

ステップ 8 [Order] セクションで、次のフィールドに入力します。

名前	説明
[Desired Order] フィールド	vHBA のユーザ指定の PCI 順序。 0 ～ 128 の範囲の整数を入力します。 サーバには 128 を超える vHBA を作成できません。
[Actual Order] フィールド	サーバの vHBA の実際の PCI 順序。

ステップ 9 [Save Changes] をクリックします。

ダイナミック vNIC の前にスタティック vNIC を配置

最適なパフォーマンスを得るために、スタティック vNIC とスタティック vHBA は、PCIe バス上のダイナミック vNIC の前に配置する必要があります。 スタティック vNIC とは、スタティック vNIC と vHBA の両方を指します。 Cisco UCS Manager リリース 2.1 は、スタティックおよびダイナミック vNIC の順序に関する次の機能を備えています。

- Cisco UCS Manager リリース 2.1 にアップグレードした後、既存のサービス プロファイル（Cisco UCS Manager リリース 2.1 以前のリリースで定義されたプロファイル）に変更がない場合は、vNIC の順序は変更されません。
- Cisco UCS Manager リリース 2.1 へのアップグレード後、vNIC 関連の変更によって vNIC マップの順序が変更される場合があります。 その場合、結果としてすべてのダイナミック vNIC がスタティック vNIC の後に配置されます。
- Cisco UCS Manager リリース 2.1 で新しく作成されたサービス プロファイルでは、スタティック vNIC が常にダイナミック vNIC の前に順序付けられます。
- 上記の動作は、スタティック vNIC またはダイナミック vNIC の作成または削除の順番に依存しません。
- SRIOV 対応のサービス プロファイルの場合は、UCSM によって対応する仮想関数（VF）の前に vNIC 物理関数（PF）が挿入されます。 この方式では、VF が PCIe バスおよび BDF 上の親 PF vNIC の近くに配置され、VF の継続的な増分順序になることが保証されます。

例

Cisco UCS Manager リリース 2.0 での当初のデバイス順序

```
dyn-vNIC-1 1
dyn-vNIC-2 2
```

Cisco UCS Manager リリース 2.0 での新たなデバイス順序（2 つのスタティック vNIC を追加）

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

Cisco UCS Manager リリース 2.1 へのアップグレード後（vNIC 関連の変更がサービス プロファイルで行われる前）

```
dyn-vNIC-1 1
dyn-vNIC-2 2
eth-vNIC-1 3
eth-vNIC-2 4
```

Cisco UCS Manager リリース 2.1 での新たなデバイス順序（ポリシー数を 2 から 4 に変更することによって 2 つのダイナミック vNIC を追加）

```
dyn-vNIC-1 3
dyn-vNIC-2 4
eth-vNIC-1 1
eth-vNIC-2 2
dyn-vNIC-3 5
dyn-vNIC-4 6
```

多機能 PCIe デバイスとしてのダイナミック vNIC

Cisco UCS Manager バージョン 2.1 は、0 機能デバイス（すべてのスタティック vNIC に対応する新しい BUS）としてスタティック vNIC をプロビジョニングします。 多機能ダイナミック vNIC は、新しいバス スロットから最後のスタティック vNIC/vHBA の後に配置されます。

（注） Cisco UCS Manager バージョン 2.1 は、新しい StaticZero モードをサポートしています。

表 *8*：バージョンの互換性

Cisco UCS Manager		
バージョン 1.4 **方式：ZeroFunction**	**Version 2.0** **方式：ZeroFunction/MultiFunction**	**バージョン 2.1** **方式：** **ZeroFunction/MultiFunction/StaticZero**
スタティックおよびダイナミック vNIC はすべて、バス [0-57]、関数 [0] 上にあります。 < ZeroFunction モード >	スタティック vNIC およびダイナミック vNIC は、バス [0-57]、関数 [0-7] 上にあります バス 0、関数 0 バス 0、関数 7 バス 1、関数 0 < MultiFunction モード >	スタティック vNIC または PF は、バス [0-57]、関数 [0] 上にあります。 SRIOV：対応する VF が同一バスおよび関数 [1-255] 上にあります。 No-SRIOV：ダイナミック vNIC は、バス [0-57]、関数 [0-7] 上にあります。 < StaticZero モード>
	Balboa からのアップグレードでは、バスが <= 57 になるまで BDF の番号の付け直しは行われません（ZeroFunction モードのまま）。 デバイスが 58 台を超えると、MultiFunction モードに切り替わります。	Balboa からのアップグレードでは、バスが <= 57 になるまで BDF の番号の付け直しは行われません（ZeroFunction モードのまま）。 デバイスが 58 台またはプラットフォーム固有の最大 PCIe バス数を超えるか、SRIOV 設定に変更されると、StaticZero モードに切り替わります。

Cisco UCS Manager		
バージョン 1.4 方式：ZeroFunction	Version 2.0 方式：ZeroFunction/MultiFunction	バージョン 2.1 方式： ZeroFunction/MultiFunction/StaticZero
		Cisco UCS Manager バージョン 2.0 からのアップグレードでは、BDF の番号の付け直しは行われません（ZeroFunction/MultiFunction モードのまま）。 デバイスが 58 台またはプラットフォーム固有の最大 PCIe バス数を超えるか、SRIOV 設定に変更されると、StaticZero モードに切り替わります。

CIMC マウント vMedia

スクリプト可能な vMedia の使用

Cisco UCS Manager では、リモート UCS サーバの vMedia デバイス ISO イメージをプロビジョニングできます。 スクリプト可能な vMedia を使用して、リモート サーバに IMG または ISO イメージをマウントするようにプログラミングできます。 CIMC マウント vMedia を使用すると、メディア接続を追加することなく、データセンター内の他のマウント メディア間で通信できるようになります。 スクリプト可能な vMedia を使用すると、ブラウザを使用せずに仮想メディア デバイスを制御して、手動で各 UCS サーバを個別にマッピングできます。

スクリプト可能な vMedia は、NFS、CIFS、HTTP、および HTTPS の共有など、複数の共有タイプをサポートします。 **スクリプト可能な vMedia** は BIOS 設定によって有効になり、Web GUI および CLI インターフェイスを介して設定されます。

Cisco UCS Manager のスクリプト可能な vMedia は次の機能をサポートしています。

- 特定の vMedia デバイスからのブート
- マウントされた共有からローカル ディスクへのファイルのコピー
- OS ドライバのインストールおよび更新

（注） Cisco UCS Manager によるスクリプト可能な vMedia のサポートは、CIMC にマッピングされているデバイスにのみ適用されます。 既存の KVM ベースの vMedia デバイスはサポートされません。

vMedia ポリシーの作成

リモートの vMedia デバイスのマッピング情報を設定するために、vMedia ポリシーが使用されます。 vMedia ポリシー内で 2 つの vMedia デバイスと、CD および HDD に対するマッピングが使用できます。 同時に、1 つの ISO と 1 つの IMG を設定できます。 ISO 構成は CD ドライブに、IMG 構成は HDD デバイスにマッピングします。

（注） デバイスをリモート フォルダにマッピングする場合、IMG を作成し、HDD デバイスとしてマッピングします。

はじめる前に

次にアクセスできることを確認します。

- リモート vMedia サーバ
- vMedia デバイス

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 [vMedia Policies] ポリシーを右クリックし、[Create vMedia Policy] を選択します。

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

名前	説明
名前	vMedia ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
説明	ポリシーの説明。 ポリシーを使用すべき場所や条件についての情報を含めることを推奨します。

名前	説明
Retry on Mount Failure	障害の発生時にvMediaがマウントを続行するかどうかを指定します。 ここに表示される値は次のとおりです。 • Yes • No （注） デフォルト設定は、[Yes] です。 [Yes] を選択すると、マウントに成功するか、このオプションが無効化されるまで、リモートサーバはvMediaマウントプロセスのマウントを試行し続けます。 [No] を選択すると、警告メッセージが表示され、マウントが失敗した場合にはリトライが機能しないことが示されます。

ステップ 6 テーブルの右側のアイコン バーの [+] をクリックします。

ステップ 7 [Create vMedia Mount] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
名前	vMedia マウント ポリシーの名前。
Device Type	マウントするリモート vMedia のタイプ。 ここに表示される値は次のとおりです。 • [CDD]：スクリプト可能 vMedia CD。 • [HDD]：スクリプト可能 vMedia HDD。
プロトコル	リモート サーバとの通信時に使用するプロトコル。 次のオプション ボタンのいずれかをクリックして、マウントされたリモートサーバとの通信に使用するプロトコルを指定します。 ここに表示される値は次のとおりです。 • [NFS]：Network Files System。 • [CIFS]：Common Internet File System。 • [HTTP]：Hypertext Transfer Protocol。 • [HTTPS]：Hypertext Transfer Protocol over Secure。

名前	説明
[Hostname/IPAddress]	バックアップ ファイルを格納する場所の IP アドレスまたはホスト名を入力します。 これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。 ホスト名を使用する場合は、DNS サーバを使用するように Cisco UCS Manager を設定する必要があります。 [Inband] ネットワークがそのサーバに設定されている場合、ホスト名（DNS）を使用できます。
[Remote File]	バックアップ コンフィギュレーション ファイルのフル パスを入力します。 このフィールドにはファイル名（ファイル拡張子付き）だけを含めることができます。
Remote Path	リモートの vMedia コンフィギュレーション ファイルのフル パスを入力します。
[Username]	Cisco UCS Manager がリモート サーバへのログインに使用するユーザ名を入力します。 プロトコルが NFS の場合、このフィールドは適用されません。プロトコルが HTTP の場合、このフィールドの選択は任意です。
パスワード	ユーザ名に関連付けるパスワードを入力します。 プロトコルが NFS の場合、このフィールドは適用されません。プロトコルが HTTP の場合、このフィールドの選択は任意です。

ステップ 8 [OK] をクリックします。
リモート サーバの詳細は、[Create vMedia Mount] ダイアログ ボックスの [vMedia Mounts] 領域に一覧表示されます。

次の作業

vMedia ブート ポリシーを作成します。

サービス プロファイルへの vMedia ポリシーの追加

Scriptable vMedia を使用する前に、vMedia および Boot ポリシーをサービス プロファイルに追加する必要があります。 vMedia ポリシーとブート ポリシーがサービス プロファイルに追加された後、

そのサービスプロファイルをCisco UCSサーバに関連付けることができます。 次の手順に、vMediaポリシーをサービス プロファイルに追加する方法を示します。

はじめる前に

サービス プロファイルに追加する vMedia ポリシーを設定します。

手順

ステップ 1 [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。
[Unified Computing System Manager] ペインが表示されます。

ステップ 5 [Name] フィールドに、サービス プロファイルの識別に使用できる一意の名前を入力します。
この名前には、2 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービスプロファイルおよびサービスプロファイル テンプレートで一意であることが必要です。

この名前は、サービス プロファイルを作成する組織またはサブ組織内で一意である必要があります。

ステップ 6 [UUID Assignment] ドロップダウン リストで、次のいずれかの手順を実行します。

オプション	説明
Select (pool default used by default)	デフォルトの UUID 接尾辞プールから UUID を割り当てます。 ステップ 8 に進みます。
	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUIDはサービスプロファイルがサーバと関連付けられるまで割り当てられません。 この時点で、UUID は製造元によってサーバに割り当てられたUUID値に設定されます。 サービスプロファイルを後で別のサーバに移動すると、UUIDは新しいサーバに一致するように変更されます。 ステップ 8 に進みます。
	手動で割り当てる UUID を使用します。 ステップ 7 に進みます。

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 8 に進みます。

ステップ 7 （任意） オプションを選択した場合は、次の手順を実行します。

a) [UUID] フィールドに、このサービス プロファイルを使用するサーバに割り当てる有効な UUID を入力します。

b) 選択した UUID が使用可能であることを確認するには、[here] リンクをクリックします。

ステップ 8 （任意） このサービス プロファイルで使用する新しい UUID 接尾辞プールを作成する場合は、[Create UUID Suffix Pool] をクリックし、[Create UUID Suffix Pool] ウィザードのフィールドに値を入力します。
詳細については、UUID 接尾辞プールの作成, （344 ページ）を参照してください。

ステップ 9 （任意） テキスト ボックスに、このサービス プロファイルの説明を入力します。
このサービス プロファイルのユーザ定義による説明。

256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 10 [Next] クリックします。

ステップ 11 [vMedia] ドロップダウン リストから、次のいずれかを選択します。

オプション	説明
使用する vMedia ポリシーを選択します	このサービス プロファイルに vMedia ポリシーを割り当てられるようにします。 ステップ 12 に進みます。
特定の vMedia ポリシーを作成します。	このサービス プロファイル テンプレートだけがアクセスできるローカル vMedia ポリシーを作成できます。

オプション	説明
[vMedia Policies] [*Policy_Name*]	サービス プロファイルに既存の vMedia ポリシーを割り当てます。このオプションを選択した場合、Cisco UCS Manager でポリシーの詳細が表示されます。 既存のポリシーを使用するのではなく、すべてのサービス プロファイルがアクセスできるポリシーを作成する場合は、[Create vMedia Policy] をクリックします。 それ以外の場合は、リストでポリシーを選択し、ステップ 13 に進みます。

ステップ 12 すべてのサービス プロファイルおよびテンプレートがアクセスできる新しい vMedia ポリシーを作成した場合は、[vMedia] をドロップ ダウン リストから選択します。

ステップ 13 [Next] をクリックします。

CIMC vMedia ポリシーの表示

はじめる前に

vMedia ポリシーを設定しておきます。

手順

ステップ 1 [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、[Policies] > [vMedia Policies] の順に展開します。

ステップ 3 [vMedia Policies] ノードを展開して、[vMedia Policies] のリストを表示します。

ステップ 4 vMedia ポリシーの名前をダブルクリックし、選択した [vMedia Mount] のプロパティを表示します。
[Properties] ページで、[vMedia Mounts] で使用されるプロパティを変更できます。

第 30 章

サーバ ブートの設定

この章の内容は、次のとおりです。

- ブート ポリシー，459 ページ
- UEFI ブート モード，460 ページ
- UEFI セキュア ブート，461 ページ
- ブート ポリシーの作成，461 ページ
- SAN ブート，463 ページ
- iSCSI ブート，464 ページ
- LAN ブート，491 ページ
- ローカル デバイス ブート，492 ページ
- ブート ポリシーの削除，499 ページ

ブート ポリシー

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

- ブート デバイスの選択
- サーバのブート元である場所
- 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。

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

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

（注） ブート ポリシーに対する変更は、そのブート ポリシーを含んでいる、更新中のサービス プロファイルテンプレートを使って作成されたすべてのサーバに伝播されます。 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。

UEFI ブート モード

Unified Extensible Firmware Interface（UEFI）は、オペレーティング システムとプラットフォーム ファームウェア間のソフトウェア インターフェイスを定義する仕様です。 Cisco UCS Manager は、UEFI を使用して BIOS ファームウェア インターフェイスを置き換えします。 これにより、BIOS は従来のサポートを提供しながら、UEFI モードで動作できるようになります。

ブート ポリシーを作成する際は、レガシー ブート モードまたは UEFI ブート モードのいずれかを選択できます。 レガシー ブート モードは、すべての Cisco UCS サーバでサポートされます。 UEFI ブート モードは M3 サーバでのみサポートされ、ユーザは UEFI セキュア ブート モードを有効にすることができます。

UEFI ブート モードには以下の制限が適用されます。

- UEFI ブート モードは、Cisco UCS B シリーズ M3 ブレードサーバと、Cisco UCS C シリーズ M3 ラック サーバでのみサポートされます。
- UEFI ブート モードは、次の組み合わせではサポートされません。
  - Cisco UCS Manager と統合された Cisco UCS ブレードおよびラック サーバ上の Gen-3 Emulex および QLogic アダプタ。
  - Cisco UCS Manager と統合された Cisco UCS ラック サーバ上のすべてのアダプタに対する PXE ブート。
  - Cisco UCS Manager と統合された Cisco UCS ラック サーバ上の Broadcom アダプタに対する iSCSI ブート。
- 同じサーバで UEFI ブート モードとレガシー ブート モードを混在させることはできません。
- ブート ポリシーに設定されているブート デバイスに UEFI 対応オペレーティング システムがインストールされている場合にのみ、サーバは UEFI モードで正常に起動します。 互換性のある OS が存在しない場合、ブート デバイスは [Boot Order Details] 領域の [Actual Boot Order] タブに表示されません。
- ごくまれですが、UEFI ブート マネージャ エントリが BIOS NVRAM に正しく保存されなかったため、UEFI ブートが成功しない場合があります。 UEFI シェルを使用すると、UEFI ブート マネージャ エントリを手動で入力することができます。 この状況は、以下の場合に発生する可能性があります。

- UEFIブートモードが有効になっているブレードサーバをサービスプロファイルとの関連付けから解除し、[Equipment] タブまたは前面パネルを使用して、手動でそのブレードサーバに電源を投入した場合。
- UEFIブートモードが有効になっているブレードサーバをサービスプロファイルとの関連付けから解除し、VIC ファームウェアの直接アップグレードを試みた場合。
- UEFIブートモードが有効になっているブレードサーバまたはラックサーバをSAN LUNから起動し、サービス プロファイルを移行した場合。

UEFI セキュア ブート

Cisco UCS Manager は、Cisco UCS B シリーズ M3 ブレード サーバで UEFI セキュア ブートをサポートします。 UEFI セキュア ブートを有効にすると、すべての実行可能ファイル（ブート ローダ、アダプタ ドライバなど）はロードされる前に BIOS によって認証されます。 認証されるには、そのイメージに Cisco 認証局（CA）または Microsoft CA による署名が必要です。

UEFI セキュア ブートには次の制限が適用されます。

- UEFI ブート モードは、ブート ポリシーで有効にする必要があります。
- Cisco UCS Manager ソフトウェアと BIOS ファームウェアは、リリース 2.2 以降である必要があります。
- ユーザにより生成された暗号キーはサポートされません。
- UEFI セキュア ブートは、Cisco UCS Manager でのみ制御できます。
- Cisco UCS Managerの以前のバージョンにダウングレードする必要があり、ブレード サーバがセキュア ブート モードになっている場合は、ダウングレードを実行する前に、ブレード サーバの関連付けを解除し、再び関連付ける必要があります。 これを行わないと、そのブレード サーバは正常に検出されません。

ブート ポリシーの作成

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。 しかし、複数のサービス プロファイルまたはサービス プロファイルテンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

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。
シスコ以外の VIC アダプタがあるサーバに適用されるブート ポリシーの場合、[Reboot on Boot Order Change] チェックボックスがオフでも、SAN デバイスが追加、削除または順序の変更がなされると、ブート ポリシーの変更の保存時にサーバは常にリブートします。

ステップ 7 （任意） 必要に応じて、[Enforce vNIC/vHBA/iSCSI Name] チェックボックスをオンにします。

- オンにした場合、Cisco UCS Manager は設定エラーを表示し、[Boot Order] テーブルにリストされた 1 つ以上の vNIC、vHBA、iSCSI、vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかをレポートします。
- オフにした場合、Cisco UCS Manager は、サービス プロファイルから（ブート オプションに応じて）vNIC、vHBA、iSCSI、または vNIC を使用します。

ステップ 8 次の 1 つ以上のオプションをブート ポリシーに設定し、ブート順序を設定します。

- [Local Devices boot]：サーバのローカル ディスクなどのローカル デバイスから、仮想メディアまたはリモート仮想ディスクを起動するには、ブート ポリシー用ローカル ディスク ブート ポリシー設定, （493 ページ） に進みます。
- [SAN boot]：SAN のオペレーティング システム イメージから起動するには、ブート ポリシー用 SAN ブート ポリシー設定, （463 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。
- [LAN boot]：集中型プロビジョニング サーバから起動するには、ブート ポリシー用 LAN ブート ポリシー設定, （491 ページ） に進みます。
- [iSCSI boot]：iSCSI LUN から起動するには、iSCSI ブート ポリシーの作成, （474 ページ） に進みます。

次の作業

ブート ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

SAN ブート

SAN 上のオペレーティング システム イメージから 1 つ以上のサーバがブートするように、ブート ポリシーを設定できます。 ブート ポリシーにはプライマリとセカンダリの SAN ブート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、次の項目が設定されていることを確認してください。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージ デバイスと通信できること。
- オペレーティング システム イメージが置かれているデバイス上のブート ターゲット LUN。

（注） SAN ブートは、Cisco UCS ブレードおよびラック サーバ上の Gen-3 Emulex アダプタではサポートされていません。

ブート ポリシー用 SAN ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。 しかし、複数のサービス プロファイルまたはサービス プロファイル テンプレートに含むことのできるグローバルなブート ポリシーの作成を推奨します。

ヒント 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, （461 ページ） から直接続いています。

手順

ステップ 1 下矢印をクリックして [vHBAs] 領域を展開します。

ステップ 2 [Add SAN Boot] リンクをクリックします。

ステップ 3 [Add San Boot] ダイアログ ボックスで、vHBA とタイプを指定して、[OK] をクリックします。

ステップ 4 この vHBA がブート可能な SAN イメージを参照する場合は、[Add SAN Boot Target] リンク をクリックし、[Add SAN Boot Target] ダイアログボックス で、ブート ターゲット LUN、ブート ターゲット WWPN、およびタイプを指定して、[OK] をクリックします。

ステップ 5 次のどちらかを実行します。

- [Boot Order] テーブルに別のブート デバイスを追加します。
- 終了するには、[OK] をクリックします。

次の作業

ブート ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

iSCSI ブート

iSCSI ブートを利用すると、サーバはネットワークにリモートに配置されている iSCSI ターゲット マシンからオペレーティング システムを起動できます。

iSCSI ブートは次の Cisco UCS ハードウェアでサポートされます。

- Cisco UCS VIC-1240 仮想インターフェイス カード
- Cisco UCS VIC-1280 仮想インターフェイス カード
- Cisco UCS ラック サーバ上の Cisco UCS VIC1225 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, （465 ページ）を参照してください。

iSCSI ブートを実装するための手順の概要については、iSCSI ブートの設定, （468 ページ）を参照してください。

iSCSI ブート プロセス

Cisco UCS Manager は、サーバにあるアダプタをプログラムするための関連付けプロセスで、サービス プロファイル用に作成された iSCSI vNIC と iSCSI のブート情報を使用します。 アダプタの

プログラミング後に、サーバは最新のサービスプロファイル値で再起動します。電源投入時セルフ テスト（POST）の後、アダプタは、それらのサービス プロファイル値を使用して初期化を試みます。 値を使用して指定されたターゲットにログインできる場合、アダプタは iSCSI ブート ファームウェア テーブル（iBFT）を初期化してホスト メモリにポスト紙、有効なブート可能 LUN をシステム BIOS にポストします。 ホスト メモリにポストされる iBFT には、プライマリ iSCSI VNIC にプログラミングされた、イニシエータとターゲットの設定が含まれています。

（注） これまでホストは、LUN 検出が最初に終了したパスに応じて、設定されたブート パスのうち 1 つだけを参照し、そのパスから起動していました。 現在は、設定された iSCSI ブート vNIC が 2 つある場合、ホストは両方のブート パスを参照するようになりました。 したがってマルチパス設定については、単一の IQN を両方のブート vNIC で設定する必要があります。ホストのブート vNIC に異なる IQN が設定されている場合、ホストは下位の PCI を持つブート vNIC で設定された IQN で起動します。

次の手順であるオペレーティング システム（OS）のインストールでは、iBFT 対応の OS が必要です。 OS のインストール時、OS インストーラはホスト メモリをスキャンして iBFT テーブルを調べ、そ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 への 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すると、OS 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 インストールのソフトウェア レベルで動作し、HBA モード（別名 TCP オフロード）では動作しない場合があります。 iBFT が HBA モードで動作するかどうかは、インストール中の OS の機能によって異なります。 また、Cisco UCS M51KR-B Broadcom BCM57711 アダプタを含むサーバの場合、iBFT は、MTU ジャンボ設定に関係なく、通常、1500 の最大伝送単位（MTU）サイズで動作します。 OS が HBA モードをサポートしている場合は、iSCSI インストール プロセスの後に、HBA モード、デュアル ファブリックのサポート、ジャンボ MTU サイズの設定が必要になることがあります。

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、以下のガイドラインと前提条件を満たす必要があります。

- iSCSI ブート ポリシーの作成後、ls-compute 権限を持つユーザは、そのポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに組み込むことができます。 ただし、ls-compute 権限しかないユーザは iSCSI ブート ポリシーを作成できません。
- セカンド vNIC（フェールオーバー vNIC）が iSCSI LUN から起動する必要がある Windows 2008 サーバからの iSCSI ブートを設定するには、Microsoft Knowledge Base Article 976042 を参照してください。 Microsoft には、ネットワーキング ハードウェアが変更されたときに、Windows が iSCSI ドライブからの起動に失敗するか、bugcheck エラーが発生する可能性がある、という既知の問題があります。 この問題を回避するには、Microsoft が推奨する解決方法に従ってください。

- ストレージ アレイは、iSCSI ブートのライセンスが付与され、アレイ サイド LUN マスキングが正しく設定されている必要があります。
- 各 iSCSI イニシエータに 1 つずつ、2 つの IP アドレスを決定する必要があります。 IP アドレスは、ストレージ アレイと同じサブネット上にある必要があります（可能な場合）。 IP アドレスは、Dynamic Host Configuration Protocol（DHCP）を使用して静的または動的に割り当てられます。
- グローバル ブート ポリシーのブート パラメータは設定できません。 代わりに、ブート パラメータの設定後、ブート ポリシーを適切なサービス プロファイルに含める必要があります。
- 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 VIC-1240 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ていません。
  - iSCSI ターゲットに OS をインストールするときは、iSCSI ターゲットの順番を OS イメージが存在するデバイスよりも後にしておく必要があります。 たとえば、CD から iSCSI ターゲットに OS をインストールする場合、ブート順序は最初に CD、その後 iSCSI ターゲットとする必要があります。
  - DHCP Vendor ID（オプション 43）を使用している場合は、オーバレイ vNIC の MAC アドレスを /etc/dhcpd.conf に設定する必要があります。
  - サーバの iSCSI ブート後は、オーバレイ 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 ディスクに書き込む必要があります。

イニシエータ IQN の設定

Cisco UCS は、サービス プロファイルが物理サーバに関連付けられた時点で、以下のルールを使用してアダプタ iSCSI vNIC のイニシエータ IQN を決定します。

- サービス プロファイル レベルのイニシエータ IQN と iSCSI vNIC レベルのイニシエータ IQN を、1 つのサービス プロファイルで一緒に使用することはできません。
- イニシエータ IQN をサービス プロファイル レベルで指定すると、DHCP オプション 43 の場合（イニシエータ IQN はアダプタ iSCSI vNIC で空に設定される）を除き、すべてのアダプタ iSCSI vNIC が同じイニシエータ IQN を使用するように設定されます。
- イニシエータ IQN を iSCSI vNIC レベルで設定すると、サービス プロファイル レベルのイニシエータ IQN は削除されます（存在する場合）。
- サービス プロファイルに 2 つの iSCSI vNIC があり、一方にだけイニシエータ IQN が設定されている場合、もう一方にはデフォルトの IQN プールが設定されます。 この設定は後で変

更できます。 唯一の例外は、DHCP オプション 43 が設定されている場合です。 その場合、もう一方の iSCSI vNIC のイニシエータ IQN は、サービス プロファイルを関連付けるときに削除されます。

（注） ベンダー ID を設定して、DHCP Option 43 を使用するように iSCSI vNIC を変更した場合、サービス プロファイル レベルで設定したイニシエータ IQN は削除されません。 サービス プロファイル レベルのイニシエータ IQN は、DHCP オプション 43 を使用しない別の iSCSI vNIC で使用できます。

Windows での MPIO のイネーブル化

（注） ネットワーク ハードウェアを変更すると、Windows が iSCSI ドライブからの起動に失敗する場合があります。 詳細については、「Microsoft 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、Cisco VIC ドライバが必要です。

ブート LUN に設定されたパスが複数ある場合、LUN がインストールされるときにイネーブルにするパスは 1 つのみです。

手順

ステップ 1 サーバに関連付けられたサービス プロファイルで、プライマリ iSCSI vNIC を設定します。
詳細については、サービス プロファイル用 iSCSI vNIC の作成, （475 ページ）を参照してください。

ステップ 2 プライマリ iSCSI vNIC を使用して、iSCSI ターゲット LUN に Windows オペレーティング システムをインストールします。

ステップ 3 Windows のインストールが完了したら、ホスト上で MPIO をイネーブルにします。

ステップ 4 サーバ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, （474 ページ）を参照してください。

iSCSI ブートの設定

LUN ターゲットから iSCSI ブートするように Cisco UCS でアダプタまたはブレードを設定する場合、次のすべてのステップを完了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, （469 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が使用する認証プロファイルを設定します。	（任意） 詳細については、iSCSI 認証プロファイルの作成, （471 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 IP プールの作成, （473 ページ）を参照してください。
ステップ 4	すべてのサービス プロファイルで使用できるブート ポリシーを作成します。 または、特定のサービス ポリシーに対してのみローカル ブート ポリシーを作成できます。 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, （474 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した場合、それをサービス プロファイルに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。	ステップ 7 において、サービス プロファイルで iSCSI ブートおよび vNIC パラメータを設定するときに、サービス プロファイルにブート ポリシーを割り当てることができます。
ステップ 6	サービス プロファイルで iSCSI vNIC を作成します。	詳細については、サービス プロファイル用 iSCSI vNIC の作成, （475 ページ）を参照してください。
ステップ 7	expert モードでサービス プロファイルにおいて、またはサービス プロファイル テンプレートにおいて、iSCSI ブート パ	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, （528 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, （532 ページ）を参照してください。

	コマンドまたはアクション	目的
	ラメータ（iSCSI 修飾子名（IQN）、イニシエータ、ターゲット インターフェイスなど）および iSCSI vNIC パラメータを設定します。	
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、次のいずれかのドキュメント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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[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。
[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、または両方に含めます。

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。

iSCSI 認証プロファイルの作成

iSCSI ブートの場合、イニシエータおよびターゲットの iSCSI 認証プロファイルを作成する必要があります。

手順

ステップ 1 [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 [iSCSI Authentication Profiles] を右クリックし、[iSCSI Authentication Profile] を選択します。
ステップ 5 [Create Authentication Profile] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	認証プロファイルの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[User ID] フィールド	このプロファイルに関連付けられたユーザ ID。 1 ～ 128 文字の文字、スペース、特殊文字を入力します。
[Password] フィールド	このプロファイルに関連付けられたパスワード。 12 ～ 16 文字（特殊文字を含む）を入力します。
[Confirm Password] フィールド	確認のためのパスワードの再入力。

ステップ 6 [OK] をクリックします。

次の作業

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、または両方に含めます。

iSCSI 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 [iSCSI Authentication Profiles] ノードを展開します。
ステップ 5 削除する IP プールを右クリックし、[Delete] を選択します。
ステップ 6 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 IP プールの作成

iSCSI ブートに使用する IP アドレスのグループを作成できます。 Cisco UCS Manager は指定した IPv4 アドレスのブロックを予約します。

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

手順

ステップ 1 [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 IPv4 Addresses] を選択します。

ステップ 6 [Create a Block of IPv4 Addresses] ダイアログ ボックスで、次のフィールドに入力します。

名前	説明
[名前] カラム	ブロックに割り当てられた IPv4 アドレスの範囲。
[From] カラム	ブロック内の最初の IPv4 アドレス。
[To] カラム	ブロック内の最後の IPv4 アドレス。
[Subnet] カラム	ブロック内の IPv4 アドレスと関連付けられたサブネット マスク。
[Default Gateway] カラム	ブロック内の IPv4 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] カラム	IPv4 アドレスのこのブロックがアクセスする必要のあるプライマリ DNS サーバ。
[Secondary DNS] カラム	IPv4 アドレスのこのブロック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、iSCSI イニシエータ IP プールから iSCSI イニシエータ IP アドレスを取得します。

iSCSI ブート ポリシーの作成

ブート ポリシーあたり最大 2 つの iSCSI vNIC を追加できます。 一方の vNIC はプライマリ iSCSI ブート ソースとして動作し、もう一方はセカンダリ iSCSI ブート ソースとして動作します。

手順

ステップ 1 [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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

ステップ 6 （任意） ブート順序の変更後にこのブート ポリシーを使用するサーバをリブートするには、[Reboot on Boot Order Change] チェックボックス をオンにします。
Cisco UCS Manager GUI で、[Reboot on Boot Order Change] チェックボックスがブート ポリシーについて選択されており、CD-ROM またはフロッピーがブート順の最後のデバイスの場合に、デバイスを取り外すか、装着すると、ブート順に直接効力がなく、サーバがリブートされません。

（注） これは、標準のブート順序を使用しているサーバにのみ適用されます。

ステップ 7 （任意） 必要に応じて、[Enforce vNIC/vHBA/iSCSI Name] チェックボックスをオンにします。

- オンにした場合、Cisco UCS Manager は設定エラーを表示し、[Boot Order] テーブルにリストされた 1 つ以上の vNIC、vHBA、iSCSI、vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかをレポートします。
- オフにした場合、Cisco UCS Manager は、サービス プロファイルから（ブート オプションに応じて）vNIC、vHBA、iSCSI、または vNIC を使用します。

ステップ 8 iSCSI ブートをブート ポリシーに追加するには、次の手順を実行します。

a) 下矢印をクリックして [iSCSI vNICs] 領域を展開します。

b) [Add iSCSI Boot] リンクをクリックします。

c) [Add iSCSI Boot] ダイアログボックスで、iSCSI vNIC の名前を入力し、[OK] をクリックします。
d) 別の iSCSI vNIC を作成するには、ステップ b、c を繰り返します。

次の作業

ブート ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

サービス プロファイル用 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ている組織のノードを展開します。
ステップ 4 iSCSI vNIC を作成するサービス プロファイルを展開します。
ステップ 5 [iSCSI vNICs] ノードを右クリックし、[Create vNICs] を選択します。
ステップ 6 [Create iSCSI vNIC] ダイアログ ボックスで、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	iSCSI vNIC の名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Overlay vNIC] ドロップダウン リスト	この iSCSI vNIC に関連付けられた LAN vNIC（存在する場合）。
[iSCSI Adapter Policy] ドロップダウン リスト	この iSCSI vNIC に関連付けられた iSCSI アダプタ ポリシー（存在する場合）。
[Create iSCSI Adapter Policy] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI アダプタを作成するには、このリンクをクリックします。

名前	説明
[MAC Address] フィールド	この iSCSI vNIC に関連付けられた MAC アドレス（存在する場合）。 MAC アドレスが設定されていない場合は、Cisco UCS Manager GUI に [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（存在する場合）。
[VLAN] ドロップダウン リスト	この iSCSI vNIC に関連付けられた仮想 LAN。 デフォルトの VLAN は [default] です。 （注） Cisco UCS M81KR 仮想インターフェイス カードおよび Cisco UCS VIC-1240 仮想インターフェイス カードの場合は、オーバレイ vNIC のネイティブ VLAN と同じ VLAN を指定する必要があります。 Cisco UCS M51KR-B Broadcom BCM57711の場合は、オーバーレイ vNIC に割り当てられているどの VLAN でも指定できます。

ステップ 7 [iSCSI MAC Address] 領域の [MAC Address Assignment] ドロップダウン リストで、次のいずれかを選択します。

- MAC アドレスの割り当てを解除したままにして、[Select (None used by default)] を選択します。 このサービス プロファイルに関連付けるサーバに Cisco UCS M81KR 仮想インターフェイス カード または Cisco UCS VIC-1240 仮想インターフェイス カードがある場合は、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るサーバに Cisco UCS NIC M51KR-Bがある場合は、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、[MAC Address] フィールドにアドレスを入力します。 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、プール カテゴリが 2 つ存在することがあります。 ドメイン プールは Cisco UCS ドメインでローカルに定義され、グローバル プールは、Cisco UCS Central で定義されます。

ステップ 8 （任意） すべてのサービス プロファイルで使用できる MAC プールを作成する場合は、[Create MAC Pool] をクリックし、[Create MAC Pool] ウィザードでフィールドに値を入力します。
詳細については、MAC プールの作成, （224 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

ステップ 10 （任意） イニシエータ名を設定または変更する場合は、[iSCSI vNICs] タブから [Reset Initiator Name] または [Change Initiator Name] をクリックし、[Change Initiator Name] ダイアログボックスのフィールドを入力するかクリックします。 詳細については、サービス プロファイル レベルでのイニシエータ IQN の設定, （477 ページ）またはサービス プロファイル レベルでのイニシエータ IQN の設定, （477 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ている組織のノードを展開します。

ステップ 4 iSCSI vNIC を削除するサービス プロファイルを展開します。

ステップ 5 [iSCSI vNICs] ノードを展開します。

ステップ 6 削除する iSCSI vNIC を右クリックし、[Delete] を選択します。

ステップ 7 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 レベルでのイニシエータ IQN 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 対象となる組織のノードを展開します。

ステップ 4 変更する iSCSI vNIC が含まれるサービス プロファイルをクリックします。

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

ステップ 6 [Reset Initiator Name] をクリックします。

ステップ 7 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 レベルでのイニシエータ IQN 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 対象となる組織のノードを展開します。

ステップ 4 変更する iSCSI vNIC が含まれるサービス プロファイルをクリックします。

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

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

ステップ 7 [Change Initiator Name] ダイアログ ボックスで、次のフィールドの値を変更します。

名前	説明
[Initiator Name Assignment] ドロップダウン リスト	ドロップダウン リストから、使用する IQN イニシエータ名を選択します。
[Initiator Name] フィールド	手動によるイニシエータ名の割り当てを選択した場合は、イニシエータ名を入力します。
[Create IQN Suffix Pool] リンク	これをクリックして、新しい IQN 接尾辞プールを作成します。

ステップ 8 [OK] をクリックします。

iSCSI ブート パラメータの設定

iSCSI vNIC のブート順序、ブート ポリシー、iSCSI 認証プロファイル、イニシエータ インターフェイス、ターゲット インターフェイスなど、iSCSI ブート パラメータを設定できます。

手順

ステップ 1 [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 プロファイルを含む組織のノードを展開します。 システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 iSCSI ブート パラメータを作成するサービス プロファイルをクリックします。

ステップ 5 [Boot Order] タブをクリックします。

ステップ 6 [Specific Boot Policy] 領域で、下矢印をクリックして [iSCSI vNICs] 領域を展開します。

ステップ 7 [iSCSI vNICs] 領域で、サーバのブート元の iSCSI vNIC をダブルクリックしてそれらを [Boot Order] テーブルに追加します。

ステップ 8 [iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。
2 つの iSCSI vNIC がある場合は、ブート パラメータを設定する方を選択します。

ステップ 9 [Set iSCSI Boot Parameters] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[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	関連する iSCSI 認証プロファイルの名前。
[Create Authentication Profile] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。

ステップ 10 [Initiator Name] 領域で、次のフィールドに入力します。

名前	説明
[Initiator Name Assignment] ドロップダウン リスト	iSCSI ブート イニシエータ名の割り当て方法を選択します。 次の方法の中から 1 つを選択してください。 • [Manual]：[Initiator Name] フィールドに名前を入力します。イニシエータ名には、最大で 223 文字まで使用できます。 • [Pools]：IQN 接尾辞プールを選択します。このプールから名前が割り当てられます。 （注） 必要に応じて、イニシエータ名を変更またはリセットできます。 詳細については、サービス プロファイル レベルでのイニシエータ IQN の変更，（478 ページ）を参照してください。 （注） [Set iSCSI Boot Parameters] ダイアログボックスでイニシエータ名を設定すると、サービス プロファイル レベルではなく、iSCSI vNIC レベルでイニシエータ IQN が設定されます。 複数のパスが設定されている場合は、[iSCSI vNICs] タブから、またはサービス プロファイルの作成時に、イニシエータ IQN を設定する必要があります。
[Create IQN Suffix Pool] リンク	すべての iSCSI vNIC で使用可能な新しい IQN 接尾辞プールを作成するには、このリンクをクリックします。
[Initiator Name] フィールド	iSCSI イニシエータ名を定義する正規表現。 任意の英数字および次の特殊文字を入力することができます。 • .（ピリオド） • :（コロン） • -（ダッシュ）

ステップ 11 [Initiator IP Address Policy] ドロップダウン リストで、次のいずれかを選択します。

オプション	説明
[Select (DHCP used by default)]	システムが DHCP を使用してインターフェイスを自動的に選択します。 ステップ 13 に進みます。
スタティック	スタティック IPv4 アドレスが、この領域に入力された情報に基づいて iSCSI ブート vNIC に割り当てられます。 ステップ 12 に進みます。

オプション	説明
Pool	IPv4 アドレスが管理 IP アドレス プールから iSCSI ブート vNIC に割り当てられます。 ステップ 13 に進みます。

ステップ 12 [Initiator IP Address Policy] ドロップダウン リストから [Static] を選択した場合は、次のフィールドに入力します。

名前	説明
[IPv4 Address] フィールド	iSCSI ブート vNIC に割り当てられた IPv4 アドレス。 このアドレスを指定する場合は、[Initiator IP Address Policy] ドロップダウン リストで [Static] を選択する必要があります。
[Subnet Mask] フィールド	IPv4 アドレスに関連付けられたサブネット マスク。
[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 サーバのアドレス。
[Secondary DNS] フィールド	セカンダリ DNS サーバのアドレス。

ステップ 13 iSCSI ターゲット インターフェイスでは、次のいずれかのオプション ボタンを選択します。

オプション	説明
[iSCSI Static Target Interface]	システムにより、設定する必要があるスタティック ターゲット インターフェイスが作成されます。 ステップ 14 に進みます。
[iSCSI Auto Target Interface]	システムにより、自動ターゲット インターフェイスが作成されます。 自動ターゲットがイニシエータと DHCP ベンダー ID のどちらを使用するか指定する必要があります。 ステップ 16 に進みます。

ステップ 14 [iSCSI Static Target Interface] を選択した場合、[Static Target Interface] テーブルで [Add] をクリックします。

ステップ 15 [Create iSCSI Static Target] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[iSCSI Target Name] フィールド	iSCSI ターゲットの iSCSI 修飾名（IQN）または拡張固有識別子（EUI）の名前を定義する正規表現。 任意の英数字および次の特殊文字を入力することができます。 • .（ピリオド） • :（コロン） • -（ダッシュ） **重要** この名前は、標準の IQN または EUI のガイドラインに従って適切な形式にする必要があります。 以下に、正しい形式の iSCSI ターゲット名の例を示します。 • iqn.2001-04.com.example • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 • iqn.2001-04.com.example:storage.tape1.sys1.xyz • iqn.2001-04.com.example:storage.disk2.sys1.xyz • eui.02004567A425678D
[Priority] フィールド	システムによって iSCSI ターゲットに割り当てられたプライオリティ。
[Port] フィールド	iSCSI ターゲットに関連付けられたポート。 1 ～ 65535 の整数を入力します。 デフォルトは 3260 です。
[Authentication Profile] ドロップダウン リスト	関連する iSCSI 認証プロファイルの名前。
[Create iSCSI Authentication Profile] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。
[IPv4 Address] フィールド	iSCSI ターゲットに割り当てられた IPv4 アドレス。
[LUN ID] フィールド	iSCSI ターゲットの LUN 識別子。

ステップ 16 [iSCSI Auto Target Interface] を選択した場合、[DHCP Vendor Id] フィールドにイニシエータ名または DHCP ベンダー ID を入力します。 イニシエータがすでに設定済みである必要があります。 ベンダー ID には、最大 32 文字の英数字を指定できます。

ステップ 17 [OK] をクリックします。

iSCSI ブート パラメータの変更

iSCSI vNIC のブート順序、ブート ポリシー、iSCSI 認証プロファイル、イニシエータ インターフェイス、ターゲット インターフェイスなど、iSCSI ブート パラメータを変更できます。

手順

ステップ 1 [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 プロファイルを含む組織のノードを展開します。 システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 iSCSI ブート パラメータを変更するサービス プロファイルをクリックします。

ステップ 5 [Boot Order] タブをクリックします。

ステップ 6 [Specific Boot Policy] 領域で、下矢印をクリックして [iSCSI vNICs] 領域を展開します。

ステップ 7 ブート順序の iSCSI vNIC を追加または削除する、またはブート順序を変更するには、次のいずれかを実行します。

- iSCSI vNIC を追加するには、[iSCSI vNICs] 領域で、iSCSI vNIC をダブルクリックして [Boot Order] テーブルに追加します。
- ブート順序から iSCSI vNIC を削除するには、[Boot Order] テーブルで、iSCSI vNIC を選択して [Delete] をクリックします。
- iSCSI vNIC のブート順序を変更するには、[Boot Order] テーブルで、iSCSI vNIC を選択して [Move Up] または [Move Down] をクリックします。

ステップ 8 ブート パラメータを変更するには、[iSCSI vNICs] 領域で、[Set Boot Parameters] リンクをクリックします。
2 つの iSCSI vNIC がある場合は、ブート パラメータを変更する方を選択します。

ステップ 9 [Set iSCSI Boot Parameters] ダイアログボックスで、次のいずれかのフィールドの値を変更します。

名前	説明
[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	関連する iSCSI 認証プロファイルの名前。
[Create Authentication Profile] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。

ステップ 10 [Initiator Name] 領域で、次のフィールドに入力します。

名前	説明
[Initiator Name Assignment] ドロップダウン リスト	iSCSI ブート イニシエータ名の割り当て方法を選択します。 次の方法の中から 1 つを選択してください。 • [Manual]：[Initiator Name] フィールドに名前を入力します。イニシエータ名には、最大で 223 文字まで使用できます。 • [Pools]：IQN 接尾辞プールを選択します。このプールから名前が割り当てられます。 （注） 必要に応じて、イニシエータ名を変更またはリセットできます。 詳細については、サービス プロファイル レベルでのイニシエータ IQN の変更, （478 ページ）を参照してください。 （注） [Set iSCSI Boot Parameters] ダイアログボックスでイニシエータ名を設定すると、サービス プロファイル レベルではなく、iSCSI vNIC レベルでイニシエータ IQN が設定されます。 複数のパスが設定されている場合は、[iSCSI vNICs] タブから、またはサービス プロファイルの作成時に、イニシエータ IQN を設定する必要があります。
[Create IQN Suffix Pool] リンク	すべての iSCSI vNIC で使用可能な新しい IQN 接尾辞プールを作成するには、このリンクをクリックします。
[Initiator Name] フィールド	iSCSI イニシエータ名を定義する正規表現。 任意の英数字および次の特殊文字を入力することができます。 • .（ピリオド） • :（コロン） • -（ダッシュ）

ステップ 11 [Initiator IP Address Policy] ドロップダウン リストの選択を、次のいずれかに変更します。

オプション	説明
[Select (DHCP used by default)]	システムが DHCP を使用してインターフェイスを自動的に選択します。 ステップ 13 に進みます。
スタティック	スタティック IPv4 アドレスが、この領域に入力された情報に基づいて iSCSI ブート vNIC に割り当てられます。 ステップ 12 に進みます。

オプション	説明
Pool	IPv4 アドレスが管理 IP アドレス プールから iSCSI ブート vNIC に割り当てられます。 ステップ 13 に進みます。

ステップ 12 [Initiator IP Address Policy] ドロップダウン リストで [Static] を選択した場合、次のフィールドを入力するか変更してください。

名前	説明
[IPv4 Address] フィールド	iSCSI ブート vNIC に割り当てられた IPv4 アドレス。 このアドレスを指定する場合は、[Initiator IP Address Policy] ドロップダウン リストで [Static] を選択する必要があります。
[Subnet Mask] フィールド	IPv4 アドレスに関連付けられたサブネット マスク。
[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 サーバのアドレス。
[Secondary DNS] フィールド	セカンダリ DNS サーバのアドレス。

ステップ 13 iSCSI ターゲット インターフェイスでは、次のいずれかのオプション ボタンを選択します。

オプション	説明
[iSCSI Static Target Interface]	システムにより、設定する必要があるスタティック ターゲット インターフェイスが作成されます。 ステップ 14 に進みます。
[iSCSI Auto Target Interface]	システムにより、自動ターゲット インターフェイスが作成されます。 自動ターゲットがイニシエータと DHCP ベンダー ID のどちらを使用するか指定する必要があります。 ステップ 15 に進みます。

ステップ 14 [iSCSI Static Target Interface] を選択した場合は、[Static Target Interface] テーブルで次のいずれかを実行します。

- iSCSI スタティック ターゲット インターフェイスを追加するには、[Add] をクリックします。 iSCSI ターゲット インターフェイスを変更するには、変更する iSCSI ターゲット インターフェイスを選択して [Modify] をクリックします。 次に、[Create iSCSI Static Target] ダイアログボックスで、次のフィールドを入力または変更します。

名前	説明
[iSCSI Target Name] フィールド	iSCSI ターゲットの iSCSI 修飾名（IQN）または拡張固有識別子（EUI）の名前を定義する正規表現。 任意の英数字および次の特殊文字を入力することができます。 • .（ピリオド） • :（コロン） • -（ダッシュ） **重要** この名前は、標準の IQN または EUI のガイドラインに従って適切な形式にする必要があります。 以下に、正しい形式の iSCSI ターゲット名の例を示します。 • iqn.2001-04.com.example • iqn.2001-04.com.example:storage:diskarrays-sn-a8675309 • iqn.2001-04.com.example:storage.tape1.sys1.xyz • iqn.2001-04.com.example:storage.disk2.sys1.xyz • eui.02004567A425678D
[Priority] フィールド	システムによって iSCSI ターゲットに割り当てられたプライオリティ。
[Port] フィールド	iSCSI ターゲットに関連付けられたポート。 1 ～ 65535 の整数を入力します。 デフォルトは 3260 です。
[Authentication Profile] ドロップダウン リスト	関連する iSCSI 認証プロファイルの名前。
[Create iSCSI Authentication Profile] リンク	すべての iSCSI vNIC で使用可能な新しい iSCSI 認証プロファイルを作成するには、このリンクをクリックします。
[IPv4 Address] フィールド	iSCSI ターゲットに割り当てられた IPv4 アドレス。
[LUN ID] フィールド	iSCSI ターゲットの LUN 識別子。

- iSCSI ターゲット インターフェイスを削除するには、削除する iSCSI ターゲット インターフェイスを選択して [Delete] をクリックします。

（注） 2 つの iSCSI スタティック ターゲットがあり、優先順位 1 位のターゲットを削除すると、優先順位 2 位のターゲットが優先順位 1 位のターゲットになります。ただし、このターゲットは、Cisco UCS Manager では、引き続き優先順位 2 位のターゲットとして表示されます。

ステップ 15 [iSCSI Auto Target Interface] を選択した場合、[DHCP Vendor Id] フィールドのエントリをイニシエータ名または DHCP ベンダー ID に変更します。 イニシエータがすでに設定済みである必要があります。 ベンダー ID には、最大 32 文字の英数字を指定できます。

ステップ 16 [OK] をクリックします。

IQN プール

IQN プールは、iSCSI vNIC が Cisco UCS ドメインでイニシエータ ID として使用する iSCSI 修飾名（IQN）の集合です。

IQN プールのメンバの形式は、プレフィックス:サフィックス:番号となり、プレフィックス、サフィックス、および番号のブロック（範囲）を指定できます。

IQN プールには、番号の範囲やサフィックスが異なる（ただし、プレフィクスは共通している）複数の IQN ブロックを含めることができます。

IQN プールの作成

（注） ほとんどの場合、最大 IQN サイズ（プレフィックス + サフィックス + 追加文字）は 223 文字です。 Cisco UCS NIC M51KR-B アダプタを使用する場合、IQN サイズを 128 文字に制限する必要があります。

手順

ステップ 1 [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、次のフィールドに値を入力します。

名前	説明
[Name] フィールド	iSCSI 修飾名（IQN）プールの名前。 この名前には、1 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	プールのユーザ定義による説明。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Prefix] フィールド	このプール用に作成された任意の IQN ブロックのプレフィクス。 1 ～ 150 文字を入力します。 任意の文字や数字、および次の特殊文字を使用できます：.（ピリオド）、:（コロン）、-（ハイフン）。 たとえば、iqn1.alpha.com を使用できます。
[割り当て順序] フィールド	次のいずれかになります。 • [デフォルト]：Cisco UCS Manager はプールからランダム ID を選択します。 • [シーケンシャル]：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	iSCSI 修飾名（IQN）のこのブロックの接尾辞。 1 ～ 64 文字を入力します。 任意の文字や数字、および次の特殊文字を使用できます：.（ピリオド）、:（コロン）、-（ハイフン）。 たとえば、alphadc-1 を使用できます。
[From] フィールド	ブロック内の最初の接尾辞番号。
[Size] フィールド	ブロック内の接尾辞の数。

ステップ 9 [OK] をクリックします。

ステップ 10 [Finish] をクリックして、ウィザードを終了します。

次の作業

IQN サフィックス プールをサービス プロファイルとテンプレートのうち一方、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	iSCSI 修飾名（IQN）のこのブロックの接尾辞。 1 ～ 64 文字を入力します。 任意の文字や数字、および次の特殊文字を使用できます：.（ピリオド）、:（コロン）、-（ハイフン）。 たとえば、alphadc-1 を使用できます。
[From] フィールド	ブロック内の最初の接尾辞番号。
[Size] フィールド	ブロック内の接尾辞の数。

ステップ 7 [OK] をクリックします。

IQN プールからのブロックの削除

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

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

手順

ステップ 1 [Navigation] ペインの [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 接尾辞のブロックを削除する IQN プールを選択します。
ステップ 6 [Work] ペインで、[IQN Blocks] タブをクリックします。
ステップ 7 削除するブロックを右クリックし、[Delete] を選択します。
ステップ 8 [Yes] をクリックして削除を確認します。
ステップ 9 [Save Changes] をクリックします。

IQN プールの削除

プールを削除した場合、Cisco UCS Manager は、 でそのプールの vNIC または vHBA に割り当てられたアドレスを再割り当てしません。 削除されたプールのすべての割り当て済みブロックは、次のいずれかが起きるまで、割り当てられた vNIC または vHBA に残ります。

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

手順

ステップ 1 [Navigation] ペインの [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 の集中プロビジョニング サーバから 1 つまたは複数のサーバをブートするブート ポリシーを設定できます。 LAN（または PXE）ブートは、その LAN サーバからサーバに OS をインストールする際に頻繁に使用されます。

LAN ブート ポリシーには、複数のタイプのブート デバイスを追加できます。 たとえば、ローカル ディスクや仮想メディア ブートをセカンダリ ブート デバイスとして追加できます。

ブート ポリシー用 LAN ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。 しかし、複数のサービス プロファイルまたはサービス プロファイルテンプレートに含むことのできるグローバルなブート ポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。 たとえば、セカンダリ ブート デバイスとして、ローカル ディスクや仮想メディア 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, （461 ページ） から直接続いています。

手順

ステップ 1 下矢印をクリックして [vNICs] 領域を展開します。

ステップ 2 [Add LAN Boot] リンクをクリックします。

ステップ 3 **[Add LAN Boot]** ダイアログボックスで、LAN ブートに使用する vNIC の名前を [vNIC] フィールドに入力して、[OK] をクリックします。

ステップ 4 次のどちらかを実行します。

- [Boot Order] テーブルに別のブート デバイスを追加します。

- 終了するには、[OK] をクリックします。

次の作業

ブート ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ローカル デバイス ブート

Cisco UCS Manager では、異なるローカル デバイスから起動することができます。

（注） Cisco UCS M3 ブレード/ラック サーバで拡張ブート順序を使用する場合は、最上位と第 2 レベルの両方のブート デバイスを選択できます。 Cisco UCS M1 および M2 ブレード/ラック サーバで標準ブート順序を使用する場合は、最上位のデバイスのみを選択できます。

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、ブート ポリシーを設定して、最上位のローカル ディスク デバイスまたは以下の第 2 レベルのデバイスからサーバを起動できます。

- ローカル LUN
- SD カード
- 内蔵 USB
- 外部 USB

（注） 第 2 レベルのデバイスは、Cisco UCS M3 ブレード/ラック サーバで拡張ブート順序を使用する場合にのみ使用できます。 Cisco UCS M1 および M2 ブレード/ラック サーバで標準ブート順序を使用する場合は、最上位の [Add Local Disk] のみ選択できます。

仮想メディア ブート

ブート ポリシーを設定して、サーバ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できます。 仮想メディア デバイスは、物理 CD/DVD ディスク（読み取り専用）またはフロッピーディスク（読み取り書き込み）のサーバへの挿入を疑似的に実行します。 このタイプのサーバブートは、通常、サーバに手動でオペレーティング システムをインストールするために使用されます。

（注） 第 2 レベルのデバイスは、Cisco UCS M3 ブレード/ラック サーバで拡張ブート順序を使用する場合にのみ使用できます。 Cisco UCS M1 および M2 ブレード/ラック サーバで標準ブート順序を使用する場合は、最上位の [Add CD/DVD] または [Add Floppy] のみ選択できます。

リモート仮想ドライブのブート

ブート ポリシーを設定して、サーバからアクセスできるリモート仮想ドライブから 1 つ以上のサーバを起動できます。

ブート ポリシー用ローカル ディスク ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。 しかし、複数のサービス プロファイルまたはサービス プロファイルテンプレートに含むことのできるグローバルなブート ポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。 たとえば、セカンダリ ブート デバイスとして SD カードのブートを追加できます。

この手順は、ブート ポリシーの作成, （461 ページ） から直接続いています。

手順

ステップ 1 下矢印をクリックして [Local Devices] 領域を展開します。

ステップ 2 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- [Add Local Disk] または
  - Add Local LUN
  - Add SD Card
  - Add Internal USB
  - Add External USB

（注） Cisco UCS M3 ブレード/ラック サーバで拡張ブート順序を使用する場合は、最上位と第 2 レベルの両方のブート デバイスを選択できます。 Cisco UCS M1 および M2 ブレード/ラック サーバで標準ブート順序を使用する場合は、最上位のデバイスのみを選択できます。

ステップ 3 次のどちらかを実行します。

- [Boot Order] テーブルに別のブート デバイスを追加します。
- 終了するには、[OK] をクリックします。

次の作業

ブート ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

ブート ポリシー用仮想メディア ブート ポリシー設定

サービス プロファイルまたはサービス プロファイル テンプレートに制限されたローカル ブート ポリシーを作成することもできます。 しかし、複数のサービス プロファイルまたはサービス プロファイルテンプレートに含むことのできるグローバルなブートポリシーの作成を推奨します。

ブート ポリシーには複数のタイプのブート デバイスを追加できます。 ローカル ディスク ブートをセカンダリ ブート デバイスとして追加できます。

（注） 仮想メディアでは、USB を有効にする必要があります。 USB の機能に影響する BIOS 設定を変更した場合は、仮想メディアにも影響します。 したがって、最適なパフォーマンスを実現するためには、次の USB BIOS をデフォルト設定のままにしておくことをお勧めします。

- [Make Device Non Bootable]：[disabled] に設定します。
- [USB Idle Power Optimizing Setting]：[high-performance] に設定します。

この手順は、ブート ポリシーの作成, （461 ページ） から直接続いています。

手順

ステップ 1 下矢印をクリックして [Local Devices] 領域を展開します。

ステップ 2 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- [ADD CD/DVD] または
  - Add Local CD/DVD
  - [Add Remote CD/DVD]
- [Add Floppy] または
  - Add Local Floppy
  - Add Remote Floppy
- Add Remote Virtual Drive

（注） Cisco UCS M3 ブレード/ラック サーバで拡張ブート順序を使用する場合は、最上位と第 2 レベルの両方のブート デバイスを選択できます。 Cisco UCS M1 および M2 ブレード/ラック サーバで標準ブート順序を使用する場合は、最上位のデバイスのみを選択できます。

ステップ 3 次のどちらかを実行します。

- [Boot Order] テーブルに別のブート デバイスを追加します。
- 終了するには、[OK] をクリックします。

次の作業

ブート ポリシーをサービス プロファイルとテンプレートのうち一方、または両方に含めます。

このブート ポリシーを含むサービス プロファイルがサーバに関連付けられた後で、サーバの [General] タブの [Boot Order Details] 領域で実際のブート順序を確認できます。

vMedia ブート 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 [Boot Policies] を右クリックし、[Create Boot Policy] を選択します。

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

名前	説明
[名前] フィールド	ポリシーの名前。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

名前	説明
[Reboot on Boot Order Change] 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、ブート順序を変更した場合にサーバがリブートされます。 このオプションが選択されると、次のアクションが実行されます。 • **CDD/HDD** のデバイスが vMedia ポリシーに存在し、同じデバイスがブートポリシーにある場合、そのデバイスに対する vmedia ポリシーを変更すると、サーバが再起動されます。 この再起動は、マウントされた最新のイメージから起動することが目的です。 • **CDD/HDD** のデバイスが vMedia ポリシーに存在し、同じデバイスがブートポリシーにある場合、そのデバイスに対する vmedia ポリシーを変更すると、サーバが再起動されます。 （注） このオプションが選ばれなければ、vMedia ポリシーを変更してもホストは再起動されません。 非仮想化アダプタのブートデバイスを追加または変更すると、常にサーバがリブートされます。
[Boot Mode] フィールド	有効なブート モードのタイプ。 次のいずれかになります。 • [Legacy]：システムが UEFI 対応でない場合に選択します。 • [Uefi]：システムが UEFI 対応の場合に選択します。 （注） UEFI ブートモードを使用するには、アダプタ ファームウェアが UEFI 対応であること、ブートデバイスが UEFI 対応のオペレーティング システムを備えていること、サービス プロファイルが Cisco UCS M3 ブレードまたはラック サーバに関連付けられていることが必要です。

ステップ 5 ブート順序に仮想リモート vMedia デバイスを追加するために [CIMC Mounted vMedia] を展開します。

ステップ 6 [Add Remote vMedia HDD or Add Remote vMedia CD/DVD] リンクをクリックします。
選択する **vMedia** デバイスに応じて [Add Remote vMedia] ダイアログボックスが表示されます。

ステップ 7 ドロップダウン リストから [CIMC Mounted CD/DVD] または [CIMC Mounted HDD] を追加します。

ステップ 8 [OK] をクリックします。
vMedia ブート ポリシーが [Boot Order] ペインに追加されます。

次の作業

vMedia およびブート ポリシーを**サービス プロファイル**に関連付けます。

vMedia サービス プロファイルへのブート ポリシーの追加

この手順では、[Create Service Profile (expert)] ウィザードの [Server Boot Order] ページで、vMedia のブート ポリシーのオプションを設定する方法について説明します。

手順

ステップ 1 [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。
[Unified Computing System Manager] ペインが表示されます。

ステップ 5 [Name] フィールドに、サービス プロファイルの識別に使用できる一意の名前を入力します。
この名前には、2 ～ 32 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービスプロファイルおよびサービスプロファイル テンプレートで一意であることが必要です。

この名前は、サービス プロファイルを作成する組織またはサブ組織内で一意である必要があります。

ステップ 6 [UUID Assignment] ドロップダウン リストで、次のいずれかの手順を実行します。

オプション	説明
Select (pool default used by default)	デフォルトの UUID 接尾辞プールから UUID を割り当てます。 ステップ 8 に進みます。
	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUIDはサービスプロファイルがサーバと関連付けられるまで割り当てられません。 この時点で、UUID は製造元によってサーバに割り当てられたUUID値に設定されます。 サービス プロファイルを後で別のサーバに移動すると、UUIDは新しいサーバに一致するように変更されます。 ステップ 8 に進みます。
	手動で割り当てる UUID を使用します。 ステップ 7 に進みます。

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 8 に進みます。

ステップ 7 （任意） オプションを選択した場合は、次の手順を実行します。

a) [UUID] フィールドに、このサービス プロファイルを使用するサーバに割り当てる有効な UUID を入力します。

b) 選択した UUID が使用可能であることを確認するには、[here] リンクをクリックします。

ステップ 8 （任意） このサービス プロファイルで使用する新しい UUID 接尾辞プールを作成する場合は、[Create UUID Suffix Pool] をクリックし、[Create UUID Suffix Pool] ウィザードのフィールドに値を入力します。
詳細については、UUID 接尾辞プールの作成, （344 ページ）を参照してください。

ステップ 9 （任意） テキスト ボックスに、このサービス プロファイルの説明を入力します。
このサービス プロファイルのユーザ定義による説明。

256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 10 [Next] をクリックします。

ステップ 11 [Create Service Profile (expert)] に**移動し**、[Server Boot Order] をクリックします。
[Boot Policy] ペインが表示されます。

ステップ 12 [Boot Policy] ドロップダウン リストから、次のいずれかを選択します。

オプション	説明
Select Boot Policy to use	このサービス プロファイルにデフォルトのブート ポリシーを割り当てます。 ステップ 13 に進みます。
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。

オプション	説明
[Boot Policies *Policy_Name*]	サービス プロファイルに既存のブート ポリシーを割り当てます。 このオプションを選択した場合、Cisco UCS Manager でポリシーの詳細が表示されます。 既存のポリシーを使用するのではなく、すべてのサービス プロファイルがアクセスできるポリシーを作成する場合は、[Create Boot Policy] をクリックします。 それ以外の場合は、リストでポリシーを選択し、ステップ 13 に進みます。

ステップ 13 すべてのサービスプロファイルおよびテンプレートにアクセスできる新しいブートポリシーを作成したら、[Boot Policy] ドロップダウン リストからそのポリシーを選択します。

ステップ 14 [Next] をクリックします。

次の作業

サービス プロファイルを Cisco UCS サーバに関連付けます。

ブート ポリシーの削除

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 31 章

サービス プロファイル更新の遅延展開

この章の内容は、次のとおりです。

- サービス プロファイルの遅延展開，501 ページ
- スケジュールの設定，505 ページ
- メンテナンス ポリシーの設定，518 ページ
- 保留アクティビティの管理，521 ページ

サービス プロファイルの遅延展開

サービス プロファイルの変更の一部、またはサービス プロファイル テンプレートの更新は、中断をともなうことや、サーバのリブートが必要になることがあります。 ただし、これらの中断をともなう設定変更をいつ実行するかを、遅延展開によって制御できます。 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、指定されたメンテナンス時間帯に展開するかを選択できます。 また、サービスプロファイルの展開にユーザの明示的な確認応答が必要かどうかを選択できます。

遅延展開は、サーバとサービス プロファイルとの関連付け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 プロファイルへの変更、サービス プロファイルに含まれるポリシーへの変更、更新サービスプロファイルテンプレートへの変更によってプロンプト表示される場合があります。 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 パッケージや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およびアクティブ化を延期することもできます。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、ファームウェアパッケージを使用し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遅延させることはできません。

遅延展開は、サーバのリブートを必要とする次のアクションに使用できません。

- サーバのサービス プロファイルの最初の関連付け

- サービス プロファイルと別のサーバを関連付けない、サービス プロファイルのサーバからの関連付けの最終解除
- サーバの解放
- サーバの再認識
- サーバのリセット

サービス プロファイル変更の展開を遅延させる場合、1 つ以上のメンテナンス ポリシーを設定し、各サービス プロファイルにメンテナンス ポリシーを設定する必要があります。 展開が発生する時間帯を指定する場合、1 つ以上の繰り返しオカレンスまたはワンタイム オカレンスを持つ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があります。

遅延展開スケジュール

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 回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。 オカレンスの時間長や実行されるタスクの最大数といった、オカレンスで定義されるオプションにより、サービス プロファイルの変更が展開されるかどうかが決まります。 たとえば、最大時間長またはタスク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、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、Cisco UCS ドメインが 1 つまたは複数のメンテナンス時間に入っているかどうか、定期的に確認します。 入っている場合、スケジュールはメンテナンス ポリシーで指定された制限に対し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。

ワンタイム オカレンス

ワンタイム オカレンスは、単一のメンテナンス時間を定義します。 これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。

繰り返しオカレンス

繰り返しオカレンスは、一連のメンテナンス時間を定義します。 これらの時間帯は、タスクの最大数に達するまで、またはオカレンスに指定された日の終わりに達するまで継続します。

メンテナンス ポリシー

メンテナンス ポリシーは、サーバに関連付けられたサービス プロファイル、または 1 つ以上のサービス プロファイルに関連付けられた更新中のサービス プロファイルに対して、サーバのリブートが必要になるような変更が加えられた場合の Cisco UCS Manager の対処方法を定義します。

メンテナンス ポリシーは、Cisco UCS Manager でのサービス プロファイルの変更の展開方法を指定します。 展開は、次のいずれかの方法で実行されます。

- 即時
- ユーザが管理者権限で承認したときに実行する
- スケジュールで指定された時間に自動的に実行する

スケジュール済みのメンテナンス ウィンドウ中に変更を展開するように設定されているメンテナンスポリシーでは、ポリシーに有効なスケジュールが含まれていることが必要です。 この場合、最初に使用可能なメンテナンス ウィンドウ中に変更が展開されます。

（注） メンテナンス ポリシーでは、関連付けられたサービス プロファイルに設定変更が加えられた場合に、サーバの即時リブートは回避できますが、 次のアクションの即時実行は回避されません。

- 関連付けられたサービス プロファイルのシステムからの削除
- サーバ プロファイルのサーバからの関連付けの解除
- サービス ポリシーを使用しないファームウェア アップグレードの直接インストール
- サーバのリセット

保留アクティビティ

Cisco UCS ドメインで遅延展開を設定すると、Cisco UCS Manager を使用して保留中のアクティビティすべてを表示することができます。 ユーザの確認応答を待っているアクティビティと、スケジュールされたアクティビティを表示できます。

Cisco UCS ドメイン 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 は管理者権限を持つユーザがログインしたときに通知します。

Cisco UCS Manager は、すべての保留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、サーバに関連付けられているサービス プロファイルの名前
- 展開の影響を受けるサーバ
- 展開により発生する中断
- 展開によって実行される変更

（注） 特定の保留アクティビティをサーバに適用するメンテナンス時間帯を指定することはできません。 メンテナンス時間帯は、保留アクティビティの数およびサービス プロファイルに割り当てられているメンテナンス ポリシーに応じて変化します。 ただし、保留アクティビティがユーザの確認応答またはメンテナンス時間帯のいずれを待っているかにかかわらず、管理者権限を持つユーザは、手動で保留アクティビティを開始して、ただちにサーバをリブートできます。

遅延展開に関するガイドラインおよび制限事項

サービス プロファイルまたはサービス プロファイル テンプレートへのすべての変更を元に戻すことはできない

保留中の変更をキャンセルする場合、Cisco UCS Manager はサーバを再起動せずに変更のロールバックを試みます。 ただし、複雑な変更を行った場合、Cisco UCS Manager は変更のロール バックのためサーバを 2 回リブートしなければならない場合があります。 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 プロファイルで元の vNIC を復元しても、この再起動および変更はキャンセルできません。 代わりに、Cisco UCS Manager は 2 回目の展開とサーバのリブートをスケジュールします。

サービス プロファイルの関連付けはメンテナンス時間の境界を超えてもよい

Cisco UCS Manager がサービス プロファイルの関連付けを開始した後、スケジューラとメンテナンス ポリシーは手順を制御する方法を持っていません。 サービス プロファイルの関連付けが割り当てられたメンテナンス時間に完了しない場合、プロセスが完了するまで続行されます。 たとえば、いくつかの段階の再試行やその他の問題のため、関連付けが完了しなかった場合に発生することがあります。

保留中のアクティビティの順序を指定できない

スケジュールされた展開は、独立して並行実行されます。 展開が発生する順序は指定できません。 また、あるサービスプロファイルの変更を他のものの完了を条件として実行することもできません。

保留中のアクティビティの部分的な展開を実行できない

Cisco UCS Manager は、サーバ プロファイルに加えられたすべての変更をスケジュールされたメンテナンス時間に適用します。 サービスプロファイルに複数の変更を加えた後にそれらの変更を別々のメンテナンス時間に振り分けることはできません。 サービスプロファイルの変更を展開するとき、Cisco UCS Manager はデータベース内の最新の設定に一致するようにサービス 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、[スケジュール] をクリックし、[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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Description] フィールド	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関する情報を含めることを推奨します。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[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]：Cisco UCS Manager がこのCisco UCS ドメインで設定されたスケジュールを所有しています。 • [Pending Global]：Cisco UCS Manager は Cisco UCS Central にこのスケジュールを転送中です。 • [Global]：Cisco UCS Central がリモート サーバで設定されたスケジュールを所有しています。

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。 このスケジュールのワン タイム 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。
追加	[Create a One Time Occurrence] ダイアログボックスを開き、このスケジュールを実行する単一の時間を指定できます。 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ワンタイム 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Start Time] フィールド	オカレンスが実行される日時。 フィールドの端にある下矢印をクリックして、カレンダーから日付を選択します。

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 [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可能な限り多くのスケジュールされたタスクを完了させます。 デフォルトでは、最大時間は [none] に設定されます。 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時間が続きます。
[Max Number of Tasks] フィールド	このオカレンスの間に実行可能な、スケジュール設定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、それらのタスクをすべて実行します。 [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時間が続きます。 • [other]：Cisco UCS Manager GUI にテキスト 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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[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、システムで処理できる、可能な限り多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンス中に同時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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

名前	説明
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。 次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に [dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最小時間長を指定できます。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

d) [OK] をクリックします。

ステップ 7 もう 1 つワン タイム オカレンスを追加するには、[Add] をクリックし、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） このスケジュールの繰り返しオカレンスを定義する場合は、[Recurring Occurrences] ページで [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しオカレンスの名前。 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

名前	説明
[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。 • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日
[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 の整数で指定します。0 と 24 は両方とも深夜を指します。 （注） Cisco UCS は、最長期間に到達していない場合でも、すべての繰り返しオカレンスを開始されたその日のうちに終了します。 たとえば、開始時刻を午後 11 時に指定し、 最長期間を 3 時間に設定した場合、Cisco UCS はオカレンスを 11 時に開始しますが、 午後 11:59 に終了させます。 これはわずか 59 分後になります。 午後 11:59 までに繰り返しオカレンスが完了するように、開始時刻として早めの時刻を設定してください。
[Minute] フィールド	スケジュール オカレンスを開始する時刻（分単位）。 0 ～ 60 の整数を指定できます。

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 [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可能な限り多くのスケジュールされたタスクを完了させます。
[Max Number of Tasks] フィールド	各オカレンス中に実行可能な、スケジュール設定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、それらのタスクをすべて実行します。 [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時間が続きます。 • [other]：Cisco UCS Manager GUI にテキスト 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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[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、システムで処理できる、可能な限り多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンス中に同時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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

名前	説明
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。 次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に [dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最小時間長を指定できます。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

d) [OK] をクリックします。
e) 別の繰り返しオカレンスを追加するには、[Add] をクリックし、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。

スケジュールのワンタイム オカレンスの作成

（注） デフォルトでは、タスクの最大期間と最大数は [none] に設定されています。 これらのデフォルトをどちらも変更しない場合、Cisco UCS Manager は、メンテナンス ウィンドウが続く期間に対する制限は課せられません。 保留中のすべてのアクティビティは、スケジュールされたメンテナンス ウィンドウが開始されるとすぐに適用され、Cisco UCS Manager は、これら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る影響を受けるサーバのリブートを続行します。

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、[Schedules] を展開します。
ステップ 3 オカレンスを追加するスケジュールを右クリックし、[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ワンタイム 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[Start Time] フィールド	オカレンスが実行される日時。 フィールドの端にある下矢印をクリックして、カレンダーから日付を選択します。

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 [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可能な限り多くのスケジュールされたタスクを完了させます。 デフォルトでは、最大時間は [none] に設定されます。 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時間が続きます。

名前	説明
[Max Number of Tasks] フィールド	このオカレンスの間に実行可能な、スケジュール設定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、それらのタスクをすべて実行します。 [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時間が続きます。 • [other]：Cisco UCS Manager GUI にテキスト 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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[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、システムで処理できる、可能な限り多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンス中に同時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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。 次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に [dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最小時間長を指定できます。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

ステップ 7 [OK] をクリックします。

スケジュールの繰り返しオカレンスの作成

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 オカレンスを追加するスケジュールを右クリックし、[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しオカレンスの名前。 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[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。 • 毎日 • 月曜日 • 火曜日 • 水曜日 • 木曜日 • 金曜日 • 土曜日 • 日曜日 • 奇数日 • 偶数日

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 の整数で指定します。0 と 24 は両方とも深夜を指します。 （注） Cisco UCS は、最長期間に到達していない場合でも、すべての繰り返しオカレンスを開始されたその日のうちに終了します。 たとえば、開始時刻を午後 11 時に指定し、 最長期間を 3 時間に設定した場合、Cisco UCS はオカレンスを 11 時に開始しますが、 午後 11:59 に終了させます。 これはわずか 59 分後になります。 午後 11:59 までに繰り返しオカレンスが完了するように、開始時刻として早めの時刻を設定してください。
[Minute] フィールド	スケジュール オカレンスを開始する時刻（分単位）。 0 ～ 60 の整数を指定できます。

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 [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可能な限り多くのスケジュールされたタスクを完了させます。

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、スケジュール設定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、それらのタスクをすべて実行します。 [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時間が続きます。 • [other]：Cisco UCS Manager GUI にテキスト 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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[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、システムで処理できる、可能な限り多くの同時タスクを実行します。 • [other]：Cisco UCS Manager GUI にテキスト フィールドが表示され、このオカレンス中に同時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） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。
[Minimum Interval Between Tasks] フィールド	システムが新しいタスクを開始するまで待機する最小時間長。この設定は、同時実行タスクの最大数が [None] 以外の値に設定されている場合にのみ有効です。 次のいずれかになります。 • [None]：Cisco UCS は次のタスクを可能な限り早く実行します。 • [other]：Cisco UCS Manager GUI に [dd:hh:mm:ss] フィールドが表示され、Cisco UCS がタスク間で待機する最小時間長を指定できます。 （注） このスケジュールがエラー抑制タスクに関連付けられている場合、このオプションは適用されません。

ステップ 7 [OK] をクリックします。

スケジュールからのワンタイム オカレンスの削除

これがスケジュールにおける唯一の実行である場合には、そのスケジュールは実行なしで再設定されます。 スケジュールがメンテナンス ポリシーに含まれており、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ているサーバに関連する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回限りの実行か繰り返し実行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しオカレンスの削除

これがスケジュールにおける唯一の実行である場合には、そのスケジュールは実行なしで再設定されます。 スケジュールがメンテナンス ポリシーに含まれており、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ているサーバに関連する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回限りの実行か繰り返し実行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設定されます。 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ているサーバに関連する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、スケジュールをメンテナンス ポリシー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] 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

このメンテナンス ポリシーを自動遅延展開用に設定する予定の場合は、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
[名前] フィールド	ポリシーの名前。 この名前には、1～16文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および.（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[Reboot Policy] フィールド	サービスプロファイルをサーバに関連付けたときや、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ときは、プロセスを完了するために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 プロファイルのいずれかに関連付けられたサーバをリブートする時期を決定します。 次のいずれかになります。 • [Immediate]：サービス プロファイルの関連付けが完了したときや、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たときに、ただちにサーバが自動リブートされます。 • [User Ack]：サービス プロファイルの関連付けが完了したときや変更を加えたときは、サーバを手動でリブートする必要があります。 • [Timer Automatic]：Cisco UCS は、[Schedule] フィールドのスケジュールで定義されているメンテナンス時間帯まで、すべてのサービス プロファイルの関連付けや変更を延期します。

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は、メンテナンス操作をサーバに適用できる時期をスケジュールで指定します。 スケジュールした時間に Cisco UCS よってサーバがリブートされ、サービス プロファイルの変更が完了します。
[Create Schedule] リンク	この Cisco UCS ドメイン内のすべてのオブジェクトで使用できる新しいスケジュールを作成するには、このリンクをクリックします。

ステップ 6 [OK] をクリックします。

次の作業

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

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。

保留アクティビティの管理

保留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確認が必要なタスクを表示する [Service Profiles] タブと [Fabric Interconnects] タブが含まれています。
- [Scheduled Activities]：関連するメンテナンス 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 表の行をクリックし、保留アクティビティの詳細を表示します。
[Server] 列のリンクをクリックすると、Cisco UCS Manager によってサーバのプロパティが表示されます。

ユーザの確認応答待ちサービス 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、Cisco UCS Manager が影響のあるサーバをリブートすることは禁止できません。

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] タブをクリックしてから [Service Profiles] タブをクリックします。

ステップ 3 即時展開する保留中の各アクティビティの [Reboot Now] 列の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 保留中のアクティビティの影響を受けるサーバがただちにリブートします。

ユーザの確認応答待ちのすべてのサービス 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、Cisco UCS Manager が影響のあるサーバをリブートすることは禁止できません。

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] タブをクリックしてから [Service Profiles] 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 が、テーブル内のすべての保留中のアクティビティに対して [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 が、テーブル内にリストされている保留中のアクティビティに影響されるすべてのサーバをただちにリブートします。

スケジュールされたサービス プロファイル変更の即時展開

重要　保留中のアクティビティを確認した後、Cisco UCS Manager が影響のあるサーバをリブートすることは禁止できません。

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の [Scheduled Activities] タブをクリックします。

ステップ 3　即時展開する保留中の各アクティビティの [Reboot Now] 列の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 保留中のアクティビティの影響を受けるサーバがただちにリブートします。

スケジュールされたすべてのサービス プロファイル変更の即時展開

重要 保留中のアクティビティを確認した後、Cisco UCS Manager が影響のあるサーバをリブートすることは禁止できません。

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の [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 が、テーブル内のすべての保留中のアクティビティに対して [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 が、テーブル内にリストされている保留中のアクティビティに影響されるすべてのサーバをただちにリブートします。

第 32 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，525 ページ
- サーバ ID を継承するサービス プロファイル，526 ページ
- サービス プロファイル テンプレート，527 ページ
- サービス プロファイルに関するガイドラインおよび推奨事項，527 ページ
- サービス プロファイルの作成，528 ページ
- サービス プロファイル テンプレートの使用，532 ページ
- サービス プロファイルの管理，536 ページ
- サービス プロファイル テンプレートの管理，549 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、アソシエーション時にサーバに設定されたID値を上書きし、Cisco UCS Managerで設定されたリソース プールとポリシーを使用して一部の管理タスクを自動化できます。

このサービス プロファイルは、あるサーバとの関連付けを解除して、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。 UUID や MAC アドレスなど、新しいサーバの工場出荷時の設定は、サービスプロファイルでの設定で上書きされます。その結果、サーバ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、サーバプール資格情報ポリシー、または特定のハードウェア設定が必要な別のポリシーが含まれていない場合は、そのサービスプロファイルをCisco UCS ドメインのどのタイプのサーバにも使用できます。

これらのサービス プロファイルは、ラックマウント サーバまたはブレード サーバのどちらかに関連付けることができます。 サービス プロファイルの移行の可否は、サービス プロファイルの移行制限を選択するかどうかによって決まります。

（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。 これは特定のサーバに関連付けられているため、別のサーバへの移動や移行はできません。

このサービス プロファイルを使用するために、プールや設定ポリシーを作成する必要はありません。

このサービス プロファイルは、アソシエーション時に存在する次のような ID 情報および設定情報を継承し、適用します。

- 2 つの NIC の MAC アドレス
- 統合ネットワーク アダプタまたは仮想インターフェイス カードについては、2 つの HBA の WWN アドレス
- BIOS バージョン
- サーバの 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 テンプレートを使用して、vNIC や vHBA の個数などの同じ基本パラメータ、および同じプールから取得された ID 情報を使ってすばやく複数のサービス プロファイルを作成できます。

ヒント　既存のサービス プロファイルに類似した値を持つ 1 つのサービス プロファイルだけが必要な場合は、Cisco UCS Manager GUI でサービス プロファイルを複製できます。

たとえば、データベース ソフトウェアをホストするサーバの設定に、類似した値を持つ数個のサービスプロファイルが必要である場合、手動、または既存のサービスプロファイルから、サービス プロファイル テンプレートを作成できます。 その後、このテンプレートを使用して、サービス プロファイルを作成します。

Cisco UCS は、次のタイプのサービス プロファイル テンプレートをサポートしています。

初期テンプレート

初期テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承します。 初期のサービスプロファイルテンプレートから作成されたサービスプロファイルはテンプレートにバインドされます。 ただし、初期のテンプレートに対して行われた変更は、バインドされたサービス プロファイルに自動的に伝播されません。 バインドされたサービス プロファイルに変更を伝播したい場合は、そのサービス プロファイルをアンバインドしてから、再び初期テンプレートにバインドします。

アップデート テンプレート

アップデート テンプレートから作成されたサービス プロファイルはテンプレートのプロパティをすべて継承し、そのテンプレートへの接続をそのまま保持します。 アップデート テンプレートを変更すると、このテンプレートから作成されたサービス プロファイルが自動的にアップデートされます。

サービスプロファイルに関するガイドラインおよび推奨事項

サービス プロファイルまたはサービス プロファイル テンプレートに含まれるポリシー（ローカル ディスク設定ポリシーなど）やプールに固有のガイドラインと推奨事項に加え、以下のガイドラインと推奨事項にも留意する必要があります。これらの事項は、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します。

ラックマウント サーバで設定できる vNIC 数の制限

Cisco UCS Manager と統合されているラックマウント サーバでは、サポート対象のアダプタ（Cisco UCS P81E 仮想インターフェイス カード（N2XX-ACPCI01）など）ごとに最大 56 の vNIC を設定できます。

ラックマウント サーバの電力制限はサポート対象外

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ているサービス プロファイルに電力制御ポリシーを含めた場合、そのポリシーは実行されません。

vNIC に関する QoS ポリシーのガイドライン

QoS ポリシーのプライオリティ設定が fc（ファイバ チャネル システム クラス）ではない場合にのみ、そのポリシーを vNIC に割り当てることができます。 QoS ポリシーのプライオリティに他のシステム クラスを設定できます。

vHBA に関する QoS ポリシーのガイドライン

QoS ポリシーのプライオリティ設定が fc（ファイバ チャネル システム クラス）である場合にのみ、そのポリシーを vHBA に割り当てることができます。

QoS ポリシーのホスト制御設定は vNIC にのみ適用されます。 vHBA には影響しません。

サービス プロファイルの作成

[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 [Identify Service Profile] パネルで、サービス プロファイルの [Name]、[UUID assignment] を指定して、[Next] をクリックします。
このサービス プロファイルに任意で説明を設定できます。 UUID が使用できない場合、このパネルから UUID 接尾辞プールを作成することもできます。

（注） サービス プロファイルを手早く作成する場合は、名前を指定した後で [Finish] をクリックして構いません。 Cisco UCS Manager は、指定された名前とすべてのデフォルト値を使用して新しいサービス プロファイルを作成します。

ステップ 6 （任意）[Networking] パネルで、[Dynamic vNIC Connection Policy] と [LAN Connectivity] のセクションに必要な情報を指定して、[Next] をクリックします。
このパネルからダイナミック vNIC 接続ポリシーおよび LAN 接続ポリシーを作成できます。

ステップ 7 （任意）[Storage] パネルで、[Local Storage Policy]、[SAN Connectivity]、[WWNN]、[VSAN] などの、SAN 構成情報を指定して、[Next] をクリックします。
このパネルからローカル ディスク設定ポリシーおよび SAN 接続ポリシーを作成できます。

ステップ 8 （任意）[Zoning] パネルで、必要なゾーン分割情報を指定して [Next] をクリックします。
このパネルから vHBA イニシエータ グループを作成できます。

ステップ 9 （任意）[vNIC/vHBA Placement] パネルで、配置方法と PCI 順序を指定して [Next] をクリックします。
このパネルから配置ポリシーを作成できます。

ステップ 10 （任意）[Server Boot Order] パネルで、ドロップダウン リストから [Boot Policy] を指定して [Next] をクリックします。
このパネルからブート ポリシーを作成できます。

ステップ 11 （任意）[Maintenance Policy] パネルで、メンテナンス ポリシーを指定して [Next] をクリックします。
このパネルから、新しいメンテナンス ポリシーを作成してメンテナンス スケジュールを指定できます。

ステップ 12 （任意）[Server Assignment] パネルで、ドロップダウン リストから [Server Assignment] を、また、サーバ割り当てに適用する電源状態を指定して [Next] をクリックします。
このパネルからサーバ プールまたはホスト ファームウェア パッケージを作成できます。

ステップ 13 （任意）[Operational Policies] パネルで、[BIOS Configuration]、[External IPMI Management Configuration]、[Management IP Address]、[Monitoring Configuration(Thresholds)]、[Power Control Policy Configuration]、[Scrub Policy] などのシステムの動作情報を指定して [Finish] をクリックします。

（注） アウトバンド IPv4 アドレス、またはインバンドの IPv4 か IPv6 のアドレスをセットアップするには、それぞれのタブをクリックして、必須フィールドに値を入力します。

これらの各設定に必要なポリシーが見つからない場合は、このパネルで作成できます。

サーバ ID を継承するサービス プロファイルの作成

手順

ステップ 1 [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）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

b) [Description] フィールドに、このサービス プロファイルの説明を入力します。

ステップ 6 [Create Service Profile] ダイアログボックスの [vNICs] 領域で、プライマリおよびセカンダリの vNIC を選択します。

ステップ 7 [Create Service Profile] ダイアログボックスの [vHBAs] 領域で、プライマリおよびセカンダリの vHBA を選択します。

ステップ 8 [Create Service Profile] ダイアログボックスの [Boot Order] 領域で、プライマリおよびセカンダリのブート デバイスを選択します。

ステップ 9 （任意） [Server Association (optional)] 領域の [Select] カラムで、サーバのオプション ボタンをクリックして、このサービスとこのサーバを関連付けます。

ステップ 10 [OK] をクリックします。

ブレード サーバのハードウェア ベースのサービス プロファイルの作成

ハードウェア ベースの サービス プロファイルを別のサーバに移動することはできません。

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 リストから、サービス プロファイルを作成する組織を選択します。

b) 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

d) Cisco UCS Manager でサービス プロファイルの vNIC を作成する場合、[Create Default vNICs] チェックボックスをオンにします。

e) Cisco UCS Manager でサービス プロファイルの vHBA を作成する場合、[Create Default vHBAs] チェックボックスをオンにします。

f) [OK] をクリックします。

Cisco UCS Manager がサーバの ID および設定情報を継承して適用し、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 リストから、サービス プロファイルを作成する組織を選択します。

b) 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

d) Cisco UCS Manager でサービス プロファイルの vNIC を作成する場合、[Create Default vNICs] チェックボックスをオンにします。

e) Cisco UCS Manager でサービス プロファイルの vHBA を作成する場合、[Create Default vHBAs] チェックボックスをオンにします。

f) [OK] をクリックします。

Cisco UCS Manager がサーバの ID および設定情報を継承して適用し、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 テンプレートの使用

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 [Identify Service Profile Template] パネルで、サービス プロファイルの [Name]、[Type]、[UUID Assignment] を指定し、[Next] をクリックします。
このサービス プロファイル テンプレートの説明を任意に設定できます。

（注） サービス プロファイル テンプレートを手早く作成するには、名前を指定した後で、[Finish] をクリックして構いません。 Cisco UCS Manager は、指定された名前とすべてのシステム デフォルト値で新しいサービス プロファイル テンプレートを作成します。

ステップ 6 （任意）[Networking] パネルで、[Dynamic vNIC Connection Policy] と [LAN Connectivity] セクションに必要な情報を指定して、[Next] をクリックします。
このパネルからダイナミック vNIC 接続ポリシーおよび LAN 接続ポリシーを作成できます。

ステップ 7 （任意）[Storage] パネルで、SAN 構成情報（[Local Storage Policy]、[SAN Connectivity]、[WWNN]、[vHBAs] など）を指定して、[Next] をクリックします。
このパネルからローカル ディスク設定ポリシーおよび SAN 接続ポリシーを作成できます。

ステップ 8 （任意）[Zoning] パネルで、必要なゾーン分割情報を指定して [Next] をクリックします。
このパネルから vHBA イニシエータ グループを作成できます。

ステップ 9 （任意）[vNIC/vHBA Placement] パネルで、配置方法と PCI 順序を指定して [Next] をクリックします。
このパネルから配置ポリシーを作成できます。

ステップ 10 （任意）[Server Boot Order] パネルで、ドロップダウン リストから [Boot Policy] を指定して [Next] をクリックします。
このパネルからブート ポリシーを作成できます。

ステップ 11 （任意）[Maintenance Policy] パネルで、メンテナンス ポリシーを指定して [Next] をクリックします。
このパネルから、新しいメンテナンス ポリシーを作成してメンテナンス スケジュールを指定できます。

ステップ 12 （任意）[Server Assignment] パネルで、ドロップダウン リストの [Pool Assignment] と、割り当てに適用する電源状態からプールを指定して、[Next] をクリックします。
このパネルからサーバ プールまたはホスト ファームウェア パッケージを作成できます。

ステップ 13 （任意）[Operational Policies] パネルで、[BIOS Configuration]、[External IPMI Management Configuration]、[Management IP Address]、[Monitoring Configuration (Thresholds)]、[Power Control Policy Configuration]、[Scrub Policy] などのシステムの動作情報を指定して [Finish] をクリックします。

（注） アウトバンド IPv4 アドレス、またはインバンドの IPv4 か IPv6 のアドレスをセットアップするには、それぞれのタブをクリックして、必須フィールドに値を入力します。

これらの各設定に必要なポリシーが見つからない場合は、このパネルで作成できます。

サービス プロファイル テンプレートから 1 つ以上のサービス プロファイルの作成

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 プロファイルのベースとして使用するサービス プロファイル テンプレートを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 プロファイルの作成元となるサービス プロファイル テンプレートを右クリックし、[Create Service Profiles From Template] を選択します。

ステップ 5 [Create Service Profiles From Template] ダイアログボックスで、必要なフィールドに値を入力します。

ステップ 6 [OK] をクリックします。

ブレード サーバのテンプレート ベースのサービス プロファイルの作成

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) 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

c) ドロップダウンリストで、このサーバに関連付けるサービスプロファイルの作成元となるテンプレートを選択します。
（注） ドロップダウンリストには、選択したブレードサーバと互換性のあるサービスプロファイル テンプレートだけが表示されます。

d) [OK] をクリックします。

ラックマウント サーバのテンプレート ベースのサービス プロファイルの作成

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) 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）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

c) ドロップダウンリストで、このサーバに関連付けるサービス プロファイルの作成元となるテンプレートを選択します。

d) [OK] をクリックします。

サービス プロファイルからのサービス プロファイル テンプレートの作成

手順

ステップ 1 [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、必須フィールドに値を入力します。

ステップ 6 [OK] をクリックします。

サービス プロファイルの管理

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）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービス プロファイルおよびサービス プロファイル テンプレートで一意であることが必要です。

この名前は、サービスプロファイルを作成する組織またはサブ組織内で一意である必要があります。

b) [OK] をクリックします。

ステップ 6 作成したサービス プロファイルに移動し、すべてのオプションが正しいことを確認します。

サービス プロファイルとサーバまたはサーバ プールの関連付け

作成時にサービスプロファイルとブレードサーバまたはサーバプールを関連付けなかった場合、またはサービス プロファイルを関連付けるブレード サーバまたはサーバ プールを変更する場合には、次の手順を実行します。

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 新しいサーバまたはサーバプールに関連付けるサービスプロファイルが含まれている組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 サーバに関連付けるサービス プロファイルを右クリックし、[Associate Service Profile] をします。

ステップ 5 [Associate Service Profile] ダイアログボックスで、次のいずれかのオプションを選択します。

オプション	説明
サーバ プール	ドロップダウン リストからサーバ プールを選択します。 Cisco UCS Manager で、サービス プロファイルにこのプールのサーバ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 ツリーで適切な使用可能サーバに移動し、サービス プロファイルに割り当てるサーバを選択します。 ステップ 7 に進みます。
Custom Server	サービスプロファイルに割り当てられるサーバが含まれるシャーシおよびスロットを指定します。 サーバがスロット内に存在しない場合、またはそれ以外の理由で使用できない場合、サービスプロファイルは、サーバが使用できるようになったらサーバに関連付けられます。 ステップ 6 に進みます。

ステップ 6 [Custom Server] を選択した場合は、次の手順を実行します。

a) [Chassis Id] フィールドに、選択したサーバが配置されるシャーシの番号を入力します。

b) [Server Id] フィールドで、選択したサーバが配置されているスロットの番号を入力します。

ステップ 7 サー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。

サービス プロファイルとサーバまたはサーバ プールの関連付け解除

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。 ある程度の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 サーバまたはサーバプールとの関連付けを解除するサービスプロファイルが含まれる組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 サーバとの関連付けを解除するサービスプロファイルを右クリックし、[Disassociate Service Profile] を選択します。

ステップ 5 [Disassociate Service Profile] ダイアログボックスで、[Yes] をクリックしてサービス プロファイルの関連付けを解除することを確認します。

ステップ 6 （任意） サーバのステータスおよび有限状態マシン（FSM）をモニタして、アソシエーションの解除が完了したことを確認します。

サービス プロファイルからのインバンド設定の削除

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

手順

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

ステップ 2 [Servers] タブの [Servers] > [Service Profiles] > *[Service_Profile_Name]* を展開します。

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

ステップ 4 [Actions] 領域で、[Delete Inband Configuration] をクリックします。

ステップ 5 [Delete] の確認ダイアログボックスで [Yes] をクリックします。
サービス プロファイルのインバンド管理 IP アドレスの設定が削除されます。

サービス プロファイルの名前の変更

サービス プロファイルの名前を変更すると、次のことが起こります。

- サービス プロファイルの以前の名前を参照するイベント ログと監査ログは、その名前のまま保持されます。
- 名前変更の操作を記録する、新しい監査データが作成されます。

- サービス プロファイルの以前の名前で生じたすべての障害データは、新しいサービス プロファイル名に転送されます。

（注） 保留中の変更があるサービス プロファイルの名前は変更できません。

手順

ステップ 1 [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 プロファイルを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 名前を変更するサービス プロファイルをクリックします。

ステップ 5 [Work] ペインの [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で、[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）は使用できますが、それ以外の特殊文字とスペースは使用できません。この名前は、同じ組織内のすべてのサービスプロファイルおよびサービスプロファイル テンプレートで一意であることが必要です。

ステップ 8 [OK] をクリックします。

サービス プロファイルの 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 を変更したいサービス プロファイルを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 関連付けられたサーバの UUID を変更する必要のあるサービス プロファイルを選択します。

ステップ 5 [Work] ペインの [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。
	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。
	手動で割り当てる UUID を使用します。 ステップ 8 に進みます。
Pools *Pool_Name*	ドロップダウン リストの下部のリストから選択する UUID 接尾辞プールから UUID を割り当てます。 各プール名の後には、プール内で利用可能な UUID の数および UUID の合計数を示す、括弧に囲まれた 2 つの数字が表示されます。 ステップ 9 に進みます。

ステップ 8 （任意） オプションを選択した場合は、次の手順を実行します。

a) [UUID] フィールドに、このサービス プロファイルを使用するサーバに割り当てる有効な UUID を入力します。

b) 選択した UUID が使用可能であることを確認するには、[here] リンクをクリックします。

ステップ 9 [OK] をクリックします。

サービス プロファイルのブート順序の変更

手順

ステップ 1 [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 プロファイルを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 ブート順序を変更するサービス プロファイルをクリックします。

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

ステップ 6 [Modify Boot Policy] をクリックして既存のブート ポリシーを変更します。

ステップ 7 [Modify Boot Policy] ダイアログボックスで、[Boot Policy] ドロップダウン リストから次のいずれかを選択します。

オプション	説明
Select Boot Policy to use	このサービス プロファイルにデフォルトのブート ポリシーを割り当てます。 ステップ 14 に進みます。
Create a Specific Boot Policy	このサービス プロファイル テンプレートだけがアクセスできるローカル ブート ポリシーを作成できます。 ステップ 8 に進みます。
[Boot Policies *Policy_Name*]	サービス プロファイルに既存のブート ポリシーを割り当てます。 このオプションを選択した場合、Cisco UCS Manager でポリシーの詳細が表示されます。 既存のポリシーを使用するのではなく、すべてのサービス プロファイルがアクセスできるポリシーを作成する場合は、[Create Boot Policy] をクリックし、ステップ 2 に進みます。 それ以外の場合はステップ 14 に進みます。

ステップ 8 ブート ポリシーの作成を選択した場合は、[Create Boot Policy] ダイアログボックスにポリシーの一意の名前と説明を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、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 ポリシーについて選択されており、CD-ROM またはフロッピーがブート順の最後のデバイスの場合に、デバイスを取り外すか、装着すると、ブート順に直接効力がなく、サーバが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オンにします。

- オンにした場合、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た 1 つ以上の vNIC、vHBA、iSCSI、vNIC がサーバ プロファイル内のサーバ設定に一致するかどうかをレポートします。
- オフにした場合、Cisco UCS Manager は、サービス プロファイルから（ブート オプションに応じて）vNIC、vHBA、iSCSI、または vNIC を使用します。

ステップ 11 ローカルディスク、仮想CD-ROM、または仮想フロッピーをブート順序に追加するには、次の手順を実行します。

a) 下矢印をクリックして [Local Devices] 領域を展開します。

b) 次のリンクのいずれかをクリックして、デバイスを [Boot Order] テーブルに追加します。

- [Add Local Disk] または
  - Add Local LUN
  - Add SD Card
  - Add Internal USB
  - Add External USB
- [Add CD/DVD] または
  - Add Local CD/DVD
  - Add Local Remote CD/DVD

c) 別のブート デバイスを [Boot Order] テーブルに追加するか、[OK] をクリックして作業を終了します。

ステップ 12 LAN ブートをブート順序に追加するには、次の手順を実行します。

a) 下矢印をクリックして [vNICs] 領域を展開します。

b) [Add LAN Boot] リンクをクリックします。

c) **[Add LAN Boot]** ダイアログボックスで、LAN ブートに使用する vNIC の名前を [vNIC] フィールドに入力して、[OK] をクリックします。

d) 別のデバイスを [Boot Order] テーブルに追加するか、[OK] をクリックして作業を終了します。

ステップ 13 SAN ブートをブート順序に追加するには、次の手順を実行します。

a) 下矢印をクリックして [vHBAs] 領域を展開します。

b) [Add SAN Boot] リンクをクリックします。

c) [Add San Boot] ダイアログ ボックスで、vHBA とタイプを指定して、[OK] をクリックします。

d) この vHBA がブート可能な SAN イメージを参照する場合は [Add SAN Boot Target] リンク をクリックし、[Add SAN Boot Target] ダイアログボックス で、ブート ターゲット LUN、ブート ターゲット WWPN、およびタイプを指定して、[OK] をクリックします。

e) 別のブート デバイスを [Boot Order] テーブルに追加するか、[OK] をクリックして作業を終了します。

ステップ 14 [OK] をクリックします。

サービス プロファイル用の vNIC の作成

手順

ステップ 1 [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、必須フィールドに値を入力します。
ステップ 7 [OK] をクリックします。

サービス プロファイルからの 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、必須フィールドに値を入力します。
ステップ 7 [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、必須フィールドに入力します。
ステップ 9 [OK] をクリックします。

vHBA の永続的なバインディングのクリア

手順

ステップ 1 [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 プロファイルを含む組織のノードを展開します。

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

ステップ 3 vHBA イニシエータ グループを追加するサービス プロファイルを選択します。

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

ステップ 5 [Select vHBA Initiator Groups] テーブルテーブルの右のアイコン バーで、[+] をクリックします。

ステップ 6 [Create vHBA Initiator Group] ダイアログ ボックスで、名前と説明を設定するには、次のフィールドに入力します。

名前	説明
[Name] フィールド	vHBA イニシエータ グループの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、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。次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 7 [Select vHBA Initiators][Select vHBA Initiators] テーブルテーブルで、vHBA イニシエータ グループに含める各 vHBA の [Select] 列のチェック ボックスをオンにします。

ステップ 8 イニシエータ グループにストレージ接続ポリシーを追加するには、次のオプションの 1 つを選択します。

- [Storage Connection Policy] ドロップダウン リストドロップダウン リストから既存のストレージ接続ポリシーを選択します。 ステップ 10 に進みます。
- Cisco UCS ドメイン内の他の vHBA のイニシエータ グループで使用可能な新しいストレージ接続ポリシーを作成する場合は、[Create Storage Connection Policy] リンクのリンクをクリックします。 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, （338 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後、ステップ 10 に進みます。
- この vHBA のイニシエータ グループにのみ利用可能なストレージ接続ポリシーを作成するには、[Specific Storage Connection Policy] オプションオプションを選択します。 ステップ 9 に進みます。

ステップ 9 この vHBA のイニシエータ グループにのみ利用可能なストレージ接続ポリシーを作成するには、[Specific Storage Connection Policy] 領域領域で、次のフィールドを入力します。

名前	説明
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。
[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、vHBA とストレージポートの組み合わせごとに1つのゾーンを自動作成します。各ゾーンには2つのメンバが含まれます。ゾーンの数がサポートされる最大数を超える見込みがない場合は、このタイプのゾーン分割を設定することをお勧めします。 • [Single Initiator Multiple Targets]：Cisco UCS Manager は、vHBA ごとに 1 つゾーンを自動作成します。 ゾーンの数がサポートされている最大値に到達またはそれを超えると予想される場合は、このタイプのゾーン分割を設定することを推奨します。
[FC Target Endpoints] テーブル	このポリシーに関連付けられたファイバ チャネル ターゲット エンドポイント このテーブルには、次のカラムとボタンがあります。 • [WWPN] カラム：エンドポイントに関連付けられたワールド ワイド ポート名。 • [Path] カラム：エンドポイントへのパス。 • [VSAN] カラム：エンドポイントに関連付けられた VSAN。 • [Add] ボタン：新しい FC ターゲット エンドポイントを作成します。 • [Delete] ボタン：選択したエンドポイントを削除します。 • [Properties] ボタン：選択したエンドポイントのすべてのプロパティを表示します。

ステップ 10 [OK] をクリックします。

ステップ 11 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した場合、Cisco UCS Manager により、サービス プロファイル テンプレートで定義された値を使ってサービス プロファイルが設定されます。既存のサービスプロファイル設定がテンプレートと一致しない場合、Cisco UCS Manager により、サービス プロファイルが再設定されます。 バインドされたサービス プロファイルの設定は、関連付けられたテンプレートを使用してのみ変更できます。

手順

ステップ 1 [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*] を展開します。
ステップ 3 削除するサービス プロファイルを右クリックし、[Delete] を選択します。
ステップ 4 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

サービス プロファイル テンプレートとサーバ プールの関連付け

作成時にサービス プロファイル テンプレートとサーバ 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 プールからのサービス プロファイル テンプレートの関連付け解除

手順

ステップ 1 [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 テンプレートを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 UUID 割り当てを変更するサービス プロファイル テンプレートを選択します。

ステップ 5 [Work] ペインの [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 リストから、次のいずれかを選択します。

オプション	説明
Select (pool default used by default)	デフォルトの UUID 接尾辞プールから UUID を割り当てます。
	製造元によってサーバに割り当てられた UUID を使用します。 このオプションを選択した場合、UUID はサービス プロファイルがサーバと関連付けられるまで割り当てられません。 この時点で、UUID は製造元によってサーバに割り当てられた UUID 値に設定されます。 サービス プロファイルを後で別のサーバに移動すると、UUID は新しいサーバに一致するように変更されます。
Pools *Pool_Name*	ドロップダウン リストの下部のリストから選択する UUID 接尾辞プールから UUID を割り当てます。 各プール名の後には、プール内で利用可能な UUID の数および UUID の合計数を示す、括弧に囲まれた 2 つの数字が表示されます。

ステップ 8 [OK] をクリックします。

サービス プロファイルに割り当てられた UUID の、サービス プロファイル テンプレートのプールからのリセット

更新中のサービス プロファイル テンプレートに割り当てられている UUID サフィックス プールを変更しても、Cisco UCS Manager により、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 UUID は変更されません。 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 が含まれている。
- UUID 接尾辞プール名がサービス プロファイルで指定されている。 たとえば、プール名が空でない場合です。
- UUID の値が 0 でない（サーバ ハードウェアに由来しない）。

手順

ステップ 1 [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、Cisco UCS Manager より、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] の順に展開します。

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、Cisco UCS Manager により、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 WWPN は変更されません。 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。

サービス プロファイル テンプレートからのインバンド設定の削除

この手順では、サービス プロファイル テンプレートからインバンド管理 IP アドレスの設定を削除します。 このアクションがグレー表示されている場合、インバンド設定は設定されていません。

手順

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

ステップ 2 [Servers] タブの [Servers] > [Service Profile Template] > *[Service_Profile_Template_Name]* を展開します。

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

ステップ 4 [Actions] 領域で、[Delete Inband Configuration] をクリックします。

ステップ 5 [Delete] の確認ダイアログボックスで [Yes] をクリックします。
サービス プロファイル テンプレートのインバンド管理 IP アドレスの設定が削除されます。

次の作業

第 33 章

Cisco UCS での電源管理

この章の内容は、次のとおりです。

- Cisco UCS での電源管理，555 ページ
- ラック サーバの電源管理，555 ページ
- 電源管理の注意事項，556 ページ
- 電源ポリシーの設定，556 ページ
- グローバル電力割り当てポリシーの設定，557 ページ
- グローバル電力プロファイリング ポリシーの設定，558 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，559 ページ
- 手動ブレード レベル電力制限の設定，566 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で、Cisco UCS Manager で電源を管理できます。

- Cisco UCS ドメイン内のすべてのシャーシの電源冗長性
- ポリシー方式のシャーシ レベルの電力制限
- 手動によるブレード レベルの電力制限

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

電源ポリシーの設定

電源ポリシー

電源ポリシーは、Cisco UCS ドメイン内のすべてのシャーシに電源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 つ加えた数です。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。 さらに電源装置を取り付けた場合、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。オンにならない場合は、シャーシに N+1 よりも高い冗長性が必要です。 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。

グローバル電力割り当てポリシーの設定

グローバル電力割り当てポリシー

グローバル電力割り当てポリシーは、ポリシー方式のシャーシ グループ電力制限または手動によるブレード レベル電力制限のいずれを、シャーシ内のすべてのサーバに適用するか指定するグローバル ポリシーです。

デフォルトの電力割り当て方法である、ポリシー方式のシャーシ グループ電力制限を使用することを推奨します。

重要 手動によるブレード レベル電力割り当ての設定に変更を加えると、ポリシー方式のシャーシ グループ電力割り当てで設定されたグループや設定オプションが失われます。

グローバル電力割り当てポリシーの設定

手順

ステップ 1 [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 Power Allocation Policy] 領域で、Cisco UCS ドメインで使用される電力制限管理モードを設定するために [Cap Policy][Allocation Method] フィールドフィールドの以下のオプション ボタンから 1 つをクリックします。

- [Manual Blade Level Cap]：電力割り当ては、すべてのシャーシの個々のブレード サーバに設定されます。 このオプションを選択した場合、電源グループは作成できません。

- [Policy Driven Chassis Group Cap]：電力割り当ては、関連付けられたサービス プロファイルに含まれる電力制御ポリシーによって、シャーシ レベルで設定されます。 このオプションを選択すると、Cisco UCS ドメインに 1 つ以上のシャーシを含む電源グループを作成できます。

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

ステップ 6 [Save Changes] をクリックします。

グローバル電力プロファイリング ポリシーの設定

グローバル電力プロファイリング ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope power-cap-mgmt**	電力制限管理モードを開始します。
ステップ 2	UCS-A /power-cap-mgmt # **set profile-policy** {**no** | **yes**}	電力プロファイリング ポリシーをイネーブル化またはディセーブル化します。
ステップ 3	UCS-A /power-cap-mgmt # **commit-buffer**	トランザクションをシステムの設定にコミットします。

次の例で、グローバル電力プロファイリング ポリシーをイネーブルにし、トランザクションをコミットする方法を示します。

```
UCS-A# scope power-cap-mgmt
UCS-A /power-cap-mgmt # set profile-policy yes
UCS-A /power-cap-mgmt* # commit-buffer
UCS-A /power-cap-mgmt #
```

グローバル電力プロファイル ポリシーの設定

手順

ステップ 1 [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 Power Profile Policy] 領域で、グローバル電力プロファイル ポリシーをイネーブルにする [Profile Power] チェックボックスをオンにします。

ステップ 6 [Save Changes] をクリックします。

ポリシー方式のシャーシ グループの電力制限の設定

ポリシー方式のシャーシ グループの電力制限

グローバル制限ポリシーでポリシー方式の電源シャーシ グループ電力制限を選択すると、費用のかかる電力障害のリスクを冒すことなく、Cisco UCS で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、二重のプロセスによって実現されます。 シャーシ レベルでは、Cisco UCS は使用可能な電力量を電源グループのメンバに分配します。ブレード レベルでは、シャーシに割り当てられた電力量が優先順位に基づいてブレードに分配されます。

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

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

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

電源グループの設定

電源グループ

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

シャーシ レベルの電力制限を設定するには、以下が必要です。

- IOM、CIMC、および BIOS バージョン 1.4 以上
- 2 台の PSU

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

最低 AC 1556 ワットが各シャーシに設定されます。 これは、満載したシャーシに電源を供給するために必要な最低電力量である DC 電力 1400 ワットに変換されます。

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

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

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

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

エラー メッセージ	Cause	推奨処置
`Insufficient budget for power group POWERGROUP_NAME`	このメッセージは、シャーシに電力制限を割り当てる際に最小限度を満たしていない場合に表示されます。	電力制限を AC 1556 ワット（DC 1400 ワット）以上に増加します。

エラー メッセージ	Cause	推奨処置
`Insufficient power available to discover server Chassis ID/BladeID`	このメッセージは、新しいブレードの導入時にブレードの検出に使用可能なブート電力が不十分な場合に表示されます。	次のいずれかを実行して、電源バジェットを再度割り当てることができます。 • 電源グループ内のシャーシまたはブレードを削除または解放します。 • グループの電源バジェットを増加します。 • 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。

電源グループの作成

はじめる前に

グローバル電力割り当てポリシーが [Global Policies] タブで [Policy Driven Chassis Group Cap] に設定されていることを確認します。

手順

ステップ 1 [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) 電源グループの一意の名前および説明を入力します。
この名前には、1 ～ 16 文字の英数字を使用できます。-（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。

b) [Next] をクリックします。

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

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

b) 電源グループに含まれるすべてのシャーシを表示する [Selected Chassis] テーブルにシャーシを追加するには、[>>] ボタンをクリックします。
電源グループから 1 つ以上のシャーシを除外するには、[<<] ボタンを使用します。

c) [Next] をクリックします。

ステップ 8 [Create Group Wizard] の [Power Group Attributes] ページで、次の手順を実行します。

a) 次のフィールドに入力します。

名前	説明
[Power Cap] フィールド	電源グループで使用可能な最大ピーク時電力（W）。 0 ～ 10000000 の整数を入力します。
[Enable Dynamic Reallocation] フィールド	次のいずれかになります。 • [Chassis]：Cisco UCS は電力消費量をモニタし、電力使用量の最大化に適合するようにブレードの割り当てを変更します。 • [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。

電源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] ペインで、[Power Groups] タブをクリックします。

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

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

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

b) 電源グループに含まれるすべてのシャーシを表示する [Selected Chassis] テーブルにシャーシを追加するには、[>>] ボタンをクリックします。
電源グループから 1 つ以上のシャーシを除外するには、[<<] ボタンを使用します。

c) [OK] をクリックします。

電源グループからのシャーシの削除

手順

ステップ 1 [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] ペインで、[Power Groups] タブをクリックします。
ステップ 4 シャーシを削除する電源グループを展開します。
ステップ 5 電源グループから削除するシャーシを右クリックし、[Delete] を選択します。
ステップ 6 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。

電源グループの削除

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] ペインで、[Power Groups] タブをクリックします。
ステップ 4 削除する電源グループを右クリックして、[Delete] を選択します。
ステップ 5 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。

電源制御ポリシーの設定

電源制御ポリシー

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

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

ミッション クリティカルなアプリケーションには、no-cap という特殊な優先順位も使用できます。 優先順位を no-cap に設定すると、Cisco UCS が特定のサーバの未使用電力を利用するのを回避できます。この設定を行うと、サーバタイプに対して許可されている最大の電力容量がサーバに割り当てられます。

（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
[名前] フィールド	ポリシーの名前。 この名前には、1 ～ 16 文字の英数字を使用できます。 -（ハイフン）、_（アンダースコア）、:（コロン）、および .（ピリオド）は使用できますが、それ以外の特殊文字とスペースは使用できません。また、オブジェクトが保存された後で、この名前を変更することはできません。
[説明] 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。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

名前	説明
[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。
[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

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

電力制御ポリシーの削除

手順

ステップ 1 [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 レベル電力制限の設定

手動によるブレード レベルの電力制限

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

次の設定オプションを使用できます。

イネーブル

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。

ディセーブル

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が瞬間的に上昇し、設定されている最大値以上になった場合でも、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 は、サーバにとって適切な量まで電力を低減します。 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） 手動によるブレード レベル電力制限は、[Equipment] > [Policies] > [Global Policies] > [Global Power Allocation Policy] の順に設定します。電力制御ポリシーで設定された優先順位は関係ありません。

サーバのブレード レベル電力制限の設定

はじめる前に

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

手順

ステップ 1 [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) 見出しの右側の [Expand] アイコンをクリックしてフィールドを表示します。

b) 次のフィールドに入力します。

名前	説明
[Admin Status] フィールド	このサーバが電力制限されているかどうか。 次のいずれかになります。 • [Unbounded]：どのような場合でもサーバは電力制限されません。 • [Enabled]：Cisco UCS Manager GUI に [Watts] フィールドが表示されます。 （注） 電力制限は、要求を満たす十分な電力がシャーシにない場合にのみ有効になります。 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	要求を満たす十分な電力がシャーシにない場合に、サーバが使用できる最大ワット数です。 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 次のどちらかを実行します。

- 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 34 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，569 ページ
- 時間帯の設定，569 ページ
- NTP サーバの追加，570 ページ
- NTP サーバの削除，570 ページ

タイム ゾーン

Cisco UCS では、Cisco UCS Manager で正しい時刻を表示するために、ドメイン固有のタイムゾーン設定と NTP サーバが必要です。 これらの両方を Cisco UCS ドメインに設定しないと、時間が正確に表示されません。

時間帯の設定

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、ユーザがこの Cisco UCS ドメインに使用する NTP サーバの IPv4 または IPv6 のアドレス、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 35 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 のシャーシ管理，571 ページ
- シャーシの削除および解放に関するガイドライン，571 ページ
- シャーシの確認，572 ページ
- シャーシの稼働中止，573 ページ
- シャーシの削除，573 ページ
- 単一シャーシの再稼動，573 ページ
- 複数のシャーシの再稼動，574 ページ
- シャーシの番号付け直し，575 ページ
- ロケータ LED の切り替え，576 ページ
- ヘルス LED アラーム，576 ページ
- シャーシの POST 結果の表示，578 ページ

Cisco UCS Manager GUI のシャーシ管理

Cisco UCS Manager GUI によって Cisco UCS ドメインのすべてのシャーシを管理および監視できます。

シャーシの削除および解放に関するガイドライン

Cisco UCS Manager を使ってシャーシを削除するか解放するかを決定する場合は、次のガイドラインを考慮してください。

シャーシの稼働中止

解放は、シャーシが物理的に存在し接続しているときに、一時的に設定から削除する場合に実行します。 解放されたシャーシは最終的に再稼働することが予測されるので、シャーシの情報部分は、将来の使用に備え、Cisco UCS Manager によって保持されます。

シャーシの削除

削除は、システムから物理的にシャーシを削除する（取り外す）場合に実行します。 シャーシの物理的な削除が完了した後、その設定を Cisco UCS Manager から削除できます。

（注） シャーシが物理的に存在し接続しているときは、Cisco UCS Manager から削除できません。

削除したシャーシを再び設定に追加する場合は、それを再び接続して検出する必要があります。再検出時、Cisco UCS Manager によって以前の ID とは異なる新しい ID がシャーシに割り当てられます。

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

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 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動

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 再稼動するシャーシについて、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] フィールドに、シャーシに割り当てる ID を入力するか、矢印を使用して選択します

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はシャーシディスカバリ 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動

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動する場合、シャーシに番号を付け直すことはできません。 Cisco UCS Manager はシャーシに前と同じ 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 再稼動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はシャーシディスカバリ 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。

シャーシの番号付け直し

（注） Cisco UCS Manager を通じたブレード サーバの番号の再設定はできません。 ブレード サーバに割り当てられる ID は、シャーシ内のその物理スロットで決まります。 ブレード サーバの番号を再設定するには、サーバをシャーシ内の別のスロットに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、まず両方のシャーシを解放し、シャーシ解放 FSM が完了するのを待ってから、番号の再設定手順に進みます。

手順

ステップ 1 [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] ノードに以下が含まれていないことを確認してください。

- 番号を付け直すシャーシ
- 使用する番号を持つシャーシ

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、これらのシャーシを解放します。 続行前に、解放 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。 これには数分かかる場合があります。

ステップ 4 [Equipment] タブで [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 番号を付け直すシャーシについて、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] フィールドに、シャーシに割り当てる ID を入力するか、矢印を使用して選択します

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。

ヘルス LED アラーム

ブレード ヘルス LED は、各 Cisco UCS B シリーズ ブレード サーバの前面にあります。 Cisco UCS Manager では、センサー故障が発生すると、ブレード ヘルス LED が緑色からオレンジ色またはオレンジ色の点滅に変化します。

ヘルス LED アラームには次の情報が表示されます。

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

ヘルス LED アラームの表示

手順

ステップ 1 [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 ヘルス LED アラーム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、[View Health LED Alarms] をクリックします。
[View Health LED Alarms] ダイアログボックスに、選択したサーバのヘルス LED アラームが一覧表示されます。

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

ヘルス LED ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *chassis-id* / *blade-id*	指定サーバのシャーシ サーバ モードを開始します。
ステップ 2	UCS-A /chassis/server # **show health-led expand**	選択したサーバのヘルス LED およびセンサー アラームを表示します。

次の例では、シャーシ 1 サーバ 1 のヘルス LED ステータスとセンサー アラームを表示する方法を示します。

```
UCS-A# scope server 1/1
UCS-A /chassis/server # show health-led
Health LED:
    Severity: Minor
    Reason:: P0V75_STBY:Voltage Threshold Crossed;TEMP_SENS_FRONT:Temperature Threshold
Crossed;
    Color: Amber
    Oper State:: On

    Sensor Alarm:
        Severity: Minor
        Sensor ID: 7
        Sensor Name: P0V75_STBY
        Alarm Desc: Voltage Threshold Crossed

        Severity: Minor
        Sensor ID: 76
        Sensor Name: TEMP_SENS_FRONT
        Alarm Desc: Temperature Threshold Crossed

        Severity: Minor
        Sensor ID: 91
        Sensor Name: DDR3_P1_D2_TMP
        Alarm Desc: Temperature Threshold Crossed

UCS-A /chassis/server #
```

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 36 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，582 ページ
- ブレード サーバの削除および解放に関するガイドライン，583 ページ
- 予期しないサーバ電力変更を回避するための推奨事項，584 ページ
- ブレード サーバのブート，585 ページ
- ブレード サーバのシャット ダウン，587 ページ
- ブレード サーバのリセット，588 ページ
- ブレード サーバの再確認，589 ページ
- シャーシからのサーバの削除，590 ページ
- ブレード サーバからのインバンド設定の削除，590 ページ
- ブレード サーバの解放，591 ページ
- ブレード サーバの再稼動，592 ページ
- シャーシ内のサーバ スロットの再確認，592 ページ
- 存在しないブレード サーバの設定データベースからの削除，593 ページ
- ブレード サーバのロケータ LED の切り替え，593 ページ
- ブレード サーバの CMOS のリセット，594 ページ
- ブレード サーバの CIMC のリセット，594 ページ
- ブレード サーバの破損した BIOS の復旧，595 ページ
- ブレード サーバの POST 結果の表示，596 ページ
- ブレード サーバからの NMI の発行，596 ページ
- ヘルス LED アラーム，597 ページ

• ヘルス LED アラームの表示，597 ページ

ブレード サーバ管理

Cisco UCS Manager を使用して Cisco UCS ドメインのすべてのブレード サーバを管理および監視できます。 電源状態の変更など一部のブレード サーバ管理タスクは、サーバおよびサービス 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、スロットを再認識させることもできます。

Cisco UCS B460 M4 ブレード サーバの管理

Cisco UCS B460 M4 ブレード サーバは、Cisco UCS 拡張コネクタで接続された 2 台の Cisco UCS B260 最大幅ブレード サーバから構成されています。 各ブレード サーバはノードと呼ばれ、マスター ノードまたはスレーブ ノードになることができます。

各 Cisco UCS B460 M4 ブレード サーバには 2 つの異なるノードが存在するため、以下について注意する必要があります。

- マスター ノードは常に、最も大きな番号が付いたスロットのノードです。
- Cisco UCS B460 ブレード サーバが Cisco UCS Manager で参照される際は、マスターのスロット番号が参照されます。
- Cisco UCS B460 M4 ブレード サーバから Cisco UCS 拡張コネクタを取り外すと、Cisco UCS Manager GUI の [Physical Display] 領域に、両方のマスター ノード スロットと両方のスレーブ ノード スロットに [Needs Resolution] が表示されます。
- ヘルス LED には、マスター ノードとスレーブ ノードの個々の状態、および両方のノードを組み合せた状態が表示されます。 複合ヘルス LED には常に、最も状態が悪いノードのステータスが表示されます。 ヘルス LED アラームは個別に表示されます。
- Cisco UCS Manager GUI では、マスターまたはスレーブ ノードのロケータ LED のオン/オフを切り替えることができます。 Cisco UCS Manager CLI では、ロケータ LED のオン/オフを個々に切り替えるか、両方のロケータ LED のオン/オフを同時に切り替えることができます。
- Cisco UCS B460 M4 ブレード サーバに対する電力制限はサーバ レベルで適用され、各ノードは合計値の 2 分の 1 に制限されます。
- ファームウェアを更新すると、マスターとスレーブ ノードの両方が同時に更新されます。個々のノードのファームウェアは更新できません。
- ローカル ディスク構成はマスター ノードでのみサポートされます。

- Cisco UCS B460 ブレード サーバは、マスターまたはスレーブ ノードによって生成された SEL ログを区別しません。 ログは同じページに表示され、スロット番号で区別されます。
- Cisco UCS Manager GUI では、[Storage] タブの [Local Disk Configuration Policy] と [Actual Disk Configurations] 領域に、Cisco UCS B460 ブレード サーバのマスター ノードのデータだけが表示されます。 スレーブ ノード用のフィールドは表示されません。

Cisco UCS B460 M4 ブレード サーバへのアップグレード

Cisco UCS B260 M4 ブレード サーバがある場合、アップグレード キットを購入して Cisco UCS B460 M4 ブレード サーバにすることができます。 詳細については、該当の『*Cisco UCS Hardware Installation Guide*』を参照してください。

はじめる前に

2 台の Cisco UCS B260 M4 ブレード サーバと Cisco UCS スケーラビリティ コネクタが必要です。

手順

ステップ 1 既存の Cisco UCS B260 M4 ブレード 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ことを確認します。

ステップ 2 1 台目のブレード サーバの上か下のシャーシに 2 台目の Cisco UCS B260 M4 ブレード サーバを挿入します。

（注） 2 台目のブレード サーバに Cisco UCS スケーラビリティ ターミネータが付いていない場合は、1 台目のブレード サーバのターミネータを使用します。

ステップ 3 両方の Cisco UCS B260 M4 ブレード サーバを停止させます。

ステップ 4 ファームウェアを同期させます。
自動的に新しいサーバを更新するには、UCSCisco UCS Manager の [Firmware Auto Sync Server] ポリシーを使用します。 詳細については、適切な『*Cisco UCS B-Series Firmware Management Guide*（*Cisco UCS B* シリーズのファームウェアの管理ガイド）』を参照してください。

ステップ 5 Cisco UCS スケーラビリティ コネクタを Cisco UCS スケーラビリティ ターミネータで置き換えます。
スロットのプレゼンスはミスマッチに変わりますが、検出はトリガーされません。

ステップ 6 新しい Cisco UCS B460 M4 ブレード サーバを再認識します。

ブレードサーバの削除および解放に関するガイドライン

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

ブレード サーバの解放

解放は、ブレード サーバが物理的に存在し接続しているときに、一時的に設定から削除する場合に実行します。解放された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ので、サーバの情報部分は、将来の使用に備え、Cisco UCS Manager によって保持されます。

ブレード サーバの削除

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

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

（注） 自動的に削除されるのは、検出時に自動的にサーバ プールに追加されたサーバだけです。 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 サーバを再び設定に追加する場合は、それを再び接続して検出する必要があります。 Cisco UCS Manager に再導入したサーバは、新しいサーバとして処理され、詳細な検出プロセスが実施されます。 このため、Cisco UCS Manager によって以前とは異なる新しい ID がサーバに割り当てられることがあります。

予期しないサーバ電力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は、サーバの物理的な [Power] 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、サーバの電源状態の変更は次の方法でのみ行う必要があります。

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

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

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

現在電源がオフになっているサーバに対して、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、サーバの実際の電力状態がサービス プロファイルで必要とされる電源状態の設定と同期しなくなる可能性があります。 サーバと 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 によって、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場合があり、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	通信が中断された後のサーバの電源状態
Up	Powered Off	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 プロファイルに必要とされる電源状態に関係なくシャットダウンされません。

ブレード サーバのブート

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 システムにより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 システムにより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） 電源切断状態からサーバをブートする場合は、[Reset] を使用しないでください。

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

Cisco UCS Manager はサーバの接続を解除し、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、[Decommission] をクリックし、[OK] をクリックします。
サーバが Cisco UCS の設定から削除されます。

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、スロットを再認識して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

詳細については、シャーシ内のサーバ スロットの再確認, （592 ページ）を参照してください。

ブレード サーバからのインバンド設定の削除

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

手順

ステップ 1 [Navigation] ペインの [Servers] 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 Name]* を展開します。

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

ステップ 4 [CIMC] サブタブをクリックします。

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

ステップ 6 [Delete] の確認ダイアログボックスで [Yes] をクリックします。
サーバのインバンド設定が削除されます。

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

ブレード サーバの解放

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 の設定から削除されます。

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、スロットを再認識して、Cisco UCS Manager にこのサーバを再検出させる必要があります。

詳細については、シャーシ内のサーバ スロットの再確認, （592 ページ）を参照してください。

ブレード サーバの再稼動

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 [Chassis] ノードをクリックします。

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

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

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

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ブレードサーバを解放した場合、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。

存在しないブレードサーバの設定データベースからの削除

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

サーバを物理的に削除する場合は、シャーシからのサーバの削除, （590 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、[Remove] をクリックし、[OK] をクリックします。
Cisco UCS Manager は、設定データベースからそのサーバに関するすべてのデータを削除します。サーバ スロットは、新しいサーバ ハードウェアの挿入に使用できます。

ブレード サーバのロケータ LED の切り替え

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

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

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、[Reset CIMC (Server Controller)] をクリックし、[OK] をクリックします。

ブレード サーバの破損した BIOS の復旧

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で使用できない場合、サーバの BIOS を更新および起動する手順を実行してください。

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
[アクティブ化するバージョン] 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

システムが応答しないままになっており、Cisco UCS Manager で、CIMC から Non Maskable Interrupt（NMI）を BIOS またはオペレーティング システムに発行する必要がある場合は、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

手順

ステップ 1 [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。

ヘルス LED アラーム

ブレード ヘルス LED は、各 Cisco UCS B シリーズ ブレード サーバの前面にあります。 Cisco UCS Manager では、センサー故障が発生すると、ブレード ヘルス LED が緑色からオレンジ色またはオレンジ色の点滅に変化します。

ヘルス LED アラームには次の情報が表示されます。

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

ヘルス LED アラームの表示

手順

ステップ 1 [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 ヘルス LED アラーム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、[View Health LED Alarms] をクリックします。
[View Health LED Alarms] ダイアログボックスに、選択したサーバのヘルス LED アラームが一覧表示されます。

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

第 37 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，600 ページ
- ラックマウント サーバの削除および解放に関するガイドラインと推奨事項，600 ページ
- 予期しないサーバ電力変更を回避するための推奨事項，601 ページ
- ラックマウント サーバのブート，602 ページ
- ラックマウント サーバのシャット ダウン，604 ページ
- ラックマウント サーバのリセット，605 ページ
- ラックマウント サーバの再確認，606 ページ
- ラック サーバからのインバンド設定の削除，606 ページ
- ラックマウント サーバの解放，607 ページ
- ラックマウント サーバの再稼動，607 ページ
- ラックマウント サーバの番号付け直し，608 ページ
- 存在しないラックマウント サーバの設定データベースからの削除，608 ページ
- ラックマウント サーバのロケータ LED の切り替え，609 ページ
- ラックマウント サーバの CMOS のリセット，609 ページ
- ラックマウント サーバの CIMC のリセット，610 ページ
- ラックマウント サーバの破損した BIOS の復旧，610 ページ
- ラックマウント サーバの POST 結果の表示，611 ページ
- ラックマウント サーバからの NMI の発行，612 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。 電力制限を除くすべての管理およびモニタリング機能が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一部のラックマウント サーバ管理タスクは、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　サポート対象の 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、使用している Cisco UCS Manager のリリースに応じた Cisco UCS C シリーズ サーバのインストール 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解放に関するガイドラインと推奨事項

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

ラックマウント サーバの解放

解放は、ラックマウント サーバが物理的に存在し接続しているときに、一時的に設定から削除する場合に実行します。 解放された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ので、サーバの情報部分は、将来の使用に備え、Cisco UCS Manager によって保持されます。

ラックマウント サーバの削除

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

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

（注）　自動的に削除されるのは、検出時に自動的にサーバプールに追加されたサーバだけです。 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 サーバを再び設定に追加する場合は、それを再び接続して検出する必要があります。 Cisco UCS Manager に再導入したサーバは、新しいサーバとして処理され、詳細な検出プロセスが実施されます。 このため、Cisco UCS Manager によって以前とは異なる新しい ID がサーバに割り当てられることがあります。

予期しないサーバ電力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は、サーバの物理的な [Power] 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、サーバの電源状態の変更は次の方法でのみ行う必要があります。

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

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

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

現在電源がオフになっているサーバに対して、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、サーバの実際の電力状態がサービス プロファイルで必要とされる電源状態の設定と同期しなくなる可能性があります。 サーバと 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 によって、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場合があり、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	通信が中断された後のサーバの電源状態
Up	Powered Off	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	通信が中断された後のサーバの電源状態
Down	電源オン	電源オン （注） 実行中のサーバは、サービス プロファイルに必要とされる電源状態に関係なくシャットダウンされません。

ラックマウント サーバのブート

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 システムにより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 システムにより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） 電源切断状態からサーバをブートする場合は、[Reset] を使用しないでください。

この手順を使用して電源投入を続けると、サーバの望ましい電源状態が実際の電源状態と同期しなくなり、サーバが後で予期せずシャットダウンすることがあります。 選択したサーバを電源切断状態から安全にリブートするには、[Cancel] をクリックし、[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 はサーバの接続を解除し、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 サーバからのインバンド設定の削除

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

手順

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

ステップ 2 [Equipment] タブで、[Equipment] > [Rack-Mounts] > [Servers] > *[Server Name]* を展開します。

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

ステップ 4 [CIMC] サブタブをクリックします。

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

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

サーバのインバンド設定が削除されます。

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

ラックマウント サーバの解放

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、[Decommission] をクリックし、[OK] をクリックします。サーバが Cisco UCS の設定から削除されます。

ラックマウント サーバの再稼動

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

ラックマウント サーバの番号付け直し

はじめる前に

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

手順

ステップ 1 [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、以下が含まれていないことを確認します。

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

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

ステップ 4 番号を付け直すラックマウント サーバを選択します。

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

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

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

a) [ID] フィールド内でダブルクリックし、ラックマウント サーバに割り当てる新しい番号を入力します。

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

c) [Save Changes] をクリックします

ステップ 8 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） サーバの再稼動と検出の進行状況を、そのサーバの [FSM] タブでモニタします。

存在しないラックマウントサーバの設定データベースからの削除

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

手順

ステップ 1 [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、[Remove] をクリックし、[OK] をクリックします。
Cisco UCS Manager は、設定データベースからそのサーバに関するすべてのデータを削除します。サーバ スロットは、新しいサーバ ハードウェアの挿入に使用できます。

ラックマウント サーバのロケータ LED の切り替え

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、[Reset CMOS] をクリックし、[OK] をクリックします。

ラックマウント サーバの 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、[Reset CIMC (Server Controller)] をクリックし、[OK] をクリックします。

ラックマウント サーバの破損した BIOS の復旧

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、[Recover Corrupt BIOS] をクリックし、[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、アクティブにするバージョンを指定し、[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

システムが応答しないままになっており、Cisco UCS Manager で、CIMC から Non Maskable Interrupt（NMI）を BIOS またはオペレーティング システムに発行する必要がある場合は、次の手順を実行します。このアクションにより、サーバにインストールされているオペレーティング システム応じて、コア ダンプまたはスタック トレースが作成されます。

手順

ステップ 1 [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 [Diagnostic Interrupt] をクリックし、[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

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，613 ページ
- サーバからの [KVM Console]KVM コンソールの起動，619 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，620 ページ
- KVM Launch Manager からの KVM コンソールの起動，621 ページ
- [Cisco UCS KVM Direct] Web ページからの KVM コンソールの起動，622 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。

KVM コンソールを使用してサーバにアクセスする場合は、サーバまたはサーバに関連付けられているサービス プロファイルのいずれかに CIMC IP アドレスが設定されていることを確認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、そ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 のインストールに KVM コンソールを使用する場合の推奨事項

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。 遠隔地のサーバから接続して制御し、この KVM セッション中にアクセスできる仮想ドライブに物理ロケーションをマッピングすることができます。

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 Console] 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。 このタブで使用可能なメニューオプションは以下のとおりです。

[File] メニュー

メニュー項目	説明
[Capture to File] ボタン	現在の画面を JPG 画像として保存できる [Save] ダイアログ ボックスを開きます。
[Exit] ボタン	KVM コンソールを閉じます。

の [View] メニュー

メニュー項目	説明
[Refresh] ボタン	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。
[Fit] ボタン	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コンソール ウィンドウのサイズを変更します。 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。
[Video Scaling] ボタン	コンソール ウィンドウ内に全体が収まるようにビデオ映像のサイズを決定します。
[Full Screen] ボタン	画面全体になるように KVM コンソールを拡大します。
[Mini Mode] ボタン	ホスト サーバのサムネイル ビューを表示し、キーボード、マウスの入力を無効にします。

[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。

メニュー項目	説明
[Server Macros] メニュー	Cisco IMC からダウンロードされたサーバ サイド マクロがある場合、表示します。 サーバ サイド マクロがダウンロードされていない場合、このメニュー項目は無効になります。
[Static Macros] メニュー	マクロの定義済みのセットを表示します。
[User Defined Macros] メニュー	作成済みのユーザ定義マクロを表示します。
[Manage] ボタン	マクロの作成および管理ができる [Configure User Defined Macros] ダイアログ ボックスを開きます。 システム定義されたマクロは削除できません。

[Tools] メニュー

メニュー項目	説明
[Session Options] ボタン	構成設定のための、以下のタブを含む [Session Options] ダイアログ ボックスを開きます。 • [General] タブ：コンソールが Windowed モードの場合に、すべてのキーストロークをターゲット システムに送るかどうか。 デフォルトは no です。 • [Mouse] タブ：ターゲット システムで使用します。 以下の項目を指定できます。 ◦ [Termination Key]：シングル カーソル モードを終了するために使用するキー。 デフォルトは F12 です。 ◦ [Mouse Acceleration]：USB マウスの位置決めを変更できます。 デフォルトは [Absolute Positioning] です。 • [Security] タブ：ユーザの同意なしで受け入れるセキュアでない接続の種類を決定します。また、以前に受け入れた接続をクリアできます。 • [Scaling] タブ：コンソールが Windowed モードまたは全画面モードのときにアスペクト比メンテナンスを有効にするかどうか。 デフォルトは、[Windowed Mode] です。 • [Mini-Mode] タブ：ミニモードのときの KVM/vMedia クライアントのサイズを決めます。 • [Certificate] タブ：現在のセッションで使用される証明書の詳細を表示します。エクスポートされる証明書ファイルの名前とパスを設定できます。
[Single Cursor] ボタン	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位置決めの問題を補正するシングル 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 ポインタの位置がビューワ ウィンドウ内に制限されます。 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。 デフォルトは F12 です。

メニュー項目	説明
[Stats] ボタン	以下の項目を表示する [Stats] ダイアログ ボックスを開きます。 • KVM セッションの統計情報 • フレーム レート。単位は、フレーム数/秒です。 • 帯域幅。単位は、KB/秒です。 • 圧縮率。単位は、使用される圧縮パーセンテージです。 • パケット レート。単位は、パケット/秒です。 vMedia がアクティヴになると、[Stats] ダイアログ ボックスに以下の項目が表示されます。 • vMedia の転送速度。1 秒間に転送されたデータ量です。 • ホスト サーバのデバイスがマッピングされているローカルのデバイスまたはイメージ ファイルの種類。 • マッピングするデバイスの経過時間。 • サーバで送受信されたバイト数。 • サーバに接続されたすべての USB デバイスをリセットするための [USB Reset] ボタン
[Session User List] ボタン	アクティブ KVM セッションを持つすべてのユーザ ID を表示する [Session User List] ダイアログ ボックスを開きます。
[Chat] ボタン	仮想コンソール ビューワで使用できるチャット インターフェイスを通じて、他の仮想コンソール ユーザと通信します。チャットはすべての Cisco UCS サーバでサポートされているわけではありません。 （注） チャット ウィンドウは最小化できず、ウィンドウを閉じるとチャット履歴は保存されません。 サーバの電源をオフにしてもチャットはできます。

[Virtual Media] メニュー

名前	説明
[Create Image]	[Create Image from Folder] ダイアログ ボックスが開き、ユーザがローカル フォルダにマップするサーバのフォルダのイメージを作成できます。 システムはイメージを作成すると、ユーザのシステム上に IMG ファイルを保存します。
[Activate Virtual Devices]	vMedia セッションをアクティブにし、ユーザがローカル コンピュータまたはネットワークから、ドライブまたはイメージファイルをアタッチできるようにします。 （注） セキュアでない接続を許可していない場合は、セッションを受け入れるためのプロンプトが表示されます。セッションを拒否すると、その仮想メディア セッションは終了します。
[Map CD/DVD]	ユーザがアクセスする CD/DVD を選択し、[Map Device] ボタンをクリックしてそれをホスト サーバのデバイスにマップします。 （注） [Read Only] チェックボックスがオンの場合、デバイスに書き込み機能があってもサーバはその vMedia デバイスに書き込むことができません。
[Map Removable Disk]	ユーザがアクセスするリムーバブル ディスクを選択し、[Map Device] ボタンをクリックしてそれをホスト サーバのデバイスにマップします。 （注） [Read Only] チェックボックスがオンの場合、デバイスに書き込み機能があってもサーバはその vMedia デバイスに書き込むことができません。
[Map Floppy]	ユーザがアクセスするフロッピーを選択し、[Map Device] ボタンをクリックしてそれをホスト サーバのデバイスにマップします。 （注） [Read Only] チェックボックスがオンの場合、デバイスに書き込み機能があってもサーバはその vMedia デバイスに書き込むことができません。

KVM ダイレクト アクセス

KVM ダイレクト アクセスにより、ユーザの Cisco UCS Manager ドメイン内のブレードおよびラック サーバを管理する管理者は、Web ブラウザを使用してサーバの KVM に直接アクセスすることができます。 この機能により、管理者に彼らが管理するサーバの KVM コンソールへのアクセスを許可する一方で、ファブリック インターコネクトの IP アドレスへのアクセスを制限することができます。

（注） アウトオブバンド IPv4 管理インターフェイス アドレスのみが KVM ダイレクト アクセスに対してサポートされます。

KVM ダイレクト アクセスは、ユーザが Cisco UCS Manager GUI インターフェイスまたは KVM Launch Manager を使用せずにサーバの管理 IP アドレスに移動できるカスタム アプリケーションもサポートします。

KVM ダイレクト アクセスは、サーバに直接割り当てられた管理 IP アドレス、またはサービス プロファイルによってサーバに関連付けられた管理 IP アドレスをサーバの管理者に提供することでサポートされます。 サーバ管理者は、ブラウザに IP アドレスを入力し、Cisco UCS KVM Direct ログイン ページに移動します。 ログイン ページで、ユーザはユーザ名とパスワードを入力し、認証ドメインを選択します。 Cisco UCS KVM Direct を起動すると、Cisco UCS Manager GUI からサーバにアクセスした場合と同様に、サーバのコンソールが表示されます。

KVM ダイレクト アクセスは、認証に自己署名証明書を使用します。 ユーザがサーバの管理 IP アドレスまたはサービス プロファイルの IP アドレスに初めてアクセスしたときに、警告ダイアログ ボックスが表示され、ブラウザのキャッシュに証明書の例外を追加する必要があることが告げられます。

Cisco UCS KVM ダイレクト アクセスをサポートするデフォルトの通信サービスは HTTPS です。これは無効化できません。 ユーザがアドレスの一部として HTTP を使用してブラウザで管理 IP を入力すると、HTTPS サービスに自動的にリダイレクトされます。

KVM ダイレクト アクセスに対応するには、Cisco UCS Manager で CIMC Web サービス（通信サービス）が有効になっていることを確認してください。

（注） CIMC Web サービスは、Cisco UCS Manager ではデフォルトで有効になっています。

サーバからの [KVM Console]KVM コンソールの起動

サーバに割り当てられたアドレスを使用して複数の KVM コンソール セッションを開始できます。

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 [KVM Console]**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] の右側の [>>] ボタンをクリックします。
別のウィンドウで [**KVM コンソール**] が開き、サーバに関連付けられている使用可能なアウトオブバンド アドレスおよびインバンド アドレスのリストが表示されます。

（注） [>>] ボタンではなく [KVM Console] をクリックすると、セッションは、最初がインバンド IPv6、2 番目がインバンド IPv4、3 番目がアウトオブバンド IPv4 の優先順序でサーバ アドレスを使用して起動します。

ステップ 6 [Select IP Address] リストからアドレスを選択します。
[(Inband)] と表示されるアドレスは、アップリンク ポート経由でサーバにアクセスし、[(Outband)] と表示されるアドレスは、管理インターフェイスのポート経由でサーバにアクセスします。

ステップ 7 [OK] をクリックします。
KVM コンソールは、選択したアドレスを使用して起動します。

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 Caps Lock キーをオフにすると、[KVM Console]**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 Console]**KVM コンソール**にフォーカスがない状態で Caps Lock キーを 1 度押し、次に [KVM Console]**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。

ステップ 8 同じサーバの別の KVM セッションを開始するには、ステップ 5 ～ 7 を繰り返します。
別の KVM セッションが開始されます。 設定されているアドレスの数に応じて、サーバに対して最大 6 つのセッションを開始できます。

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 コンソールを起動するサービス プロファイルを含む組織のノードを展開します。
システムにマルチテナント機能が備えられていない場合は、[root] ノードを展開します。

ステップ 4 関連付けられているサーバへの KVM のアクセスが必要なサービス 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] の右側の [>>] ボタンをクリックします。
別のウィンドウで [**KVM コンソール**] が開き、サーバに関連付けられている使用可能なアウトオブバンド アドレスおよびインバンド アドレスのリストが表示されます。

（注） [>>] ボタンではなく [KVM Console] をクリックすると、セッションは、最初がインバンド IPv6、2 番目がインバンド IPv4、3 番目がアウトオブバンド IPv4 の優先順序でサーバ アドレスを使用して自動的に起動します。

ステップ 7 [Select IP Address] リストからアドレスを選択します。
[(Inband)] と表示されるアドレスは、アップリンク ポート経由でサーバにアクセスし、[(Outband)] と表示されるアドレスは、管理インターフェイスのポート経由でサーバにアクセスします。

ステップ 8 [OK] をクリックします。
KVM コンソールは、選択したアドレスを使用して起動します。

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 Caps Lock キーをオフにすると、[KVM Console]**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 Console]**KVM コンソール**にフォーカスがない状態で Caps Lock キーを 1 度押し、次に [KVM Console]**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。

ステップ 9 同じサーバの別のセッションを開始するには、ステップ 6 ～ 8 を繰り返します。
別の KVM セッションが開始されます。 設定されているアドレスの数に応じて、サーバに対して最大 6 つのセッションを開始できます。

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：

HTTP アクセスのデフォルトの Web リンクは、IPv4 アドレスの場合は `http://UCSManager_IP`、IPv6 アドレスの場合は `http://UCSManager_IP6` です。 HTTPS アクセスのデフォルトの Web リンクは、IPv4 アドレスの場合は `https://UCSManager_IP`、IPv6 アドレスの場合は `https://UCSManager_IP6` です。 スタンドアロン設定では、*UCSManager_IP* または *UCSManager_IP6* はそれぞれ、ファブリック インターコネクトの管理ポートの IPv4 アドレスまたは IPv6 アドレスです。 クラスタ設定では、*UCSManager_IP* または *UCSManager_IP6* はそれぞれ、Cisco UCS Manager に割り当てられた IPv4 アドレスまたは IPv6 アドレスです。

ステップ 2 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 Caps Lock キーをオフにすると、[KVM Console]**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 Console]**KVM コンソール**にフォーカスがない状態で Caps Lock キーを 1 度押し、次に [KVM Console]**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。

[Cisco UCS KVM Direct] Web ページからの KVM コンソールの起動

Cisco UCS KVM Direct] のログイン ページでは、Cisco UCS Manager にログインせずに Web ブラウザから直接サーバにアクセスできます。

はじめる前に

Cisco UCS KVM Direct] のログイン ページを使用してサーバの 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 のユーザ名とパスワード。
- アクセスするサーバのサーバ CIMC またはサービス プロファイル IPv4 管理アドレス。

手順

ステップ 1 Webブラウザで、アクセスするサーバの管理IPアドレスのWebリンクを入力または選択します。

ステップ 2 [Security Alert] ダイアログボックスが表示されたら、[Yes] をクリックしてセキュリティ例外を作成します。
セキュリティ例外はブラウザのキャッシュに永続的に保存されます。

ステップ 3 Cisco UCS [KVM Direct] ダイアログボックスで、名前、パスワード、およびドメインを指定します。

ステップ 4 [Lauch KVM] をクリックします。
KVM コンソールが起動します。

第 39 章

CIMC セッション管理

この章の内容は、次のとおりです。

- CIMC セッション管理，625 ページ

CIMC セッション管理

Cisco UCS Manager 内の KVM、vMedia、および SoL セッションを表示および終了できます。 管理者権限を持つユーザは、任意のユーザの KVM、vMedia、および SoL セッションを切断できます。 . Cisco Integrated Management Controller（CIMC）により、セッション情報が Cisco UCS Manager に提供されます。 Cisco UCS Manager は CIMC からイベントを取得すると、そのセッション テーブルを更新し、すべてのユーザに情報を表示します。

セッション情報は次のとおりです。

- 名前：セッションを開始したユーザの名前。
- セッション ID：セッションに関連付けられた ID。 ブレードのセッション ID の形式は [unique identifier] _ [chassis id] _ [Blade id] です。 ラックのセッション ID の形式は [unique identifier] _ 0 _ [Rack id] です。
- セッション タイプ：KVM、vMedia、または SoL。
- ユーザの権限レベル：読み取り/書き込み、読み取り専用、または付与。
- 管理状態：アクティブまたは非アクティブ。 値は、セッションがアクティブの場合はアクティブです。 値は、セッション終了コマンドが発行されたが、セッションが終了していない場合は非アクティブとなります。 この状況は、サーバの FSM が別の操作で進行中である場合、または CIMC への接続が失われた場合に発生します。
- 送信元アドレス：セッションが開かれたコンピュータの IP アドレス。
- サービス プロファイル：セッションに関連付けられたサービス プロファイル。 CIMC セッションのサービス プロファイルの属性値は、セッションがサービス プロファイルから提供された IP アドレスで開くときにだけ表示されます。

- サーバ：セッションに関連付けられたサーバの名前。
- ログイン時刻：セッションが開始された日時。
- 最終更新時刻：セッション情報が CIMC により更新された最終時刻。

新しいセッションは通常、ユーザがKVM、vMedia、またはSOLに接続するときに追加されます。Pnuos vMedia セッションは、ユーザ名 __vmediausr__ を用いたサーバ検出時にセッション テーブルに表示されます。

CIMC セッション データは Cisco UCS Manager GUI の [CIMC Sessions] タブで使用できます。 ユーザによって終了された CIMC セッションは、適切な詳細とともにログに記録された監査です。

（注） このガイドに記載されている GUI および CLI タスクを実行するには、2.1(2a) 以上の CIMC イメージ バージョンがブレード サーバのセッション管理サポートに必要です。 1.5(1l) 以上の最新の CIMC イメージ バージョンが、ラック サーバに必要です。

すべての CIMC セッションの表示

ここでは、Cisco UCS Manager でグローバルに開かれている CIMC セッションの表示方法を 1 つ説明します。 ローカル ユーザ、リモート ユーザ、IPMI ユーザによって開かれたすべてのサーバの CIMC セッションを表示できます。

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、[User Management] > [User Services] の順にクリックします。

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

サーバの CIMC セッションの表示

ここでは、特定のサーバの CIMC セッションの表示方法について説明します。 サーバおよびサービス プロファイルで開かれている CIMC セッションを表示できます。

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

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

サービス プロファイルの CIMC セッションの表示

ここでは、特定のサービス プロファイルの CIMC セッションの表示方法について説明します。

（注） サービス プロファイルの下に CIMC セッションが表示されるのは、そのサービス プロファイルで指定された IP アドレスで CIMC セッションが開かれた場合だけです。

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] > [Root] > *[Service Profile Name]* を展開します。

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

ローカル ユーザによって開かれた CIMC セッションの表示

ここでは、ローカル ユーザによって開かれた CIMC セッションの表示方法について説明します。

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] > [User Services] > [Locally Authenticated Users] > *[User Name]* の順に展開します。

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

リモート ユーザによって開かれた CIMC セッションの表示

ここでは、リモート ユーザによって開かれた CIMC セッションの表示方法について説明します。

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] > [User Services] > [Remotely Authenticated Users] > *[User Name]* の順に展開します。

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

開いているすべての CIMC セッションのクリア

このタスクでは、開いているすべての CIMC セッションをクリアする方法を示します。 ローカル、リモート、および IPMI ユーザが開いているすべてのサーバとサービスプロファイルの CIMC セッションをクリアできます。

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] タブの [User Management] をクリックします。

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

ステップ 4 クリアする CIMC セッションを選択して右クリックし [Clear CIMC Session] 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。

サーバの CIMC セッションのクリア

このタスクでは、サーバの CIMC セッションをクリアする方法について説明します。 サーバ上で開いている 1 つ以上の CIMC セッションをクリアできます。

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、[Servers] > *[Server Name]* を展開します。

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

ステップ 4 クリアする CIMC セッションを選択して右クリックし、[Clear CIMC Session] 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 プロファイルの CIMC セッションのクリア

このタスクは、サービス プロファイルの CIMC セッションをクリアする方法について説明します。 サービス プロファイルで提供されている IP アドレスで開いている 1 つ以上の CIMC セッションをクリアできます。

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] > [root] > *[Service Profile Name]* を展開します。
ステップ 3 [Work] ペインの [CIMC Sessions] タブをクリックします。
ステップ 4 クリアする CIMC セッションを選択して右クリックし、[Clear CIMC Session] 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 ユーザの CIMC セッションのクリア

このタスクは、ローカル ユーザの CIMC セッションをクリアする方法について説明します。 ローカル ユーザが開いている、1 つ以上の CIMC セッションをクリア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 [Admin] タブで、[User Services] > [Locally Authenticated Users] > *[User Name]* を展開します。
ステップ 3 [Work] ペインで、[General] タブをクリックします。
ステップ 4 [General] タブ下で、[CIMC Sessions] セクションを展開します。
ステップ 5 クリアする CIMC セッションを選択して右クリックし [Clear CIMC Session] 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。

リモート ユーザの CIMC セッションのクリア

このタスクでは、リモート ユーザの CIMC セッションをクリアする方法について説明します。 リモート ユーザによって開かれている、1 つ以上の CIMC セッションをクリアできます。

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、[User Services] > [Remotely Authenticated Users] > *[User Name]* を展開します。

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

ステップ 4 [General] タブ下で、[CIMC Sessions] セクションを展開します。

ステップ 5 クリアする CIMC セッションを選択して右クリックし、[Clear CIMC Session] 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 40 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，631 ページ
- バックアップ タイプ，632 ページ
- バックアップ操作の考慮事項と推奨事項，632 ページ
- スケジュール バックアップ，633 ページ
- Import Configuration，634 ページ
- インポート方法，634 ページ
- システムの復元，635 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，635 ページ
- バックアップ操作の設定，636 ページ
- スケジュール バックアップの設定，642 ページ
- インポート操作の設定，646 ページ
- ファブリック インターコネクトの設定の復元，651 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 Manager および Cisco UCS Central で、次のバックアップのタイプのうちの 1 つ以上を実行できます。

- [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。

（注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

- [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

バックアップ場所とは、Cisco UCS Manager でバックアップ 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 ファイル上書きの可能性

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 Manager 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。

バックアップの複数のタイプ

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。

スケジュール 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ができます。 Cisco UCS Manager 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。

増分バックアップ

Cisco UCS Manager または Cisco UCS Central の増分バックアップを実行できません。

完全な状態のバックアップの暗号化

パスワードなどの機密情報がクリア テキストでエクスポートされることがないように、完全な状態のバックアップは暗号化されます。

スケジュール 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 にポリシーを設定できます。

- Full ステート
- All 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。

Full State バックアップ ポリシー

Full State バックアップ ポリシーを使用すると、システム全体のスナップショットの定期的な Full State バックアップをスケジュールすることができます。 Full State バックアップを行う間隔は、日単位、週単位、または隔週単位で設定できます。

Cisco UCS Manager 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。 maxfiles パラメータは、Cisco UCS Manager を Cisco UCS Central に登録するときに使用されます。 maxfiles

パラメータは Cisco UCS Central でユーザが設定できるパラメータで、Cisco UCS Central に保存するバックアップ ファイルの数を制御します。

Cisco UCS Manager が Cisco UCS Central に登録されておらず、ユーザがリモート バックアップ サーバにバックアップ ファイルを保存している場合、バックアップ ファイルは Cisco UCS Manager によって管理されません。 リモート マシンのサーバ管理者は、ディスク使用率を監視してバックアップ ファイルのローテンションを行い、新しいバックアップ ファイル用の領域を確保する必要があります。

All Configuration エクスポート ポリシー

All Configuration バックアップ ポリシーでは、定期的なバックアップをスケジュールし、すべてのシステム設定と論理設定をエクスポートできます。 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。 All Configuration バックアップを行う間隔は、日単位、週単位、または隔週単位で設定できます。

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 は最も古いバックアップ ファイルを上書きします。

Import Configuration

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たものであ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 vNIC 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 ファイルに対するインポート操作は実行されません。

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により、Cisco UCS を介してシステム設定をインポートしてアップデートできます。

- [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。 情報が一致しない場合は、インポートしたコンフィギュレーション ファイルの情報によって 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、および I/O モジュールまたは FEX 接続を含めて、同じまたは同様のシステム設定およびハードウェアを持つシステム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が一致しない場合、復元されたシステムが完全には機能しないことがあります。 2 つのシステムの I/O モジュール リンク間またはサーバ間に不一致がある場合は、復元操作後にシャーシまたはサーバまたはそ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。

（注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

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 IPv4 アドレスまたは IPv6 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 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。 （注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。 • [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。
[プロトコル] 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] • [USB A]：ファブリック インターコネクト A に装着された USB ドライブ。 • [USB B]：ファブリック インターコネクト B に装着された USB ドライブ。
[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（IPv4 または IPv6）。 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） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で 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 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

名前	説明
[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。
[ユーザ] 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。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[パスワード] フィールド	リモート サーバのユーザ名のパスワード。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。 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 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 [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。

（注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。

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 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 [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 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 [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

Full State 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 IPv4 アドレスまたは IPv6 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] ペインで、[Backup and Export Policy] タブをクリックします。

ステップ 4 [Full State Backup Policy] 領域で、次のフィールドに入力します。

名前	説明
[Hostname] フィールド	ポリシーのバックアップ 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（IPv4 または IPv6）。 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） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で 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 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

名前	説明
[プロトコル] 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] • [USB A]：ファブリック インターコネクト A に装着された USB ドライブ。 • [USB B]：ファブリック インターコネクト B に装着された USB ドライブ。
[ユーザ] 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。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[パスワード] フィールド	リモート サーバのユーザ名のパスワード。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[Remote File] フィールド	ポリシーのバックアップ 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] フィールドで指定された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 Files] 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。

名前	説明
[Description] フィールド	バックアップ ポリシーの説明。 デフォルトの説明は [Database Backup Policy] です。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 5 [Save Changes] をクリックします。

All Configuration 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 IPv4 アドレスまたは IPv6 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] ペインで、[Policy Backup & Export] タブをクリックします。

ステップ 4 [Config Export Policy] 領域で、次のフィールドに入力します。

名前	説明
[Hostname] フィールド	設定のバックアップ 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（IPv4 または IPv6）。 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） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で 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 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。

名前	説明
[プロトコル] 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] • [USB A]：ファブリック インターコネクト A に装着された USB ドライブ。 • [USB B]：ファブリック インターコネクト B に装着された USB ドライブ。
[ユーザ] 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。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[パスワード] フィールド	リモート サーバのユーザ名のパスワード。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[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] フィールドで指定された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 Files] フィールド	Cisco UCS Manager が保持する設定のバックアップ ファイルの最大数。 この値は変更できません。

名前	説明
[Description] フィールド	設定のエクスポート ポリシーの説明。デフォルトの説明は [Configuration Export Policy] です。 256 文字以下で入力します。 次を除く任意の文字またはスペースを使用できます。`（アクセント記号）、\（円記号）、^（カラット）、"（二重引用符）、=（等号）、>（大なり）、<（小なり）、または'（一重引用符）は使用できません。

ステップ 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。

- All コンフィギュレーション
- システム設定
- Logical 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] をクリックするとただちに、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が実行されません。 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。
[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ています。 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ています。 Cisco UCS Manager GUI に [Filename] フィールドとそれに関連する [Browse] ボタンが表示され、インポートするバックアップファイルの名前と場所を指定できます。

名前	説明
[プロトコル] 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] • [USB A]：ファブリック インターコネクト A に装着された USB ドライブ。 • [USB B]：ファブリック インターコネクト B に装着された USB ドライブ。
[Hostname] フィールド	コンフィギュレーション ファイルのインポート元のホスト名、IPv4 または IPv6 アドレス。 （注） IPv4 または IPv6 アドレスではなくホスト名を使用する場合、 で 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 管理が [Local] に設定されている場合は、Cisco UCS Manager で DNS サーバを設定します。 Cisco UCS ドメイン Cisco UCS Central に登録されていないか、DNS 管理が [Global] に設定されている場合は、Cisco UCS Central で DNS サーバを設定します。
[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。
[ユーザ] 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。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。
[パスワード] フィールド	リモート サーバのユーザ名のパスワード。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。 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。

- All コンフィギュレーション
- システム設定
- Logical 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コンフィギュレーション 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 IPv4 アドレスとサブネット マスク、または IPv6 アドレスとプレフィックス
- デフォルトのゲートウェイの IPv4 アドレスまたは IPv6 アドレス
- バックアップ サーバの IPv4 アドレスまたは IPv6 アドレスと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 IPv4 アドレスまたは IPv6 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 マスクまたはプレフィックス
- 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 IPv4 アドレスまたは IPv6 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IPv4アドレスまたはIPv6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。 （注） Full State バックアップ ファイルを使用した場合にのみ、バックアップ ファイルのエクスポート元のシステムと同じバージョンを実行しているシステムを復元できます。
ユーザ 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。 このフィールドは、プロトコルがTFTPまたはUSBの場合は適用されません。
パスワード	リモート サーバのユーザ名のパスワード。 このフィールドは、プロトコルが TFTP または USB の場合は適用されません。

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 41 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，655 ページ

失われたパスワードの復旧

amin 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。

他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

次の手順に従って、Cisco UCS ドメイン内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-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

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-mini-k9-system.5.0.3.N2.3.01a.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-mini-k9-kickstart.5.0.3.N2.3.01a.bin
```

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-mini-k9-system.5.0.3.N2.3.01a.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
```